

H3C MSR 5600 路由器

二层技术-广域网接入配置指导(V7)

新华三技术有限公司
<http://www.h3c.com>

资料版本：6W400-20200429
产品版本：MSR-CMW710-R0809

Copyright © 2020 新华三技术有限公司及其许可者 版权所有，保留一切权利。

未经本公司书面许可，任何单位和个人不得擅自摘抄、复制本书内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

由于产品版本升级或其他原因，本手册内容有可能变更。**H3C** 保留在没有任何通知或者提示的情况下对本手册的内容进行修改的权利。本手册仅作为使用指导，**H3C** 尽全力在本手册中提供准确的信息，但是 **H3C** 并不确保手册内容完全没有错误，本手册中的所有陈述、信息和建议也不构成任何明示或暗示的担保。

前言

本配置指导主要介绍广域网协议的原理及配置，包括 ATM、PPP、帧中继、HDLC、L2TP 等。
前言部分包含如下内容：

- [读者对象](#)
- [本书约定](#)
- [资料意见反馈](#)

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。
<i>斜体</i>	命令行参数（命令中必须由实际值进行替代的部分）采用 <i>斜体</i> 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择一个或者不选。
{ 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择一个、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
1.1 PPP简介	1-1
1.1.1 PPP协议	1-1
1.1.2 PPP链路建立过程	1-1
1.1.3 PPP认证	1-2
1.1.4 PPP支持IPv4	1-3
1.1.5 PPP支持IPv6	1-3
1.1.6 协议规范	1-4
1.2 PPP与硬件适配关系	1-4
1.3 PPP配置任务简介	1-4
1.4 配置接口封装PPP协议	1-5
1.5 配置虚拟模板接口	1-6
1.5.1 创建虚拟模板接口	1-6
1.5.2 恢复当前虚拟模板接口的缺省配置	1-6
1.5.3 配置处理虚拟模板接口流量的slot	1-7
1.6 配置PPP认证	1-8
1.6.1 功能简介	1-8
1.6.2 配置PAP认证	1-8
1.6.3 配置CHAP认证（认证方配置了用户名）	1-9
1.6.4 配置CHAP认证（认证方未配置用户名）	1-10
1.6.5 配置MSCHAP或MSCHAPv2 认证	1-10
1.7 配置轮询功能	1-11
1.8 配置PPP协商参数	1-12
1.8.1 配置协商超时时间间隔	1-12
1.8.2 配置Client端PPP协商IP地址	1-13
1.8.3 配置Server端PPP协商IP地址	1-13
1.8.4 配置接口IP网段检查	1-17
1.8.5 配置Client端DNS服务器地址协商	1-17
1.8.6 配置Server端DNS服务器地址协商	1-17
1.8.7 配置ACFC协商	1-18
1.8.8 配置PFC协商	1-19
1.9 配置PPP IPHC压缩功能	1-19
1.10 配置PPP用户的nas-port-type属性	1-20

1.11 配置PPP计费统计功能	1-21
1.12 配置PPP接入用户日志信息功能	1-21
1.13 PPP显示和维护	1-22
1.14 PPP典型配置举例	1-23
1.14.1 PAP单向认证配置举例	1-23
1.14.2 PAP双向认证配置举例	1-24
1.14.3 CHAP单向认证配置举例	1-26
1.14.4 在接口下指定为Client端分配的IP地址配置举例	1-29
1.14.5 从接口下指定的PPP地址池中分配IP地址配置举例	1-30
1.14.6 从ISP域下关联的PPP地址池中分配IP地址配置举例	1-31
2 MP	2-1
2.1 MP简介	2-1
2.1.1 MP主要作用	2-1
2.1.2 MP支持的接口类型	2-1
2.2 MP配置任务简介	2-1
2.3 配置通过虚拟模板接口进行MP捆绑	2-2
2.3.1 功能简介	2-2
2.3.2 配置限制和指导	2-2
2.3.3 通过虚拟模板接口进行MP捆绑配置任务简介	2-2
2.3.4 创建虚拟模板接口	2-2
2.3.5 将物理接口或用户名与虚拟模板接口关联	2-3
2.3.6 配置MP参数	2-4
2.4 配置通过MP-group接口进行MP捆绑	2-5
2.4.1 功能简介	2-5
2.4.2 通过MP-group接口进行MP捆绑配置任务简介	2-5
2.4.3 创建MP-group接口	2-5
2.4.4 将物理接口加入MP-group接口	2-5
2.4.5 配置MP参数	2-6
2.4.6 恢复当前MP-group接口的缺省配置	2-7
2.5 配置DDR链路的MP参数	2-7
2.6 配置MP捆绑模式	2-8
2.7 配置MP短序协商方式	2-9
2.8 配置MP Endpoint选项	2-9
2.9 配置链路分片与交叉	2-10
2.10 MP显示和维护	2-11
2.11 MP典型配置举例	2-11

2.11.1 通过将物理接口直接绑定到VT接口方式进行MP捆绑配置举例	2-11
2.11.2 通过按用户名找VT方式进行MP捆绑配置举例	2-13
2.11.3 通过将链路绑定到MP-group接口方式进行MP捆绑配置举例	2-16
3 PPPoE	2-1
3.1 PPPoE简介	2-1
3.1.1 PPPoE组网结构	2-1
3.1.2 协议规范	2-2
3.2 PPPoE与硬件适配关系	2-2
3.3 PPPoE配置限制和指导	2-2
3.4 配置PPPoE Server	2-3
3.4.1 PPPoE Server配置任务简介	2-3
3.4.2 配置PPPoE会话	2-3
3.4.3 配置VA池	2-4
3.4.4 配置可通过MIB节点查询和配置VA接口	2-5
3.4.5 配置允许创建PPPoE会话的最大数目	2-5
3.4.6 配置限制用户创建PPPoE会话的速度	2-6
3.4.7 配置PPPoE会话的NAS-PORT-ID属性相关参数	2-7
3.5 配置PPPoE Client	2-8
3.5.1 工作模式介绍	2-8
3.5.2 PPPoE Client配置任务简介	2-8
3.5.3 配置拨号接口	2-8
3.5.4 配置PPPoE会话	2-9
3.5.5 复位PPPoE会话	2-10
3.6 PPPoE显示和维护	2-10
3.6.1 PPPoE Server显示和维护	2-10
3.6.2 PPPoE Client显示和维护	2-11
3.7 PPPoE典型配置举例	2-12
3.7.1 PPPoE Server通过PPP地址池为用户分配IPv4 地址配置举例	2-12
3.7.2 PPPoE Server通过本地DHCP服务器为用户分配IP地址配置举例	2-13
3.7.3 PPPoE Server通过远端DHCP服务器为用户分配IP地址配置举例	2-14
3.7.4 PPPoE Server通过ND协议、IPv6CP协商生成信息用于用户生成IPv6 地址配置举例	2-16
3.7.5 PPPoE Server通过DHCPv6 协议为用户分配IPv6 地址配置举例	2-17
3.7.6 PPPoE Server通过DHCPv6 协议分配代理前缀用于用户生成IPv6 地址配置举例	2-18
3.7.7 PPPoE Server为接入用户授权地址池和VPN配置举例	2-19
3.7.8 PPPoE Client永久在线模式配置举例	2-22
3.7.9 PPPoE Client按需拨号模式配置举例	2-23

3.7.10 PPPoE Client诊断模式配置举例	2-24
3.7.11 利用ADSL Modem将局域网接入Internet.....	2-25

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：

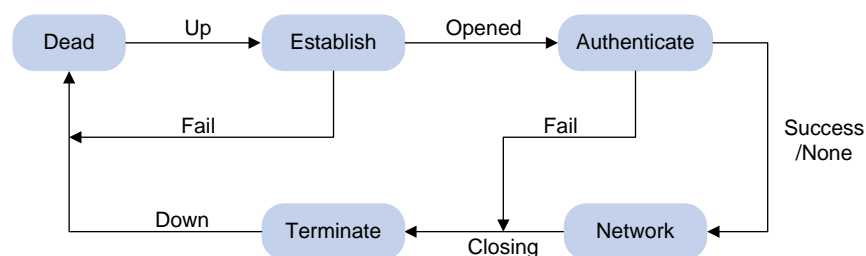
- 链路控制协议（Link Control Protocol，LCP）：用来建立、拆除和监控数据链路。
- 网络控制协议（Network Control Protocol，NCP）：用来协商在数据链路上所传输的网络层报文的一些属性和类型。
- 认证协议：用来对用户进行认证，包括 PAP（Password Authentication Protocol，密码认证协议）、CHAP（Challenge Handshake Authentication Protocol，质询握手认证协议）、MSCHAP（Microsoft CHAP，微软 CHAP 协议）和 MSCHAPv2（微软 CHAP 协议版本 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 采用的加密算法是 0x80。
- MSCHAP 支持重传机制。在被认证方认证失败的情况下，如果认证方允许被认证方进行重传，被认证方会将认证相关信息重新发回认证方，认证方根据此信息重新对被认证方进行认证。认证方最多允许被认证方重传 3 次。

4. MSCHAPv2 认证

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

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

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（可以是 PPP 地址池或者 DHCP 地址池），然后在 ISP 域下关联地址池，或者在接口下指定为 Client 端分配的 IP 地址或者地址池，最后再配置 Server 端的 IP 地址，开始进行 IPCP 协商。

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

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

2. DNS服务器地址协商

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

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

1.1.5 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“三层技术-IP 业务配置指导”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。

1.1.6 协议规范

与 PPP 相关的协议规范有：

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

1.2 PPP与硬件适配关系



说明

本特性仅在路由器上安装了 SAE、AS、ASE、BS、E1、E1-F、T1、T1-F、POS、CPOS、CE3、CT3 或 AM 接口模块时支持。

1.3 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) [配置虚拟模板接口](#)
 - [创建虚拟模板接口](#)

在 PPPoE、L2TP 和 MP 组网中，需要本配置。

- (可选) [恢复当前虚拟模板接口的缺省配置](#)
- (可选) [配置处理虚拟模板接口流量的slot](#)

(3) [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。

(4) (可选) [配置轮询功能](#)

(5) (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IP地址](#)
- [配置Server端PPP协商IP地址](#)
- [配置接口IP网段检查](#)
- [配置Client端DNS服务器地址协商](#)
- [配置Server端DNS服务器地址协商](#)
- [配置ACFC协商](#)
- [配置PFC协商](#)

(6) (可选) [配置PPP IPHC压缩功能](#)

在低速链路上，每个语音报文中报文头消耗大部分的带宽。为了减少报文头对带宽的消耗，可以在 PPP 链路上使用 IPHC 压缩功能，对报文头进行压缩。

(7) (可选) [配置PPP用户的nas-port-type属性](#)

(8) (可选) [配置PPP计费统计功能](#)

(9) (可选) [配置PPP接入用户日志信息功能](#)

1.4 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。

1.5 配置虚拟模板接口

1.5.1 创建虚拟模板接口

1. 功能简介

VT (Virtual Template, 虚拟模板) 是用于配置一个 VA (Virtual Access, 虚拟访问) 接口的模板。在 PPPoE、L2TP 和 MP 应用中需要创建一个 VA 接口与对端交换数据。此时, 系统将选择一个 VT, 以便动态地创建一个 VA 接口。

在 PPPoE 和 L2TP 应用中可借助 VT 接口来实现 PPP 协议的相关功能。有关 PPPoE 和 L2TP 的相关介绍, 请参见“二层技术-广域网接入配置指导”中的“PPPoE”和“L2TP”。

在 MP 应用中可借助 VT 接口进行 MP 捆绑。有关 MP 的相关介绍, 请参见“二层技术-广域网接入配置指导”中的“MP”。

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 创建虚拟模板接口并进入虚拟模板接口视图。

```
interface virtual-template 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: Virtual-Template1 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)。

1.5.2 恢复当前虚拟模板接口的缺省配置

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) 进入虚拟模板接口视图。

```
interface virtual-template number
```

- (3) 恢复当前接口的缺省配置。

```
default
```

1.5.3 配置处理虚拟模板接口流量的slot

1. 功能简介

当要求同一个虚拟模板接口的流量必须在同一个 slot 上进行处理时，可以在虚拟模板接口下配置处理接口流量的 slot。

为提高当前接口处理流量的可靠性，可以通过 **service** 命令和 **service standby** 命令为接口分别指定一个主用 slot 和一个备用 slot 进行流量处理。

接口上同时配置了主用 slot 和备用 slot 时，流量处理的机制如下：

- 当主用 slot 不可用时，流量由备用 slot 处理。之后，即使主用 slot 恢复可用，流量也继续由备用 slot 处理；仅当备用 slot 不可用时，流量才切换到主用 slot。
- 当主用 slot 和备用 slot 均不可用时，流量由接收报文的 slot 处理；之后，主用 slot 和备用 slot 谁先恢复可用，流量就由谁处理。

如果接口上未配置主用 slot 和备用 slot，则业务处理在接收报文的 slot 上进行。

2. 配置限制和指导

为避免不必要的流量切换，建议配置主用 slot 后，再配置备用 slot。如果先配置备用 slot，则流量由备用 slot 处理；在配置主用 slot 后，流量将会从备用 slot 切换到主用 slot。

3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入虚拟模板接口视图。

```
interface virtual-template number
```

- (3) 配置处理接口流量的主用 slot。

（独立运行模式）

```
service slot slot-number
```

（IRF 模式）

```
service chassis chassis-number slot slot-number
```

缺省情况下，未配置处理接口流量的主用 slot。

- (4) 配置处理接口流量的备用 slot。

（独立运行模式）

```
service standby slot slot-number
```

（IRF 模式）


```
service standby chassis chassis-number slot slot-number
```

缺省情况下，未配置处理接口流量的备用 slot。

1.6 配置PPP认证

1.6.1 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。

1.6.2 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 [ [ call-in ] 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。

1.6.3 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 [ [ call-in ] 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”。

1.6.4 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 [ [ call-in ] 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 } password
```

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。

1.6.5 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。

L2TP 环境下仅支持 MSCHAP 认证，不支持 MSCHAPv2 认证。

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

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 } [ [ call-in ] 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 } [ [ call-in ] 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”。

1.7 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。

在 MP 应用中, 仅子通道支持轮询功能, 主通道不支持。在主通道上即使配置轮询功能也不会生效。

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, 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, 接口在 5 个 **keepalive** 周期内未收到 **keepalive** 报文的应答就拆除链路。

1.8 配置PPP协商参数

1.8.1 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。

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。

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。

- (4) （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。

1.8.2 配置Client端PPP协商IP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”。

1.8.3 配置Server端PPP协商IP地址

1. 功能简介

目前 Server 端为 Client 端分配 IP 地址支持以下三种方式：

- 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（支持 PPP 地址池和 DHCP 地址池）中为 Client 端分配 IP 地址。
- 从 ISP 域下关联的地址池（支持 PPP 地址池和 DHCP 地址池）中为 Client 端分配 IP 地址。

2. 配置限制和指导

不需要进行 PPP 认证的 PPP 用户可以使用在接口下指定为 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 地址两种地址分配方式。同时配置这两种方式，最后一次的配置生效。

需要进行 PPP 认证的 PPP 用户可以使用全部的三种方式。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（接口下同时配置这两种方式时，最后一次的配置生效）。

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为对端分配 IP 地址，则系统只会使用 PPP 地址池来分配 IP 地址。

当通过 PPP 地址池给用户分配 IP 地址时，请确保 PPP 地址池中不包含该 PPP 地址池的网关地址。

3. 在接口下指定为Client端分配的IP地址

- (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。

- (4) 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。

4. 从接口下指定的PPP地址池中分配IP地址

- (1) 进入系统视图。

system-view

- (2) 配置 PPP 地址池。

ip pool *pool-name start-ip-address [end-ip-address] [group group-name]*

- (3) （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，未为 PPP 地址池配置网关地址。

- (4) （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，未配置 PPP 地址池路由。

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。

- (5) 进入接口视图。

interface *interface-type interface-number*

- (6) 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。

- (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。

5. 从接口下指定的DHCP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、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 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) 进入接口视图。

```
interface interface-type interface-number
```

- (4) 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。

- (5) （可选）配置 PPP 用户作为 DHCP 客户端时使用的 DHCP 客户端 ID。

```
remote address dhcp client-identifier { callingnum | username }
```

缺省情况下，未配置 PPP 用户作为 DHCP 客户端时使用的 DHCP 客户端 ID。

当使用 PPP 用户名作为 DHCP 客户端 ID 时，请确保各个上线用户分别使用不同的 PPP 用户名上线。

- (6) 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。

6. 从ISP域下关联的PPP地址池中分配IP地址

- (1) 进入系统视图。

```
system-view
```

- (2) 配置 PPP 地址池。

```
ip pool pool-name start-ip-address [ end-ip-address ] [ group  
group-name ]
```

缺省情况下，未配置 PPP 地址池。

- (3) （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，未为 PPP 地址池配置网关地址。

- (4) （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，未配置 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。

- (5) 进入 ISP 域视图。

```
domain isp-name
```

- (6) 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 域下未关联 PPP 地址池。

本命令的详细介绍请参见“安全命令参考”中的“AAA”。

- (7) 退回系统视图。

```
quit
```


- (8) 进入接口视图。

```
interface interface-type interface-number
```

- (9) 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。

7. 从ISP域下关联的DHCP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、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 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 isp-name
```

- (4) 在 ISP 域下关联 DHCP 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 DHCP 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) （可选）配置 PPP 用户作为 DHCP 客户端时使用的 DHCP 客户端 ID。

```
remote address dhcp client-identifier { callingnum | username }
```

缺省情况下，未配置 PPP 用户作为 DHCP 客户端时使用的 DHCP 客户端 ID。

当使用 PPP 用户名作为 DHCP 客户端 ID 时，请确保各个上线用户分别使用不同的 PPP 用户名上线。

- (8) 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。

1.8.4 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。

1.8.5 配置Client端DNS服务器地址协商

1. 功能简介

一般情况下，Client 端配置了 `ppp ipcp dns request` 命令后，Server 端才会为本端指定 DNS 服务器地址。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` 命令以便可以被被动地接收对端指定的 DNS 服务器地址。

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。

- (4) 配置设备可以被被动地接收对端指定的 DNS 服务器地址，即设备不发送 DNS 请求，也能接收对端设备分配的 DNS 服务器地址。

```
ppp ipcp dns admit-any
```

缺省情况下，设备不会被动地接收对端设备指定的 DNS 服务器的 IP 地址。

在配置了 `ppp ipcp dns request` 命令的情况下，可以不配置本命令。

1.8.6 配置Server端DNS服务器地址协商

- (1) 进入系统视图。

```
system-view
```

- (2) 进入接口视图。

```
interface interface-type interface-number
```

- (3) 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。

配置本命令后，Server 端不会主动给 Client 端指定 DNS 的地址，只有收到 Client 端的请求后，Server 端才会为对端指定 DNS 服务器地址。

1.8.7 配置ACFC协商

1. 功能简介

缺省情况下，PPP 报文中的地址字段的值固定为 0xFF，控制字段的值固定为 0x03，既然这两个字段的值是固定的，就可以对这两个字段进行压缩。

ACFC 协商选项字段用来通知对端，本端可以接收地址和控制字段被压缩的报文。

ACFC 协商在 LCP 协商阶段进行，对于 LCP 报文不进行地址字段和控制字段压缩，以确保 LCP 协商过程顺利进行。当 LCP 协商通过后，对于发送的非 LCP 报文将进行地址字段和控制字段压缩，以增加链路的有效载荷。

2. 配置限制和指导

建议在低速链路上配置本功能。

3. 配置本地发送ACFC协商请求

- (1) 进入系统视图。

```
system-view
```

- (2) 进入接口视图。

```
interface interface-type interface-number
```

- (3) 配置本地发送 ACFC 协商请求，即 LCP 协商时本地发送的协商请求携带 ACFC 协商选项。

```
ppp acfc local-request
```

缺省情况下，LCP 协商时本地发送的协商请求不携带 ACFC 协商选项。

4. 配置拒绝对端的ACFC协商请求

- (1) 进入系统视图。

```
system-view
```

- (2) 进入接口视图。

```
interface interface-type interface-number
```

- (3) 配置拒绝对端的 ACFC 协商请求，即 LCP 协商时拒绝对端携带的 ACFC 协商选项。

```
ppp acfc remote-reject
```

缺省情况下，接受对端的 ACFC 协商请求，即 LCP 协商时接受对端携带的 ACFC 协商选项，并且发送的报文进行地址控制字段压缩。

1.8.8 配置PFC协商

1. 功能简介

缺省情况下，PPP 报文中的协议字段长度为 2 字节，然而，目前典型的协议字段取值都小于 256，所以可以压缩成一个字节来区分协议类型。

PFC 协商选项字段用来通知对端，本端可以接收协议字段被压缩成一个字节的报文。

PFC 协商在 LCP 协商阶段进行，对于 LCP 报文不进行协议字段压缩，以确保 LCP 协商过程顺利进行。当 LCP 协商通过后，对于发送的非 LCP 报文将进行协议字段压缩，如果协议字段的头 8 比特为全零，则不添加此 8 比特，以增加链路的有效载荷；

2. 配置限制和指导

建议在低速链路上配置本功能。

3. 配置本地发送PFC协商请求

- (1) 进入系统视图。

```
system-view
```

- (2) 进入接口视图。

```
interface interface-type interface-number
```

- (3) 配置本地发送 PFC 协商请求，即 LCP 协商时本地发送的协商请求携带 PFC 协商选项。

```
ppp pfc local-request
```

缺省情况下，LCP 协商时本地发送的协商请求不携带 PFC 协商选项。

4. 配置拒绝对端的PFC协商请求

- (1) 进入系统视图。

```
system-view
```

- (2) 进入接口视图。

```
interface interface-type interface-number
```

- (3) 配置拒绝对端的 PFC 协商请求，即 LCP 协商时拒绝对端携带的 PFC 协商选项。

```
ppp pfc remote-reject
```

缺省情况下，接受对端的 PFC 协商请求，即 LCP 协商时接受对端携带的 PFC 协商选项，并且发送的报文进行协议字段压缩。

1.9 配置PPP IPHC压缩功能

1. 功能简介

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

在低速链路上，每个语音报文中报文头消耗大部分的带宽。为了减少报文头对带宽的消耗，可以在 PPP 链路上使用 IPHC 压缩功能，对报文头进行压缩。

IPHC 压缩分为如下两种：

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

2. 配置限制和指导

用户必须在链路的两端同时开启 IPHC 压缩功能，该功能才生效。

在虚拟模板接口、Dialer 接口、ISDN 接口上开启/关闭 IPHC 压缩功能时，配置不会立即生效，只有对此接口或者其绑定的物理接口依次进行 **shutdown** 和 **undo shutdown** 操作后，配置才能生效。

只有在开启 IPHC 压缩功能后，才能配置接口上允许进行 RTP 头/TCP 头压缩的最大连接数，并且需要对接口依次进行 **shutdown** 和 **undo shutdown** 操作后，配置才能生效。在关闭 IPHC 压缩功能后，配置将被清除。

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 IPHC 压缩功能。

```
ppp compression iphc enable [ nonstandard ]
```

缺省情况下，IPHC 压缩功能处于关闭状态。

与非 H3C 设备互通时需要配置 **nonstandard** 参数。

配置 **nonstandard** 参数后，仅支持 RTP 头压缩，不支持 TCP 头压缩。

- (4) 配置接口上允许进行 RTP 头压缩的最大连接数。

```
ppp compression iphc rtp-connections number
```

缺省情况下，接口上允许进行 RTP 头压缩的最大连接数为 16。

- (5) 配置接口上允许进行 TCP 头压缩的最大连接数。

```
ppp compression iphc tcp-connections number
```

缺省情况下，接口上允许进行 TCP 头压缩的最大连接数为 16。

1.10 配置PPP用户的nas-port-type属性

1. 功能简介

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。

2. 配置限制和指导

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) 进入虚拟模板接口视图。

```
interface virtual-template number
```

- (3) 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 | sds1 | sync | virtual | wireless-other | x.25 | x.75 | xdsl }
```

缺省情况下，nas-port-type 属性由 PPP 用户的业务类型和承载链路类型决定：

- 如果是 PPPoE 业务，当承载链路类型为三层虚拟以太网接口时，nas-port-type 属性为 **xdsl**，否则 nas-port-type 属性为 **ethernet**。
- 如果是 PPPoA 业务，nas-port-type 属性为 **xdsl**。
- 如果是 L2TP 业务，nas-port-type 属性为 **virtual**。

1.11 配置PPP计费统计功能

1. 功能简介

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

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 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。

1.12 配置PPP接入用户日志信息功能

1. 功能简介

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”。

2. 配置限制和指导

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。

3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 开启 PPP 接入用户日志信息功能。

```
ppp access-user log enable [ abnormal-logout | failed-login |  
normal-logout | successful-login ] *
```

缺省情况下，PPP 接入用户日志信息功能处于关闭状态。

1.13 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接入用户的信息	display ppp access-user { domain <i>domain-name</i> interface <i>interface-type</i> <i>interface-number</i> [count] ip-address <i>ipv4-address</i> ipv6-address <i>ipv6-address</i> username <i>user-name</i> user-type { lac lns pppoa pppoe } [count] }
显示PPP的协商报文统计信息	(独立运行模式) display ppp packet statistics [slot <i>slot-number</i>] (IRF模式) display ppp packet statistics [chassis <i>chassis-number</i> slot <i>slot-number</i>]
显示PPP地址池的信息	display ip pool [<i>pool-name</i> group <i>group-name</i>]
显示虚拟模板接口的相关信息	display interface [virtual-template [<i>interface-number</i>]] [brief [description down]]
显示虚拟访问接口的相关信息	display interface [virtual-access [<i>interface-number</i>]] [brief [description down]]
显示IPHC压缩的统计信息	display ppp compression iphc { rtp tcp } [interface <i>interface-type</i> <i>interface-number</i>]
清除VA接口的统计信息	reset counters interface [virtual-access [<i>interface-number</i>]]
清除IPHC压缩的统计信息	reset ppp compression iphc [rtp tcp] [interface <i>interface-type</i> <i>interface-number</i>]
强制PPP用户下线	reset ppp access-user { ip-address <i>ipv4-address</i> [vpn-instance <i>ipv4-vpn-instance-name</i>] ipv6-address <i>ipv6-address</i> [vpn-instance <i>ipv6-vpn-instance-name</i>] username <i>user-name</i> }
清除PPP的协商报文统计信息	(独立运行模式) reset ppp packet statistics [slot <i>slot-number</i>] (IRF模式) reset ppp packet statistics [chassis <i>chassis-number</i> slot <i>slot-number</i>]

1.14 PPP典型配置举例

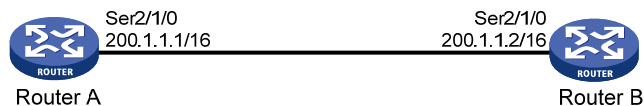
1.14.1 PAP单向认证配置举例

1. 组网需求

如 图 1-2 所示，Router A和Router B之间用接口Serial2/1/0 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 2/1/0  
[RouterA-Serial2/1/0] link-protocol ppp
```

配置本地认证 Router B 的方式为 PAP。

```
[RouterA-Serial2/1/0] ppp authentication-mode pap domain system
```

配置接口的 IP 地址。

```
[RouterA-Serial2/1/0] ip address 200.1.1.1 16  
[RouterA-Serial2/1/0] 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 2/1/0  
[RouterB-Serial2/1/0] 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-Serial2/1/0] ppp pap local-user userb password simple passb
# 配置接口的 IP 地址。
[RouterB-Serial2/1/0] ip address 200.1.1.2 16
```

4. 验证配置

通过 **display interface serial** 命令，查看接口 Serial2/1/0 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-Serial2/1/0] display interface serial 2/1/0
Serial2/1/0
Current state: UP
Line protocol state: UP
Description: Serial2/1/0 Interface
Bandwidth: 64kbps
Maximum transmission unit: 1500
Internet address: 200.1.1.2/16 (primary)
Link layer protocol: PPP
LCP: opened, IPCP: opened
...略...

[RouterB-Serial2/1/0] 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
```

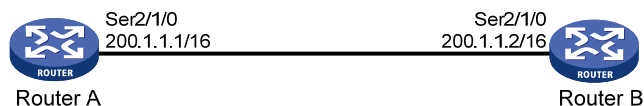
1.14.2 PAP双向认证配置举例

1. 组网需求

如 [图 1-3](#) 所示，Router A 和 Router B 之间用接口 Serial2/1/0 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 2/1/0
[RouterA-Serial2/1/0] link-protocol ppp
# 配置本地认证 Router B 的方式为 PAP。
[RouterA-Serial2/1/0] 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-Serial2/1/0] ppp pap local-user usera password simple passa
# 配置接口的 IP 地址。
[RouterA-Serial2/1/0] ip address 200.1.1.1 16
[RouterA-Serial2/1/0] 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 2/1/0
[RouterB-Serial2/1/0] link-protocol ppp
# 配置本地认证 Router A 的方式为 PAP。
[RouterB-Serial2/1/0] 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-Serial2/1/0] ppp pap local-user userb password simple passb
# 配置接口的 IP 地址。
[RouterB-Serial2/1/0] ip address 200.1.1.2 16
[RouterB-Serial2/1/0] 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 Serial2/1/0 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 2/1/0
Serial2/1/0
Current state: UP
Line protocol state: UP
Description: Serial2/1/0 Interface
Bandwidth: 64kbps
Maximum transmission 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
```

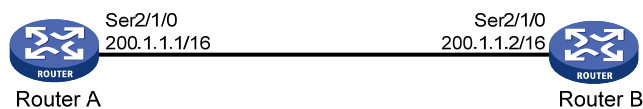
1.14.3 CHAP单向认证配置举例

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 2/1/0  
[RouterA-Serial2/1/0] link-protocol ppp
```

配置采用 CHAP 认证时 Router A 的用户名。

```
[RouterA-Serial2/1/0] ppp chap user usera
```

配置本地认证 Router B 的方式为 CHAP。

```
[RouterA-Serial2/1/0] ppp authentication-mode chap domain system
```

配置接口的 IP 地址。

```
[RouterA-Serial2/1/0] ip address 200.1.1.1 16  
[RouterA-Serial2/1/0] 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 2/1/0  
[RouterB-Serial2/1/0] link-protocol ppp
```

配置采用 CHAP 认证时 Router B 的用户名。

```
[RouterB-Serial2/1/0] ppp chap user userb
```

配置接口的 IP 地址。

```
[RouterB-Serial2/1/0] 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 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 2/1/0
[RouterA-Serial2/1/0] ppp authentication-mode chap domain system
# 配置接口的 IP 地址。
[RouterA-Serial2/1/0] ip address 200.1.1.1 16
[RouterA-Serial2/1/0] 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 2/1/0
[RouterB-Serial2/1/0] ppp chap user userb
# 设置缺省的 CHAP 认证密码。
[RouterB-Serial2/1/0] ppp chap password simple hello
# 配置接口的 IP 地址。
[RouterB-Serial2/1/0] ip address 200.1.1.2 16

```

5. 验证配置

通过 **display interface serial** 命令，查看接口 Serial2/1/0 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-Serial2/1/0] display interface serial 2/1/0
Serial2/1/0
Current state: UP
Line protocol state: UP
Description: Serial2/1/0 Interface
Bandwidth: 64kbps
Maximum transmission unit: 1500
Internet address: 200.1.1.2/16 (primary)
Link layer protocol: PPP
LCP opened, IPCP opened
...略...
[RouterB-Serial2/1/0] 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

```

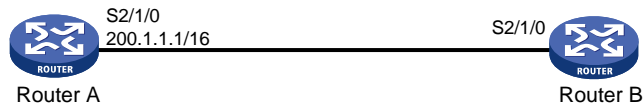
1.14.4 在接口下指定为Client端分配的IP地址配置举例

1. 组网需求

Router A 通过 PPP 协商，为 Router B 的接口 Serial2/1/0 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 在接口下指定为 Client 端分配的 IP 地址组网图



3. 配置步骤

(1) 配置 Router A

配置接口 Serial2/1/0 为 Router B 的接口分配的 IP 地址。

```
<RouterA> system-view
[RouterA] interface serial 2/1/0
[RouterA-Serial2/1/0] remote address 200.1.1.10
```

配置接口 Serial2/1/0 的 IP 地址。

```
[RouterA-Serial2/1/0] ip address 200.1.1.1 16
```

(2) 配置 Router B

配置接口 Serial2/1/0 通过协商获取 IP 地址。

```
<RouterB> system-view
[RouterB] interface serial 2/1/0
[RouterB-Serial2/1/0] ip address ppp-negotiate
```

4. 验证配置

配置完成后，查看设备 Router B 的接口 Serial2/1/0 的概要信息，可见接口 Serial2/1/0 通过 PPP 协商获取的 IP 地址为 200.1.1.10。

```
[RouterB-Serial2/1/0] display interface serial 2/1/0 brief
Brief information on interfaces in route mode:
Link: ADM - administratively down; Stby - standby
Protocol: (s) - spoofing
Interface          Link Protocol Primary IP      Description
Ser2/1/0           UP    UP      200.1.1.10
```

在 Router B 上可以 Ping 通 Router A 的 Serial2/1/0 接口。

```
[RouterB-Serial2/1/0] 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

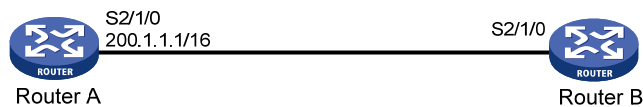
1.14.5 从接口下指定的PPP地址池中分配IP地址配置举例

1. 组网需求

Router A 通过 PPP 协商，为 Router B 的接口 Serial2/1/0 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 从接口下指定的 PPP 地址池中分配 IP 地址组网图



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 PPP 地址池路由。

```
[RouterA] ppp ip-pool route 200.1.1.1 24
```

配置接口 Serial2/1/0 使用 PPP 地址池为 Router B 的接口分配 IP 地址。

```
[RouterA] interface serial 2/1/0  
[RouterA-Serial2/1/0] remote address pool aaa
```

配置接口 Serial2/1/0 的 IP 地址。

```
[RouterA-Serial2/1/0] ip address 200.1.1.1 16
```

(2) 配置 Router B

配置接口 Serial2/1/0 通过协商获取 IP 地址。

```
<RouterB> system-view  
[RouterB] interface serial 2/1/0  
[RouterB-Serial2/1/0] ip address ppp-negotiate
```

4. 验证配置

配置完成后，查看设备 Router B 的接口 Serial2/1/0 的概要信息，可见接口 Serial2/1/0 通过 PPP 协商获取的 IP 地址为 200.1.1.10。

```
[RouterB-Serial2/1/0] display interface serial 2/1/0 brief  
Brief information on interfaces in route mode:  
Link: ADM - administratively down; Stby - standby  
Protocol: (s) - spoofing  
Interface          Link Protocol Primary IP      Description  
Ser2/1/0           UP    UP      200.1.1.10
```

在 Router B 上可以 Ping 通 Router A 的 Serial2/1/0 接口。

```
[RouterB-Serial2/1/0] 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-Serial2/1/0] 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     Ser2/1/0
```

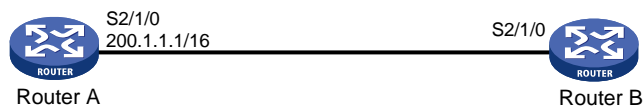
1.14.6 从ISP域下关联的PPP地址池中分配IP地址配置举例

1. 组网需求

Router A 通过 PPP 协商，为 Router B 的接口 Serial2/1/0 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 从 ISP 域下关联的 PPP 地址池中分配 IP 地址组网图



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 PPP 地址池路由。

```
[RouterA] ppp ip-pool route 200.1.1.1 24
```

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 Serial2/1/0 在 ISP 域 bbb 中采用 PAP 方式认证 Router B。
[RouterA] interface serial 2/1/0
[RouterA-Serial2/1/0] ppp authentication-mode pap domain bbb
# 配置接口 Serial2/1/0 的 IP 地址。
[RouterA-Serial2/1/0] 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 2/1/0
[RouterB-Serial2/1/0] ppp pap local-user userb password simple 123
# 配置接口 Serial2/1/0 通过协商获取 IP 地址。
[RouterB-Serial2/1/0] ip address ppp-negotiate

```

4. 验证配置

配置完成后，查看设备 Router B 的接口 Serial2/1/0 的概要信息，可见接口 Serial2/1/0 通过 PPP 协商获取的 IP 地址为 200.1.1.10。

```

[RouterB-Serial2/1/0] display interface serial 2/1/0 brief
Brief information on interfaces in route mode:
Link: ADM - administratively down; Stby - standby
Protocol: (s) - spoofing
Interface          Link Protocol Primary IP      Description
Ser2/1/0           UP    UP      200.1.1.10

```

在 Router B 上可以 Ping 通 Router A 的 Serial2/1/0 接口。

```

[RouterB-Serial2/1/0] 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-Serial2/1/0] 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	Ser2/1/0

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、ISDN 的 BRI/PRI 接口等，也包括支持 PPPoX（PPPoE、PPPoA、PPPoFR 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。

2.2 MP配置任务简介

MP 配置任务如下：

(1) 配置 MP

请选择以下一项任务进行配置。

- [配置通过虚拟模板接口进行MP捆绑](#)
- [通过MP-group接口进行MP捆绑](#)

(2) （可选）[配置DDR链路的MP参数](#)

(3) （可选）[配置MP捆绑模式](#)

(4) （可选）[配置MP短序协商方式](#)

(5) （可选）[配置MP Endpoint选项](#)

(6) （可选）[配置链路分片与交叉](#)

2.3 配置通过虚拟模板接口进行MP捆绑

2.3.1 功能简介

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

虚拟模板接口配置方式可以与认证相结合，可以根据对端的用户名找到指定的虚拟模板接口，从而利用模板上的配置，创建相应的捆绑（Bundle），以对应一条 MP 链路。

由一个虚拟模板接口可以派生出若干个捆绑，每个捆绑对应一条 MP 链路。从网络层看来，这若干条 MP 链路会形成一个点对多点的网络拓扑。系统可以根据接口接收到的认证用户名或终端标识符来进行 MP 捆绑，并以此来区分虚模板接口下的多个捆绑（对应多条 MP 链路）。

系统支持 3 种绑定方式：

- **authentication:** 根据 PPP 的认证用户名进行 MP 捆绑，每个认证用户名对应一个捆绑。认证用户名是指 PPP 链路进行 PAP、CHAP、MSCHAP 或 MSCHAPv2 认证时所接收到的对端用户名。
- **descriptor:** 根据 PPP 的终端描述符进行 MP 捆绑，每个终端描述符对应一个捆绑。终端标识符是用来唯一标识一台设备的标志，是指进行 LCP 协商时所接收到的对端终端标识符。
- **both:** 同时根据 PPP 的认证用户名和终端描述符进行 MP 捆绑。

2.3.2 配置限制和指导

实际使用中也可以配置单向认证，即一端直接将物理接口绑定到虚拟模板接口，另一端则通过用户名查找虚拟模板接口。

不推荐使用同一个虚拟模板接口配置多种业务（如 MP、L2TP、PPPoE 等）。

2.3.3 通过虚拟模板接口进行MP捆绑配置任务简介

通过虚拟模板接口配置 MP 配置任务如下：

- (1) [创建虚拟模板接口](#)
- (2) [将物理接口或用户名与虚拟模板接口关联](#)
- (3) （可选）[配置MP参数](#)

2.3.4 创建虚拟模板接口

- (1) 进入系统视图。
system-view
- (2) 创建虚拟模板接口并进入虚拟模板接口视图。
interface virtual-template 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：Virtual-Template1 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)。

2.3.5 将物理接口或用户名与虚拟模板接口关联

1. 功能简介

通过虚拟模板接口配置 MP 时，支持如下两种配置方式：

- 将物理接口与虚拟模板接口直接关联：使用命令 **ppp mp virtual-template** 直接将链路绑定到指定的虚拟模板接口上，这时可以配置认证也可以不配置认证。如果不配置认证，系统将通过对端的终端描述符捆绑出 MP 链路；如果配置了认证，系统将通过用户名和对端的终端描述符捆绑出 MP 链路。
- 将用户名与虚拟模板接口关联：根据认证通过后的用户名查找相关联的虚拟模板接口，然后根据用户名和对端终端描述符捆绑出 MP 链路。这种方式需在要绑定的接口下配置 **ppp mp** 及双向认证 (PAP、CHAP、MSCHAP 或 MSCHAPv2)，否则链路协商不通。

2. 配置限制和指导

针对同一接口多次执行 **ppp mp** 命令和 **ppp mp virtual-template** 命令，最后一次执行的命令生效。即同一个接口只能采用一种配置方式。

对于需要绑在一起的接口，必须采用同样的配置方式。

3. 将物理接口与虚拟模板接口关联

- (1) 进入系统视图。

system-view

- (2) 进入接口视图。

interface interface-type interface-number

- (3) 配置接口所要绑定的虚拟模板接口号，并使接口工作在 MP 方式。

ppp mp virtual-template number

缺省情况下，接口未绑定虚拟模板接口，接口工作在普通 PPP 方式。

- (4) (可选) 在接口下配置 PPP 认证。

具体配置请参见“[1.6 配置PPP认证](#)”。

PPP 认证对 MP 连接的建立没有影响。

4. 将用户名与虚拟模板接口关联

- (1) 进入系统视图。

system-view

- (2) 建立虚拟模板接口与 MP 用户的对应关系。

```
ppp mp user username bind virtual-template number
```

缺省情况下，虚拟模板接口未与 MP 用户进行绑定。

- (3) 进入接口视图。

```
interface interface-type interface-number
```

- (4) 配置封装 PPP 的接口工作在 MP 方式。

```
ppp mp
```

缺省情况下，封装 PPP 的接口工作在普通 PPP 方式。

- (5) 在接口下配置 PPP 认证。

具体配置请参见“[1.6 配置PPP认证](#)”。

2.3.6 配置MP参数

- (1) 进入系统视图。

```
system-view
```

- (2) 进入虚拟模板接口视图。

```
interface virtual-template number
```

- (3) 配置 MP 捆绑的条件。

```
ppp mp binding-mode { authentication | both | descriptor }
```

缺省情况下，同时根据 PPP 的认证用户名和终端标识符进行 MP 捆绑。

- (4) （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。

- (5) （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。

- (6) （可选）配置 MP 排序窗口的大小。

```
ppp mp sort-buffer-size size
```

缺省情况下，MP 排序窗口大小系数为 1。

- (7) （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 等待期望分片报文的时间为 30 秒。

- (8) （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。

关闭 MP 报文分片功能后，接口的 `ppp mp lfi enable`、`ppp mp min-fragment` 命令不再起作用。

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。与虚拟模板接口配置方式相比，MP-group 接口配置方式更加快速高效、配置简单、容易理解。

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参数](#)
- (4) (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-group2/0/0 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 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。

- (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 排序窗口的大小。

```
ppp mp sort-buffer-size size
```

缺省情况下，MP 排序窗口大小系数为 1。

- (6) （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。

- (7) （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。

关闭 MP 报文分片功能命令后，接口的 **ppp mp lfi enable**、**ppp mp min-fragment** 命令不再起作用。

- (8) （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。

2.4.6 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DDR链路的MP参数

1. 功能简介

配置 DDR 链路的 MP 捆绑的详细介绍，请参见“二层技术-广域网接入配置指导”中的“DDR”。

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入 Dialer 接口视图。

```
interface dialer number
```

- (3) 配置 MP 捆绑的条件。

```
ppp mp binding-mode { authentication | both | descriptor }
```

缺省情况下，同时根据 PPP 的认证用户名和终端标识符进行 MP 捆绑。

- (4) （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。

- (5) （可选）配置 MP 最小捆绑链路数。

```
ppp mp min-bind min-bind-num
```

缺省情况下，最小捆绑链路数为 0，即 MP 拨号将依赖流量检测。

本命令配置的最小捆绑链路数应该小于等于 **ppp mp max-bind** 命令配置的最大捆绑链路数。

- (6) （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。

- (7) (可选) 配置 MP 排序窗口的大小。

ppp mp sort-buffer-size size

缺省情况下，MP 排序窗口大小系数为 1。

- (8) (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 等待期望分片报文的时间为 30 秒。

- (9) (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。

关闭 MP 报文分片功能后，接口的 **ppp mp lfi enable**、**ppp mp min-fragment** 命令不再起作用。

2.6 配置MP捆绑模式

1. 功能简介

MP 捆绑有如下两种捆绑模式：

- 硬件捆绑模式：报文的分片和重组通过硬件实现，效率高。
- 软件捆绑模式：报文的分片和重组通过 CPU 实现，效率较低。

2. 配置限制和指导

不同接口支持的 MP 捆绑模式不同，有的接口只支持硬件捆绑模式，有的接口只支持软件捆绑模式，有的接口同时支持两种捆绑模式。

同时支持两种捆绑模式的接口，缺省采用硬件捆绑模式，在如下情况可以通过命令切换为软件捆绑模式：

- CPOS E1/T1 接口卡不支持跨 CPOS 接口的硬件 MP 捆绑，只能将同一个 CPOS 接口通道化生成的多个同步串口进行硬件 MP 捆绑，如果用户想将不同 CPOS 接口通道化生成的多个同步串口进行 MP 捆绑，必须先将这些同步串口的捆绑模式切换为软件捆绑模式。
- 硬件捆绑模式的接口不能和软件捆绑模式的接口进行 MP 捆绑。当用户想将支持两种捆绑模式的接口和只支持软件捆绑模式的接口进行 MP 捆绑时，必须先将硬件捆绑模式的接口切换为软件捆绑模式。

3. 配置步骤

- (1) 进入系统视图。

system-view

- (2) 进入同步串口视图。

interface interface-type interface-number

- (3) 配置接口采用软件捆绑模式。

ppp mp soft-binding

缺省情况下，采用硬件捆绑模式。

2.7 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，对于拨号 MP，建议在 Dialer 接口及 ISDN 的 D 信道下均配置触发 MP 短序协商；对于普通 MP，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。

2.8 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：

- 在通过虚拟模板接口配置 MP 时，会根据 Endpoint 选项值来进行 MP 捆绑。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。如果网络中存在相同的设备名称，导致无法区分 MP 捆绑时，用户可以修改接口发送报文中携带的 Endpoint 选项的内容。
- 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。

2.9 配置链路分片与交叉

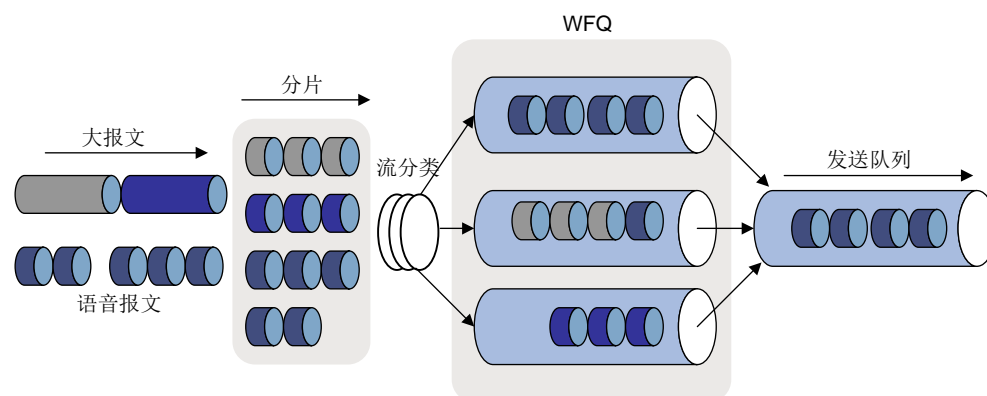
1. 功能简介

在低速串行链路上，实时交互式通信（如 Telnet 和 VoIP）往往会由于大型分组的发送而导致阻塞延迟。

LFI（Link Fragmentation and Interleaving，链路分片与交叉）将大型数据帧分割成小型帧，与其它小片的报文一起发送，从而减少在低速链路上的延迟和抖动。被分割的数据帧在目的地被重组。

[图 2-1](#) 描述了 LFI 的处理过程。大报文和小的语音报文一起到达某个接口，将大报文分割成小的分片，如果在接口配置了 WFQ（Weighted Fair Queuing，加权公平队列），语音包与这些小的分片一起交叉放入 WFQ。

图2-1 LFI 的处理过程



开启 LFI 功能后，LFI 最大分片大小由 LFI 分片的最大时延（通过 `ppp mp lfi delay-per-frag` 命令配置）和 LFI 分片的最大字节数（通过 `ppp mp lfi size-per-frag` 命令配置）决定：

- 如果配置了 LFI 分片的最大字节数，LFI 最大分片大小就是该最大字节数。
- 如果配置了 LFI 分片的最大时延，未配置 LFI 分片的最大字节数，则 LFI 最大分片大小通过接口的期望带宽和配置的最大时延计算得出： $\text{LFI 最大分片大小} = (\text{接口的期望带宽} \times \text{最大时延}) \div 8$ 。

2. 配置步骤

(1) 进入系统视图。

```
system-view
```

(2) 进入虚拟模板接口视图、MP-group 接口视图或 Dialer 接口视图。

```
interface { dialer | mp-group | virtual-template } mp-number
```

(3) 开启 LFI 功能。

```
ppp mp lfi enable
```

缺省情况下，LFI 功能处于关闭状态。

关闭 LFI 功能会同时删除用户配置的 LFI 分片的最大时延或 LFI 分片的最大字节数。

(4) 配置传输一个 LFI 分片的最大时延或 LFI 分片的最大字节数。

○ 配置传输一个 LFI 分片的最大时延。

```
ppp mp lfi delay-per-frag time
```

缺省情况下，传输一个 LFI 分片的最大时延为 10ms。

○ 配置 LFI 分片的最大字节数。

```
ppp mp lfi size-per-frag size
```

缺省情况下，最大分片大小 = (接口的期望带宽 × 最大时延) ÷ 8。

2.10 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	<pre>display interface [mp-group [interface-number]] [brief [description down]]</pre>
显示MP的相关信息	<pre>display ppp mp [interface interface-type interface-number]</pre>
清除MP-group接口的统计信息	<pre>reset counters interface [mp-group [interface-number]]</pre>

2.11 MP典型配置举例

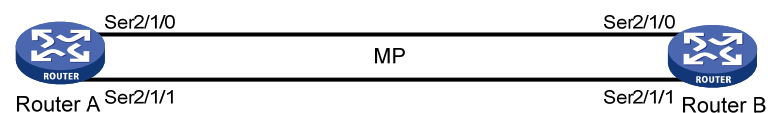
2.11.1 通过将物理接口直接绑定到VT接口方式进行MP捆绑配置举例

1. 组网需求

设备 Router A 和 Router B 的 Serial2/1/1 和 Serial2/1/0 分别对应连接。要求通过将物理接口直接绑定到 VT 接口方式进行 MP 捆绑。

2. 组网图

图2-2 通过将物理接口直接绑定到 VT 接口方式进行 MP 捆绑组网图



3. 配置步骤

(1) 配置 Router A

创建虚拟模板接口，配置相应的 IP 地址。

```
<RouterA> system-view
[RouterA] interface virtual-template 1
[RouterA-Virtual-Template1] ip address 8.1.1.1 24
[RouterA-Virtual-Template1] quit
```

配置串口 Serial2/1/1。

```
[RouterA] interface serial 2/1/1
[RouterA-Serial2/1/1] link-protocol ppp
[RouterA-Serial2/1/1] ppp mp virtual-template 1
[RouterA-Serial2/1/1] quit
```

配置串口 Serial2/1/0。

```
[RouterA] interface serial 2/1/0
[RouterA-Serial2/1/0] link-protocol ppp
[RouterA-Serial2/1/0] ppp mp virtual-template 1
[RouterA-Serial2/1/0] quit
```

(2) 配置 Router B

创建虚拟模板接口，配置相应的 IP 地址。

```
<RouterB> system-view
[RouterB] interface virtual-template 1
[RouterB-Virtual-Template1] ip address 8.1.1.2 24
[RouterB-Virtual-Template1] quit
```

配置串口 Serial2/1/1。

```
[RouterB] interface serial 2/1/1
[RouterB-Serial2/1/1] link-protocol ppp
[RouterB-Serial2/1/1] ppp mp virtual-template 1
[RouterB-Serial2/1/1] quit
```

配置串口 Serial2/1/0。

```
[RouterB] interface serial 2/1/0
[RouterB-Serial2/1/0] link-protocol ppp
[RouterB-Serial2/1/0] ppp mp virtual-template 1
[RouterB-Serial2/1/0] quit
```

4. 验证配置

(1) 在 Router A 上查看绑定结果

查看 MP 的相关信息。

```
[RouterA] display ppp mp
Template: Virtual-Template1
max-bind: 16, fragment: enabled, min-fragment: 128
  Master link: Virtual-Access0, Active members: 2, Bundle RouterB
  Peer's endPoint descriptor: RouterB
  Sequence format: long (rcv)/long (sent)
  Bundle Up Time: 2013/01/10 07:13:10:723
  0 lost fragments, 0 reordered, 0 unassigned, 0 interleaved
  Sequence: 0 (rcv)/0 (sent)
```

```
Active member channels: 2 members
      Serial2/1/1                Up-Time:2013/01/10  07:13:10:724
      Serial2/1/0                Up-Time:2013/01/10  07:13:11:945
```

查看 VA 状态。

```
[RouterA] display interface virtual-access
Virtual-Access0
Current state: UP
Line protocol state: UP
Description: Virtual-Access0 Interface
Bandwidth: 128kbps
Maximum transmission unit: 1500
Hold timer: 10 seconds,retry times: 5
Internet address: 8.1.1.1/24 (primary)
Link layer protocol: PPP
LCP: opened, MP: opened, IPCP: opened
Physical: MP, baudrate: 128000 bps
Main interface: Virtual-Template1
Output queue - Urgent queuing: Size/Length/Discards 0/100/0
Output queue - Protocol queuing: Size/Length/Discards 0/500/0
Output queue - FIFO queuing: Size/Length/Discards 0/75/0
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
```

(2) 在 Router B 上 ping 对端 IP 地址 8.1.1.1

```
[RouterB] ping 8.1.1.1
Ping 8.1.1.1 (8.1.1.1): 56 data bytes, press CTRL_C to break
56 bytes from 8.1.1.1: icmp_seq=0 ttl=255 time=4.000 ms
56 bytes from 8.1.1.1: icmp_seq=1 ttl=255 time=0.000 ms
56 bytes from 8.1.1.1: icmp_seq=2 ttl=255 time=0.000 ms
56 bytes from 8.1.1.1: icmp_seq=3 ttl=255 time=0.000 ms
56 bytes from 8.1.1.1: icmp_seq=4 ttl=255 time=1.000 ms

--- Ping statistics for 8.1.1.1 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 0.000/1.000/4.000/1.549 ms
```

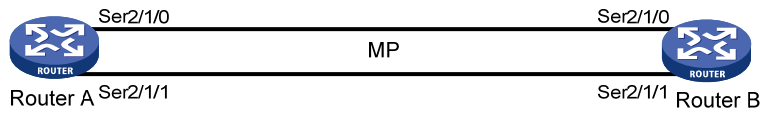
2.11.2 通过按用户名找VT方式进行MP捆绑配置举例

1. 组网需求

设备 Router A 和 Router B 的 Serial2/1/1 和 Serial2/1/0 分别对应连接。要求通过按用户名找 VT 方式进行 MP 捆绑。

2. 组网图

图2-3 通过按用户名找 VT 方式进行 MP 捆绑组网图



3. 配置步骤

(1) 配置 Router A

配置对端设备 Router B 在 Router A 上的用户名和密码。

```
<RouterA> system-view
[RouterA] local-user usera class network
[RouterA-luser-network-usera] password simple aaa
[RouterA-luser-network-usera] service-type ppp
[RouterA-luser-network-usera] quit
```

指定用户对应的 VT。

```
[RouterA] ppp mp user usera bind virtual-template 1
```

创建 VT，配置相应的 IP 地址。

```
[RouterA] interface virtual-template 1
[RouterA-Virtual-Templat1] ip address 8.1.1.1 24
[RouterA-Virtual-Templat1] ppp mp binding-mode authentication
[RouterA-Virtual-Templat1] quit
```

配置串口 Serial2/1/1。

```
[RouterA] interface serial 2/1/1
[RouterA-Serial2/1/1] link-protocol ppp
[RouterA-Serial2/1/1] ppp authentication-mode pap
[RouterA-Serial2/1/1] ppp pap local-user userb password simple bbb
[RouterA-Serial2/1/1] ppp mp
[RouterA-Serial2/1/1] quit
```

配置串口 Serial2/1/0。

```
[RouterA] interface serial 2/1/0
[RouterA-Serial2/1/0] link-protocol ppp
[RouterA-Serial2/1/0] ppp authentication-mode pap
[RouterA-Serial2/1/0] ppp pap local-user userb password simple bbb
[RouterA-Serial2/1/0] ppp mp
[RouterA-Serial2/1/0] quit
```

(2) 配置 Router B

配置对端设备 Router A 在 Router B 上的用户名和密码。

```
<RouterB> system-view
[RouterB] local-user userb class network
[RouterB-luser-network-userb] password simple bbb
[RouterB-luser-network-userb] service-type ppp
[RouterB-luser-network-userb] quit
```

指定用户对应的 VT。

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


创建 VT，配置相应的 IP 地址。

```
[RouterB] interface virtual-template 1
[RouterB-Virtual-Template1] ip address 8.1.1.2 24
[RouterB-Virtual-Template1] ppp mp binding-mode authentication
[RouterB-Virtual-Template1] quit
```

配置串口 Serial2/1/1。

```
[RouterB] interface serial 2/1/1
[RouterB-Serial2/1/1] link-protocol ppp
[RouterB-Serial2/1/1] ppp authentication-mode pap
[RouterB-Serial2/1/1] ppp pap local-user usera password simple aaa
[RouterB-Serial2/1/1] ppp mp
[RouterB-Serial2/1/1] quit
```

配置串口 Serial2/1/0。

```
[RouterB] interface serial 2/1/0
[RouterB-Serial2/1/0] link-protocol ppp
[RouterB-Serial2/1/0] ppp authentication-mode pap
[RouterB-Serial2/1/0] ppp pap local-user usera password simple aaa
[RouterB-Serial2/1/0] ppp mp
[RouterB-Serial2/1/0] 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: Virtual-Template1
max-bind: 16, fragment: enabled, min-fragment: 128
  Master link: Virtual-Access0, Active members: 2, Bundle usera
  Peer's endPoint descriptor: RouterB
  Sequence format: long (rcv)/long (sent)
  Bundle Up Time: 2013/01/10 08:02:34:881
  0 lost fragments, 0 reordered, 0 unassigned, 0 interleaved
  Sequence: 0 (rcv)/0 (sent)
  Active member channels: 2 members
    Serial2/1/1          Up-Time:2013/01/10 08:02:34:881
    Serial2/1/0          Up-Time:2013/01/10 08:06:26:634
```

(2) 在 Router B 上查看绑定效果

查看 MP 的相关信息。

```
[RouterB] display ppp mp
Template: Virtual-Template1
max-bind: 16, fragment: enabled, min-fragment: 128
  Master link: Virtual-Access0, Active members: 2, Bundle userb
  Peer's endPoint descriptor: RouterA
  Sequence format: long (rcv)/long (sent)
  Bundle Up Time: 2013/01/10 12:31:13:391
  0 lost fragments, 0 reordered, 0 unassigned, 0 interleaved
  Sequence: 0 (rcv)/0 (sent)
  Active member channels: 2 members
```

```
Serial2/1/1          Up-Time:2013/01/10 12:31:13:392
Serial2/1/0          Up-Time:2013/01/10 12:35:05:892
```

查看 VA 状态。

```
[RouterB] display interface virtual-access
Virtual-Access2
Current state: UP
Line protocol state: UP
Description: Virtual-Access0 Interface
Bandwidth: 64kbps
Maximum transmission unit: 1500
Hold timer: 10 seconds, retry times: 5
Internet address: 8.1.1.2/24 (primary)
Link layer protocol: PPP
LCP: opened, MP: opened, IPCP: opened
Physical: MP, baudrate: 64000 bps
Main interface: Virtual-Templatel
Output queue - Urgent queuing: Size/Length/Discards 0/100/0
Output queue - Protocol queuing: Size/Length/Discards 0/500/0
Output queue - FIFO queuing: Size/Length/Discards 0/75/0
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 Router B 上 ping 对端 IP 地址 8.1.1.1。

```
[RouterB] ping 8.1.1.1
Ping 8.1.1.1 (8.1.1.1): 56 data bytes, press CTRL_C to break
56 bytes from 8.1.1.1: icmp_seq=0 ttl=255 time=0.000 ms
56 bytes from 8.1.1.1: icmp_seq=1 ttl=255 time=0.000 ms
56 bytes from 8.1.1.1: icmp_seq=2 ttl=255 time=1.000 ms
56 bytes from 8.1.1.1: icmp_seq=3 ttl=255 time=1.000 ms
56 bytes from 8.1.1.1: icmp_seq=4 ttl=255 time=0.000 ms

--- Ping statistics for 8.1.1.1 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 0.000/0.400/1.000/0.490 ms
```

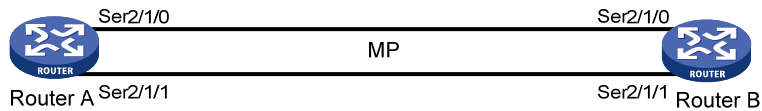
2.11.3 通过将链路绑定到MP-group接口方式进行MP捆绑配置举例

1. 组网需求

设备 Router A 和 Router B 的 Serial2/1/1 和 Serial2/1/0 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2-4 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 2/0/0
[RouterA-MP-group2/0/0] ip address 1.1.1.1 24
```

配置串口 Serial2/1/1。

```
[RouterA-MP-group2/0/0] quit
[RouterA] interface serial 2/1/1
[RouterA-Serial2/1/1] link-protocol ppp
[RouterA-Serial2/1/1] ppp mp mp-group 2/0/0
[RouterA-Serial2/1/1] shutdown
[RouterA-Serial2/1/1] undo shutdown
[RouterA-Serial2/1/1] quit
```

配置串口 Serial2/1/0。

```
[RouterA] interface serial 2/1/0
[RouterA-Serial2/1/0] link-protocol ppp
[RouterA-Serial2/1/0] ppp mp mp-group 2/0/0
[RouterA-Serial2/1/0] shutdown
[RouterA-Serial2/1/0] undo shutdown
[RouterA-Serial2/1/0] quit
```

(2) 配置 Router B

创建 MP-group 接口，配置相应的 IP 地址。

```
[RouterB] interface mp-group 2/0/0
[RouterB-Mp-group2/0/0] ip address 1.1.1.2 24
[RouterB-Mp-group2/0/0] quit
```

配置串口 Serial2/1/1。

```
[RouterB] interface serial 2/1/1
[RouterB-Serial2/1/1] link-protocol ppp
[RouterB-Serial2/1/1] ppp mp mp-group 2/0/0
[RouterB-Serial2/1/1] shutdown
[RouterB-Serial2/1/1] undo shutdown
[RouterB-Serial2/1/1] quit
```

配置串口 Serial2/1/0。

```
[RouterB] interface serial 2/1/0
[RouterB-Serial2/1/0] link-protocol ppp
[RouterB-Serial2/1/0] ppp mp mp-group 2/0/0
[RouterB-Serial2/1/0] shutdown
```

```
[RouterB-Serial2/1/0] undo shutdown
[RouterB-Serial2/1/0] 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-group2/0/0
max-bind: 16, fragment: enabled, min-fragment: 128
Master link: MP-group2/0/0, Active members: 2, Bundle Multilink
Peer's endPoint descriptor: MP-group2/0/0
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
    Serial2/1/1                Up-Time:2012/11/04 09:03:16:613
    Serial2/1/0                Up-Time:2012/11/04 09:03:42:945
```

查看 MP-group2/0/0 接口的相关信息。

```
[RouterA] display interface mp-group 2/0/0
MP-group2/0/0
Current state: UP
Line protocol state: UP
Description: MP-group2/0/0 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
Output queue - Urgent queuing: Size/Length/Discards 0/100/0
Output queue - Protocol queuing: Size/Length/Discards 0/500/0
Output queue - FIFO queuing: Size/Length/Discards 0/75/0
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
```

3 PPPoE

3.1 PPPoE简介

PPPoE (Point-to-Point Protocol over Ethernet, 在以太网上承载 PPP 协议) 是对 PPP 协议的扩展, 它在以太网上建立 PPPoE 会话, 将 PPP 报文封装在以太网帧之内, 在以太网上提供点对点的连接, 解决了 PPP 无法应用于以太网的问题。PPPoE 还可以通过远端接入设备对接入的每台主机实现控制、认证、计费功能。由于很好地结合了以太网的经济性及 PPP 良好的可扩展性与管理控制功能, PPPoE 被广泛应用于小区接入组网等环境中。

3.1.1 PPPoE组网结构

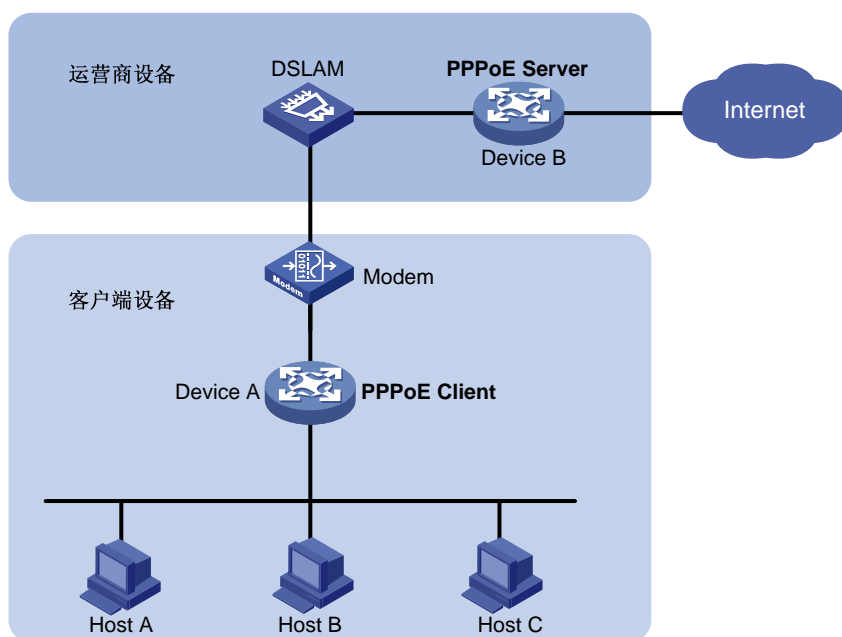
PPPoE 使用 Client/Server 模型。PPPoE Client 向 PPPoE Server 发起连接请求, 两者之间会话协商通过后, 就建立 PPPoE 会话, 此后 PPPoE Server 向 PPPoE Client 提供接入控制、认证、计费等功能。

根据 PPPoE 会话的起点所在位置的不同, PPPoE 分为 Router-Initiated 和 Host-Initiated 两种组网结构。

1. Router-Initiated组网结构

如 [图 3-1](#) 所示, Router-Initiated 组网结构是在两台设备之间建立 PPPoE 会话, 所有主机通过同一个 PPPoE 会话传送数据, 主机上不用安装 PPPoE 客户端拨号软件, 一般是一个企业共用一个账号接入网络 (图中 PPPoE Client 位于企业/公司内部, PPPoE Server 是运营商的设备)。

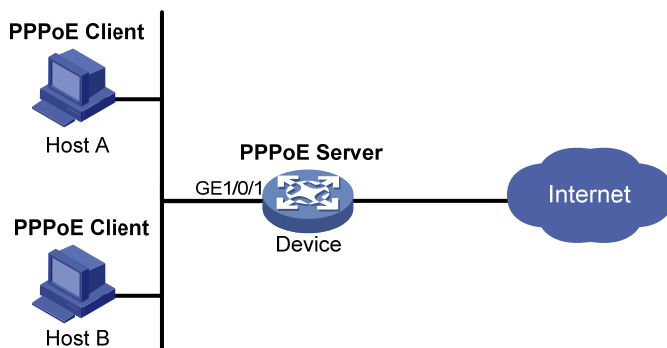
图3-1 Router-Initiated 组网结构图



2. Host-Initiated组网结构

如 图 3-2 所示，Host-Initiated组网结构是将PPPoE会话建立在Host和运营商的设备之间，为每一个Host建立一个PPPoE会话，每个Host都是PPPoE Client，每个Host使用一个帐号，方便运营商对用户进行计费和控制。Host上必须安装PPPoE客户端拨号软件。

图3-2 Host-Initiated 组网结构图



3.1.2 协议规范

与 PPPoE 相关的协议规范有：

RFC 2516: A Method for Transmitting PPP Over Ethernet (PPPoE)

3.2 PPPoE与硬件适配关系



说明

设备在 IRF 模式下不支持本特性。

3.3 PPPoE配置限制和指导

PPPoE Server 目前支持以下接口类型：

- 三层以太网接口/三层以太网子接口
- 三层聚合接口/三层聚合子接口
- VEth 接口/VEth 子接口
- VLAN 接口
- L3VE 接口/L3VE 子接口
- EFM 接口/EFM 子接口

3.4 配置PPPoE Server

3.4.1 PPPoE Server配置任务简介

PPPoE Server 配置任务如下：

- (1) [配置PPPoE会话](#)
- (2) (可选) [配置VA池](#)
- (3) (可选) [配置可通过MIB节点查询和配置VA接口](#)
- (4) (可选) [配置允许创建PPPoE会话的最大数目](#)
- (5) (可选) [配置限制用户创建PPPoE会话的速度](#)
- (6) (可选) [配置PPPoE会话的NAS-PORT-ID属性相关参数](#)

3.4.2 配置PPPoE会话

- (1) 进入系统视图。

```
system-view
```

- (2) 创建虚拟模板接口并进入指定的虚拟模板接口视图。

```
interface virtual-template number
```

- (3) 配置 PPP 的工作参数

具体工作参数的配置请参见“二层技术-广域网接入配置指导”中的“PPP”。

当配置 PPP 认证时，需要配置 PPPoE Server 作为认证方。

- (4) 开启 PPPoE 应用的 MRU 检测功能。

```
ppp lcp echo mru verify [ minimum value ]
```

PPPoE 应用的 MRU 检测功能处于关闭状态。

- (5) 退回系统视图。

```
quit
```

- (6) 进入接口视图。

```
interface interface-type interface-number
```

- (7) 在接口上启用 PPPoE Server 协议，将该接口与指定的虚拟模板接口绑定。

```
pppoe-server bind virtual-template number
```

缺省情况下，接口上的 PPPoE Server 协议处于关闭状态。

- (8) (可选)配置 PPPoE Server 的 AC Name (Access Concentrator Name，接入集中器名称)。

```
pppoe-server tag ac-name name
```

缺省情况下，PPPoE Server 的 AC Name 为设备名称。

PPPoE Client 可以根据 AC Name 来选择 PPPoE Server (H3C 实现的 PPPoE Client 暂不支持该功能)。

- (9) (可选)配置对 PPP 最大负载 TAG 的支持，并指定最大负载的范围。

```
pppoe-server tag ppp-max-payload [ minimum minvalue maximum maxvalue ]
```

缺省情况下，不支持 PPP 最大负载 TAG。

- (10) (可选)配置 PPPoE Server 的 Service Name。


```
pppoe-server tag service-name name
```

缺省情况下，PPPoE Server 的 Service Name 为空。

- (11) (可选) 配置用户接入响应延迟时间。

```
pppoe-server access-delay delay-time
```

缺省情况下，对用户接入响应不延迟。

- (12) 退回系统视图。

```
quit
```

- (13) 配置 PPPoE Server 对 PPP 用户进行认证、授权、计费。

相关内容请参见“安全配置指导”中的“AAA”。

3.4.3 配置VA池

1. 功能简介

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

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

2. 配置限制和指导

每个虚拟模板接口只能关联一个全局 VA 池，在每个单板上只能关联一个局部 VA 池。通过某单板上的以太网接口上线的用户，只能使用上线以太网接口绑定的虚拟模板接口在该单板上关联的 VA 池。如果想要修改使用的 VA 池的大小，只能先删除原来的配置，然后重新配置 VA 池。

创建/删除 VA 池需要花费一定的时间，请用户耐心等待。在 VA 池创建/删除过程中（还没创建/删除完成）允许用户上线/下线，但正在创建/删除的 VA 池不生效。

系统可能由于资源不足不能创建用户指定容量的 VA 池，用户可以通过 `display pppoe-server va-pool` 命令查看实际可用的 VA 池的容量以及 VA 池的状态。

删除 VA 池时，如果已有在线用户使用该 VA 池中的 VA 接口，不会导致这些用户下线。

3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 配置 VA 池

(独立运行模式)

```
pppoe-server virtual-template template-number [ slot slot-number ]  
va-pool va-volume
```

(IRF 模式)

```
pppoe-server virtual-template template-number [ chassis chassis-number  
slot slot-number ] va-pool va-volume
```

3.4.4 配置可通过MIB节点查询和配置VA接口

1. 功能简介

在配置大容量 VA 池或有大量用户上线的情况下，设备上会创建大量的 VA 接口。由于大多情况下，管理员通过 MIB 获取设备信息时并不关心 VA 接口，所以，缺省情况下，不能通过 MIB 节点查询和配置 VA 接口。此时，设备会忽略 NMS 发送的关于 VA 接口的配置和查询请求，这不仅可以提高设备获取其它接口信息的效率，提升用户体验度，还可以降低设备的工作量，避免 CPU 资源浪费。如果管理员需要通过 MIB 对 VA 接口进行配置或查询，请配置本功能。

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 配置可通过 MIB 节点查询和配置 VA 接口。

```
snmp virtual-access visible
```

缺省情况下，不能通过 MIB 节点查询和配置 VA 接口。

有关该命令的详细介绍，请参见“网络管理和监控命令参考”中的“SNMP”。

3.4.5 配置允许创建PPPoE会话的最大数目

1. 功能简介

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

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

2. 配置限制和指导

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

3. 在接口上配置允许创建PPPoE会话的最大数目

- (1) 进入系统视图。

```
system-view
```

- (2) 进入接口视图。

```
interface interface-type interface-number
```

该接口为启用 PPPoE Server 协议的接口。

- (3) 配置允许创建 PPPoE 会话的最大数目。

- 配置每个接口上所能创建 PPPoE 会话的最大数目。

```
pppoe-server session-limit number
```

缺省情况下，不限制接口上所能创建 PPPoE 会话的数目。

- 配置每个 VLAN 所能创建 PPPoE 会话的最大数目。

```
pppoe-server session-limit per-vlan number
```

缺省情况下，不限制每个 VLAN 所能创建 PPPoE 会话的数目。

- 配置每个用户所能创建 PPPoE 会话的最大数目。

```
pppoe-server session-limit per-mac number
```

缺省情况下，每个用户可创建 100 个 PPPoE 会话。

4. 在系统视图配置允许创建 PPPoE 会话的最大数目

- (1) 进入系统视图。

```
system-view
```

- (2) 配置允许创建 PPPoE 会话的最大数目。

（独立运行模式）

```
pppoe-server session-limit slot slot-number total number
```

（IRF 模式）

```
pppoe-server session-limit chassis chassis-number slot slot-number  
total number
```

缺省情况下，不限制允许创建的 PPPoE 会话数目。

3.4.6 配置限制用户创建 PPPoE 会话的速度

1. 功能简介

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

系统使用监控表和扼制表来共同控制用户创建会话的速度：

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

2. 配置限制和指导

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

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
```

该接口为启用 PPPoE Server 协议的接口。

- (3) 配置接口允许每个用户创建会话的速度。

```
pppoe-server throttle per-mac session-requests session-request-period
blocking-period
```

缺省情况下，不限制会话建立的速度。

3.4.7 配置PPPoE会话的NAS-PORT-ID属性相关参数

1. 功能简介

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

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

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
```

该接口为启用 PPPoE Server 协议的接口。

- (3) 配置上传给 RADIUS 服务器的 NAS-PORT-ID 属性中包含的内容。

```
pppoe-server access-line-id content { all [ separator ] | circuit-id |
remote-id }
```

缺省情况下，上传给 RADIUS 服务器的 NAS-PORT-ID 属性中仅包含 circuit-id。

- (4) 配置在 NAS-PORT-ID 属性中自动插入 BAS 信息。

```
pppoe-server access-line-id bas-info [ cn-163 ]
```

缺省情况下，在 NAS-PORT-ID 属性中不自动插入 BAS 信息。

- (5) 配置设备信任接收到的报文中的接入线路 ID 的内容。

```
pppoe-server access-line-id trust
```

缺省情况下，设备不信任接收到的报文中的接入线路 ID 的内容。

- (6) 配置接入线路 ID 中 circuit-id 的解析格式。

```
pppoe-server access-line-id circuit-id parse-mode { cn-telecom |
tr-101 }
```

缺省情况下，接入线路 ID 中 circuit-id 的解析格式为 TR-101 格式。

- (7) 配置接入线路 ID 中 circuit-id 的传输格式。

```
pppoe-server access-line-id circuit-id trans-format { ascii | hex }
```

缺省情况下，接入线路 ID 中 circuit-id 的传输格式为字符串格式。

- (8) 配置接入线路 ID 中 remote-id 的传输格式。

```
pppoe-server access-line-id remote-id trans-format { ascii | hex }
```

缺省情况下，接入线路 ID 中 remote-id 的传输格式为字符串格式。

3.5 配置PPPoE Client

3.5.1 工作模式介绍

PPPoE 会话有三种工作模式：永久在线模式、按需拨号模式、诊断模式。

- 永久在线模式：当物理线路 up 后，设备会立即发起 PPPoE 呼叫，建立 PPPoE 会话。除非用户删除 PPPoE 会话，否则此 PPPoE 会话将一直存在。
- 按需拨号模式：当物理线路 up 后，设备不会立即发起 PPPoE 呼叫，只有当有数据需要传送时，设备才会发起 PPPoE 呼叫，建立 PPPoE 会话。如果 PPPoE 链路的空闲时间超过用户配置的值，设备会自动中止 PPPoE 会话。
- 诊断模式：设备在配置完成后立即发起 PPPoE 呼叫，建立 PPPoE 会话。每隔用户配置的重建时间间隔，设备会自动断开该会话、并重新发起呼叫建立会话。通过定期建立、删除 PPPoE 会话，可以监控 PPPoE 链路是否处于正常工作状态。

PPPoE 会话的工作模式由对应的拨号接口的配置决定：

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

3.5.2 PPPoE Client配置任务简介

PPPoE Client 配置任务如下：

- (1) [配置拨号接口](#)
- (2) [配置PPPoE会话](#)
- (3) （可选）[复位PPPoE会话](#)

3.5.3 配置拨号接口

1. 功能简介

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

关于拨号接口、Dialer 接口、共享 DDR、Dialer bundle 的详细介绍和相关配置，请参见“二层技术-广域网接入配置指导”中的“DDR”。

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 创建拨号访问组，并配置拨号控制规则。

```
dialer-group group-number rule { ip | ipv6 } { deny | permit | acl  
{ acl-number | name acl-name } }
```

仅工作在按需拨号模式下需要配置本命令。

- (3) 创建 Dialer 接口，并进入该 Dialer 接口视图。

```
interface dialer number
```

- (4) 配置接口 IP 地址。

```
ip address { address mask | ppp-negotiate }
```

缺省情况下，接口未配置 IP 地址。

- (5) 开启共享 DDR。

```
dialer bundle enable
```

缺省情况下，接口上未开启共享 DDR。

- (6) 配置该拨号接口关联的拨号访问组，将该接口与拨号控制规则关联起来。

```
dialer-group group-number
```

缺省情况下，接口不与任何拨号访问组相关联。

仅工作在按需拨号模式下需要配置本命令。

- (7) 配置链路空闲时间。

```
dialer timer idle idle [ in | in-out ]
```

缺省情况下，链路空闲时间为 120 秒。

未配置 **dialer diagnose** 时，当 *idle* 配置为 0 时，PPPoE 会话工作在永久在线模式下，不为 0 时工作在按需拨号模式下。

- (8) 配置 DDR 应用工作在诊断模式。

```
dialer diagnose [ interval interval ]
```

缺省情况下，工作在非诊断模式。

仅工作在诊断模式下需要配置本命令。

- (9) （可选）配置 DDR 自动拨号的间隔时间。

```
dialer timer autodial autodial-interval
```

缺省情况下，DDR 自动拨号的间隔时间为 300 秒。

当链路断开后将启动自动拨号定时器，等待自动拨号定时器超后再重新发起呼叫。

为了在链路断开时可以尽快自动重新拨号，建议将自动拨号的时间间隔配置的小一些。

- (10) （可选）配置 Dialer 接口的 MTU 值。

```
mtu size
```

缺省情况下，Dialer 接口的 MTU 值为 1500 字节。

对于 PPPoE Client 应用的 Dialer 接口，应修改其 MTU 值，保证分片后的报文加上 2 个字节的 PPP 头和 6 个字节的 PPPoE 头之后的总长度不超过对应 PPPoE 会话所在接口的 MTU 值。

3.5.4 配置 PPPoE 会话

1. 功能简介

当成功建立 PPPoE 会话后，系统将自动创建一个 VA 接口，用于和对端进行报文交互。VA 接口支持通过 **display interface virtual-access** 命令查看接口相关信息，但不支持对该接口进行配置。

VA 接口随着 PPPoE 会话的建立，由系统自动创建，PPPoE 会话拆除后，系统自动删除。

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) 建立一个 PPPoE 会话，并且指定该会话所对应的 Dialer bundle。

```
pppoe-client dial-bundle-number number [ no-hostuniq ]
```

该 Dialer bundle 的序号 *number* 需要与 Dialer 接口的编号相同。

3.5.5 复位PPPoE会话

1. 功能简介

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

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

2. 配置步骤

请在用户视图下执行本命令，复位 PPPoE 会话。

```
reset pppoe-client { all | dial-bundle-number number }
```

3.6 PPPoE显示和维护

3.6.1 PPPoE Server显示和维护

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

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

表3-1 PPPoE Server 显示和维护

操作	命令
显示PPPoE的协商报文统计信息	(独立运行模式) display pppoe-server packet statistics [slot slot-number] (IRF模式) display pppoe-server packet statistics [chassis chassis-number slot slot-number]
显示PPPoE会话的数据报文统计信息	(独立运行模式) display pppoe-server session packet { slot slot-number interface interface-type interface-number } (IRF模式) display pppoe-server session packet { chassis chassis-number slot slot-number interface

操作	命令
	<code>interface-type interface-number }</code>
显示PPPoE会话的摘要信息	(独立运行模式) <code>display pppoe-server session summary { slot slot-number interface interface-type interface-number }</code> (IRF模式) <code>display pppoe-server session summary { chassis chassis-number slot slot-number interface interface-type interface-number }</code>
显示被扼制的用户信息	(独立运行模式) <code>display pppoe-server throttled-mac { slot slot-number interface interface-type interface-number }</code> (IRF模式) <code>display pppoe-server throttled-mac { chassis chassis-number slot slot-number interface interface-type interface-number }</code>
显示VA池信息	<code>display pppoe-server va-pool</code>
清除PPPoE会话	<code>reset pppoe-server { all interface interface-type interface-number virtual-template number }</code>
清除PPPoE的协商报文统计信息	(独立运行模式) <code>reset pppoe-server packet statistics [slot slot-number]</code> (IRF模式) <code>reset pppoe-server packet statistics [chassis chassis-number slot slot-number]</code>

3.6.2 PPPoE Client显示和维护

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

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

表3-2 PPPoE Client 显示和维护

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

3.7 PPPoE典型配置举例

3.7.1 PPPoE Server通过PPP地址池为用户分配IPv4 地址配置举例

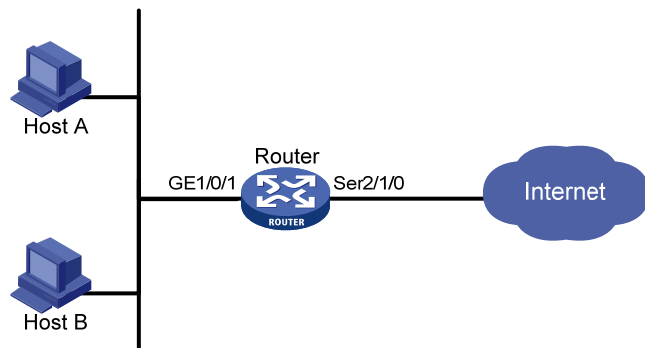
1. 组网需求

要求以太网内的主机可以通过 PPPoE 接入 Router，并连接到外部网络。

- 主机作为 PPPoE Client，运行 PPPoE 客户端拨号软件。
- Router 作为 PPPoE Server，配置本地 CHAP 认证，并通过 PPP 地址池为主机分配 IP 地址。

2. 组网图

图3-3 PPPoE Server 通过 PPP 地址池为用户分配 IPv4 地址配置组网图



3. 配置步骤

创建一个 PPPoE 用户。

```
<Router> system-view
[Router] local-user user1 class network
[Router-luser-network-user1] password simple pass1
[Router-luser-network-user1] service-type ppp
[Router-luser-network-user1] quit
```

配置虚拟模板接口 1 的参数，采用 CHAP 认证对端，并使用 PPP 地址池为对端分配 IP 地址，并配置为对端指定 DNS 服务器的 IP 地址。

```
[Router] interface virtual-template 1
[Router-Virtual-Template1] ppp authentication-mode chap domain system
[Router-Virtual-Template1] ppp chap user user1
[Router-Virtual-Template1] remote address pool 1
[Router-Virtual-Template1] ppp ipcp dns 8.8.8.8
[Router-Virtual-Template1] quit
```

配置 PPP 地址池（包含 9 个可分配的 IP 地址），和地址池网关地址。

```
[Router] ip pool 1 1.1.1.2 1.1.1.10
[Router] ip pool 1 gateway 1.1.1.1
```

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

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

在系统缺省的 ISP 域 system 下，配置域用户使用本地认证方案。

```
[Router] domain system
[Router-isp-system] authentication ppp local
[Router-isp-system] quit
```

4. 验证配置

以太网上各主机安装 PPPoE 客户端软件后，配置好用户名和密码（此处为 user1 和 pass1）就能使用 PPPoE 协议，通过设备 Router 接入到 Internet。

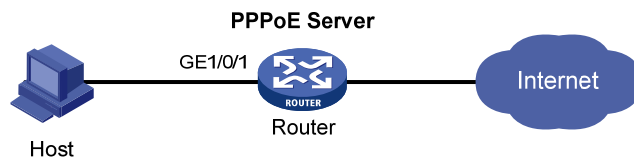
3.7.2 PPPoE Server通过本地DHCP服务器为用户分配IP地址配置举例

1. 组网需求

Host 和 Router 之间通过以太网接口相连, Host 通过 PPPoE 接入 Router, Router 作为 PPPoE Server 通过 DHCPv4 协议为 Host 分配 IP 地址。

2. 组网图

图3-4 配置 PPPoE Server 通过本地 DHCP 服务器为用户分配 IP 地址组网图



3. 配置步骤

配置虚拟模板接口 10 的参数，采用 PAP 认证对端，使用 DHCP 地址池 pool1 为用户分配 IP 地址及 DNS 服务器地址。

```
<Router> system-view
[Router] interface virtual-template 10
[Router-Virtual-Template10] ppp authentication-mode pap
[Router-Virtual-Template10] remote address pool pool1
[Router-Virtual-Template10] quit
```

在 GigabitEthernet1/0/1 接口上启用 PPPoE Server 协议，将该以太网接口与虚拟模板接口 10 绑定。

```
[Router] interface gigabitethernet 1/0/1
[Router-GigabitEthernet1/0/1] pppoe-server bind virtual-template 10
[Router-GigabitEthernet1/0/1] quit
```

启用 DHCP 服务。

```
[Router] dhcp enable
```

配置 DHCP 地址池 pool1。

```
[Router] dhcp server ip-pool pool1
[Router-dhcp-pool-pool1] network 1.1.1.0 24
[Router-dhcp-pool-pool1] gateway-list 1.1.1.1 export-route
[Router-dhcp-pool-pool1] dns-list 8.8.8.8
```

将 IP 地址 1.1.1.1 配置为禁用地址。

```
[Router-dhcp-pool-pool1] forbidden-ip 1.1.1.1
[Router-dhcp-pool-pool1] quit
```

配置 PPPoE 用户。

```
[Router] local-user user1 class network
[Router-luser-network-user1] password simple pass1
[Router-luser-network-user1] service-type ppp
[Router-luser-network-user1] quit
```

4. 验证配置

配置完成后，当 Host 使用用户名 user1、密码 pass1，通过 PPPoE 接入 Router 后，Router 通过 DHCPv4 协议为 Host 分配一个 IP 地址。

显示所有 DHCP 地址绑定信息。

```
[Router] display dhcp server ip-in-use
IP address      Client identifier/      Lease expiration      Type
                Hardware address
1.1.1.2         3030-3030-2e30-3030-   Unlimited            Auto(C)
                662e-3030-3033-2d45-
                7468-6572-6e65-74
```

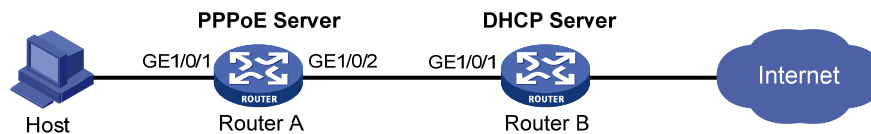
3.7.3 PPPoE Server通过远端DHCP服务器为用户分配IP地址配置举例

1. 组网需求

Host 和 Router A 之间通过以太网接口相连，Router B 为远端 DHCP 服务器。Host 通过 PPPoE 接入 Router A，Router A 作为 PPPoE Server、DHCP 中继向远端 DHCP 服务器申请 IP 地址。

2. 组网图

图3-5 PPPoE Server 通过远端 DHCP 服务器为用户分配 IP 地址组网图



3. 配置步骤

(1) 配置 Router A (PPPoE Server)

配置虚拟模板接口 10 的参数，采用 PAP 认证对端，使用 DHCP 地址池 pool1 为用户分配 IP 地址。

```
<RouterA> system-view
[RouterA] interface virtual-template 10
[RouterA-Virtual-Template10] ppp authentication-mode pap
[RouterA-Virtual-Template10] remote address pool pool1
[RouterA-Virtual-Template10] quit
```

在 GigabitEthernet1/0/1 接口上启用 PPPoE Server 协议，将该以太网接口与虚拟模板接口 10 绑定。

```
[RouterA] interface gigabitethernet 1/0/1
[RouterA-GigabitEthernet1/0/1] pppoe-server bind virtual-template 10
[RouterA-GigabitEthernet1/0/1] quit
```

启用 DHCP 服务。

```

[RouterA] dhcp enable
# 启用 DHCP 中继的用户地址表项记录功能。
[RouterA] dhcp relay client-information record
# 创建中继地址池 pool1，指定匹配该地址池的 DHCPv4 客户端所在的网段地址，并指定中继地址池对应的 DHCP 服务器地址。
[RouterA] dhcp server ip-pool pool1
[RouterA-dhcp-pool-pool1] gateway-list 2.2.2.1 export-route
[RouterA-dhcp-pool-pool1] remote-server 10.1.1.1
[RouterA-dhcp-pool-pool1] quit
# 配置与 DHCP 服务器连接的 GigabitEthernet1/0/2 接口的 IP 地址。
[RouterA] interface gigabitethernet 1/0/2
[RouterA-GigabitEthernet1/0/2] ip address 10.1.1.2 24
[RouterA-GigabitEthernet1/0/2] quit
# 配置 PPPoE 用户。
[RouterA] local-user user1 class network
[RouterA-luser-network-user1] password simple pass1
[RouterA-luser-network-user1] service-type ppp
[RouterA-luser-network-user1] quit

```

(2) 配置 Router B（DHCP 服务器）

```

# 启用 DHCP 服务。
<RouterB> system-view
[RouterB] dhcp enable
# 创建 DHCP 地址池 pool1，配置为 DHCP 客户端分配的 IP 地址网段和网关地址。
[RouterB] dhcp server ip-pool pool1
[RouterB-dhcp-pool-pool1] network 2.2.2.0 24
[RouterB-dhcp-pool-pool1] gateway-list 2.2.2.1
[RouterB-dhcp-pool-pool1] dns-list 8.8.8.8
# 将 IP 地址 2.2.2.1 配置为禁用地址。
[RouterB-dhcp-pool-pool1] forbidden-ip 2.2.2.1
[RouterB-dhcp-pool-pool1] quit
# 配置与 PPPoE Server 连接的 GigabitEthernet1/0/1 接口的 IP 地址。
[RouterB] interface gigabitethernet 1/0/1
[RouterB-GigabitEthernet1/0/1] ip address 10.1.1.1 24
[RouterB-GigabitEthernet1/0/1] quit
# 配置到 PPPoE Server 的静态路由。
[RouterB] ip route-static 2.2.2.0 24 10.1.1.2

```

4. 验证配置

配置完成后，当 Host 使用用户名 user1、密码 pass1，通过 PPPoE 接入 Router A 后，Router B 通过 DHCPv4 协议为 Host 分配一个 IP 地址。

显示 DHCP 中继 Router A 的用户地址表项信息。

```

[RouterA] display dhcp relay client-information
Total number of client-information items: 1
Total number of dynamic items: 1
Total number of temporary items: 0

```

IP address	MAC address	Type	Interface	VPN name
2.2.2.3	00e0-0000-0001	Dynamic	VA0	N/A

显示 DHCP 服务器 Router B 的 DHCP 地址绑定信息。

```
[RouterB] display dhcp server ip-in-use
```

IP address	Client identifier/ Hardware address	Lease expiration	Type
2.2.2.3	00e0-0000-0001	Unlimited	Auto(C)

3.7.4 PPPoE Server通过ND协议、IPv6CP协商生成信息用于用户生成IPv6 地址配置举例

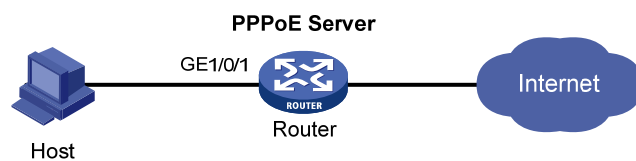
1. 组网需求

Host 和 Router 之间通过以太网接口相连, Host 通过 PPPoE 接入 Router, Router 作为 PPPoE Server 通过 ND 协议为 Host 分配 IPv6 地址。

在该场景下, Host 通过 ND 协议中的 RA 报文获得 IPv6 地址前缀, 通过 IPv6CP 协商获取 IPv6 接口标识, 二者组合生成 IPv6 全球单播地址。

2. 组网图

图3-6 配置 PPPoE Server 通过 ND 协议、IPv6CP 协商生成信息用于用户生成 IPv6 地址组网图



3. 配置步骤

配置虚拟模板接口 10 的参数, 采用 PAP 认证对端, 配置本端 IPv6 地址, 关闭对 RA 消息发布的抑制。

```
<Router> system-view
[Router] interface virtual-template 10
[Router-Virtual-Template10] ppp authentication-mode pap domain system
[Router-Virtual-Template10] ipv6 address 2001::1 64
[Router-Virtual-Template10] undo ipv6 nd ra halt
[Router-Virtual-Template10] quit
```

在 GigabitEthernet1/0/1 接口上启用 PPPoE Server 协议, 将该以太网接口与虚拟模板接口 10 绑定。

```
[Router] interface gigabitethernet 1/0/1
[Router-GigabitEthernet1/0/1] pppoe-server bind virtual-template 10
[Router-GigabitEthernet1/0/1] quit
```

配置 PPPoE 用户。

```
[Router] local-user user1 class network
[Router-luser-network-user1] password simple pass1
[Router-luser-network-user1] service-type ppp
[Router-luser-network-user1] quit
```

在 ISP 域下配置为用户授权 IPv6 前缀属性。

```
[Router] domain system
```

```
[Router-isp-system] authorization-attribute ipv6-prefix 2003:: 64
[Router-isp-system] quit
```

4. 验证配置

配置完成后,当 Host 使用用户名 user1、密码 pass1,通过 PPPoE 接入 Router 后,通过授权的 IPv6 前缀和 IPv6CP 协商获取的 IPv6 接口标识就自动生成一个 IPv6 全球单播地址。

```
[Router] display ppp access-user interface gigabitethernet 1/0/1
Interface Username   MAC address   IP address   IPv6 address   IPv6 PDPrefix
VA0          user1         0000-5e08-9d00 -             2003::9CBC:3898:0:605 -
```

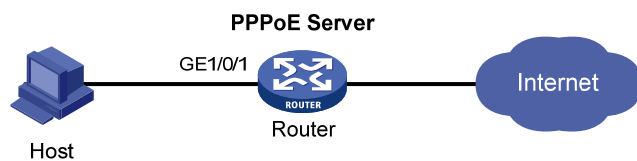
3.7.5 PPPoE Server通过DHCPv6 协议为用户分配IPv6 地址配置举例

1. 组网需求

Host 和 Router 之间通过以太网接口相连,Host 通过 PPPoE 接入 Router,Router 作为 PPPoE Server 通过 DHCPv6 协议为 Host 分配 IPv6 地址。

2. 组网图

图3-7 配置 PPPoE Server 通过 DHCPv6 协议为用户分配 IPv6 地址组网图



3. 配置步骤

配置虚拟模板接口 10 的参数,采用 PAP 认证对端,配置本端 IPv6 地址,关闭对 RA 消息发布的抑制,配置主机通过 DHCPv6 协议获取 IPv6 地址。

```
<Router> system-view
[Router] interface virtual-template 10
[Router-Virtual-Template10] ppp authentication-mode pap domain system
[Router-Virtual-Template10] ipv6 address 3001::1 64
[Router-Virtual-Template10] undo ipv6 nd ra halt
[Router-Virtual-Template10] ipv6 nd autoconfig managed-address-flag
```

开启 DHCPv6 Server 功能。

```
[Router-Virtual-Template10] ipv6 dhcp select server
[Router-Virtual-Template10] quit
```

在 GigabitEthernet1/0/1 接口上启用 PPPoE Server 协议,将该以太网接口与虚拟模板接口 10 绑定。

```
[Router] interface gigabitethernet 1/0/1
[Router-GigabitEthernet1/0/1] pppoe-server bind virtual-template 10
[Router-GigabitEthernet1/0/1] quit
```

创建名称为 pool1 的 DHCPv6 地址池,配置 DHCPv6 地址池动态分配的地址网段为 3001::/32,分配的 DNS 服务器地址为 2001:2::3。

```
[Router] ipv6 dhcp pool pool1
[Router-dhcp6-pool-pool1] network 3001::/32
[Router-dhcp6-pool-pool1] dns-server 2001:2::3
```

```
[Router-dhcp6-pool-pool1] quit
# 配置 PPPoE 用户。
[Router] local-user user1 class network
[Router-luser-network-user1] password simple pass1
[Router-luser-network-user1] service-type ppp
[Router-luser-network-user1] quit
# 在 ISP 域下配置为用户授权地址池属性。
[Router] domain system
[Router-isp-system] authorization-attribute ipv6-pool pool1
[Router-isp-system] quit
```

4. 验证配置

配置完成后，当 Host 使用用户名 user1、密码 pass1，通过 PPPoE 接入 Router 后，Router 通过 DHCPv6 协议为 Host 分配一个 IPv6 全球单播地址。

```
[Router] display ppp access-user interface gigabitethernet 1/0/1
Interface Username   MAC address      IP address  IPv6 address  IPv6 PDPrefix
VA0          user1            0000-5e08-9d00  -            3001::2       -
```

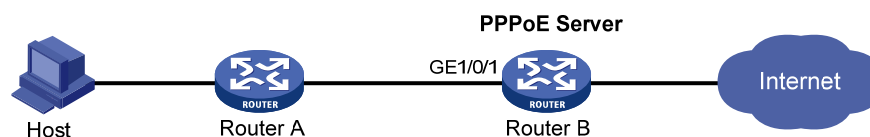
3.7.6 PPPoE Server通过DHCPv6 协议分配代理前缀用于用户生成IPv6 地址配置举例

1. 组网需求

Router A 和 Router B 之间通过以太网接口相连，Router A 通过 PPPoE 接入 Router B，Router B 作为 PPPoE Server 通过 DHCPv6 协议给 Router A 分配代理前缀，Router A 再通过代理前缀给下面的主机分配 IPv6 地址。

2. 组网图

图3-8 配置 PPPoE Server 通过 DHCPv6 协议分配代理前缀用于用户生成 IPv6 地址组网图



3. 配置步骤

配置虚拟模板接口 10 的参数，采用 PAP 认证对端，配置本端 IPv6 地址，关闭对 RA 消息发布的抑制。

```
<RouterB> system-view
[RouterB] interface virtual-template 10
[RouterB-Virtual-Template10] ppp authentication-mode pap domain system
[RouterB-Virtual-Template10] ipv6 address 2001::1 64
[RouterB-Virtual-Template10] undo ipv6 nd ra halt
```

开启 DHCPv6 Server 功能。

```
[RouterB-Virtual-Template10] ipv6 dhcp select server
[RouterB-Virtual-Template10] quit
```

在 GigabitEthernet1/0/1 接口上启用 PPPoE Server 协议，将该以太网接口与虚拟模板接口 10 绑定。

```
[RouterB] interface gigabitethernet 1/0/1
[RouterB-GigabitEthernet1/0/1] pppoe-server bind virtual-template 10
[RouterB-GigabitEthernet1/0/1] quit
```

配置 DHCPv6 前缀池 6，包含的前缀为 4001::/32，分配的前缀长度为 42。

```
[RouterB] ipv6 dhcp prefix-pool 6 prefix 4001::/32 assign-len 42
```

创建名称为 pool1 的 DHCPv6 地址池，配置地址池网段为 4001::/64，在地址池下引用前缀池 6，分配的 DNS 服务器地址为 2:2::3。

```
[RouterB] ipv6 dhcp pool pool1
[RouterB-dhcp6-pool-pool1] network 4001::/64
[RouterB-dhcp6-pool-pool1] prefix-pool 6
[RouterB-dhcp6-pool-pool1] dns-server 2:2::3
[RouterB-dhcp6-pool-pool1] quit
```

配置 PPPoE 用户。

```
[RouterB] local-user user1 class network
[RouterB-luser-network-user1] password simple pass1
[RouterB-luser-network-user1] service-type ppp
[RouterB-luser-network-user1] quit
```

在 ISP 域下配置为用户授权地址池属性。

```
[RouterB] domain system
[RouterB-isp-system] authorization-attribute ipv6-pool pool1
```

4. 验证配置

配置完成后，当 Router A 使用用户名 user1、密码 pass1，通过 PPPoE 接入 Router B 后，Router B 通过 DHCPv6 协议为 Router A 分配一个代理前缀。

显示 DHCPv6 前缀绑定信息。

```
[RouterB] display ipv6 dhcp server pd-in-use
Pool: 1
IPv6 prefix                                Type      Lease expiration
-----
4001::1/42                                  Auto(O)   Jul 10 19:45:01 2013
```

Router A 把分配到的代理前缀 4001::1/42 再分配给 Host，Host 用来生成 IPv6 全球单播地址。

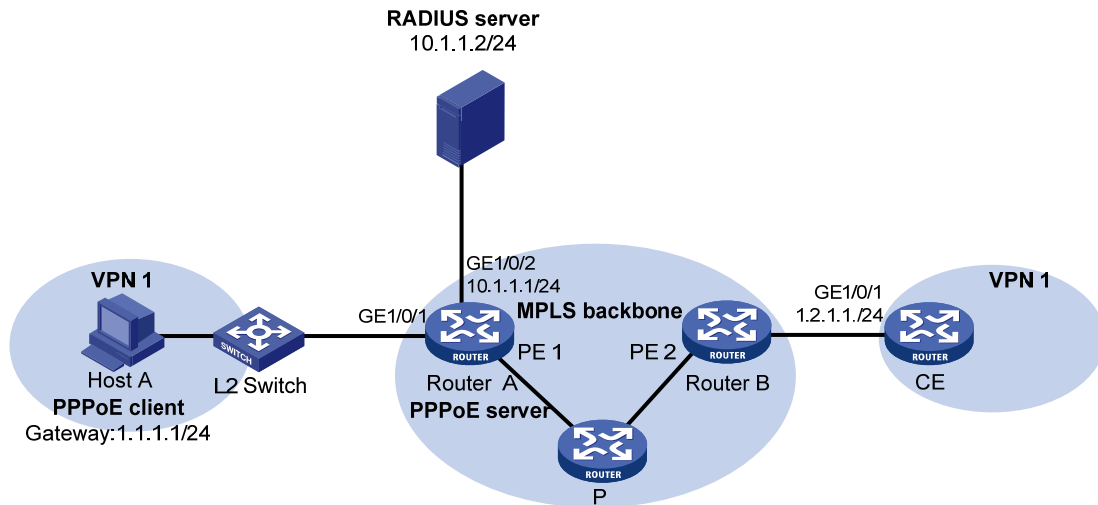
3.7.7 PPPoE Server为接入用户授权地址池和VPN配置举例

1. 组网需求

- 采用 RADIUS 作为认证、授权和计费服务器。
- RADIUS 服务器为 PPPoE 接入用户授权的 PPP 地址池和 VPN 实例分别为 pool1、vpn1。
- vpn1 中的用户在服务器授权的 PPP 地址池 pool1 中获取 IP 地址。

2. 组网图

图3-9 PPPoE Server 为接入用户授权地址池和 VPN 配置组网图



3. 配置步骤



说明

启动 PPPoE 功能之前，需要首先配置 MPLS L3VPN 功能，通过为两端的 VPN 1 指定匹配的 VPN Target，确保两端的 VPN 1 之间可以互通。本例仅介绍连接客户端的 PE 1 上接入认证的相关配置，其它配置请参考“MPLS 配置指导”中的“MPLS L3VPN”。

(1) 配置 RADIUS 服务器



说明

下面以 Linux 系统下的 Free RADIUS 服务器为例，说明 RADIUS 服务器的基本配置。

配置 RADIUS 客户端信息。

在 `clients.conf` 文件中增加如下信息：

```
client 10.1.1.1/24 {
    secret = radius
    shortname = sr88
}
```

以上信息表示：RADIUS 客户端的 IP 地址为 10.1.1.1，共享密钥为字符串 `radius`。

配置合法用户信息。

在 `users` 文件中增加如下信息：

```
user1 Auth-Type == CHAP,User-Password := pass1
      Service-Type = Framed-User,
      Framed-Protocol = PPP,
      Framed-Pool = "pool1",
```

```
H3C-VPN-Instance = "vpn1",
```

以上信息表示：用户名为 **user1**，用户密码为字符串 **pass1**，授权 VPN 实例名称为 **vpn1**，授权 IP 地址池名称为 **pool1**。

(2) 配置 Router A

○ 配置 PPPoE Server

配置虚拟模板接口 1 的参数，采用 CHAP 认证对端，并使用 ISP 域 dm1 作为认证域。

```
<RouterA> system-view
[RouterA] interface virtual-template 1
[RouterA-Virtual-Template1] ppp authentication-mode chap domain dm1
[RouterA-Virtual-Template1] quit
```

创建名为 **pool1** 的 PPP 地址池（包含 9 个可分配的 IP 地址）。

```
[RouterA] ip pool pool1 1.1.1.2 1.1.1.10 group 1
```

配置 PPP 地址池 **pool1** 的网关地址为 **1.1.1.1**，所在 VPN 实例为 **vpn1**。

```
[RouterA] ip pool pool1 gateway 1.1.1.1 vpn-instance vpn1
```

配置 PPP 地址池路由。

```
[RouterA] ppp ip-pool route 1.1.1.1 24 vpn-instance vpn1
```

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

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

○ 配置 RADIUS 方案

创建名称为 **rs1** 的 RADIUS 方案并进入该方案视图。

```
[RouterA] radius scheme rs1
```

配置 RADIUS 方案的主认证和主计费服务器及其通信密钥。

```
[RouterA-radius-rs1] primary authentication 10.1.1.2
[RouterA-radius-rs1] primary accounting 10.1.1.2
[RouterA-radius-rs1] key authentication simple radius
[RouterA-radius-rs1] key accounting simple radius
```

配置发送给 RADIUS 服务器的用户名不携带 ISP 域名。

```
[RouterA-radius-rs1] user-name-format without-domain
[RouterA-radius-rs1] quit
```

○ 配置认证域

创建并进入名称为 **dm1** 的 ISP 域。

```
[RouterA] domain dm1
```

配置 ISP 域使用的 RADIUS 方案 **rs1**。

```
[RouterA-isp-dm1] authentication ppp radius-scheme rs1
[RouterA-isp-dm1] authorization ppp radius-scheme rs1
[RouterA-isp-dm1] accounting ppp radius-scheme rs1
[RouterA-isp-dm1] quit
```

4. 验证配置

用户认证通过后，在 **Host A** 上可以 Ping 通对端 VPN1 中的 CE。

在 **Router A** 上可以看到 PPP 地址池 **pool1** 中已为 PPPoE Client 分配了一个地址。

```
[RouterA] display ip pool pool1
Group name: 1
Pool name      Start IP address  End IP address  Free  In use
pool1          1.1.1.2          1.1.1.10       8     1
In use IP addresses:
IP address      Interface
1.1.1.2        VA0
```

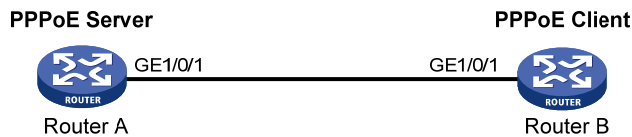
3.7.8 PPPoE Client永久在线模式配置举例

1. 组网需求

Router A 和 Router B 之间通过各自的 GigabitEthernet1/0/1 接口相连，其中 Router A 作为 PPPoE Server，Router B 作为 PPPoE Client 工作在永久在线模式。

2. 组网图

图3-10 PPPoE Client 组网图



3. 配置步骤

(1) 配置 Router A 作为 PPPoE Server

配置虚拟模板接口 1 的 IP 地址，并指定为对端分配的 IP 地址。

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

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

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

(2) 配置 Router B 作为 PPPoE Client

在 Dialer1 接口上开启共享 DDR。

```
<RouterB> system-view
[RouterB] interface dialer 1
[RouterB-Dialer1] dialer bundle enable
```

配置 Dialer1 接口通过协商获取 IP 地址。

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

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

```
[RouterB] interface gigabitethernet 1/0/1
```

```

[RouterB-GigabitEthernet1/0/1] pppoe-client dial-bundle-number 1
[RouterB-GigabitEthernet1/0/1] quit
# 配置 PPPoE Client 工作在永久在线模式。
[RouterB] interface dialer 1
[RouterB-Dialer1] dialer timer idle 0
# 配置 DDR 自动拨号的间隔时间为 60 秒。
[RouterB-Dialer1] dialer timer autodial 60
[RouterB-Dialer1] quit
# 配置静态路由。
[RouterB] ip route-static 1.1.1.1 255.0.0.0 dialer 1

```

4. 验证配置

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

```

[RouterB-Dialer1] display pppoe-client session summary

```

Bundle ID	Interface	VA	RemoteMAC	LocalMAC	State	
1	1	GE1/0/1	VA0	00e0-1400-4300	00e0-1500-4100	SESSION

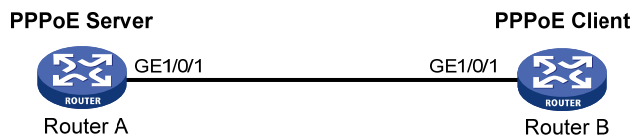
3.7.9 PPPoE Client按需拨号模式配置举例

1. 组网需求

Router A 和 Router B 之间通过各自的 GigabitEthernet1/0/1 接口相连，其中 Router A 作为 PPPoE Server，Router B 作为 PPPoE Client 工作在按需拨号模式，空闲时间间隔为 150 秒。

2. 组网图

图3-11 PPPoE Client 组网图



3. 配置步骤

(1) 配置 Router A 作为 PPPoE Server

配置虚拟模板接口 1 的 IP 地址，并指定为对端分配的 IP 地址。

```

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

```

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

```

[RouterA] interface gigabitethernet 1/0/1
[RouterA-GigabitEthernet1/0/1] pppoe-server bind virtual-template 1
[RouterA-GigabitEthernet1/0/1] quit

```

(2) 配置 Router B 作为 PPPoE Client

```

# 配置拨号访问组 1 以及对应的拨号访问控制条件。
<RouterB> system-view
[RouterB] dialer-group 1 rule ip permit
# 在 Dialer1 接口上开启共享 DDR。
[RouterB] interface dialer 1
[RouterB-Dialer1] dialer bundle enable
# 将 Dialer1 接口与拨号访问组 1 关联。
[RouterB-Dialer1] dialer-group 1
# 配置 Dialer1 接口通过协商获取 IP 地址。
[RouterB-Dialer1] ip address ppp-negotiate
[RouterB-Dialer1] quit
# 配置一个 PPPoE 会话，该会话对应 Dialer bundle 1（Dialer bundle 1 对应 Dialer1 接口）。
[RouterB] interface gigabitethernet 1/0/1
[RouterB-GigabitEthernet1/0/1] pppoe-client dial-bundle-number 1
[RouterB-GigabitEthernet1/0/1] quit
# 配置静态路由。
[RouterB] ip route-static 1.1.1.1 255.0.0.0 dialer 1
# 配置空闲时间间隔为 150 秒。
[RouterB] interface dialer 1
[RouterB-Dialer1] dialer timer idle 150
[RouterB-Dialer1] quit

```

4. 验证配置

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

```

[RouterB-Dialer1] display pppoe-client session summary

```

Bundle ID	Interface	VA	RemoteMAC	LocalMAC	State	
1	1	GE1/0/1	VA0	00e0-1400-4300	00e0-1500-4100	SESSION

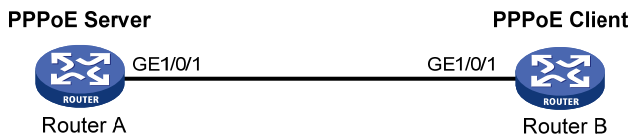
3.7.10 PPPoE Client 诊断模式配置举例

1. 组网需求

Router A 和 Router B 之间通过各自的 GigabitEthernet1/0/1 接口相连，其中 Router A 作为 PPPoE Server，Router B 作为 PPPoE Client 工作在诊断模式，诊断时间间隔为 200 秒。

2. 组网图

图3-12 PPPoE Client 组网图



3. 配置步骤

(1) 配置 Router A 作为 PPPoE Server

```

# 配置虚拟模板接口 1 的 IP 地址，并指定为对端分配的 IP 地址。

```

```

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

```

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

```

[RouterA] interface gigabitethernet 1/0/1
[RouterA-GigabitEthernet1/0/1] pppoe-server bind virtual-template 1
[RouterA-GigabitEthernet1/0/1] quit

```

(2) 配置 Router B 作为 PPPoE Client

在 Dialer1 接口上开启共享 DDR。

```

<RouterB> system-view
[RouterB] interface dialer 1
[RouterB-Dialer1] dialer bundle enable
# 配置 Dialer1 接口通过协商获取 IP 地址。
[RouterB-Dialer1] ip address ppp-negotiate
[RouterB-Dialer1] quit

```

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

```

[RouterB] interface gigabitethernet 1/0/1
[RouterB-GigabitEthernet1/0/1] pppoe-client dial-bundle-number 1
[RouterB-GigabitEthernet1/0/1] quit

```

PPPoE Client 工作在诊断模式，诊断时间间隔为 200 秒。

```

[RouterB] interface dialer 1
[RouterB-Dialer1] dialer diagnose interval 200

```

配置自动拨号的时间间隔为 10 秒。

```

[RouterB-Dialer1] dialer timer autodial 10

```

4. 验证配置

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

```

[RouterB-Dialer1] display pppoe-client session summary

```

Bundle ID	Interface	VA	RemoteMAC	LocalMAC	State	
1	1	GE1/0/1	VA0	00e0-1400-4300	00e0-1500-4100	SESSION

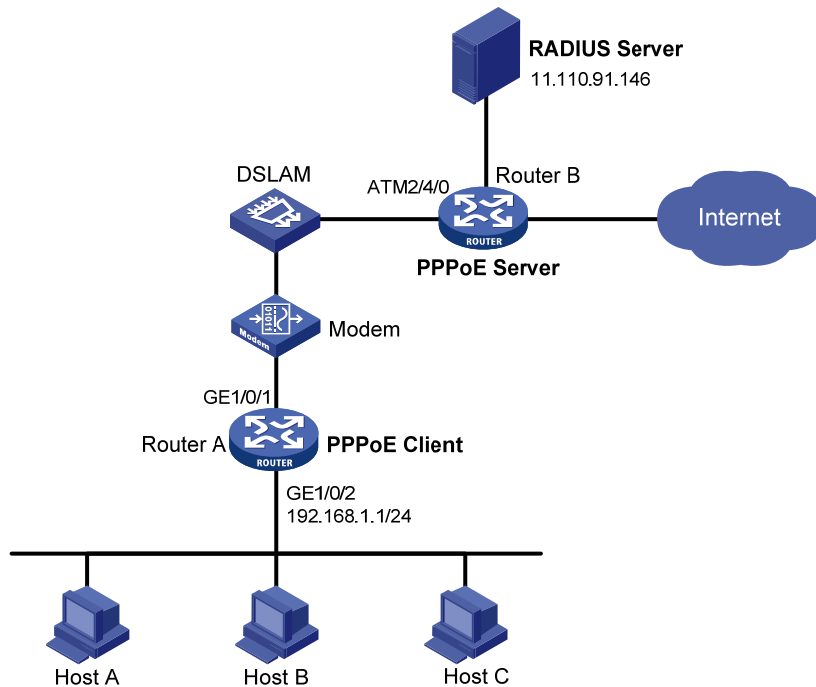
3.7.11 利用ADSL Modem将局域网接入Internet

1. 组网需求

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

2. 组网图

图3-13 利用 ADSL 将局域网接入 Internet 组网图



3. 配置步骤

(1) 配置 Router A 作为 PPPoE Client

配置拨号访问组 1 以及对应的拨号访问控制条件。

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

在 Dialer1 接口上开启共享 DDR。

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

将 Dialer1 接口与拨号访问组 1 关联。

```
[RouterA-Dialer1] dialer-group 1  
# 配置 Dialer1 接口通过协商获取 IP 地址。
```

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

配置 PPPoE Client 工作在永久在线模式。

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

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

配置 PPPoE 会话。

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

配置局域网接口的 IP 地址。

```
[RouterA] interface gigabitethernet 1/0/2
[RouterA-GigabitEthernet1/0/2] ip address 192.168.1.1 255.255.255.0
[RouterA-GigabitEthernet1/0/2] quit
```

配置缺省路由。

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

如果局域网内计算机使用的 IP 地址为私有地址，还需要在设备上配置 NAT(Network Address Translation, 网络地址转换)。NAT 的相关内容请参见“三层技术-IP 业务配置指导”中的“NAT”。

(2) 配置 Router B 作为 PPPoE Server

配置虚拟模板参数，采用 PAP 认证对端，配置本端 IP 地址，并使用 PPP 地址池为对端分配 IP 地址，并配置为对端指定 DNS 服务器的 IP 地址。

```
<RouterB> system-view
[RouterB] interface virtual-template 1
[RouterB-Virtual-Template1] ppp authentication-mode pap domain system
[RouterB-Virtual-Template1] remote address pool 1
[RouterB-Virtual-Template1] ppp ipcp dns 8.8.8.8
[RouterB-Virtual-Template1] quit
```

配置 PPP 地址池（包含 9 个可分配的 IP 地址），和地址池网关地址。

```
[RouterB] ip pool 1 1.1.1.2 1.1.1.10
[RouterB] ip pool 1 gateway 1.1.1.1
```

在 Virtual-Ethernet 接口上启用 PPPoE Server 协议，将该接口与虚拟模板接口 1 绑定。

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

对 ATM 接口进行配置。

```
[RouterB] interface atm 2/4/0.1
[RouterB-ATM2/4/0.1] pvc to_adsl_a 0/60
[RouterB-ATM2/4/0.1-pvc-to_adsl_a-0/60] map bridge virtual-ethernet 1
[RouterB-ATM2/4/0.1-pvc-to_adsl_a-0/60] quit
[RouterB-Atm2/4/0.1] quit
```

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

```
[RouterB] domain system
[RouterB-isp-system] authentication ppp radius-scheme rs1
[RouterB-isp-system] authorization ppp radius-scheme rs1
[RouterB-isp-system] accounting ppp radius-scheme rs1
[RouterB-isp-system] quit
```

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

```
[RouterB] radius scheme rs1
[RouterB-radius-rs1] primary authentication 11.110.91.146 1812
[RouterB-radius-rs1] primary accounting 11.110.91.146 1813
```

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

```
[RouterB-radius-rs1] key authentication simple expert
[RouterB-radius-rs1] key accounting simple expert
[RouterB-radius-rs1] quit
```


(3) 配置 RADIUS 服务器

在 RADIUS 服务器上配置认证与计费的共享密钥 expert。

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

具体配置过程请参考实际使用的 RADIUS 服务器的用户手册。

4. 验证配置

配置完成后，Router A 就可以与远端的 Router B 建立 PPPoE 会话。

```
[RouterA] display pppoe-client session summary
```

Bundle	ID	Interface	VA	RemoteMAC	LocalMAC	State
1	1	GE1/0/1	VA0	0001-0000-0001	00e0-1500-4100	SESSION

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

目 录

1 L2TP.....	1-1
1.1 L2TP简介	1-1
1.1.1 L2TP典型组网.....	1-1
1.1.2 L2TP消息类型及封装结构.....	1-2
1.1.3 L2TP隧道和会话.....	1-2
1.1.4 L2TP隧道模式及隧道建立过程.....	1-2
1.1.5 L2TP协议的特点.....	1-6
1.1.6 基于L2TP接入的EAD功能.....	1-8
1.1.7 协议规范.....	1-8
1.2 配置准备.....	1-8
1.3 L2TP配置任务简介	1-9
1.3.1 LAC端配置任务简介	1-9
1.3.2 LNS端配置任务简介	1-9
1.4 配置L2TP基本功能	1-10
1.5 配置LAC端.....	1-11
1.5.1 配置向LNS发起隧道建立请求的触发条件	1-11
1.5.2 配置LNS的IP地址	1-11
1.5.3 配置隧道的源端地址.....	1-12
1.5.4 配置AVP数据的隐藏传输	1-12
1.5.5 配置LAC端的AAA认证	1-13
1.5.6 配置LAC自动建立L2TP隧道	1-13
1.5.7 配置虚拟PPP接口的轮询功能	1-14
1.5.8 配置处理虚拟PPP接口流量的slot	1-14
1.5.9 恢复当前虚拟PPP接口的缺省配置.....	1-15
1.6 配置LNS端.....	1-16
1.6.1 配置虚拟模板接口	1-16
1.6.2 配置VA池.....	1-16
1.6.3 配置LNS接受L2TP隧道建立请求	1-17
1.6.4 配置LNS端的用户验证	1-17
1.6.5 配置LNS端的AAA认证	1-19
1.6.6 配置LNS端每秒能处理ICRQ报文的数目.....	1-19
1.7 配置L2TP公共参数	1-19
1.7.1 配置隧道验证.....	1-19

1.7.2 配置隧道Hello报文发送时间间隔	1-20
1.7.3 配置L2TP会话的流控功能.....	1-20
1.7.4 配置隧道报文的DSCP优先级.....	1-21
1.7.5 配置隧道对端所属的VPN.....	1-21
1.7.6 配置LTS设备的TSA ID.....	1-22
1.7.7 配置L2TP隧道接收窗口的大小.....	1-22
1.7.8 配置L2TP隧道发送窗口的大小.....	1-23
1.8 配置基于L2TP接入的EAD功能	1-23
1.9 配置L2TP支持IMSI/SN捆绑协商功能	1-24
1.9.1 配置LNS端发起IMSI/SN捆绑协商	1-24
1.9.2 配置LAC client支持与LNS端进行IMSI/SN捆绑协商.....	1-25
1.10 L2TP显示和维护.....	1-26
1.11 L2TP典型配置举例.....	1-26
1.11.1 NAS-Initiated模式L2TP隧道配置举例.....	1-26
1.11.2 Client-Initiated模式L2TP隧道配置举例	1-28
1.11.3 LAC-Auto-Initiated模式L2TP隧道配置举例.....	1-30
1.12 L2TP常见故障处理.....	1-32
1.12.1 远端系统无法访问企业内部网络	1-32
1.12.2 隧道建立成功，但无法传输数据	1-33

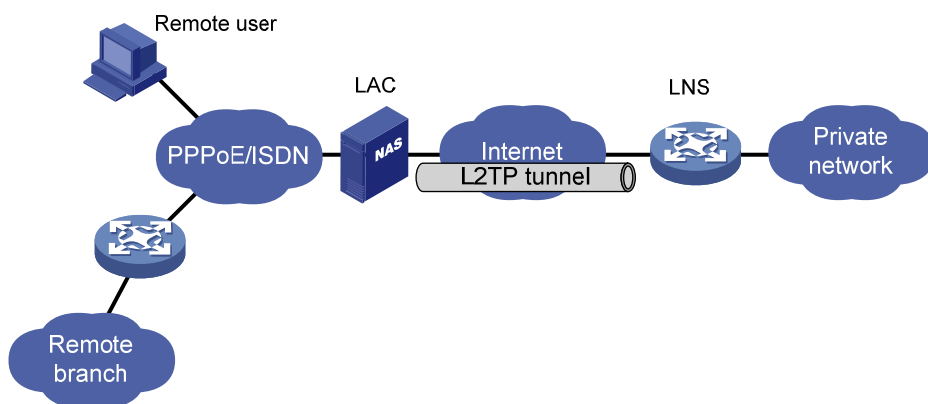
1 L2TP

1.1 L2TP简介

L2TP（Layer 2 Tunneling Protocol，二层隧道协议）通过在公共网络（如 Internet）上建立点到点的 L2TP 隧道，将 PPP（Point-to-Point Protocol，点对点协议）数据帧封装后通过 L2TP 隧道传输，使得远端用户（如企业驻外机构和出差人员）利用 PPP 接入公共网络后，能够通过 L2TP 隧道与企业内部网络通信，访问企业内部网络资源，从而为远端用户接入私有的企业网络提供了一种安全、经济且有效的方式。

1.1.1 L2TP典型组网

图1-1 L2TP 典型组网



如 [图 1-1](#) 所示，L2TP 的典型组网中包括以下三个部分：

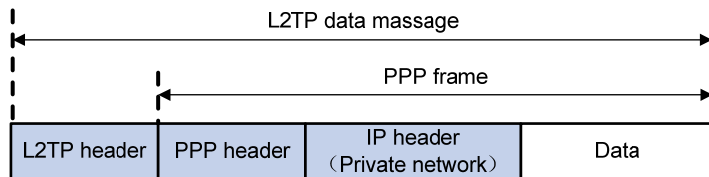
- 远端系统
远端系统是要接入企业内部网络的远端用户和远端分支机构，通常是一个拨号用户的主机或私有网络中的一台设备。
- LAC（L2TP Access Concentrator，L2TP 访问集中器）
LAC 是具有 PPP 和 L2TP 协议处理能力的设备，通常是一个当地 ISP 的 NAS（Network Access Server，网络接入服务器），主要用于为 PPP 类型的用户提供接入服务。
LAC 作为 L2TP 隧道的端点，位于 LNS 和远端系统之间，用于在 LNS 和远端系统之间传递报文。它把从远端系统收到的报文按照 L2TP 协议进行封装并送往 LNS，同时也将从 LNS 收到的报文进行解封装并送往远端系统。
- LNS（L2TP Network Server，L2TP 网络服务器）
LNS 是具有 PPP 和 L2TP 协议处理能力的设备，通常位于企业内部网络的边缘。
LNS 作为 L2TP 隧道的另一侧端点，是 LAC 通过隧道传输的 PPP 会话的逻辑终点。L2TP 通过在公共网络中建立 L2TP 隧道，将远端系统的 PPP 连接由原来的 NAS 延伸到了企业内部网络的 LNS 设备。

1.1.2 L2TP消息类型及封装结构

L2TP 协议定义了两种消息：

- 控制消息：用于 L2TP 隧道和 L2TP 会话的建立、维护和拆除。控制消息的传输是可靠的，并且支持流量控制和拥塞控制。
- 数据消息：用于封装PPP帧，其格式如 [图 1-2](#)所示。数据消息的传输是不可靠的，若数据消息丢失，不予重传。数据消息支持流量控制，即支持对乱序的数据消息进行排序。

图1-2 L2TP 数据消息格式



如 [图 1-3](#)所示，L2TP控制消息和L2TP数据消息均封装在UDP报文中。

图1-3 L2TP 消息封装结构图



1.1.3 L2TP隧道和会话

L2TP 隧道是 LAC 和 LNS 之间的一条虚拟点到点连接。控制消息和数据消息都在 L2TP 隧道上传输。在同一对 LAC 和 LNS 之间可以建立多条 L2TP 隧道。每条隧道可以承载一个或多个 L2TP 会话。L2TP 会话复用在 L2TP 隧道之上，每个 L2TP 会话对应于一个 PPP 会话。当远端系统和 LNS 之间建立 PPP 会话时，LAC 和 LNS 之间将建立与其对应的 L2TP 会话。属于该 PPP 会话的数据帧通过该 L2TP 会话所在的 L2TP 隧道传输。

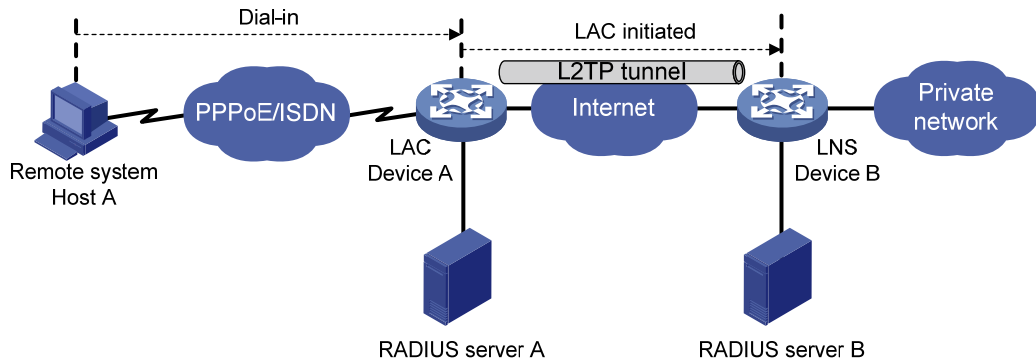
1.1.4 L2TP隧道模式及隧道建立过程

L2TP 隧道包括 NAS-Initiated、Client-Initiated 和 LAC-Auto-Initiated 三种模式。

1. NAS-Initiated模式

如 [图 1-4](#)所示，NAS-Initiated模式L2TP隧道的建立由LAC（即NAS）发起。远端系统的拨号用户通过PPPoE/ISDN拨入LAC后，由LAC向LNS发起建立L2TP隧道的请求。

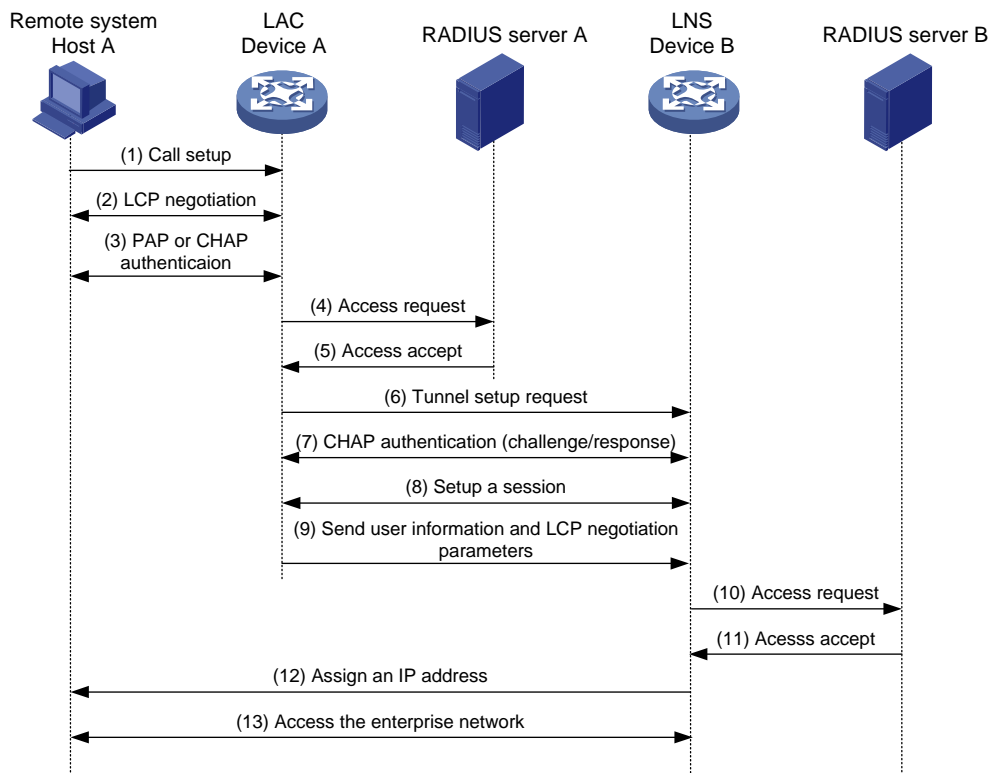
图1-4 NAS-Initiated 模式 L2TP 隧道示意图



NAS-Initiated 模式 L2TP 隧道具有如下特点：

- 远端系统只需支持 PPP 协议，不需要支持 L2TP。
- 对远端拨号用户的身份认证与计费既可由 LAC 代理完成，也可由 LNS 完成。

图1-5 NAS-Initiated 模式 L2TP 隧道的建立流程



如 图 1-5 所示，NAS-Initiated模式L2TP隧道的建立过程为：

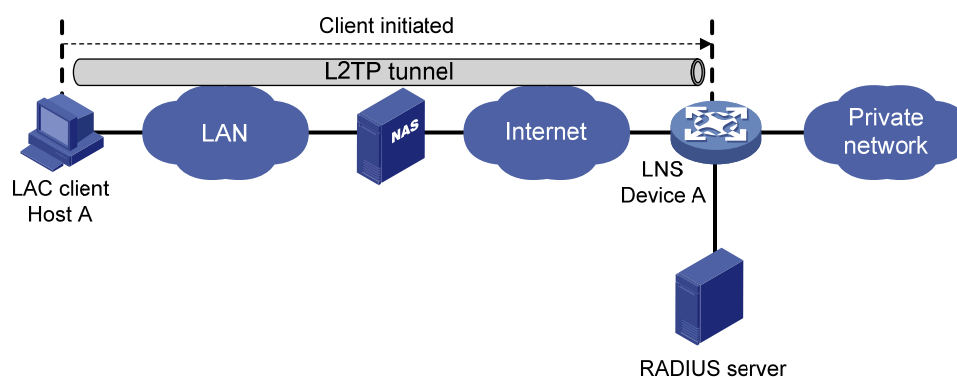
- (1) 远端系统 Host A 发起呼叫，请求建立连接。
- (2) Host A 和 LAC (Device A) 进行 PPP LCP 协商。
- (3) LAC 对 Host A 提供的 PPP 用户信息进行 PAP 或 CHAP 认证。
- (4) LAC 将认证信息（用户名、密码）发送给 RADIUS 服务器进行认证。
- (5) RADIUS 服务器认证该用户，并返回认证结果。

- (6) 如果认证通过，且根据用户名或用户所属 ISP 域判断该用户为 L2TP 用户，则 LAC 向 LNS (Device B) 发起 L2TP 隧道建立请求。
 - (7) 在需要对隧道进行认证的情况下，LAC 和 LNS 分别发送 CHAP challenge 信息，以验证对方身份。隧道验证通过后，LAC 和 LNS 之间成功建立了 L2TP 隧道。
 - (8) LAC 和 LNS 在 L2TP 隧道上协商建立 L2TP 会话。
 - (9) LAC 将 PPP 用户信息和 PPP 协商参数等传送给 LNS。
 - (10) LNS 将认证信息发送给 RADIUS 服务器进行认证。
 - (11) RADIUS 服务器认证该用户，并返回认证结果。
 - (12) 认证通过后，LNS 为 Host A 分配一个企业网内部的 IP 地址。
 - (13) 获得 IP 地址后，PPP 用户可以通过 Host A 访问企业内部资源。
- 在步骤(12)和(13)中，LAC 负责在 Host A 和 LNS 之间转发报文。Host A 和 LAC 之间交互的是 PPP 数据帧，LAC 和 LNS 之间交互的是 L2TP 数据报文。

2. Client-Initiated模式

如 图 1-6 所示，Client-Initiated模式L2TP隧道的建立直接由LAC client（指本地支持L2TP协议的远端系统）发起。LAC client具有公网地址，并能够通过Internet与LNS通信后，如果在LAC client上触发L2TP拨号，则LAC client直接向LNS发起L2TP隧道建立请求，无需经过LAC设备建立隧道。

图1-6 Client-Initiated 模式 L2TP 隧道示意图

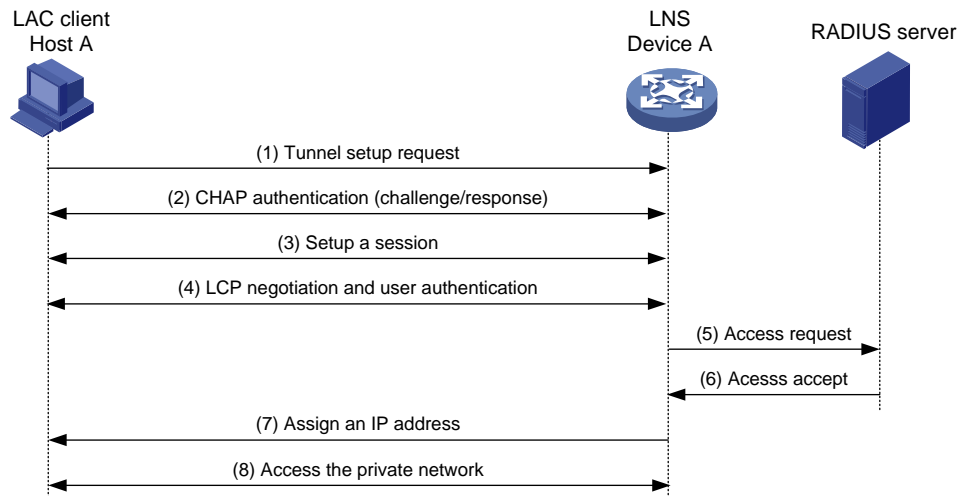


Client-Initiated 模式 L2TP 隧道具有如下特点：

- L2TP 隧道在远端系统和 LNS 之间建立，具有较高的安全性。
- Client-Initiated 模式 L2TP 隧道对远端系统要求较高（远端系统必须是支持 L2TP 协议的 LAC client，且能够与 LNS 通信），因此它的扩展性较差。

如 图 1-7 所示，Client-Initiated模式L2TP隧道的建立过程与NAS-Initiated模式类似，此处不再赘述。

图1-7 Client-Initiated 模式 L2TP 隧道的建立流程

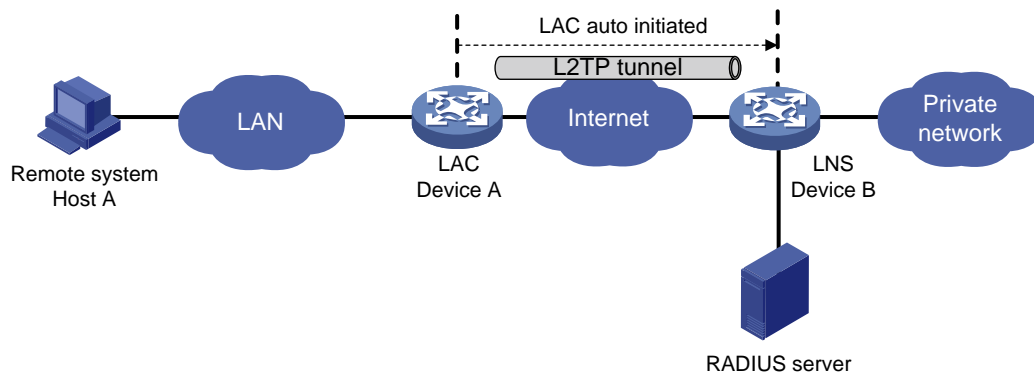


3. LAC-Auto-Initiated模式

采用 NAS-Initiated 方式建立 L2TP 隧道时，要求远端系统必须通过 PPPoE/ISDN 等拨号方式拨入 LAC，且只有远端系统拨入 LAC 后，才能触发 LAC 向 LNS 发起建立隧道的请求。

如 图 1-8 所示，在 LAC-Auto-Initiated 模式下，不需要远端系统拨号触发，在 LAC 上通过执行 `l2tp-auto-client` 命令即可触发 LAC 建立 L2TP 隧道。远端系统访问 LNS 连接的内部网络时，LAC 将通过 L2TP 隧道转发这些访问数据。

图1-8 LAC-Auto-Initiated 模式 L2TP 隧道示意图

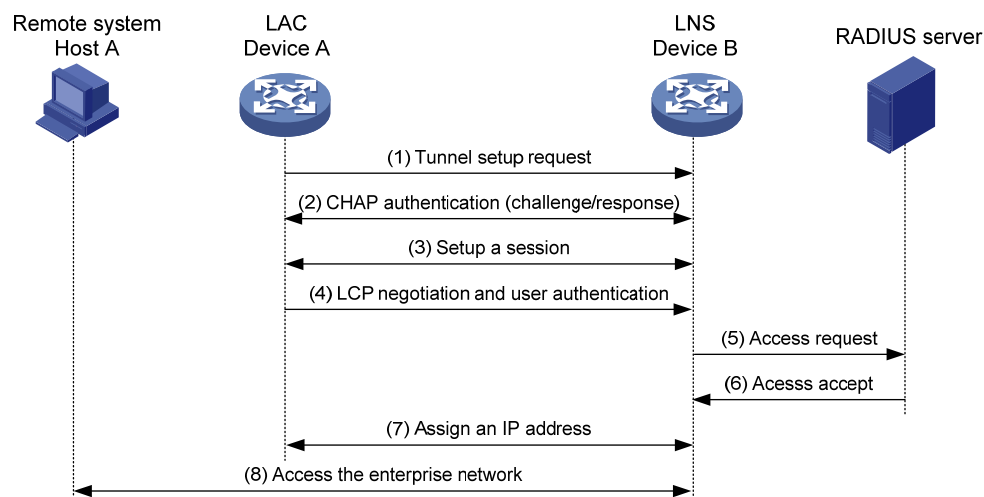


LAC-Auto-Initiated 模式 L2TP 隧道具有如下特点：

- 远端系统和 LAC 之间可以是任何基于 IP 的连接，不局限于拨号连接。
- 不需要远端系统上的拨号接入来触发建立 L2TP 隧道。
- L2TP 隧道创建成功后立即建立 L2TP 会话，然后在 LAC 和 LNS 之间进行 PPP 协商，LAC 和 LNS 分别作为 PPP 客户端和 PPP 服务器端。
- LNS 为 LAC 分配企业网内部的 IP 地址，而不是为远端系统分配。

如 图 1-9 所示，LAC-Auto-Initiated 模式 L2TP 隧道的建立过程与 NAS-Initiated 模式类似，此处不再赘述。

图1-9 LAC-Auto-Initiated 模式 L2TP 隧道的建立流程



1.1.5 L2TP协议的特点

1. 灵活的身份验证机制以及高度的安全性

L2TP 协议本身并不提供连接的安全性，但它可依赖于 PPP 提供的认证（比如 CHAP、PAP 等），因此具有 PPP 所具有的所有安全特性。

L2TP 还可以与 IPsec 结合起来实现数据安全，使得通过 L2TP 所传输的数据更难被攻击。

2. 多协议传输

L2TP 传输 PPP 数据包，在 PPP 数据包内可以封装多种协议。

3. 支持RADIUS服务器的认证

LAC 和 LNS 可以将用户名和密码发往 RADIUS 服务器，由 RADIUS 服务器对用户身份进行认证。

4. 支持内部地址分配

LNS 可以对远端系统的地址进行动态的分配和管理，可支持私有地址应用（RFC 1918）。为远端系统分配企业内部的私有地址，可以方便地址的管理并增加安全性。

5. 网络计费的灵活性

可在 LAC 和 LNS 两处同时计费，即 ISP 处（用于产生帐单）及企业网关（用于付费及审计）。L2TP 能够提供数据传输的出/入包数、字节数以及连接的起始、结束时间等计费数据，AAA 服务器可根据这些数据方便地进行网络计费。

6. 可靠性

L2TP 协议支持备份 LNS，当主 LNS 不可达之后，LAC 可以与备份 LNS 建立连接，增加了 L2TP 服务的可靠性。

7. 支持由RADIUS服务器为LAC下发隧道属性

L2TP 隧道采用 NAS-Initiated 模式时，LAC 上的 L2TP 隧道属性可以通过 RADIUS 服务器来下发。此时，在 LAC 上只需开启 L2TP 服务，并配置采用 AAA 远程认证方式对 PPP 用户进行身份验证，无需进行其他 L2TP 配置。

当 L2TP 用户拨入 LAC 时，LAC 作为 RADIUS 客户端将用户的身份信息发送给 RADIUS 服务器。RADIUS 服务器对 L2TP 用户的身份进行验证。RADIUS 服务器将验证结果返回给 LAC，并将该用户对应的 L2TP 隧道属性下发给 LAC。LAC 根据下发的隧道属性，创建 L2TP 隧道和会话。

目前，RADIUS 服务器可以为 LAC 下发的属性如 [表 1-1](#) 所示。

表1-1 RADIUS 服务器为 LAC 下发的属性列表

属性编号	属性名称	描述
64	Tunnel-Type	隧道类型，目前只支持L2TP隧道类型
65	Tunnel-Medium-Type	隧道的传输媒介类型，目前只支持IPv4
67	Tunnel-Server-Endpoint	LNS的IP地址
69	Tunnel-Password	隧道验证密钥
81	Tunnel-Private-Group-ID	隧道的Group ID LAC将该值发送给LNS，以便LNS根据该值进行相应的处理
82	Tunnel-Assignment-ID	隧道的Assignment ID 用来标识会话承载在哪条隧道上，具有相同Tunnel-Assignment-ID、Tunnel-Server_Endpoint和Tunnel-Password的L2TP用户共用同一条L2TP隧道
90	Tunnel-Client-Auth-ID	隧道的名称 用来标识本端隧道

目前，仅支持通过 RADIUS 服务器下发一组 L2TP 隧道属性，不支持同时下发多组隧道属性。

如果既通过 RADIUS 服务器为 LAC 下发了隧道属性，又在 LAC 上通过命令行手工配置了隧道属性，则以 RADIUS 服务器下发的属性为准。

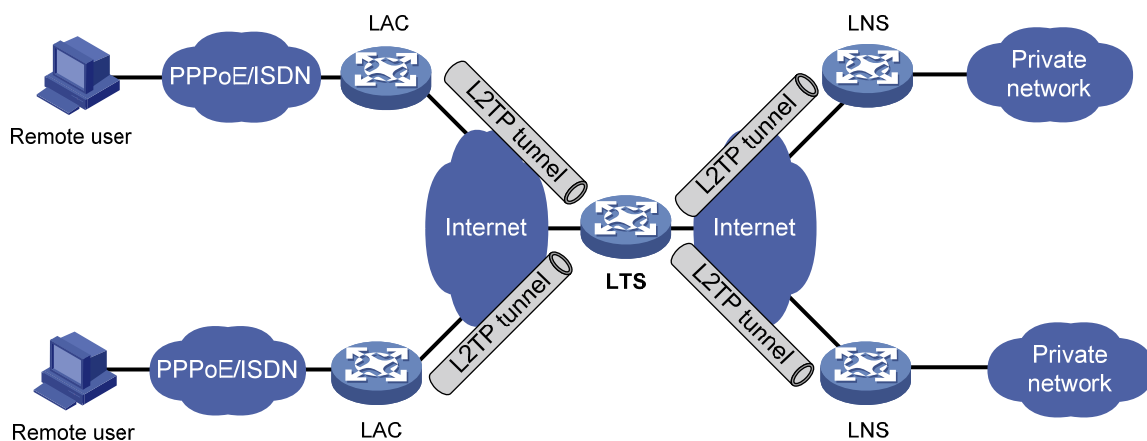
8. 支持L2TP隧道交换

如 [图 1-10](#) 所示，设备可以同时作为 LNS 和 LAC，终结来自 LAC 的 L2TP 报文后，再将其通过 L2TP 隧道发送给最终的 LNS，实现 L2TP 隧道的交换，即多跳 L2TP 隧道。同时作为 LNS 和 LAC 的设备称为 LTS（L2TP Tunnel Switch，L2TP 隧道交换）设备。

L2TP 隧道交换功能具有如下作用：

- LAC 和 LNS 位于不同的管理域时，可以简化 LAC 和 LNS 的配置与部署。所有的 LAC 都将 LTS 当作 LNS，不需要感知网络中是否存在多个 LNS，不需要区分 LNS；所有 LNS 都将 LTS 当作 LAC，不需要感知 LAC 的新增和删除。
- 不同用户可以共用 LAC 和 LTS 之间的 L2TP 隧道，由 LTS 将不同用户的数据分发给不同的 LNS。

图1-10 L2TP 隧道交换组网图



1.1.6 基于L2TP接入的EAD功能

L2TP 接入的 EAD 功能是指，在 L2TP 身份认证的基础之上，通过和安全策略服务器配合进一步对接入网络的用户终端强制实施企业安全策略，加强网络用户终端的主动防御能力，并严格控制终端用户的网络使用行为，保护网络安全。

具体流程如下：

- (1) iNode 客户端（即主机）通过 L2TP 接入到 LNS 设备，通过 PPP 认证后，CAMS/iMC 服务器给设备下发隔离 ACL，对报文进行入方向防火墙过滤；
- (2) 通过 IPCP 协商后，CAMS/iMC 服务器通过设备把自己的 IP 地址（该 IP 地址可以通过隔离 ACL）等信息通知给 iNode 客户端；
- (3) iNode 客户端直接和 CAMS/iMC 服务器进行 EAD 认证和安全检查，通过安全检查后，CAMS/iMC 服务器针对这个用户给设备下发安全 ACL，使用户可以正常使用网络资源。

1.1.7 协议规范

与 L2TP 相关的协议规范有：

- RFC 1661: The Point-to-Point Protocol (PPP)
- RFC 1918: Address Allocation for Private Internets
- RFC 2661: Layer Two Tunneling Protocol "L2TP"
- RFC 2868: RADIUS Attributes for Tunnel Protocol Support

1.2 配置准备

配置 L2TP 时，需要执行以下操作：

- (1) 根据实际组网环境，判断需要的网络设备。
 - 对于 NAS-Initiated 和 LAC-Auto-Initiated 模式，需要配置 LAC 和 LNS 两台网络设备。
 - 对于 Client-Initiated 模式，只需要配置 LNS 一台网络设备。

- (2) 规划好设备在网络中的角色，然后分别进行 LAC 或 LNS 端的相关配置，使设备具有 LAC 或 LNS 端功能。

1.3 L2TP配置任务简介

1.3.1 LAC端配置任务简介

LAC 端配置任务如下：

- (1) [配置L2TP基本功能](#)
- (2) [配置LAC端](#)
 - [配置向LNS发起隧道建立请求的触发条件](#)
仅 NAS-Initiated 模式下为必选，LAC-Auto-Initiated 模式下不建议配置。
 - [配置LNS的IP地址](#)
 - [配置隧道的源端地址](#)
 - （可选）[配置AVP数据的隐藏传输](#)
 - [配置LAC端的AAA认证](#)
仅 NAS-Initiated 模式下为必选，LAC-Auto-Initiated 模式下不建议配置。
 - [配置LAC自动建立L2TP隧道](#)
仅 LAC-Auto-Initiated 模式下为必选，NAS-Initiated 模式下不建议配置。
 - （可选）[配置虚拟PPP接口的轮询功能](#)
 - （可选）[配置处理虚拟PPP接口流量的slot](#)
 - （可选）[恢复当前虚拟PPP接口的缺省配置](#)
- (3) （可选）[配置L2TP公共参数](#)
 - [配置隧道验证](#)
 - [配置隧道Hello报文发送时间间隔](#)
 - [配置L2TP会话的流控功能](#)
 - [配置隧道报文的DSCP优先级](#)
 - [配置隧道对端所属的VPN](#)
 - [配置LTS设备的TSA ID](#)

1.3.2 LNS端配置任务简介

LNS 端配置任务如下：

- (1) [配置L2TP基本功能](#)
- (2) [配置LNS端](#)
 - [配置虚拟模板接口](#)
 - （可选）[配置VA池](#)
 - [配置LNS接受L2TP隧道建立请求](#)
 - （可选）[配置LNS端的用户验证](#)
 - （可选）[配置LNS端的AAA认证](#)

- (可选) [配置LNS端每秒能处理ICRQ报文的最大数目](#)
- (3) (可选) [配置L2TP公共参数](#)
 - [配置隧道验证](#)
 - [配置隧道Hello报文发送时间间隔](#)
 - [配置L2TP会话的流控功能](#)
 - [配置隧道报文的DSCP优先级](#)
 - [配置隧道对端所属的VPN](#)
 - [配置LTS设备的TSA ID](#)
 - [配置L2TP隧道接收窗口的大小](#)
 - [配置L2TP隧道发送窗口的大小](#)
- (4) [配置基于L2TP接入的EAD功能](#)
 当需要在 L2TP 身份认证的基础之上, 通过和安全策略服务器配合进一步对用户进行安全性检查时, 需要配置本功能。
- (5) [配置L2TP支持IMSI/SN捆绑协商功能](#) [配置L2TP支持IMSI/SN捆绑协商功能](#)
 当 3G 和 4G 路由器作为 LAC client 并按照 Client-Initiated 模式接入 LNS 或 4G 路由器作为 LAC 端并按照 LAC-Auto-Initiated 模式自动触发接入 LNS 时, 需要配置本功能。

1.4 配置L2TP基本功能

1. 功能简介

L2TP 基本功能的配置包括如下内容:

- 启用 L2TP 功能: 只有启用 L2TP 后, 设备上的 L2TP 功能才能正常发挥作用。
- 创建 L2TP 组: L2TP 组用于配置 L2TP 的相关参数, 它不仅增加了 L2TP 配置的灵活性, 还方便地实现了 LAC 和 LNS 之间一对一、一对多的组网应用。L2TP 组在 LAC 和 LNS 上独立编号, 只需要保证 LAC 和 LNS 之间关联的 L2TP 组的相关配置(如隧道对端名称、LNS 地址等)保持对应关系即可。
- 配置隧道本端的名称: 隧道本端的名称在 LAC 和 LNS 进行隧道协商时使用, 它用来标识本端隧道, 以供对端识别。

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 开启 L2TP 功能。

```
l2tp enable
```

缺省情况下, L2TP 功能处于关闭状态。

- (3) 创建 L2TP 组, 指定 L2TP 组的模式, 并进入 L2TP 组视图。

```
l2tp-group group-number mode { lac | lns }
```

在 LAC 端需要指定 L2TP 组的模式为 **lac**; 在 LNS 端需要指定 L2TP 组的模式为 **lns**。

- (4) 配置隧道本端的名称。

```
tunnel name name
```

缺省情况下，隧道本端的名称为设备的名称。

LAC 端配置的隧道本端名称要与 LNS 端配置的允许接受的 L2TP 隧道请求的隧道对端名称保持一致。

1.5 配置LAC端

1.5.1 配置向LNS发起隧道建立请求的触发条件

1. 功能简介

本配置用来指定 LAC 向 LNS 发起隧道建立请求的触发条件。只有 PPP 用户的信息与指定的触发条件匹配时，LAC 才认为该 PPP 用户为 L2TP 用户，向 LNS 发起 L2TP 隧道建立请求。

触发条件分为如下两种：

- 完整的用户名（**fullusername**）：只有 PPP 用户的用户名与配置的完整用户名匹配时，才会向 LNS 发起 L2TP 隧道建立请求。
- 带特定域名的用户名（**domain**）：PPP 用户的 ISP 域名与配置的域名匹配时，即向 LNS 发起 L2TP 隧道建立请求。

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入 LAC 模式的 L2TP 组视图。

```
l2tp-group group-number [ mode lac ]
```

- (3) 配置向 LNS 发起隧道建立请求的触发条件。

```
user { domain domain-name | fullusername user-name }
```

缺省情况下，没有指定本端作为 LAC 端时向 LNS 发起隧道建立请求的触发条件。

1.5.2 配置LNS的IP地址

1. 功能简介

LAC 上最多可以配置五个 LNS 地址，即允许存在备用 LNS。LAC 按照 LNS 配置的先后顺序依次向每个 LNS 发送建立 L2TP 隧道的请求。LAC 接收到某个 LNS 的接受应答后，该 LNS 就作为隧道的对端；否则，LAC 向下一个 LNS 发起隧道建立请求。

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入 LAC 模式的 L2TP 组视图。

```
l2tp-group group-number [ mode lac ]
```

- (3) 配置 LNS 的 IP 地址。

```
lns-ip { ip-address }&<1-5>
```

缺省情况下，没有指定 LNS 的 IP 地址。

1.5.3 配置隧道的源端地址

1. 功能简介

在 LAC 上配置了 L2TP 隧道的源端地址后，LAC 会将该地址作为封装后 L2TP 隧道报文的源 IP 地址。

2. 配置限制和指导

建议将 L2TP 隧道的源端地址配置为设备上某 LoopBack 接口的 IP 地址，以减小物理接口故障对 L2TP 业务造成的影响。但当 LAC 和 LNS 之间存在等价路由时，必须将 L2TP 隧道的源端地址通过 **source-ip** 命令配置或通过 RADIUS 服务器授权为设备上某 LoopBack 接口的 IP 地址。

3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入 LAC 模式的 L2TP 组视图。

```
l2tp-group group-number [ mode lac ]
```

- (3) 配置 L2TP 隧道的源端地址。

```
source-ip ip-address
```

缺省情况下，L2TP 隧道的源端地址为本端隧道出接口的 IP 地址。

1.5.4 配置 AVP 数据的隐藏传输

1. 功能简介

L2TP 协议通过 AVP (Attribute Value Pair, 属性值对) 来传输隧道协商参数、会话协商参数和用户认证信息等。如果用户不希望这些信息 (如用户密码) 被窃取，则可以使用本配置将 AVP 数据的传输方式配置成为隐藏传输，即利用隧道验证密钥 (通过 **tunnel password** 命令配置) 对 AVP 数据进行加密传输。

2. 配置限制和指导

只有使能了隧道验证功能，本配置才会生效。隧道验证功能的详细配置，请参见“[1.7.1 配置隧道验证](#)”。

3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入 LAC 模式的 L2TP 组视图。

```
l2tp-group group-number [ mode lac ]
```

- (3) 配置隧道采用隐藏方式传输 AVP 数据。

```
tunnel avp-hidden
```

缺省情况下，隧道采用明文方式传输 AVP 数据。

1.5.5 配置LAC端的AAA认证

本配置用来通过 AAA 对远端拨入用户的身份信息（用户名、密码）进行认证。用户身份认证通过后，LAC 才能发起建立隧道的请求，否则不会为用户建立隧道。

设备支持的 AAA 认证包括本地和远程两种认证方式：

- 如果选择本地认证方式，则需要在 LAC 端配置本地用户名和密码。LAC 通过检查拨入用户的用户名/密码是否与本地配置的用户名/密码相符来验证用户身份。
- 如果选择远程认证方式，则需要在 RADIUS/HWTACACS 服务器上配置用户名和密码。LAC 将拨入用户的用户名和密码发往服务器，由服务器对用户身份进行认证。

AAA 相关的配置请参见“安全配置指导”中的“AAA”。

配置 LAC 端的 AAA 认证时，接入用户的接口上需要配置 PPP 用户的验证方式为 PAP 或 CHAP，配置方法请参见“二层技术-广域网接入配置指导”中的“PPP”。

1.5.6 配置LAC自动建立L2TP隧道

- (1) 进入系统视图。

```
system-view
```

- (2) 创建虚拟 PPP 接口，并进入虚拟 PPP 接口视图。

```
interface virtual-ppp interface-number
```

- (3) 配置虚拟 PPP 接口的 IP 地址或 IP 地址可协商属性。

- 配置虚拟 PPP 接口的 IP 地址。

```
ip address address mask
```

缺省情况下，未配置接口的 IP 地址。

- 配置虚拟 PPP 接口的 IP 地址可协商属性，使该接口接受 PPP 协商产生的由对端分配的 IP 地址。

```
ip address ppp-negotiate
```

缺省情况下，未配置接口的 IP 地址可协商属性。

- (4) 配置 PPP 验证的被验证方。

通过 **ppp pap** 或 **ppp chap** 命令指定 PPP 用户支持的验证方法、PPP 用户的用户名和密码，LNS 对该 PPP 用户进行身份验证。配置方法请参见“二层技术-广域网接入命令参考”中的“PPP”。

- (5) （可选）配置当前接口的描述信息。

```
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：Virtual-PPP254 Interface。

- (6) （可选）配置接口的 MTU 值。

```
mtu size
```

缺省情况下，虚拟 PPP 接口的 MTU 值为 1500 字节。

- (7) （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）。

- (8) （可选）打开当前接口。

undo shutdown

缺省情况下，接口处于打开状态。

- (9) 触发 LAC 自动建立 L2TP 隧道。

l2tp-auto-client l2tp-group group-number

缺省情况下，LAC 没有建立 L2TP 隧道。

触发 LAC 建立 L2TP 隧道后，该隧道将始终存在，直到通过 **undo l2tp-auto-client** 或 **undo l2tp-group group-number** 命令拆除该隧道。

1.5.7 配置虚拟PPP接口的轮询功能

1. 功能简介

虚拟 PPP 接口使用轮询机制来确认链路状态是否正常。

虚拟 PPP 接口会周期性地对端发送 **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) 创建虚拟 PPP 接口，并进入虚拟 PPP 接口视图。

interface virtual-ppp 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。

- (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。

1.5.8 配置处理虚拟PPP接口流量的slot

1. 功能简介

当要求同一个虚拟 PPP 接口的流量必须在同一个 slot 上进行处理时，可以在虚拟 PPP 接口下配置处理接口流量的 slot。

为提高当前接口处理流量的可靠性，可以通过 **service** 命令和 **service standby** 命令为接口分别指定一个主用 slot 和一个备用 slot 进行流量处理。

接口上同时配置了主用 slot 和备用 slot 时，流量处理的机制如下：

- 当主用 slot 不可用时，流量由备用 slot 处理。之后，即使主用 slot 恢复可用，流量也继续由备用 slot 处理；仅当备用 slot 不可用时，流量才切换到主用 slot。
- 当主用 slot 和备用 slot 均不可用时，流量由接收报文的 slot 处理；之后，主用 slot 和备用 slot 谁先恢复可用，流量就由谁处理。

如果接口上未配置主用 slot 和备用 slot，则业务处理在接收报文的 slot 上进行。

本节配置仅对 L2TP 数据报文的处理产生影响，L2TP 控制报文始终在主用主控板上处理，不受 **service** 命令和 **service standby** 命令的控制。

2. 配置限制和指导

为避免不必要的流量切换，建议配置主用 slot 后，再配置备用 slot。如果先配置备用 slot，则流量由备用 slot 处理；在配置主用 slot 后，流量将会从备用 slot 切换到主用 slot。

3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入虚拟 PPP 接口视图。

```
interface virtual-ppp interface-number
```

- (3) 配置处理接口流量的主用 slot。

（独立运行模式）

```
service slot slot-number
```

（IRF 模式）

```
service chassis chassis-number slot slot-number
```

缺省情况下，未配置处理接口流量的主用 slot。

- (4) 配置处理接口流量的备用 slot。

（独立运行模式）

```
service standby slot slot-number
```

（IRF 模式）

```
service standby chassis chassis-number slot slot-number
```

缺省情况下，未配置处理接口流量的备用 slot。

1.5.9 恢复当前虚拟PPP接口的缺省配置

1. 配置限制和指导



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) 进入虚拟 PPP 接口视图。

```
interface virtual-ppp interface-number
```

(3) 恢复当前接口的缺省配置。

```
default
```

1.6 配置LNS端

1.6.1 配置虚拟模板接口

L2TP 会话建立之后，LNS 需要创建一个 VA（Virtual Access，虚拟访问）接口用于和 LAC 交换数据。VA 接口基于 VT（Virtual Template，虚拟模板）接口上配置的参数动态创建。因此，配置 LNS 时需要首先创建 VT 接口，并配置该接口的参数。

VT 接口的参数主要包括：

- 接口的 IP 地址
- 对 PPP 用户的验证方式
- LNS 为 PPP 用户分配的 IP 地址

关于 VT 接口配置的详细介绍，请参见“二层技术-广域网接入配置指导”中的“PPP 和 MP”以及“三层技术-IP 业务配置指导”中的“IP 地址”。

1.6.2 配置VA池

1. 功能简介

VA 池是在建立 L2TP 连接前事先创建的 VA 接口的集合。VA 池可以用来解决大量用户同时上线/下线，无法及时创建/删除 VA 接口，以至于影响 L2TP 连接建立和拆除性能的问题。

创建 VA 池后，当需要创建 VA 接口时，直接从 VA 池中获取一个 VA 接口，加快了 L2TP 连接的建立速度。当用户下线后，直接把 VA 接口放入 VA 池中，不需要删除 VA 接口，加快了 L2TP 连接的拆除速度。当 VA 池中的 VA 接口耗光后，仍需在建立 L2TP 连接时再创建 VA 接口，在用户下线后删除 VA 接口。

2. 配置限制和指导

每个虚拟模板接口只能关联一个 VA 池。如果想要修改使用的 VA 池的大小，只能先删除原来的配置，然后重新配置 VA 池。

创建/删除 VA 池需要花费一定的时间，请用户耐心等待。在 VA 池创建/删除过程中（还没创建/删除完成）允许用户上线/下线，但正在创建/删除的 VA 池不生效。

系统可能由于资源不足不能创建用户指定容量的 VA 池，用户可以通过 **display l2tp va-pool** 命令查看实际可用的 VA 池的容量以及 VA 池的状态。

VA 池会占用较多的系统内存，请用户根据实际情况创建大小合适的 VA 池。
删除 VA 池时，如果已有在线用户使用该 VA 池中的 VA 接口，不会导致这些用户下线。

3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 配置 VA 池。

```
l2tp virtual-template template-number va-pool va-volume
```

1.6.3 配置LNS接受L2TP隧道建立请求

1. 功能简介

接收到 LAC 发来的隧道建立请求后，LNS 需要检查 LAC 的隧道本端名称是否与本地配置的隧道对端名称相符合，从而决定是否与对端建立隧道，并确定创建 VA 接口时使用的 VT 接口。

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入 LNS 模式的 L2TP 组视图。

```
l2tp-group group-number [ mode lns ]
```

- (3) 配置 LNS 接受来自指定 LAC 的隧道建立请求，并指定建立隧道时使用的虚拟模板接口。请选择其中一项进行配置。

- o L2TP 组号不为 1。

```
allow l2tp virtual-template virtual-template-number remote  
remote-name
```

- o L2TP 组号为 1。

```
allow l2tp virtual-template virtual-template-number [ remote  
remote-name ]
```

缺省情况下，LNS 不接受任何 LAC 的隧道建立请求。

使用 L2TP 组号 1 时，可以不指定隧道对端名，即在组 1 下 LNS 可以接受任何名称的隧道对端的隧道建立请求。

1.6.4 配置LNS端的用户验证

1. 功能简介

当 LAC 对用户进行验证后，为了增强安全性，LNS 可以再次对用户进行验证。在这种情况下，将对用户进行两次验证，第一次发生在 LAC 端，第二次发生在 LNS 端，只有两次验证全部成功后，L2TP 隧道才能建立。

在 L2TP 组网中，LNS 端对用户的验证方式有三种：

- 代理验证：由 LAC 代替 LNS 对用户进行验证，并将用户的所有验证信息及 LAC 端本身配置的验证方式发送给 LNS。LNS 根据接收到的信息及本端配置的验证方式，判断用户是否合法。
- 强制 CHAP 验证：强制在 LAC 代理验证成功后，LNS 再次对用户进行 CHAP 验证。

- LCP 重协商：忽略 LAC 端的代理验证信息，强制 LNS 与用户间重新进行 LCP（Link Control Protocol，链路控制协议）协商。

验证方式的优先级从高到底依次为：LCP 重协商、强制 CHAP 验证和代理验证。

- 如果在 LNS 上同时配置 LCP 重协商和强制 CHAP 验证，L2TP 将使用 LCP 重协商。
- 如果只配置强制 CHAP 验证，则在 LAC 代理验证成功后，LNS 再次对用户进行 CHAP 验证。
- 如果既不配置 LCP 重协商，也不配置强制 CHAP 验证，则对用户进行代理验证。

2. 配置限制和指导

强制 CHAP 验证和 LCP 重协商两种验证方式仅对 NAS-Initiated 模式的 L2TP 隧道有效。

配置强制 CHAP 验证时，在 LNS 的 VT 接口下必须且只能配置 PPP 用户的验证方式为 CHAP 认证。

在某些特定的情况下（如 LNS 不接受 LAC 的 LCP 协商参数，希望和用户重新进行参数协商），需要强制 LNS 与用户重新进行 LCP 协商，并采用相应的虚拟模板接口上配置的验证方式对用户进行验证时可配置 LCP 重协商验证方式。

3. 配置强制CHAP验证

- (1) 进入系统视图。

```
system-view
```

- (2) 进入 LNS 模式的 L2TP 组视图。

```
l2tp-group group-number [ mode lns ]
```

- (3) 强制 LNS 重新对用户进行 CHAP 验证。

```
mandatory-chap
```

缺省情况下，LNS 不会重新对用户进行 CHAP 验证。

对于不支持进行第二次验证的用户，不建议配置本功能，否则将因 LNS 端的 CHAP 重新验证失败而导致 L2TP 隧道无法建立。

- (4) 退回系统视图。

```
quit
```

- (5) 进入 VT 接口并在该接口下配置 PPP 用户的验证方式为 CHAP 认证。

关于 VT 接口配置的详细介绍，请参见“二层技术-广域网接入配置指导”中的“PPP”。

4. 配置强制LCP重新协商

- (1) 进入系统视图。

```
system-view
```

- (2) 进入 LNS 模式的 L2TP 组视图。

```
l2tp-group group-number [ mode lns ]
```

- (3) 配置强制 LNS 与用户重新进行 LCP 协商。

```
mandatory-lcp
```

缺省情况下，LNS 不会与用户重新进行 LCP 协商。

启用 LCP 重协商后，如果相应的虚拟模板接口上没有配置验证，则 LNS 将不对用户进行二次验证（这时用户只在 LAC 端接受一次验证）。

1.6.5 配置LNS端的AAA认证

本配置用来通过 AAA 对远端拨入用户的身份信息（用户名、密码）进行认证。认证通过后，远端系统可以通过 LNS 访问企业内部网络。

对于 NAS-Initiated 隧道模式，当 LNS 端没有配置强制 LCP 重新协商时，必须在 LNS 端配置 AAA 认证；或者当 LNS 端配置了强制 LCP 重新协商，并且虚拟模板接口上配置了需要对 PPP 用户进行验证时，也必须在 LNS 端配置 AAA 认证。对于 Client-Initiated 和 LAC-Auto-Initiated 隧道模式，当虚拟模板接口上配置了需要对 PPP 用户进行验证时，必须在 LNS 端配置 AAA 认证。其他情况下无需在 LNS 端配置 AAA 认证。

LNS端支持的AAA配置与LAC端的相同，具体介绍及配置方法请参见“[1.5.5 配置LAC端的AAA认证](#)”。

1.6.6 配置LNS端每秒能处理ICRQ报文的最大数目

1. 配置限制和指导

为避免大量 L2TP 用户的突发上线请求对设备性能造成影响，同时又确保 L2TP 用户能够平稳上线，可以通过本节配置调整设备接收处理 ICRQ 报文的速率。

2. 配置步骤

(1) 进入系统视图。

```
system-view
```

(2) 配置 LNS 端每秒能处理 ICRQ 报文的最大数目。

```
l2tp icrq-limit number
```

缺省情况下，未限制 LNS 端每秒能处理 ICRQ 报文的最大数目。

1.7 配置L2TP公共参数

1.7.1 配置隧道验证

1. 功能简介

隧道验证请求可由 LAC 或 LNS 任何一端发起。

如果 LAC 和 LNS 两端都开启了隧道验证功能，则两端密钥（通过 `tunnel password` 命令配置）不为空并且完全一致的情况下，二者之间才能成功建立 L2TP 隧道。

如果 LAC 和 LNS 中的一端开启了隧道验证功能，则另一端可不开启隧道验证功能，但需要两端密钥（通过 `tunnel password` 命令配置）不为空并且完全一致，二者之间才能成功建立 L2TP 隧道。

如果 LAC 和 LNS 两端都禁用隧道验证功能，则无论两端是否配置密钥、密钥是否相同，都不影响隧道建立。

2. 配置限制和指导

为了保证隧道安全，建议用户不要禁用隧道验证功能。

隧道建立成功后，修改隧道验证的密钥不影响当前隧道的正常通信；当隧道断开后重新建立时使用修改后的密钥进行隧道验证。

3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入 L2TP 组视图。

```
l2tp-group group-number [ mode { lac | lns } ]
```

- (3) 开启 L2TP 的隧道验证功能。

```
tunnel authentication
```

缺省情况下，L2TP 隧道验证功能处于开启状态。

- (4) 配置隧道验证密钥。

```
tunnel password { cipher | simple } password
```

缺省情况下，未配置隧道验证密钥。

1.7.2 配置隧道Hello报文发送时间间隔

1. 功能简介

为了检测 LAC 和 LNS 之间隧道的连通性，LAC 和 LNS 会定期向对端发送 Hello 报文，接收方接收到 Hello 报文后会进行响应。当 LAC 或 LNS 在指定时间间隔内未收到对端的 Hello 响应报文时，重复发送，如果重复发送 5 次仍没有收到对端的响应信息则认为 L2TP 隧道已经断开。

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入 L2TP 组视图。

```
l2tp-group group-number [ mode { lac | lns } ]
```

- (3) 配置隧道中 Hello 报文的发送时间间隔。

```
tunnel timer hello hello-interval
```

缺省情况下，隧道中 Hello 报文的发送时间间隔为 60 秒。

1.7.3 配置L2TP会话的流控功能

1. 功能简介

L2TP 会话的流控功能是指在 L2TP 会话上传递的报文中携带序列号，通过序列号检测是否丢包，并根据序列号对乱序报文进行排序。

L2TP 会话的流控功能应用在 L2TP 数据报文的接收与发送过程中。只要 LAC 和 LNS 中的一端开启了流控功能，二者之间建立的 L2TP 会话就支持流控功能。

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入 L2TP 组视图。

```
l2tp-group group-number [ mode { lac | lns } ]
```

- (3) 开启 L2TP 会话的流控功能。

```
tunnel flow-control
```

缺省情况下，L2TP 会话的流控功能处于关闭状态。

1.7.4 配置隧道报文的DSCP优先级

1. 功能简介

DSCP (Differentiated Services Code Point, 区分服务编码点) 携带在 IP 报文中的 ToS 字段, 用来体现报文自身的优先等级, 决定报文传输的优先程度。

通过本配置指定隧道报文的 DSCP 优先级后, 当流量经过 L2TP 隧道转发时, L2TP 将其封装为 IP 报文并将 IP 报文头中的 DSCP 优先级设置为指定的值。

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入 L2TP 组视图。

```
l2tp-group group-number [ mode { lac | lns } ]
```

- (3) 配置隧道报文的 DSCP 优先级。

```
ip dscp dscp-value
```

缺省情况下，L2TP 隧道报文的 DSCP 优先级为 0。

1.7.5 配置隧道对端所属的VPN

1. 功能简介

缺省情况下, 设备在公网上发送 L2TP 控制消息和数据消息。通过本配置指定隧道对端所属的 VPN 后, 设备将在指定的 VPN 内发送 L2TP 控制消息和数据消息, 即在指定 VPN 内查找到达控制消息和数据消息目的地址的路由, 根据指定 VPN 的路由转发控制消息和数据消息。

2. 配置限制和指导

当 L2TP 隧道的一个端点位于某个 VPN 中时, 需要在 L2TP 隧道的另一个端点上通过本配置指定隧道对端属于该 VPN, 以便正确地在 L2TP 隧道端点之间转发报文。

隧道对端所属的 VPN 必须与本端设备连接 L2TP 隧道对端的物理接口所属的 VPN (通过 **ip binding vpn-instance** 命令配置) 相同。

3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入 L2TP 组视图。

```
l2tp-group group-number [ mode { lac | lns } ]
```

- (3) 配置隧道对端所属的 VPN。

```
vpn-instance vpn-instance-name
```

缺省情况下，L2TP 隧道对端属于公网。

1.7.6 配置LTS设备的TSA ID

1. 功能简介

在 L2TP 隧道交换组网中，LTS 通过 ICRQ（Incoming Call Request，入呼叫请求）报文中的 TSA（Tunnel Switching Aggregator，隧道交换聚合）ID AVP 来避免环路。

LTS 接收到 ICRQ 报文后，将报文中携带的所有 TSA ID AVP 中的 TSA ID 逐一与本地配置的 TSA ID 进行比较。如果 TSA ID AVP 中存在与本地相同的 TSA ID，则表示存在环路，LTS 立即拆除会话。否则，LTS 将自己的 TSA ID 封装到新的 TSA ID AVP 中，LTS 向它的下一跳 LTS 发送 ICRQ 报文时携带接收到的所有 TSA ID AVP 及本地封装的 TSA ID AVP。

2. 配置限制和指导

需要为不同 LTS 设备配置的不同的 TSA ID，否则会导致环路检测错误。

3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 配置 LTS 设备的 TSA ID，并开启 LTS 设备的 L2TP 环路检测功能。

```
l2tp tsa-id tsa-id
```

缺省情况下，未指定 LTS 设备的 TSA ID，且 LTS 设备的 L2TP 环路检测功能处于关闭状态。

1.7.7 配置L2TP隧道接收窗口的大小

1. 功能简介

如果乱序报文过多，可以通过调整 L2TP 接收窗口的大小进行缓解。当出现乱序报文的时候，如果乱序报文 NS（L2TP 报文中用于标识当前报文序列号的字段）在接收窗范围内，设备会先将报文缓存起来，等待 NS 等于接收窗下沿的报文到达。当收到 NS 等于接收窗下沿的报文时，则对其（NS 等于接收窗下沿的报文）进行处理，处理完该报文后，接收窗下沿加 1；如果此时缓存中存在 NS 等于接收窗下沿的报文，则继续处理；如不存在，则继续等待 NS 等于接收窗下沿的报文到达；依次类推。对于超过接收窗范围的报文进行丢弃。

2. 配置限制和指导

在 L2TP 隧道建立时，接收窗口大小以 L2TP 组视图下配置的接收窗口大小为准。隧道建立完成后通过本特性修改 L2TP 隧道接收窗口的大小对已经建立的隧道接收窗口的大小无影响。

3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入 L2TP 组视图。

```
l2tp-group group-number [ mode { lac | lns } ]
```

- (3) 配置 L2TP 隧道接收窗口的大小。

```
tunnel window receive size
```

缺省情况下，L2TP 隧道接收窗口的大小为 1024。

1.7.8 配置L2TP隧道发送窗口的大小

1. 功能简介

在某些组网中可能出现对端的报文接收处理能力和对端接收窗口的大小不匹配的情况（例如：对端实际的报文接收处理能力为 10，但接收窗口的大小为 20），此时可以通过本特性调整本端 L2TP 隧道发送窗口的大小来适配对端的实际报文接收处理能力，以保证 L2TP 用户平稳上线。

2. 配置限制和指导

在 L2TP 隧道建立时会获取 L2TP 组视图下配置的发送窗口大小。如果配置的发送窗口大小为 0，则按缺省情况处理；如果配置的发送窗口大小非 0，则以配置的发送窗口大小为准。隧道建立完成后通过本配置修改 L2TP 隧道发送窗口的大小对已经建立的隧道发送窗口的大小无影响。

3. 配置步骤

(1) 进入系统视图。

```
system-view
```

(2) 进入 L2TP 组视图。

```
l2tp-group group-number [ mode { lac | lns } ]
```

(3) 配置 L2TP 隧道发送窗口的大小。

```
tunnel window send size
```

缺省情况下，L2TP 隧道发送窗口的大小为 0，即本端发送窗口的大小以隧道建立过程中对端携带的接收窗口大小的属性值为准，如果隧道建立过程中对端没有携带接收窗口大小属性，则本端隧道发送窗口的大小为 4。

1.8 配置基于L2TP接入的EAD功能

1. 功能简介

在一些安全性要求比较高的网络环境中，可通过配置本功能并和安全策略服务器配合对 L2TP 认证通过的用户做进一步的安全性检查。只有通过安全检查，用户才可以正常访问网络资源；否则，用户将只能访问隔离区的资源。

2. 配置限制和指导

如果 LNS 设备上开启了基于 L2TP 接入的 EAD 功能，但未配置认证服务器下发的 ACL 号或未准确配置 ACL 规则，会导致认证不通过。

不同的主机用户 ACL 可以不同，设备根据不同的 ACL 对不同的用户进行报文过滤。

建议只在跨越 Internet 的远端客户端使用此功能，局域网用户不建议使用此功能，应该使用 Portal 认证。

3. 配置准备

完成 L2TP、Portal、AAA、RADIUS 及安全策略服务器的相关配置。

关于 Portal 的相关内容，请参见“安全配置指导”中的“Portal”。

关于 AAA 和 RADIUS 的相关内容，请参见“安全配置指导”中的“AAA”。

关于安全策略服务器的配置，请参见“CAMS EAD 安全策略组件联机帮助”以及“iMC EAD 安全策略组件联机帮助”。

4. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 创建并进入虚拟模板接口。

```
interface virtual-template interface-number
```

- (3) 开启基于 L2TP 接入的 EAD 功能。

```
ppp access-control enable
```

缺省情况下，基于 L2TP 接入的 EAD 功能处于关闭状态。

1.9 配置L2TP支持IMSI/SN捆绑协商功能

1.9.1 配置LNS端发起IMSI/SN捆绑协商

1. 功能简介

在 3G/4G 网络应用环境中，基于安全性考虑，仅仅根据用户名对客户端或 LAC 进行认证已不能满足用户需求。通过配置 IMSI/SN 捆绑协商功能可以进一步提高 3G/4G 网络的安全性。配置本功能后 LNS 向 AAA 服务器进行认证时会发送用户名/密码和 IMSI/SN 信息，AAA 服务器根据已有的配置对这些信息进行认证。只有用户名/密码认证和 IMSI/SN 信息检测认证都通过时才允许用户上线，否则用户上线失败。有关 3G/4G 的相关介绍，请参见“二层技术-广域网接入配置指导”中的“3G Modem 和 4G Modem 管理”。

2. 配置限制和指导

当 3G 和 4G 路由器作为 LAC client 并按照 Client-Initiated 模式接入 LNS 或 4G 路由器作为 LAC 端并按照 LAC-Auto-Initiated 模式自动触发接入 LNS 时，需要配置 LNS 端发起 IMSI/SN 捆绑协商功能。

在和本 LNS 端建立 L2TP 隧道的 LAC client 或 LAC（4G 路由器）上配置其支持与 LNS 端进行 IMSI/SN 协商，否则 LNS 端将因协商不到 LAC client 或 LAC 端的 IMSI/SN 信息导致认证不通过。

3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入虚拟模板接口视图。

```
interface virtual-template interface-number
```

- (3) 开启 LNS 端 IMSI/SN 捆绑协商功能。请至少选择其中一项进行配置。

- 请依次执行以下命令配置 LNS 端发起 IMSI/SN 捆绑协商请求。

```
ppp lcp imsi request
```

```
ppp lcp sn request
```

缺省情况下，LNS 端不发起 IMSI/SN 捆绑协商请求。

- 配置协商时拆分对端用户名使用的分隔符。

```
ppp user accept-format imsi-sn split splitchart
```

缺省情况下，未配置协商认证时拆分对端用户名使用的分隔符。

如果二者同时配置，则优先使用协商到的 IMSI/SN 信息进行认证（这里认证是指 LNS 上送 AAA 服务器的 IMSI/SN 信息和 AAA 服务器上配置的 IMSI/SN 信息进行对比认证。）；如果没有协商到对端的 IMSI/SN 信息，则使用从对端用户名中拆分出来的 IMSI/SN 信息进行认证。

- (4) （可选）配置使用 IMSI/SN 信息替换用户名进行认证。

```
ppp user replace { imsi | sn }
```

缺省情况下，使用用户名进行认证。

1.9.2 配置LAC client支持与LNS端进行IMSI/SN捆绑协商

1. 功能简介

配置本功能后，当 LAC client 收到 LNS 端的 IMSI/SN 协商请求会把本地的 IMSI/SN 信息通过应答消息上送给 LNS 端。即使没有收到 LNS 端的 IMSI/SN 协商请求，LAC client 也会把本地的 IMSI/SN 信息按照 `ppp user attach-format imsi-sn split` 命令配置的规则组合到用户名中和用户名一起发送给 LNS 端。

2. 配置限制和指导

仅 3G 和 4G 路由器作为 LAC client 时支持本功能。有关 3G 和 4G 路由器的详细介绍，请参见“二层技术-广域网接入配置指导”中的“3G Modem 和 4G Modem 管理”。

3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入 Serial 接口视图。

```
interface serial cellular-number:set-number
```

Serial 接口是通过在 Cellular 接口配置 `serial-set` 命令后通道化出的一个接口。

- (3) 配置 LAC client 端接受 LNS 端发起的 IMSI 捆绑协商请求。

```
ppp lcp imsi accept
```

缺省情况下，LAC client 端不接受 LNS 端发起的 IMSI 捆绑协商请求。

- (4) 配置 LAC client 端接受 LNS 端发起的 SN 捆绑协商请求。

```
ppp lcp sn accept
```

缺省情况下，LAC client 端不接受 LNS 端发起的 SN 捆绑协商请求。

- (5) （可选）配置 LAC client 端的 IMSI 信息。

```
ppp lcp imsi string imsi-info
```

缺省情况下，IMSI 信息从本设备上自动获取。

- (6) （可选）配置 LAC client 端的 SN 信息。

```
ppp lcp sn string sn-info
```

缺省情况下，SN 信息从本设备上自动获取。

- (7) 配置协商认证时发送对端用户名使用的分隔符。

```
ppp user attach-format imsi-sn split splitchart
```

缺省情况下，未配置协商认证时发送对端用户名使用的分隔符。

1.10 L2TP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 L2TP 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** 命令可以强制断开指定的 L2TP 隧道。

表1-2 L2TP 显示和维护

操作	命令
显示当前L2TP隧道的信息	display l2tp tunnel [statistics]
显示当前L2TP会话的信息	display l2tp session [statistics]
显示当前L2TP非稳态会话的信息	display l2tp session temporary
显示虚拟PPP接口的相关信息	display interface [virtual-ppp [interface-number] [brief [description down]]
显示L2TP的VA池信息	display l2tp va-pool
显示VT接口产生的PPP会话的动态防火墙的统计信息	display ppp access-control interface virtual-template interface-number
强制断开指定的L2TP隧道	reset l2tp tunnel { id tunnel-id name remote-name }
清除虚拟PPP接口的统计信息	reset counters interface [virtual-ppp [interface-number]]

1.11 L2TP典型配置举例

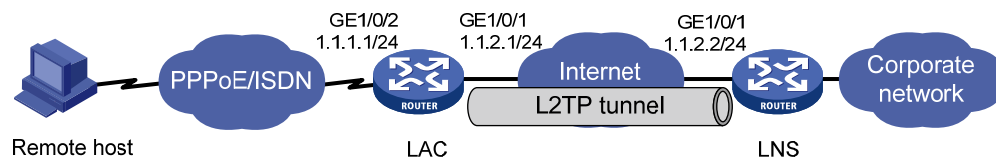
1.11.1 NAS-Initiated模式L2TP隧道配置举例

1. 组网需求

PPP 用户通过 LAC 接入 LNS，在 LAC 和 LNS 之间建立 L2TP 隧道，以使用户通过该 L2TP 隧道访问公司总部。

2. 组网图

图1-11 NAS-Initiated 模式 L2TP 隧道组网图



3. 配置步骤

(1) 配置 LAC 端

配置各接口的 IP 地址（略）。

创建本地 PPP 用户 vpduser，设置密码为 Hello。

```
<LAC> system-view
```

```
[LAC] local-user vpdnuser class network
[LAC-luser-network-vpdnuser] password simple Hello
[LAC-luser-network-vpdnuser] service-type ppp
[LAC-luser-network-vpdnuser] quit
```

配置 ISP 域 system 对 PPP 用户采用本地验证。

```
[LAC] domain system
[LAC-isp-system] authentication ppp local
[LAC-isp-system] quit
```

配置虚拟模板接口 1 的参数，采用 CHAP 认证对端。

```
[LAC] interface virtual-template 1
[LAC-Virtual-Template1] ppp authentication-mode chap domain system
[LAC-Virtual-Template1] quit
```

在接口 GigabitEthernet1/0/2 上启用 PPPoE Server 协议，并将该接口与虚拟模板接口 1 绑定。

```
[LAC] interface gigabitethernet 1/0/2
[LAC-GigabitEthernet1/0/2] pppoe-server bind virtual-template 1
[LAC-GigabitEthernet1/0/2] quit
```

开启 L2TP 功能。

```
[LAC] l2tp enable
```

创建 LAC 模式的 L2TP 组 1，配置隧道本端名称为 LAC，指定接入的 PPP 用户的用户名为 vpdnuser 时 LAC 向 LNS 发起隧道建立请求，并指定 LNS 地址为 1.1.2.2。

```
[LAC] l2tp-group 1 mode lac
[LAC-l2tp1] tunnel name LAC
[LAC-l2tp1] user fullusername vpdnuser
[LAC-l2tp1] lns-ip 1.1.2.2
```

启用隧道验证功能，并设置隧道验证密钥为 aabbcc。

```
[LAC-l2tp1] tunnel authentication
[LAC-l2tp1] tunnel password simple aabbcc
[LAC-l2tp1] quit
```

(2) 配置 LNS 端

配置各接口的 IP 地址。（略）

创建本地 PPP 用户 vpdnuser，设置密码为 Hello。

```
<LNS> system-view
[LNS] local-user vpdnuser class network
[LNS-luser-network-vpdnuser] password simple Hello
[LNS-luser-network-vpdnuser] service-type ppp
[LNS-luser-network-vpdnuser] quit
```

配置 ISP 域 system 对 PPP 用户采用本地验证。

```
[LNS] domain system
[LNS-isp-system] authentication ppp local
[LNS-isp-system] quit
```

开启 L2TP 功能。

```
[LNS] l2tp enable
```

#配置 PPP 地址池。

```
[LNS] ip pool aaa 192.168.0.10 192.168.0.20
```

```

[LNS] ip pool aaa gateway 192.168.0.1
# 创建接口 Virtual-Template1，PPP 认证方式为 CHAP，并使用地址池 aaa 为 LAC client 端
分配 IP 地址。
[LNS] interface virtual-template 1
[LNS-virtual-template1] ppp authentication-mode chap domain system
[LNS-virtual-template1] remote address pool aaa
[LNS-virtual-template1] quit
# 创建 LNS 模式的 L2TP 组 1，配置隧道本端名称为 LNS，指定接收呼叫的虚拟模板接口为
VT1，并配置隧道对端名称为 LAC。
[LNS] l2tp-group 1 mode lns
[LNS-l2tp1] tunnel name LNS
[LNS-l2tp1] allow l2tp virtual-template 1 remote LAC
# 启用隧道验证功能，并设置隧道验证密钥为 aabbcc。
[LNS-l2tp1] tunnel authentication
[LNS-l2tp1] tunnel password simple aabbcc
[LNS-l2tp1] quit

```

(3) 配置 Remote host 端

在 Remote host 上配置 PPPoE 拨号连接，在拨号网络窗口中输入用户名 vpdnuser 和密码 Hello 进行拨号。

4. 验证配置

拨号连接成功后，在 LNS 端通过命令 **display ppp access-user** 可查看在线用户的信息。

```

[LNS] display ppp access-user user-type lns
Interface Username MAC address IP address IPv6 address IPv6 PDPrefix
BAS0 vpdnuser - 192.168.0.10 - -

```

拨号连接成功后，Remote host 获取到 IP 地址 192.168.0.10，并可以 ping 通 LNS 的私网地址 192.168.0.1。

在 LNS 端，通过命令 **display l2tp tunnel** 可查看建立的 L2TP 隧道。

```

[LNS] display l2tp tunnel
LocalTID RemoteTID State Sessions RemoteAddress RemotePort RemoteName
196 3542 Established 1 1.1.2.1 1701 LAC

```

在 LNS 端，通过命令 **display l2tp session** 可查看建立的 L2TP 会话。

```

[LNS] display l2tp session
LocalSID RemoteSID LocalTID State
2041 64 196 Established

```

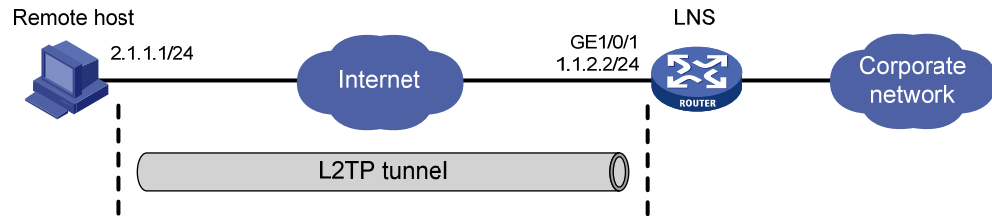
1.11.2 Client-Initiated模式L2TP隧道配置举例

1. 组网需求

PPP 用户直接与 LNS 建立 L2TP 隧道，通过 L2TP 隧道访问公司总部。

2. 组网图

图1-12 Client-Initiated 模式 L2TP 隧道组网图



3. 配置步骤

(1) 配置 LNS 端

配置接口的 IP 地址。（略）

配置路由，使得 LNS 与用户端主机之间路由可达。（略）

创建本地 PPP 用户 vpdnuser，设置密码为 Hello。

```
[LNS] local-user vpdnuser class network
[LNS-luser-network-vpdnuser] password simple Hello
[LNS-luser-network-vpdnuser] service-type ppp
[LNS-luser-network-vpdnuser] quit
```

配置 ISP 域 system 对 PPP 用户采用本地验证。

```
[LNS] domain system
[LNS-isp-system] authentication ppp local
[LNS-isp-system] quit
```

开启 L2TP 功能。

```
[LNS] l2tp enable
```

#配置 PPP 地址池。

```
[LNS] ip pool aaa 192.168.0.10 192.168.0.20
[LNS] ip pool aaa gateway 192.168.0.1
```

创建接口 Virtual-Template1，PPP 认证方式为 CHAP，并使用地址池 aaa 为 LAC client 端分配 IP 地址。

```
[LNS] interface virtual-template 1
[LNS-virtual-template1] ppp authentication-mode chap domain system
[LNS-virtual-template1] remote address pool aaa
[LNS-virtual-template1] quit
```

创建 LNS 模式的 L2TP 组 1，配置隧道本端名称为 LNS，指定接收呼叫的虚拟模板接口为 VT1。

```
[LNS] l2tp-group 1 mode lns
[LNS-l2tp1] tunnel name LNS
[LNS-l2tp1] allow l2tp virtual-template 1
```

关闭 L2TP 隧道验证功能。

```
[LNS-l2tp1] undo tunnel authentication
```

(2) 配置 Remote host 端

配置 IP 地址为 2.1.1.1，并配置路由，使得 Remote host 与 LNS（IP 地址为 1.1.2.2）之间路由可达。

利用 Windows 系统创建虚拟专用 L2TP 网络连接，或安装 L2TP 客户端软件，如 WinVPN Client。

在 Remote host 上进行如下 L2TP 配置（设置的过程与相应的客户端软件有关，以下为设置的内容）：

- 设置 PPP 用户名为 vpdnuser，密码为 Hello。
- 将 LNS 的 IP 地址设为安全网关的 Internet 接口地址（本例中 LNS 端与隧道相连接的以太网接口的 IP 地址为 1.1.2.2）。
- 修改连接属性，将采用的协议设置为 L2TP，将加密属性设为自定义，并选择 CHAP 验证。

4. 验证配置

在 Remote host 上触发 L2TP 拨号。拨号连接成功后，在 LNS 端通过命令 **display ppp access-user** 可查看在线用户的信息。

```
[LNS] display ppp access-user user-type lns
Interface Username MAC address      IP address      IPv6 address    IPv6 PDPprefix
BAS0      vpdnuser -                192.168.0.10   -                -
```

拨号连接成功后，Remote host 获取到 IP 地址 192.168.0.10，并可以 Ping 通 LNS 的私网地址 192.168.0.1。

在 LNS 端，通过命令 **display l2tp session** 可查看建立的 L2TP 会话。

```
[LNS-l2tp1] display l2tp session
LocalSID      RemoteSID      LocalTID      State
89            36245         10878        Established
```

在 LNS 端，通过命令 **display l2tp tunnel** 可查看建立的 L2TP 隧道。

```
[LNS-l2tp1] display l2tp tunnel
LocalTID RemoteTID State          Sessions RemoteAddress  RemotePort RemoteName
10878    21      Established    1        2.1.1.1        1701      PC
```

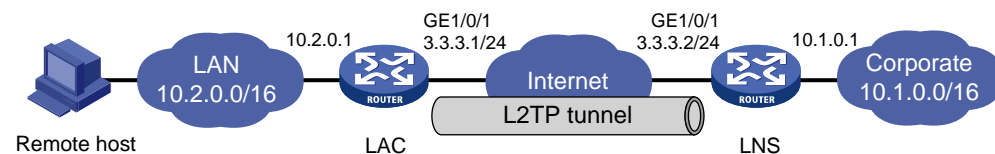
1.11.3 LAC-Auto-Initiated模式L2TP隧道配置举例

1. 组网需求

PPP 用户接入之前，在 LAC 和 LNS 之间采用 LAC-Auto-Initiated 模式建立 L2TP 隧道。PPP 用户接入后，通过已经建立的 L2TP 隧道访问公司总部。

2. 组网图

图1-13 LAC-Auto-Initiated 模式 L2TP 隧道组网图



3. 配置步骤

(1) 配置 LAC 端

```

# 配置各接口的 IP 地址（略）。
# 开启 L2TP 功能。
<LAC> system-view
[LAC] l2tp enable
# 创建 LAC 模式的 L2TP 组 1。
[LAC] l2tp-group 1 mode lac
# 配置 LAC 端本端名称为 LAC，并指定 LNS 的 IP 地址为 3.3.3.2。
[LAC-l2tp1] tunnel name LAC
[LAC-l2tp1] lns-ip 3.3.3.2
# 开启隧道验证功能，并设置隧道验证密钥为 aabbcc。
[LAC-l2tp1] tunnel authentication
[LAC-l2tp1] tunnel password simple aabbcc
[LAC-l2tp1] quit
# 创建虚拟 PPP 接口 Virtual-PPP 1，配置 PPP 用户的用户名为 vpdnuser、密码为 Hello，并配置 PPP 验证方式为 PAP。
[LAC] interface virtual-ppp 1
[LAC-Virtual-PPP1] ip address ppp-negotiate
[LAC-Virtual-PPP1] ppp pap local-user vpdnuser password simple Hello
[LAC-Virtual-PPP1] quit
# 配置私网路由，访问公司总部的报文将通过 L2TP 隧道转发。
[LAC] ip route-static 10.1.0.0 16 virtual-ppp 1
# 触发 LAC 发起 L2TP 隧道建立请求。
[LAC] interface virtual-ppp 1
[LAC-Virtual-PPP1] l2tp-auto-client l2tp-group 1

```

(2) 配置 LNS 端

```

# 配置各接口的 IP 地址（略）。
# 创建本地 PPP 用户 vpdnuser，配置密码为 Hello。
<LNS> system-view
[LNS] local-user vpdnuser class network
[LNS-luser-network-vpdnuser] password simple Hello
[LNS-luser-network-vpdnuser] service-type ppp
[LNS-luser-network-vpdnuser] quit
# 创建接口 Virtual-Template1，配置 VT 口 IP 地址，PPP 认证方式为 PAP，并指定为 LAC client 端分配 IP 地址为 192.168.0.10。
[LNS] interface virtual-template 1
[LNS-virtual-template1] ip address 192.168.0.1 24
[LNS-virtual-template1] ppp authentication-mode pap
[LNS-virtual-template1] remote address 192.168.0.10
[LNS-virtual-template1] quit
# 配置 ISP 域 system 对 PPP 用户采用本地验证。
[LNS] domain system
[LNS-isp-system] authentication ppp local
[LNS-isp-system] quit
# 开启 L2TP 功能，并创建 LNS 模式的 L2TP 组 1。

```

```

[LNS] l2tp enable
[LNS] l2tp-group 1 mode lns
# 配置 LNS 端本端名称为 LNS，指定接收呼叫的虚拟模板接口为 VT1，并配置隧道对端名称为 LAC。
[LNS-l2tp1] tunnel name LNS
[LNS-l2tp1] allow l2tp virtual-template 1 remote LAC
# 启用隧道验证功能，并设置隧道验证密钥为 aabbcc。
[LNS-l2tp1] tunnel authentication
[LNS-l2tp1] tunnel password simple aabbcc
[LNS-l2tp1] quit
# 配置私网路由，下一跳指定为 LNS 为 LAC 的 Virtual-PPP 1 接口分配的私网 IP 地址 192.168.0.10 使得访问 PPP 用户的报文将通过 L2TP 隧道转发。
[LNS] ip route-static 10.2.0.0 16 192.168.0.10

```

(3) 配置 Remote host 端

Remote host 上应将 LAC 设置为网关。

4. 验证配置

在 LNS 端，通过命令 **display l2tp session** 可查看建立的 L2TP 会话。

```

[LNS] display l2tp session
LocalSID      RemoteSID      LocalTID      State
21409         3395          4501         Established

```

在 LNS 端，通过命令 **display l2tp tunnel** 可查看建立的 L2TP 隧道。

```

[LNS] display l2tp tunnel
LocalTID RemoteTID State      Sessions RemoteAddress  RemotePort RemoteName
4501     524     Established 1         3.3.3.1         1701     LAC

```

在 LNS 端，可以 Ping 通 LAC 的私网地址 10.2.0.1，说明 10.2.0.0/16 和 10.1.0.0/16 网络内的主机可以通过 L2TP 隧道通信。

```

[LNS] ping -a 10.1.0.1 10.2.0.1
Ping 10.2.0.1 (10.2.0.1): 56 data bytes, press CTRL_C to break
56 bytes from 10.2.0.1: icmp_seq=0 ttl=128 time=1.000 ms
56 bytes from 10.2.0.1: icmp_seq=1 ttl=128 time=1.000 ms
56 bytes from 10.2.0.1: icmp_seq=2 ttl=128 time=1.000 ms
56 bytes from 10.2.0.1: icmp_seq=3 ttl=128 time=1.000 ms
56 bytes from 10.2.0.1: icmp_seq=4 ttl=128 time=1.000 ms

--- Ping statistics for 10.2.0.1 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 1.000/1.000/1.000/0.000 ms

```

1.12 L2TP常见故障处理

1.12.1 远端系统无法访问企业内部网络

1. 故障现象

远端系统无法访问企业内部网络。

2. 故障分析

主要有以下几种原因：

- 可能是如下原因导致 Tunnel 建立失败：
 - 在 LAC 端，LNS 的地址设置不正确。
 - LNS 端没有设置可以接收该隧道对端的 L2TP 组。
 - 只有一端启用 Tunnel 验证或两端均启用 Tunnel 验证但验证密码不一致。
- 可能是如下原因导致 PPP 协商不通过：
 - LAC 端设置的用户名与密码有误，或者是 LNS 端没有设置相应的用户。
 - LNS 端不能分配地址。
 - 密码验证类型不一致。

3. 故障处理

- (1) 检查在 LAC 端配置的 LNS 的 IP 地址是否正确，具体可以查看 **lns-ip** 命令的说明。
- (2) 检查在 LNS 端配置的接受来自 LAC 的 L2TP 隧道建立请求是否正确，具体可查看 **allow l2tp** 命令的说明。
- (3) 如果配置了验证，检查并保证双方都启用了隧道验证并且配置相同的验证密钥。
- (4) 检查 LAC 端配置的用户名和密码是否正确，以及 LNS 端是否配置了相应的用户。
- (5) 检查远端系统和 LNS 对 IP 地址协商相关的配置是否正确。
- (6) 检查密码验证类型是否一致。例如，Windows 2000 所创建的 VPN 连接缺省的验证类型为 MSCHAP，如果对端不支持 MSCHAP，建议改为 CHAP。

1.12.2 隧道建立成功，但无法传输数据

1. 故障现象

数据传输失败，在隧道建立后数据不能传输，如 Ping 不通对端。

2. 故障分析

可能有如下原因：

- 路由问题：LAC 和 LNS 上需要存在到达对端私网的路由，否则会导致数据传输失败。
- 网络拥挤：Internet 主干网产生拥挤，丢包现象严重。L2TP 是基于 UDP 进行传输的，UDP 不对报文进行差错控制。如果是在线路质量不稳定的情况下进行 L2TP 应用，有可能会产生 Ping 不通对端的情况。

3. 故障处理

- (1) 在 LAC 和 LNS 上执行 **display ip routing-table** 命令，查看设备上是否存在到达对端私网的路由。若不存在，则需要配置静态路由或动态路由协议，在设备上添加该路由。
- (2) 增加链路带宽，提高线路质量。

目 录

1 HDLC	1-1
1.1 HDLC简介	1-1
1.1.1 HDLC特点.....	1-1
1.1.2 HDLC链路状态轮询机制.....	1-1
1.2 配置接口封装HDLC协议	1-1
1.3 配置轮询功能.....	1-2
1.4 HDLC显示和维护	1-2
1.5 HDLC典型配置举例	1-2
1.5.1 HDLC基本组网配置举例.....	1-2
2 HDLC链路捆绑	2-1
2.1 HDLC链路捆绑简介	2-1
2.1.1 技术优点.....	2-1
2.1.2 基本概念.....	2-1
2.1.3 成员接口状态.....	2-2
2.1.4 负载分担方式.....	2-2
2.2 配置HDLC捆绑接口	2-3
2.2.1 配置HDLC捆绑接口基本功能.....	2-3
2.2.2 配置处理接口流量的slot	2-4
2.2.3 恢复HDLC捆绑接口的缺省配置.....	2-5
2.3 配置接口加入HDLC捆绑	2-5
2.4 HDLC链路捆绑显示和维护.....	2-6
2.5 HDLC链路捆绑典型配置举例.....	2-7
2.5.1 HDLC链路捆绑基本组网配置举例.....	2-7

1 HDLC



说明

本特性仅在路由器上安装了 SAE、E1、E1-F、T1、T1-F、POS、CPOS、CE3 和 CT3 接口模块时支持。

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，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。

1.1.2 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	<pre>display interface serial <i>interface-number</i> display interface pos <i>interface-number</i></pre>
清除封装HDLC协议接口的统计信息	<pre>reset counters interface [serial [<i>interface-number</i>]] reset counters interface [pos [<i>interface-number</i>]]</pre>

1.5 HDLC典型配置举例

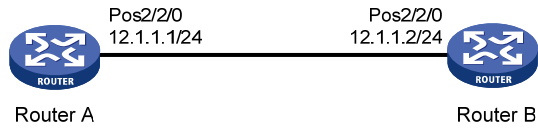
1.5.1 HDLC基本组网配置举例

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 2/2/0
[RouterA-Pos2/2/0] clock master
[RouterA-Pos2/2/0] link-protocol hdlc
[RouterA-Pos2/2/0] ip address 12.1.1.1 24
[RouterA-Pos2/2/0] quit
```

(2) 配置 Router B

```
<RouterB> system-view
[RouterB] interface pos 2/2/0
[RouterB-Pos2/2/0] link-protocol hdlc
[RouterB-Pos2/2/0] 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



说明

本特性仅在路由器上安装了SAE、E1、E1-F、T1、T1-F、POS、CPOS、CE3和CT3接口模块时支持。

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 接口和 Serial 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。



说明

可以将不同类型的接口加入同一个 HDLC 捆绑。

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 $M \leq N$ 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 $P \geq Q$ 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；如果用户未配置或配置值大于设备支持的最多选中成员接口数目，则以设备支持的最多选中成员接口数目为准。

2.1.4 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。

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) 配置负载分担方式。

```
bundle load-balance { per-flow | per-packet }
```

缺省情况下，采用逐包负载分担。

建议 HDLC 捆绑链路两端采用相同的负载分担方式。

- (4) （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。

- (5) 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。

- (6) 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准。

设备支持的最多选中成员接口数目为 64。

- (7) （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”。

- (8) （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”。

- (9) (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。

- (10) 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 配置处理接口流量的slot

1. 功能简介

当要求同一个处理接口的流量必须在同一个 slot 上进行处理时，可以在处理接口下配置处理接口流量的 slot。

为提高当前接口处理流量的可靠性，可以通过 **service** 命令和 **service standby** 命令为接口分别指定一个主用 slot 和一个备用 slot 进行流量处理。

接口上同时配置了主用 slot 和备用 slot 时，流量处理的机制如下：

- 当主用 slot 不可用时，流量由备用 slot 处理。之后，即使主用 slot 恢复可用，流量也继续由备用 slot 处理；仅当备用 slot 不可用时，流量才切换到主用 slot。
- 当主用 slot 和备用 slot 均不可用时，流量由接收报文的 slot 处理；之后，主用 slot 和备用 slot 谁先恢复可用，流量就由谁处理。

如果接口上未配置主用 slot 和备用 slot，则业务处理在接收报文的 slot 上进行。

2. 配置限制和指导

为避免不必要的流量切换，建议配置主用 slot 后，再配置备用 slot。如果先配置备用 slot，则流量由备用 slot 处理；在配置主用 slot 后，流量将会从备用 slot 切换到主用 slot。

3. 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) 配置处理接口流量的主用 slot。

(独立运行模式)

service slot slot-number

(IRF 模式)

service chassis chassis-number slot slot-number

缺省情况下，未配置处理接口流量的主用 slot。

- (4) 配置处理接口流量的备用 slot。

(独立运行模式)

```
service standby slot slot-number
```

(IRF 模式)

```
service standby chassis chassis-number slot slot-number
```

缺省情况下，未配置处理接口流量的备用 slot。

2.2.3 恢复HDLC捆绑接口的缺省配置

1. 配置限制和指导



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

- POS 接口、Serial 接口支持加入 HDLC 捆绑，并且支持加入同一个 HDLC 捆绑中。
- 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 接口或者 Serial 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。接口加入 HDLC 捆绑之后不允许修改链路层协议。

- (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	(独立运行模式) display bundle hdlc-bundle [<i>bundle-id</i>] slot <i>slot-number</i> (IRF模式) display bundle hdlc-bundle [<i>bundle-id</i>] chassis <i>chassis-number</i> slot <i>slot-number</i>
显示HDLC捆绑接口的相关信息	display interface [hdlc-bundle [<i>bundle-id</i>]] [brief [description down]]
清除HDLC捆绑接口的统计信息	reset counters interface [hdlc-bundle [<i>bundle-id</i>]]

2.5 HDLC链路捆绑典型配置举例

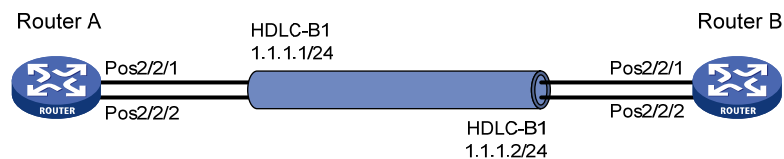
2.5.1 HDLC链路捆绑基本组网配置举例

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 POS2/2/1、POS2/2/2 加入到 HDLC 捆绑 1（POS 接口采用主时钟模式）。

```
[RouterA] interface pos 2/2/1
[RouterA-Pos2/2/1] clock master
[RouterA-Pos2/2/1] link-protocol hdlc
[RouterA-Pos2/2/1] bundle id 1
[RouterA-Pos2/2/1] quit
[RouterA] interface pos 2/2/2
[RouterA-Pos2/2/2] clock master
[RouterA-Pos2/2/2] link-protocol hdlc
[RouterA-Pos2/2/2] bundle id 1
[RouterA-Pos2/2/2] 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 POS2/2/1、POS2/2/2 加入到 HDLC 捆绑 1。

```
[RouterB] interface pos 2/2/1
[RouterB-Pos2/2/1] link-protocol hdlc
[RouterB-Pos2/2/1] bundle id 1
[RouterB-Pos2/2/1] quit
```

```
[RouterB] interface pos 2/2/2
[RouterB-Pos2/2/2] link-protocol hdlc
[RouterB-Pos2/2/2] bundle id 1
[RouterB-Pos2/2/2] 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
Bundle: HDLC-bundle1
  Selected members: 2, Total bandwidth: 1244160 kbps
  Member           State           Bandwidth(kbps)  Priority
  Pos2/2/1         Selected        622080           32768
  Pos2/2/2         Selected        622080           32768
```

上述信息表明，POS2/2/1 和 POS2/2/2 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 ISDN.....	1-1
1.1 ISDN简介	1-1
1.1.1 ISDN接口.....	1-1
1.1.2 ISDN协议栈.....	1-2
1.1.3 ISDN典型组网.....	1-2
1.2 ISDN PRI接口配置准备.....	1-3
1.3 ISDN配置任务简介	1-3
1.3.1 ISDN BRI接口配置任务简介	1-3
1.3.2 ISDN PRI接口配置任务简介	1-4
1.4 配置ISDN接口所使用的ISDN协议	1-4
1.5 配置ISDN接口所使用的协议模式.....	1-5
1.6 配置ISDN NI协议SPID参数.....	1-5
1.6.1 SPID参数简介.....	1-5
1.6.2 动态获取SPID.....	1-6
1.6.3 静态配置SPID.....	1-7
1.6.4 配置NIT模式	1-7
1.7 配置ISDN Q.931 协议的协商参数.....	1-8
1.8 配置ISDN Q.931 协议的呼叫管理参数.....	1-9
1.8.1 配置本地管理ISDN B通道.....	1-9
1.8.2 配置允许呼入的主叫号码.....	1-10
1.8.3 配置入呼叫时需要检查的被叫号码及子地址	1-10
1.8.4 配置在出呼叫中携带主叫号码.....	1-11
1.9 配置ISDN Q.921 协议的运行参数.....	1-11
1.9.1 配置ISDN BRI接口的工作模式	1-11
1.9.2 配置ISDN BRI接口的TEI值处理方式	1-12
1.9.3 配置ISDN BRI专线.....	1-12
1.9.4 配置ISDN BRI接口的Q.921 常建链功能	1-13
1.9.5 配置ISDN BRI接口的物理层常激活功能	1-13
1.9.6 配置ISDN BRI接口的远程供电功能	1-14
1.9.7 配置ISDN BRI接口的滑动窗口的大小	1-14
1.9.8 配置ISDN PRI接口的滑动窗口的大小	1-15
1.10 ISDN显示和维护.....	1-15
1.11 ISDN典型配置举例.....	1-16

1.11.1 设备通过ISDN PRI线路互连传输数据	1-16
1.11.2 设备通过ISDN BRI线路的NI协议互连传输数据.....	1-17
1.12 ISDN常见故障的诊断与排除	1-19
1.12.1 通过ISDN PRI或BRI线路相连的两台设备之间无法ping通	1-19

1 ISDN

1.1 ISDN简介

ISDN(Integrated Services Digital Network, 综合业务数字网)是由 IDN(Integrated Digital Network, 综合数字网)演变而成, 提供端到端的数字连接, 支持一系列广泛的业务(包括语音和数据业务)。

ISDN 产生于 80 年代初期, 它的基本特点是利用单一的通信网络实现包括语音、数据在内的综合业务。ISDN 对于提高通信网的效率, 满足社会对通信业务的日益增长的需求具有十分重要的意义。

ISDN 是一个数字网络。在这个网络中, 一切信号都以数字形式进行传输和交换。这就是说, 不论原始信号是语音还是数据, 都先在终端中转换成数字信号, 然后通过数字信道将信号送到 ISDN 网络, 由 ISDN 网络负责将这些数字信号传递到通信另一方的终端设备。

由于 ISDN 实现了端到端的数字连接, 所以它能够支持包括语音、数据在内的各种综合业务。从理论上说, 任何形式的原始信号, 只要能够转变成数字信号, 都可以利用 ISDN 来进行传送和交换, 实现用户之间的通信。

另外, ISDN 为用户提供一组标准的多用途用户—网络接口。所谓“多用途”, 是指该接口对各种各样的业务都是通用的, 也就是说不同的业务和不同的终端可以经过同一个接口接入网络。

1.1.1 ISDN接口

ISDN 定义了两种接口结构:

- BRI (Basic Rate Interface, 基本速率接口)
- PRI (Primary Rate Interface, 基群速率接口)

ISDN 接口通过时分复用技术, 在物理上把一个接口划分为多个信道(时隙)来使用。ISDN 的信道分为 B、D 两种类型, 其中:

- B 信道为用户信道, 用来传送语音、数据等用户信息, 传输速率是 64kbit/s;
- D 信道为控制信道, 用来传送公共信道信令, 这些信令用来控制同一接口的 B 信道上的呼叫。D 信道的速率是 16kbit/s (BRI) 或 64kbit/s (PRI)。

正是这样通过 B 通道和 D 通道的划分, ISDN 接口实现了数据和控制流的分离。

1. BRI接口

BRI 接口为 2B+D, 是把一个总带宽为 144kbit/s 的物理接口划分为 3 个时隙, 一个时隙作为 D 信道, 用于传输控制信息, 另外两个时隙(编号为 1、2)分别作为两个 B 信道, 用于传输数据、语音等信息。

2. PRI接口

PRI 接口为 30B+D (总带宽近 2Mbit/s) 或 23B+D (总带宽近 1.5Mbit/s), 其中 30B+D 的 PRI 接口为 CE1 PRI, 一般在中国、亚洲部分国家和地方、欧洲使用, 23B+D 的 PRI 接口为 CT1 PRI 接口, 一般在北美、加拿大和日本使用, 香港地区也多数使用 CT1 PRI。

- (1) CE1 PRI 是把接口划分为 32 个时隙, 对应编号为 0~31, 其中时隙 0 用于传输同步信息, 时隙 16 作为 D 信道用于传输控制信息, 时隙 1~15、17~31 作为 B 信道用于传输数据、语音等信息。

(2) CT1 PRI 是把接口划分为 24 个时隙，对应编号为 1~24，其中时隙 24 作为 D 信道用于传输控制信息，其它时隙作为 B 信道用于传输数据、语音等信息。

ANSI 推荐使用 T1 系统，ITU-T 推荐使用 E1 系统。

1.1.2 ISDN协议栈

ISDN 是按需呼叫链路，当有通信需求时，通过 ISDN 协议建立一条连接，之后可以在该连接上传输语音或数据。在整个数通网络协议栈中，ISDN 属于物理层。但是，单看 ISDN，它也有自己的协议栈，并且 ISDN 的 B 信道协议栈和 D 信道协议栈是相对独立的。

1. B信道协议栈

B 信道是数据信息的协议栈。B 信道的链路层支持 PPP 等协议，链路层之上支持传输语音和数据信息。

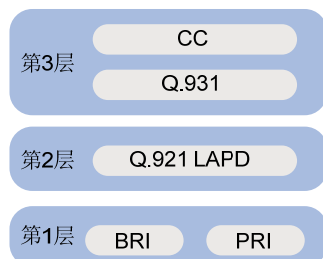
2. D信道协议栈

D 信道是控制信息的协议栈。对于 ISDN 接口，主要关注 D 信道上的协议。

如 [图 1-1](#) 所示，ISDN D 信道协议栈分为三层，其中：

- Q.921 是 D 信道的数据链路层协议，它定义了接口上第二层实体间通过 D 信道交换信息的规则，同时支持第三层实体 Q.931 的接入。
- Q.931 是 D 信道的网络层协议，它提供了在通信应用实体间建立、保持和终结网络连接的方法。
- CC (Call Control, 呼叫控制) 是对 Q.931 协议进一步的封装，Q.931 把由网络侧传递过来的消息转发给 CC，由 CC 和高层应用（高层应用包括：DDR、语音）进行信息转换。

图1-1 ISDN D 信道协议栈



1.1.3 ISDN典型组网

数据 ISDN 典型应用组网如 [图 1-2](#) 所示。语音 ISDN 典型应用组网如 [图 1-3](#) 所示。

图1-2 数据 ISDN 组网图

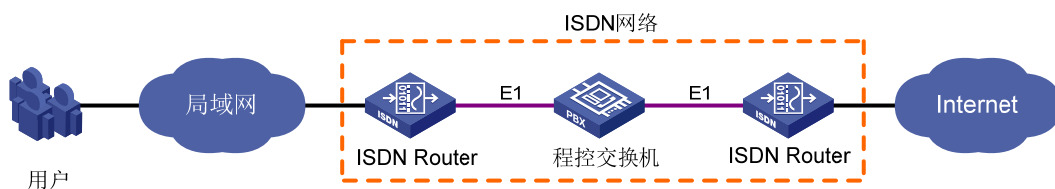
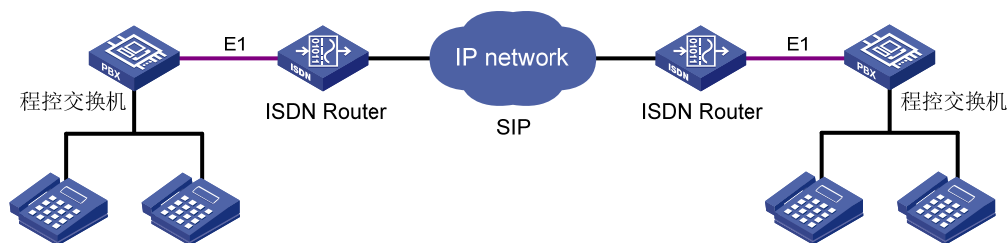


图1-3 语音 ISDN 组网图



1.2 ISDN PRI接口配置准备

CE1 PRI 接口通过 CE1/PRI 接口封装而成，CT1 PRI 接口通过 CT1/PRI 接口封装而成，在进行下面的 ISDN 配置前需要通过 `pri-set` 命令将 CE1/PRI 接口和 CT1/PRI 接口的时隙捆绑为 pri set，此后系统会自动创建一个 Serial 接口来对应生成的 ISDN PRI 接口，本文关于 ISDN PRI 接口的 ISDN 配置都是在该 Serial 接口上进行的。

1.3 ISDN配置任务简介

本文仅介绍 BRI 接口、PRI 接口上支持的 ISDN 相关配置，关于这两个接口的详细介绍以及基本配置，请参见“接口管理配置指导”中的“WAN 接口”。

1.3.1 ISDN BRI接口配置任务简介

ISDN BRI 接口配置任务如下：

- (1) [配置ISDN接口所使用的ISDN协议](#)
- (2) [配置ISDN接口所使用的协议模式](#)
- (3) [（可选）配置ISDN NI协议SPID参数](#)
- (4) [配置ISDN Q.931 协议的协商参数](#)
- (5) [（可选）配置ISDN Q.931 协议的呼叫管理参数](#)
 - [配置本地管理ISDN B通道](#)
 - [配置允许呼入的主叫号码](#)
 - [配置入呼叫时需要检查的被叫号码及子地址](#)
 - [配置在出呼叫中携带主叫号码](#)
- (6) [（可选）配置ISDN Q.921 协议的运行参数](#)
 - [配置ISDN BRI接口的工作模式](#)
 - [配置ISDN BRI接口的TEI值处理方式](#)
 - [配置ISDN BRI专线](#)
 - [配置ISDN BRI接口的Q.921 常建链功能](#)
 - [配置ISDN BRI接口的物理层常激活功能](#)
 - [配置ISDN BRI接口的远程供电功能](#)
 - [配置ISDN BRI接口的滑动窗口的大小](#)

1.3.2 ISDN PRI接口配置任务简介

ISDN PRI 接口配置任务如下：

- (1) [配置ISDN接口所使用的ISDN协议](#)
- (2) [配置ISDN接口所使用的协议模式](#)
- (3) [配置ISDN Q.931 协议的协商参数](#)
- (4) [（可选）配置ISDN Q.931 协议的呼叫管理参数](#)
 - [配置本地管理ISDN B通道](#)
 - [配置允许呼入的主叫号码](#)
 - [配置入呼叫时需要检查的被叫号码及子地址](#)
 - [配置在出呼叫中携带主叫号码](#)
- (5) [（可选）配置ISDN PRI接口的滑动窗口的大小](#)

1.4 配置ISDN接口所使用的ISDN协议

1. 功能简介

由于 ITU-T 提出的 ISDN 协议在不同的地区提供业务的不同，由此产生了适用于部分地区或者国家的 ISDN 协议，比如日本的 NTT（Nippon Telegraph and Telephone Corporation，日本电报电话公司）、欧洲的 ETSI（European Telecommunications Standards Institute，欧洲电信标准协会）、北美的 NI（National ISDN，国家 ISDN）、AT&T、ANSI（American National Standards Institute，美国国家标准协会）等。

除了缺省支持 ITU-T 的 DSS1 ISDN 协议之外，设备还支持 NTT、ETSI、AT&T、ANSI、NI、NI2、QSIG、5ESS 这几种协议的基本呼叫功能，但不支持这几种协议的补充业务功能。

用户可以根据所在地区选择使用合适的 ISDN 协议。

2. 配置限制和指导

工作在网络侧模式时，不可以配置 ANSI、AT&T、ETSI、NI、NTT 协议。

当 ISDN 接口上存在呼叫时，不能配置本功能。

不同类型接口上协议的支持情况如 [表 1-1](#) 所示。

表1-1 ISDN 协议支持的接口

协议	支持的接口
ANSI	BRI和CT1/PRI接口
AT&T	CT1/PRI接口
5ESS	CT1/PRI接口
DSS1	BRI、CE1/PRI以及CT1/PRI接口
ETSI	BRI、CE1/PRI以及CT1/PRI接口
NI（National ISDN）	BRI接口
NI2	CT1/PRI接口
QSIG	CE1/PRI以及CT1/PRI接口

协议	支持的接口
NTT	BRI和CT1/PRI接口

3. 配置步骤

(1) 进入系统视图。

```
system-view
```

(2) 进入 ISDN BRI 接口或者 ISDN PRI 接口视图。

```
interface interface-type interface-number
```

(3) 配置 ISDN 接口所使用的 ISDN 协议。

```
isdn protocol-type protocol
```

缺省情况下，ISDN 的 BRI 和 PRI 接口都是使用 DSS1 协议。

1.5 配置ISDN接口所使用的协议模式

1. 功能简介

协议模式分为两种：用户侧模式、网络侧模式。当两台 ISDN 设备互通时，必须一端工作在用户侧模式，另一端工作在网络侧模式。

当语音 BSV 板卡上的 BRI 接口和 ISDN 电话直接相连时，BRI 接口需要配置为网络侧模式，在其它场景下，设备上的 ISDN 接口通常都需要配置为用户侧模式。

2. 配置限制和指导

运行数据业务的 BRI 接口不支持网络侧模式。

ANSI、AT&T、ETSI、NI、NTT 协议不支持网络侧模式。

当 ISDN 接口上存在呼叫时，不能配置本功能。

3. 配置步骤

(1) 进入系统视图。

```
system-view
```

(2) 进入 ISDN BRI 接口或者 ISDN PRI 接口视图。

```
interface interface-type interface-number
```

(3) 配置 ISDN 接口所使用的协议模式。

```
isdn protocol-mode { network | user }
```

缺省情况下，ISDN 接口所使用的协议模式为用户侧模式。

1.6 配置ISDN NI协议SPID参数

1.6.1 SPID参数简介

北美地区的 NI 协议只适用于 BRI 接口。该 ISDN 网络在 BRI 接口上使用 SPID (Service Profile Identification, 业务轮廓标识) 作为向用户提供不同业务的标识，程控交换机根据 SPID 为终端用户提供该 SPID 所对应的一组业务 (音频、数字、语音)。BRI 接口的每一个 B 信道对应一个 SPID，

对于 ISDN 终端用户而言，只有在利用 SPID 与程控交换机完成 SPID 的握手交互后才能进行正常的呼叫、挂断流程。因此，在 Q.921 成功建立链路之后且开始 Q.931 的呼叫处理之前，需要经过获取 SPID 和利用获取的 SPID 与程控交换机交互完成第三层（Q.931）初始化的操作之后，才能够正常开始呼叫和挂断流程，否则无法正常完成呼叫功能。

SPID 信息的获取可以通过静态配置，也可以通过动态协商。通过哪种方式获取，由程控交换机决定。

动态获取 SPID 时，设备作为 ISDN 终端，发送 Q931 INFORMATION 消息给程控交换机，该 INFORMATION 消息中携带一个非法的 SPID 值，程控交换机收到这个 INFORMATION 消息后发送携带合法 SPID 值的 INFORMATION 消息（一次或多次）给设备，设备选中一个合法的 SPID 值作为自己的 SPID，后面开始第三层初始化流程。

动态获取 SPID 或静态配置 SPID 都需要进行第三层初始化流程，这个流程仍然通过 Q931 INFORMATION 消息完成。设备发送 INFORMATION 消息给程控交换机，携带已经获得（动态获取或静态配置）的一个合法的 SPID 值，程控交换机收到这个 INFORMATION 消息后用了一个 INFORMATION 消息作为应答，携带终端 ID 信息单元，第三层初始化流程结束。

1.6.2 动态获取SPID

1. 功能简介

缺省情况下，设备采用动态协商方式获取 SPID，由程控交换机为设备动态分配 SPID。

动态协商 SPID 时，如果程控交换机提供了多个 SPID 给设备，则设备根据每个 SPID 提供的业务类型是否满足当前配置的可接受业务类型来决定选择哪一个 SPID。缺省情况下，设备优先接受程控交换机发送的同时支持语音（speech）和数据（data）业务的 SPID。

2. 配置限制和指导

当 ISDN BRI 接口正在进行 SPID 协商时，不能配置本功能。

3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入 ISDN BRI 接口视图。

```
interface bri interface-number
```

- (3) 配置 SPID 协商时设备可接受的业务类型。

```
isdn spid service [ audio | data | speech ]
```

缺省情况下，设备可接受程控交换机发送的支持语音（speech）和数据（data）业务的 SPID。

- (4) 配置 TSPID 定时器的时长。

```
isdn spid timer seconds
```

缺省情况下，TSPID 定时器的时长为 30 秒。

当设备采用 INFORMATION 消息发起协商或者初始化请求之后，将启用 TSPID 定时器，若协商或初始化请求无响应，当 TSPID 定时器超时后设备将重发 INFORMATION 消息。

- (5) 配置 INFORMATION 消息的重发次数。

```
isdn spid resend times
```

缺省情况下，INFORMATION 消息重发次数为 1 次。

- (6) (可选) 触发一次 SPID 的协商请求。

```
isdn spid auto-trigger
```

缺省情况下, 没有呼叫触发时, BRI 接口不会主动发起 SPID 的协商请求。

1.6.3 静态配置SPID

1. 功能简介

静态配置 SPID 时, 用户需要手工分别配置 B1 通道和 B2 通道的 SPID (LDN) 值。配置的 SPID 值要与程控交换机上的 SPID (LDN) 值相同。程控交换机的 SPID (LDN) 值是由运营商在规划网络时配置的。

2. 配置限制和指导

配置了 LDN (Local Dialing Number, 本地拨号号码) 后, **isdn calling** 命令的配置将失效。

当 ISDN BRI 接口上存在呼叫时, 不能配置本功能。

当 ISDN BRI 接口正在进行 SPID 协商时, 不能配置本功能。

3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入 ISDN BRI 接口视图。

```
interface bri interface-number
```

- (3) 配置 BRI 接口 B1 通道的 SPID 值。

```
isdn spid1 spid [ ldn ]
```

缺省情况下, BRI 接口 B1 通道的 SPID 和 LDN 值均为空。

- (4) 配置 BRI 接口 B2 通道的 SPID 值。

```
isdn spid2 spid [ ldn ]
```

缺省情况下, BRI 接口 B2 通道的 SPID 和 LDN 值均为空。

- (5) 配置 TSPID 定时器的时长。

```
isdn spid timer seconds
```

缺省情况下, TSPID 定时器的时长为 30 秒。

当设备采用 INFORMATION 消息发起初始化请求之后, 将启用 TSPID 定时器, 若初始化请求无响应, 当 TSPID 定时器超时后设备将重发 INFORMATION 消息。

- (6) 配置 INFORMATION 消息的重发次数。

```
isdn spid resend times
```

缺省情况下, INFORMATION 消息重发次数为 1 次。

1.6.4 配置NIT模式

1. 功能简介

对于采用 NI 协议的 BRI 接口, 通常需要在协商或者初始化 SPID 之后才能发起呼叫。如果当设备与采用 NI 协议但不支持 SPID 协商的程控交换机互通时, 就采用此命令将其 SPID 处理设置为 NIT (Not Initial Terminal, 非初始化终端) 模式, 从而使设备和程控交换机忽略 SPID 协商和初始化的过程。

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入 ISDN BRI 接口视图。

```
interface bri interface-number
```

- (3) 将 SPID 处理设置为 NIT 模式。

```
isdn spid nit
```

缺省情况下，BRI 接口不采用 NIT 模式，使用动态协商 SPID 方式。

1.7 配置ISDN Q.931协议的协商参数

- (1) 进入系统视图。

```
system-view
```

- (2) 进入 ISDN BRI 接口或者 ISDN PRI 接口视图。

```
interface interface-type interface-number
```

- (3) 配置 ISDN 接口发起呼叫时所使用呼叫参考的长度。

```
isdn crlength call-reference-length
```

缺省情况下，CE1 PRI 接口和 CT1 PRI 接口的呼叫参考的长度为 2 字节，BRI 接口的呼叫参考的长度为 1 字节。

- (4) 配置 ISDN 协议对 CONNECT ACK 消息的处理。

```
isdn ignore connect-ack [ incoming | outgoing ]
```

缺省情况下，当设备和程控交换机互通时：

- ISDN 协议在发送了 CONNECT 消息之后，需要等待接收到程控交换机的 CONNECT ACK 消息后才切换到 ACTIVE 状态，并开始数据和语音业务的通信。
- ISDN 协议在收到 CONNECT 消息之后，需要向对端回应 CONNECT ACK 消息，并切换到 ACTIVE 状态。

- (5) 配置在发起 ISDN 语音呼叫时 Setup 消息中不携带的兼容性信息单元。

- 配置在发起 ISDN 语音呼叫时 Setup 消息中不携带高层兼容性信息单元。

```
isdn ignore hlc
```

缺省情况下，当 ISDN 协议为 5ESS、QSIG 时都不携带高层兼容性信息单元，在其它 ISDN 协议下都携带高层兼容性信息单元。

- 配置在发起 ISDN 语音呼叫时 Setup 消息中不携带低层兼容性信息单元。

```
isdn ignore llc
```

缺省情况下，当 ISDN 协议为 5ESS、QSIG 时都不携带低层兼容性信息单元，在其它 ISDN 协议下都携带低层兼容性信息单元。

- (6) 配置 ISDN 协议在入呼叫和出呼叫方向上对发送完全信息单元（Sending Complete Information Element）的处理。

```
isdn ignore sending-complete [ incoming | outgoing ]
```

缺省情况下，当设备和程控交换机互通时，对于入呼叫，检查接收到的 Setup 消息是否携带发送完全信息单元，对于出呼叫，发送 Setup 消息时携带发送完全信息单元。

- (7) 配置 ISDN 协议三层定时器的时长。

```
isdn l3-timer timer-name time-interval
```

缺省情况下，不同类型 ISDN 协议的三层定时器的时长不同，用户可以通过 **display isdn parameters** 命令查看各 ISDN 协议的三层定时器时长的缺省值。

- (8) 配置 ISDN 入呼叫和出呼叫时的主叫号码或被叫号码的号码类型和编码方案。

```
isdn number-property number-property [ calling | called ] [ in | out ]
```

缺省情况下，根据上层具体业务的不同，系统采用相应的号码类型和编码方案。

- (9) 配置 ISDN 接口被叫号码的发送方式为重叠发送。

```
isdn overlap-sending [ digits ]
```

缺省情况下，ISDN 接口被叫号码的发送方式为整体发送。

- (10) 配置 ISDN 协议在出方向报文中携带的参数。

- 配置 ISDN 协议在出方向报文中携带 calling-name 字段。

```
isdn carry calling-name
```

缺省情况下，ISDN 协议在出方向报文中不携带 calling-name 字段。

- 配置 ISDN 协议在出方向报文中携带 connected-name 字段。

```
isdn carry connected-name
```

缺省情况下，ISDN 协议在出方向报文中不携带 connected-name 字段。

- (11) 配置 ISDN 接口上把接收到的 Progress 消息转义成 Alerting 消息。

```
isdn progress-to-alerting enable
```

缺省情况下，Progress 消息转义成 Alerting 消息的功能处于关闭状态。

- (12) 配置 ISDN 信令中的 Progress indicator 值。

```
isdn progress-indicator indicator
```

缺省情况下，ISDN 信令使用上层语音业务指示的 Progress indicator 值。

1.8 配置ISDN Q.931协议的呼叫管理参数

1.8.1 配置本地管理ISDN B通道

1. 功能简介

本地管理 ISDN B 通道有两种模式：

- 设备工作在本地管理 B 通道的模式时，由本地自主选择空闲的 B 通道。但即使设置了本地管理 B 通道，程控交换机仍然享有优先权。如果程控交换机选定了一条与本地指定不同的空闲 B 通道，设备还是会按照程控交换机的指示完成通信。
- 设备工作在强制本地管理 B 通道的模式时，在出呼叫 Setup 消息的 Channel ID 信息单元中会指示 B 通道为“必选，不可更改”，由本地来分配一条空闲的 B 通道，如果程控交换机指示的 B 通道与之前本地的要求不一致时，将会导致呼叫失败。

在呼叫过程中，对呼叫所用 B 通道进行适当的管理是很重要的，尤其是在 PRI 方式下，适当的通道管理可以提高呼叫效率，减小呼叫损耗。一般来说，由程控交换机统一对 B 通道进行管理是比较合适的方式，所以虽然设备提供了 B 通道本地管理功能，但建议还是以程控交换机为主。

isdn bch-local-manage exclusive 表示强制本地管理 B 通道模式，这种模式适用于设备作为网络侧的情况。设备连接程控交换机时，是作为用户侧，此时如果程控交换机指示的 B 通道与本地的要求不一致时，会导致呼叫失败。

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入 ISDN BRI 接口或者 ISDN PRI 接口视图。

```
interface interface-type interface-number
```

- (3) 配置本地管理 ISDN B 通道。

```
isdn bch-local-manage [ exclusive ]
```

缺省情况下，未配置本地管理 ISDN B 通道，由程控交换机负责 B 通道的管理。

- (4) 配置 ISDN B 通道的选择方式。

```
isdn bch-select-way { ascending | descending }
```

缺省情况下，在本地管理 ISDN B 通道的情况下，按照升序方式选择 ISDN B 通道；在程控交换机管理 ISDN B 通道的情况下，本命令不起作用。

1.8.2 配置允许呼入的主叫号码

1. 功能简介

可以通过本配置来限制允许呼入的主叫号码，如果收到的呼叫建立消息中未携带主叫号码或者携带的主叫号码和本命令配置的不一样，都将导致呼叫失败。

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入 ISDN BRI 接口或者 ISDN PRI 接口视图。

```
interface interface-type interface-number
```

- (3) 配置允许呼入的主叫号码。

```
isdn caller-number caller-number
```

缺省情况下，不对呼入的主叫号码进行检查。

1.8.3 配置入呼叫时需要检查的被叫号码及子地址

1. 功能简介

本命令用于设置入呼叫时的检查项。可以只配置被叫号码，也可以同时配置被叫号码和子地址。

只要设定了被叫号码或者子地址，当对方未发送或发送错被叫号码或者子地址时，设备就会拒绝该呼叫。

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入 ISDN BRI 接口或者 ISDN PRI 接口视图。

```
interface interface-type interface-number
```

- (3) 配置入呼叫时需要检查的被叫号码或子地址。

```
isdn check-called-number check-index called-party-number
```

缺省情况下，入呼叫时不对被叫号码或子地址进行检查。

1.8.4 配置在出呼叫中携带主叫号码

1. 功能简介

主叫方配置该功能把主叫号码发送给被叫方后，被叫方通过查看 **display isdn call-info** 命令就可以看到主叫方号码。如果被叫方配置了允许呼入的主叫号码，则被叫方会对主叫方发送过来的主叫号码进行检查。

配置本功能后，如果电话网络中的程控交换机可以携带主叫号码，那么主叫号码可以发送给被叫方，如果电话网络中的程控交换机不能携带主叫号码，那么主叫号码也不能发送给被叫方。

2. 配置限制和指导

对于语音业务，不建议通过本命令配置出呼叫中携带的主叫号码。

3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入 ISDN BRI 接口或者 ISDN PRI 接口视图。

```
interface interface-type interface-number
```

- (3) 配置在出呼叫中携带主叫号码。

```
isdn calling calling-number
```

缺省情况下，语音业务的出呼叫中携带主叫号码，其它业务的出呼叫中不携带主叫号码。

1.9 配置ISDN Q.921协议的运行参数

1.9.1 配置ISDN BRI接口的工作模式

1. 功能简介

ISDN BRI 接口有两种工作模式：点到点、点到多点。工作在点到点模式下的 BRI 接口只能连接一台终端设备，工作在点到多点的 BRI 接口可以连接多台终端设备。

某些程控交换机只能工作在点到点模式下，为了互通，需要配置 BRI 接口工作在点到点模式下。当一个 BRI 接口通过程控交换机连接多台 ISDN 电话时，需要配置 BRI 接口工作在点到多点模式下。

2. 配置限制和指导

当 BRI 接口配置了 **isdn two-tei** 时，不能配置 BRI 接口工作在点到点模式。

当 BRI 接口上存在呼叫时，不能配置本功能。

3. 配置步骤

- (1) 进入系统视图。
system-view
- (2) 进入 ISDN BRI 接口视图。
interface bri interface-number
- (3) 配置 BRI 接口工作模式。
 - 配置 BRI 接口工作在点到点模式下。
isdn link-mode p2p
 - 配置 BRI 接口工作在点到多点模式下。
undo isdn link-mode缺省情况下, BRI 接口工作在点到多点模式下。

1.9.2 配置ISDN BRI接口的TEI值处理方式

1. 功能简介

一个 TEI (Terminal Endpoint Identifier, 终端设备标识符) 标识一个终端 (比如 ISDN 电话), 一个用户侧设备就是一个终端。TEI 由网络侧设备分配。

在设备的 ISDN BRI 接口与部分程控交换机 (如北美的采用 NI 协议的程控交换机 DMS100) 进行互通的时候, 程控交换机要求不同的 B 通道采用不同的 TEI 值呼叫, 否则 MP 呼叫无法成功 (现象为只能呼起一个 B 通道), 这时就需要通过配置使每一个 B 通道呼叫之前向程控交换机申请一个新的 TEI 值。

2. 配置限制和指导

当 ISDN BRI 接口上存在呼叫时, 不能配置本功能。

当 ISDN BRI 接口工作在点到点模式下时, 不能配置本功能。

3. 配置步骤

- (1) 进入系统视图。
system-view
 - (2) 进入 ISDN BRI 接口视图。
interface bri interface-number
 - (3) 配置 BRI 接口的每一个 B 通道呼叫之前向交换机申请一个新的 TEI 值。
isdn two-tei
- 缺省情况下, BRI 接口所有 B 通道的呼叫都使用同一个 TEI 值。

1.9.3 配置ISDN BRI专线

1. 功能简介

用户可以将一个 BRI 接口最多划分为两条 64kbps 的 ISDN 专线, 也可配置成一条 128kbps 的 ISDN 专线。

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入 ISDN BRI 接口视图。

```
interface bri interface-number
```

- (3) 配置用于 ISDN 专线。

```
isdn leased-line [ B1 | B2 | 128 ]
```

缺省情况下，未配置 ISDN 专线连接。

1.9.4 配置ISDN BRI接口的Q.921 常建链功能

1. 功能简介

对于 PRI 接口，Q.921 层处于常建链状态，即用户侧和网络侧正确相连后，在不需任何呼叫触发 Q.921 层协商的情况下就进入多帧建立状态。对于 BRI 接口来说，Q.921 层不会主动进入多帧建立状态，当有呼叫触发时，才会进入该状态。BRI 接口的 Q.921 进入多帧建立状态后，如果在指定时间（T325 定时器）内一直没有第三层呼叫，便会拆掉 Q.921 的链路。

当在 BRI 接口下配置 **isdn q921-permanent** 命令后，该 BRI 接口会自动建立链路层连接并一直维持，不论其是否承载网络层呼叫。若 BRI 接口配置了 **isdn two-tei** 命令，Q.921 常建链功能会自动建立两条链路层连接并一直维持。

当使用 ISDN NI 协议，呼叫不能一次建立成功，这是由于 Q.921 未处于常建链状态造成的，使用 ISDN NI 协议时，若要呼叫一次成功，需要配置 ISDN BRI 接口 Q.921 常建链功能。

2. 配置限制和指导

当 BRI 接口工作在网络侧模式时，不能配置本功能。

3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入 ISDN BRI 接口视图。

```
interface bri interface-number
```

- (3) 使能 BRI 接口的 Q.921 常建链功能。

```
isdn q921-permanent
```

缺省情况下，BRI 接口的 Q.921 常建链功能处于关闭状态。

1.9.5 配置ISDN BRI接口的物理层常激活功能

1. 功能简介

对于 BRI 接口的网络侧，链路层拆链后会启动 T325 定时器，T325 定时器超时后链路层向物理层发送去激活请求，使物理层切换到去激活模式，这样可以使设备减少功耗。如果用户希望物理层一直处于激活状态（即使链路层无链路），则可以使能物理层常激活功能，这样链路层就不会向物理层发送去激活请求。

物理层常激活功能只能供工作在网络侧模式下的 BRI 接口使用，目前只有语音 BSV 板卡上的 BRI 接口可以工作在网络侧模式。当 BRI 接口工作在用户侧模式时，不能配置本功能。

使用物理层常激活功能时注意和 Q.921 常建链功能的区别。Q.921 常建链功能的作用是使 Q.921 处于常建链状态（只能在用户侧使用），如果 Q.921 未建链时使能该功能则 Q.921 会试图进行链路层建链操作；而物理层常激活功能的作用是维持物理层的激活状态（只能在网络侧使用），物理层处于去激活时使能该功能并不会触发物理层激活。

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入 ISDN BRI 接口视图。

```
interface bri interface-number
```

- (3) 使能 BRI 接口的物理层常激活功能。

```
permanent-active
```

缺省情况下，BRI 接口的物理层常激活功能处于关闭状态。

1.9.6 配置ISDN BRI接口的远程供电功能

1. 功能简介

当 BRI 接口工作在网络侧模式时可以提供远程供电功能，比如工作在网络侧模式下的 BSV 接口和 ISDN 数字电话相连时，BSV 接口可以为数字电话供电。

2. 配置限制和指导

当 BRI 接口工作在用户侧模式时，不能配置本功能。

当 BRI 接口上存在呼叫时，不能配置本功能。

3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入 ISDN BRI 接口视图。

```
interface bri interface-number
```

- (3) 使能 BRI 接口的远程供电功能。

```
power-source
```

缺省情况下，BRI 接口的远程供电功能处于关闭状态。

1.9.7 配置ISDN BRI接口的滑动窗口的大小

1. 功能简介

Q.921 缓冲区中的帧是按序号发送的，每个发送出去的帧都要被接收端确认。系统在发送时会连续发送几帧，但在发送时会判断未确认帧的个数，如果 $V(A) + K = V(S)$ ，则不再进行发送。其中， $V(A)$ 是已确认帧的序号， $V(S)$ 是下次要发送帧的序号， K 是滑动窗口大小。

滑动窗机制使得系统在发送帧时不必等待上一帧的确认，提高了发送效率。滑动窗口的大小决定了未确认帧的最大个数。

2. 配置步骤

- (1) 进入系统视图。
system-view
- (2) 进入 ISDN BRI 接口视图。
interface bri *interface-number*
- (3) 配置 ISDN BRI 接口的滑动窗口的大小。
isdn bri-slipwnd-size *window-size*
缺省情况下，ISDN BRI 接口的滑动窗口大小为 1。

1.9.8 配置ISDN PRI接口的滑动窗口的大小

1. 功能简介

Q.921 缓冲区中的帧是按序号发送的，每个发送出去的帧都要被接收端确认。系统在发送时会连续发送几帧，但在发送时会判断未确认帧的个数，如果 $V(A) + K = V(S)$ ，则不再进行发送。其中， $V(A)$ 是已确认帧的序号， $V(S)$ 是下次要发送帧的序号， K 是滑动窗口大小。

滑动窗机制使得系统在发送帧时不必等待上一帧的确认，提高了发送效率。滑动窗口的大小决定了未确认帧的最大个数。

2. 配置步骤

- (1) 进入系统视图。
system-view
- (2) 进入 ISDN PRI 接口视图。
interface *interface-type* *interface-number*
- (3) 配置 ISDN PRI 接口的滑动窗口的大小。
isdn pri-slipwnd-size *window-size*
缺省情况下，ISDN PRI 接口的滑动窗口大小为 7。

1.10 ISDN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 ISDN 的运行情况，通过查看显示信息验证配置的效果。

表1-2 ISDN 显示和维护

操作	命令
显示ISDN接口上Q.931呼叫成功的呼叫信息	display isdn active-channel [interface <i>interface-type</i> <i>interface-number</i>]
显示ISDN接口的呼叫信息	display isdn call-info [interface <i>interface-type</i> <i>interface-number</i>]
显示ISDN的呼叫历史记录	display isdn call-record [interface <i>interface-type</i> <i>interface-number</i>]
显示ISDN协议二层和三层系统参数	display isdn parameters { <i>protocol</i> interface <i>interface-type</i> <i>interface-number</i> }

操作	命令
显示采用NI协议的BRI接口上SPID的相关信息	<code>display isdn spid [interface interface-type interface-number]</code>

1.11 ISDN典型配置举例

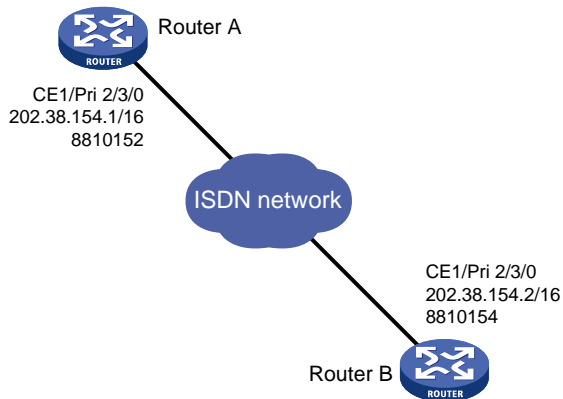
1.11.1 设备通过ISDN PRI线路互连传输数据

1. 组网需求

Router A 与 Router B 连接，通过 ISDN PRI 线路互连传输数据。

2. 组网图

图1-4 配置设备通过 ISDN PRI 线路互连传输数据组网图



3. 配置步骤



说明

在本组网中，Router A 和 Router B 上的 ISDN PRI 接口都工作在用户侧模式（缺省协议模式），ISDN 网络中与 Router A 和 Router B 相连的设备上的接口需要工作在网络侧模式。

(1) 配置 Router A

创建 ISDN PRI 接口，即将 CE1/PRI 接口的时隙捆绑为 pri-set。

```
<RouterA> system-view
[RouterA] controller e1 2/3/0
[RouterA-E1 2/3/0] pri-set
[RouterA-E1 2/3/0] quit
```

配置拨号访问组 1 以及对应的拨号访问控制条件。

```
[RouterA] dialer-group 1 rule ip permit
```

配置 ISDN PRI 接口的 IP 地址，启动轮询 DDR，配置到达 Router B 的拨号串，将拨号访问组 1 与 ISDN PRI 接口关联。

```
[RouterA] interface serial 2/3/0:15
```

```
[RouterA-Serial2/3/0:15] ip address 202.38.154.1 255.255.0.0
[RouterA-Serial2/3/0:15] dialer circular enable
[RouterA-Serial2/3/0:15] dialer route ip 202.38.154.2 8810154
[RouterA-Serial2/3/0:15] dialer-group 1
```

(2) 配置 Router B

创建 ISDN PRI 接口，即将 CE1/PRI 接口的时隙捆绑为 pri-set。

```
<RouterB> system-view
[RouterB] controller e1 2/3/0
[RouterB-E1 2/3/0] pri-set
[RouterB-E1 2/3/0] quit
```

配置拨号访问组 1 以及对应的拨号访问控制条件。

```
[RouterB] dialer-group 1 rule ip permit
```

配置 ISDN PRI 接口的 IP 地址，启动轮询 DDR，配置到达 Router A 的拨号串，将拨号访问组 1 与 ISDN PRI 接口关联。

```
[RouterB] interface serial 2/3/0:15
[RouterB-Serial2/3/0:15] ip address 202.38.154.2 255.255.0.0
[RouterB-Serial2/3/0:15] dialer circular enable
[RouterB-Serial2/3/0:15] dialer route ip 202.38.154.1 8810152
[RouterB-Serial2/3/0:15] dialer-group 1
```

4. 验证配置

在 Router A 上 ping 202.38.154.2 触发拨号，通过日志信息可以看到 E1 2/3/0 的某个 B 通道 Line up，随后 ping 202.38.154.2 可以 ping 通，且没有报文丢失。

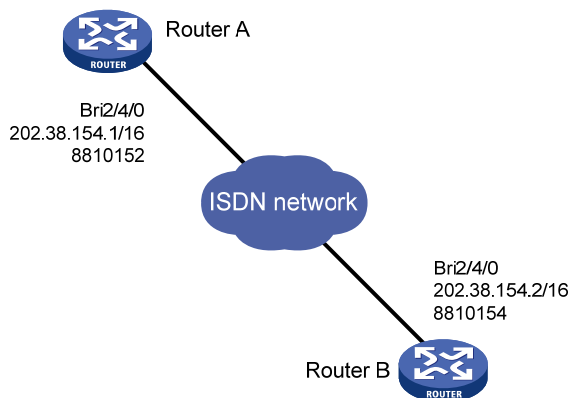
1.11.2 设备通过 ISDN BRI 线路的 NI 协议互连传输数据

1. 组网需求

Router A 与 Router B 连接，通过 ISDN BRI 线路的 NI 协议互连传输数据。

2. 组网图

图1-5 配置设备通过 ISDN BRI 线路互连传输数据组网图



3. 配置步骤



说明

在本组网中，Router A 和 Router B 上的 ISDN BRI 接口都工作在用户侧模式（缺省协议模式），ISDN 网络中与 Router A 和 Router B 相连的设备上的接口需要工作在网络侧模式。

(1) 配置 Router A

配置拨号访问组 1 以及对应的拨号访问控制条件。

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

```
[RouterA] dialer-group 1 rule ip permit
```

配置 ISDN BRI 接口的 IP 地址，启动轮询 DDR，配置到达 Router B 的拨号串，将拨号访问组 1 与 ISDN BRI 接口关联。

```
[RouterA] interface bri 2/4/0
```

```
[RouterA-Bri2/4/0] ip address 202.38.154.1 255.255.0.0
```

```
[RouterA-Bri2/4/0] dialer circular enable
```

```
[RouterA-Bri2/4/0] dialer route ip 202.38.154.2 8810154
```

```
[RouterA-Bri2/4/0] dialer-group 1
```

配置 ISDN NI 协议参数，使 BRI 接口 B 通道支持静态配置的 SPID 值，并且当协商消息没有响应时重传 2 次。

```
[RouterA-Bri2/4/0] isdn protocol-type ni
```

```
[RouterA-Bri2/4/0] isdn spid1 54321
```

```
[RouterA-Bri2/4/0] isdn spid2 65432
```

```
[RouterA-Bri2/4/0] isdn spid resend 2
```

(2) 配置 Router B

配置拨号访问组 1 以及对应的拨号访问控制条件。

```
<RouterB> system-view
```

```
[RouterB] dialer-group 1 rule ip permit
```

配置 ISDN BRI 接口的 IP 地址，启动轮询 DDR，配置到达 Router A 的拨号串，将拨号访问组 1 与 ISDN BRI 接口关联。

```
[RouterB] interface bri 2/4/0
```

```
[RouterB-Bri2/4/0] ip address 202.38.154.2 255.255.0.0
```

```
[RouterB-Bri2/4/0] dialer circular enable
```

```
[RouterB-Bri2/4/0] dialer route ip 202.38.154.1 8810152
```

```
[RouterB-Bri2/4/0] dialer-group 1
```

配置 ISDN NI 协议参数，使 BRI 接口 B 通道支持静态配置的 SPID 值，并且当协商消息没有响应时重传 2 次。

```
[RouterB-Bri2/4/0] isdn protocol-type ni
```

```
[RouterB-Bri2/4/0] isdn spid1 12345
```

```
[RouterB-Bri2/4/0] isdn spid2 23456
```

```
[RouterB-Bri2/4/0] isdn spid resend 2
```

4. 验证配置

在 Router A 上 ping 202.38.154.2 触发拨号，通过日志信息可以看到 Bri2/4/0 的某个 B 通道 Line up，随后 ping 202.38.154.2 可以 ping 通，且没有报文丢失。

1.12 ISDN常见故障的诊断与排除

1.12.1 通过ISDN PRI或BRI线路相连的两台设备之间无法ping通

1. 故障现象

两台设备通过 ISDN PRI 或 BRI 线路相连，它们之间无法 ping 通。

2. 故障分析

两台设备无法 ping 通，可能有以下原因：

- 相应的接口没有配置或者没有激活
- 拨号配置错误
- 线缆没有接好

3. 故障排除

- 使用命令 **display isdn call-info**，如果系统没有任何显示，则说明没有 ISDN PRI 接口，应该配置相应的接口，具体配置方法请参见“接口管理配置指导”中“WAN 接口”中的 CE1/PRI 接口和 CT1/PRI 接口配置部分。在 PRI 接口下，ISDN 状态如果不是处于多帧操作状态或者在 BRI 接口下 ISDN 状态不是处于 TEI 已分配的状态（TEI_ASSIGNED），则说明 Q.921 层协商不成功，可能是物理上没有连接好。
- 如果 Q.921 调试信息开关已经打开，并且在 PRI 下 ISDN 状态是多帧建立而 BRI 是 TEI 已分配，则检查拨号配置是否有错。如果系统输出“Failed to send”调试信息，说明物理层没有激活。可以尝试使用 **shutdown** 和 **undo shutdown** 命令关闭和重新打开相关接口。
- 检查拨号配置是否正确。如果拨号配置正确并且系统没有输出“Failed to send”调试信息，则有可能是 ISDN 线缆没有接好。

目 录

1 ATM.....	1-1
1.1 ATM简介.....	1-1
1.1.1 ATM信元.....	1-1
1.1.2 ATM连接和ATM交换.....	1-1
1.1.3 ATM层次结构.....	1-2
1.1.4 ATM服务类型.....	1-3
1.1.5 ATM应用.....	1-3
1.1.6 ATM OAM.....	1-4
1.2 ATM配置限制和指导.....	1-4
1.3 ATM配置任务简介.....	1-4
1.4 配置PVC.....	1-5
1.5 配置PVC-group.....	1-5
1.6 配置ATM AAL5 封装类型.....	1-6
1.7 配置ATM的服务类型.....	1-7
1.8 配置ATM上承载的应用.....	1-8
1.8.1 配置IPoA.....	1-8
1.8.2 配置IPoEoA.....	1-10
1.8.3 配置PPPoA.....	1-12
1.8.4 配置PPPoEoA.....	1-13
1.9 配置VP监管.....	1-16
1.10 配置重新标记ATM信元的CLP标志位.....	1-16
1.11 配置ATM OAM功能.....	1-17
1.11.1 开启ATM OAM功能.....	1-17
1.11.2 检测链路连接情况.....	1-18
1.12 ATM显示和维护.....	1-18
1.13 ATM典型配置举例.....	1-19
1.13.1 IPoA典型配置举例.....	1-19
1.13.2 IPoEoA典型配置举例.....	1-20
1.13.3 PPPoA典型配置举例.....	1-22
1.13.4 PPPoEoA典型配置举例.....	1-23
1.13.5 ATM PVC传输优先级典型配置举例.....	1-25
1.14 ATM常见故障处理.....	1-26
1.14.1 采用IPoA时，链路状态为down.....	1-26

1.14.2 采用PPPoA时，链路不上报up	1-26
1.14.3 ping不通对方.....	1-26
1.14.4 ATM接口状态为up，但PVC状态为down	1-27
1.14.5 配置PPPoA等应用之后，无法ping通对端	1-27

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。

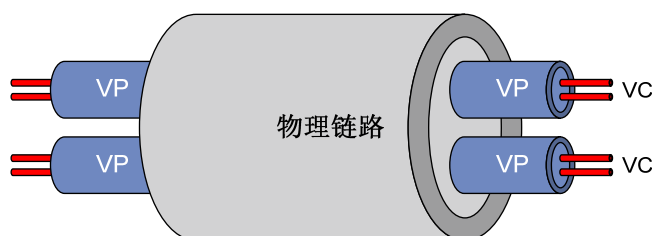
1.1.1 ATM信元

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。

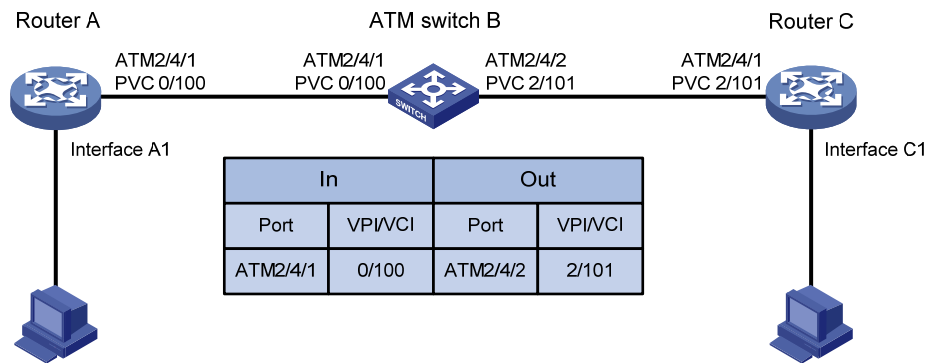
图1-1 VP、VC 和物理链路关系



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



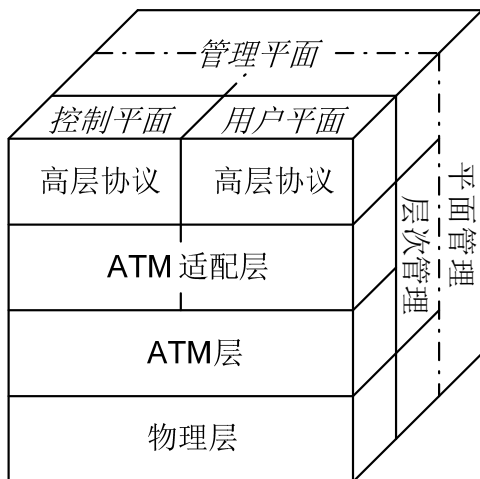
1.1.3 ATM层次结构

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、承载多种协议（IP 协议、IPoE 协议、PPP 协议、PPPoE 协议）等功能。

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

1. IPoA

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。

2. IPoEoA

IPoEoA (IP over Ethernet over ATM, 在 ATM 上承载 IPoE 协议) 有三层结构: 最上层封装 IP 协议; 中间为 IPoE, 即以太网承载 IP 协议; 最下一层为 ATM 承载 IPoE。这就要求在 ATM 接口承载以太网报文, 这就是 IPoEoA。

3. PPPoA

PPPoA (PPP over ATM, 在 ATM 上承载 PPP 协议): ATM 信元封装 PPP 报文, IP 或其它协议的报文则封装在 PPP 报文中。在这种情况下, 可以将 ATM 简单地看成是 PPP 报文的承载层。PPPoA 的意义在于: PPPoA 的通讯过程由 PPP 协议管理, 可以利用 PPP 的灵活性及其丰富的应用。

4. PPPoEoA

PPPoEoA (PPPoE over ATM, 在 ATM 上承载 PPPoE 协议): 其实质是用 ATM 信元封装以太网报文, 这时候可以用一个 PVC 来模拟以太网的全部功能。PPPoE 协议采用 Client/Server 方式, 它将 PPP 报文封装在以太网帧之内, 在以太网上提供点对点的连接。

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 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 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

本特性仅在路由器上安装了 ATM-OC3、ADSL2+、G.shdsl、或 G.shdsl.Bis 接口模块时支持。

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 或者配置 PVC-group
 - [配置PVC](#)
 - [配置PVC-group](#)
- (3) [配置ATM AAL5 封装类型](#)
- (4) [配置ATM的服务类型](#)
- (5) 配置 ATM 上承载的应用
 - [配置IPoA](#)
 - [配置IPoEoA](#)
 - [配置PPPoA](#)
 - [配置PPPoEoA](#)
- (6) (可选) [配置VP监管](#)
- (7) (可选) [配置重新标记ATM信元的CLP标志位](#)
- (8) (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PVC-group

1. 功能简介

使用 PVC-group 后，可以在 PVC-group 下的各 PVC 上进行流量的负载分担，将不同优先级的 IP 报文通过不同的 PVC 进行传输。用户可以配置每条 PVC 承载的 IP 报文的优先级。

当收到 IP 报文后，根据 IP 报文的优先级来找到对应的 PVC 进行传输，如果没有找到对应的 PVC，则从缺省 PVC (`precedence` 命令中使用了 `default` 参数) 进行传输，如果没有配置缺省 PVC，

则从未设置优先级的所有 PVC 轮询地进行传输。如果没有未设置优先级的 PVC，则将该 IP 报文丢弃。

如果收到的不是 IP 报文，则从该 PVC-group 下所有 PVC 轮询地进行传输。

PVC-group 下的 PVC 的封装类型、承载的协议类型直接从 PVC-group 获取。

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-group 并进入 PVC-group 视图。

```
pvc-group group-number
```

(4) 在 PVC-group 下创建 PVC 并进入 PVC 视图。

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

(5) 配置 PVC 承载的 IP 报文的优先级。

```
precedence { min-number [ to max-number ] | default }
```

缺省情况下，未设置优先级。

(6) 开启当前 PVC。

```
undo shutdown
```

缺省情况下，PVC 处于打开状态。

1.6 配置 ATM AAL5 封装类型

1. 功能简介

ATM AAL5 封装主要有如下几种类型：

- **aal5snap**: LLC (Logical Link Control, 逻辑链路控制) / SNAP (Subnet Access Protocol, 子网访问协议) 封装类型。
- **aal5mux**: MUX 复用封装类型。
- **aal5nlpid**: RFC 1490 封装类型。

如 [表 1-1](#) 所示，不同的封装类型对报文的封装格式各不相同，而且支持的映射也不同。

表 1-1 封装类型和支持的应用的关系

应用	aal5snap	aal5mux	aal5nlpid
IPoA	支持	支持 (不支持 InARPoA)	支持 (不支持 InARPoA)
IPoEoA	支持	支持	不支持
PPPoA	支持	支持	不支持
PPPoEoA	支持	支持	不支持



说明

aal5snap 可以支持同时承载两种以上协议，**aal5mux** 只支持同时承载一种协议。

2. 配置限制和指导

- 相互通信的两端设备上配置的 ATM AAL5 封装类型要保持一致。
- 只有 **aal5snap** 封装支持 InARP 协议，当采用 **aal5mux** 和 **aal5nlpid** 封装时不能配置 InARP。
- 在 PVC/PVC-group 切换封装时，如果已经配置了与切换后封装类型冲突的映射，切换封装后的 PVC/PVC-group 将会删除所有冲突的映射对应的配置。

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 视图或 PVC-group 视图。

- 进入 PVC 视图。

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

- 进入 PVC-group 视图。

```
pvc-group group-number
```

- (4) 配置 ATM AAL5 封装类型。

```
encapsulation { aal5mux | aal5nlpid | aal5snap }
```

缺省情况下，ATM AAL5 封装类型为 **aal5snap**。

1.7 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，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。

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 视图或 PVC-group 下 PVC 视图。

- 进入 PVC 视图。

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

- 请依次执行以下命令进入 PVC-group 下 PVC 视图。

```
pvc-group group-number
```

```
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，同一个接口下或同一个 PVC-group 下的不同 PVC 可以配置不同的服务类型。

- (5) 配置 PVC 的传输优先级。

```
transmit-priority priority
```

缺省情况下，UBR 服务的传输优先级为 0，VBR-NRT 服务的传输优先级为 5，VBR-RT 服务的传输优先级为 8。

当改变 PVC 的服务类型时，传输优先级变为当前服务的缺省值。

1.8 配置ATM上承载的应用

1.8.1 配置IPoA

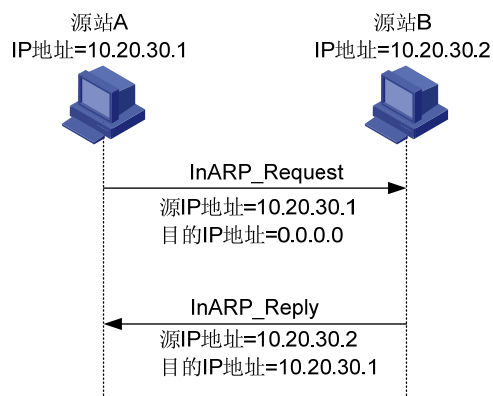
1. IP地址映射简介

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 或 PVC-group 与对端设备的 IP 地址关联起来，即配置 PVC 或 PVC-group 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 或 PVC-group 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 或 PVC-group 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 或 PVC-group 配置了 default 映射，则报文将从该 PVC 或 PVC-group 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 或 PVC-group 相连的对端接口的 IP 地址，这样不需要为 PVC 或 PVC-group 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 或 PVC-group 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

- 所有的封装类型都支持 IPoA 映射。但只有 **aa15snap** 封装支持配置 InARP 映射，当采用 **aa15mux** 和 **aa15nlpid** 封装时不能配置 InARP 映射。
- 相同 PVC 或 PVC-group 下可以映射多个 IP 地址，且静态 IP 地址映射、default 映射和 InARP 映射三者可以同时配置。相同接口下不同的 PVC 或 PVC-group 不能映射到同一个 IP 地址。同一个接口下的 PVC 和 PVC-group 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 视图或 PVC-group 视图。

- 进入 PVC 视图。

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

- 进入 PVC-group 视图。

```
pvc-group group-number
```

- (4) 配置 IPoA 映射，使 PVC 或 PVC-group 承载 IP 协议报文。

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

- (5) 为 PVC 或 PVC-group 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 或 PVC-group 上发送广播或者组播报文，请务必配置本命令。

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

1.8.2 配置IPoEoA

1. VEth和VEth子接口介绍

在 IPoEoA 应用中使用三层 VEth（Virtual Ethernet，虚拟以太网）接口，一个 VEth 接口可以关联多个 PVC。在同一个 VEth 接口关联的 PVC 之间二层互通。

为了实现在 ATM 上承载以太网报文，在 PPPoEoA 应用中使用 broa 三层 VEth 接口。VEth 接口具有以太网的特性，由用户通过配置命令动态创建。VEth 接口的协议栈是：底层为 ATM 的 PVC，通过 PVC 收发报文；链路层为以太网协议；网络层及以上各层协议与普通以太网接口相同。

2. 配置限制和指导

配置 IPoEoA、PPPoEoA 应用时，必须指定一个 VEth 接口与之对应。如果对应的 VEth 接口没有创建，则不能配置对应的应用。

3. 配置VEth接口映射到PVC

- (1) 进入系统视图。

```
system-view
```

- (2) 创建 VEth 接口或 VEth 子接口，并进入一个 VEth 接口或 VEth 子接口视图。

```
interface virtual-ethernet { interface-number |  
interface-number.subnumber }
```

- (3) 配置接口的 IP 地址。

```
ip address ip-address { mask | mask-length }
```

在 IPoEoA 应用中，需要在 VEth 接口下配置 IP 地址，ATM 接口下配置的 IP 地址无效。

- (4) 退回系统视图。

```
quit
```

- (5) 进入 ATM 接口视图或 ATM 子接口视图。

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

- (6) 进入 PVC 视图或 PVC-group 视图。

- o 进入 PVC 视图。

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

- o 进入 PVC-group 视图。

```
pvc-group group-number
```

- (7) 配置 IPoEoA 映射。

```
map bridge virtual-ethernet { interface-number |  
interface-number.subnumber }
```

缺省情况下，没有配置任何映射。

本命令中的 *interface-number* 必须是已经创建的 VEth 接口或 VEth 子接口的编号。

4. 配置VEth接口

- (1) 进入系统视图。

```
system-view
```

- (2) 进入 VEth 接口视图。

interface virtual-ethernet *interface-number*

用户最多可以创建 1024 个 VEth 接口。

- (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：Virtual-Ethernet0 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 MAC 地址。

mac-address *mac-address*

缺省情况下，VEth 接口在创建时会使用设备的桥 MAC 地址作为自己的 MAC 地址。

- (6) (可选) 设置接口的期望带宽。

bandwidth *bandwidth-value*

缺省情况下，接口的期望带宽 = 接口的波特率 ÷ 1000 (kbit/s)。

期望带宽供业务模块使用，不会对接口实际带宽造成影响。

- (7) 开启当前接口。

undo shutdown

缺省情况下，接口处于打开状态。

5. 配置 VEth 子接口

- (1) 进入系统视图。

system-view

- (2) 进入 VEth 子接口视图。

interface virtual-ethernet *interface-number.subnumber*

- (3) (可选) 配置 VEth 子接口的描述信息。

description *text*

缺省情况下，VEth 子接口的描述信息为“该接口的接口名 Interface”。

- (4) (可选) 配置 VEth 子接口的 MTU 值。

mtu *size*

缺省情况下，VEth 子接口的 MTU 值为 1500 字节。

- (5) (可选) 设置 VEth 子接口的期望带宽。

bandwidth *bandwidth-value*

缺省情况下，VEth 子接口的期望带宽 = 接口的波特率 ÷ 1000 (kbit/s)。

期望带宽供业务模块使用，不会对接口实际带宽造成影响。

- (6) 开启当前接口。

undo shutdown

缺省情况下，接口处于打开状态。

6. 恢复VEth接口或VEth子接口的缺省配置



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。

- (1) 进入系统视图。

```
system-view
```

- (2) 进入 VEth 接口或 VEth 子接口视图。

```
interface virtual-ethernet { interface-number |  
interface-number.subnumber }
```

- (3) 恢复 VEth 接口或 VEth 子接口的缺省配置。

```
default
```

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。

1.8.3 配置PPPoA

1. 配置限制和指导

为了在 ATM 上传送 PPP 报文，用户必须创建一个虚拟模板（Virtual Template，VT）接口。

当设备采用 DSL 接口通过拨号方式互连时，路由器作 PPPoA Server 或 Client 使用均可，两侧配置的区别仅在于 PPPoA Server 端为 PPP Server，需要配置地址池，为对端分配 IP 地址；PPPoA Client 端为 PPP Client，需要配置地址协商，接受 Server 端分配的 IP 地址，相关内容请参见“二层技术-广域网接入配置指导”中的“PPP 和 MP”。

对于 VT 接口，如果配置静态路由，请指定下一跳而不要指定出接口。如果必须指定出接口的话，请保证 VT 下绑定的物理接口有效，从而保证报文能够正常传输。

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 创建一个虚拟模板（VT）接口，并进入虚拟模板（VT）接口视图。

```
interface virtual-template vt-number
```

- (3) 配置 PPP 的认证方式、IP 地址。

- 如果是 PPP Server，需要配置地址池，为对端分配 IP 地址。
- 如果是 PPP Client，需要配置地址协商，接受 Server 端分配的 IP 地址。

详细配置请参见“二层技术-广域网接入配置指导”中的“PPP 和 MP”。

PPP 认证、IP 地址等均需要在 VT 接口下进行配置，ATM 接口下配置 IP 地址无效。

- (4) 退回系统视图。

```
quit
```

- (5) 进入 ATM 接口视图或 ATM 子接口视图。

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

- (6) 进入 PVC 视图或 PVC-group 视图。

- 进入 PVC 视图。

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

- 进入 PVC-group 视图。

```
pvc-group group-number
```

- (7) 配置 PPPoA 映射。

```
map ppp virtual-template vt-number
```

1.8.4 配置 PPPoEoA

1. VEth和VEth子接口介绍

在 IPoEoA 应用中使用三层 VEth（Virtual Ethernet，虚拟以太网）接口，一个 VEth 接口可以关联多个 PVC。在同一个 VEth 接口关联的 PVC 之间二层互通。

为了实现在 ATM 上承载以太网报文，在 PPPoEoA 应用中使用三层 VEth 接口。VEth 接口具有以太网的特性，由用户通过配置命令动态创建。VEth 接口的协议栈是：底层为 ATM 的 PVC，通过 PVC 收发报文；链路层为以太网协议；网络层及以上各层协议与普通以太网接口相同。

2. 配置限制和指导

配置 IPoEoA、PPPoEoA 应用时，必须指定一个 VEth 接口与之对应。如果对应的 VEth 接口没有创建，则不能配置对应的应用。

对于 VT 接口，如果配置静态路由，请指定下一跳而不要指定出接口。如果必须指定出接口的话，请保证 VT 下绑定的物理接口有效，从而保证报文能够正常传输。

3. 配置VEth接口映射到PVC

- (1) 进入系统视图。

```
system-view
```

- (2) 创建一个虚拟模板（VT）接口，并进入虚拟模板（VT）接口视图。

```
interface virtual-template vt-number
```

- (3) 配置 PPP 的认证方式、IP 地址。

- 如果是 PPP Server，需要配置地址池，为对端分配 IP 地址。
- 如果是 PPP Client，需要配置地址协商，接受 Server 端分配的 IP 地址。

详细配置请参见“二层技术-广域网接入配置指导”中的“PPP 和 MP”。

PPP 认证、IP 地址等均需要在 VT 接口下进行配置，ATM 接口下配置 IP 地址无效。

- (4) 退回系统视图。

```
quit
```

- (5) 创建 VEth 接口或 VEth 子接口，并进入一个 VEth 接口或 VEth 子接口视图。

```
interface virtual-ethernet { interface-number |  
interface-number.subnumber }
```

- (6) 在 VEth 接口下配置 PPPoE 的各项参数。

根据角色的不同进行不同的配置：PPPoE Server 端需要绑定 VT 接口，PPPoE Client 端需要绑定 Dialer 接口进行拨号。详细配置请参见“二层技术-广域网接入配置指导”中的“PPPoE”。

- (7) 退回系统视图。

quit

- (8) 进入 ATM 接口视图或 ATM 子接口视图。

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

- (9) 进入 PVC 视图或 PVC-group 视图。

- 进入 PVC 视图。

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

- 进入 PVC-group 视图。

pvc-group *group-number*

- (10) 配置 PPPoEoA 映射。

map bridge virtual-ethernet { *interface-number* | *interface-number.subnumber* }

缺省情况下，没有配置任何映射。

本命令中的 *interface-number* 必须是已经创建的 VEth 接口或 VEth 子接口的编号。

4. 配置 VEth 接口

- (1) 进入系统视图。

system-view

- (2) 进入 VEth 接口视图。

interface virtual-ethernet *interface-number*

用户最多可以创建 1024 个 VEth 接口。

- (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：Virtual-Ethernet0 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 MAC 地址。

mac-address *mac-address*

缺省情况下，VEth 接口在创建时会使用设备的桥 MAC 地址作为自己的 MAC 地址。

- (6) （可选）设置接口的期望带宽。

bandwidth *bandwidth-value*

缺省情况下，接口的期望带宽 = 接口的波特率 ÷ 1000 (kbit/s)。

期望带宽供业务模块使用，不会对接口实际带宽造成影响。

- (7) 开启当前接口。

undo shutdown

缺省情况下，接口处于打开状态。

5. 配置VEth子接口

- (1) 进入系统视图。

system-view

- (2) 进入 VEth 子接口视图。

interface virtual-ethernet *interface-number.subnumber*

- (3) （可选）配置 VEth 子接口的描述信息。

description *text*

缺省情况下，VEth 子接口的描述信息为“该接口的接口名 Interface”。

- (4) （可选）配置 VEth 子接口的 MTU 值。

mtu *size*

缺省情况下，VEth 子接口的 MTU 值为 1500 字节。

- (5) （可选）设置 VEth 子接口的期望带宽。

bandwidth *bandwidth-value*

缺省情况下，VEth 子接口的期望带宽=接口的波特率÷1000（kbit/s）。

期望带宽供业务模块使用，不会对接口实际带宽造成影响。

- (6) 开启当前接口。

undo shutdown

缺省情况下，VEth 子接口处于打开状态。

6. 恢复VEth接口或VEth子接口的缺省配置



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。

- (1) 进入系统视图。

system-view

- (2) 进入 VEth 接口或 VEth 子接口视图。

interface virtual-ethernet { *interface-number* |
interface-number.subnumber }

- (3) 恢复 VEth 接口或 VEth 子接口的缺省配置。

default

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。

1.9 配置VP监管

1. 功能简介

VP 是具有相同 VPI 的所有 PVC 的集合，VP 监管用来管理 VP 的最大带宽，对一个物理接口下的虚通道（VP）流量进行入方向、出方向的监管，即保证 VP 的最大传输速率不能超过设定值，超出的流量将被丢弃。在应用 VP 监管时，PVC 的参数仍然有效，只有满足 PVC 的参数与 VP 监管的参数时，分组才会被接收或发送。在计算流量时，已经包括了 LLC/SNAP、MUX 和 NLPID 封装头部，但不包括 ATM 信元头。

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入 ATM 接口视图。

```
interface atm interface-number
```

- (3) 配置 VP 监管的参数。

```
vp limit vpi scr
```

缺省情况下，不进行 VP 监管。

1.10 配置重新标记ATM信元的CLP标志位

1. 功能简介

用户可以通过重新标记 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”。

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 配置类。

- a. 定义类并进入类视图。

```
traffic classifier classifier-name [ operator { and | or } ]
```

- b. 定义匹配数据包的规则。

```
if-match [ not ] match-criteria
```

缺省情况下，没有定义匹配数据包的规则。

- c. 退回系统视图。

```
quit
```

- (3) 配置流行为。

- a. 定义一个流行为并进入流行为视图。

```
traffic behavior behavior-name
```

- b. 重新标记 ATM 信元的 CLP 标志位的值。

```
remark [ green | red | yellow ] atm-clp atm-clp-value
```

缺省情况下，没有配置重新标记 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。

- c. 退回系统视图。

quit

- (4) 配置 QoS 策略。

- a. 定义策略并进入策略视图。

qos policy *policy-name*

- b. 在策略中为类指定采用的流行为。

classifier *classifier-name* **behavior** *behavior-name* [**insert-before** *before-classifier-name*]

缺省情况下，没有为类指定流行为。

- c. 退回系统视图。

quit

- (5) 进入 ATM 接口视图或者 ATM 子接口视图。

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

- (6) 进入 PVC 视图或 PVC-group 下 PVC 视图。

- o. 进入 PVC 视图。

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

- o. 请依次执行以下命令进入 PVC-group 下 PVC 视图。

pvc-group *group-number*

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

- (7) 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。

1.11 配置 ATM OAM 功能

1.11.1 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 视图或 PVC-group 下 PVC 视图。

- o. 进入 PVC 视图。

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

- o. 请依次执行以下命令进入 PVC-group 下 PVC 视图。

pvc-group *group-number*

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) （可选）配置 AIS/RDI 告警信元检测的相关参数。

```
oam ais-rdi up up-seconds down down-seconds
```

缺省情况下，当系统连续 1 秒收到 AIS/RDI 告警信元后，PVC 状态转变为 DOWN，当连续 3 秒没有收到 AIS/RDI 告警信元后，PVC 状态转变为 UP。

1.11.2 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 ]
```

1.12 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1-2 ATM 显示和维护

操作	命令
显示PVC的信息	<pre>display atm pvc-info [interface interface-type { interface-number interface-number.subnumber } [pvc { pvc-name vpi/vci }]]</pre>
显示PVC-group的信息	<pre>display atm pvc-group [interface interface-type { interface-number interface-number.subnumber } [pvc-group group-number]]</pre>
显示PVC或PVC-group的映射信息	<pre>display atm map-info [interface interface-type { interface-number interface-number.subnumber } [pvc { pvc-name vpi/vci } pvc-group group-number]]</pre>
显示VEth接口的相关信息	<pre>display interface [virtual-ethernet [interface-number]] [brief [description down]]</pre>
清除PVC的统计信息	<pre>reset atm interface [interface-type { interface-number interface-number.subnumber }]</pre>
清除VEth接口的统计信息	<pre>reset counters interface [virtual-ethernet [interface-number interface-number.subnumber]]</pre>

1.13 ATM典型配置举例

1.13.1 IPoA典型配置举例

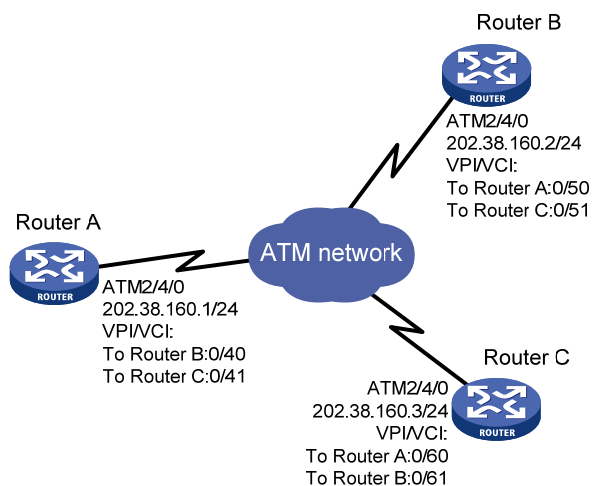
1. 组网需求

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 2/4/0
[RouterA-ATM2/4/0] ip address 202.38.160.1 255.255.255.0
```

创建 PVC，并指定承载 IP 协议。

```
[RouterA-ATM2/4/0] pvc to_b 0/40
[RouterA-ATM2/4/0-pvc-to_b-0/40] map ip 202.38.160.2
[RouterA-ATM2/4/0-pvc-to_b-0/40] quit
[RouterA-ATM2/4/0] pvc to_c 0/41
[RouterA-ATM2/4/0-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 2/4/0
```

```
[RouterB-ATM2/4/0] ip address 202.38.160.2 255.255.255.0
# 创建 PVC，并指定承载 IP 协议。
[RouterB-ATM2/4/0] pvc to_a 0/50
[RouterB-ATM2/4/0-pvc-to_a-0/50] map ip 202.38.160.1
[RouterB-ATM2/4/0-pvc-to_a-0/50] quit
[RouterB-ATM2/4/0] pvc to_c 0/51
[RouterB-ATM2/4/0-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 2/4/0
[RouterC-ATM2/4/0] ip address 202.38.160.3 255.255.255.0
# 创建 PVC，并指定承载 IP 协议。
[RouterC-ATM2/4/0] pvc to_a 0/60
[RouterC-ATM2/4/0-pvc-to_a-0/60] map ip 202.38.160.1
[RouterC-ATM2/4/0-pvc-to_a-0/60] quit
[RouterC-ATM2/4/0] pvc to_b 0/61
[RouterC-ATM2/4/0-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。

1.13.2 IPoEoA典型配置举例

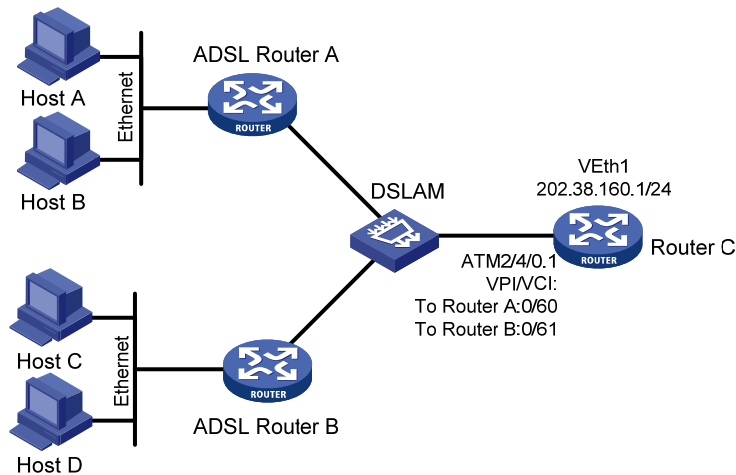
1. 组网需求

两个以太网中的多台主机各自通过一台 ADSL Router 接入 ATM 网络，并通过 DSLAM 与 Router C 通讯。要求：

- Router C 虚拟以太网接口的 IP 地址为 202.38.160.1；
- Router C 连接至 DSLAM 的两条 PVC 的 VPI/VCI 为 0/60、0/61，分别指向 Router A 和 Router B；
- Router C 广域网端口和 ADSL Router 的 DSL 接口均采用 IPoEoA 应用方式。

2. 组网图

图1-6 IPoEoA 配置组网图



3. 配置步骤

(1) 配置 Router C

创建 VEth 接口，并为其配置 IP 地址。

```
<RouterC> system-view
[RouterC] interface virtual-ethernet 1
[RouterC-Virtual-Ethernet1] ip address 202.38.160.1 255.255.255.0
[RouterC-Virtual-Ethernet1] quit
```

创建 PVC，配置 IPoEoA 的承载方式。

```
[RouterC] interface atm 2/4/0.1
[RouterC-ATM2/4/0.1] pvc to_adsl_a 0/60
[RouterC-ATM2/4/0.1-pvc-to_adsl_a-0/60] map bridge virtual-ethernet 1
[RouterC-ATM2/4/0.1-pvc-to_adsl_a-0/60] quit
[RouterC-ATM2/4/0.1] pvc to_adsl_b 0/61
[RouterC-ATM2/4/0.1-pvc-to_adsl_b-0/61] map bridge virtual-ethernet 1
```

(2) 配置 ADSL Router A

创建 VEth 接口，并为其配置 IP 地址。

```
<RouterA> system-view
[RouterA] interface virtual-ethernet 1
[RouterA-Virtual-Ethernet1] ip address 202.38.160.2 255.255.255.0
[RouterA-Virtual-Ethernet1] quit
```

创建 PVC，配置 IPoEoA 的承载方式。

```
[RouterA] interface atm 2/4/0.1
[RouterA-ATM2/4/0.1] pvc to_c 0/60
[RouterA-ATM2/4/0.1-pvc-to_c-0/60] map bridge virtual-ethernet 1
```

(3) ADSL Router B 的配置与 ADSL Router A 相似。

4. 验证配置

ADSL Router A 和 ADSL Router B 都能 ping 通 Router C。

1.13.3 PPPoA典型配置举例

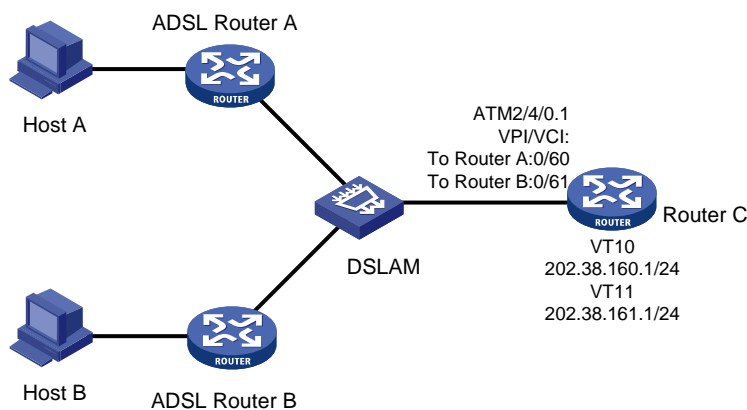
1. 组网需求

两台主机各自通过 ADSL Router A/B 拨号接入 ATM 网，并通过 DSLAM 与 Router C 通讯。要求：

- 在 Router C 上为多用户创建虚模板，并在虚模板上配置 PPP 的映射；
- Router C 连接至 DSLAM 的两条 PVC 的 VPI/VCI 为 0/60、0/61，分别指向 ADSL Router A 和 ADSL Router B；
- Router C 广域网端口和 ADSL Router A/B 的 DSL 接口均采用 PPPoA 应用方式，不进行 PPP 协议认证，ADSL Router A/B 的 IP 地址由该路由器提供。

2. 组网图

图1-7 PPPoA 配置组网图



3. 配置步骤

(1) 配置 Router C (PPPoA Server)

创建虚拟模板接口，配置 IP 地址，并为对端分配 IP 地址。

```
<RouterC> system-view
[RouterC] interface virtual-template 10
[RouterC-Virtual-Template10] ip address 202.38.160.1 255.255.255.0
[RouterC-Virtual-Template10] remote address 202.38.162.1
[RouterC-Virtual-Template10] quit
[RouterC] interface virtual-template 11
[RouterC-Virtual-Template11] ip address 202.38.161.1 255.255.255.0
[RouterC-Virtual-Template11] remote address 202.38.162.2
[RouterC-Virtual-Template11] quit
```

创建 PVC，并指定承载 PPP 协议。

```
[RouterC] interface atm 2/4/0.1
[RouterC-ATM2/4/0.1] pvc to_adsl_a 0/60
[RouterC-ATM2/4/0.1-pvc-to_adsl_a-0/60] map ppp virtual-template 10
[RouterC-ATM2/4/0.1-pvc-to_adsl_a-0/60] quit
[RouterC-ATM2/4/0.1] pvc to_adsl_b 0/61
[RouterC-ATM2/4/0.1-pvc-to_adsl_b-0/61] map ppp virtual-template 11
```

(2) 配置 ADSL Router A (PPPoA Client)

创建虚拟模板接口，配置 IP 地址协商。

```
<RouterA> system-view
[RouterA] interface virtual-template 0
[RouterA-Virtual-Template0] ip address ppp-negotiate
[RouterA-Virtual-Template0] quit
# 创建 PVC，并指定承载 PPP 协议。
[RouterA] interface atm 2/4/0
[RouterA-ATM2/4/0] pvc pppoa 0/60
[RouterA-ATM2/4/0-pvc-pppoa-0/60] map ppp virtual-template 0
[RouterA-ATM2/4/0-pvc-pppoa-0/60] quit
[RouterA-ATM2/4/0] quit
```

(3) ADSL Router B 的配置与 ADSL Router A 相似。

4. 验证配置

ADSL Router A 和 ADSL Router B 都可以 ping 通 Router C。

1.13.4 PPPoEoA 典型配置举例

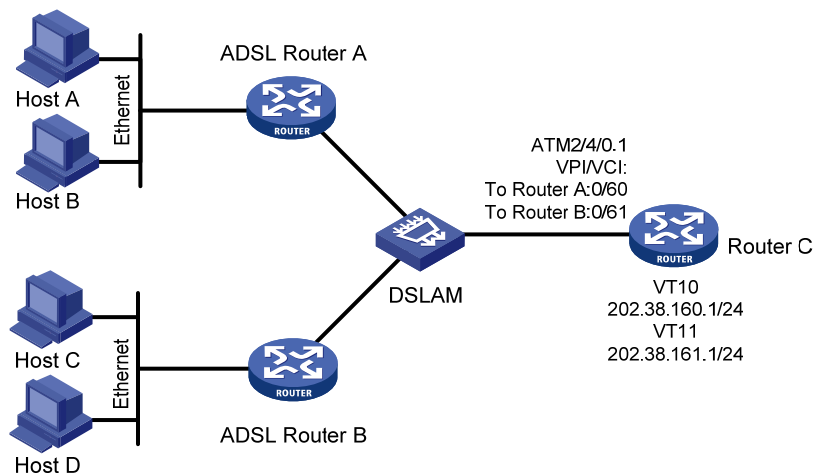
1. 组网需求

两个以太网中的多主机各自通过一台 ADSL Router 拨号接入 ATM 网，并通过 DSLAM 与路由器通讯。要求：

- Router C 虚拟模板接口的 IP 地址分别为 202.38.160.1 和 202.38.161.1；
- Router C 连接至 DSLAM 的两条 PVC 的 VPI/VCI 为 0/60、0/61，分别指向 ADSL Router A 和 ADSL Router B；
- Router C 广域网端口和 ADSL Router 的 DSL 接口均采用 PPPoEoA 应用方式，不进行 PPP 协议认证，并从路由器处获取 IP 地址。

2. 组网图

图1-8 PPPoEoA 配置组网图



3. 配置步骤

(1) 配置 Router C (PPPoEoA Server)

创建虚拟模板接口，配置 IP 地址，并为对端分配 IP 地址。

```
<RouterC> system-view
[RouterC] interface virtual-template 10
[RouterC-Virtual-Template10] ip address 202.38.160.1 255.255.255.0
[RouterC-Virtual-Template10] remote address 202.38.162.1
[RouterC-Virtual-Template10] quit
[RouterC] interface virtual-template 11
[RouterC-Virtual-Template11] ip address 202.38.161.1 255.255.255.0
[RouterC-Virtual-Template11] remote address 202.38.162.2
[RouterC-Virtual-Template11] quit
```

创建 VEth 接口，并指定承载 PPP 协议。

```
[RouterC] interface virtual-ethernet 1
[RouterC-Virtual-Ethernet1] pppoe-server bind virtual-template 10
[RouterC-Virtual-Ethernet1] quit
[RouterC] interface virtual-ethernet 2
[RouterC-Virtual-Ethernet2] pppoe-server bind virtual-template 11
[RouterC-Virtual-Ethernet2] quit
```

创建 PVC，并指定承载 PPPoE 协议。

```
[RouterC] interface atm 2/4/0.1
[RouterC-ATM2/4/0.1] pvc to_adsl_a 0/60
[RouterC-ATM2/4/0.1-pvc-to_adsl_a-0/60] map bridge virtual-ethernet 1
[RouterC-ATM2/4/0.1-pvc-to_adsl_a-0/60] quit
[RouterC-ATM2/4/0.1] pvc to_adsl_b 0/61
[RouterC-ATM2/4/0.1-pvc-to_adsl_b-0/61] map bridge virtual-ethernet 2
```

(2) 配置 ADSL Router A (PPPoEoA Client)

配置拨号访问组 1 以及对应的拨号访问控制条件。

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

创建 Dialer 接口，并在接口上使能共享 DDR。

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

将 Dialer1 接口与拨号访问组 1 关联。

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

配置 PPPoE Client 工作在永久在线模式。

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

配置 DDR 自动拨号的间隔时间为 1 秒。

```
[RouterA-Dialer1] dialer timer autodial 1
```

配置 IP 地址协商。

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

创建 VEth 接口，并指定承载 PPP 协议。

```
[RouterA] interface virtual-ethernet 2
[RouterA-Virtual-Ethernet2] pppoe-client dial-bundle-number 1
```

```

[RouterA-Virtual-Ethernet2] quit
# 创建 PVC，并指定承载 PPPoE 协议。
[RouterA] interface atm 2/4/0
[RouterA-ATM2/4/0] pvc 0/60
[RouterA-ATM2/4/0-pvc-0/60] map bridge virtual-ethernet 2

```

(3) ADSL Router B 的配置与 ADSL Router A 相似。

4. 验证配置

ADSL Router A 和 ADSL Router B 都可以 ping 通 Router C。

1.13.5 ATM PVC传输优先级典型配置举例

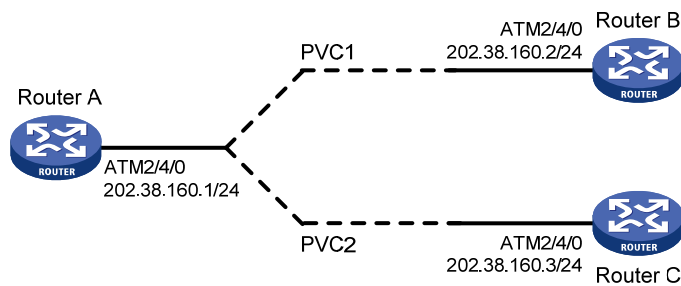
1. 组网需求

在同一个 ATM 155Mbps 接口下建立两个 PVC: PVC1 和 PVC2, 两个 PVC 带宽都设置为 100Mbps, 用于 UBR 服务。设定 PVC1 的优先级为 1, PVC2 的优先级为 3。

从 Router A 通过两个 PVC 分别向 Router B 和 Router C 发送流量相同的数据流, 观察统计结果(包括收发和丢包等数值)。

2. 组网图

图1-9 ATM PVC 优先级典型配置组网图



3. 配置步骤

配置 ATM 接口。

```

<RouterA> system-view
[RouterA] interface atm 2/4/0
[RouterA-Atm2/4/0] ip address 202.38.160.1 255.255.255.0

```

创建 PVC，并为各 PVC 指定不同的传输优先级。

```

[RouterA-ATM2/4/0] pvc 1 0/33
[RouterA-ATM2/4/0-pvc-1-0/33] map ip 202.38.160.2
[RouterA-ATM2/4/0-pvc-1-0/33] service ubr 100000
[RouterA-ATM2/4/0-pvc-1-0/33] transmit-priority 1
[RouterA-ATM2/4/0-pvc-1-0/33] quit
[RouterA-ATM2/4/0] pvc 2 0/32
[RouterA-ATM2/4/0-pvc-2-0/32] map ip 202.38.160.3
[RouterA-ATM2/4/0-pvc-2-0/32] service ubr 100000
[RouterA-ATM2/4/0-pvc-2-0/32] transmit-priority 3

```


4. 验证配置

在 Router A 向 Router B 和 Router C 发送超过 ATM 带宽的两种相同流量后，在 Router B 和 Router C 端通过 `display atm pvc-info interface atm 2/4/0 pvc` 命令显示每个 PVC 统计结果（可以多次测试，观察平均统计数据），可以看出对应优先级高的 PVC 收到的报文数量多，优先级低的 PVC 收到的报文数量少，即 ATM 接口在分配带宽时优先满足优先级较高的 PVC，其他的 PVC（若存在多个，且优先级不同）不论优先级如何在分配带宽时一样处理。

1.14 ATM常见故障处理

1.14.1 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。

1.14.2 采用PPPoA时，链路不上报up

1. 故障现象

采用 PPPoA 时，链路不上报 up。

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。

1.14.3 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。）

如果两端是 PPPoA，检查两端的 IP 地址及认证的配置情况。

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。

1.14.4 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后, 本端 PVC 的状态无法转变成 up。

1.14.5 配置PPPoA等应用之后, 无法ping通对端

1. 故障现象

PVC 状态为 up, 但在配置 PPPoA 等应用之后, 却无法 ping 通对端。

2. 故障排除

请查看对端是否支持所配置的应用方式。比如本侧采用 PPPoA 应用时, 对端也应采用 PPPoA 应用。如果对端支持所配置的应用方式, 请检查两边的 AAL5 封装协议类型是否相同。比如一边使用 aal5snap, 而另一边却使用 aal5mux, 则无法互通。可以打开 ATM 的报文调试开关, 可以从中得到相应的提示信息。

目 录

1 Modem管理.....	1-1
1.1 Modem管理简介.....	1-1
1.2 Modem配置限制和指导.....	1-1
1.3 Modem管理配置任务简介.....	1-1
1.4 开启Modem的呼入/呼出权限.....	1-1
1.5 配置Modem等待链路建立的有效时间间隔.....	1-2
1.6 配置Modem的应答方式.....	1-2
1.7 开启Modem模块获取终端主叫号码功能.....	1-3
1.8 开启Modem的回呼功能.....	1-3
1.9 通过AT指令配置Modem.....	1-3
1.10 配置Modem的编码格式.....	1-4
1.11 Modem管理典型配置举例.....	1-4
1.11.1 Modem管理基本组网配置举例.....	1-4
1.12 Modem管理常见故障处理.....	1-6
1.12.1 Modem状态不正常.....	1-6

1 Modem管理

1.1 Modem管理简介

Modem是目前使用广泛的一种网络设备，实现对 Modem 的良好管理和控制是路由器的一个重要功能。Modem 的厂家众多而且类型各异，虽然都支持业界标准的 AT 指令集，但在具体的实现和命令的细节上存在着或多或少的差别。

1.2 Modem配置限制和指导

支持的用户线包括：

- 异步串口对应的 TTY 用户线
- 工作在异步方式的同/异步串口对应的 TTY 用户线
- AM 接口对应的 TTY 用户线
- AUX 接口对应的 AUX 用户线

1.3 Modem管理配置任务简介

Modem 管理配置任务如下：

- (1) [开启Modem的呼入/呼出权限](#)
- (2) (可选) [配置Modem等待链路建立的有效时间间隔](#)
- (3) (可选) [配置Modem的应答方式](#)
- (4) (可选) [开启Modem模块获取终端主叫号码功能](#)
- (5) (可选) [开启Modem的回呼功能](#)
- (6) (可选) [通过AT指令配置Modem](#)
- (7) (可选) [配置Modem的编码格式](#)

1.4 开启Modem的呼入/呼出权限

1. 功能简介

允许 Modem 呼入，Modem 才可以接受对端的呼叫。允许 Modem 呼出，Modem 才可以对外发起呼叫。

2. 配置限制和指导

当 Modem 处于连接状态时，配置本功能会使 Modem 连接断开。

3. 配置步骤

- (1) 进入系统视图。
`system-view`
- (2) 进入用户线视图。

```
line { first-num1 [ last-num1 ] | { aux | tty } first-num2 [ last-num2 ] }
```

(3) 开启 Modem 的呼入/呼出权限。

```
modem enable { both | call-in | call-out }
```

缺省情况下，禁止 Modem 呼入和呼出。

1.5 配置Modem等待链路建立的有效时间间隔

1. 功能简介

当 Modem 等待链路建立的时间间隔超过配置的有效时间间隔后，Modem 将拆除本次呼叫。

Modem 作为主叫侧设备或被叫侧设备时，Modem 等待链路建立的时间间隔的含义不同：

- Modem 作为主叫侧设备时，该间隔是指从拨号到通话的时间间隔。
- Modem 作为被叫侧设备时，该间隔是指从摘机到通话的时间间隔。

2. 配置步骤

(1) 进入系统视图。

```
system-view
```

(2) 进入用户线视图。

```
line { first-num1 [ last-num1 ] | { aux | tty } first-num2 [ last-num2 ] }
```

(3) 配置 Modem 等待链路建立的有效时间间隔。

```
modem answer-timer time
```

缺省情况下，Modem 等待链路建立的有效间隔时间为 60 秒。

1.6 配置Modem的应答方式

1. 功能简介

需要根据路由器外接 Modem 的当前应答状态配置 Modem 的应答方式，使得用户接口的状态与外接 Modem 的状态一致，具体如下：

- 当外接 Modem 状态为自动应答（Modem 的 AA 灯亮）时，配置 `modem auto-answer`（以避免 Modem 自动应答后，路由器又发出应答指令）；
- 当外接 Modem 为非自动应答方式时，配置 `undo modem auto-answer`。

如果应答方式不一致，会造成应答不正常。

2. 配置步骤

(1) 进入系统视图。

```
system-view
```

(2) 进入用户线视图。

```
line { first-num1 [ last-num1 ] | { aux | tty } first-num2 [ last-num2 ] }
```

(3) 配置 Modem 的应答方式。

- 配置 Modem 的应答方式为自动应答方式。

```
modem auto-answer
```

- 配置 Modem 的应答方式为非自动应答方式。

undo modem auto-answer

缺省情况下，Modem 为非自-动应答方式。

1.7 开启Modem模块获取终端主叫号码功能

1. 功能简介

通过 AM 接口接入的 POS 终端，若前置机需要获取 POS 终端的主叫号码，则 POS 接入设备在向前置机转发终端的数据前，首先等待获取 POS 终端的主叫号码，然后将获取到的终端的主叫号码发送给前置机，并等待前置机响应之后，再转发该终端的数据。本功能用于配合 POS 接入终端实现主叫号码发送功能，关于 POS 接入终端主叫号码功能的相关介绍请参考“终端接入配置指导”中的“POS 终端接入”。

2. 配置限制和指导

目前，本功能只对 AM 接口接入的 POS（Point of Sale，销售点）终端有效。
当 Modem 处于连接状态时，配置本功能会使 Modem 连接断开。

3. 配置步骤

- (1) 进入系统视图。

system-view

- (2) 进入 AM 接口对应的 TTY 用户线视图。

line { *first-num1* [*last-num1*] | **tty** *first-num2* [*last-num2*] }

- (3) 开启 Modem 模块获取终端主叫号码功能。

modem caller-number resolve [**ata-waiting-time** *time*]

缺省情况下，Modem 模块接受终端呼叫时，不获取其主叫号码。

1.8 开启Modem的回呼功能

1. 功能简介

Modem 回呼功能是指 Modem 作为被叫侧设备和主叫方用户建立连接之后，对于需要回呼的主叫方用户，断开当前 Modem 连接并主动呼出。

2. 配置步骤

- (1) 进入系统视图。

system-view

- (2) 开启 Modem 的回呼功能。

modem callback

缺省情况下，Modem 的回呼功能处于关闭状态。

1.9 通过AT指令配置Modem

1. 配置限制和指导

通过 AT 指令配置 Modem 后，Modem 的工作状态会被改变，有可能导致 Modem 的状态混乱从而影响到拨号等基本功能。请在专业人员的指导下慎重使用本功能。

Modem 处于 AT 指令模式下才能接受 AT 指令，若处于数据传输状态，使用该命令发送的 AT 指令无效。

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
```

可以是异步串口、工作在异步方式的同/异步串口、AUX 接口、AM 接口。

- (3) 手工向 Modem 发送 AT 指令。

```
sendat at-string
```

通过 **sendat** 命令一次只能发送一条 AT 指令。

1.10 配置Modem的编码格式

1. 功能简介

在不同的地区，Modem 的编码格式有所不同，为了适应不同地区的编码格式，可以配置本命令。

2. 配置限制和指导

本功能只对 AM 接口有效。

当 Modem 处于连接状态时，配置本功能会使 Modem 连接断开。

3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入 AM 接口视图。

```
interface analogmodem interface-number
```

- (3) 配置 Modem 的编码格式。

```
country-code area-name
```

缺省情况下，地区编码格式为 **united-states**。

1.11 Modem管理典型配置举例

1.11.1 Modem管理基本组网配置举例

1. 组网需求

Router A 使用 Serial2/1/0 接口，通过 DDR 拨号可以与 Router B 建立连接。当 IP 地址 1.1.1.1/16 与 IP 地址 2.2.2.2/16 之间有数据需要传输时，Router A 可以通过 DDR 建立拨号连接完成数据传输需求。

关于通过 DDR 建立拨号连接的详细内容，请参见“二层技术-广域网接入配置指导”中的“DDR”。

2. 组网图

图1-1 通过 Modem 互通组网图



3. 配置步骤

(1) 配置 Router A

配置拨号访问组 1 以及对应的拨号访问控制条件。

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

```
[RouterA] dialer-group 1 rule ip permit
```

配置 Serial2/1/0 接口工作在异步方式、协议模式。

```
[RouterA] interface serial 2/1/0
```

```
[RouterA-Serial2/1/0] physical-mode async
```

```
[RouterA-Serial2/1/0] async-mode protocol
```

配置 Serial2/1/0 接口的 IP 地址。

```
[RouterA-Serial2/1/0] ip address 1.1.1.1 255.255.0.0
```

在 Serial2/1/0 接口上启动传统 DDR。

```
[RouterA-Serial2/1/0] dialer circular enable
```

将拨号访问组 1 与 Serial2/1/0 接口关联。

```
[RouterA-Serial2/1/0] dialer-group 1
```

配置 Serial2/1/0 接口去往对端的拨号串。

```
[RouterA-Serial2/1/0] dialer number 666666
```

```
[RouterA-Serial2/1/0] quit
```

在用户线 1 上，配置允许 Modem 呼入和呼出。

```
[RouterA] line tty 1
```

```
[RouterA-line-tty1] modem enable both
```

(2) 配置 Router B

配置拨号访问组 1 以及对应的拨号访问控制条件。

```
<RouterB> system-view
```

```
[RouterB] dialer-group 1 rule ip permit
```

配置 Serial2/1/0 接口工作在异步方式、协议模式。

```
[RouterB] interface serial 2/1/0
```

```
[RouterB-Serial2/1/0] physical-mode async
```

```
[RouterB-Serial2/1/0] async-mode protocol
```

配置 Serial2/1/0 接口的 IP 地址。

```
[RouterB-Serial2/1/0] ip address 2.2.2.2 255.255.0.0
```

在 Serial2/1/0 接口上启动传统 DDR。

```
[RouterB-Serial2/1/0] dialer circular enable
```

将拨号访问组 1 与 Serial2/1/0 接口关联。

```
[RouterB-Serial2/1/0] dialer-group 1
```

配置 Serial2/1/0 接口去往对端的拨号串。


```
[RouterB-Serial2/1/0] dialer number 888888
```

```
[RouterB-Serial2/1/0] quit
```

在用户线 1 上，配置允许 Modem 呼入和呼出。

```
[RouterB] line tty 1
```

```
[RouterB-line-tty1] modem enable both
```

关于 DDR 命令的详细说明，请参见“二层技术-广域网接入命令参考”中的“DDR”。

4. 验证配置

Router A 和 Router B 之间可以互相 ping 通。

1.12 Modem管理常见故障处理

1.12.1 Modem状态不正常

1. 故障现象

外置 Modem 状态不正常（如啸叫声长时间不停止或持续忙音）。

2. 故障排除

可以按照如下步骤进行：

- 在与外置 Modem 连接的路由器物理接口上执行 **shutdown** 和 **undo shutdown** 命令，检查外置 Modem 状态是否恢复正常；
- 若外置 Modem 状态仍不正常，则可将外置 Modem 重新上电。

目 录

1 3G/4G Modem管理	1-1
1.1 3G/4G Modem管理简介	1-1
1.2 3G/4G Modem配置限制和指导	1-1
1.3 3G/4G Modem管理配置任务简介	1-1
1.4 配置 3G Modem模块Cellular接口基本参数	1-2
1.5 配置 4G Modem模块Cellular接口基本参数	1-2
1.6 配置 4G Modem模块以太网通道接口	1-3
1.6.1 配置接口基本参数	1-3
1.6.2 恢复接口缺省配置	1-3
1.6.3 配置 4G Modem模块以太网通道接口的IP地址	1-4
1.7 配置 3G/4G Modem无线网络	1-5
1.8 配置 3G/4G Modem参数模板	1-6
1.8.1 3G/4G Modem参数模板简介	1-6
1.8.2 创建 3G Modem参数模板	1-6
1.8.3 配置 4G Modem参数模板	1-6
1.8.4 配置 3G/4G Modem拨号使用的参数模板	1-7
1.9 配置 3G/4G Modem使用主用SIM卡或者备用SIM卡	1-7
1.10 配置 3G/4G Modem链路备份与Track项联动	1-8
1.11 配置 3G/4G Modem PIN码认证功能	1-9
1.12 配置 3G/4G Modem本地信任的IMSI	1-10
1.13 配置 3G/4G Modem的DM功能	1-10
1.14 配置 3G/4G Modem的RSSI检测功能	1-10
1.15 通过配置指令配置 3G/4G Modem	1-11
1.16 配置 3G/4G Modem重启功能	1-11
1.16.1 配置自动重启 3G/4G Modem功能	1-11
1.16.2 手动重启 3G/4G Modem	1-12
1.17 配置本地SIM卡的IMSI与接口绑定	1-12
1.18 3G/4G Modem管理显示和维护	1-12
1.19 3G/4G Modem管理典型配置举例	1-13
1.19.1 3G Modem管理配置举例	1-13
1.19.2 4G Modem管理配置举例	1-14
1.20 3G/4G Modem管理常见故障处理	1-15
1.20.1 3G/4G Modem状态不正常	1-15

1 3G/4G Modem管理

1.1 3G/4G Modem管理简介

在设备上安装 3G/4G Modem 模块后，设备就可以接入 3G/4G 网络。

3G/4G Modem 模块包括 USB 3G/4G Modem 模块和 SIC-3G/4G Modem 模块。

- USB 3G/4G Modem 模块支持热插拔并采用固定的 Cellular 接口对其配置进行管理。在设备没有安装模块的情况下，用户可以进入该 Cellular 接口对模块进行配置，配置的参数在 USB 3G/4G Modem 模块被拔出后，可以继续保存。
- SIC-3G/4G Modem 模块不支持热插拔，采用动态生成的 Cellular 接口视图对其配置进行管理。系统只有在模块安装后，才会根据该模块安装的槽位号创建一个 Cellular 接口。当模块被拔出后，系统会删除该 Cellular 接口以及接口上的配置。

Cellular 接口可以派生出工作在协议模式下的 Serial 和 Eth-channel 两种接口。Serial 接口链路层协议为 PPP，Eth-channel 接口链路层协议为以太网，两者网络层都支持 IP 协议。

目前，3G Modem 只支持 Cellular 接口派生出来的 Serial 接口，4G Modem 只支持 Cellular 接口派生出来的 Eth-channel 接口。

1.2 3G/4G Modem配置限制和指导

- 在 USB 3G/4G Modem 传输数据的过程中，请不要强行将其拔出。在拔出 USB 3G/4G Modem 之前，建议使用 **shutdown** 命令关闭 USB 3G/4G Modem。
- USB 3G/4G Modem 模块是插到设备的 USB 接口上的，如果关闭 USB 接口，则 USB 3G/4G Modem 模块的功能不可用。关闭 USB 接口的详细介绍，请参见“基础配置指导”中的“设备管理”。
- 本章关于 3G/4G Modem 的配置一般被保存在 3G/4G Modem 的非易失性存储介质中。配置成功后，可以通过 **display cellular** 命令查看配置是否生效。下文中，如无特殊说明，配置均保存在 3G/4G Modem 上。

1.3 3G/4G Modem管理配置任务简介

3G/4G Modem 管理配置任务如下：

- (1) [配置 3G Modem模块Cellular接口基本参数](#)
- (2) [配置 4G Modem模块Cellular接口基本参数](#)
- (3) [配置 4G Modem模块以太网通道接口](#)
- (4) [配置 3G/4G Modem无线网络](#)
- (5) [配置 3G/4G Modem参数模板](#)
- (6) [（可选）配置 3G/4G Modem使用主用SIM卡或者备用SIM卡](#)
- (7) [（可选）配置 3G/4G Modem链路备份与Track项联动](#)
- (8) [（可选）配置 3G/4G Modem PIN码认证功能](#)

- (9) [\(可选\) 配置 3G/4G Modem本地信任的IMSI](#)
- (10) [\(可选\) 配置 3G/4G Modem的DM功能](#)
- (11) [\(可选\) 配置 3G/4G Modem的RSSI检测功能](#)
- (12) [\(可选\) 通过配置指令配置 3G/4G Modem](#)
- (13) [\(可选\) 配置 3G/4G Modem重启功能](#)
 - o [配置自动重启 3G/4G Modem功能](#)
 - o [手动重启 3G/4G Modem](#)
- (14) [\(可选\) 配置本地SIM卡的IMSI与接口绑定](#)

1.4 配置3G Modem模块Cellular接口基本参数

- (1) 进入系统视图。

system-view

- (2) 进入 Cellular 接口视图。

controller cellular *cellular-number*

- (3) (可选) 配置 Cellular 接口的描述信息。

description *text*

缺省情况下，Cellular 接口的描述信息为“该接口的接口名 Interface”，比如：Cellular2/4/0 Interface。

- (4) 将 Cellular 接口通道化出同/异步串口。

serial-set *set-number*

Cellular 接口在配置该命令后通道化出一个 Serial 接口，接口名是 **serial** *cellular-number:set-number*，在该接口上还可配置 PPP 参数、DDR 参数、IP 地址等。

- (5) 打开 Cellular 接口。

undo shutdown

缺省情况下，Cellular 接口处于打开状态。

1.5 配置4G Modem模块Cellular接口基本参数

- (1) 进入系统视图。

system-view

- (2) 进入 Cellular 接口视图。

controller cellular *cellular-number*

- (3) (可选) 配置 Cellular 接口的描述信息。

description *text*

缺省情况下，Cellular 接口的描述信息为“该接口的接口名 Interface”，比如：Cellular2/4/0 Interface。

- (4) 将 Cellular 接口通道化出以太网通道接口。

eth-channel *channel-number*

Cellular 接口在配置该命令后通道化出一个以太网通道接口，接口名是 **eth-channel** *cellular-number:channel-number*，在该接口上还可配置 DDR 参数、IP 地址等。

- (5) 打开 Cellular 接口。

undo shutdown

缺省情况下，Cellular 接口处于打开状态。

1.6 配置4G Modem模块以太网通道接口

1.6.1 配置接口基本参数

- (1) 进入系统视图。

system-view

- (2) 进入以太网通道接口视图。

interface eth-channel *interface-number*

- (3) 配置接口的描述信息。

description *text*

缺省情况下，以太网通道接口的描述信息为“*该接口的接口名* Interface”，比如“Echannel2/4/0:0 Interface”。

- (4) 配置接口的 MTU 值。

mtu *size*

缺省情况下，以太网通道接口的 MTU 值为 1500 字节。

- (5) 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)。

以太网通道接口的波特率为 100Mbps。

- (6) 打开以太网通道接口。

undo shutdown

缺省情况下，以太网通道接口为开启状态。

1.6.2 恢复接口缺省配置

1. 配置限制和指导



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) 进入以太网通道接口视图。

```
interface eth-channel interface-number
```

- (3) 恢复接口的缺省配置。

```
default
```

1.6.3 配置 4G Modem 模块以太网通道接口的 IP 地址

1. 以太网通道接口的 IP 地址获取方式

以太网通道接口有了 IP 地址后才可以与其它主机进行 IP 通信。以太网通道接口获取 IP 地址的方式有以下几种：

- 通过 DHCP 协议获取 IP 地址：部分 Modem 支持 DHCP 服务，以太网通道接口可以通过 DHCP 协议从 Modem 处获取 IP 地址，Modem 的 IP 地址由运营商自动分配。
- 通过 Modem 私有协议获取 IP 地址：部分 Modem 支持以厂商自己的私有协议从 Modem 处获取 IP 地址，Modem 的 IP 地址由运营商自动分配。
- 手动指定 IP 地址：部分情况下，如果不能从 Modem 处获得 IP 地址，则必须手动配置接口 IP 地址。

上述几种方式是互斥的，通过新的配置方式获取的 IP 地址会覆盖通过原有方式获取的 IP 地址。例如，首先通过手动指定了 IP 地址，然后使用 DHCP 协议获取 IP 地址，那么手动指定的 IP 地址会被删除，接口使用的是通过 DHCP 协议获取到的 IP 地址。

2. 配置限制和指导

改变以太网通道接口的 IP 地址配置会导致拨号断开，部分运营商不支持断开后马上进行拨号。

3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入以太网通道接口视图。

```
interface eth-cahnnel interface-number
```

- (3) 配置以太网通道接口的 IP 地址。请选择其中一项进行配置。

- 配置接口通过 DHCP 协议获取 IP 地址。

```
ip address dhcp-alloc
```

缺省情况下，接口不通过 DHCP 协议获取 IP 地址。

关于本命令的详细介绍请参见“三层技术-IP 业务命令参考”中的“DHCP”。

- 配置接口通过 Modem 私有协议获取 IP 地址。

(IPv4 网络)

```
ip address cellular-alloc
```

(IPv6 网络)

```
ipv6 address cellular-alloc
```

缺省情况下，接口不通过 Modem 私有协议获取 IP 地址。

- 手动指定接口 IP 地址。

```
ip address ip-address { mask-length | mask } [ sub ]
```

缺省情况下，没有为接口配置 IP 地址。

1.7 配置3G/4G Modem无线网络

1. 配置限制和指导

3G Modem 可以接入 GSM 网络、CDMA2000 网络、TD-SCDMA 网络和 WCDMA 网络，4G Modem 可以接入 GSM 网络、CDMA2000 网络、TD-SCDMA 网络、WCDMA 网络和 LTE 网络。

使用 3G/4G Modem 时，需要在 PLMN（Public Land Mobile Network，公共地带移动网络）中选择接入的移动网络。每个 PLMN 由 MCC（Mobile Country Code，移动国家编码）和 MNC（Mobile Network Code，移动网络编码）唯一标识。有的 3G/4G Modem 能自动选择接入合适的网络。如果用户需要手工指定接入的移动网络，则需要先搜索移动网络，获取当前区域内有信号的移动网络列表。

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入 Cellular 接口视图。

```
controller cellular interface-number
```

- (3) （可选）搜索移动网络。

```
plmn search
```

- (4) 配置选择移动网络的方式。

```
plmn select { auto | manual mcc mnc }
```

本命令的缺省情况与 3G/4G Modem 设备的型号有关，请以设备的实际情况为准。

- (5) 选择网络连接方式。

```
mode { lxrtd | auto | evdo | gsm | gsm-precedence | hybrid | lte | td |  
td-precedence | wcdma | wcdma-precedence }
```

本命令的缺省情况以及各参数的支持情况与 3G/4G Modem 设备的型号有关，请以设备的实际情况为准。

- (6) 选择 GSM 模块工作的频段。

```
gsm band { egsm900 | gsm450 | gsm480 | gsm750 | gsm850 | gsm1800 | gsm1900  
| pgsm900 | rsgm900 }
```

缺省情况下，未配置 3G/4G Modem 接入 GSM 网络的工作频段。

- (7) 选择 WCDMA 模块工作的频段。

```
wcdma band { wcdma800 | wcdma850 | wcdma900 | wcdma1700ip | wcdma1700us  
| wcdma1800 | wcdma1900 | wcdma2100 | wcdma2600 }
```

缺省情况下，未配置 3G/4G Modem 接入 WCDMA 网络的工作频段。

- (8) 选择 LTE 模块工作的频段。

lte band *band-number*

本命令的缺省情况以及各参数的支持情况与 4G Modem 设备的型号有关，请以设备的实际情况为准。

1.8 配置3G/4G Modem参数模板

1.8.1 3G/4G Modem参数模板简介

3G/4G Modem 参数模板用于配置 3G/4G Modem 的接入点和认证方式，3G/4G Modem 会根据配置的接入点和认证方式，来和对应的服务商进行认证：

- 当选用 None 方式时，不需要输入用户名和密码。
- 当选用 CHAP 或 PAP 方式时，需要根据运营商的要求，选择配置用户名和密码。

1.8.2 创建 3G Modem参数模板

- (1) 进入系统视图。

```
system-view
```

- (2) 进入 Cellular 接口视图。

```
controller cellular interface-number
```

- (3) 创建参数模板。

```
profile create profile-number { dynamic | static apn }  
authentication-mode { none | { chap | pap } user username [ password  
password ] }
```

本命令的缺省情况与 3G/4G Modem 设备的型号有关，请以设备的实际情况为准。

1.8.3 配置 4G Modem参数模板

- (1) 进入系统视图。

```
system-view
```

- (2) 创建参数模板，并进入参数模板视图。

```
apn-profile profile-name
```

- (3) 配置 PDP 协议的数据负载类型。

```
pdp-type { ipv4 | ipv6 | ipv4v6 }
```

缺省情况下，PDP 协议的数据负载类型为 IPv4 和 IPv6。

- (4) 配置接入 4G 网络时的接入点。

```
apn { dynamic | static apn }
```

缺省情况下，未配置接入 4G 网络时的接入点。

- (5) 配置接入 4G 网络时的认证方式。

```
authentication-mode { pap | chap | pap-chap } user user-name password  
{ cipher | simple } string
```

缺省情况下，认证方式为不认证。

- (6) 配置 IMSI/SN 捆绑协商认证时发送用户名使用的分隔符。

```
attach-format imsi-sn split splitchart
```

缺省情况下，未配置协商认证时发送用户名使用的分隔符。

1.8.4 配置 3G/4G Modem拨号使用的参数模板

1. 功能简介

缺省情况下，3G/4G Modem 使用参数模板 1 进行拨号。如果参数模板 1 不存在，则拨号失败。

用户也可以通过下面的命令配置 3G/4G Modem 拨号使用的主备参数模板。配置该命令后，3G/4G Modem 每次拨号都优先选择主参数模板，如果主参数模板拨号失败，将使用备份参数模板进行拨号。无论备份参数模板拨号是否成功，下次拨号时都使用主参数模板拨号。

2. 配置限制和指导

使用的主备参数模板的用户名和密码必须一致。

3. 配置 3G Modem拨号使用的参数模板

- (1) 进入系统视图。

```
system-view
```

- (2) 进入 Cellular 接口视图。

```
controller cellular interface-number
```

- (3) 配置 3G Modem 拨号使用的主备参数模板。

```
profile main main-profile-number backup backup-profile-number
```

缺省情况下，3G Modem 使用参数模板 1 进行拨号。

4. 配置 4G Modem拨号使用的参数模板

- (1) 进入系统视图。

```
system-view
```

- (2) 进入以太网通道接口视图。

```
interface eth-channel interface-number
```

- (3) 指定 4G Modem 拨号使用的主备参数模板。

```
apn-profile apply profile-name [ backup profile-name ]
```

缺省情况下，4G Modem 未指定参数模板进行拨号。

1.9 配置3G/4G Modem使用主用SIM卡或者备用SIM卡

1. 功能简介

在主备双 SIM 卡的组网下，当 SIM 卡建立的 3G/4G 链路信号质量差、接入的运营商网络发生故障或者 SIM 卡发生故障时，用户可以切换至另一 SIM 卡。

2. 硬件适配关系



说明

仅 MSR810-LMS/810-LUS 路由器和安装了 SIC-4G-CNDE 接口的路由器支持。

3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入 Cellular 接口视图。

```
controller cellular interface-number
```

- (3) 配置 3G/4G Modem 使用主用 SIM 卡或者备用 SIM 卡。

```
sim switch-to card-number
```

缺省情况下，3G/4G Modem 使用主用 SIM 卡。

- (4) 开启 3G/4G Modem 由备用 SIM 卡自动切换至主用 SIM 卡功能。

```
sim switch-back enable [wait-time time]
```

缺省情况下，3G/4G Modem 由备用 SIM 卡自动切换至主用 SIM 卡功能处于关闭状态。

1.10 配置3G/4G Modem链路备份与Track项联动

1. 功能简介

在配置 3G/4G Modem 链路备份与 Track 项关联后，设备可以通过 Track 项来监测主链路的状态，根据网络环境的变化实现双卡单待的 3G/4G Modem 链路备份功能。

2. 硬件适配关系



说明

仅 MSR810-LMS/810-LUS 路由器和安装了 SIC-4G-CNDE 接口的路由器支持。

3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入 Cellular 接口视图。

```
controller cellular interface-number
```

- (3) 配置 3G/4G Modem 链路备份与 Track 项联动。

```
sim backup enable track entry-number
```

缺省情况下，未配置 3G/4G Modem 链路备份与 Track 项联动。

1.11 配置3G/4G Modem PIN码认证功能

1. 功能简介

每个 SIM/UIM 卡(UIM 卡用于 CDMA 网络, SIM 卡用于其它网络)都有 PIN(Personal Identification Number, 个人识别号码)码。PIN 码认证功能可以防止 SIM/UIM 卡在未授权的情况下被使用。

如果开启了 3G/4G Modem 的 PIN 码认证功能, 当 3G/4G Modem 插入或重启时, 会使用 `pin verify` 命令配置的 PIN 码进行认证, 否则 3G/4G Modem 的数据通信功能不可用。重启 3G/4G Modem 的途径包括: 重启设备、使用 `modem reboot` 命令重启 3G/4G Modem、热拔插 USB 3G/4G Modem。对于 SIC-3G/4G-CDMA 模块, 只有设备冷启动后, 才需要重新进行 PIN 码认证。

用户可以在需要 PIN 码认证时配置 `pin verify` 命令, 也可以提前配置 `pin verify` 命令, 只要配置一次 `pin verify` 命令, PIN 码就会保存在设备上, 在需要认证时, 自动完成 PIN 码认证。

在进行 PIN 码认证时, 如果 PIN 码连续输入错误达到一定次数(该次数与 3G/4G Modem 的设备型号有关)时, SIM/UIM 卡会被锁。此时, 必须使用 SIM/UIM 卡的 PUK(PIN Unlocking Key, PIN 码解锁码)码才能解锁。

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入 Cellular 接口视图。

```
controller cellular interface-number
```

- (3) 开启 3G/4G Modem 的 PIN 码认证功能。

```
pin verification enable [ pin ]
```

本命令的缺省情况与 3G/4G Modem 设备的型号有关, 请以设备的实际情况为准

配置本功能时, 可能要求输入当前的 PIN 码。该要求与 3G/4G Modem 设备的型号有关, 请以设备的实际情况为准。

- (4) 配置 3G/4G Modem 进行认证的 PIN 码。

```
pin verify { cipher | simple } string
```

缺省情况下, 未配置 3G/4G Modem 进行认证的 PIN 码。

该配置保存在设备上, 而不是保存在 3G/4G Modem 上。

- (5) (可选) 使用 PUK 码解锁 PIN 码。

```
pin unlock puk new-pin
```

如果开启了 3G/4G Modem 的 PIN 码认证功能, 解锁 PIN 码后, 需要配置 `pin verify` 命令以保持和重新设置的 PIN 码一致。

- (6) (可选) 修改 SIM/UIM 卡的 PIN 码。

```
pin modify current-pin new-pin
```

修改后的 PIN 码保存在 SIM/UIM 卡上。

如果开启了 3G/4G Modem 的 PIN 码认证功能, 修改 PIN 码后, 需要配置 `pin verify` 命令以保持和修改后的 PIN 码一致。

1.12 配置3G/4G Modem本地信任的IMSI

1. 功能简介

配置了本地信任的 IMSI 后，只有安装的 SIM 卡的 IMSI 与配置的本地信任的 IMSI 一致时，才可以进行拨号。

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入 Cellular 接口视图。

```
controller cellular interface-number
```

- (3) 配置本地信任的 IMSI。

```
trust-imsi string-imsi
```

最多可以配置 16 个本地信任的 IMSI。

1.13 配置3G/4G Modem的DM功能

1. 功能简介

DM (Diagnostic and Monitoring, 诊断和监控), 指某些类型的 3G/4G Modem 支持通过 3G/4G Modem 上的调试信息输出接口输出调试信息功能, 用于连接第三方的调试工具 (如高通 QXDM 软件) 进行诊断和监控。



说明

不同型号的 3G/4G Modem 对于 DM 功能支持情况不同, 具体使用请参考相应的 3G/4G Modem 用户手册。

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入 Cellular 接口视图。

```
controller cellular interface-number
```

- (3) 打开 3G/4G Modem 的 DM 功能。

```
dm-port open
```

本命令的缺省情况与 3G/4G Modem 设备的型号有关, 请以设备的实际情况为准。

1.14 配置3G/4G Modem的RSSI检测功能

1. 功能简介

rssI 检测功能用于配置 3G/4G 网络 RSSI 监控阈值, 用户可以通过监控 RSSI 值来了解信号强弱的变化。配置 *mediumthreshold* 必须大于等于 *lowthreshold*。

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入 Cellular 接口视图。

```
controller cellular interface-number
```

- (3) 配置 3G/4G Modem 的 rssi 检测功能。

```
rssi { gsm | lxrtd | evdo | lte } { low lowthreshold | medium  
mediumthreshold }*
```

缺省情况下，3G/4G 网络 RSSI 监控下限阈值为-150dBm、上限阈值为 0dBm。

1.15 通过配置指令配置3G/4G Modem

1. 配置限制和指导

通过配置指令配置 3G/4G Modem 后，3G/4G Modem 的工作状态会被改变，有可能导致 3G/4G Modem 的状态混乱从而影响到拨号等基本功能，请慎重使用本功能。

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入 Cellular 接口视图。

```
controller cellular interface-number
```

- (3) 手工向 3G/4G Modem 发送配置指令。

```
sendat at-string
```

sendat 命令一次只能配置一条配置指令。

1.16 配置3G/4G Modem重启功能

1.16.1 配置自动重启 3G/4G Modem功能

1. 功能简介

3G/4G 无线网络的不稳定运行或应用环境变化可能导致 3G/4G Modem 功能故障，无法自动拨号并连接网络。设备提供自动重启 3G/4G Modem 功能，尽可能减少需要用户手工重启 3G/4G Modem 的情况。

开启自动重启 3G/4G Modem 功能后，如果连续多次下发配置指令失败或配置指令响应超时，系统将自动重启 3G/4G Modem。为避免因配置错误引起的多次拨号失败，而导致的反复自动重启 3G/4G Modem 的情况，系统仅在上次自动重启 3G/4G Modem 后有过至少一次拨号成功记录，并且多次发配置指令失败或配置指令响应超时的情况下才会自动重启 3G/4G Modem。

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入 Cellular 接口视图。

controller cellular interface-number

- (3) 配置 3G/4G Modem 的自动重启参数。

modem response timer time auto-recovery threshold

缺省情况下，系统等待 3G/4G Modem 回复的时间间隔为 10 秒，连续不响应系统配置指令次数的阈值为 3 次。

该配置保存在设备上，而不是保存在 3G/4G Modem 上。

1.16.2 手动重启 3G/4G Modem

1. 功能简介

3G/4G Modem 在运行过程中能够自动检测异常，并实施自动重启。如果无法自动重启，用户可以通过本配置手动重启 3G/4G Modem。

2. 配置步骤

- (1) 进入系统视图。

system-view

- (2) 进入 Cellular 接口视图。

controller cellular interface-number

- (3) 手动重启 3G/4G Modem。

modem reboot

1.17 配置本地SIM卡的IMSI与接口绑定

1. 功能简介

4G 路由器作为 LAC 端时，并按照 L2TP 的 LAC-Auto-Initiated 模式自动触发接入 LNS 时需要配置 LAC 端支持 PPP LCP 协商 IMSI/SN 号。配置了本地 SIM 卡的 IMSI 与 Virtual-PPP 接口绑定后，4G 路由器发送的报文携带 4G 路由器的 IMSI。

2. 配置步骤

- (1) 进入系统视图。

system-view

- (2) 进入 Cellular 接口视图。

controller cellular interface-number

- (3) 配置本地 SIM 卡的 IMSI 与接口绑定。

imsi bind interface-type interface-number

分布式和 IRF 环境不支持该特性。

缺省情况下，本地 SIM 卡的 IMSI 未绑定到任何接口。

1.18 3G/4G Modem管理显示和维护

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 3G/4G Modem 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** 命令可以清除相关接口的统计信息。

表1-1 3G/4G Modem 管理显示和维护

操作	命令
显示3G/4G Modem的呼叫连接信息	display cellular [<i>interface-number</i>]
显示Cellular接口的相关信息	display controller [cellular [<i>interface-number</i>]]
显示以太网通道接口的相关信息	display interface [eth-channel [<i>channel-id</i>]] [brief [description down]]
清除Cellular接口的统计信息	reset counters controller [cellular [<i>interface-number</i>]]
清除以太网通道接口的统计信息	reset counters interface [eth-channel [<i>channel-id</i>]]

1.19 3G/4G Modem管理典型配置举例

1.19.1 3G Modem管理配置举例

1. 组网需求

设备上插有 USB 3G Modem/SIC-3G 接口模块，用户通过 DDR 拨号接入 3G 网络。

关于通过 DDR 建立拨号连接的详细内容，请参见“二层技术-广域网接入配置指导”中的“DDR”。

2. 组网图

图1-1 配置 3G Modem 组网图



3. 配置步骤

配置拨号访问组 1 以及对应的拨号访问控制条件。

```
<Router> system-view
```

```
[Router] dialer-group 1 rule ip permit
```

将 Cellular 接口通道化出同/异步串口。

```
[Router] controller cellular 2/4/0
```

```
[Router-Cellular2/4/0] serial-set 0
```

```
[Router-Cellular2/4/0] quit
```

配置接口的 IP 地址。

```
[Router] interface serial 2/4/0:0
```

```
[Router-Serial2/4/0:0] ip address 1.1.1.1 255.255.0.0
```

在接口上使能传统 DDR。

```
[Router-Serial2/4/0:0] dialer circular enable
```

将接口加入拨号访问组 1。

```
[Router-Serial2/4/0:0] dialer-group 1
```



```

# 配置 DDR 可以进行下一次呼叫的间隔时间为 5 秒。
[Router-Serial2/4/0:0] dialer timer autodial 5
# 配置接口去往对端的拨号串。
[Router-Serial2/4/0:0] dialer number 666666
[Router-Serial2/4/0:0] quit
# 在 TTY 1 用户线上，配置允许 Modem 呼入和呼出。
[Router] line tty 1
[Router-line-tty1] modem enable both

```

1.19.2 4G Modem管理配置举例

1. 组网需求

设备上插有 USB 4G Modem/SIC-4G 接口模块，用户通过 DDR 拨号接入 4G 网络。

关于通过 DDR 建立拨号连接的详细内容，请参见“二层技术-广域网接入配置指导”中的“DDR”。

2. 组网图

图1-2 配置 4G Modem 组网图



3. 配置步骤

配置拨号访问组 1 以及对应的拨号访问控制条件。

```

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

```

将 Cellular 接口通道化出以太网通道接口。

```

[Router] controller cellular 2/4/0
[Router-Cellular2/4/0] eth-channel 0
[Router-Cellular2/4/0] quit

```

配置以太网通道接口的 IP 地址。

```

[Router] interface eth-channel 2/4/0:0
[Router-Eth-channel2/4/0:0] ip address cellular-alloc

```

在接口上使能传统 DDR。

```

[Router-Eth-channel2/4/0:0] dialer circular enable

```

将接口加入拨号访问组 1。

```

[Router-Eth-channel2/4/0:0] dialer-group 1

```

配置 DDR 可以进行下一次呼叫的间隔时间为 5 秒。

```

[Router-Eth-channel2/4/0:0] dialer timer autodial 5

```

配置接口去往对端的拨号串。

```

[Router-Eth-channel2/4/0:0] dialer number 666666

```

1.20 3G/4G Modem管理常见故障处理

1.20.1 3G/4G Modem状态不正常

1. 故障现象

3G/4G Modem 状态不正常（如搜不到信号或不能连接到运营商网络）。

2. 故障排除

可以按照如下步骤进行：

- 在 3G/4G Modem 对应的 Cellular 接口上执行 **shutdown** 和 **undo shutdown** 命令，检查 3G/4G Modem 状态是否恢复正常；
- 若 3G/4G Modem 状态仍不正常，则在 3G/4G Modem 对应的 Cellular 接口上执行 **modem reboot**。

目 录

1 DDR	1-1
1.1 DDR简介	1-1
1.1.1 DDR接口	1-1
1.1.2 DDR方式	1-1
1.1.3 DDR分类	1-3
1.2 DDR配置任务简介	1-4
1.2.1 报文触发DDR配置任务简介	1-4
1.2.2 自动拨号DDR配置任务简介	1-4
1.2.3 路由触发DDR配置任务简介	1-4
1.3 DDR基本配置	1-5
1.3.1 配置物理接口	1-5
1.3.2 配置拨号接口的链路层协议、网络协议及路由协议	1-5
1.4 配置接口的DDR拨号控制规则	1-5
1.5 配置传统DDR	1-6
1.5.1 配置限制和指导	1-6
1.5.2 配置传统DDR的发起端	1-6
1.5.3 配置传统DDR的接收端	1-8
1.6 配置共享DDR	1-9
1.6.1 配置共享DDR的发起端	1-9
1.6.2 配置共享DDR的接收端	1-10
1.7 配置拨号接口	1-10
1.7.1 配置拨号接口的基本属性	1-10
1.7.2 配置呼叫定时器	1-11
1.7.3 配置拨号接口缓冲队列长度	1-12
1.7.4 配置keepalive报文参数	1-12
1.7.5 配置处理拨号接口流量的slot	1-13
1.7.6 恢复当前拨号接口的缺省配置	1-13
1.8 配置DDR链路的MP捆绑	1-14
1.9 配置PPP回呼	1-16
1.9.1 功能简介	1-16
1.9.2 配置限制和指导	1-16
1.9.3 配置PPP回呼的Client端	1-16
1.9.4 配置PPP回呼的Server端	1-17

1.10 配置根据ISDN主叫号码来过滤呼叫、回呼	1-19
1.10.1 功能简介	1-19
1.10.2 配置限制和指导	1-19
1.10.3 配置Server端（传统DDR）	1-20
1.10.4 配置Server端（共享DDR）	1-20
1.11 配置自动拨号	1-20
1.12 配置动态路由备份	1-21
1.12.1 功能简介	1-21
1.12.2 配置限制和指导	1-21
1.12.3 创建动态路由备份组	1-22
1.12.4 在备份接口上启用动态路由备份功能	1-22
1.12.5 配置主链路接通后断开备份链路的延迟时间	1-22
1.12.6 配置动态路由备份功能在系统启动后的生效延时	1-23
1.13 拆除拨号链路	1-23
1.14 DDR显示和维护	1-23
1.15 DDR典型配置举例	1-24
1.15.1 基于PSTN的传统DDR配置举例	1-24
1.15.2 基于PSTN的共享DDR配置举例	1-26
1.15.3 基于ISDN的传统DDR配置举例	1-29
1.15.4 基于ISDN的共享DDR配置举例	1-31
1.15.5 DDR链路的MP捆绑配置举例	1-33
1.15.6 根据ISDN主叫号码进行回呼的配置举例	1-35
1.15.7 路由器PPP回呼路由器的配置举例	1-36
1.15.8 路由器PPP回呼PC机的配置举例	1-39
1.15.9 NT服务器PPP回呼路由器的配置举例	1-41
1.15.10 拨号串循环备份并提供Internet接入服务的配置举例	1-43
1.15.11 通过传统DDR实现动态路由备份配置举例	1-47
1.15.12 通过共享DDR实现动态路由备份配置举例	1-49
1.15.13 通过一个动态路由备份组监控多个网段配置举例	1-52
1.16 DDR常见故障处理	1-54
1.16.1 无法建立DDR拨号连接	1-54
1.16.2 Modem已经接通，但是无法ping通对方	1-54

1 DDR

1.1 DDR简介

DDR 可在路由器通过公用交换网进行互连时，提供按需拨号服务。因其仅在需要时建立连接，能有效控制通信成本，在实际组网中得到广泛应用。

除 PSTN、ISDN 网络以外，以太网、ATM 也常常使用 DDR 技术作为接入控制的手段，具体介绍请参见“二层技术-广域网接入配置指导”中的“PPPoE”和“ATM”。

1.1.1 DDR接口

DDR 中用到的接口含义如下：

- 物理接口：支持 DDR 功能的物理接口，包括异步串口、工作在异步方式下的同/异步串口、AM 接口、AUX 接口、ISDN BRI 接口、ISDN PRI 接口、Celluler 接口。
- Dialer 接口：为了配置 DDR 参数而设置的逻辑接口。
- 拨号接口：拨号相关接口的统称。可以是 Dialer 接口，也可以是支持 DDR 功能的物理接口。

1.1.2 DDR方式

DDR 支持两种方式：传统 DDR 方式、共享 DDR 方式。

1. 传统DDR方式

传统 DDR 方式支持如下两种配置方式：

- 在物理接口上直接配置 DDR 参数
在此方式下，根据物理接口上配置的 DDR 参数，直接在该物理接口上发起或接收呼叫。
每个物理接口可以对应一个或多个呼叫目的地址。
本方式仅适用于一个接口发起/接收呼叫。
- 借助拨号循环组配置 DDR 参数
在此方式下，在 Dialer 接口上配置 DDR 呼叫参数，然后将一个 Dialer 接口与一组物理接口对应起来，由 Dialer 接口来控制通过哪个物理接口来发起或接收呼叫。
每个 Dialer 接口可以对应一个或多个呼叫目的地址。如果 Dialer 接口上配置了多个呼叫目的地址，则通过拨号循环组中的任一物理接口都可以呼叫设定好的任意一个目的地。
同一物理接口仅能属于一个 Dialer 接口。
本方式既适用于多个接口发起/接收呼叫，又适用于一个接口发起/接收呼叫。

2. 共享DDR方式

共享 DDR 方式下，不能在物理接口上直接配置 DDR 参数，只能在 Dialer 接口上配置 DDR 参数。物理接口必须绑定到 Dialer 接口才能实现 DDR 拨号功能。

每个 Dialer 接口对应一个 Dialer bundle，每个 Dialer bundle 中可以包含多个不同优先级别的物理接口，优先级高的物理接口会被优先使用，优先级相同时，会轮询选择各物理接口。

每个 Dialer 接口只能对应一个呼叫目的地址，呼叫不同的对端时使用不同的 Dialer 接口。

同一个物理接口可以属于多个 Dialer bundle，可以在不同的时候服务于不同的 Dialer 接口，与不同的目的地建立连接。

3. 两种DDR方式比较

传统 DDR 方式和共享 DDR 方式是互斥的，两种方式具有各自不同的特点：

- 传统 DDR 方式功能强大、应用广泛，但是由于一种拨号业务对应一个拨号接口，一个物理接口只能属于一个 Dialer 接口，所以每种拨号业务使用的物理接口都不同，当新增拨号业务时，就需要采用新的物理接口，因此传统 DDR 方式受限于拨号业务设置与物理接口配置之间的静态绑定，缺乏伸缩性、扩展性。
- 共享 DDR 方式比传统 DDR 方式简单，并具有良好的灵活性。共享 DDR 方式将物理接口和呼叫的逻辑配置分开进行，再将两者动态的捆绑起来，使得同一物理接口可以服务于多个 Dialer 接口，从而实现同一物理接口为多种不同的拨号业务服务。

两种方式下，物理接口、Dialer接口和呼叫目的地的对应关系如 [图 1-1](#) 和 [图 1-2](#) 所示。

图1-1 传统 DDR 的物理接口、Dialer 接口和呼叫目的地的对应关系图

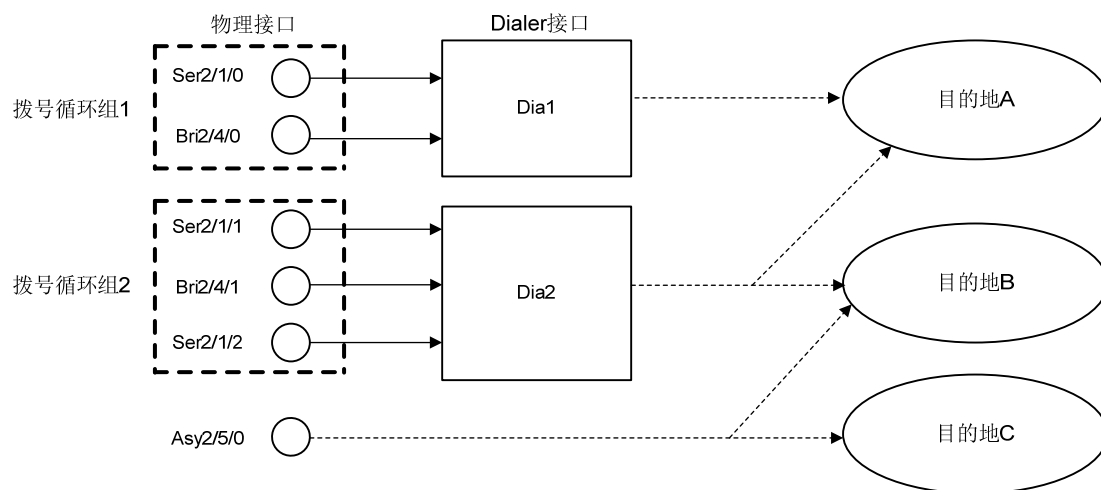
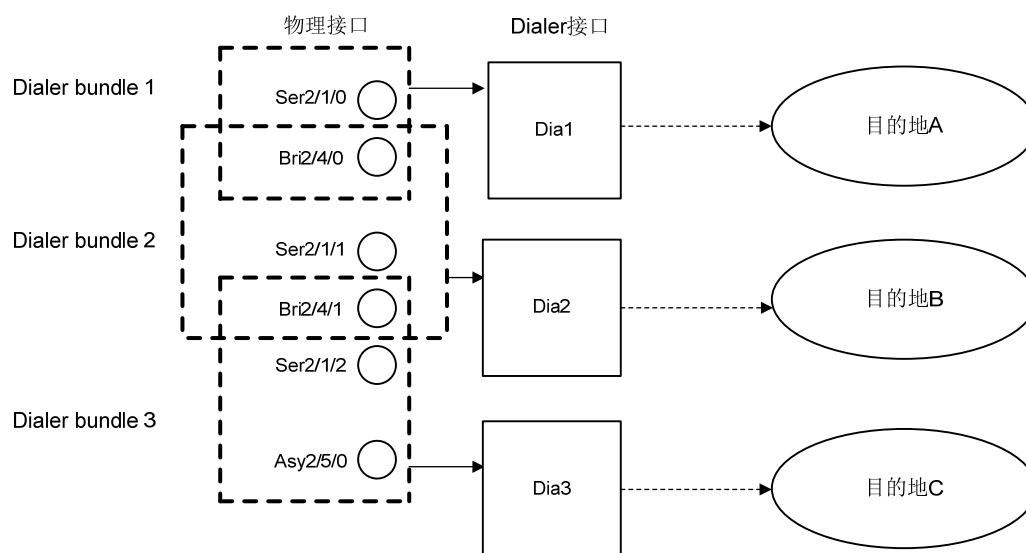


图1-2 共享 DDR 的物理接口、Dialer 接口和呼叫目的地的对应关系图



1.1.3 DDR分类

路由器的 DDR 功能主要用来控制链路建立和中断呼叫的。DDR 更准确的说是一个控制中心——决定链路何时建链和断开以及报文是否能够从该链路转发等。根据触发 DDR 拨号方式的不同，可将 DDR 分为如下几类：报文触发 DDR、自动拨号 DDR、路由触发 DDR。

1. 报文触发DDR

通过 DDR 拨号控制规则将拨号接口转发的数据报文分为两类：感兴趣报文、非感兴趣报文。

只有感兴趣报文才触发拨号。在拨号链路建立之前，非感兴趣的报文会被丢弃。直到有感兴趣报文触发拨号建立链路后，非感兴趣报文才同感兴趣报文一起转发。拨号链路建立后，如果链路的空闲时间超过了 Idle 定时器指定的时间，DDR 将断开链路。只有感兴趣报文会刷新 Idle 定时器，非感兴趣报文只是被“悄悄地转发”。

用户可以配置拨号控制规则来精确的定义感兴趣报文，然后在各个拨号接口下关联拨号控制规则，从而可以实现各个拨号接口由各自关注的感兴趣报文来触发拨号建立链路。

2. 自动拨号DDR

在路由器启动后，DDR 将自动尝试拨号连接对端，无需通过数据报文进行触发。若无法与对端正常建立拨号连接，则每隔一段时间 DDR 将再次自动尝试建立拨号连接。与报文触发的 DDR 相比，该连接建立后不会因超时而自动挂断。

3. 路由触发DDR

用户可以配置要监控的网段，然后将拨号接口与被监控的网段关联起来，当到达被监控的网段不存在有效路由时，会在拨号接口上通过 DDR 拨号启动备份链路来转发数据流量。备份链路启动后，系统会定时检查主链路的状态。当主链路恢复后，根据用户的配置可以选择直接挂断备份链路，也可以等待定时器超时后再挂断备份链路。

1.2 DDR配置任务简介

1.2.1 报文触发DDR配置任务简介

报文触发 DDR 配置任务如下：

- (1) [DDR基本配置](#)
- (2) [配置接口的DDR拨号控制规则](#)
- (3) 配置 DDR 拨号功能
 - [配置传统DDR](#)
 - [配置共享DDR](#)
- (4) [配置拨号接口](#)
- (5) （可选）[配置DDR链路的MP捆绑](#)
- (6) （可选）[配置PPP回呼](#)
- (7) （可选）[配置根据ISDN主叫号码来过滤呼叫、回呼](#)
- (8) （可选）[拆除拨号链路](#)

1.2.2 自动拨号DDR配置任务简介

自动拨号 DDR 配置任务如下：

- (1) [DDR基本配置](#)
- (2) 配置 DDR 拨号功能
 - [配置传统DDR](#)
 - [配置共享DDR](#)
- (3) [配置拨号接口](#)
- (4) （可选）[配置DDR链路的MP捆绑](#)
- (5) [配置自动拨号](#)
- (6) （可选）[拆除拨号链路](#)

1.2.3 路由触发DDR配置任务简介

路由触发 DDR 配置任务如下：

- (1) [DDR基本配置](#)
- (2) 配置 DDR
 - [配置传统DDR](#)
 - [配置共享DDR](#)
- (3) [配置拨号接口](#)
- (4) （可选）[配置DDR链路的MP捆绑](#)
- (5) [配置动态路由备份](#)
- (6) （可选）[拆除拨号链路](#)

1.3 DDR基本配置

1.3.1 配置物理接口

当连接 ISDN 网络时，路由器使用的物理接口可以是 ISDN BRI 接口、ISDN PRI 接口。当连接 PSTN 网络时，路由器使用的物理接口可以是异步串口、同/异步串口、AM 接口、AUX 接口。关于这些物理接口配置的详细介绍请参见“接口管理配置指导”中的“WAN 接口”。

配置同/异步串口时需要注意：

- 如果连接异步 Modem，则需要配置为异步方式（使用命令 **physical-mode async**）、工作在协议模式（使用命令 **async-mode protocol**），同时在对应的用户线上开启 Modem 的呼入/呼出权限（使用命令 **modem enable**）。
 - 如果连接同步 Modem，则需要配置为同步方式（使用命令 **physical-mode sync**）。
- 关于 Modem 的详细配置介绍请参见“二层技术-广域网接入配置指导”中的“Modem 管理”。

1.3.2 配置拨号接口的链路层协议、网络协议及路由协议

拨号接口支持链路层的 PPP 协议，支持网络层的 IP 协议，支持 RIP、OSPF 等动态路由协议。关于这些协议的详细配置介绍请参见“二层技术-广域网接入配置指导”中的“PPP 和 MP”、“三层技术-IP 业务配置指导”和“三层技术-IP 路由配置指导”。

请按照如下原则配置 PPP：

- 对于传统 DDR，如果直接在物理接口上配置 DDR 参数，则在物理接口上配置 PPP 相关命令；如果借助拨号循环组配置 DDR 参数，请在 Dialer 接口下配置 PPP 相关命令。
- 对于共享 DDR，如果是主叫端，请在 Dialer 接口下配置 PPP 相关命令，为确保 PPP 链路参数协商的可靠性，建议在物理接口下也配置相同的 PPP 相关命令；如果是被叫端，请在物理接口下配置 PPP 相关命令。

1.4 配置接口的DDR拨号控制规则

1. 功能简介

接口的 DDR 拨号控制规则用于控制接口什么时候发起 DDR 呼叫。用户需要在 DDR 呼叫的发起端配置接口的 DDR 拨号控制规则，在 DDR 呼叫的接收端不用配置接口的 DDR 拨号控制规则。

DDR 拨号控制规则的过滤方法有如下两种：

- 根据协议类型过滤报文：本方法目前只能匹配 IP 协议报文。
- 根据 ACL 过滤报文：本方法可以对报文进行更精细的区分。

根据匹配 DDR 拨号控制规则的结果，报文分为两种：

- 感兴趣报文：**permit** 的协议报文或者符合 ACL 的 **permit** 条件的报文。
- 非感兴趣报文：**deny** 的协议报文或者不符合 ACL 的 **permit** 条件的报文或者没有匹配任何规则的报文。

对上述两种报文的处理方式如下：

- 对于感兴趣报文：如果相应链路没有建立，则发起新呼叫建立链路并发送报文；如果相应链路已经建立，DDR 将通过该链路发送报文，并重置 Idle 超时定时器。

- 对于非感兴趣报文：如果相应链路没有建立，则不发起呼叫并丢弃此报文；如果相应链路已经建立，DDR 将通过此链路发送报文，但是不重置 Idle 超时定时器。

2. 配置限制和指导

用户必须配置 DDR 拨号控制规则，并将拨号接口与拨号控制规则相关联，DDR 才能正常拨号。一个接口只能关联一个拨号访问组。

3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 创建拨号访问组，并配置拨号控制规则。

```
dialer-group group-number rule { ip | ipv6 } { deny | permit | acl  
  { acl-number | name acl-name } }
```

- (3) 进入拨号接口视图。

```
interface interface-type interface-number
```

- (4) 配置该拨号接口关联的拨号访问组，将该接口与拨号控制规则相关联。

```
dialer-group group-number
```

缺省情况下，接口不与任何拨号访问组相关联。

1.5 配置传统DDR

1.5.1 配置限制和指导

应用传统 DDR 方法配置时，拨号双方可以选择配置 PAP 或 CHAP 认证。为确保拨号身份的安全性，推荐配置认证，配置方法请参见“二层技术-广域网接入配置指导”中的“PPP 和 MP”，同时注意以下约束：

- 如果物理接口直接配置 DDR 参数，则直接在物理接口上配置 PAP 或 CHAP 认证。
- 如果借助拨号循环组配置 DDR 参数，则在 Dialer 接口上配置 PAP 或 CHAP 认证。

1.5.2 配置传统DDR的发起端

1. 配置限制和指导

当接口作为呼叫的发起端时，需要为接口使能 DDR 功能并配置呼叫对端的拨号串。

进行发起端的配置时需要注意：

- 如果从一个接口发起呼叫，可以在物理接口上直接配置，也可以借助拨号循环组配置。如果从多个接口发起呼叫，则只能借助拨号循环组配置。
- 当向一个对端发起呼叫时，可以使用命令 **dialer number** 或 **dialer route** 配置到达对端的拨号串；当向多个对端发起呼叫时，需要多次使用 **dialer route** 命令分别配置到不同目的地址对应的拨号串。
- 对应同一个目的地址也可配置多条 **dialer route** 命令分别指定对应不同的拨号串，从而实现拨号串备份，即如果使用当前拨号串无法呼通对端，则下次呼叫时则自动选择另一个拨号串进行拨号。

2. 配置传统DDR的发起端（使用物理接口配置）

- (1) 进入系统视图。

```
system-view
```

- (2) 进入物理接口视图。

```
interface interface-type interface-number
```

- (3) 使能传统 DDR。

```
dialer circular enable
```

缺省情况下，接口上未使能传统 DDR。

- (4) 配置呼叫一个或多个对端的目的地址及拨号串。

- 配置呼叫一个对端的目的地址及拨号串。

```
dialer number dial-number
```

- 配置呼叫一个或多个对端的目的地址及拨号串。

```
dialer route ip next-hop-address [ mask network-mask-length ]  
[ vpn-instance vpn-instance-name ] dial-number number [ broadcast ]
```

缺省情况下，没有配置呼叫对端的目的地址及拨号串。

3. 配置传统DDR的发起端（使用拨号循环组配置）

- (1) 进入系统视图。

```
system-view
```

- (2) 创建 Dialer 接口，并进入 Dialer 接口视图。

```
interface dialer number
```

- (3) 使能传统 DDR。

```
dialer circular enable
```

缺省情况下，接口上未使能传统 DDR。

- (4) 配置呼叫一个或多个对端的目的地址及拨号串。

- 配置呼叫一个对端的目的地址及拨号串。

```
dialer number dial-number
```

- 配置呼叫一个或多个对端的目的地址及拨号串。

```
dialer route ip next-hop-address [ mask network-mask-length ]  
[ vpn-instance vpn-instance-name ] dial-number number [ broadcast ]
```

缺省情况下，没有配置呼叫对端的目的地址及拨号串。

- (5) 退回系统视图。

```
quit
```

- (6) 进入物理接口视图。

```
interface interface-type interface-number
```

- (7) 将物理接口加入指定的拨号循环组。

```
dialer circular-group number
```

缺省情况下，物理接口不属于任何一个拨号循环组。

拨号循环组的序号 *number* 要与 Dialer 接口的编号相同。

- (8) 配置物理接口在拨号循环组中的优先级。

```
dialer priority priority
```

缺省情况下，物理接口在拨号循环组中的优先级为 1。

如果从一个接口发起呼叫，不需要配置本命令；如果从多个接口发起呼叫，需要配置本命令，高优先级的物理接口会被优先使用，优先级相同时，会轮询选择各物理接口。

1.5.3 配置传统DDR的接收端

1. 配置限制和指导

当接口作为呼叫的接收端时，只需要为接口使能 DDR 功能即可，不需要配置拨号串。

配置时需要注意：

- 如果从一个接口接收呼叫，可以在物理接口上直接配置，也可以借助拨号循环组配置。
- 如果从多个接口接收呼叫，则只能借助拨号循环组配置。
- 配置接收对端的呼叫时进行认证时，如果需要接收多个对端的呼叫，则需要多次配置 **dialer route** 命令，并且必须通过 **ip** 和 **user** 参数指定主叫方的 IP 地址和用户名。只有当主叫方的 IP 地址和认证用户名与配置的 IP 地址和用户名一致时，设备才会接收其呼叫。

2. 配置传统DDR的接收端（使用物理接口配置）

- (1) 进入系统视图。

```
system-view
```

- (2) 进入物理接口视图。

```
interface interface-type interface-number
```

- (3) 使能传统 DDR。

```
dialer circular enable
```

缺省情况下，接口上未使能传统 DDR。

配置本命令后，如果不配置对主叫方进行认证，则接口可接收所有呼叫。

- (4) （可选）配置接收对端的呼叫时进行认证。

```
dialer route ip next-hop-address [ mask network-mask-length ]  
[ vpn-instance vpn-instance-name ] [ broadcast | user hostname ] *
```

缺省情况下，未配置接收对端的呼叫时进行认证。

3. 配置传统DDR的接收端（使用拨号循环组配置）

- (1) 进入系统视图。

```
system-view
```

- (2) 创建 Dialer 接口，并进入 Dialer 接口视图。

```
interface dialer number
```

- (3) 使能传统 DDR。

```
dialer circular enable
```

缺省情况下，接口上未使能传统 DDR。

配置本命令后，如果不配置对主叫方进行认证，则接口可接收所有呼叫。

- (4) （可选）配置接收对端的呼叫时进行认证。

```
dialer route ip next-hop-address [ mask network-mask-length ]  
[ vpn-instance vpn-instance-name ] [ broadcast | user hostname ] *
```

- (5) 退回系统视图。

```
quit
```

- (6) 进入物理接口视图。

```
interface interface-type interface-number
```

- (7) 将物理接口加入指定的拨号循环组。

```
dialer circular-group number
```

缺省情况下，物理接口不属于任何一个拨号循环组。

拨号循环组的序号 *number* 要与 Dialer 接口的编号相同。

1.6 配置共享DDR

1.6.1 配置共享DDR的发起端

1. 配置限制和指导

当接口作为呼叫的发起端时，需要在 Dialer 接口上使能 DDR 功能并配置呼叫对端的拨号串。每个 Dialer 接口仅可以配置呼叫一个对端的拨号串。

在共享 DDR 的发起端，系统根据拨号控制规则来确定使用哪个 Dialer 接口进行呼叫，物理接口将使用该 Dialer 接口的配置信息进行拨号（包括 PPP 认证协商等）。当 Dialer bundle 中包含多个物理接口时，优先使用高优先级的物理接口，优先级相同时，会轮询选择各物理接口。

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 创建 Dialer 接口，并进入 Dialer 接口视图。

```
interface dialer number
```

- (3) 使能共享 DDR。

```
dialer bundle enable
```

缺省情况下，接口未使能共享 DDR。

- (4) 配置呼叫一个对端的拨号串。

```
dialer number dial-number
```

- (5) 配置发起端对接收端认证。

对接收端进行认证，则要在 Dialer 接口上配置 PAP 或 CHAP 认证，详细介绍请参见“二层技术-广域网接入命令参考”中的“PPP 和 MP”。

- (6) 退回系统视图。

```
quit
```

- (7) 进入物理接口视图。

```
interface interface-type interface-number
```

- (8) 将物理接口加入指定的 Dialer bundle。

```
dialer bundle-member number [ priority priority ]
```

缺省情况下，物理接口不属于任何一个 Dialer bundle。

该 Dialer bundle 的序号 *number* 要与 Dialer 接口的编号相同。

1.6.2 配置共享DDR的接收端

1. 配置限制和指导

当接口作为呼叫的接收端时，只需要为接口使能 DDR 功能即可，不需要配置拨号串。

接收端必须对发起端进行认证，用户需要在接收物理接口上配置 PAP 或 CHAP 认证，同时在 Dialer 接口上配置 **dialer peer-name**。这是因为在共享 DDR 的接收端，由于一个物理接口可能服务于多个 Dialer 接口，在进行 PPP 协商认证前还无法确定物理接口所属的 Dialer 接口，只有当 PPP 协商认证通过后，再根据认证用户名匹配 Dialer 接口上的 **dialer peer-name** 来确定物理接口和哪个 Dialer 接口绑定，PPP 应用哪个 Dialer 接口的配置进行 IPCP 协商。关于认证的详细配置介绍请参见“二层技术-广域网接入配置指导”中的“PPP 和 MP”。

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 创建 Dialer 接口，并进入 Dialer 接口视图。

```
interface dialer number
```

- (3) 使能共享 DDR。

```
dialer bundle enable
```

缺省情况下，接口未使能共享 DDR。

- (4) 设置对端用户名。

```
dialer peer-name username
```

在一个 Dialer 接口下最多可以配置 255 个对端用户名。当一个 Dialer 接口下配置多个对端用户名时，就实现了用一个 Dialer 接口同时接入多个物理接口的连接。

- (5) 退回系统视图。

```
quit
```

- (6) 进入物理接口视图。

```
interface interface-type interface-number
```

- (7) 将物理接口加入指定的 Dialer bundle。

```
dialer bundle-member number [ priority priority ]
```

缺省情况下，物理接口不属于任何一个 Dialer bundle。

该 Dialer bundle 的序号 *number* 要与 Dialer 接口的编号相同。

1.7 配置拨号接口

1.7.1 配置拨号接口的基本属性

- (1) 进入系统视图。

system-view

- (2) 进入拨号接口视图。

```
interface interface-type interface-number
```

- (3) 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：Dialer1 Interface。

- (4) 配置接口的 MTU 值。

```
mtu size
```

缺省情况下，接口的 MTU 值为 1500 字节。

- (5) 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”。

- (6) 打开接口。

```
undo shutdown
```

缺省情况下，接口处于打开状态。

1.7.2 配置呼叫定时器

1. 功能简介

- 链路空闲时间：一条链路建立后，如果链路的空闲时间超过了指定的时间，DDR 将断开链路。
- 当链路断开后进行下次呼叫的间隔时间：当 DDR 呼叫链路因故障或挂断等原因进入断开状态，必须经过指定时间（即进行下一次呼叫的间隔时间）后才能建立新的拨号连接，从而避免对端程控交换机过载。
- 接口发生呼叫竞争后的链路空闲时间：通常一条链路建立后 Idle 超时定时器将起作用。当 DDR 开始发起新呼叫时，若所有物理接口都被占用则进入“竞争”状态，此时 DDR 使用 Compete-idle 超时定时器取代 Idle 超时定时器，即链路空闲时间超过 Compete-idle 超时定时器的时间后将自动断开。
- 呼叫建立超时时间：和某些对端建立 DDR 呼叫时，从呼叫发起到连接建立的时间长短不一，为了有效控制发起呼叫到呼叫连接建立之间允许等待的时间，可以配置 Wait-carrier 定时器，若在指定时间内呼叫仍未建立，则 DDR 将终止该呼叫。

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入拨号接口视图。

```
interface interface-type interface-number
```

- (3) 配置允许链路空闲的时间。

```
dialer timer idle idle [ in | in-out ]
```

缺省情况下，允许链路空闲的时间为 120 秒，只有出方向的感兴趣报文重置定时器。

- (4) 配置当链路断开后进行下次呼叫的间隔时间。

```
dialer timer enable interval
```

缺省情况下，当链路断开后进行下次呼叫的间隔时间为 5 秒。

- (5) 配置接口发生呼叫竞争后的链路空闲时间。

```
dialer timer compete compete-idle
```

缺省情况下，接口发生呼叫竞争后的链路空闲时间为 20 秒。

- (6) 配置呼叫建立超时时间。

```
dialer timer wait-carrier wait-carrier
```

缺省情况下，呼叫建立超时时间为 60 秒。

1.7.3 配置拨号接口缓冲队列长度

1. 功能简介

没有为拨号接口配置缓冲队列的情况下，当拨号接口收到一个报文时，如果此时连接还没有成功建立，则这个报文将被丢弃。如果为拨号接口配置了缓冲队列，则在连接成功建立之前报文将被缓存而不是被丢弃，待连接成功后再发送。

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入拨号接口视图。

```
interface interface-type interface-number
```

- (3) 配置拨号接口缓冲队列长度。

```
dialer queue-length packets
```

缺省情况下，不对报文进行缓存。

1.7.4 配置keepalive报文参数

- (1) 进入系统视图。

```
system-view
```

- (2) 进入拨号接口视图。

```
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。

- (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。

- (5) 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。

1.7.5 配置处理拨号接口流量的slot

1. 功能简介

当要求同一个处理拨号接口的流量必须在同一个 slot 上进行处理时，可以在处理拨号接口下配置处理接口流量的 slot。

为提高当前接口处理流量的可靠性，可以通过 **service** 命令为接口指定一个 slot 进行流量处理。如果接口上未配置 slot，则业务处理在接收报文的 slot 上进行。

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入拨号接口视图。

```
interface interface-type interface-number
```

- (3) 配置处理接口流量的主用 slot。

（独立运行模式）

```
service slot slot-number
```

（IRF 模式）

```
service chassis chassis-number slot slot-number
```

缺省情况下，未配置处理接口流量的主用 slot。

- (4) 配置处理接口流量的备用 slot。

（独立运行模式）

```
service standby slot slot-number
```

（IRF 模式）

```
service standby chassis chassis-number slot slot-number
```

缺省情况下，未配置处理接口流量的备用 slot。

1.7.6 恢复当前拨号接口的缺省配置

1. 配置限制和指导



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) 进入拨号接口视图。

```
interface interface-type interface-number
```

- (3) 恢复接口的缺省配置。

```
default
```

1.8 配置DDR链路的MP捆绑

1. 功能简介

在 DDR 链路上配置 MP 捆绑后，设备会每隔一段时间统计一次流量的信息，并且根据以下三个配置决定 MP 链路的增加或者减少：

- 链路的负载阈值

在 DDR 应用中，可以配置链路的负载阈值。当负载阈值在 1~99 之间时，MP 捆绑根据实际流量百分比适当调节分配的带宽，即如果一条链路的实际流量与带宽的比例超过设定的负载阈值，则系统会自动启用第二条链路，并将两条链路进行 MP 捆绑；当两条链路的流量与带宽的比例超过设定的负载阈值，系统会启动第三条链路并进行 MP 捆绑，依此类推，从而确保 DDR 链路具有合理的负载流量。相反，若 N 条（N 为大于等于 2 的整数）链路的流量与 N-1 条链路带宽的比例小于设定的负载阈值时，系统自动关闭一条链路，依此类推，从而确保 DDR 链路的利用率保持在合理范围。

- 最大捆绑链路数

在 DDR 中必须借助 Dialer 接口来实现 MP 捆绑。在 Dialer 接口上配置 `ppp mp` 和 `dialer threshold` 命令后，当 Dialer 接口中的某个物理接口上的流量与带宽的比例超过负载阈值时，DDR 会启用该 Dialer 接口中的另一个物理接口，并对这些链路进行 MP 捆绑（如果物理接口为 ISDN BRI 或 PRI 接口，则 DDR 会从该物理接口中选择空闲 B 通道进行 MP 捆绑）。当拨起的链路数达到 `max-bind-num` 时，PPP MP 捆绑的链路数达到上限，此时将停止启动新的链路。

- 最小捆绑链路数

在拨号使用中，有时需要能够同时使用多条链路来承载业务，因此需要一次报文触发能够呼起多条链路以保证需要的最小带宽，此时可以配置 `ppp mp min-bind` 命令。配置 `ppp mp min-bind` 命令时，路由器首先拨起第一条链路，在链路 UP 后检测捆绑的链路数是否达到 `min-bind-num`，如果没有达到，则再拨起一条链路，依此类推，直至达到最小捆绑链路数为止。

2. 配置限制和指导

- `ppp mp min-bind`、`dialer threshold`、`ppp mp max-bind` 三条命令只能在 Dialer 接口上进行配置。当三条命令同时配置时，系统首先拨起 `min-bind-num` 条链路，如此时流量仍超过 `traffic-percentage`，则继续拨起下一条空闲链路，直至捆绑链路数达到 `max-bind-num` 或流量低于 `traffic-percentage` 为止。对于呼起的 `min-bind-num` 条链路，不会因为超时而主动拆链。

- 当负载阈值配置为 0 时，在链路由于自动拨号或者报文触发拨号而开始呼叫的时候，将自动启动 *max-bind-num* 条可用链路进行呼叫，而不依靠流量检测决定呼叫策略，并且对于已经呼叫建立的链路也不会因为超时而主动拆链，即 **dialer timer idle** 命令将会失效。
- 当不配置链路的负载阈值时，如果配置了 MP 最小捆绑链路数为 *min-bind-num*，系统会启动 *min-bind-num* 条链路进行 MP 捆绑；如果不配置 MP 最小捆绑链路数，则系统只启动一条链路进行呼叫。此时，MP 最大捆绑链路数不起作用。
- 建议只在呼叫的一端配置负载阈值、MP 最大捆绑链路数、MP 最小捆绑链路数。如果在呼叫的发起端和接收端都配置了该值，当两端配置的值不一致时，则负载阈值较小的值、MP 最大捆绑链路数较小的值、MP 最小捆绑链路数较大的值起作用。

3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 配置 DDR 提供流量统计信息的间隔时间。

```
dialer flow-interval interval
```

缺省情况下，DDR 提供流量统计信息的间隔时间为 20 秒。

DDR 以用户配置的时间间隔为 MP 捆绑提供拨号链路上的流量统计信息。

- (3) 进入 Dialer 接口视图。

```
interface dialer number
```

- (4) 开启 DDR 链路的捆绑功能。

```
ppp mp
```

缺省情况下，不启动该功能。

关于 MP 捆绑的详细介绍请参见“二层技术-广域网接入配置指导”中的“PPP 和 MP”。

对应的物理接口上均需要配置该命令。

- (5) （可选）设置 MP 捆绑的负载阈值。

```
dialer threshold traffic-percentage [ in | in-out | out ]
```

缺省情况下，不启动该功能。

- (6) （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。

关于本命令的详细介绍请参见“二层技术-广域网接入命令参考”中的“PPP 和 MP”。

- (7) （可选）配置 MP 最小捆绑链路数。

```
ppp mp min-bind min-bind-num
```

缺省情况下，最小捆绑链路数为 0，即拨号将依赖流量检测。

关于本命令的详细介绍请参见“二层技术-广域网接入命令参考”中的“PPP 和 MP”。

1.9 配置PPP回呼

1.9.1 功能简介

回呼是指“接受呼叫方”反方向呼叫“发送呼叫方”，其中，发送呼叫方作为 Client 端，接受呼叫方作为 Server 端。在 PPP 回呼中，由 Client 端首先发起呼叫，Server 端确认该呼叫是否需要进行回呼，若需要回呼，Server 端则立即挂断该次呼入连接，并根据用户名或回呼字符串等信息向 Client 端重新发起呼叫。进行回呼的好处是：

- 增强安全性：回呼时，Server 端根据本端配置的呼叫号码呼叫 Client 端，可以避免主叫欺骗。
- 改变话费承担方，当两个方向的呼叫费率不同时可以节省话费。

1.9.2 配置限制和指导

- 实现 PPP 回呼必须配置认证。在 Client 端和 Server 端，建议物理接口和 Dialer 接口上都配置 PAP 或 CHAP 认证命令。
- 为了使 Server 端有足够的时间进行回呼，Client 端当链路断开后进行下次呼叫的间隔时间(通过 `dialer timer enable` 命令配置)应至少比 Server 端的长 10 秒。建议 Server 端使用默认值 5 秒，Client 端配置为 15 秒。
- 配置回呼时不能同时在接口上配置动态路由备份组。因为在接口上配置动态路由备份时，只允许从动态路由备份组开始拨号，此时该接口上不接受入呼叫和其它情况的出呼叫。

1.9.3 配置PPP回呼的Client端

1. 功能简介

路由器作为 Client 端可以向对端（具备 PPP 回呼 Server 功能的路由器、Windows NT Server）发起呼叫，并可以正常接收对端的回呼。

使用传统 DDR 和共享 DDR 实现 PPP 回呼的 Client 端配置基本相同，区别仅在于共享 DDR 必须使用 `dialer number` 命令配置呼叫拨号串。

2. 配置Client端（传统DDR）

- (1) 进入系统视图。

```
system-view
```

- (2) 进入拨号接口视图。

```
interface interface-type interface-number
```

- (3) 配置本端为 PPP 回呼的 Client 端。

```
ppp callback client
```

缺省情况下，系统未启动回呼功能。

- (4) 配置 Windows NT Server 回呼路由器时所需要的拨号串。

```
ppp callback ntstring dial-number
```

缺省情况下，没有设置 Windows NT Server 回呼拨号串。

当路由器作为 PPP 回呼的 Client 端呼叫作为 PPP 回呼 Server 端的 Windows NT Server 时，如果 Windows NT Server 需要路由器发送回呼号码，则需要配置此命令。

3. 配置Client端（共享DDR）

- (1) 进入系统视图。

```
system-view
```

- (2) 进入 Dialer 接口视图。

```
interface dialer number
```

- (3) 配置本端为 PPP 回呼的 Client 端。

```
ppp callback client
```

缺省情况下，系统未启动回呼功能。

- (4) 配置 Windows NT Server 回呼路由器时所需要的拨号串。

```
ppp callback ntstring dial-number
```

缺省情况下，没有设置 Windows NT Server 回呼拨号串。

当路由器作为 PPP 回呼的 Client 端呼叫作为 PPP 回呼 Server 端的 Windows NT Server 时，如果 Windows NT Server 需要路由器发送回呼号码，则需要配置此命令。

1.9.4 配置PPP回呼的Server端

1. 功能简介

使用传统 DDR 和共享 DDR 实现 PPP 回呼的 Server 端配置区别如下：

- 使用传统 DDR 实现 PPP 回呼时，Server 端既可以根据 **dialer route** 命令中配置的对端用户名对应的拨号串进行回呼（必须配置 PPP 认证），也可以根据 PPP 用户的回呼号码进行回呼，因此需要使用 **dialer callback-center** 命令配置回呼的参照依据。
- 使用共享 DDR 实现 PPP 回呼时，Server 端只能根据 PPP 用户的回呼号码进行回呼，设置的 PPP 回呼的参照依据只能是 **dial-number**。

2. 配置Server端（传统DDR）

- (1) 进入系统视图。

```
system-view
```

- (2) 进入拨号接口视图。

```
interface interface-type interface-number
```

- (3) 配置本端为 PPP 回呼的 Server 端。

```
ppp callback server
```

缺省情况下，系统未启动回呼功能。

- (4) 配置 PPP 回呼的参照依据。

```
dialer callback-center [ dial-number | user ] *
```

缺省情况下，未配置 PPP 回呼的参照依据，无法进行 PPP 回呼。

- (5) 退回系统视图。

```
quit
```

- (6) 根据回呼参照依据的不同进行不同的配置。请选择其中一项进行配置。

- 请依次执行以下命令配置回呼用户及回呼号码。

```
local-user user-name class network  
service-type ppp  
authorization-attribute callback-number callback-number
```

- 请依次执行以下命令配置回呼用户及回呼号码。

```
interface interface-type interface-number  
dialer route ip next-hop-address [ mask network-mask-length ]  
[ vpn-instance vpn-instance-name ] dial-number number [ interface  
interface-type interface-number ] [ broadcast ] user hostname.
```

当 Client 端采用动态分配的网络地址时，Server 端的回呼参照依据只能是 **dial-number**。

如果回呼参照依据是 **dial-number**，则需要根据 PPP 认证中接收的对端用户名确定回呼的拨号串。如果回呼参照依据是 **user**，则需要根据 **dialer route** 命令中配置的对端用户名对应的拨号串进行回呼。

3. 配置Server端（共享DDR）

- (1) 进入系统视图。

```
system-view
```

- (2) 进入 Dialer 接口视图。

```
interface dialer number
```

- (3) 配置本端为 PPP 回呼的 Server 端。

```
ppp callback server
```

缺省情况下，系统未启动回呼功能。

- (4) 配置 PPP 回呼的参照依据。

```
dialer callback-center dial-number
```

缺省情况下，未配置 PPP 回呼的参照依据，无法进行 PPP 回呼。

- (5) 退回系统视图。

```
quit
```

- (6) 配置回呼用户及回呼号码。

- 加本地用户，并进入本地用户视图。

```
local-user user-name class network
```

- 设置用户使用的服务类型为 PPP。

```
service-type ppp
```

缺省情况下，系统不对用户授权任何服务，即用户不能使用任何服务。

- 设置本地用户或用户组的授权属性。

```
authorization-attribute callback-number callback-number
```

缺省情况下，未配置本地用户或用户组的授权属性。

1.10 配置根据ISDN主叫号码来过滤呼叫、回呼

1.10.1 功能简介

在 ISDN 环境中，可以根据 ISDN 主叫号码来过滤呼叫，并根据过滤结果来决定是否接受该呼叫或者进行回呼。

1. 回呼简介

回呼是指“接受呼叫方”反方向呼叫“发送呼叫方”，其中，发送呼叫方作为 Client 端，接受呼叫方作为 Server 端。由 Client 端首先发起呼叫，Server 端确认该呼叫是否需要回呼，若需要回呼，Server 端则立即挂断该次呼入连接，并向 Client 端重新发起呼叫。进行回呼的好处是：

- 增强安全性：回呼时，Server 端根据本端配置的呼叫号码呼叫 Client 端，可以避免主叫欺骗。
- 改变话费承担方，当两个方向的呼叫费率不同时可以节省话费。

2. 基于ISDN主叫号码过滤呼叫的过程

根据 ISDN 主叫号码来过滤呼叫的工作过程如下：

- (1) 当 Server 端收到一个呼叫时，首先确定与呼入号码相关的 **dialer call-in**。
 - 在传统 DDR 中，会在物理接口或物理接口所属的 Dialer 接口上配置的 **dialer call-in** 中查找与呼入号码相匹配的 **dialer call-in**。
 - 在共享 DDR 中，会在拨入呼叫所对应的 Dialer 接口配置的 **dialer call-in** 中查找与呼入号码相匹配的 **dialer call-in**。
- (2) 找到与呼入号码相关的 **dialer call-in** 后，采用右端匹配的规则，来比较呼入号码与 **dialer call-in** 命令配置的 ISDN 主叫号码是否匹配。

右端匹配规则是指：从最右端的号码开始，逐位比较呼入号码与配置的 ISDN 主叫号码是否相同（“*”符号代表任意字符），比较的号码位数以两个号码中位数较少的为准。例如：配置的 ISDN 主叫号码为 12345，呼入号码为 45，比较最右端的 2 位号码，比较的结果是两个号码匹配；配置的 ISDN 主叫号码为 345，呼入号码为 12345，比较最右端的 3 位号码，比较的结果是两个号码也匹配。

如果呼入号码与多个 **dialer call-in** 命令匹配，则优先选择“*”符号较少的，如果“*”符号个数相同，则选择最先找到的。
- (3) 根据呼入号码与本端 **dialer call-in** 命令的匹配情况，采用如下处理方式：
 - 拒绝该呼入：配置了 **dialer call-in** 命令，但呼入号码和所有 **dialer call-in** 命令都不匹配。
 - 接受该呼入：没有配置 **dialer call-in** 命令或呼入号码与一个没有“**callback**”关键字的 **dialer call-in** 命令相匹配。
 - 回呼：配置了 **dialer call-in** 命令，且呼入号码与某个包含“**callback**”关键字的 **dialer call-in** 命令相匹配。

1.10.2 配置限制和指导

- 当 **dialer call-in** 命令中携带了 **callback** 参数时，在配置了 **dialer call-in** 的拨号接口上同时需要配置 **dialer route** 或者 **dialer number** 命令，**dialer route** 或者

dialer number 命令中的 *number* 要与 **dialer call-in** 命令中的 *remote-number* 一致，以保证进行正确的回呼。

- 为了使 Server 端有足够的时间进行回呼，Client 端当链路断开后进行下次呼叫的间隔时间（通过 **dialer timer enable** 命令配置）应至少比 Server 端的长 10 秒。建议 Server 端使用默认值 5 秒，Client 端配置为 15 秒。

1.10.3 配置Server端（传统DDR）

- (1) 进入系统视图。

```
system-view
```

- (2) 进入拨号接口视图。

```
interface interface-type interface-number
```

- (3) 配置允许呼入的 ISDN 主叫号码，或按照该 ISDN 主叫号码进行回呼。

```
dialer call-in remote-number [ callback ]
```

缺省情况下，未配置按照 ISDN 主叫号码来过滤呼叫。

1.10.4 配置Server端（共享DDR）

- (1) 进入系统视图。

```
system-view
```

- (2) 进入 Dialer 接口视图。

```
interface dialer interface-number
```

- (3) 配置允许呼入的 ISDN 主叫号码，或按照该 ISDN 主叫号码进行回呼。

```
dialer call-in remote-number [ callback ]
```

缺省情况下，未配置按照 ISDN 主叫号码来过滤呼叫。

1.11 配置自动拨号

1. 功能简介

该功能可以和传统 DDR、共享 DDR 结合使用。所谓自动拨号是指：在路由器启动后，DDR 将自动尝试拨号连接对端，无需通过数据报文进行触发。若无法与对端正常建立拨号连接，则每隔一段时间 DDR 将再次自动尝试建立拨号连接。与数据触发的非自动拨号 DDR 相比，该连接建立后不会因超时而自动挂断（即 **dialer timer idle** 命令对自动拨号不起作用）。

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入拨号接口视图。

```
interface interface-type interface-number
```

- (3) 配置自动呼叫一个或多个对端的目的地址及拨号串。

- 配置自动呼叫一个对端的目的地址及拨号串。

```
dialer number number autodial
```


- 配置自动呼叫多个对端的目的地址及拨号串。

```
dialer route ip next-hop-address [ mask network-mask-length ]  
[ vpn-instance vpn-instance-name ] dial-number number autodial  
[ interface interface-type interface-number ] [ broadcast ]
```

缺省情况下，未配置自动拨号功能。

当向一个对端发起呼叫时，可以使用命令 **dialer number** 或 **dialer route** 配置拨号串；当向多个对端发起呼叫时，需要使用 **dialer route** 命令多次配置拨号串和目的地址。

- (4) 设置自动拨号的时间间隔。

```
dialer timer autodial autodial-interval
```

当配置自动拨号功能后，自动拨号的间隔时间缺省为 300 秒。

1.12 配置动态路由备份

1.12.1 功能简介

动态路由备份功能通过配置要监控的网段，可以实现当到达被监控网段不存在有效路由时，通过 DDR 拨号启动备份链路，从而实现对路由的动态备份。

动态路由备份主要对动态路由协议产生的路由进行备份，也可以对静态路由和直连路由进行备份。使用动态路由备份功能时，必须精确定义被监控的网段。当备份接口启用动态路由备份功能后，系统监控路由、启动备份链路的过程如下：

- (1) 系统监控到达需监控网段是否存在路由更新，并检查路由表中到达需监控网段是否存在至少一条有效路由。
- (2) 如果存在至少一条到达需监控网段的路由，并且这条路由从其他接口（未启动动态路由备份功能的接口）出发，则认为主链路接通。
- (3) 如果不存在有效路由，则认为主链路故障并且不可用，在备份接口通过 DDR 拨号启动备份链路。
- (4) 备份链路启动后，拨号链路承载通信数据。在此过程中，系统会定时检查主链路的状态。
- (5) 当主链路恢复后，根据用户的配置可以选择直接挂断备份链路，也可以等待定时器（主链路接通后断开备份链路的延迟时间）超时后再挂断备份链路。

1.12.2 配置限制和指导

有些路由协议（如 BGP）默认使用优选路由，当到达被监控网段的主链路因为故障中断，启用备份链路之后，备份链路通过 BGP 协议学习到达被监控网段的路由；当主链路再次启用后，主链路通过 BGP 协议学到的路由和备份链路学到的路由相比可能不是最优路由，因此继续使用从备份链路学到的路由，这样备份链路在主链路恢复时无法挂断。对于 BGP 协议，需要用户通过配置保证，当主链路和备份链路同时有效时，系统优选从主链路学到的路由。

1.12.3 创建动态路由备份组

1. 功能简介

每个动态路由备份组可以监控多个网段，各监控网段之间是“与”的关系，即当到达所有被监控网段都不存在有效路由时，才试图拨通备份链路。拨通备份链路时依次查找各监控网段在备份接口是否配有 **dialer route**，当配置多个时，用查到的第一个 **dialer route** 拨号，且只能拨通一条链路。

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 创建动态路由备份组，并配置需监控的网段。

```
standby routing-group group-number rule ip ip-address { mask |  
mask-length } [ vpn-instance vpn-instance-name ]
```

本命令配置的需监控网段地址和 VPN 实例应与相对应的 **dialer route** 命令中的拨号目的网段和 VPN 实例完全一致。

1.12.4 在备份接口上启用动态路由备份功能

1. 功能简介

启用动态路由备份功能之前，必须确保备份接口上已经配置了 DDR 拨号功能。

每个备份接口上可以同时引用多个动态路由备份组。

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入备份接口的视图。

```
interface interface-type interface-number
```

- (3) 启用动态路由备份功能，并配置引用的动态路由备份组。

```
standby routing-group group-number
```

缺省情况下，动态路由备份功能处于关闭状态。

1.12.5 配置主链路接通后断开备份链路的延迟时间

1. 功能简介

在主链路接通后，为了防止路由震荡，可以经过指定延迟时间再断开备份链路。

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入备份接口的视图。

```
interface interface-type interface-number
```

- (3) 配置主链路接通后断开备份链路的延迟时间。

standby timer routing-disable delay

缺省情况下，主链路接通后断开备份链路的延迟时间为 20 秒。

1.12.6 配置动态路由备份功能在系统启动后的生效延时

1. 功能简介

系统启动后会进行配置恢复，配置恢复过程中由于主接口状态为 **down**，因此主接口上的路由不可达，导致备份链路被进行呼叫。配置恢复后，所有接口的状态变为 **up**，备份链路被呼叫成功。然后由于主接口路由恢复，备份链路被禁用，状态变为 **down**。为了避免系统启动后的短时间内备份链路 **up/down** 切换一次，可以配置在系统启动指定时间后动态路由备份功能才生效，在这段时间内不对路由进行监控，不对备份链路进行呼叫。

2. 配置步骤

- (1) 进入系统视图。

system-view

- (2) 配置动态路由备份功能在系统启动后的生效延时。

dialer timer warmup delay

缺省情况下，动态路由备份功能在系统启动 30 秒后生效。

一般情况下，请使用缺省情况。

1.13 拆除拨号链路

可在任意视图下执行本命令，拆除拨号链路。

dialer disconnect [interface interface-type interface-number]

1.14 DDR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 DDR 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 Dialer 接口的统计信息。

表1-1 DDR 显示和维护

操作	命令
显示接口的DDR信息	display dialer [interface interface-type interface-number]
显示Dialer接口的相关信息	display interface [dialer [interface-number]] [brief [description down]]
清除Dialer接口的统计信息	reset counters interface [dialer [interface-number]]

1.15 DDR典型配置举例

1.15.1 基于PSTN的传统DDR配置举例

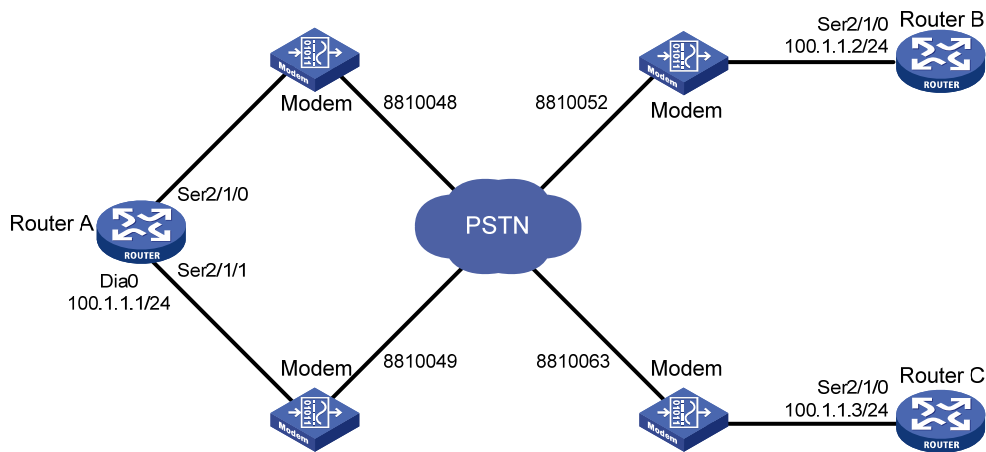
1. 组网需求

路由器 Router A、Router B 和 Router C 地址在同一网段。路由器 Router A 通过多个接口与 Router B、Router C 之间可以互相呼叫，而 Router B 和 Router C 之间不能互相呼叫。

要求使用传统 DDR 完成上述功能。

2. 组网图

图1-3 基于 PSTN 的传统 DDR 配置组网图



3. 配置步骤

(1) 配置 Router A

配置拨号访问组 1 以及对应的拨号访问控制条件。

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

配置 Dialer0 接口 IP 地址，将拨号访问组 1 与接口关联，启动传统 DDR，分别配置到达 Router B 和 Router C 的拨号串。

```
[RouterA] interface dialer 0
[RouterA-Dialer0] dialer circular enable
[RouterA-Dialer0] ip address 100.1.1.1 255.255.255.0
[RouterA-Dialer0] dialer-group 1
[RouterA-Dialer0] dialer route ip 100.1.1.2 dial-number 8810052
[RouterA-Dialer0] dialer route ip 100.1.1.3 dial-number 8810063
[RouterA-Dialer0] quit
```

配置 Serial2/1/0 接口工作在异步方式、协议模式以及使用的拨号循环组。

```
[RouterA] interface serial 2/1/0
[RouterA-Serial2/1/0] physical-mode async
[RouterA-Serial2/1/0] async-mode protocol
[RouterA-Serial2/1/0] dialer circular-group 0
[RouterA-Serial2/1/0] quit
```

配置 Serial2/1/1 接口工作在异步方式、协议模式以及使用的拨号循环组。

```
[RouterA] interface serial 2/1/1
[RouterA-Serial2/1/1] physical-mode async
[RouterA-Serial2/1/1] async-mode protocol
[RouterA-Serial2/1/1] dialer circular-group 0
[RouterA-Serial2/1/1] quit
```

配置用户线，允许 Modem 呼入和呼出。

```
[RouterA] line tty1
[RouterA-line-tty1] modem enable both
[RouterA-line-tty1] quit
[RouterA] line tty2
[RouterA-line-tty2] modem enable both
```

(2) 配置 Router B

配置拨号访问组 1 以及对应的访问控制条件。

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

配置 Serial2/1/0 接口工作在异步方式、协议模式。

```
[RouterB] interface serial 2/1/0
[RouterB-Serial2/1/0] physical-mode async
[RouterB-Serial2/1/0] async-mode protocol
```

配置 Serial2/1/0 接口 IP 地址，启动传统 DDR，配置到达对端的两个拨号串。

```
[RouterB-Serial2/1/0] ip address 100.1.1.2 255.255.255.0
[RouterB-Serial2/1/0] dialer circular enable
[RouterB-Serial2/1/0] dialer-group 1
[RouterB-Serial2/1/0] dialer route ip 100.1.1.1 dial-number 8810048
[RouterB-Serial2/1/0] dialer route ip 100.1.1.1 dial-number 8810049
[RouterB-Serial2/1/0] quit
```

配置用户线，允许 Modem 呼入和呼出。

```
[RouterB] line tty1
[RouterB-line-tty1] modem enable both
```

(3) 配置 Router C

配置拨号访问组 1 以及对应的拨号访问控制条件。

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

配置 Serial2/1/0 接口工作在异步拨号方式。

```
[RouterC] interface serial 2/1/0
[RouterC-Serial2/1/0] physical-mode async
[RouterC-Serial2/1/0] async-mode protocol
```

配置 Serial2/1/0 接口的 IP 地址，启动传统 DDR，配置到达对端的两个拨号串。

```
[RouterC-Serial2/1/0] ip address 100.1.1.3 255.255.255.0
[RouterC-Serial2/1/0] dialer circular enable
[RouterC-Serial2/1/0] dialer-group 1
[RouterC-Serial2/1/0] dialer route ip 100.1.1.1 dial-number 8810048
[RouterC-Serial2/1/0] dialer route ip 100.1.1.1 dial-number 8810049
[RouterC-Serial2/1/0] quit
```

```
# 配置用户线，允许 Modem 呼入和呼出。
```

```
[RouterC] line tty1
```

```
[RouterC-line-tty1] modem enable both
```

4. 验证配置

Router A 和 Router B、Router C 之间可以互相 ping 通，而 Router B 和 Router C 之间不能互相 ping 通。

1.15.2 基于PSTN的共享DDR配置举例

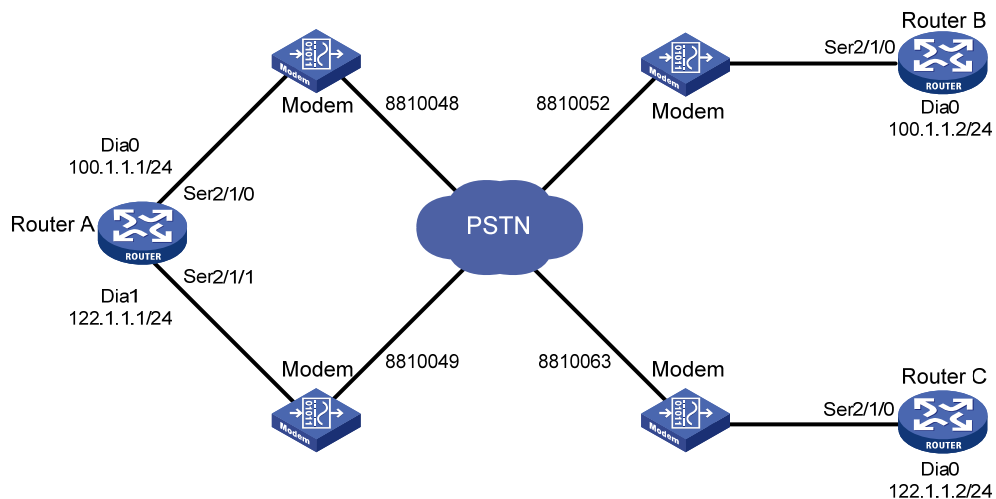
1. 组网需求

Router A、Router B 地址在同一网段，Router A 和 Router C 地址也在同一网段。路由器 Router A 通过多个接口与 Router B、Router C 之间可以互相呼叫，而 Router B 和 Router C 之间不能互相呼叫。

要求使用共享 DDR 完成上述功能。

2. 组网图

图1-4 基于 PSTN 的共享 DDR 配置组网图



3. 配置步骤

(1) 配置 Router A

```
# 配置拨号访问组 1 以及对应的拨号访问控制条件，配置 PPP 认证的本地用户 userb 和 userc。
```

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

```
[RouterA] dialer-group 1 rule ip permit
```

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

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

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

```
[RouterA-luser-network-userb] quit
```

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

```
[RouterA-luser-network-userc] password simple userc
```

```
[RouterA-luser-network-userc] service-type ppp
```

```
[RouterA-luser-network-userc] quit
```

配置 Dialer0 接口的 IP 地址，启动共享 DDR，配置允许拨入的对端用户名。

```
[RouterA] interface dialer 0
[RouterA-Dialer0] ip address 100.1.1.1 255.255.255.0
[RouterA-Dialer0] dialer bundle enable
[RouterA-Dialer0] dialer peer-name userb
```

配置 PPP 认证信息以及到达对端的拨号串（本端采用 PAP 认证对端）。

```
[RouterA-Dialer0] dialer-group 1
[RouterA-Dialer0] ppp authentication-mode pap
[RouterA-Dialer0] ppp pap local-user usera password simple usera
[RouterA-Dialer0] dialer number 8810052
[RouterA-Dialer0] quit
```

配置 Dialer1 接口的 IP 地址，启动共享 DDR，配置允许拨入的对端用户名。

```
[RouterA] interface dialer 1
[RouterA-Dialer1] ip address 122.1.1.1 255.255.255.0
[RouterA-Dialer1] dialer bundle enable
[RouterA-Dialer1] dialer peer-name userc
```

配置 PPP 认证信息以及到达对端的拨号串（本端采用 PAP 认证对端）。

```
[RouterA-Dialer1] dialer-group 1
[RouterA-Dialer1] ppp authentication-mode pap
[RouterA-Dialer1] ppp pap local-user usera password simple usera
[RouterA-Dialer1] dialer number 8810063
[RouterA-Dialer1] quit
```

配置 Serial2/1/0 接口工作在异步方式、协议模式，配置 PPP 认证信息，配置该接口属于 Dialer0 和 Dialer1。

```
[RouterA] interface serial 2/1/0
[RouterA-Serial2/1/0] physical-mode async
[RouterA-Serial2/1/0] async-mode protocol
[RouterA-Serial2/1/0] dialer bundle-member 0
[RouterA-Serial2/1/0] dialer bundle-member 1
[RouterA-Serial2/1/0] link-protocol ppp
[RouterA-Serial2/1/0] ppp authentication-mode pap
[RouterA-Serial2/1/0] ppp pap local-user usera password simple usera
[RouterA-Serial2/1/0] quit
```

配置 Serial2/1/1 接口工作在异步方式、协议模式，配置 PPP 认证信息，配置该接口属于 Dialer0 和 Dialer1。

```
[RouterA] interface serial 2/1/1
[RouterA-Serial2/1/1] physical-mode async
[RouterA-Serial2/1/1] async-mode protocol
[RouterA-Serial2/1/1] dialer bundle-member 0
[RouterA-Serial2/1/1] dialer bundle-member 1
[RouterA-Serial2/1/1] link-protocol ppp
[RouterA-Serial2/1/1] ppp authentication-mode pap
[RouterA-Serial2/1/1] ppp pap local-user usera password simple usera
[RouterA-Serial2/1/1] quit
```

配置用户线，允许 Modem 呼入和呼出。

```
[RouterA] line tty1
```

```
[RouterA-line-tty1] modem enable both
[RouterA-line-tty1] quit
[RouterA] line tty2
[RouterA-line-tty2] modem enable both
```

(2) 配置 Router B

配置拨号访问组 2 以及对应的拨号访问控制条件，配置 PPP 认证的本地用户 **usera**。

```
<RouterB> system-view
[RouterB] dialer-group 2 rule ip permit
[RouterB] local-user usera class network
[RouterB-luser-network-usera] password simple usera
[RouterB-luser-network-usera] service-type ppp
[RouterB-luser-network-usera] quit
```

配置 **Dialer0** 接口的 IP 地址，启动共享 DDR，配置 **Dialer0** 接口允许拨入的用户以及到达对端的拨号串。

```
[RouterB] interface dialer 0
[RouterB-Dialer0] ip address 100.1.1.2 255.255.255.0
[RouterB-Dialer0] dialer bundle enable
[RouterB-Dialer0] dialer peer-name usera
[RouterB-Dialer0] dialer number 8810048
```

配置 PPP 认证信息（本端采用 PAP 认证对端）。

```
[RouterB-Dialer0] dialer-group 2
[RouterB-Dialer0] ppp authentication-mode pap
[RouterB-Dialer0] ppp pap local-user userb password simple userb
[RouterB-Dialer0] quit
```

配置 **Serial2/1/0** 接口工作在异步方式、协议模式，配置 PPP 认证信息，配置该接口属于 **Dialer0**。

```
[RouterB] interface serial 2/1/0
[RouterB-Serial2/1/0] physical-mode async
[RouterB-Serial2/1/0] async-mode protocol
[RouterB-Serial2/1/0] dialer bundle-member 0
[RouterB-Serial2/1/0] link-protocol ppp
[RouterB-Serial2/1/0] ppp authentication-mode pap
[RouterB-Serial2/1/0] ppp pap local-user userb password simple userb
[RouterB-Serial2/1/0] quit
```

配置用户线，允许 **Modem** 呼入和呼出。

```
[RouterB] line tty1
[RouterB-line-tty1] modem enable both
```

(3) 配置 Router C

配置拨号访问组 1 以及对应的拨号访问控制条件，配置 PPP 认证的本地用户 **usera**。

```
<RouterC> system-view
[RouterC] dialer-group 1 rule ip permit
[RouterC] local-user usera class network
[RouterC-luser-network-usera] password simple usera
[RouterC-luser-network-usera] service-type ppp
[RouterC-luser-network-usera] quit
```


配置 Dialer0 接口的 IP 地址，启动共享 DDR，配置 Dialer0 接口允许拨入的用户以及到达对端的拨号串。

```
[RouterC] interface dialer 0
[RouterC-Dialer0] ip address 122.1.1.2 255.255.255.0
[RouterC-Dialer0] dialer bundle enable
[RouterC-Dialer0] dialer peer-name usera
[RouterC-Dialer0] dialer number 8810049
```

配置 PPP 认证信息（本端采用 PAP 认证对端）。

```
[RouterC-Dialer0] dialer-group 1
[RouterC-Dialer0] ppp authentication-mode pap
[RouterC-Dialer0] ppp pap local-user userc password simple userc
[RouterC-Dialer0] quit
```

配置 Serial2/1/0 接口工作在异步方式、协议模式，配置 PPP 认证信息，配置该接口属于 Dialer0。

```
[RouterC] interface serial 2/1/0
[RouterC-Serial2/1/0] physical-mode async
[RouterC-Serial2/1/0] async-mode protocol
[RouterC-Serial2/1/0] dialer bundle-member 0
[RouterC-Serial2/1/0] link-protocol ppp
[RouterC-Serial2/1/0] ppp authentication-mode pap
[RouterC-Serial2/1/0] ppp pap local-user userc password simple userc
[RouterC-Serial2/1/0] quit
```

配置用户线，允许 Modem 呼入和呼出。

```
[RouterC] line tty1
[RouterC-line-tty1] modem enable both
```

4. 验证配置

Router A 和 Router B、Router C 之间可以互相 ping 通，而 Router B 和 Router C 之间不能互相 ping 通。

1.15.3 基于ISDN的传统DDR配置举例

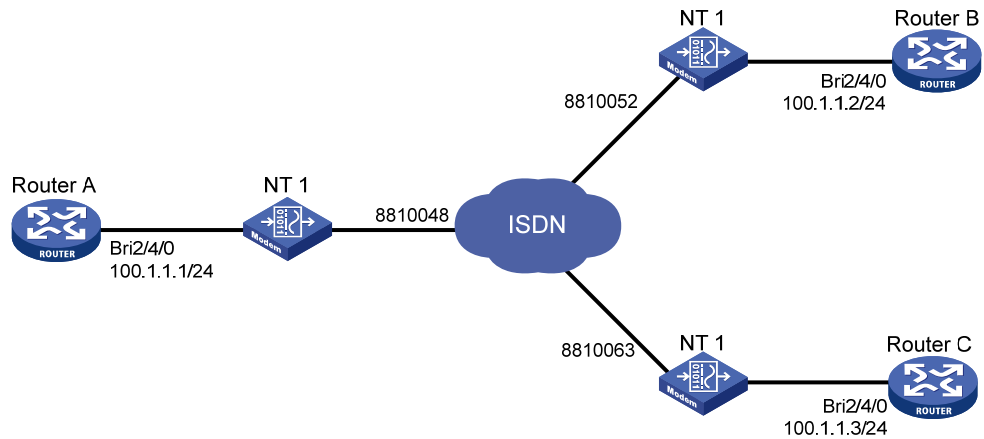
1. 组网需求

路由器 Router A、Router B 和 Router C 地址在同一网段。路由器 Router A 通过多个接口与 Router B、Router C 之间可以互相呼叫，而 Router B 和 Router C 之间不能互相呼叫。

要求使用传统 DDR 完成上述功能。

2. 组网图

图1-5 基于 ISDN 的传统 DDR 配置组网图



3. 配置步骤

(1) 配置 Router A

配置拨号访问组 1 以及对应的拨号访问控制条件。

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

```
[RouterA] dialer-group 1 rule ip permit
```

配置 BRI2/4/0 接口的 IP 地址，启动传统 DDR，配置到达对端的拨号串。

```
[RouterA] interface bri 2/4/0
```

```
[RouterA-Bri2/4/0] ip address 100.1.1.1 255.255.255.0
```

```
[RouterA-Bri2/4/0] dialer circular enable
```

```
[RouterA-Bri2/4/0] dialer-group 1
```

```
[RouterA-Bri2/4/0] dialer route ip 100.1.1.2 dial-number 8810052
```

```
[RouterA-Bri2/4/0] dialer route ip 100.1.1.3 dial-number 8810063
```

(2) 配置 Router B

配置拨号访问组 2 以及对应的拨号访问控制条件。

```
<RouterB> system-view
```

```
[RouterB] dialer-group 2 rule ip permit
```

配置 BRI2/4/0 接口的 IP 地址，启动传统 DDR，配置到达对端的拨号串。

```
[RouterB] interface bri 2/4/0
```

```
[RouterB-Bri2/4/0] ip address 100.1.1.2 255.255.255.0
```

```
[RouterB-Bri2/4/0] dialer circular enable
```

```
[RouterB-Bri2/4/0] dialer-group 2
```

```
[RouterB-Bri2/4/0] dialer route ip 100.1.1.1 dial-number 8810048
```

(3) 配置 Router C

配置拨号访问组 1 以及对应的拨号访问控制条件。

```
<RouterC> system-view
```

```
[RouterC] dialer-group 1 rule ip permit
```

配置 BRI2/4/0 接口的 IP 地址，启动传统 DDR，配置到达对端的拨号串。

```
[RouterC] interface bri 2/4/0
```

```
[RouterC-Bri2/4/0] ip address 100.1.1.3 255.255.255.0
```

```

[RouterC-Bri2/4/0] dialer circular enable
[RouterC-Bri2/4/0] dialer-group 1
[RouterC-Bri2/4/0] dialer route ip 100.1.1.1 dial-number 8810048

```

4. 验证配置

Router A 和 Router B、Router C 之间可以互相 ping 通，而 Router B 和 Router C 之间不能互相 ping 通。

1.15.4 基于ISDN的共享DDR配置举例

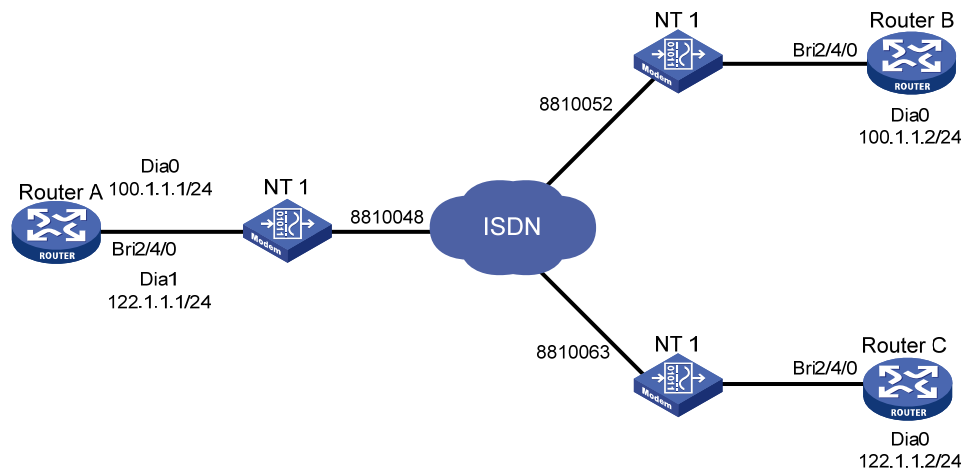
1. 组网需求

Router A、Router B 地址在同一网段，Router A 和 Router C 地址也在同一网段。路由器 Router A 通过多个接口与 Router B、Router C 之间可以互相呼叫，而 Router B 和 Router C 之间不能互相呼叫。

要求使用共享 DDR 完成上述功能。

2. 组网图

图1-6 基于 ISDN 的共享 DDR 配置组网图



3. 配置步骤

(1) 配置 Router A

配置拨号访问组 1 以及对应的拨号访问控制条件，配置 PPP 认证的本地用户 userb 和 userc。

```

<RouterA> system-view
[RouterA] dialer-group 1 rule ip permit
[RouterA] local-user userb class network
[RouterA-luser-network-userb] password simple userb
[RouterA-luser-network-userb] service-type ppp
[RouterA-luser-network-userb] quit
[RouterA] local-user userc class network
[RouterA-luser-network-userc] password simple userc
[RouterA-luser-network-userc] service-type ppp
[RouterA-luser-network-userc] quit

```

配置 Dialer0 接口的 IP 地址，启动共享 DDR，配置 Dialer0 接口允许拨入的用户。

```
[RouterA] interface dialer 0
[RouterA-Dialer0] ip address 100.1.1.1 255.255.255.0
[RouterA-Dialer0] dialer bundle enable
[RouterA-Dialer0] dialer peer-name userb
```

配置 Dialer0 接口的 PPP 认证信息以及到达对端的拨号串。

```
[RouterA-Dialer0] dialer-group 1
[RouterA-Dialer0] ppp authentication-mode pap
[RouterA-Dialer0] ppp pap local-user usera password simple usera
[RouterA-Dialer0] dialer number 8810052
[RouterA-Dialer0] quit
```

配置 Dialer1 接口的 IP 地址，启动共享 DDR，配置 Dialer1 接口允许拨入的用户。

```
[RouterA] interface dialer 1
[RouterA-Dialer1] ip address 122.1.1.1 255.255.255.0
[RouterA-Dialer1] dialer bundle enable
[RouterA-Dialer1] dialer peer-name userc
```

配置 Dialer1 接口的 PPP 认证信息以及到达对端的拨号串。

```
[RouterA-Dialer1] dialer-group 1
[RouterA-Dialer1] ppp authentication-mode pap
[RouterA-Dialer1] ppp pap local-user usera password simple usera
[RouterA-Dialer1] dialer number 8810063
[RouterA-Dialer1] quit
```

配置 BRI2/4/0 接口的 PPP 认证信息以及所属的 Dialer bundle。

```
[RouterA] interface bri 2/4/0
[RouterA-Bri2/4/0] dialer bundle-member 0
[RouterA-Bri2/4/0] dialer bundle-member 1
[RouterA-Bri2/4/0] link-protocol ppp
[RouterA-Bri2/4/0] ppp authentication-mode pap
[RouterA-Bri2/4/0] ppp pap local-user usera password simple usera
```

(2) 配置 Router B

配置拨号访问组 2 以及对应的拨号访问控制条件，配置 PPP 认证的本地用户 usera。

```
<RouterB> system-view
[RouterB] dialer-group 2 rule ip permit
[RouterB] local-user usera class network
[RouterB-luser-network-usera] password simple usera
[RouterB-luser-network-usera] service-type ppp
[RouterB-luser-network-usera] quit
```

配置 Dialer0 接口的 IP 地址，启动共享 DDR，配置接口允许拨入的用户。

```
[RouterB] interface dialer 0
[RouterB-Dialer0] ip address 100.1.1.2 255.255.255.0
[RouterB-Dialer0] dialer bundle enable
[RouterB-Dialer0] dialer peer-name usera
```

配置 Dialer0 接口的 PPP 认证信息以及到达对端的拨号串。

```
[RouterB-Dialer0] dialer-group 2
[RouterB-Dialer0] ppp authentication-mode pap
[RouterB-Dialer0] dialer number 8810048
```

```
[RouterB-Dialer0] ppp pap local-user userb password simple userb
[RouterB-Dialer0] quit
```

配置 BRI2/4/0 接口的 PPP 认证信息以及所属的 Dialer bundle。

```
[RouterB] interface bri 2/4/0
[RouterB-Bri2/4/0] dialer bundle-member 0
[RouterB-Bri2/4/0] link-protocol ppp
[RouterB-Bri2/4/0] ppp authentication-mode pap
[RouterB-Bri2/4/0] ppp pap local-user userb password simple userb
```

(3) 配置 Router C

配置拨号访问组 1 以及对应的拨号访问控制条件，配置 PPP 认证的本地用户 usera。

```
<RouterC> system-view
[RouterC] dialer-group 1 rule ip permit
[RouterC] local-user usera class network
[RouterC-luser-network-usera] password simple usera
[RouterC-luser-network-usera] service-type ppp
[RouterC-luser-network-usera] quit
```

配置 Dialer0 接口的 IP 地址，启动共享 DDR，配置接口允许拨入的用户。

```
[RouterC] interface dialer 0
[RouterC-Dialer0] ip address 122.1.1.2 255.255.255.0
[RouterC-Dialer0] dialer bundle enable
[RouterC-Dialer0] dialer peer-name usera
```

配置 Dialer0 接口的 PPP 认证信息以及到达对端的拨号串。

```
[RouterC-Dialer0] dialer-group 1
[RouterC-Dialer0] dialer number 8810048
[RouterC-Dialer0] ppp authentication-mode pap
[RouterC-Dialer0] ppp pap local-user userc password simple userc
[RouterC-Dialer0] quit
```

配置 BRI2/4/0 接口的 PPP 认证信息以及所属的 Dialer bundle。

```
[RouterC] interface bri 2/4/0
[RouterC-Bri2/4/0] dialer bundle-member 0
[RouterC-Bri2/4/0] link-protocol ppp
[RouterC-Bri2/4/0] ppp authentication-mode pap
[RouterC-Bri2/4/0] ppp pap local-user userc password simple userc
```

4. 验证配置

Router A 和 Router B、Router C 之间可以互相 ping 通，而 Router B 和 Router C 之间不能互相 ping 通。

1.15.5 DDR链路的MP捆绑配置举例

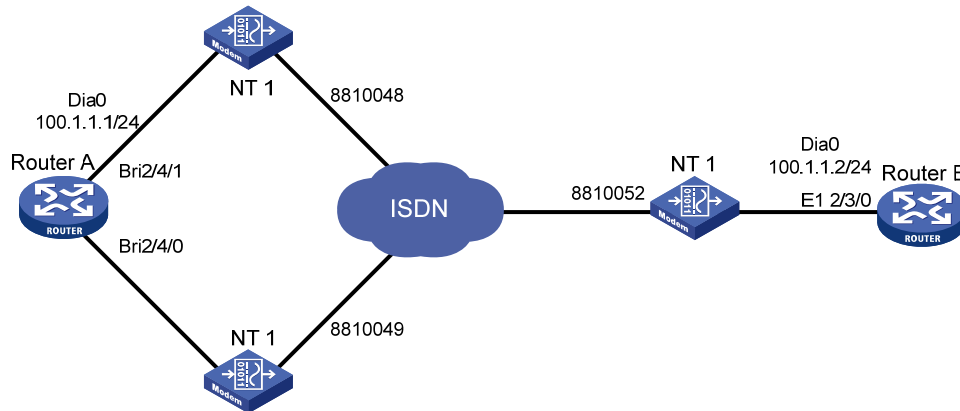
1. 组网需求

本地路由器通过两个 ISDN BRI 接口和远端连接，要求通过设定流量负载阈值来控制接口的流量分配，从而根据实际流量进行带宽分配。

如下图所示，Router A 和 Router B 之间利用 ISDN BRI 和 PRI 接口通过 ISDN 网络进行连接，要求 Router A 以共享 DDR 方式呼叫 Router B，Router B 以传统 DDR 方式呼叫 Router A。

2. 组网图

图1-7 DDR 链路的 MP 捆绑配置组网图



3. 配置步骤

(1) 配置 Router A

配置拨号访问组 1 以及对应的拨号访问控制条件，配置 PPP 认证的本地用户 userb，配置 DDR 提供流量统计信息的间隔时间为 3 秒。

```
<RouterA> system-view
[RouterA] dialer-group 1 rule ip permit
[RouterA] local-user userb class network
[RouterA-luser-network-userb] password simple userb
[RouterA-luser-network-userb] service-type ppp
[RouterA-luser-network-userb] quit
[RouterA] dialer flow-interval 3
```

配置 Dialer0 接口的 IP 地址，启动共享 DDR，配置 MP 捆绑的相关信息。

```
[RouterA] interface dialer 0
[RouterA-Dialer0] ip address 100.1.1.1 255.255.255.0
[RouterA-Dialer0] dialer bundle enable
[RouterA-Dialer0] ppp mp
[RouterA-Dialer0] dialer threshold 50
```

配置 Dialer0 接口允许拨入的用户，PPP 认证信息，以及到达对端的拨号串。

```
[RouterA-Dialer0] dialer peer-name userb
[RouterA-Dialer0] dialer-group 1
[RouterA-Dialer0] ppp authentication-mode pap
[RouterA-Dialer0] ppp pap local-user usera password simple usera
[RouterA-Dialer0] dialer number 8810052
[RouterA-Dialer0] quit
```

配置 BRI2/4/1 接口的 PPP 认证信息、所属的 Dialer bundle。

```
[RouterA] interface bri 2/4/1
[RouterA-Bri2/4/1] dialer bundle-member 0
[RouterA-Bri2/4/1] ppp mp
[RouterA-Bri2/4/1] link-protocol ppp
[RouterA-Bri2/4/1] ppp authentication-mode pap
[RouterA-Bri2/4/1] ppp pap local-user usera password simple usera
```

```
[RouterA-Bri2/4/1] quit
# 配置 BRI2/4/0 接口 PPP 认证信息、所属的 Dialer bundle。
[RouterA] interface bri 2/4/0
[RouterA-Bri2/4/0] dialer bundle-member 0
[RouterA-Bri2/4/0] ppp mp
[RouterA-Bri2/4/0] link-protocol ppp
[RouterA-Bri2/4/0] ppp authentication-mode pap
[RouterA-Bri2/4/0] ppp pap local-user usera password simple usera
```

(2) 配置 Router B

配置拨号访问组 2 以及对应的拨号访问控制条件，配置 PPP 认证的本地用户 usera，配置 DDR 提供流量统计信息的间隔时间为 3 秒。

```
<RouterB> system-view
[RouterB] dialer-group 2 rule ip permit
[RouterB] local-user usera class network
[RouterB-luser-network-usera] password simple usera
[RouterB-luser-network-usera] service-type ppp
[RouterB-luser-network-usera] quit
[RouterB] dialer flow-interval 3
```

配置 Dialer0 接口的 IP 地址、到达对端的拨号串、MP 捆绑、PPP 认证信息。

```
[RouterB] interface dialer 0
[RouterB-Dialer0] ip address 100.1.1.2 255.255.255.0
[RouterB-Dialer0] dialer circular enable
[RouterB-Dialer0] dialer-group 2
[RouterB-Dialer0] dialer route ip 100.1.1.1 dial-number 8810048
[RouterB-Dialer0] dialer route ip 100.1.1.1 dial-number 8810049
[RouterB-Dialer0] ppp mp
[RouterB-Dialer0] ppp authentication-mode pap
[RouterB-Dialer0] ppp pap local-user userb password simple userb
[RouterB-Dialer0] quit
```

配置 CE1/PRI 接口 E1 2/3/0，使其工作在 PRI 方式。

```
[RouterB] controller e1 2/3/0
[RouterB-E1 2/3/0] pri-set
[RouterB-E1 2/3/0] quit
```

在 CE1/PRI 接口 E1 2/3/0 生成的接口 Serial2/3/0:15 上配置加入拨号循环组 0 与 Dialer0 关联。

```
[RouterB] interface serial 2/3/0:15
[RouterB-Serial2/3/0:15] dialer circular-group 0
```

1.15.6 根据ISDN主叫号码进行回呼的配置举例

1. 组网需求

两台路由器在 ISDN 网络中根据 ISDN 主叫号码进行 ISDN 回呼。

如下图所示，Router A 和 Router B 之间利用 ISDN BRI 接口通过 ISDN 网络进行连接，采用传统 DDR 配置方法。规定 Router A 为回呼 Client 端，Router B 为回呼 Server 端。

2. 组网图

图1-8 根据 ISDN 主叫号码进行回呼的配置组网图



3. 配置步骤



说明

ISDN 网络中的程控交换机需要支持 ISDN 主叫号码发送功能。

(1) 配置 Router A

配置拨号访问组 1 及对应的拨号访问控制条件。

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

```
[RouterA] dialer-group 1 rule ip permit
```

配置接口 BRI2/4/0 的 IP 地址以及传统 DDR 参数，配置到达 RouterB 的拨号串。

```
[RouterA] interface bri 2/4/0
```

```
[RouterA-Bri2/4/0] ip address 100.1.1.1 255.255.255.0
```

```
[RouterA-Bri2/4/0] dialer circular enable
```

```
[RouterA-Bri2/4/0] dialer-group 1
```

```
[RouterA-Bri2/4/0] dialer route ip 100.1.1.2 dial-number 8810052
```

```
[RouterA-Bri2/4/0] dialer timer enable 15
```

配置接口 BRI2/4/0 在向被叫方发送的消息中带上 ISDN 主叫号码 8810048。

```
[RouterA-Bri2/4/0] isdn calling 8810048
```

(2) 配置 Router B

配置拨号访问组 2 及对应的拨号访问控制条件。

```
<RouterB> system-view
```

```
[RouterB] dialer-group 2 rule ip permit
```

配置接口 BRI2/4/0 的 IP 地址以及传统 DDR 参数，配置到达 RouterA 的拨号串。

```
[RouterB] interface bri 2/4/0
```

```
[RouterB-Bri2/4/0] ip address 100.1.1.2 255.255.255.0
```

```
[RouterB-Bri2/4/0] dialer circular enable
```

```
[RouterB-Bri2/4/0] dialer-group 2
```

```
[RouterB-Bri2/4/0] dialer route ip 100.1.1.1 dial-number 8810048
```

当本端识别出 ISDN 主叫号码为 8810048 时进行回呼。

```
[RouterB-Bri2/4/0] dialer call-in 8810048 callback
```

1.15.7 路由器PPP回呼路由器的配置举例

1. 组网需求

两台路由器在 PSTN 网络中通过串口实现 PPP 回呼。

如下图所示，Router A 和 Router B 利用串口通过 PSTN 网络连接，采用传统 DDR 配置方法。规定 Router A 为回呼 Client 端，Router B 为回呼 Server 端。

2. 组网图

图1-9 路由器 PPP 回呼路由器的配置组网图



3. 配置步骤（方案一）

使用传统 DDR 方法实现 PPP 回呼，Server 端按照 `dialer route` 命令配置的用户名来选择回呼 Client 端的拨号串。

(1) 配置 Router A

配置拨号访问组 1 以及对应的拨号访问控制条件。

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

```
[RouterA] dialer-group 1 rule ip permit
```

配置接口 Serial2/1/0 的 IP 地址、物理层参数以及传统 DDR 参数。

```
[RouterA] interface serial 2/1/0
```

```
[RouterA-Serial2/1/0] ip address 100.1.1.1 255.255.255.0
```

```
[RouterA-Serial2/1/0] physical-mode async
```

```
[RouterA-Serial2/1/0] async-mode protocol
```

```
[RouterA-Serial2/1/0] dialer circular enable
```

```
[RouterA-Serial2/1/0] dialer-group 1
```

```
[RouterA-Serial2/1/0] dialer route ip 100.1.1.2 dial-number 8810052
```

```
[RouterA-Serial2/1/0] link-protocol ppp
```

```
[RouterA-Serial2/1/0] ppp pap local-user usera password simple usera
```

配置接口 Serial2/1/0 作为回呼 Client 端。

```
[RouterA-Serial2/1/0] ppp callback client
```

```
[RouterA-Serial2/1/0] dialer timer enable 15
```

```
[RouterA-Serial2/1/0] quit
```

配置用户线，允许 Modem 呼入和呼出。

```
[RouterA] line tty1
```

```
[RouterA-line-tty1] modem enable both
```

(2) 配置 Router B

配置拨号访问组 2 以及对应的拨号访问控制条件，配置 PPP 认证的本地用户名 usera。

```
<RouterB> system-view
```

```
[RouterB] dialer-group 2 rule ip permit
```

```
[RouterB] local-user usera class network
```

```
[RouterB-luser-network-usera] password simple usera
```

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

```
[RouterB-luser-network-usera] quit
```

配置接口 Serial2/1/0 的 IP 地址、物理层参数以及传统 DDR 参数。

```
[RouterB] interface serial 2/1/0
```

```

[RouterB-Serial2/1/0] ip address 100.1.1.2 255.255.255.0
[RouterB-Serial2/1/0] physical-mode async
[RouterB-Serial2/1/0] async-mode protocol
[RouterB-Serial2/1/0] dialer circular enable
[RouterB-Serial2/1/0] dialer-group 2
[RouterB-Serial2/1/0] link-protocol ppp
[RouterB-Serial2/1/0] ppp authentication-mode pap
# 配置本端作为回呼 Server，回呼方式为 user，根据 dialer route 命令中配置的用户名
对应的拨号串进行回呼。
[RouterB-Serial2/1/0] dialer callback-center user
[RouterB-Serial2/1/0] dialer route ip 100.1.1.1 dial-number 8810048 user usera
[RouterB-Serial2/1/0] ppp callback server
[RouterB-Serial2/1/0] quit
# 配置用户线，允许 Modem 呼入和呼出。
[RouterB] line tty2
[RouterB-line-tty2] modem enable both

```

4. 配置步骤（方案二）

使用传统 DDR 方法实现 PPP 回呼，Server 端根据 PPP 认证中接收的对端用户名查找本地用户表确定回呼的拨号串。

(1) 配置 Router A

```

# 配置拨号访问组 1 以及对应的拨号访问控制条件。
<RouterA> system-view
[RouterA] dialer-group 1 rule ip permit
# 配置接口 Serial2/1/0 的 IP 地址、物理层参数以及传统 DDR 参数。
[RouterA] interface serial 2/1/0
[RouterA-Serial2/1/0] ip address 100.1.1.1 255.255.255.0
[RouterA-Serial2/1/0] physical-mode async
[RouterA-Serial2/1/0] async-mode protocol
[RouterA-Serial2/1/0] dialer circular enable
[RouterA-Serial2/1/0] dialer-group 1
[RouterA-Serial2/1/0] dialer route ip 100.1.1.2 dial-number 8810052
[RouterA-Serial2/1/0] link-protocol ppp
[RouterA-Serial2/1/0] ppp pap local-user usera password simple usera
# 配置接口 Serial2/1/0 作为回呼 Client 端。
[RouterA-Serial2/1/0] ppp callback client
[RouterA-Serial2/1/0] dialer timer enable 15
[RouterA-Serial2/1/0] quit
# 配置用户线，允许 Modem 呼入和呼出。
[RouterA] line tty1
[RouterA-line-tty1] modem enable both

```

(2) 配置 Router B

```

# 配置拨号访问组 2 及对应的拨号访问控制条件，配置 PPP 认证的本地用户名 usera 以及对
应的拨号串。
<RouterB> system-view
[RouterB] dialer-group 2 rule ip permit

```

```

[RouterB] local-user usera class network
[RouterB-luser-network-usera] password simple usera
[RouterB-luser-network-usera] service-type ppp
[RouterB-luser-network-usera] authorization-attribute callback-number 8810048
[RouterB-luser-network-usera] quit
# 配置接口 Serial2/1/0 的 IP 地址、物理层参数以及传统 DDR 参数。
[RouterB] interface serial 2/1/0
[RouterB-Serial2/1/0] ip address 100.1.1.2 255.255.255.0
[RouterB-Serial2/1/0] physical-mode async
[RouterB-Serial2/1/0] async-mode protocol
[RouterB-Serial2/1/0] dialer circular enable
[RouterB-Serial2/1/0] dialer-group 2
# 配置本端作为回呼 Server，回呼方式为 dial-number，根据 PPP 认证中接收的对端用户名查找本地用户表确定回呼的拨号串。
[RouterB-Serial2/1/0] dialer callback-center dial-number
[RouterB-Serial2/1/0] link-protocol ppp
[RouterB-Serial2/1/0] ppp authentication-mode pap
[RouterB-Serial2/1/0] ppp callback server
[RouterB-Serial2/1/0] quit
# 配置用户线，允许 Modem 呼入和呼出。
[RouterB] line tty2
[RouterB-line-tty2] modem enable both

```

1.15.8 路由器PPP回呼PC机的配置举例

1. 组网需求

Router 和 PC 机在 PSTN 网络中通过串口实现 PPP 回呼。如下图所示，PC 机借助 Modem 与路由器 Router 在 PSTN 网络中连接，采用传统 DDR 配置方法。规定 PC 机为回呼 Client 端，Router 为回呼 Server 端，根据 **dialer route** 命令配置进行回呼。Router 地址为 100.1.1.1/24，PC 机接受由 Router 分配的地址。

2. 组网图

图1-10 路由器 PPP 回呼 PC 机的配置组网图



3. 配置步骤

(1) 配置 PC 机（以 Windows XP 为例）

在 Windows XP 系统的 PC 上建立一个拨号网络连接，该连接具有“呼叫回拨”的能力。

- a. 配置 PC 机连接的 Modem 为“自动应答方式”，然后打开[开始/程序/附件/通讯/网络连接]，在“网络连接”窗口中，单击[创建一个新的连接]；

- b. 或者右键单击网上邻居，选择“属性”，打开“网络连接”对话框，单击[新建一个连接]，出现新建连接向导对话框。
- c. 单击“下一步”，出现“网络连接类型”对话框，选择第一项“连接到 Internet”。
- d. 单击“下一步”，进入“您想怎样连接到 Internet”对话框，选择第二项“手动设置我的连接”。
- e. 单击“下一步”，进入“Internet 连接”对话框，选择“用拨号调制解调器连接”。单击“下一步”，进入“连接名”对话框，设置该连接的连接名。单击“下一步”，进入“要拨的电话号码”，设置拨叫回呼 Server 端的电话号码。单击“下一步”，进入“Internet 账户信息”，设置连接到 Server 端进行 PPP 认证时的用户名和密码。
- f. 单击“下一步”，进入“完成新建连接向导”对话框，完成该连接的创建。
- g. 在“网络连接”对话框中，在刚才新创建的连接上单击右键，选择“属性”，打开连接属性对话框，选择“网络”选项。在“我正在呼叫的拨号服务器类型”下拉框中选择“PPP”，单击“设置”按钮，选择[启用 LCP 扩展]选项，取消[启用软件压缩]选项，取消[为单链路连接协商多重链接]选项，其他设置为缺省值，单击“确认”按钮，完成设置。
- h. 返回“网络连接”对话框，选中刚才新创建的连接，选择[高级/拨号首选项]菜单，打开“拨号首选项”对话框，选择“回拨”选项卡。如果选择“不回拨”，当 Client 端向 Server 端拨号认证身份后，Server 端将不回拨，保持现有连接，Client 端机可以直接访问局域网或者通过局域网访问互联网。如果选择“当服务器提供回拨时在拨号期间询问我”（需要用户输入一个回拨号码），或者选择“总是按以下号码回拨”（设置一个固定的回拨号码），Server 端将使用用户输入的回拨号码或者设置好的回拨号码回拨 Client 端。

(2) 配置 Router

配置拨号访问组 1 及对应的拨号访问控制条件，配置 PPP 认证使用的本地用户 userpc。

```
<Router> system-view
[Router] dialer-group 1 rule ip permit
[Router] local-user userpc class network
[Router-luser-network-userpc] password simple userpc
[Router-luser-network-userpc] service-type ppp
[Router-luser-network-userpc] quit
```

配置接口 Serial2/1/0 的物理层参数以及 IP 地址。

```
[Router] interface serial 2/1/0
[Router-Serial2/1/0] ip address 100.1.1.1 255.255.255.0
[Router-Serial2/1/0] physical-mode async
[Router-Serial2/1/0] async-mode protocol
```

配置接口 Serial2/1/0 的链路层协议为 PPP，配置 PPP 的相关参数。

```
[Router-Serial2/1/0] link-protocol ppp
[Router-Serial2/1/0] ppp authentication-mode pap
[Router-Serial2/1/0] ppp pap local-user Router password simple Router
```

配置接口 Serial2/1/0 为对端分配 IP 地址。

```
[Router-Serial2/1/0] remote address 100.1.1.2
```

配置接口 Serial2/1/0 作为 PPP 回呼的 Server 端，回呼方式为 user，根据 dialer route 命令中配置的用户名对应的拨号串进行回呼。

```
[Router-Serial2/1/0] ppp callback server
[Router-Serial2/1/0] dialer callback-center user
```

```

# 配置接口 Serial2/1/0 启动传统 DDR，并且配置传统 DDR 参数。
[Router-Serial2/1/0] dialer circular enable
[Router-Serial2/1/0] dialer-group 1
[Router-Serial2/1/0] dialer route ip 100.1.1.2 dial-number 8810048 user userpc
[Router-Serial2/1/0] quit
# 配置用户线，允许 Modem 呼入和呼出。
[Router] line tty1
[Router-line-tty1] modem enable both

```

1.15.9 NT服务器PPP回呼路由器的配置举例

1. 组网需求

Router 和 NT 服务器在 PSTN 网络中通过串口实现 PPP 回呼。

如下图所示，Router 与 NT 服务器借助 Modem 在 PSTN 网络中连接，采用传统 DDR 配置方法。规定 Router 为回呼 Client 端，NT 服务器为回呼 Server 端，根据 **dialer route** 命令配置进行回呼。NT 服务器地址为 100.1.1.254/24，Router 地址接受由 NT 服务器分配的地址。

2. 组网图

图1-11 NT 服务器 PPP 回呼路由器的配置组网图



3. 配置步骤

(1) 配置 Router

配置拨号访问组 1 及对应的拨号访问控制条件，配置 PPP 认证使用的本地用户 usernt。

```

<Router> system-view
[Router] dialer-group 1 rule ip permit
[Router] local-user usernt class network
[Router-luser-network-userc] password simple usernt
[Router-luser-network-userc] service-type ppp
[Router-luser-network-userc] quit

```

配置接口 Serial2/1/0 的物理层参数。

```

[Router] interface serial 2/1/0
[Router-Serial2/1/0] physical-mode async
[Router-Serial2/1/0] async-mode protocol

```

配置接口 Serial2/1/0 的链路层协议为 PPP 以及 PPP 的相关参数。

```

[Router-Serial2/1/0] link-protocol ppp
[Router-Serial2/1/0] ppp authentication-mode pap
[Router-Serial2/1/0] ppp pap local-user Router password simple Router

```

配置接口 Serial2/1/0 的 IP 地址可协商属性。

```

[Router-Serial2/1/0] ip address ppp-negotiate

```

配置接口 Serial2/1/0 作为 PPP 回呼的 Client 端。

```

[Router-Serial2/1/0] ppp callback client
[Router-Serial2/1/0] dialer timer enable 15
# 配置接口 Serial2/1/0 启动传统 DDR，并且配置传统 DDR 参数。
[Router-Serial2/1/0] dialer circular enable
[Router-Serial2/1/0] dialer-group 1
[Router-Serial2/1/0] dialer route ip 100.1.1.254 dial-number 8810052
[Router-Serial2/1/0] quit
# 配置用户线，允许 Modem 呼入和呼出。
[Router] line tty1
[Router-line-tty1] modem enable both

```

(2) 配置 NT 服务器

Server 端可以用 Windows 2000 或 Windows XP，因为微软只在 Windows 2000 以后的操作系统中才加入了网络服务的模块，而在以前的（如 Windows 98）操作系统中没有该模块。

Server 端设置（以 Windows XP 为例）的目的是建立一个拨号网络连接，其连接具有“呼叫回拨”的能力。

- a. 右键单击“网上邻居”，选择[属性]菜单项，然后单击“新建一个连接”，用户将看到“新建连接向导”对话框。
- b. 单击“下一步”，用户将看到“网络连接类型”对话框，选择第四项“设置高级连接”。
- c. 单击“下一步”，进入“高级连接选项”对话框，选择第一项“接受传入的连接”。
- d. 单击“下一步”，进入“传入的虚拟专用网（VPN）连接”对话框，如果此服务器连接在 Internet 上，那么它可以提供给客户机连接 Internet 的请求，此时选择“允许虚拟专用连接”，否则选择“不允许虚拟专用连接”。
- e. 单击“下一步”，进入“用户权限”对话框，在此对话框中设置允许呼叫回拨的客户机的用户名及口令。单击“添加”按钮，进入“新用户”对话框，输入需要的用户名和口令后然后单击“确定”。用户将在对话框中看到新添加的用户名。然后，单击新建的用户名，单击“属性”，用户将看到“常规”项和“回拨”项，“常规”内为用户已经设置的用户名及密码，不需要改动，下面来设置“回拨”项。
- f. 选择“不允许回拨”，当客户机向服务器拨号时，认证身份后，服务器将不回拨，保持现有连接，客户机可以直接访问局域网以及通过局域网访问互联网。
- g. 选择“允许呼叫方设置回拨号码”，那么当客户机向服务器拨号时，认证身份后，服务器将自动断开连接，等待几秒后自动向客户机所在的电话拨号。选择此种方式则需要路由器上配置 `ppp callback ntstring dial-number` 命令。“不允许回拨”选项与“允许呼叫方设置回拨号码”选项效果上是没有区别的，惟一的区别就在于电话费，若选择第一项，电话费将由客户机端电话支付，若选择第二项，电话费将由服务器端电话支付。
- h. 选择第三项“总是使用下面的回拨号码”，设置一个固定的回拨号码。
- i. 单击“下一步”，进入“网络软件”窗口，设置网络组件。对于网络协议使用默认即可。
- j. 单击“下一步”，进入“完成新建连接向导”窗口，完成该连接的创建。

1.15.10 拨号串循环备份并提供Internet接入服务的配置举例

1. 组网需求

在 PSTN 网络中，拨号侧 Router A 通过配置 `dialer route` 命令实现拨号串循环备份；接入侧 Router B 使用异步串口提供 DDR 拨号的接入服务，并采用 PAP 认证方式认证拨号侧的合法性。在 ISDN 网络中，使用单一串拨号，采用 CHAP 认证，其它配置与 PSTN 侧相似。

如下图所示，Router B 和 Router D 提供接入服务器功能，拨号侧路由器 Router A 和 Router C 接受对端分配的协商地址。可供分配的地址池地址为 100.1.1.1/24~100.1.1.16/24，Router B 和 Router D 的地址为 100.1.1.254/24，从电信局得到的 PSTN 拨号串资源为 8810048~8810055，ISDN 拨号串为 8810048，共服务于 16 个上网用户。

2. 组网图

图1-12 拨号串循环备份并提供 Internet 接入服务的配置组网图（PSTN 方式）

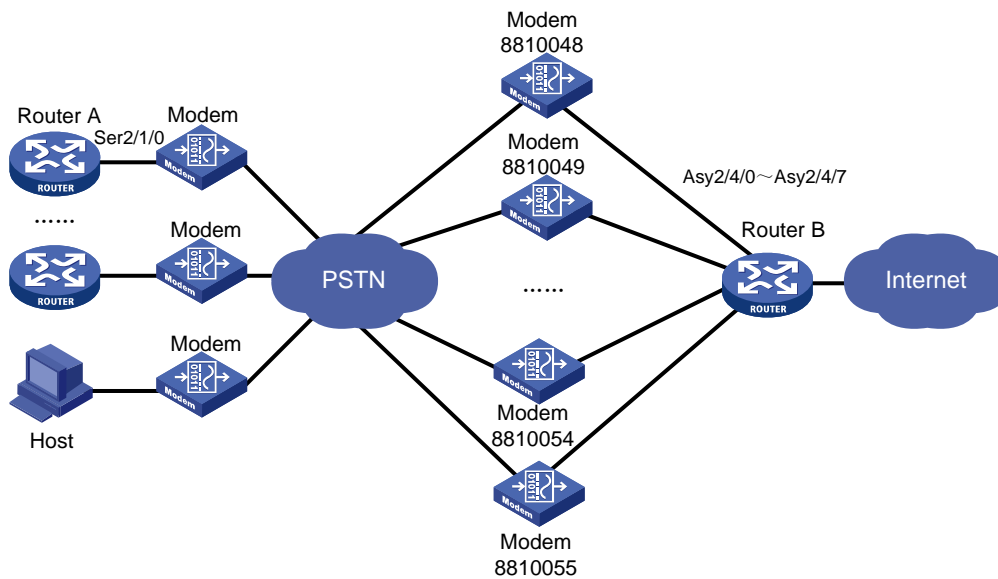
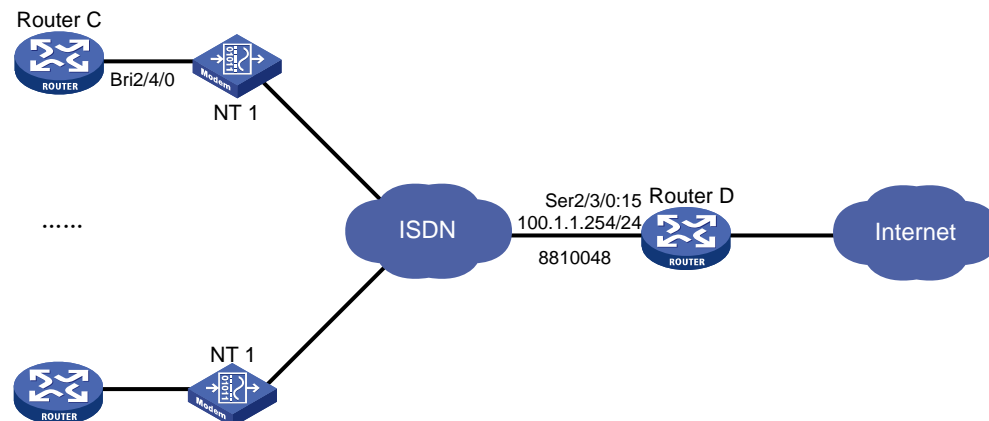


图1-13 拨号串循环备份并提供 Internet 接入服务的配置组网图（ISDN 方式）



3. 配置步骤（方案一）

拨号侧 Router A 配置拨号串循环备份；接入侧 Router B 配置使用传统 DDR 方法通过 8 异步串口建立连接，在 Dialer 接口上配置 DDR 参数。

(1) 配置 Router A

配置拨号访问组 1 及对应的拨号访问控制条件，配置 PPP 认证使用的本地用户 userb。

```
<RouterA> system-view
[RouterA] dialer-group 1 rule ip permit
[RouterA] local-user userb class network
[RouterA-luser-network-userb] password simple userb
[RouterA-luser-network-userb] service-type ppp
[RouterA-luser-network-userb] quit
```

配置接口 Serial2/1/0 的物理层参数以及 IP 地址可协商属性。

```
[RouterA] interface serial 2/1/0
[RouterA-Serial2/1/0] physical-mode async
[RouterA-Serial2/1/0] async-mode protocol
[RouterA-Serial2/1/0] ip address ppp-negotiate
```

配置接口 Serial2/1/0 的链路层协议为 PPP，配置 PPP 认证的相关参数。

```
[RouterA-Serial2/1/0] link-protocol ppp
[RouterA-Serial2/1/0] ppp authentication-mode pap
[RouterA-Serial2/1/0] ppp pap local-user user1 password simple user1
```

配置接口 Serial2/1/0 启动传统 DDR，并且配置传统 DDR 参数以及到达 RouterB 的 9 个拨号串，实现拨号串循环备份。

```
[RouterA-Serial2/1/0] dialer circular enable
[RouterA-Serial2/1/0] dialer-group 1
[RouterA-Serial2/1/0] dialer route ip 100.1.1.254 dial-number 8810048
[RouterA-Serial2/1/0] dialer route ip 100.1.1.254 dial-number 8810049
.....
[RouterA-Serial2/1/0] dialer route ip 100.1.1.254 dial-number 8810055
[RouterA-Serial2/1/0] quit
```

配置用户线，允许 Modem 呼入和呼出。

```
[RouterA] line tty1
[RouterA-line-tty1] modem enable both
```

(2) 配置 RouterB

配置拨号访问组 2 及对应的拨号访问控制条件，配置 PPP 认证使用的本地用户 user1、user2、user3、……、user16。

```
<RouterB> system-view
[RouterB] dialer-group 2 rule ip permit
[RouterB] local-user user1 class network
[RouterB-luser-network-user1] password simple user1
[RouterB-luser-network-user1] service-type ppp
[RouterB-luser-network-user1] quit
[RouterB] local-user user2 class network
[RouterB-luser-network-user2] password simple user2
[RouterB-luser-network-user2] service-type ppp
[RouterB-luser-network-user2] quit
```



```

.....
[RouterB] local-user user16 class network
[RouterB-luser-network-user16] password simple user16
[RouterB-luser-network-user16] service-type ppp
[RouterB-luser-network-user16] quit
# 配置拨号接口 Dialer0 的 IP 地址，并且将为 PPP 对端分配 IP 地址。
[RouterB] interface dialer 0
[RouterB-Dialer0] link-protocol ppp
[RouterB-Dialer0] ppp authentication-mode pap
[RouterB-Dialer0] ppp pap local-user userb password simple userb
[RouterB-Dialer0] ip address 100.1.1.254 255.255.255.0
[RouterB-Dialer0] remote address pool 1
# 配置拨号接口 Dialer0 启动传统 DDR，并且配置传统 DDR 参数。
[RouterB-Dialer0] dialer circular enable
[RouterB-Dialer0] dialer-group 2
[RouterB-Dialer0] quit
# 配置接口 Async2/4/0 的物理层以及链路层参数。
[RouterB] interface async 2/4/0
[RouterB-Async2/4/0] async-mode protocol
[RouterB-Async2/4/0] dialer circular-group 0
[RouterB-Async2/4/0] link-protocol ppp
[RouterB-Async2/4/0] ppp authentication-mode pap
[RouterB-Async2/4/0] ppp pap local-user userb password simple userb
[RouterB-Async2/4/0] quit
# 配置接口 Async2/4/1~Async2/4/7 的物理层以及链路层参数，配置方法同配置接口
Async2/4/0，配置步骤略。
# 配置接口 Async2/4/0~接口 Async2/4/7 对应的用户线 tty1~tty7，允许 Modem 呼入和呼
出。
[RouterB] line tty1
[RouterB-line-tty1] modem enable both
[RouterB-line-tty1] quit
[RouterB] line tty2
[RouterB-line-tty2] modem enable both
.....
[RouterB-line-tty8] quit
# 配置为 PPP 对端分配 IP 地址时使用的地址池。
[RouterB] domain system
[RouterB-isp-system] ip pool 1 100.1.1.1 100.1.1.16
[RouterB-isp-system] quit

```

(3) 配置用户 PC

在 Windows XP 系统的 PC 上建立一个拨号网络连接。

- a. 配置 PC 机连接的 Modem 为“自动应答方式”，然后打开[开始/程序/附件/通讯/拨号网络]，在“拨号网络”窗口中，单击[建立新连接]。
- b. 或者右键单击网上邻居，选择“属性”，打开“网络连接”对话框，单击新建一个连接，出现新建连接向导对话框。

- c. 单击“下一步”，出现“网络连接类型”对话框，选择第一项“连接到 Internet”。
- d. 单击“下一步”，进入“您想怎样连接到 Internet”对话框，选择第二项“手动设置我的连接”。
- e. 单击“下一步”，进入“Internet 连接”对话框，选择“用拨号调制解调器连接”。单击“下一步”，进入“连接名”对话框，设置该连接的连接名。单击“下一步”，进入“要拨的电话号码”，设置拨叫回呼 Server 端的电话号码。单击“下一步”，进入“Internet 账户信息”，设置连接到 Server 端进行 PPP 认证时的用户名和密码（用户名 user16，口令 user16）。
- f. 单击“下一步”，进入“完成新建连接向导”对话框，完成该连接的创建。
- g. 在“网络连接”对话框中，在刚才新创建的连接上单击右键，选择“属性”，打开连接属性对话框，选择“网络”选项。在“我正在呼叫的拨号服务器类型”下拉框中选择“PPP”，单击“设置”按钮，进行如下操作，选择[启用 LCP 扩展]选项，取消[启用软件压缩]选项，取消[为单链路连接协商多重链接]选项，其他设置为缺省值，单击“确认”按钮，完成设置。
- h. 返回“网络连接”对话框，选中刚才新创建的连接，选择[高级/拨号首选项]菜单，打开“拨号首选项”对话框，选择“回拨”选项卡，设置为“不回拨”。
- i. 双击刚才新创建的连接，就可以开始拨号了。

4. 配置步骤（方案二）

拨号侧 Router C 使用单一拨号串；接入侧 Router D 使用传统 DDR 方法通过 ISDN PRI 接口建立连接，在 Dialer 接口上配置 DDR 参数。

(1) 配置 Router C

配置拨号访问组 1 及对应的拨号访问控制条件，配置 PPP 认证使用的本地用户 userd。

```
<RouterC> system-view
[RouterC] dialer-group 1 rule ip permit
[RouterC] local-user userd class network
[RouterC-luser-network-userd] password simple user1
[RouterC-luser-network-userd] service-type ppp
[RouterC-luser-network-userd] quit
```

配置接口 BRI2/4/0 的物理层参数以及 IP 地址可协商属性。

```
[RouterC] interface bri 2/4/0
[RouterC-Bri2/4/0] ip address ppp-negotiate
```

配置接口 BRI2/4/0 的链路层协议为 PPP，配置 PPP CHAP 认证的相关参数。

```
[RouterC-Bri2/4/0] link-protocol ppp
[RouterC-Bri2/4/0] ppp authentication-mode chap
[RouterC-Bri2/4/0] ppp chap user user1
```

配置接口 BRI2/4/0 启动传统 DDR，并且配置传统 DDR 参数以及到达 RouterD 的拨号串。

```
[RouterC-Bri2/4/0] dialer circular enable
[RouterC-Bri2/4/0] dialer-group 1
[RouterC-Bri2/4/0] dialer route ip 100.1.1.254 dial-number 8810048
```

(2) 配置 Router D

配置拨号访问组 2 及对应的拨号访问控制条件，配置 PPP CHAP 认证使用的本地用户 user1、user2、user3、……、user16。

```

<RouterD> system-view
[RouterD] dialer-group 2 rule ip permit
[RouterD] local-user user1 class network
[RouterD-luser-network-user1] password simple user1
[RouterD-luser-network-user1] service-type ppp
[RouterD-luser-network-user1] quit
[RouterD] local-user user2 class network
[RouterD-luser-network-user2] password simple user1
[RouterD-luser-network-user2] service-type ppp
[RouterD-luser-network-user2] quit
.....
[RouterD] local-user user16 class network
[RouterD-luser-network-user16] password simple user1
[RouterD-luser-network-user16] service-type ppp
[RouterD-luser-network-user16] quit
# 配置 CE1/PRI 接口 2/3/0，使其工作在 PRI 方式。
[RouterD] controller e1 2/3/0
[RouterD-E1 2/3/0] pri-set
[RouterD-E1 2/3/0] quit
# 在 CE1/PRI 接口 2/3/0 生成的接口 Serial2/3/0:15 上启动传统 DDR。
[RouterD-E1 2/3/0] interface serial 2/3/0:15
[RouterD-Serial2/3/0:15] dialer circular enable
[RouterD-Serial2/3/0:15] dialer-group 2
# 配置接口 Serial2/3/0:15 的 IP 地址。
[RouterD-Serial2/3/0:15] ip address 100.1.1.254 255.255.255.0
# 配置接口 Serial2/3/0:15 的链路层协议为 PPP，并且配置 PPP 的相关参数。
[RouterD-Serial2/3/0:15] link-protocol ppp
[RouterD-Serial2/3/0:15] ppp authentication-mode chap
[RouterD-Serial2/3/0:15] ppp chap user userd
[RouterD-Serial2/3/0:15] remote address pool 1
[RouterD-Serial2/3/0:15] quit
# 配置为 PPP 对端分配 IP 地址时使用的地址池。
[RouterD] domain system
[RouterD-isp-system] ip pool 1 100.1.1.1 100.1.1.16
[RouterD-isp-system] quit

```

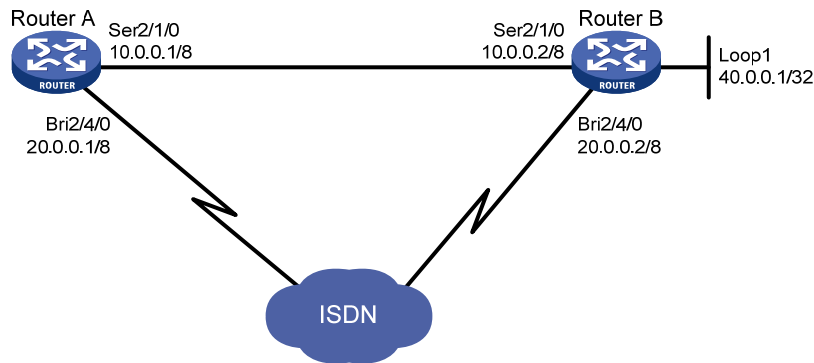
1.15.11 通过传统DDR实现动态路由备份配置举例

1. 组网需求

- Router A 与 Router B 通过一个串口直接相连，运行 PPP 协议。
- Router A 与 Router B 通过 ISDN BRI 接口与 ISDN 交换网相连，它们之间通过传统 DDR 可以互相拨号呼叫，Router B 的电话号码为 8810052。
- Router A 上配置动态路由备份功能，监控 Router B 上的 40.0.0.0/8 网段。
- 正常时候 PPP 链路作为 Router A 与 Router B 之间的主用链路；当到达 Router B 的 40.0.0.0/8 网段的路由断掉时（如 PPP 网络出现故障），Router A 自动拨起 ISDN BRI 线路。

2. 组网图

图1-14 通过传统 DDR 实现动态路由备份配置组网图



3. 配置步骤

(1) 配置 Router A

配置拨号访问组 1 以及对应的拨号访问控制条件。

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

配置 BRI2/4/0 接口拨号参数。

```
[RouterA] interface bri 2/4/0
[RouterA-Bri2/4/0] ip address 20.0.0.1 8
[RouterA-Bri2/4/0] dialer circular enable
[RouterA-Bri2/4/0] dialer-group 1
[RouterA-Bri2/4/0] dialer route ip 40.0.0.1 dial-number 8810052
[RouterA-Bri2/4/0] quit
```

配置 Serial2/1/0。

```
[RouterA] interface serial 2/1/0
[RouterA-Serial2/1/0] link-protocol ppp
[RouterA-Serial2/1/0] ip address 10.0.0.1 8
[RouterA-Serial2/1/0] quit
```

配置动态路由协议 OSPF。

```
[RouterA] ospf
[RouterA-ospf-1] area 0
[RouterA-ospf-1-area-0.0.0.0] network 10.0.0.0 0.255.255.255
[RouterA-ospf-1-area-0.0.0.0] network 20.0.0.0 0.255.255.255
[RouterA-ospf-1-area-0.0.0.0] quit
[RouterB-ospf-1] import-route direct
[RouterA-ospf-1] quit
```

创建动态备份路由组。

```
[RouterA] standby routing-group 1 rule ip 40.0.0.1 32
```

配置拨号接口上的路由使用优先级比串口的低。

```
[RouterA] interface bri 2/4/0
[RouterA-Bri2/4/0] ospf cost 2000
[RouterA-Bri2/4/0] ospf network-type broadcast
```

启用动态路由备份功能。

```
[RouterA-Bri2/4/0] standby routing-group 1
```

(2) 配置 Router B

配置拨号访问组 1 以及对应的拨号访问控制条件。

```
<RouterB> system-view
```

```
[RouterB] dialer-group 1 rule ip permit
```

配置 BRI2/4/0 接口拨号参数。

```
[RouterB] interface bri 2/4/0
```

```
[RouterB-Bri2/4/0] ip address 20.0.0.2 8
```

```
[RouterB-Bri2/4/0] dialer circular enable
```

```
[RouterB-Bri2/4/0] dialer-group 1
```

```
[RouterB-Bri2/4/0] quit
```

配置 Serial2/1/0。

```
[RouterB] interface serial 2/1/0
```

```
[RouterB-Serial2/1/0] link-protocol ppp
```

```
[RouterB-Serial2/1/0] ip address 10.0.0.2 8
```

```
[RouterB-Serial2/1/0] quit
```

配置 Loopback1 接口。

```
[RouterB] interface loopback 1
```

```
[RouterB-Loopback1] ip address 40.0.0.1 32
```

```
[RouterB-Loopback1] quit
```

配置动态路由协议 OSPF。

```
[RouterB] ospf
```

```
[RouterB-ospf-1] area 0
```

```
[RouterB-ospf-1-area-0.0.0.0] network 10.0.0.0 0.255.255.255
```

```
[RouterB-ospf-1-area-0.0.0.0] network 20.0.0.0 0.255.255.255
```

```
[RouterB-ospf-1-area-0.0.0.0] network 40.0.0.0 0.0.0.0
```

```
[RouterB-ospf-1-area-0.0.0.0] quit
```

```
[RouterB-ospf-1] import-route direct
```

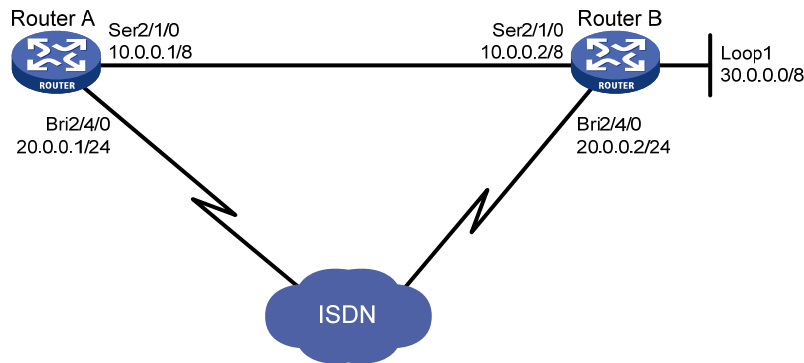
1.15.12 通过共享DDR实现动态路由备份配置举例

1. 组网需求

- Router A 与 Router B 通过一个串口直接相连，运行 PPP 协议。
- Router A 和 Router B 通过 ISDN BRI 接口与 ISDN 交换网相连，它们之间通过共享 DDR 可以互相拨号呼叫。Router A 的电话号码为 8810010，Router B 的电话号码为 8810052。
- Router A 上配置动态路由备份功能，监控 Router B 上的 30.0.0.0/8 网段。
- 正常时候 PPP 链路作为 Router A 与 Router B 之间的主用链路；当到达 Router B 的 30.0.0.0/8 网段的路由断掉时（如 PPP 网络出现故障），Router A 自动拨起 ISDN BRI 线路。

2. 组网图

图1-15 通过共享 DDR 实现动态路由备份配置组网图



3. 配置步骤

(1) 配置 Router A

配置拨号访问控制条件及本地用户数据库。

```
<RouterA> system-view
[RouterA] dialer-group 1 rule ip permit
[RouterA] local-user userb class network
[RouterA-luser-network-userb] password simple userb
[RouterA-luser-network-userb] service-type ppp
[RouterA-luser-network-userb] quit
```

创建动态路由备份组。

```
[RouterA] standby routing-group 1 rule ip 30.0.0.1 32
```

在 Dialer0 口上配置共享 DDR。

```
[RouterA] interface dialer 0
[RouterA-Dialer0] link-protocol ppp
[RouterA-Dialer0] ip address 20.0.0.1 24
[RouterA-Dialer0] dialer bundle enable
[RouterA-Dialer0] dialer peer-name userb
[RouterA-Dialer0] dialer-group 1
[RouterA-Dialer0] dialer number 8810052
[RouterA-Dialer0] ppp authentication-mode pap
[RouterA-Dialer0] ppp pap local-user usera password simple usera
[RouterA-Dialer0] standby routing-group 1
[RouterA-Dialer0] quit
```

将 BRI2/4/0 接口与 Dialer0 捆绑。

```
[RouterA] interface bri 2/4/0
[RouterA-Bri2/4/0] dialer bundle-member 0
[RouterA-Bri2/4/0] ppp authentication-mode pap
[RouterA-Bri2/4/0] ppp pap local-user usera password simple usera
[RouterA-Bri2/4/0] quit
```

配置 Serial2/1/0 运行 PPP 协议。

```
[RouterA] interface serial 2/1/0
[RouterA-Serial2/1/0] link-protocol ppp
```

```

[RouterA-Serial2/1/0] ip address 10.0.0.1 8
[RouterA-Serial2/1/0] quit
# 配置动态路由协议 RIP。
[RouterA] rip
[RouterA-rip-1] network 10.0.0.0
[RouterA-rip-1] network 20.0.0.0
[RouterA-rip-1] import-route direct
[RouterA-rip-1] quit
# 配置拨号接口上的路由使用优先级比串口的低。
[RouterA] interface bri 2/4/0
[RouterA-Bri2/4/0] rip metricin 2

```

(2) 配置 Router B

```

# 配置拨号访问控制列表及本地用户数据库。
<RouterB> system-view
[RouterB] dialer-group 1 rule ip permit
[RouterB] local-user usera class network
[RouterB-luser-network-usera] password simple usera
[RouterB-luser-network-usera] service-type ppp
[RouterB-luser-network-usera] quit
# 在 Dialer0 口上配置共享 DDR。
[RouterB] interface dialer 0
[RouterB-Dialer0] link-protocol ppp
[RouterB-Dialer0] ip address 20.0.0.2 24
[RouterB-Dialer0] dialer bundle enable
[RouterB-Dialer0] dialer peer-name usera
[RouterB-Dialer0] dialer-group 1
[RouterB-Dialer0] dialer number 8810010
[RouterB-Dialer0] ppp authentication-mode pap
[RouterB-Dialer0] ppp pap local-user userb password simple userb
[RouterB-Dialer0] quit
# 配置 BRI2/4/0 接口拨号参数。
[RouterB] interface bri 2/4/0
[RouterB-Bri2/4/0] dialer bundle-member 0
[RouterB-Bri2/4/0] ppp authentication-mode pap
[RouterB-Bri2/4/0] ppp pap local-user userb password simple userb
[RouterB-Bri2/4/0] quit
# 配置 Serial2/1/0 运行 PPP 协议。
[RouterB] interface serial 2/1/0
[RouterB-Serial2/1/0] link-protocol ppp
[RouterB-Serial2/1/0] ip address 10.0.0.2 8
[RouterB-Serial2/1/0] quit
# 配置 LoopBack1 接口。
[RouterB] interface loopback 1
[RouterB-Loopback1] ip address 30.0.0.1 32
[RouterB-Loopback1] quit
# 配置动态路由协议 RIP。

```

```

[RouterB] rip
[RouterB-rip-1] network 10.0.0.0
[RouterB-rip-1] network 20.0.0.0
[RouterB-rip-1] network 30.0.0.0
[RouterB-rip-1] import-route direct

```

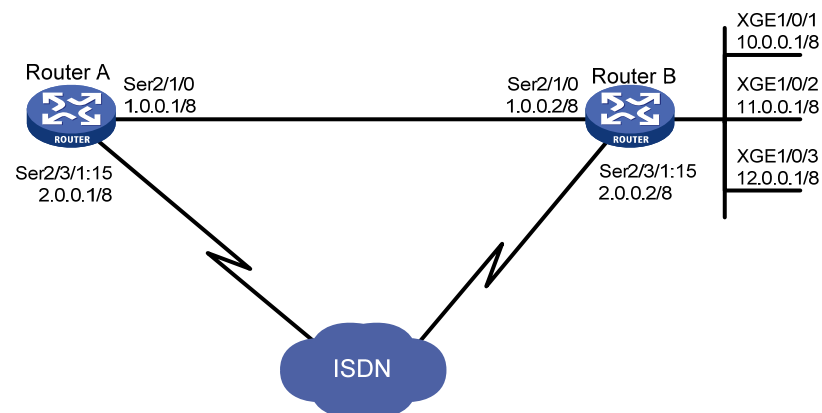
1.15.13 通过一个动态路由备份组监控多个网段配置举例

1. 组网需求

- Router A 与 Router B 通过一个串口直接相连，运行 PPP 协议。
- Router A 与 Router B 通过 ISDN PRI 接口与 ISDN 交换网相连，可以互相拨号呼叫。Router A 的电话号码为 660330，Router B 的电话号码为 660220。
- Router A 作为动态路由备份的主控设备，监控 Router B 上的 10.0.0.1/8、11.0.0.1/8、12.0.0.1/8 三个网段。
- 正常情况下 PPP 链路作为 Router A 与 Router B 之间的主用链路；当到达所有被监控网段的有效路由都不存在时，Router A 拨通备份链路。

2. 组网图

图1-16 通过一个动态路由备份组监控多个网段配置组网图



说明

本组网图是一个简单的示例，实际应用中监控网段可能分布多台设备上。

3. 配置步骤

(1) 配置 Router A

配置拨号访问组 1 以及对应的拨号访问控制条件。

```

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

```

创建动态路由备份组，该备份组共监控三个网段。

```

[RouterA] standby routing-group 1 rule ip 10.0.0.0 255.0.0.0
[RouterA] standby routing-group 1 rule ip 11.0.0.0 255.0.0.0

```



```

[RouterA] standby routing-group 1 rule ip 12.0.0.0 255.0.0.0
# 将 CE1 接口捆绑为 pri-set。
[RouterA] controller e1 2/3/1
[RouterA-E1 2/3/1] pri-set
[RouterA-E1 2/3/1] quit
# 配置 Serial2/1/0 运行 PPP 协议。
[RouterA] interface serial 2/1/0
[RouterA-Serial2/1/0] ip address 1.0.0.1 255.0.0.0
[RouterA-Serial2/1/0] link-protocol ppp
[RouterA-Serial2/1/0] quit
# 在 PRI 接口上配置传统 DDR。
[RouterA] interface serial 2/3/1:15
[RouterA-Serial2/3/1:15] ip address 2.0.0.1 255.0.0.0
[RouterA-Serial2/3/1:15] dialer circular enable
[RouterA-Serial2/3/1:15] dialer-group 1
[RouterA-Serial2/3/1:15] dialer route ip 10.0.0.0 mask 8 dial-number 660220
[RouterA-Serial2/3/1:15] standby routing-group 1
[RouterA-Serial2/3/1:15] quit
# 配置动态路由协议 RIP。
[RouterA] rip
[RouterA-rip-1] network 1.0.0.0
[RouterA-rip-1] network 2.0.0.0
[RouterA-rip-1] import-route direct
# 配置拨号接口上的路由使用优先级比串口的低。
[RouterA] interface serial 2/3/1:15
[RouterA-Serial2/3/1:15] rip metricin 2

```

(2) 配置 Router B

```

# 配置拨号访问组 1 以及对应的拨号访问控制条件。
[RouterB] system
[RouterB] dialer-group 1 rule ip permit
# 将 CE1 接口捆绑为 pri-set。
[RouterB] controller e1 2/3/1
[RouterB-E1 2/3/1] pri-set
[RouterB-E1 2/3/1] quit
# 配置 Serial2/1/0 运行 PPP 协议。
[RouterB] interface serial 2/1/0
[RouterB-Serial2/1/0] ip address 1.0.0.2 255.0.0.0
[RouterB-Serial2/1/0] link-protocol ppp
[RouterB-Serial2/1/0] quit
# 在 PRI 接口上配置传统 DDR。
[RouterB] interface serial 2/3/1:15
[RouterB-Serial2/3/1:15] ip address 2.0.0.2 255.0.0.0
[RouterB-Serial2/3/1:15] dialer circular enable
[RouterB-Serial2/3/1:15] dialer-group 1
[RouterB-Serial2/3/1:15] dialer route ip 2.0.0.1 mask 8 dial-number 660330
[RouterB-Serial2/3/1:15] quit

```

```
# 配置以太网接口。
[RouterB] interface gigabitethernet 1/0/1
[RouterB-GigabitEthernet1/0/1] ip address 10.0.0.1 255.0.0.0
[RouterB-GigabitEthernet1/0/1] quit
[RouterB] interface gigabitethernet 1/0/2
[RouterB-GigabitEthernet1/0/2] ip address 11.0.0.1 255.0.0.0
[RouterB-GigabitEthernet1/0/2] quit
[RouterB] interface gigabitethernet 1/0/3
[RouterB-GigabitEthernet1/0/3] ip address 12.0.0.1 255.0.0.0
[RouterB-GigabitEthernet1/0/3] quit
# 配置动态路由协议 RIP。
[RouterB] rip
[RouterB-rip-1] network 1.0.0.0
[RouterB-rip-1] network 2.0.0.0
[RouterB-rip-1] network 10.0.0.0
[RouterB-rip-1] network 11.0.0.0
[RouterB-rip-1] network 12.0.0.0
[RouterB-rip-1] import-route direct
```

1.16 DDR常见故障处理

1.16.1 无法建立DDR拨号连接

1. 故障现象

从路由器向外发送数据时，Modem 不拨号，无法建立 DDR 拨号连接。

2. 故障排除

可以按照如下步骤进行：

- 检查 Modem 连线是否正确，电话线连接是否正确，Modem 初始化过程是否正确；
- 对同/异步串口，检查接口是否配置为异步、拨号方式；
- 检查拨号接口上是否使能 DDR；
- 检查是否配置与数据包对应的 **dialer route** 或 **dialer number** 命令。

1.16.2 Modem已经接通，但是无法ping通对方

1. 故障现象

Modem 接通后，无法 ping 通对方。

2. 故障排除

可以按照如下步骤进行：

- 检查本端和对端配置封装协议是否一致，配置的 PPP 认证参数是否正确；
- 使用 **debugging ppp all** 命令打开 PPP 调试开关，观察 PPP 协商过程，确保 PPP 协商参数正确；
- 检查是否在拨号接口上正确配置 IP 地址；
- 检查是否在拨号接口上使能 DDR；

- 检查 **dialer-group** 和 **dialer-group rule** 命令是否配置，是否配置正确，确保配置 **dialer-group rule** 允许报文通过，并且两条命令存在相关联；
- 使用 **debugging dialer event** 和 **debugging dialer packet** 命令打开 DDR 调试开关，根据输出信息进行定位。

目 录

1 帧中继	1-1
1.1 帧中继简介	1-1
1.1.1 帧中继协议	1-1
1.1.2 帧中继网络组成	1-1
1.1.3 虚电路	1-2
1.1.4 DLCI	1-2
1.1.5 帧中继地址映射	1-2
1.1.6 LMI协议	1-3
1.1.7 帧中继应用	1-4
1.2 帧中继配置限制和指导	1-5
1.3 帧中继配置任务简介	1-5
1.3.1 帧中继DTE侧	1-5
1.3.2 帧中继DCE侧	1-6
1.4 配置帧中继DTE侧基本功能	1-6
1.5 配置帧中继DCE侧基本功能	1-7
1.6 配置帧中继本地虚电路	1-8
1.7 配置帧中继地址映射	1-8
1.7.1 帧中继地址映射建立方式简介	1-8
1.7.2 配置静态帧中继地址映射	1-9
1.7.3 配置动态帧中继IPv4 地址映射	1-9
1.7.4 配置动态帧中继IPv6 地址映射	1-9
1.8 配置帧中继子接口	1-10
1.9 配置帧中继IPHC压缩功能	1-10
1.9.1 功能简介	1-10
1.9.2 配置限制和指导	1-11
1.9.3 在接口上配置帧中继IPHC压缩功能	1-11
1.9.4 在虚电路上配置帧中继IPHC压缩功能	1-12
1.10 配置帧中继STAC压缩功能	1-12
1.11 配置帧中继FRF.12 分片功能	1-13
1.12 开启帧中继告警功能	1-14
1.13 帧中继显示和维护	1-14
1.14 帧中继典型配置举例	1-15
1.14.1 通过专线互连局域网配置举例	1-15

1.15 帧中继常见故障处理.....	1-17
1.15.1 物理层处于down状态	1-17
1.15.2 物理层已经处于up状态，但链路层协议处于down状态	1-17
1.15.3 链路层up，但是ping不通对方	1-17
2 多链路帧中继.....	2-1
2.1 多链路帧中继简介.....	2-1
2.2 多链路帧中继配置任务简介.....	2-1
2.3 配置MFR捆绑	2-1
2.3.1 创建MFR接口	2-1
2.3.2 恢复MFR接口的缺省配置	2-3
2.4 配置捆绑链路.....	2-3
2.5 多链路帧中继显示和维护.....	2-4
2.6 多链路帧中继典型配置举例.....	2-4
2.6.1 多链路帧中继典型配置举例	2-4

1 帧中继



说明

本特性仅在路由器上安装了 SAE、E1、E1-F、T1、T1-F、POS、CPOS、CE3 或 CT3 接口模块时支持。

1.1 帧中继简介

1.1.1 帧中继协议

FR（Frame Relay，帧中继）协议是一种简化的 X.25 广域网协议，是一种统计复用的协议，它能够在单一物理传输线路上提供多条虚电路。每条虚电路用 DLCI（Data Link Connection Identifier，数据链路连接标识符）来标识。每条虚电路通过 LMI（Local Management Interface，本地管理接口）协议检测和维护虚电路的状态。

1.1.2 帧中继网络组成

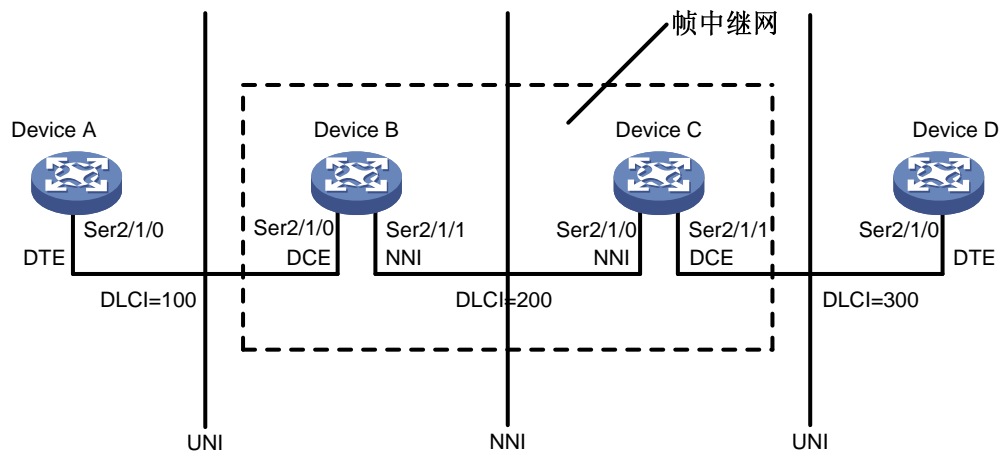
帧中继网络提供了用户设备（如路由器和主机等）之间进行数据通信的能力。对于帧中继网络，涉及如下概念：

- DTE（Data Terminal Equipment，数据终端设备）：帧中继终端用户设备被称作 DTE。
- DCE（Data Circuit-terminating Equipment，数据电路终接设备）：为用户设备提供接入的设备属于帧中继网络设备，被称为 DCE。
- UNI（User-to-Network Interface，用户网络接口）：DTE 和 DCE 之间的相连接口被称为 UNI。
- NNI（Network-to-Network Interface，网间接口）：网络与网络之间的接口被称为 NNI。

在实际应用中，DTE 接口只能和 DCE 接口连接，NNI 接口只能和 NNI 接口连接。如果把设备用做帧中继交换机，帧中继接口类型应该为 NNI 或 DCE。

如 [1.1](#) 所示，两台 DTE 设备（Device A 和 Device D）通过帧中继网络实现互连，Device B 和 Device C 用来代表一个简单的帧中继交换网。可以看出，DTE 和 DCE 只是在 UNI 处才进行区分；对于两台 DTE 之间建立的虚电路，不同虚电路段可以对应不同的 DLCI。

图1-1 帧中继网络接口类型



1.1.3 虚电路

VC (Virtual Circuit, 虚电路) 是建立在两台网络设备之间共享网络的逻辑电路。根据建立方式的不同, 可以将虚电路分为两种类型:

- PVC (Permanent Virtual Circuit, 永久虚电路): 可以通过手工配置产生或者通过 LMI 协商动态学习产生。永久虚电路方式需要检测虚电路是否可用。
- SVC (Switched Virtual Circuit, 交换虚电路): 在两个帧中继终端用户之间通过呼叫建立虚电路连接, 网络在建好的虚电路上提供数据信息的传送服务, 终端用户提供呼叫清除来终止虚电路连接。

目前在帧中继网络中使用最多的是永久虚电路方式。

对于 DTE 侧设备, 永久虚电路的状态完全由 DCE 侧设备决定。而 DCE 侧设备根据不同的网络环境, 其虚电路状态分为如下两种情况:

- 用于两台设备直连的情况, 其状态由与 DTE 侧设备进行 LMI 协商结果来决定;
- 用于交换网络的情况, 其状态由与 DTE 侧设备进行 LMI 协商的结果和网络侧虚电路的状态来决定。

1.1.4 DLCI

DLCI 用于标识不同的虚电路, DLCI 只在本地接口和与之直接相连的对端接口有效, 只具有本地意义, 不具有全局有效性。在帧中继网络中, 不同的物理接口上相同的 DLCI 并不表示是同一个虚电路。

帧中继网络用户接口上最多支持 1024 条虚电路, 其中, 用户可用的 DLCI 范围是 16~1007。由于帧中继虚电路是面向连接的, 本地不同的 DLCI 连接到不同的对端设备, 因此可以认为本地 DLCI 就是对端设备的“帧中继地址”。

1.1.5 帧中继地址映射

帧中继地址映射是把对端设备的协议地址与对端设备的帧中继地址 (本地的 DLCI) 关联起来, 使本端设备高层协议能通过对端设备的协议地址寻址到对端设备。

帧中继主要用来承载 IPv4/IPv6 协议，因为在发送 IPv4/IPv6 报文时，设备根据路由表只能知道报文的下一跳地址，发送报文前必须由该地址确定它对应的 DLCI。这个过程可以通过查找帧中继地址映射表来完成，地址映射表中存放的是下一跳 IPv4/IPv6 地址和与其对应的 DLCI 的映射关系（MAP）。

地址映射表可以由手工配置，也可以由 InARP（Inverse Address Resolution Protocol，逆向地址解析协议）/IND（Inverse Neighbor Discovery，逆向邻居发现）动态维护。

InARP 的工作机制如下：每当发现一条新的虚电路时，如果本地接口上已经配置了 IPv4 地址，InARP 将启动定时器并同时在该虚电路上发送 InARP 请求报文给对端，该请求报文中携带了本地的 IPv4 地址。发送请求报文的时间间隔缺省为 1 分钟（该时间称为探测时间，可以通过 `fr inarp interval` 命令配置）。IND 的工作机制与 InARP 类似。

- 如果对端设备收到该请求报文，可以获得本地的 IPv4 地址，从而生成地址映射，并发送 InARP 应答报文进行响应，该应答报文中携带了对端的 IPv4 地址，这样本地收到应答报文后同样生成地址映射。本端生成地址映射后，将发送 InARP 请求报文的时间间隔修改为 12 分钟（该时间是固定的，称为老化时间），定时器超时后继续发送 InARP 请求报文，如果某次定时器超时，发现没有收到 InARP 应答报文，将定时器时间修改为探测时间，如果探测 3 次都在探测时间内没有得到回应，将学习到的动态地址映射删除。
- 如果本端在探测时间内没有收到 InARP 应答报文，则一直进行探测，直至进行 InARP 协商的条件不存在时（本地接口上没有配置 IPv4 地址或者 PVC 处于非激活状态）停止探测。

1.1.6 LMI协议

LMI 协议用于管理永久虚电路 PVC，包括：通知 PVC 的增加、探测 PVC 的删除、监控 PVC 状态的变更、验证链路的完整性。

系统支持三种 LMI 协议：

- ITU-T 的 Q.933 附录 A
- ANSI 的 T1.617 附录 D
- 非标准兼容协议

为了保证正常通信，DTE 侧和 DCE 侧需要采用相同的 LMI 协议。

1. LMI消息类型和报文类型

LMI 协议的消息类型有两种：状态请求（Status Enquiry）消息和状态（Status）消息。

- 状态请求消息由 DTE 端发送，用来向 DCE 端请求虚电路的状态或验证链路完整性。
- 状态消息是当 DCE 端收到状态请求消息后向 DTE 端发送的一个应答消息，用于传送虚电路的状态或验证链路完整性。

LMI 协议的报文类型有两种：全状态（full）报文、链路完整性验证（LIV，link integrity verification）报文。

- 链路完整性验证报文只用于验证链路的完整性；
- 全状态报文除了用于验证链路的完整性，还传递 PVC 的状态。

2. LMI协商参数

LMI协议的协商过程中需要用到的一些参数定义，这些参数由Q.933 的附录A规定，含义如 [表 1-1](#) 所示。用户可以对这些参数进行配置，达到优化设备运行的目的。

表1-1 LMI 协商参数含义

设备角色	参数	取值范围	缺省值	含义
DTE	请求PVC状态的计数器 (N391)	1~255	6	用来定义链路完整性请求报文和全状态请求报文的发送比例, 即(链路完整性请求报文数: 全状态请求报文数) = (N391-1: 1)
	错误门限 (N392)	1~10	3	表示在被观察的事件总数中发生错误的门限
	事件计数器 (N393)	1~10	4	表示被观察的事件总数
	用户侧轮询定时器 (T391)	0~32767 (单位: 秒)	10 (单位: 秒)	这是一个时间变量, 它定义了DTE设备发送状态请求报文的时间间隔, 当为0时, 表示禁止LMI协议
DCE	错误门限 (N392)	1~10	3	表示在被观察的事件总数中发生错误的门限
	事件计数器 (N393)	1~10	4	表示被观察的事件总数
	网络侧轮询定时器 (T392)	5~30 (单位: 秒)	15 (单位: 秒)	这是一个时间变量, 它定义了DCE设备等待一个状态请求报文的 longest 时间

3. LMI工作机制

LMI 协议的简要工作过程如下:

- (1) DTE 在物理 Up 后, 先向 DCE 发送一个全状态请求消息, 查询虚电路的状态, 且定时器 T391 开始计时。T391 的间隔即为每一个轮询的时间间隔, 即每隔 T391, DTE 发送一个状态请求消息, 同时, DTE 的计数器 V391 进行计数。当 $V391 < N391$ 时, DTE 发送链路完整性验证的状态请求消息, 仅询问“链路完整性”; 当 $V391 = N391$ 时, V391 清 0, 且 DTE 发送全状态请求消息, 不仅询问“链路完整性”, 而且还询问所有 PVC 的状态。
- (2) DCE 收到请求消息后, 发送状态消息对 DTE 所要了解的状态进行应答, 同时 DCE 的轮询定时器 T392 开始计时, 等待下一个状态请求消息。如果 T392 超时时, DCE 没有收到状态请求消息, DCE 就记录该错误, 错误次数加 1。如果在 N393 个事件中, 发生的错误次数超过 N392, DCE 就认为该物理通路不可用, 所有的虚电路不可用。
- (3) DTE 收到应答消息后, 更新链路状态和 PVC 状态。如果定时器 T391 超时时, DTE 没有收到作为应答的状态消息, 就记录该错误, 错误次数加 1。如果在 N393 个事件中, 发生的错误次数超过 N392, DTE 就认为该物理通路不可用, 所有的虚电路不可用。

1.1.7 帧中继应用

帧中继比较典型的应用之一是帧中继接入。帧中继接入即作为用户端承载上层报文, 接入到帧中继网络中。

帧中继网络可以是公用网络或者是某一企业的私有网络, 如 [图 1-2](#) 所示。帧中继网络也可以是直接连接, 如 [图 1-3](#) 所示。

图1-2 通过帧中继网络互连局域网

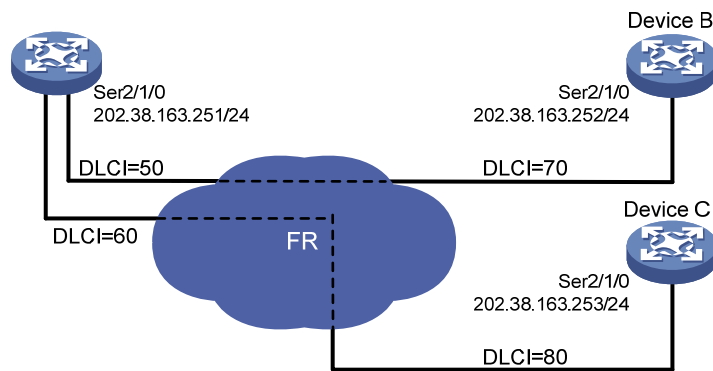
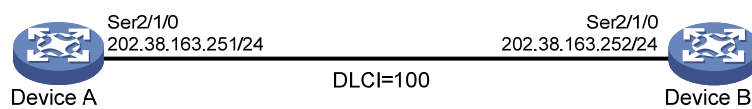


图1-3 通过专线互连局域网



1.2 帧中继配置限制和指导

- 支持 FR 协议的接口有：同步串口（包括其它接口派生出来的同步串口）、POS 接口、POS 通道接口。
- 帧中继网络 NNI 接口既是 DTE 侧又是 DCE 侧，可以配置 DTE 侧和 DCE 侧的功能，但它不能学习 DLCI，需要两端都配置 DLCI。
- 如果一端设置为 NNI 接口，则通信的另一端也必须设置为 NNI 接口。

1.3 帧中继配置任务简介

1.3.1 帧中继DTE侧

帧中继 DTE 侧配置任务如下：

- (1) [配置帧中继DTE侧基本功能](#)
- (2) [配置帧中继本地虚电路](#)
- (3) [配置帧中继地址映射](#)
- (4) (可选) [配置帧中继子接口](#)
- (5) (可选) 配置帧中继压缩功能
 - [配置帧中继IPHC压缩功能](#)
 - [配置帧中继STAC压缩功能](#)
- (6) (可选) [配置帧中继FRF.12分片功能](#)
- (7) (可选) [开启帧中继告警功能](#)

1.3.2 帧中继DCE侧

帧中继 DCE 侧配置任务如下：

- (1) [配置帧中继DCE侧基本功能](#)
- (2) [配置帧中继本地虚电路](#)
- (3) [配置帧中继地址映射](#)
- (4) (可选) [配置帧中继子接口](#)
- (5) (可选) 配置帧中继压缩功能
 - [配置帧中继IPHC压缩功能](#)
 - [配置帧中继STAC压缩功能](#)
- (6) (可选) [配置帧中继FRF.12分片功能](#)
- (7) (可选) [开启帧中继告警功能](#)

1.4 配置帧中继DTE侧基本功能

- (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帧中继。

```
link-protocol fr
```

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

- (4) (可选) 配置帧中继接口的封装格式。

```
fr encapsulation { ietf | nonstandard }
```

缺省情况下，封装格式为 IETF。

- (5) (可选) 配置帧中继接口类型为 DTE。

```
fr interface-type dte
```

缺省情况下，帧中继接口类型为 DTE。

- (6) (可选) 配置帧中继 LMI 协议类型。

```
fr lmi type { ansi | nonstandard | q933a }
```

缺省情况下，接口的 LMI 协议类型为 q933a。

- (7) (可选) 配置帧中继链路状态参数。

- 配置 DTE 侧 N391 参数的值。

```
fr lmi n391dte n391-value
```

缺省情况下，DTE 侧 N391 参数的值为 6。

- 配置 DTE 侧 N392 参数的值。

```
fr lmi n392dte n392-value
```

缺省情况下，DTE 侧 N392 参数的值为 3。

- 配置 DTE 侧 N393 参数的值。

fr lmi n393dte *n393-value*

缺省情况下，DTE 侧 N393 参数的值为 4。

- 配置 DTE 侧 T391 参数的值。

timer-hold *seconds*

缺省情况下，DTE 侧 T391 参数的值为 10 秒。

1.5 配置帧中继DCE侧基本功能

- (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帧中继。

link-protocol fr

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

- (4) （可选）配置帧中继接口的封装格式。

fr encapsulation { **ietf** | **nonstandard** }

缺省情况下，封装格式为 IETF。

- (5) （可选）配置帧中继接口类型为 DCE 或者 NNI。

fr interface-type { **dce** | **nni** }

缺省情况下，帧中继接口类型为 DTE。

DCE 设备互联的帧中继接口类型为 NNI，DCE 连接 DTE 的帧中继接口类型为 DCE。

- (6) （可选）配置帧中继 LMI 协议类型。

fr lmi type { **ansi** | **nonstandard** | **q933a** }

缺省情况下，接口的 LMI 协议类型为 q933a。

- (7) （可选）配置帧中继链路状态参数。

- 配置 DCE 侧 N392 参数的值。

fr lmi n392dce *n392-value*

缺省情况下，DCE 侧 N392 参数的值为 3。

- 配置 DCE 侧 N393 参数的值。

fr lmi n393dce *n393-value*

缺省情况下，DCE 侧 N393 参数的值为 4。

- 配置 DCE 侧 T392 参数的值。

fr lmi t392dce *t392-value*

缺省情况下，DCE 侧 T392 参数的值为 15 秒。

1.6 配置帧中继本地虚电路

1. 功能简介

当帧中继接口类型是 DCE 或 NNI 时，需要为接口（不论是主接口还是子接口）手动创建虚电路。当帧中继接口类型是 DTE 时，如果接口是主接口，则系统会根据对端设备，通过协议协商自动创建虚电路，也可以手动配置虚电路；如果是子接口，则必须手动为接口指定虚电路。通过本配置，可以完成手动指定虚接口。

2. 配置限制和指导

- 如果要在 DTE 侧手动配置虚电路，则配置的虚电路号必须与相连的 DCE 侧保持一致。
- 如果 DCE 侧的 DLCI 值被改变，在不影响业务的前提下，可以重启两端设备的接口，或者在两端的设备上分别执行命令 `reset fr inarp` 清除 InARP 协议建立的动态地址映射信息，保证 DTE 能重新尽快学习到正确的地址映射信息。
- 虚电路号在一个主接口及其所有子接口上是唯一的。

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
```

进入的接口可以是主接口或子接口。

- (3) 为接口创建虚电路，并进入相应的帧中继虚电路视图。

```
fr dlci dlci-number
```

- (4) （可选）配置帧中继虚电路的封装格式。

```
fr encapsulation { ietf | nonstandard }
```

缺省情况下，帧中继虚电路采用接口配置的封装格式。

- (5) （可选）配置帧中继虚电路的广播属性。

```
broadcast
```

缺省情况下，静态配置的帧中继虚电路不具备广播属性，动态学习的帧中继虚电路具备广播属性。

如果帧中继虚电路具备了广播属性，则所属接口上的广播或组播报文都要在该虚电路上发送一份。

1.7 配置帧中继地址映射

1.7.1 帧中继地址映射建立方式简介

帧中继地址映射可以通过下面两种方式建立：

- 静态配置：当网络拓扑比较稳定，短时间内不会有变化或新的用户加入，可以使用静态配置。一方面，它可以保障映射链路不发生变化，使网络链路连接比较稳定，另一方面，它可以防止其他未知用户的攻击，提高网络安全性。
- 动态建立：适用于对端设备也支持 InARP 且网络较复杂的情况。

1.7.2 配置静态帧中继地址映射

- (1) 进入系统视图。

```
system-view
```

- (2) 进入接口视图。

```
interface interface-type interface-number
```

可以是主接口或 P2MP 子接口。

- (3) 增加一条静态地址映射。

(IPv4 网络)

```
fr map ip { ip-address | default } dlci-number
```

(IPv6 网络)

```
fr map ipv6 { ipv6-address | default } dlci-number
```

建议为对端的 Link-local 地址也配置地址映射，确保以 Link-local 地址为目的地址的报文能够正确转发。

1.7.3 配置动态帧中继 IPv4 地址映射

- (1) 进入系统视图。

```
system-view
```

- (2) 进入接口视图。

```
interface interface-type interface-number
```

- (3) 使能帧中继 InARP 功能以建立动态地址映射。

```
fr inarp ip [ dlci-number ]
```

缺省情况下，帧中继 InARP 功能处于使能状态。

- (4) (可选) 配置 InARP 学习时的请求报文发送间隔时间。

```
fr inarp interval interval
```

缺省情况下，InARP 学习时的请求报文发送间隔时间为 60 秒。

1.7.4 配置动态帧中继 IPv6 地址映射

- (1) 进入系统视图。

```
system-view
```

- (2) 进入接口视图。

```
interface interface-type interface-number
```

- (3) 使能帧中继 IPv6 的 IND 功能以建立动态地址映射。

```
fr ipv6 ind [ dlci-number ]
```

缺省情况下，帧中继 IPv6 的 IND 功能处于关闭状态。

- (4) (可选) 配置 IND 学习时的请求报文发送间隔时间。

```
ipv6 ind holdtime seconds
```

缺省情况下，IND 学习时的请求报文发送间隔时间为 30 秒。

(5) 配置 IND 请求报文连续发送的时间间隔。

```
ipv6 ind solicitation retrans-timer seconds
```

缺省情况下，IND 请求报文连续发送的时间间隔为 1 秒。

1.8 配置帧中继子接口

1. 帧中继子接口简介

帧中继有两种类型的接口：主接口和子接口。其中子接口是一个逻辑结构，可以配置协议地址和虚电路等，一个物理接口可以有多个子接口。虽然子接口是逻辑结构，并不实际存在，但对于网络层而言，子接口和主接口是没有区别的，都可以配置虚电路与远端设备相连。

帧中继的子接口又可以分为两种类型：P2P（Point-to-Point，点到点）子接口和 P2MP（Point-to-Multipoint，点到多点）子接口。P2P 子接口用于连接单个远端目标，P2MP 子接口用于连接多个远端目标。P2MP 子接口在一个子接口上配置多条虚电路，每条虚电路都和它相连的远端网络地址建立一个地址映射，这样不同的虚电路就可以到达不同的远端而不会混淆。

地址映射的建立可以用手工配置的方法，也可以利用逆向地址解析协议来动态建立。P2P 子接口和 P2MP 子接口配置虚电路以及地址映射的方法是不同的：

- P2P 子接口：对 P2P 子接口，因为只有唯一的一个对端地址，所以在给子接口配置一条 PVC 时实际已经确定了对端地址，不能配置静态地址映射，也不能动态学习地址映射。
- P2MP 子接口：对 P2MP 子接口，对端地址与本地 DLCI 映射可以通过配置静态地址映射或者通过逆向地址解析协议来确定（InARP 在主接口上配置即可）。如果要建立静态地址映射，则应该对每一条虚电路建立静态地址映射关系。

2. 配置步骤

(1) 进入系统视图。

```
system-view
```

(2) 创建子接口并进入子接口视图。

```
interface interface-type interface-number.subnumber [ p2mp | p2p ]
```

创建子接口时，如果不指定接口类型，缺省创建 P2MP 子接口。

(3) 配置帧中继子接口的虚电路。

请参见“[1.6 配置帧中继本地虚电路](#)”

帧中继子接口必须手工配置虚电路。

(4) 建立地址映射。

请参见“[1.7 配置帧中继地址映射](#)”

对于 P2MP 子接口可以配置该项。

1.9 配置帧中继 IPHC 压缩功能

1.9.1 功能简介

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

在低速链路上，每个语音报文中报文头消耗大部分的带宽，网络带宽利用率很差。为了减少报文头对带宽的消耗，可以在帧中继链路上使用 IPHC 压缩功能，对报文头进行压缩。

IPHC 压缩分为如下两种：

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

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

1.9.2 配置限制和指导

- 帧中继 STAC 压缩与 IPHC 压缩不能同时配置。
- 用户必须在链路的两端同时开启帧中继 IPHC 压缩功能，该功能才生效。
- 用户可以在接口视图下和 DLCI 视图下配置帧中继 IPHC 压缩功能或 RTP 头/TCP 头压缩的最大连接数，接口视图下的配置对该接口下的所有虚电路生效，DLCI 视图下的配置只对本虚电路生效。如果接口视图的配置与 DLCI 视图的配置不同，则以 DLCI 视图下的配置为准。
- 当帧中继的封装格式为 **ietf** 时（通过命令 **fr encapsulation** 配置），开启 IPHC 压缩功能后会触发 IPHC 协商，协商成功后压缩功能才生效；当帧中继的封装格式为 **nonstandard** 时，开启 IPHC 压缩功能后不会触发 IPHC 协商，压缩功能直接生效，而且仅支持 RTP 头压缩，不支持 TCP 头压缩。此时，需要链路两端的封装格式都配置为 **nonstandard** 才能正常通信。
- 关闭 IPHC 压缩功能时，不会立即停止压缩，需要在接口下或者虚电路所在的接口下执行 **shutdown** 与 **undo shutdown** 操作后，才会关闭压缩功能。
- 只有在开启 IPHC 压缩功能后，才能配置接口或虚电路上允许进行 RTP 头/TCP 头压缩的最大连接数，并且需要在接口下或者虚电路所在的接口下执行 **shutdown** 与 **undo shutdown** 操作后，配置才能生效。在关闭 IPHC 压缩功能后，配置将被清除。

1.9.3 在接口上配置帧中继IPHC压缩功能

- (1) 进入系统视图。

```
system-view
```

- (2) 进入接口视图。

```
interface interface-type interface-number
```

- (3) 开启接口的帧中继 IPHC 压缩功能。

```
fr compression iphc enable [ nonstandard ]
```

缺省情况下，帧中继 IPHC 压缩功能处于关闭状态。

配置 **nonstandard** 参数后，仅支持 RTP 头压缩，不支持 TCP 头压缩。

- (4) 配置接口上允许进行 RTP 头压缩的最大连接数。

```
fr compression iphc rtp-connections
```

缺省情况下，接口上允许进行 RTP 头压缩的最大连接数为 16。

- (5) 配置接口上允许进行 TCP 头压缩的最大连接数。


```
fr compression iphc tcp-connections
```

缺省情况下，接口上允许进行 TCP 头压缩的最大连接数为 16。

1.9.4 在虚电路上配置帧中继IPHC压缩功能

- (1) 进入系统视图。

```
system-view
```

- (2) 进入接口视图。

```
interface interface-type interface-number
```

进入的接口可以是主接口或子接口。

- (3) 进入帧中继虚电路视图。

```
fr dlci dlci-number
```

- (4) 开启虚电路的帧中继 IPHC 压缩功能。

```
fr compression iphc enable [ nonstandard ]
```

缺省情况下，虚电路的帧中继 IPHC 压缩功能处于关闭状态。

配置 **nonstandard** 参数后，仅支持 RTP 头压缩，不支持 TCP 头压缩。

- (5) 配置虚电路上允许进行 RTP 头压缩的最大连接数。

```
fr compression iphc rtp-connections
```

缺省情况下，虚电路上允许进行 RTP 头压缩的最大连接数为 16。

- (6) 配置虚电路上允许进行 TCP 头压缩的最大连接数。

```
fr compression iphc tcp-connections
```

缺省情况下，虚电路上允许进行 TCP 头压缩的最大连接数为 16。

1.10 配置帧中继STAC压缩功能

1. 功能简介

STAC 压缩功能可以对帧中继数据报文和 InARP/IND 报文进行压缩，提高数据传输效率。STAC 压缩功能不对 LMI 报文进行压缩。

开启了 STAC 压缩功能的一端会向 PVC 的对端发送 STAC 控制报文，进行 PVC 状态协商，只有两端都开启了 STAC 压缩功能，协商才能成功。协商成功后，两端设备将在 PVC 上传输经过压缩的帧中继数据报文。如果 STAC 控制报文发送 10 次后仍无法协商成功，将停止协商，STAC 压缩功能不生效。

2. 配置限制和指导

- 帧中继 STAC 压缩与 IPHC 压缩不能同时配置。
- 用户必须在 PVC 的两端同时开启帧中继 STAC 压缩功能，该功能才生效。
- 只有当 PVC 的帧中继报文封装类型为 IETF 时，帧中继 STAC 压缩才能起作用。在配置帧中继 STAC 压缩功能时，如果 PVC 的帧中继报文封装类型不是 IETF，则系统会自动将 PVC 的报文封装类型改为 IETF。

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*

进入的接口可以是主接口或子接口。

- (3) 进入帧中继虚电路视图。

fr dlci *dlci-number*

- (4) 开启虚电路的帧中继 STAC 压缩功能。

fr compression stac enable

缺省情况下，虚电路的帧中继 STAC 压缩功能处于关闭状态。

1.11 配置帧中继FRF.12分片功能

1. 功能简介

在低速帧中继线路上，大数据报文将会造成传输时延的增大。帧中继分片功能仅对发送的报文有效。帧中继分片功能可以将较大的数据报文分割成若干个较小的数据报文，然后在接收端再把数据重新组装起来，这样能够降低报文的传输时延，提高传输效率。

当语音和数据同时传输时，对数据报文进行分片，可以减少语音报文的延时，保证语音的实时性。在对数据报文分片时，可以配置数据报文分片的大小，保证语音报文及时均匀地得到处理，降低时延。

FRF.12 分片功能规定了两种类型分片：NNI&UNI 类型和 end-to-end 类型。目前仅支持 end-to-end 类型的分片方式。

2. 配置限制和指导

- 接口的 FRF.12 分片功能和帧中继流量整形功能不能同时进行配置。关于帧中继流量整形功能的详细介绍，请参见“ACL 和 QoS 配置指导”中的“帧中继 QoS”。
- MFR 接口上不支持 FRF.12 分片功能。如果链路两端都是 MFR 接口，且配置了 FRF.12 分片功能，此时 FRF.12 分片功能不起作用，两端均可收发完整的报文；如果本端是 MFR 接口，对端是帧中继接口，则本端 FRF.12 分片功能不起作用，本端报文会完整发出，而对端的 FRF.12 分片功能起作用。

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) 使能接口的帧中继 FRF.12 分片功能。

fr fragment enable

缺省情况下，接口的 FRF.12 分片功能处于关闭状态。

- (4) （可选）配置帧中继接口允许的报文分片大小。

fr fragment size

缺省情况下，帧中继接口允许的分片大小为 45 字节。

1.12 开启帧中继告警功能

1. 功能简介

开启帧中继的告警功能后，帧中继会生成告警信息，用于报告本模块的重要事件。生成的告警信息将发送至 SNMP 模块，通过配置 SNMP 中告警信息的发送参数，来决定告警信息输出的相关属性。有关告警信息的详细介绍，请参见“网络管理和监控配置指导”中的“SNMP”。

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 开启帧中继的告警功能。

```
snmp-agent trap enable fr
```

缺省情况下，帧中继的告警功能处于关闭状态。

1.13 帧中继显示和维护

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帧中继的运行情况，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 InARP 协议建立的动态地址映射信息、PVC 统计信息、IPHC 压缩统计信息。

表1-2 帧中继显示和维护

操作	命令
显示帧中继地址映射表	<code>display fr map [interface interface-type interface-number]</code>
显示帧中继LMI信息	<code>display fr lmi [interface interface-type interface-number]</code>
显示帧中继的永久虚电路状态和该虚电路收发数据的统计信息	<code>display fr pvc [interface interface-type interface-number] [dlci dlci-number]</code>
显示帧中继InARP报文统计信息	<code>display fr inarp [interface interface-type interface-number]</code>
显示帧中继IPv6地址映射表	<code>display fr ipv6 map [static dynamic] [interface interface-type interface-number [dlci dlci-number]]</code>
显示帧中继IPHC压缩的统计信息	<code>display fr compression iphc { rtp tcp } [interface interface-type interface-number [dlci dlci-number]]</code>
显示帧中继STAC压缩的统计信息	<code>display fr compression stac [interface interface-type interface-number [dlci dlci-number]]</code>
显示帧中继FRF.12分片的统计信息	<code>display fr fragment [interface interface-type interface-number [dlci dlci-number]]</code>
清除InARP协议建立的动态地址映射	<code>reset fr inarp [interface interface-type interface-number [dlci dlci-number]]</code>
清除IND协议建立的动态地址映射	<code>reset fr ipv6 ind [interface interface-type</code>

操作	命令
	<code>interface-number [dlci dlci-number]]</code>
清除帧中继的PVC统计信息	<code>reset fr pvc [interface interface-type interface-number [dlci dlci-number]]</code>
清除帧中继IPHC压缩的统计信息	<code>reset fr compression iphc [rtp tcp] [interface interface-type interface-number [dlci dlci-number]]</code>

1.14 帧中继典型配置举例

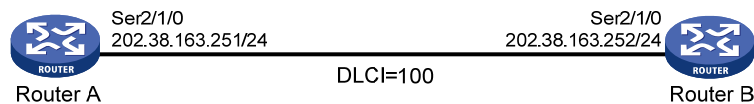
1.14.1 通过专线互连局域网配置举例

1. 组网需求

两台路由器通过帧中继接口直连, Router A 作为帧中继 DCE 设备, Router B 作为帧中继 DTE 设备。

2. 组网图

图1-4 通过专线互连局域网组网图



3. 配置步骤

(1) 方法一：采用主接口方式

• 配置 Router A

配置接口的 IP 地址。

```
<RouterA> system-view
[RouterA] interface serial 2/1/0
[RouterA-Serial2/1/0] ip address 202.38.163.251 255.255.255.0
```

配置接口封装的链路层协议为帧中继，接口类型为 DCE。

```
[RouterA-Serial2/1/0] link-protocol fr
[RouterA-Serial2/1/0] fr interface-type dce
```

配置本地虚电路。

```
[RouterA-Serial2/1/0] fr dlci 100
```

• 配置 Router B

配置接口的 IP 地址。

```
<RouterB> system-view
[RouterB] interface serial 2/1/0
[RouterB-Serial2/1/0] ip address 202.38.163.252 255.255.255.0
```

配置接口封装的链路层协议为帧中继，接口类型为缺省的 DTE。

```
[RouterB-Serial2/1/0] link-protocol fr
[RouterB-Serial2/1/0] fr interface-type dte
[RouterB-Serial2/1/0] quit
```

(2) 方法二：采用子接口方式

• 配置 Router A

配置接口封装的链路层协议为帧中继，接口类型为 DCE。

```
<RouterA> system-view
[RouterA] interface serial 2/1/0
[RouterA-Serial2/1/0] link-protocol fr
[RouterA-Serial2/1/0] fr interface-type dce
[RouterA-Serial2/1/0] quit
```

配置子接口的 IP 地址及本地虚电路。

```
[RouterA] interface serial 2/1/0.1 p2p
[RouterA-Serial2/1/0.1] ip address 202.38.163.251 255.255.255.0
[RouterA-Serial2/1/0.1] fr dlci 100
```

• 配置 Router B

配置接口封装的链路层协议为帧中继，接口类型为缺省的 DTE。

```
<RouterB> system-view
[RouterB] interface serial 2/1/0
[RouterB-Serial2/1/0] link-protocol fr
[RouterB-Serial2/1/0] fr interface-type dte
[RouterB-Serial2/1/0] quit
```

配置子接口的 IP 地址及本地虚电路。

```
[RouterB] interface serial 2/1/0.1 p2p
[RouterB-Serial2/1/0.1] ip address 202.38.163.252 255.255.255.0
[RouterB-Serial2/1/0.1] fr dlci 100
[RouterB-Serial2/1/0.1] quit
```

4. 验证配置

验证过程以采用主接口配置方式为例：

在 Router B 上通过 **display fr pvc** 命令可以查看接口 Serial2/1/0 的 PVC 信息，发现 PVC 的状态为 Active。

```
[RouterB] display fr pvc
PVC information for interface Serial2/1/0 (DTE, physically up)
  DLCI: 100  Type: Dynamic  Interface: Serial2/1/0
  Encapsulation: IETF  Broadcast
  Creation time: 2014/02/19 01:38:00  Status: Active
  Input: 2 packets, 60 bytes, 0 dropped
  Output: 2 packets, 60 bytes, 0 dropped
```

Router A 和 Router B 可以互相 ping 通对方。

```
[RouterB] ping 202.38.163.251
Ping 202.38.163.251 (202.38.163.251): 56 data bytes, press CTRL_C to break
56 bytes from 202.38.163.251: icmp_seq=0 ttl=255 time=76.007 ms
56 bytes from 202.38.163.251: icmp_seq=1 ttl=255 time=8.790 ms
56 bytes from 202.38.163.251: icmp_seq=2 ttl=255 time=1.630 ms
56 bytes from 202.38.163.251: icmp_seq=3 ttl=255 time=0.841 ms
56 bytes from 202.38.163.251: icmp_seq=4 ttl=255 time=1.012 ms

--- Ping statistics for 202.38.163.251 ---
```

```
5 packets transmitted, 5 packets received, 0.0% packet loss
round-trip min/avg/max/std-dev = 0.841/17.656/76.007/29.326 ms
```

1.15 帧中继常见故障处理

1.15.1 物理层处于down状态

1. 故障现象

物理层处于 **down** 状态。

2. 故障分析

可能是物理连接故障或者对端设备未启动。

3. 处理过程

- 检查物理线路是否正常。
- 检查对端设备是否正常运行。

1.15.2 物理层已经处于up状态，但链路层协议处于down状态

1. 故障现象

物理层已经处于 **up** 状态，但链路层协议处于 **down** 状态。

2. 故障分析

- 可能是两端设备链路层接口封装协议配置有误。
- 可能是两端设备帧中继接口配置有误。
- 可能是两端设备 LMI 协议类型配置不一致。

3. 处理过程

- 确认本地设备和对端设备是否都封装了帧中继协议。
- 如果两台设备直连，确认本地设备和对端设备是否配置成一端是帧中继 **DTE** 接口类型，一端是帧中继 **DCE** 接口类型。
- 确认两端配置的 LMI 协议类型是否相同。
- 如果以上检查都已经通过，可以打开帧中继 LMI 消息的调试命令 **debugging fr lmi**，看状态请求报文与状态报文是否一一对应。如果不一一对应，说明物理层数据收发不正确，请检查物理层的问题。

1.15.3 链路层up，但是ping不通对方

1. 故障现象

链路层协议处于 **up** 状态，但不能 **ping** 通对方。

2. 故障分析

可能是两端设备地址映射配置有误或者路由不可达。

3. 处理过程

- 确认两端设备是否都为对端配置（或产生）了正确的地址映射。

- 如果两端的 IP 地址不在同一个子网段，确认路由表是否有到达对端的路由。

2 多链路帧中继

2.1 多链路帧中继简介

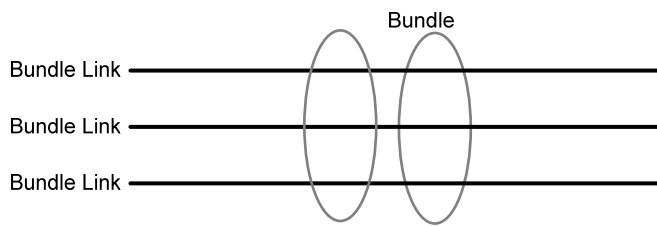
MFR（Multilink Frame Relay，多链路帧中继）是为帧中继用户提供的一种性价比比较高的带宽解决方案，它基于帧中继论坛的 FRF.16 协议，实现在 DTE/DCE 接口下的多链路帧中继功能。

多链路帧中继特性提供一种逻辑接口：MFR 接口。它由多个帧中继物理链路捆绑而成，可以在帧中继网络上提供高速率、大带宽的链路。

捆绑（Bundle）和捆绑链路（Bundle Link）是多链路帧中继的两个基本概念。

一个 MFR 接口对应一个捆绑，一个捆绑中可以包含多个捆绑链路，一个捆绑链路对应着一个物理接口。捆绑对它的捆绑链路进行管理。对于实际的物理层可见的是捆绑链路；对于实际的数据链路层可见的是捆绑。二者的关系如 [图 2-1](#) 所示。

图2-1 Bundle 和 Bundle Link 示意图



捆绑建立后，捆绑链路之间通过定期发送 Hello 消息维护链路状态，当 Hello 消息重发次数达到最大值而仍没有收到应答，系统就认为此捆绑链路的链路层协议发生故障。

MFR 接口的功能和配置与帧中继接口相同，也支持 DTE、DCE 接口类型，并支持 QoS 队列机制。当多个物理接口捆绑为一个 MFR 接口后，这些物理接口原来配置的网络层和帧中继链路层参数将不再起作用，而是使用该 MFR 接口的参数。

2.2 多链路帧中继配置任务简介

多链路帧中继配置任务如下：

- (1) [配置MFR捆绑](#)
- (2) [配置捆绑链路](#)

2.3 配置MFR捆绑

2.3.1 创建MFR接口

- (1) 进入系统视图。
`system-view`
- (2) 创建 MFR 接口并进入该 MFR 接口视图。


```
interface mfr { interface-number | interface-number.subnumber [ p2mp | p2p ] }
```

在创建 MFR 子接口之前，MFR 主接口必须已经存在，否则无法创建 MFR 子接口。

- (3) (可选) 配置 MFR 接口的描述信息。

```
description text
```

缺省情况下，MFR 接口的描述信息为“该接口的接口名 Interface”，比如：MFR4 Interface。

- (4) (可选) 设置捆绑标识符。

```
mfr bundle-name name
```

缺省情况下，捆绑标识符是“MFR 帧中继捆绑编号”，例如：MFR4。

设置标识符时不允许出现“MFR 数字”形式。

- (5) (可选) 开启 MFR 分片功能。

```
mfr fragment enable
```

缺省情况下，多链路帧中继捆绑的分片功能处于关闭状态。

- (6) (可选) 设置 MFR 滑动窗口的尺寸。

```
mfr window-size number
```

缺省情况下，滑动窗口尺寸等于 MFR 捆绑的物理接口数。

- (7) (可选) 设置捆绑链路允许的最大分片。

```
mfr fragment size size
```

缺省情况下，最大分片是 300 字节。

- (8) (可选) 开启 MFR 子接口的速率统计功能。

```
sub-interface rate-statistic
```

缺省情况下，MFR 子接口的速率统计功能处于关闭状态。

开启子接口速率统计功能后，用户可以定时通过 **display interface** 命令查看统计结果。

开启本功能后可能需要耗费大量系统资源，请谨慎使用。

- (9) (可选) 配置 MFR 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)。

- (10) 打开 MFR 接口。

```
undo shutdown
```

缺省情况下，MFR 接口处于打开状态。

- (11) (可选) 配置 MFR 接口的其它参数。

除 **fr interface-type** 命令和 **fr inarp** 命令只能用于 MFR 主接口，不能用于 MFR 子接口外，其余配置均可在 MFR 主接口和子接口上执行。详细介绍请参见“[1 帧中继](#)”。

2.3.2 恢复MFR接口的缺省配置

1. 配置限制和指导

接口下的某些配置取消后，会对现有功能产生影响，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 MFR 接口视图。

```
interface mfr { interface-number | interface-number.subnumber [ p2mp | p2p ] }
```

- (2) 恢复 MFR 接口的缺省配置。

```
default
```

2.4 配置捆绑链路

1. 配置限制和指导

- 建议对同一个 MFR 接口捆绑速率一致的物理接口，以减少管理开销。
- 目前仅支持同步串口和 POS 接口作为捆绑链路的物理接口。

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) 将当前接口封装为多链路帧中继捆绑类型。

```
link-protocol mfr
```

缺省情况下，接口为 PPP 封装。

- (4) 将当前接口捆绑到指定的 MFR 接口。

```
fr mfr interface-number
```

缺省情况下，接口不与任何 MFR 接口捆绑。

- (5) （可选）设置捆绑链路标识符名称。

```
mfr link-name name
```

缺省情况下，捆绑链路标识符是当前接口的名称。

- (6) （可选）设置捆绑链路的 Hello 消息发送周期。

```
mfr timer hello seconds
```

缺省情况下，捆绑链路的 Hello 消息发送周期为 10 秒。

- (7) （可选）设置捆绑链路重发 Hello 消息前等待 Hello 应答消息的时间。

```
mfr timer ack seconds
```

缺省情况下，重发 Hello 消息前等待 Hello 应答消息的时间为 4 秒。

(8) (可选) 设置捆绑链路最多可重发 Hello 消息的次数。

```
mfr retry retries
```

缺省情况下，发送 Hello 消息的重试次数 2 次。

2.5 多链路帧中继显示和维护

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多链路帧中继的运行情况，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 MFR 接口的统计信息。

表2-1 多链路帧中继显示和维护

配置	命令
查看MFR接口的配置和状态信息	<code>display interface [mfr [interface-number]] [brief [description down]]</code>
查看多链路帧中继捆绑和捆绑链路的配置和统计信息	<code>display mfr [interface interface-type interface-number] [verbose]</code>
清除接口的统计信息	<code>reset counters interface [mfr [interface-number interface-number.subnumber]]</code>

2.6 多链路帧中继典型配置举例

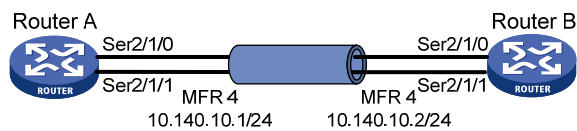
2.6.1 多链路帧中继典型配置举例

1. 组网需求

路由器 Router A 和 Router B 之间分别通过接口 Serial2/1/0 和接口 Serial2/1/1 直连，使用多链路帧中继协议将两个接口捆绑以提供更大的带宽。

2. 组网图

图2-2 多链路帧中继直连组网图



3. 配置步骤

(1) 配置 Router A

配置 MFR4 接口的 IP 地址。

```
<RouterA> system-view
[RouterA] interface mfr 4
[RouterA-MFR4] ip address 10.140.10.1 255.255.255.0
```

```

# 配置 MFR4 接口的接口类型为 DTE。
[RouterA-MFR4] fr interface-type dte
# 配置 MFR4 接口的静态地址映射。
[RouterA-MFR4] fr map ip 10.140.10.2 100
[RouterA-MFR4] quit
# 将接口 Serial2/1/0 和接口 Serial2/1/1 捆绑至 MFR4。
[RouterA] interface serial 2/1/0
[RouterA-Serial2/1/0] link-protocol mfr
[RouterA-Serial2/1/0] fr mfr mfr4
[RouterA-Serial2/1/0] quit
[RouterA] interface serial 2/1/1
[RouterA-Serial2/1/1] link-protocol mfr
[RouterA-Serial2/1/1] fr mfr mfr4
[RouterA-Serial2/1/1] quit

```

(2) 配置 Router B

```

# 配置 MFR4 接口的 IP 地址。
<RouterB> system-view
[RouterB] interface mfr 4
[RouterB-MFR4] ip address 10.140.10.2 255.255.255.0
# 配置 MFR4 接口的接口类型为 DCE。
[RouterB-MFR4] fr interface-type dce
# 配置 MFR4 接口的本地虚链路。
[RouterB-MFR4] fr dlci 100
[RouterB-MFR4-fr-dlci-100] quit
# 配置 MFR4 接口的静态地址映射。
[RouterB-MFR4] fr map ip 10.140.10.1 100
[RouterB-MFR4] quit
# 将接口 Serial2/1/0 和接口 Serial2/1/1 捆绑至 MFR4。
[RouterB] interface serial 2/1/0
[RouterB-Serial2/1/0] link-protocol mfr
[RouterB-Serial2/1/0] fr mfr mfr4
[RouterB-Serial2/1/0] quit
[RouterB] interface serial 2/1/1
[RouterB-Serial2/1/1] link-protocol mfr
[RouterB-Serial2/1/1] fr mfr mfr4
[RouterB-Serial2/1/1] quit

```

4. 验证配置

在 Router A 上通过 **display fr pvc** 命令可以查看接口 MFR4 的 PVC 信息，发现 PVC 的状态为 Active。

```

[RouterA] display fr pvc
PVC information for interface MFR4 (DTE, physically up)
  DLCI: 100  Type: Static  Interface: MFR4
  Encapsulation: IETF
  Creation time: 2014/08/18 06:38:00  Status: Active
  Input: 0 packets, 0 bytes, 0 dropped

```

Output: 0 packets, 0 bytes, 0 dropped

Router A 和 Router B 可以互相 ping 通对方。

```
[RouterA] ping 10.140.10.2
```

```
Ping 10.140.10.2 (10.140.10.2): 56 data bytes, press CTRL_C to break
```

```
56 bytes from 10.140.10.2: icmp_seq=0 ttl=255 time=76.007 ms
```

```
56 bytes from 10.140.10.2: icmp_seq=1 ttl=255 time=8.790 ms
```

```
56 bytes from 10.140.10.2: icmp_seq=2 ttl=255 time=1.630 ms
```

```
56 bytes from 10.140.10.2: icmp_seq=3 ttl=255 time=0.841 ms
```

```
56 bytes from 10.140.10.2: icmp_seq=4 ttl=255 time=1.012 ms
```

```
--- Ping statistics for 10.140.10.2 ---
```

```
5 packets transmitted, 5 packets received, 0.0% packet loss
```

```
round-trip min/avg/max/std-dev = 0.841/17.656/76.007/29.326 ms
```