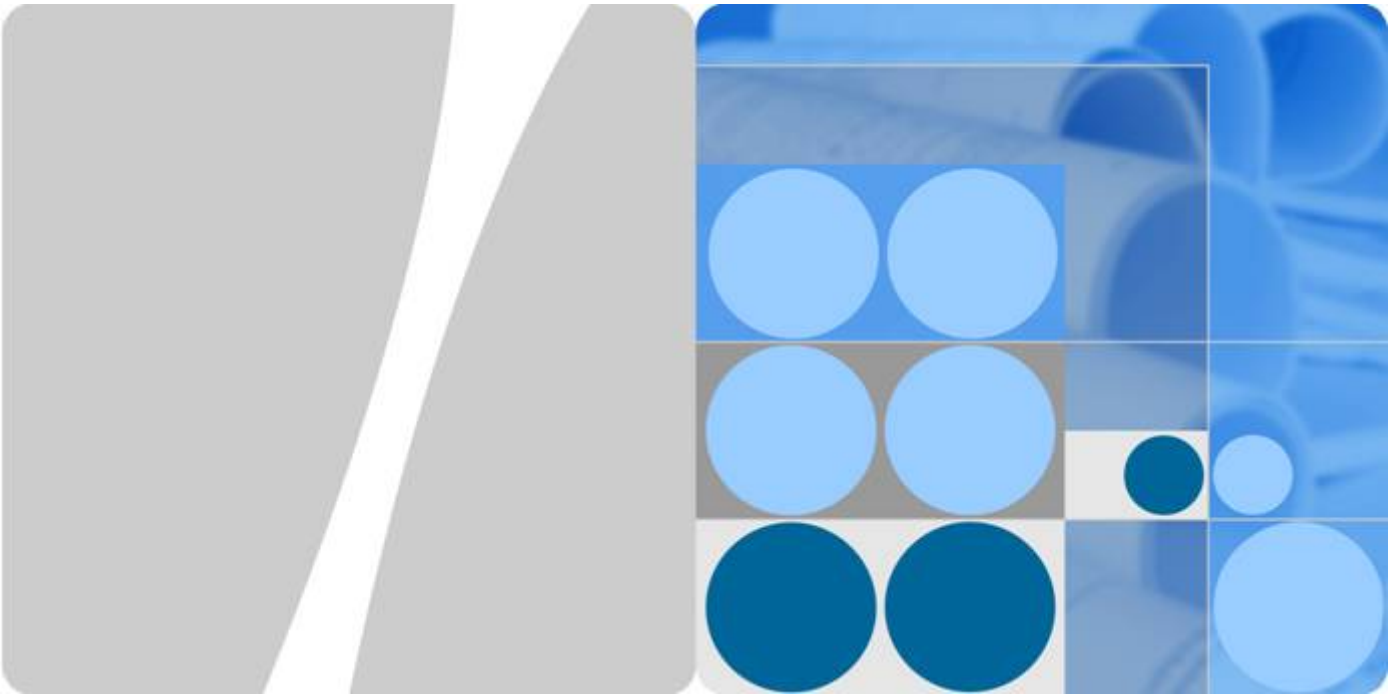


# Huawei AR200-S 系列企业路由器

# V200R002C00

# 特性描述-广域网互联

文档版本　01

发布日期　2011-12-30

华为技术有限公司

## 商标声明


和其他华为商标均为华为技术有限公司的商标。
本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

## 注意

您购买的产品、服务或特性等应受华为公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为公司对本文档内容不做任何明示或默示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

# 华为技术有限公司

地址： 深圳市龙岗区坂田华为总部办公楼 邮编：518129

网址： http://www.huawei.com

客户服务邮箱： support@huawei.com

客户服务电话： 4008302118

# 前 言

## 读者对象

本文档针对 AR200-S 的广域网互联特性，从简介、原理描述和应用三个方面介绍 AR200-S 支持的各种广域网协议。包括，ATM、FR、PPPoE、PPP 和 MP 等。

本文档与其它类型手册相结合，便于读者深入掌握特性的实现原理。

本文档主要适用于以下工程师：

- 网络规划工程师
- 调测工程师
- 数据配置工程师
- 系统维护工程师

## 符号约定

在本文中可能出现下列标志，它们所代表的含义如下。

| 符号 | 说明 |
| --- | --- |
| 危险 | 以本标志开始的文本表示有高度潜在危险，如果不能避免，会导致人员死亡或严重伤害。 |
| 警告 | 以本标志开始的文本表示有中度或低度潜在危险，如果不能避免，可能导致人员轻微或中等伤害。 |
| 注意 | 以本标志开始的文本表示有潜在风险，如果忽视这些文本，可能导致设备损坏、数据丢失、设备性能降低或不可预知的结果。 |
| 窍门 | 以本标志开始的文本能帮助您解决某个问题或节省您的时间。 |
| 说明 | 以本标志开始的文本是正文的附加信息，是对正文的强调和补充。 |

# 命令行格式约定

| 格式 | 意义 |
| --- | --- |
| **粗体** | 命令行关键字（命令中保持不变、必须照输的部分）采用**加粗**字体表示。 |
| *斜体* | 命令行参数（命令中必须由实际值进行替代的部分）采用*斜体*表示。 |
| [ ] | 表示用“[ ]”括起来的部分在命令配置时是可选的。 |
| { x \| y \| ... } | 表示从两个或多个选项中选取一个。 |
| [ x \| y \| ... ] | 表示从两个或多个选项中选取一个或者不选。 |
| { x \| y \| ... }* | 表示从两个或多个选项中选取多个，最少选取一个，最多选取所有选项。 |
| [ x \| y \| ... ]* | 表示从两个或多个选项中选取多个或者不选。 |
| &<1-n> | 表示符号&前面的参数可以重复 1 ～ n 次。 |
| # | 由“#”开始的行表示为注释行。 |

# 修订记录

修改记录累积了每次文档更新的说明。最新版本的文档包含以前所有文档版本的更新内容。

## 文档版本 01 (2011-12-30)

第一次正式发布。

# 目 录

# 1 ATM

## 关于本章

介绍了 ATM 接口及协议的基本原理、基本概念和各种应用。

# 1.1 介绍

## 定义

ATM 是原国际电报电话咨询委员会 CCITT（International Telegraph and Telephone Consultative Committee），也就是现在的国际电信联盟-电信标准部 ITU-T（International Telecommunication Union - Telecommunication Standardization Sector）1992 年 6 月定义的信元（Cell）传输标准。

ATM 交换中分组长度固定是 53 字节，简称为信元。根据 ITU-T 定义，ATM 以信元为基本单位进行信息传输、复用和交换。如语音、视频和数据等各种服务类型的信息都是以固定长度的信元为单位来传输的，这样有利于信息的快速传输。

## 目的

ATM 为具有统一结构的网络提供了一种通用且适于不同业务的面向连接型的转移模式。

在千兆以太网技术之前，业界似乎比较倾向于在网络的主干采用 ATM 骨干交换机，以提供高带宽的保证。的确，ATM 曾经以高带宽、提供良好 QoS、传送语音、数据和视频多媒体信息等优点，在网络技术中独树一帜。

但是 ATM 最初的构想是通过 ATM 技术可以解决所有的网络通信问题。由于从一开始定位实现的目标太理想化，从而导致 ATM 实现非常复杂。由于 ATM 技术过于完善，其协议体系的复杂性造成了 ATM 系统研制、配置、管理和故障定位的难度。

所以 ATM 网络设备也非常昂贵，价格一直居高不下。ATM 诞生后始终没有机会建立一个纯 ATM 网来表现其卓越的性能。

到了 90 年代后期，Internet 及相应的 IP 技术以其简单性和灵活性在市场上压倒了 ATM，在应用领域取得了迅猛的发展，使 B-ISDN 计划受到严重冲击。

现在 ATM 更多应用于数据链路层，主要用来传输 IP 分组。不过，ATM 在提供有质量保证的综合业务传送能力方面的优势无可置疑，它仍被公认为 B-ISDN 的最佳传输技术。于是，IP 和 ATM 技术结合起来，形成了 IP over ATM 技术建设宽带网络的新时期。

# 1.2 参考标准和协议

本特性的参考资料清单如下：

| 文档编号 | 描述 |
| --- | --- |
| RFC1755 | ATM Signaling Support for IP over ATM |
| RFC1926 | An Experimental Encapsulation of IP Datagrams on Top of ATM |
| RFC1932 | IP over ATM:A Framework Document |
| RFC2684 | Multiprotocol Encapsulation over ATM Adaptation Layer 5 |

# 1.3 可获得性

## 涉及网元

IPoA、IPoEoA、PPPoA、PPPoEoA 应用时，AR200-S 设备需要和 DSLAM 及 BRAS 设备配合使用。

## License 支持

本特性不需要 License 支持。

## 版本支持

**表 1-1** ATM 特性的版本支持

| 产品 | 最低支持版本 |
| --- | --- |
| AR200-S | V200R002C00 |

## 硬件要求

设备型号为 AR207-S。

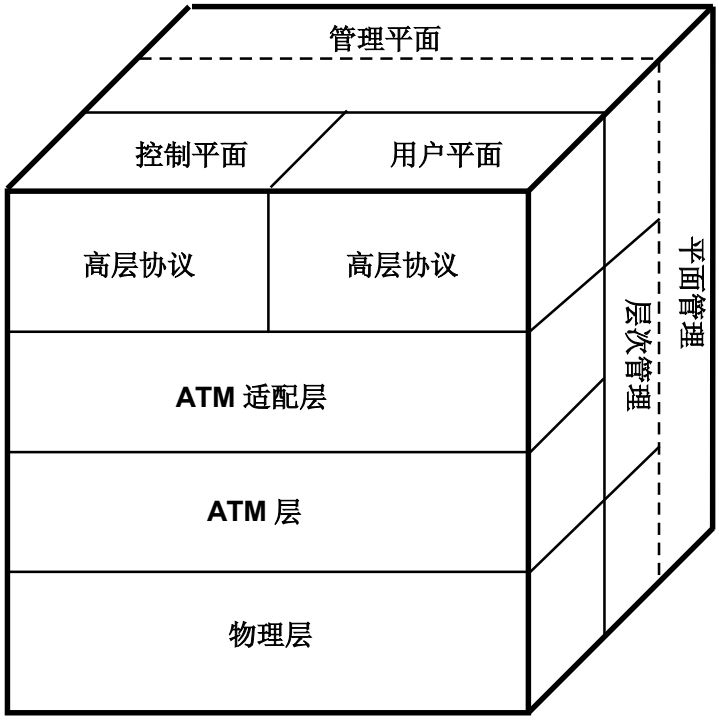
# 1.4 原理描述

# 1.4.1 ATM 的层次结构

## ATM 参考模型

ATM 参考模型的各平面与各层的关系请见图 1-1。

**图 1-1** ATM 参考模型图




ATM 参考模型由以下三个平面组成。

- 控制平面：该平面负责生成和管理信令请求，主要通过信令协议完成连接的建立、监视和拆除。
- 用户平面：该平面负责管理数据的传输。
- 管理平面：该平面包括两部分功能：
  - 层次管理：负责管理各平面中的各层。具有与其它平面相对应的层次结构。
  - 平面管理：负责管理系统和各平面之间的通信。

ATM 参考模型又由以下四个层组成。

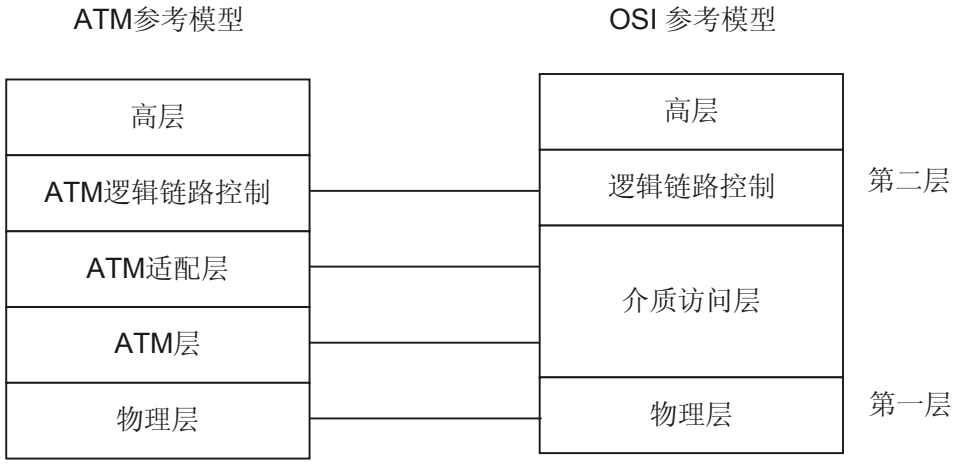
- 物理层：与 OSI 参考模型的物理层类似，主要管理与介质相关的传输。
- ATM 层：与 ATM 适配层结合在一起，与 OSI 参考模型的数据链路层类似。ATM 层主要负责共享物理链路上的虚电路和在 ATM 网络中传输 ATM 信元。
- ATM 适配层 AAL（ATM Adaptation Layer）：与 ATM 层结合在一起，与 OSI 参考模型的数据链路层类似。ATM 适配层主要负责把高层协议与 ATM 层的详细处理隔离开。它主要准备用户数据到信元的转换及将用户数据分割成 48 字节大小的信元有效载荷。
- 高层：接收用户数据，将其组成数据包，然后交给 ATM 适配层处理。

ATM 的每个平面都跨越所有层。ATM 参考模型的各层中还有更精细的子层划分，将在本章后续部分进行介绍。

ATM 参考模型与 OSI 参考模型和 TCP/IP 参考模型都不相同。

ATM 参考模型和 OSI 参考模型层次结构的比较如图 1-2 所示。

**图 1-2** ATM 参考模型和 OSI 参考模型比较




## ATM 各层和子层的功能概述

ATM 参考模型中的各层和子层的功能概括如表 1-2 所示。

**表 1-2** ATM 参考模型中各层和子层的功能

| ATM 参考模型的层次 | ATM 参考模型的子层 | 功能 |
| --- | --- | --- |
| AAL 层 | CS | 汇聚子层，提供标准的接口。 |
| | SAR | 分段和重组子层。 |
| ATM 层 | | ● 流控制<br>● 信元头的生成和提取<br>● 虚电路 VPI/VCI 管理<br>● 信元多路复用/解复用 |
| 物理层 | TC | ● 信元速率解耦合<br>● 头部校验和的生成和检验<br>● 信元的产生、适配和恢复 |
| | PMD | ● 时钟恢复<br>● 线路编码<br>● 物理网络访问 |

ATM 参考模型中各层和子层的详细功能介绍请参看本文档后面的介绍。

# 1.4.2 ATM 物理层

ATM 物理层位于 ATM 参考模型的底层，它涉及具体的传输介质。ATM 物理层主要在高层与传输介质之间传送有效的信元和相应的定时信号。

AR200-S 设备的 ADSL 接口和 G.SHDSL 接口支持工作在 ATM 模式，提供 ATM 特性。因此，对于 AR200-S 设备来说，ATM 物理层即为 ADSL 接口或 G.SHDSL 接口。

AR200-S 支持的 G.SHDSL 接口的传输标准为：

- G.991.2 Annex A：G.991.2 Annex A 标准为北美标准。
- G.991.2 Annex B：G.991.2 Annex B 标准为欧洲标准。

AR200-S 支持的 ADSL 接口的传输标准为:

- G.DMT（G992.1）
- ADSL2（G992.3）
- ADSL2+（G992.5）
- T1.413
- AnnexL
- AnnexM

  说明

  AR200-S 支持的 ADSL 单板分为 ADSL-A/M 和 ADSL-B，仅 ADSL-A/M 支持此标准。

具体标准内容请参见 ITU-T 颁布的标准。

## 1.4.3 ATM 层

### ATM 层的基本功能

ATM 层位于物理层之上，负责通过 ATM 网络对信元进行交换和多路复用。

输入 ATM 层的是 48 字节的净荷，被称为分段和重组协议数据单元 SAR-PDU（Segmentation And Reassembly-Protocol Data Unit），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 层的基本功能概括讲有以下三点：

- 负责产生 5 个字节的信元头和对信元头的校验
- 传输虚电路号 VPI/VCI，对信元进行多路复用/解复用
- 一般流量控制 GFC（Generic Flow Control）

### ATM 的网络接口

ATM 网络由一组通过点到点的 ATM 接口互连的 ATM 交换机构成。ATM 网络接口类型主要有以下几种：

- 用户网络接口

  UNI（User-to-Network Interface）是指连接外围设备与 ATM 交换机之间的接口。

  根据交换机是由客户端所有还是由运营商所有，UNI 还可以分为两种：公共 UNI 和专有 UNI。

  专有 UNI 将 ATM 外围设备连接到专有 ATM 交换机上；公共 UNI 将 ATM 外围设备或 ATM 专有交换机连接到公共交换机上。

- 网络-网络接口

  NNI（Network-to-Network Interface）是指连接 ATM 交换机之间的接口。

  根据交换机是由客户端所有还是由运营商所有，NNI 也可以分为两种：公共 NNI 和专有 NNI。

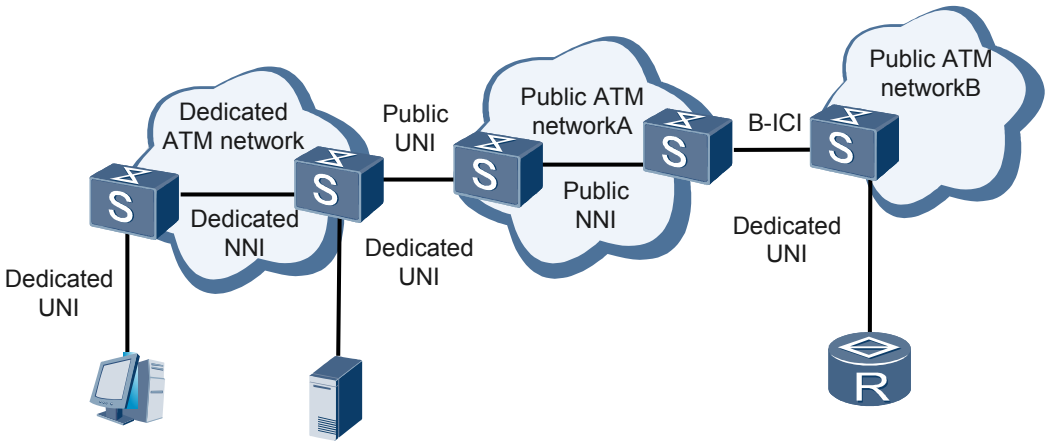
专用 NNI 连接同一专有 ATM 网络的两台交换机，是在专用 ATM 网络内使用的；公共 NNI 则连接同一公共网络运营商的两台 ATM 交换机，由一个 ATM 服务提供商使用。

- 宽带载波间接口

  B-ICI（B-ISDN Inter Carrier Interface）接口是指连接不同网络运营商的公共交换机之间的接口，提供对多个 ATM 网络运营商的内部连接。B-ICI 与 NNI 直接相连。

  各种 ATM 网络接口的连接如图 1-3 所示。

**图 1-3 专用和公共网络的 ATM 网络接口**




说明

AR200-S 支持的 ATM 网络接口类型只有“用户网络接口”。

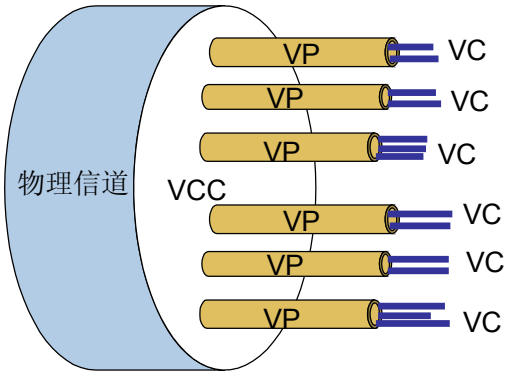
## ATM 虚电路

在 ATM 中，使用 VPI/VCI 来标识一条虚电路。VPI/VCI 的值只是在本地接口才有意义。

VPI 用于标识虚电路连接的虚通道号，而 VCI 用于标识虚通道中的虚电路号。两者的组合构成了虚拟连接标识符。

如图 1-4 所示，一条虚电路连接 VCC（Virtual Circuit Connection）包含了多条虚通道 VP，一条 VP 又包含了多条虚电路 VC。

**图 1-4 VP 和 VC 的关系图**



虚通道概念的发展是为了适应高速网络的趋势，在这种网络中，网络控制开销占整个网络开销的比例正在日益增大。虚通道技术通过将共享网络中相同通道的连接绑定为一个单元来降低控制开销。这样，网络管理就可以只处理数量较少的连接组而不是大量的独立连接。

在 ATM 通信中，ATM 交换机根据输入信元的 VPI/VCI 标识和在连接建立时产生的路由表，把到达的信元交换到相应的输出接口。同时，将信元中的 VPI/VCI 改变为出接口的 VPI/VCI，完成 VP 交换或 VC 交换以及数据的转发。

ATM 虚电路有三种，分别是永久虚电路 PVC、交换虚电路 SVC（Switched Virtual Circuit）和 Soft VC（Soft Virtual Circuit）。

- PVC 是通过管理员静态配置的，一旦连接就不会自动释放。适合一直使用有高级需求的连接。
- SVC 是通过信令方式建立的，可以通过命令的方式建立连接和释放。

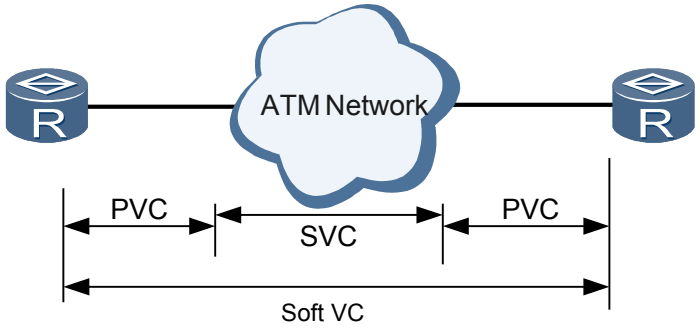
  每个节点收到其他节点发来的建立请求时，如果满足配置要求，需要向此节点发送连接响应信息。等连接建立后再向下一个目标节点发送建立连接请求。

  链路的释放过程同建立连接类似。
- Soft VC 是指 ATM 网络是基于 SVC 的，而外围设备通过 PVC 方式接入 ATM 网络中。

  Soft VC 建立步骤同 SVC 类似。唯一不同的是，外围设备和 ATM 交换机入口出口间必须手工配置 PVC。

  这种方式的优点是，PVC 连接到用户便于对用户的管理。而 SVC 又能保障骨干链路的合理利用。

**图 1-5** Soft VC



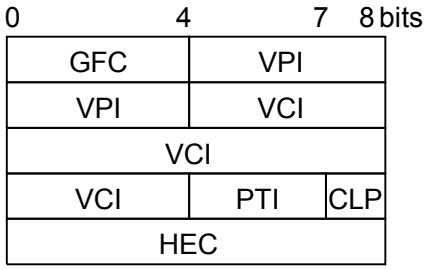

## ATM 信元头格式

ATM 信元头根据网络接口的不同分为 UNI 和 NNI 两种信元头类型。

UNI 信元头用于在 ATM 专用网络中的 ATM 终端设备和 ATM 交换机间的通信。

UNI 信元头格式如图 1-6 所示。

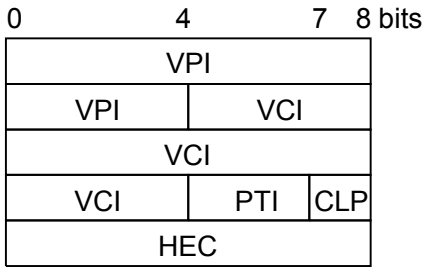
**图 1-6** ATM UNI 信元头格式




NNI 信元头格式用于两个 ATM 交换机之间的通信。

NNI 信元头格式如图 1-7 所示。

**图 1-7** ATM NNI 信元头格式




上面两个图中的各字段解释如下。

- GFC：一般流量控制，长度是 4 比特，只用于 UNI 接口，进行流量控制或在共享媒体的网络中标识不同的接入访问。
- VPI：虚通道标识符，在 UNI 中长度是 8 比特，可标识 256 个 VP；在 NNI 中长度是 12 比特，可标识 4096 个 VP。
- VCI：虚通路标识符，长度是 16 比特，可标识 65536 个 VC。
- CLP：信元丢弃优先等级（Cell Loss Priority），长度是 1 比特，用于拥塞控制。发生拥塞时优先丢弃 CLP=1 的信元。
- PTI：净荷类型标识（Payload Type Indicator），长度是 3 比特，用于标识净荷的类型。
- HEC：信头差错控制，长度是 8 比特，用于信元头中的差错控制和信元定界。可纠正 1 位错码，发现多位错码。在物理层进行 HEC 处理。

对于一些特定的 VPI/VCI 值已经保留作为特殊信元使用，下面对它们进行简单介绍。

- 空闲信元：VPI=0，VCI=0，PTI=0，CLP=1，用于速率适配。
- 未赋值信元：VPI=0，VCI=0，PTI=任意值，CLP=1。
- OAM 信元：
  - 对于 VP，VCI=3 用于 VP 链路；VCI=4 用于 VP 连接。
  - 对于 VC，PTI=4 用于 VC 链路；PTI=5 用于 VC 连接。

- 信令信元：它分为以下三种类型：
  - 元信令信元：VPI 为任意值，VCI=1。
  - 一般广播信令信元：VPI 为任意值，VCI=2。
  - 点对点信令信元：VPI 为任意值，VCI=5。
- 净荷类型 PT（Payload Type）：该域长度是 3 比特。用于标识信息域，也就是净荷的类型。下面列出的是 ITU-T I.361 已定义的 PT 值及其含义。
  - PT=000：用户数据信元，未经历拥塞，ATM 层用户到 ATM 层用户指示 AUU（ATM User to User）为 0。
  - PT=001：用户数据信元，未经历拥塞，AUU=1。
  - PT=010：用户数据信元，经历拥塞，AUU=0。
  - PT=011：用户数据信元，经历拥塞，AUU=1。
  - PT=100：OAM F5 段相关信元。
  - PT=101：OAM F5 端到端相关信元。
  - PT=110：资源管理信元。
  - PT=111：将来用。

由此可见，当信元用于承载用户数据时：

- PT 第一位为 0。
- 第二位标识信元是否经历拥塞，这一位可通过处于拥塞的网络节点设置。
- 第三位是 AUU 指示，其中，AUU=0 表明对应的 SAR-PDU 是起始段或中间段，AUU=1 表明为结束段。

## ATM OAM

OAM（Operation, Administration and Maintenance）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。ITU-T B-ISDN（Broadband-Integrated Services Digital Network）系列的 I.610 定义了 ATM 网络的 OAM 功能，将 ATM 网络中的 OAM 功能划分为如表 1-3 所示的 5 层。

**表 1-3** OAM 功能层次划分

| 层次 | 说明 |
| --- | --- |
| F1：再生段层 | 物理层 OAM：物理层 OAM 流依赖于具体传输系统的传输机制，ATM 网络中包括三种传输机制：<br>● 基于 SDH 的传输系统（G.707 和 G.783 中定义）；<br>● 基于信元的传输系统（I.432.1、I.432.2 和 I.432.4 中定义）；<br>● 基于 PDH 的传输系统（G.702、G.804 和 G.832 中定义）。 |
| F2：数字段层 | |
| F3：传输通道层 | |
| F4：VP（Virtual Path）层 | ATM 层 OAM：基于 VP/VC 的 OAM 功能，不依赖于传输系统。 |
| F5：VC（Virtual Channel）层 | |

其中，在 ATM 层定义了两种操作流：F4 和 F5。

- F4 流为 VPC（Virtual Path Connect）中的 OAM 信元流，提供 VP 级的操作管理与维护功能；
- F5 流为 VCC（Virtual Channel Connect）中的 OAM 信元流，提供 VC 级的操作管理与维护功能。

当 OAM 在 F4 和 F5 上被激活之后，特定的 OAM 信元就被插入到用户信元中，和其他的用户信元在相同的物理通道上传输并占用一定的带宽。

F4 和 F5 流支持四种类型的 OAM 信元：故障管理 OAM 信元，性能管理 OAM 信元，激活-去激活 OAM 信元和系统管理 OAM 信元，如**表 1-4**。

**表 1-4** ATM 层 OAM 功能

| 信元类型 | 内容 | 说明 |
| --- | --- | --- |
| FM（故障管理） | AIS（用于向下游报告错误） | 故障管理 OAM 信元用来实现 in-service（实时、不中断业务）的故障检测和故障定位。 |
| | RDI（用于向上游报告错误） | |
| | LoopBack（用于链路通断性检测和错误定位） | |
| | CC（连续性检测） | |
| PM（性能管理） | FM（前向性能监视） | 性能管理 OAM 信元用来实现性能监测的功能。 |
| | BM（后向性能监视） | |
| Active/Deactive（激活/去激活） | Active PM（激活性能监视功能） | 激活/去激活 OAM 信元用来激活和去激活 OAM 信元的产生和处理。 |
| | Active CC（激活连续检测功能） | |
| | Deactive PM（去激活性能监视功能） | |
| | Deactive CC（去激活连续检测功能） | |
| SM（系统管理） | 仅可由终端系统使用 | 系统管理 OAM 信元用来维护和控制终端用户设备之间的不同功能，只能在端到端的 F4/F5 上存在。 |

在 ATM 网络中，实现 OAM 功能节点有以下三种类型：

- 端端点

  在 I.610 中定义为 ATM 网络连接的端点，一般指 ATM 网络的边界。端端点是一切 OAM 信元的终结点。如果端端点监测到链路故障，它不向下游插入 OAM 信元，而是反方向插入端 RDI（Remote Defect Indication）信元，告知上游链路故障。

- 段端点

  在 I.610 中定义为段的端点。一条 ATM 链路可以由多个段组成。段端点不能终结端信元，但终结所有段信元。段端点监测到故障后只会向下游插入端 AIS（Alarm Indication Signal）信元，同时反向插入段 RDI 信元。

- 中间点

  位于两个段或端端点之间的 OAM 节点，可以再分为端中间点和段中间点。中间点不终结任何信元，段、端信元都能透传过去。如果中间点监测到链路故障，它将向下游发送段 AIS 信元和端 AIS 信元。

AR200-S 设备支持 VC 层 OAM（F5），支持故障管理 OAM 信元。AR200-S 设备实现 OAM 功能时，只能作为端端点。

## 1.4.4 ATM 适配层

### AAL 的层次

AAL 是高层协议与 ATM 层间的接口，主要负责转发 ATM 层与高层协议之间的信息。

AAL 位于 ATM 层之上，与 OSI 参考模型的数据链路层相对应。

AAL 分为以下两层：

- 汇聚子层

  汇聚子层 CS（Convergence Sub-layer）又包含以下两层：

  - 业务特定汇聚子层 SSCS（Service Special Convergence Sub-layer）
  - 公共部分汇聚子层 CPCS（Common Part Convergence Sub-layer）

  CS 子层的作用是将上层的信息转化为一种适应分段的，相同大小的 ATM 净荷。

  SSCS 部分与各种业务的特性相关联。CPCS 则通过在帧的前后加入可变长度的填充字符来形成帧，进行错误检测。同时支持通过填充使帧成为净荷（48 字节）的整数倍。

- 分组和重组子层

  分组和重组子层 SAR（Segmentation And Reassembly）的作用是在外围设备向外发送数据时，把聚合的帧分成相等大小的 48 字节净荷；在外围设备接收数据时，把 48 字节的净荷重新组装为聚合帧。

### AAL 的类型

目前，已经提出 4 种类型的 AAL：AAL1、AAL2、AAL3/4 和 AAL5，每一种类型支持 ATM 网中某些特征业务。大多数 ATM 设备制造商现在生产的产品普遍采用 AAL5 来支持数据通信业务。

说明

AR200-S 设备仅支持 AAL5。

- AAL1

  AAL1 用于 CBR（Constant Bit Rate）类型，以固定的间隔发送数据。

  AAL1 使用 48 字节净荷内的一部分承载如序列号 SN（Sequence Number）和序列号保护 SNP（Sequence Number Protection）等附加信息。其中 SN 包括 1 位汇聚子层指示 CSI（Convergence Sub-layer Identifier）和 3 位序列计数 SC（Sequence Counting）。CSI 还用于定时。

- AAL2

  AAL2 与 AAL1 相比，主要改进的地方是可以传输压缩语音，以及可以在 ISDN 内实现通用信道信令 CCS（Common Channel Signaling）。

  在 ITU-T 363.2 规范中定义了 AAL2 的细节。

  AAL2 支持以 5.3 Kbit/s 的上限速率处理压缩语音，实现了静音检测、抑制、消除和 CCS。并提供了更大的带宽利用率。也提供了把小分组封装到一个或多个 ATM 信元的功能。

  AAL2 的 CS 子层也是分为 CPCS 和 SSCS，SSCS 在 CPCS 之上。在 CPCS 上，可以识别 AAL2 用户的基本结构、进行差错检验、对数据封装或分解各种净荷。

  AAL2 的特殊之处是允许在一个 ATM 信元内或在多个 ATM 信元内存在可变长度的净荷。

- AAL3/4

  AAL3/4 是第一种尝试实现信元延迟的技术，规定面向连接和无连接的数据传输。

  CPCS 的作用是差错检测和处理，标识将要传输的 CPCS-SDU（Service Data Unit）并决定 CPCS-PDU 的长度。

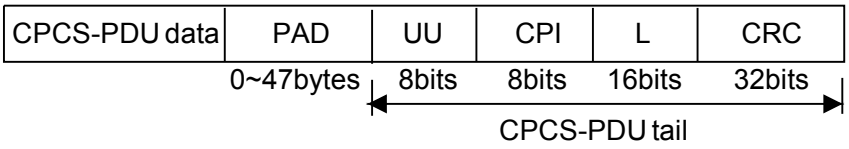
- AAL5

  AAL5 也能够处理面向连接和无连接的数据。AAL5 被称为简单和有效的适配层。它使用整个 48 字节承载净荷。没有使用额外的信息位，没有序列号，没有信元差错等功能。

  AAL5 SAR 子层非常简单，只是将 CPCS-PDU 划分成 48 字节长的 SAR-PDU，不需要任何开销，在接收时实现逆向功能。

  AAL5 CPCS 子层 CPCS-PDU 格式如图 1-8 所示。

  **图 1-8** CPCS-PDU 格式




  CPCS-PDU 净荷的长度是可变的，取值范围是 1 ～ 65535 字节。

  在图 1-8 中可以看到，没有 CPCS-PDU 头，但 CPCS-PDU 尾部占 8 个字节。下面对各个字段做简要说明：

  - PAD：填充位，使整个 CPCS-PDU 长度为 48 字节的整数倍。
  - UU：用于 CPCS 用户信息的透明传输。
  - CPI：用作使 CPCS-PDU 尾部长为 8 个字节。
  - L：指示 CPCS-PDU 的净载荷长度。
  - CRC：保护 CPCS-PDU。

  AAL5 的汇聚子层内的 SSCS 同 AAL3/4 类似，CPCS 也是被所有高层共用。CPCS 对差错进行检查和处理，填充字节完成 48 字节的净荷，丢弃收到不完整的 CPCS-PDU。

# 1.4.5 ATM 多协议封装

RFC2684 中描述的 ATM 多协议封装定义了以 AAL5 帧格式在一个 ATM 网络上传送多协议数据分组的技术标准。

RFC 定义了以下两种格式的封装，它们都是通过 AAL5 的 CPCS 负载区来承载 PDU。AAL5 CPCS-PDU 的格式如图 1-8 所示。

- 逻辑链路控制/子网接入点 LLC/SNAP（Logical Link Control/Sub-Network Attachment Point），是 RFC2684 中使用的缺省封装技术。
- LLC/SNAP 允许在单一的 ATM 虚电路上复用多种协议，承载 PDU 的协议类型通过给 PDU 加一个 IEEE802.2 标准的逻辑链路控制 LLC（Logical Link Control）头部来标识。
- VC 复用
- VC 复用将高层协议类型承载在 ATM 虚电路上，每一种协议都承载在不同的 ATM 虚电路上。

## LLC/SNAP 封装

当需要在相同的一条 VC 上传输多种协议时，就需要使用 LLC 封装。为了保证接收端正确地处理接收到的 AAL5 CPCS-PDU 报文，承载区必须包含必要的信息来标识是路由协议还是桥接协议。在 LLC 封装中，这些信息在承载 PDU 前面的 LLC 头中进行定义。

LLC 有两种类型：

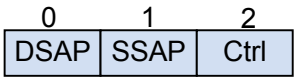
- LLC 类型 1：unacknowledged connectionless mode
- LLC 类型 2：connection-mode

本文档中提到的 LLC，如没有特殊说明，都是指的 LLC 类型 1，在 LLC 类型 2 中的应用类似。

- LLC 封装路由协议

  在 LLC 封装中，路由 PDU 的协议类型必须由每个 PDU 的 IEEE802.2 LLC 头的前缀定义。LLC 头必须包括三个长度都是 1 字节的字段，如图 1-9 所示。

  **图 1-9** LLC 头结构

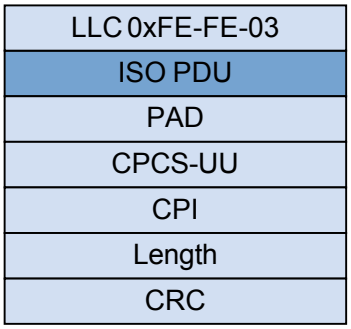
  
  

  在 LLC 封装路由协议中，

  - LLC 头的值是 0xFE-FE-03，标识后面是 ISO NLPID 格式的路由 PDU。
  - Ctrl 字段的值是 0x03，指定是无编号的信息命令 PDU。

  因此，对于 ISO NLPID 格式的路由 PDU，AAL5 CPCS-PDU 有效载荷的格式如图 1-10 所示。

**图 1-10** NLPID 格式的路由 PDU 的格式




各字段的长度如下所示：

- LLC：固定值是 0xFE-FE-03。
- ISO PDU：长度范围是 1 ～ 65532，单位是字节。
- PAD：长度范围是 0 ～ 47，单位是字节。
- CPCS-UU：长度范围是 1，单位是字节。
- CPI：长度范围是 1，单位是字节。
- Length：长度范围是 2，单位是字节。
- CRC：长度范围是 4，单位是字节。

ISO 路由协议必须由一个字节的 NLPID（Network Layer Protocol Identifier）字段来标识，这个字段是协议数据的一部分。NLPID 的值由 ISO 和 ITU-T 来确定。

按照 ISO/IEC TR 9577 中的定义，一个 NLPID 的值为 0x00 是标识空的网络层或者设置为非活动状态。由于在这种封装形式下它没有意义，所以在 ATM 封装中，一个 NLPID 的值为 0x00 是无效的。

尽管用 NLPID 值 0xCC 来标识 IP，但是 NLPID 格式不允许被 IP 使用。所以必须通过 SNAP 头来中标识 IP 报文。

当 LLC 头的值是 0xAA-AA-03 时表示是 IEEE802.1a 的 SNAP 头，其格式如图 1-11 所示。

**图 1-11** SNAP 头格式

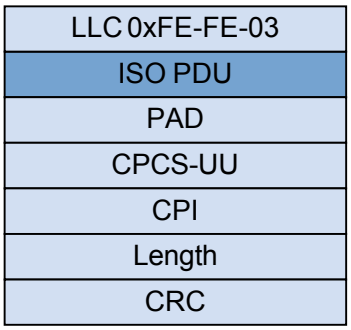

SNAP 头长度是 5 字节，其中：

- 组织唯一标识符 OUI（Organizationally Unique Identifier）：长度是三个字节。由 IEEE 管理，标识后面协议标识符 PID（Protocol Identifier）规定的组织。OUI 的值 0x00-00-00 说明后面的 PID 是以太网类型。
- PID：长度是两个字节。

二者的组合标识一个唯一的路由或桥接协议。

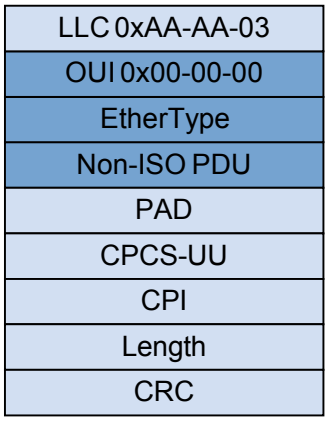
对于非 ISO NLPID 格式路由 PDU，AAL5 CPCS-PDU 有效载荷的格式如图 1-12 所示，其中以太网类型长度是 2 字节。

**图 1-12** 非 ISO NLPID 格式路由 PDU 的有效载荷报文格式




在 IPv4 PDU 报文中，以太网类型的值为 0x08-00，因此报文格式如图 1-13 所示。

**图 1-13** 路由 IPv4 PDU 的格式




- LLC 封装桥协议

  在 LLC 封装中，通过定义 SNAP 头中的桥接介质的类型对桥接 PDU 报文进行封装。

  对于桥接 PDU，LLC 头的值必须是 0xAA-AA-03，表示 SNAP 头。SNAP 头中 OUI 的值是 802.1 组织的代码 0x00-80-C2。

  目前桥接媒体的类型是由两个字节的 PID 指明的。另外，PID 指明在桥接 PDU 中是否保留了帧校验序列 FCS（Frame Check Sequence）。

  用于 ATM 封装的媒体类型如表 1-5 所示。

**表 1-5** OUI 00-80-C2 的局部指定值列表

| 保留 FCS | 不保留 FCS | 媒体类型 |
| --- | --- | --- |
| 0x00-01 | 0x00-07 | 802.3/Ethernet |
| - | 0x00-0D | Fragments |
| - | 0x00-0E | BPDUs |

当 AAL5 CPCS-PDU 的有效载荷承载桥接 PDU 时，必须具有以下几种帧格式中的一种格式。

为了对齐以太/802.3 LLC 数据域，必须在 PID 后面添加一定数量的填充字符。

MAC 地址的位序必须和它在局域网或城域网中相同。

**图 1-14** 以太/802.3 桥接 PDU 有效载荷格式

| LLC 0xAA-AA-03 |
| --- |
| OUI 0x00-80-C2 |
| PID 0x00-01 or 0x00-07 |
| PAD 0x00-00 |
| MAC destination address |
| (remainder of MAC frame) |
| LAN FCS (if PID is 0x00-01) |

为了保证以太/802.3 物理层的帧达到最小长度，可以对其进行填充。当使用带有保留 LAN FCS 的以太/802.3 桥接 PDU 封装格式时，必须添加填充字符。如果不带有保留 LAN FCS 时，可以不添加填充字符。

当收到不带 LAN FCS 的帧时，网桥必须在把帧转发到以太/802.3 子网前插入一些必需的填充字符。

## VC 复用

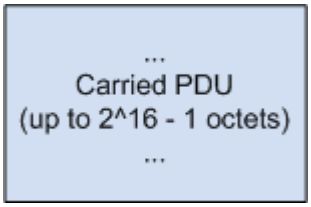
在基于 VC 的多路复用技术中，承载网络互连的协议隐含着由连接两个 ATM 站点的 VC 来区分的。也就是说，每一种协议必须运行于各自不同的 VC 上。

因此在 AAL5 CPCS-PDU 的负载上就没有必要再包含额外的多路复用信息，这样就可以节省带宽并减少处理开销。

- 路由协议的 VC 复用

  在路由协议的 VC 复用中，AAL5 CPCS-PDU 有效载荷的内容只能是路由协议 PDU 报文，其报文格式如**图 1-15** 所示。

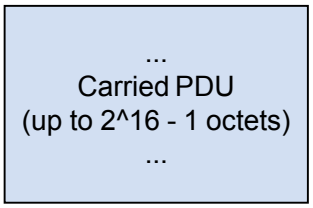
  **图 1-15** 路由协议 PDU 有效载荷格式

- 桥接协议的 VC 复用

  在桥接协议的 VC 复用中，桥协议 PDU 在 AAL5 CPCS-PDU 有效载荷中的承载必须和 **LLC 封装桥协议**中描述的相同，除非必须只有 PID 后的域包含在报文中。

**图 1-16** 以太/802.3 桥接 PDU 有效载荷格式




由于不包含 PID 域，所以在以太/802.3 的 PDU 报文中，LAN FCS 必须由 VC 来确定。虽然桥接介质可能相同，但 PDU 仍可以属于不同协议，不论是否带有 LAN FCS。

## 1.4.6 ATM 业务类型

AR200-S 设备提供的 ATM 特性支持四种业务类型：CBR（Constant Bit Rate）、UBR（Unspecified Bit Rate）、VBR-RT（Variable Bit Rate- Real Time）、VBR-NRT（Variable Bit Rate - Non Real Time）。这些服务类型的选择与网络的 QoS 需求有关。

### 恒定比特流速率 CBR

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

CBR 业务一般用来支持对时延要求较高的实时业务（例如：语音、视频）。

### 实时的可变比特率业务 VBR-RT

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

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

### 非实时的可变比特率业务 VBR-NRT

VBR-NRT 业务支持突发性的非实时的应用，和 VBR-RT 业务相比，VBR-NRT 业务最大的特点就是对业务本身的实时性要求不高，参数和 VBR-RT 业务一样。

### 未定义比特率业务 UBR

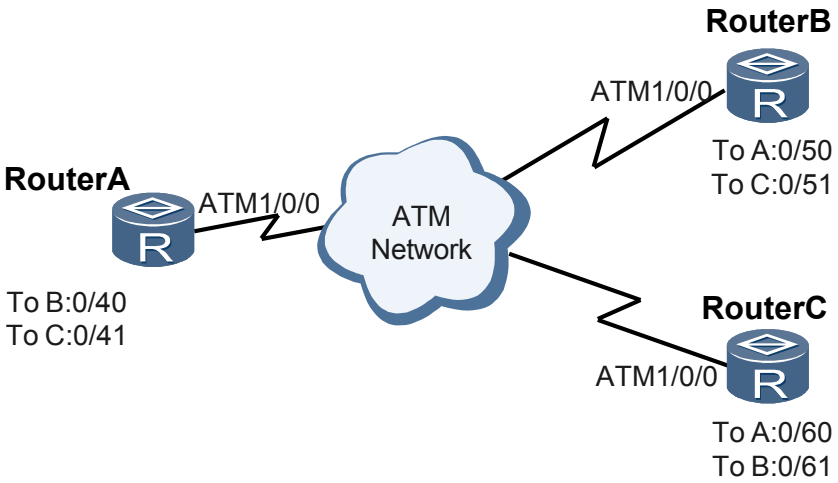
UBR 业务用于对时延和带宽都要求不高的应用，也就是那些对时延和时延变化要求都不太严格的应用。UBR 业务不保证服务质量，连接的信元丢失率和信元传输时延均没有数值保证，如果发生拥塞，UBR 信元最先被丢弃。

# 1.5 应用

## 1.5.1 IPoA

IPoA（IP over AAL5）是指在 AAL5 上承载 IP 协议报文。即将 IP 报文封装在 ATM 信元内在 ATM 网络上传输。

**图 1-17** IPoA 应用组网图




### 实现方法

如图 1-17 所示，在 RouterA 上，有到达 RouterB 的 PVC0/40，也有到达 RouterC 的 PVC0/41。我们希望能将发送给 RouterB 的 IP 报文准确的从 PVC0/40 上发送出去，就需要在 0/40 上映射 RouterB 的 IP 地址。建立映射后，路由器就会建立一条到 RouterB 的 IP 地址的路由，出接口为 ATM 的 PVC0/40 所在的接口。

## 1.5.2 IPoEoA

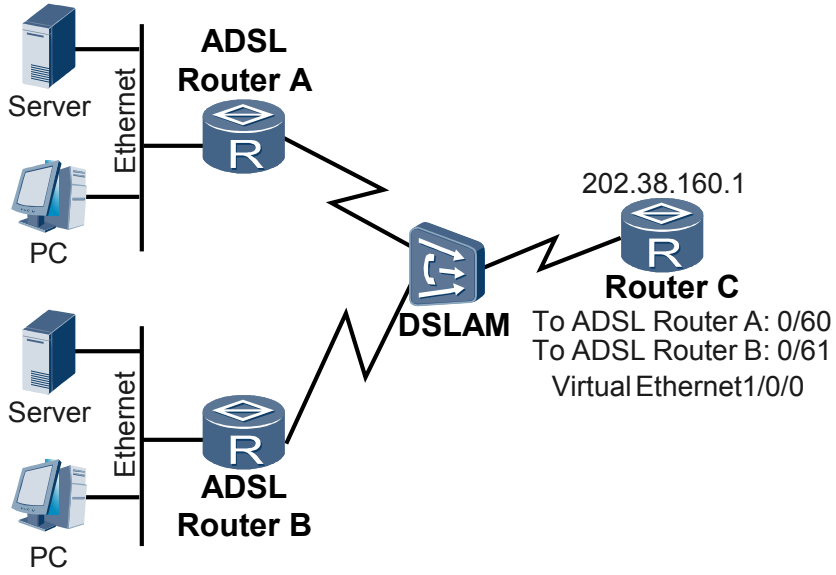
IPoEoA（IP Protocol over Ethernet over AAL5）有三层结构。最上层封装 IP 协议，中间为以太网承载 IP 协议，最下一层为 AAL5 承载 IPoE，通过将 IPoE 的报文封装在 ATM 上传输。

当通过设备高速连入远端的接入服务器，可以采用在 ATM 端口利用 PVC 承载以太网报文来实现对外部网络的访问。

对于 IPoEoA，AR200-S 实现的基本功能有以下两点。

- 一个虚拟逻辑以太网接口 VE（Virtual Ethernet）接口可以关联多个 PVC。
- 和同一个 VE 接口关联的 PVC 之间通过二层互通。

**图 1-18** IPoEoA 组网图




### 实现方法

如图 1-18，采用 IPoEoA 的方式，需要将 IP 报文封装在以太帧内，再封装为 ATM 信元传输。此时设备需要配置 IP 地址和以太网地址，并且通过建立 VE，将 VE 映射到 ATM 的 PVC 上的方式来实现 IPoEoA。也理解为所有由本路由器发送到虚拟以太网接口的报文都通过映射的 ATM 接口封装成 ATM 信元传输。

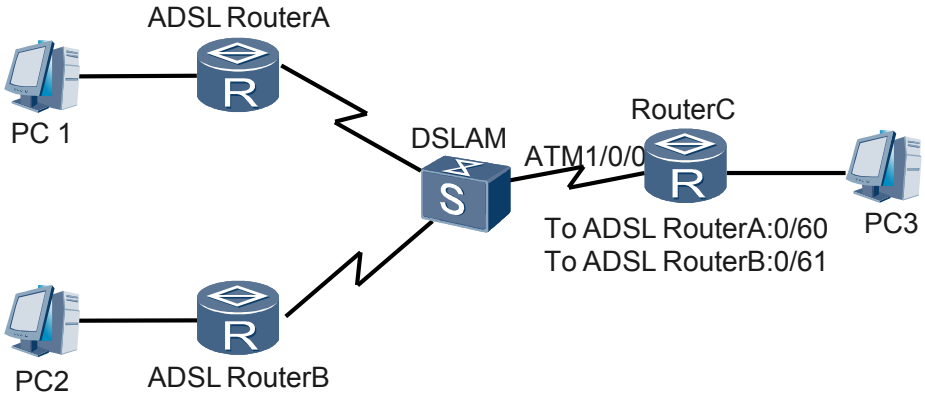
## 1.5.3 PPPoA

PPPoA（PPP over AAL5）是指在 AAL5 上承载 PPP 报文。ATM 信元封装 PPP 报文，PPP 报文封装 IP 或其它协议的报文。在这种模式下，可以将 AAL5 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 的灵活性和广泛的应用性。

为了在 AAL5 上传送 PPP 报文，用户必须创建一个虚拟接口模板 VT（Virtual Template）。PPPoA 的典型组网如图 1-19 所示。

**图 1-19** PPPoA 组网图



### 实现方法

PPPoA 的方式是通过 PPP 的报文封装在 ATM 信元内，在 ATM 网络上传输。原理和 IPoEoA 类似。

因为 PPP 的建立需要认证等相关操作，所以通过建立一个虚拟接口模板的方式来完成。

在 RouterC 上实现认证时，需要在 RouterC 上建立认证的用户名、密码、为用户分配的 IP 地址池。在 VT 上设置本地 IP 地址、远端用户的认证方式（PAP 或 CHAP）、指定为认证用户分配地址的地址池等参数。然后在 ATM 的 PVC 下映射建立的 VT，实现 PPP 同 ATM 之间的关联操作。

而在客户端的 ADSL RouterA 上，只需要建立相应 VT 并映射相应的 ATM 接口上即可。VT 上配置需要在 RouterC 上认证的用户名、密码、认证方式和 IP 地址获取方式等。

## 1.5.4 PPPoEoA

PPPoEoA（PPPoE over AAL5）是指在 AAL5 上承载 PPPoE（PPP over Ethernet）协议报文，其实质是用 ATM 信元封装以太网报文。在这种模式下，可以用一个 PVC 来模拟以太网的全部功能。

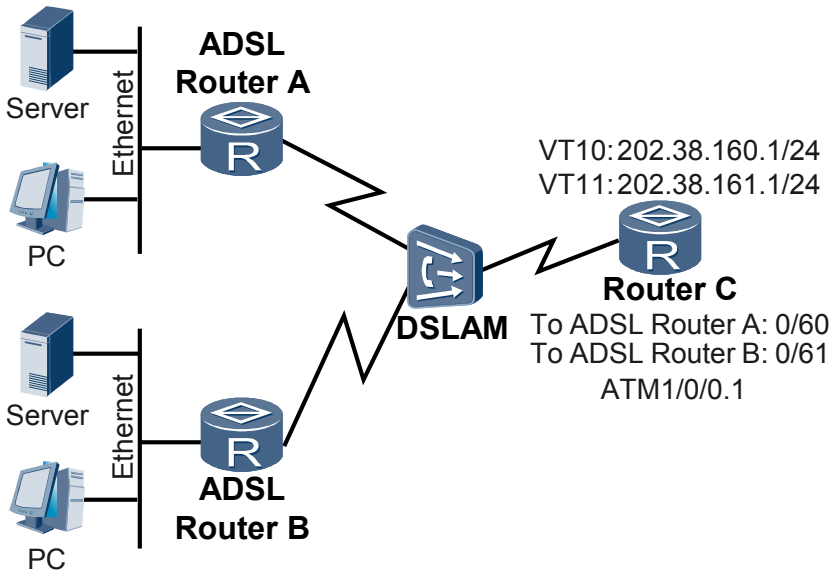
AR200-S 通过 VE 实现在 AAL5 上承载以太网报文。VE 具有以太网的特性，由用户通过配置命令动态创建。

接口的协议栈有如下结构：

- 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。

将 PPP 报文封装在以太网报文内，再将此报文封装在 ATM 网络上传输。

**图 1-20** PPPoEoA 组网图



### 实现方法

PPPoEoA 的实现方法实际上就是在 VT 上实现 PPP 封装，在 VE 上实现将 PPP 封装成 PPPoE，在 ATM 接口上封装为 PPPoEoA 的过程。实现方法和 PPPoA 类似。

首先需要在做认证的路由器上配置用户和地址池等参数，也可以用外置的 RADIUS 等，这里只介绍本机认证方式。在 VT 上的配置同 PPPoA 中介绍的 VT 配置一样。然后再建立一个 VE 接口。在 VE 接口上映射 VT，实现封装或解封装 PPPoE 报文。最后将 VE 映射到 ATM 接口上。

## 1.6 术语与缩略语

### 术语

| 术语 | 解释 |
| --- | --- |
| ATM | 在 ITU-RF. 1499 建议书中，指一种使用固定长度为 53 字节的信元来传输各类数字信号的协议。在 ITU-R M. 1224 建议书中，指一种用信息来构成信元的转移模式；从信元循环取决于所要求的瞬时比特率这一意义上讲，它是非同步的。统计性的和确定性的值也可以用来描述这一转移模式的特性。 |
| Cell | ATM 以信元（Cell）为基本单位进行信息传输、复用和交换。ATM 信元具有 53 字节的固定长度，其中 5 个字节构成信元头，主要用作路由信息和优先级信息，其余 48 个字节是有效载荷。 |
| Multi-network PVC | 当一个 PVC 经过多个网络时，该 PVC 称为多网络 PVC（Multi-network PVC）。它是由每个单一网络的 PVC 构成，这种单一网络的 PVC 称为 PVC 段（PVC segment）。 |
| Sub-interface | 子接口提供在一个物理接口上支持多个逻辑接口的功能。即，将多个逻辑接口与一个物理接口建立关联。 |

### 缩略语

| 缩略语 | 英文全称 | 中文全称 |
| --- | --- | --- |
| AAL | ATM Adaptation Layer | ATM 适配层 |
| AAL1 | ATM Adaptation Layer Type 1 | ATM 适配层类型 1 |
| AAL2 | ATM Adaptation Layer Type 2 | ATM 适配层类型 2 |
| AAL3 | ATM Adaptation Layer Type 3 | ATM 适配层类型 3 |
| AAL5 | ATM Adaptation Layer Type 5 | ATM 适配层类型 5 |
| ADSL | Asymmetric Digital Subscriber Line | 非对称数字用户线路 |

| 缩略语 | 英文全称 | 中文全称 |
| --- | --- | --- |
| AIS | Alarm Indication Signal | 告警指示信号 |
| ANSI | American National Standards Institute | 美国国家标准学会 |
| ATM | Asynchronous Transfer Mode | 异步传输模式 |
| B-ICI | B-ISDN Inter Carrier Interface | 宽带综合业务数字网内部承载接口 |
| B-ISDN | Broadband Integrated Services Digital Network | 宽带综合业务数字网 |
| CBR | Constant Bit Rate | 固定比特率 |
| CC | Continuity Check | 连通性检测 |
| CCITT | International Telegraph and Telephone Consultative Committee | 国际电报电话咨询委员会，现已更名为 ITU。 |
| CHAP | Challenge Handshake Authentication Protocol | 质询握手验证协议 |
| CLP | Cell Loss Priority | 信元丢弃优先等级 |
| CPCS | Common Part Convergence Sublayer | 公共部分汇聚子层 |
| CS | Convergence Sublayer | 汇聚子层 |
| FDDI | Fiber Distributed Digital Interface | 光纤分布式数字接口 |
| GFC | Generic Flow Control | 流量控制 |
| HEC | Header Error Control | 信头差错控制 |
| IPoA | Internet Protocol over ATM | ATM 承载 IP 协议 |
| IPoEoA | IP over Ethernet over ATM | ATM 网络承载 IPoA |
| ITU-T | International Telecommunication Union - Telecommunication Standardization Sector | 国际电信联盟-电信标准部 |
| LLC | logical link control | 逻辑链路控制 |
| NNI | Network-to-Network Interface | 网络-网络接口 |
| OAM | Operation, Administration and Maintenance | 运行管理和维护 |
| OSI | Open System Interconnection | 开放系统互连（模型） |
| PAP | Password Authentication Protocol | 密码验证协议 |
| PLCP | Physical Layer Convergence Protocol | 物理层汇聚协议 |
| PM | Performance Monitoring | 性能监视 |
| PPP | Point-to-Point Protocol | 点到点协议 |

| 缩略语 | 英文全称 | 中文全称 |
| --- | --- | --- |
| PPPoA | Point-to-Point Protocol over ATM | ATM 承载 PPP 协议 |
| PPPoE | Point-to-Point Protocol over Ethernet | 以太网承载 PPP 协议 |
| PPPoEoA | PPP over Ethernet over ATM | 在 ATM 网络上承载 PPPoE 报文 |
| PT | Payload Type | 净荷类型 |
| PTI | Payload Type Indicator | 净荷类型标识 |
| PVC | Permanent Virtual Circuit | 永久虚电路 |
| QoS | Quality of Service | 服务质量 |
| RDI | Remote Defect Indication | 远端缺陷指示 |
| SAR | Segmentation And Reassembly | 分段与重组 |
| SAR-PDU | Segmentation And Reassembly-Protocol Data Unit | 分段和重组协议数据单元 |
| SDH | Synchronous Digital Hierarchy | 同步数字体系 |
| SNAP | Subnetwork Access Protocol | 子网访问协议 |
| SNAP | Sub-Network Attachment Point | 子网接入点 |
| Soft VC | Soft Virtual Circuit | 软交换 VC |
| SSCS | Service Special Convergence Sub-layer | 业务特定汇聚子层 |
| TC | Transmission Convergence Sub-layer | 传输汇聚子层 |
| UBR | Unspecified Bit Rate | 未定义比特率 |
| UNI | User-to-Network Interface | 用户-网络接口 |
| VBR-RT | Variable Bit Rate- Real Time | 实时的可变比特率 |
| VBR-NRT | Variable Bit Rate - Non Real Time | 非实时的可变比特率 |
| VC | Virtual Channel | 虚拟信道 |
| VCC | Virtual Channel Connection | 虚通路连接 |
| VCI | Virtual Channel Identifier | 虚信道标识 |
| VE | Virtual-Ethernet | 虚拟以太网接口 |
| VP | Virtual Path | 虚拟通路 |
| VPI | Virtual Path Identifier | 虚通路标识 |
| VT | Virtual-Template | 虚拟接口模板 |

# 2 PPP 和 MP

## 关于本章

介绍了 PPP 和 MP 的基本原理、特点和应用。

# 2.1 介绍

## 定义

PPP（Point-to-Point Protocol）协议是一种在点到点链路上承载网络层数据包的数据链路层协议，主要被设计用来支持全双工的同异步链路上进行点到点之间的数据传输。

MP 是出于增加带宽的考虑，将多个 PPP 链路捆绑使用的技术。

## 目的

PPP 协议是在串行线 IP 协议 SLIP（Serial Line IP）的基础上发展起来的。由于 SLIP 协议只支持异步传输方式、无协商过程（尤其不能协商如双方 IP 地址等网络层属性）、只能承载 IP 一种网络层报文等缺陷，在发展过程中，逐步被 PPP 协议所替代。

PPP 协议有如下优点：

- 对物理层而言，既支持同步链路又支持异步链路，而如 X.25、FR（Frame Relay）等数据链路层协议只对同步链路提供支持，SLIP 仅支持异步链路。
- 有一个易扩充的协议框架，便于扩充各种其他协议。
- 支持各种链路层参数的协商。
- 能承载多种网络层报文，提供各种 NCP（Network Control Protocol）协议（如 IPCP、IPXCP），用于各网络层属性的协商，更好地支持了网络层协议。
- 提供验证协议 CHAP（Challenge-Handshake Authentication Protocol）、PAP（Password Authentication Protocol），更好的保证了网络的安全性。
- 无重传机制，网络开销小，速度快。

# 2.2 参考标准和协议

本特性的参考资料清单如下：

| 文档 | 描述 | 备注 |
| --- | --- | --- |
| RFC1661 | The Point-to-Point Protocol (PPP) | - |
| RFC1570 | PPP LCP Extensions | - |
| RFC1990 | The PPP Multilink Protocol (MP) | - |
| RFC1661 | The Point-to-Point Protocol (PPP) | - |
| RFC1332 | The PPP Internet Protocol Control Protocol (IPCP) | - |
| RFC1334 | PPP Authentication Protocols | - |

| 文档 | 描述 | 备注 |
| --- | --- | --- |
| RFC1994 | PPP Challenge Handshake Authentication Protocol (CHAP) | - |

# 2.3 可获得性

## 涉及网元

无

## License 支持

本特性不需要 License 支持。

## 版本支持

**表 2-1** PPP 和 MP 特性的版本支持

| 产品 | 最低支持版本 |
| --- | --- |
| AR200-S | V200R002C00 |

## 硬件要求

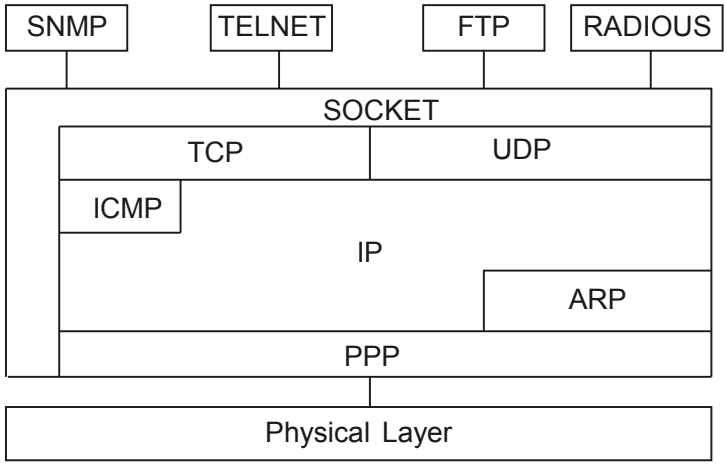
无

# 2.4 原理描述

## 2.4.1 PPP 的基本构架

PPP 协议处于 TCP/IP 的数据链路层，主要用在支持全双工的同异步链路上，进行点到点之间的数据传输。

**图 2-1** PPP 在协议栈中的位置




PPP 主要由三类协议族组成：

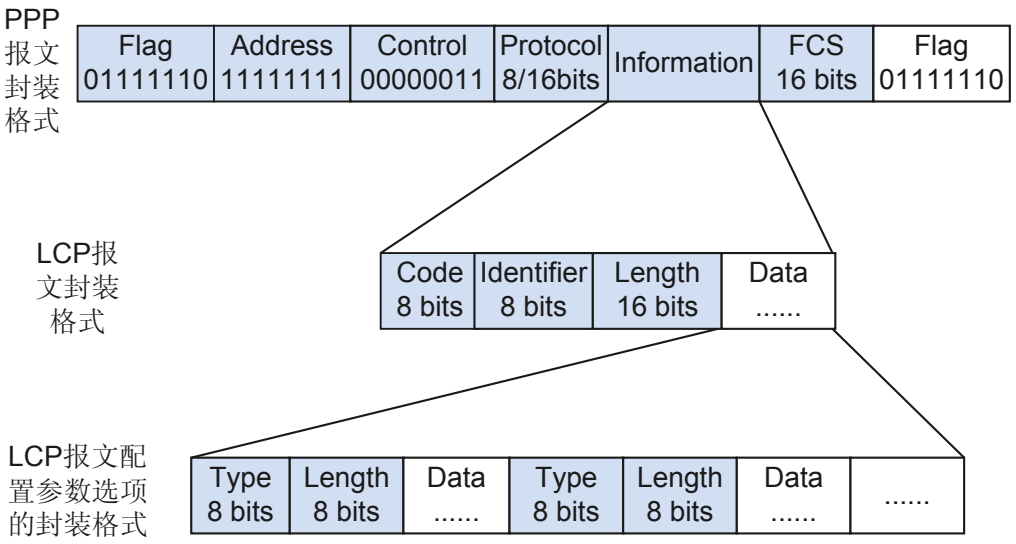
- 链路控制协议族（Link Control Protocol），主要用来建立、拆除和监控 PPP 数据链路。
- 网络层控制协议族（Network Control Protocol），主要用来协商在该数据链路上所传输的数据包的格式与类型。
- PPP 扩展协议族主要用于提供对 PPP 功能的进一步支持。例如：PPP 提供了用于网络安全方面的验证协议族（PAP 和 CHAP）。

## 2.4.2 PPP 报文格式

### PPP 报文封装的帧格式

PPP 报文封装格式如图 2-2 所示。

**图 2-2** PPP 报文格式



各字段的含义如下：

- Flag 域

  Flag 域标识一个物理帧的起始和结束，该字节为 0x7E。

- Address 域

  Address 域可以唯一标识对端。PPP 协议是被运用在点对点的链路上，因此，使用 PPP 协议互连的两个通信设备无须知道对方的数据链路层地址。按照协议的规定将该字节填充为全 1 的广播地址，对于 PPP 协议来说，该字段无实际意义。

- Control 域

  该字段默认值为 0x03，表明为无序号帧，PPP 默认没有采用序列号和确认来实现可靠传输。

  Address 和 Control 域一起标识此报文为 PPP 报文，即 PPP 报文头为 FF03。

- Protocol 域

  协议域可用来区分 PPP 数据帧中信息域所承载的数据报类型。

  协议域的内容必须依据 ISO3309 的地址扩展机制所给出的规定。该机制规定协议域所填充的内容必须为奇数，也就是要求最低有效字节的最低有效位为“1”，最高有效字节的最低有效位为“0”。

  如果当发送端发送的 PPP 数据帧的协议域字段不符合上述规定，接收端则会认为此数据帧是不可识别的。接收端向发送端发送一个 Protocol-Reject 报文，在该报文尾部将填充被拒绝报文的协议号。

**表 2-2 常见的协议代码**

| 协议代码 | 协议类型 |
| --- | --- |
| 0021 | Internet Protocol |
| 002b | Novell IPX |
| 002d | Van Jacobson Compressed TCP/IP |
| 002f | Van Jacobson Uncompressed TCP/IP |
| 8021 | Internet Protocol Control Protocol |
| 802b | Novell IPX Control Protocol |
| 8031 | Bridging NC |
| C021 | Link Control Protocol |
| C023 | Password Authentication Protocol |
| C223 | Challenge Handshake Authentication Protocol |

- Information 域

  信息域最大长度是 1500 字节，其中包括填充域的内容。信息域的最大长度称为最大接收单元 MRU（Maximum Receive Unit）。MRU 的缺省值为 1500 字节，在实际应用当中可根据实际需要进行 MRU 的协商。

如果信息域长度不足，可被填充，但不是必须的。如果填充则需通信双方的两端能辨认出填充信息和真正需要传送的信息，方可正常通信。

- FCS 域

  校验域的功能主要对 PPP 数据帧传输的正确性进行检测。

  在数据帧中引入了一些传输的保证机制，会引入更多的开销，这样可能会增加应用层交互的延迟。

## LCP 报文封装的帧格式

LCP 报文封装格式请参见图 2-2。

在链路建立阶段，PPP 协议通过 LCP 报文进行链路的建立和协商过程。此时 LCP 报文作为 PPP 的净载荷被封装在 PPP 数据帧的信息域中，PPP 数据帧的协议域的值固定填充 0xC021。

在链路建立阶段的整个过程中信息域的内容是变化的，它包括很多种类型的报文，所以这些报文也要通过相应的字段来区分。

- Code 域

  代码域的长度为一个字节，主要是用来标识 LCP 数据报文的类型。

  在链路建立阶段，接收方接收到 LCP 数据报文。当其代码域的值无效时，就会向对端发送一个 LCP 的代码拒绝报文（Code-Reject 报文）。

**表 2-3** 常见 code 值

| code 值 | 报文类型 |
| --- | --- |
| 0x01 | Configure-Request |
| 0x02 | Configure-Ack |
| 0x03 | Configure-Nak |
| 0x04 | Configure-Reject |
| 0x05 | Terminate-Request |
| 0x06 | Terminate-Ack |
| 0x07 | Code-Reject |
| 0x08 | Protocol-Reject |
| 0x09 | Echo-Request |
| 0x0A | Echo-Reply |
| 0x0B | Discard-Request |
| 0x0C | Reserved |

- Identifier 域

  标识域为 1 个字节，用来匹配请求和响应，当标识域值为非法时，该报文将被丢弃。

通常一个配置请求报文的 ID 是从 0x01 开始逐步加 1 的。当对端接收到该配置请求报文后，无论使用何种报文回应对方，但必须要求回应报文中的 ID 要与接收报文中的 ID 一致。

- Length 域

  长度域的值就是该 LCP 报文的总字节数据。它是代码域、标志域、长度域和数据域四个域长度的总和。

  长度域所指示字节数之外的字节将被当作填充字节而忽略掉，而且该域的内容不能超过 MRU 的值。

- Data 域

  数据域所包含的是协商报文的内容，这个内容包含以下字段。

  - Type 为协商选项类型。
  - Length 为协商选项长度，它是指 Data 域的总长度，也就是包含 Type、Length 和 Data。
  - Data 为协商的选项具体内容。

**表 2-4** 常见 Type 中的协商类型值

| 协商类型值 | 协商报文类型 |
| --- | --- |
| 0x01 | Maximum-Receive-Unit |
| 0x02 | Async-Control-Character-Map |
| 0x03 | Authentication-Protocol |
| 0x04 | Quality-Protocol |
| 0x05 | Magic-Number |
| 0x06 | RESERVED |
| 0x07 | Protocol-Field-Compression |
| 0x08 | Address-and-Control-Field-Compression |

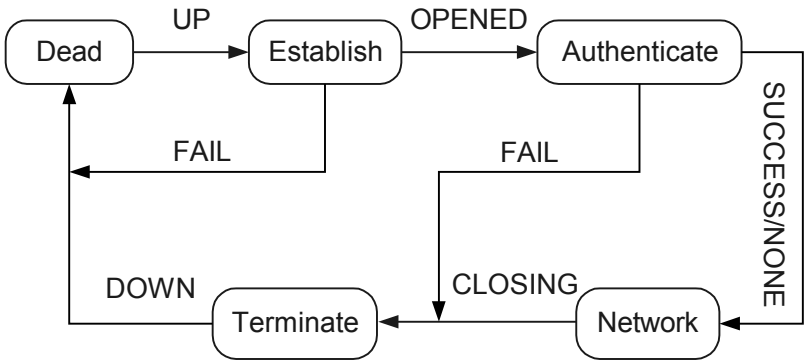
## 2.4.3 PPP 的建链过程

PPP 链路的建立是通过一系列的协商完成的。

- LCP 除了用于建立、拆除和监控 PPP 数据链路，还主要进行链路层参数的协商，如 MRU、验证方式。
- NCP 主要用于协商在该数据链路上所传输的数据包的格式与类型，如 IP 地址。

下图是 PPP 协议整个链路过程需经历阶段的状态转移图：

**图 2-3** PPP 链路建立过程




PPP 链路建立过程的简单描述如下：

1. PPP 协议运行总是以 Dead 阶段开始和结束。通常处在这个状态的时间很短，仅仅是检测到硬件设备后（即硬件连接状态为 Up）就进入 Establish 阶段。
2. 在 Establish 阶段，PPP 链路进行 LCP 协商。协商内容包括工作方式是 SP（Single-link PPP）还是 MP（Multilink PPP）、最大接收单元 MRU、验证方式、魔术字（magic number）和异步字符映射等选项。LCP 协商成功后进入 Opened 状态，表示底层链路已经建立。
3. 如果配置了验证，将进入 Authenticate 阶段，开始 CHAP 或 PAP 验证。如果没有配置验证，则直接进入 Network 阶段。
4. 对于 Authenticate 阶段，如果验证失败，进入 Terminate 阶段，拆除链路，LCP 状态转为 Closed。如果验证成功，进入 Network 阶段，此时 LCP 状态仍为 Opened，而 NCP 状态从 Initial 转到 Starting。
5. 在 Network 阶段，PPP 链路进行 NCP 协商，NCP 协商包括 IPCP（IP Control Protocol）、MPLSCP（MPLS Control Protocol）等协商。IPCP 协商主要包括双方的 IP 地址。通过 NCP 协商来选择和配置一个网络层协议。只有相应的网络层协议协商成功后（相应协议的 NCP 协商状态为 Opened），该网络层协议才可以通过这条 PPP 链路发送报文。例如：IPCP 协商通过后，这条 PPP 链路才可以承载 IP 报文。
6. NCP 协商成功后，PPP 链路将一直保持通信。PPP 运行过程中，可以随时中断连接，物理链路断开、认证失败、超时定时器时间到、管理员通过配置关闭连接等动作都可能导致进入链路进入 Terminate 阶段。
7. 进入 Terminate 阶段后且资源释放完，即进入 Dead 阶段。

在点对点链路的配置、维护和终止过程中，PPP 需经历以下几个阶段：

## 链路不可用阶段（Dead）

它有时也称为物理层不可用阶段。PPP 链路都需从这个阶段开始和结束。

当通信双方的两端检测到物理线路激活（通常是检测到链路上有载波信号）时，就会从当前这个阶段跃迁至下一个阶段，即链路建立阶段。

在链路建立阶段主要是通过 LCP 协议进行链路参数的配置，LCP 在此阶段的状态机也会根据不同的事件发生变化。当处于在链路不可用阶段时，LCP 的状态机是处于初始化 Initial 状态或准备启动 Starting 状态，一旦检测到物理线路可用，则 LCP 的状态机就要发生改变。

当然链路被断开后也同样会返回到链路不可用阶段。

在实际过程中这个阶段所停留的时间是很短的，只是检测到对端设备的存在。

## 链路建立阶段（Establish）

它是 PPP 协议最关键和最复杂的阶段。

该阶段主要是发送一些配置报文来配置数据链路，这些配置的参数不包括网络层协议所需的参数。当完成配置报文的交换后，则会继续向下一个阶段跃迁。

下一个阶段既可能是验证阶段，也可能是网络层协议阶段。下一阶段的选择是依据链路两端的设备配置的，通常由用户来配置。

在链路建立阶段，LCP 的状态机会发生两次改变。

- 当链路处于不可用阶段时，此时 LCP 的状态机处于 Initial 或 Starting。当检测到链路可用时，则物理层会向链路层发送一个 Up 事件。链路层收到该事件后，会将 LCP 的状态机从当前状态改变为 Request-Sent（请求发送状态），根据此时的状态机 LCP 会进行相应的动作，也就是开始发送 Configure-Request 报文来配置数据链路。
- 无论哪一端接收到了 Configure-Ack 报文时，LCP 的状态机又要发生改变，从当前状态改变为 opened 状态。进入 Opened 状态后收到 Configure-Ack 报文的一方则完成了当前阶段，应该向下一个阶段跃迁。

同理可知，另一端也是一样的。如果在该阶段收到了非 LCP 数据报文，则会将这些报文丢弃。

## 验证阶段（Authenticate）

PPP 链路缺省情况下，不进行验证。如果要求验证，在链路建立阶段必须指定验证协议。

PPP 验证有两种用途：

- 主要是用于主机和路由器之间，通过 PPP 网络服务器交换电路或拨号接入连接的链路。
- 偶尔也用于专用线路。

PPP 提供两种验证方式。

- PAP：Password Authentication Protocol，密码验证协议
- CHAP：Challenge-Handshake Authentication Protocol，质询握手验证协议

验证方式的选择是依据在链路建立阶段双方进行协商的结果。然而，链路质量的检测也会在这个阶段同时发生，但协议规定不会让链路质量的检测无限制的延迟验证过程。

在这个阶段仅支持链路控制协议、验证协议和质量检测数据报文，其它的数据报文都会被丢弃。如果在这个阶段再次收到了 Configure-Request 报文，则又会返回到链路建立阶段。

## 网络层协议阶段（Network）

一旦 PPP 完成了前面几个阶段，每种网络层协议（IP、IPX 和 AppleTalk）会通过各自相应的网络控制协议进行配置，例如：通过 IPCP 进行 IP 协议的配置。每个 NCP 协议可在任何时间打开和关闭，当一个 NCP 的状态机变成 Opened 状态时，则 PPP 就可以开始在链路上承载网络层的数据包报文了。

如果在这个阶段收到了 Configure-Request 报文，则又会返回到链路建立阶段。

### 网络终止阶段（Terminate）

PPP 能在任何时候终止链路。当载波丢失、认证失败、链路质量检测失败或管理员人为关闭链路等情况均会导致链路终止。

链路建立阶段可能通过交换 LCP 的链路终止报文来关闭链路，当链路关闭时，链路层会通知网络层做相应的操作，而且也会通过物理层强制关断链路。

## 2.4.4 PPP 的 PAP 验证协议

### PAP 验证过程概述

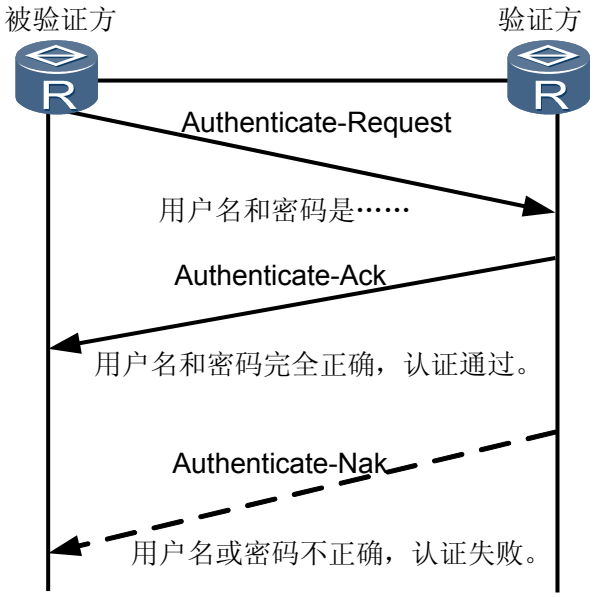
PAP 验证协议为两次握手验证，口令为明文。验证过程仅在链路初始建立阶段进行。

当链路建立阶段结束后，用户名和密码将由被验证方重复地在链路上发送给验证方，直到验证通过或者中止连接。

如果必须在远端主机上使用明文密码进行模拟登录，这种验证方式是最合适的。

PAP 验证的过程如图 2-4 所示。

**图 2-4** PAP 认证过程

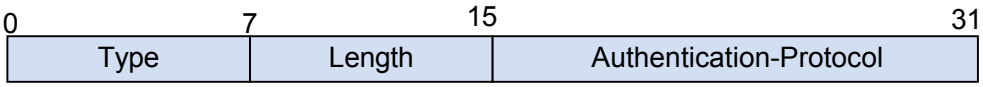



- 被验证方把本地用户名和口令发送到验证方。
- 验证方根据本地用户表查看是否有被验证方的用户名以及口令是否正确，然后返回不同的响应（接受或拒绝）。

### 协商验证协议的配置参数选项格式

协商验证协议类型是在 LCP 协商中完成的，协商 PAP 验证协议的配置参数选项帧格式如图 2-5 所示。

**图 2-5** 协商验证协议的配置参数选项帧格式




各字段的含义如下表所示。

**表 2-5** PAP 的配置参数选项各字段解释表

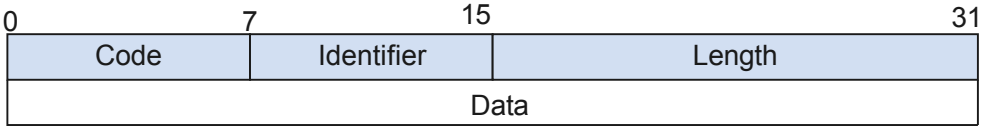
| 字段 | 长度（字节） | 取值与含义 |
| --- | --- | --- |
| Type | 1 | 验证报文的该字段取值为 Ox03。 |
| Length | 1 | 此时固定值是 4，表示这个配置参数选项帧的总长度是 4 个字节。 |
| Authenticati on-Protocol | 2 | PAP 验证协议的该字段取值为 0xC023。协商验证协议时，配置参数选项的 DATA 字段就表示认证协议的类型。 |

## PAP 验证报文帧格式

PAP 报文封装在协议域为 0xC023 的 PPP 数据链路层帧的信息域中。

PAP 报文的帧格式如图 2-6 所示。

**图 2-6** PAP 数据报的帧格式




各字段的含义如表 2-6 所示。

**表 2-6** PAP 数据报的帧格式各字段解释表

| 字段 | 长度（字节） | 取值与含义 |
| --- | --- | --- |
| Code | 1 | 标识 PAP 数据报的类型。<br>● 1 表示是 Authenticate-Request 报文<br>● 2 表示是 Authenticate-Ack 报文<br>● 3 表示是 Authenticate-Nak 报文 |
| Identifier | 1 | 表示请求报文和应答报文是否匹配的标识。 |

| 字段 | 长度（字节） | 取值与含义 |
| --- | --- | --- |
| Length | 2 | 表示包括 Code、Identifier、Length 和 Data 域在内的 PAP 报文长度。超出此长度的报文将被认为是填充字节并被丢弃。 |
| Data | 0 或多个字节 | Data 域的内容由 Code 域来决定。具体内容请参见 **PAP 验证报文**。 |

## PAP 验证报文

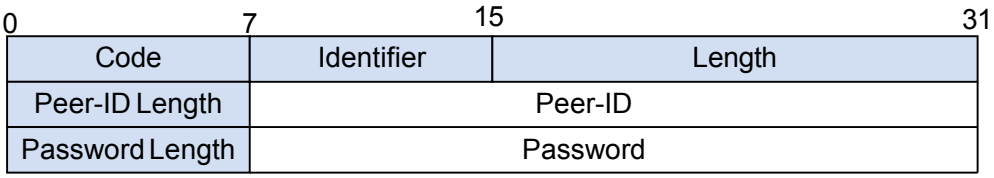
- Authenticate-Request 报文

  Authenticate-Request 报文用于表示 PAP 验证的开始。Authenticate-Request 报文被重复发送，直到收到有效的应答报文或达到重传次数上限。当达到重传次数上限时，应该终止链路连接。

  验证方只能等待被验证方发送 Authenticate-Request 报文。当收到 Authenticate-Request 报文后，必须根据实际情况回复不同的应答报文。

  Authenticate-Request 报文的帧格式如**图 2-7** 所示。

**图 2-7** Authenticate-Request 报文格式




各字段的解释如**表 2-7** 所示。

**表 2-7** Authenticate-Request 报文帧格式各字段解释表

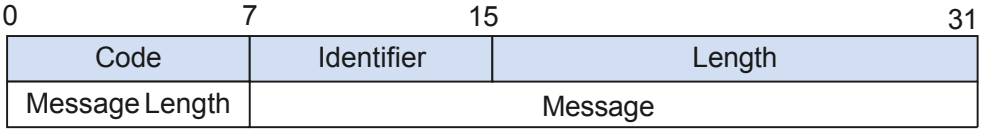
| 字段 | 长度（字节） | 取值与含义 |
| --- | --- | --- |
| Code | 1 | Authenticate-Request 报文的该字段取值为 0x01。 |
| Identifier | 1 | 表示请求报文和应答报文是否匹配的标识。 |
| Length | 2 | 表示该报文的总长度。 |
| Peer-ID Length | 1 | 标识 Peer-ID 域的长度。 |
| Peer-ID | 0 或多个 | 标识被验证方的名字。 |
| Password Length | 1 | 标识 Password 域的长度。 |
| Password | 0 或多个 | 标识被验证的密码。 |

- Authenticate-Ack 和 Authenticate-Nak 报文帧格式

  如果 Authenticate-Request 报文中的用户名和密码都能被验证方验证通过，则验证方返回 Authenticate-Ack 报文；如果 Authenticate-Request 报文中的用户名或密码有一项没有通过验证，则验证方返回 Authenticate-Nak 报文。

  Authenticate-Ack 和 Authenticate-Nak 报文的帧格式如图 2-8 所示。

**图 2-8** Authenticate-Ack 和 Authenticate-Nak 报文的帧格式




各字段的含义如表 2-8 所示。

**表 2-8** Authenticate-Ack 和 Authenticate-Nak 报文帧格式各字段解释表

| 字段 | 长度（字节） | 取值与含义 |
| --- | --- | --- |
| Code | 1 | Authenticate-Ack 报文的该字段取值为 0x02;Authenticate-Nak 报文的该字段取值为 0x03。 |
| Identifier | 1 | 表示请求报文和应答报文是否匹配的标识。 |
| Length | 2 | 表示该报文的总长度。 |
| Message Length | 1 | 标识 Message 域的长度。 |
| Message | 0 或多个 | Authenticate-Ack 或 Authenticate-Nak 报文的补充描述信息，一般使用 ASCII 字符表示。 |

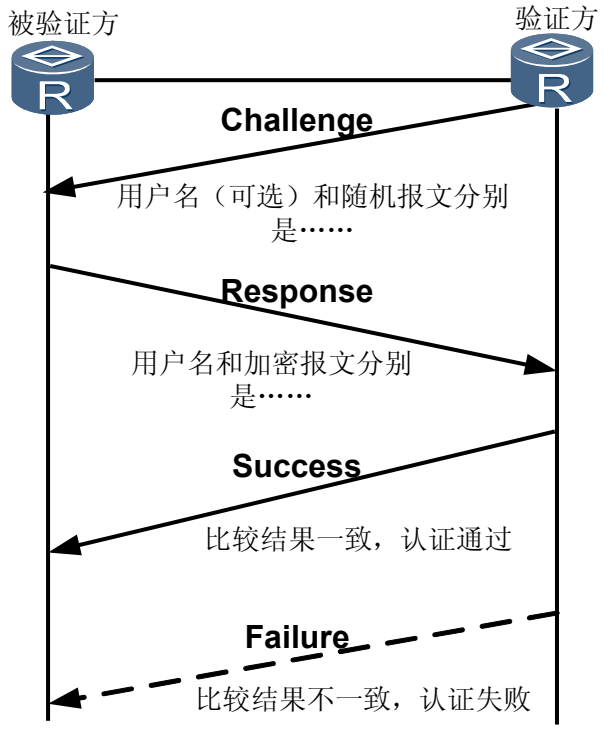
# 2.4.5 PPP 的 CHAP 验证协议

## CHAP 验证过程概述

CHAP（Challenge Handshake Authentication Protocol）验证协议为三次握手验证协议。它只在网络上传输用户名，而并不传输用户密码，因此安全性要比 PAP 高。

CHAP 的验证过程如图 2-9 所示。

**图 2-9** CHAP 的验证过程




CHAP 单向验证是指一端作为验证方，另一端作为被验证方。双向验证是单向验证的简单叠加，即两端都是既作为验证方又作为被验证方。在实际应用中一般只采用单向验证。

CHAP 单向验证过程分为两种情况：验证方配置了用户名和验证方没有配置用户名。推荐使用验证方配置用户名的方式，这样可以对验证方的用户名进行确认。

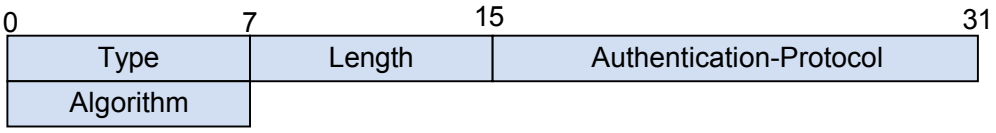
- 验证方配置了用户名的验证过程
  - 验证方主动发起验证请求，验证方向被验证方发送一些随机产生的报文（Challenge），并同时将本端的用户名附带上一起发送给被验证方。
  - 被验证方接到验证方的验证请求后，先检查本端接口上是否配置了 **ppp chap password** 命令，如果配置了该命令，则被验证方用报文 ID、命令中配置的用户密码和 MD5 算法对该随机报文进行加密，将生成的密文和自己的用户名发回验证方（Response）。如果接口上未配置 **ppp chap password** 命令，则根据此报文中验证方的用户名在本端的用户表查找该用户对应的密码，用报文 ID、此用户的密钥（密码）和 MD5 算法对该随机报文进行加密，将生成的密文和被验证方自己的用户名发回验证方（Response）
  - 验证方用自己保存的被验证方密码和 MD5 算法对原随机报文加密，比较二者的密文，根据比较结果返回不同的响应。
- 验证方没有配置用户名
  - 验证方主动发起验证请求，验证方向被验证方发送一些随机产生的报文（Challenge）。
  - 被验证方接到验证方的验证请求后，利用报文 ID、**ppp chap password** 命令配置的 CHAP 密码和 MD5 算法对该随机报文进行加密，将生成的密文和自己的用户名发回验证方（Response）。

- 验证方用自己保存的被验证方密码和 MD5 算法对原随机报文加密，比较二者的密文，根据比较结果返回不同的响应。

## 协商验证协议的配置参数选项格式

协商 CHAP 协议的配置参数选项帧格式如图 2-10 所示。

**图 2-10** CHAP 的配置参数选项帧格式




各字段含义如表 2-9 所示。

**表 2-9** CHAP 的配置参数选项各字段解释表

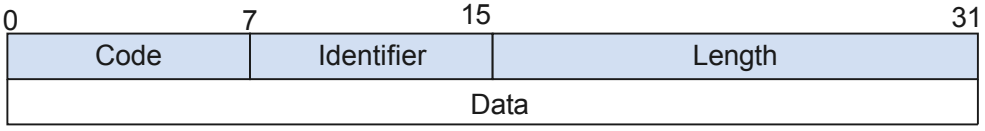
| 字段 | 长度（字节） | 取值与含义 |
| --- | --- | --- |
| Type | 1 | 验证报文的该字段取值为 Ox03。 |
| Length | 1 | 此时固定是 5，表示该报文的总长度是 5 个字节。 |
| Authentication-Protocol | 2 | CHAP 验证协议的该字段取值为 0xC223。协商验证协议时，配置参数选项的 DATA 字段就表示认证协议的类型。 |
| Algorithm | 1 | 表示使用的一次加密算法。<br>● 0 ～ 4：不用，保留<br>● 5：MD5 算法 |

## CHAP 验证报文帧格式

CHAP 报文封装在协议域为 0xC223 的 PPP 数据链路层帧的信息域中。

CHAP 报文格式如图 2-11 所示。

**图 2-11** CHAP 报文的帧格式




各字段含义如表 2-10 所示。

**表 2-10** CHAP 报文帧格式各字段解释表

| 字段 | 长度（字节） | 取值与含义 |
| --- | --- | --- |
| Code | 1 | 表示 CHAP 报文的类型。<br>● 1 表示 Challenge 报文<br>● 2 表示 Response 报文<br>● 3 表示 Success 报文<br>● 4 表示 Failure 报文 |
| Identifier | 1 | 表示挑战报文、应答报文等之间的对应。 |
| Length | 2 | 表示包括 Code、Identifier、Length 和 Data 域在内的 CHAP 报文的长度。超出该长度值的字节应该被认为是数据链路层的填充字节，在接收时应该被忽略。 |
| Data | 0 或多个 | Data 域的格式由 Code 域值决定。具体请参见 **CHAP 验证报文** |

## CHAP 验证报文

- Challenge 报文和 Response 报文

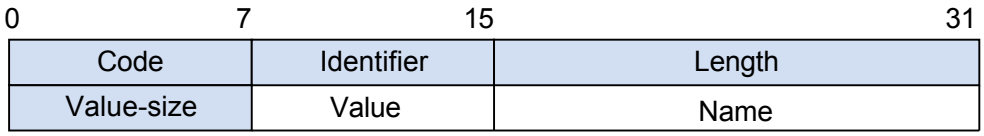
  Challenge 报文用来发起 CHAP 验证。

  在验证阶段，被验证方要等待验证方发送 Challenge 报文。只要接收到 Challenge 报文，被验证方必须返回一个 Response 报文。

  只要接收到 Response 报文，验证方就会把自己计算的值和返回值进行比较。根据比较的结果，验证方返回不同的 Response 报文。

  Challenge 报文和 Response 报文的帧格式如**图 2-12** 所示。

  **图 2-12** Challenge 报文和 Response 报文帧格式

  各字段的含义如**表 2-11** 所示。

  **表 2-11** Challenge 报文和 Response 报文的帧格式各字段解释表

| 字段 | 长度（字节） | 取值与含义 |
| --- | --- | --- |
| Code | 1 | ● 1 表示是 Challenge 报文<br>● 2 表示是 Response 报文 |
| Identifier | 1 | 它标识 Challenge 报文和 Response 报文的对应关系。 |

| 字段 | 长度（字节） | 取值与含义 |
| --- | --- | --- |
| Length | 2 | 表示该报文的总长度。 |
| Value-size | 1 | 表示 Value 域的长度。 |
| Value | 1 或多个 | Challenge 报文中，此域的内容是一些字节流。Response 报文中此域的内容是 Challenge 报文字节流经过一次哈希算法后得到的值。 |
| Name | 1 或多个 | 表示发送该报文的系统标识。该域的长度由 Length 域决定。 |

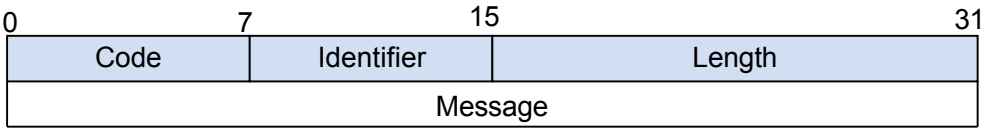
- Success 报文和 Failure 报文

  如果验证方接收到的值和自己计算的值相同，验证方必须要返回一个 Success 报文，表示验证通过。

  如果验证方接收到的值和自己计算出的值不同，验证方必须返回一个 Failure 报文，表示验证失败。并且应该终止链路连接。

  Success 报文和 Failure 报文格式如图 2-13 所示。

**图 2-13** Success 报文和 Failure 报文帧格式




各字段的含义如表 2-12 所示。

**表 2-12** Success 报文和 Failure 报文帧格式各字段解释表

| 字段 | 长度（字节） | 取值与含义 |
| --- | --- | --- |
| Code | 1 | ● 3 表示 Success 报文<br>● 4 表示 Failure 报文 |
| Identifier | 1 | 表示 Success 报文和 Failure 报文的对应关系。 |
| Length | 2 | 表示该报文的总长度。 |
| Message | 0 或多个 | Success 报文和 Failure 报文的补充描述信息，一般使用 ASCII 字符表示。 |

## 2.4.6 MP 的协商过程

MP 的协商较为特殊。MP 一些选项的协商是在 LCP 协商过程中完成的，如 MRRU、Endpoint Discriminator(终端描述符)等。

MP 的协商包括 LCP 协商和 NCP 协商两个过程：

- LCP 协商：两端首先进行 LCP 协商，除了协商一般的 LCP 参数外，还要验证对端接口是否也工作在 MP 方式下。如果两端工作方式不同，LCP 协商不成功。
- NCP 协商：根据 MP-Group 接口或指定虚拟接口模板的各项 NCP 参数（如 IP 地址等）进行 NCP 协商，物理接口配置的 NCP 参数不起作用。

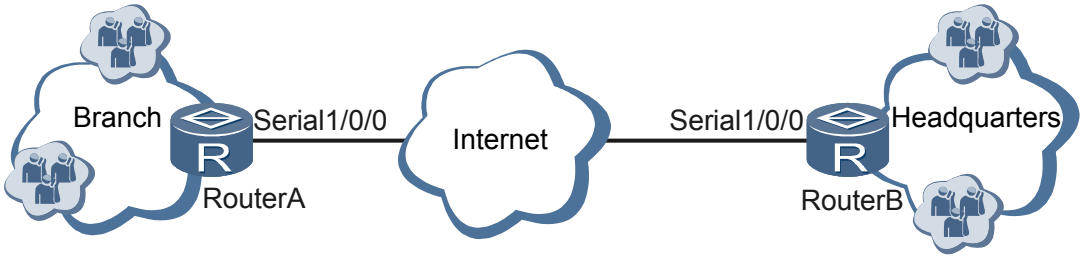
  NCP 协商通过后，即可建立 MP 链路。

# 2.5 应用

## 2.5.1 PPP

企业分支机构和总部间可以通过 PPP 链路实现园区网间的互联。

**图 2-14** 通过 PPP 链路通信示意图



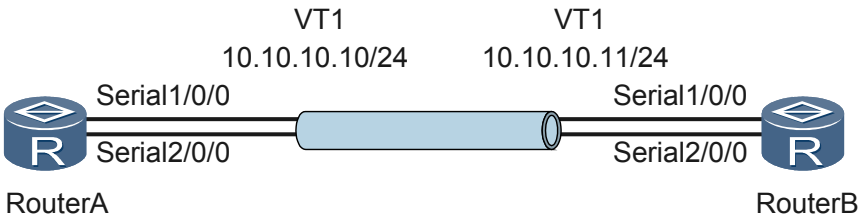

## 2.5.2 MP

为了增加带宽，可以将多个 PPP 链路捆绑成 MP 使用。

为了减少语音报文的传输延时，需要使用 MP 的分片功能。较大报文在通过链路时，传输的时间也较长，占用链路的时间也长。对于队列中后续对实时性要求高的报文（例如：语音报文），可能造成延时，影响用户体验。这时，将大报文进行分片，将小报文和大报文的分片一起加入到队列，即可解决上述问题。

将多个串口绑定实现 MP 的场景如图 2-15 所示。

**图 2-15** 路由器通过 MP 链路通信示意图



# 2.6 术语与缩略语

## 术语

| 术语 | 解释 |
| --- | --- |
| 虚拟访问接口 | 虚拟访问接口是动态生成、临时存在的虚拟接口模板的实例。不同的应用可以创建不同的虚拟访问接口。 |
| 虚拟接口模板 | 虚拟接口模板是虚拟访问接口的模板，它只提供虚拟访问接口的公共属性。真正用于通信的是虚拟访问接口。但是虚拟访问接口不能由用户配置，用户只能通过配置虚拟接口模板来配置虚拟访问接口。 |

## 缩略语

| 缩略语 | 英文全称 | 中文全称 |
| --- | --- | --- |
| CHAP | Challenge-Handshake Authentication Protocol | 盘问握手认证协议 |
| FCS | Frame Check Sequence | 帧校验序列 |
| LCP | Link Control Protocol | 链路控制协议 |
| MP | Multilink Point-to-Point Protocol | 多链路点到点协议 |
| MRRU | Max Receive Reconstructed Unit | 最大接收重组单元 |
| MRU | Max Receive Unit | 最大接收单元 |
| NCP | Network Control Protocol | 网络控制协议 |
| OSI | Open System Interconnection | 开放系统互联 |
| PAP | Password Authentication Protocol | 密码认证协议 |
| PPP | Point-to-Point Protocol | 点到点协议 |
| SLIP | Serial Line Internet Protocol | 串行线路因特网协议 |

# 3 PPPoE

## 关于本章

介绍了 PPPoE 的基本原理、基本概念和实际应用。

# 3.1 介绍

## 定义

PPPoE（PPP over Ethernet）协议提供了在广播式的网络（如以太网）中多台主机连接到远端的访问集中器（访问集中器也称为宽带接入服务器）上的一种标准。

## 目的

当用户接入服务器、服务提供商为多个用户同时提供服务时：

- 用户希望接入成本低，不要或者很少改变配置即可接入成功。以太网无疑是最好的组网方式。
- 服务提供商希望通过同一个接入服务器连接到远程站点上的多个主机，同时要求服务器能提供与使用 PPP 拨号上网类似的访问控制功能和支付功能。

PPP 协议应用虽然很广泛，但是不能应用于以太网，因此提出了 PPPoE 技术。PPPoE 协议是对 PPP 的扩展，它可以使 PPP 协议应用于以太网。

## 受益

PPPoE 特性给企业用户带来了如下的受益：

- PPPoE Server 为网吧、小区、酒店、学校等特殊场合提供了灵活的网络接入控制方式，包括认证、计费等。
- 通过 PPPoE Client，同一局域网内的用户可以使用同一个帐号拨入 Internet，且用户不需要安装 PPPoE 拨号软件，简化了用户的操作和企业的维护工作。

# 3.2 参考标准和协议

本特性的参考资料清单如下：

| 文档 | 描述 | 备注 |
| --- | --- | --- |
| RFC2516 | A Method for Transmitting PPP Over Ethernet (PPPoE) | - |
| RFC1661 | The Point-to-Point Protocol (PPP) | - |

# 3.3 可获得性

## 涉及网元

PPPoE 属于一种接入技术，所以需要 PPPoE Server 与 PPPoE Client 配合才能完成 PPPoE 功能。

当 AR200-S 设备作为 PPPoE Server 时，局域网内的 PC 需要安装 PPPoE 拨号软件，充当 PPPoE Client 的角色；当 AR200-S 设备将 PPPoE 作为一种 WAN（Wide Area

Network）接入方式时，AR200-S 充当 PPPoE Client 的角色，BRAS（Broadband Remote Access Server）作为 PPPoE Server。

### License 支持

本特性不需要 License 支持。

### 版本支持

**表 3-1** PPPoE 特性的版本支持

| 产品 | 最低支持版本 |
| --- | --- |
| AR200-S | V200R002C00 |

### 硬件要求

无。

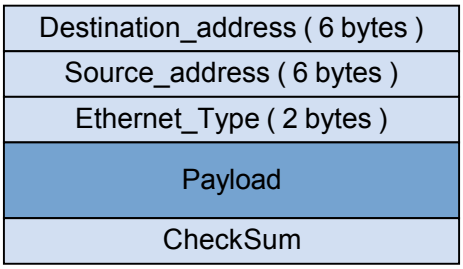
## 3.4 原理描述

PPPoE 协议描述了 PPPoE 帧格式及 PPPoE 会话的建立过程。

### 3.4.1 PPPoE 帧格式

RFC2516 定义了以太网的帧格式如图 3-1 所示。

**图 3-1** 以太网的帧格式




以太网帧格式中各域的含义如下。

#### Destination_address 域

以太网单播目的地址或者以太网广播地址（0xFFFFFFFF）。

- 在 Discovery 数据包中，该域的值是以太网广播地址。
- 在 PPPoE 会话流量中，该域必须是 Discovery 阶段已经确定的通信对方的单播地址。

## Source_address 域

源设备的以太网 MAC 地址。

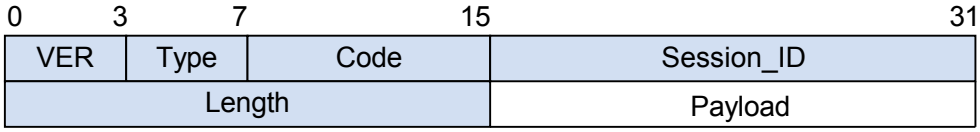
## Ethernet_Type 域

- 当值为 0x8863 时表示 Discovery 阶段
- 当值为 0x8864 时表示 PPPoE 会话阶段

## Payload 域

PPPoE 的 Payload 报文格式如图 3-2 所示。

**图 3-2** PPPoE 的 Payload 报文格式



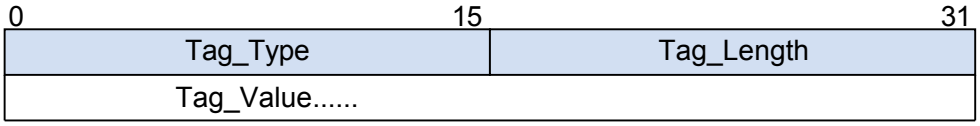

PPPoE 的 Payload 报文中各域的含义如下：

- VER：长度是 4 比特。PPPoE 规范的本版本必须设置为 0x01。
- Type：长度是 4 比特。PPPoE 规范的本版本必须设置为 0x01。
- Code：长度是 8 比特。其定义在后面的 Discovery 和 PPPoE 会话中分别指定。
- Session_ID：长度是 16 比特。是一个网络字节序的无符号值。其值在后面 Discovery 数据包中定义。

  对一个给定的 PPPoE 会话来说该值是一个固定值，并且与以太网 Source_address 和 Destination_address 一起实际地定义了一个 PPPoE 会话。

  值 0xFFFF 为将来的使用保留，不允许使用。
- Length：长度是 16 比特。该值是 PPPoE 的 Payload 长度。它不包括以太网头部和 PPPoE 头部的长度。
- Payload：PPPoE 的 Payload，包含 0 个或多个 Tag。一个 Tag 是一个 TLV（Type-Length-Value）结构，其帧结构定义如图 3-3 所示。

  **图 3-3** Tag 帧结构

  - Tag_Type：长度是 16 比特，也就是网络字节序。表 3-2 列出了各种 Tag_Type 和 Tag_Value 的对应关系和含义。
  - Tag_Length 域的长度是 16 比特，是一个网络字节序的无符号值，表明 Tag_Value 的字节数。

  如果收到的 Discovery 数据包中包含未知的 Tag_Type，则必须忽略掉该 Tag。

**表 3-2** Tag_Type 和 Tag_Value 对应关系表

| Tag_Value | Tag_Type | 含义 |
| --- | --- | --- |
| 0x0000 | End-Of-List | 该 Tag 表明是最后一个 Tag。该 Tag 的 Tag_Length 必须总是 0。不要求使用该标签，它是为了向后兼容。 |
| 0x0101 | Service-Name | 该 Tag 表明后面紧跟的是服务的名称。<br>● Tag_Value 是不以 NULL 结束的字符串。<br>● 当 Tag_Length 为 0 时，该 Tag 用于表明接受任何服务。<br>Service-Name 标签是表明 Internet 服务提供商 ISP 或者一类服务或者服务的质量。 |
| 0x0102 | AC-Name | 该 Tag 表明后面紧跟的字符串唯一地表示了某个特定的接入服务器。它可以是商标、型号以及序列号等信息的集合，或者该接入服务器 MAC 地址的一个简单表示。它不以 NULL 来结束。 |
| 0x0103 | Host-Uniq | 该 Tag 由主机用于把接入服务器的响应报文（PADO 或者 PADS）与主机的某个唯一特定的请求联系起来。Tag_Value 是主机选择的长度和值，可以是任意的二进制数据。它不能由接入服务器解释。主机可以在 PADI 或者 PADR 中包含一个 Host-Uniq 标签。如果接入服务器收到了该标签，它必须在对应的 PADO 或者 PADS 中不加改变的包含该标签。 |
| 0x0104 | AC-Cookie | 该 Tag 由接入服务器用于防止服务攻击。接入服务器可以在 PADO 数据包中包含该 Tag。如果主机收到了该标签，它必须在接下来的 PADR 中不加改变的包含该标签。Tag_Value 的长度和值都是任意的二进制数据。 |
| 0x0105 | Vendor-Specific | 该 Tag 用来传送厂商自定义的信息。Tag_Value 的前 4 个字节包含了厂商的识别码，其余字节尚未定义。厂商识别码的高字节为 0，低 3 个字节为网络字节序的厂商的 SMI 网络管理专用企业码。不推荐使用该 Tag。为了确保互操作性，在实现过程中，可以忽略 Vendor-Specific Tag。 |

| Tag_Value | Tag_Type | 含义 |
| --- | --- | --- |
| 0x0110 | Relay-Session-Id | 该 Tag 可由中继流量的中间代理加入到 Discovery 数据包中。Tag_Value 对主机和接入服务器都是不透明。如果主机或接入服务器收到该 Tag，则它们必须在所有的 Discovery 数据包中包含该 Tag 以作为响应。所有的 PADI 数据包必须保证足够空间来加入 Tag_Value 长度为 12 字节的 Relay-Session-Id 标签。如果 Discovery 数据包中已经包含一个 Relay-Session-Id 标签，则不允许再加入该标签。这种情况下，中间代理应该使用该 Relay-Session-Id 标签。如果它不能使用现有的标签，或者没有足够空间来增加一个 Relay-Session-Id 标签，那么它应该向发送者返回一个 Generic-Error 标签。 |
| 0x0201 | Service-Name-Error | 该 Tag 典型的有一个长度为零的数据部分。它表明了由于某种原因，没有理睬所请求的 Service-Name。如果有数据部分，并且数据部分的头一个字节非 0，那么它必须是一个可打印字符串，解释请求被拒绝的原因。该字符串可以不以 NULL 结束。 |
| 0x0202 | AC-System-Error | 该 Tag 表明了接入服务器在处理主机请求时出现了某个错误。例如没有足够资源来创建一个虚拟电路。PADS 数据包中可以包含该标签。如果有数据，并且数据的第一个字节不为 0，那么数据必须是一个可打印字符串，该字符串解释了错误的性质。该字符串可以不以 NULL 结束。 |
| 0x0203 | Generic-Error | 该 Tag 表明发生了一个错误。当发生一个不可恢复的错误并且没有其它合适的 Tag 时，它可被加到 PADO、PADR 或 PADS 数据包中。如果出现数据部分，那么数据必须是一个解释错误性质的字符串。该字符串不允许以 NULL 结束。 |

### Checksum 域

校验和字段，用于检验报文的正确性。

## 3.4.2 PPPoE 会话建立过程

PPPoE 会话建立过程分为以下两个阶段：

- Discovery 阶段：地址发现阶段
- PPPoE Session 阶段：PPPoE 会话阶段

为了在以太网上建立点到点连接，每一个 PPPoE 会话必须知道通信对方的以太网地址，并建立一个唯一的会话标识符。PPPoE 通过地址发现协议查找对方的以太网地址。

当某个主机希望发起一个 PPPoE 会话时，它首先通过地址发现协议来确定对方的以太网 MAC 地址并建立起一个 PPPoE 会话标识符 Session ID。

虽然 PPP 定义的是点到点的对等关系，地址发现却是一种客户端-服务器关系。在地址发现的过程中，主机作为客户端，发现某个作为服务器的接入访问集中器 AC（Access Concentrator）的以太网地址。

根据网络的拓扑结构，可能主机跟不止一个访问集中器通信。Discovery 阶段允许主机发现所有的访问集中器，并从中选择一个进行通信。

当 Discovery 阶段成功完成之后，主机和访问集中器两者都具备了在以太网上建立点到点连接所需的所有信息。

在开始建立一个 PPPoE 会话之前，Discovery 阶段一直保持无状态（stateless）。

一旦开始建立 PPPoE 会话，主机和作为接入服务器的访问集中器都必须为一个 PPP 虚拟接口分配资源。

进入 PPPoE 会话阶段后，需要进行 LCP 协商，协商得到的 MRU 值最大为 1492 字节。因为以太帧长最大为 1500 字节，而 PPPoE 帧头为 6 字节、PPP 协议 ID 为 2 字节，因此 PPP 的 MTU 值最大为 1492。当 LCP 断开连接时，主机和访问集中器之间停止 PPPoE 会话，如果主机需要重新开始 PPPoE 会话，需要重新回到 PPPoE Discovery 阶段。

LCP 协商成功后，还需要进行 NCP 协商，协商成功后，主机和接入服务器便可以通信了。关于 LCP 和 NCP 协商过程，请参见 **2.4.3 PPP 的建链过程**。

## Discovery 阶段

### Discovery 阶段基本原理

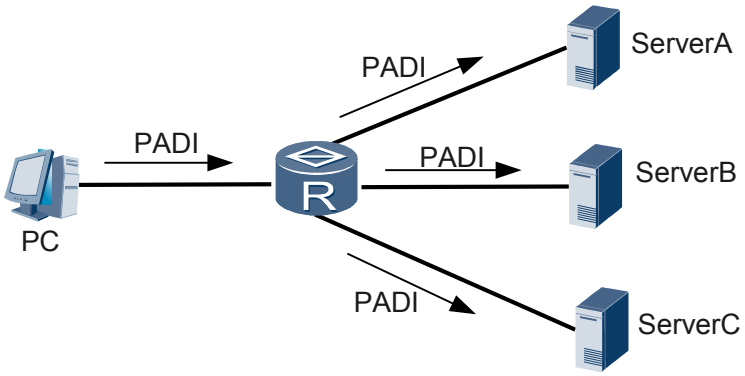
当主机开始通过 PPPoE 接入服务器时，它必须先识别接入端的以太网 MAC 地址，建立 PPPoE 的 Session_ID。这就是 Discovery 阶段的目的。

Discovery 阶段由四个过程组成。完成之后通信双方都会知道 PPPoE 的 Session_ID 以及对方以太网地址，它们共同确定了唯一的 PPPoE 会话。

Discovery 阶段的四个过程如下。

1. 主机在本以太网内广播一个 PADI（PPPoE Active Discovery Initial）报文，在此报文中包含主机想要得到的服务类型信息。

**图 3-4 主机以广播形式发送 PADI 报文**



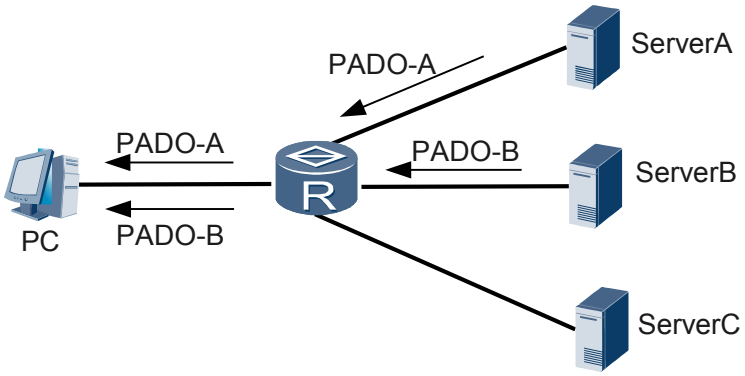
说明

- 如果在 PPPoE 的服务器端配置 service-name，Client 将发送 Discovery 阶段的 PADI 报文给服务器端请求建立连接。
- 如果该 PADI 报文中包含有不为空的 service-name 时，服务器端将用配置的 service-name 和该报文中的 service-name 进行完全匹配性检测。如果两者完全相同，服务器端提供后续服务，否则，服务器端不提供服务。
- 以上是两者的 service-name 都不为空时的情况。但如果两者中有一个 service-name 为空，就不进行此项检测，直接按照原来的程序执行。AR200-S 设备不支持配置 service-name。

2. 以太网内的所有服务器收到这个 PADI 报文后，将其中请求的服务与自己能提供的服务进行比较，可以提供此服务的服务器发回 PADO（PPPoE Active Discovery Offer）报文。

   如图 3-5 中，ServerA 和 ServerB 都可以提供服务，所以都会向主机发回 PADO 报文。

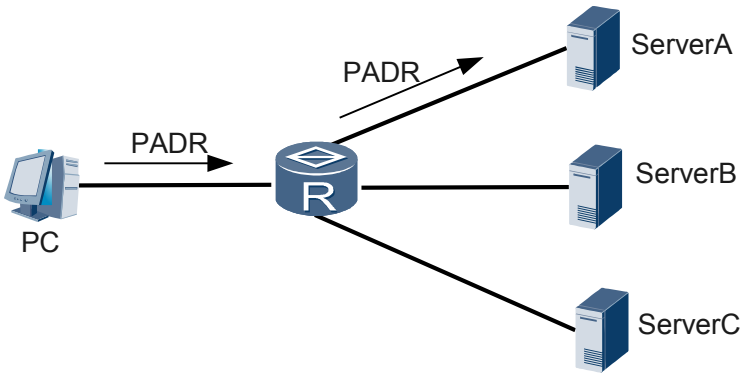
**图 3-5 服务器发回 PADO 报文**




3. 主机可能收到多个服务器的 PADO 报文，主机将依据 PADO 的内容，从多个服务器中选择一个，并向它发回一个会话请求报文 PADR（PPPoE Active Discovery Request）。

   如图 3-6 所示，主机选择 ServerA，并发回 PADR 报文。

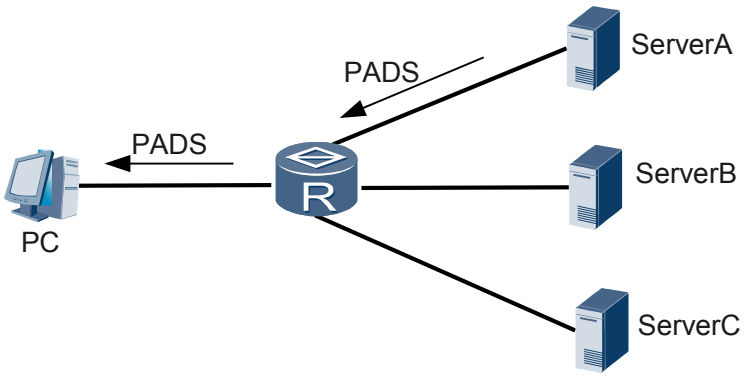
**图 3-6 主机选择一个服务器并发送 PADR 报文**



4. 服务器产生一个唯一的会话标识，标识和主机的这段 PPPoE 会话。并把此会话标识通过会话确认报文 PADS（PPPoE Active Discovery Session-confirmation）发回给主机，如果没有错误，双方进入 PPPoE Session 阶段。

   例如在图 3-7 中，ServerA 收到 PADR 报文后，会向主机发送 PADS 报文。

**图 3-7** 服务器向主机发回 PADS 报文



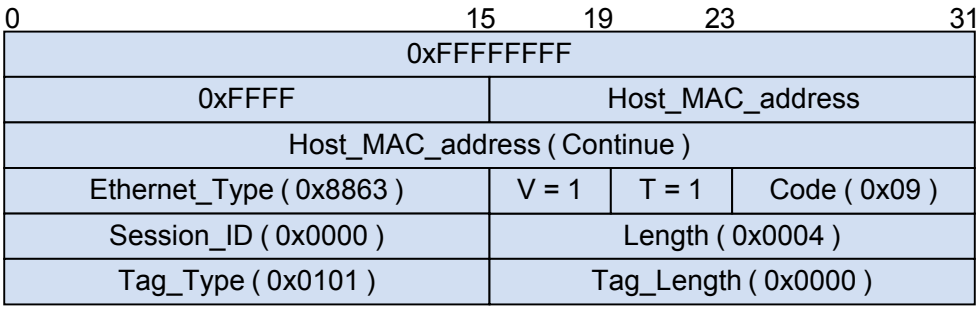

接入服务器发送确认数据包后，它就可以进入到 PPPoE 会话阶段。当主机接收到该确认数据包后，它就可以进入 PPPoE 会话阶段。

**PADI 数据包**

主机发送的 PADI 数据包中，Destination_address 域为广播地址，Code 域设置为 0x09，Session_ID 域设置为 0x0000。

PADI 数据包必须包含且仅包含一个 Tag_Type 为 Service-Name 的 Tag，以表明主机请求的服务，以及任意数目的其它类型的 TAG。整个 PADI 数据包，包括 PPPoE 头部不允许超过 1484 个字节，以预留空间让中继代理向数据包中增加类型为 Relay-Session-Id 的 Tag。

**图 3-8** PADI 报文结构示例图



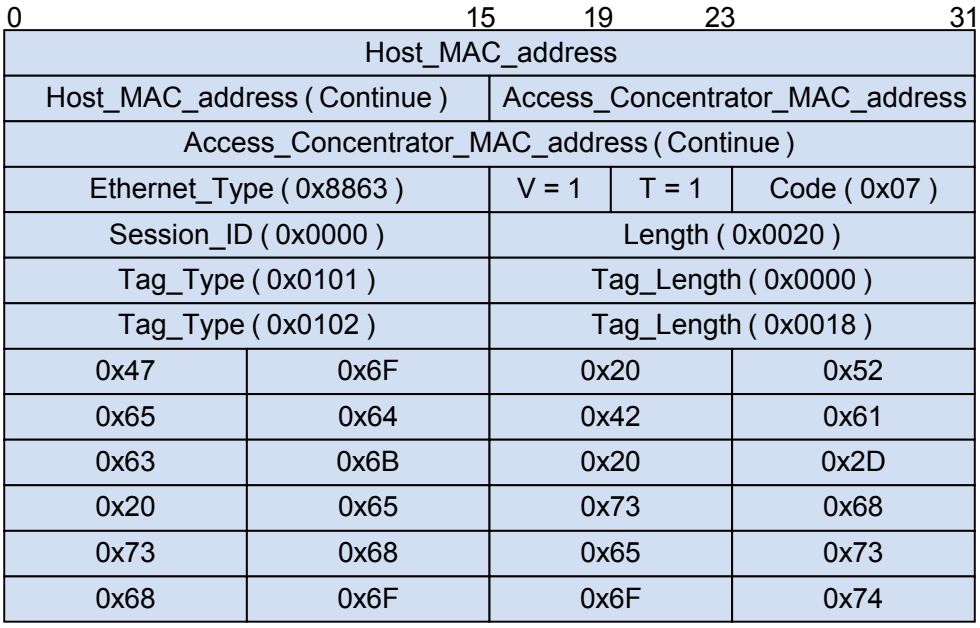

**PADO 数据包**

如果接入服务器能够为收到的 PADI 请求提供服务，它将通过发送一个 PADO 数据包来做出应答。Destination_address 是发送 PADI 报文的主机的单播地址，Code 域设置为 0x07，Session_ID 域设置为 0x0000。

PADO 数据包必须包含一个类型为 AC-Name 的 Tag，AC 是接入服务器的名字。还必须包含与 PADI 中相同的 Service-Name，以及任意数目的类型为 Service-Name 的 Tag，表明接入服务器提供的其它服务。

如果接入服务器不能为 PADI 提供服务，则不允许用 PADO 作响应。

**图 3-9** PADO 报文结构示例图




**PADR 数据包**

由于 PADI 是广播的，主机可能收到不止一个 PADO 回应报文。它将审查接收到的所有 PADO 报文，并根据其中的 AC-Name 或 PADO 所提供的服务来选择一个做为自己的服务器。

主机向选中的接入服务器发送一个 PADR 数据包。其中，Destination_address 域设置为发送 PADO 的接入服务器的单播地址，Code 域设置为 0x19，Session_ID 设置为 0x0000。

PADR 必须包含且仅包含一个 Tag_Type 为 Service-Name 的 TAG，表明主机请求的服务，以及任意数目其他类型的 Tag。

**PADS 数据包**

当接入服务器收到一个 PADR 数据包，它就准备开始一个 PPPoE 会话。接入服务器为 PPPoE 会话创建一个唯一的 Session_ID 并用一个 PADS 数据包向主机响应。Destination_address 域是发送 PADR 数据包的主机的单播以太网地址，Code 域设置为 0x65，Session_ID 设置为创建好的 PPPoE 会话标识符。

PADS 数据包中包含且仅包含一个 Tag_Type 为 Service-Name 的 Tag，表明接入服务器已经接受的该 PPPoE 会话的服务类型，以及任意数目的其他类型的 Tag。

如果接入服务器不接受 PADR 中的 Service-Name，则接入服务器也回应给主机一个 PADS 报文，但该 PADS 中带有类型为 Service-Name-Error 的 Tag 以及任意数目的其它 TAG 类型。这种情况下，Session_ID 必须设置为 0x0000。

**PADT 数据包**

PADT（PPPoE Active Discovery Terminate）数据包可以在会话建立以后的任意时刻发送，表明 PPPoE 会话已经终止。

它可以由主机或接入服务器发送，Destination_address 域为单播以太网地址，Code 域设置为 0xA7，Session_ID 必须表明终止的会话，这种数据包不需要任何 Tag。

当收到 PADT 以后，就不允许再使用该会话发送 PPP 流量了。在发送或接收到 PADT 后，即使是常规的 PPP 结束数据包也不允许发送。

PPP 通信双方应该使用 PPP 协议自身来结束 PPPoE 会话，但在无法使用 PPP 时可以使用 PADT 结束通信。

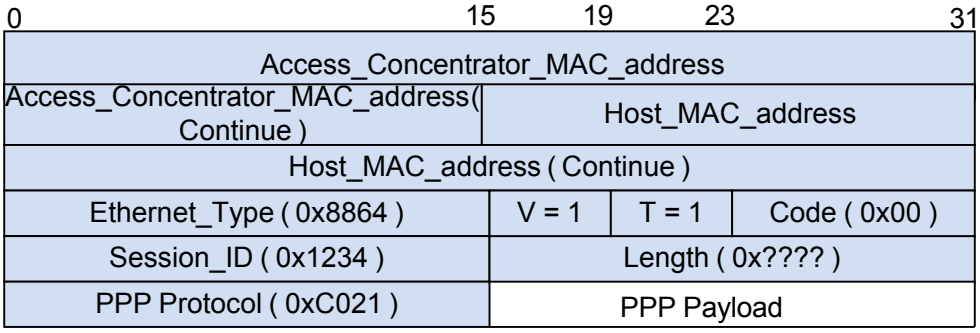
## PPPoE 会话阶段

PPPoE 会话（PPPoE Session）开始后，PPP 报文作为 PPPoE 帧的净荷，封装在以太网帧发送到对端。

这时所有的以太网数据包都是单播的。

- Ethernet_Type 域设置为 0x8864。
- PPPoE 的 Code 必须设置为 0x00。
- PPPoE 会话的 Session_ID 不允许发生改变，必须是 Discovery 阶段所指定的值。
- PPPoE 的 Payload 包含一个 PPP 帧。PPP 帧的开始字段是 PPP Protocol-ID。

**图 3-10 从主机发送到接入服务器的 PPP LCP 数据包示例图**




进入 PPPoE Session 阶段后，主机或服务器任何一方都可发 PADT 报文通知对方结束 PPPoE 会话。

# 3.5 应用

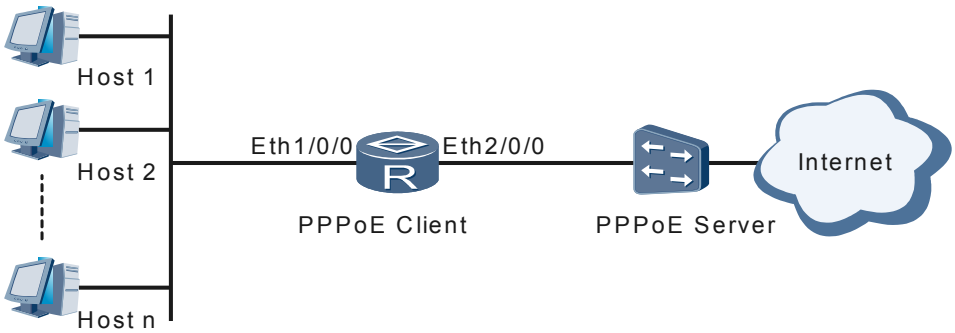
## 3.5.1 PPPoE Client

当 AR200-S 设备将 PPPoE 作为一种 WAN（Wide Area Network）接入方式时，AR200-S 充当 PPPoE Client 的角色，BRAS（Broadband Remote Access Server）作为 PPPoE Server。

如图 3-11 所示，在 AR200-S 和 PPPoE Server 之间建立 PPPoE 会话，局域网内的所有主机通过同一个会话传送数据。

一般情况下，局域网内的主机使用私网 IP 地址，这就要求 AR200-S 需要提供 NAT（Network Address Translation）功能，实现将主机的私网 IP 地址转换为公网 IP 地址。

**图 3-11** AR200-S 作为 PPPoE Client 典型组网图

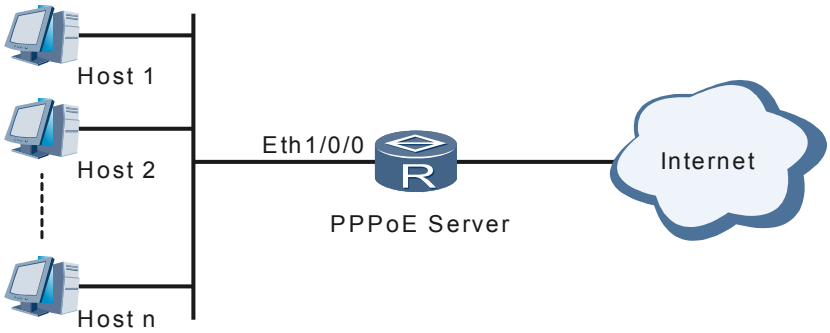



这种组网方式不需要在用户主机上安装 PPPoE 客户端拨号软件。

## 3.5.2 PPPoE Server

AR200-S 设备提供了 PPPoE Server 的功能，支持动态分配 IP 地址，提供本地认证、RADIUS/HWTACACS 等多种认证方式，配合包过滤防火墙及状态防火墙，可以对内部网络提供安全保障，适用于校园、智能小区等通过以太网接入 Internet 的组网应用。

**图 3-12** AR200-S 作为 PPPoE Server 典型组网图




这种组网方式需要在用户主机上安装 PPPoE 客户端拨号软件。

# 3.6 术语与缩略语

## 缩略语

| 缩略语 | 英文全称 | 中文全称 |
| --- | --- | --- |
| PADI | PPPoE Active Discovery Initial | PPPoE 激活发现阶段起始报文 |
| PADO | PPPoE Active Discovery Offer | PPPoE 激活发现阶段服务报文 |
| PADR | PPPoE Active Discovery Request | PPPoE 激活发现阶段会话请求报文 |
| PADS | PPPoE Active Discovery Session-confirmation | PPPoE 激活发现阶段会话确认报文 |
| PADT | PPPoE Active Discovery Terminate | PPPoE 激活发现阶段会话终止报文 |
| PPPoE | PPP over Ethernet | 以太网承载 PPP 协议 |

# 4 DCC

## 关于本章

# 4.1 介绍

## 定义

拨号控制中心 DCC（Dial Control Center）是指路由器之间通过 ISDN 网络、3G 网络等进行互联时或者路由器作为 PPPoE/PPPoEoA Client 与 PPPoE/PPPoEoA Server 之间互联时所采用的技术，DCC 主要提供按需拨号服务。

所谓按需拨号是指跨 ISDN 网络、3G 网络等相连的路由器之间或者路由器作为 PPPoE/PPPoEoA Client 与 PPPoE/PPPoEoA Server 之间不预先建立连接，当它们之间有数据需要传送时才启动 DCC 拨号流程以拨号的方式建立连接并传送信息，当链路再次空闲时，DCC 会自动断开连接。

## 目的

由于某些场合下，路由器之间仅在有数据需要传送时才建立连接并通信，传送的信息具有时间不相关性、突发性、总体数据量小等特点，DCC 为此种应用提供了灵活、经济、高效的解决方案。

实际应用中，DCC 主要应用于以下两种场景：

- 以备份形式为干线通讯提供保障，在干线因为线路或其它原因出现故障而不能正常通信时，提供替代的辅助通路，确保业务正常进行。
- 当路由器作为 PPPoE/PPPoEoA Client 时，DCC 通过按需拨号的功能，为用户节省费用。

## 受益

DCC 特性给企业用户带来了如下的受益。

- 费用的节省：路由器之间不预先建立连接，当它们之间有数据需要传送时才以拨号的方式建立连接，当连接再次空闲，DCC 会切断当前的连接，以节省用户的费用。
- 通讯保障：DCC 作为干线备份为用户提供了通讯保障，在干线因为线路或其它原因出现故障而不能正常通信时，提供替代的辅助通路，确保业务正常进行运转。
- 灵活的部属：共享 DCC 可以使物理接口根据连接选择不同的工作参数，从而实现一口多用。

# 4.2 参考标准和协议

无

# 4.3 可获得性

## License 支持

无需获得 License 许可，均可获得该特性的服务。

### 版本支持

| 产品 | 最低支持版本 |
| --- | --- |
| AR200-S | V200R002C00 |

### 特性依赖

DCC 特性的实现依赖以下特性：DCC 结合其他特性实现拨号。DCC 结合 PPPoE 特性实现 PPPoE 拨号；结合 PPP、xDSL 特性实现 PPPoA 及 PPPoEoA 拨号。

AR200-S 只支持共享 DCC。

### 硬件要求

无

## 4.4 原理描述

AR 支持两种 DCC：轮询 DCC（Circular DCC，C-DCC）和共享 DCC（Resource-Shared DCC，RS-DCC）。两种方式具有各自不同的特点，适用于不同的应用需求，在应用时呼叫双方可以根据需要灵活选用配置方法，例如一端采用轮询 DCC，另一端采用共享 DCC。

在介绍 DCC 的原理之前先介绍几个 DCC 配置术语，以方便用户理解 DCC。

- 物理接口

  实际存在的物理接口，如 ISDN BRI、ISDN PRI、Cellular 等接口。
- Dialer 接口

  为了配置 DCC 参数而设置的逻辑接口。物理接口可以通过绑定到 Dialer 接口而继承配置信息。
- 拨号接口

  是对拨号连接接口的泛称。可以是 Dialer 接口，也可以是捆绑到 Dialer 接口的物理接口，或者是直接配置 DCC 参数的物理接口。

### 4.4.1 轮询 DCC

轮询 DCC 中同一个物理接口只能属于一个拨号接口，所以轮询 DCC 适用于物理链路较多，连接情况复杂的大中型站点。

轮询 DCC 具有功能强大、应用广泛的优势，但是相对缺乏伸缩性、扩展性。具体来说轮询 DCC 有以下特点：

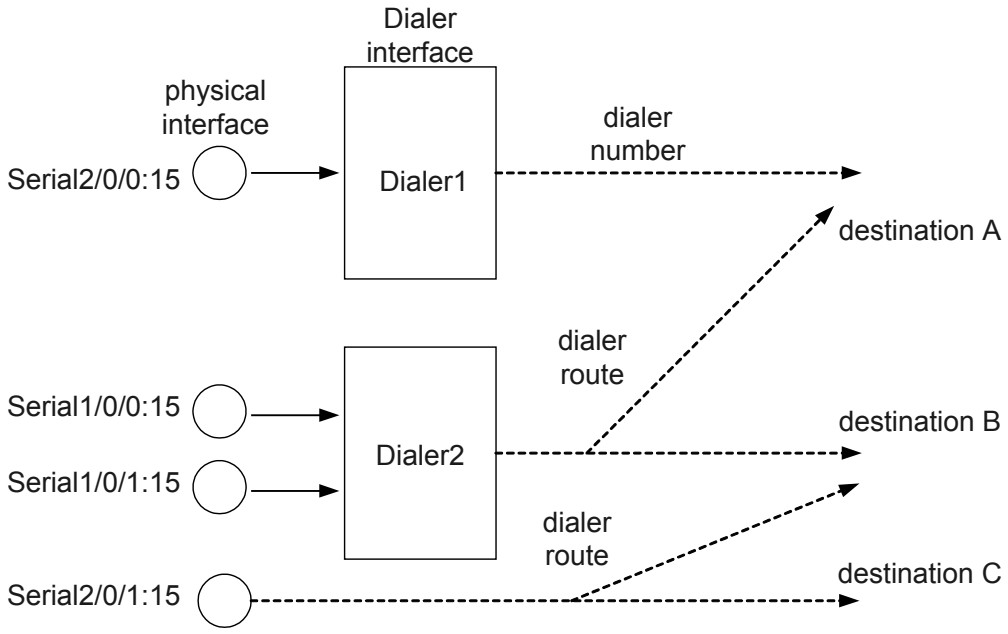
- 一个 Dialer 接口可以有多个物理接口为它服务，而任意一个物理接口只能属于一个 Dialer 接口，即一个物理接口只能服务于一种拨号服务。
- 物理接口既可以借助拨号循环组（Dialer Circular Group）绑定到 Dialer 接口来继承 DCC 参数，又可以直接配置 DCC 参数。
- 服务于同一个 Dialer Circular Group 的所有物理接口都继承同一个 Dialer 接口的属性。

- 一个 Dialer 接口可以通过配置多个 **dialer route** 命令对应多个呼叫目的地址，也可以配置 **dialer number** 命令对应单个呼叫目的地址。

此外，由于 ISDN BRI 接口中所有 B 通道都会继承该物理接口的相同配置信息，并且 **dialer route** 会随着网络规模的增大和支持协议的增多而逐渐复杂化，因此轮询 DCC 应用就受限于目的站呼叫设置与物理接口配置之间的静态绑定。

轮询 DCC 的物理接口和 Dialer 接口对应关系如图 4-1 所示。

**图 4-1** 轮询 DCC 的物理接口和 Dialer 接口对应关系




从上图可以看出，如果使用 Dialer 接口，同一物理接口仅能属于一个 Dialer 接口，每个 Dialer 接口可以对应多个目的地址；每个 Dialer 接口可以包含多个物理接口。另外，物理接口也可以不属于任何 Dialer 接口，而直接映射到一个或多个目的地址。

## 4.4.2 共享 DCC

共享 DCC 中不同的拨号接口可以共享同一个物理链路，在不同的拨号中，同一个物理链路可以使用不同的工作参数。物理链路工作参数的切换自动根据连接来决定，不需要管理员的干预。因此共享 DCC 适用于可用物理链路较少，但连接需求较多的中小型站点。

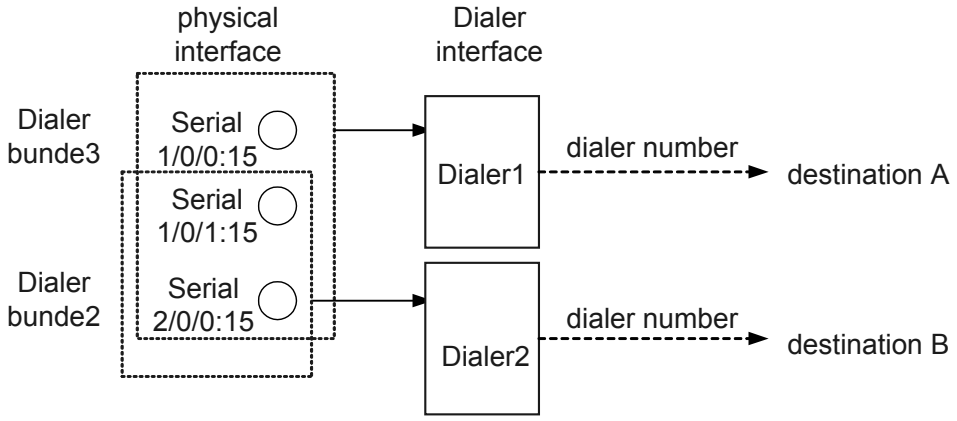
由于实现了逻辑配置和物理配置的相互分离，共享 DCC 比轮询 DCC 简单，并具有良好的灵活性。具体来说共享 DCC 有以下特点：

- 将物理接口的配置与呼叫的逻辑配置分开进行，再将两者动态的捆绑起来，从而实现相同物理接口为多种不同拨号应用服务。
- 一个 Dialer 接口只对应一个呼叫目的地址。
- 每个 Dialer 接口可以有多个物理接口为它提供服务，同时任意一个物理接口也可服务于多个 Dialer 接口。

- 共享 DCC 使用共享属性集（RS-DCC set）来描述拨号属性，去往同一个目的网络的所有呼叫使用同一个共享属性集（包括 Dialer 接口、Dialer bundle 和物理接口等参数）。
- 在物理接口上不能直接配置共享 DCC 参数，物理接口必须通过绑定到 Dialer 接口才能实现共享 DCC 拨号功能。

共享 DCC 的物理接口、Dialer bundle 和 Dialer 接口对应关系如图 4-2 所示。

**图 4-2 共享 DCC 的物理接口、Dialer bundle 和 Dialer 接口对应关系**




从上图可以看出，在共享 DCC 方式，同一物理接口可以属于多个 Dialer bundle，并进而服务于多个 Dialer 接口。每个 Dialer 接口只能使用一个 Dialer bundle，同时也只能设置一个目的地址。

同一个 Dialer bundle 中的物理接口可以有不同的优先级，Dialer bundle 对应的 Dialer 口可以根据优先级选择呼叫时使用的物理接口。比如，Dialer2 使用 Dialer bundle2，物理接口 Serial2/0/0:15、Serial1/0/1:15 属于 Dialer bundle2，每个物理接口具有不同的优先级。假设在 Dialer bundle2 中 Serial2/0/0:15 的优先级是 100，Serial1/0/1:15 的优先级是 50，由于 Serial2/0/0:15 的优先级高于 Serial1/0/1:15 的优先级，当 Dialer2 从 Dialer bundle2 中选择一个物理接口时，会优先使用 Serial2/0/0:15 接口。

相同的物理接口在不同的 Dialer bundle 中可以有不同的优先级。

## 4.4.3 动态路由备份

### 特点

动态路由备份作为一种新的备份方式，主要使用 DCC 功能动态维护拨号链路，即基于路由进行的拨号备份。

动态路由备份很好地集成了备份和路由功能，提供了可靠的连接和规范的按需拨号服务。

动态路由备份的特点：

- 动态路由备份主要是针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。

- 动态路由备份不对特定接口或特定链路进行备份，适用于多接口和多路由器的情况。
- 动态路由备份的主链路断开时备份链路将自动启动，不会导致拨号延迟（该延迟未包括路由收敛时间）。
- 动态路由备份不依赖于具体的路由协议，可以和 RIP-1、RIP-2、OSPF、IS-IS、BGP 等路由协议配合工作。但有些路由协议（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，导致动态路由监控失败，备份链路在主链路恢复时无法挂断。

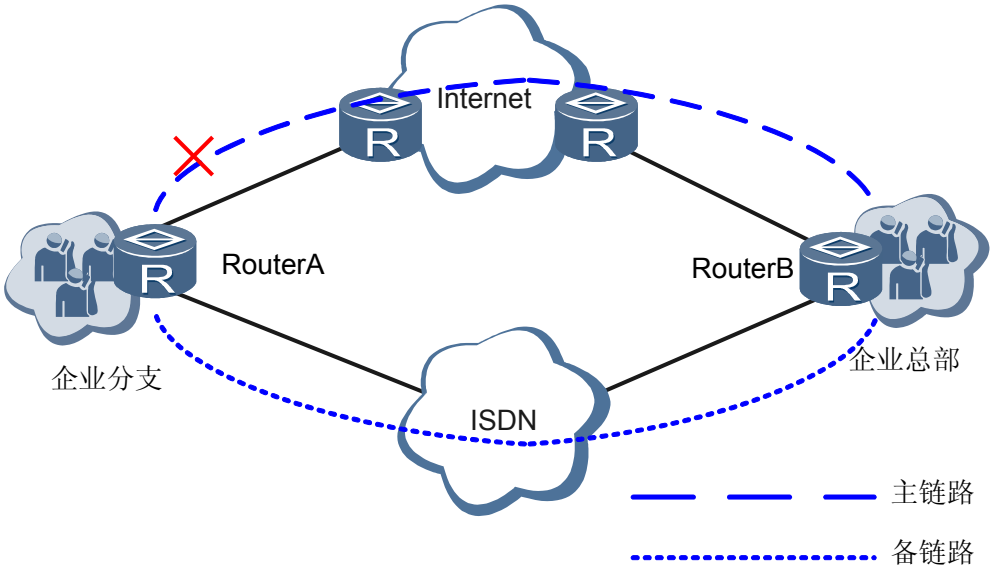
  对于 BGP 协议，需要使用下面的方法来解决这种问题：

  - 备份链路的 IP 地址要大于主链路的 IP 地址；
  - 配置负载分担，即让同一路由可以通过多条链路学到。

## 动态路由备份的实现步骤

通过配置要监控的网段，可以实现在主链路故障时启动备份链路。

**图 4-3 动态路由备份**




图中，RouterA 和 RouterB 是 AR200-S。动态路由备份监控路由、启动备份链路的顺序如下：

1. 系统监控到达需监控网段（企业总部所在网段）是否存在路由更新，并检查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，则认为主链路关闭并且不可用，拨号启动备份链路；
4. 备份链路启动后，由备份链路承载通信数据。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。

# 4.5 应用

实际应用中，通过对 DCC 提供的按需拨号的扩展应用，DCC 有了更广的应用范围。DCC 主要应用于以下两种场景：

- 以备份形式为干线通讯提供保障，在干线因为线路或其它原因出现故障而不能正常通信时，提供替代的辅助通路，确保业务正常进行。

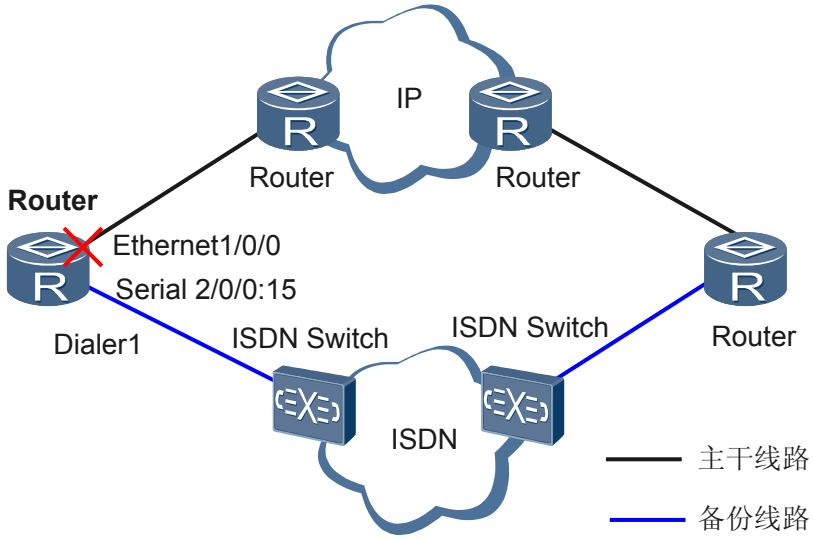
  一般来讲是通过与现有网络不同的网络进行备份，比如通过 ISDN 网络或者 3G 网络备份 IP 网络中的干线链路。AR200-S 提供备份功能时，支持两种备份方式：

  - 通过接口备份实现
  - 通过动态路由备份实现
- 当路由器作为 PPPoE/PPPoEoA/PPPoA Client 时，DCC 通过按需拨号的功能，为用户节省费用。

**通过接口备份实现干线通信备份**

通过接口备份实现干线通信备份组网图如图 4-4 所示。Serial2/0/0:15 接口是拨号接口，用来备份 Ethernet1/0/0。当接口 Ethernet1/0/0 因故障不能传输数据时，接口上的所有流量会切换到 Serial2/0/0:15 上。流量会触发 DCC 拨号，从而实现使用 ISDN 网络备份干线通信。

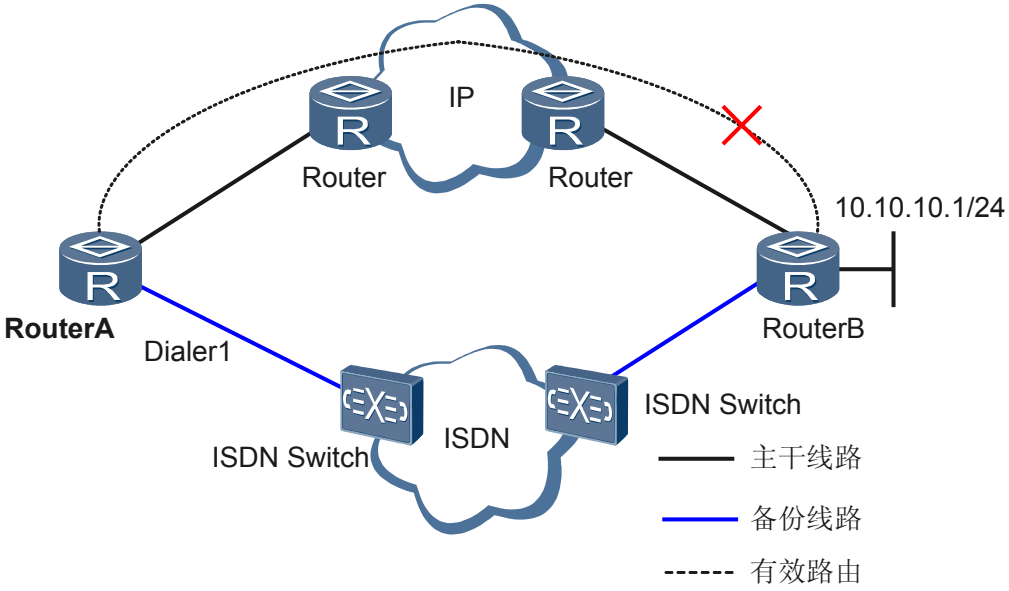
**图 4-4 通过接口备份实现干线通信备份组网图**




**通过动态路由备份实现干线通信备份**

通过动态路由备份实现干线通信备份组网图如图 4-5 所示。当 RouterA 到 RouterB 的 10.10.10.1/24 网段没有有效路由时，RouterA 的拨号接口会启动 DCC 拨号，从而实现使用 ISDN 网络备份干线通信。

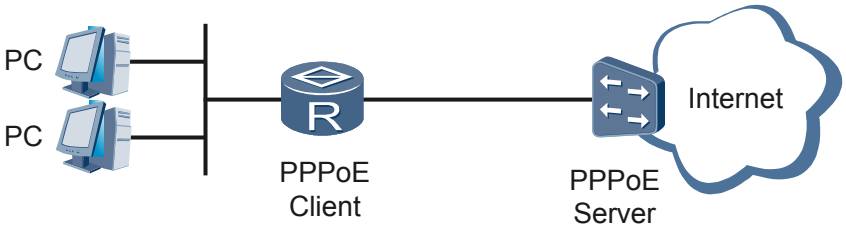
**图 4-5** 通过动态路由备份实现干线通信备份组网图




**路由器作为 PPPoE Client 时的按需拨号**

路由器作为 PPPoE Client 时的按需拨号组网图如图 4-6 所示。在拨号连接已经建立的情况下，当 PPPoE Client 到 PPPoE Server 之间没有流量时，PPPoE Client 启用闲时断开功能将 PPPoE 连接断开。一旦 PPPoE Client 到 PPPoE Server 再有流量，会触发 DCC 拨号并建立 PPPoE 连接。

**图 4-6** 路由器作为 PPPoE Client 时的按需拨号组网图




说明

如果路由器作为 PPPoEoA Client，组网时还需要通过 DSLAM 设备接入 PPPoEoA Server。用于该场景的 DCC 必须是共享 DCC。

# 4.6 术语与缩略语

## 术语

| 术语 | 解释 |
| --- | --- |
| 拨号控制中心 | 拨号控制中心是指路由器之间通过 ISDN 网络、3G 网络等进行互联时或者路由器作为 PPPoE/PPPoEoA Client 与 PPPoE Server 之间互联时所采用的技术，DCC 主要提供按需拨号服务。 |
| 按需拨号 | 按需拨号是指跨 ISDN 网络、3G 网络等相连的路由器之间或者路由器作为 PPPoE/PPPoEoA Client 与 PPPoE Server 之间不预先建立连接，当它们之间有数据需要传送时才以拨号的方式建立连接，即启动 DCC 拨号流程建立连接并传送信息，当链路再次空闲时，DCC 会自动断开连接。 |
| 物理接口 | 实际存在的接口，如 ISDN BRI、ISDN PRI、Cellular 等接口。 |
| Dialer 接口 | 为了配置 DCC 参数而设置的逻辑接口。物理接口可以通过绑定到 Dialer 接口而继承配置信息。 |
| 拨号接口 | 是对拨号连接接口的泛称。可以是 Dialer 接口，也可以是捆绑到 Dialer 接口的物理接口，或者是直接配置 DCC 参数的物理接口。 |

## 缩略语

| 缩略语 | 英文全称 | 中文全称 |
| --- | --- | --- |
| 3G | 3rd Generation | 第三代技术 |
| DCC | Dial Control Center | 拨号控制中心 |
| ISDN | Integrated Services Digital Network | 综合业务数字网 |
| PPPoE | Point-to-Point Protocol over Ethernet | 以太网承载 PPP 协议 |