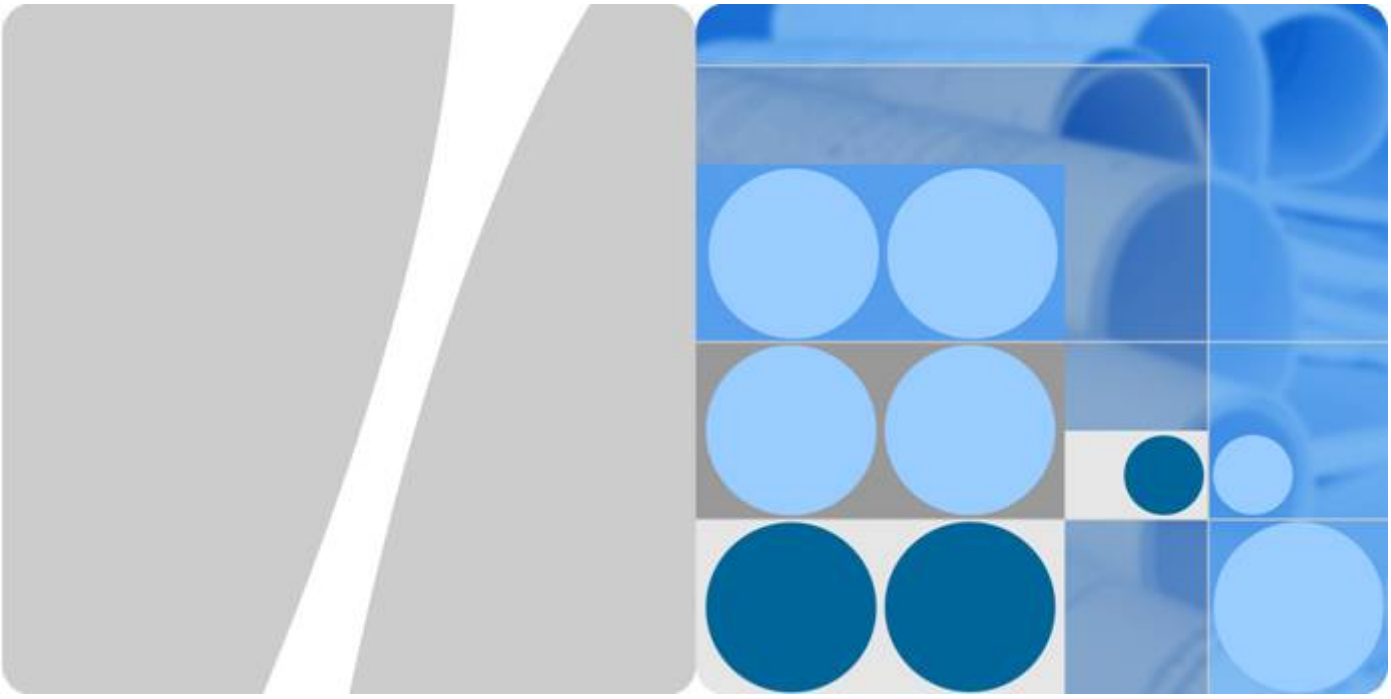


UA5000 一体化接入单元

V100R019C02

特性描述

文档版本　02

发布日期　2011-08-30

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

UA5000 综合接入设备（以下简称 UA5000）在提供高质量语音接入业务、宽带接入业务的同时，还向用户提供完善的 IP 语音接入业务以及多媒体业务。

本文档针对 UA5000 的主要特性，从定义、目的、规格和实现原理等方面，对系统功能进行详细介绍。

本文档主要适用于以下工程师：

- 网络规划工程师
- 数据配置工程师

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。

修订记录

修订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 02 (2011-08-30)

相对产品版本 V100R019C02 文档版本 01 (2011-07-30)的变更如下。

修改：

- **3.1 介绍**

文档版本 01 (2011-07-30)

相对产品版本 V100R019C01 文档版本 01 (2010-12-30)的变更如下。

修改：

- **43.1 介绍**
- **37.2 可获得性**
- **24.1 介绍**
- **24.4 原理描述(PVM)**

目 录

1 GPON 上行

关于本章

GPON（Gigabit-capable Passive Optical Network）上行是指上行口为 GPON 接口。GPON 是一种一对多的宽带光传输系统，支持 GEM 功能，能够传输任何类型的数据。

1.1 介绍

介绍 GPON 上行特性的定义、目的、规格等信息。

定义

xPON 是一种点到多点（P2MP）结构的无源光网络。GPON（Gigabit-capable Passive Optical Network）是由 ITU-T G.984.x 系列标准规范的千兆比特 PON（Passive Optical Network）。UA5000 采用 GP1A 单板提供 GPON 上行接口，和 OLT 设备一起组成 GPON 网络。

目的

GPON 支持高带宽传输，可以有效解决双绞线接入的带宽瓶颈，满足用户对高带宽业务的需求，如高清电视、实况转播等。GPON 支持长距离接入，可以解决双绞线接入长距离覆盖的问题，减少网络节点。

UA5000 作为 MDU（Multi Dwelling Unit）设备，可利用 GPON 网络覆盖广、组网灵活、维护成本低的特点，和 OLT 设备一起向用户提供高带宽接入方式，同时提高 OLT 端的用户密度。

规格

- 支持一个 GPON 上行端口，下行速率 2.488Gbit/s，上行速率 1.244Gbit/s。
- 支持 8 个 T-CONT，32 个 GEM 端口。
- OLT 通过 OMCI（Optical Network Termination Management and Control Interface）对 UA5000 的 PON 板业务进行配置管理即当作 ONT 的终端进行管理。OLT 不管理 UA5000 原有的业务。

约束

无

术语

表 1-1 GPON 上行特性术语表

术语	解释
GPON 网络	GPON 是一种一对多的宽带光传输系统，支持 GEM 功能，能够传输任何类型的数据。

术语	解释
T-CONT	T-CONT 管理传输汇聚层的无源光网络的上行带宽分配，主要用于提高无源光网络的上行带宽使用效率。 ● T-CONT 携带 GEM 端口，并向相关的 OLT 报告其缓存状态。T-CONT 由其 Alloc-ID 唯一标识，并从 OLT 处动态接收许可（即允许其发送上行数据的许可）。 ● 一个 T-CONT 可以携带不同业务等级的 GEM 业务流。 ● 一个 T-CONT 可以容纳一个或者多个物理队列，并能将队列聚合成单一的逻辑缓存。 ● 支持动态带宽分配的 T-CONT 的状态报告中包含了本 T-CONT 的逻辑缓存的状态。 ● T-CONT 是传输汇聚层的传输实体，从入口向出口透明传输高层信息。 ● 通过 T-CONT 的信息不会改变，除非在传输过程中质量降低。

缩略语

表 1-2 GPON 上行特性缩略语表

缩略语	英文全称	中文全称
GEM	GPON Encapsulation Mode	GPON 封装模式
OLT	Optical Line Terminal	光线路终端
ONU	Optical Network Unit	光网络单元
ONT	Optical Network Terminal	光网络终端
OMCI	Optical Network Termination Management and Control Interface	光网络终端管理控制接口

1.2 可获得性

介绍 GPON 上行特性需要哪些硬件和 License 的支持才能提供相应的服务。

硬件支持

支持 GPON 上行特性的单板是 GP1A 单板。

License 支持

GPON 上行特性是 UA5000 的基本特性，无需获得 License 许可即可获得该特性的服务。

1.3 原理描述

介绍 GPON 上行特性的实现原理。

- UA5000 通过 GPON 上行接口采用 PLOAM 协议，向 OLT 设备进行注册，上报自身的 Serial Number，OLT 根据内部 Serial Number 数据库判定是否允许其注册。
- UA5000 向 OLT 设备注册成功后，由 OLT 为其分配 T-CONT，T-CONT 的索引是 Alloc ID，范围从 0 到 4095。UA5000 支持最大 8 个 T-CONT，OLT 将给这些 T-CONT 分配带宽，设置带宽参数。
- UA5000 从交换网片上行的数据报文经过分类器，被映射到指定 GEM Port，再映射到 T-CONT。

用户通过 OLT 配置各个业务流的映射动作。

1.4 参考信息

介绍与 GPON 上行特性相关的参考信息。

本特性的参考资料清单如下：

- ITU-T G.984.2，Gigabit-capable Passive Optical Networks (GPON): Physical Media Dependent (PMD) Layer Specification
- ITU-T G.984.3，Gigabit-capable Passive Optical Networks (GPON): Transmission Convergence Layer Specification

2 EPON 上行

关于本章

EPON（Ethernet Passive Optical Network）上行是指上行口为 EPON 接口。EPON 的开发旨在实现全业务接入网络，即在一条光纤上传输汇聚的数据、视频和语音数据。

2.1 介绍

介绍 EPON 上行特性的定义、目的、规格等信息。

定义

UA5000 采用 EP1A 单板提供 EPON 上行端口，和 OLT 设备一起组成 EPON 网络。

目的

UA5000 支持上行 EPON 接口，作为 MDU 设备，可利用 EPON 网络覆盖广、组网灵活、维护成本低的特点，和 OLT 设备一起向用户提供高带宽接入方式，同时提高 OLT 端的用户密度。

规格

- 支持一个 EPON 上行端口，下行速率 1.25Gbit/s，上行速率 1.25Gbit/s。
- 支持最远 20km 的传输距离。

约束

无。

术语

无。

缩略语

表 2-1 EPON 上行特性缩略语表

缩略语	英文全称	中文全称
EPON	Ethernet Passive Optical Network	以太网无源光网络
MDU	Multi Dwelling Unit	多住户单元
MPCP	Multi-point Control Protocol	多点控制协议
OAM	Operations，Administration，and Maintenance	操作管理维护
OLT	Optical Line Terminal	光线路终端

2.2 可获得性

介绍 EPON 上行特性需要哪些硬件和 License 的支持才能提供相应的服务。

硬件支持

支持 EPON 上行特性的单板是 EP1A 单板。

License 支持

EPON 上行特性是 UA5000 的基本特性，无需获得 License 许可即可获得该特性的服务。

2.3 原理描述

介绍 EPON 上行特性的实现原理。

EPON 上行端口通过 MPCP（Multi-Point Control Protocol）的发现过程完成在 OLT 的注册，该过程符合 IEEE 802.3-2005 中 Clause 64.3.3 的规定。

UA5000 的 EPON 上行端口支持符合 IEEE802.3-2005 中 Clause 57 规定的 OAM 功能，并支持 IEEE802.3-2005 中 Clause 30 规定的管理对象（Managed Object Class）、属性（Attribute）和操作（Action）。

2.4 参考信息

介绍与 EPON 上行特性相关的参考信息。

本特性的参考资料清单如下：

- IEEE 802.3-2005 Local and metropolitan area networks - specific requirements Part 3

3 ADSL2+接入

关于本章

介绍 ADSL2+接入特性的定义、目的、规格、原理以及参考的术语、缩略语和相关协议标准。

3.1 介绍
介绍该特性的定义、目的、规格和约束条件。

3.2 可获得性
介绍该特性需要的硬件支持和 License 支持。

3.3 原理描述
介绍该特性的实现原理。

3.4 参考信息
介绍该特性相关的参考信息。

3.1 介绍

介绍该特性的定义、目的、规格和约束条件。

定义

ADSL（Asymmetrical Digital Subscriber Line）是在普通双绞线上为用户提供非对称的高速专线接入业务的一种技术。

ADSL2+是对 ADSL 技术的扩展，支持最高达 24Mbit/s 的下行速率和 2.8Mbit/s 的上行速率，最长传输距离可达 6.5km。

目的

ADSL 技术采用了适合用户数据接入业务的上下行不对称的传输业务，可为用户提供高速的数据传输通道。

规格

- ADSL2+兼容 ADSL、ADSL2。
- 实现的 ADSL2+速率下行最大可达 24Mbit/s，上行最大可达 2.5Mbit/s。
- 支持最长达 6.5km 的传输距离。
- 支持 ADSL2+业务，并且支持与 POTS 同时接入。
- 支持 G992.1 Annex A/B、G992.3 Annex A/B/M、G992.5 Annex A/B/M 传输模式。
- 支持快速的比特位交换。
- 支持功率管理功能，在 CO 及 CPE 设备都具有 Power cut back 功能。
- 支持在初始化时根据线路情况自动调整速率。
- 支持导频浮动，根据信道情况选择最合适的 TONE 作为导频。
- 支持频谱整形，通过 CO-MIB 对每一个 TONE 发射功率进行控制。
- 支持动态无缝速率自适应，增强对线路参数变化的适应能力。
- 支持 SELT 测试功能。
- 支持 ADSL 线路和频谱的配置、修改和查询。
- 支持线路、信道告警维护信息上报功能。
- 支持针对 ADSL2+的 Tone 的 PSD Value 进行配置和修改，也支持通过网管来配置，可以最多对 512 个 TONE 中的 32 个进行修改。

术语

表 3-1 ADSL 接入特性术语表

术语	解释
SELT	SELT（Single Ended Loop Test）是指单端测试，测试线路类型，线路长度，终端类型，近端噪声，桥接抽头。

术语	解释
TONE	TONE 是指子载波，例如将一个 1MHz 的带宽资源分为 256 个子载波，那每个子载波是一个 TONE。

缩略语

表 3-2 ADSL 接入特性缩略语表

缩略语	英文全称	中文全称
ADSL	Asymmetrical Digital Subscriber Loop	非对称数字用户环线
POTS	Plain Old Telephone Service	普通电话业务
ISDN	Integrated Services Digital Network	综合服务数字网
CO	Central office	中心局
CPE	Customer Premise Equipment	用户驻地设备
DMT	Discrete Multi-Tone	离散多频调制

3.2 可获得性

介绍该特性需要的硬件支持和 License 支持。

硬件支持

支持本特性的单板包括：ADRI、ADRB、CSRB 单板。

Modem 需要支持 ADSL2+协议。

License 支持

ADSL2+端口速率达标统计特性是 UA5000 的可选特性，只有获得 License 许可后才能获得该特性的服务。

ADSL/ADSL2+端口个数、ADSL2+ INP 端口资源和 ADSL2+ Annex M 端口资源均受 License 控制。

3.3 原理描述

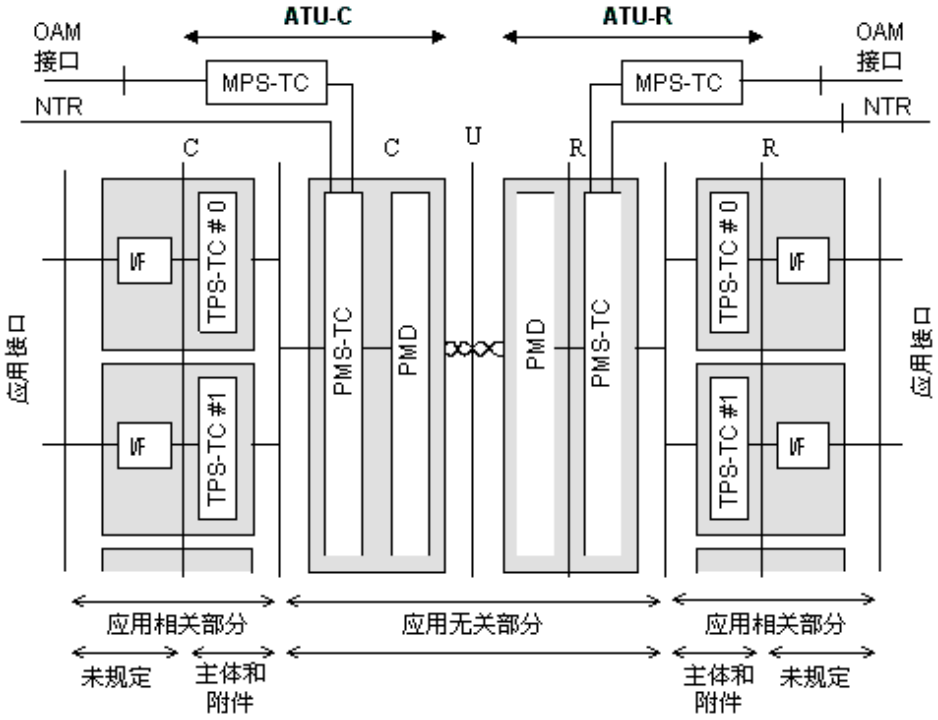
介绍该特性的实现原理。

ADSL 系统架构

ADSL2/2+ 将 ADSL 收发器按照功能分成 TPS-TC（传输协议相关的汇聚子层）， PMS-TC（物理媒质相关的汇聚子层）， PMD（物理媒质相关子层）以及 MPS-TC（管理协

议相关的汇聚子层，用于网管接口）。将每一个子层封装起来并定义了各子层之间的消息有助于不同厂家的设备之间实现互通。ADSL 的体系参考结构如图 3-1 所示。

图 3-1 ADSL 体系参考结构



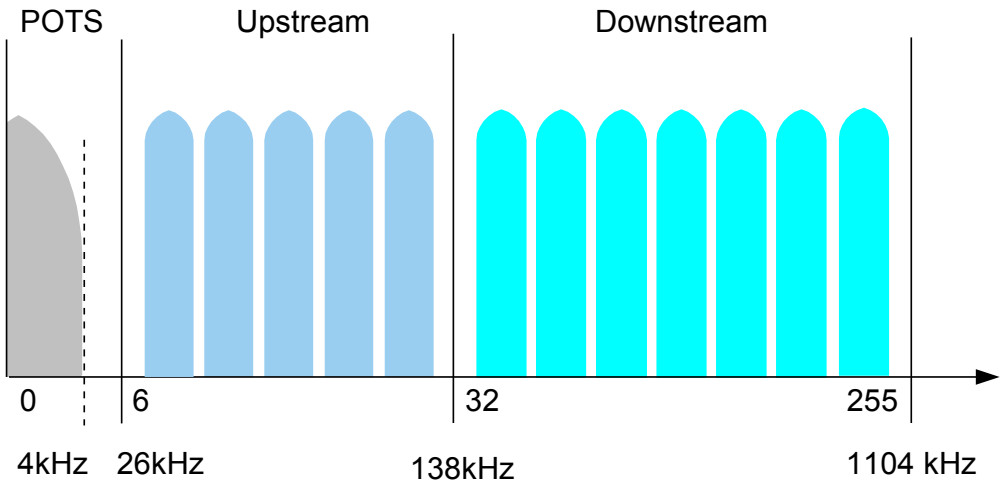
- TPS-TC
  - 与具体的应用相关，主要完成用户接口数据和控制信号到 TPS-TC 同步数据接口的适配。
  - TPS-TC 层也通过 PMS-TC 层开销通道发送和接收控制消息。
  - MPS-TC 功能模块提供了实施 ATU 管理的规程，MPS-TC 功能模块与管理平面的高层功能实体进行通信，管理信息通过 ADSL 开销通道（EOC）在 ATU 的 MPS-TC 功能实体间进行交换。
- PMS-TC
  - 主要完成 ADSL 开销与 TPS-TC 数据流的复用。
  - 基本功能包括成帧和帧同步、扰码和解扰及前向纠错和差错检测。
  - P 提供开销信道用于传送 TPS-TC、PMS-TC 和 PMD 层控制消息以及管理接口的消息。
- PMD
  - 基本功能包括码元定时生成和恢复、编码和解码、调制和解调、回波抵消、线路均衡及链路启动等。
  - PMD 层也通过 PMS-TC 层开销信道发送和接收控制消息。

ADSL 原理

ADSL 频谱带宽为 1.104MHz。ADSL 通过 DMT 技术将整个带宽分割成 256（0 ～ 255）个子信道。针对 ADSL over POTS 信号、ADSL over ISDN 信号的承载不同，ADSL 对 256 个子信道及带宽的划分也不相同。

ADSL over POTS 子信道及带宽划分如图 3-2 所示。

图 3-2 ADSL over POTS 子信道及带宽划分

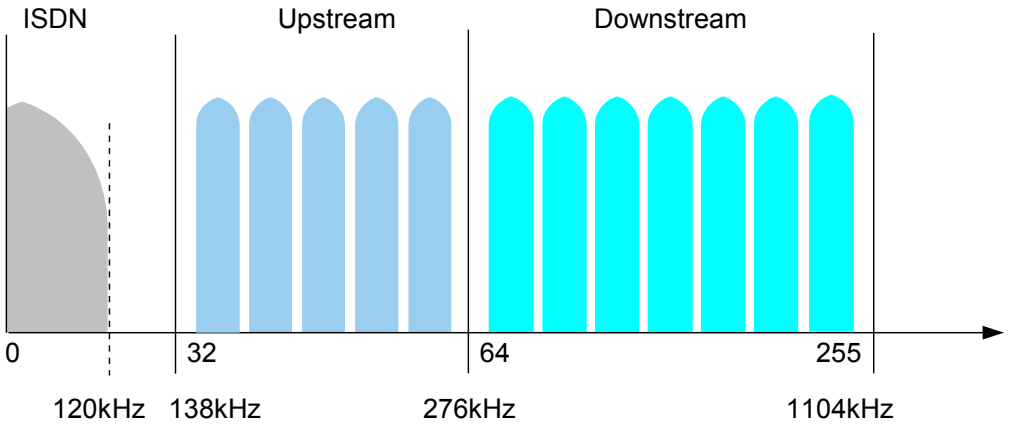


如上图所示：

- 0 ～ 5 子信道保留用于传输 4kHz 的模拟语音信号。
- 6 ～ 31 子信道用于传输上行数据，传输带宽为 26kHz ～ 138kHz。
- 32 ～ 255 子信道用于传输下行数据，传输带宽为 138kHz ～ 1104kHz。

ADSL over ISDN 子信道及带宽划分如图 3-3 所示。

图 3-3 ADSL over ISDN 子信道及带宽划分



如上图所示：

- 0 ～ 31 子信道保留用于传输 120kHz 的 ISDN 信号。
- 32 ～ 63 子信道用于传输上行数据，传输带宽为 138 kHz ～ 276kHz。
- 64 ～ 255 子信道用于传输下行数据，传输带宽为 276 kHz ～ 1104kHz。

说明

每个子信道占用的传输带宽为 4.3125KHz。

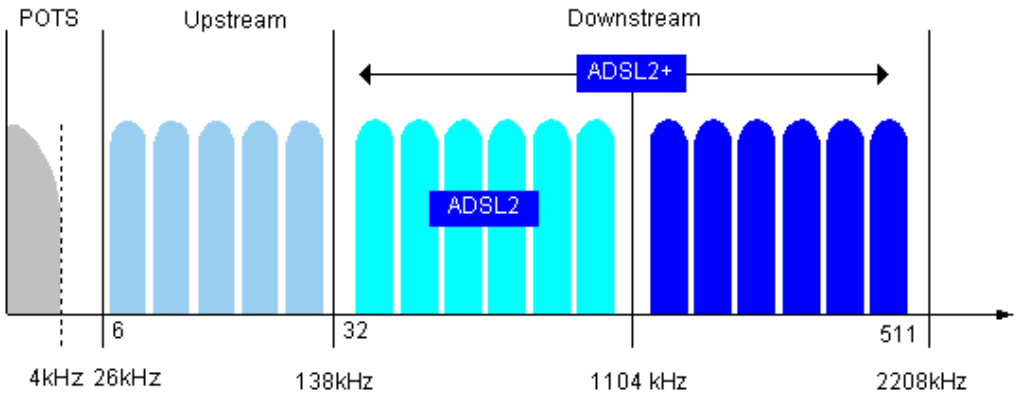
当 ATU 采用回波抵消技术时，ADSL 信号可以采用 overlapped 方式传输，即将下行传输带宽扩展到上行传输带宽上，使下行 ADSL 信号可以与下行 ADSL 信号共享传输通道。

ADSL 每个子信道可以传送 1bit ～ 15bit 的数据（即每个子载波调制的 bit 位数）。子信道上实际的传输容量由该子信道当前的传输性能（衰减特性、时延特性和噪声特性）决定。

ADSL2+原理

ADSL2+将 ADSL 的频谱带宽扩展到 2.208MHz，并采用 DMT 技术将整个带宽分割成 512（0 ～ 511）个子信道。ADSL2+子通道及带宽划分如图 3-4 所示。

图 3-4 ADSL2+子通道及带宽划分



如上图所示：

- 0 ～ 5 子载波保留用于传输 4kHz 的模拟语音信号。
- 6 ～ 31 子载波用于传输上行数据，传输带宽为 26 kHz ～ 138kHz。
- 32 ～ 511 子载波用于传输下行数据，传输带宽为 138 kHz ～ 2208kHz。

在 ADSL 技术的基础上，ADSL2+除了采用扩展传输带宽的方式外，还通过提高调制效率、减少开销、优化帧结构等方式，进一步提高数据的传输效率。

3.4 参考信息

介绍该特性相关的参考信息。

本特性的参考资料清单如下：

- ITU-T Recommendation G992.5：Asymmetric Digital Subscriber Line (ADSL) transceivers – Extended bandwidth ADSL2 (ADSL2+)
- G992.1 Asymmetric digital subscriber line (ADSL) transceivers
- G992.3 Asymmetric digital subscriber line transceivers 2 (ADSL2)

4 VDSL2 接入

关于本章

介绍 VDSL2 接入特性的定义、目的、规格、原理以及参考的术语、缩略语和相关协议标准。

4.1 介绍
介绍该特性的定义、目的、规格和约束条件。

4.2 可获得性
介绍该特性需要的硬件支持和 License 支持。

4.3 原理描述
介绍该特性的实现原理。

4.4 参考信息
介绍该特性相关的参考信息。

4.1 介绍

介绍该特性的定义、目的、规格和约束条件。

定义

VDSL2（Very High Speed Digital Subscriber Lines 2）是 VDSL 的扩展，是在普通双绞线上为用户提供对称或非对称的高速专线接入业务。

目的

VDSL2 拥有最高达 200Mbit/s 对称速率的高带宽，支持多种频谱模板、多种封装形式，为新一代 FTTx 接入场景提供短距离、高速率的接入解决方案。

规格

- 符合 ITU G.993.2 标准。
- 支持 VDSL2(G993.2)的 Annex A。
- 支持最长达 3.5km 的传输距离。
- 支持 VDSL2/ADSL2+兼容的单板方案，并且支持 POTS（Plain Old Telephone Service）和 ISDN（Integrated Services Digital Network）的 VDSL2 单板，以满足不同业务需求。
- 支持多种频谱模板的配置，包括 8a、8b、8c、8d、12a、12b、17a，满足不同的应用场景需求。
- 支持功率谱密度控制功能，通过 UPBO/DPBO、RFI、PSD Mask、Tone Blackout 等技术完成功率谱的管理。
- 支持 ATM 和 PTM 两种封装模式，并且在接入 ADSL/ADSL2+的终端时，能够工作在 ADSL/ADSL2+模式下。
- 支持 VDSL2 线路、信道模板参数的配置、修改和查询。
- 支持激活、去激活、环回 VDSL2 端口。支持复位 VDSL2 套片。
- 支持 INP（Impulse Noise Protection）、动态速率调整即 SRA（Seamless Rate Adaptation）和 DRR（Dynamic Rate Repartitioning）。
- 支持 VDSL2 的 BitSwap、NTR 时钟功能和虚拟噪音。
- 支持线路、信道告警维护信息上报功能。
- 支持 BandPlan998，BandPlan997。
- 支持 16 端口的 VDSL2 单板。

术语

表 4-1 VDSL2 接入特性术语表

术语	解释
UPBO/DPBO	PBO（Power back off）是指功率反馈控制，即 VTU 可以调整自己的输出 PSD，使其能够达到传输要求而不使得发送功率过大。VDSL2 要求同时支持上行 PBO（UPBO）和下行（DPBO），而 ADSL 只支持下行 PBO。
RFI	RFI 指的是无线频率干扰问题。VDSL2 技术使用的频率范围比较宽，高端达 30MHz，其整个频谱覆盖了中波、短波广播及业余无线电的频谱。因此 VDSL2 技术必须解决 RFI 问题。
PSD Mask	PSD Mask 是对传输信号的功率谱密度的约束。PSD Mask 是通过断点来设置的，VDSL2 中规定下行频段断点为 32 个，上行频段断点为 16 个。

缩略语

表 4-2 VDSL2 接入特性缩略语表

缩略语	英文全称	中文全称
VDSL2	Very High Speed Digital Subscriber Lines 2	甚高比特率数字用户线 2
FTTx	Fiber To The x	光纤到户/大楼等
ATM	Asynchronous Transfer Mode	异步转移模式
PTM	Packet Transfer Mode	分组传输模式
DMT	Discrete Multi-Tone	离散多频音线路编码技术/离散多频调制
RFI	Radio Frequency Interference	无线频率干扰
PBO	Power Back Off	功率反馈控制

4.2 可获得性

介绍该特性需要的硬件支持和 License 支持。

硬件支持

- 支持 8a，8b，8c，8d，12a，12b 和 17a 频谱模板的 VDSL2 单板是 VDMB。
- H605VDMB 支持 VDSL2。
- Modem 需要支持 VDSL2 协议。

License 支持

UA5000 中 VDSL2 的激活端口数和 A/V 自适应功能受 License 控制，需要授权才能使用。

4.3 原理描述

介绍该特性的实现原理。

VDSL2 兼容性

VDSL2 实现原理基于 G993.2 标准。

ITU（International Telecommunications Union）定义了 VDSL2 采用 DMT 调制方式，VDSL2 技术着眼于与 ADSL、ADSL2、ADSL2+的兼容，由于 VDSL 没有被广泛应用，因此 VDSL2 与 VDSL 不兼容。

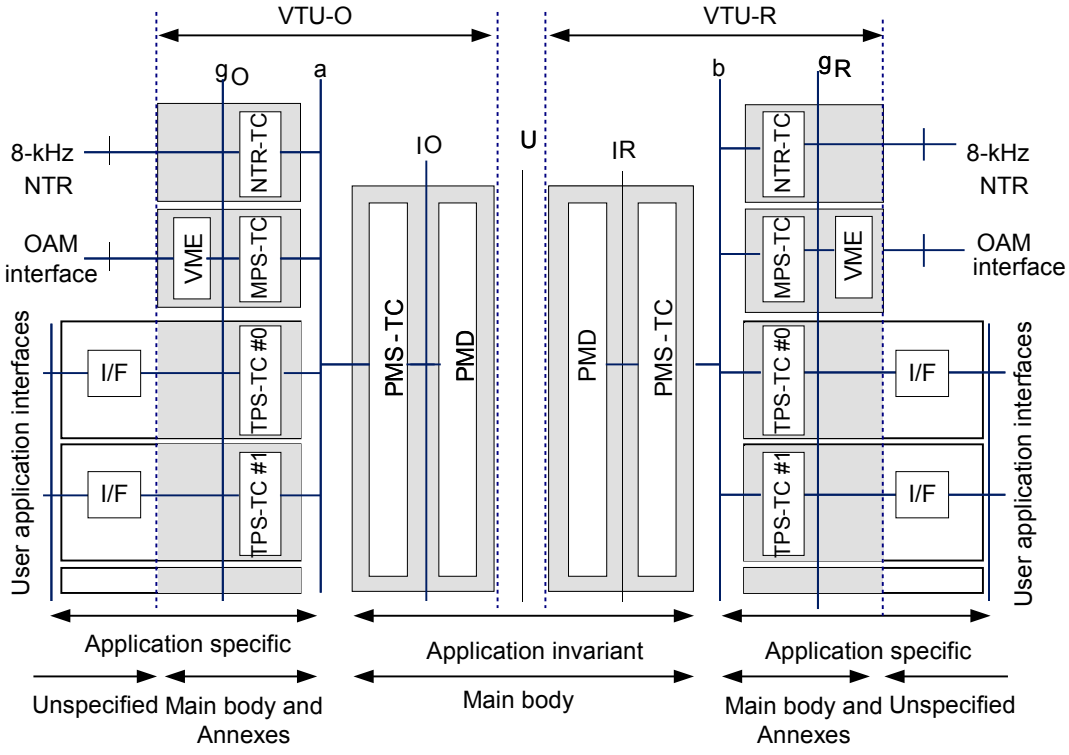
VDSL2 系统架构

VDSL2 的系统架构与 ADSL 比较类似，支持 3 种独立的应用模型：

- 纯数据业务模型
- 数据业务承载 POTS 业务模型
- 数据业务承载 ISDN 业务模型

VDSL2 传输系统结构如图 4-1 所示。

图 4-1 VDSL2 传输体系结构



一个 VDSL2 线路接口主要由 TPS-TC、PMS-TS 和 PMD 三部分组成。

- TPS-TC
  - 与具体的应用相关，主要完成用户接口数据和控制信号到 TPS-TC 同步数据接口的适配。
  - TPS-TC 层也通过 PMS-TC 层开销通道发送和接收控制消息。
  - MPS-TC 功能模块提供了实施 VTU 管理的规程，MPS-TC 功能模块与管理平面的高层功能实体进行通信，管理信息通过 VDSL 开销通道在 VTU 的 MPS-TC 功能实体间进行交换。
- PMS-TC
  - 主要完成 VDSL 开销通道与 TPS-TC 数据流的复用。
  - 基本功能包括成帧和帧同步、扰码和解扰及前向纠错和差错检测。
  - P 提供开销信道用于传送 TPS-TC、PMS-TC 和 PMD 层控制消息以及管理接口的消息。
- PMD
  - 基本功能包括码元定时生成和恢复、编码和解码、调制和解调、回波抵消、线路均衡及链路启动等。
  - PMD 层也通过 PMS-TC 层开销信道发送和接收控制消息。

UA5000 提供的 VDSL2 单板完全按照 G993.2 标准实现的上述功能模块。此外，UA5000 按照 G997.1 标准和 TR090 标准实现了 VDSL2 管理模块，提供了基于线路、信道、频谱模板配置的线路管理功能，满足用户不同的需求。

4.4 参考信息

介绍该特性相关的参考信息。

本特性的参考资料清单如下：

- ITU-T G.993.1：Very high speed digital subscriber line transceivers
- ITU-T G.993.2：Very high speed digital subscriber line 2

5 SHDSL 接入

关于本章

SHDSL 可以在普通双绞线上为用户提供对称的高速专线接入业务，可以满足中小企业、SOHO 用户的宽带上网需求。

5.1 ATM SHDSL 接入
介绍 ATM SHDSL 接入特性的定义、目的、规格、原理以及参考的术语、缩略语和相关协议标准。

5.2 EFM SHDSL 接入
介绍 EFM SHDSL 接入特性的定义、目的、规格、原理以及参考的术语、缩略语和相关协议标准。

5.3 TDM SHDSL 接入
介绍 TDM SHDSL 特性的定义、目的、规格、原理以及参考的术语、缩略语和相关协议标准。

5.1 ATM SHDSL 接入

介绍 ATM SHDSL 接入特性的定义、目的、规格、原理以及参考的术语、缩略语和相关协议标准。

5.1.1 介绍

介绍该特性的定义、目的、规格和约束条件。

定义

SHDSL 是对应 ADSL、VDSL 出现的另一种 xDSL 接入技术，可以提供对称的上下行速率。

ATM SHDSL 上下行速率对称的特点决定其支持的业务双向速率基本一致，传输距离相比 ADSL 更远，应用非常广泛。

目的

ATM SHDSL 提供对称宽带用户接入，可以满足 SOHO 用户对高下行速率的要求，与 ADSL 的应用类似，二者互为补充。

规格

- 支持 2 线和 4 线、8 线 SHDSL。线路速率在 2 线模式为 192Kbit/s ～ 2312Kbit/s，4 线模式的速率为 2 线模式的 2 倍。速率调节粒度为 16Kbit/s。
- 支持 NTR 时钟功能。
- 在初始化时根据线路情况自动调整速率。
- 支持线路告警维护信息上报功能。

术语

无。

缩略语

表 5-1 ATM SHDSL 接入特性缩略语表

缩略语	英文全称	中文全称
SHDSL	Single-line high speed digital subscriber line	单线对高速数字用户线
HDSL	High-speed digital subscriber line	高速数字用户线
TC-PAM	Trellis Coded Pulse Amplitude Modulation	格栅编码脉冲幅度调制
ATM	Asynchronous Transfer Mode	异步传输模式

5.1.2 可获得性

介绍该特性需要的硬件支持和 License 支持。

硬件支持

- 支持本特性的单板是 SHLB。
- Modem 需要支持 ATM SHDSL 协议。如果需要支持多线对模式，终端也要支持相同端口的多线对模式。

License 支持

- UA5000 中 ATM SHDSL 端口资源受 license 控制。
- 使用 G.SHDSL.bis 模板激活或批量激活 SHDSL 端口，需要申请 License 授权。
- 绑定 SHDSL 端口需要申请 License 授权。系统对绑定的端口数进行 License 控制，即绑定几个端口就需要申请几个 License。

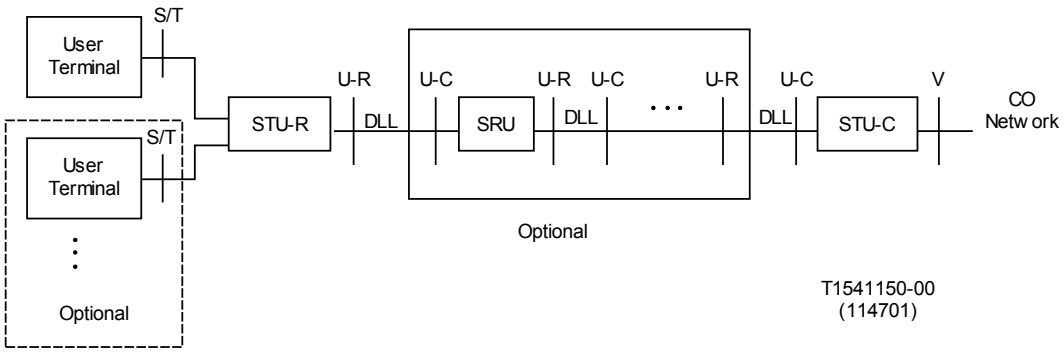
5.1.3 原理描述

介绍该特性的实现原理。

典型应用模型

SHDSL 实现原理基于 G.991.2（2001）标准。

图 5-1 SHDSL 典型应用模型



一个 SHDSL 系统由一个 STU-C、一个 STU-R 和用户终端组成，在 STU-C 和 STU-R 之间的连接可以加入几个中继器。

- STU-C 提供局端业务接口。
- STU-R 端提供用户接口，STU-R 端可以接多个用户终端。
- SRU 即中继器，应用于超长距离传输时，把信号恢复续传，增长传输距离。

UA5000 不支持中继器的使用。

终端模型

SHDSL 终端模型包括以下部分：

- PDM 模块
  - 完成码元定时生成和恢复，编码和解码，调制和解调，回波抵消，线性均衡和链路启动等功能。
  - SHDSL 主要运用了 TC-PAM（Trellis Coded Pulse Amplitude Modulation 格栅编码脉冲幅度调制）编码技术。
- PMS-TC 模块

  完成定帧和帧同步，加扰码和解扰码功能。
- TPS-TC 模块

  完成数据帧映射和封装，复用、解复用和多用户数据信道定时校准等功能。
- 局端设备的 I/F 接口
  - 主要提供 ATM 接口。
  - 对于 ATM 接口直接通过 ATM 网络进行传输或根据承载的报文通过 SAR 模块完成以太网报文组装或 E1/V.35 报文的组装，并通过以太网进行传输。
- 用户端设备的 I/F 接口

  同局端相对应，而对外一般提供以太网口或 E1/V.35 接口。

UA5000 的 SHLB 单板基于 ATM 方式，用户端支持以太网口输出（宽带接入）或 E1/V.35 接口输出（专线接入），上行方向接入到城域网。

帧数据速率

在 UA5000 中采用的帧数据速率如下。

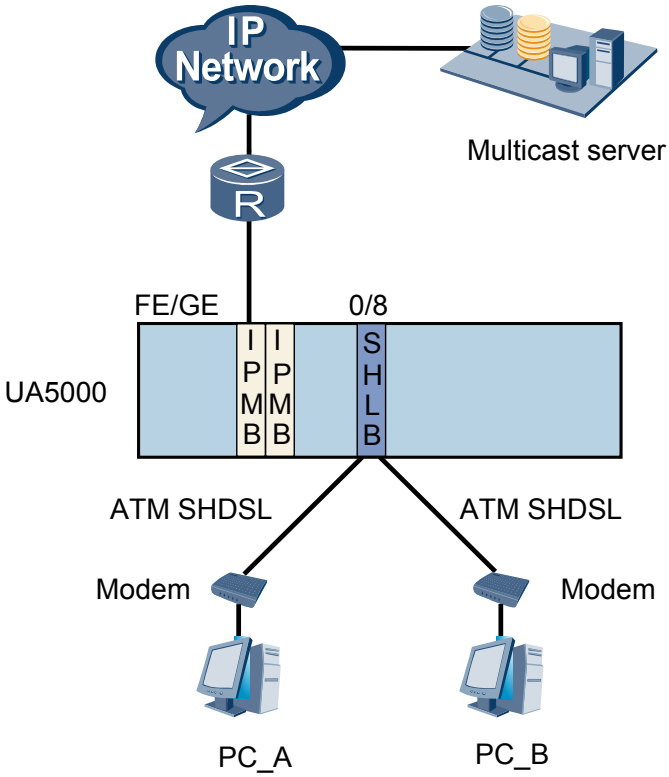
表 5-2 帧数据速率

对应的单板	净荷数据速率	调制模式
SHLB	$R=n\times 64+(i)\times 8$，$3\leqslant n\leqslant 36$ 且 $0\leqslant i\leqslant 7$（192Kbit/s ～ 2312Kbit/s）	16-TCPAM
	$R=n\times 64+(i)\times 8$，$12\leqslant n\leqslant 89$ 且 $0\leqslant i\leqslant 7$（768Kbit/s ～ 5696Kbit/s）	32-TCPAM

典型应用组网

ATM SHDSL 的典型应用组网如下图所示。

图 5-2 ATM SHDSL 应用组网



5.1.4 参考信息

介绍与该特性相关的参考信息。

本特性的参考资料清单如下：

- ITU-T Recommendation G.991.2 (2001), *Single-pair high-speed digital subscriber line (SHDSL) transceivers*

5.2 EFM SHDSL 接入

介绍 EFM SHDSL 接入特性的定义、目的、规格、原理以及参考的术语、缩略语和相关协议标准。

5.2.1 介绍

介绍该特性的定义、目的、规格和约束条件。

定义

SHDSL 是对应 ADSL、VDSL 出现的另一种 XDSL 接入技术，可以提供对称的上下行速率。

EFM（Ethernet in the first mile） SHDSL 结合了 SHDSL 技术和以太网技术的优点，在普通双绞线上即可同时提供传统话音业务及高速上网，并能满足用户高清晰电视和视频点播的要求，适合宽带到小区的“最后 1 英里”接入。

目的

对于 SHDSL 的接入业务，如果用户终端同时支持 ATM 和 EFM，则优先选择 EFM 接入业务，因为在同样的激活速率下，EFM 接入业务的使用率更高。

规格

- SHDSL 传输距离最大可达 6km。
- 支持 NTR 时钟功能。
- 支持以太网的接入。
- 在初始化时根据线路情况自动调整速率。
- 支持线路告警维护信息上报功能。
- 支持 1、2、3、4 线对（1、2、3、4 端口）四种方式的 EFM 类型端口绑定。
- 线路速率范围在单线对时为 192Kbit/s ～ 5696Kbit/s。
- 2、3、4 端口 EFM 绑定时的线路速率分别为单线对速率的 2、3、4 倍（因为 EFM 类型的端口绑定组允许对绑定组内对端口分别进行激活、去激活操作，所以具体应用时要根据 EFM 端口绑定组内激活端口的数量来确定绑定组的速率为单线对端口激活速率的多少倍）。

术语

无。

缩略语

表 5-3 EFM SHDSL 接入特性缩略语表

缩略语	英文全称	中文全称
EFM	Ethernet in the first mile	最后一公里以太网
SHDSL	Single-line high speed digital subscriber line	单线对高速数字用户线
HDSL	High-speed digital subscriber line	高速数字用户线

5.2.2 可获得性

介绍该特性需要的硬件支持，包括单板和终端。

- 支持本特性的单板是 SHLB。
- Modem 需要支持 EFM SHDSL 协议，并且支持 EFM 的端口绑定。

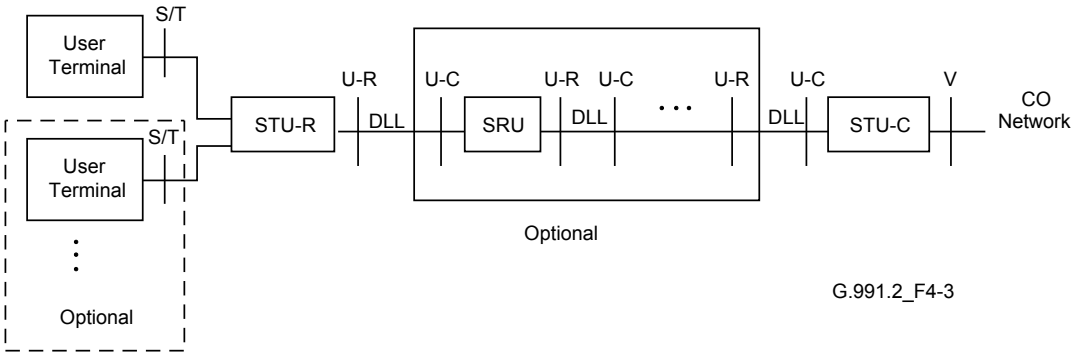
5.2.3 原理描述

介绍该特性的实现原理。

典型应用模型

SHDSL 实现原理基于 G.991.2（2003）标准。

图 5-3 SHDSL 典型应用模型



一个 SHDSL 系统由一个 STU-C、一个 STU-R 和用户终端组成，在 STU-C 和 STU-R 之间的连接可以加入几个中继器。

- STU-C 提供局端业务接口。
- STU-R 端提供用户接口，STU-R 端可以接多个用户终端。
- SRU 即中继器，应用于超长距离传输时，把信号恢复续传，增长传输距离。

UA5000 不支持中继器的使用。

终端模型

SHDSL 终端模型包括以下部分：

- PDM 模块
  - 完成码元定时生成和恢复，编码和解码，调制和解调，回波抵消，线性均衡和链路启动等功能。
  - SHDSL 主要运用了 TC-PAM（Trellis Coded Pulse Amplitude Modulation 格栅编码脉冲幅度调制）编码技术。
- PMS-TC 模块

  完成定帧和帧同步，加扰码和解扰码功能。
- TPS-TC 模块

  完成数据帧映射和封装，复用、解复用和多用户数据信道定时校准等功能。
- 局端设备的 I/F 接口
  - 主要提供 ATM 接口或电路接口。
  - 对于 ATM 接口直接通过 ATM 网络进行传输或根据承载的报文通过 SAR 模块完成以太网报文组装或 E1/V.35 报文的组装，并通过以太网或 E1 链路进行传输。
  - 对于电路接口，直接通过 TDM 网络进行 E1/V.35 的传输。
- 用户端设备的 I/F 接口

  同局端相对应，而对外一般提供以太网口（ATM 信元通过 SAR）或 E1/V.35 接口。

帧数据速率

在 UA5000 中采用的帧数据速率如下。

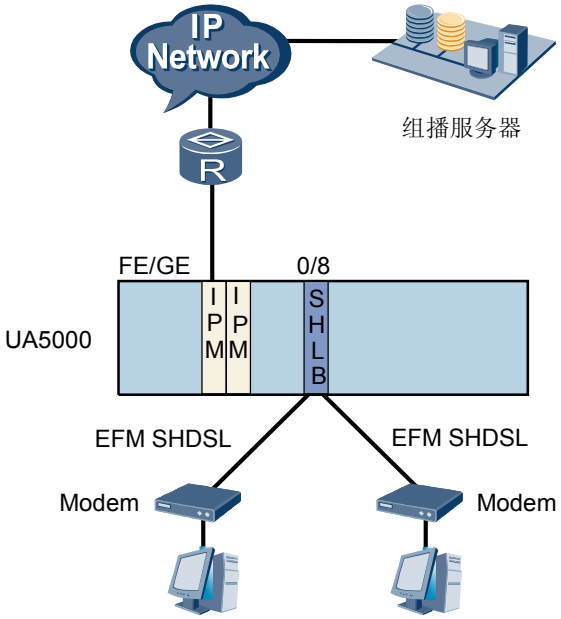
表 5-4 帧数据速率

对应的单板	净荷数据速率	调制模式
SHLB	$R=n'64+(i)'8$，$3 \leqslant n \leqslant 36$ 且 $0 \leqslant i \leqslant 7$（192Kbit/s ～ 2312Kbit/s）	16-TCPAM
	$R=n'64+(i)'8$，$12 \leqslant n \leqslant 89$ 且 $0 \leqslant i \leqslant 7$（768Kbit/s ～ 5696Kbit/s）	32-TCPAM

典型应用组网

EFM SHDSL 的典型应用组网如下图所示。

图 5-4 EFM SHDSL 应用组网



5.2.4 参考信息

介绍与该特性相关的参考信息。

本特性的参考资料清单如下：

- ITU-T Recommendation G.991.2 (2001), *Single-pair high-speed digital subscriber line (SHDSL) transceivers*

5.3 TDM SHDSL 接入

介绍 TDM SHDSL 特性的定义、目的、规格、原理以及参考的术语、缩略语和相关协议标准。

5.3.1 介绍

介绍该特性的定义、目的、规格和约束条件。

定义

SHDSL 是对应 ADSL、VDSL 出现的另一种 xDSL 接入技术，可以提供对称的上下行速率。

TDM SHDSL 最高可以达到 2Mbit/s，上下行速率对称的特点决定其支持的业务双向速率基本一致，传输距离更远，可以替代过去的 E1 线，用于高速的数据业务接入。

目的

增加 E1 及 V.35 的接入距离。

规格

SDLE 单板提供 8 路 SHDSL 和 8 路 E1。

约束

无。

术语

无。

缩略语

表 5-5 TDM SHDSL 特性缩略语表

缩略语	英文全称	中文全称
SHDSL	single-line high speed digital subscriber line	单线对高速数字用户线
TDM	Time Division Multiplexing	时分复用
PRA	Primary Rate Adaptation	基群速率适配

5.3.2 可获得性

介绍该特性需要的硬件支持，包括单板和终端。

支持本特性的单板是 SDLE。

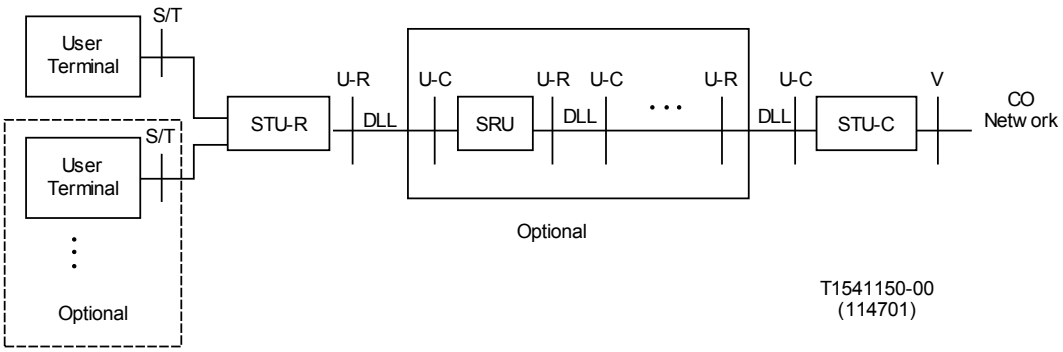
5.3.3 原理描述

介绍该特性的实现原理。

典型应用模型

SHDSL 实现原理基于 G.991.2（2001）标准。

图 5-5 SHDSL 典型应用模型



一个 SHDSL 系统由一个 STU-C、一个 STU-R 和用户终端组成，在 STU-C 和 STU-R 之间的连接可以加入几个中继器。

- STU-C 提供局端业务接口。
- STU-R 端提供用户接口，STU-R 端可以接多个用户终端。
- SRU 即中继器，应用于超长距离传输时，把信号恢复续传，达到增长传输距离的目的。

UA5000 不支持中继器的使用。

终端模型

SHDSL 终端模型包括以下部分：

- PDM 模块
  - 完成码元定时生成和恢复，编码和解码，调制和解调，回波抵消，线性均衡和链路启动等功能。
  - SHDSL 主要运用了 TC-PAM（Trellis Coded Pulse Amplitude Modulation 格栅编码脉冲幅度调制）编码技术。
- PMS-TC 模块

  完成定帧和帧同步，加扰码和解扰码功能.
- TPS-TC 模块

  完成数据帧映射和封装，复用、解复用和多用户数据信道定时校准等功能。
- 局端设备的 I/F 接口
  - 主要提供电路接口。
  - 直接通过 TDM 网络进行 E1/V.35 的传输。

- 用户端设备的 I/F 接口

  同局端相对应，对外一般提供 E1/V.35 接口。

工作模式

SDLE 支持两种工作模式：普通模式和传输模式。

- 普通模式

  各个 G.SHDSL 端口和 E1 端口都是孤立的端口，可以进行半永久配置，以及速率、端口模式的配置。

- 传输模式

  单板自动将第 x 路 G.SHDSL 与第 x 路 E1 直接对接，实现 2M 数据透传。E1 端口为无帧格式，G.SHDSL 为 V.35 模式，时钟锁第 x 路的 E1 线路时钟，因此，每一路都有自己的独立时钟。在传输模式下，不能配置半永久业务。

表 5-6 工作模式与业务类型关系表

工作模式	业务类型
普通模式	半永久、框间链接。
传输模式	与远端工作在 MODEM 工作模式下的 SDLE 单板联合进行级联组网。
业务模式	半永久、框间链接、PRA 业务。

典型应用组网

TDM SHDSL 的典型应用组网如下图所示，图 5-6 表示工作在传输模式下的级联组网。图 5-7 表示工作在业务模式下的 ISDN PRA 业务组网。

图 5-6 SHDSL 远端级联组网

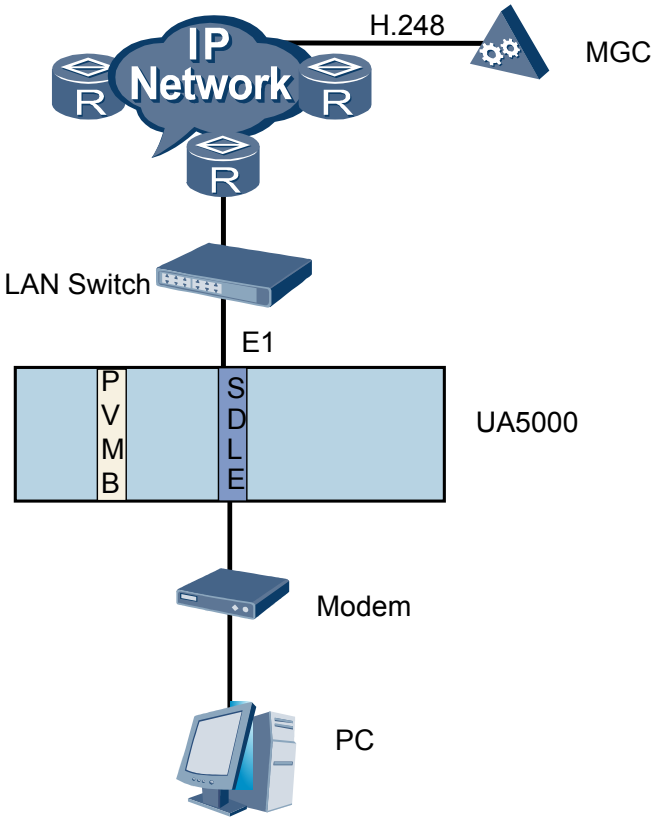
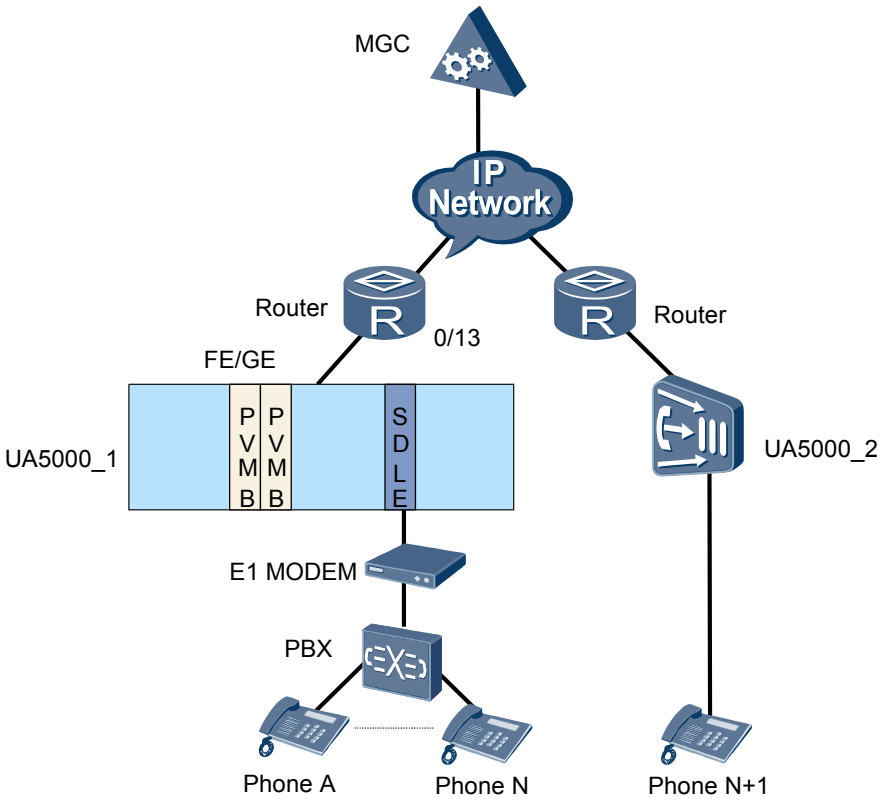


图 5-7 ISDN PRA 业务组网图



5.3.4 参考信息

介绍与该特性相关的参考信息。

本特性的参考资料清单如下：

- GPP TS 25.101，“User Equipment (UE) radio transmission and reception (FDD), V5.8.0”.

6 PPPoA 接入

关于本章

介绍 PPPoA 接入特性的定义、目的、规格、原理以及参考的术语、缩略语和相关协议标准。

6.1 介绍
介绍该特性的定义、目的、规格、术语和缩略语。

6.2 可获得性
介绍该特性需要的硬件支持和 License 支持。

6.3 原理描述
介绍该特性的实现原理。

6.4 参考信息
介绍与该特性相关的维护信息。

6.1 介绍

介绍该特性的定义、目的、规格、术语和缩略语。

定义

PPPoA（PPP over ATM）接入特性是指设备支持用户以 PPPoA 方式接入，上行到基于 Ethernet 的 PPPoE 服务器（BRAS）。

设备需要对用户的 PPPoA 报文和服务器的 PPPoE 报文进行处理，实现 PPPoA 到 PPPoE 的互通功能（IWF，Interworking Function）。

目的

设备支持 PPPoA 接入方式，可以实现 PPPoA 到 PPPoE 的互通功能，满足 ATM 网络到 IP 网络的过渡需求。

规格

- 支持 PPP LLC 封装和 PPP VC-MUX 封装，支持两者的自适应。
- 支持 PPP MRU≥1492。
- 支持最多 1024 个 PPPoA 用户。
- 支持单 MAC 地址模式和多 MAC 地址模式。

术语

无。

缩略语

表 6-1 PPPoA 接入特性缩略语表

缩略语	英文全称	中文全称
PPPoA	Point to Point Protocol over ATM	基于 ATM 的 PPP 协议
PPPoE	Point-to-Point Protocol over Ethernet	基于以太网封装的 PPP 协议
IWF	Interworking Function	互相传输数据的功能

6.2 可获得性

介绍该特性需要的硬件支持和 License 支持。

硬件支持

支持本特性的单板是所有 ATM 方式接入的业务单板。

License 支持

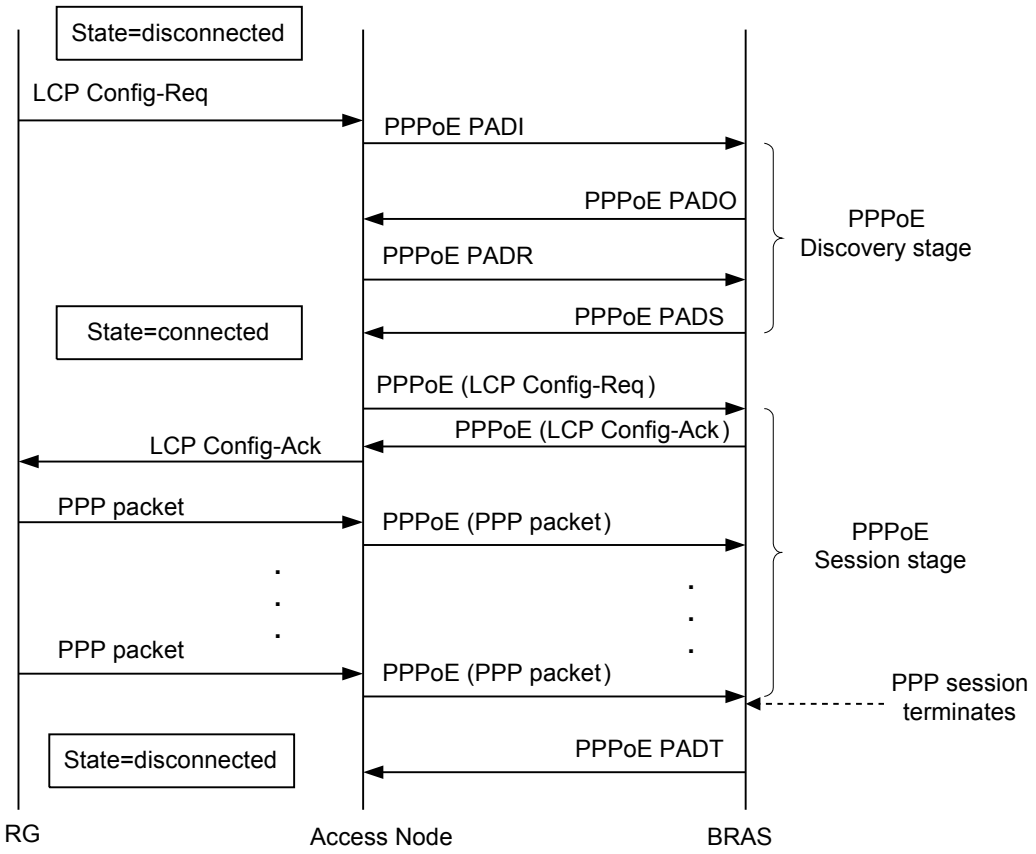
UA5000 可以支持的 PPPoA 转 PPPoE 的用户数目受 License 控制。

6.3 原理描述

介绍该特性的实现原理。

PPPoA 接入业务处理流程如图 6-1 所示。

图 6-1 PPPoA 转 PPPoE 报文处理流程图



其处理过程是：

1. 收到 PPPoA 用户的 LCP Configure Request 报文后，UA5000 将该报文缓存起来，发起一个 PPPoE Session：以广播方式发送 PADI 报文，报文的源 MAC 地址为 UA5000 为 PPPoA 用户分配的 MAC 地址。
2. BRAS 向 UA5000 发送 PADO 报文。
3. UA5000 获得 BRAS 的 MAC 地址，向 BRAS 发送 PADR 报文。
4. BRAS 向 UA5000 发送 PADS 报文。
5. UA5000 获取 SessionID 后，将缓存的 LCP Configure Request 报文发往 BRAS，进入 PPPoE 会话阶段。

6. 用户发送 PPP 数据包，UA5000 根据 BRAS MAC 地址和 UA5000 为用户分配的 MAC 地址，封装 PPPoE 数据包，发往 BRAS；下行报文，UA5000 进行相反的处理。
7. BRAS 发送 PADT 报文，或者 PPPoA 用户发送 LCP Configure Terminate 报文，终结会话。

6.4 参考信息

介绍与该特性相关的维护信息。

本特性的参考资料清单如下：

- IETF RFC2364: PPP Over AAL5
- IETF RFC2516: A Method for Transmitting PPP Over Ethernet (PPPoE)
- DSL Froum TR-101: Migration to Ethernet-Based DSL Aggregation

7 IPoA 接入

关于本章

介绍 IPoA 接入特性的定义、目的、规格、原理以及参考的术语、缩略语和相关协议标准。

7.1 介绍
介绍该特性的定义、目的、规格、术语和缩略语。

7.2 可获得性
介绍该特性需要的硬件支持，包括单板和终端。

7.3 原理描述
介绍该特性的实现原理。

7.4 参考信息
介绍与该特性相关的参考信息。

7.1 介绍

介绍该特性的定义、目的、规格、术语和缩略语。

定义

分析 IPoA 协议报文，将 IP 报文净荷承载在相应的以太网帧上行送入上层网络；同时将下行的 IPoE 报文转换成 IPoA 报文转发到用户。

目的

IPoA 常用于专线接入，满足运营商 ATM 网络到 IP 网络的过渡需求。

规格

- 符合 RFC2684，支持 IPoA 静态用户。
- 符合 RFC1577，支持 IPoA 动态用户。
- 最多支持 1024 个 IPoA 用户。
- 最多支持 15 个不同的用户网关。
- 支持 LLC-IP 封装的自动发现。
- 支持二层、三层 IPoA 应用。

术语

无。

缩略语

表 7-1 IPoA 接入特性缩略语表

缩略语	英文全称	中文全称
IPoA	Internet Protocol Over ATM	承载于 ATM 网的 IP 报文

7.2 可获得性

介绍该特性需要的硬件支持，包括单板和终端。

硬件支持

- ADSL2+，SHDSL，VDSL2 业务板支持 IPoA 接入业务。
- Modem 需要支持 RFC2684 或 RFC1577 协议。

License 支持

UA5000 可以支持的 IPoA 转 IPoE 的用户数目受 License 控制。

7.3 原理描述

介绍该特性的实现原理。

二层 IPoA

UA5000 工作在二层路由方式，用户的默认网关为上层设备对应的三层接口的 IP 地址；UA5000 完成 IPoA 到 IPoE 的转换，不需要三层路由功能；IPoA 的用户网关需要管理员配置，多个 IPoA 用户可以对应同一个网关。

三层 IPoA

UA5000 工作在三层路由方式，用户的默认网关为 UA5000 对应的三层接口的 IP 地址；UA5000 完成 IPoA 到 IPoE 的转换，然后根据目的 IP 路由转发；IPoA 的用户网关需要管理员配置，多个 IPoA 用户可以对应同一个网关。

静态/动态 IPoA 用户

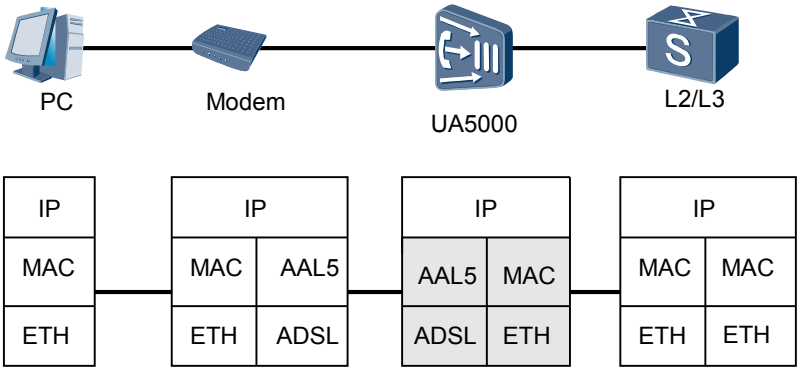
如果 Modem 只支持 IPoA-VCMUX 封装的 AAL5 帧，UA5000 无法获取 Modem 的接口 IP，需要 UA5000 设备管理员配置静态用户的源 IP 地址，UA5000 上配置的源 IP 地址即 xDSL 用户 Modem 的 IP 地址。

如果动态 IPoA 用户终端支持 RFC1577，UA5000 可以通过 ATM ARP 协议报文，获取 Modem 的 WAN 接口 IP 地址。

实现流程

UA5000 为每个 IPoA 用户分配一个源 MAC 地址，同时通过 ARP 协议获取用户网关对应的 MAC 地址，以此作为以太网帧的源 MAC 和目的 MAC 地址，实现 ATM 帧和以太网帧之间的转换，如图 7-1 所示。

图 7-1 IPoA 原理实现流程图



7.4 参考信息

介绍与该特性相关的参考信息。

本特性的参考资料清单如下：

- RFC2684 : Multiprotocol Encapsulation over ATM Adaptation Layer 5
- RFC1577 : Classical IP and ARP over ATM

8 VLAN

关于本章

介绍 VLAN 的定义、目的、规格、原理以及参考的术语、缩略语和相关协议标准。

8.1 Standard VLAN
介绍 Standard VLAN 基本特性以及在 UA5000 上的实现原理。

8.2 Smart VLAN
介绍 Smart VLAN 基本特性以及在 UA5000 上的实现原理。

8.3 MUX VLAN
介绍 MUX VLAN 基本特性以及在 UA5000 上的实现原理。

8.4 QinQ VLAN
介绍 QinQ VLAN 基本特性以及在 UA5000 上的实现原理。

8.5 VLAN Stacking
介绍 VLAN Stacking 基本特性以及在 UA5000 上的实现原理。

8.6 Super VLAN
介绍 Super VLAN 基本特性以及在 UA5000 上的实现原理。

8.1 Standard VLAN

介绍 Standard VLAN 基本特性以及在 UA5000 上的实现原理。

8.1.1 介绍

介绍该特性的定义、目的、规格和约束条件。

定义

VLAN（Virtual Local Area Network）即虚拟局域网，是指在交换局域网的基础上，采用网络管理软件构建的可跨越不同网段、不同网络的端到端的逻辑而非物理的网络。一个 VLAN 组成一个逻辑子网，即一个逻辑广播域，可以覆盖多个网络设备。IEEE 于 1999 年颁布了用于标准化 VLAN 实现方案的 IEEE 802.1Q 协议标准。

Standard VLAN 中的各个端口是互通的标准以太网口，在逻辑上是对等的。

目的

相同 Standard VLAN 内的以太网端口可相互通信，不同 Standard VLAN 间的以太网端口相互隔离。

Standard VLAN 的典型应用是作为上行端口或级联端口的 VLAN。

规格

- 系统最多支持 4000 个 Standard VLAN。
- VLAN ID 范围为 1 ～ 4093，系统缺省 VLAN 的 ID 为 1。

约束

UA5000 Standard VLAN 的端口包括 IPM 主控板的标准以太网端口。

术语

无。

缩略语

表 8-1 Standard VLAN 特性缩略语表

缩略语	英文全称	中文全称
VLAN	Virtual Local Area Network	虚拟局域网
CFI	Canonical Format Indicator	规范格式标识符
FDDI	Fiber Distributed Digital Interface	光纤分布式数字接口

8.1.2 可获得性

介绍该特性需要的硬件支持，包括单板和终端。

无需额外硬件支持。

8.1.3 原理描述

介绍该特性的实现原理。

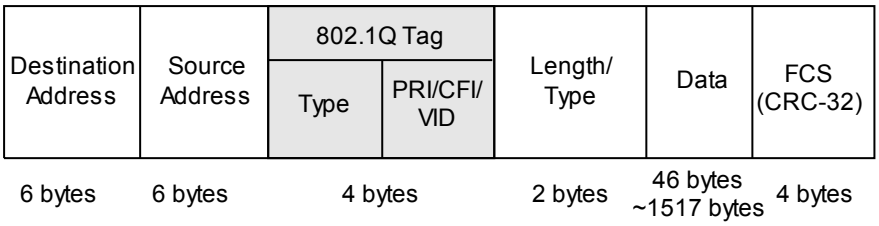
VLAN 的划分方法有很多，可以：

- 基于端口
- 基于 MAC 地址
- 基于协议类型
- 基于 IP 地址映射
- 基于组播
- 基于策略

目前业界通用的划分方法是基于端口的 VLAN，本文档中的 VLAN，如果没有特别说明，都是指基于端口的 VLAN。

Standard VLAN 是严格符合 802.1Q 标准的 VLAN，IEEE 802.1Q 标准对 Ethernet 帧格式进行了修改，在源 MAC 地址字段和协议类型字段之间加入 4 字节的 802.1Q Tag，如图 8-1 所示。

图 8-1 基于 802.1Q 的 VLAN 帧格式



802.1Q Tag 包含 4 个字节，其含义如下:

- Type：长度为 2 字节，表示帧类型。取值为 0x8100 时表示 802.1Q Tag 帧。如果不支持 802.1Q 的设备收到这样的帧，会将其丢弃。
- PRI：长度为 3 比特，表示帧的优先级，取值范围为 0 ～ 7，用于 QoS。0 表示优先级最低，0 ～ 7 优先级依次升高，7 表示优先级最高。
- CFI：Canonical Format Indicator，长度为 1 比特，表示 MAC 地址是否是经典格式，主要用于总线型的以太网与令牌环网和 FDDI（Fiber Distributed Digital Interface）交换数据时的帧格式。
- VID：VLAN ID，长度为 12 比特，表示该帧所属的 VLAN。

8.1.4 参考信息

介绍与该特性相关的参考信息。

本特性的参考资料清单如下：

- IEEE 802.1q：IEEE standards for Local and metropolitan area networks-Virtual Bridged Local Area Networks

8.2 Smart VLAN

介绍 Smart VLAN 基本特性以及在 UA5000 上的实现原理。

8.2.1 介绍

介绍该特性的定义、目的、规格和约束条件。

定义

Smart VLAN 是一种包含上行端口和业务虚端口的 VLAN。一个 Smart VLAN 可以包含多个上行端口和多个业务虚端口，业务虚端口相互隔离。

目的

一个 Smart VLAN 可接入多个 xDSL 用户，减少对系统 VLAN 数量的占用。

规格

UA5000 支持最多 4000 个 Smart VLAN，每个 Smart VLAN 中上行端口的数目没有限制，业务虚端口最多为 4095 个。

约束

如果已经创建 VLAN 三层接口，在删除 VLAN 之前，必须先删除已创建的 VLAN 三层接口。如果已经创建业务虚端口，在删除 VLAN 之前，必须先删除已创建的业务虚端口。

UA5000 支持三层功能以后，Smart VLAN 下的用户需要通过 ARP Proxy 实现互通。

术语

无。

缩略语

表 8-2 Smart VLAN 特性缩略语表

缩略语	英文全称	中文全称
xDSL	x Digital Subscriber Line	各类数字用户线

8.2.2 可获得性

介绍该特性需要的硬件支持，包括单板和终端。

无需额外硬件支持。

8.2.3 原理描述

介绍该特性的实现原理。

Smart VLAN 是一种特殊的 VLAN，除了具备 Standard VLAN 所有的特点之外，还具有以下独有特点：

- Smart VLAN 中端口的地位是不对等的，端口分为两种：上行端口和业务虚端口。业务虚端口之间相互隔离不能直接互通，上行口之间可以直接互通，业务虚端口与上行口之间可以直接互通。
- Smart VLAN 的上行口的广播域遍及 VLAN 的所有端口，但是业务虚端口的广播域只包含上行口。相比之下 Standard VLAN 的每个端口的广播域都包含该 VLAN 的所有端口。

8.2.4 参考信息

介绍与该特性相关的参考信息。

本特性的参考资料清单如下：

- IEEE 802.1q：IEEE standards for Local and metropolitan area networks-Virtual Bridged Local Area Networks

8.3 MUX VLAN

介绍 MUX VLAN 基本特性以及在 UA5000 上的实现原理。

8.3.1 介绍

介绍该特性的定义、目的、规格和约束条件。

定义

MUX VLAN 是一种包含上行端口和业务虚端口的 VLAN。一个 MUX VLAN 可包含多个上行端口，但只包含一个业务虚端口。不同 MUX VLAN 间的业务流相互隔离。

目的

MUX VLAN 与接入用户存在一对一的映射关系，因此可根据 VLAN 区分不同的接入用户。例如，当需要用 VLAN 区分用户时，可以使用 MUX VLAN。

规格

UA5000 最多支持 4000 个 MUX VLAN。

约束

- 如果 VLAN 已经创建 VLAN 三层接口，删除 VLAN 之前，先删除 VLAN 三层接口。
- 如果 VLAN 已经创建业务虚端口，删除 VLAN 之前，先删除 VLAN 业务虚端口。

术语

无。

缩略语

无。

8.3.2 可获得性

介绍该特性需要的硬件支持，包括单板和终端。

无需额外硬件支持。

8.3.3 原理描述

介绍该特性的实现原理。

MUX VLAN 区分用户的原理是：MUX VLAN 与业务虚端口一一对应，即一个业务虚端口只对应一个 MUX VLAN，因而可以区分接入用户。

8.3.4 参考信息

介绍与该特性相关的参考信息。

本特性的参考资料清单如下：

- IEEE 802.1q：IEEE standards for Local and metropolitan area networks-Virtual Bridged Local Area Networks

8.4 QinQ VLAN

介绍 QinQ VLAN 基本特性以及在 UA5000 上的实现原理。

8.4.1 介绍

介绍该特性的定义、目的、规格和约束条件。

定义

QinQ（802.1Q in 802.1Q）是基于 802.1 Q 标准封装的隧道协议，在用户私有 802.1Q 的报文基础上，再封装一层 802.1Q 标签头，从而实现私网 VLAN 在公网透传，达到二层 VPN 的应用效果。

目的

QinQ 的核心思想是将用户私网 VLAN Tag 封装到公网 VLAN Tag 上。报文带着两层 802.1Q 格式的 VLAN Tag 穿越服务商的骨干网络，从而为用户提供一种较为简单的二层 VPN 隧道。QinQ 可以实现私网 VLAN 的业务直接透传到对端的功能，在一定程度上拓展私网的地域广度。

此处的专线业务是指私网业务直接透传到网络对端，例如企业内部网等。

规格

UA5000 支持最多 4000 个 QinQ VLAN。

约束

Super VLAN、Standard VLAN、Sub VLAN，已创建 VLAN 三层接口的 VLAN 及系统缺省 VLAN 都不能设其属性为 QinQ 属性。系统缺省 VLAN 的 VLAN ID 为 1，缺省 VLAN 不能删除，但可以修改缺省 VLAN 的类型。

术语

无。

缩略语

表 8-3 QinQ VLAN 特性缩略语表

缩略语	英文全称	中文全称
QinQ	802.1Q in 802.1Q	-
VPN	Virtual Private Network	虚拟专用网

8.4.2 可获得性

介绍该特性需要的硬件支持，包括单板和终端。

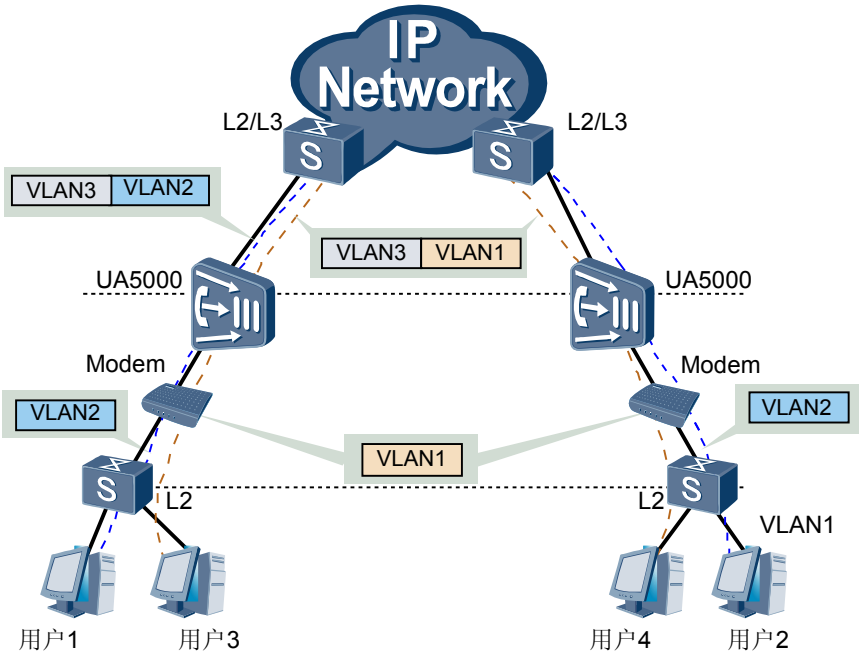
无需额外硬件支持。

8.4.3 原理描述

介绍该特性的实现原理。

QinQ VLAN 的业务处理过程如图 8-2 所示。

图 8-2 QinQ VLAN 业务处理过程



UA5000 通过 QinQ VLAN 实现不同地域同一私网（VLAN1 或 VLAN2）内用户的互连。业务的处理过程如下：

1. PC 发出 untagged 报文。
2. LAN switch 为该报文加上 PC 用户在私网中的 VLAN Tag（VLAN1 或 VLAN2）并发送给 UA5000。
3. UA5000 设备为报文统一加上公网 VLAN Tag（VLAN3），并传入上层网络。
4. 上层网络设备根据公网 VLAN Tag 传送报文。
5. 对端的 UA5000 接收到报文后剥离其公网 VLAN Tag（VLAN3），并将其传给 LAN switch。
6. LAN switch 识别并剥离私网 VLAN Tag（VLAN1 或 VLAN2），将报文转发给该私网 VLAN 中的用户。

这样就实现了 VLAN1 内用户 1 和用户 2 的互通，以及 VLAN2 内用户 3 和用户 4 的互通。

8.4.4 参考信息

介绍与该特性相关的参考信息。

本特性的参考资料清单如下：

- IEEE 802.1q：IEEE standards for Local and metropolitan area networks-Virtual Bridged Local Area Networks
- IEEE P802.1ad：Virtual Bridged Local Area Networks— Amendment 4: Provider Bridges

8.5 VLAN Stacking

介绍 VLAN Stacking 基本特性以及在 UA5000 上的实现原理。

8.5.1 介绍

介绍该特性的定义、目的、规格和约束条件。

定义

VLAN Stacking 是对 802.1 Q 标识的堆叠。接入设备为 untagged 的用户报文添加两层 802.1Q 格式的 VLAN Tag，报文带着两层 VLAN Tag 穿越服务商的骨干网络到达 BRAS。BRAS 使用双层 VLAN 进行认证，或者剥离外层 VLAN，根据内层标签来标识用户。

目的

具有 Stacking 属性的 VLAN 报文包含有 UA5000 分配的内、外两层 VLAN 标签。

VLAN Stacking 特性可用于扩展 VLAN 和提供批发业务。

- 通过两层 VLAN 标签提高 VLAN 的重用度。
- 通过 VLAN Stacking 的内层 VLAN 标识用户，通过外层 VLAN 来标识用户所属的 ISP（Internet Service Provider），将用户批量接入各自的 ISP。

批发业务是指当二层城域网中存在多个 ISP 时，将用户根据一定规则批量接入各自 ISP 的业务。

规格

UA5000 支持最多 4000 个 VLAN Stacking。

约束

- Standard VLAN、Super VLAN、Sub VLAN、已创建 VLAN 三层接口的 VLAN 及系统缺省 VLAN 都不能设其属性为 stacking 属性。
- 系统缺省 VLAN 的 VLAN ID 为 1，缺省 VLAN 不能删除，但可以修改缺省 VLAN 的类型。

术语

无。

缩略语

表 8-4 VLAN Stacking 特性缩略语表

缩略语	英文全称	中文全称
BRAS	Broadband Remote Access Server	宽带接入服务器

8.5.2 可获得性

介绍该特性需要的硬件支持和 License 支持。

硬件支持

无需额外硬件支持。

License 支持

VLAN Stacking 特性是 UA5000 的可选特性，只有获得 License 许可后才能获得该特性的服务。

说明

UA5000 的 VLAN Stacking 特性、DHCP option82 特性和 PPPoE 快速转发代理特性作为一个 License 功能项进行控制。

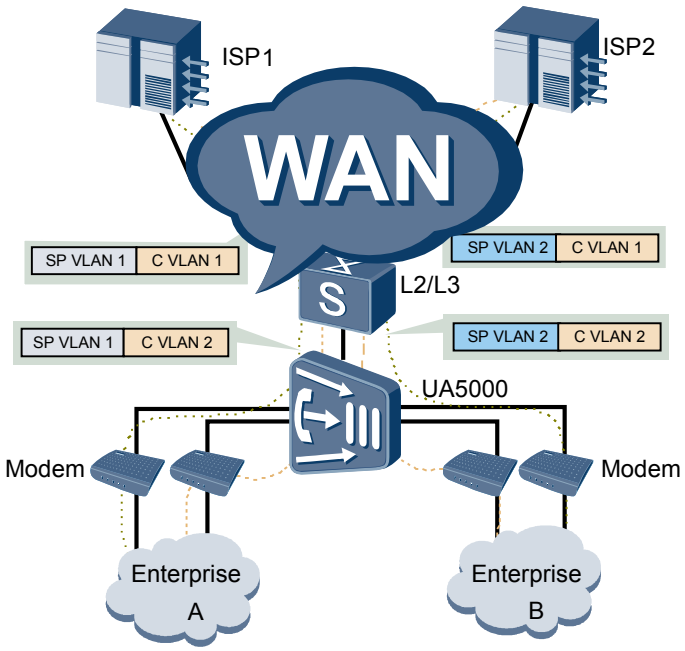
8.5.3 原理描述

介绍该特性的实现原理。

VLAN Stacking 如果应用于 VLAN 数目扩展和标识用户，需要 BRAS 配合。如果应用于提供专线批发业务，要求上层网络工作于二层工作模式，直接根据 VLAN 和 MAC 转发。

UA5000 VLAN Stacking 业务处理过程如图 8-3 所示。

图 8-3 VLAN Stacking 业务处理过程



说明

- SP VLAN: Service Provider VLAN
- C VLAN: Customer VLAN

UA5000 通过不同 VLAN Stacking 将企业 A 的用户接入 ISP1，企业 B 的用户接入 ISP2。业务的处理过程如下：

1. 用户发出 untagged 报文，经 Modem 到达 UA5000。
2. UA5000 为用户报文（untagged）封装两层 VLAN Tag。不同 ISP 的用户对应不同的外层 SP VLAN。
   - 企业 A 的用户报文外层统一封装 SP VLAN1，内层封装对应的 C VLAN。
   - 企业 B 的用户报文外层统一封装 SP VLAN2，内层封装对应的 C VLAN。
3. 交换城域网设备根据 SP VLAN 来转发报文。
4. ISP1 和 ISP2 设备接收到报文后剥离 SP VLAN，根据内层标签来区分企业内的不同类用户。

8.5.4 参考信息

介绍与该特性相关的参考信息。

本特性的参考资料清单如下：

- IEEE 802.1q：IEEE standards for Local and metropolitan area networks-Virtual Bridged Local Area Networks

8.6 Super VLAN

介绍 Super VLAN 基本特性以及在 UA5000 上的实现原理。

8.6.1 介绍

介绍该特性的定义、目的、规格和约束条件。

定义

Super VLAN，又称 VLAN Aggregation(VLAN 聚合)，该技术涉及 Sub VLAN、Super VLAN 的概念。

Super VLAN 和通常意义上的 VLAN 不同，它是一种只能包含 Sub VLAN，不包含物理端口和业务虚端口的 VLAN。

Sub VLAN 的类型可以是 Standard VLAN、Smart VLAN、MUX VLAN，当加入 Super VLAN 后就称为 Sub VLAN。Sub VLAN 只包含物理端口和业务虚端口，不能建立 VLAN 三层接口。Super VLAN 包含的所有 Sub VLAN 共用 Super VLAN 三层接口地址与上层通信。

目的

Super VLAN 主要用节省 IP 地址，提高 IP 地址的利用率。

规格

- UA5000 支持最多 16 个 Super VLAN，每个 Super VLAN 支持 480 个 Sub VLAN。
- Super VLAN 可以创建 VLAN 三层接口，并可以在 VLAN 三层接口下启动关闭 ARP Proxy。

约束

- 如果 Sub VLAN 中的用户端口包含 trunk 口，则不允许该 Sub VLAN 加入到 Super VLAN 中。

术语

无。

缩略语

无。

8.6.2 可获得性

介绍该特性需要的硬件支持，包括单板和终端。

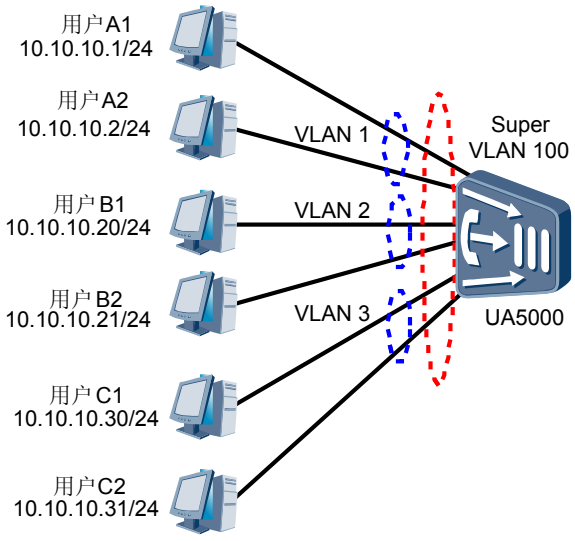
无需额外硬件支持。

8.6.3 原理描述

介绍该特性的实现原理。

为了更好说明 Super VLAN 的实现原理，举例说明，如图 8-4 所示，VLAN 1 包含 A 用户组：用户 A1 和用户 A2； VLAN 2 包含 B 用户组：用户 B1 和用户 B2；VLAN 3 包含 C 用户组：用户 C1 和 C2。用户组 A、B、C 的主机地址在相同的网段 10.10.10.0 内。

图 8-4 Super VLAN 原理



用户组 A、B、C 分布位于不同的 VLAN 内，由于 VLAN 的广播隔离作用，用户组 A、B、C 之间是不可以互通的。也就是说用户组 A、B、C 之间是二层隔离的。

为了使不同 VLAN 下 PC 互通，可以使用 VLAN 三层接口技术，但是三层接口技术要求不同 VLAN 三层接口下 PC 地址属于不同的网段。上面举例中为了节省 IP 地址用户组 A、B、C 属于同一个网段，这种情况下可以使用 Super VLAN 来解决 VLAN 之间互通的需求。

为了使用户组 A、B、C 之间可以相互访问，创建 Super VLAN 100，并且将 VLAN 1, VLAN 2，VLAN 3 作为 Sub VLAN 加入 Super VLAN 100。同时在 Super VLAN 100 创建 VLAN 三层接口，配置 VLAN 三层接口 IP，并启动 ARP proxy。

用户 A1 访问用户 C1 的过程：

1. 由于用户 C1 的主机地址与 A1 处在同一个网段内，A1 第一次访问 C1 是会发送 ARP 报文获取 C1 的 MAC 地址。
2. 由于用户 A1 和用户 C1 二层隔离，ARP 请求报文不会直接发送给用户 C1。ARP 请求报文由 Super VLAN 的 ARP proxy 功能捕获，ARP proxy 功能模块会获取用户 C1 的 MAC 地址，获取成功后会将 Super VLAN 接口的 MAC 作为 C1 的 MAC 地址告诉用户 A1。
3. 用户 A1 发送给用户 C1 的报文都先发送给 Super VLAN，Super VLAN 通过三层转发功能将报文转发给用户 C1。用户 C1 访问用户 A1 的过程与上面过程类似。

从上面的过程可以看出，通过建立 Super VLAN 和 Sub VLAN 间的映射关系，把三层接口和物理端口这两部分结合起来，用一个 Super VLAN 来实现所有 Sub VLAN 共享同一个 VLAN 三层接口，使不同 Sub VLAN 内的 PC 可以共用同一个 Super VLAN 的网关，从而在实现 Standard VLAN 的功能的同时，达到节省 IP 地址的目的。

8.6.4 参考信息

介绍与该特性相关的参考信息。

本特性的参考资料清单如下：

- IEEE 802.1q：IEEE standards for Local and metropolitan area networks-Virtual Bridged Local Area Networks
- RFC3069：VLAN Aggregation for Efficient IP Address Allocation

9 DHCP Relay

关于本章

介绍 DHCP Relay 特性的定义、目的、规格、原理以及参考的术语、缩略语和相关协议标准。

9.1 介绍
介绍该特性的定义、目的、规格和约束条件。

9.2 可获得性
介绍该特性需要的硬件支持，包括单板和终端。

9.3 原理描述
介绍该特性的实现原理。

9.4 参考信息
介绍与该特性相关的参考信息。

9.1 介绍

介绍该特性的定义、目的、规格和约束条件。

定义

DHCP Relay 是指这样一个过程：在 DHCP 客户机和 DHCP 服务器之间实现对 DHCP 广播报文的跨网段转发。能够使位于不同物理网段的 DHCP 客户机从同一台 DHCP 服务器上正确地获得动态分配地 IP 地址。

目的

- DHCP（Dynamic Host Configuration Protocol）协议以客户机—服务器（Client-Server）模式工作。
  - DHCP 客户机向 DHCP 服务器动态地请求配置信息。
  - DHCP 服务器为客户机动态配置 IP 地址等信息。
- 早期的 DHCP 协议只适用于 DHCP 客户机和服务器处于同一个子网内的情况，不可以跨网段工作，这样就需要为每一个子网设置一个 DHCP 服务器，浪费了资源。DHCP Relay（DHCP 中继）的引入解决了这一问题。
- DHCP Relay 在处于不同子网间的 DHCP 客户机和服务器之间承担中继服务，可以将 DHCP 协议报文中继到跨网段的目的 DHCP 服务器或客户机，于是许多网络上的 DHCP 客户机可以使用同一个 DHCP 服务器。这样，既节省开销又便于集中管理。

规格

- 支持配置 20 个 DHCP Server 组，每组包含主/备两个 DHCP 服务器。
- 支持三种方式来进行 DHCP 服务器的选取：DHCP Relay 标准方式、DHCP Option60 方式和 MAC 地址段方式。
- 支持配置 128 个 DHCP Option60 域，域名为不区分大小写的字符串，长度为：1 ～ 32 字符。
- 支持配置 128 个 MAC 地址段，MAC 地址段的名字为不区分大小写的字符串，长度为：1 ～ 32 字符。

约束

DHCP Relay 基于全局启动，启用后对设备接入的所有用户都有效。

术语

无。

缩略语

表 9-1 DHCP Relay 特性缩略语表

缩略语	英文全称	中文全称
DHCP	Dynamic Host Configuration Protocol	动态主机配置协议
DHCP Relay	Dynamic Host Configuration Protocol Relay	DHCP 中继

9.2 可获得性

介绍该特性需要的硬件支持，包括单板和终端。

无需额外硬件支持。

9.3 原理描述

介绍该特性的实现原理。

当 DHCP 客户机启动并进行 DHCP 初始化时，会在本网络广播配置请求报文。

如果本网络存在 DHCP 服务器，则不需要使用 DHCP Relay 功能，DHCP 服务器直接就可以对本网络的 DHCP 客户机进行 DHCP 配置。

如果本网络里没有 DHCP 服务器，则需要在本网络中的 UA5000 上启动 DHCP Relay 功能，DHCP Relay 在收到该广播报文后进行处理，包括根据指定的方式来选择 DHCP 服务器组，最后将该广播报文转换为单播 IP 报文，转发给选定的 DHCP 服务器组。

UA5000 支持以下三种方式选择 DHCP 服务器组。

- DHCP Relay 标准方式

  根据接收 DHCP 报文的接口来选择 DHCP 服务器组。此为系统缺省方式，需要事先配置好接口绑定的 DHCP 服务器组。

  该模式的实质是按照 VLAN 来区分用户，也是一种最常用、最简单的 DHCP Relay 模式。缺点是不能区分位于相同 VLAN 中的不同业务类型。

- DHCP Option60 方式

  按照 DHCP 报文的 Option60 选项中的字符串（称之为域名）来选择 DHCP 服务器组。需要事先配置好 Option60 域名和域名绑定的 DHCP 服务器组。

  该模式的实质是按照报文的“域”信息来区分用户，也是一种常用的 DHCP Relay 模式，可以区分位于相同 VLAN 中的不同业务类型。

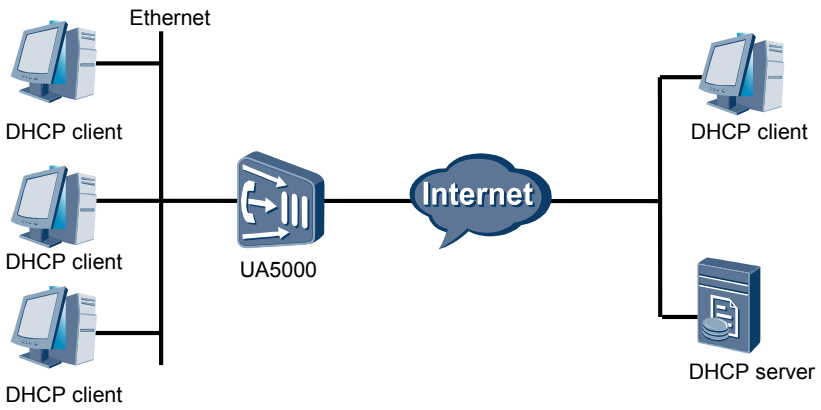
- MAC 地址段方式

  按照 DHCP 报文的源 MAC 地址来选择 DHCP 服务器组。需要事先配置好 MAC 地址段和其绑定的 DHCP 服务器组。

  该模式的实质是按照报文的源 MAC 地址段来区分用户，也可以用来区分位于相同 VLAN 中的不同业务类型。

DHCP 服务器根据客户机提供的配置申请信息，为其作相应的配置，并通过 DHCP Relay 将该配置信息转发给客户机，完成对客户机的动态配置。

图 9-1 DHCP Relay 组网示意图



9.4 参考信息

介绍与该特性相关的参考信息。

本特性的参考资料清单如下：

- RFC 2131：Dynamic Host Configuration Protocol

10 ARP Proxy

关于本章

介绍 ARP Proxy 特性的定义、目的、规格、原理以及参考的术语、缩略语和相关协议标准。

10.1 ARP
介绍 ARP 特性以及在 UA5000 上的实现原理。

10.2 ARP Proxy
介绍 ARP Proxy 特性以及在 UA5000 上的实现原理。

10.1 ARP

介绍 ARP 特性以及在 UA5000 上的实现原理。

10.1.1 介绍

介绍该特性的定义、目的、规格和约束条件。

定义

地址解析协议 ARP（Address Resolution Protocol）属于 TCP/IP 协议族，用来将 IP 地址解析为 MAC 地址。

目的

因为 IP 地址只是计算机在网络层中的地址，如果要将网络层数据报文传送给目的计算机，必须知道目的计算机的物理地址，即 MAC 地址，因此必须将 IP 地址解析为 MAC 地址。此时，需要应用到 ARP 协议。

规格

UA5000 最大支持手工配置 500 个静态 ARP 表项，最多可以动态学习到 2048 个动态 ARP 表项。

术语

无。

缩略语

表 10-1 ARP 特性缩略语表

缩略语	英文全称	中文全称
ARP	Address Resolution Protocol	地址解析协议
MAC	Media Access Control	媒质接入控制

10.1.2 可获得性

介绍该特性需要的硬件支持，包括单板和终端。

无需额外硬件支持。

10.1.3 原理描述

介绍该特性的实现原理。

ARP 映射表

每台计算机都要维护 IP 地址到 MAC 地址的转换表，称为 ARP 映射表。

ARP 映射表中存放着最近用到的一系列与本设备通信的其他计算机的 IP 地址和 MAC 地址的映射。在设备启动时，ARP 映射表为空。

ARP 实现原理

ARP 实现网络间设备的二层互通。这里以两台计算机 A、B 为例来说明 ARP 的实现过程。计算机 A 的 IP 地址为 IP_A，计算机 B 的 IP 地址为 IP_B，计算机 A 要向计算机 B 发送信息。

1. 计算机 A 首先查看自己的 ARP 映射表，确定其中是否包含有 IP_B 对应的 ARP 映射表项。
2. 如果找到了对应的 MAC 地址，则计算机 A 直接利用 ARP 映射表中的 MAC 地址，对 IP 数据包进行封装，并将数据发送给计算机 B。
3. 如果在 ARP 映射表中找不到对应的 MAC 地址，则计算机 A 将该数据包放入 ARP 发送等待队列，然后创建一个 ARP request，并以广播方式在以太网上发送。ARP request 数据包中包含有计算机 B 的 IP 地址，以及计算机 A 的 IP 地址和 MAC 地址。
4. 由于 ARP request 数据包以广播方式发送，以太网上的所有计算机都可以接收到该请求，但只有被请求的计算机（即计算机 B）会对该请求进行应答。
5. 计算机 B 首先把 ARP request 数据包中的请求发起者（即计算机 A）的 IP 地址和 MAC 地址存入自己的 ARP 映射表中。
6. 然后计算机 B 组织 ARP 响应数据包，在数据包中填入计算机 B 的 MAC 地址，发送给计算机 A。这个响应不再以广播形式发送，而是直接以单播形式发送给计算机 A。
7. 计算机 A 收到响应数据包后，提取出计算机 B 的 IP 地址及其对应的 MAC 地址，加入到自己的 ARP 映射表中，并把放在发送等待队列中的发往计算机 B 的所有数据包都发送出去。

静态 ARP 和动态 ARP

可以静态或动态维护 ARP 映射表。通常将用户手工配置的 IP 地址到 MAC 地址的映射，称之为静态 ARP。而如果 ARP 映射表由 ARP 协议动态维护，称之为动态 ARP。

一般情况下采用 ARP 协议动态维护，如果用户需要手工干预调整 ARP 映射表时，才需要手工配置静态表项。

静态 ARP 表项在 UA5000 正常工作时间一直有效，而动态 ARP 表项的老化时间为 20 分钟。

10.1.4 参考信息

介绍与该特性相关的参考信息。

本特性的参考资料清单如下：

- IETF RFC 826:An Ethernet Address Resolution Protocol or Converting Network Protocol Addresses to 48.bit Ethernet Address for Transmission on Ethernet Hardware

10.2 ARP Proxy

介绍 ARP Proxy 特性以及在 UA5000 上的实现原理。

10.2.1 介绍

介绍该特性的定义和目的。

定义

ARP Proxy 是指这样一个过程：当 ARP 请求报文从计算机 A 发往计算机 B 时，该请求报文由连接这两个计算机的接入设备进行处理。

目的

在 UA5000 上，当要实现 Super VLAN 下的 Sub VLAN 互通时，通常采用 ARP Proxy。当 UA5000 支持三层功能以后，Smart VLAN 下的用户也需要通过 ARP Proxy 实现互通。

10.2.2 可获得性

介绍该特性需要的硬件支持，包括单板和终端。

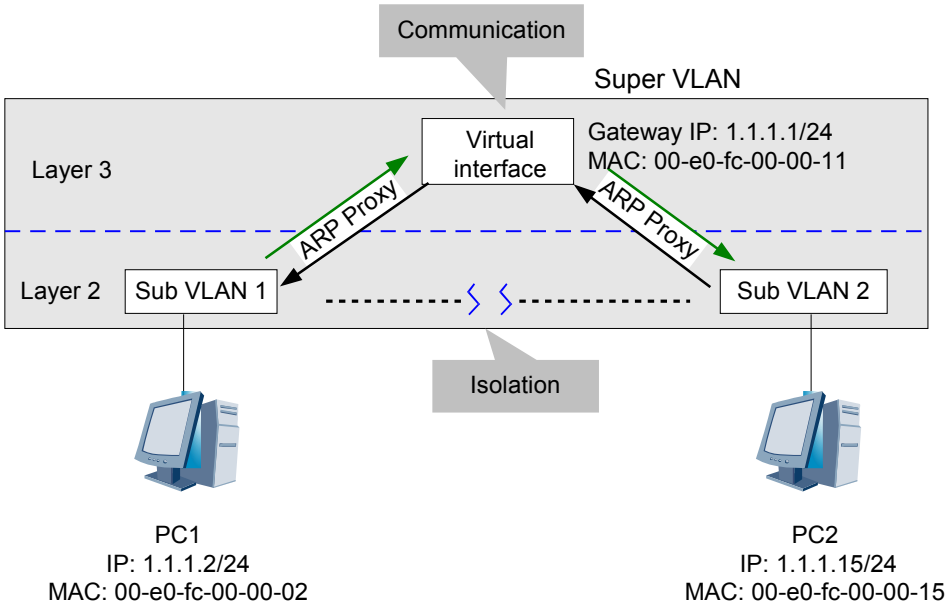
无需额外硬件支持。

10.2.3 原理描述

介绍该特性的实现原理。

如图 10-1 所示，PC1、PC2 分别处于 VLAN1、VLAN2 中，它们在二层上被隔离。PC1、PC2 以及三层虚拟接口都处于同一子网里。

图 10-1 ARP Proxy 实现原理



实现 PC1、PC2 互通的步骤如下所示。

1. 由于 PC1、PC2 处于同一子网，当 PC1 发送报文给 PC2 时，将直接广播 ARP 报文，请求 PC2 的 MAC 地址。由于 PC1、PC2 在不同的广播域，因此 PC1 不会得到 PC2 的 ARP 响应报文。
2. UA5000（已使能 ARP Proxy 功能）收到 ARP 请求报文后，将其虚拟三层接口的 MAC 地址和 PC2 的 IP 地址组合后发送应答报文给 PC1，并在 ARP 表中查找是否存在 PC2 的 MAC 地址。
3. 如果 ARP 表中存在 PC2 的 MAC 表项，则 ARP Proxy 工作完成，PC1 的报文可以经 UA5000 虚拟三层接口转发给 PC2。
4. 如果 ARP 表中没有 PC2 的 MAC 地址，UA5000 将通过三层虚拟接口广播 ARP 报文，请求 PC2 的 MAC 地址。
5. UA5000 得到 PC2 的 APR 响应报文后，将 PC2 的 MAC 地址加入 ARP 表中。此时，ARP Proxy 结束，PC1、PC2 可以通过 UA5000 实现互通。

10.2.4 参考信息

介绍与该特性相关的参考信息。

本特性的参考资料清单如下：

- IETF RFC1027:Using ARP to Implement Transparent Subnet Gateways

11 ACL

关于本章

介绍 ACL 特性的定义、目的、规格、原理以及参考的术语、缩略语和相关协议标准。

11.1 介绍
介绍该特性的定义、目的、规格和约束条件。

11.2 可获得性
介绍该特性需要的硬件支持，包括单板和终端。

11.3 原理描述
介绍该特性的实现原理。

11.1 介绍

介绍该特性的定义、目的、规格和约束条件。

定义

访问控制列表 ACL（Access Control List）是指通过配置的一系列匹配规则对特定的数据包进行过滤，从而识别需要过滤的对象。在识别出特定的对象之后，根据预先设定的策略允许或禁止相应的数据包通过。

目的

ACL 过滤报文流过程是在为进行 QoS 处理做准备，与 QoS 策略共同提高系统的安全性。

规格

- ACL 编号在 2000 ～ 5999 之间，最多允许定义 4000 条 ACL，每个 ACL 下最多设置 64 条规则。各种类型 ACL 说明如表 11-1 所示。
- 每个端口可以激活的 ACL 有效规则数 128 条。

表 11-1 ACL 分类列表

项目	数字取值范围	特点
基本 ACL	2000 ～ 2999	只能根据三层源 IP 制定规则，对数据包进行相应的分析处理。
高级 ACL	3000 ～ 3999	可以根据数据包的源地址信息、目的地址信息、IP 承载的协议类型、针对协议的特性，例如 TCP 的源端口、目的端口，ICMP 协议的类型、code 等内容定义规则。利用高级 ACL 可以定义比基本 ACL 更准确、更丰富、更灵活的规则。
链路层 ACL	4000 ～ 4999	可以根据源 MAC 地址、源 VLAN ID、二层协议类型、目的 MAC 地址等链路层信息制定规则，对数据进行相应处理。
用户自定义 ACL	5000 ～ 5999	可以根据二层数据帧的前 80 个字节中的任意 32 字节进行匹配，对数据报文做出相应的处理。

约束

由于硬件资源有限，软件上采取了尽可能共享硬件资源的方式来最大限度地利用硬件。这导致了后下发的 ACL 规则不一定比前面下发的 ACL 规则优先级高。

术语

无。

缩略语

表 11-2 ACL 特性缩略语表

缩略语	英文全称	中文全称
ACL	Access Control List	访问控制列表
QoS	Quality of Service	服务质量
ToS	Type of Service	服务类型
DSCP	Differentiated Services Codepoint	区分服务节点

11.2 可获得性

介绍该特性需要的硬件支持，包括单板和终端。

无需额外硬件支持。

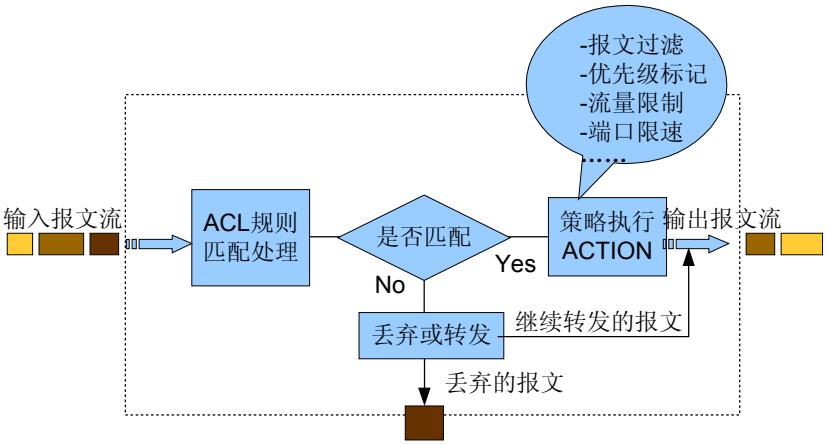
11.3 原理描述

介绍该特性的实现原理。

系统对输入的报文流将按照 ACL 所定义的规则进行匹配处理：

- 如果有匹配的 ACL 规则，则交 QoS 策略进一步执行处理，包括报文过滤、优先级标记、端口限速、流量限制、流量统计、报文重定向、报文镜像，在完成策略执行处理后再转发输出报文流；
- 否则，按照 ACL 规则的定义，不匹配规则的报文将被丢弃或者被转发。

图 11-1 ACL 规则过滤处理原理图



- 报文过滤：按照匹配 ACL 规则匹配的结果确定是否丢弃报文。

- 优先级标记：对匹配 ACL 规则的数据包进行优先级标记，标记内容包括 ToS、DSCP、802.1p 等。
- 流量限制：对匹配访问 ACL 规则的数据包进行流量限制。
- 端口限速：对以太网端口发送报文的总速率进行限制。
- 流量统计：对匹配 ACL 规则的数据包进行流量统计。
- 报文重定向：对匹配 ACL 的数据包进行重定向操作，重新指定报文的转发端口（原来的端口不再进行报文的接收或转发）。
- 报文镜像：对匹配访问控制列表的数据包进行流镜像，可以将匹配 ACL 的报文流拷贝输出到其他端口。

12 QoS

关于本章

介绍 QoS 特性的定义、目的、规格、原理以及参考的术语、缩略语和相关协议标准。

12.1 QoS 特性描述
概括介绍 QoS 基本特性以及在 UA5000 上的实现原理。

12.2 严格优先级队列调度
详细介绍严格优先级队列调度特性以及在 UA5000 上的实现原理。

12.3 加权轮循队列调度
详细介绍加权轮循队列调度特性以及在 UA5000 上的实现原理。

12.4 CoS 优先级和调度队列的灵活映射
详细介绍 CoS 优先级和调度队列的灵活映射特性以及在 UA5000 上的实现原理。

12.1 QoS 特性描述

概括介绍 QoS 基本特性以及在 UA5000 上的实现原理。

12.1.1 介绍

介绍该特性的定义、目的、规格和约束条件。

定义

QoS（Quality of Service），即服务质量，是指通过一系列的度量指标，包括业务可用性、延迟、抖动、丢失率等，为用户业务提供端到端的质量保证。

目的

QoS 的目的是利用有限的网络资源，为不同的业务流提供不同的服务质量。

规格

- 支持报文 802.1p 优先级设置。
- 上行以太网端口支持 8 个优先级队列（0 ～ 7）。
- 对于主控板 IPMB，用户端口支持 4 个优先级队列。对于主控板 IPMD，用户端口支持 8 个优先级队列。
- 队列调度支持 PQ（优先级队列）、WRR（加权轮循）的方式，其中 WRR 调度方式只有上行以太网端口支持。

术语

表 12-1 QoS 特性术语表

术语	解释
可用性	用户能够使用业务的时间占业务全部工作时间的百分数。
时延	指在两个参考点间某一 IP 包从发送到接收之间的时间间隔。
抖动	指不同分组之间在延迟上的偏差。
丢包率	指在两个参考点间传输时丢失的 IP 包数与已发送的 IP 包总数的比值。丢包主要是由网络拥塞引起的。

缩略语

表 12-2 QoS 特性缩略语表

缩略语	英文全称	中文全称
QoS	Quality of Service	服务质量

缩略语	英文全称	中文全称
WRR	Weighted Round Robin	加权循环调度队列
PQ	Priority Queuing	优先级队列

12.1.2 可获得性

介绍该特性需要的硬件支持，包括单板和终端。

无需额外硬件支持。

12.1.3 原理描述

介绍该特性的实现原理。

- 基于流灵活设置报文的 802.1p 优先级。

  支持针对每个流设置优先级，以满足不同业务对 QoS 的应用需求。

  对于语音等对时延和抖动敏感的业务，可以设置高的优先级，如：7；对于宽带上网业务，可以设置低的优先级，如：0。
- 基于流进行上下行速率限制。

  为限制某个流占用过大的带宽，影响其它业务流，可以设置每个流的最大速率，对于超过速率的报文直接丢弃。
- 队列调度，分为严格优先级队列调度和加权轮循队列调度。请参见“**12.2 严格优先级队列调度**”和“**12.3 加权轮循队列调度**”。

12.2 严格优先级队列调度

详细介绍严格优先级队列调度特性以及在 UA5000 上的实现原理。

12.2.1 介绍

介绍该特性的定义、目的和规格。

定义

严格优先级队列调度给每个队列赋予不同的优先级，之后每次调度时，最先对具有最高优先级的非空队列中的报文进行服务。严格优先级队列调度严格按照优先级从高到低的次序优先发送较高优先级队列中的报文，当较高优先级队列为空时，再发送较低优先级队列中的报文。

目的

解决当网络拥塞时多个报文流同时竞争使用资源的问题。

规格

上行以太网端口支持 8 个优先级队列，优先级为 0 ～ 7 依次升高。对于主控板 IPMB，用户端口支持 4 个优先级队列，优先级为 0 ～ 3 依次升高。对于主控板 IPMD，用户端口支持 8 个优先级队列，优先级为 0 ～ 7 依次升高。

12.2.2 原理描述

介绍该特性的实现原理。

PQ 队列调度，是针对关键业务型应用设计的。关键业务有一个重要的特点是在拥塞发生时要求优先获得服务以减小响应的延迟。

在队列调度时，PQ 严格按照优先级从高到低的次序优先发送较高优先级队列中的分组，当较高优先级队列为空时，再发送较低优先级队列中的分组。

图 12-1 优先队列示意图（主控板为 IPMB）

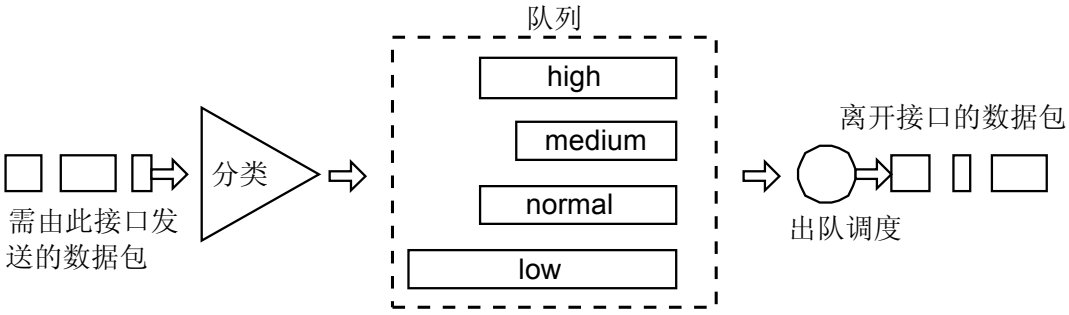
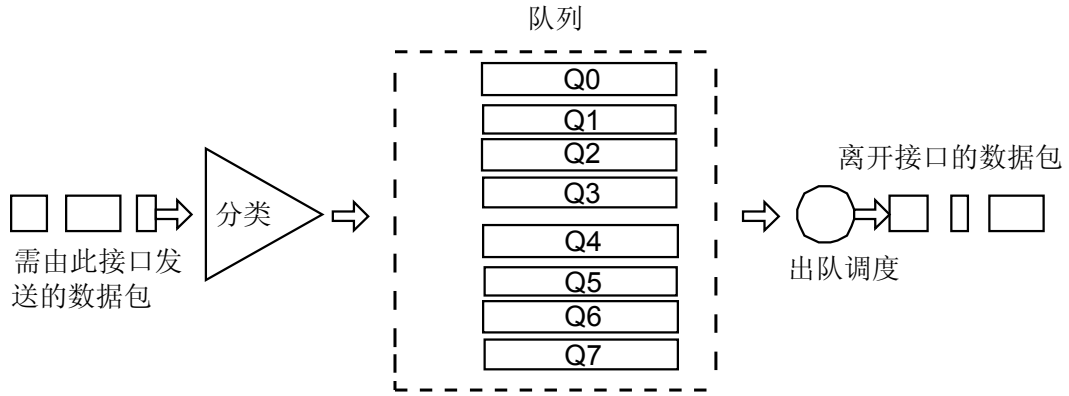


图 12-2 优先队列示意图（主控板为 IPMD）



这样，将关键业务（如语音业务）的分组放入较高优先级的队列，将非关键业务（如 E-Mail）的分组放入较低优先级的队列，可以保证关键业务的分组被优先传送，非关键业务的分组在处理关键业务数据的空闲间隙被传送。

PQ 的缺点：拥塞发生时，如果较高优先级队列中长时间有分组存在，那么低优先级队列中的报文就会由于得不到服务而被丢弃。

12.3 加权轮循队列调度

详细介绍加权轮循队列调度特性以及在 UA5000 上的实现原理。

12.3.1 介绍

介绍该特性的定义、目的、规格和约束条件。

定义

加权轮循队列调度给每个队列赋予不同的权重值，代表一次完整循环队列被服务的报文数，一次调度发送一个报文，使得不同队列在报文个数上按比例使用带宽资源。

目的

解决当网络拥塞时多个报文流同时竞争使用资源的问题。

规格

加权轮循队列调度仅上行以太网端口支持，每个端口支持 8 个优先级，优先级为 0 ～ 7 依次升高。

QoS 功能增强。每个用户端口支持 8 个优先级队列，支持用户端口 PQ+WRR 调度。

12.3.2 原理描述

介绍该特性的实现原理。

WRR 队列调度是在队列之间轮流调度，保证每个队列都得到一定的服务。

以端口有 4 个优先级队列为例，WRR 可为每个队列配置一个加权值（由高到低依次为 w3、w2、w1、w0），加权值表示获取资源的比重。

如一个 100M 的端口，配置它的 WRR 队列调度算法的加权值为 13、10、8、5（依次对应 w3、w2、w1、w0），这样可以保证最低优先级队列至少获得 14Mbit/s 带宽，避免了采用 PQ 调度时低优先级队列中的报文可能长时间得不到服务的缺点。

WRR 队列还有一个优点是，虽然多个队列的调度是轮循进行，但对每个队列不是固定地分配服务时间片——如果某个队列为空，那么马上换到下一个队列调度，这样带宽资源可以得到充分的利用。

SP 队列调度严格按照优先级从高到低的次序，优先发送较高优先级队列中的分组。当较高优先级队列为空时，再发送较低优先级队列中的分组。

这样，将关键业务的分组放入较高优先级的队列，将非关键业务（如 E-Mail）的分组放入较低优先级的队列，可以保证关键业务的分组被优先传送，非关键业务的分组在处理关键业务数据的空闲间隙被传送。

SP 队列调度的缺点是：拥塞发生时，如果较高优先级队列中长时间有分组存在，那么低优先级队列中的报文就会由于得不到服务而被丢弃。

SP+WRR 调度是 SP 和 WRR 的混合体。即先满足 SP 严格优先级调度，再满足 WRR 队列调度。

以端口有 4 个优先级队列为例，WRR 可为每个队列配置一个加权值（由高到低依次为 w3、w2、w1、w0），加权值表示获取资源的比重。如一个 100M 的端口，配置它的 WRR 队列调度算法的加权值为 70、30、0、0（依次对应 w3、w2、w1、w0），这样可以保证 w1、w0 按照严格优先级调度，剩下的 W3、W2 按照加权值轮循调度。

12.4 CoS 优先级和调度队列的灵活映射

详细介绍 CoS 优先级和调度队列的灵活映射特性以及在 UA5000 上的实现原理。

12.4.1 介绍

介绍该特性的定义、目的、规格和约束条件。

定义

CoS 优先级和调度队列的灵活映射是指接入设备支持灵活地配置优先级和队列的映射关系，可以指定某个优先级的报文要送到指定的队列。

目的

可以满足运营商对业务管理的特定需求。比如使用优先级 1 和 2 代表语音业务，则可将优先级 1 和 2 映射到队列 3，保证语音业务获得较优先的调度。

12.4.2 原理描述

介绍该特性的实现原理。

对以太网报文进行入队调度时，需要使用某一优先级确定报文入队的队列，这个优先级称为报文服务优先级，一般即是根据报文本身（如 802.1p 域）携带的优先级，根据这个优先级将报文映射到相应的优先级队列中。

缺省情况下，报文服务优先级和要进入的队列的关系是固定的，例如优先级为 7 进入 7 号队列（7 号队列拥有最高优先级），优先级为 6 进入 6 号队列。

实际组网运营中，可能需要进行不同于上述缺省对应关系的配置。比如实际用到优先级 1、2、3、4、5，其中 1 和 2 表示数据业务、3 表示视频业务、4 和 5 表示语音业务；实际配置的队列为 0、2、4、6 四个队列，则可如表 12-3 所示配置优先级和队列的映射关系。

表 12-3 报文服务优先级和队列优先级的映射关系

报文服务优先级	队列优先级	
	缺省情况	某种应用情况的配置
7	7	7
6	6	6
5	5	6
4	4	6
3	3	4

报文服务优先级	队列优先级	
	缺省情况	某种应用情况的配置
2	2	2
1	1	0
0	0	0

13 RRPP

关于本章

RRPP（Rapid Ring Protection Protocol）快速环网保护协议是一个专门应用于以太网环的链路层协议。

13.1 介绍
介绍 RRPP 的定义、目的、规格、原理以及参考的术语、缩略语和相关协议标准。

13.2 可获得性
介绍该特性需要的硬件支持。

13.3 原理描述
介绍该特性的实现原理。

13.4 参考信息
介绍该特性相关的参考信息。

13.1 介绍

介绍 RRPP 的定义、目的、规格、原理以及参考的术语、缩略语和相关协议标准。

定义

RRPP 快速环网保护协议是一个专门应用于以太网环的链路层协议。它在以太网环完整时能够防止数据环路引起的广播风暴，而当以太网环上一条链路断开时能迅速恢复环网上各个节点之间的通信通路。

目的

城域网和企业网大多采用环网来构建以提供高可靠性，环上任意一个节点发生故障，都不会影响业务。相比其他以太环网技术，RRPP 具有以下优势：

- 拓扑收敛速度快，低于 50ms。
- 收敛时间与环网上节点数无关，可应用于网络直径较大的网络。
- 在以太网环完整时能够防止数据环路引起的广播风暴。
- 当以太网环上一条链路断开时能迅速启用备份链路以恢复环网上各个节点之间的通信通路。

规格

- UA5000 只支持 RRPP 单域单环组网，并且环只能是主环。
- RRPP 环上的一条链路故障，其 RRPP 环上业务中断的时间小于 200ms。
- RRPP 环上的主节点不支持组播的 RRPP 模式。
- RRPP 环上的传输节点在 IGMP Proxy 模式下，支持组播的 RRPP 模式，并且需要将 RRPP 端口同时设置为上行口和级联口。
- RRPP 协议和 RSTP（Rapid Spanning Tree Protocol）协议在同一端口互斥。
- RRPP 协议和手动端口隔离在同一端口上互斥。
- H612IPMD 主控板 RRPP 端口支持端口链路聚合。
- UA5000 提供平滑处理机制，保证 IPM 主备倒换后，RRPP 正常运行。

术语

表 13-1 RRPP 术语表

术语	解释
RRPP 域	用整数表示的 ID 来唯一标识一个 RRPP 域。
RRPP 环	一个 RRPP 环物理上对应一个环形连接的以太网拓扑。
主节点	以太网环上每一台交换机都称为一个节点，每个 RRPP 环上必须有一个主节点，而且只能有一个。
传输节点	在 RRPP 环中，除了主节点以外的其他节点都是传输节点。传输节点负责监测自己的直连 RRPP 链路的状态，并把链路变化通知主节点，然后由主节点来决策如何处理。

缩略语

表 13-2 RRPP 缩略语表

缩略语	英文全称	中文全称
RRPP	Rapid Ring Protection Protocol	快速环网保护协议
RSTP	Rapid Spanning Tree Protocol	快速生成树协议

13.2 可获得性

介绍该特性需要的硬件支持。

支持本特性的单板包括：IPMB 和 IPMD。

13.3 原理描述

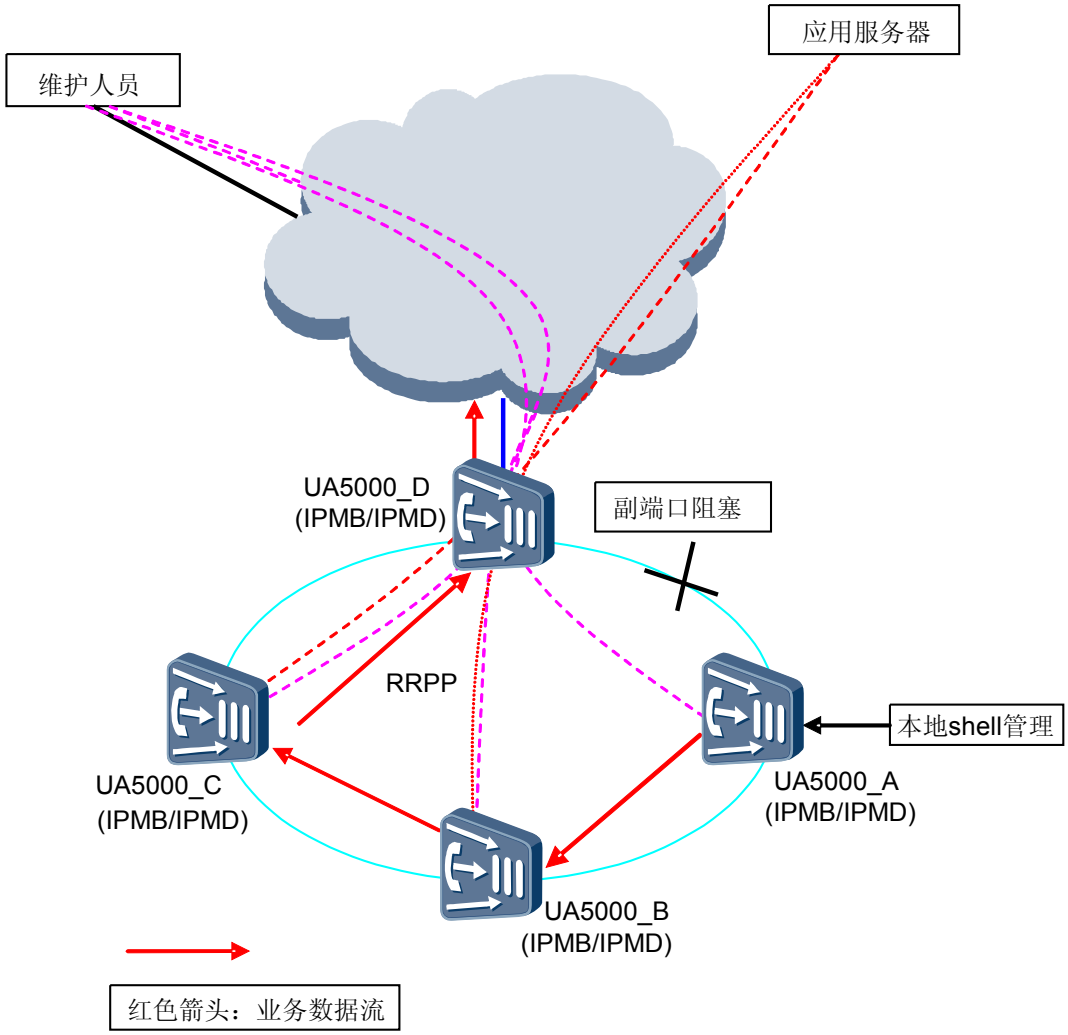
介绍该特性的实现原理。

UA5000 提供 RRPP 环网主要是在接入部分提供链路的保护机制，并且要求故障时，业务倒换收敛时间非常短（一般要求 50ms ～ 200ms 之间）。

环路正常时 RRPP 的工作原理

环路正常时 RRPP 的工作原理如图 13-1 所示。

图 13-1 RRPP 工作原理图 1



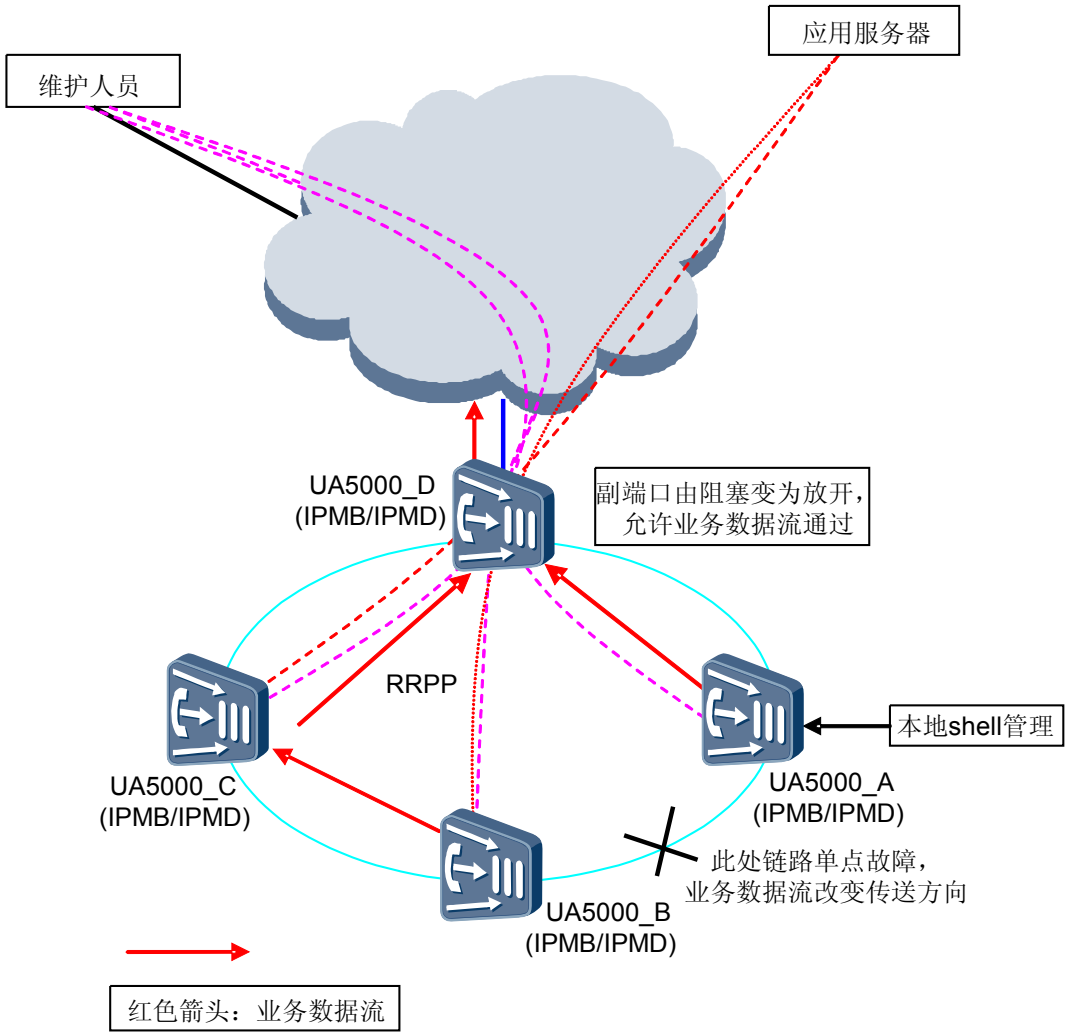
在链路正常的时候，由 RRPP 环的主节点（UA5000_D）阻塞其副端口(只有协议报文可以通过，其它数据报文禁止通过)，阻止环路的发生。

业务数据流由主节点的主端口进入，完成汇聚上行；同时 RRPP 环的主节点按用户配置的周期（HELLO 定时器周期），周期性地发送 HELLO 报文。中间的传输节点在二层直接转发收到的 HELLO 报文，HELLO 报文最终在主节点的副端口收到。采用这种方式检测环路是否完整。如果在用户配置的时间内（FAIL 定时器周期）主节点的副端口没有收到 HELLO 报文，则主节点认为环路发生故障，进行相应的故障处理。

环路故障时 RRPP 的工作原理

环路故障时 RRPP 的工作原理如图 13-2 所示。

图 13-2 RRPP 工作原理图 2



RRPP 协议采用以下两种方式进行环路故障的检测，

- 传输节点在检测到接入到 RRPP 环的 GE 口端口状态为 Down 后，其 CPU 会通过另外一个 GE 口向主节点发送 LINK-DOWN 控制报文，告知 RRPP 环路故障的发生。
- 主节点周期性地发送 HELLO 报文，如果在配置的超时时间内，副端口没有收到主节点发送的 HELLO 报文，则认为环路发生故障。

无论哪种方式检测到环路故障，主节点（UA5000_D）均进行故障处理（打开副端口，刷新 FDB 报文，通知其它传输节点刷新其 FDB 报文）。故障处理之后，业务数据流按照新的传输方向进行传输，不影响业务应用。

说明

主节点向传输节点发送刷新 FDB 报文的控制报文，需要从主端口和副端口同时发送，否则因为环路物理故障，可能导致部分节点无法刷新 FDB 报文。

环路故障恢复

检测环路故障恢复有如下两种方式：

- 中间的传输节点检测到接入 RRPP 环的 GE 口状态为 Up。
- 当环路故障时，主节点依旧周期性地从其主端口发送 HELLO 报文，在 fail-period 定时器超时前，主节点从其副端口收到了自己发送的 HELLO 报文，则认为环路恢复。

在 RRPP 协议中采用了第二种方式。主节点收到自己发送的 HELLO 报文后，认为环路故障恢复。接着主节点进行故障恢复后的操作，即阻塞其副端口，刷新 FDB 报文，通知传输节点刷新其 FDB 报文。传输节点收到控制报文后，刷新 FDB 报文，解阻塞其刚刚恢复的端口。

环路故障恢复瞬间主节点和传输节点状态不一致

链路故障后，传输节点在检测到链路端口状态为 Up 后，传输节点需要马上临时阻塞刚刚恢复的端口，此时传输节点处于 Pre-forwarding 状态。传输节点直到收到主节点发送的 COMPLETE_FLUSH_FDB 报文之后，才解阻塞此端口，这样处理可以避免临时的环路发生。

13.4 参考信息

介绍该特性相关的参考信息。

本特性的参考资料清单如下：

- Extreme Networks IETF RFC 3619 EAPS

14 RSTP

关于本章

介绍 RSTP 特性的定义、目的、规格、原理以及参考的术语、缩略语和相关协议标准。

14.1 介绍
介绍该特性的定义、目的、规格和约束条件。

14.2 可获得性
介绍该特性需要的硬件支持，包括单板和终端。

14.3 原理描述
介绍该特性的实现原理。

14.4 参考信息
介绍与该特性相关的参考信息。

14.1 介绍

介绍该特性的定义、目的、规格和约束条件。

定义

STP（Spanning Tree Protocol）协议应用于环路网络，通过一定的算法实现路径冗余，同时将环路网络修剪成无环路的树型网络，从而避免报文在环路网络中的增生和无限循环。

RSTP（Rapid Spanning Tree Protocol）协议是生成树协议的优化版。其“快速”体现在根端口和指定端口进入转发状态的时延在某种条件下（端口快速进入转发状态条件，请参见“14.3 原理描述”）大大缩短，从而缩短了网络拓扑稳定需要的时间。

目的

STP 协议虽然能够解决环路问题，但是 STP 不能快速迁移。即使是在点对点链路或边缘端口，也必须等待 2 倍 Forward Delay 的时间延迟，端口才能迁移到转发状态。

RSTP 改进了 STP 协议，具有 STP 协议的所有功能，同时具备更快速的拓扑收敛特点。

规格

- 支持符合 IEEE std 802.1w 的 RSTP 协议。
- 端口状态分为 3 种：Discarding、Learning、Forwarding 。

术语

无。

缩略语

表 14-1 RSTP 特性缩略语表

缩略语	英文全称	中文全称
STP	Spanning Tree Protocol	生成树协议
RSTP	Rapid Spanning Tree Protocol	快速生成树协议

14.2 可获得性

介绍该特性需要的硬件支持，包括单板和终端。

支持本特性的单板有主控板 IPMB。

14.3 原理描述

介绍该特性的实现原理。

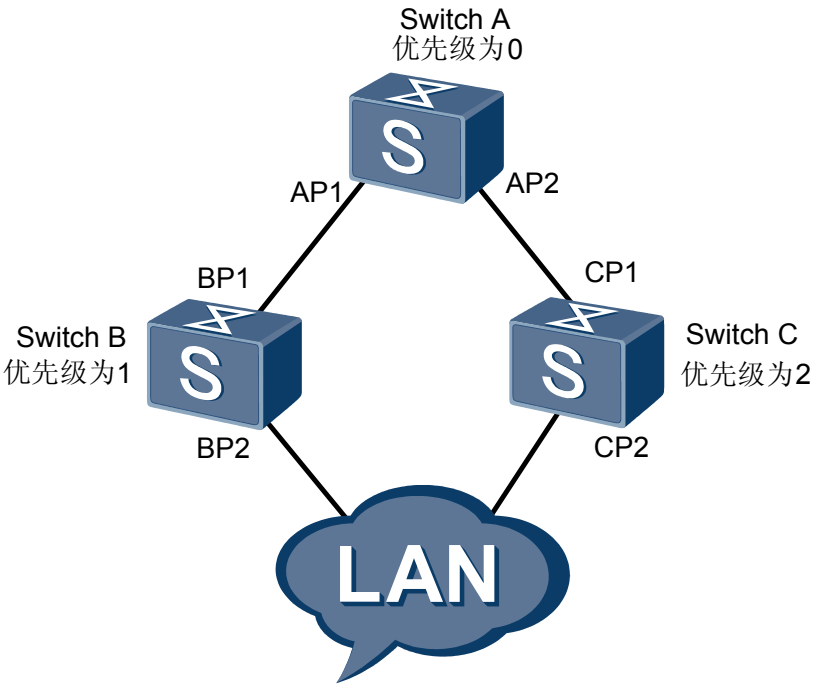
STP 基本原理

STP 通过在网桥之间传递一种特殊的协议报文（在 IEEE 802.1D 中这种协议报文被称为“配置消息”）来确定网络的拓扑结构。配置消息中包含了足够的信息来保证网桥完成生成树计算。

指定端口和指定网桥的含义，请参见下面的说明：

- 对一台网桥而言，指定网桥就是与本机直接相连并且负责向本机转发数据包的网桥，指定端口就是指定网桥向本机转发数据的端口。
- 对于一个局域网而言，指定网桥就是负责向这个网段转发数据包的网桥，指定端口就是指定网桥向这个网段转发数据的端口。

图 14-1 指定网桥和指定端口示意图



如图 14-1 所示，AP1、AP2、BP1、BP2、CP1、CP2 分别表示 Switch A、Switch B、Switch C 的端口，Switch A 通过端口 AP1 向 Switch B 转发数据，则 Switch B 的指定网桥就是 Switch A，指定端口就是 Switch A 的端口 AP1；与局域网 LAN 相连的有两台网桥：Switch B 和 Switch C，如果 Switch B 负责向 LAN 转发数据包，则 LAN 的指定网桥就是 Switch B，指定端口就是 Switch B 的 BP2。

生成树协议的配置消息传递机制如下：

1. 当网络初始化时，所有的网桥都将自己作为树根。
2. 网桥的指定端口以 HelloTime 为周期，定时发送本端口的配置消息；接收到配置消息的端口如果是根端口，则网桥将配置消息中携带的 MessageAge 按照一定的原则递增，并启动定时器为这条配置消息计时。
3. 如果某条路径发生故障，则这条路径上的根端口不会再收到新的配置消息，旧的配置消息将会因为超时而被丢弃，从而引发生成树的重新计算，得到一条新的通路替代发生故障的链路，恢复网络连通性。

不过，重新计算得到的新配置消息不会立刻就传遍整个网络，因此那些没有发现网络拓扑已经改变的旧的根端口和指定端口仍旧会按照原来的路径继续转发数据，如果新选出的根端口和指定端口立刻就开始数据转发的话，可能会造成暂时性的路径回环。

为此 STP 采用了一种状态迁移的机制，根端口和指定端口重新开始数据转发之前要经历一个中间状态，中间状态经过 Forward Delay 延时后才能进入转发状态，这个延时保证了新的配置消息已经传遍整个网络。

STP 缺陷

- 当拓扑变化或者链路故障时，端口从阻塞状态到转发状态需要两倍的 Forward Delay 延时，所以网络拓扑结构改变之后需要至少两倍的 Forward Delay 时间，才能恢复连通性。导致网络的连通性至少要几十秒的时间之后才能恢复。
- 整个桥接网络应用单一的生成树实例。当网络规模较大的时候，需要更长的收敛时间，同时会频繁的发生拓扑的改变。

RSTP 基本原理

RSTP 与 STP 相比，在以下三方面进行了改进：

- 为根端口和指定端口设置了快速切换用的替换端口（Alternate Port）和备份端口（Backup Port）两种角色。当根端口失效的情况下，替换端口就会快速转换为新的根端口并无时延地进入转发状态；当指定端口失效的情况下，备份端口就会快速转换为新的指定端口并无时延地进入转发状态。
- 在只连接了两个交换端口的点对点链路中，指定端口只需与下游网桥进行一次握手就可以无时延地进入转发状态。如果是连接了三个以上网桥的共享链路，下游网桥是不会响应上游指定端口发出的握手请求的，只能等待两倍 Forward Delay 时间进入转发状态。
- 直接与终端相连而不是把其他网桥相连的端口定义为边缘端口（Edge Port）。边缘端口可以直接进入转发状态，不需要任何延时。由于网桥无法知道端口是否是直接与终端相连，所以需要人工配置。

应用快速生成树协议的网桥可以兼容应用生成树协议的网桥，两种协议报文都可以被应用快速生成树协议的网桥识别并应用于生成树计算。

14.4 参考信息

介绍与该特性相关的参考信息。

本特性的参考资料清单如下：

- IEEE Std 802.1d, 1998 Edition, Spanning Tree Protocol
- IEEE Std 802.1w-2001, Rapid Spanning Tree Protocol

15 NTP

关于本章

介绍 NTP 特性的定义、目的、规格、原理以及参考的术语、缩略语和相关协议标准。

15.1 介绍
介绍该特性的定义、目的、规格和约束条件。

15.2 可获得性
介绍该特性需要的硬件支持，包括单板和终端。

15.3 原理描述
介绍该特性的实现原理。

15.4 参考信息
介绍与该特性相关的参考信息。

15.1 介绍

介绍该特性的定义、目的、规格和约束条件。

定义

NTP（Network Time Protocol）网络时间协议属于应用层协议，是用于在分布式时间服务器和客户端之间进行时间同步的，其实现基于 IP 和 UDP。NTP 协议从时间协议和 ICMP 时间戳报文演变而来，主要是从准确性和强壮性方面进行了特殊的设计。

目的

NTP 用来在整个网络内发布精确时间。

随着网络拓扑的日益复杂，整个网络内设备的时钟同步将变得十分重要。NTP 的目标是对网络内所有具有时钟的设备进行时钟同步，使网络内所有设备的时钟基本保持一致，从而使设备能够提供基于统一时间的多种应用。

UA5000 使用 NTP 功能，用以保证设备能够与网络中的其他设备时钟同步。

规格

- 支持 NTP Version3。
- 支持 NTP 客户/服务器服务方式。
- 支持 NTP 局域网广播服务方式。
- 支持 NTP 组播服务方式。
- 支持 NTP 时钟对等体服务方式。
- 支持时钟过滤和时钟选择。
- 支持本地时钟校准。
- 支持时钟源优先选择机制。
- 支持对参考时钟的支持。
- 支持 NTP 安全特性需求。
- 支持静态配置最多对等体个数为 128 个。
- 支持动态创建最多对等体个数为 100 个。

术语

表 15-1 NTP 特性术语表

术语	解释
层数	层数是 NTP 中一个比较重要的概念，代表了一个时钟的准确度。层数为 1 的时钟准确度最高，从 1 到 15 依次递减。
时间戳	每个 NTP 报文中都包含这四个时间戳，时间戳是 NTP 中实现时钟同步的基础。

术语	解释
时钟过滤	针对本地时钟的同一个对等体而言，用来从给定的对等体选择最好的时间样本。
时钟选择	针对不同的对等体（比如一个客户端可以配置多个服务器或者多个对等体），这样它分别向各个服务器和被动对等体发送时钟同步报文，在接收到应答报文后利用时钟选择算法选择出最好的时钟进行同步。

缩略语

表 15-2 NTP 特性缩略语表

缩略语	英文全称	中文全称
NTP	Network Time Protocol	网络时间协议
UTC	Universal Time Coordinated	世界调整时间

15.2 可获得性

介绍该特性需要的硬件支持，包括单板和终端。

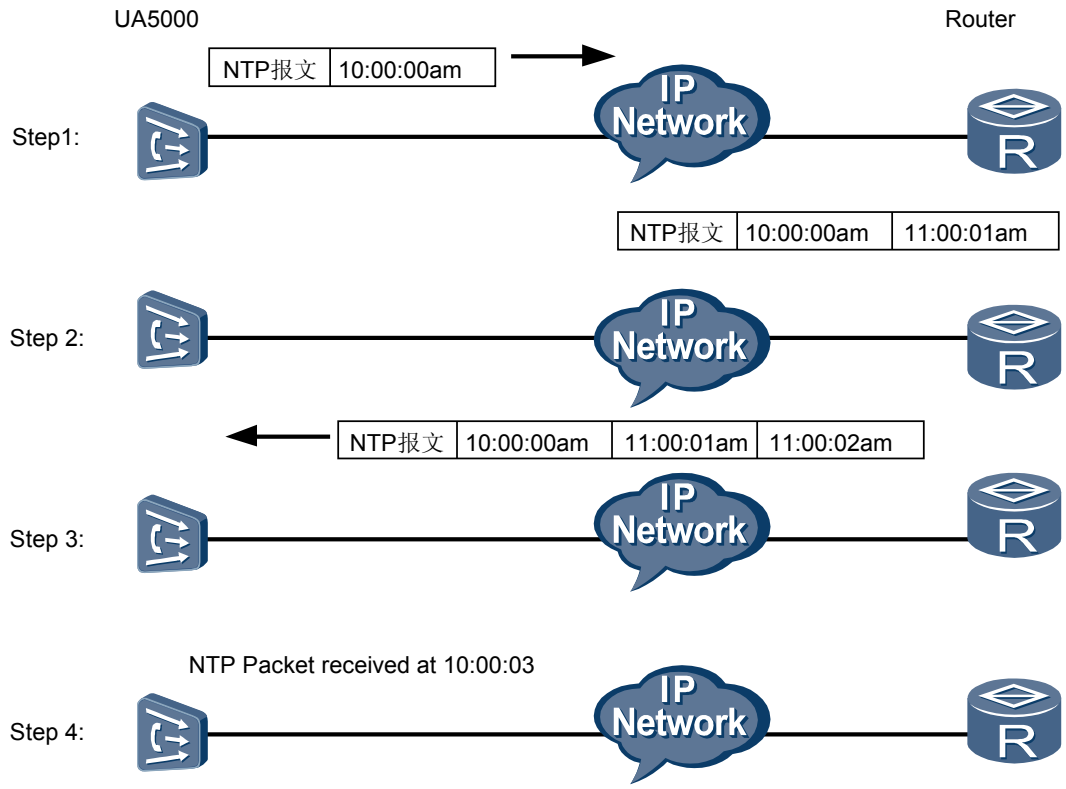
无需额外硬件支持。

15.3 原理描述

介绍该特性的实现原理。

NTP 的工作原理如图 15-1 所示，工作过程如下：

图 15-1 NTP 工作原理图



1. UA5000 发送一个 NTP 消息包给路由器，该消息包带有它离开 UA5000 时的时间戳，该时间戳为 10:00:00am（T1）。
2. 当此 NTP 消息包到达路由器时，路由器加上自己的时间戳，该时间戳为 11:00:01am（T2）。
3. 当此 NTP 消息包离开路由器时，路由器再加上自己的时间戳，该时间戳为 11:00:02am（T3）。
4. 当 UA5000 接收到该响应消息包时，加上一个新的时间戳，该时间戳为 10:00:03am（T4）。

至此，UA5000 已经拥有足够的信息来计算两个重要参数：

NTP 消息来回一个周期的时延 Delay=（T4-T1）-（T3-T2）

UA5000 相对 Router 的时间差 Offset=（（T2-T1）+（T3-T4））/2

这样 UA5000 就能够根据这些信息来设定自己的时钟，使之与 Router 的时钟同步。

15.4 参考信息

介绍与该特性相关的参考信息。

本特性的参考资料清单如下：

- RFC1305, Network Time Protocol (Version 3) Specification, Implementation and Analysis

16 组播

关于本章

组播是一种同时向多个接收者传输数据的通信方式。

16.1 介绍

定义

组播是一种同时向多个接收者传输数据的通信方式。

目的

设备采用组播技术为运营商提供 IP 视频业务，业务形式包括直播电视、准视频点播等。

通过组播技术的引入，在网络设备上可以完成 IP 视频业务的管理、控制和转发，满足运营商发放 IP 视频业务的需求。

16.2 规格

组播协议

- 不支持 IGMPv1
- 支持 IGMPv2
- 支持 IGMPv3，不支持 Exclude 模式
- 支持 IGMP Proxy
- 支持 IGMP Snooping
- 支持基于 VLAN 的组播（TR101 组播）

IGMP 性能

- 加入时延：小于 50ms
- 离开时延：小于 50ms

组播管理

- 支持 1024 个节目配置
- 支持 1024 个组播节目同时转发
- 支持 1024 个 xDSL 用户
- 支持 2000 个权限模板
- 每个用户最多可以绑定 64 个权限模板
- 每个用户最多可以同时观看 32 个不同的节目
- 支持 32 个预览模板
- 支持组播带宽 CAC
- 支持组播 CDR
- 支持 IGMP 报文统计
- 支持查询组播节目流量
- 支持 xDSL 的组播远程验收

组播组网

- 组播上行口和组播级联口支持聚合、保护

16.3 参考标准与协议

本特性的参考资料清单如下：

- TR101: Technical Report DSL Forum, TR-101 Migration to Ethernet-Based DSL Aggregation, April 2006
- RFC 1112 : Deering, S., "Host Extensions for IP Multicasting",STD 5, RFC 1112, August 1989
- RFC-2236: Fenner, W., "Internet Group Management Protocol, Version 2", RFC 2236, November 1997
- RFC 3376: B. Cain., "Internet Group Management Protocol, Version 3 ", RFC 3376,October 2002

16.4 可获得性

硬件支持

无需额外硬件支持。

说明

H601IPMD 单板不支持 MVLAN 方式的组播。

License 支持

- 设备可以接入的组播用户数量受 License 控制，只有获得了 License 许可后才能配置许可数量的组播用户。
- 设备接入用户可以配置或点播的组播节目数量受 License 控制，只有获得了 License 许可后才能配置或点播许可数量的组播节目。
- 设备只能使用上述两种方式之一进行 License 控制。

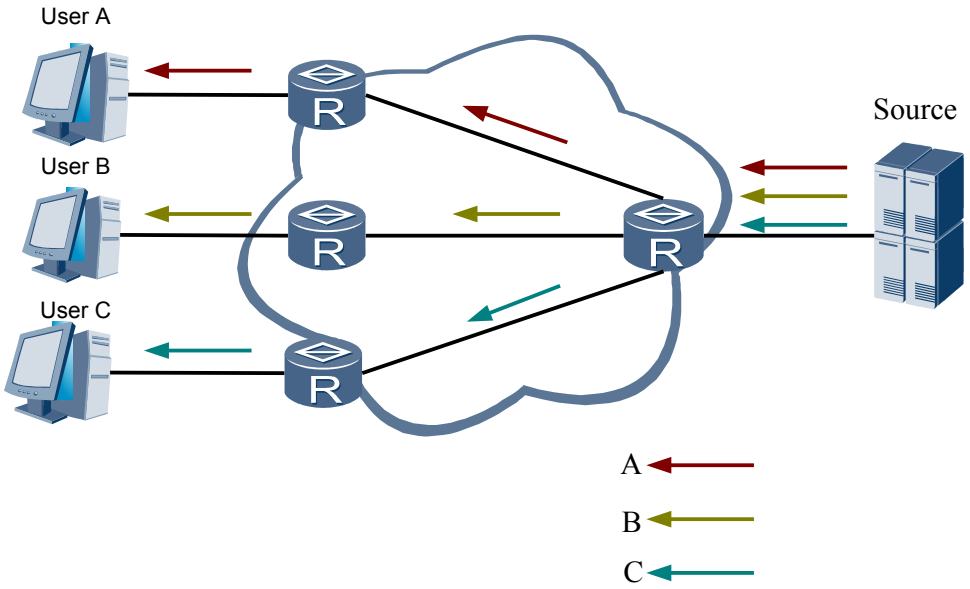
16.5 组播概述

组播与单播的差异

网络传输主要有三种基本形式：单播、广播和组播。

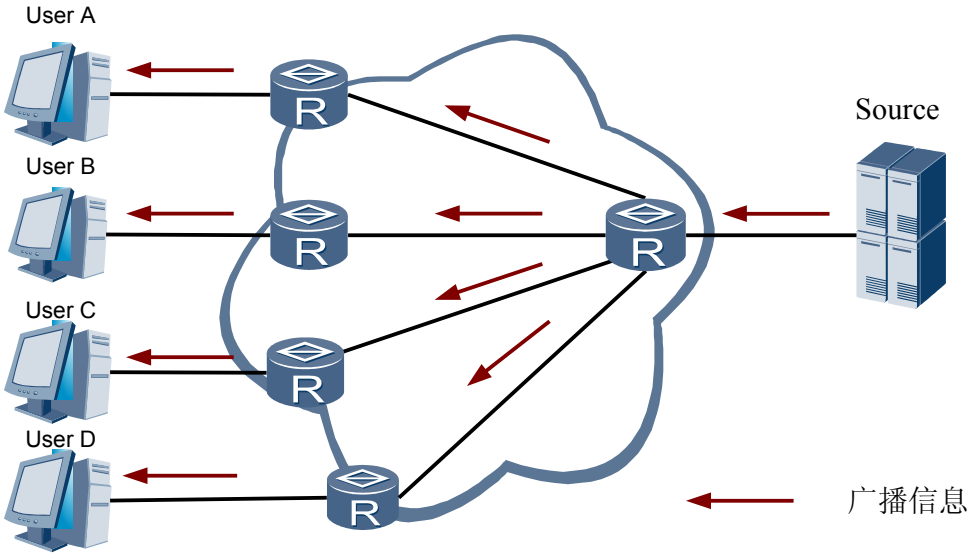
单播：实现点到点传输，只有一个发送者和一个接收者。

图 16-1 单播方式



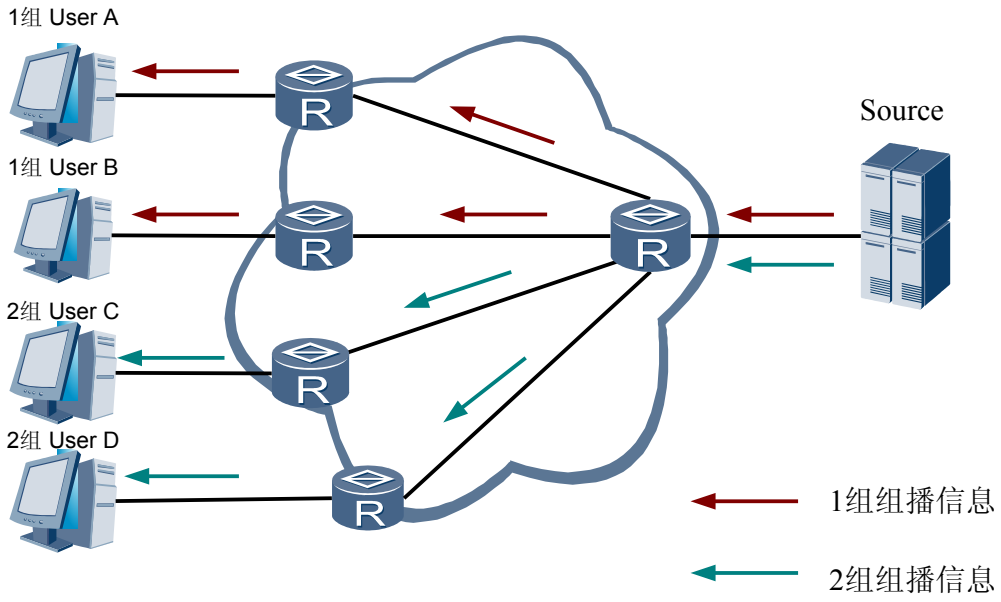
广播：实现点到所有点传输，只有一个发送者和局域网内所有的可达接收者。

图 16-2 广播方式



组播：实现点到多点传输，只有一个发送者和对该组播地址感兴趣的多个接收者。

图 16-3 组播方式



由上比较可知：

- 在组播方式下，单一的数据流被同时发送给一组用户，相同的组播数据流在每一条链路上最多仅有一份。相比单播来说，使用组播方式传递信息，用户的增加不会显著增加网络的负载，减轻了服务器和 CPU 的负荷。
- 组播报文可以跨网段传输，不需要此报文的用户不能收到此报文。相比广播来说，使用组播方式可以远距离传输信息，且只将信息传输到有接收者的地方，保障了信息的安全性。

综上所述，组播技术有效地解决了单点发送多点接收的问题，实现了 IP 网络中点到多点的高效数据传送。

组播术语

- 组播组

组播组使用一个 IP 组播地址标识。任何用户主机（或其他接收设备）加入一个组播组，就成为了该组成员，可以识别并接收以该 IP 组播地址为目的地址的 IP 报文。

- 组播源

以组播组地址为目的地址，发送 IP 报文的信源称为组播源。一个组播源可以同时向多个组播组发送数据。

- 组播组成员

组播组中的成员是动态的，网络中的用户主机可以在任何时刻加入和离开组播组。组成员可能广泛分布在网络中的任何地方。

组播源通常不会同时是数据的接收者，不属于组播组成员。

- 组播复制

组播复制是指网络设备支持把入口一份组播报文复制多份到多个出口的能力。为了实现海量数据的有效传输只能由硬件实现。

下文类比收看某电视频道的节目，可以帮助理解 IP 组播中的概念。

- 组播组是发送者和接收者之间的一个约定，如同电视频道。
- 电视台是组播源，它向某频道内发送数据。
- 电视机是接收者主机，观众打开电视机选择收看某频道的节目，表示主机加入某组播组；然后电视机播放该频道电视节目，表示主机接收到发送给这个组的数据。
- 观众可以随时控制电视机的开关和频道间的切换，表示主机动态的加入或退出某组播组。

组播地址

为了让组播源和组播组成员进行通信，需要提供网络层组播地址，即 IP 组播地址，同时必须存在一种技术将 IP 组播地址映射为链路层 MAC 组播地址。下面分别介绍这两种组播地址：

- IP 组播地址

根据 IANA（Internet Assigned Numbers Authority）规定，组播报文的目的地址使用 D 类 IP 地址（从 224.0.0.0 到 239.255.255.255），且 D 类地址不能出现在 IP 报文的源 IP 地址字段。其中，224.0.0.0 到 224.0.0.255 网段地址被预留给本地网络中的网络协议使用；239.0.0.0 到 239.255.255.255 网段地址属于管理范围地址（之所以定义管理范围地址主要为了方便把该组播限制在确定的组播域范围内，保证不同域的地址重用）。

组播地址并不是用于分配给接收设备或者组播源设备进行网络位置标识；对于组播源，是使用分配的组播地址进行组播数据的生成和承载，对于接收者，通过该地址对组播数据进行识别。

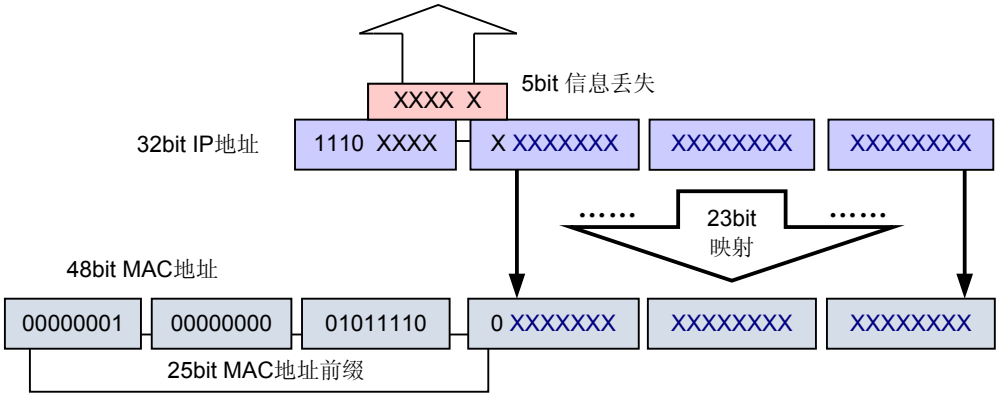
对于一个真实的组播应用，通常不需要手工输入组播地址。比如常见的直播电视，都有一个菜单界面，当通过遥控器点播时，应用软件会自动提取节目对应的 IP 组播地址。

- 以太网组播 MAC 地址

以太网传输单播 IP 报文的时候，目的 MAC 地址使用的是接收者的 MAC 地址。但是在传输组播报文时，传输目的不再是一个具体的接收者，而是一个成员不确定的组，所以使用的是组播 MAC 地址。

IANA 规定，组播 MAC 地址的高 25bit 为 0x01005e，MAC 地址的低 23bit 为组播 IP 地址的低 23bit，映射关系如图 1-4 所示。

图 16-4 组播 MAC 地址与 IP 地址映射关系



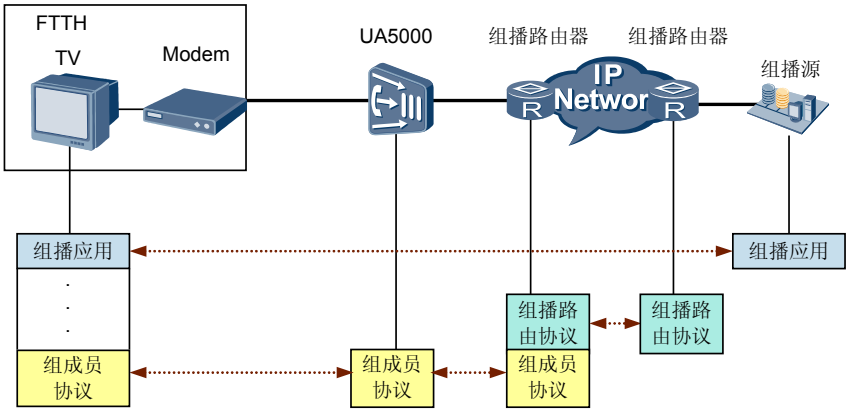
由于 IP 组播地址的前 4bit 是 1110，代表组播标识，而后 28bit 中只有 23bit 被映射到 MAC 地址，这样 IP 地址中就有 5bit 信息丢失，直接的结果是出现了 32 个 IP 组播地址映射到同一 MAC 地址上。

组播业务

组播属于一种端到端服务，一项组播应用的开展需要网络上各设备承担不同的角色来共同完成。

组播业务组网如图所示。

图 16-5 组播业务应用



组成员协议：常用于路由器和主机之间，允许用户主机动态加入和离开某组播组，实现组播成员管理。

组播路由协议：常用于路由器之间，构建报文分发树进行组播路由，从组播源传输报文到接收者。

组播应用：基于 TCP/IP 协议栈之上的组播源与接收者的视频等组播应用软件。通常所说一次频道切换包含 2 个协议动作——发送离开旧组播组，同时发送加入新组播组。

IGMP 协议

IGMP(Internet Group Management Protocol)是用于维护主机和路由器之间组播组成员关系的协议。IGMP 目前包含三个版本，分别是 v1、v2 和 v3，而且新版本完全兼容旧版本。v1 已经鲜有系统支持，所以按照 TR101 要求设备已经不再兼容——丢弃 v1 报文。

此处以 IGMPv2 为例介绍协议的主要内容。

表 16-1 IGMP 报文

角色	报文类型	说明
路由器	通用查询	通过周期发送该报文来维护与之相连的所有主机的对全部组播组的需要。通过老化机制来发现意外掉线的主机。
	特定组查询	通过该报文来确定某个组播组是否还有主机需要。通常是在路由器收到离开报文时发送。

角色	报文类型	说明
主机	报告	主机主动加入一个组播组，或者对通用查询和特定组查询的响应。
	离开	主机主动通知路由器不再需要某个组播组。

IGMPv3 包含 v2 的基本概念，详见“IGMPv3”。

16.6 组播实现原理

16.6.1 基本管理对象

基本组播管理对象是指最简化的组播管理元素，换句话说，就是在设备单个组播 VLAN 内开展组播业务必不可少的配置对象。

组播节目

组播节目就等同于组播组，其最基本的属性就是组播 IP。设备可以通过该对象进行更精细的管理，比如权限控制、CAC 等。

根据在业务发放前，是否预先配置每个节目的组播 IP 等节目属性，节目可以分为 2 类：预配置节目和动态节目。关于动态节目详见“动态节目”。

组播上行口

组播上行口是组播源与设备相连的端口，同时也是上层组播路由器和设备相连的端口。

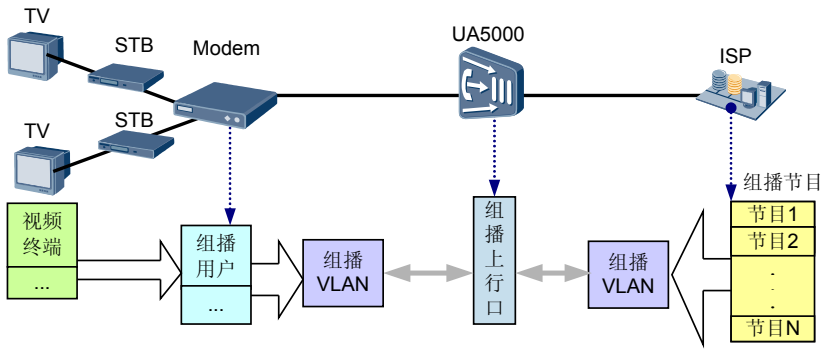
根据是否依赖链路层环路协议，上行口可以分为 2 类：手工配置上行口和动态上行口。关于动态上行口详见“上行口环网”。

组播用户

组播用户就是组播数据的接收者，必须为其配置一个上行承载组播控制报文的业务流（设备可以通过流分类识别出该用户），所以它是对应一个唯一的终端或发放用户。同时，必须为组播用户指定一个组播 VLAN，即该发放用户隶属于哪个 ISP。

基本对象之间的关系如图 16-6 所示。

图 16-6 组播管理对象

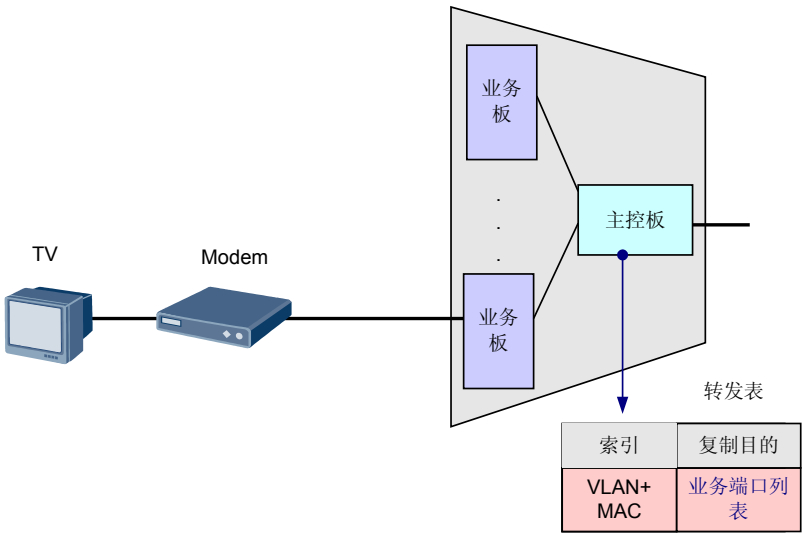


16.6.2 设备转发框架

介绍组播的硬件转发面框架。

组播转发表

图 16-7 组播转发表



UA5000 支持由主控板进行转发。主控板以(VLAN+MAC)为索引，按需复制给对该节目感兴趣的组播用户。

16.6.3 IGMP 控制框架

介绍 IGMP 报文的控制面框架，以 IGMP Proxy 为实例。

IGMP Proxy

组播代理（IGMP Proxy）指在树型网络拓扑下，设备不对组播转发建立路由，只负责对组播协议报文的代理功能，具体如下：

- 从终端的角度看，设备是一台组播路由器，完成 IGMP 协议中路由器部分的功能：固定充当用户侧网路的 IGMP 查询器（为了安全起见，不支持查询器选举）；接收并终结所有组播用户的加入和离开报文，根据维护的组成员关系表只把组播节目复制给感兴趣的组播用户。

表 16-2 组成员关系表结构

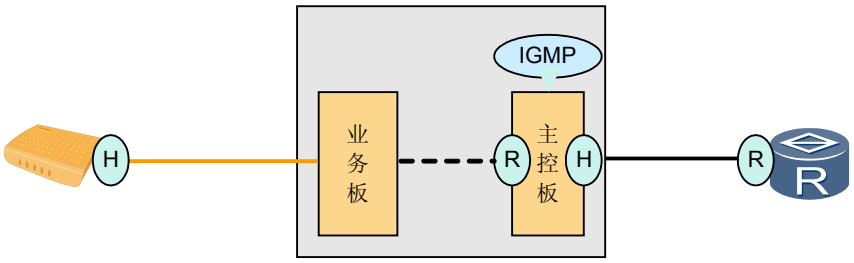
索引	在线成员
VLAN+IP	组播用户列表（比如组播用户 1、组播用户 2）

- 从组播路由器来看，设备是一个组播组成员，完成 IGMP 协议中主机部分的功能：根据组成员关系表的记录变化——新增或删除，从组播上行口向上发送节目的加入或离开报文；另外，根据组成员关系表的状态响应组播路由器的查询。

所以，采用 IGMP Proxy，可以有效减少了网络侧的 IGMP 报文的交互数量，减轻组播路由器的负荷。下行 IGMP 通用查询报文是向所有组播用户发送还是只向感兴趣的组播用户发送，设备是可以配置的。

IGMP 协议栈架构

图 16-8 IGMP 协议栈架构



R 代表 IGMP 协议的路由器功能，H 代表 IGMP 协议的主机功能。

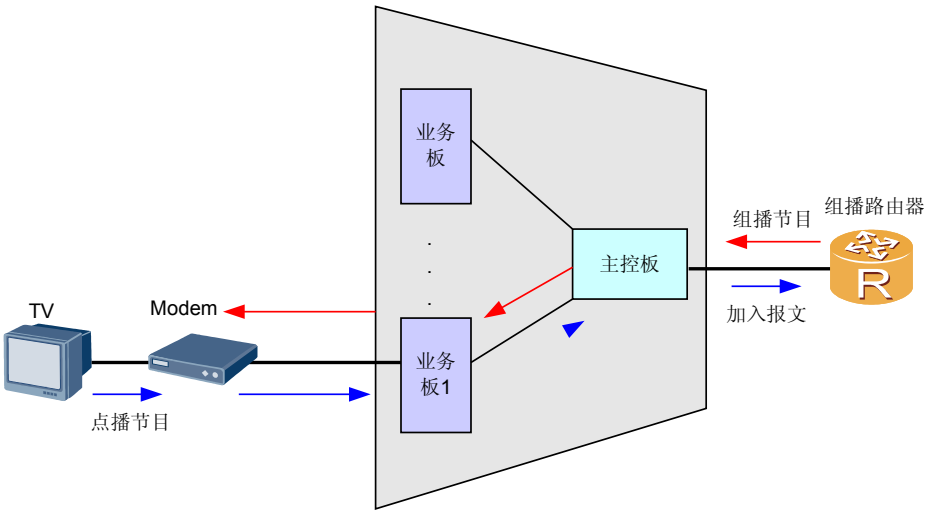
IGMP 协议栈架构：在主控板，网络侧可以基于 MVLAN，也可以基于非 MVLAN；用户侧基于组播用户——保证各个用户之间的控制面互不干扰。

16.6.4 组播转发流程

以 IGMPv2 Proxy 为例，结合管理面、控制面和转发面介绍组播整体转发流程。

加入流程

图 16-9 加入流程



1. 组播用户切换频道，发送点播新节目 IP1 的加入报文。
2. 主控板接收加入报文，进入该用户的 IGMP 协议栈，通过组播控制（详见“组播CAC”）后，在主控板创建如下的组成员关系表。

索引	在线成员
MVLAN1+IP1	组播用户 1

- 同时在主控板创建如下组播转发表（如何把 IP1 映射到 MAC1，详见“组播地址”）。

索引	复制目的
MVLAN1+ MAC1	用户端口 1

3. 然后主控板从 MVLAN1 的组播上行口向组播路由器发送加入报文。
4. 当设备收到组播流后，主控板按组播转发表复制到用户端口 1。

说明

虽然组播用户对应的 SVLAN 不同于 MVLAN，但是设备可以通过组播成员配置关系实现到 MVLAN 的映射，自然支持跨 VLAN 的组播，不需要额外配置。

离开流程

离开报文的处理流程与加入流程的步骤相同，仅仅是动作不同。具体可以参见“快速离开”。

查询流程

根据 IGMP 协议，需要通过通用组查询维护组播用户的状态，避免因为组播用户静默离开而没有删除表项。所以，主控板会按照配置的查询间隔依次发送通用组查询报文给所有组播用户（为了节约性能可以配置只查询在线组播用户），如果主控板在配置老化时间内（健壮性系数×查询间隔+最大响应时间）没有收到用户的报告报文则分别删除组播关系表和组播转发表中该组播用户对应的表项。

特定组查询报文的发送流程类似，不再赘述。

组播路由器查询流程

设备收到组播路由器发送的通用组查询报文，主控板首先会查询组成员关系表，在对应的 MVLAN 内是否还有在线的业务板，如果有则代理对应的业务板一一发送报告报文回应组播路由器的响应。

特定组查询报文的处理流程类似，不再赘述。

16.7 高级组播技术

16.7.1 业务发放

多实例组播

随着开放网络的推行，运营商网络需要给不同的组播内容提供商（ISP）提供独立的组播域，避免不同 ISP 之间的干扰。在设备上通过不同组播 VLAN 的划分在管理面、控制面和转发面实现各自独立的组播域。

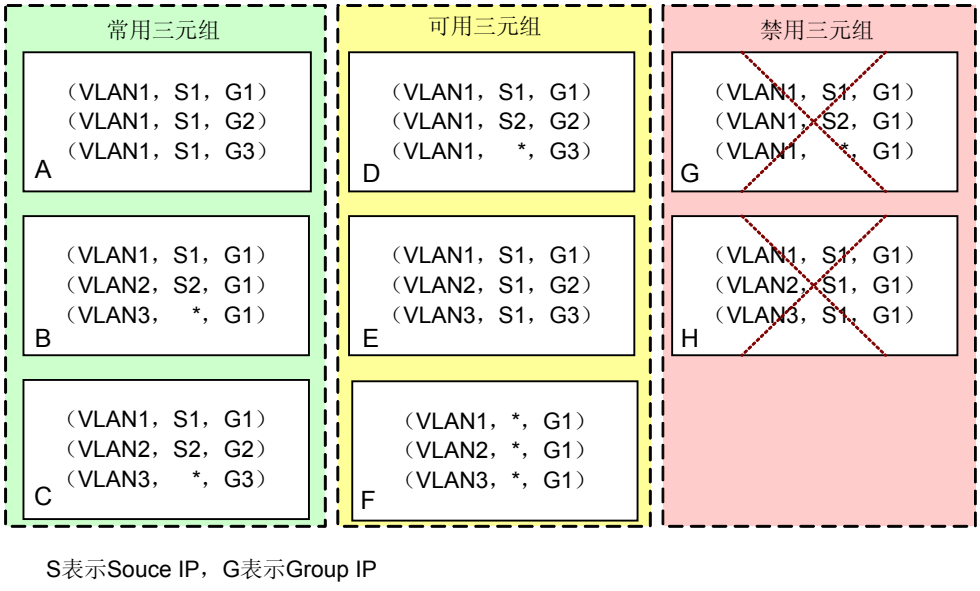
- 管理面

  在每个 MVLAN 内，可以配置每个 ISP 需要发放的组播节目、组播上行口和组播用户。这里特别强调组播节目，为了保证每个 ISP 可以独立的规划各自组播节目，组播节目三元组（组播 VLAN，源 IP，组播 IP）需要满足以下规则：

  - 如果 2 个 IP 映射到同 1 个 MAC（映射方法参见“组播地址”），则判断时认为是同一个 IP；
  - 为了保证转发面上组播转发表项的唯一性，必须保证（组播 VLAN，组播 IP）的唯一性；
  - 为了保证控制面 IGMPv3 报文的点播节目的唯一性，必须保证（组播 IP，组播源 IP）的唯一性。
  - 特别的，对于 IGMPv2 报文或者 ASM 模式的 IGMPv3 报文就相当于组播源 IP 等于任意值（常表示为*或 any），此时只要满足第二条即可。

  以下图中的子图 G 为例，由于第二条规则要求（组播 VLAN，组播 IP）唯一，而子图 G 中（VLAN1，G1）并不唯一，所以子图 G 是禁止配置或生成的。其他的子图也可以按照上述 4 个规则来判断。

图 16-10 组播节目三元组示例



- 控制面

  在网路侧，每个 MVLAN 都有独立的 IGMP 协议栈——每个 ISP 可以选择协议的版本、报文优先级和 Proxy 或 Snooping。在用户侧，每个组播用户都有独立的 IGMP 协议栈，不会受其他组播用户的影响。

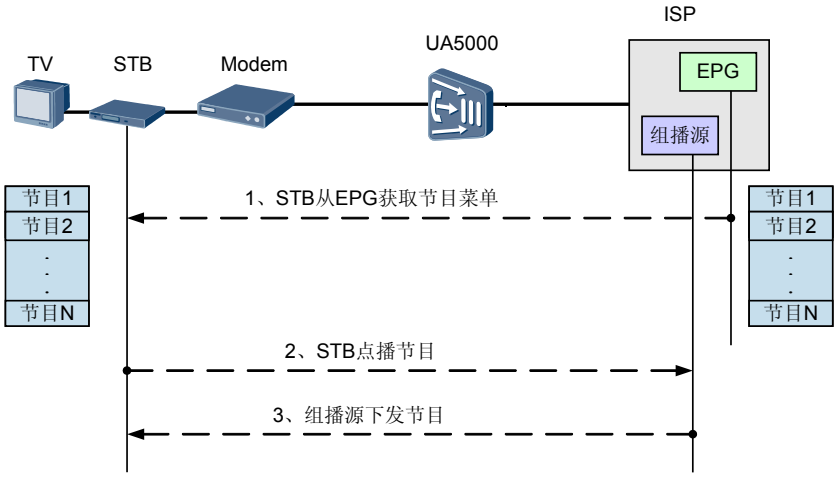
- 转发面

  在转发面上，组播转发表都是以组播 VLAN 和组播 MAC 为索引，保证了不同组播 VLAN 间不会互相干扰。详见“组播转发表”。而对于在主控板、业务板上不同组播 VLAN 的流量在同一个端口的 QoS 调度等同于单播，详见“QoS”。

动态节目

在现实应用场景中，如果不需要在设备上进行精细化的管理，那么可以使用动态节目，来免去节目频繁变更带来的维护麻烦。此时节目的维护可以统一到 EPG（Electronic Program Guide）系统上。

图 16-11 动态节目生成流程



1. STB 在启动后会自动从 EPG 服务器上获取节目菜单信息，并呈现给用户。
2. 用户点播节目，会产生相应的 IGMP 报文发送给设备。所以，此时设备上的节目信息不是管理员输入的，而是从组播用户实时的 IGMP 报文中把组 IP 和源 IP 提取出来，并在组播用户所在的 MVLAN 内动态生成的。
3. 组播源组播节目到达 STB。

   为了防止用户使用不合适的组 IP，也可以在设备上基于 MVLAN 为动态节目配置合法的组播地址范围，只有符合该范围才会生成组播节目，否则用户的 IGMP 报文会被丢弃。除了范围匹配之外，实际可以动态生成的节目数量受到硬件规格和 License 限制。

   动态节目不支持在设备上的精细管理，包括：CAC、权限管理、组播预览和预加入节目。

权限管理

通过把不同的组播节目划分到不同的模板，可以在设备上提供基于套餐的权限管理方式。

- 权限模板

  在每个模板中都可以指定任何组播节目的权限，并为之命有意义的名字。其中权限包括 4 种类型：

  禁止：表示不允许组播用户以观看和预览方式点播该组播节目。

  预览：表示组播用户可以点播该组播节目，但是观看时长和次数受限。

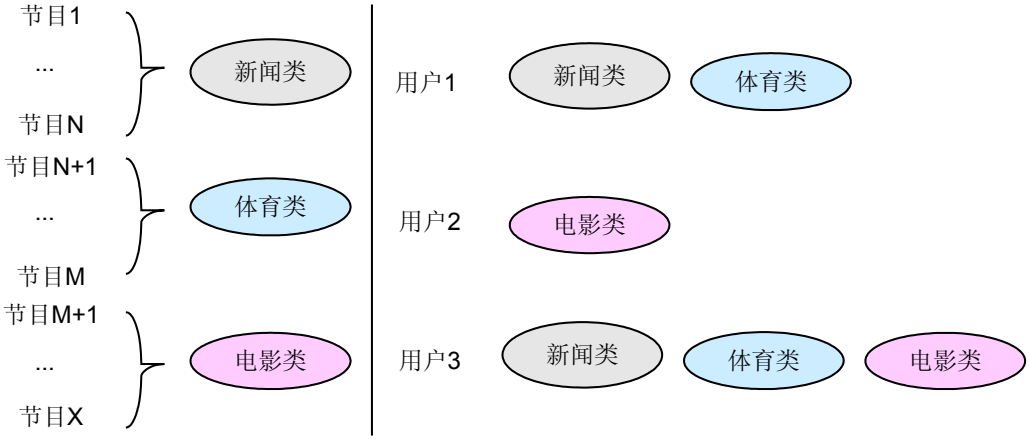
  观看：表示组播用户可以正常点播该组播节目，没有任何限制。

  无权限：是模板的默认值，表示未为该组播节目分配具体权限，效果等同于“禁止”。

  运营商可以按照自定义的规则进行模板的规划，常见有 3 种方式。

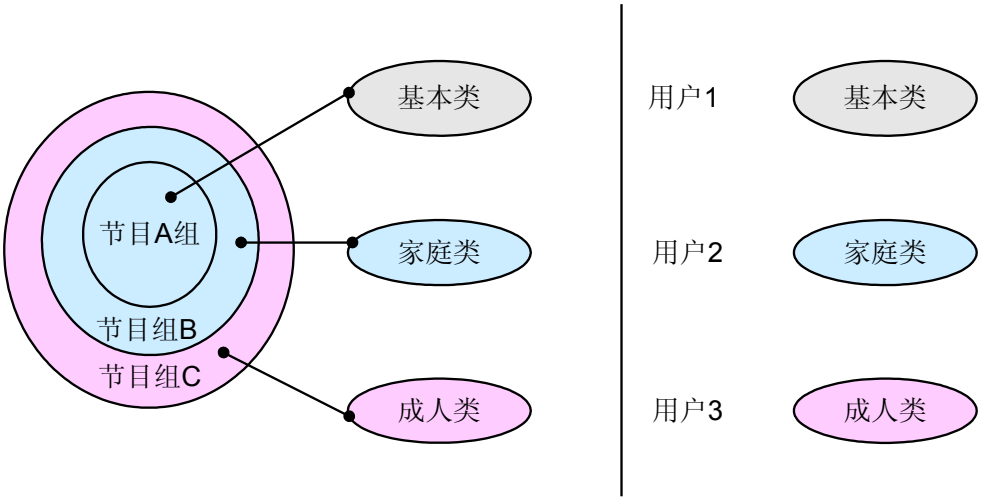
  - 第一种是以内容差异进行划分，比如划分为新闻类、体育类、电影类。此时，一个组播节目只会属于一个模板，不存在模板间节目的重叠。所以，一个用户通常会绑定多个模板。如图 16-12 所示。

    图 16-12 权限模板第一种划分示例

  - 第二种是以包含内容多少进行级别划分，比如划分为基本类、家庭类、成人类。此时，一个组播节目可能会属于多个模板，模板间存在重叠。所以，一个用户通常只会绑定一个模板。如图 16-13 所示。

    图 16-13 权限模板第二种划分示例

- 第三种是第一种和第二种的混合，这种使用方式最复杂也最灵活。此时，组播节目存在重叠且一个用户也会绑定多个模板。为了保证多个权限模板对同一个节目叠加后得到运营商想要的结果，需要配置模板中权限的优先级，该配置建议在开局之初就规划好，避免变化带来不正确的结果。例子如下。

表 16-3 权限优先级例子：禁止>预览>观看>无权限

模板 1	节目 1：观看	用户 1	节目 1：禁止
模板 2	节目 1：禁止		

表 16-4 权限优先级例子：观看>预览>禁止>无权限

模板 1	节目 1：观看	用户 1	节目 1：观看
模板 2	节目 1：禁止		

- 权限控制

  可以通过以下 2 个步骤来配置每个组播用户的权限：

  1. 规划所有组播节目的权限模板。
  2. 按用户订阅的服务内容来绑定需要的权限模板。

     设备提供开放的 MIB 接口来提供以上操作。

     另外，权限的控制还有一种常用方式——通过头端系统和 STB 的加密来实现，此时就不需要在设备上进行权限管理，运营商可以通过系统级或组播用户级配置把权限控制功能关闭。

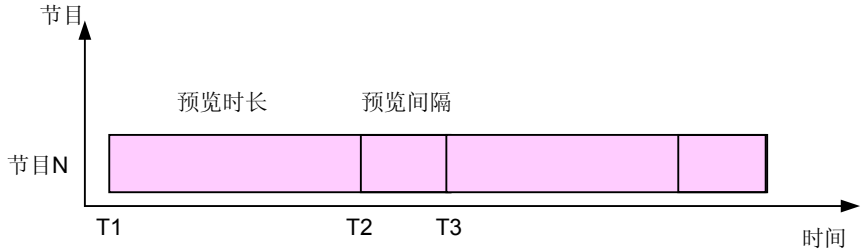
组播预览

通过给组播用户提供某些特色频道的预览功能，来吸引用户订购更多的节目观看权限，达到推销的目的。

设备是通过预览模板来管理每个组播节目的预览参数，也就是说，每个组播节目可以绑定一个预览模板来配置预览参数，类似的节目可以绑定到同一个预览模板来简化管理。

预览模板包括 3 个预览参数。

图 16-14 预览参数



T1：第一次预览开始时间点

T2：第一次预览结束时间点

T3：第二次预览开始时间点

- 预览间隔：两次预览最小时间间隔要求，间隔跨度为新点播开始到上次点播结束（如图就是从 T2 到 T3）；如果用户两次预览该节目的时间间隔未达到该时间间隔，则暂时不能再次预览该节目。可以保证用户不会出现“流氓”行为——通过不断预览同一个节目来达到不订阅“观看”权限的目的。
- 预览次数：限制组播用户对同一个节目一天最多可以预览多少次，当离开该节目后增加 1 次计数；超过该次数后，用户点播请求将会被拒绝——等同于权限降级为“禁止”，但第二天可以恢复。
- 预览时长：限制组播用户对同一个节目一次最长可以观看多久，从点播开始计算（如图就是从 T1 到 T2）；超过该时长后，用户将接收不到该组播节目数据。

组播用户预览的访问控制可以参见“权限管理”。

组播 CAC

CAC（Call Admission Control）是呼叫准入控制，这里是特指 IGMP 会话建立的控制，如果会话建立不成功则组播用户就不能接收到请求的组播节目。

从广义上看，CAC 控制首先要通过系统一级控制，目前包括：

- 防御 DoS 攻击。来自用户侧的 IGMP 报文速率不能超过系统限制，否则也会被认为是 DoS 攻击而被丢弃；当然，不仅仅是针对 IGMP，而是包括 DHCP、PPPoE 等控制报文。详见“防御 DoS 攻击”。
- 防御 IP 欺骗。打开该功能后，用户进行正常点播前，必须先通过 DHCP 获得合法的 IP 地址，然后以合法 IP 地址为源 IP 的 IGMP 报文才会被系统接受，否则会被认为是非法用户而被丢弃。详见“防御 IP Spoofing”。
- 宽带报文过载。当出现大量业务时，系统资源不足以支撑所有业务，会按定义的策略进行丢弃保证部分高优先级业务不受影响。在这种情况下，为了减轻系统的负荷，IGMP 报文有可能被“牺牲”。详见“宽带报文过载”。

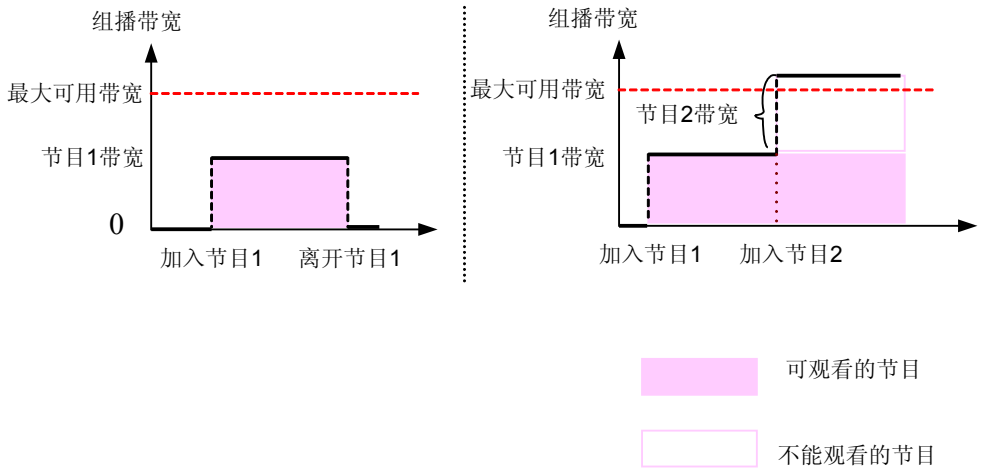
其次，才是组播一级控制，包括：

- 组播用户并发节目数，限制一个组播用户下可以同时点播多少个频道，可以基于组播用户配置。
- 权限控制，参见“权限管理”。
- 带宽校验。虽然设备支持对各种流量的 QoS 控制，但是在某个传输点出现带宽过载，就会出现丢包（按优先级丢或尾丢弃），可是由于组播节目实时性、不可重传的特质决定事后 QoS 的做法，直接造成所有被丢包节目的花屏（而不只是新点节目），不能很好满足 IPTV 高质量体验的要求。而带宽校验可以事前控制新点频道，保证已点频道的带宽充裕——不受影响，这样受影响的就只有新点节目不能观看。

系统支持组播用户带宽 CAC。

首先为每一个预配置节目配置带宽（可以参考视频的码流，再加上报文封装、网络传输抖动的余量；如果有实测的网络流量就更合适）；然后为每一个组播用户配置可用带宽（可以参考实际线路带宽或者业务发放的规划）。这样，当设备收到节目的第一个 IGMP 加入报文，就会从该用户的可用带宽减掉相应节目的所占带宽，如果余数小于 0 则拒绝用户的点播请求；如果收到一个 IGMP 离开报文，就可以归还相应节目的带宽给该用户（归还的时刻是在停止转发组播数据时，即该终端下没有任何终端用户需要该节目，参见“快速离开”）。

图 16-15 组播用户带宽 CAC



该功能可以基于系统级或用户级配置。

计费模式

对于组播业务，运营商或内容提供商通常有 2 种计费模式：

- 固定计费：就是将节目分成不同的套餐，不同套餐在固定的周期（比如年、月）上收取确定的费用，这种方式就不限制组播用户的点播次数或点播流量。
- PPV（Pay Per View）：就是根据不同的节目的点播次数进行费用收取。

对于第一种，由于是固定收费，和组播用户的行为无关，所以，设备天然支持，不需要提供额外的功能。

对于第二种，设备可以记录每个组播用户的点播行为，并以 CDR（Call Detail Record）方式提供给计费系统进行费用结算。完整 CDR 功能配置包含 3 步：

1. 使能日志功能，开关可以基于组播用户、组播节目（预配置节目可配置，动态节目默认打开）或系统级配置；当用户产生一个完整的观看行为——从点播开始到点播结束，或者未通过组播 CAC 造成点播失败，就会产生日志。

   说明

   系统可以记录 10K 条组播日志，记满后会覆盖旧的记录；所以为了避免用户快速浏览频道而消耗大量日志资源，可以配置日志生成的标识时间——如果组播用户观看频道的时长小于该值，则不会产生日志。相反，为了及时记录长时间用户在线的日志，当用户在线时间超过配置值，设备会自动生成日志。

2. 配置文件服务器：选择 CDR 的传输协议，可以在 TFTP/FTP/SFTP 中选择；配置主备服务器的 IP 地址等。
3. 使能 CDR 功能（系统级配置）。使能后，设备会在满足上报 2 个条件之一后——达到上报的时间间隔或者达到上报的日志数量阈值，自动把需上传的日志合成为一个文本文件传送给文件服务器。

   文本文件名的格式为：HWCDR-主机名称-YYYYMMDDHHMMSS.txt

图 16-16 文本文件的格式

表 16-5 CDR 项目具体格式

ID	Field Name	Specification	Commentary
0	TAG	3 Bytes	Fixed as “Log”. “Log” is the module name which generate syslog
1	SN	0..5 Bytes	Using a 16 bit variable to record. The max value is “65535” which occupies 5 Bytes
2	FrameSlotPortGemport	5..13 Bytes	F/S/P/GemPort for GPON user
	FrameSlotPortFlow	5..14 Bytes	F/S/P/FlowID for xDSL user
3	ProgramIP	0..15 Bytes	Sample: 239.1.1.1
4	OperMode	0..1 Bytes	0-Watch; 1-Preview; 2-No Right; Other is invalid
5	StartDate	0..18 Bytes	YYYY-MM-DD HH:MM:SS
6	EndDate	0..18 Bytes	YYYY-MM-DD HH:MM:SS
7	ProgramName	0..16 Bytes	Sample: cctv1, if program is not exist, this parameter is “No-Name”
8	ProgramSrcIP	0..15 Bytes	Sample: 192.168.1.1, if the IP is invalid, this parameter is “*”
9	Reason	1..2 Bytes	Syslog generation reason: 11: User’s online time is too long 0: User leave.

点播行为分析

相对于传统的电视业务，IP 组播业务的点播行为可以得到更精确的统计和分析，包括热点节目统计、用户兴趣分析、点播高峰时段等。对此，设备需要准确记录每个用户的点播行为作为日志，并以开放的接口输出该日志内容。根据不同的输出方式，设备有 2 种方法：一种是 CDR；另外一种是 syslog（RFC 3164）。两者组播部分的格式是一致的，参见“计费模式”；两者的优劣详见下表。

表 16-6 两种日志传输的优缺点

	优点	缺点
CDR	传输可靠，可以选择 TFTP、FTP 或 SFTP 作为承载协议	只有在满足上报条件时（达到上报间隔或上报数量阈值），才传输给文件服务器
syslog	上报及时，产生后立即上传 syslog 服务器	传输不可靠，syslog 是 UDP 协议

组播验收

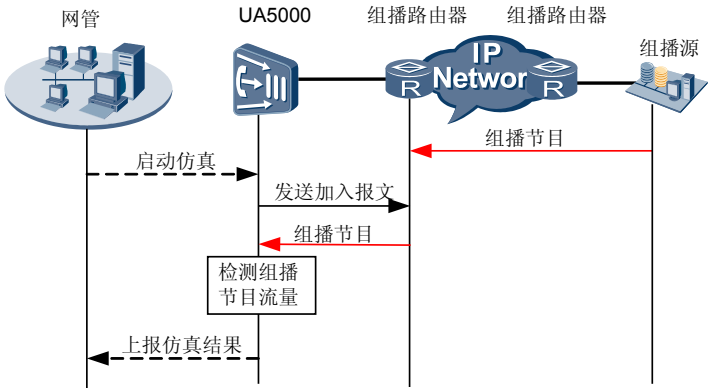
在完成站点的建设后，通常会进行站点的测试验收。测试验收主要目的是检查工程安装工艺和质量（硬件的连通性）、验证设备配置（软件配置和外部对接参数的正确性）。

在 BMS 上，操作员通过以下几步配置实现高效率、低成本的验收。

1. 远程配置接入设备数据
2. 启动仿真，可以多个设备并行仿真
3. 自动获得仿真结果，无需人工干预

   其中，组播仿真的流程如下：

图 16-17 启动组播仿真流程



基于方案的限制，组播仿真可以验收的仿真项目如下：

	验收项目	可仿真项目	不可仿真项目
组播业务	组播业务 用户 CAC 控制	网络侧组播网络的硬件连通性 接入认证 网络侧组播网络的业务连通性 组播业务通道配置的正确性	用户端口 实际速率

同时，以上组播仿真功能设备提供开放的 MIB 接口供第三方进行二次开发。

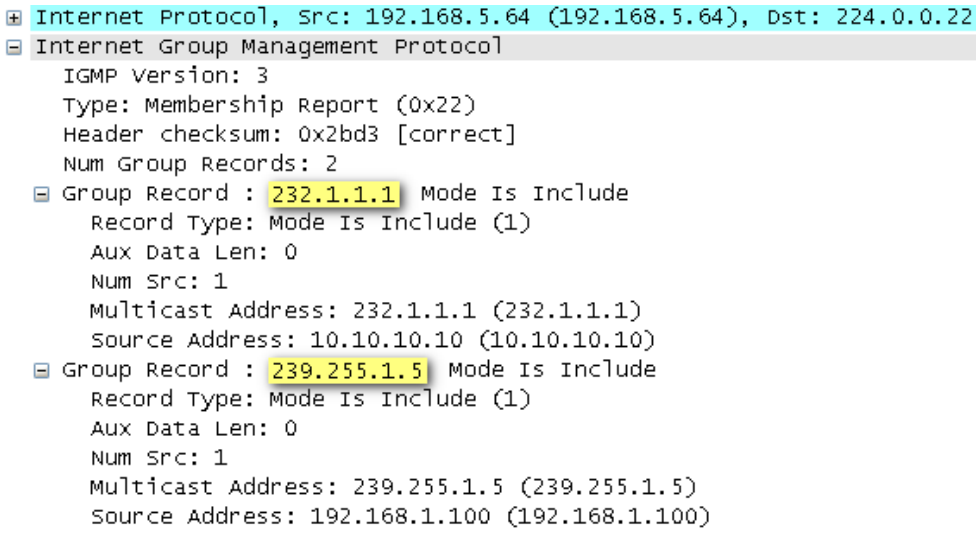
16.7.2 协议对接

IGMPv3

IGMPv3 是在 RFC 3376 中定义的，相比 IGMPv2（RFC 2236）主要有以下改进点：

- 批量报告：报告报文的目的 IP 地址固定填写为 224.0.0.22，同时 IGMP 净荷可以携带多条组记录信息，可以减少设备间报告报文个数。如下图所显示的抓包工具中的 IGMP 报文携带了 232.1.1.1 和 239.255.1.5 两个组的信息。而 IGMPv2 目的 IP 必须填写为相应的组 IP，所以无法实现携带多个组记录信息。

图 16-18 IGMPv3 报告报文示例



- 查询报文中最大查询响应时间支持范围从 IGMPv2 的 25.5 秒扩大到 3174.4 秒，从而使 IGMP 能够适应更大的网络规模。
- 支持源过滤功能，所谓源过滤：指主机能指定接收或不接收来自特定组播源 IP 地址的组播数据。而 IGMPv2 只支持 ASM。下面通过不同报文类型的说明，来解释源过滤功能的实现。
  - 查询报文

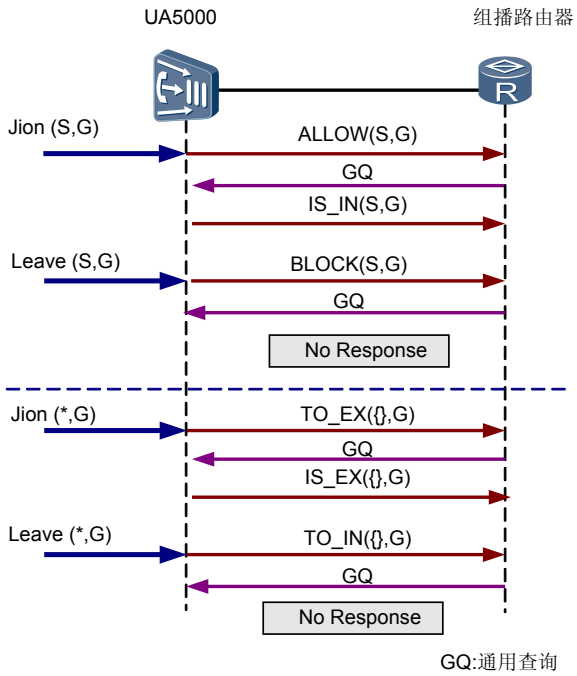
通用组查询	通过发送该报文来学习接口对“全部”组播的接收状态。与 IGMPv2 相似。
特定组查询	通过发送该报文来学习接口对“指定组地址”组播的接收状态。与 IGMPv2 相似。
特定源组查询	通过发送该报文来学习接口对“指定组地址和指定源地址”组播的接收状态。IGMPv3 新增。

  - 报告报文

IS_IN（G，S）	报告当前状态，说明当前组的模式是 INCLUDE 模式，收到查询报文时触发，源地址列表中包含了该组的源地址 S。
TO_IN（G，S）	改变组播组过滤模式为 INCLUDE，源地址列表中包含了新的源地址 S。TO_IN（G，{}）表示离开 G 的所有源，相当于 IGMPv2 的离开报文。
ALLOW（G，S）	改变源地址列表，源地址改变时触发，记录中包含的源地址是系统希望加入的源 S。
BLOCK（G，S）	改变源地址列表，源地址改变时触发，记录中包含的源地址是系统不再希望加入的源 S。
IS_EX（G，S）	报告当前状态，说明当前组的模式是 EXCLUDE 模式，收到查询报文时触发，源地址列表中包含了该组不希望加入的源地址 S。IS_EX（G，{}）表示当前对 G 的所有源都感兴趣，相当于 IGMPv2 的加入报文。设备不支持 S 不为空的 IS_EX 报文。
TO_EX（G，S）	改变组播组过滤模式为 EXCLUDE，源地址列表中包含了新的不希望加入的源地址 S。TO_EX（G，{}）表示对加入 G 的所有源，相当于 IGMPv2 的加入报文。设备不支持 S 不为空的 TO_EX 报文。

下面以实例说明报告报文的使用。

图 16-19 点播行为转换为 IGMPv3 报文



IGMP 版本兼容

接入设备的 IGMP 版本兼容策略是区分网络侧和用户侧。

网络侧的 IGMP 版本是基于 MVLAN 配置。通过下表可知：根据组播路由器的版本，设备的 IGMP 版本应该配置推荐的版本，避免不兼容造成的丢包问题。

组播路由器	接入设备 MVLAN 版本	对接结果
v1	v2/v3	不兼容
v2	v2（推荐）	正常
v3	v2（推荐）	设备不处理 v3 报文，直到组播路由器降级为 v2 才可以正常交互。 在正常应用场景中， 设备通常是主动发起方，组播路由器可以平滑降级，不会丢包。
v2	v3	组播路由器不处理 v3 报文，直到设备降级为 v2 才可以正常交互。 降级前，可能存在丢包。
v3	v3（推荐）	正常

用户侧的 IGMP 版本是不能直接配置的，而是由组播用户所属 MVLAN 中的最低版本决定。通过下表可知：根据终端的版本，设备的 IGMP 版本应该配置推荐的版本，避免不兼容造成的丢包问题。

终端	接入设备组播用户版本	对接结果
v1	v2/v3	不兼容
v2	v2（推荐）	正常
v3	v2	设备不处理 v3 报文，直到终端降级为 v2 才可以正常交互。 降级前，可能存在丢包。
v2	v3（推荐）	终端不处理 v3 报文，直到设备降级为 v2 才可以正常交互。即使降级为 v2 后，设备还可以识别来自其他终端的 v3 报文以保证更大兼容性。 在正常应用场景中， 终端通常是主动发起方，设备可以平滑降级，不会丢包。
v3	v3（推荐）	正常

IGMP Snooping

IGMP snooping 可以分为以下 2 种：

- IGMP transparent snooping

  这种 Snooping 是指不带 proxy 的 snooping 功能。设备支持基于 MVLAN 选择采用 proxy 或者 snooping 或者带 proxy 的 snooping 功能。

  设备通过学习组播用户的 IGMP 加入、离开报文来维护组播成员关系表，然后根据这张表把组播上行口的组播数据转发给对应的组播用户。为了维护组播成员关系表的老化信息，设备同时还会充当查询器。

  对 IGMP 报文的处理如下：

  - 查询报文

  接收来自组播上行口的通用组查询报文和特定组查询报文，直接触发本地查询器马上向用户侧发送查询（重新构造查询报文）。

  说明

  - 为保证组播用户及时响应查询，设备配置的最大查询响应时间应该小于上层组播路由器的值。
  - 设备的网络侧 IGMP 工作版本不受组播路由器影响。

  - 加入和离开报文

  接收来自组播用户的加入报文和离开报文，向 MVLAN 进行透传。

  说明

  对于 IGMPv3 可能包含多个组记录，匹配到不同的 MVLAN，设备会拆分报文，分别复制到对应的 MVLAN 进行透传。

- IGMP snooping with proxy

  带 proxy 的 snooping 功能在 IGMP 上行基本等同于 IGMP Proxy，仅仅是 IGMP 下行没有进行查询报文的抑制。

  - 查询报文

  接收来自组播上行口的查询报文，一方面触发向用户查询，另一方面会根据设备的组播成员关系表，响应组播路由器的查询。

  说明

  设备的网络侧 IGMP 工作版本同 IGMP proxy 一样受组播路由器影响。

  - 加入和离开报文

  接收来自组播用户的加入报文，只有第一个加入报文才会向 MVLAN 发送；接收来自组播用户的离开报文，只有最后一个离开报文才会向 MVLAN 发送。

Global leave

该报文是在 TR101 中定义的，是一种组 IP 为全 0 的 IGMP 离开报文，表达的意思就是离开所有的组。

- 网络侧

当网络拓扑发生变化时，设备向上层组播路由器发送该报文，对端收到后会马上发送通用组查询报文，且报文中的最大响应时间填写为特定组最大响应时间；当设备收到查询后，就会以感兴趣组的加入报文进行响应。这样，就可以加快组播业务的恢复。这里的网络拓扑变化事件包括环网切换、线路的 UP/DOWN 和保护组内的主备端口切换。

说明

- 当和其他类型的网络设备对接时，如果对端不支持 Global leave 报文则需要把该功能关闭，否则会造成拓扑变化时组播业务中断。
- 设备只在 IGMPv2 下支持发送 Global leave。

- 用户侧

当 STB 突然掉电后又马上上电，由于 STB 不会记得之前观看的节目，这时候旧节目会一直占用带宽和节目数资源，只有该节目等通用组查询老化后才会释放。

如果 STB 支持 Global leave，则再重新上电后先发送一个 Global leave 报文；设备收到该报文后，判断该组播用户如果是快速离开或基于 MAC 地址的快速离开则马上释放该用户的所有节目资源；即使该用户是正常离开，设备会发送一个以通用组查询报文，报文中的最大响应时间填写为特定组最大响应时间，这样也能够比通用组查询老化时间更快老化并释放该用户的节目资源。

16.7.3 网络侧对接

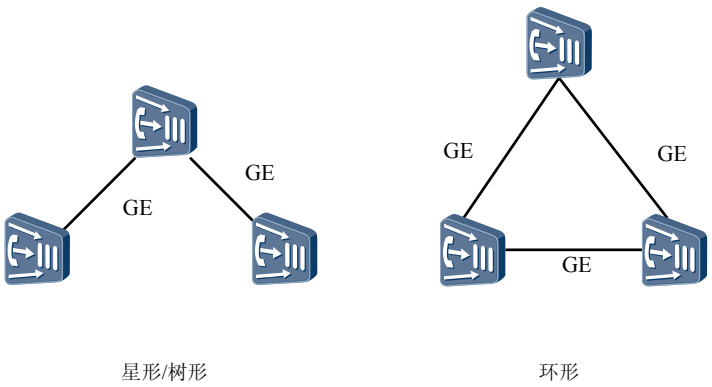
组播级联

UA5000 的组播级联采用以太级联。

通过在接入设备上进行以太级联，可以节约汇聚设备的端口数，同时比较容易实现在小区接入范围内的用户扩容。

常见级联组网形态有 2 种——星形（树形）和环形，如下图所示。此处只描述星形组网下的组播，环形组网组播详见“上行口环网”。

图 16-20 级联组网形态

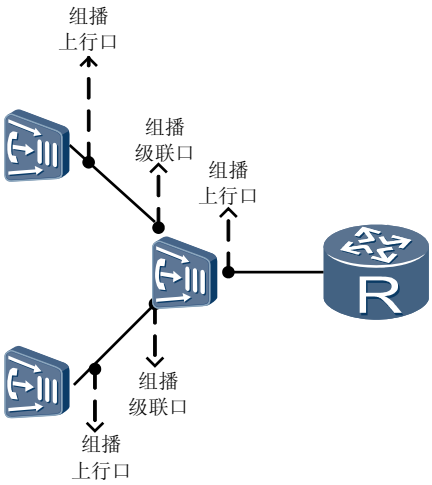


星形/树形　　环形

- 组播级联口配置

  设备可以通过 IPM 板上的以太端口实现与下一级设备间的物理连接。组播业务通过组播级联口配置来管理设备间的对接，一个组播级联口对应一个物理接口（承载的通道可以通过 port VLAN 或业务流创建），组播级联口和上行口的关系如下图所示。

图 16-21 组播级联口和上行口

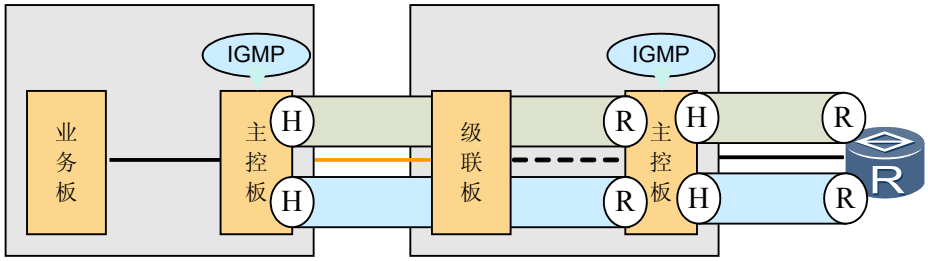


- IGMP 控制报文

  在组播级联场景中，上级设备和下级设备独立运行 IGMP 协议栈。对于本设备而言，级联口（下级设备）的角色等同于组播用户；但是由于组播接入用户的控制都是在下级设备执行，所以本设备对于级联口不支持以下对组播用户的业务功能，包括：权限管理、组播预览、组播 CAC、计费和组播验收等。只支持快速离开功能。

  在组播级联口上，IGMP 协议栈是基于不同 VLAN。如下图所示：

图 16-22 级联口 IGMP 协议栈



说明

如果以太端口未配置为组播级联口，则丢弃收到的 IGMP 报告报文。

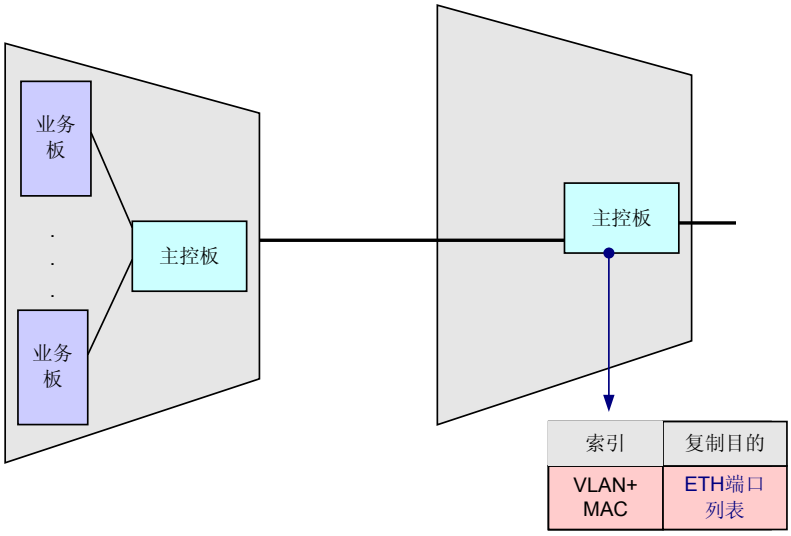
以 IGMP 报文的（SIP，GIP）和报文的 VLAN 同时进行节目匹配；不匹配的报文的处理策略可以基于级联口进行配置。

考虑到源头节点的 IGMP 处理性能，建议所有级联设备使用 IGMP Proxy，而不是 Snooping。

- 组播数据转发

  每个组播业务的数据只支持在同一个 VLAN 内转发。

图 16-23 组播级联转发架构



上行口环网

这里的环网组网是指在物理链路上把接入设备一个连接一个组成一个环，环上设备通过运行二层链路协议来维护环路的状态。

接入设备的环网组网有 2 个优点：

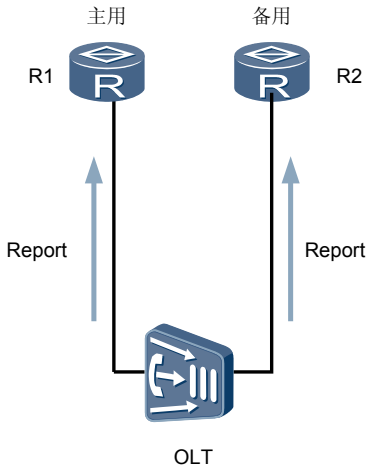
- 建网成本低：由于接入设备不需要和汇聚交换机直联，都是连接到最近的接入设备，节省了大量的光纤资源。其次交换机提供给接入设备的端口数少，只要部署少量的交换机即可满足接入要求。
- 可靠性较强：由二层链路协议来提供上行链路的备份保护功能——单个接入设备上行链路故障时，可以切换到另外一条备份链路。

组播业务在网络侧支持 2 种环网组网：RSTP 和 RRPP。

上行口双归属

如下图组网所示，组播路由器 1 和 2 分别处于主备状态；为了加速倒换后组播业务的快速恢复，可以使用设备提供的 IGMP 报文广播功能。

图 16-24 上行口广播发送 IGMP 报文



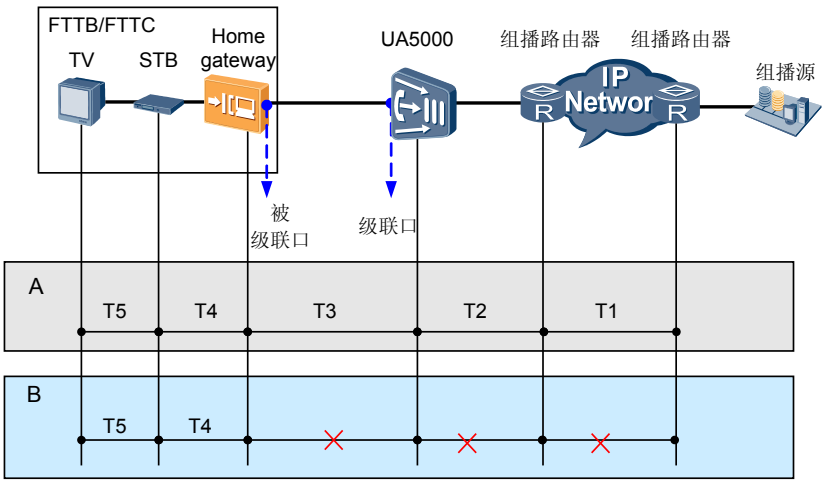
首先，在设备上把连接路由器 1 和路由器 2 的端口指定为组播上行口（这两个端口不能为同一个聚合组端口或保护组端口）；然后，当设备在向路由器 1 发送 IGMP 报文时，就会同时往路由器 2 发送相同的 IGMP 报文；这样路由器 2 就实时维护和路由器 1 一致的组播转发表项，一旦发生倒换，路由器 2 不需要通过其他手段重新获得转发表项，保证组播业务在更短时间内恢复。

说明：如果路由器支持私有协议传递组播转发表项，也可以达到替代该功能的效果。此时应该把接入设备的这两个端口放到同一个聚合组内。在实际应用中，这种更常用。

预加入节目

为了改善用户频道切换的体验，可以使用该功能缩短切换时延。因为切换延时其中包括每一段网络的处理消耗，如下图。使用该功能后，网络侧的处理消耗（T1+T2）相当于 0。

图 16-25 端到端组播时延示意图



A：未预加入节目处理时延=T1+T2+T3+T4+T5

B：预加入节目处理时延=T4+T5

预加入功能，适用于 IGMP Proxy 场景，等同于该节目一直有用户在线。

- 预加入节目的加入流程和正常节目相同（可以参考 1.6.4），一旦点播成功组播流就送到设备了。
- 预加入节目的离开流程，与正常节目相比，设备对于最后 1 个组播用户的离开也不向组播路由器发送离开报文。
- 预加入节目的查询流程，与正常节目相比，设备不管该节目的组成员关系表是否存在组播用户，都按协议响应组播路由器的查询。

综上所述，对于路由器来看，使能预加入的节目一直有用户在线。

该功能可以基于节目配置，通常可以把点播率最高的节目设置为预加入。动态节目不支持该功能。

组播路由器的源 IP 匹配

部分组播路由器只能处理与其三层接口同一个网段的 IGMP 报文，而在 Proxy 场景下，组播用户上行的 IGMP 报文会被接入设备终结，由其重新填写 IGMP 报文的源 IP。这时需要在设备上配置 IGMP 报文的源 IP。用户可以根据不同的需要，选择其中一种方式配置。

生效顺序	配置方式
第一优先级	对应三层接口的主 IP
第二优先级	对应节目的主机 IP（动态节目不可配置）
第三优先级	0

其他解决方法：部分组播路由器支持把三层接口设置成为混合模式，不再关注 IGMP 报文的源 IP。

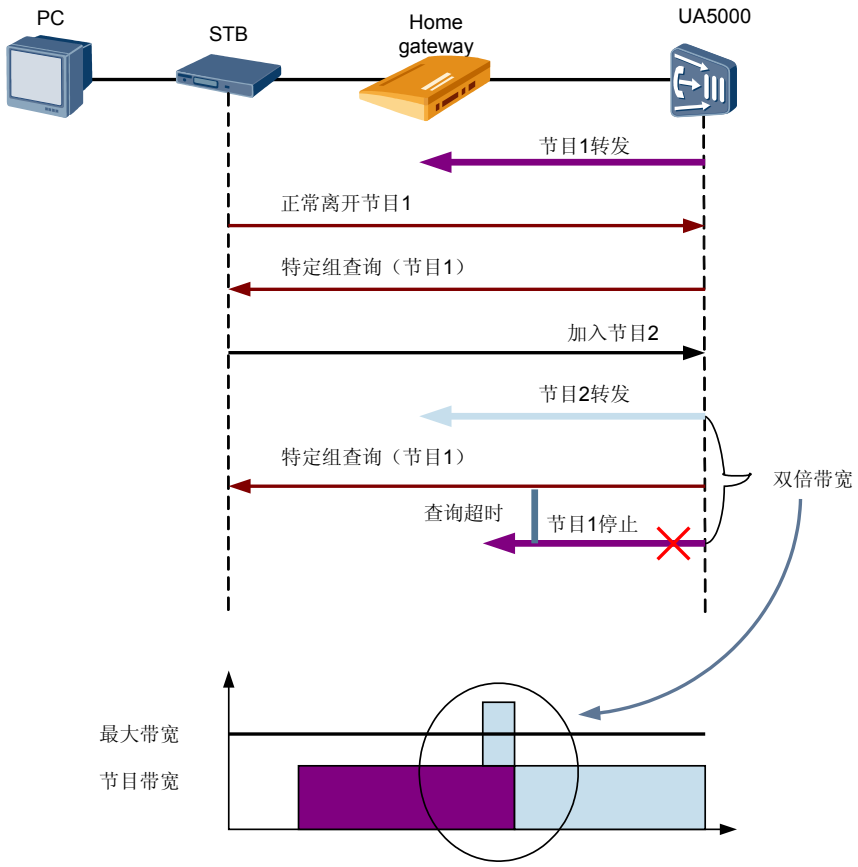
16.7.4 用户侧对接

快速离开

- 正常离开

  正常离开是指：按照 IGMPv2 标准定义，收到主机的离开报文后，路由器需要发送特定组查询报文，在查询超时后，才认为该主机不再需要该组数据。如下图所示：（IGMPv3 同理）

图 16-26 正常离开流程

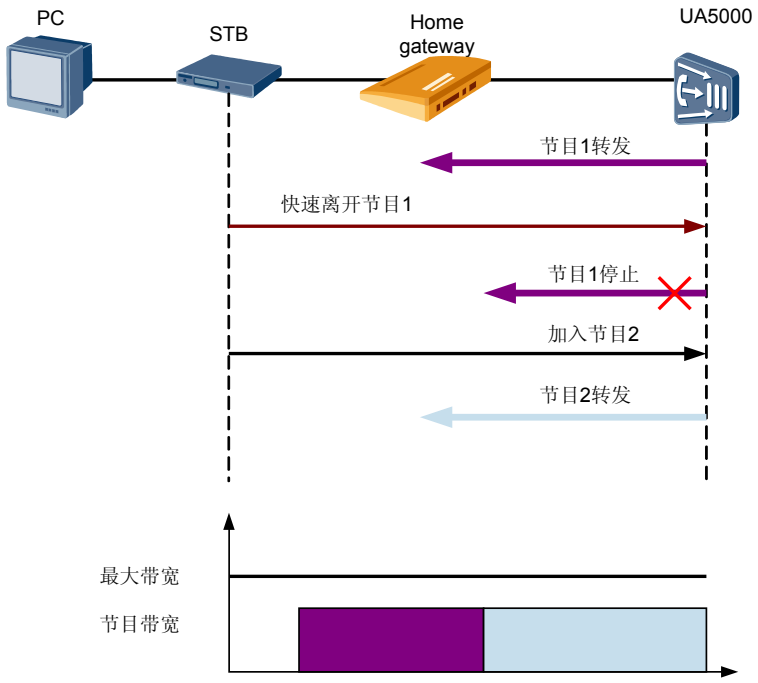


用户用遥控器进行一次频道切换会同时发出 2 个 IGMP 报文——1 个离开旧组播组和 1 个加入新组播组，所以在旧组播组未停止前，用户线路上会同时存在 2 个组播组的流量。如果线路没有预留足够的带宽承载 2 个组播组的流量，则流量就会溢出——造成丢包（如果承载的内容是视频就会出现花屏）。

- 快速离开

  快速离开是指：当设备收到组播用户的离开报文，就马上停止组播组对该用户的转发。如下图所示：

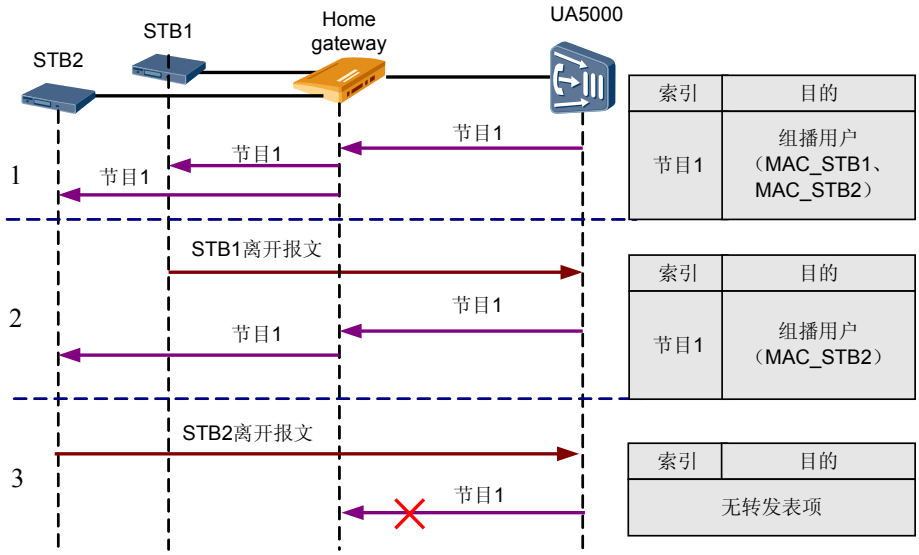
图 16-27 快速离开流程



- 基于 MAC 的快速离开

  基于 MAC 的快速离开是指：设备在生成组成员关系表时，不但会记录组播用户同时还会统计记录组播用户下组播组成员的 MAC 地址（每个节目最多记录 8 个）。当收到离开报文时，会先删除组成员关系表的 MAC 地址，只有当该组播用户下所有 MAC 地址都被删除完时才会停止组播组的转发。如下图所示：

图 16-28 基于 MAC 的快速离开流程



综上所述，三种方式各有优劣，用户可以根据需要选择，且支持基于组播用户配置。

	支持用户侧多 STB	带宽占用时间
正常离开	YES，STB 数量不限	直到特定组查询老化
快速离开	NO	马上释放带宽
基于 MAC 的快速离开	YES，1 个节目同时最多 8 个 STB	马上释放带宽

对于不同的用户家庭网络情况，可以参考下面推荐的配置方式：

HG 功能	STB 数量	预留带宽	正常离开	快速离开	基于 MAC 的快速离开
无 IGMP	1 个	不足		√	√
		充足	√	√	√
	多个	不足			√（不超过 8 个）
		充足	√		√（不超过 8 个）
IGMP Snooping	1 个	不足		√	√
		充足	√	√	√
	多个	不足			√（不超过 8 个）
		充足	√		√（不超过 8 个）
IGMP Proxy	1 个	不足		√	√（不限）
		充足	√	√	√（不限）
	多个	不足		√	√（不限）
		充足	√	√	√（不限）

16.8 组网应用

图 16-29 基于 MVLAN 的组播组网

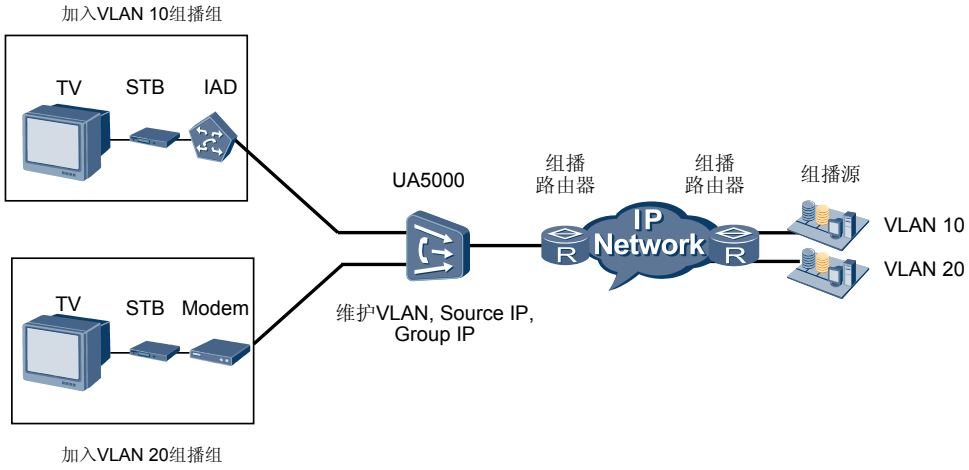
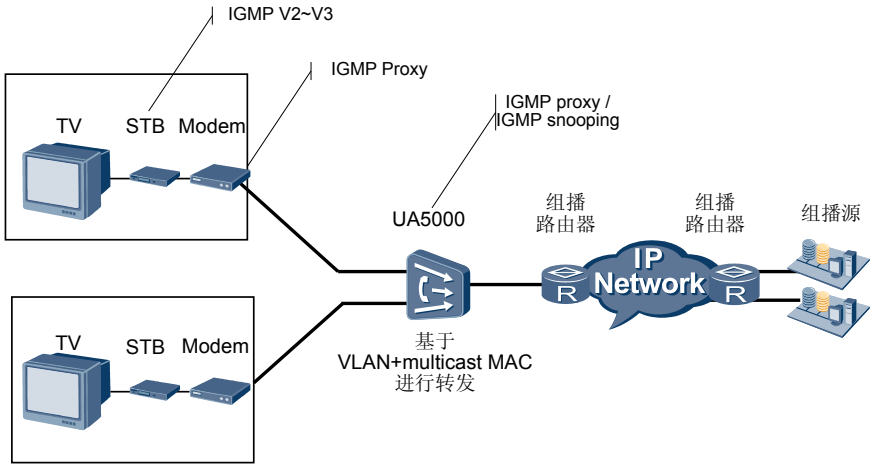


图 16-30 基于非 MVLAN 的组播组网



17 Triple Play

关于本章

介绍 Triple Play 特性的定义、目的、规格、原理以及参考的术语、缩略语和相关协议标准。

17.1 Triple Play 特性描述
介绍 Triple play 基本特性以及在 UA5000 上的实现原理。

17.2 单 PVC 多业务方案
介绍 Triple play 特性单 PVC 多业务方案以及在 UA5000 上的实现原理。

17.3 多 PVC 多业务方案
介绍 Triple play 特性多 PVC 多业务方案以及在 UA5000 上的实现原理。

17.1 Triple Play 特性描述

介绍 Triple play 基本特性以及在 UA5000 上的实现原理。

17.1.1 介绍

介绍该特性的定义、目的、规格、术语和缩略语。

定义

Triple Play 是指在一条用户线路上，同时提供多种不同业务接入方式。目前最普遍的是同时提供高速 Internet 上网业务、VoIP 业务和 IPTV 业务。

目的

Triple Play 业务的目的是通过将宽带上网、VoIP、视频业务封装在一个独立宽带连接上提供，方便用户使用，同时降低运营商的维护成本。

规格

支持单 PVC 多业务的 Triple play 方式和多 PVC 多业务的 Triple play 方式。

术语

无。

缩略语

表 17-1 Triple Play 特性缩略语表

缩略语	英文全称	中文全称
VoIP	Voice over IP	基于 IP 的语音
PSTN	Public Switched Telephone Network	公共电话交换网
PVC	Permanent Virtual Channel	永久虚通路

17.1.2 可获得性

介绍该特性需要的硬件支持，包括单板和终端。

无需额外硬件支持。

17.1.3 原理描述

介绍该特性的实现原理。

Triple play 业务，主要是需要考虑如何将同一个用户端口内的不同业务进行不同的优先级的处理，并保证将不同业务之间的互相影响降到最低。

- 对于 VoIP 业务

  占用的带宽比较小，对时延等要求比较高，所以在三种不同的业务中，VoIP 的优先级是最高的。（如果时延太大，可能会存在产生回声等问题，影响话音质量。）

- 对于视频业务（IPTV 业务）

  占用带宽比较大，对误码率/丢包率的要求比较高。如果误码率太大，或者丢包率太大，会造成视频帧的丢失，从而导致图像效果出现马赛克，甚至出现花屏的情况，会影响到观看效果。所以在三种不同的业务中，IPTV 的优先级要比 VoIP 低，但是需要比高速 Internet 高。

- 对于高速 Internet 接入业务

  一般用于浏览网页，对实时性的要求不强，对丢包率的要求也没有 IPTV 那么高（因为一般都会有重传机制可以保证传输的可靠性）。所以在三种业务中，高速 Internet 上网的优先级是最低的。

对于同一个端口上的三种不同业务，为了管理方便，在 UA5000 的上行接口上都是分为三个不同的 VLAN 上行，VoIP 业务在一个 VLAN，IPTV 业务在一个 VLAN，高速 Internet 在一个 VLAN。

说明
当按照以太网类型（IPoE/PPPoE）进行区分业务时，仅需要通过两个不同的 VLAN 上行。

17.2 单 PVC 多业务方案

介绍 Triple play 特性单 PVC 多业务方案以及在 UA5000 上的实现原理。

17.2.1 介绍

介绍该特性的定义、目的、规格和约束条件。

定义

单 PVC 多业务方案指从 UA5000 到每个 DSL 用户终端，采用唯一的 PVC 通道，承载多种不同业务的 Triple play 方案。

目的

采用单 PVC 多业务方案，对 DSL 用户终端维护比较简单，只需要建立一条 PVC 即可。在 DSL 用户终端上也不需要支持 PVC 和以太网端口的绑定功能。

规格

- 支持通过以太网类型（IPoE/PPPoE）区分不同的业务。
- 支持通过 DSL 用户终端带上来的 VLAN ID 区分不同的业务。
- 支持通过 DSL 用户终端带上来的 802.1p 值区分不同的业务。
- 每个 DSL 用户端口上最多可以支持 8 种不同的业务。
- 支持多种优先级标签映射，使用单 PVC 多优先级方式。

约束

- 每个 DSL 端口只支持一种单 PVC 多业务的方式。
- 不能支持同时按照以太网类型（IPoE/PPPoE）和 DSL 用户终端带上来的 VLAN ID 进行区分不同的业务。
- 不能支持同时按照以太网类型（IPoE/PPPoE）和 DSL 用户终端带上来的 802.1p 值区分不同的业务。

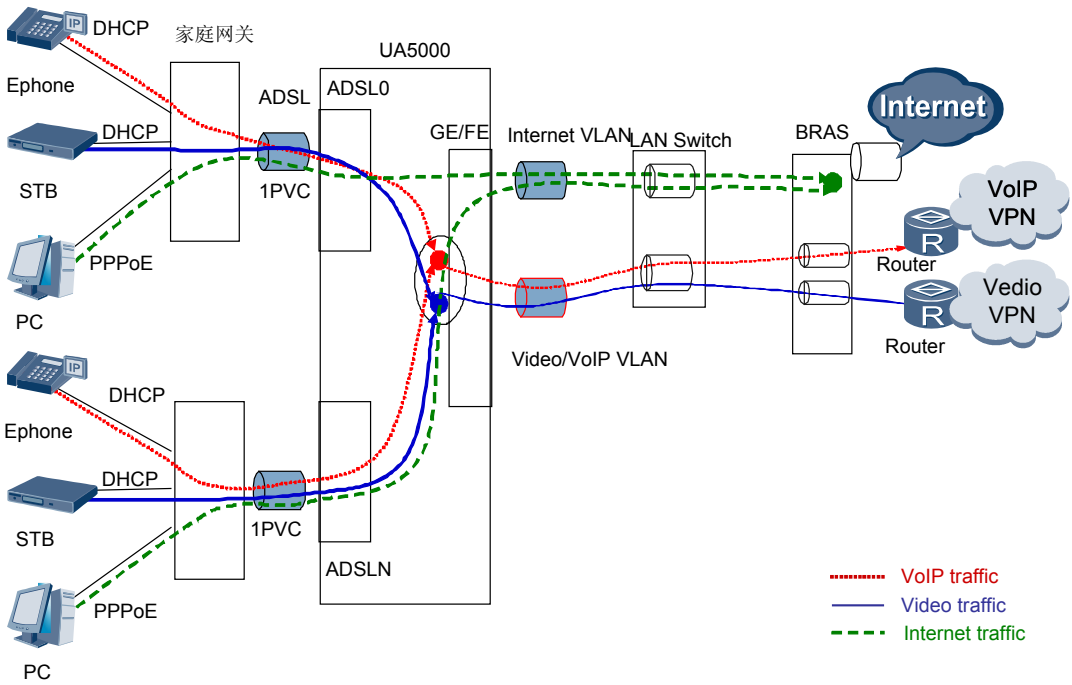
17.2.2 原理描述

介绍该特性的实现原理。

在用户侧，VoIP、IPTV、Internet 三种业务由同一个 PVC 接入，每 xDSL 端口只需配置一个 PVC。在网络侧，通过对上行口进行配置，让三种业务走不同的 VLAN。

- 对于按照以太网类型（IPoE/PPPoE）进行区分不同的业务的应用方式，具体实现原理如图 17-1 所示。

图 17-1 单 PVC 多业务按照以太网类型区分业务的 Triple play 方案实现原理

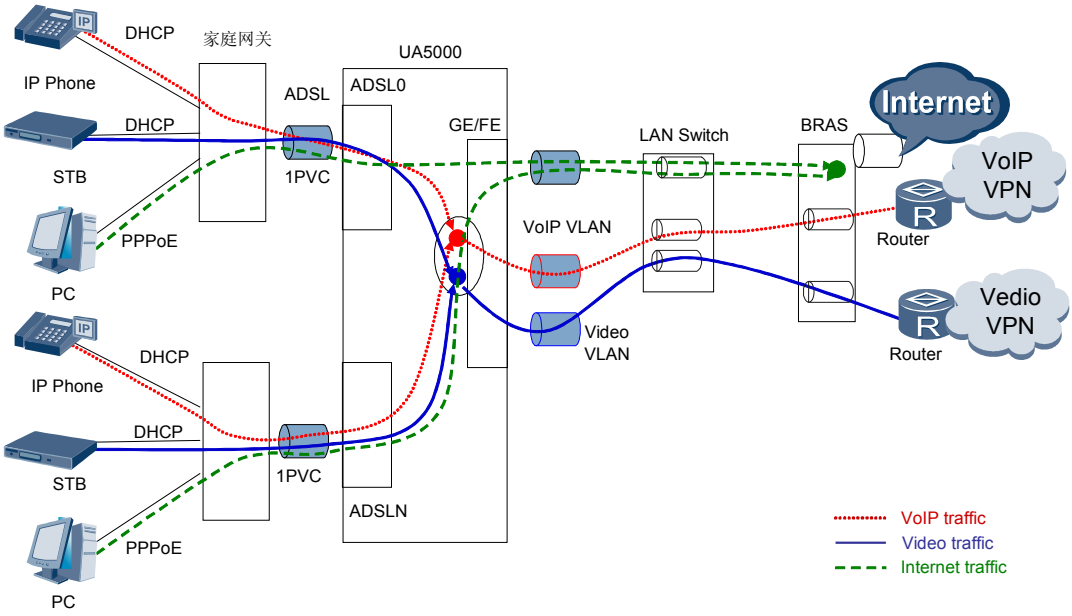


- DSL 用户终端采用家庭网关，完成将三种不同的业务混合，通过一条 PVC 上行。
- 一般而言，高速 Internet 上网业务的 PC 是采用 PPPoE 的方式；STB（IPTV 业务）和 Ephone（VoIP 业务）采用的是 IPoE 的方式，家庭网关将三种不同的业务混合，通过唯一的 PVC 送到 UA5000。
- UA5000 根据收到报文的以太网类型，将单 PVC 内的业务流分成 2 种不同的业务流（一种是 PPPoE 业务流，另一种是 IPoE 的业务流），每种业务流通过一个 VLAN 上行。

- 对于同一个 UA5000，其内部所有的 PPPoE 业务流采用统一的一个 VLAN 上行；其内部所有的 IPoE 业务采用统一的另一个 VLAN 上行。

- ?对于按照 DSL 用户终端带上来的 VLAN ID 区分不同的业务的应用方式，具体实现原理如图 17-2 所示。

图 17-2 单 PVC 多业务按照 VLAN ID 区分业务的 Triple play 方案实现原理



  - DSL 用户终端采用家庭网关，提供 3 个以太网接口，分别接到 Ephone（VoIP 业务）、STB（视频业务）和 PC（高速 Internet 接入）上，每一个端口固定绑定一个 VLAN ID（只要从这个端口上来的数据流，固定打这个 VLAN ID），然后家庭网关将这些数据流封装到 ATM 信元中，通过唯一的 PVC 送往 UA5000 处理。
  - UA5000 在解开 ATM 封装，恢复数据流之后，并根据数据流所带的 VLAN ID，拆分为 3 条数据流，然后再根据数据流所带的 VLAN ID，分别将三种业务映射到 3 个不同的上行 VLAN 中。
  - 对于这种区分业务方式，要求每台 UA5000 所带的 DSL 用户终端（家庭网关）上所带上来的三个 VLAN 是不同的。

- 对于按照通过 DSL 用户终端带上来的 802.1p 区分不同的业务的应用方式，具体实现原理如图 17-2 所示。
  - DSL 用户终端采用家庭网关，提供 3 个以太网接口，分别接到 Ephone（VoIP 业务）、STB（视频业务）和 PC（高速 Internet 接入）上，每一个端口固定绑定一个 802.1p（只要从这个端口上来的数据流，固定打这个 802.1p），然后家庭网关将这些数据流封装到 ATM 信元中，通过唯一的 PVC 送往 UA5000 处理。
  - UA5000 在解开 ATM 封装，恢复数据流之后，并根据数据流所带的 802.1p，拆分为 3 条数据流，然后再根据数据流所带的 802.1p，分别将三种业务映射到 3 个不同的上行 VLAN 中。
  - 对于这种区分业务方式，要求每台 UA5000 所带的 DSL 用户终端（家庭网关）上所带上来的三个 802.1p 是不同的。

17.3 多 PVC 多业务方案

介绍 Triple play 特性多 PVC 多业务方案以及在 UA5000 上的实现原理。

17.3.1 介绍

介绍该特性的定义、目的、规格和约束条件。

定义

多 PVC 多业务方案，是指从接入设备到每个 DSL 用户终端，采用多条 PVC 承载多种业务的 Triple play 方案。

目的

兼容已有的运维管理系统。

规格

当系统使用 IPMB 主控板时，每个 xDSL 端口可以支持最多 6 条 PVC。

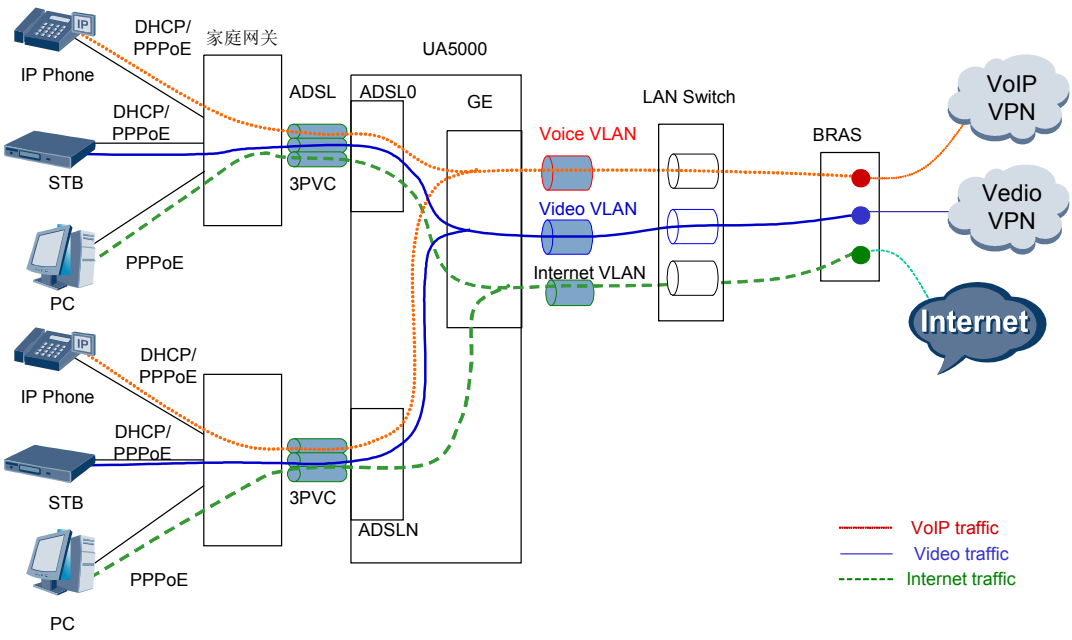
当系统使用 IPMD 主控板时，每个 xDSL 端口可以支持最多 8 条 PVC。

17.3.2 原理描述

介绍该特性的实现原理。

多 PVC 多业务指的是在用户侧，VoIP、IPTV、Internet 三种业务分别由不同的 PVC 接入，每个 xDSL 端口至少配置三个 PVC。在网络侧，通过对上行口进行配置，让三种业务通过不同的 VLAN 上行，具体实现原理如图 17-3 所示。

图 17-3 多 PVC 多业务的 Triple play 方案实现原理



- 对于多 PVC 多业务的方案，要求 DSL 用户终端也采用家庭网关，家庭网关对外提供 3 个以太网接口，分别接到 Ephone（VoIP 业务）、STB（视频业务）和 PC（高速 Internet 接入）上。
- 每一个以太网端口固定和一条 PVC 绑定（只要从这个端口上来的数据流，固定以这条 PVC 的 VPI/VCI 进行标识），家庭网关将这个端口上来的数据流从这条 PVC 送到 UA5000 进行处理。
- UA5000 从这条 PVC 上收到报文后，恢复为数据流，将这个数据流用某个特定的业务 VLAN 进行标识，通过上行接口送到上层设备中。

18 路由

关于本章

介绍路由特性的定义、目的、规格、原理以及参考的术语、缩略语和相关协议标准。

18.1 路由特性描述
概括介绍路由基本特性以及在 UA5000 上的实现原理。

18.2 静态路由
详细介绍静态路由特性以及在 UA5000 上的实现原理。

18.3 RIP 路由协议
RIP 是一种基于 V-D 算法的动态路由协议，通过 UDP 数据报交换路由信息。本特性从介绍、原理描述等方面进行描述。

18.4 OSPF 路由协议
OSPF 是 IETF 组织开发的一个基于链路状态的内部网关协议。本特性从介绍、原理描述等方面进行描述。

18.1 路由特性描述

概括介绍路由基本特性以及在 UA5000 上的实现原理。

18.1.1 介绍

介绍该特性的定义、目的、规格、术语和缩略语。

定义

路由（routing）是一个通用的术语，用来描述某一个网络中的主机所发出的分组经过一个或多个路由器传输到位于另一个网络中的主机的过程。在 Internet 中进行路由选择要使用路由器，路由器根据所收到的报文的目的地址选择一条合适的路由（通过某一网络），将报文传送到下一个路由器，路由中最后的路由器负责将报文送交目的主机。

目的

接入设备作为整个电信网中的基本元素之一，必须支持设备的远程操作、管理和维护等功能，以后随着设备的小型化、远端化，也要求接入设备具有某些 BRAS 的功能，如网络地址的分配、用户管理等，这些都要求设备能够支持路由功能，此时，UA5000 具备路由器的功能。

规格

目前 UA5000 系统支持静态路由和动态路由中的 RIP 和 OSPF 协议。

术语

无。

缩略语

表 18-1 路由特性缩略语表

缩略语	英文全称	中文全称
RIP	Routing Information Protocol	路由信息协议
OSPF	Open Shortest Path First	开放最短路径优先
AS	Autonomous System	自治系统
ABR	Area Border Router	区域边界路由器
ASBR	Autonomous System Boundary Router	自治系统边界路由器

18.1.2 可获得性

介绍该特性需要的硬件支持，包括单板和终端。

无需额外硬件支持。

18.1.3 原理描述

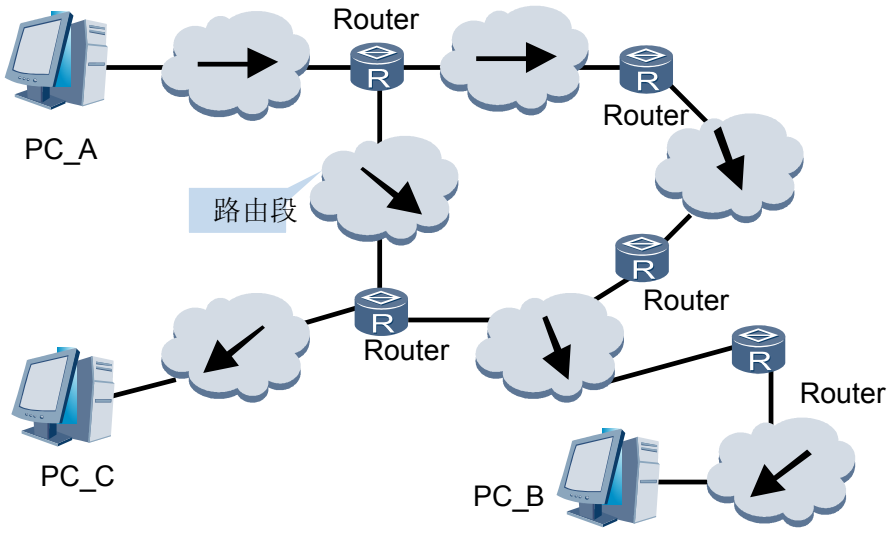
介绍该特性的实现原理。

路由器工作原理

路由器将报文在某一个网络中走过的通路（从进入网络开始到离开网络为止）在逻辑上看成是一个路由单位，并将此路由单位称为一跳（Hop）。每跳走过的通路称为一个路由段。

例如，在图 18-1 中，主机 A 到主机 C 的最短路径共经过了 3 个网络和 2 个路由器，跳数为 3。由此可见，若一结点通过一个网络与另一结点相连接，因而在互联网中是相邻的。相邻的路由器是指这两个路由器都连接在同一个网络上。一个路由器到本网络中的某个主机的路由跳数算作零。

图 18-1 路由段工作原理示意图



路由表

路由器转发报文必须依靠路由表。在每个路由器中都保存着一张路由表，表中的每条路由项都指明报文到某子网或某主机应通过路由器的哪个物理端口发送，然后就可到达该路径的下一个路由器，或者不再经过别的路由器而传送到直接相连的网络中的目的主机。

路由表中包含了下列关键项：

- 目的地址：用来标识 IP 报文的目的 IP 地址或目的网络，32 比特。
- 子网掩码：子网掩码由若干个连续“1”构成，写成文本形式时既可以用点分十进制表示，也可以用子网掩码中连续“1”的个数来表示。它与目的地址一起标识目的主机或路由器所在网段的地址。其具体做法，是将目的地址和网络子网掩码“逻辑与”，然后即得到目的主机或路由器所在网段的地址。

例如：某个目的地址为 129.102.8.10，子网掩码为 255.255.0.0 的主机或路由器所在网段的地址为 129.102.0.0。

- 输出接口：说明 IP 报文将从该路由器的哪个接口转发出去。
- 下一跳 IP 地址：说明 IP 报文所经由的下一个路由器。
- 本条路由加入 IP 路由表的优先级：优先级高（数值小）的路由将成为当前的最优路由。用户可以配置多条到同一目的地但优先级不同的路由，路由器将按优先级顺序选取唯一的一条路由供转发 IP 报文时使用。
- 路由开销：当到达同一目的地的多条路由具有相同的优先级时，路由开销最小的将成为当前的最优路由。

路由分类

根据路由目的地的不同，可以划分为：

- 子网路由：目的地为子网。
- 主机路由：目的地为主机。

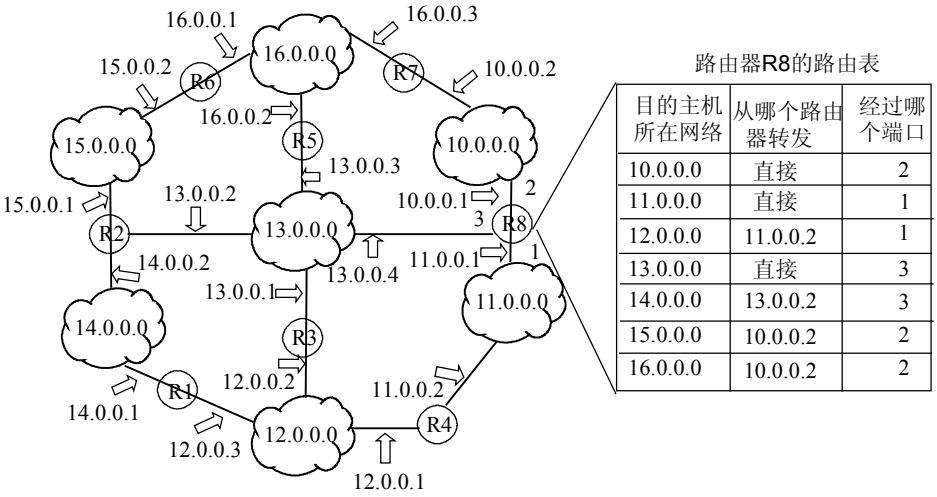
另外，根据目的地与该路由器是否直接相连，又可分为：

- 直接路由：目的地所在网络与路由器直接相连。
- 间接路由：目的地所在网络与路由器并不直接相连。

为了不使路由表过于庞大，可以设置一条缺省路由。凡遇到查找路由表失败的 IP 报文，就选择按缺省路由进行转发。

如图 18-2 所示的网络中，各网络云图中的数字代表该网络的网络地址。路由器 R8 与三个网络相连，因此有三个 IP 地址和三个物理端口，其路由表如图 18-2 所示。

图 18-2 路由表示意图



路由器R8的路由表

目的主机所在网络	从哪个路由器转发	经过哪个端口
10.0.0.0	直接	2
11.0.0.0	直接	1
12.0.0.0	11.0.0.2	1
13.0.0.0	直接	3
14.0.0.0	13.0.0.2	3
15.0.0.0	10.0.0.2	2
16.0.0.0	10.0.0.2	2

路由管理策略

UA5000 支持对静态路由的配置，同时支持 RIP、OSPF 动态路由协议。UA5000 中是统一管理用户设置的静态路由和动态路由，静态路由与 RIP，OSPF 等路由协议配置的路由可以互相共享。

路由协议及其发现路由的优先级

在某一时刻，到某一目的地的当前路由仅能由唯一的路由协议来决定。这样，各路由协议（包括静态路由）都被赋予了一个优先级，当存在多个路由信息源时，具有较高优先级的路由协议发现的路由将成为当前路由。各种路由协议及其发现路由的缺省优先级（数值越小表明优先级越高）如**表 18-2** 示。

表 18-2 路由协议及其发现路由的缺省优先级

路由协议或路由种类	相应路由的优先级
DIRECT	0
OSPF	10
INTERNAL EIGRP	50
STATIC	60
RIP	100
OSPF ASE	150
EXTERNAL EIGRP	160
IBGP	256
EBGP	256
UNKNOWN	255

在优先级的取值中，0 表示直接连接的路由，255 表示任何来自不可信源端的路由。

除了直接路由（Direct）和 BGP（IBGP、EBGP）外，各动态路由协议的优先级都可根据用户需求，手工进行配置。另外，每条静态路由的优先级都可以不相同。

路由协议之间的共享

由于各路由协议的算法不同，不同的协议可能会发现不同的路由，因此各路由协议之间存在如何共享各自发现结果的问题。一种路由协议可能需要引入其它的路由协议发现的路由信息，从而丰富自己的路由知识。路由器在引入其它路由协议的路由信息时，可能需要只引入一部分满足条件的路由信息，并对所引入的路由信息的某些属性进行设置，以使其满足本协议的要求。

为实现路由策略，首先要定义将要实施路由策略的路由信息的特征，即定义一组匹配规则，可以以路由信息中的不同属性作为匹配依据进行设置，如目的地址、发布路由信息的路由器地址等。匹配规则可以预先设置好，然后再将它们应用于路由的发布、接收和引入等过程的路由策略中。

UA5000 支持将一种路由协议发现的路由引入到另一种路由协议中，每种协议都有相应的路由引入机制。

过滤器

在 UA5000 中，提供了访问控制列表、地址前缀列表、Route-policy 几种过滤器供路由协议引用。下面对各种过滤器逐个进行介绍。

- 访问控制列表

  用户在定义 ACL 时可以指定 IP 地址和子网范围，用于匹配路由信息的目的网段地址或下一跳地址。

- 地址前缀列表

  地址前缀列表的作用类似于 ACL，但比它更为灵活，且更易于为用户理解。地址前缀列表在应用于路由信息的过滤时，其匹配对象为路由信息的目的地址信息域。

  一个地址前缀列表由前缀列表名标识。每个前缀列表可以包含多个表项，每个表项可以独立指定一个网络前缀形式的匹配范围，并用一个 index-number 来标识，index-number 指明了进行匹配检查的顺序。

  在匹配的过程中，路由器按升序依次检查由 index-number 标识的各个表项，只要有某一表项满足条件，就意味着通过该地址前缀列表的过滤（不进入下一个表项的测试）。

- Route-policy

  Route-policy 是一种比较复杂的过滤器，它不仅可以匹配给定路由信息的某些属性，并在条件满足时改变路由信息的属性。Route-policy 可以使用前面几种过滤器定义自己的匹配规则。

  一个 Route-policy 可以由多个节点（node）构成，每个节点是进行匹配测试的一个单元，节点间依据顺序号（node-number）进行匹配。每个节点可以由一组 **if-match** 和 **apply** 子句组成。**if-match** 子句定义匹配规则，匹配对象是路由信息的一些属性。同一节点中的不同 **if-match** 子句是“与”的关系，只有满足节点内所有 **if-match** 子句指定的匹配条件，才能通过该节点的匹配测试。**apply** 子句指定动作，也就是在通过节点的匹配测试后所执行的动作——对路由信息的一些属性进行设置。

  一个 Route-policy 的不同节点间是“或”的关系，系统依次检查 Route-policy 的各个节点，如果通过了 Route-policy 的某一节点，就意味着通过该 Route-policy 的匹配测试（不进入下一个节点的测试）。

路由策略主要有两种应用方式

路由策略的两种应用方式如下：

- 路由协议在引入其它路由协议发现的路由时，通过路由策略只引入满足条件的路由信息。
- 路由协议在发布或接收路由信息时，通过路由策略对信息进行过滤，只接收或发布满足给定条件的路由信息。

18.1.4 参考信息

介绍与该特性相关的参考信息。

本特性的参考资料清单如下：

- RFC 2453, Routing Information Protocol
- RFC 2328, Open Shortest Path First

18.2 静态路由

详细介绍静态路由特性以及在 UA5000 上的实现原理。

18.2.1 介绍

介绍该特性的定义、目的、规格和约束条件。

定义

静态路由是一种特殊的路由，它由网络操作人员手工输入到设备的配置信息中。

目的

当网络结构比较简单时，只需配置静态路由就可以使网络正常工作。仔细设置和使用静态路由可以改进网络的性能，并可为重要的应用保证带宽。

静态路由配置方便，对系统要求低，适用于拓扑结构简单并且稳定的小型网络，缺点是不能自动适应网络拓扑的变化，需要人工干预。

规格

UA5000 静态路由的最大数目为 1000 条。

18.2.2 原理描述

介绍该特性的实现原理。

静态路由的原理比较简单，管理者通过配置途径（如 CLI、SNMP）将路由添加到路由表中即可。转发模块采用最长匹配（Longest Match Algorithm）的原则找到相应的路由表项，并将报文转发到下一跳地址。

18.3 RIP 路由协议

RIP 是一种基于 V-D 算法的动态路由协议，通过 UDP 数据报交换路由信息。本特性从介绍、原理描述等方面进行描述。

18.3.1 介绍

介绍 RIP 路由协议的定义、目的、规格等信息。

定义

动态路由是指能够针对网络拓扑或者流量的变化进行自我调节的路由。RIP 是一种基于 V-D 算法的动态路由协议，通过 UDP 数据报交换路由信息。

目的

RIP 路由协议有自己的路由算法，能够自动适应网络拓扑的变化，适用于具有一定数量三层设备的网络。缺点是配置比较复杂，对系统的要求高于静态路由，并将占用一定的网络资源。

规格

路由表项最多为 2300 条。UA5000 只支持一个 RIP 进程，UA5000 单进程可以配置 1024 条 network，可以配置 256 个邻居。

18.3.2 原理描述

介绍 RIP 路由协议的实现原理。

RIP（Routing Information Protocol）是一种基于 V-D 算法的动态路由协议，它通过 UDP（User Datagram Protocol）数据报交换路由信息，每隔 30s 向外发送一次路由更新。如果路由设备经过 180s 没有收到来自对端的路由更新信息，则将所有来自此路由器的路由信息标志为不可达，并且如果在其后 120s 内仍没有收到更新信息就将其删除。

RIP 有两个版本：RIP 1 和 RIP 2。

RIP 1 是有类别路由协议（Classful Routing Protocol），它只支持以广播方式发布协议报文。RIP-1 的协议报文中没有携带掩码信息，它只能识别 A、B、C 类这样的自然网段的路由，因此 RIP-1 无法支持路由聚合，也不支持不连续子网（Discontiguous Subnet）。

RIP 2 是一种无分类路由协议（Classless Routing Protocol），与 RIP 1 相比，它有以下优势：

- 支持外部路由标记（Route Tag），可以在路由策略中根据 Tag 对路由进行灵活的控制。
- 报文中携带掩码信息，支持路由聚合和 CIDR（Classless Inter-Domain Routing）。
- 支持指定下一跳，在广播网上可以选择到最优下一跳地址。
- 支持组播路由发送更新报文，只有 RIP-2 路由器才能收到协议报文，减少资源消耗。
- 支持对协议报文进行验证，并提供明文验证和 MD5 验证两种方式，增强安全性。

说明

RIP-2 有两种报文传送方式：广播方式和组播方式，缺省将采用组播方式发送报文，使用的组播地址为 224.0.0.9。当接口运行 RIP-2 广播方式时，也可接收 RIP-1 的报文。

RIP 使用跳数（Hop Count）来衡量到达信宿机的距离，称为路由权（Routing Metric）。在 RIP 中设备到与它直接相连的网络的跳数为 0（在某些协议中被定义为 1），到通过一个设备可达的网络的距离为 1 跳，其余依此类推。为限制收敛时间，RIP 规定 metric 为 0 ～ 15 间的整数，若跳数等于 16 被当作无穷大。

RIP 通过以下机制来避免路由环路的产生：

- 计数到无穷（Counting to infinity）：将开销值等于 16 时定义为不可达（Infinity），在路由环路发生时，当某条路由的开销值计算到 16 时，该路由被认为是不可达路由。
- 水平分割（Split Horizon）：RIP 从某个接口学到的路由，不会从该接口再发回给邻居路由器。这样不但减少了带宽消耗，还可以防止路由循环。

- 毒性反转（Poison Reverse）：RIP 从某个接口学到路由后，将该路由的开销设置为16（不可达），并从原接口发回邻居路由器。利用这种方式，可以清除对方路由表中的无用信息。
- 触发更新（Triggered Updates）：RIP 通过触发更新来避免在多个路由器之间形成路由循环的可能，而且可以加速网络的收敛速度。一旦某条路由的开销发生了变化，就立刻向邻居路由器发布更新报文，而不是等到定时周期的到来。

18.4 OSPF 路由协议

OSPF 是 IETF 组织开发的一个基于链路状态的内部网关协议。本特性从介绍、原理描述等方面进行描述。

18.4.1 介绍

介绍 OSPF 路由协议的定义、目的、规格等信息。

定义

动态路由是指能够针对网络拓扑或者流量的变化进行自我调节的路由。OSPF 是 IETF 组织开发的一个基于链路状态的动态路由协议。

目的

OSPF 路由协议有自己的路由算法，能够自动适应网络拓扑的变化，适用于具有一定数量三层设备的网络。缺点是配置比较复杂，对系统的要求高于静态路由，并将占用一定的网络资源。

规格

路由表项最多为 2300 条。UA5000 只支持一个 OSPF 进程，UA5000 单进程支持 10 个区域，501 个网段，可配置 128 个邻居，可对每个区域执行 513 次路由聚合操作。

18.4.2 原理描述

介绍 OSPF 路由协议的实现原理。

OSPF（Open Shortest Path First）是 IETF 组织开发的一个基于链路状态的内部网关协议。目前使用的是版本 2（RFC2328），其特性如下：

- 适应范围——支持各种规模的网络，最多可支持几百台路由器。
- 快速收敛——在网络的拓扑结构发生变化后立即发送更新报文，使这一变化在自治系统中同步。
- 无自环——由于 OSPF 根据收集到的链路状态用最短路径树算法计算路由，从算法本身保证了不会生成自环路由。
- 区域划分——允许自治系统的网络被划分成区域来管理，区域间传送的路由信息被进一步抽象，从而减少了占用的网络带宽。
- 等值路由——支持到同一目的地址的多条等值路由。
- 路由分级——使用 4 类不同的路由，按优先顺序来说分别是：区域内路由、区域间路由、第一类外部路由、第二类外部路由。

- 支持验证——支持基于接口的报文验证以保证路由计算的安全性。
- 组播发送——支持组播地址。

整个网络可看成由多个自治系统 AS（Autonomous System）组成，通过收集和传递自治系统链路状态来动态地发现并传播路由，达到自治系统的信息同步。每个自治系统又可划分为不同的区域（Area）。如果一个路由器的端口被分配到多个区域中，这个路由器就被称为区域边界路由器 ABR（Area Border Router），它是那些处在区域边缘的连接了多个区域的路由器。

OSPF 骨干区域（Backbone）是一个特殊的区域，该区域以 0.0.0.0 标识。它负责交换非骨干区域（Non-backbone）的路由信息。由于骨干区域都必须在逻辑上保持连接，特别引入了虚连接的概念，使那些物理上分割的区域仍可保持逻辑上的连通性。跟其他自治系统交换路由信息的路由器叫做自治系统边界路由器 ASBR（Autonomous System Boundary Router），它在整个自治系统中发布 AS External 路由。

19 以太网链路聚合

关于本章

介绍以太网链路聚合特性的定义、目的、规格、原理以及参考的术语、缩略语和相关协议标准。

19.1 介绍
介绍该特性的定义、目的、规格、约束条件、术语和缩略语。

19.2 可获得性
介绍该特性需要的硬件支持，包括单板和终端。

19.3 原理描述
介绍该特性的实现原理。

19.4 参考信息
介绍与该特性相关的参考信息。

19.1 介绍

介绍该特性的定义、目的、规格、约束条件、术语和缩略语。

定义

以太网链路聚合是指将多个以太网端口聚合到一起，当作一个端口来处理，提供更高的带宽和链路安全性。

IEEE 802.3ad 是关于以太网链路聚合的标准。LACP（Link Aggregation Control Protocol）是 IEEE 802.3ad 标准中实现链路聚合的控制协议。通过该协议，不但可以自动实现设备之间端口聚合不需要用户干预，而且还可以检测端口的链路层故障，完成链路的聚合控制。

目的

手工链路聚合由于没有使用 LACP 协议，链路两端的设备缺少对聚合进行协商的必要交互，因此对聚合的控制不够准确和有效，只能根据端口物理状态（down 和 up）来确定是否进行聚合。例如，如果用户错误地将物理链路连接到不同的设备上或者同一设备的不能形成聚合的端口上，那么系统是无法发现的。另外，手工链路聚合只能工作在负载分担方式，应用也存在一定限制。

动态链路聚合在完全没有人工干预的情况下自动生成聚合，它使设备具有了某些即插即用的特性。但在实际应用中，这种聚合方式显得过于灵活，会给用户带来使用上的不便与困难。例如，由于聚合组是设备动态生成的，因此在设备重启等情况下聚合组 ID 就可能会发生变化，这将给设备的管理带来麻烦。

静态链路聚合汇集了手工链路聚合和动态链路聚合各自的优点，既易于管理和使用，又能够准确和有效地对聚合进行控制。聚合组和成员端口采用手工管理，即聚合组的创建与删除，以及成员端口的加入与退出都是在用户操作控制下完成的，设备不会自动完成，更不会修改用户的配置结果，这一点与手工链路聚合相同。

在静态链路聚合组中，其成员端口可能处于两种状态，即 Selected 和 Standby。Selected 端口是实际工作的端口，上面有流量发生。Standby 端口则相反，它们只是处于一种备用状态，上面不会有流量发生。因此，静态链路聚合组可能并非所有的成员端口都同时工作，而且端口的 Selected 和 Standby 状态会随着设备的运行和外部环境的变化而改变，使静态链路聚合实现负载分担聚合和非负载分担聚合成为可能。

此处描述的特性就是采用 LACP 协议来实现静态链路聚合的方式。

在 UA5000 上，LACP 端口保护对用于 IPMB 主备板间 1+1 端口故障保护。

规格

- 最多支持 8 组以太网端口汇聚，每组可支持最多 8 个同速率的端口汇聚。
- 系统优先级：0 ～ 65535。
- 端口优先级：0 ～ 32767。
- LACP 交互短周期时间：1s ～ 10s，缺省值是 1s。
- LACP 交互长周期时间：20s ～ 40s，缺省值是 30s。
- 支持单块主控板端口间 LACP 方式端口聚合。
- 支持主备用端口启动 LACP 主备聚合功能。

约束

- 相同类型的端口（包括端口属性、工作模式和速率）才能配置聚合组。
- 不支持动态链路聚合。

术语

表 19-1 以太网链路聚合特性术语表

术语	解释
手工链路聚合	完全由用户手工创建聚合组，手工增删成员端口，不运行 LACP 协议，聚合组内成员端口有 down 和 up 两种物理状态。

缩略语

表 19-2 以太网链路聚合特性缩略语表

缩略语	英文全称	中文全称
LACP	Link Aggregation Control Protocol	链路聚合控制协议

19.2 可获得性

介绍该特性需要的硬件支持，包括单板和终端。

支持本特性的单板为主控板 IPMB 和 IPMD。

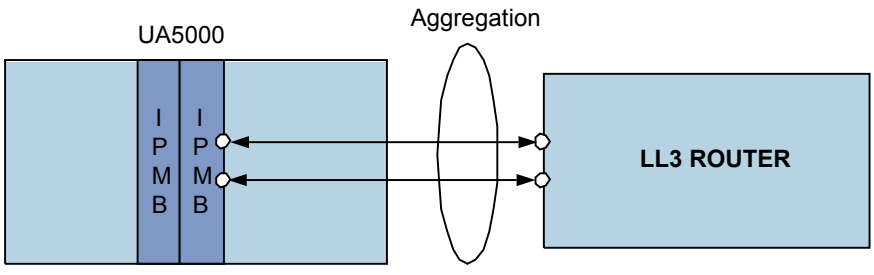
19.3 原理描述

介绍该特性的实现原理。

手工链路聚合实现原理

在介绍基于 LACP 的静态链路聚合以前，以主控板两个端口进行聚合为例，如图 19-1 所示，介绍手工链路聚合的实现原理。

图 19-1 手工链路聚合图



UA5000 的两个上行端口加入了一个聚合组，对端设备同样要把对应的两个端口加入一个聚合组。

只要两个端口的状态都是正常，UA5000 与对端设备之间的流量就会分担到两条链路上。分担的策略可以根据源 MAC 地址，也可以根据源 MAC 地址和目的 MAC 地址的组合。如果其中一个端口故障或者对应的链路故障，UA5000 的主控板就不会把流量发送到故障端口。

静态链路聚合实现原理

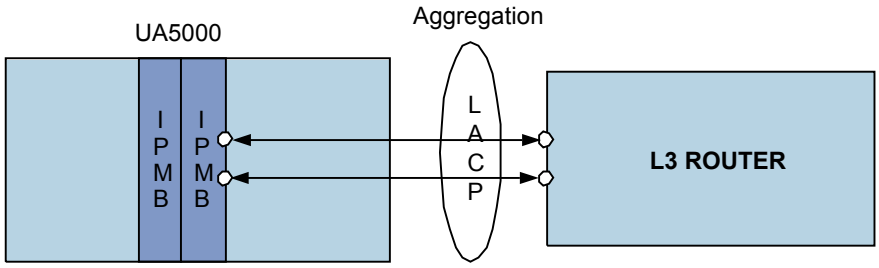
静态链路聚合采用 LACP 协议，设备之间都需要运行 LACP 协议，但是聚合组的创建与删除以及成员端口的加入与退出都需要用户配置完成。

在静态链路聚合中，LACP 主要完成以下功能：

- 检测和维护链路聚合端口的状态信息，包括 Selected 和 Standby。
- 与其它互连设备交换聚合端口的状态信息。

LACP 协议采用 LACPDU（LACP Data Unit）在设备之间交互聚合信息，对聚合组的信息达成一致。UA5000 与 Switch 之间通过 LACP 协议交互聚合组信息如图 19-2 所示。

图 19-2 静态链路聚合图



聚合组内的成员端口，如果状态是 Selected，则流量会分担到该端口；如果状态是 Standby，则流量不会分担到该端口。

- Selected 和 Standby 状态是 LACP 协议层维护的聚合端口状态，并不是端口的物理状态，但是端口的物理状态变化会引起 LACP 协议层的端口状态变化。例如，如果聚合端口故障，LACP 协议层的端口状态会迁移到 Standby。
- 除了物理端口状态变化会引起 LACP 协议层端口状态变化以外，通过 LACPDU 交互也可以引起 LACP 协议层的端口状态变化。例如，接收到对端 LACPDU 通知的时候，可能会对端口状态进行改变。

所以，支持 LACP 以后，聚合链路状态检测不仅仅是物理端口状态变化，单板故障、端口转发失效、对端聚合端口状态变化等都可以通过 LACP 协议交互完成，提高了链路聚合的安全性。

LACP 协议还支持系统优先级、端口优先级、快慢交互周期等机制。

- 系统优先级

在 LACP 协议中，通过系统优先级来控制对接设备的主从关系。从设备必须要遵从主设备的选择结果进行 Selected 端口的选择，否则会导致设备无法进行正常的对接。

- 端口优先级

  通过端口优先级选择主端口和从端口。

- 交互周期

  为了保证 LACP 协议检测的灵敏度，协议中规定了两个定时周期（short timeout，long timeout），可以调整交互周期达到最佳效果。除非对端设备通知使用慢周期，设备才使用慢周期进行交互，否则设备一直使用快周期进行报文交互和发送。UA5000 支持的时间周期值如下：

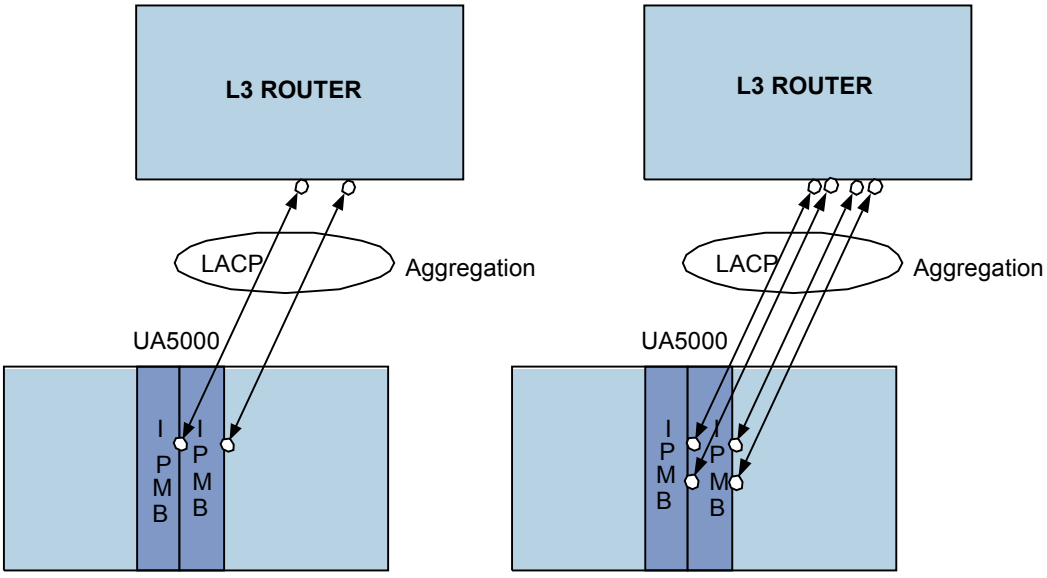
  - 短周期时间值：1s-10s
  - 长周期时间值：20s-40s

LACP 方式保护组实现原理

在 UA5000 上，还提供了 LACP 方式保护组功能。LACP 与保护倒换特性协同工作可通过 LACP 协议去检测链路是否存在故障，当备用主控板的链路可用性高于主用主控板时，触发保护性倒换，从而使得系统更可靠。

LACP 保护对的典型应用组网如图 19-3 所示。

图 19-3 LACP 保护组



左图是 IPMB 上主备板各出一个端口上行接到上层路由器上，形成 1+1 保护，当主板端口故障（包括物理层和链路层故障）时，LACP 协议检测备板端口是否可用，如果备板端口可用，则需要主动触发保护性倒换，使备板接替主板进行工作。

右图是 IPMB 上主备板各出两个端口，形成保护组，保护组中的端口通过 LACP 协议完成链路聚合协商。正常情况下，只有一块 IPMB 板上的两个端口进行工作，这两个端口形成负荷分担，共同分担报文流量，当检测到主板端口故障（包括物理层和链路层故

障）后，判断备用主控板的链路可用性如果高于主用主控板，则触发保护性倒换，使备板接替主板进行工作。

19.4 参考信息

介绍与该特性相关的参考信息。

本特性的参考资料清单如下：

- IEEE 802.3ad Link Aggregation

20 系统和用户安全

关于本章

介绍系统和用户安全特性的定义、目的、规格、原理以及参考的术语、缩略语。

20.1 系统和用户安全概述
简要介绍系统和用户安全特性。

20.2 系统安全
介绍系统安全特性的定义、目的、规格、原理以及参考的术语、缩略语。

20.3 用户安全
介绍用户安全特性的定义、目的、规格、原理以及参考的术语、缩略语。

20.1 系统和用户安全概述

简要介绍系统和用户安全特性。

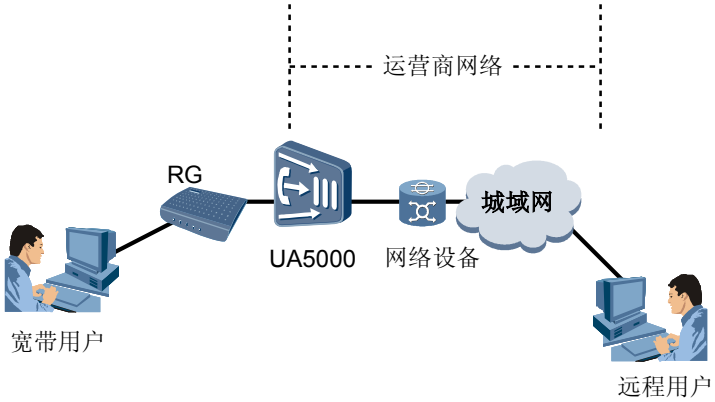
定义

系统和用户安全特性是指对设备的系统起到网络安全、保护作用和防御用户攻击网络设备的特性。

目的

系统安全应用模型，如图 20-1 所示。

图 20-1 系统安全应用模型



在接入网络中可能存在多种攻击模式：

- 本地用户对系统的攻击。
- 本地用户对网络设备的攻击。
- 远程用户对本地用户的攻击。
- 远程用户对系统的攻击。

系统安全主要是针对本地用户对系统的攻击，保护设备本身；其中部分特性（如防火墙功能等）也能防御远程用户对系统的攻击。

用户安全特性在防御用户对系统攻击的同时，也起到防御用户攻击网络设备、保护运营商网络的作用。

规格

系统支持的系统安全特性包括：

- 防御 ICMP/IP 攻击。
- 防御 DoS 攻击。
- MAC 地址过滤。

- 防火墙黑名单功能。
- 防火墙功能。
- 设置允许/拒绝访问地址段。

系统支持的用户安全特性包括：

- IP 地址绑定。
- 防御 MAC Spoofing。
- 防御 IP Spoofing。

20.2 系统安全

介绍系统安全特性的定义、目的、规格、原理以及参考的术语、缩略语。

20.2.1 防御 DoS 攻击

介绍防御 DoS 攻击特性以及在 UA5000 上的实现原理。

介绍

介绍该特性的定义、目的、规格和约束条件。

定义

DoS（Denial of Service）攻击指恶意用户发送大量的控制报文攻击系统，引起系统无法处理正常用户的服务请求（“拒绝对正常用户的服务”）。

防御 DoS 攻击特性指系统对用户发送的控制报文进行限制性接收的防御攻击措施。

目的

DoS 攻击影响系统的正常运行，可能引起系统无法接受正常用户的服务请求，甚至导致系统瘫痪。

为了保护系统，可以将系统接收的用户控制报文数量限制在正常范围内。对于超出范围的报文，作为非正常报文丢弃；对于发起 DoS 攻击的用户，将其加入黑名单，禁止其控制报文送交控制模块。

规格

- 系统能够防御用户以各种控制报文进行的 DoS 攻击，包括 PPPoE Discover 报文、DHCP 报文、ARP 报文、ICMP 报文、IGMP 报文、PPP LCP 报文、BPDU 报文。
- 支持最多 1984 项 DoS 攻击黑名单。
- 支持 DoS 攻击出现和消失时发出告警。

约束

以物理端口为粒度检测是否发生 DoS 攻击。

原理描述

介绍该特性的实现原理。

防御 DoS 攻击功能的实现原理如下：

- 系统维护一个 DoS 攻击黑名单。对于黑名单中的用户，系统管理维护人员可以手动强迫该用户下线（如进行“去激活端口”操作）。
- 打开防御 DoS 攻击控制开关时，根据下面的流程判断是否发生 DoS 攻击及是否停止攻击：
  - 系统对每个用户端口送交控制模块报文的情况进行监测，如果连续多次检测到某一个端口待送交控制模块的报文数远远超出用户正常业务发送的控制报文平均数目，则判断为发生 DoS 攻击。
  - 发生 DoS 攻击时，系统将该端口加入黑名单，并丢弃该端口的所有报文，并禁止该端口的报文送交控制模块。
  - 系统检测到用户不再进行 DoS 攻击时，将端口从黑名单中删除，允许该端口的报文送交控制模块。

20.2.2 防御 ICMP/IP 攻击

介绍防御 ICMP/IP 攻击特性以及在 UA5000 上的实现原理。

介绍

介绍该特性的定义、目的和规格。

定义

ICMP/IP 攻击是指恶意用户发送目的 IP 为系统 IP 的 ICMP 报文或 IP 报文，这些报文影响系统的正常运行。

防御 ICMP/IP 攻击特性是指系统丢弃从用户侧发给设备本身的 ICMP 报文、IP 报文。

目的

正常用户发送的报文，目的 IP 地址不会是系统的 IP 地址。但恶意用户则可能伪造目的 IP 地址为系统 IP 地址的 ICMP 报文或 IP 报文，对系统发起攻击。

防御 ICMP/IP 攻击特性可以识别并丢弃目的 IP 为系统 IP 地址的 ICMP 报文、IP 报文，从而对系统提供保护。

规格

无。

原理描述

介绍该特性的实现原理。

如果用户发出的 ICMP/IP 报文的目的 IP 地址为系统 IP 地址，则丢弃该报文。

20.2.3 MAC 地址过滤

介绍 MAC 地址过滤特性以及在 UA5000 上的实现原理。

介绍

介绍该特性的定义、目的、规格和约束。

定义

MAC 地址过滤指对用户报文携带的 MAC 地址进行检查，要求不能是指定的某些知名 MAC、网络设备 MAC，例如：LACP 协议的 MAC：01-80-C2-00-00-02、RIP 协议的 MAC：01-00-5E-00-00-09。

目的

MAC 地址过滤特性支持配置禁止用户携带的 MAC 地址，主要是为了防止恶意用户对运营商网络的攻击。

规格

系统支持 4 个源 MAC 地址及 4 个目的 MAC 地址的过滤。

约束

MAC 地址过滤特性和防御 MAC Spoofing 特性可以同时使用，此时 MAC 地址过滤的优先级更高（即禁止的优先级大于允许的优先级）。

可获得性

介绍该特性需要的硬件支持，包括单板和终端。

UA5000 所有的宽带接入业务单板支持本特性。

原理描述

介绍该特性的实现原理。

源 MAC 地址过滤功能的实现原理如下：

1. 为了防止用户假冒网络侧设备的 MAC 地址，可以将网络侧设备的 MAC 地址设置为要过滤的地址。
2. 用户报文上行时，系统检查源 MAC 地址，如果和配置的网络侧设备的 MAC 地址相同，则丢弃报文。

目的 MAC 地址过滤功能的实现原理如下：

1. 为了防止用户攻击接入侧设备，可以将接入侧设备的 MAC 地址设置为要过滤的地址。
2. 用户报文上行时，系统检查目的 MAC 地址，如果和配置的接入侧设备的 MAC 地址相同，则丢弃报文。

20.2.4 防火墙黑名单功能

介绍防火墙黑名单滤特性以及在 UA5000 上的实现原理。

介绍

介绍该特性的定义、目的、规格和约束条件。

定义

防火墙黑名单是一个 IP 地址集。防火墙黑名单功能是指系统过滤掉所有源 IP 地址在黑名单上的控制报文，从而提高系统安全性和网络安全性。

目的

防火墙黑名单特性的目的是通过设置黑名单屏蔽有恶意行为的 IP 地址用户对系统的攻击。

规格

- 支持手动配置 2000 条防火墙黑名单项。
- 配置黑名单项时支持指定 IP 地址的有效时间（老化时间），范围 1min ～ 1000min；如果不指定有效时间，则为不老化。

约束

启动防火墙黑名单功能的同时可以应用 ACL 规则，两者共同作用时，ACL 规则的优先级比防火墙黑名单的优先级要高。

原理描述

介绍该特性的实现原理。

防火墙黑名单功能的实现原理如下：

1. 如果报文的源 IP 地址为防火墙黑名单中的 IP 地址，则丢弃报文。
2. 对于匹配 ACL 规则的报文，如果 ACL 规则指定拒绝访问，则丢弃报文；如果指定允许访问，无论报文 IP 地址是否在黑名单列表中，都允许报文通过。

20.2.5 防火墙功能

介绍防火墙特性以及在 UA5000 上的实现原理。

介绍

介绍该特性的定义、目的、规格和约束条件。

定义

防火墙功能是指根据 ACL（Access Control List）进行数据包过滤，防止未授权的用户入侵系统的一种安全措施。

目的

通过设置包过滤防火墙，可以保证只有指定的用户才能通过维护网口（带外）或者业务通道（带内）对系统进行维护。

未授权的用户可能通过设备维护网口（带外）或者业务通道（带内）入侵系统，对系统进行非法操作，影响系统和运营商网络的正常运行。

规格

系统在以下接口支持防火墙功能：

- 设备维护网口
- 每个 VLAN 三层接口

每个接口可以分别针对出方向、入方向配置用于包过滤的 ACL 规则。

约束

- 防火墙必须根据 ACL 进行数据包的过滤，应用的 ACL 必须存在。如果没有配置 ACL，则根据缺省规则允许或禁止进行包过滤。
- 应用于防火墙的 ACL 规则必须是基本 ACL 规则或高级 ACL 规则。

原理描述

介绍该特性的实现原理。

防火墙功能的实现原理如下：

1. 使能防火墙功能后，当用户通过维护网口或者业务通道登录系统时，系统会根据配置在该接口上的 ACL 规则判断是否允许用户连接。不符合 ACL 规则要求的用户将被拒绝连接。
2. 此处 ACL 规则的内容一般是指允许访问的一组 IP 地址和/或禁止访问的一组 IP 地址，也可以指定协议类型、端口号等。

20.2.6 设置允许/拒绝访问地址段

介绍设置允许/拒绝访问地址段特性以及在 UA5000 上的实现原理。

介绍

介绍该特性的定义、目的、规格和约束条件。

定义

设置指定协议类型防火墙允许访问的 IP 地址段、拒绝访问的 IP 地址段。

目的

防止非法 IP 地址段的用户登录系统，维护系统的安全。

规格

系统支持通过 Telnet、SSH、SNMP 三种协议登录系统，对于每种类型，都支持设置允许/拒绝访问地址段功能。

每种类型的防火墙可以配置 10 条允许访问的 IP 地址段，10 条拒绝访问的 IP 地址段。

约束

- 增加一个地址段时，不允许首地址和已有地址段的首地址重复。

- 仅当使能指定协议类型防火墙功能后，才能使配置的基于该协议的允许通过 IP 地址段和拒绝访问地址段生效。

术语

表 20-1 设置允许/拒绝访问地址段特性术语表

术语	解释
SSH	用户通过一个不能保证安全的网络环境远程登录到设备时，SSH 特性可以提供安全的信息保障和强大的认证功能，以保护 Eudemon 防火墙不受诸如 IP 地址欺诈、明文密码截取等攻击。

缩略语

表 20-2 设置允许/拒绝访问地址段特性缩略语表

缩略语	英文全称	中文全称
ACL	Access Control List	访问控制列表
SSH	Secure Shell	安全外壳
SNMP	Simple Network Management Protocol	简单网络管理协议

原理描述

介绍该特性的实现原理。

用户以 Telnet、SSH 或 SNMP 协议登录系统时，系统检查用户的 IP 地址是否在允许或拒绝的 IP 地址段内，决定是否允许用户登录。

20.3 用户安全

介绍用户安全特性的定义、目的、规格、原理以及参考的术语、缩略语。

20.3.1 PITP

介绍 PITP 特性以及在 UA5000 上的实现原理。

介绍

介绍该特性的定义、目的、规格、约束条件、术语和缩略语。

定义

PITP（Policy Information Transfer Protocol）是在接入设备和 BRAS 之间定义的一种通过二层点对点通信方式实现策略信息传送的协议，用来传送用户物理端口信息，即 RAIO（Relay Agent Information Option），包括 V 模式、PITP sub-option90 模式和 P 模式。

- V 模式是由 BRAS 主动向接入设备查询用户物理位置信息的协议。
- P 模式则是系统在 PPPoE Discovery 阶段的 PPPoE 报文中添加用户物理位置信息，以方便 BRAS 进行用户认证的协议。
- PITP sub-option90 则是在使能 PPPoE+情况下，在 PPPoE Discover 阶段的 PPPoE 报文中加入用户的端口模式、用户的封装类型。

目的

PITP 特性的目的在于为上层的认证服务器提供接入用户的物理位置信息。BRAS 设备获取用户端口信息后，可实现对用户账号与接入端口的绑定认证，避免用户账号漫游或用户帐户被盗用。

规格

PITP 有两种模式：P 模式和 V 模式。

PITP 开关是全局级。只有开关打开，才会向 BRAS 提供用户物理位置信息，如果 PITP Sub-Option90 开关打开，还会添加用户的端口模式、用户的封装类型。

约束

- 系统在某一时间内只能设定 PITP 工作于某一种方式（V 模式或者 P 模式），不支持同时启动 V 模式和 P 模式。
- V 模式协议类型不能设置为标准的以太网协议类型。
- 在使用 V 模式时不允许设置 V 模式以太网协议类型。如果要修改缺省的 V 模式协议类型，必须先关闭 V 模式。
- PITP Sub-Option90 特性要在 PITP 功能的 pmode 使能后才会生效。缺省情况下，PITP Sub-Option90 特性开关处于关闭状态。

术语

无。

缩略语

表 20-3 PITP 特性缩略语表

缩略语	英文全称	中文全称
PITP	Policy Information Transfer Protocol	策略信息传送协议
PPPoE	Point to Point Protocol over Ethernet	以太网承载 PPP 协议
RAIO	Relay Agent Information Option	中继代理信息选项

可获得性

介绍该特性需要的硬件支持，包括单板和终端。

无需额外硬件支持。

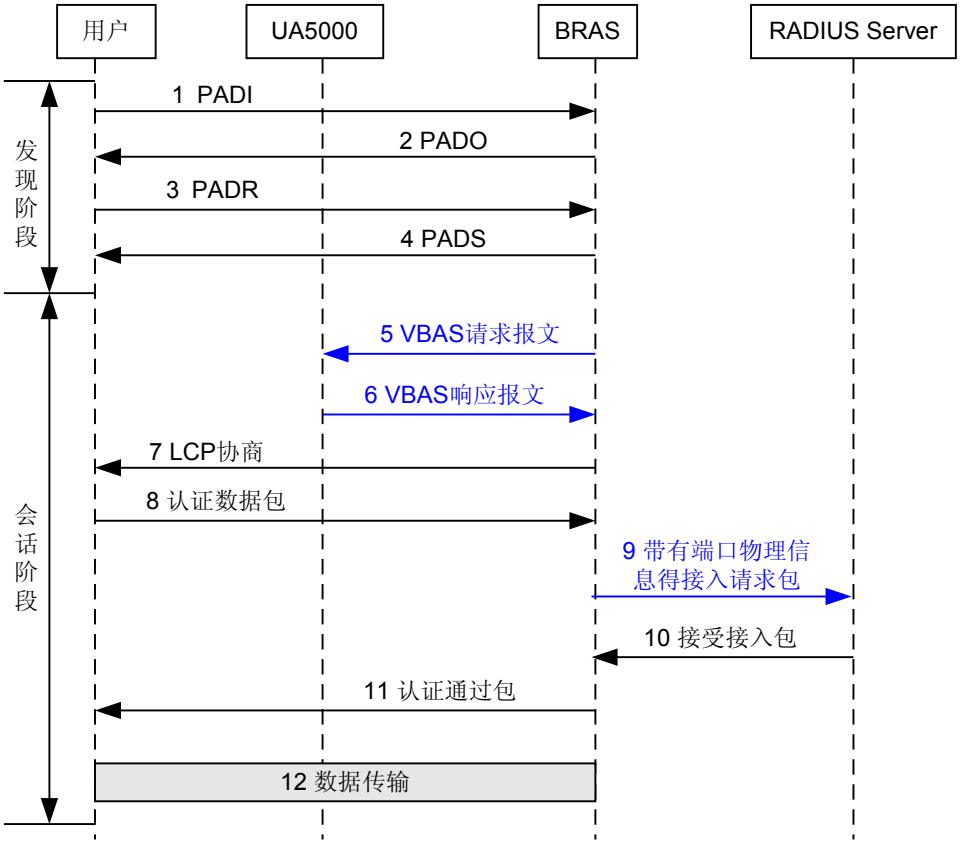
原理描述

介绍该特性的实现原理。

V 模式实现原理

启动 PITP 功能 V 模式后，PPPoE 拨号过程如图 20-2 所示。

图 20-2 启动 V 模式功能的 PPPoE 拨号过程



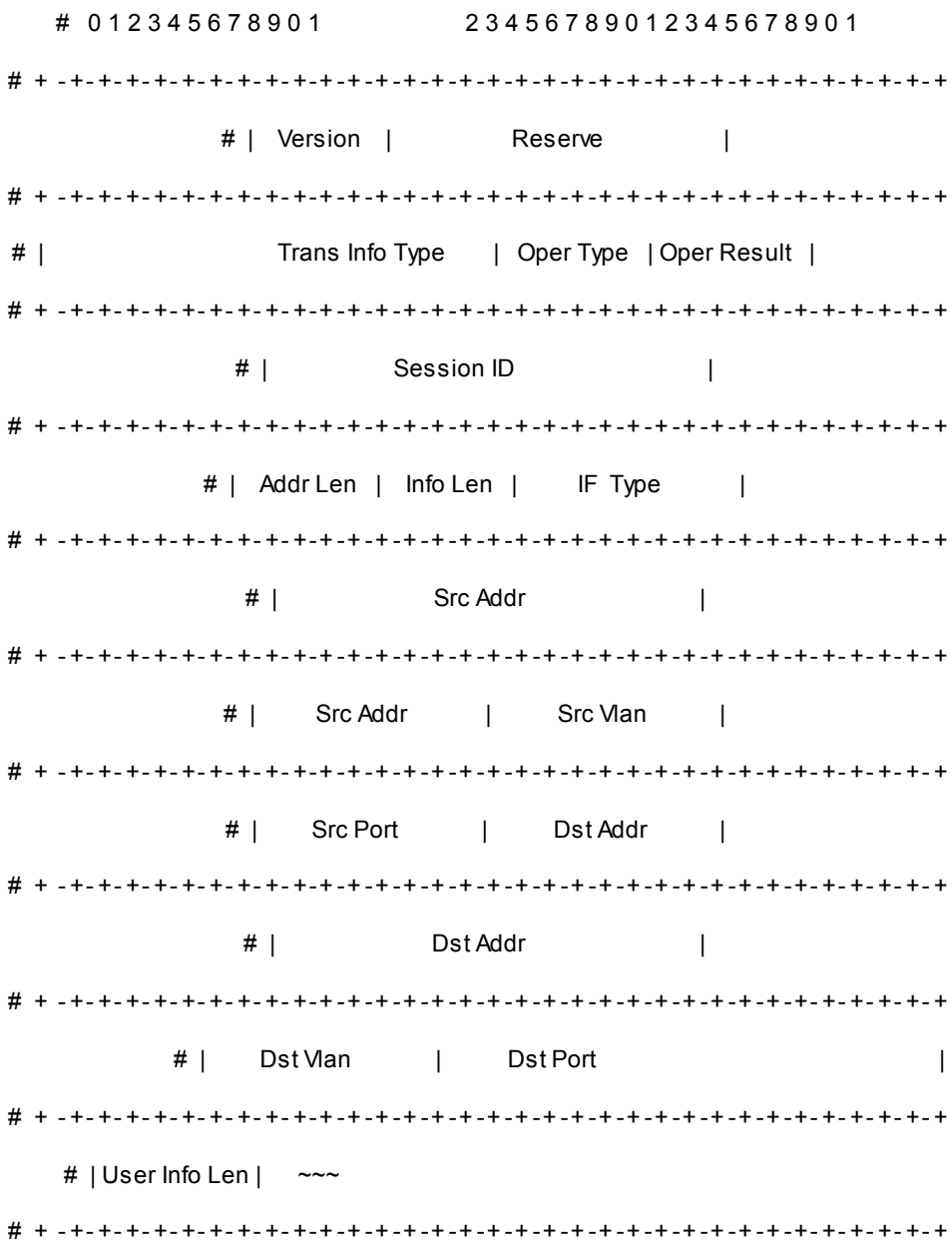
V 模式的三个过程为：

1. 在 PPPoE 发现阶段，当 BRAS 收到接入设备发送的 PADR 报文后，BRAS 向设备发送 V 模式请求报文，请求用户所在的物理位置信息。
2. 设备收到 V 模式请求报文后，根据 V 模式请求报文中的用户 MAC 和 VLAN 信息，查询用户所在的物理位置信息（包括框/槽/端口等）。
3. 如果查询成功，则向 BRAS 回应 V 模式应答报文，该 V 模式应答报文中包含接入用户的物理位置信息，否则不应答。

V 模式报文格式

常见的一种 V 模式报文的格式如图 20-3 所示。

图 20-3 常见的一种 V 模式报文格式



V 模式报文的以太网协议类型可以设置，默认为 0x8200。具体各个字段含义，如表 20-4 所示。

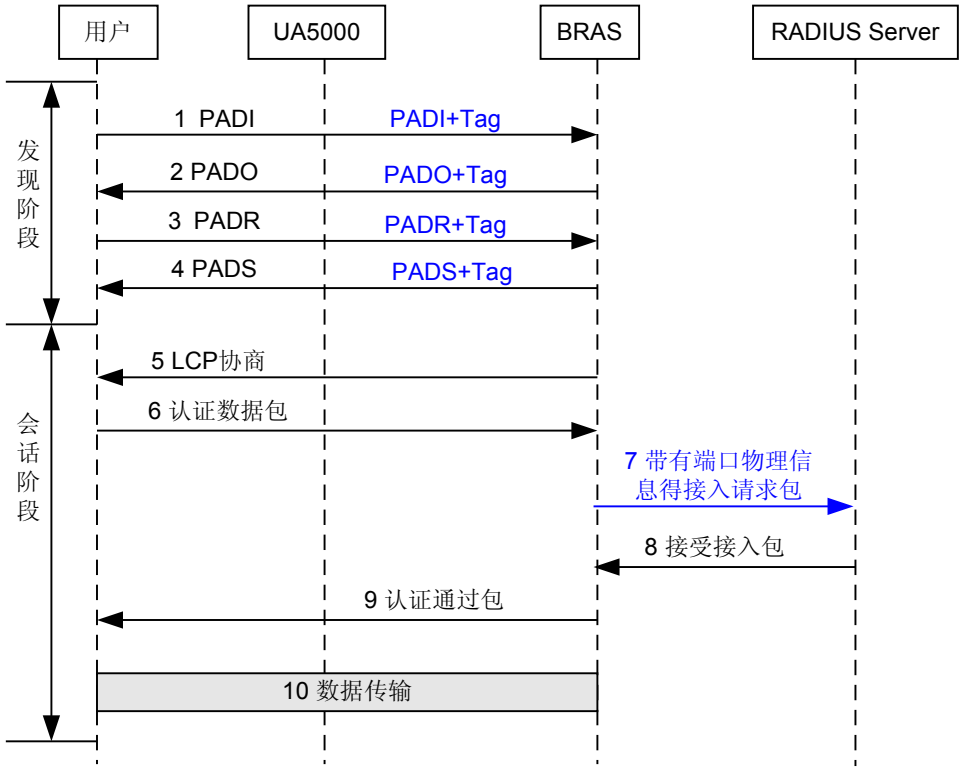
表 20-4 V 模式报文字段含义

报文字段	字段含义
Version	版本号，1 个字节，请求和响应报文中都填 1。
Reserve	保留字段，3 字节。
Trans Info Type	传送信息类型，2 字节，请求和响应报文都填 1，表示物理端口信息类型。以后可以扩展。
Oper Type	操作类型，1 字节，请求报文填 1，响应报文填 2。
Oper Result	操作结果，1 字节，请求报文填 0，响应报文成功填 0，无法识别报文内容填 1，目的 VLAN 不存在填 2，目的 MAC 不存在填 3。为了处理方便，只响应成功的，失败的情况没有响应。
Session ID	会话标识，4 字节，BAS 填写，响应报文同请求报文保持一致。
Addr LEN	硬件地址长度，1 字节，请求和响应报文都填 6。
Info LEN	信息长度，1 字节，请求响应报文都填 4。
IF Type	硬件接口类型，2 字节，请求报文填 0，响应报文根据用户接入端口的类型填写，以太网端口填 15，XDSL 端口填 16，详情参见 RFC2865。
Src Addr	源硬件地址，4 字节，请求报文填 BRAS 的 MAC 地址，响应报文填被查用户的 MAC 地址。
Src VLAN	源 VLAN ID，2 字节。请求报文填 PPPOE 发现阶段报文所带的 VLAN ID，不带 VLAN ID 的报文填全 F。响应报文填写 4/4/8bits 对应 F/S/P 端口的编码数值。系统填充时把 16bits 信息全部填入，不进行低 12bits 的截断处理，BRAS 处理时只使用低 12bits 信息。
Src Prot	源端口，2 字节，目前不使用。
Dst Addr	目的硬件地址，6 字节，请求报文填被查用户的 MAC 地址，响应报文填 BRAS 的 MAC 地址。
Dst VLAN	目的 VLAN ID，2 字节，取值同请求报文中的源 VLAN ID。
Dst Port	目的端口，2 字节，目前不使用。
User Info LEN	用户信息长度，1 字节，请求报文中该字段无效，响应报文中填写用户端口信息字符串的长度。用户端口信息为变长字符串，即 RAIO 信息，不同模式的具体格式请参见 **20.3.4 RAIO**。

P 模式实现原理

启动 PITP 功能 P 模式后，PPPoE 拨号过程如**图 20-4** 所示。

图 20-4 启动 P 模式功能的 PPPoE 拨号过程



启动 P 模式功能后，在 PPPoE Discovery 阶段，设备向用户侧发送的 PPPoE 报文中添加用户物理位置信息，以配合上层服务器进行用户认证，其它与 PPPoE 过程完全相同。

从图 20-4 可以看出，启动 P 模式功能和不启动 P 模式的 PPPoE 拨号过程的主要区别如下：

- 在 PPPoE Discovery 阶段，UA5000 和 BRAS 之间交互的 PPPoE 报文中都携带了用户位置信息。UA5000 负责在收到来自用户的 PPPoE 报文后插入用户位置信息，然后转发给 BRAS；收到来自 BRAS 的带用户位置信息的 PPPoE 报文后（BRAS 回传的 PPPoE 报文不一定携带用户位置信息），去除该信息，然后转发给用户。
- PPPoE 用户如果需要到 Radius 服务器认证，BRAS 则将来自 UA5000 的 PPPoE 报文中携带的用户位置信息提取出来，放到认证请求报文中，为服务器认证提供用户物理位置信息。

P 模式报文格式

PPPoE 报文格式如图 20-5 所示。

图 20-5 PPPoE 报文格式

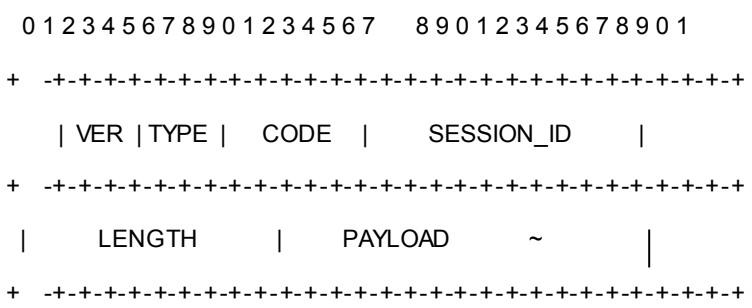
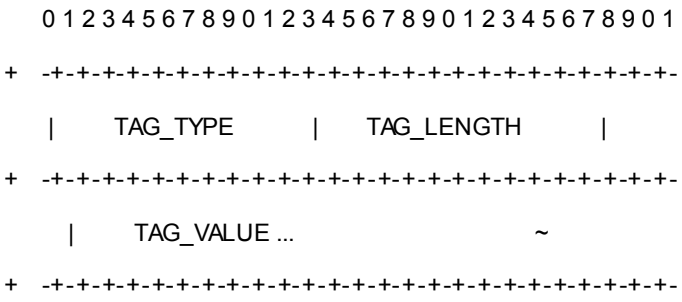


图 20-6 PPPoE 负载字段报文格式



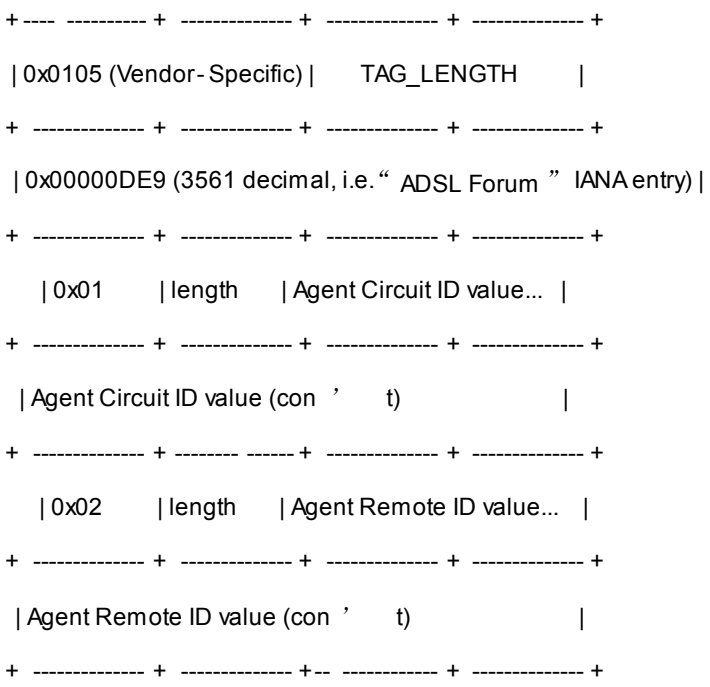
PPPoE 报文各字段具体含义，如**表 20-5** 所示。

表 20-5 PPPoE 报文字段含义

报文字段	字段含义
Version 和 Type	都填 1。
Code	表示 PPPoE 发现阶段的报文类型。Code 取值与 PPPOE 发现阶段报文类型的对应关系：PADI：0x09、PADO：0x07、PADR：0x19、PADS：0x65、PADT：0xa7。
SessionID	为会话 ID，通过用户与 BRAS 设备协商获取。
Length	表示 PPPoE 负载的长度。
PAYLOAD	全部采用 type-length-value 的格式，具体报文结构如**图 20-6** 所示。

在论坛上规定的 Vendor Tag（即 P 模式 Tag）格式如**图 20-7** 所示。

图 20-7 Vendor Tag 格式



为了满足不同客户的需求，支持多种格式的 tag 信息，即 RAIO 信息，不同模式的具体格式，请参见“**20.3.4 RAIO**”。

实施

介绍该特性的激活、调整和去激活的操作过程。

PITP 特性自动生效。如何激活、调整和去激活 PITP 特性的具体配置操作，请参见“UA5000 配置指南 IPM”的“配置用户安全”。

参考信息

介绍与该特性相关的参考信息。

本特性的参考资料清单如下：

- RFC2516，“PPP Over Ethernet”

20.3.2 DHCP Option82

介绍 DHCP Option82 特性以及在 UA5000 上的实现原理。

介绍

介绍该特性的定义、目的、规格、术语和缩略语。

定义

DHCP Option82 与 P 模式类似，在用户发起的 DHCP 请求报文的 Option82 字段中，填充用户的物理位置信息，以配合上层认证服务器进行用户认证。

目的

在 DHCP 请求报文中携带用户物理位置信息，配合服务器进行用户认证。

规格

DHCP Option82 开关分为三级：全局、端口和流。只有各个级别开关全部打开，系统才会在上行的 DHCP 报文中添加 Option82 信息。

术语

无。

缩略语

表 20-6 DHCP Option82 缩略语表

缩略语	英文全称	中文全称
DHCP	Dynamic Host Configuration Protocol	动态主机配置协议

可获得性

介绍该特性需要的硬件支持和 License 支持。

硬件支持

支持 DHCP Option82 特性的单板所有宽带业务接入板。

License 支持

DHCP Option82 特性是 UA5000 的可选特性，只有获得 License 许可后才能获得该特性的服务。

说明

UA5000 的 VLAN Stacking 特性、DHCP option82 特性、PPPoE 快速转发代理特性作为一个 License 功能项进行控制。

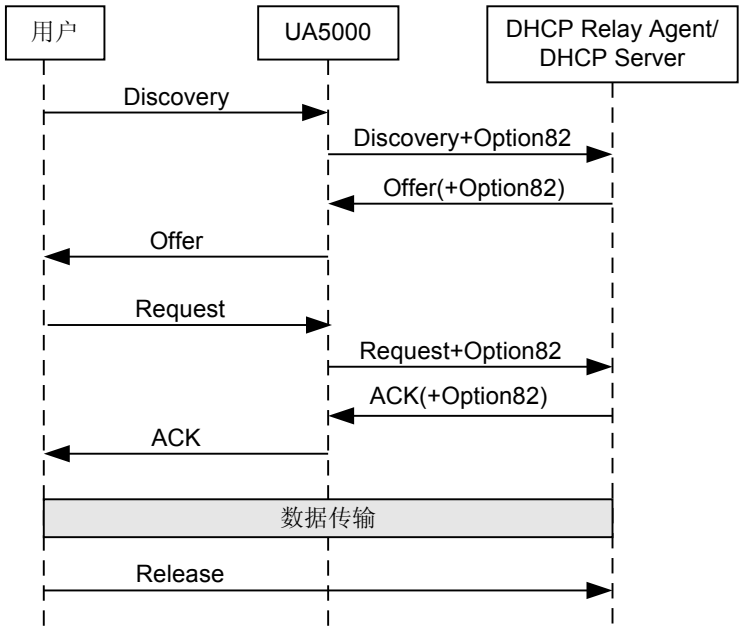
原理描述

介绍该特性的实现原理。

基本原理

DHCP Option82 功能启动时，DHCP 过程如图 20-8 所示。

图 20-8 启动 Option82 功能的 DHCP 过程



DHCP Option82 的原理与 P 模式类似，在用户请求配置阶段，在用户侧发送的 DHCP 报文中添加用户物理位置信息，以配合上层服务器进行用户认证，其它与一般的 DHCP 过程完全相同。

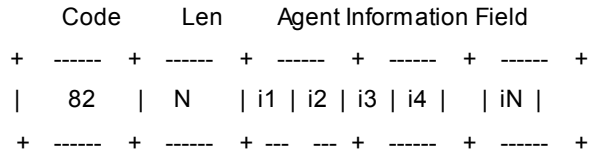
DHCP Option82 报文格式

对于 DHCP Option82 特性，仅需要关注 DHCP 报文中的 Option 字段，本文仅对 Option 字段进行详细介绍。

Option（可选变长选项）字段中包含了大量可选的终端初始配置信息和网络配置信息，如决定终端的 IP 特性配置信息，域名信息，标识终端的特殊信息，终端的默认网关 IP 地址，DNS 服务器的 IP 地址，WINS 服务器的 IP 地址，用户使用 IP 地址的有效租期等信息。

DHCP Option82 字段的报文格式如图 20-9 所示。

图 20-9 DHCP Option82 字段报文格式



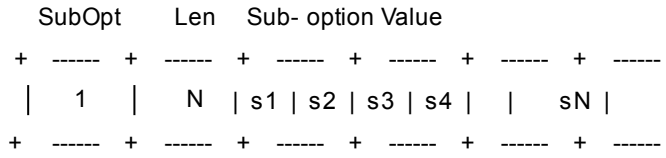
DHCP Option82 报文各字段具体含义，如表 20-7 所示。

表 20-7 DHCP Option82 报文字段含义

字段	含义
Code	此字段采用“CLV”方式构成，即 code:标识号，唯一标识后面的信息内容，占 1byte。
Len	表示后面信息内容的长度，占 1byte。
Agent Information Field	信息内容，其长度为 length 所指定，以 byte 为单位。

Option82 中包含多个子选项，每个子选项的内容都位于 Option82 的 Value 部分，各个子选项的格式如图 20-10 所示。

图 20-10 DHCP Option82 sub-option 格式



Option82 的子选项，主要有两个：CID（Circuit ID）和 RID（Remote ID）。

- CID 记录了接收用户侧 DHCP 报文的 DHCP 代理本地电路标识，如路由接口号、ATM PVC 号等，其子选项标识为 1。
- RID 用户用于标识该电路的远端主机，例如远端呼叫者的 ATM 地址、Modem ID 等，其子选项标识为 2。

与 P 模式类似，为了满足不同客户的需求，设备支持不同 Option82 的信息格式，不同模式的具体格式请参见“20.3.4 RAIO”。

实施

介绍该特性的激活、调整和去激活的操作过程。

DHCP Option82 特性自动生效。如何激活、调整和去激活 DHCP Option82 特性的具体配置操作，请参见“UA5000 配置指南 IPM”的“配置用户安全”。

参考信息

介绍与该特性相关的参考信息。

本特性的参考资料清单如下：

- RFC2131，“Dynamic Host Configuration Protocol”
- RFC3046，“DHCP Relay Agent Information Option”

20.3.3 DHCP Sub-Option90

介绍 DHCP Sub-Option90 特性以及在 UA5000 上的实现原理。

介绍

介绍该特性的定义、目的、规格、术语和缩略语。

定义

DHCP Sub-Option90 与 DHCP Option82 配合使用，只有在 DHCP Option82 使能情况下才能使能 DHCP sub-Option90 功能，在用户发起的 DHCP 请求报文中，填充用户的端口模式、单 PVC 多 VLAN 类型、用户的封装类型，以配合上层认证服务器进行用户认证。

目的

在 DHCP 请求报文中携带用户端口的模式、单 PVC 多 VLAN 类型、用户的封装类型。

规格

DHCP Sub-Option90 开关是全局级，只有 DHCP Option82 开关和 DHCP Sub-Option90 开关全部使能情况下，系统才会在上行的 DHCP 报文中添加 Sub-Option90 信息。

DHCP Sub-Option90 支持 TR-101 中包含的所有 DSL Line Characteristics。

术语

无。

缩略语

无。

可获得性

介绍该特性需要的硬件支持，包括单板和终端。

不需要额外硬件支持。

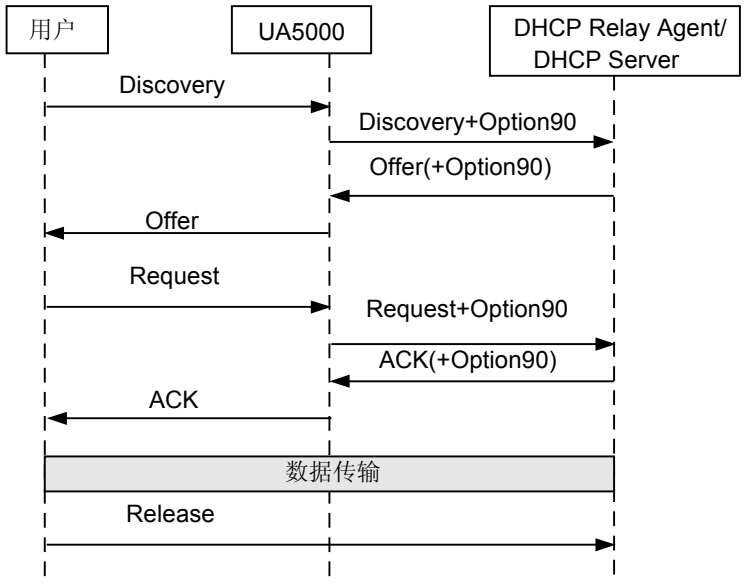
原理描述

介绍该特性的实现原理。

基本原理

DHCP Sub-Option90 功能启动时，DHCP 过程如**图 20-11** 所示。

图 20-11 启动 Sub-Option90 功能的 DHCP 过程



DHCP sub-Option90 在 DHCP Option82 使能的情况下才能使用，在用户请求配置阶段，在用户侧发送的 DHCP 报文中添加 sub-Option90 信息，以配合上层服务器进行用户认证，其它与一般的 DHCP 过程完全相同。

DHCP Sub-Option90 报文格式

Option（可选变长选项）字段中包含了端口的模式、单 PVC 多 VLAN 类型、用户的封装类型。

DHCP Sub-Option90 各子选项格式如图 20-12 所示。

图 20-12 DHCP Sub-Option90 子选项格式

Sub-option type	Length	Data link	Encaps 1	Encaps 2
0x90	0x03	1 byte	1 byte	1 byte

DHCP sub-Option90 报文各字段具体含义，如表 20-8 所示。

表 20-8 DHCP sub-Option90 报文字段含义

字段	含义
DataLink	此字段表明端口模式是 ATM 类型的端口还是以太网类型。当是 ATM 类型时此字段填充 0，是 Ethernet 类型时此字段填充 1。
Encaps1	此字段表明是否是单 PVC 多 VLAN 类型。如果是则用户带了一层 VLAN TAG，此字段填充 1；不是则是 UNTAG，此字段填充 0。
Encaps2	此字段表明用户的封装类型。如果获取封装类型失败时此字段填充 0；为 LLC-PPPOA 时此字段填充 1；为 VC-PPPOA 时此字段填充 2；为 LLC-IPOA 时此字段填充 3；为 VC-IPOA 时此字段填充 4；为 LLC-Bridge 且带 FCS 校验时此字段填充 5；为 LLC-Bridge 且不带 FCS 校验时此字段填充 6；为 VC-Bridge 且带 FCS 校验时此字段填充 7；为 VC-Bridge 且不带 FCS 校验时此字段填充 8。

说明

UA5000 不支持 FCS 校验。

DHCP Sub-Option90 支持 TR-101 中包含的所有 DSL Line Characteristics。

实施

介绍该特性的激活、调整和去激活的操作过程。

DHCP sub-Option90 特性缺省是关闭的。

DHCP Option82 特性使能后，DHCP sub-Option90 配置使能才能生效

DHCP Sub-Option90 支持 TR-101 中包含的所有 DSL Line Characteristics。

如何配置 DHCP sub-Option90 特性的具体配置操作，请参见“UA5000 配置指南 IPM”的“配置用户安全”。

参考信息

介绍与该特性相关的参考信息。

本特性的参考资料清单如下：

- RFC1531，“Dynamic Host Configuration Protocol”
- RFC3046，“DHCP Relay Agent Information Option”

20.3.4 RAIO

介绍 RAIO 特性以及在 UA5000 上的实现原理。

介绍

介绍该特性的定义、目的、规格、术语和缩略语。

定义

RAIO（Relay Agent Information Option）是 PITP 和 DHCP Option82 功能使能时，设备在 VBAS 应答报文（PITP V-mode）、PPPoE Discovery 报文（PITP P-mode）和 DHCP 报文（DHCP Option82）向 BRAS 提供的用户物理位置信息，如设备上的框/槽/端口等。

目的

RAIO 的目的在于设备向 BRAS 提供用户的物理位置信息。

规格

RAIO 主要包括 PITP Tag 和 DHCP Option82 Tag，目前尚没有标准化，因此不同的运营商提出的格式可能都不一样。为了满足不同运营商的个性化需求，提供了多个 RAIO 工作模式供选择。

RAIO 工作模式包括：common、xdsl-port-rate、cntel、port-userlabel、bt。

缺省情况下，RAIO 工作模式为 common 模式。

对 PITP 和 DHCP Option82，其 RAIO 模式不能分别配置，RAIO 配置完后对这两种都有效。

DHCP Sub-Option90 是 DHCP option82 特性的一个子选项，只有开启了 DHCP Option82 特性，DHCP Sub- Option90 特性才会生效。缺省情况下，DHCP Sub-Option90 特性开关处于关闭状态。

对于 PITP Sub-Option90 特性要在 PITP 功能的 pmode 启动后才会生效。缺省情况下，PITP Sub-Option90 特性开关处于关闭状态。

术语

无。

缩略语

表 20-9 RAIO 特性缩略语表

缩略语	英文全称	中文全称
RAIO	Relay Agent Information Option	中继代理信息选项
BRAS	Broadband Remote Access Server	宽带接入服务器

可获得性

介绍该特性需要的硬件支持，包括单板和终端。

无需额外硬件支持。

原理描述

介绍该特性的实现原理。

下面针对 RAIO 支持的各种模式，分别介绍其字段格式及具体含义。

Common 模式

CID 格式一般用于标识设备的属性信息（全局信息）。根据接入方式的不同，格式也有所不同，不同接入方式的 CID 格式表 20-10 所示。

表 20-10 不同接入方式的 CID 格式

接入方式	CID 格式
ATM 类型端口	设备名 atm 框号/槽号/子槽/端口号:vpi.vci
VDSL/LAN 接入方式	设备名 eth 框号/槽号/子槽/端口号:vlanid

- 当设备名字段为缺省名字“UA5000”时，使用设备的 MAC 地址来填充设备名字段，格式为“00E0FC000001”，采用大写。
- 当设备名不为“UA5000”时，采用实际的设备名填充设备名字段。

RID 格式一般用于标识用户的接入信息（局部信息）。通常为自定义格式，在 UA5000 中，该部分不填充，所以 RID 信息就只有 Code 和 Len 字段，没有 Value 字段。

Common 模式 RAIO 字段格式举例：

- CID ---------> 00E0FC112233 atm 0/12/0/49:0.35
- RID ---------> NULL（不填）

xDSL Port Rate 模式

xDSL Port Rate 模式是在 CID 默认格式后面加上 ADSL 端口上下行的激活速率，目前仅支持 ADSL2+单板。

RAIO 字段具体格式如下所示。

“AccessNodeIdentifier {atm|eth} frame/slot/subslot/port[:vpi.vci|vlan]%Up：xxxkbps Dowm：xxxkbps”

- %：信息标识符，表示后面是激活速率。
- XXX：以 kbps 为单位的 ADSL 端口激活速率。
- Up：表示上行激活速率。
- Down：表示下行激活速率。

xDSL Port Rate 模式 RAIO 字段格式举例：

- CID ----> 00E0FC112233 atm 0/12/0/49:0.35%Up:1020kbps Down:24540kbps
- RID ----> NULL(不填)

CNTEL 模式

CNTEL 模式是中国电信要求的编码格式，RAIO 字段具体格式如下所示：“NAS_slot/NAS_subslot/NAS_port:XPI.XCI AccessNodeIdentifier/ANI_rack/ANI_frame/ANI_slot/ANI_subslot/ANI_port[:ANI_XPI.ANI_XCI]”

其中各字段解释如下：

- NAS_slot：BRAS 槽号 0~31
- NAS_subslot：BRAS 子槽号 0~31
- NAS_Port：BRAS 端口号 0~63
- XPI: 如接口类型为 atm，XPI 对应于 VPI，XPI 为 0~255；如接口类型为 eth（或 trunk）,XPI 对应于 PVLAN，XPI 为 0~4095
- XCI: 如接口类型为 atm，XCI 对应于 VCI，XCI 为 0~65535；如接口类型为 eth（或 trunk）,XCI 对应于 CVLAN，XCI 为 0~4095
- AccessNodeIdentifier：接入节点标识，长度不超过 50 个字符的字符

中国电信宽带用户接入线路标识编码格式要求串，字符串中间不能有空格。

- ANI_rack：接入节点机架号（如支持紧耦合的 UA5000 设备） 0~15
- ANI_frame：接入节点机框号 0~31
- ANI_slot: 接入节点槽号 0~127
- ANI_subslot: 接入节点子槽号 0~31
- ANI_port：接入节点端口号 0~255
- ANI_XPI：可选项，如接口类型为 atm，XPI 对应于 VPI，XPI 为 0~255；如接口类型为 eth，XPI 对应于 PVLAN，XPI 为 0~4095
- ANI_XCI：如接口类型为 atm，XCI 对应于 VCI，XCI 为 0~65535；如接口类型为 eth,XCI 对应于 CVLAN，XCI 为 0~4095
- ANI_XPI.ANI_XCI，主要是携带 CPE 侧的业务信息，可用于标识未来的业务类型需求，如在多 PVC 应用场合下可标识具体的业务。字符串之间用一个空格隔开，要求字符串中间不能有空格。

对于某些设备没有机架、框、子槽的概念，相应位置应统一填 0,对于无效的 VLAN ID 值都填 4096。

如接口类型为 ATM，则 AccessNodeIdentifier 、ANI_rack、ANI_frame、ANI_slot、

ANI_subslot、ANI_port 域可统一填 0。如运营商未使用 SVLAN 技术，则 XPI=4096,XCI=VLAN,取值为 0~4095。

如运营商未使用 VLAN 技术区分用户（用户 PC 直连 BAS 端口），则 XPI=4096,XCI=4096。

目前 NAS_slot/NAS_subslot/NAS_port:XPI 中国电信要求固定填为 0 0/0/0:4096。

举例：CID ----> 0 0/0/0:4096.101 00E0FC112233/0/0/12/0/49:0.35

RID ----> NULL(不填)

Port-userlabel 模式

Port-userlabel 模式中，CID 除了携带普通格式所描述的信息外，还需要用户所在端口的 LABEL，即自定义的端口描述信息，最大长度 32 字节。在 RID 中也要带上端口 label。

Port-userlabel 模式 RAIO 字段格式举例：

- CID ----> 00E0FC112233 atm 0/12/0/49:0.35 075528978944
- RID ----> 075528978944

User-defined 模式实现原理

用户可以指定 CID/RID 的字符串格式，这里介绍自定义模式的语法规则。

- 只支持对系统中已定义关键字段集和分隔符集的解析。关键字段集包括 TR-101 定义的关键字段最小集合及 IAS 扩展的关键字集合，如**表 20-11** 所示。
- 最大宽度

  指关键字对应数据的最大占用列数（系统中定义的关键字的最大宽度有些比标准有所增加，主要是考虑到有些厂商的需求已经超出了标准的最大宽度）。接入节点的名称 ANID 的最大宽度受限于系统名称最大字符串长度（目前只支持 50 字符）。
- 可订宽度

  指关键字对应数据的占用列数可配置，用于数据占用列数不足所订宽度后在前面补 0 的情况。语法为：关键字 0m，m 为占用列数。例：slot03，表示 Slot 的字段长度为 3，不足 3 位的前面补 0，如果槽位号为 2 则报文中为 002；m 必须不大于最大宽度，如果数据所占列数大于 m，则按实际列数输出。

表 20-11 用户自定义关键字段集

关键字	描述	可订宽度	最大宽度
ANID	接入节点的名称	No	63
ETH	ETH 接入方式	No	3
ATM	ATM 接入方式	No	3
Chassis	接入节点的机架号	Yes	4
Rack	接入节点的机架号	Yes	4
Frame	机框号	Yes	4
Slot	槽位号	Yes	4
Subslot	子槽位号	Yes	4
Port	端口号	Yes	4
VLANID	如果用户所在业务虚端口承载的业务是根据用户侧的 vlanid 进行区分的，此 VLANID 为用户侧的 vlanid，除此之外为网络侧的 vlanid	Yes	4
Priority	对于二层 PPPoE 与 DHCP Option82 为用户所在的业务虚端口流量模板的优先级，对于 PPPoA 转 PPPoE 固定为 6，对于三层 DHCP Option82 固定为 2	Yes	4
Plabel	用户所在端口的 label	No	32
SPlabel	用户所在业务虚端口的 label	No	63

关键字	描述	可订宽度	最大宽度
Bslot	BRAS 槽位号	Yes	4
Bsubslot	BRAS 子槽号	Yes	4
Bslot	BRAS 槽位号	Yes	4
Bport	BRAS 接入端口号	Yes	4
Bporttype	BAS 接入方式	Yes	4
VPI	适用接入方式为 ATM，VPI 为用户端口的 VPI	Yes	4
VCI	适用接入方式为 ATM，VCI 为用户端口的 VCI	Yes	5
XPI	网络侧 VLAN 的属性为 stacking XPI 为网络侧的 vlanid	Yes	4
	网络侧 VLAN 的属性不为 stacking XPI 固定为 4096		
XCI	网络侧 VLAN 的属性为 stacking XCI 为用户所在业务虚端口的标签值	Yes	5
	网络侧 VLAN 的属性不为 stacking XCI 为网络侧的 vlanid		
AXPI	如果为 ATM 接入方式，AXPI 对应于 VPI	Yes	4
	如果为 ETH 接入方式，AXPI 对应于网络侧的 vlanid		
AXCI	如果为 ATM 接入方式，AXCI 对应于 VCI	Yes	5
	如果为 ETH 接入方式： 网络侧 VLAN 的属性为 stacking，如果用户所在业务虚端口承载的业务是根据用户侧的 vlanid 进行区分的，AXCI 为用户侧的 vlanid，如果不是根据用户侧的 vlanid 进行区分，AXCI 为用户所在业务虚端口的标签值 网络侧 VLAN 的属性不为 stacking，如果用户所在业务虚端口承载的业务是根据用户侧的 vlanid 进行区分的，AXCI 为用户侧的 vlanid，如果不是根据用户侧的 vlanid 进行区分，AXCI 固定为 4096		
UpRate	xDSL 线路上行激活速率，以 kbit/s 为单位	Yes	10
DnRate	xDSL 线路下行激活速率，以 kbit/s 为单位	Yes	10

- 如果用户针对 CID 定义 RAIO 的格式，则格式字符串中必须含有接入节点的名称 ANID 的关键字。

- 接口类型关键字用于识别不同接口类型的格式。
- 不允许格式字符串中同时出现适用不同接口类型的关键字；例如同时出现 ETH 与 VCI 是不合法的。
- 如果未指定某种接口类型，则这种接口类型对应的 CID/RID 字段的内容为空。
- 分隔符在用户输入 RAIO 模式字符串时起识别作用，代表相应的符号，分隔符表示的符号会最终添加到 CID/RID 中。系统定义的 RAIO 分隔符，如表 20-12 所示。

表 20-12 用户自定义分隔符集

分隔符	表示符号
空格	空格“ ”
.	句点“.”
:	冒号“：”
/	斜线“/”
-	连字符“-”
%	百分号“%”

- 其他规则
- 长度为 1 ～ 127 个字符，全部为小写字母。
- CID 字符串必须带接入节点的名称关键字 ANID。
- 接入节点名称关键字 ANID 必须出现在依赖接口类型关键字的前面。
- CID 字符串中关键字 ANID 前面的全部分隔符和 ANID 所代表的系统名称中的 RAIO 分隔符（如果有的话）以及 ANID 后面的一个分隔符，作为下行报文解析识别关键字 ANID 的依据。

实施

介绍该特性的激活、调整和去激活的操作过程。

RAIO 特性自动生效。如何激活、调整和去激活 RAIO 特性的具体配置操作，请参见“UA5000 配置指南 IPM”的“配置用户安全”。

参考信息

介绍与该特性相关的参考信息。

本特性的参考资料清单如下：

- RFC3046，“DHCP Relay Agent Information Option”
- DSL Forum, TR-101，“Migration to Ethernet-Based DSL Aggregation”

20.3.5 IP 地址绑定

介绍 IP 地址绑定特性以及在 UA5000 上的实现原理。

介绍

介绍该特性的定义、目的、规划、术语和缩略语。

定义

IP 地址绑定，是指在业务虚端口上绑定 IP 地址。业务虚端口绑定 IP 地址后，设备只允许源地址是被绑定地址的上行报文通过，并丢弃源地址为其它地址的报文。

目的

IP 地址绑定可以对用户进行认证，保证运营商的利益。

规格

系统支持 1024 个业务虚端口进行 IP 地址的绑定，每个业务虚端口最多可以绑定 8 个 IP 地址。

术语

无。

缩略语

无。

可获得性

介绍该特性需要的硬件支持，包括单板和终端。

无需额外硬件支持。

原理描述

介绍该特性的实现原理。

在业务虚端口绑定 IP 地址后，业务转发模块对用户侧报文的源 IP 地址进行检查。如果用户侧的源 IP 地址与接收该用户报文的业务虚端口所绑定的所有 IP 地址都不相同，则进行丢弃，否则允许通过。

实施

介绍该特性的激活、调整和去激活的操作过程。

IP 地址绑定特性自动生效。如何激活、调整和去激活 IP 地址绑定特性的具体配置操作，请参见“UA5000 配置指南 IPM”的“配置用户安全”。

20.3.6 防御 MAC Spoofing

介绍防御 MAC Spoofing 特性以及在 UA5000 上的实现原理。

介绍

介绍该特性的定义、目的、规格、约束、术语和缩略语。

定义

MAC Spoofing 攻击指恶意用户伪造 MAC 地址发送报文攻击系统。如果伪造正常用户的 MAC 地址，则会影响正常用户的业务；如果伪造系统的 MAC 地址，或者向系统发送大量含有不同 MAC 地址的伪造报文，则可能导致系统不能正常工作，甚至系统瘫痪。

防御 MAC Spoofing 攻击特性指系统防御用户伪造 MAC 地址进行攻击的措施。

目的

为了保护系统和运营商网络，对于 PPPoE 接入用户和 DHCP 接入用户，可以禁止动态 MAC 地址学习，仅允许有限的、系统认为可以信任的 MAC 地址通过，从而避免不可信任的大量 MAC 地址进入运营商网络的情况。

同时，恶意用户伪造已上线的正常用户的 MAC 地址的行为也会被发现和禁止，从而保护正常用户的业务不受影响。

规格

系统最多允许 1024 个业务虚端口动态绑定 MAC 地址，每个业务虚端口最多允许动态绑定 8 个 MAC 地址。

约束

- 对于静态 IP 地址用户，如果使能防御 MAC Spoofing 特性，必须手工配置静态 MAC 地址。
- 使能防御 MAC Spoofing 功能将禁止动态 MAC 地址学习。

术语

无。

缩略语

无。

可获得性

介绍该特性需要的硬件支持，包括单板和终端。

所有的宽带接入的业务单板支持本特性。

原理描述

介绍该特性的实现原理。

PPPoE 用户防御 MAC Spoofing

系统对于 PPPoE 用户防御 MAC 欺骗的实现原理如下：

1. 打开防御 MAC Spoofing 特性开关后，系统根据用户发送的 PPPoE 报文将 MAC 地址和用户绑定
2. 用户在 MAC 地址绑定之前发送的数据报文将被丢弃

3. 用户报文携带的源 MAC 地址如果和已经绑定的 MAC 地址相同，则允许报文上行，否则丢弃
4. 用户下线时，系统解除 MAC 地址和用户的绑定

DHCP 用户防御 MAC Spoofing

系统对于 DHCP 用户防御 MAC 欺骗的实现原理如下：

1. 打开防御 MAC Spoofing 特性开关后，系统根据用户发送的 DHCP 报文将 MAC 地址和用户绑定
2. 用户在 MAC 地址绑定之前发送的数据报文将被丢弃
3. 用户报文携带的源 MAC 地址如果和已经绑定的 MAC 地址相同，则允许报文上行，否则丢弃
4. 用户下线时，系统解除 MAC 地址和用户的绑定

实施

介绍该特性的激活、调整和去激活的操作过程。

防御 MAC Spoofing 特性自动生效，无需配置。

如何调整防御 MAC Spoofing 特性的具体配置操作，请参见“UA5000 配置指南 IPM”的“配置用户安全”。

20.3.7 防御 IP Spoofing

介绍防御 IP Spoofing 特性以及在 UA5000 上的实现原理。

介绍

介绍该特性的定义、目的、规格、约束、术语和缩略语。

定义

IP Spoofing 攻击指恶意用户伪造 IP 地址发送报文攻击系统。防御 IP Spoofing 攻击特性指系统防御用户伪造 IP 地址进行攻击的措施。

目的

为了保护系统和运营商网络，对于 DHCP 接入用户，可以开启防御 IP Spoofing 功能，仅允许有限的、DHCP Server 分配的 IP 地址通过，从而避免恶意用户伪造的或不可信任的 IP 地址进入运营商网络的情况。

规格

系统最多允许 1024 个业务虚端口动态绑定 IP 地址。

每个业务虚端口最多允许动态绑定 8 个 IP 地址。

约束

对于 DHCP 接入用户，不要手工配置 IP 地址和用户的绑定，由防御 IP Spoofing 特性保证进入运营商网络的 IP 地址受控；对于静态 IP 地址用户，需要手工配置 IP 地址绑定才能保证进入网络的 IP 地址受控。

术语

无。

缩略语

无。

可获得性

介绍该特性需要的硬件支持，包括单板和终端。

UA5000 支持本特性的宽带接入业务单板包括：SHLB、ADRI/ADRB 和 VDMB。

原理描述

介绍该特性的实现原理。

防御 IP Spoofing 的实现原理如下：

1. 打开防御 IP Spoofing 特性开关后，系统根据用户发送的 DHCP 报文将 IP 地址和用户绑定。
2. 用户在 IP 地址绑定之前发送的数据报文将被丢弃。
3. 用户报文携带的源 IP 地址如果和已经绑定的 IP 地址相同，则允许报文上行，否则丢弃。
4. 用户下线时，系统解除 IP 地址和用户的绑定。

实施

介绍该特性的激活、调整和去激活的操作过程。

防御 IP Spoofing 特性自动生效。如何激活、调整和去激活防御 IP Spoofing 特性的具体配置操作，请参见“UA5000 配置指南 IPM”的“配置用户安全”。

21 Ethernet CFM OAM

关于本章

Ethernet CFM OAM 提供了端到端的故障检测手段，可以对以太网进行监控、诊断、检查故障。本特性从介绍、原理描述和参考信息方面进行描述。

21.1 介绍

介绍该特性的定义、目的和规格等信息。

定义

OAM 定义

OAM （Operations, Administration and Maintenance 操作管理维护）泛指监控，诊断网络故障的工具。

Ethernet CFM OAM 定义

Ethernet CFM OAM 提供了端到端的故障检测手段，可以对以太网进行监控、诊断、检查故障。其由 IEEE 802.1ag 进行定义。

MD 定义

MD（Maintenance Domain）：维护域。指被 CFM 管理的网络范围，可以是被管理的整个网络或者网络的一部分区域，其范围由桥接设备和维护域级别共同决定。

MD Level：维护域级别。分为 0 ～ 7 共 8 个级别，数值越大表示维护域的级别越高，其携带于 CFM 报文中。高级别维护域的 CFM 报文可以穿越低级别维护域，从而实现不同级别的 MD 可嵌套部署。

MA 定义

MA（Maintenance Association）：维护集。在维护域下可以划分若干个维护集，每个维护集对应维护域上的一个业务实例 SI（Service Instance），此业务实例用 VLAN 来标识，即维护集是维护域和 VLAN 的组合。Ethernet CFM OAM 对每个 MA 分别进行连通性故障检测。

MA 由维护节点 MP（Maintenance Point）组成。MP 定义在桥接设备的端口上，即 MP 是桥端口、VLAN 和维护级别的组合。MP 分为维护实体端点（MEP）和维护实体中间点（MIP）。

MEP 定义

MEP(Maintenance association End Point)：维护实体端点。MEP 是 MA 的边缘节点，和其他 MP 共同组成 MA 维护集。设备在每个 MA 中可配置一个 MEP，MEP 关联一个设备的一个端口。

MEP 分为 UP MEP 和 Down MEP。

UP MEP 表示朝桥中继方向发送报文，Down MEP 表示朝物理介质方向发送报文。设备端口定义 MEP 的同时必须定义其为 UP MEP 或者 Down MEP，且只能定义为一种 MEP。即设备端口定义为 MEP，其只能朝一个方向发送报文。

举例说明：定义上行端口为 MEP，如果定义此 MEP 只能朝上行方向（汇聚层）发送 CFM 报文，则此 MEP 就是 Down MEP；如果定义此 MEP 只能朝下行方向（朝向用户）发送报文，则此 MEP 就是 UP MEP。

RMEP 定义

RMEP（Remote Maintenance association End Point）：远端维护实体端点。运行 Ethernet CFM OAM 的任意一台设备，该设备上的 MEP 称为本地 MEP。同一个 MA 内其它设备上的 MEP 对本设备而言称为远端维护实体端点 RMEP。

MIP 定义

MIP(Maintenance domain Intermediate Point)：维护域中间节点。在 MD 内转发路径桥设备端口上创建，用于转发路径的探测及故障定位。

MIP 由两个 MHF(MIP Half Function)构成。MHF 同维护级别和 VLAN 相关，只响应接收到的 CFM 消息。

规格

- 支持最多 8 个维护域（Maintenance Domain, MD）。
- 每个 MD 下支持最多 256 个维护集 MA（Maintenance Association, MA）。
- 所有 MD 下支持最多 256 个维护集 MA。
- 每个 MA 下支持 1 个维护实体端点（Maintenance End Point，MEP），1 个 MEP 对应 1 个远端维护实体端点（Remote Maintenance End Point，RMEP）。
- 连续性检查消息（Continuity Check Message，CCM）发送周期可以配置为 1m、10m。

约束

- 只能在上行口上配置 MEP。
- 不支持配置用户侧的维护关联中间节点 MIP（Maintenance association Intermediate Point）及内向端口。

21.2 可获得性

介绍该特性需要的硬件支持。

涉及网元

Ethernet CFM OAM 需要两个或两个以上网元配合才能完成。

与 UA5000 配合的网元需要兼容 IEEE 802.1ag-2007 VLAN Amendment 5 Connectivity Fault Management 标准。

License 支持

Ethernet CFM OAM 特性是 UA5000 的可选特性，只有获得了 License 许可后才能获得该特性的服务。

硬件要求

上行口仅 GE 接口支持本特性，其他接口不支持。用户侧接口暂时不支持。

21.3 原理描述

介绍该特性的实现原理。

说明

本特性中，除非特别说明，MEP 代指 UA5000 设备端口。

CFM 诊断、故障检测的手段包括：

- 连续性检查 CC（Continuity Check）
- 环回检测 LB（Loop Back）
- 链路跟踪 LT（Link Trace）

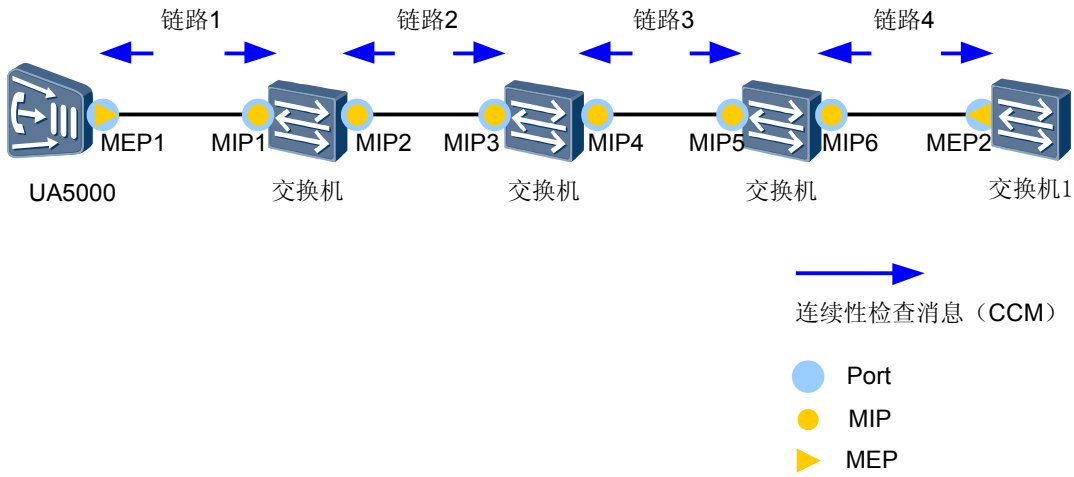
连续性检查

为了保证两台设备的连通性（假设 UA5000 和交换机 1），将两台设备配置在同一个维护域内（假设 MD 0）的同一个维护集（假设 MA 0）下，并将两设备互相配置成远端。

- UA5000：假设在上行端口配置 MEP1，如图 1-1 所示，MEP1 需要向上行方向发送报文，则 MEP1 配置为 Down MEP。
- 交换机 1：假设在交换机 1 的端口配置 MEP2，如图 21-1 所示，MEP2 需要向 UA5000 方向发送报文，则 MEP2 配置为 Down MEP。

连续性检查原理如图 21-1 所示。

图 21-1 连续性检查原理图



CCM（Connectivity Check Message）连续性检查消息通过向域内组播发送的定时消息来监控网络的连通性，原理描述如下：

1. 每个 MEP（例如：MEP1）主动周期性向域内组播发送定时“hello”消息（CCM），消息中携带了本端设备的配置信息。
2. 所有域内 MIP 和 MEP（例如：MEP2）都可以收到 CCM，但无需响应。
3. 收到 CCM 的 MIP 和 MEP2 会建立 MEP 数据库格式如：[MEP DA, Port]。MEP2 接收到 MEP1 的消息后会对消息中携带的信息进行检查，并会存储 CCM，了解不同的 MA。
4. 在 MEP2 上需要配置一组期望的 MEP 源地址（该举例中是 MEP1），如果 MEP2 在一定时间内收不到 CCM 或 CCM 中携带的信息不是 MEP2 期待的信息（MEP2 会用收到的 CCM 与期望 MEP 源地址，即 MEP1 比较），则认为 UA5000 和交换机 1 之间的网络出现故障。
5. 交换机 1 则会上报丢失消息告警。

说明

连续性检查（CC）只能判断网络出现故障，但不能具体定位是哪一段链路出现故障。

当网络出现故障时，可能有如下情况，并产生告警：

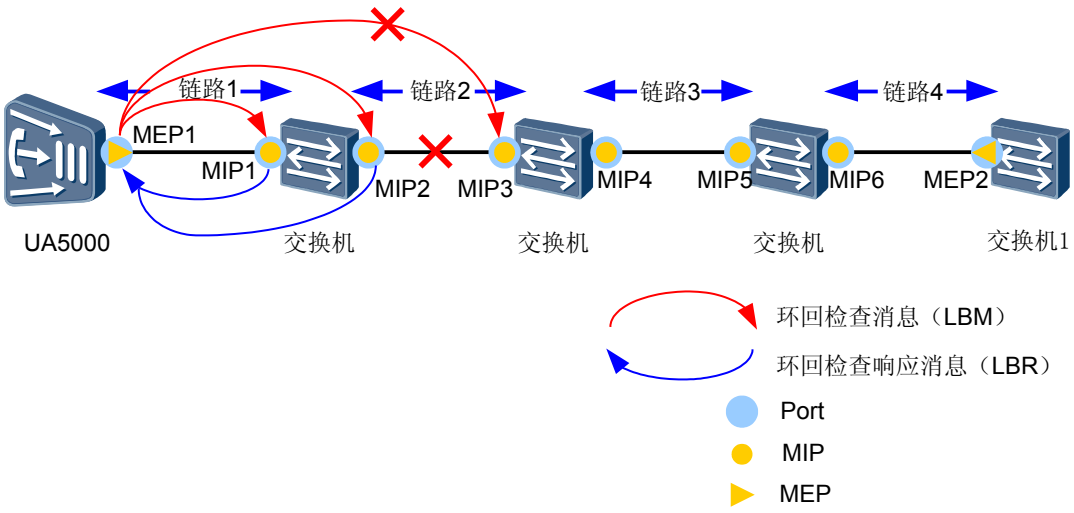
- **ETHOAM CCM 丢失告警**：低层交换链路故障，导致 MEP 不能收到 CCM，此时 MEP 的预期远端的 RMEP 定时器超时告警。
- **ETHOAM CCM 交叉连接缺陷告警**：MEP 接收到的 CCM 中 MA 的 ID 和本地配置不符合，MEP 接收到的 CCM 中的 MD 级别和本地配置不符合。
- **ETHOAM CCM 错误连接缺陷**：MIP（Maintenance association Intermediate Point）和 MEP 收到的 CCM 中 MEPID 与其配置的远端 MEPID 不匹配，以及远端 MEP 和本地 MEP 的 CCM 报文的发送周期不一致。
- **ETHOAM CCM RDI 缺陷告警**：远端 MEP 接收到 RDI 位被置位为 1 的 CCM 报文。

环回检测

环回消息从 MEP 发到指定 MIP（或 MEP），帮助 MEP 在 MA 中精确定位故障位置。

环回检测原理如图 21-2 所示。

图 21-2 环回检测原理图



故障位置前的 MIP（或 MEP）能够响应环回检测消息（即发送 LBR 报文），而故障位置后的 MIP（或 MEP）不能够响应环回检测消息（LBR），从而实现故障的定位。环回检测（LB）的原理描述如下：

说明

MEP 必须要知道发送 LBM 给中间 MIP(或 MEP) 的 MAC 地址，在进行环回检测之前：

- 通过配置发现，CCM 可记录远端的 MEP 信息；
- 使用链路跟踪消息（LTM）获得，LTM 可获知中间的 MIP 和目的 MEP 的 MAC 地址。

1. 如图 21-2 所示，MEP1 向 MIP1 发送环回检测消息（LBM）。
2. 链路 1 正常，MEP1 收到 MIP1 响应的环回检测消息（LBR）。

说明

MIP 只响应 LBM，不会转发给下一跳 MIP（或 MEP）。

3. MEP1 向 MIP1 的下一跳 MIP2 发送环回检测消息（LBM）。
4. MEP1 收到 MIP2 响应的环回检测消息（LBR）。
5. MEP1 继续向 MIP2 的下一跳 MIP3 发送环回检测消息（LBM）。
6. 因为链路 2 故障，MEP1 无法收到 MIP3 响应的环回检测消息（LBR）。
7. UA5000 可以判断 MIP2 和 MIP3 之间的链路故障，即链路 2 故障。

说明

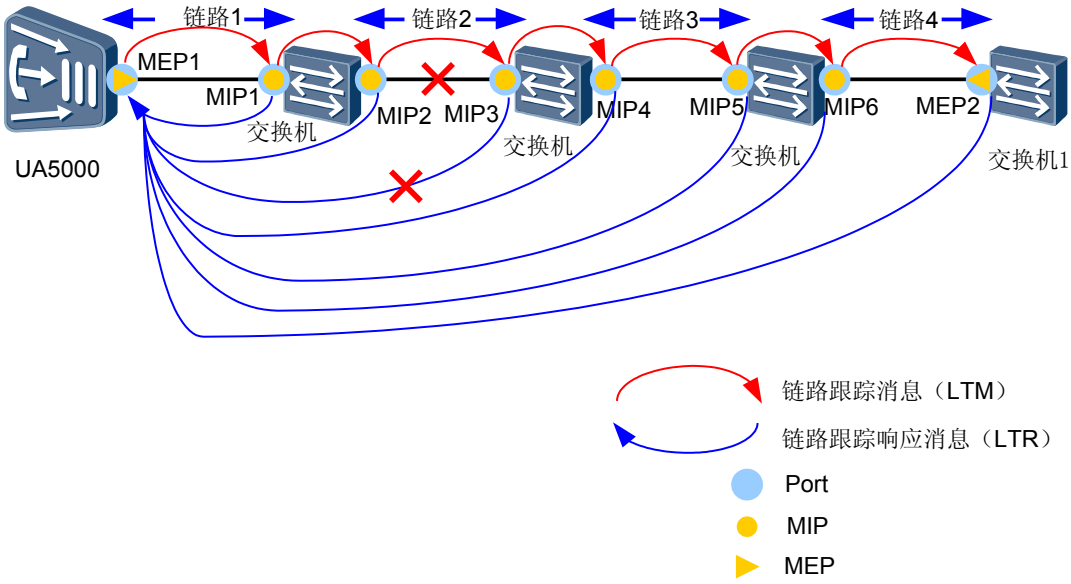
环回检测是一种手段，只要知道 UA5000 和交换机 1 之间所有 MIP(或 MEP) 的 MAC 地址，诊断路径可以自由安排。

链路跟踪

链路跟踪消息用来检测两个 MEP 间所通过的 MIP 路径。链路中所有中间 MIP 向发起链路跟踪消息的 MEP 响应链路跟踪消息，并转发链路跟踪消息，直到到达目的 MIP（或 MEP）。

链路跟踪原理如图 21-3 所示。

图 21-3 链路跟踪原理图



如果目的是一个 MEP，则 MA 的每个 MIP 都向发起 MEP 回响应。通过链路跟踪响应消息（LTR），发起 MEP 将会得到 MA 上所有 MIP 的 MAC 地址与相对发起 MEP 的位置，以及出现故障的链路位置区间。链路跟踪的原理描述如下：

1. 所有链路正常时，MEP1 向 MEP2 发起一个链路跟踪消息（LTM）。
2. 中间 MIP1、2、3、4、5、6 收到 LTM 后，向 MEP1 回应一个消息 LTR，并将 TTL 减 1 后转发 LTM 到下一跳。
3. 目的 MEP2 收到 LTM 后，不再转发该消息，直接向 MEP1 发送回应消息 LTR。

4. 如图 21-3 所示，当 MIP2 和 MIP3 之间的链路 2 故障时，MEP1 向 MEP2 发送 LTM，只能 MIP1、MIP2 返回的 LTR，不能收到 MIP3 返回的 LTR，从而判断出故障位置。

21.4 参考信息

介绍与 Ethernet CFM OAM 特性相关的参考信息。

本特性的参考资料清单如下：

- IEEE 802.1ag-2007 VLAN Amendment 5 Connectivity Fault Management
- WT-156v17 – Straw

22 线路调优

关于本章

线路调优是指通过调整线路参数，对线路的质量和性能进行提高和改善，是动态优化线路的一种解决方案。主要通过 N2510 线路保障系统实现。

22.1 介绍

介绍该特性的定义、目的、规格、约束、术语和缩略语。

定义

线路调优是指通过调整线路参数，对线路的质量和性能进行提高和改善。线路调优是动态优化线路的一种解决方案，主要通过 N2510 系统实现。

N2510 提供运营商铜线线路测试及保障功能，满足运营期间的线路业务保证与线路故障定位，为用户提供完善的线路管理解决方案，很好地满足线路分析管理的需求，降低运营成本。

目的

线路调优的主要目的是实现线路的动态管理。包括：

- 定位线路故障
- 提高线路质量
- 改善线路性能

规格

- 支持启动指定单板的 DLM/DSM 调优信息收集和查询指定单板或所有单板 DLM/DSM 调优信息收集状态的功能。
- 支持配置 1000 个调优模板。
  - 模板支持添加、修改、删除和查询的操作。
  - 模板的参数按照分组进行配置，即
    - 噪声容限参数：必须同时配置上/下行目标噪声容限、上/下行最小噪声容限和上/下行最大噪声容限；
    - 通道位交换参数：必须同时配置上/下行通道位交换使能开关；
    - 信道参数：必须同时配置上/下行最小噪声脉冲保护参数和上/下行最大时延；
    - 功率管理参数配置：必须同时配置是否允许转换到空闲状态、是否允许转换到低功率状态、全功率状态的最短时间、从进入低功率状态到功率开始减少的最小时间、L2 功率状态每次功率衰减所减少的值、L2 功率状态能够减少的总功率值。
    - 模式参数配置：必须首先配置模式才可以进行参数配置，即首先选定频谱模板，才可以配置模板中的参数。
  - 支持配置 ADSL 上/下行子载波关闭。
  - 模式配置的参数包括：用户指定频谱模式下的上/下行最大标称总传输功率、上/下行 PSD 掩码和上/下行传输功率谱密度。
- 支持给端口绑定和解绑定调优模板和查询端口绑定的调优模板。调优模板优先级高于扩展模板和线路模板。

约束

仅支持 H603CSR 和 H603ADR 系列单板的 ADSL 端口调优。

术语

表 22-1 线路调优特性术语表

术语	解释
线路传输模式	线路传输模式是指 CO 与 CPE 之间使用的 ADSL 连接协议。 ● 目前常用协议有： – ETSI – T1.413 – G.992.1 – G.992.2 – G.992.3 – G.992.4 – G.992.5 ● G.992.x 协议分为： – AnnexA – AnnexB – AnnexC – AnnexI – AnnexJ – AnnexL – AnnexM ● AnnexA，也叫 ADSL over POTS，它是在同一对双绞线上存在 POTS 与 ADSL 的应用。其频谱为上行 25kHz ～ 138kHz，下行 138kHz ～ 1104kHz（ADSL2+为 2208kHz）。 ● AnnexB，也叫 ADSL over ISDN，它是在同一对双绞线上存在 2B1A 或者 4B3T 编码方式 ISDN 与 ADSL 的应用。 ● AnnexC，时分双工方式，主要在日本使用。 ● AnnexI、AnnexJ，增加了对全数字环路模式的支持，其中 AnnexI 适用于临路线对 POTS 的情况，AnnexJ 适用于临路线对为 ISDN 的情况。 ● AnnexL，支持长距离 ADSL2，简称 READSL2。 ● AnnexM，支持上行频带扩展，上行最大速率超过 2Mbit/s，基于 POTS。
通道位交换	通道位交换功能主要作用是在不用去激活线路的情况下即可在子信道的内部之间进行比特分布的调整或功率调整，以保证线路误码率低于 10^{-7}。
噪声容限	噪声容限的作用是在分配 bit 时，留有一定余量，当环境变化导致的信噪比下降的幅度只要不超过噪声容限，就能保证误码率小于 10^{-7}。噪声容限分为：上行目标噪声容限、上行最小噪声容限、上行最大噪声容限；下行目标噪声容限、下行最小噪声容限、下行最大噪声容限。

术语	解释
交织时延	交织会带来时延，交织时延由两部分组成，一部分是 FEC 编码的时间，另一部分是交织的时间。
脉冲噪声保护	INP 是描述 ADSL 抗脉冲干扰的能力的参数，其单位（unit）是 DMT SYMBOL。如果 INP=1 的话，那么表示当前的该 ADSL 延时信道可以抵抗 1 个 DMT 符号长度的脉冲噪声；如果转换成时间单位来理解的话，可以这样理解：因为 ADSL 线路 1 秒钟发 4000 个 DMT 符号，就是说每个符号持续时间为 250us，那么 INP=1 就代表可以允许脉冲噪声长度为 250us。
比特分布	上下行的比特分配是由 CO 端和 CPE 端分别来完成，在 CPE 端计算完所有子信道的比特数，并进行了子载波排序（实际并不是按照子载波的顺序进行比特分配的，而是会先进行子载波排序，然后按照排序后的子载波顺序进行比特分配）之后，会把最后结果发送给 CO 端，以便 CO 端在下行调制时能够与 CPE 端达成一致的约定，所以局端本身就存有下行的比特分布数据，通过局端即可查询到上下行的比特分布情况。
PSD Mask	PSD Mask 是对传输信号的功率谱密度的约束。PSD Mask 是通过断点来设置的，调优模板中支持下行频段断点为 32 个，上行频段断点为 4 个。

缩略语

表 22-2 线路调优特性缩略语表

缩略语	英文全称	中文全称
ADSL	Asymmetric Digital Subscriber Line	非对称数字用户线
ATU-C	ADSL transceiver unit,central office end	局端 ADSL 收发器
ATU-R	ADSL transceiver unit, remote end	ADSL 收发器远端终端用户
CO	Central Office	中心局
CPE	Customer Premises Equipment	用户驻地设备
DLM	Dynamic Line Management	动态线路管理
DSM	Dynamic Spectrum Management	动态频谱管理
SNR	Signal Noise Ratio	信噪比
INP	Impulse Noise Protection	脉冲噪声保护
POTS	Plain old telephone service	普通电话业务

22.2 可获得性

介绍该特性需要的硬件支持和 License 支持。

硬件支持

支持 IFX 套片的 ADSL2+单板：H603ADRI、H603ADRB、H603CSRI、H603CSRB 和 H603CSRK。

License 支持

只有获得了 License 许可后才能获得线路调优特性的服务。License 控制如下资源：

- ADSL 端口资源
- AnnexM、AnnexL 资源
- INP+资源

22.3 原理描述

介绍该特性的实现原理。

线路调优兼容性

线路调优目前只支持对 ADSL 接入方式的线路进行调优，实现的原理基于 ETSI、T1.413、G992.1 ～ G992.5 标准。目前还不支持对其他接入方式的线路调优。

实现线路调优特性

线路调优特性由 N2510 操作实现，分为以下步骤：

1. 收集调优信息

   主要实现 ADSL 端口参数的查询。在 UA5000 的 ADSL 单板侧生成激活参数信息文件，给 N2510 提供线路诊断和优化的原始数据。

2. 管理调优模板

   主要实现 N2510 对调优模板的添加、修改、删除、查询操作。N2510 通过对原始数据的分析，生成能够改善线路性能的调优模板。

3. 下发调优参数

   主要实现 N2510 将调优模板绑定到端口，实现线路性能优化。

说明

线路调优特性的实现原理请参见“N2510 特性描述”中的“线路调优”。

22.4 参考信息

介绍与该特性相关的参考信息。

本特性的参考资料清单如下：

- ITU-T G.992.1、G.992.2、G.992.3、G.992.4、G.992.5
- ETSI
- T1.413

23 宽带电源关断

关于本章

UA5000 支持的绿色节能是通过宽带电源关断特性来实现的。

23.1 介绍
介绍该特性的定义、目的、规格和约束条件。

23.2 可获得性
介绍该特性需要的硬件支持。

23.3 原理描述
介绍该特性的实现原理。

23.1 介绍

介绍该特性的定义、目的、规格和约束条件。

定义

宽带电源关断指系统在市电掉电或 Combo 单板仅使用窄带单元时，关断宽带电源，以延长窄带的供电时长，降低系统的无效功耗。

目的

Combo 单板为宽窄带合一板，通常情况下宽带单元和窄带单元同时工作。在实际应用中，当宽带部分业务还未发放，仅使用窄带单元时，宽带单元产生的功耗为无效功耗。通过关断宽带电源可以降低功耗。

同时，UA5000 一般都配有蓄电池，市电掉电后，由蓄电池给设备供电。在实际应用中，窄带业务较宽带业务的优先级高。通过在市电掉电后自动关断宽带电源，可以延长蓄电池对设备供电时长，即延长窄带单元在市电掉电后的正常应用时长。

规格

- 只有 Combo 单板支持宽带电源关断特性。
- Combo 单板支持 Combo、Power-Saving、Auto 三种模式，分别对应宽窄带同时工作、只有窄带工作和宽带部分智能工作。

约束

使用宽带电源关断特性时，必须同时配置电源监控单元，且电源监控单元监控窄带主控板。

术语

表 23-1 宽带电源关断特性术语表

术语	解释
Combo 单板	Combo 单板为宽窄带合一板，在同一块单板提供 ADSL2+和 POTS 接入功能。

23.2 可获得性

介绍该特性需要的硬件支持。

需要支持宽带电源关断的 Combo 单板 CSR 系列单板以及市电掉电检测的环境监控单元。

23.3 原理描述

介绍该特性的实现原理。

使用 Combo 单板的情况：

- 在 UA5000 中使用 Combo 单板，宽带业务开通前，Combo 单板工作在 Power-Saving 模式，宽带单元不工作。
- 宽带业务开通后，配置 Combo 单板工作模式为自动模式。

市电掉电的情况：

- 环境监控单元检测到市电掉电后，通知窄带主控板。
- 窄带主控板向 Combo 单板下发宽带端口电源关断命令，Combo 单板关断宽带单元的电源，宽带业务中断，以延长窄带单元供电时间。
- 市电恢复后，宽带单元自动上电，宽带业务恢复正常。

24 级联组网

关于本章

级联组网是指接入设备之间通过 FE/GE 或 E1 线互连组网的一种方式。UA5000 支持两种级联方式：宽带级联和窄带级联。

24.1 介绍
介绍该特性的定义、目的、规格和约束条件。

24.2 可获得性
介绍该特性需要的硬件支持。

24.3 原理描述(IPM)
介绍宽带级联特性的实现原理。

24.4 原理描述(PVM)
介绍窄带级联特性的实现原理。

24.5 参考信息
介绍与该特性相关的参考信息。

24.1 介绍

介绍该特性的定义、目的、规格和约束条件。

定义

级联组网是指接入设备之间通过 FE/GE 或 E1 线互连组网的一种方式。

目的

级联组网使 UA5000 产品组网更加灵活，而且可以节省接入点上行线路资源。

规格

UA5000 宽带级联特性规格如下：

- UA5000 宽带级联端口通过 H612IPMB 或 H612IPMD 主控板提供。
- H612IPMB 单板最多可以提供 2 个 GE 口和 6 个 FE 口。
- H612IPMD 单板最多可以提供 4 个 GE 口和 6 个 FE 口。
- STP/RSTP 级联组环网，建议最多不超过 3 个节点。

UA5000 支持如下两种窄带级联：

- RSU 级联：在局端通过 H601PVMB、H601PVMD 板的 E1 端口或者用 EDTB 板的 E1 端口级联远端用户框，从而扩大 UA5000 的容量。远端用户框采用 RSU4/RSU8 主控板，局端与远端之间由 E1 电缆通过 MSTP (Multiservice Transport Platform)或 SDH (Synchronous Digital Hierarchy)连接。
- PV8+RSP 级联：在局端通过 H601PVMD 或者 EDTB 单板的 E1 端口级联远端 PV8 用户框，而远端的 PV8 用户框可以再级联 RSP 用户框，从而扩大 UA5000 的容量。局端与远端之间由 E1 电缆通过 MSTP (Multiservice Transport Platform)或 SDH (Synchronous Digital Hierarchy)连接。

约束

无。

术语

无。

缩略语

表 24-1 级联组网特性缩略语表

缩略语	英文全称	中文全称
RSTP	Rapid Spanning Tree Protocol	快速生成树协议
STP	Spanning Tree Protocol	生成树协议

24.2 可获得性

介绍该特性需要的硬件支持。

支持级联的单板如下：

- 宽带级联：需要 IPMB/IPMD 单板。
- 窄带 RSU 级联：局端需要 EDTB 或 H601PVMB/H601PVMD 单板，远端需要 RSU4/RSU8 单板。
- 窄带 PV8+RSP 级联：局端需要 EDTB 或 H601PVMD 单板，远端需要 PV4/PV8 单板，远端用户框的 PV4/PV8 单板可以再级联 RSP 用户框的 RSP 单板。

24.3 原理描述(IPM)

介绍宽带级联特性的实现原理。

UA5000 宽带级联支持环形组网、链型组网和星型组网。

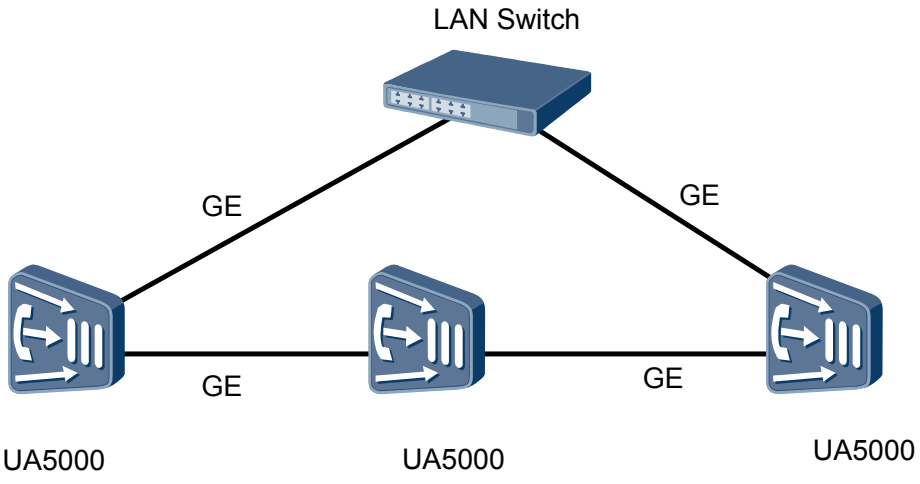
环形级联

多个 UA5000 之间互联，并和上行设备间形成环路，所有 UA5000 和上行设备均启动 STP 或 RSTP 协议。

采用 RSTP 环网级联可以节省光纤，增强组网的可靠性。建议 UA5000 之间采用 GE 互联以提高上行带宽。

环形级联如图 24-1 所示。

图 24-1 环形级联



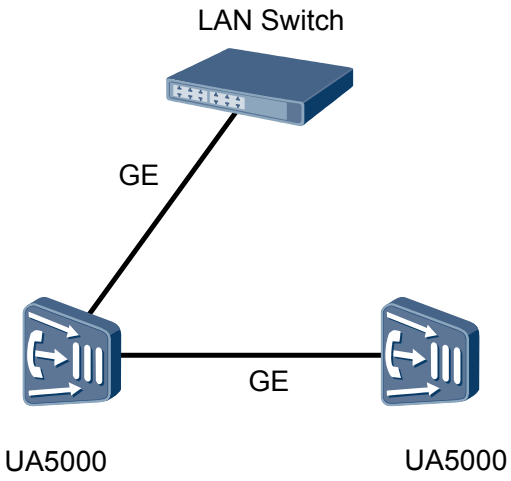
链型级联

链型级联是多个 UA5000 和上行设备间组成链型，通过一个 UA5000 连接到上行设备。这种组网方式可靠性较差，当一个设备故障后，其下级互联的所有设备都不能上行。

实际使用时建议只配置 2 个 UA5000 互联组成链型。

链型级联如图 24-2 所示。

图 24-2 链型级联

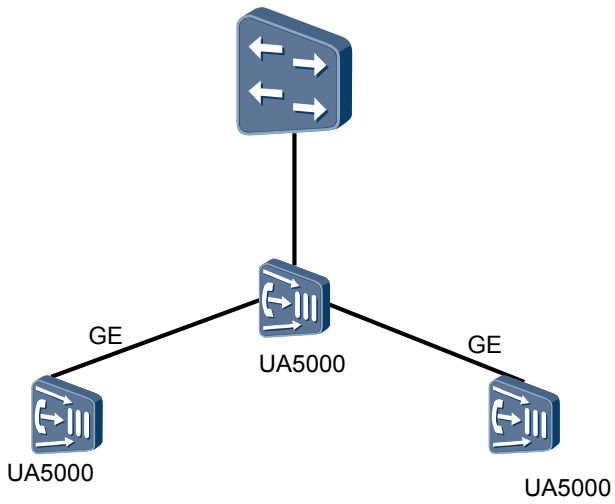


星型级联

星型级联是多个 UA5000 和上行设备间组成星型，通过一个 UA5000 连接到上行设备。这种组网方式可靠性较好，组网简单。

星型级联如图 24-3 所示。

图 24-3 星型级联



24.4 原理描述(PVM)

介绍窄带级联特性的实现原理。

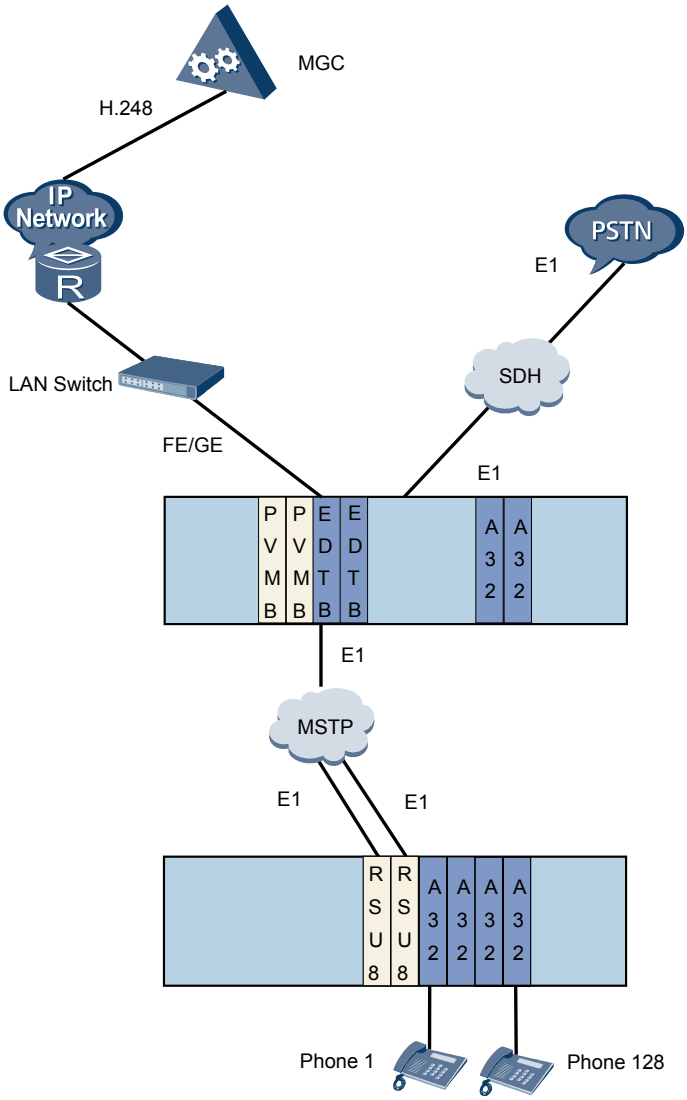
UA5000 支持两种窄带级联：RSU 级联和 PV8+RSP 级联。

RSU 级联

RSU 级联：在局端通过 H601PVMB、H601PVMD 板的 E1 端口或者用 EDTB 板的 E1 端口级联远端用户框，从而扩大 UA5000 的容量。远端用户框采用 RSU4/RSU8 主控板，局端与远端之间由 E1 电缆通过 MSTP (Multiservice Transport Platform)或 SDH (Synchronous Digital Hierarchy)连接。

RSU 级联如图 24-4 所示。

图 24-4 RSU 级联



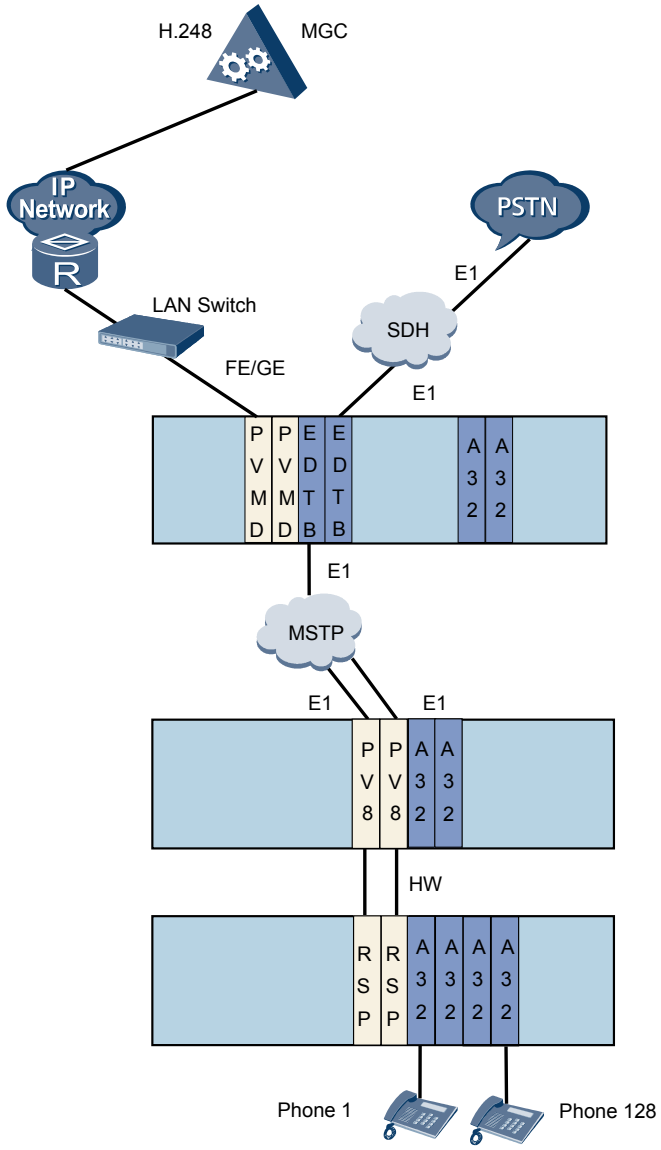
PV8+RSP 级联

PV8+RSP 级联：在局端通过 PVMD 或者 EDTB 单板的 E1 端口级联远端 PV8 用户框，而远端的 PV8 用户框可以再级联 RSP 用户框，从而扩大 UA5000 的容量。局端与远端

之间由 E1 电缆通过 MSTP (Multiservice Transport Platform)或 SDH (Synchronous Digital Hierarchy)连接。

PV8+RSP 级联如图 24-5 所示。

图 24-5 PV8+RSP 级联



24.5 参考信息

介绍与该特性相关的参考信息。

本特性的参考资料清单如下：

- IEEE 802.1w Rapid Spanning Tree

25 环境监控

关于本章

介绍环境监控特性的定义、目的、规格、原理以及参考的术语、缩略语和相关协议标准。

25.1 介绍
介绍该特性的定义、目的、规格和约束条件。

25.2 可获得性
介绍该特性需要的硬件支持，包括单板和终端。

25.3 原理描述
介绍该特性的实现原理。

25.1 介绍

介绍该特性的定义、目的、规格和约束条件。

定义

环境监控一般包含环境量、电源、风扇框和配电框的监控。

- 环境量的监控指的是对一些可能引起设备损坏、故障等环境因素的监控。监控内容包括温度、湿度、门磁、水浸、烟感、配线架、门禁等。
- 电源监控指的是对系统的供电电源的监控，其中包括对市电输入、直流配电、整流模块、电池等的监控。
- 风扇框的监控指的是对风扇运行状态的监控。
- 配电框的监控指的是对配电框的电源的监控。

环境监控的实现从外部看去，就是通过设备上的监控串口与被监控对象的通信串口间用串口线连接，利用私有协议，使用户能直接在设备上监控设备所处的环境状态。

通过环境监控可以实现以下功能：

- 直接监控电源设备供电的各种参数状态、风扇状态、电源外接电池组的状态以及一些内置环境监控量的状态等。
- 若外接各种传感器，可以对传感器提供的各项功能进行监控，如环境温度、湿度、蜂鸣器、机柜灯等。
- 用户还可以修改一些配置，如环境量的告警值、电源和电池组的控制参数，使被监控对象可以按照用户的需要工作。

目的

环境监控的目的是时刻监视设备运行情况，及时发现故障，满足电信网络对于稳定性的要求。

规格

- 支持风扇框 FAN 的监控
- 支持 H303ESC 的监控
- 支持 H304ESC 的监控
- 支持 ESCM 的监控
- 支持配电框的监控
- 支持 EPS30-4815AF（即 POWER4845）的监控
- 支持 EPS75-4815AF（即 POWER4875L）的监控
- 支持 POWER3000 的监控

术语

无。

缩略语

表 25-1 环境监控特性缩略语表

缩略语	英文全称	中文全称
EMU	Environment Monitoring Unit	环境监控单元

25.2 可获得性

介绍该特性需要的硬件支持，包括单板和终端。

支持本特性的单板为主控板 IPM 及 PVM。

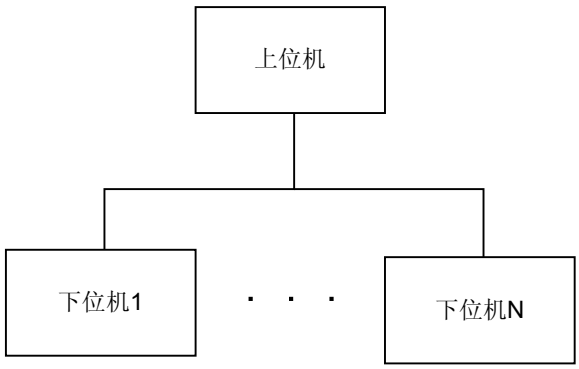
25.3 原理描述

介绍该特性的实现原理。

UA5000 的环境监控功能是基于上位机和下位机的方式实现，即一个上位机管理多个下位机。上位机与下位机之间采用主从协议进行通信。典型配置是一个 ESC 与多个 FAN。UA5000 环境监控功能的基本原理如图 25-1 所示。

这里的上位机对应为设备的主控板，而下位机是具有监控功能的监控板或监控框。

图 25-1 环境监控主从通信图



上位机与下位机的交互方式为：

- 上位机维护管理下位机的状态。
- 上位机将用户命令解析后转发给下位机，由下位机完成相应的动作。
- 下位机通过自身的硬件接口检测外部的数据，对数据进行处理，然后将数据上报给上位机。

EMU

要完成环境监控功能，必须有能够完成监控的设备。监控设备可以分为：

- 模块独立的单板，如 H303ESC。
- 内置在其他设备中的监控模块，如风扇框、POWER4845、POWER4875、POWER3000。

这些单独存在或者内置于其他实体之中的能够完成监控的设备统称为环境监控单元 EMU。

一个 EMU 必须具有监控处理板以及与主机通信的接口。

UA5000 系统中的 EMU 包括：

- H302ESC
  - 一种环境监控板，实现对环境量的监控。
  - 采用内置传感器的方式。
  - 不提供扩展的传感器通道。
  - 支持对蓄电池组的监控。
  - 不支持智能电源的监控。
  - 提供接口直接监控系统电压（直流）和系统电流（直流）。
- H303ESC

  H302ESC 的升级板，采用内置传感器和提供扩展传感器接口方式，大大提高对环境监控量支持的灵活性。
  - 支持智能电源的监控。
  - 不能直接对蓄电池进行监控（可以采用扩展传感器方式）。
- H304ESC

  H303ESC 的升级板，向下兼容 H303ESC 的所有功能，并增加了蓄电池管理功能。
- ESCM
  - ESCM 是 H303ESC 与 H304ESC 的简化版，只支持模拟量和数字量的监控，使用 RS485 串口通信时支持级联功能。MiniESC 采用内置传感器，提供扩展传感器接口，大大提高对环境监控量支持的灵活性。
  - 不支持对蓄电池组的监控。
  - 不支持智能电源的监控。
  - 不提供接口直接监控系统电压（直流）和系统电流（直流）。
- FAN

  具有监控功能的风扇框，即风扇框中集成了监控板。FAN 只提供简单的内置模拟量和内置数字量的监控，不提供扩展传感器接口，不支持监控电源和蓄电池。
- DIS

  具有监控功能的直流配电框，即配电框中集成了监控板。DIS 同时提供内置传感器和扩展传感器接口，不支持监控智能电源和蓄电池。
- POWER4875L

  嵌入式电源监控设备，支持内置传感器和提供扩展传感器接口。POWER4875L 本身就是电源，因此支持监控电源和蓄电池。
- POWER4845

嵌入式电源监控设备，支持内置传感器和提供扩展传感器接口。POWER4845 本身就是电源，因此支持监控电源和蓄电池。

- POWER3000

  嵌入式电源监控设备，支持内置传感器和提供扩展传感器接口。POWER3000 本身就是电源，因此支持监控电源和蓄电池。

说明

对于 PVM 主控板，POWER3000 作为 POWER4875L 管理。对于 IPM 主控板，POWER3000 作为 POWER4845 管理。

从节点

环境监控采用主从通信的方式，因此下位机（也称从节点机）必须具有自己的唯一标识码，否则当在“点对多点”或“多点对多点”组网方式下通信会混乱。下位机的唯一标识码称为从节点号（也称从节点地址），由硬件决定的（类似于网络适配器的 MAC 地址）。一般下位机的监控板提供拨码开关，用来调整其从节点号。

必须保证一个上位机对应的所有下位机的从节点号没有重复的，否则上位机与下位机之间无法正常通信。

模拟量

模拟量是一个连续的量，例如温度、电压、电流等。模拟量监控接口，通常使用模拟量传感器，即提供实时检测模拟量的器件。

模拟量传感器的属性包括：

- 告警上限、告警下限：用来判断该模拟量是否产生告警，即只有在当满足下面的条件，该模拟量才表示工作正常。

  告警下限 ± Δ≤当前实测值≤告警上限 ± Δ

  ：硬件的误差值
- 测量上限、测量下限：传感器都有其测量的范围。有些传感器的测量范围可调，不同的测量范围下测量的结果是不同的。告警限要求必须在测量限的范围之内。
- 传感器类型：一般传感器分为电流型传感器和电压型传感器。配置模拟量时需要该参数。
- 单位：根据传感器所检测的对象以及传感器实际检测的精度来定义。
- 当前值、当前状态：模拟量传感器可实时上报所监测的模拟量的数值，并且一般能够给出该模拟量的状态值（过高、过低、正常）。

对于 EMU，模拟量分为内置模拟量和扩展模拟量：

- 内置模拟量一般是固定的，例如 H303ESC 板上固定了温度和湿度传感器。除告警上下限外，用户不可更改其余内置模拟量的参数。
- 扩展模拟量可以更改，用户可以根据所需配置相应的模拟量传感器。

数字量

与模拟量相比，数字量是一个离散值，是一个状态量。数字量传感器只有两个值：正常或故障。数字量传感器利用高低电平的比较实现状态值的检测。

数字量的属性包括：告警电平、有效电平、传感器类型和当前状态。

- 告警电平：即当数字量的电平等于告警电平，则数字量传感器产生告警。例如当该数字量传感器告警电平被设置为高电平，当监测的数字量一旦变成高电平，则传感器产生告警，数字量变成低电平，则不会告警。
- 有效电平：正好与告警电平相反，即数字量的电平等于有效电平，则数字量传感器不会告警。
- 传感器类型：一般传感器分为电流型传感器和电压型传感器。配置数字量时需要该参数。
- 当前状态：即电压型传感器检测的状态值。

对于 EMU，数字量也分为内置数字量和扩展数字量：

- 内置数字量一般是固定的，比如 H303ESC 板上固定了门禁和配线架传感器。除有效电平外，用户不可更改其余内置数字量的参数。
- 扩展数字量可以更改的，用户可以根据所需配置相应的数字量传感器。

其他监控量

UA5000 支持的电源监控量还包括以下内容：

- 市电有无状态：检测市电的供电状态并发送相应的故障或恢复告警。
- 电源模块状态：检测电源模块的状态并发送相应的故障或恢复告警。
- 供电状态：检测当前设备的供电源（交流供电或电池供电），并在供电源切换的时候发送告警。
- 电池充电状态：检测电池的充电状态。
- 电池电压状态：检测电池的电压状态，包括正常、过压、欠压。
- 电池保护状态：检测电池的保护状态，包括正常和过温保护，用户可设置电池的过温保护禁充的温度阈值，当温度超过这个阈值时，则自动启用电池的过温保护系统，禁止继续对电池充电。
- 电池硬件状态：检测电池的硬件状态。当电池硬件发生损坏时，会发送电池故障告警。

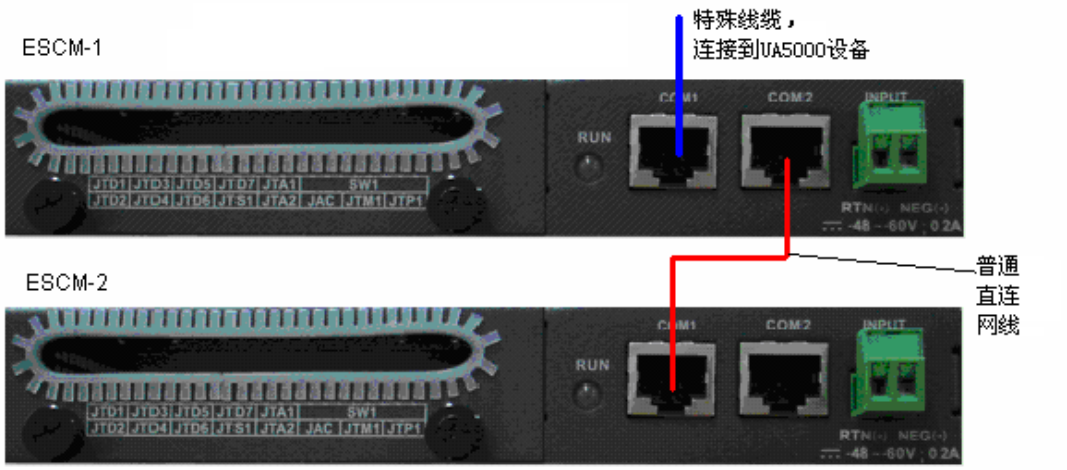
ESCM 级联

ESCM 可以通过 RS232 串口或 RS485 串口与主机通信，使用 RS485 串口通信时一台主机可以添加多个 ESCM，各个 MiniESC 配置不同的从节点，通过级联的方式相连。

当 ESCM 使用 RS232 串口通信时，波特率为 9600bit/s，使用 RS485 串口通信时，波特率为 19200bit/s。

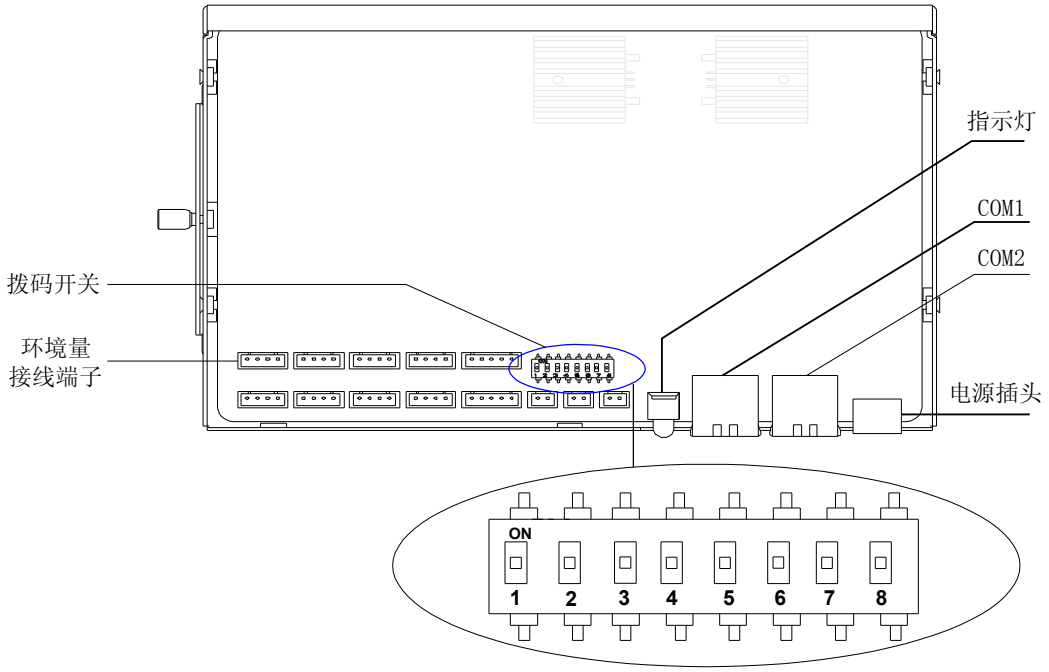
多个 ESCM 之间通过图 25-2 所示的方式级联，各个 ESCM 之间通过硬件拨码设置不同的从节点地址，级联线使用普通网线。

图 25-2 ESCM 级联图



ESCM 拨码开关布局如图 25-3 所示。

图 25-3 ESCM 拨码开关布局图



拨码开关 S1 可用拨码位共计 8 位，拨码开关的“ON”对应“0”，“OFF”对应“1”，含义及设置说明如表 25-2 所示。

表 25-2 拨码开关 S1 含义及设置说明

拨码位	设置	含义	出场设置
S1-1 ～ S1-5		从节点地址设置	S1-1：ON S1-2：ON S1-3：OFF S1-4：OFF S1-5：ON
S1-6	ON	串口上报的速率为 19200bit/s	OFF
	OFF	串口上报的速率为 9600bit/s	
S1-7	ON	JTA1 外接电流型传感器	ON
	OFF	JTA2 外接电压型传感器	
S1-8	ON	JTA1 外接电流型传感器	ON
	OFF	JTA2 外接电压型传感器	

26 光模块监控

关于本章

介绍光收发一体模块的定义、目的、规格、原理以及参考的术语、缩略语和相关协议标准。

26.1 介绍
介绍该特性的定义、目的、规格和约束条件。

26.2 可获得性
介绍该特性需要的硬件支持，包括单板和终端。

26.3 原理描述
介绍该特性的实现原理。

26.1 介绍

介绍该特性的定义、目的、规格和约束条件。

定义

光收发一体模块由光电子器件、功能电路和光接口等组成，光电子器件包括发射和接收两部分。

- 发射部分是：输入一定码率的电信号经内部的驱动芯片处理后驱动半导体激光器（LD）或发光二极管（LED）发射出相应速率的调制光信号，其内部带有光功率自动控制电路，使输出的光信号功率保持稳定。
- 接收部分是：一定码率的光信号输入模块后由光探测二极管转换为电信号。经前置放大器后输出相应码率的电信号，输出的信号一般为 PECL 电平。同时在输入光功率小于一定值后会输出一个告警信号。

目的

采用光收发一体模块可以降低成本及组网的复杂度。

规格

- 支持的传输速率：百兆、千兆、10GE，以及 POS 接口的 155Mbit/s，622Mbit/s，2.5Mbit/s，10Gbit/s。
- 支持传输距离：多模传输距离为 275 ～ 550m，单模则可以达到 2km、10km、15km、40km、70km，甚至 100km 或以上。
- 封装类型：1×9、SFF、SFP、GBIC、XENPAK、XFP。

约束

无。

术语

表 26-1 光收发一体模块特性术语表

术语	解释
Laser	light amplification by stimulated emisssion of radiation，意为“受激辐射的光放大”，激光是相位相关的相干电磁波，它具有良好的指向性、单色性、相干性、能量高度集中，亮度很强。
数字诊断功能	对光模块的光发送、光接收的各项参数进行监控的功能，监控包括实时光功率电平、激光器偏置电流、温度和工作电压等。
发射光功率	模块发射部分光源的平均输出光功率。
过载光功率	最大可接收功率叫做过载光功率；超过此功率误码率将达不到要求。

缩略语

表 26-2 光收发一体模块特性缩略语表

缩略语	英文全称	中文全称
SFP	Small Form-factor Pluggable	热插拔小封装
ESFP	Enhanced Small Form-factor Pluggable	增强型热插拔小封装
SFF	Small Form Factor	焊接小封装
GBIC	Gigabit Interface Converter	吉比特接口转换器

26.2 可获得性

介绍该特性需要的硬件支持，包括单板和终端。

在 UA5000 中，IPMB/IPMD/H601PVMD 单板支持读取 ESFP 光模块的监控参数，不支持上报 ESFP 光模块的告警。

26.3 原理描述

介绍该特性的实现原理。

光模块分为光发送模块和光接收模块两部分，发送模块主要是发送电信号调制部分和激光器光源部分。电调制部分主要去掉直流成分，用交流信号部分驱动激光器发光。激光器部分主要是光源器件，产生特定波长的光信号。

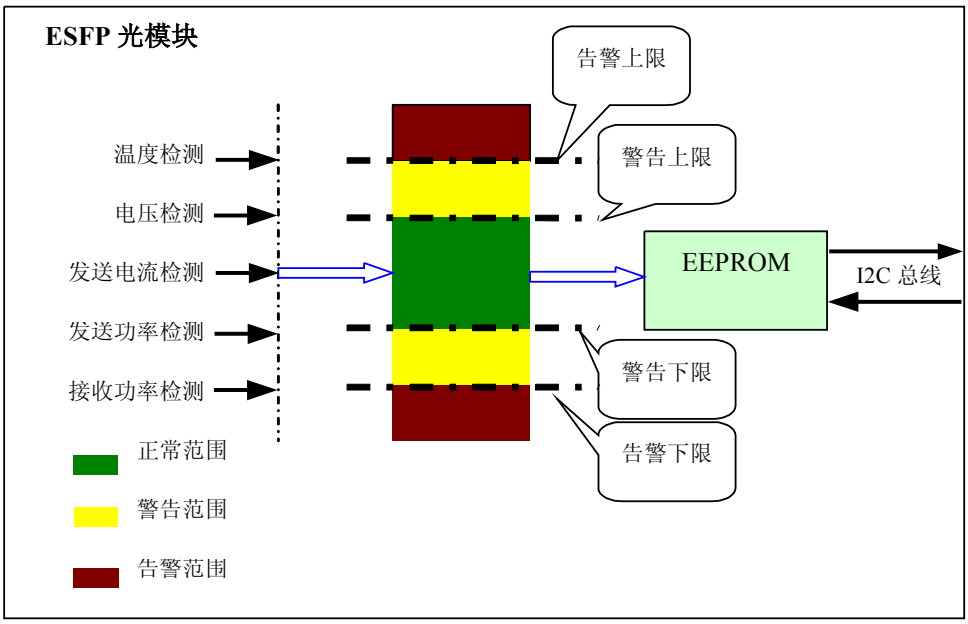
另外，光模块还有监控特性，当模块的功率，温度和电压等异常时，产生告警和警告信息。

ESFP 模块监控特性：

- ESFP 内部由于有 I2C 管理总线，可作数据诊断功能（DDF），用于监控光模块的接收功率，发送功率，发送偏置电流，光模块供电电压和温度参数。
- 以上参数存储于 ESFP 的 EEPROM 里，软件可以通过 I2C 总线设置和读取。另外，还可以通过 I2C 总线控制和监控光模块的使能，发送失败监控，接收丢包监控及接收速率的选定和监控。

ESFP 模块监控原理如图 26-1 所示。

图 26-1 ESFP 模块监控原理图



ESFP 模块监控的参数的范围如**表 26-3** 所示。

表 26-3 ESFP 模块监控的参数

参数	温度	电压	发送偏置电流	发送功率	接收功率
范围	-128 ～+128 C	0 ～ 6.55V	0 ～ 131mA	0 ～ 6.5mW	0 ～ 6.5mW
精度	1/256 C	0.1mV	2μA	0.1μW	0.1μW

27 H.248 语音

关于本章

首先对 H.248 协议进行介绍，然后分为协议机制、VoIP、MoIP 和 FoIP 等方面对 H.248 的原理进行阐述。

27.1 介绍
介绍该特性的定义、目的。

27.2 可获得性
介绍该特性需要的硬件支持和 License 支持。

27.3 原理描述
介绍与 H.248 相关的原理。

27.1 介绍

介绍该特性的定义、目的。

定义

H.248 是一种网关控制协议，媒体网关控制器（MGC）通过 H.248 协议来控制媒体网关（MG）以达到各种媒体相互通信的目的。ITU-T 于 2000 年 6 月发布了此协议的第一个标准 H.248：Version 1。

目的

H.248 主要具有如下优点：

- H.248 标准化方面做得更完善和健全，支持更多类型的接入技术。
- H.248 协议能够支持更大规模的网络应用，而且更便于对协议本身进行扩充，因而灵活性更强。
- H.248 消息可以基于 UDP/SCTP 等多种协议承载。

27.2 可获得性

介绍该特性需要的硬件支持和 License 支持。

硬件支持

- 支持本特性的单板为 A32、A64 和 CSRB/CSRI。
- 需要软交换支持 H.248 协议。

License 支持

G723&G729 编解码方式受 License 控制。

27.3 原理描述

介绍与 H.248 相关的原理。

27.3.1 协议机制

介绍 H.248 协议的基本概念和基本机制。

终端 ID

终端 ID（TerminationID）标识那些即将退出或者进入服务的终端，每一个终端都有一个唯一的 ID 作为标识。在进行业务配置时，MG 与 MGC 上需要分别为每一个终端配置对应的终端 ID。终端 ID 为根终端（ROOT）时表示整个网关，此时 ServiceChange 命令将影响到整个网关，可以使用通配符，如 ALL 通配符（*），但是不能使用 CHOOSE 通配符（$）。

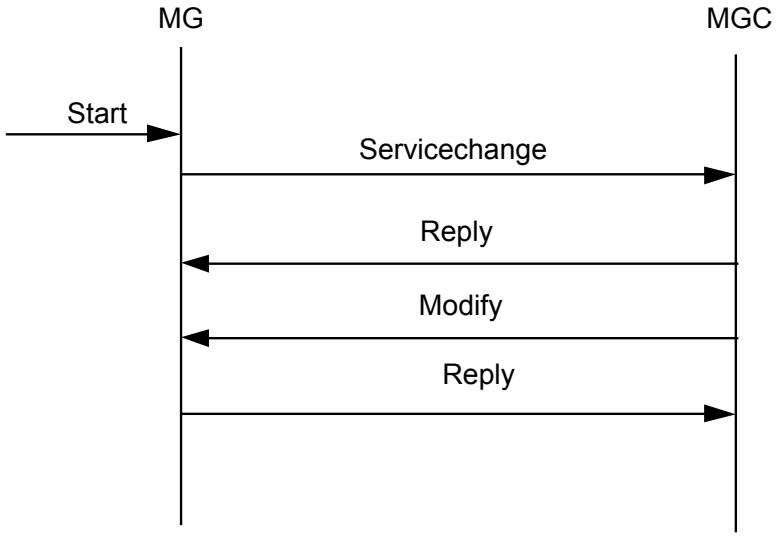
H.248 接口注册机制

MG 通过 ServiceChangeRequest 命令通知 MGC 某一个或者某一组用户将进入或者退出服务，此命令交互成功后直接影响到端点状态改变为“InService”或者“out of service”。同时，MGC 也可以通过主动发送 ServiceChangeRequest 命令使 MG 上的某一个或者某一组端点进入或者退出服务。

说明
目前 MG 不支持 MGC 主动要求 MG 上的某一个或者某一组端点进入服务的命令。

其中，网关注册流程如图 27-1 所示。

图 27-1 网关注册流程图



流程说明：

1. MG 向 MGC 发送 ServiceChangerequest 进行注册，命令中的 TerminationId 为 Root，Method 为 Restart，ServiceChangeReason 在冷启动时为 901（上电后第一次注册）；热启动时为 902（命令行重启），其他情况下为 900。
2. MGC 回送注册成功的 Reply 消息。
3. MGC 向 MG 发送 Modify 命令，要求 MG 检测所有用户的摘机（al/of）。
4. MG 应答 Reply 消息。

H.248 接口心跳机制

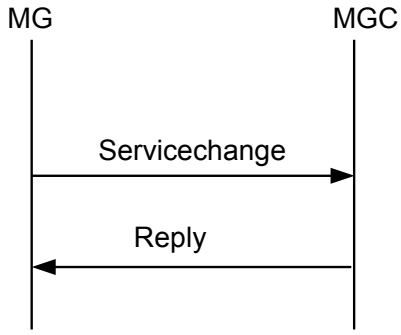
注册成功后，MG 与 MGC 之间通过发送心跳检测消息 Notify（it/ito）保持通讯，默认 60s 发送一次心跳消息，发送心跳消息的间隔可以设置（5s ～ 655s）。

当从第一次 MG 向 MGC 发起心跳开始，在配置的接口心跳时间长度内（譬如发送 3 次心跳消息），如果没有收到 MGC 的心跳响应，将会把接口状态置为“等待响应”态。之后 MG 会一直向 MGC 发起注册，如果配置了双归属，将会在两个 MGC 之间轮询的发起注册。每 30S 注册一次，每三次注册为一轮，每条注册消息重传七次，90s 内能看到 24 条注册消息，然后切换到下一个 MGC 重新注册。

H.248 接口注销机制

MG 主动注销流程如图 27-2 所示。

图 27-2 网关主动注销流程图

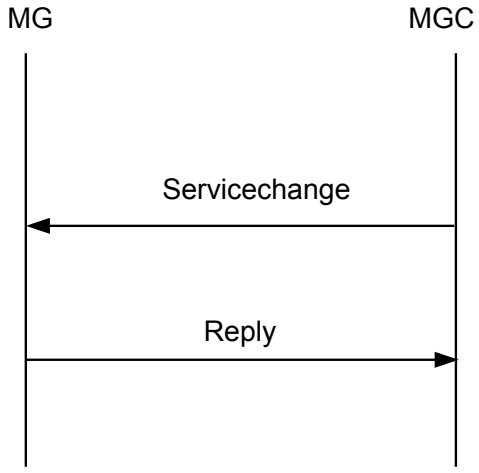


流程说明：

1. MG 向 MGC 发送 ServiceChangeRequest 进行注销，命令中的 TerminationId 为 Root，Method 为 Forced，ServiceChangeReason 为 905（指示终端由于维护操作而退出服务，现在 MG 用它实现命令行发起的 shutdown 注销请求）。
2. MGC 回送注销成功的 Reply 消息。

MGC 主动注销网关流程如图 27-3 所示。

图 27-3 MGC 主动注销网关流程图



流程说明：

1. MGC 向 MG 发送 ServiceChangeRequest 进行注销，命令中的 TerminationId 为 Root，Method 为 Forced，原因值为 905。

2. MG 回应 Reply 消息。MG 除了支持网关的注册和注销之外，还支持单端点的注册与注销，通过单端点的注册及注销改变单个用户的服务状态。

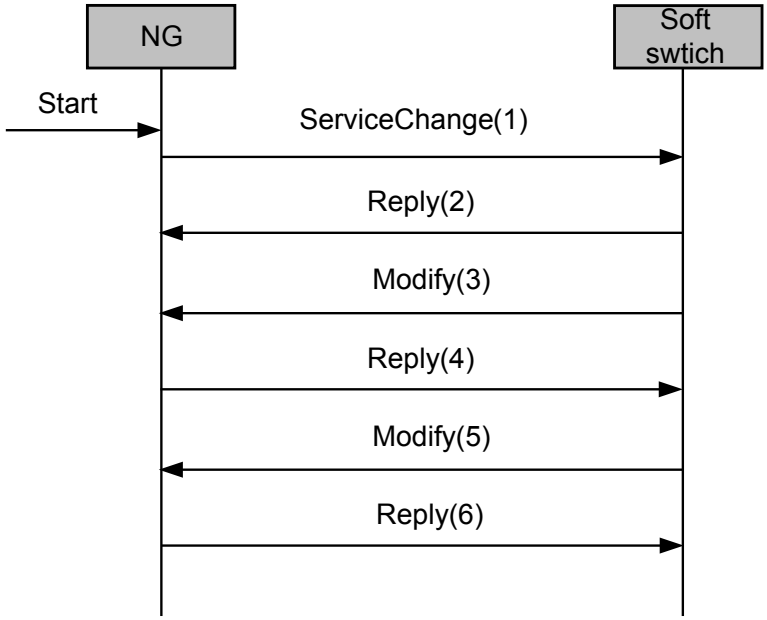
H.248 接口鉴权机制

鉴权是媒体网关控制器（MGC）为了验证识别 MG（即 UA5000）用户身份合法性而建立的安全机制。其目的是为了防止未经授权的实体利用 H.248 协议建立非法呼叫，或者干涉合法呼叫。协议的实现需要对接的软交换支持鉴权，否则该特性无法实现。

- 在 H.248 协议中，实现 AH 协议应遵循 RFC2402。
- 加密算法采用 MD5。

鉴权流程如图 27-4 所示。

图 27-4 鉴权流程图



鉴权流程如下：

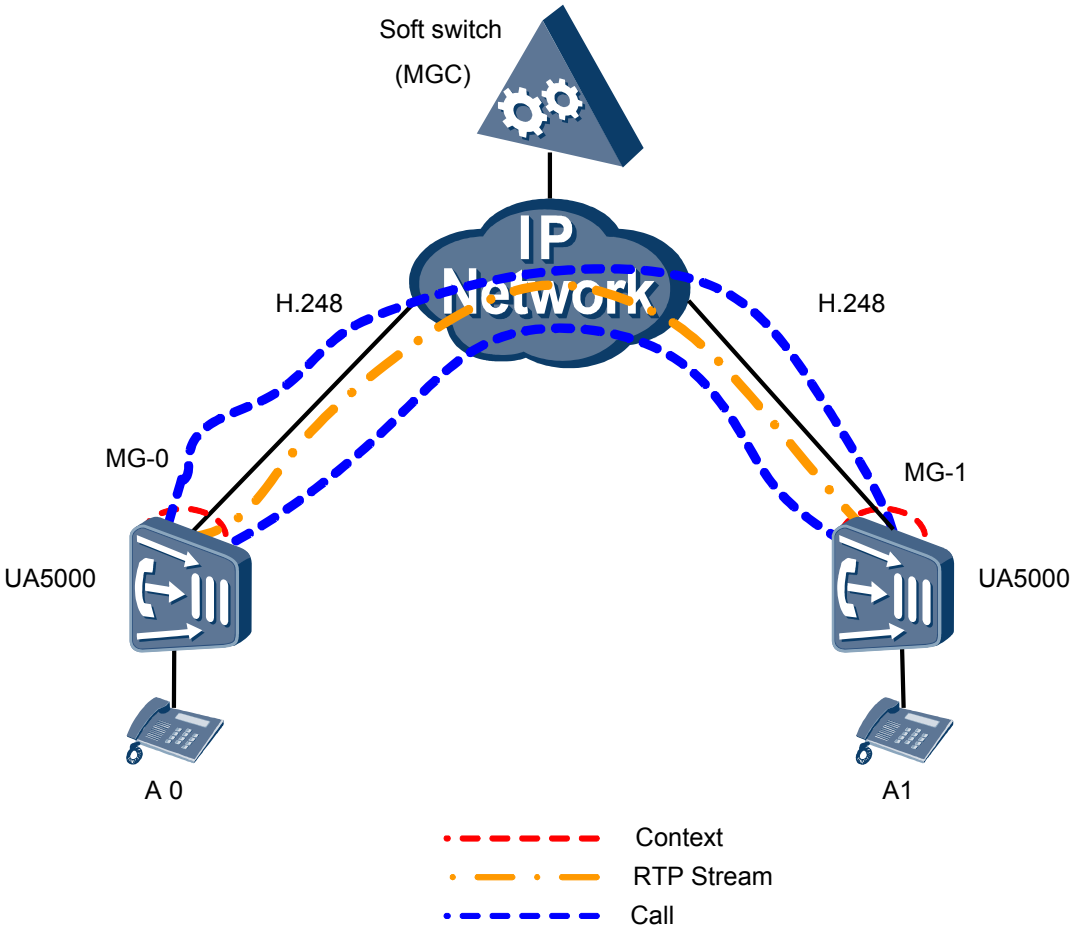
1. 网关（此处指 UA5000 设备，以下统称网关）向软交换发送 ServiceChange 进行注册，在注册消息中携带网关的数字签名。
2. 软交换收到 ServiceChange 命令后对网关身份进行认证，并应答。
3. 软交换向网关发送 Modify 消息，并带有所用到的算法 ID 和随机数。
4. 网关对收到的软交换消息进行验证，并发送应答。
5. 软交换向网关定期进行鉴权。
6. 网关对软交换进行应答。

27.3.2 VoIP（H.248）

介绍 H.248 协议的 VoIP 通话建立及释放的原理。

基于 H.248 协议的 VoIP 通话建立及释放的原理示意图如图 27-5 所示。

图 27-5 H.248 协议的 VoIP 语音原理结构图



通话建立及释放的基本流程如下：

1. MG-0 检测到用户 A0 摘机，将摘机事件通过 Notify 命令上报给 MGC。
2. MGC 收到摘机消息后，向 MG-0 发送号码表（Digitmap），并请求 MG-0 给 A0 放拨号音，同时检测收号完成事件。
3. 用户 A0 拨号，MG-0 根据 MGC 下发的号码表进行收号，并将匹配结果上报给 MGC。
4. MGC 向 MG-0 发送 Add 命令，请求创建上下文（Context），并将 A0 的 termination 和 RTP termination 加入上下文。
5. MG-0 建立上下文后，向 MGC 回送响应。响应中提供“会话描述”，给出对端向它发送分组需要的信息：IP 地址/UDP 端口号等。
6. MGC 向 MG-1 发送 Add 命令，请求创建上下文（Context），并将 A1 的 termination 和 RTP termination 加入上下文，将对端 A0 的 IP 地址/UDP 端口号下发给 A1。
7. MG-1 建立上下文后，向 MGC 回送响应，响应中提供“会话描述”，给出对端向它发送分组需要的信息：IP 地址/UDP 端口号等。
8. MG-1 检测到 A1 摘机，向 MGC 发送摘机事件，软交换使用 Modify 命令停止 A0 的回铃音和 A1 的振铃。

9. MGC 使用 Modify 命令将 MG-1 的会话描述传给 A0，于是 A0 和 A1 可进行双向通话。
10. MG-0 检测到用户 A0 挂机，将挂机事件通过 Notify 命令上报给 MGC。
11. MGC 分别向 MG-0 和 MG-1 下发 Modify 命令将 RTP 改为“只收模式”。
12. MGC 向 MG-1 发送 Modify 命令，要求 MG-1 向用户 A1 放忙音，并检测挂机事件。
13. MGC 向 MG-0 发送 Subtract 命令，释放为 A0 通话所申请的资源。
14. MG-1 检测到用户 A1 挂机，将挂机事件通过 Notify 命令上报给 MGC。
15. MGC 向 MG1 发送 Subtract 命令，释放为 A1 通话所申请的资源。
16. A0 和 A1 结束通话，并且释放全部资源。

27.3.3 MoIP（H.248）

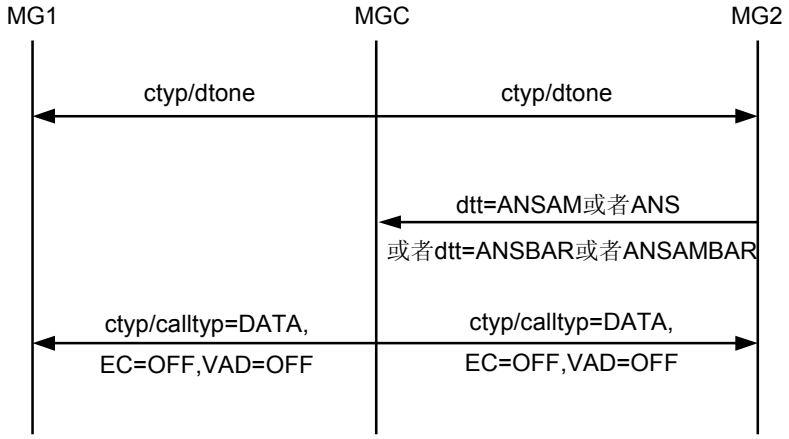
介绍 H.248 协议的 MoIP 连接建立及释放的原理。

MoIP（Modem over Internet Protocol）是在 IP 网络中或 IP 网与传统 PSTN 网络之间提供 Modem 业务。根据控制设备不同，可以分为软交换控制的 MoIP 和自切换 MoIP。

软交换控制的 MoIP

软交换控制的 Modem 流程如图 27-6 所示。

图 27-6 软交换控制的 Modem 流程



软交换控制的 Modem 基本流程如下：

1. 建立通话，如果软交换上配置了支持 Modem，给网关下发检测 Modem 事件命令。
2. 双方进入通话状态。
3. 在通话的过程中网关检测到 Modem 开始事件 ANS 或 ANSAM（这两种是低速 Modem 信号），ANSBAR 或 ANSAMBAR（这两种是高速 Modem 信号），上报给软交换。
4. 根据上报事件的不同，软交换下发命令将呼叫双方的 DSP 通道切换到高速或者低速 Modem 方式。
5. 网关根据软交换下发的命令，把通道切换到 Modem 模式，采用的编码方式是软交换下发的编码方式，采用的端口号是软交换下发的端口号。

Modem 通信中的回声抑制（EC）、静音检测（VAD）和工作模式的设置如下：

- 低速 Modem：EC 为 ON，VAD 为 OFF，DSP 工作模式为 Modem 方式。
- 高速 Modem：EC 为 OFF，VAD 为 OFF，DSP 工作模式为 Modem 方式。

自切换 MoIP

自切换的 Modem 基本流程如下：

1. 通话建立。
2. 两端网关检测 IP 和 TDM 侧的 Modem 事件，检测到事件后，若 Modem 传输模式配置为自切换模式，切换编解码为 G.711（a/μ 率可配置），根据检测到的高速、低速 Modem，修改 DSP 参数。
3. Modem 结束，呼叫释放。

27.3.4 FoIP（H.248）

介绍 H.248 协议的传真业务的实现原理。

FoIP 是一种在 IP 网络中或 IP 网与传统 PSTN 网络之间提供传真业务的方式。传真机可理解为一个特殊的 Modem，FoIP 协商时先进行 Modem 协商再进行 Fax 协商。

在 IP 网中承载传真业务根据传输协议的不同有两种方式：T.30 透传和 T.38 传真。根据控制设备不同，可以分为软交换控制下的 FoIP 和自切换的 FoIP。

软交换控制的 FoIP

传真可分为高速传真和低速传真，软交换控制下的低速传真支持 T.30 透传传真或 T.38 传真，基本流程如下：

1. 在网关软交换下配置传真业务、流程。
2. 建立语音通道后，软交换通知网关检测传真、Modem 事件。
3. 网关检测到传真事件后，将事件上报给软交换，事件包括低速 Modem（ANS 或 ANSAM）、低速传真（V.21Flag）。
4. 软交换根据配置的传真流程，指示两端网关修改 DSP 通道工作模式，使用 T.30 透传或 T.38 传真。
5. 传真开始。
6. 传真结束后，网关如果检测到传真结束事件，上报给软交换。
7. 软交换接收到传真结束事件后，指示两端网关修改 DSP 通道工作模式，切换回语音模式。
8. 继续通话。

软交换控制下的高速传真支持 T.30 透传传真，基本流程如下：

1. 在网关软交换下配置传真业务、流程。
2. 建立语音通道后，软交换通知网关检测 Fax、Modem 事件。
3. 网关检测到传真事件后，将事件上报给软交换，事件包括高速 Modem（ANSBAR 或 ANSAMBAR），低速传真（V.21Flag，如果对端为低速传真机或网络质量较差时，传真自动降速时上报此事件）。
4. 软交换根据配置的传真流程，指示两端网关修改 DSP 通道工作模式，使用 T.30 透传。

5. 传真开始。
6. 传真结束后，网关如果检测到传真结束事件，上报给软交换。
7. 软交换指示两端网关修改 DSP 通道工作模式，切换回语音模式继续通话。

自切换 FoIP

自切换的 T.30 透传传真或 T.38 传真，基本流程如下：

1. 在两端网关设备上配置自切换传真功能。
2. 呼叫建立，进入通话。
3. 网关设备检测 IP 和 TDM 侧的传真事件，检测到传真事件后，根据设置的传真模式，进行 DSP 通道的切换，使用 T.30 透传或 T.38 传真。
4. 传真结束后，如果检测到传真结束事件，切换到语音通道。
5. 继续通话。

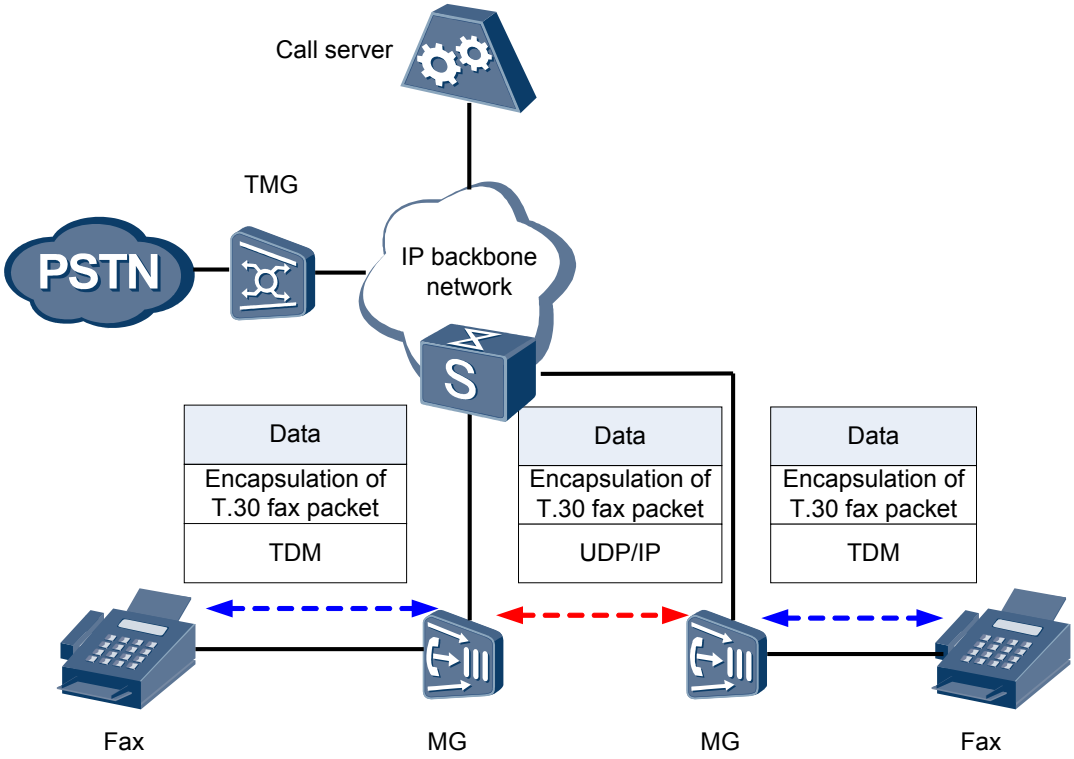
传真常用协议

分组语音网络中实现传真涉及到两个常用传真协议：ITU-T Recommendation T.30 和 T.38。

T.30 是基于 PSTN 网络的传真协议，详细定义了通用电话交换网中传真信号传送的呼叫流程，数据的调制方式（V.17/V.21/V.27/V.29/V.34）和传输格式（HDLC），以及传真信号的物理标准。网关间透传 T.30 传真消息与传真数据，即支持 T.30 方式的传真透传。这种方式的传真，可能因为 IP 网络的丢包、时延与乱序，传真质量不一定很高。

T.38 是一种基于 IP 网络的实时传真模式，网关将收到的来自传真机的 T.30 信号终结，以 T.38 协议将数据传送给对方网关，对方网关将收到的 T.38 包，还原成 T.30 信号。T.38 传真优点在于数据包有冗余处理机制，对网络要求不高（20%的丢包，传真也能通）。其缺点在于：DSP 需要参与 T.30 的解析，由于终端类型太多，可能存在兼容性问题。T.38 传真的原理图如**图 27-7** 所示。

图 27-7 T.38 传真的实现原理



28 SIP 语音

关于本章

首先对 SIP 协议进行介绍，然后详细介绍 SIP 协议的原理。

28.1 介绍
介绍该特性的定义、目的。

28.2 可获得性
介绍该特性需要的硬件支持和 License 支持。

28.3 原理描述
介绍与 SIP 相关的原理。

28.1 介绍

介绍该特性的定义、目的。

定义

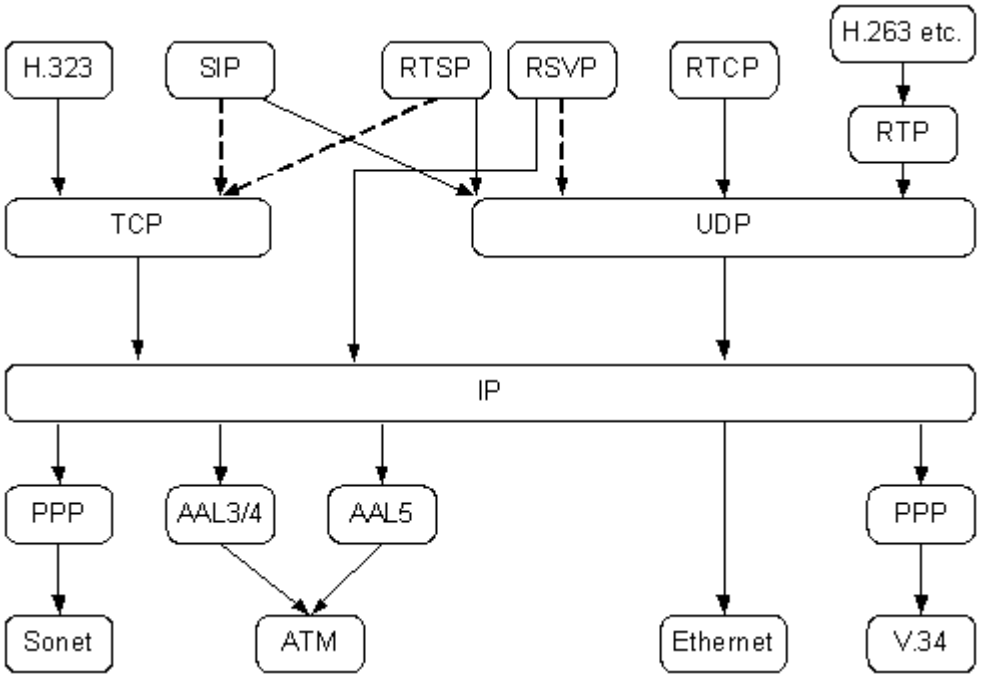
SIP（Session Initiation Protocol）协议是一个用于建立、更改或终止多媒体会话或呼叫的应用层协议。多媒体会话可以是多媒体会议，远程教学，因特网电话等各种应用。SIP 协议可用于发起会话，也可以用于邀请成员加入已经用其它方式建立的会话。SIP 协议透明地支持名字映射和重定向服务，便于实现 ISDN、智能网以及个人移动业务。一旦建立会话，媒体流将使用 RTP 协议在承载层中直接传送。

SIP 协议支持多媒体通信的五个方面：

1. 用户定位：确定用于通信的终端系统。
2. 用户能力：确定通信媒体和媒体的使用参数。
3. 用户可达性：确定被叫加入通信的意愿。
4. 呼叫建立：建立主叫和被叫的呼叫参数。
5. 呼叫处理：包括呼叫转移和呼叫终止。

SIP 协议是 IETF 多媒体数据和控制体系结构的一部分，IETF 多媒体数据及控制体系协议栈结构如图 28-1 所示。

图 28-1 IETF 多媒体数据及控制体系协议栈结构图



SIP 与其它协议相互合作，例如：RSVP（Resource ReServation Protocol）用于预约网络资源，RTP（Real-time Transmit Protocol）用于传输实时数据并提供服务质量（QoS）反馈，RTSP（ Real-Time Stream Protocol）用于控制实时媒体流的传输，SAP（Session

Announcement Protocol）用于通过组播发布多媒体会话，SDP（Session Description Protocol）用于描述多媒体会话。但是 SIP 协议的功能和实施并不依赖这些协议。

SIP 协议也可以与其他用于呼叫建立的信令协议配合。这种方式下，一个终端系统可通过 SIP 协议由一个独立于协议的特定地址得到对端的地址和协议。例如，SIP 可以用来确定对方可以通过 H.323 互通，得到 H.245 网关和用户的地址，然后用 H.225.0 来建立呼叫。又如，SIP 可用来确定被叫可通过 PSTN 互通，并且指出被叫电话号码，建议使用 Internet-to-PSTN 网关完成呼叫连接。

SIP 协议不提供会议控制服务，如场地控制，投票等，也没有对如何管理会议作出规定，但它可用来引入会议控制协议。SIP 协议不分配组播地址。

SIP 可以邀请用户参加资源预约或非预约的会话。SIP 本身并不预约资源，但可以向被邀请方传递必要的信息。

通过 SIP 协议网关执行 Internet 网与 PSTN/ISDN 网之间的互通，可以实现通过 Internet 网连接的 POTS 用户之间电话业务，也可以实现 POTS 用户与 Internet 电话用户间的呼叫连接。也可以设计实现与 H.323 协议互通的 SIP 协议网关。

SIP 协议是 IETF 提出的基于文本编码的 IP 电话/多媒体会议协议，它是一个轻量级协议（light-wight signalling），具有如下一些特性。

1. 最少状态：一个会议呼叫或电话呼叫可以包含一个或多个请求——响应事务（transaction）。代理服务器可以采用无状态方式工作。
2. 低层协议无关性：SIP 协议对低层协议作了最少的假设，低层协议可以为 SIP 协议层提供可靠或非可靠业务，可以为分组或字节流业务。Internet 环境下 SIP 协议层可以使用 UDP 协议或 TCP 协议，它首选 UDP 协议，当不能使用 UDP 协议时，使用 TCP 协议。
3. 基于文本：SIP 协议采用基于文本的 UTF-8 编码方式，采用字符集为 ISO 10646 字符集，易于用 Java 等语言实现，易于调试，灵活，扩展性好。当然，这可能造成消息长度的增大。通过对消息格式的仔细设计可以保证 SIP 消息易于解析。
4. 健壮性：SIP 协议健壮性可以通过下述方面体现。
   - 代理服务器可以不必保存呼叫状态；
   - 后续请求与重传可以采用不同路由；
   - 响应消息采用自寻路方式传送等。
5. 可扩展性：SIP 协议的可扩展性主要体现在：
   - 不可识别的头域可以忽略；
   - 用户可以指示 SIP 服务器必须理解的消息内容；
   - 新的头域容易引入；
   - 状态码采用分层编码方式进行编码。
6. 易于支持 IN 业务：通过与终端系统的配合，SIP 协议及其呼叫控制扩展能够支持绝大多数 ITU-T 的 Capability Set 1 中的业务及 Capability Set 2 中的业务。

目的

SIP 将从根本上改变通信服务提供方式以及用户的通信消费习惯，集成视音频电话、消息、web、电子邮件、同步浏览、会议等业务为一体的新的通信方式将给电信业带来创新。

采用 SIP 做为控制层协议的优势包括：

1. 基于公开的 Internet 标准，在语音、数据业务结合和互通方面具有天然优势，能跨越媒体和设备实现呼叫控制，支持丰富的媒体格式，可动态增、删媒体流，容易实现更加丰富的业务特性。
2. 支持智能向业务和终端侧发展，减轻网络的负担，方便业务开展。
3. SIP 支持应用层移动性功能：包括动态注册机制、位置管理机制、重定向机制等。
4. SIP 本身具有 Presence/Fork/订阅特性，便于扩展新业务。
5. 协议简单，具有公认的扩展潜力。

28.2 可获得性

介绍该特性需要的硬件支持和 License 支持。

硬件支持

无需额外硬件支持。

License 支持

VoIP (SIP)特性和 T.38 流程受 License 控制，需获得 License 许可方可获得该特性的服务。

28.3 原理描述

介绍与 SIP 相关的原理。

28.3.1 SIP 用户标识

介绍 SIP 协议中标识用户的原理。

SIP 用户标识包括 SIP URL 和 TEL URL，两者中任一个均可唯一标识一个 SIP 用户。用户标识在 MDU 和 IMS 上需要配置为一致。

SIP URL 用于 SIP 消息中，表示请求的发起者（From）、当前目的地（Request-URI）和最终接收者（To），还用于指定重定向地址（Contact）。SIP URL 也可以嵌入 WEB 页面或其它超链接表示某个用户或服务可以通过 SIP 来访问。当用于超链接时，SIP URL 表示使用 INVITE 方法。其表示方法如下：

SIP-URL="sip:"[userinfo "@"]hostport

例如：

sip:j.doe@big.com

sip:+1-212-555-1212:1234@gateway.com;user=phone

sip:1212@gateway.com

sip:alice@10.1.2.3

sip:alice@example.com

sip:alice%40example.com@gateway.com

TEL URL（电话 URI）用于标识占用某个电话号码的资源。号码可以是全球号码或本地号码。全球号码符合 E164 编码规范，以“＋”开始；本地号码遵从本地私有编号计划。格式：

tel:+86-755-6544487

tel:45687；phonecontext ＝ example.com

tel:45687；phonecontext ＝+86-755-65

28.3.2 SIP 消息格式

介绍 SIP 协议的消息格式。

格式

SIP 消息采用文本方式编码，行结束符为 CR 及 LF，包括请求消息与响应消息两类。格式如下：

SIP 消息 =	开始行
	*消息头域
	空行(CRLF)
	[消息体]
开始行 =	请求行 | 状态行
消息头 =	(通用头域| 请求头域| 响应头域|实体头域)

请求消息

MDU 支持的 SIP 请求消息包括 INVITE、ACK、OPTIONS、BYE、CANCEL、REGISTER、PRACK、UPDATE 等。各消息类型的用途如表 28-1 所示。

表 28-1 SIP 请求消息列表

请求消息类型	意义
INVITE	用于邀请用户加入一个呼叫
ACK	对请求消息的响应消息进行确认
OPTIONS	用于请求能力信息
BYE	用于释放已建立的呼叫
CANCEL	用于释放尚未建立的呼叫

请求消息类型	意义
REGISTER	用于向 SIP 网络服务器登记用户位置信息
PRACK	用于确认可靠临时响应
UPDATE	用于刷新会话

响应消息

SIP 响应消息用于对请求消息进行响应，指示呼叫的成功或失败状态。不同类的响应消息由状态码来区分，状态码包含三位整数，状态码的第一位用于定义响应类型，另外两位用于进一步对响应进行更加详细的说明。响应消息的分类如表 28-2 所示。

表 28-2 SIP 响应消息列表

1XX	Informational	Provisional
2XX	Success	Final
3XX	Redirection	Final
4XX	Client Error	Final
5XX	Server Error	Final
6XX	Global Failure	Final

- Provisional 用于指示呼叫正在进行。
- Final 用于结束请求消息。
- 1xx 表示已经接收到请求消息，正在对其进行处理。
- 2xx 表示请求已经被接收、处理并被成功接受。
- 3xx 表示为完成请求消息需要采取进一步的行动。
- 4xx 表示请求消息中包含语法错误或者 SIP 服务器不能完成对该请求消息的处理。
- 5xx 表示 SIP 服务器故障不能完成对正确消息的处理。
- 6xx 表示请求不能在任何 SIP 服务器上实现。

SIP 协议仅要求应用程序必须理解响应状态码的第一位，允许应用程序不对状态码的后两位进行处理。

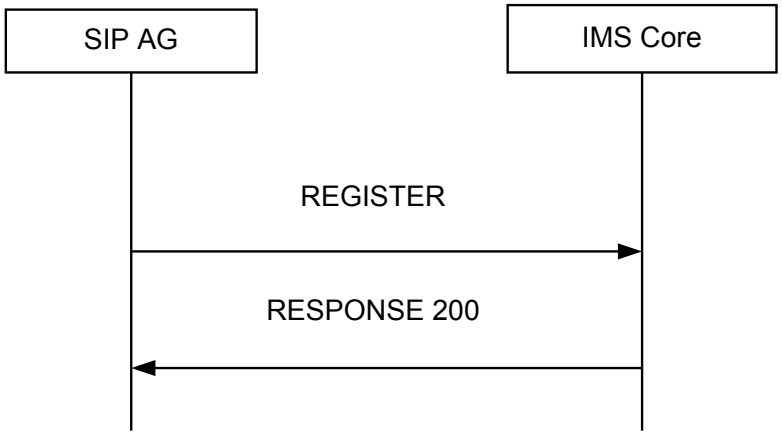
28.3.3 用户注册流程

SIP 用户在进行呼叫前，必须先向归属网络注册用户自身的信息。此处介绍用户注册的流程。

SIP 用户在进行呼叫前，必须先向归属网络注册用户自身的信息（如域名到 IP 地址的映射），注册分为无安全性连接和有安全性连接两种方式。系统上电或新添加用户后即启动用户注册流程。

无安全性连接的注册流程

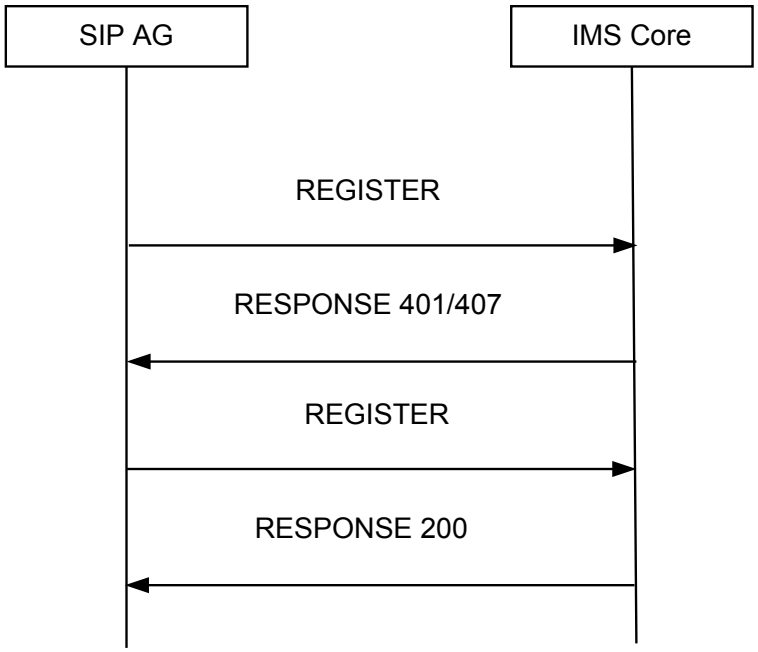
图 28-2 无安全性连接的注册流程图



如图 28-2 所示，SIP AG 为每个用户向 IMS Core 发 REGISTER 请求消息，消息中包含用户标识等信息。IMS Core 收到 REGISTER 请求消息后，判断 IMS 是否已配置该用户，若配置 OK，回复 200 消息给 SIP AG。

安全性连接的注册流程

图 28-3 安全性连接的注册流程图



如图 28-3 所示，SIP AG 为每个用户向 IMS Core 发 REGISTER 请求消息，消息中包含用户标识等信息。

IMS Core 回复 401/407 消息，其中包含密钥及加密方式等信息，SIP AG 用此密钥加密该用户的用户名和密码，重新构造 REGISTER 请求消息发送给 IMS Core，IMS Core 解密后判断用户名和密码是否正确，若正确回复 200 消息给 SIP AG。

说明

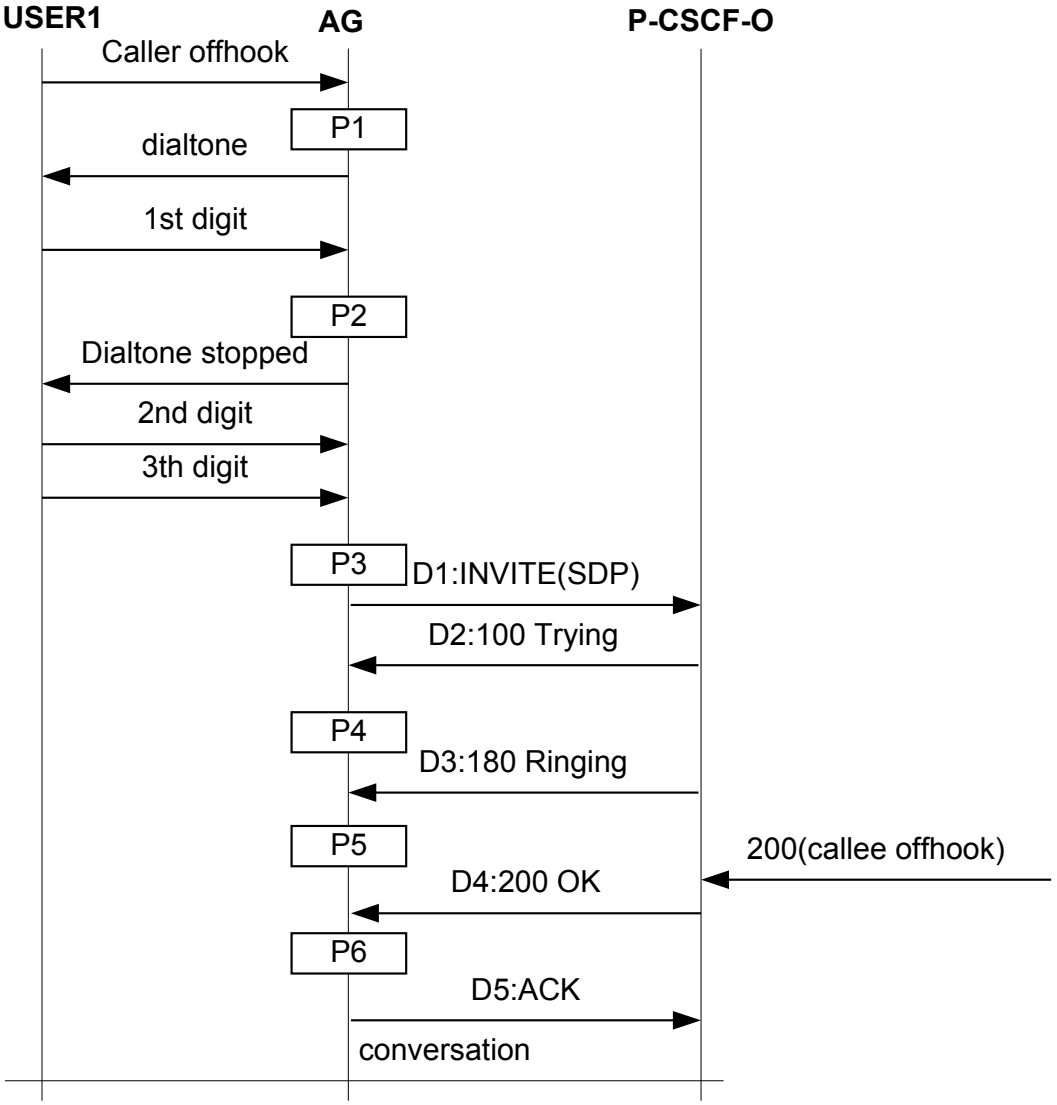
UA5000 支持 SIP 用户组注册。SIP 用户组的注册流程与单 SIP 用户注册流程一致，只是在具体的通信消息中，采用通配注册方式。

28.3.4 VoIP（SIP）普通主叫流程

介绍 VoIP（SIP）普通主叫流程。

基于 SIP 协议的 VoIP 普通主叫流程如图 28-4 所示。

图 28-4 基于 SIP 协议的 VoIP 普通主叫流程图



- P1：AG 收到主叫摘机消息，给主叫用户放拨号音。

- P2：AG 收到第一个拨号号码，停拨号音，并进行数图匹配。
- P3：AG 收到 N 个号码后，通过数图匹配，发现已经匹配上某个数图，则构造 INVITE 消息，发送给 P-CSCF。
- P4：AG 收到 100 响应，得知对端已经收到 INVITE 消息，则停止 INVITE 重发流程。
- P5：AG 收到 180，表示被叫用户已经在振铃，则 AG 给主叫用户放回铃音。
- P6：AG 收到 200，表示被叫用户已经摘机，则 AG 停止向主叫用户放回铃音，并将流模式改为双向。接着，AG 构造 ACK 消息发送给 P-CSCF。

以上为正常呼叫情况，此外还有分支的场景。当主叫用户发起呼叫时，由 P-CSCF 判断：

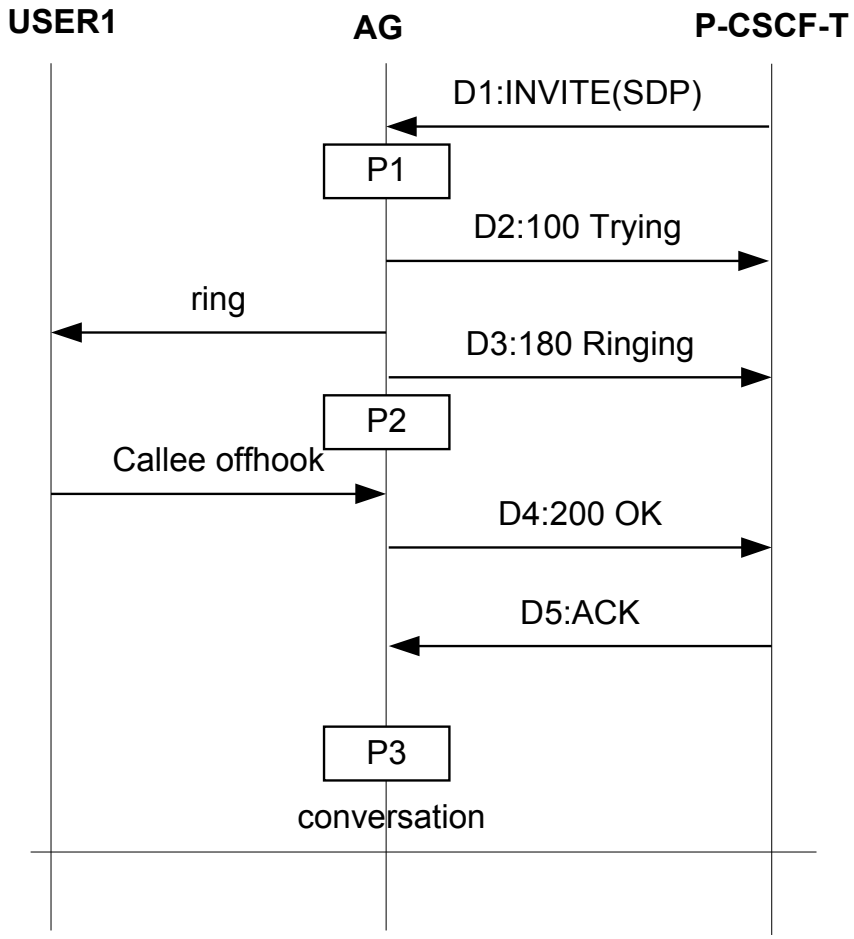
- 若主叫有数据但未注册，则拒绝主叫呼叫，回复 403。
- 若没有用户数据，则拒绝主叫呼叫，回复 404。

28.3.5 VoIP（SIP）被叫呼叫流程

介绍 VoIP（SIP）被叫呼叫流程。

基于 SIP 协议的 VoIP 被叫流程如图 28-5 所示。

图 28-5 基于 SIP 协议的 VoIP 被叫流程图



- P1：AG 收到 P-CSCF 发来的 INVITE 消息，构造 100 响应消息，发给 P-CSCF。AG 根据 INVITE 消息中携带的 P-Called-Party-ID 头域、RequestURI，TO 头域找到被叫用户（实际上，如果使用 TEL-URI 可以不要这个头域，根据 TEL-URI 上的电话号码即可找到被叫用户）。AG 找到被叫用户后，向被叫用户振铃，并构造 180 响应消息，发给 P-CSCF，告知被叫正在振铃。
- P2：AG 收到被叫用户摘机消息，停振铃，同时构造 200 消息，发给 P-CSCF，告知被叫已经摘机。
- P3：AG 收到 ACK 消息，双方进入通话态。

分支场景则由 AG 收到 INVITE 消息，进行判断：

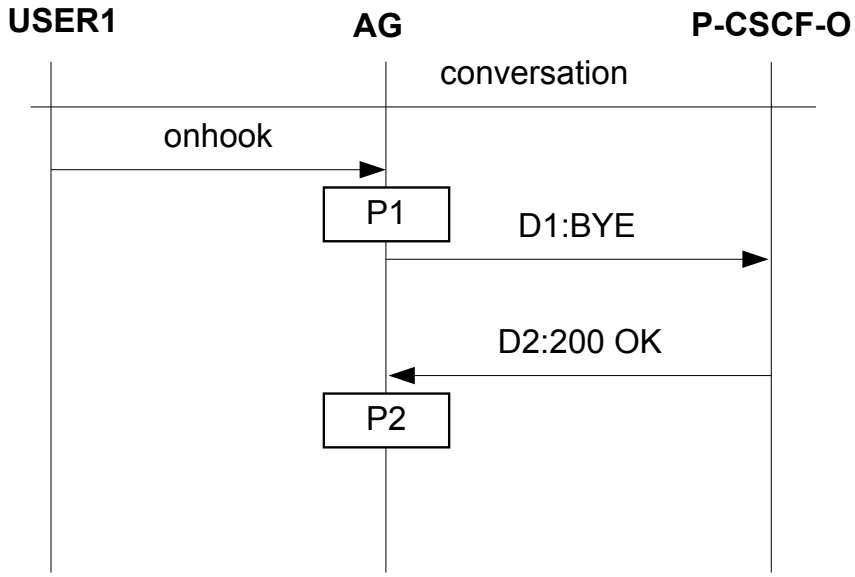
- 若被叫用户有数据但未注册，则拒绝主叫呼叫，回复 403。
- 若没有被叫用户数据，则拒绝主叫呼叫，回复 404。

28.3.6 呼叫释放流程

介绍 VoIP（SIP）呼叫中的呼叫释放流程。

呼叫释放流程如图 28-6 所示

图 28-6 呼叫释放流程图



- P1：AG 收到用户的挂机消息，构造 BYE 请求消息，发送给 P-CSCF，并释放分配给该用户的 DSP 资源。
- P2：AG 收到 P-CSCF 的 200 消息。

28.3.7 FoIP（SIP）

介绍基于 SIP 协议的传真实现机制。

FAX 根据传输协议的不同，可以分为透传和 T.38 两大类；而根据切换方式的不同又可以分为自切换和协商切换两种。这样一组合，就有了四种传真方式：自切换透传、自切换 T.38、协商切换透传、协商切换 T.38。

自切换的主要思想是：AG 检测到传真音，根据配置自行选择使用透传还是 T.38 方式，无需给对端发送任何信令。

协商切换的主要思想是：AG 检测到传真音，根据配置的协商方法，发送 re-INVITE，携带协商参数，和对端协商传真方式。

根据速率的不同，传真还可以分为低速传真和高速传真。高速传真不能使用 T.38，高速传真机实际可以看作是一个 MODEM。当然，也可以把高速传真进行降速来使用 T.38。

FAX 协商切换透传流程

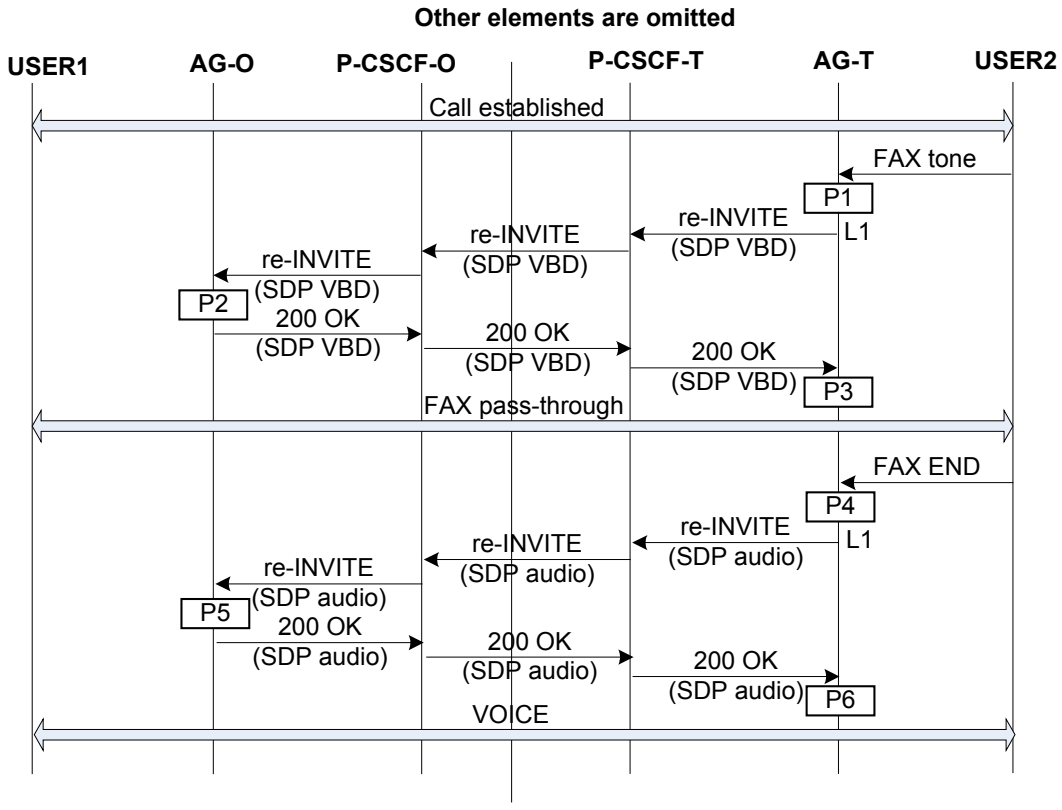
目前协商透传传真有三种方式。

- 第一种是以 a=fax 表示，由中国电信提出的 G.711 透传传真的方式。
- 第二种是以 a=silenceSupp:off 表示，是 draft-ietf-sipping-realtimefax-01.txt 提出的 G.711 透传传真的方式。
- 第三种是 VBD 的方式，表示方式 a=gpmd:99 vbd=yes，是 V.152 定义的 VBD 方式。

具体采用哪种方式进行传真，要根据参数配置来确定。

FAX 协商切换透传流程如图 28-7 所示。

图 28-7 FAX 协商切换透传流程图



- P1：AG-T 检测到 FAX 音，发送 re-INVITE 消息给主叫用户所在的 AG（AG-O）。
- L1：re-INVITE 消息携带的 SDP 消息可能有三种。在 AG 上需要配置使用哪种 FAX 的透传协商流程。协商的发起方根据配置来使用不同的 a 参数，协商的接受方则需

要兼容三种方式，即收到的 re-INVITE 消息里，无论使用哪种 a 参数，都可以完成协商流程。

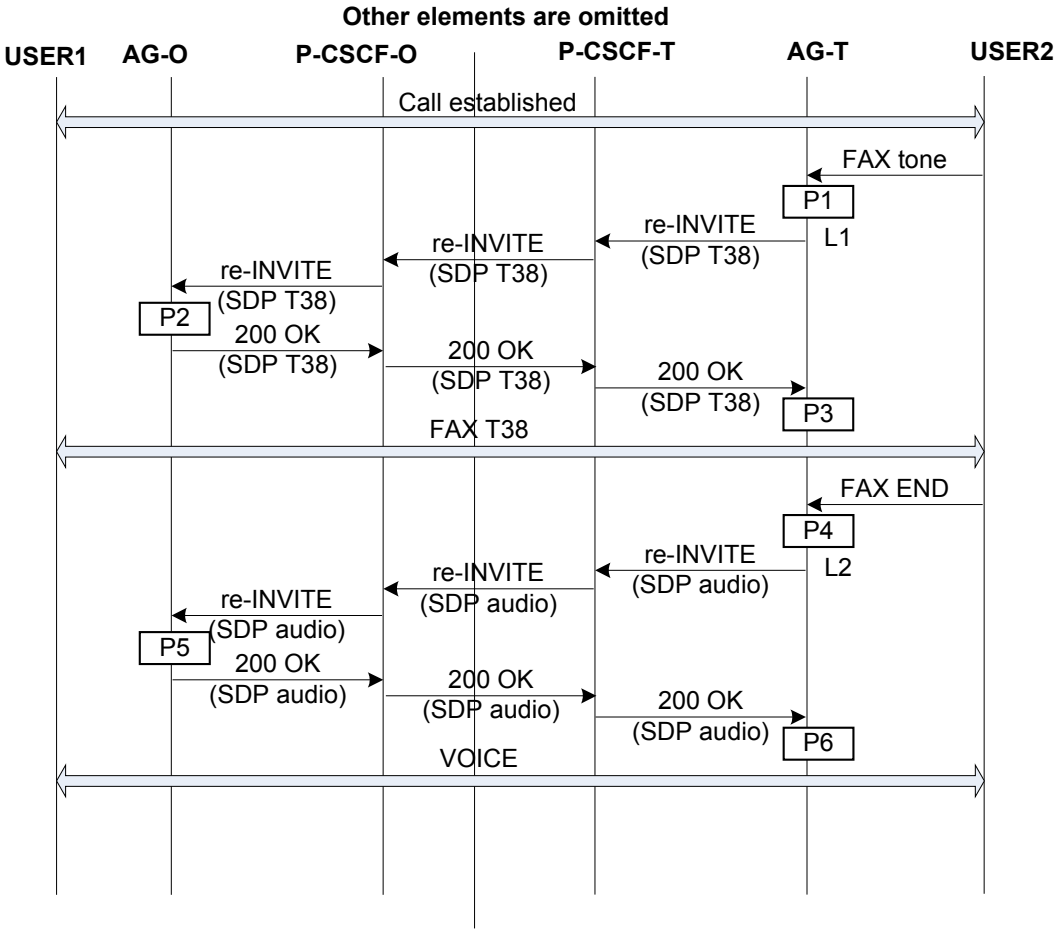
- 第一种是 draft-ietf-sipping-realtimefax-01.txt 提出的 G.711 透传 FAX/MODEM 的方式。
- 第二种是中国电信提出的 G.711 透传 FAX/MODEM 的方式。
- 第三种是 V.152 定义的 VBD 方式。

- P2：AG-O 收到 re-INVITE 消息，构造 200 OK 消息给 AG-T。
- P3：AG-T 收到 200 OK 消息，使用 FAX 方式打开 DSP 通道。
- P4：AG-T 收到传真结束信号，发送 re-INVITE 消息给 AG-O。
- L2：re-INVITE 消息携带的 SDP 信息为建立普通语音通道的 SDP 信息。
- P5：AG-O 收到 re-INVITE 消息，切换为语音模式。
- P6：AG-T 收到 200 OK 消息，也切换为语音模式。

FAX 协商切换 T.38 流程

FAX 协商切换 T.38 流程如图 28-8 所示。

图 28-8 FAX 协商切换 T.38 流程图



- P1：AG-T 检测到 FAX 音，发送 re-INVITE 消息到主叫用户所在的 AG（AG-O）。
- L1：re-INVITE 消息携带的 SDP 消息包含 T.38 相关的信息。
- P2：AG-O 收到 re-INVITE 消息，判断对端要求使用 T.38，则使用 FAX T.38 方式来打开通道，然后构造 200 OK 消息给 AG-T。
- P3：AG-T 收到 200 OK 消息，使用 FAX T.38 方式来打开 DSP 通道。
- P4：AG-T 收到传真结束信号，发送 re-INVITE 消息给 AG-O。
- L2：re-INVITE 消息携带的 SDP 信息为建立普通语音通道的 SDP 信息。
- P5：AG-O 收到 re-INVITE 消息，切换为语音模式。
- P6：AG-T 收到 200 OK 消息，切换为语音模式。

说明

如果对端设备不支持 T.38，则流程如图 28-9 和图 28-10 所示。

图 28-9 FAX 协商切换 T.38 流程图（对端不支持 T .38 的情况 1 ）

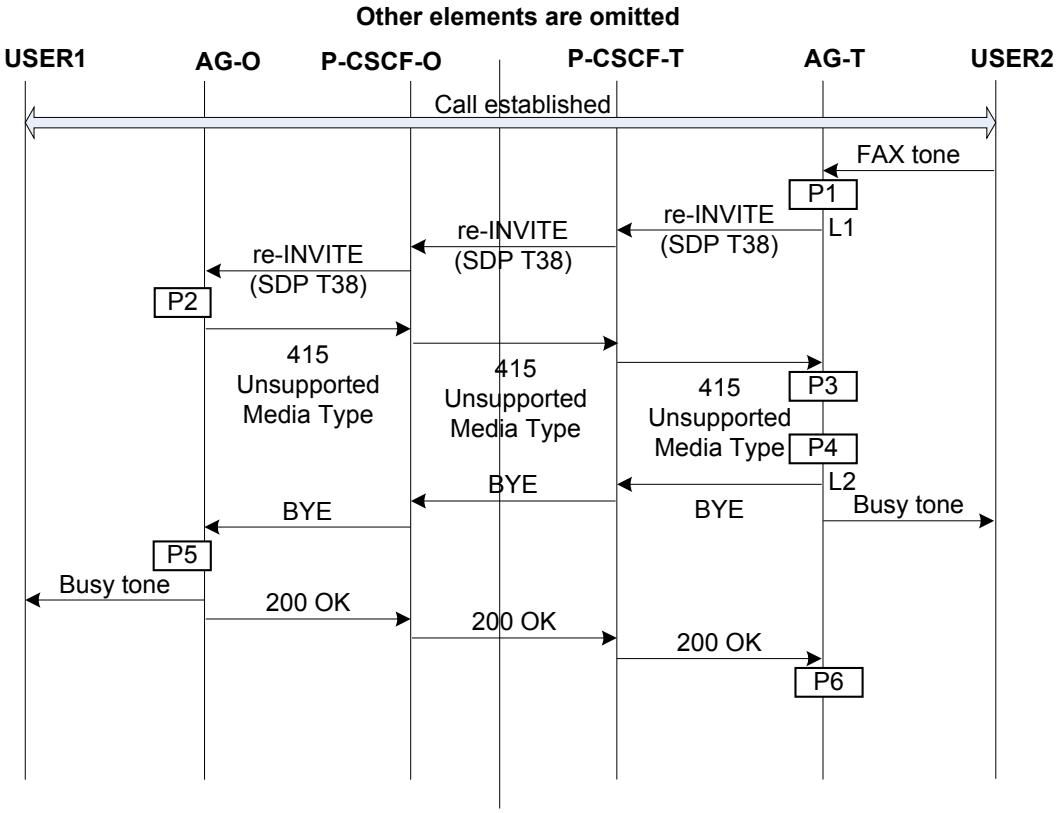
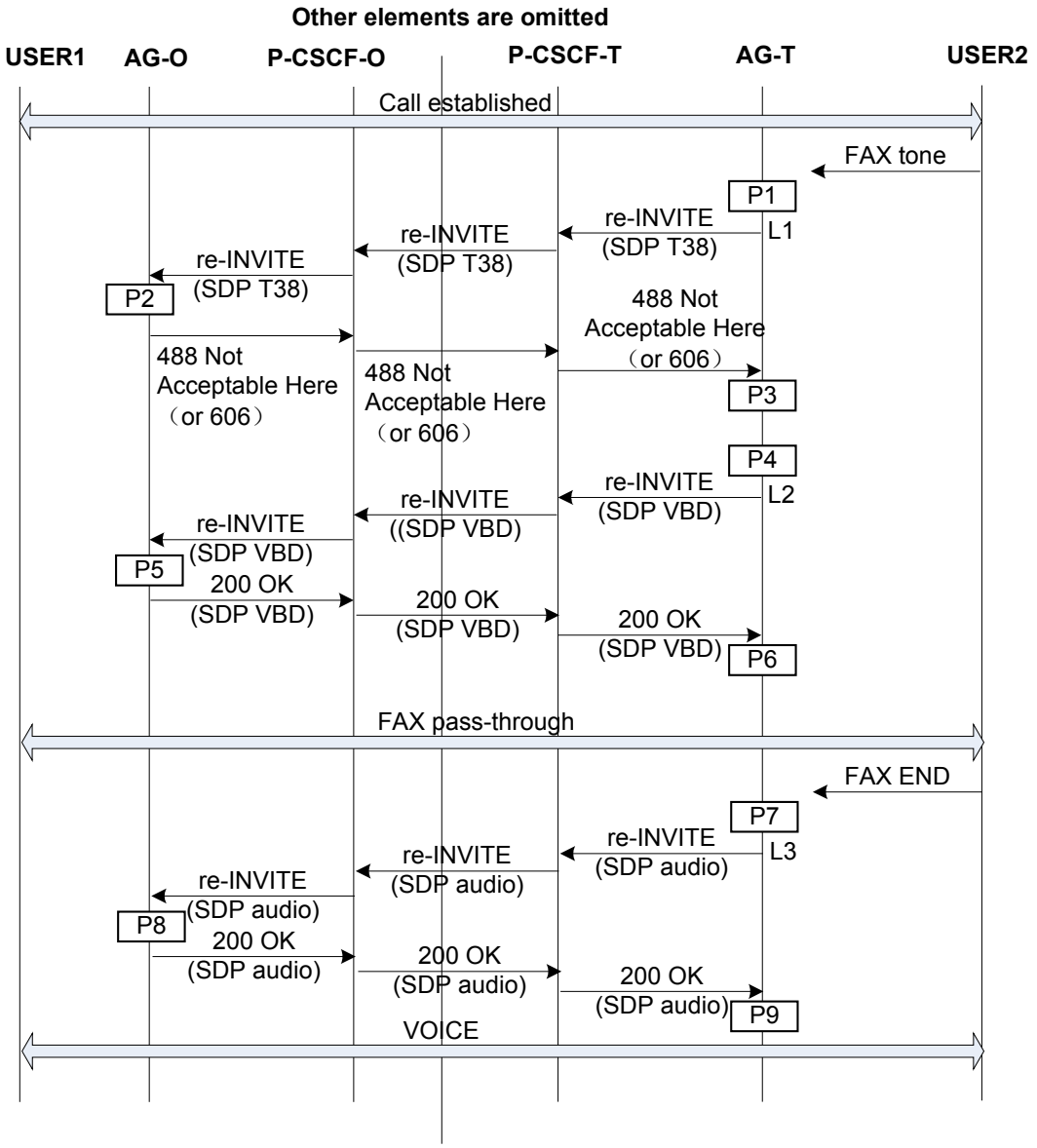


图 28-10 FAX 协商切换 T.38 流程图（对端不支持 T .38 的情况 2 ）



在图 28-9 中，如果 AG-O 不支持 T.38，则返回 415 Unsupported Media Type，AG-T 收到 415 响应，则发送 BYE，释放当前的呼叫。

在图 28-10 中，如果 AG-O 不支持 T.38，则返回 488 Not Acceptable Here 或者 606 Not Acceptable，AG-T 收到 488/606 响应，则重新构造 re-INVITE 消息，SDP 内携带的媒体类型为 VBD。即 T.38 方式协商不成功，则改为使用透传方式。

UA5000 设备支持 T.38 传真，所以 T.38 协商时是不会回 415/488/606 的，但是设备能够处理对端回来的这些错误码。

FAX 自切换透传流程

一般来说，作为被叫的 FAX 终端会先检测到 TDM 侧的 FAX 音，而作为主叫的 FAX 则会检测到 IP 侧过来的 FAX 音。检测到 FAX 音的一方自行切换到 FAX 透传模式即可，无需通过 SIP 进行协商。

FAX 自切换流程目前存在一个问题：如果之前的语音通话使用 G.729 的话，被叫检测到 FAX 音，先切换的 G.711 透传了，这时由于主叫的 DSP 还是工作在 G.729 方式下，可能无法识别 G.711 的语音包。这就要求 DSP 芯片在 G.729 或者其他编解码方式下，可以接收 G.711 的包。当然，DSP 必须能够检测 IP 侧的传真音并上报。

FAX 自切换 T.38 流程

FAX 自切换 T.38 流程和 FAX 自切换透传流程思想上是一样的，只是 AG 收到 FAX 音后，使用 T.38 模式打开 DSP 通道，而不是使用 FAX 透传模式。

28.3.8 MoIP（SIP）

介绍基于 SIP 协议的 Modem 业务流程。

MODEM 和传真透传在流程上是类似的，同样也可以分为自切换和协商切换两种。

而协商透传 Modem 有三种方式：

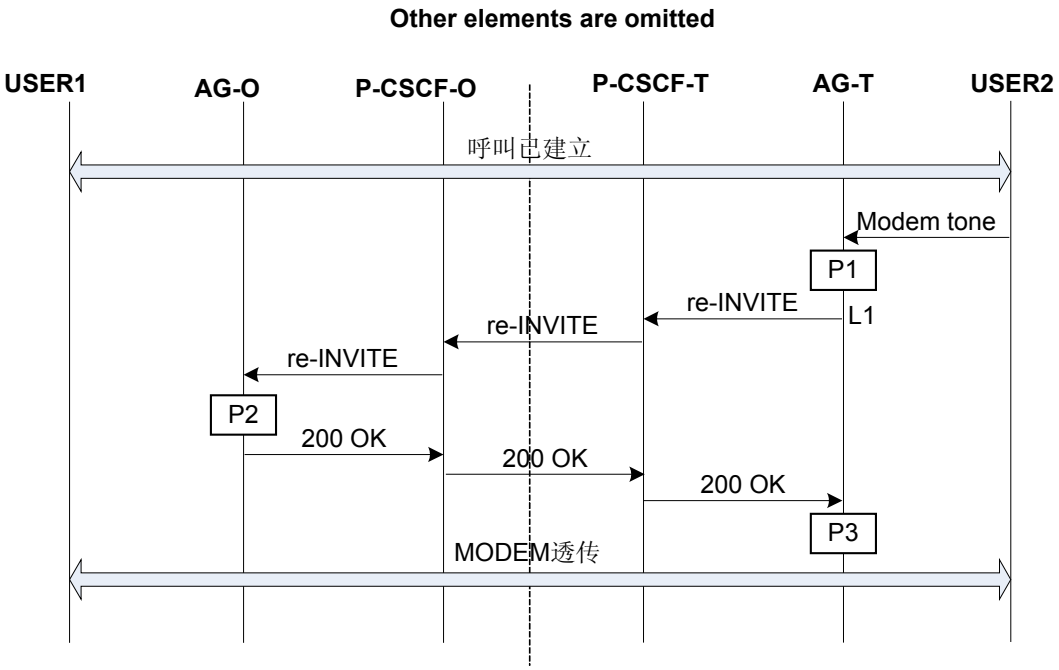
- 第一种是以 a=Modem 表示。这是由中国电信提出的 G.711 透传 Modem 的方式。
- 第二种是以 a=silenceSupp:off 表示。这是 draft-ietf-sipping-realtimefax-01.txt 提出的 G.711 透传 Modem 的方式。
- 第三种是以 a=gpmd:99 vbd=yes 表示。这是 V.152 定义的 VBD 方式。

具体采用哪种方式进行传真，需根据参数配置来确定。

MODEM 协商切换流程

MODEM 协商切换流程如图 28-11 所示。

图 28-11 MODEM 协商切换流程图



- P1：AG-T 检测到 MODEM 音，发送 re-INVITE 消息给主叫用户所在的 AG（AG-O）。
- L1：re-INVITE 消息携带的 SDP 消息可能有三种，这三种方式和上面 MODEM 协商透传的三种方式是对应的。在 AG 上，需要配置使用哪种 MODEM 的透传流程。
- P2：AG-O 收到 re-INVITE 消息后，构造 200 OK 消息发送给 AG-T。
- P3：AG-T 收到 200 OK 消息，使用 FAX 或者 MODEM 方式打开 DSP 通道。

MODEM 自切换

MODEM 自切换是指 AG 检测到 MODEM 音，自行切换到 VBD 模式，无需通知 IMS CORE 或者对端。

一般来说，作为被叫的 MODEM 终端会先检测到 TDM 侧的 MODEM 音，而作为主叫的 MODEM 则会检测到 IP 侧过来的 MODEM 音。检测到 MODEM 音的一方自行切换到 VBD 模式即可，无需通过 SIP 进行协商。

MODEM 冗余传送

MODEM 的冗余传送，目前是使用 RFC2198 协议来实现。

29 媒体流与信令流分离

关于本章

媒体流与信令流分离指一个网关可以给媒体流和信令流配置不同的 IP 和 QoS，以达到媒体流和信令流在各自的网络中传输的目的，保证业务的安全性和可靠性。

29.1 介绍

介绍该特性的定义、目的、规格和约束条件。

定义

媒体流与信令流分离指一个网关可以给媒体流和信令流配置不同的 IP 和 QoS，以达到媒体流和信令流在各自的网络中传输的目的，保证业务的安全性和可靠性。

目的

媒体流和信令流对网络 QoS 的要求不一致。由于信令存在重传机制，网络偶然丢包可以通过重传信令解决，而媒体丢包则直接影响语音业务。基于不同 QoS 需求，为了适应不同的组网环境，UA5000 支持对媒体流、信令流分别配置不同的 IP 和 QoS 参数，从而提高业务的可靠性。媒体流和信令流分离后，媒体流和信令流在各自的网络中传输，不能相互访问，可以保证业务的安全性。

规格

- 支持基于 IP 配置 802.1p/q，ToS 及 DSCP。
- 支持媒体流和信令流使用不同的 IP。
- 支持每个 VAG 使用不同的 IP。

术语

无。

缩略语

表 29-1 媒体流与信令流分离特性缩略语表

缩略语	英文全称	中文全称
DSCP	Differentiated Services Code Point	区分服务编码点
QoS	Quality of Service	业务质量
ToS	Type of Service	服务类型
VAG	Virtual Access Gateway	虚拟接入网关

29.2 可获得性

介绍该特性需要的硬件支持，包括单板和终端。

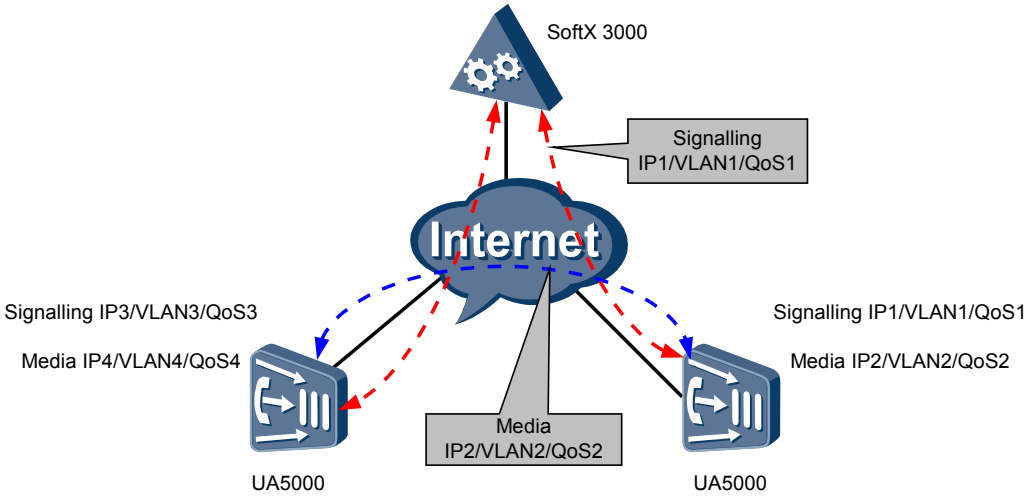
无需额外硬件支持。

29.3 原理描述（H.248）

介绍该特性的实现原理。

媒体流与信令流分离特性的应用组网图如图 29-1 所示。

图 29-1 媒体流与信令流分离应用组网图



当不使用媒体流与信令流分离特性时，媒体流 IP 和信令流 IP 配置为相同的 IP 地址，此时媒体流和信令流在同一张网络中可以相互访问。同时，媒体流和信令流使用同样的 QoS 参数，网络的质量对媒体流和信令流有相同的影响。

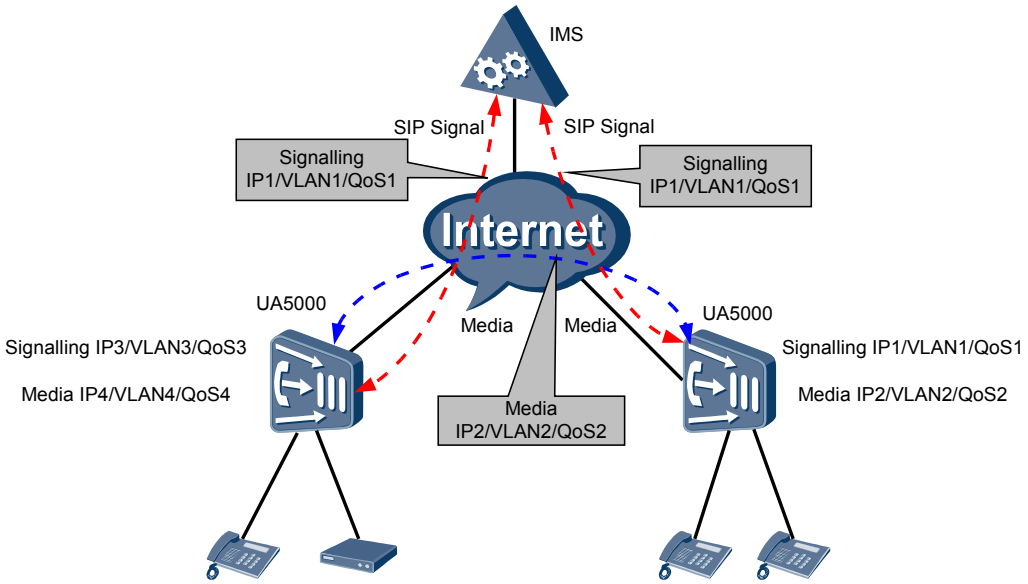
当使用媒体流与信令流分离特性后，媒体流 IP 和信令流 IP 配置为不同的 IP 地址，并可以针对每个 IP 地址配置不同的 VLAN、DSCP、ToS 等参数。这样在物理上或逻辑上隔离媒体流和信令流，两个网络不能相互访问，从而保证业务的可靠性和安全性。

29.4 原理描述（SIP）

介绍该特性的实现原理。

媒体流与信令流分离特性的应用组网图如图 29-2 所示。

图 29-2 媒体流与信令流分离应用组网图



当不使用媒体流与信令流分离特性时，媒体流 IP 和信令流 IP 配置为相同的 IP 地址，此时媒体流和信令流在同一张网络中可以相互访问。同时，媒体流和信令流使用同样的 QoS 参数，网络的质量对媒体流和信令流有相同的影响。

当使用媒体流与信令流分离特性后，媒体流 IP 和信令流 IP 配置为不同的 IP 地址，并可以针对每个 IP 地址配置不同的 VLAN、DSCP、ToS 等参数。这样在物理上或逻辑上隔离媒体流和信令流，两个网络不能相互访问，从而保证业务的可靠性和安全性。

30 VAG

关于本章

介绍 VAG 特性的定义、目的、规格、原理以及参考的术语、缩略语和相关协议标准。

30.1 介绍
介绍该特性的定义、目的、规格和约束条件。

30.2 可获得性
介绍该特性需要的硬件支持和 License 支持。

30.3 原理描述
介绍该特性的实现原理。

30.1 介绍

介绍该特性的定义、目的、规格和约束条件。

定义

虚拟接入网关（Virtual Access Gateway，VAG）可以将一台 AG 设备模拟成多台 AG 设备。

目的

VAG 的目的有以下两点：

- 区别服务

  通过在一台物理 AG 上虚拟多个逻辑 AG，实现不同的逻辑 AG 接入不同客户群的功能，为不同客户群实现不同的收敛比，满足区别的服务要求。
- 虚拟运营

  在 AG 的组网应用中，很多规模比较小的运营商并未购买独立的 AG 设备，而是通过租用其它运营商设备来实现业务。对于出租设备的运营商而言，为了提高设备的使用率，可以将一台设备租用给多个运营商。通过在一台物理 AG 上虚拟多个逻辑 AG，实现不同的逻辑 AG 接入不同软交换的功能，满足批发（Wholesale）的服务要求。

规格

- H.248 协议下最多支持 8 个 VAG。
- 每个 VAG 下用户数量不作限制。

约束

- 不同 VAG 不能实现自交换功能，只能同一个 VAG 实现自交换功能。
- 不同的 VAG 不能实现发夹功能，发卡功能只能在同一个 VAG 下实现。
- VAG 只针对 VoIP 用户，不支持 V5 用户。
- 不能为每个 VAG 单独提供网管 IP，网管 IP 是基于物理设备的，不是基于 VAG 的。
- 软件参数如数图最大匹配标志、自交换允许标志、自交换是否允许被切断标志等都是针对 VAG 实现的。
- 每个 VAG 的 MAC 地址是以太端口的 MAC 地址，主备用主控板的 MAC 地址不同。

术语

无。

缩略语

表 30-1 VAG 特性缩略语表

缩略语	英文全称	中文全称
VAG	Virtual Access Gateway	虚拟接入网关
DSP	Digital Signal Processing	数字信号处理器
AG	Access Gateway	接入网关
MG	Media Gateway	媒体网关
MGC	Media Gateway Controller	媒体网关控制器

30.2 可获得性

介绍该特性需要的硬件支持和 License 支持。

硬件支持

无需额外硬件支持。

License 支持

可使用的 VAG 数量受 License 控制。

30.3 原理描述

介绍该特性的实现原理。

VAG 的打电话流程和传统的打电话流程基本是一致的。主要的不同在于如下两点：

- DSP 资源的分配。
- 同一个 VAG 下的用户接续和通话的 IP 报文中的 IP 地址是该 VAG 对应的媒体 IP 地址。

主叫摘机处理步骤：

1. 用户摘机。
2. 主机申请 DSP 资源，如果没有为该 VAG 指定 DSP 资源，那么从共享资源池获取 DSP 资源。如果指定了 DSP 资源，那么从独占池获取 DSP 资源。
3. 呼叫接续和传统的 VoIP 用户一样。
4. 上报给 MGC 的信令流 IP 地址是该 VAG 的业务 IP 地址。
5. 后面的接续到通话整个过程与传统的 VoIP 用户一样。

在配置 VAG 的时候，首先需要增加一个 VAG 接口（即 MG 接口），然后进入到这个 VAG 的接口模式下，通过命令来配置接口参数。UA5000 可以支持 8 个独立的 IP 地址或者相同的 IP 地址但端口号不同的 VAG。每个 VAG 可以配置独立的信令 IP 地址、媒

体流 IP 地址（在同一个 VAG 中信令 IP 地址与媒体流 IP 地址可以不同），并可配置在不同的 VLAN 中。

每个 VAG 可以进行相互独立的配置及管理。每个 VAG 对于软交换来说，都是独立的媒体网关，可以分别独立配置鉴权、振铃映射、终端分层等媒体网关的相关属性而不互相影响。配置用户的时候需要指定该用户是所属的 VAG，不同 VAG 下的用户可以使用相同的终端 ID，但是所有 VAG 下用户数之和不能超过系统配置的用户数上限。

31 鉴权

关于本章

介绍鉴权特性的定义、目的、规格、原理以及参考的术语、缩略语和相关协议标准。

31.1 介绍
介绍该特性的定义、目的、规格和约束条件。

31.2 可获得性
介绍该特性需要的硬件支持，包括单板和终端。

31.3 原理描述(H.248)
介绍该特性的实现原理。

31.4 原理描述(SIP)
介绍 SIP 鉴权特性的实现原理。

31.5 参考信息
介绍该特性相关的参考信息。

31.1 介绍

介绍该特性的定义、目的、规格和约束条件。

定义

鉴权是媒体网关控制器（MGC）为了验证识别媒体网关（MG）用户身份合法性而建立的安全机制。

SIP 协议提供一种无状态的基于质询的鉴权机制。代理服务器或者 MG 设备在任何时候收到用户发来的请求时都可以向请求者质询鉴权。一旦请求方身份证实，接收方就能够确信该用户是否被授权发出请求。

目的

为了防止未经授权的实体利用 H.248 或 SIP 协议建立非法呼叫，或者干涉合法呼叫，提高系统的安全性。

规格

系统支持 MD5 和 HA1 加密算法。

在 H.248 协议中，实现 AH 协议应遵循 RFC2402。

在 SIP 协议中：

- SIP 鉴权支持 RFC3261 中定义的 Digest 鉴权模式，不支持 RFC2543 中定义的 Basic 鉴权模式。
- 单个请求消息支持一次 SIP 鉴权，不支持多次 SIP 鉴权和分叉 SIP 鉴权。
- 系统支持以下三种方式的 SIP 鉴权：
  - 针对 SIP 接口的鉴权
  - 针对 SIP 用户组的鉴权
  - 针对单个 SIP 用户的鉴权

约束

需要对接的软交换支持鉴权，否则该特性无法实现。

术语

表 31-1 鉴权特性术语表

术语	解释
Basic	RFC2617 定义的基本鉴权方案
Digest	RFC2617 定义的分类鉴权方案
IMSCore	IMS 核心域
SIPAG	支持 SIP 协议的 AG 设备

缩略语

表 31-2 鉴权特性缩略语表

缩略语	英文全称	中文全称
HTTP	Hypertext Transfer Protocol	超文本传输协议
MG	Media Gateway	媒体网关
MGC	Media Gateway Controller	媒体网关控制器
SIP	Session Initiation Protocol	会话初始协议
UAS	user agent server	用户代理服务器端
UAC	user agent client	用户代理客户端

31.2 可获得性

介绍该特性需要的硬件支持，包括单板和终端。

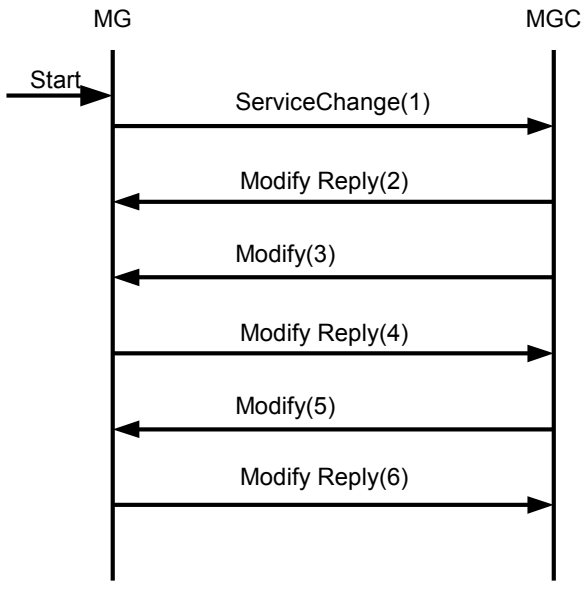
无需额外硬件支持。

31.3 原理描述(H.248)

介绍该特性的实现原理。

鉴权流程如图 31-1 所示。

图 31-1 鉴权流程图



鉴权流程如下：

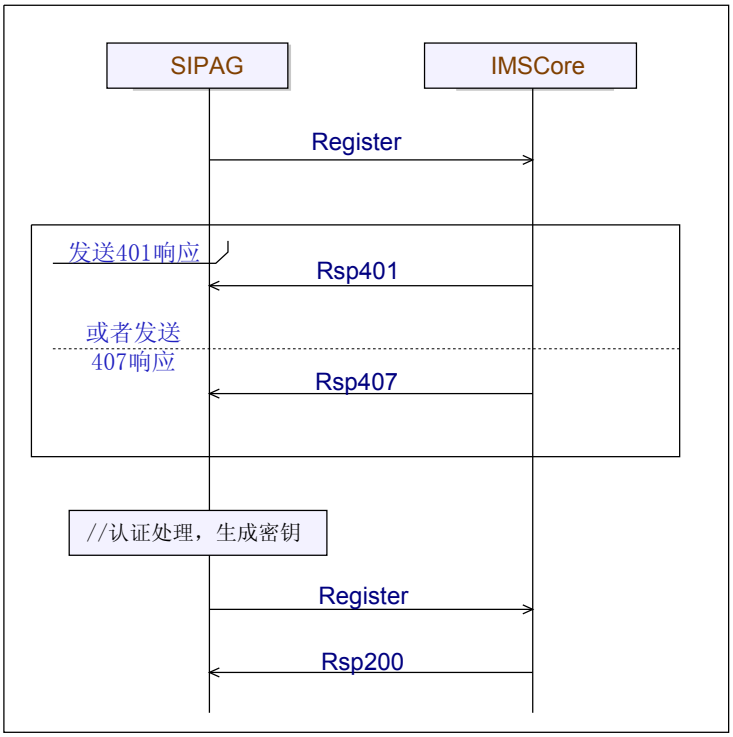
1. 网关向软交换发送 ServiceChange 进行注册，在注册消息中携带网关的数字签名。
2. 软交换收到 ServiceChange 命令后对网关身份进行认证，并应答。
3. 软交换向网关发送 Modify 消息，并带有所用到的算法 ID 和随机数。
4. 网关对收到的软交换消息进行验证，并发送应答。
5. 软交换向网关定期发送 Modify 消息进行周期性鉴权请求。
6. 网关对软交换进行应答。

31.4 原理描述(SIP)

介绍 SIP 鉴权特性的实现原理。

鉴权流程如图 31-2 所示。

图 31-2 鉴权流程图



SIP 协议鉴权的原理如下：

- SIP 鉴权的框架类似于 HTTP 鉴权。特别是 auth-scheme，auth-param，challenge，realm，realm-value 以及 credential 的 BNF（Backus-Naur form）很相似。SIP 协议提供一种无状态的基于质询的鉴权机制。代理服务器或者 UA（User Agent）在任何

时候收到用户发来的请求时都可以向请求者质询鉴权。一旦请求方身份证实，接收方就能够确信该用户是否被授权发出请求。

- 在 SIP 协议中，UAS（User Agent Server）使用 401（未鉴权）响应询问 UAC（User Agent Client）的身份。注册服务器和重定向服务器也使用该响应要求鉴权。只有代理服务器使用的是 407（代理服务器要求鉴权）响应。在不同的消息中可能分别要求包含 Proxy-Authenticate，Proxy-Authorization，WWW-Authenticate，WWW-Authorization 头域字段携带鉴权信息。

  说明

  - 由于 SIP 协议中没有 HTTP 鉴权中标准根 URL 的概念，SIP 中保护空间的概念就不同。在 RFC3261 的定义中，realm 字符串定义了保护空间。UA 和代理服务器要求对所收到的请求进行鉴权，服务器创建一个 realm 字符串的规则为：realm 字符串必须是唯一的，一个 realm 字符串包含一个主机名或一个域名。举例如下：

    INVITE sip:bob@biloxi.com SIP/2.0

    Authorization:Digest realm=" biloxi.com" , <… …>
  - 一般，SIP 协议鉴权只对某个特定的保护域有意义。对于分类鉴权，每个这样的保护域都有自己的一组用户名和密码。如果服务器对某请求不要求鉴权，它可以接受一个默认的用户名“anonymous”并且密码为空，而不是本域内特定的用户帐户。

- UAC 向 UAS 或代理服务器发送请求的时候，UAS 或代理服务器可以在处理请求之前要求 UAC 鉴权。如果请求中的相应头域字段没有证书信息，UAS 使用 401，代理服务器使用 407 状态吗拒绝请求，并要求鉴别用户权限。

  说明

  - 该 401 响应中携带 WWW-Authenticate 头域字段，407 响应中携带 Proxy-Authenticate 头域字段，头域字段中包含至少一个质询来指定适用于该 realm 的鉴权机制和参数。
  - 401 质询中的 WWW-Authenticate 头域字段示例如下：

    WWW-Authenticate: Digest realm=" biloxi.com",

    auth-scheme="MD5" qop="auth, auth-init",

    nonce="dcb45ef599gh599rf393224ggejh4566",

    opaque="fgj34r982940djak59398389djgh846"
  - Digest 指示鉴权方案为分类鉴权；realm 指示鉴权的保护空间；auth-scheme 指示鉴权使用的算法；qop 指示保护的质量，在计算认证信息时使用；nonce 指示服务器或 UAS 的现时值，计算认证信息时的输入随机值；opaque 为服务器提供的要求透传的参数。

- 当收到 401 或 407 响应后，UAC 根据返回 realm 域寻找用户鉴权使用的证书，并且根据响应返回的参数进行鉴权信息的计算和添加，在 Authorization 头域字段中带用户证书和鉴权信息。

说明

- Authorization 头域字段示例如下：

  Authorization: Digest username="bob".

  realm=" biloxi.com",

  nonce="dcb45ef599gh599rf393224ggejh4566",

  uri=" sip:bob@biloxi.com" qop="auth",

  nc=00000001,

  cnonce="0a4f113b",

  response="ace45fg599gh5f9rf393224ggejh44g5f",

  opaque="fgj34r982940djak59398389djgh846"

- Digest 指示鉴权方案为分类鉴权；username 指示鉴权的用户名；realm 指示鉴权的保护空间；nonce 指示服务器或 UAS 的现时值，计算认证信息时的输入随机值；uri 指示用户的资源定位符标识；qop 指示保护的质量，在计算认证信息时使用； nc 指示 UAC 中的认证序号；cnonce 指示 UAC 中计算鉴权信息时使用的现时参数值；opaque 为服务器提供的要求透传的参数；response 为最终根据加密算法生成的鉴权信息值。

- UAS 或代理服务器收到新的请求后，根据头域字段中证书和鉴权信息对用户进行认证，如果信息正确匹配，则鉴权成功。

31.5 参考信息

介绍该特性相关的参考信息。

本特性的参考资料清单如下：

- IETF RFC 2401 Security Architecture for the Internet Protocol
- IETF RFC 2402 IP Authentication Header
- IETF RFC 2406 IP Encapsulating Security Payload
- IETF RFC 2411 IP Security Document Roadmap

32 双归属

关于本章

介绍双归属特性的定义、目的、规格、原理以及参考的术语、缩略语和相关协议标准。

32.1 介绍
介绍该特性的定义、目的、规格和约束条件。

32.2 可获得性
介绍该特性需要的硬件支持和 License 支持。

32.3 原理描述(H.248)
介绍该特性的实现原理。

32.4 原理描述(SIP)
介绍该特性的实现原理。

32.5 原理描述(SCTP)
介绍该特性的实现原理。

32.1 介绍

介绍该特性的定义、目的、规格和约束条件。

定义

H.248 协议双归属定义为为一个 VAG 配置两个 MGC，VAG 在同一时刻只能注册在一台 MGC 上，当其中一个 MGC 发生故障，VAG 自动切换到另一个 MGC 上，保证业务的可靠性。

SIP 协议双归属定义为 MSAN 设备支持上行 P-CSCF 或 PROXY 设备的“1+1”互助模式（即主备方式部署），当上行主备设备中之一发生故障时，MSAN 业务能自动切换到另一设备，从而提供设备接入可靠性的 SIP 协议容灾解决方案。

SCTP（Stream Control Transmission Protocol）支持多归属，如果可以使用多个传输地址作为一个端点的目的地址，则这个 SCTP 端点可以被看作是多归属的。高层协议可以在多个目的地址中选择一个地址作为到这个多归属 SCTP 端点的首选通路。SCTP 采取了比较保守的策略，在连接建立时，会选择一条主用的路径（主用源地址和主用目的地址）进行传输。仅当主用路径不可达或需要重传时才使用其他路径。

目的

保证网络的高可靠性。

规格

目前，H.248 协议下的双归属有三种可配置规格：

- 不支持双归属
- 支持双归属，不支持自动回切
- 支持双归属，支持自动回切

SCTP 协议下的双归属：

- 为 IUA 链路配置两个远端 IP 地址后即可自动支持
- 不支持自动回切
- 只支持 SCTP 非平衡双归属，即只允许配置一个本端 IP 地址，最多允许配置两个远端 IP 地址（如果配置一个远端 IP 地址，则认为是 SCTP 单归属）

SIP 协议下的双归属：

- 支持上行 P-CSCF 或 PROXY 设备的主备双归属模式，不支持负荷分担多归属模式
- 上行双归属模式支持主备静态 IP 地址的配置
- 上行双归属模式支持查询主备域名 A

术语

表 32-1 双归属特性术语表

术语	解释
A 查询	DNS 协议资源记录查询的一种类型：根据域名返回对应的 IP 地址
SRV 查询	DNS 协议资源记录查询的一种类型：根据域名返回对应的 IP 地址和端口号的列表。在双归属方案中，列表中排在首位的为主用地址信息，排在第二位的为备用地址信息。
SCTP 偶联	SCTP（Stream Control Transmission Protocol）偶联实际是在两个 SCTP 端点间的一个对应关系，它包括了两个 SCTP 端点，以及包括验证标签和传送顺序号码等信息在内的协议状态信息。一个偶联可以由使用该偶联的 SCTP 端点用传送地址来唯一标识。在任何时候两个 SCTP 端点间都不会有多于一个的偶联。
SCTP 端点	SCTP 端点是 SCTP 分组中逻辑的接收方或者发送方。在一个多归属的主机上，一个 SCTP 端点可以由对端主机表示 SCTP 分组可以发送到的一组有效的目的地传输地址，或者是可以收到 SCTP 分组的一组有效的源传送地址。一个 SCTP 端点使用的所有传送地址必须使用相同的端口号，但可以使用多个 IP 地址。SCTP 端点使用的传送地址必须是唯一的。
传送地址	传送地址是用网络地址、传输层协议和传输层端口号定义的。当 SCTP 在 IP 网络层上运行时，传送地址就是由 IP 地址和 SCTP 端口号的组合来定义的，这里 SCTP 就充当传输协议。

缩略语

表 32-2 双归属特性缩略语表

缩略语	英文全称	中文全称
AG	Access Gateway	接入网关
CS	Call Server	呼叫服务器
MG	Media Gateway	媒体网关
MGC	Media Gateway Controller	媒体网关控制器
MSAN	Multi-service Access Node	多业务接入节点
NGW	Network gateway	PSTN 网络网关
P-CSCF	Proxy-Call Session Control Function	代理呼叫会话控制功能
PROXY	Proxy	代理服务器
SCTP	Stream Control Transmission Protocol	流传输控制协议

缩略语	英文全称	中文全称
VAG	Virtual Access Gateway	虚拟接入网关

32.2 可获得性

介绍该特性需要的硬件支持和 License 支持。

硬件支持

无需额外硬件支持。

License 支持

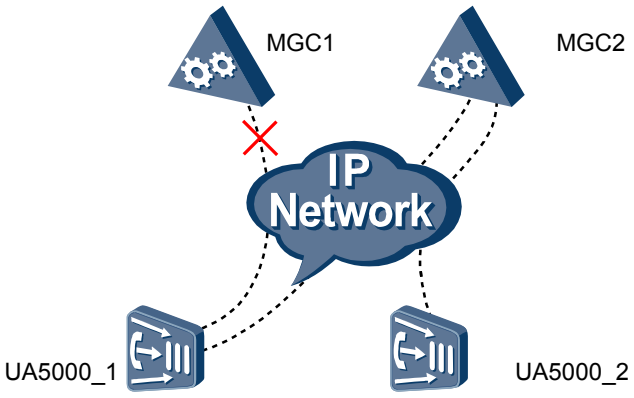
双归属特性受 License 控制。

32.3 原理描述(H.248)

介绍该特性的实现原理。

双归属的组网如图 32-1 所示。

图 32-1 双归属组网图

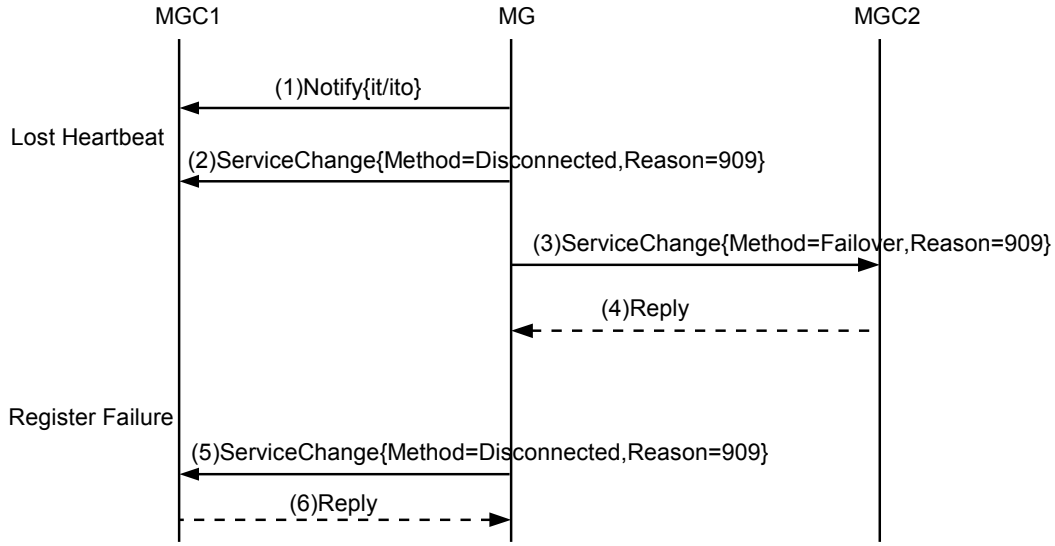


配置了两个 MGC，分别为 MGC1 和 MGC2。UA5000_1（即 UA5000）可以在 MGC1 和 MGC2 上注册，但同一时刻只能在其中一个 MGC 上注册。UA5000_2（即 UA5000）只能在 MGC2 上注册。当 MGC1 发生故障时，UA5000_1 可以自动切换到 MGC2 上。

不支持自动回切的双归属

不支持自动回切的双归属实现原理流程图如图 32-2 所示。

图 32-2 不支持双归属的自动回切原理流程图



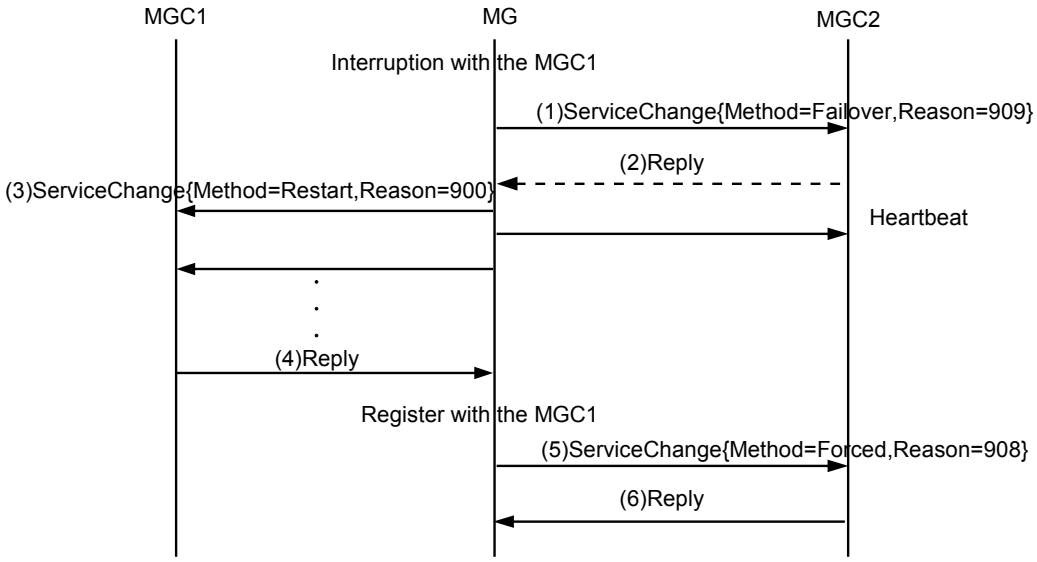
不支持双归属自动回切的基本流程如下：

1. MG 向 MGC1 发送的心跳检测消息 Notify{it/ito}连续 N 个没有得到响应，确定与 MGC1 的连接暂时中断。
2. MG 向 MGC1 发送注册消息 ServiceChange，仍然没有得到响应，判定主控的 MGC1 故障。
3. MG 根据预置的 MGC2 发送注册消息 ServiceChange{Method=Failover, Reason=909}（MGC 临近故障）。
4. MG 如果得到 MGC2 的响应消息 Reply，判定向 MGC2 注册成功，本流程结束。MG 如果向 MGC2 发送的 ServiceChange 连续 N 个没有得到响应，判定向 MGC2 注册失败。
5. 如果向 MGC2 注册失败，则向原主控 MGC1 发送注册消息 ServiceChange {Method=Disconnected, Reason=909}。
6. MG 如果得到 MGC1 的响应消息 Reply，那么判定与 MGC1 恢复通信，本流程结束。MG 如果向 MGC1 发送的 ServiceChange 连续 N 个没有得到响应，判定向 MGC1 注册失败，回到**步骤 3**。

支持自动回切的双归属

支持自动回切的双归属实现原理流程图如**图 32-3** 所示。

图 32-3 支持双归属自动回切原理流程图



双归属自动回切的基本流程如下：

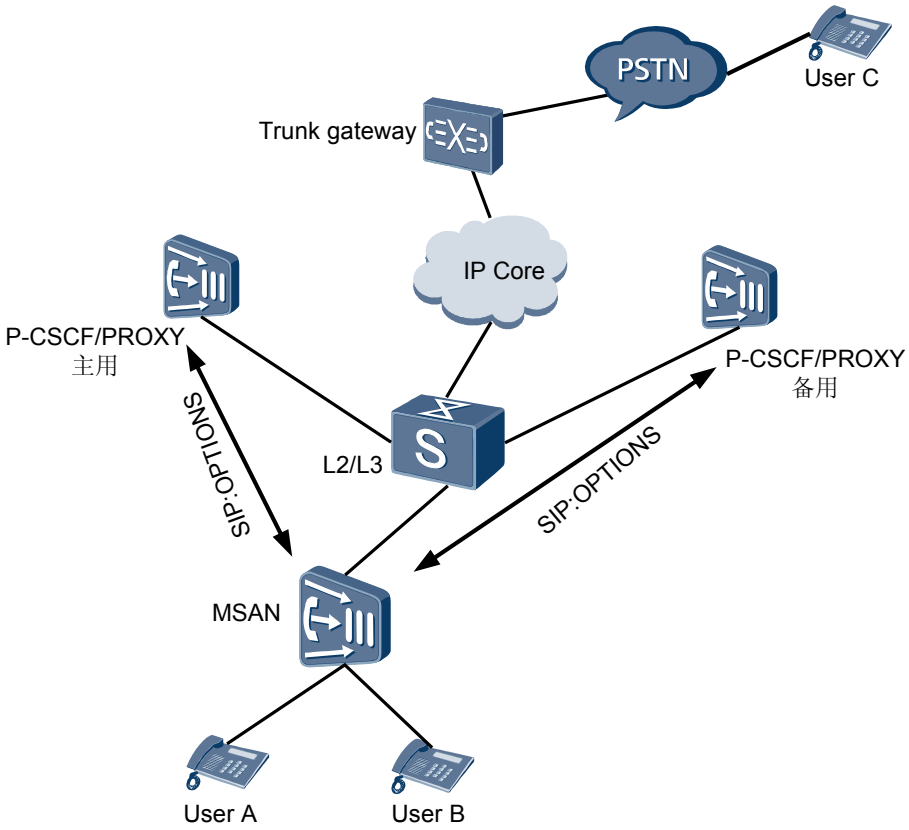
1. MG（即 UA5000）通过心跳消息检测到与主用 MGC1 联系中断，向备用 MGC2 发送注册消息 ServiceChange{Method=Failover, Reason=909}（MGC 临近故障）。
2. MG 得到 MGC2 的响应消息 Reply，注册成功，由 MGC2 开始控制 MG。
3. MG 同时定时给主用 MGC1 发送注册消息 ServiceChange {Method=Restart,Reason=900}。
4. 如果收到主用 MGC1 的响应则说明已经注册到主用 MGC1，进入**步骤 5**。没有收到响应则一直发。在此期间可以在备用软交换上建立业务。
5. 注册到主用 MGC1 后，向备用 MGC2 发退出服务 ServiceChange {Method=Forced,Reason=908}，等待 MGC2 响应。
6. MGC2 发送响应消息 Reply，结束对 MG 的控制。

32.4 原理描述(SIP)

介绍该特性的实现原理。

SIP 协议双归属的组网如**图 32-4** 所示。

图 32-4 双归属组网图



MSAN 设备分别接入到主备用上层设备，通过 SIP 信令机制检测到上行设备之间的连接状态，根据主备用上行设备的连接状态控制 MSAN 设备业务信令的流向。方案描述如下：

- MSAN 上配置并获得主备用 P-CSCF/PROXY 的 IP 地址；分别与主用 P-CSCF/PROXY、备用 P-CSCF/PROXY 建立两条链路；初始状态都为故障。
- MSAN 周期性地分别向主用 P-CSCF/PROXY 与备用 P-CSCF/PROXY 发送心跳信号（SIP : OPTIONS 消息），当正常收到响应后，设置链路正常。当连续多次无法收到响应后，设置链路故障。
- MSAN 在主备用 P-CSCF/PROXY 都正常、主备链路都正常的情况下，优先向主用 AS1 发送业务请求。
- 当 MSAN 通过定时的心跳信号检测到主用 P-CSCF/PROXY 故障并设置主用链路故障时，所有业务请求通过备用链路发给备用 P-CSCF/PROXY 处理。由于当前用户的活动上行设备为主用 P-CSCF/PROXY，所以在上行设备层面引发倒换操作，设置当前用户的活动上行设备为备用 P-CSCF/PROXY。同时减缓向主用 P-CSCF/PROXY 发送心跳信号的频率。
- 当主用 P-CSCF/PROXY 故障恢复时，MSAN 可以通过定时的心跳信号检测到，设置主用链路正常，所有业务请求通过主用链路发给主用 P-CSCF/PROXY 处理，上行设备检测到当前用户的活动设备为备用 P-CSCF/PROXY，所以在上行设备层面引发切回操作，设置当前用户的话动设备为主用 P-CSCF/PROXY。同时恢复向主用 P-CSCF/PROXY 发送心跳信号的频率。

- 当主备用 P-CSCF/PROXY 都故障时，设置主备用链路都故障，同时减缓向主备用 P-CSCF/PROXY 发送心跳信号的频率；并停止对外发送业务请求（包括注册消息）。

主备用 P-CSCF/PROXY 地址的获取

主备用 P-CSCF/PROXY 地址的获取在 MSAN 实现有两种方式：

- 直接在 MSAN 上配置主备用 P-CSCF/PROXY 的 IP 地址和端口号。
- 在 MSAN 上配置主备用 P-CSCF/PROXY 的域名和端口号，通过 DNS-A 查询获取对应的主备用 P-CSCF/PROXY 的 IP 地址。

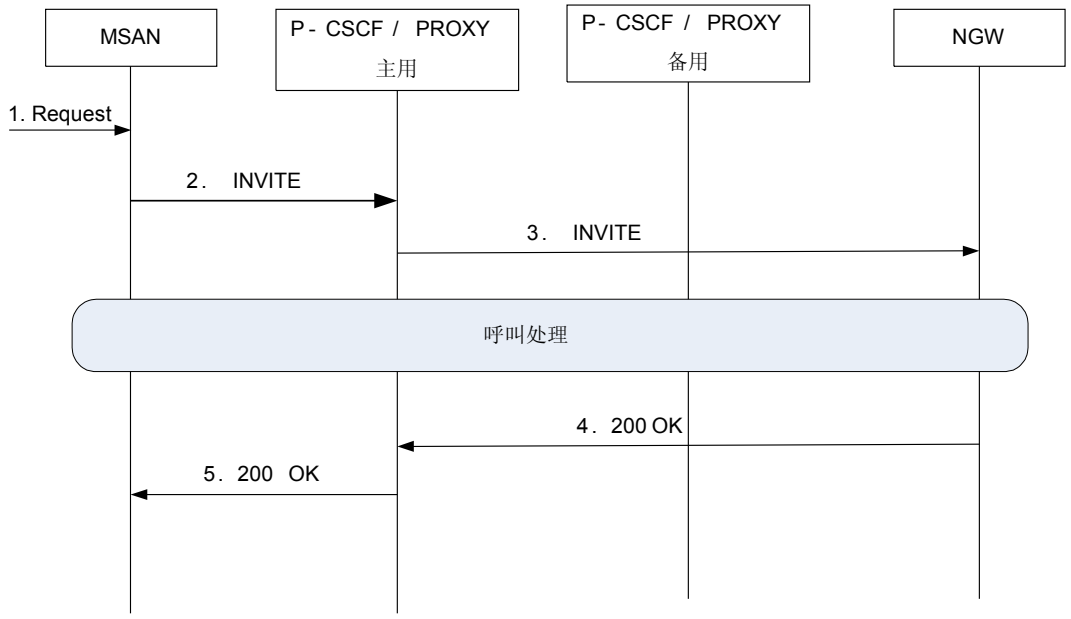
上行 P-CSCF/PROXY 故障检测机制

MSAN 对 P-CSCF/PROXY 的 SIP OPTIONS 检测是指 MSAN 周期性向主备 P-CSCF 发送 OPTIONS 消息，如果连续多个检测消息无法收到响应，则判定对端故障。SIP OPTIONS 检测的周期和故障判定条件可以配置修改。

主备用 P-CSCF/PROXY 正常场景

主备用 P-CSCF/PROXY 都正常，主叫业务流程如图 32-5 所示。

图 32-5 主备用 P-CSCF/PROXY 正常场景下主叫业务流程图



流程如下：

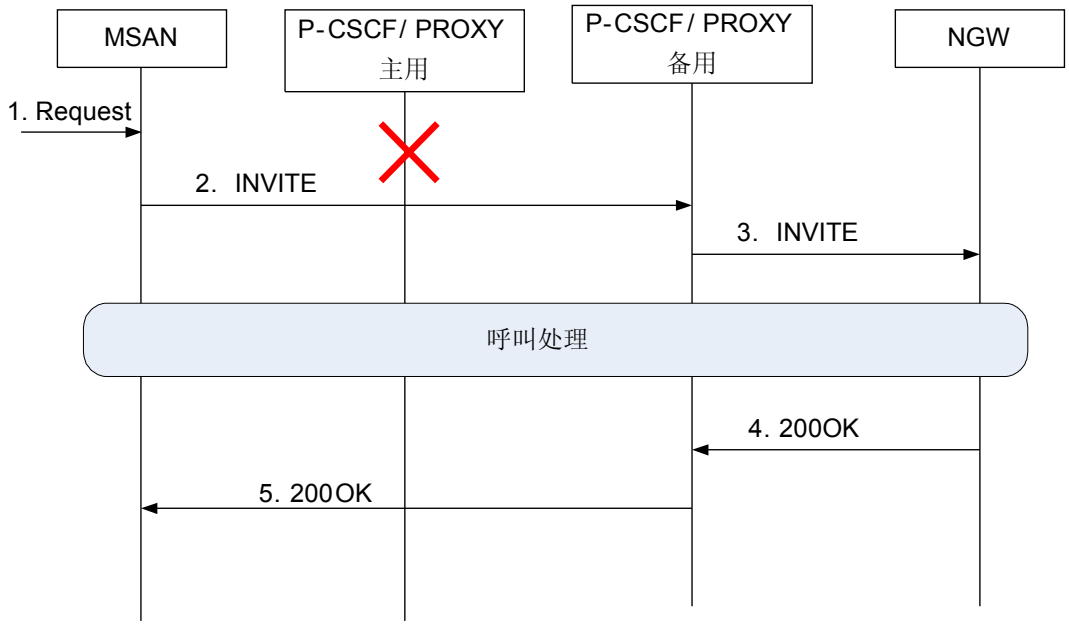
1. Request：MSAN 收到终端用户发起的业务请求。
2. INVITE：主备用 P-CSCF/PROXY 都正常，MSAN 优先向主用 P-CSCF/PROXY 发送初始业务请求。并在主用 P-CSCF/PROXY 上建呼叫。
3. INVITE：主用 P-CSCF/PROXY 将 INVITE 转发给被叫侧网关（NGW）。
4. 200 OK：被叫应答呼叫，发送 200 OK 响应到主用 P-CSCF/PROXY。

5. 200 OK：主用 P-CSCF/PROXY 将 200 OK 响应发返回给主叫，建立起通话。

主用 P-CSCF/PROXY 故障场景

主用 P-CSCF/PROXY 故障，主叫业务流程如图 32-6 所示。

图 32-6 主用 P-CSCF/PROXY 故障场景下主叫业务流程图



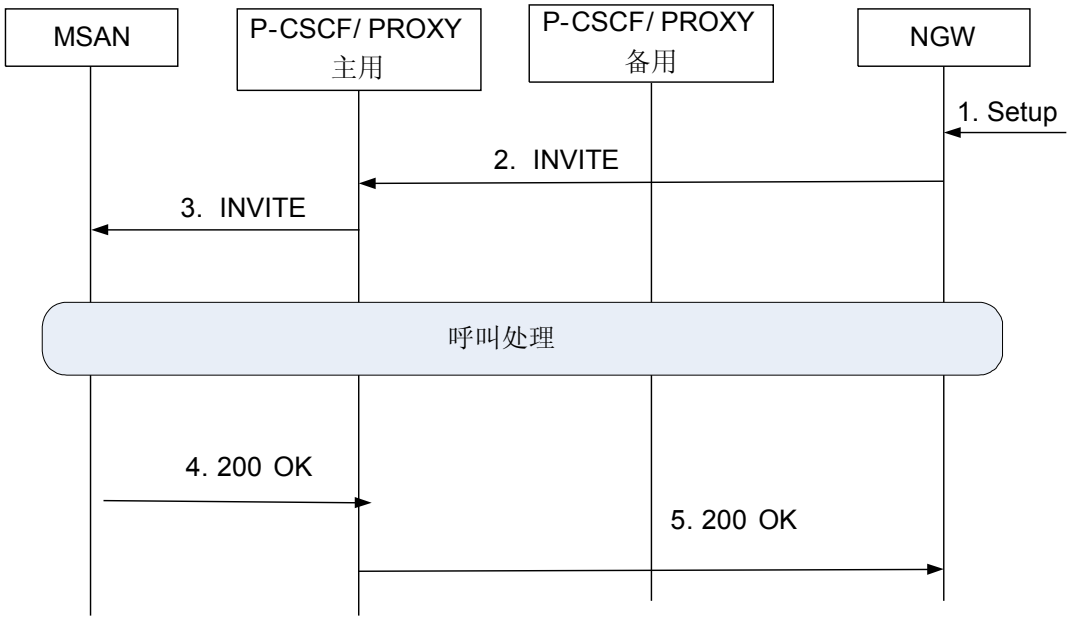
流程如下：

1. Request：MSAN 收到终端用户发起的业务请求。
2. INVITE：主用 P-CSCF/PROXY 故障，备用 P-CSCF/PROXY 正常，MSAN 向备用 P-CSCF/PROXY 发送初始业务请求。并在备用 P-CSCF/PROXY 上建立呼叫。
3. INVITE：备用 P-CSCF/PROXY 将 INVITE 转发给被叫侧网关（NGW）。
4. 200 OK：被叫应答呼叫，发送 200 OK 响应到备用 P-CSCF/PROXY。
5. 200 OK：备用 P-CSCF/PROXY 将 200 OK 响应发返回给主叫，建立起通话。

被叫业务 P-CSCF/PROXY 故障

主备用 P-CSCF/PROXY 都正常，被叫业务流程如图 32-7 所示。

图 32-7 主备用 P-CSCF/PROXY 正常场景下被叫业务流程图

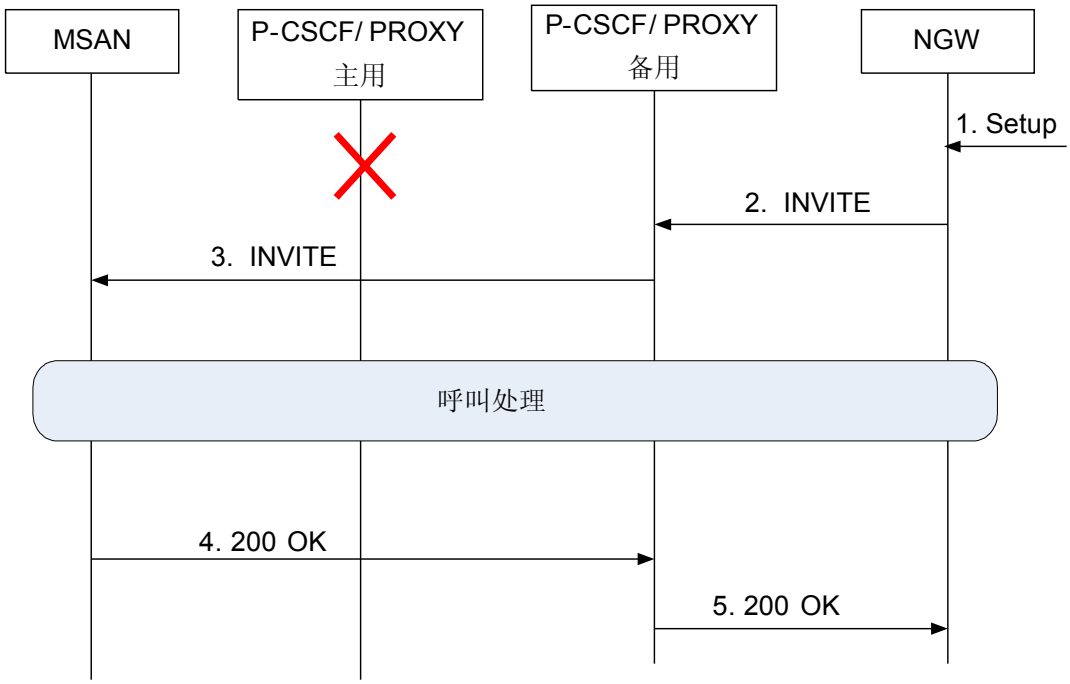


流程如下：

1. Setup：NGW 收到 PSTN 网络的业务请求。
2. INVITE：主备用 P-CSCF/PROXY 都正常，NGW 向主用 P-CSCF/PROXY 发送初始业务请求。并在主用 P-CSCF/PROXY 上建呼叫。
3. INVITE：主用 P-CSCF/PROXY 将 INVITE 转发给被叫侧 MSAN.
4. 200 OK：被叫 MSAN 应答呼叫，发送 200 OK 响应到主用 P-CSCF/PROXY。
5. 200 OK：主用 P-CSCF/PROXY 将 200 OK 响应发返回给被叫 NGW，建立起通话。

主用 P-CSCF/PROXY 故障，被叫业务流程如图 32-8 所示。

图 32-8 主用 P-CSCF/PROXY 故障场景下被叫业务流程图



流程如下：

1. Setup：NGW 收到 PSTN 侧发起的业务请求。
2. INVITE：主用 P-CSCF/PROXY 故障，备用 P-CSCF/PROXY 正常，MSAN 向备用 P-CSCF/PROXY 发送初始业务请求。并在备用 AS2 上建立呼叫。
3. INVITE：备用 P-CSCF/PROXY 将 INVITE 转发给被叫侧 MSAN.
4. 200 OK：被叫 MSAN 应答呼叫，发送 200 OK 响应到备用 P-CSCF/PROXY。
5. 200 OK：备用 P-CSCF/PROXY 将 200 OK 响应发返回给主叫 NGW，建立起通话。

32.5 原理描述(SCTP)

介绍该特性的实现原理。

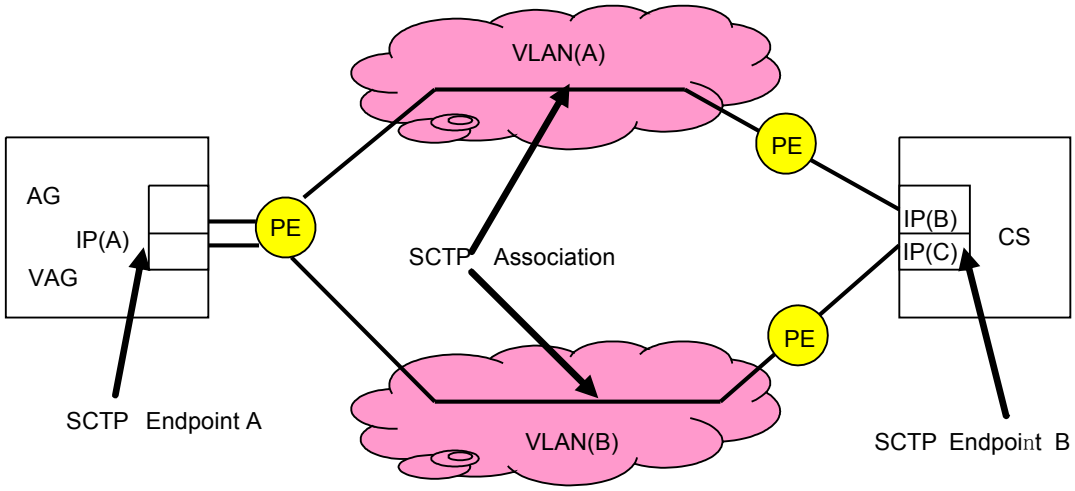
SCTP 兼容性

SCTP 多归属的实现原理基于 RFC2960 标准。 RFC2960 描述了 SCTP，同时也描述了 SCTP 多归属。

SCTP 非平衡双归属网络组网结构

SCTP 非平衡双归属属于 SCTP 多归属的一种应用方式，目前 UA5000 只支持 SCTP 非平衡双归属，即在一个 SCTP 端点 A 可以有两个目的地址偶联到另外一个 SCTP 端点 B，SCTP 端点 B 只有一个目的地址偶联到 SCTP 端点 A。SCTP 非平衡双归属组网图如图 32-9 所示。

图 32-9 SCTP 非平衡双归属组网图



说明

- AG/VAG 为接入网关/虚拟接入网关。
- CS 为呼叫服务器。
- IP（A）为 SCTP 端点 A 的 IP 地址。
- IP（B）/IP（C）为 SCTP 端点 B 的 IP 地址。
- 一般情况下给不同的 IP 地址配置不同的 VLAN，不同的 IP 地址配置相同的 VLAN 也是可以的。
- PE 为分组交换设备，一般指交换机或者路由器。

33 自交换

关于本章

介绍自交换特性的定义、目的、规格、原理以及参考的术语、缩略语和相关协议标准。

33.1 介绍
介绍该特性的定义、目的、规格和约束条件。

33.2 可获得性
介绍该特性需要的硬件支持和 License 支持。

33.3 原理描述
介绍该特性的实现原理。

33.1 介绍

介绍该特性的定义、目的、规格和约束条件。

定义

自交换是指对于 AG 内部的通话，AG 自身控制通话的接续，而无需 MGC（或 IMS）的控制，特别适用于当 AG 和 MGC（或 IMS）之间的通信中断时，AG 内部的电话仍然可以相互正常拨打。

目的

在 AG 和 MGC（或 IMS）之间失去联系时，AG 内部的电话可以相互拨打。

规格

在基于 H.248 协议或 SIP 协议上行时，UA5000 支持自交换功能，包括内部电话呼叫和紧急呼叫。

约束

- 仅支持长号和来电显示，不包括 Centrex 群、短号信息、用户呼出/呼入权限、各种新业务等。
- 只能拨打同一个设备下的用户。
- 只针对 VoIP 用户。

术语

表 33-1 自交换特性术语表

术语	解释
软交换	电路交换网向分组网演进的核心设备，也是下一代电信网络的重要设备之一。 独立于底层承载协议，主要完成呼叫控制、媒体网关接入控制、资源分配、协议处理、路由、认证、计费等主要功能，并可以向用户提供现有电路交换机所能提供的所有业务以及多样化的第三方业务。

缩略语

表 33-2 自交换特性缩略语表

缩略语	英文全称	中文全称
AG	Access Gateway	接入网关
IMS	IP multimedia subsystem	IP 多媒体子系统

缩略语	英文全称	中文全称
MG	Media Gateway	媒体网关
MGC	Media Gateway Controller	媒体网关控制器

33.2 可获得性

介绍该特性需要的硬件支持和 License 支持。

硬件支持

无需额外硬件支持。

License 支持

H.248 的自交换特性受 License 控制。

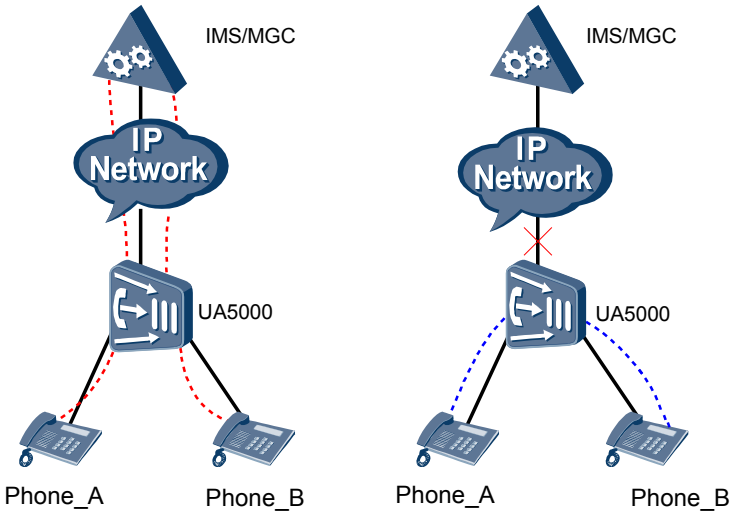
33.3 原理描述

介绍该特性的实现原理。

用户摘机后，网关（即 UA5000）判断与 MGC（或 IMS）之间的接口是否中断，如果接口不正常且设备允许自交换，则由 UA5000 控制呼叫流程。如果不允许自交换，则用户将听忙音（因为接口故障，而且不允许自交换）。

自交换原理图如图 33-1 所示。

图 33-1 自交换原理图



自交换的处理流程如下所示：

- 主叫摘机处理步骤
  1. 用户摘机。
  2. 设备自行给用户话机送拨号音。
  3. 用户拨号码。
  4. 设备分析用户所拨的号码。
     - 在 H.248 协议下，如果所拨号码与 UA5000 上配置的内部数图匹配，直接定位到被叫，否则给主叫放忙音。
     - 在 SIP 协议下，如果所拨号码与 UA5000 上配置的普通数图匹配，直接定位到被叫，否则给主叫放忙音。
  5. 设备给被叫用户送振铃信号和主叫号码。
  6. 给主叫送回铃音。
- 被叫摘机处理步骤
  1. 被叫摘机。
  2. 设备停主叫回铃音。
  3. 双方开始通话。
- 挂机处理步骤
  1. 通话任意一方挂机。
  2. 设备给通话另外一方送忙音。
  3. 另外一方挂机。

34 过载控制

关于本章

介绍过载控制特性的定义、目的、规格、原理以及参考的术语、缩略语和相关协议标准。

34.1 MG 过载
介绍 MG 过载控制的基本特性和实现原理。

34.2 上行带宽过载
介绍上行带宽过载控制的基本特性和实现原理。

34.3 MGC 过载
介绍 MGC 过载控制的基本特性和实现原理。

34.1 MG 过载

介绍 MG 过载控制的基本特性和实现原理。

34.1.1 介绍

介绍该特性的定义、目的、规格等。

定义

MG 过载控制是指当 MG 有大量任务处理时，会导致 CPU 使用率上升，甚至达到极限，此时 MG 没有办法保证正常呼叫。为了解决此问题，UA5000 提供 MG 的 CPU 过载限呼控制，通过查询 CPU 占有率来处理控制流量。

说明

过载控制是指在某些异常或极限可能导致呼叫接续能力下降或接续时间延迟增大时，UA5000 根据优先级拒绝部分优先级低的呼叫，保证设备依然能够正常运行的方法。

目的

为了最大可能地保证用户满意度，保证设备依然能够正常运行，并尽可能接近于其最大处理呼叫能力的用户接通率和正常的呼叫接续延长时间。

规格

- UA5000 过载控制分为两个等级：
  - 限制级过载
  - 阻塞级过载
- 限制级过载对应的最小 CPU 占用率可配置为（单位%）：1 ～ 99。

术语

无。

缩略语

表 34-1 过载控制特性缩略语表

缩略语	英文全称	中文全称
MG	Media Gateway	媒体网关

34.1.2 可获得性

介绍该特性需要的硬件支持，包括单板和终端。

无需额外硬件支持。

34.1.3 原理描述

介绍该特性的实现原理。

用户作为主叫

UA5000 根据端口优先级和呼叫优先级作为过载控制的评判标准。两个控制级别实现的控制功能如下：

1. 限制级过载：只允许优先端口、优先级会话、紧急呼叫通过。
2. 阻塞级过载：拒绝所有呼叫。

用户作为被叫

用户作为被叫的过载控制处理流程与用户作为主叫侧的处理流程大致相同，区别在于当对端呼叫进入到 MG 后，UA5000 仅根据呼叫的优先级作为过载控制的评判标准。

PSTN 用户摘机

PSTN 用户摘机的过载控制处理流程与用户作为被叫侧的处理流程相同。

34.1.4 参考信息

介绍该特性相关的参考信息。

本特性的参考资料清单如下：

- ITU-T.H.248.11 Infrastructure of audiovisual services – Communication procedures

34.2 上行带宽过载

介绍上行带宽过载控制的基本特性和实现原理。

34.2.1 介绍

介绍该特性的定义、目的、规格。

定义

上行带宽过载控制是 MG 接入网端的带宽流量达到或超过极限范围，对业务造成影响时，在 MG 侧通过带宽流量对呼叫进行限制，通过计算系统当前呼叫占用的带宽，来控制 MG 的呼叫流量。

目的

为了最大可能的保证呼叫用户的满意度，保证正常的呼叫语音质量。

规格

- 最大上行带宽取值范围（单位:100kbit/s）：2 ～ 1000。
- 紧急呼叫预留带宽取值范围（单位:100kbit/s）：1 ～ 999。

34.2.2 可获得性

介绍该特性需要的硬件支持，包括单板和终端。

无需额外硬件支持。

34.2.3 原理描述

介绍该特性的实现原理。

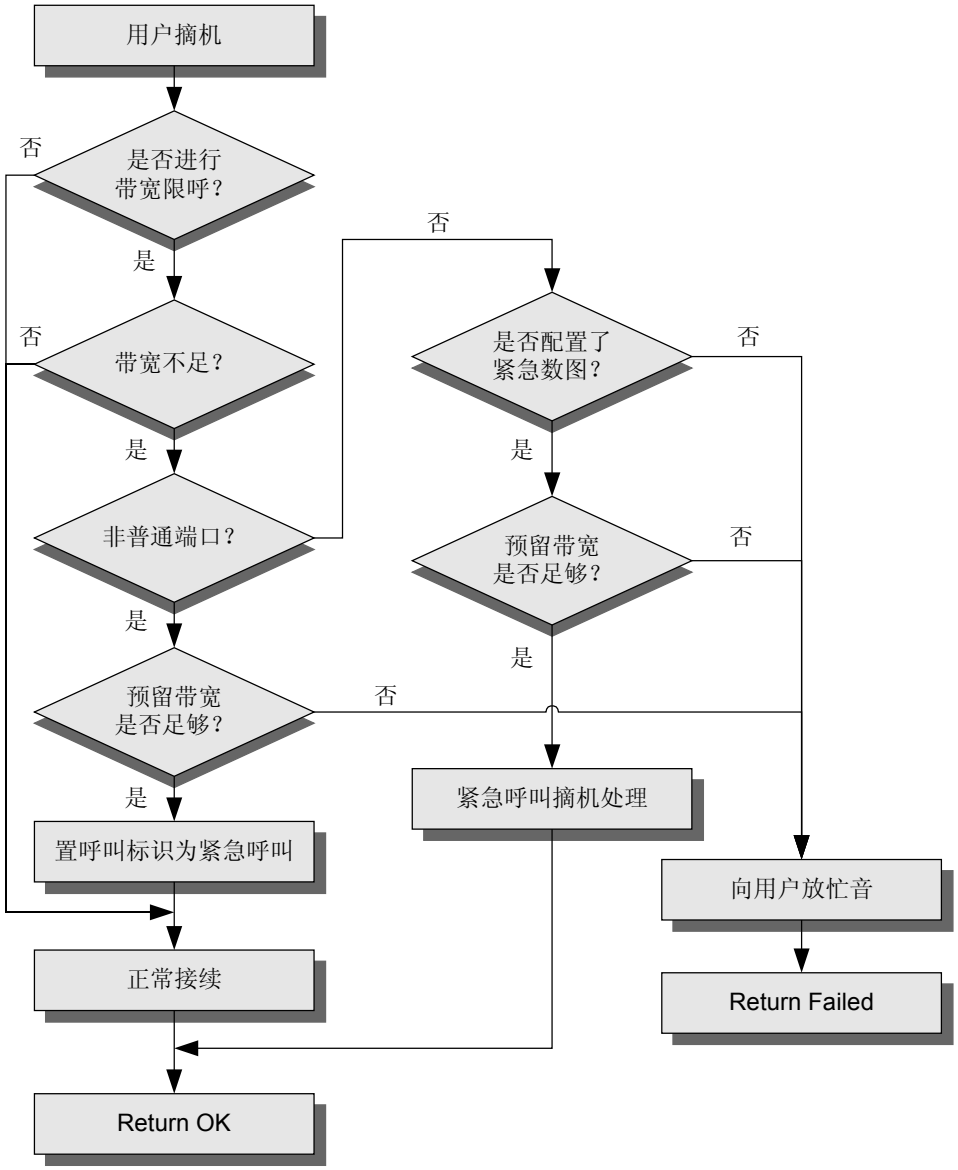
MG 通过上行带宽进行呼叫限制时，把呼叫分为两种情况：

- 普通端口用户普通呼叫。
- 非普通端口用户呼叫或普通端口用户紧急呼叫。

MG 支持上行带宽限呼时，会预留一部分带宽给第二类用户的呼叫，当呼叫带宽到达限制级别时，MG 会拒绝第一类用户的呼叫，允许第二类用户呼叫。

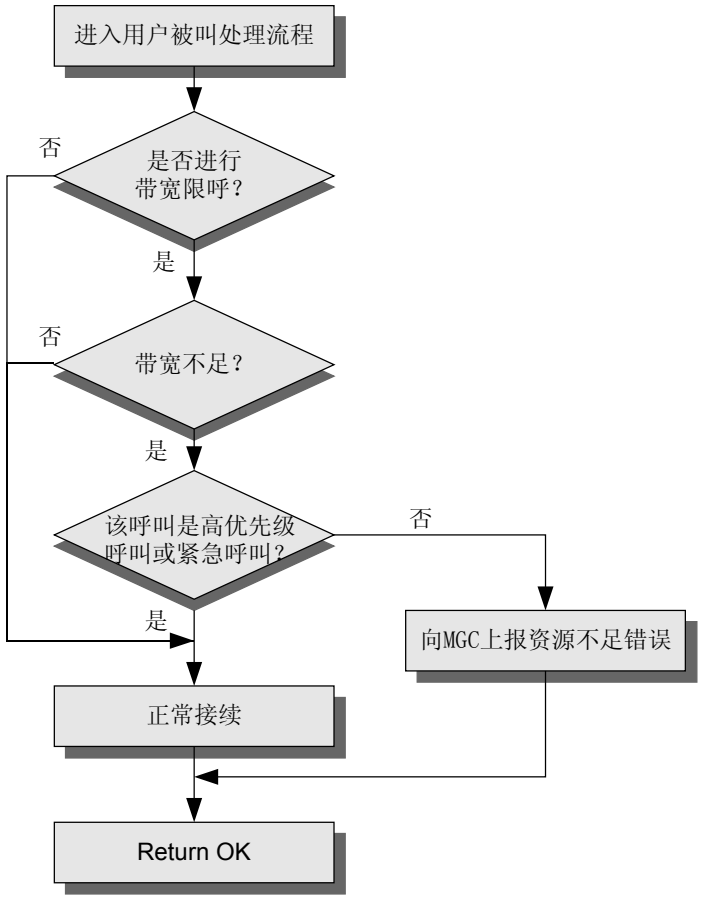
上行带宽过载控制情况下，用户摘机处理流程如图 34-1 所示。

图 34-1 上行带宽过载时的用户摘机处理流程



上行带宽过载控制情况下，被叫用户处理流程如图 34-2 所示。

图 34-2 上行带宽过载时的被叫用户处理流程



34.3 MGC 过载

介绍 MGC 过载控制的基本特性和实现原理。

34.3.1 介绍

介绍该特性的定义、目的。

定义

MGC 过载是指在某一时刻各地区呼叫量瞬间增大，或在某些异常情况下导致 MGC 自身处理负荷过重而产生过载，甚至影响正常呼叫。

目的

防止 MGC 过载以及在 MGC 发生过载时，网关（即 UA5000）配合 MGC 完成对自身呼叫量的限制和过载处理。

34.3.2 可获得性

介绍该特性需要的硬件支持，包括单板和终端。

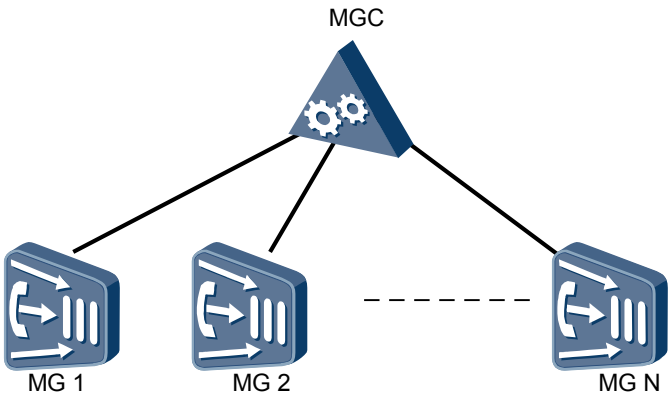
无需特殊硬件支持。

34.3.3 原理描述

介绍该特性的实现原理。

MGC 过载控制原理如图 34-3 所示。

图 34-3 MGC 过载控制原理图



MGC 通过信令控制每一个 MG（即 UA5000，以下统称 MG），每个 MG 收到呼叫都要上报给 MGC 来进行处理。此时如果每个 MG 都出现一个很小的呼叫量增加，对 MGC 来说就是一个很大呼叫量的增加，能引起 MGC 过载。

MGC 要防止自己进入过载状态，需要 MG 配合进行呼叫量的限制；MG 通过支持 MGC 的 etsi_nr 包来实现配合 MGC 对 MG 的呼叫量限制。

MG 支持 MGC 对用户呼叫进行限制时，会根据用户不同的优先级别来区别处理，在 UA5000 中将用户分为 3 个级别来区别对待（CAT3：普通用户；CAT2：次高级别用户；CAT1：最高级别用户）。

在 MG 启动 MGC 过载控制后，收到用户摘机的消息，UA5000 会根据用户的优先级别、MGC 下发的呼叫通过率，使用漏桶算法来判断是否允许当前呼叫。MG 会记录漏桶相关统计信息。

35 2833 加密

关于本章

介绍 2833 加密特性的定义、目的、规格、原理以及参考的术语、缩略语和相关协议标准。

35.1 介绍
介绍该特性的定义、目的、规格和约束条件。

35.2 可获得性
介绍该特性需要的硬件支持和 License 支持。

35.3 原理描述
介绍该特性的实现原理。

35.4 参考信息
介绍该特性相关的参考信息。

35.1 介绍

介绍该特性的定义、目的、规格和约束条件。

定义

2833 加密是指对遵守 RFC 2833 协议、使用 RTP 包独立负载格式来传送的双音多频数字信号进行加密，并对加密密钥进行加密，以保障信息的安全。

目的

通过加密语音流中的双音多频（Dual-Tone Multi-frequency，DTMF）码和密钥，对在 IP 网络中传送的卡号业务进行加密，保障信息的安全。

规格

- 只能对语音流中的 DTMF 码和密钥进行加密，不对媒体流和信令进行加密。
- 2833 加密和密钥加密均采用 HNC1 算法。
- 每次呼叫中的 DTMF 码是否加密由软交换指定，网关不做配置。
- 每个 VAG 可以配置一个密钥。

术语

无。

缩略语

表 35-1 2833 加密特性缩略语表

缩略语	英文全称	中文全称
DTMF	Dual-Tone Multi-frequency	双音多频
RTP	Real-time Transport Protocol	实时传输协议
VAG	Virtual Access Gateway	虚拟网关

35.2 可获得性

介绍该特性需要的硬件支持和 License 支持。

硬件支持

- 需要软交换指定对本次呼叫中的 DTMF 码进行加密。
- 网关和软交换的加密密钥必须一致。
- 对方网关必须也支持 2833 加密。

License 支持

2833 加密特性受 License 控制。

35.3 原理描述

介绍该特性的实现原理。

RFC 2833 技术

RFC 2833 描述了在 RTP 数据包中传送双音多频信号、其它电话信号音和电话事件的方法。

当 DTMF 信号在 NGN 网络中以带外方式传送时，根据 RFC 2833 的规定，网关处理 DTMF 数字信号和事件的方式有两种：

- 网关可以简单测量声音波段信号的频率成分并将这些信息传送到 RTP 接收端，RFC 2833 为此定义用于电话话音的 RTP 负载格式，相关的 MIME 类型为 audio/tone。
- 网关可以识别电话音并将它们译为名称，如振铃或忙音。接收端即产生电话音信号或其它相应的信号描述，RFC 2833 为此定义用于命名电话事件的 RTP 负载格式，相关的 MIME 类型为 audio/event。

UA5000 作为媒体网关支持第二种方式下对于命名电话事件负载格式的 RFC 2833 报文进行加密。在该方式下，使用命名事件作为音频流的冗余编码，信号源可以同时发送事件和已编码的音频数据包，或者在事件音活动时阻塞发出的音频，只发送作为主编码和冗余编码的命名事件。

加密密钥在 H.248 协议的 SDP 中加密传输，每次呼叫建立都动态刷新。

UA5000 RFC 2833 报文加密方案

UA5000 支持对于命名电话事件负载格式的 RFC 2833 报文进行加密。

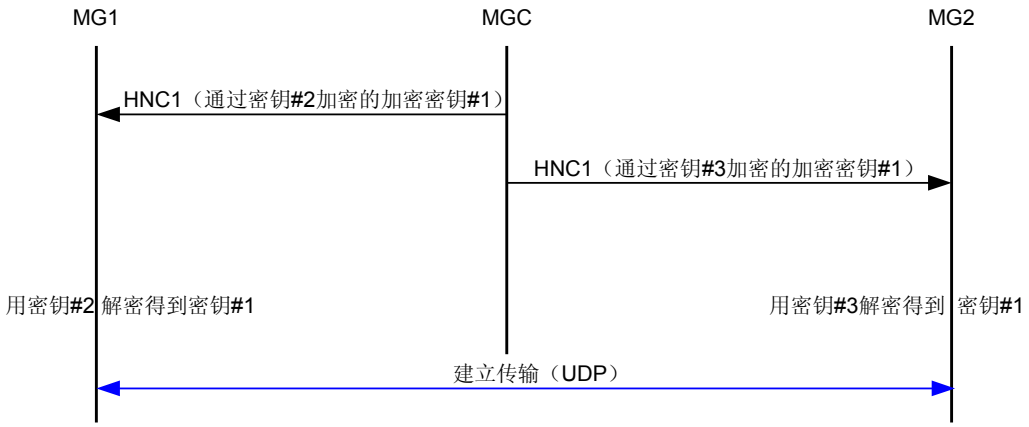
这种加密机制主要为电话银行等卡号加密业务设计，使用 HNC1（Huawei NGN Cipher Version1）加密算法对语音流中的 DTMF 码和加密密钥进行加密，不对音频流和呼叫信令进行加密；考虑到 DTMF 音频流泄密的可能，UA5000 根据 RFC 2833，只发送 DTMF 码对应事件，阻塞发出的音频。

本方案的特点如下：

- 采用带外方式传送 DTMF 信号，因此适配多种语音编码方式，支持如 G.723.1 或 G.729 等低比特率编解码器。
- 软件实现 DTMF 信号的加密，无需使用专用的 DSP 芯片，节约部署成本。
- 采用华为公司专利算法加密采用 HNC1（Huawei NGN Cipher Version1）算法，支持 128/256 位密钥，加密过程需要与 Huawei 软交换产品 Soft3000 配合完成；目前适用于 UA5000 与 Huawei 软交换产品 Soft3000 共同组网的应用场景。
- 采用动态密钥的机制保证密钥的安全：加密密钥由软交换控制，在每次呼叫时动态刷新，并且在 H.248 协议的 SDP 中加密传输。

2833 加密业务流程如图 35-1 所示。

图 35-1 2833 加密业务流程



1. 网关 1 与软交换上配置相同的加密密钥#2，网关 2 与软交换上配置相同的加密密钥#3。每个 VAG 都可以配置一个密钥，与在软交换上配置的对应媒体网关的 2833 密钥相同。
2. 在 AG 上将传输模式配成 2833 加密传输模式后，可以对语音中的 DTMF 码进行 2833 加密。
3. 网关 1 与网关 2 要进行 2833 加密传输时，软交换在分配上下文的命令中分别对网关 1 和网关 2 下发 HNC1(通过密钥#2 加密的加密密钥#1)和 HNC1(通过密钥#3 加密的加密密钥#1)（密钥 1 是软交换动态分配的，每次建链都刷新）。
4. 网关 1、网关 2 需要分别通过自己网关配置的密钥#2 和密钥#3 对 H.248 协议消息中下发的密钥#1 进行解密，得到明文密钥是真正对语音中的 DTMF 码进行加密的密钥。
5. 得到密钥之后，对语音中的 DTMF 码进行编码的时候，都使用密钥进行加密后发送。

35.4 参考信息

介绍该特性相关的参考信息。

本特性的参考资料清单如下：

- International Telecommunication Union, RFC 2833 – “RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals”
- International Telecommunication Union, RFC 2198 – “RTP Payload for Redundant Audio Data”

36 主动测试和被动测试

关于本章

介绍主动测试和被动测试特性的定义、目的、规格、原理以及参考的术语、缩略语和相关协议标准。

36.1 主动测试
主动测试即侵入式测试，指需要将测试业务流注入网络，并通过对测试业务流的分析来获得测试数据。

36.2 被动测试
介绍被动测试的基本特性和实现原理。

36.1 主动测试

主动测试即侵入式测试，指需要将测试业务流注入网络，并通过对测试业务流的分析来获得测试数据。

36.1.1 介绍

介绍该特性的定义、目的、规格和约束条件。

定义

QoS 主动测试是指网管向软件换设备下发执行测试的指令后，软交换设备下发测试命令给被测网关，完成被测网关（即 UA5000，本章统称为网关或被测网关）的呼叫连接，使被测网关通过搭建的测试通道发送测试业务流。被测网关从测试业务流中提取相关语音质量 QoS 信息，定时将测试结果上报给软交换，再通过软交换设备整理上报给网管。

主动测试是一种侵入网络的测试，需要将测试业务流注入网络，并通过对测试业务流的分析来获得测试数据，对以 IP 网络为核心承载网络的 QoS 状况进行测试。

目的

主动测试可以方便运营商和维护人员对网络进行维护和管理。

- 业务启动前进行全网测试

  在新的 NGN 网关设备已经完成网络部署，并成功上电后，可以运行一组测试，模拟真实呼叫，并观察测试结果，评估承载网络状况。
- 业务开通前进行大话务量测试

  可以在业务未正式开通前运行，进行主动测试，模拟大话务情况，通过反馈回的测试结果来评估设备和承载网络的处理能力和质量状况。
- 业务开通中进行例行测试

  可以在业务开通后，定制一套测试计划，进行例行测试，用来随时监视承载网络健康状况。
- 出现问题时辅助定位问题

  出现质量问题后，可以运行主动测试来协助定位问题，判断是否是承载网络的问题。

规格

- 同时在线的最大测试路数为 10 路，即 20 个用户。
- 测试用呼叫和正常呼叫的总数不能超过 DSP 的最大通道数。

约束

- 因为同时在线的最大呼叫数固定，所以过多的测试呼叫会对正常的业务产生影响，可能造成正常呼叫建立请求被拒绝。
- 主动测试需要网关和软交换配合来完成。

术语

无。

缩略语

表 36-1 主动测试特性缩略语表

缩略语	英文全称	中文全称
MG	Media Gateway	媒体网关
RTP	Real-time Transport Protocol	实时传输协议

36.1.2 可获得性

介绍该特性需要的硬件支持，包括单板和终端。

无需额外硬件支持。

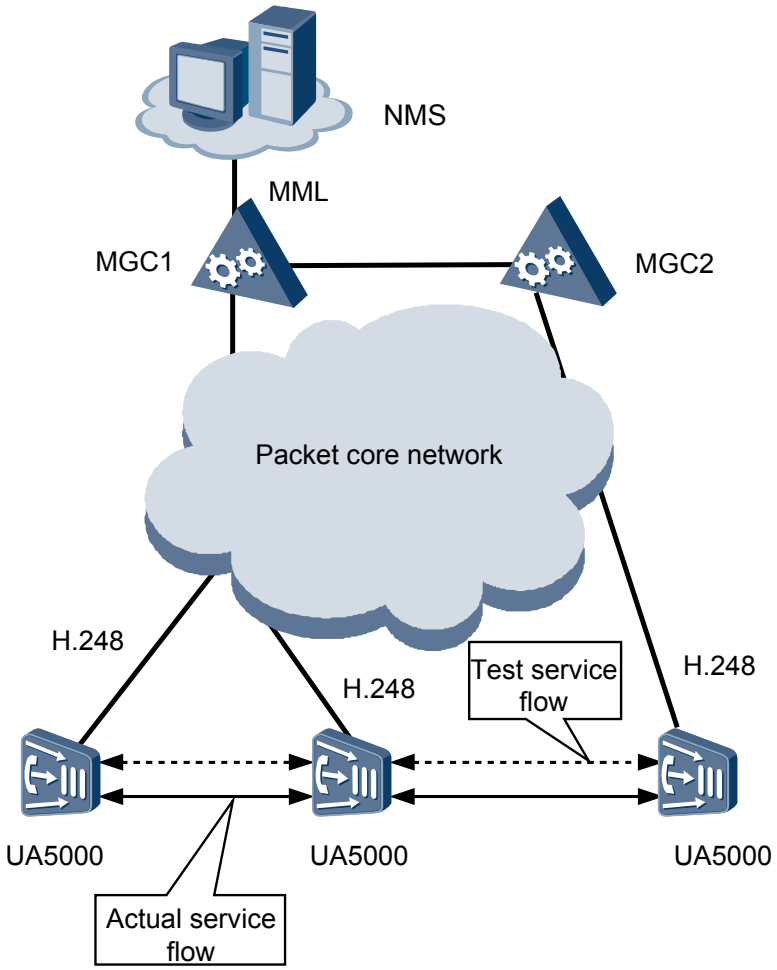
36.1.3 原理描述

介绍该特性的实现原理。

主动测试在网关中内置测试模块，与软交换配合仿真语音呼叫，发送测试业务流。测试业务流和实际业务流在 IP 承载网中的路由路径完全相同，真实反映实际业务流流经的网络状况。通过对测试业务流的分析，可以测试出实际运行时 IP 承载网络的质量效果。

主动测试的架构如图 36-1 所示。

图 36-1 主动测试架构图



主动测试的基本流程如下：

1. 网管下发测试命令，指定软交换、测试实例、测试时长、测试通道数。
2. 软交换收到测试命令后，主动发起呼叫，并完成测试实例中被测网关的呼叫连接。
3. 被测网关在搭建的测试通道互发测试语音样件。（该语音样件驻留在网关内部，为G.711A-20ms、G.711μ-20ms、G.723.1-30ms、G.729A-20ms 四种格式。）
4. 被测网关收到测试业务流，从 RTP 会话中提取相关语音质量 QoS 参数，如时延、丢包、抖动等，定时将测试结果上报到软交换；会话结束时也会把总的统计结果上报软交换。
5. 软交换收到测试报告，统计处理后上报网管。
6. 网管接收到 QoS 信息，再以图表的形式显示测试结果。

QoS 主动测试的测试结果包括以下参数指标：

- 统计信息有效性
- 呼叫发送的 RTP 包数
- 呼叫发送的 RTP 包字节数
- 呼叫接收的 RTP 包数

- 呼叫接收的 RTP 包字节数
- 呼叫丢包率(%)
- 呼叫时延抖动
- 呼叫环路时延
- 呼叫持续时间

36.2 被动测试

介绍被动测试的基本特性和实现原理。

36.2.1 介绍

介绍该特性的定义、目的、规格和约束条件。

定义

QoS 被动测试是指不侵入网络上的实际业务，只是对实际业务进行监测，通过对实际业务流的分析获得测试数据，对以 IP 网络为核心承载网络的 QoS 状况进行测试。

在 QoS 被动测试中，测试命令下发给网关（即 UA5000），由被测网关对 RTP/RTCP 进行性能统计。被测网关实时监控实际业务流，定时将统计到的语音质量 QoS 信息上报到网管。

目的

利用网关产品（即 UA5000）自身已有的 RTP/RTCP 性能统计功能，能够在不增加网络负担，不影响网络中已有业务的情况下，实现对实时业务的监控和告警，并定时将 QoS 统计消息报告给网管。

规格

最大测试任务数为 16。

约束

同时启动多个被动测试任务，对 CPU 的占用率会比较高。

术语

无。

缩略语

表 36-2 被动测试特性缩略语表

缩略语	英文全称	中文全称
MG	Media Gateway	媒体网关
RTP	Real-time Transport Protocol	实时传输协议

缩略语	英文全称	中文全称
RTCP	RTP Control Protocol	RTP 控制协议

36.2.2 可获得性

介绍该特性需要的硬件支持，包括单板和终端。

无需额外硬件支持。

36.2.3 原理描述

介绍该特性的实现原理。

被动测试的基本流程如下：

1. 网管下发测试命令，指定被测试的网关、本端 IP 地址（在多端口时需要）、对端 IP 地址（可以是 NAT 或 SAN 的地址）、测试时长、定时上报周期。
2. 被测网关收到测试命令后，收集所有符合条件的 RTP 会话的 QoS 信息，如时延、丢包、抖动等，实时刷新储存上报信息的寄存器，在定时上报时刻到来时，通过测试端口上报到网管。
3. 网管接收到 QoS 信息，再以图表的形式显示测试结果。

QoS 信息包括以下项目：

- 接收 RTP 包总数（累计量）
- 发送 RTP 包总数（累计量）
- 接收 RTP 字节总数（累计量）
- 发送 RTP 字节总数（累计量）
- 接收 RTP 包丢失总数（累计量)
- 本端统计最大丢包率（定时周期内）及对应通话的端口
- 本端统计最小丢包率（定时周期内）及对应通话的端口
- 本端统计时延抖动最大值（定时周期内）及对应通话的端口
- 本端统计时延抖动最小值（定时周期内）及对应通话的端口
- 本端统计最大环路时延（定时周期内）及对应通话的端口
- 本端统计最小环路时延（定时周期内）及对应通话的端口

定时上报周期如果设为 0，表示该统计任务仅仅执行一次，上报一次结果后即结束。定时上报周期最小为 10 秒，最大为 60 秒。

在测试过程中，不允许网管下发命令修改任务的参数。如果需要修改任务参数，网管需要主动结束原来的任务，然后重新启动一个新的任务，设置为新的参数。

37 SELT 测试

关于本章

介绍 SELT 测试的基本特性和实现原理。

37.1 介绍
介绍该特性的定义、目的、规格和约束条件。

37.2 可获得性
介绍该特性需要的硬件支持和 License 支持。

37.3 原理描述
介绍该特性的实现原理。

37.4 参考信息
介绍该特性相关的参考信息。

37.1 介绍

介绍该特性的定义、目的、规格和约束条件。

定义

SELT（Single Ended Loop Test）测试是从线路的一端对 DSL 环路进行的一种自动测试方式，为操作者们提供一种在日常操作中的评估环路的有效方法。

目的

SELT 测试是在启用线路前或后维护时，初步测试出线路的一些信息，包括线路长度，线路可达速率，线路的噪声等一些信息，来了解此线路将来的使用能力。

规格

ADSL2+和 VDSL2 端口支持 SELT 测试。

37.2 可获得性

介绍该特性需要的硬件支持和 License 支持。

硬件支持

无需特殊硬件支持。

License 支持

ADSL SELT 功能和 VDSL SELT 功能受 License 控制。

版本支持

UA5000 V100R019C01 版本开始，ADSL SELT 支持 ITU-T G.996.2 标准中的 UER 和 QLN 测试。

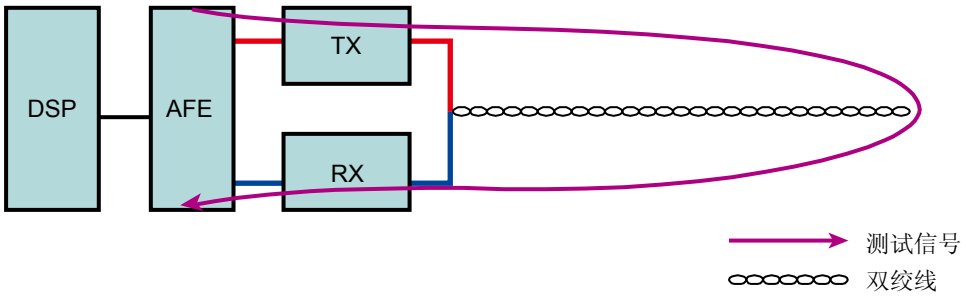
UA5000 V100R019C02 版本开始，VDSL SELT 支持 ITU-T G.996.2 标准中的 UER 和 QLN 测试。

37.3 原理描述

介绍该特性的实现原理。

SELT 测试原理如图 37-1 所示。

图 37-1 SELT 测试原理图



SELT 测试是通过 AFE 发射测试信号，测试信号经过阻抗不连续的地方就会产生反射，AFE 接收反射信号经过分析得出线路状况。

SELT 测试不需要 CPE 配合进行测试，但是因为 SELT 测试信号经过两倍的线路长度，因此测试距离将受到线路信号衰减的影响。

SELT 测试使用的测试方法一般包括：

- TDR（Time Domain Reflectometry）时域反射法，测量发射信号和反射信号的时间和电压的关系。
- FDR（Frequency Domain Reflectometry）频域反射法，测量发射信号和反射信号的频率和电压的关系。

37.4 参考信息

介绍该特性相关的参考信息。

本特性的参考资料清单如下：

- ITU-T G.996.2 Single-ended line testing for digital subscriber lines (DSL)

38 BFD

关于本章

介绍 BFD 特性的定义、目的、规格、原理以及参考的术语、缩略语和相关协议标准。

38.1 介绍
介绍该特性的定义、目的、规格和约束条件。

38.2 可获得性
介绍该特性需要的硬件支持和 License 支持。

38.3 原理描述（IPM）
介绍该特性的实现原理。

38.4 原理描述(PVM)
介绍该特性的实现原理。

38.1 介绍

介绍该特性的定义、目的、规格和约束条件。

定义

BFD（Bidirectional Forwarding Detection）是互联网工程任务组（IETF）的标准草案，通过在两个节点间相互定期快速发送 BFD 控制包（一个特定格式的 UDP 包），来检测链路或系统的流量转发能力。

BFD 在接收端检测，如果超出检测周期没有收到 BFD 包则判定此链路为断路。

目的

在传统路由网络中，路由层面的服务中断只能依靠动态路由协议中的 HELLO 机制探测，因为这些机制设计得比较早，且当时的网络环境多为低速网络，所以 timer 一般都设置在秒级。

在现在的高速网络中，网络延迟和设备延迟已经大大降低，完全可以采用更短的探测周期，BFD 正是可以帮助完成该任务的一个功能。BFD 可在极短时间内检测到转发路径中的错误，并触发切换到备用路由、接口甚至是整个网络。

BFD 可用于监控以太网，MPLS 标签交换路径(LSP)，通用路由压缩(GRE)， IPSec 隧道以及任何其他传输类型。因此 BFD 功能可提升 IP 应用（如实时话音流量）的可靠性，为服务供应商的网络稳定性提供支持。

由于 BFD 实现故障检测简单、单一，使 BFD 能够专注于转发故障的快速检测，帮助网络以良好的 QoS 实现语音、视频及其它点播业务的传输，为客户提供所需的高可靠性、高适用性 VoIP 及其它实时业务。

规格

IPMB 支持的规格如下：

- IPMB 最多可配置 32 条 BFD 会话。
- 每条 BFD 会话可配置的发包时间间隔为 250~300000 ms。
- 每条 BFD 会话可配置的收包时间间隔为 250~300000 ms。
- 每条 BFD 会话可配置的检测倍数为 3~50。
- 到同一目的地的静态路由最多可配置 6 条。
- 和 BFD 进行绑定的静态路由最多为 128 条。

PVM 支持的规格如下：

- PVM 最多可配置 2 条 BFD 会话。
- 每条 BFD 会话可配置的发包时间间隔为 10~5100 ms。
- 每条 BFD 会话可配置的收包时间间隔为 10~5100 ms。
- 每条 BFD 会话可配置的检测倍数为 3~50。

约束

无。

术语

表 38-1 BFD 特性术语表

术语	解释
检测模式	BFD 协议中实现双向检测的机制，可分为两种：异步模式、查询模式。
异步模式	在异步模式下，系统之间相互周期性地发送 BFD 控制包，如果某个系统在检测时间内没有收到对端发来的 BFD 控制报文，就宣布会话为 Down。
查询模式	在查询模式下，假定每个系统都有一个独立的方法用来确认它连接到其他系统。这样一旦一个 BFD 会话建立起来以后，系统停止发送 BFD 控制报文，除非某个系统需要显式地验证连接性。在需要显式验证连接性的情况下，系统发送一个短系列的 BFD 控制包，如果在检测时间内没有收到返回的报文就宣布会话为 Down，如果收到对端的回应报文，协议再次保持沉默。

缩略语

表 38-2 BFD 特性缩略语表

缩略语	英文全称	中文全称
BFD	Bidirectional Forwarding Detection	双向转发检测
VoIP	Voice Over IP	IP 承载语音

38.2 可获得性

介绍该特性需要的硬件支持和 License 支持。

硬件支持

无需额外硬件支持。

License 支持

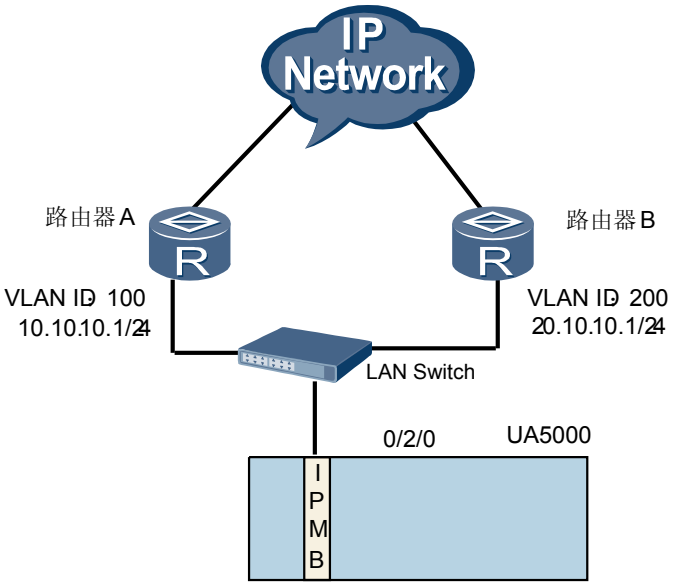
语音的 BFD 功能受 License 控制。

38.3 原理描述（IPM）

介绍该特性的实现原理。

BFD 实现原理如图 38-1 所示。

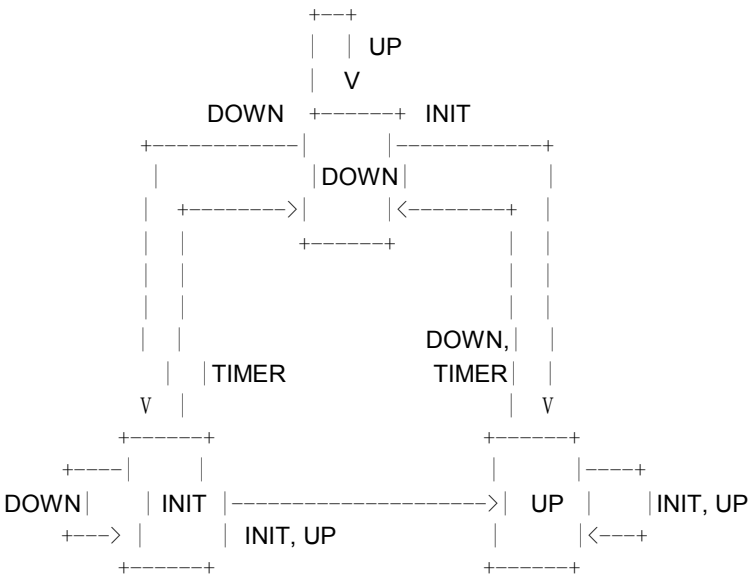
图 38-1 BFD 实现原理图



在“路由器 A”和“IPMB”之间配置一条 BFD 会话。会话建立过程是一个三次握手的过程，经过此过程后两端的会话变为 Up 状态，在此过程中同时协商好相应的参数，以后的状态变化就是根据缺陷的检测结果来进行，并做相应的处理。

会话的状态转换过程如图 38-2 所示。

图 38-2 会话状态转换图



BFD 工作过程如下：

1. 刚刚建立起来的 BFD 会话处于“DOWN”状态，本端和对端回相互发送 Your Discriminator 为 0 的 BFD 控制报文即“DOWN”报文。
2. 本端收到“DOWN”报文后，会向对端发送一个“INIT”报文。同样，对端在收到本端发送的“DOWN”报文后，也会向本端发送“INIT”报文。
3. 收到“INIT”后，根据报文所携带的配置参数和本端 BFD 会话的配置参数，计算本端的发包间隔、收包间隔、检测时间，然后本端会话状态转换为“UP”，并向对端发送本端“UP”的报文。对端处理过程和本端相同。
4. 在“UP”状态下，如果检测时间到，本端还没有收到对端的有效报文，则本端状态转变为“DOWN”状态，然后和对端开始新一轮的协商过程。

2 条以上的目的地相同的静态路由和 BFD 进行绑定后，就组成一个路由组。在路由组中只要有一条路由是的状态是 ACTIVE，则该路由组的状态为 ACTIVE，当该路由组中所有的路由都 DOWN 掉以后，该路由组才 DOWN 掉。

BFD 在和静态路由绑定后有两种工作模式：自动倒换模式、手动倒换模式。

假如目的地相同的 2 条和 BFD 绑定的静态路由为 R1(优先级高)、R2(优先级低)，最初数据包走的是 R1 路由。

- 自动倒换模式下：R1 路由 DOWN 掉以后，路由会切换到 R2 路由，如果 R1 路由重新“UP”起来。路由会自动切换到 R1。
- 手动倒换模式下：R1 路由 DOWN 掉以后，路由也会切换到 R2 路由，但如果 R1 路由重新“UP”起来。路由不会自动切换到 R1，要进行手动操作才可以将路由切换到 R1 上。

38.4 原理描述(PVM)

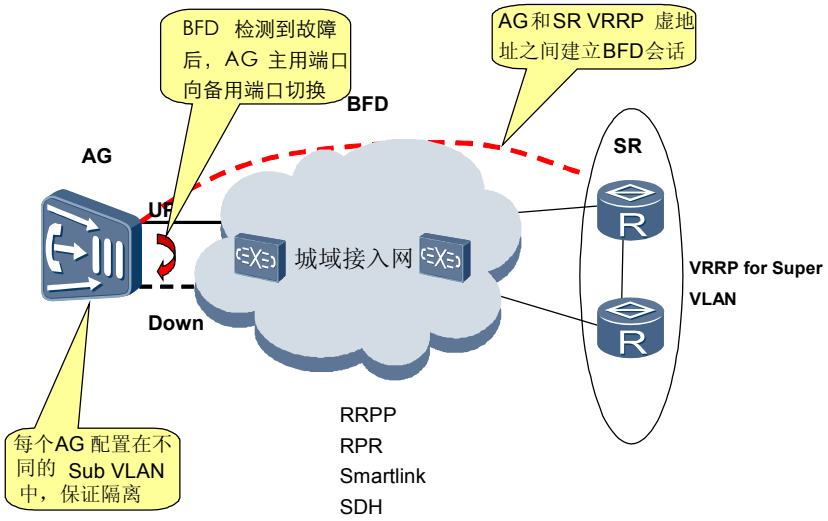
介绍该特性的实现原理。

BFD 的应用和组网，包括 3 种应用模型：

- 单链路组网模型
- 双链路 BFD 组网模型
- 双链路 LBM 组网模型

单链路 BFD 检测组网模型如图 38-3 所示。

图 38-3 单链路 BFD 检测组网模型图

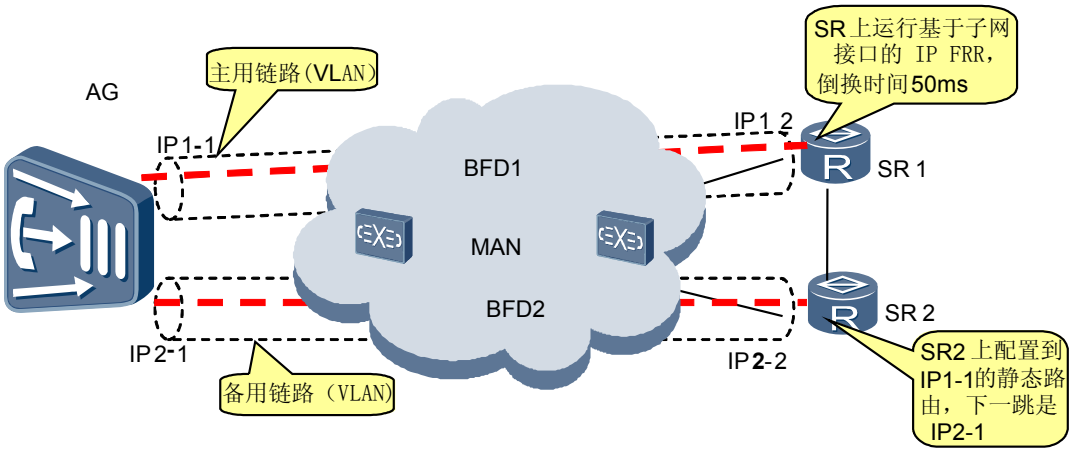


实现原理和特点：

- 在 AG 与 SR VRRP 虚地址之间建立 1 条 BFD 链路，链路启动 ECHO 功能，运行在主用上行口。
- 当检测链路故障时，进行上行网口切换，同时在切换后的上行口上重新建立 BFD 链路。
- BFD 检测解决了端口状态检测和 ARP 探测的缺陷，可以快速的检测主用接口的双向故障。
- 缺点是备用上行接口不能检测。

双链路 BFD 检测组网模型如图 38-4 所示。

图 38-4 双链路 BFD 检测组网模型图



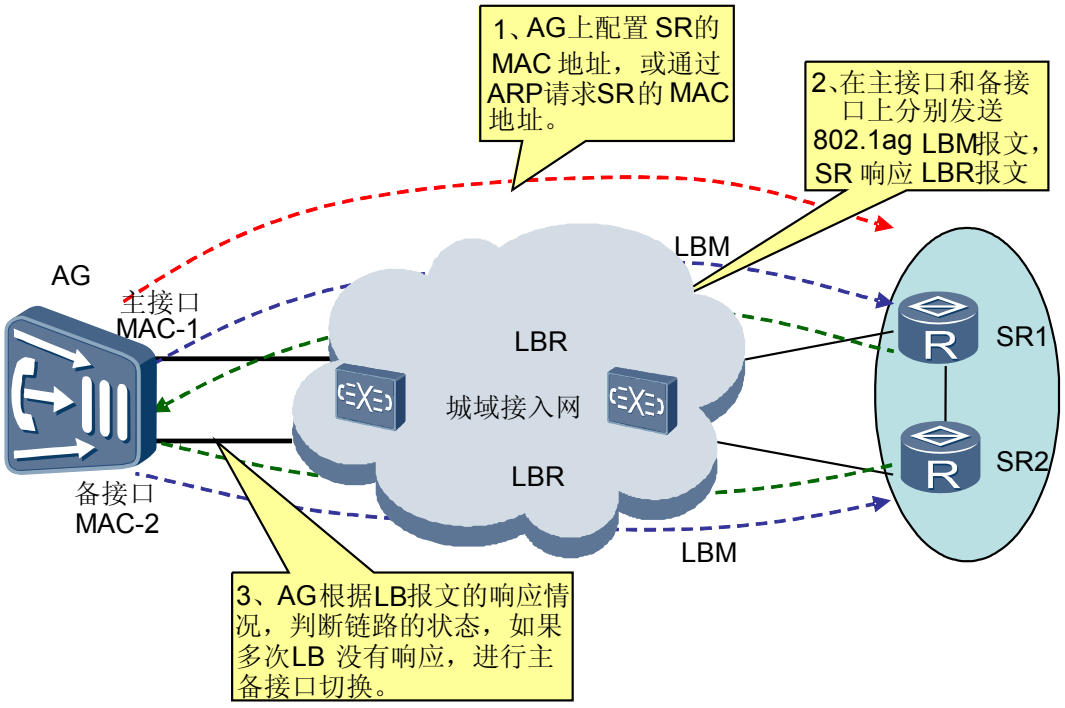
AG 配置两个 IP 地址，IP1-1 和 IP2-1，不同网段，分别对应网关 IP1-2 和 IP2-2，IP1-1 是主用接口，也是 AG 的业务 IP 地址；IP1-1 和网关 IP1-2 之间运行一个 BFD 会话 BFD1，IP2-1 和网关 IP2-2 之间运行一个 BFD 会话 BFD2；当 BFD1 故障时，AG 进行上行口切换，AG 内部业务数据经 IP2-1 接口向外转发数据。

实现原理和特点：

- SR 之间不需要启用 VRRP 协议。
- 2 条 BFD 链路使用标准的 BFD 协议，可以与支持标准 BFD 的设备对接。
- BFD 检测 AG 到 SR 的双向链路，保护能力依赖于 AG 和 SR，每个 AG 只需规划两条不同的链路，连接到不同的 SR，简化了接入承载网的可靠性设计。
- 使用 IP 地址比较多，每个 AG 需要两个 IP 地址，不同网段。加上网关的两个 IP 地址，部署一个 AG 需要 8 个地址和两个 VLAN。
- AG 和 SR 之间的消息包交换通过硬件实现，支持几十毫秒级的检测能力。

双链路 LBM 组网模型如图 38-5 所示。

图 38-5 双链路 LBM 组网模型图



实现原理和特点：

- 采用二层检测机制，不需增加 IP 地址，对网络规划没有影响。
- SR 之间启用 VRRP，虚地址为 AG 业务 IP 的路由。
- 2 条 LBM 的链路建立在 AG 的主备用接口和 SR 的实地址上。
- 检测报文为二层包，对承载网设备没有要求，使用的检测包为 802.1ag 的 LBM、LBR 包，处理机制相同。
- AG 和 SR 之间的消息包交换通过硬件实现，支持几十毫秒级的检测能力。
- 方案为私有方案，只能与华为的 NE40、NE80 对接。

39 Z 接口延伸

关于本章

介绍 Z 接口延伸特性的定义、目的、规格、原理以及参考的术语、缩略语和相关协议标准。

39.1 介绍
介绍该特性的定义、目的、规格和约束条件。

39.2 可获得性
介绍该特性需要的硬件支持，包括单板和终端。

39.3 原理描述
介绍该特性的实现原理。

39.1 介绍

介绍该特性的定义、目的、规格和约束条件。

定义

Z 接口延伸就是 POTS 用户信号的延伸，它通过对 POTS 用户信号进行模数转换，将数字信号传输到另一端，在接收端恢复为模拟信号。

通过 Z 接口的延伸，延长了双绞线的接入距离。

典型的 Z 接口延伸包含一个 Z 接口、数字传输系统和一个 POTS 端口。

目的

Z 接口延伸有以下几个目的：

- 可以满足有少量模拟电话需求的专网用户接入到本地交换机。
- 将一个本地交换机的模拟电话通过延伸的方式拉远到另一个地方，计费方式保持不变，用以节省长途话费。
- 接入远距离用户。
- 通过动态收敛提高线路的利用率。

规格

UA5000 中每块 CDI 单板支持 16 路 Z 接口。

约束

无。

术语

表 39-1 Z 接口特性术语表

术语	解释
Z 接口	Z 接口是接入网与交换机之间的模拟接口。
Z 接口延伸	Z 接口延伸就是 POTS 用户信号的延伸，它通过对 POTS 用户信号进行模数转换，将数字信号传输到另一端，在接收端恢复为模拟信号。

缩略语

无。

39.2 可获得性

介绍该特性需要的硬件支持，包括单板和终端。

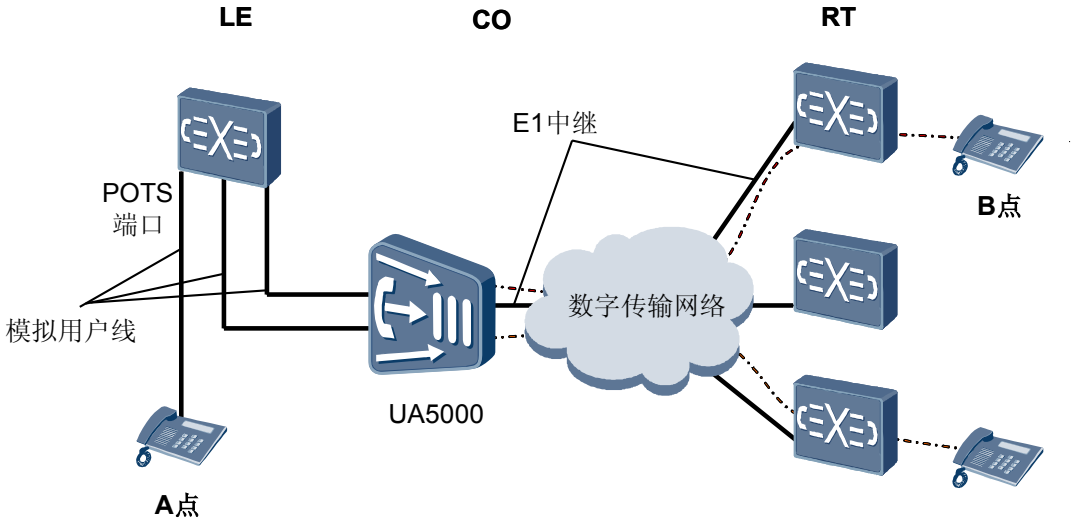
支持本特性的单板是 CDI 单板。

39.3 原理描述

介绍该特性的实现原理。

Z 接口延伸的原理如图 39-1 所示。

图 39-1 Z 接口延伸原理结构图



Z 接口延伸原理实现过程：Z 接口延伸通过模数转换将本地交换机的信号终结，并通过数字传输系统将数字信号无损的传送到另外一端的 POTS 接口上，经过数模转换将原有的信号恢复出来。图中 CO 到 RT 再到电话机的虚线是逻辑上的概念，表明从 CO 侧将 Z 接口延伸到 RT 侧，实际中并不存在。

经过 Z 接口延伸对于 B 点的用户，与 A 点的用户体验是完全一样的，包括拨打电话和接听电话。Z 接口和 B 点的 POTS 接口存在一一对应的关系，按照 1:1 进行配置。

Z 接口延伸中的 POTS 用户拨打电话流程如下：

- 被叫流程：CDI 单板检测到振铃后，通过相应的 Z 接口向 B 点的用户发送振铃命令，使 B 点用户振铃，在 B 点用户摘机后，整个话路连通，通话。
- 主叫流程：B 点用户摘机，CDI 单板向相应的 Z 接口下发摘机信号，并将本地交换机的拨号音送到 B 点用户，B 点用户拨号，CDI 单板将号码传送到本地交换机完成对外拨打电话的过程。

40 数据业务

关于本章

介绍数据业务特性的定义、目的、规格、原理以及参考的术语、缩略语和相关协议标准。

40.1 介绍
介绍该特性的定义、目的、规格和约束条件。

40.2 可获得性
介绍该特性需要的硬件支持，包括单板和终端。

40.3 原理描述
介绍 G.SHDSL 数据业务、DDU2 传输 64K 同步数据业务、SRX 子速率数据业务和 U 口透传数据业务的实现原理。

40.4 参考信息
介绍与该特性相关的参考信息。

40.1 介绍

介绍该特性的定义、目的、规格和约束条件。

定义

DDN 是利用数字信道传输数据信号的数据传输网。它的主要作用是向用户提供永久性和半永久性连接的数字数据传输信道，既可用于计算机之间的通信，也可用于传送数字化传真，数字话音，数字图像信号或其它数字化信号。

永久性连接的数字数据传输信道是指用户间建立固定连接，传输速率不变的独占带宽电路。半永久性连接的数字数据传输信道对用户来说是非交换性的，用户可提出申请，由网络管理人员对其提出的传输速率、传输数据的目的地和传输路由进行修改。

UA5000 主要完成 DDN 数据业务的透传，便于运营商构建 DDN 网路。目前 UA5000 有如下几种提供方式：

- 通过 G.SHDSL 端口提供 V.35/N*64k 数据业务
- 通过 DDU2 单板的 2 路同向 64K 接口提供同步 64K 数据业务
- 通过 MTA 方式提供 V.35/V.24 数据业务
- 通过 SRX 板提供 V.24 数据业务
- 支持 U 口透传数据业务

目的

通过半永久连接实现子速率和基本速率的专线互连。

规格

- SDLE 单板提供 8 路 G.SHDSL 接口和 8 路 E1 接口，其中 SHDSL 端口经过 Modem 变换后，可以提供 V.35（N×64kbit/s，3≤N≤32）或者 E1（2048kbit/s）接口。
- DSLD 单板提供 16 路 ISDN 端口，每个端口可以接 1 个 MTA。
- DSLD 单板提供 16 个 U 口。
- H301DDU2 板支持 2 路同向 64K 接口。
- DDU2 板与 A32 板槽位兼容。
- H301SRX 板与 A32 板槽位兼容。
- H301SRX 板是 HONET 接入网系统的子速率数据接口板，可提供五路同步或三路异步子速率数据端口。
- SRX 板各端口的速率从 2.4kbit/s、4.8kbit/s、9.6kbit/s、19.2kbit/s 到 48kbit/s 可变。
- 整个 SRX 板占用一个 64K 时隙。

约束

UA5000 不支持子速率交叉业务，传输业务的两个端口所在的物理位置必须相同（例如：本端如为 0 端口，对应对端必须也为 0 端口）。

术语

表 40-1 数据业务特性术语表

术语	解释
永久性连接	永久性连接的数字数据传输信道是指用户间建立固定连接，传输速率不变的独占带宽电路。
半永久性连接	通过业务顺序或者网络管理建立的连接，用户间不建立固定连接，由设备动态分配传输数据的时隙。

缩略语

表 40-2 数据业务特性缩略语表

缩略语	英文全称	中文全称
DDN	Digital Data Network	数字数据网
DDU	Digital Data Unit	数字单元
MTA	Multifunctional Terminal Adapter	多功能终端适配器
SCS	Sub-rate Concentrating Switch	子速率集中交叉
SRX	Sub Rate Multiplexer	子速率复用

40.2 可获得性

介绍该特性需要的硬件支持，包括单板和终端。

- 支持 G.SHDSL 数据业务的单板为 SDLE。
- 支持 MTA 数据业务的单板为 DSLD。
- 支持 U 口透传数据业务的单板为 DSLD。
- 支持 DDU2 传输同步 64K 数据业务的单板为 H301DDU2 板。
- 支持 SRX 子速率数据业务的单板为 H301SRX 板。

40.3 原理描述

介绍 G.SHDSL 数据业务、DDU2 传输 64K 同步数据业务、SRX 子速率数据业务和 U 口透传数据业务的实现原理。

40.3.1 G.SHDSL 数据业务原理

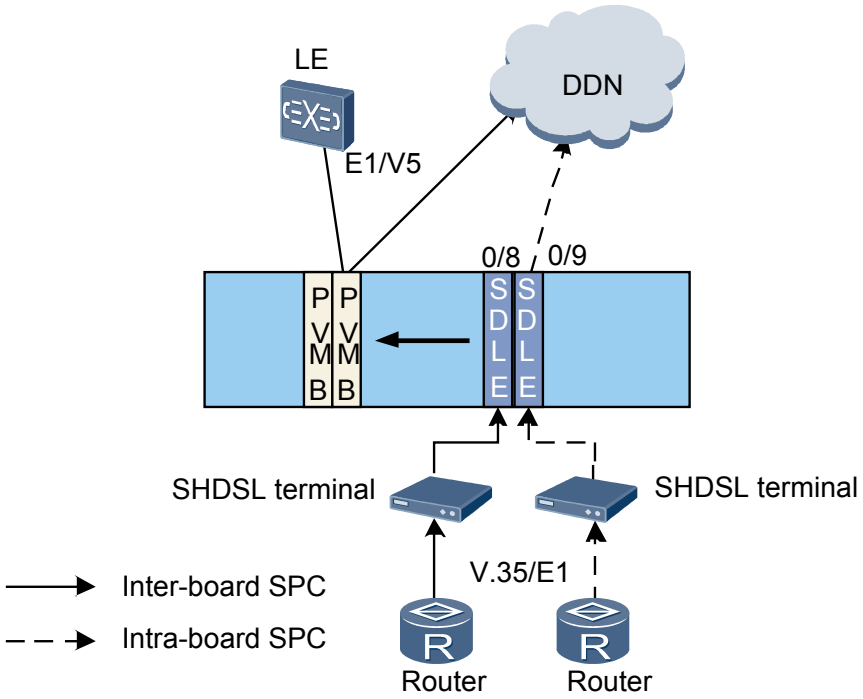
介绍 G.SHDSL 数据业务的实现原理。

G.SHDSL 是对应 ADSL、VDSL 出现的另一种技术，可以提供对称的最高能到 2Mbit/s 的速率，其传送的距离相比 ADSL 更远，应用可以非常广泛，可以替代过去的 E1 线、

可以用于高速的数据业务接入,它的特点是上下行数据对称。G.SHDSL 端口经过 modem 变换后，可以提供 V.35（N×64kbit/s，3≤N≤32）或者 E1（2048kbit/s）接口。

G.SHDSL 数据业务原理结构如图 40-1 所示。

图 40-1 G.SHDSL 数据业务原理结构图



G.SHDSL 端口下带 SHDSL 终端，可以提供 E1 或 V.35 接口。可以将该 E1 或 V.35 接口的数据通过建立半永久连接到其他 E1 端口上，有两种上行方式：

- intra-board SPC 方式

  直接通过本板 E1 端口上行。对于 DDN 网和 PSTN 网时钟不一致的情况下，应该使用该种方式。

- inter-board SPC 方式

  通过其他单板的 E1 端口上行。此种方式 DDN 网和 PSTN 网时钟必须一致。

汇聚：由于距离的原因，G.SHDSL 端口的数据一般远小于 2M，为了节省上行 E1 端口，可以将多个 G.SHDSL 端口的数据汇聚到同一个上行 E1 上。intra-board SPC 和 inter-board SPC 两种方式下都支持该汇聚功能。

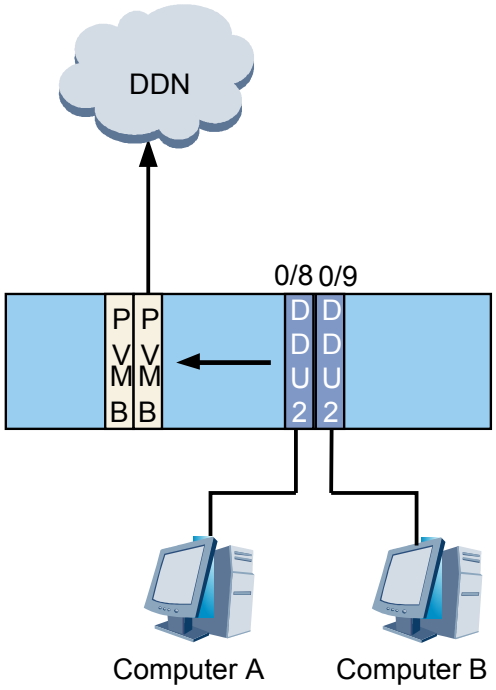
40.3.2 DDU2 传输 64K 同步数据业务原理

介绍 DDU2 传输 64K 同步数据业务的实现原理。

DDU2 传输 64K 同步数据业务通过配置内部半永久业务实现。DDU2 单板提供 2 路同步 64kbit/s 接口。DDU2 单板通过建立半永久业务实现透明通道传输，实现终端间的 64Kbit/s 数据业务交互。

DDU2 传输 64K 同步数据业务原理如图 40-2 所示。

图 40-2 DDU2 传输 64K 同步数据业务原理图



DDU2 单板提供同步 64K 接口，下带终端。UA5000 可以将该 64K 接口的数据建立半永久到其他 E1 端口上或 DDU2 端口上。

如果 UA5000 设备间的两个 DDU2 端口需要通信，可以用 E1 线连接两台设备，UA5000 设备内部的 DDU2 端口和对应的 E1 端口时隙建立内部半永久进行通信。

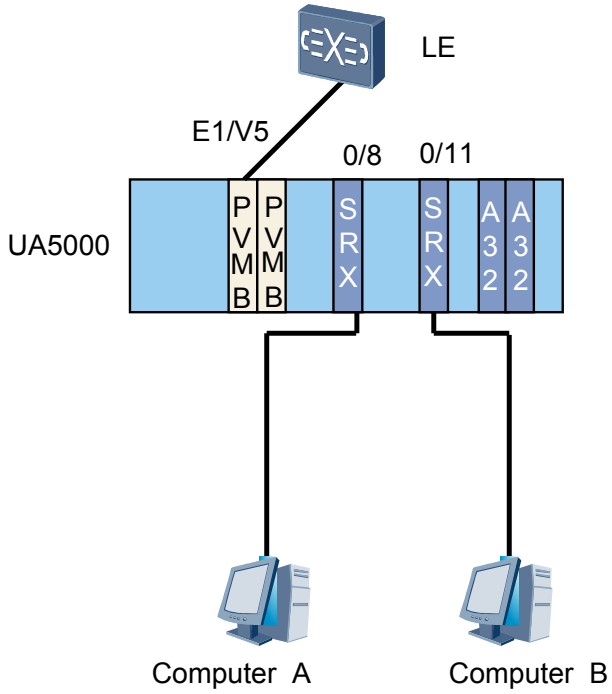
如果同一台 UA5000 设备上的两个 DDU2 端口需要通信，通过在两个 DDU2 端口上建立内部半永久实现端口间的交互。

40.3.3 SRX 子速率业务原理

介绍该特性的实现原理。

通过 SRX 板为数据终端用户提供 5 路同步 DCE 端口（支持 2.4/4.8/9.6/19.2/48kbit/s 等同步子速率业务），或者 3 路异步 DCE 端口（支持 2.4/4.8/9.6/19.2kbit/s 异步子速率业务）。子速率复用协议遵循 ITU-T 建议 X.50 Division3（20 个 8 比特包络）规定。UA5000 的 SRX 子速率业务是为数据终端用户提供一个与 DDN 网络或其他数据终端用户之间的物理通信通道。

图 40-3 SRX 子速率业务组网示意图



直接与 SRX 板相连的数据设备必须具有标准的 V.24/RS-232 串行接口。这些设备包括：

- 路由器
- 计算机
- 通信前置机
- 其它数据终端设备（DTE）

UA5000 不支持子速率交叉，所以使用子速率业务时，必须保证物理通道对应一致，比如：本端是 0/6/0 端口，对端在 0 框 7 槽，必须是 0 端口，子速率、顺相、隔相、同步、异步、复用协议的配置也必须一致。

如果 UA5000 设备间的两个端口需要通信，可以用 E1 线连接两台设备，UA5000 设备内部的 SRX 端口和对应的 E1 端口时隙建立内部半永久进行通信。

40.3.4 U 口透传数据业务原理

介绍 U 口透传数据业务的组网和原理。

U 口透传业务是指通过 DSL 数字用户板之间的半永久连接实现 ISDN BRA（U 口）接口业务的透明传输。通过 U 口的透传应用，可以延伸 DDN 节点机 U 口的传输距离，有效解决 U 接口的覆盖范围问题。

图 40-4 U 口透传数据业务示意图

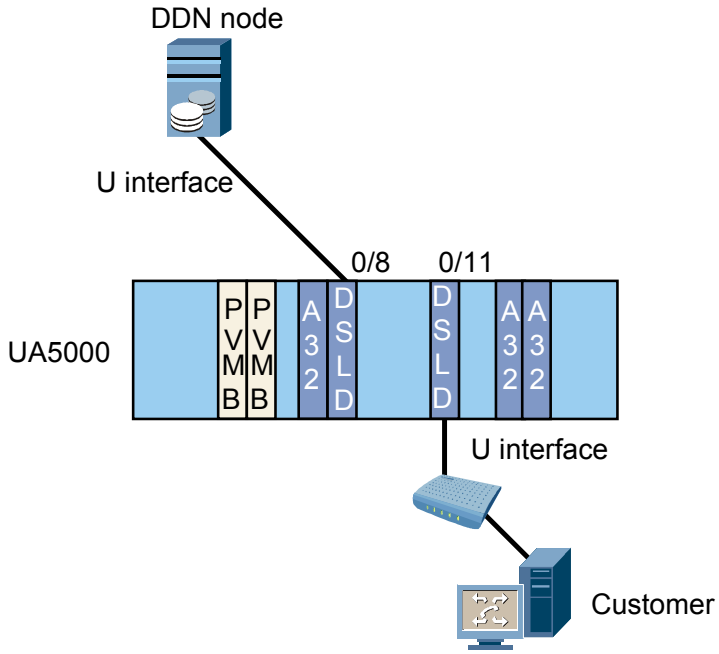


图 40-4 中 UA5000 一块 DSLD 板通过 U 口和 DDN 节点机相连，通过半永久连接将 U 口透传到另一块 DSLD 板连接的终端上，这样可以跨过传输设备组网。

设置 U 口透传业务需要两端的 DSLD 板端口分别工作在 MNT 和 MLT 方式。一般来说，连接网络侧设备的 DSLD 板端口工作在 MNT 方式，连接用户侧设备的 DSLD 板端口工作在 MLT 方式。

40.4 参考信息

介绍与该特性相关的参考信息。

本特性的参考资料清单如下：

- ITU-T V.35, "Data transmission at 48 kilobits per second using 60-108 kHz group band circuits'
- ITU-T V.24, "List of definitions for interchange circuits between data terminal equipment (DTE) and data circuit-terminating equipment (DCE)"
- ITU-T X.50, "FUNDAMENTAL PARAMETERS OF A MULTIPLEXING SCHEME FOR THE INTERNATIONAL INTERFACE BETWEEN SYNCHRONOUS DATA NETWORKS"

41 共线业务

关于本章

共线电话指铁路调度电话系统，由调度总机、传输信道（包括配套设备）和分机组成。

41.1 介绍
介绍该特性的定义、目的、规格和约束条件。

41.2 可获得性
介绍该特性需要的硬件支持。

41.3 原理描述
介绍该特性的实现原理。

41.1 介绍

介绍该特性的定义、目的、规格和约束条件。

定义

共线电话指铁路调度电话系统，由调度总机、传输信道（包括配套设备）和分机组成。在铁路专线网络中，共线业务就是调度线业务，铁路上称为行车调度、货车调度、无线列车调度等，这些调度线业务的实现方法实质上都是采用一个 64kbit/s 的传输信道。

目的

共线业务支持总站和分站之间或各分站间的音频业务交互。

规格

- 系统最多支持配置 16 个共线组。
- 每个共线组最多支持配置 64 个共线用户。
- 系统最多支持 768（12×64）个共线用户。

约束

UA5000 仅支持 M82610 型号的 Miro 芯片提供混音功能。

41.2 可获得性

介绍该特性需要的硬件支持。

UA5000 需配置 VFB 板和 ETCA 扣板或 ETCB 扣板才能支持共线业务。

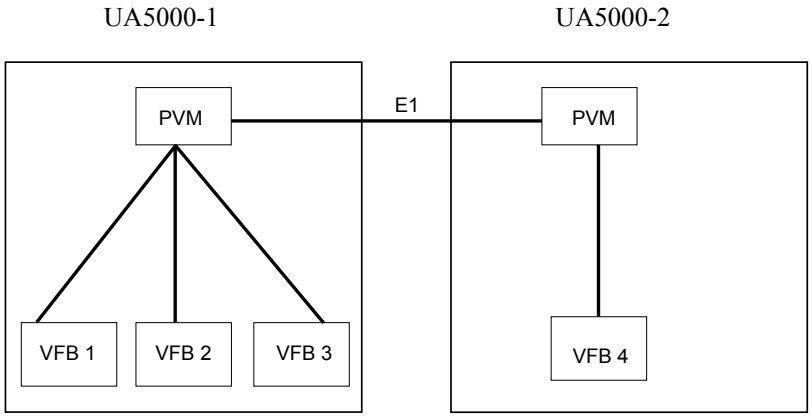
41.3 原理描述

介绍该特性的实现原理。

UA5000 设备为需要加入共线组的用户端口分配 DSP 通道，并进行联网，使用 Miro 芯片实现混音的功能，以替代 HONET 产品中的 VDM 单板。

共线业务原理如图 41-1 所示。

图 41-1 共线业务原理图



UA5000-1 上的 VFB 单板下带多个用户（VFB1 ～ VFB3 对应三个 VFB 端口下的三个用户），实现共线业务。配置共线半永久业务后，UA5000-1 为每个用户端口分配 DSP 通道，同时启动 Miro 芯片对这些 DSP 通道的混音功能，此时 VFB1 ～ VFB3 端口下的用户被加入到同一个共线组中。如果 UA5000-2 上的 VFB4 端口需要加入这个共线组，则需要在 UA5000-1 上加入一个 E1 时隙到 VFB1 ～ VFB3 所在的共线组，在 UA5000-2 设备上加入另一个 E1 时隙到 VFB4 所在的共线组，E1 时隙间的连接可以使用物理线直连的方式。

42 ISDN

关于本章

介绍 ISDN 特性的定义、目的、规格、原理以及参考的术语、缩略语和相关协议标准。

42.1 ISDN 特性描述
介绍 ISDN 的基本特性和实现原理。

42.2 BRA 基本速率适配
介绍 BRA 基本速率适配的基本特性和实现原理。

42.3 PRA 基群速率适配
介绍 PRA 基群速率适配的基本特性和实现原理。

42.1 ISDN 特性描述

介绍 ISDN 的基本特性和实现原理。

42.1.1 介绍

介绍该特性的定义、目的、规格和约束条件。

定义

综合业务数字网（Integrated Services Digital Network，ISDN）是一个 CCITT 标准，为语音、视频和数据提供综合传输业务，能够使语音、视频和数据信息在数据通道上实现同时传输。

ISDN 支持两种业务：

- 基本速率接口（BRI）：提供 144Kbit/s 的速率，包含 2 个 B 通道和 1 个 D 通道。
- 基群速率接口（PRI）：提供 2.048Mbit/s 的速率，包含 30 个 B 通道和 1 个 D 通道。

B 通道主要用来承载业务，D 通道传输呼叫控制信令和维护管理信令。

目的

在媒体网关上提供 ISDN 接入功能，从而为用户提供语音、视频和数据等综合传输业务。

规格

- BRA 提供 2B+1D 通道，B 通道速率为 64Kbit/s，D 通道速率为 16Kbit/s。
- PRA 提供 30B+1D 通道，B 通道和 D 通道速率均为 64Kbit/s。
- 支持优化的 TID 策略，实现方式与 PSTN 的 TID 优化相同。
- 支持的上行方式包括 SIP 上行、H.248 上行和 V5 上行。

术语

表 42-1 ISDN 特性术语表

术语	解释
BRA	ISDN 用户通过基本速率接口，提供 2 个 64Kbit/s 的 B 通道，1 个 16Kbit/s 的 D 通道，实现媒体网关侧的接入。
TA	终端适配器，用来适配非 ISDN 终端，使普通话机也能够接入 ISDN 网络。
TE1	ISDN 兼容终端，能够直接使用在 ISDN 网络上的数字终端。

术语	解释
TE2	ISDN 非兼容终端，即非 ISDN 数字终端，比如普通的 PSTN 电话机、传真机，需要 TA 的适配才能在 ISDN 网络中使用。
NT1	提供 U 接口和 S/T 接口，用于连接 ISDN 终端和 ISDN 交换机的设备，主要功能是在 U 接口和 S/T 接口之间进行码型转换，例如中国标准的 2B1Q/AMI 码型转换。NT1 一般是纯物理层设备，不具有软件智能，但具有线路维护和性能监控功能，保证 ISDN 终端和网络的时钟同步。
NT2	智能终端设备。常见 NT2 设备包括具有 ISDN 功能的用户小型交换机 PABX、LAN 路由器（Router）等终端控制设备。
PRA	ISDN 用户通过基群速率接口，提供 1 个 64Kbit/s 的 D 通道，30 个 64Kbit/s 的 B 通道，实现媒体网关侧的接入。

缩略语

表 42-2 ISDN 特性缩略语表

缩略语	英文全称	中文全称
BRA	Basic Rate Access	基本速率接入
BRI	Basic Rate Interface	基本速率接口
IUA	ISDN Q.921-User Adaptation Layer	ISDN Q.921 用户适配层
TA	Terminal Adapter	终端适配器
TEI	Terminal Equipment Identifier	终端设备标识
NT1	Network Terminal Type 1	-
NT2	Network Terminal Type 2	-

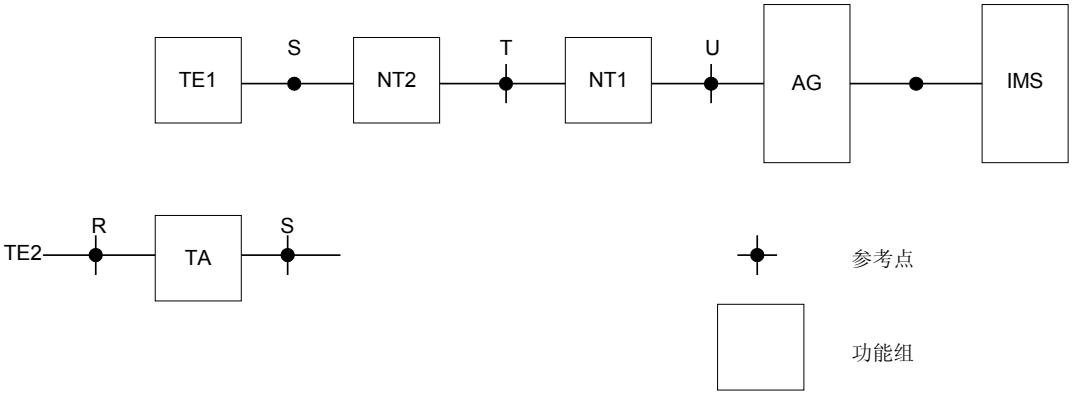
42.1.2 原理描述

介绍该特性的实现原理。

ISDN 参考模型（SIP 协议）

ISDN 接入的参考模型图如图 42-1 所示。

图 42-1 ISDN 接入的参考模型图（SIP 协议）

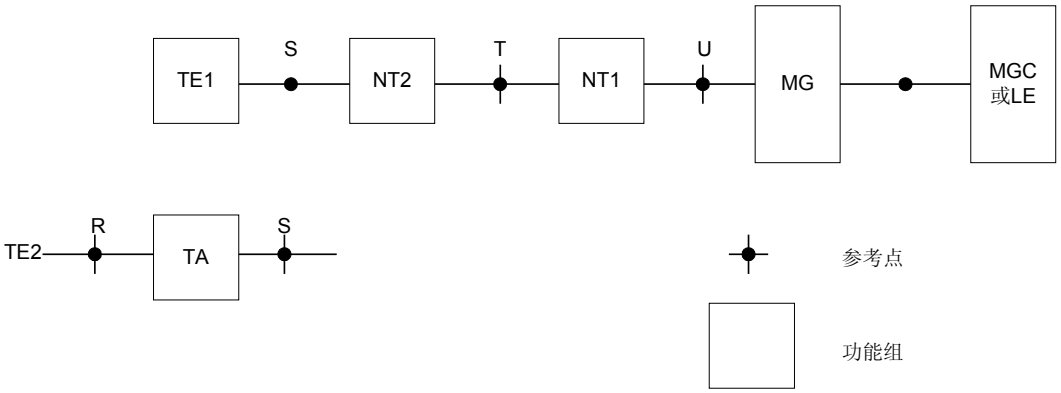


ISDN 用户通过 U 参考点接入 UA5000，用户侧的实际终端设备可能同时具备 NT1、NT2 及 TE1 的功能。当使用 SIP 上行时，UA5000 将终结 ISDN 的 Q.931 呼叫信令，并将其转换为 SIP 协议的标准呼叫信令，与 IMS 通信来控制 AG 上的媒体连接。

ISDN 参考模型（H.248/V5 协议）

ISDN 接入的参考模型图如图 42-2 所示。

图 42-2 ISDN 接入的参考模型图（H.248/V5 协议）

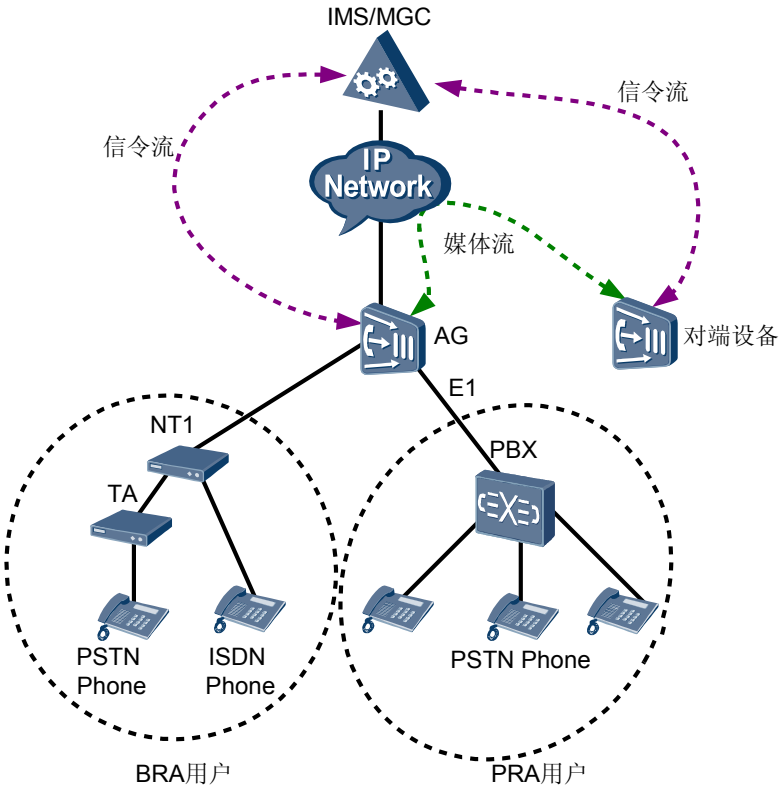


ISDN 用户通过 U 参考点接入 UA5000，用户侧的实际终端设备可能同时具备 NT1、NT2 及 TE1 的功能。当使用 H.248 上行时，MG 与 MGC 之间一般使用 IUA 协议承载 ISDN 的 Q.931 呼叫信令，使用 H.248 协议信令来控制 MG 上的媒体连接。当使用 V5 上行时，MG 与 LE 之间通过 V5 的 C 通道透传 Q.931 的信令，使用 V5 协议中的 BCC 协议完成时隙的分配和释放信令交互。

ISDN 系统结构

ISDN 系统结构原理如图 42-3 所示。

图 42-3 ISDN 系统结构图



ISDN 用户分为 BRA 用户和 PRA 用户。

- BRA 用户可以使用 ISDN 话机直接与 NT1 连接，也可以通过 TA 适配器接普通话机。在 MG 侧由 BRA 端口接入，NT1 与 MG 之间使用普通电话线连接。
- PRA 用户使用 PBX 通过 E1 端口接入，PBX 与网关之间使用 E1 线连接。

ISDN 呼叫控制流程（SIP 协议）

ISDN 使用 Q931 协议原语进行呼叫控制。网关与 NT1 之间，网关与 PBX 之间建立遵守 Q921 协议的二层链路来承载 Q931 消息。网关完成 Q.931 信令的终结，并将来自用户侧的 Q.931 协议转化为相应的 SIP 协议消息发送到 IMS 网络；同时完成网络侧下发的 SIP 协议消息到用户侧 Q.931 协议信令的转换。

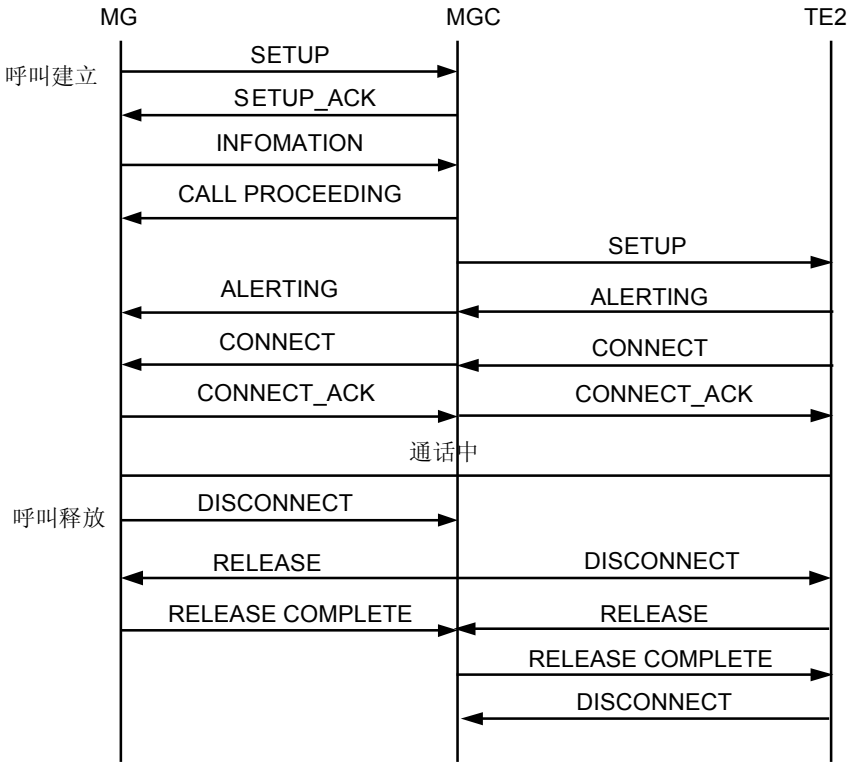
SIP 协议下，在 AG 与 IMS 之间的 ISDN 用户的呼叫流程与 SIP PSTN 用户的呼叫流程是一致的，请参考 **28.3 原理描述**。

ISDN 呼叫控制流程（H.248 协议）

ISDN 使用 Q931 协议原语进行呼叫控制。网关与 NT1 之间，网关与 PBX 之间建立遵守 Q921 协议的二层链路来承载 Q931 消息。网关与软交换之间建立 IUA 链路来承载 Q931 消息。

ISDN 呼叫的控制流程如**图 42-4** 所示。

图 42-4 ISDN 呼叫控制流程



网关不处理 Q931 原语，只是将终端来的 Q931 原语从 Q921 的消息包中取出来，封装到 IUA 的消息包中发送到软交换。Q931 原语不参与对资源的分配。

呼叫流程包括呼叫建立和呼叫释放两个阶段。

- 呼叫建立流程：
  1. 主叫方摘机发起呼叫建立 SETUP。
  2. 软交换回应 SETUP_ACK，同时请求更多呼叫信息，比如被叫号码。
  3. 主叫方拨号，号码由 IMFORMATION 原语携带上报到软交换。
  4. 软交换回应 CALL PROCEEDING，表示正在建立呼叫。
  5. 软交换向被叫发送 SETUP 请求建立呼叫。
  6. 被叫接受呼叫，开始振铃，发送 ALERTING，这个 ALERTING 也会到达主叫侧，告之主叫已经与被叫连接。
  7. 被叫摘机，发送 CONNECT，CONNECT 到达主叫，告之呼叫已经接通。
  8. 主叫响应 CONNECT_ACK。呼叫建立完成。
- 呼叫释放流程：
  1. 任一侧用户挂机，发送断开连接 DISCONNECT。
  2. 软交换向对方发送断开连接 DISCONNECT，并向挂机方发送释放呼叫 RELEASE。
  3. 挂机方释放呼叫完成，发送 RELEASE_COMPLETE 给软交换。
  4. 对方收到断开连接，发送释放呼叫 RELEASE 到软交换。

5. 软交换对对方响应 RELEASE_COMPLETE
6. 对方挂机，发送 DISCONNECT。呼叫释放完成。

42.1.3 参考信息

介绍该特性相关的参考信息。

本特性的参考资料清单如下：

- ITU-T Q.920 ISDN user-network interface data link layer General aspects
- ITU-T Q.921 ISDN user-network interface – Data link layerspecification
- ITU-T Q.930 Digital Subscriber Signalling System No.1 (DSS 1) – ISDN User-Network Interface Layer 3 – General Aspects
- ITU-T Q.931 ISDN user-network interface layer 3 specification for basic call control
- ITU-T Q.932 Digital Subscriber Signalling System No. 1 – Generic procedures for the control of ISDN supplementary services
- ITU-T H.248 Media gateway overload control package
- RFC3057 ISDN Q.921-User Adaptation Layer
- RFC3261 Session Initiation Protocol
- ITU-T G.961 Digital transmission system on metallic local lines for ISDN basic rate access
- ets_30010201e01p DSS1 basic call control
- ets_30019601e01p DSS1 generic function(For supplementary services)
- ETSI TS 183 036 V<0.8.0> (2007-09)

42.2 BRA 基本速率适配

介绍 BRA 基本速率适配的基本特性和实现原理。

42.2.1 介绍

介绍该特性的定义、目的、规格等。

定义

基本速率适配 BRA（Base Rate Adaptation）是指 ISDN 用户通过 ISDN 基本速率接口（BRI），在 H.248 协议的控制下实现媒体网关（MG）侧的接入。

BRA 提供 2 个 64Kbit/s 的 B 通道和 16Kbit/s 的 D 通道。B 通道主要用来承载业务，D 通道传输呼叫控制信令和维护管理信令。

目的

提供 BRA 用户接入，实现点到点或点到多点的语音、图像和数据的多媒体通信。

规格

- 2 个 64Kbit/s 的 B 通道，一个 16Kbit/s 的 D 通道。
- 系统支持最多配置 1000 个 BRA 用户。

- 一块 DSLD 板支持 16 路 BRA 端口。

术语

请参见表 42-1。

缩略语

请参见表 42-2。

42.2.2 可获得性

介绍该特性需要的硬件支持和 License 支持。

硬件支持

支持本特性的单板是 DSLD。

License 支持

BRA 用户数受 License 控制。

42.2.3 原理描述

介绍该特性的实现原理。

SIP 协议下的 ISDN BRA 原理结构如图 42-5 所示。H.248 协议下的 ISDN BRA 原理结构如图 42-6 所示。

图 42-5 ISDN BRA 原理结构图（SIP 协议）

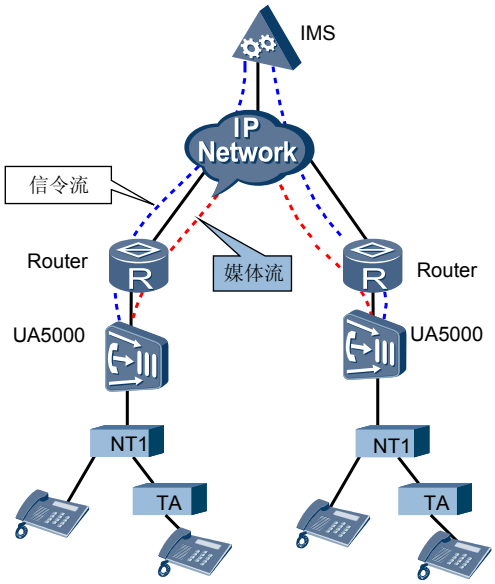
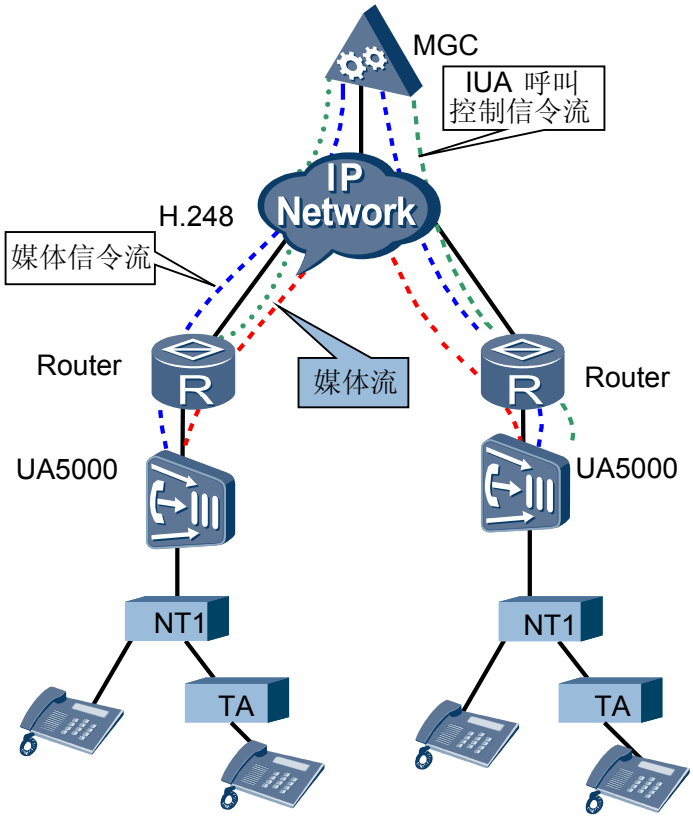


图 42-6 ISDN BRA 原理结构图（H.248 协议）



用户接入

BRA 用户通过 MG 侧的接入网，从去激活状态开始呼叫（主叫或被叫）时，要经过激活、申请 TEI、二层建链、三层呼叫控制 4 个阶段。如果端口终端从已被激活或已分配 TEI 或二层建链已成功的阶段开始呼叫，则直接进入下一个阶段。

呼叫控制（SIP 协议）

系统采用 SIP 终结 Q.931 的方式，即在 AG 上终结 ISDN 的 Q.931 协议信令，将其转化为 SIP 协议信令传递到 IMS 网络上。IMS 网络负责完成主被叫之间的流程协商。AG 自行控制 B 通道和终端资源的分配。

呼叫控制（H.248 协议）

系统中采用信令回程控制方式，即在 MG 上通过 IUA 将呼叫信令送给软交换（图中红线所示），软交换再将媒体控制信息通过 H.248 下发，控制 MG 上的 B 通道、上下文（H.248）和终端等资源（图中蓝色线所示）。

在 MG 和 MGC 侧实现一个 IUA 业务环境，将 DSLD 单板的 Q.931 信令承载在 SCTP 链路上，再通过 IUA 协议栈打包后发送到 MGC。在 MGC 侧转换成 Q.931 信令，同时 MGC 将 Q.931 信令通过 SCTP 链路发送到对端，完成 ISDN 呼叫信令的整个流程。

工作模式

BRA 工作模式分为点到多点（P2MP）和点到点（P2P）两种。

- 在点到多点的工作模式下，一个 NT1 下可以接多个终端，同一时刻可以建立多条二层链路，最多两个用户同时呼叫。在没有呼叫业务的情况下，可以自动去激活以达到省电的目的，且支持长激活。
- 在点到点的工作模式下，一个 NT1 下只能接一个终端，二层链路会始终保持建立，保证随时可以承载业务。无论是否有呼叫业务，都需要链路常激活时，采用点到点的模式。

终端供电方式

BRA 的供电是指给终端供电。提供两种终端供电方式：

- 本地供电，终端本身使用电池或连接电源。
- NT1 供电，终端使用 NT1 的电源。NT1 供电也有两种供电方式：
  - 本地供电，NT1 接本地电源。
  - 网关供电，在网关上配置 BRA 端口的远程供电属性，给 NT1 提供电源。

终端标识分配

BRA 用户完成物理线路激活后，在点到多点的工作模式下，一个 BRA 端口下可接多个终端，所以需要一个终端标识（Terminal Equipment Identifier，TEI）来唯一识别一个终端。

TEI 可以由终端指定，也可以由网络侧来分配。

- 终端指定的 TEI 范围为 0 ～ 63。
- 网络侧的 TEI 分配由用户板完成，分配的范围为 64 ～ 126。
- 127 作为广播 TEI，主要用在当 BRA 用户作为被叫时（一个端口下的所有用户使用相同的电话号码），由于不知道最终由哪个终端接收呼叫，就向所有的终端发起连接。
- 点到点模式下，终端 TEI 固定为 0。

42.3 PRA 基群速率适配

介绍 PRA 基群速率适配的基本特性和实现原理。

42.3.1 介绍

介绍该特性的定义、目的、规格等。

定义

基群速率适配（Primary Rate Adaptation，PRA）是指 ISDN 用户通过 ISDN 基群速率接口（PRI），在 H.248 协议的控制下实现媒体网关（MG）侧的接入。

E1 接口的 PRA 为语音和数据传输业务提供 1 个 D 通道加 30 个 B 通道。每个通道速率为 64Kbit/s。

目的

在媒体网关上支持 PRA 用户的接入。局方可以通过小交换机（PBX）来接入 PRA 用户，交换机内部的用户可以相互通话，对外可以满足与 PSTN 用户通话。

规格

- 采用 E1 规格，提供 32 个传输速率为 64Kbit/s 的通道。
- 0 通道用于帧同步，16 通道作为 D 通道用于信令传输，其他均作为 B 通道用于业务数据传输。
- 系统支持最多配置 32 个 PRA 用户。

术语

请参见**表 42-1**。

缩略语

请参见**表 42-2**。

42.3.2 可获得性

介绍该特性需要的硬件支持和 License 支持。

硬件支持

支持本特性的单板是 EDTB。

License 支持

PRA 用户数受 License 控制。

42.3.3 原理描述

介绍该特性的实现原理。

PRA 在呼叫过程上与 BRA 相同。BRA 的呼叫过程请参见“**42.2.3 原理描述**”。

配置一个 PRA 用户后，其有 32 个 64Kbit/s 时隙，其中第 1 ～ 15，17 ～ 31 时隙用作 B 通道，第 16 时隙用作 D 通道，第 0 时隙用作帧同步。

一个 PRA 用户二层建链使用的 TEI 固定为 0。

PRA 用户不存在工作模式和供电问题，因为由 PBX 给终端供电。

43 V5 协议

关于本章

介绍 V5 协议的定义、目的、规格、原理以及参考的术语、缩略语和相关协议标准。

43.1 介绍
介绍该特性的定义、目的、规格和约束条件。

43.2 可获得性
介绍该特性需要的硬件支持和 License 支持。

43.3 原理描述
介绍该特性的实现原理。

43.4 参考信息
介绍与该特性相关的参考信息。

43.1 介绍

介绍该特性的定义、目的、规格和约束条件。

定义

V5 接口是专为用户接入网的发展而提出的本地交换机和接入网之间的接口，该接口把交换机与接入设备之间的模拟连接转换为标准化的数字连接。

标准的 V5 接口包括 V5.1 接口和 V5.2 接口：

- V5.1 接口由单个 2M 中继构成。
- V5.2 接口支持 1 ～ 16 个 2M 中继，提供收敛的功能，时隙可以在接口的 2M 链路动态分配。

V5 接口支持的业务包括 POTS 业务，ISDN 业务和专线业务。

V5 接口由主次链路、C 路径、物理 C 通道、逻辑 C 通道、承载通路、接口变量和 ID、2M 链路 ID、保护组、协议地址和 5 个三层协议构成：PSTN 协议、控制协议、BCC 协议、保护协议和链路控制协议。

目的

通过 V5 接口可以把数字通道延伸到用户附近，降低用户线成本、扩大接入范围，同时标准的 V5 接口也使接入网可以平等的接入到本地交换机，促进接入网的发展。

规格

- 最大支持 16 个 V5 接口。
- 每个 V5.2 接口最大可以支持 16 条 2M 中继。

术语

表 43-1 V5 特性术语表

术语	解释
C 路径	运行上面 5 种协议中 1 个以上协议或者 ISDN 信令的二层链路的通称。
逻辑 C 通路	由一个或者多个 C 路径的组合组成，每一个逻辑 C 通路由 C 通路 ID 唯一标识，每个接口可以包含多个逻辑 C 通路。
物理 C 通路	是指承载逻辑 C 通路的一个 64K 时隙的物理通道，通常一个 2M 的 15、16、31 时隙可以被指定为物理 c 通道，因此对于一个 V52 接口最大的物理 C 通道为 16*3 ＝ 48。
承载通道	除了物理 C 通道和 2M 的 0 时隙外的其他所有的 64K 时隙。
接口变量和 ID	唯一标识一个接口的数字标签，无特定含义，在交换机和接入网配置上要保持一致。

术语	解释
2M 链路 ID	V5.2 接口包含多个 2M，为区分各 2M 链路，需要为每个 2M 分配一个标识，交换机接入网上配置相同标识的 2M 链路在物理上才能连接在一起。（V5.2 专有）
协议地址	交换机为每个协议地址分配电话号码，接入网为每个用户端口分配一个协议地址，使接入网的每个用户都对应交换机上的一个电话号码
主次链路	V5.2 接口中一些重要的协议都承载在一个物理 C 通路上，这些重要的协议如果不能正常工作将导致整个接口的故障，为了增加接口的可靠性，每个包含 2M 链路大于等于 2 的 V5.2 接口必须配置主次链路，其中主链路用于在正常情况下承载接口的协议信令，在主链路故障时可以保护切换到次链路上，确保接口的稳定性。V5.2 协议规定控制协议、链路控制协议和 bcc 协议都必须承载在主链路的物理 C 通道上（就是主链路的 16 时隙上）。
PSTN 协议	传送普通用户线路状态信息，呼叫控制由交换机控制。
控制协议	完成接口的启动过程和用户端口状态控制。
BCC 协议	Bear Channel Control 承载通道控制协议，完成时隙的动态分配。（V5.2 专有）
保护协议	用于保护主次信令链路。（V5.2 专有）
链路控制协议	用户管理 V5 接口中的 2M 链路。（V5.2 专有）
保护组 1	主次链路的物理 C 通道用于承载保护协议，构成保护组 1，在保护组 1 内一条物理 C 通道故障，承载信令的物理 C 通道会进行保护切换，确保业务的延续。
保护组 2	除了保护组 1 的其他所有的已配置的物理 C 通路构成保护组 2，保护组 2 最多有 3 个备用链路，用于保护 1 条 2M 中断时，15、16、31 时隙的 3 个物理 C 通道一起中断时的保护。

缩略语

表 43-2 V5 特性缩略语表

缩略语	英文全称	中文全称
PSTN	Public Switched Telephone Network	公共电话交换网
ISDN	Integrated Services Digital Network	综合业务数字网
BCC	Bear Channel Connect	承载通路连接
LAP	Link Access Procedure	链路接入规程
LapV5	Link Access Procedure on the V5	V5 接口链路接入协议
LapV5-DL	LapV5 Data link	Lapv5 的数据链路子层

缩略语	英文全称	中文全称
LapV5-EF	LapV5 Encapsulation Function	Lapv5 的封装功能子层
AN	Access Network	接入网
LE	Local Exchange	本地交换机
TS	Time Slot	时隙
VID	Variant and Identify	接口变量和标识

43.2 可获得性

介绍该特性需要的硬件支持和 License 支持。

硬件支持

V5 接口通过中继提供 E1 接口来实现，UA5000 支持 E1 接口的单板有 EDTB 和 PVMB/PVMD，协议处理由 PVMB/PVMD 完成。

License 支持

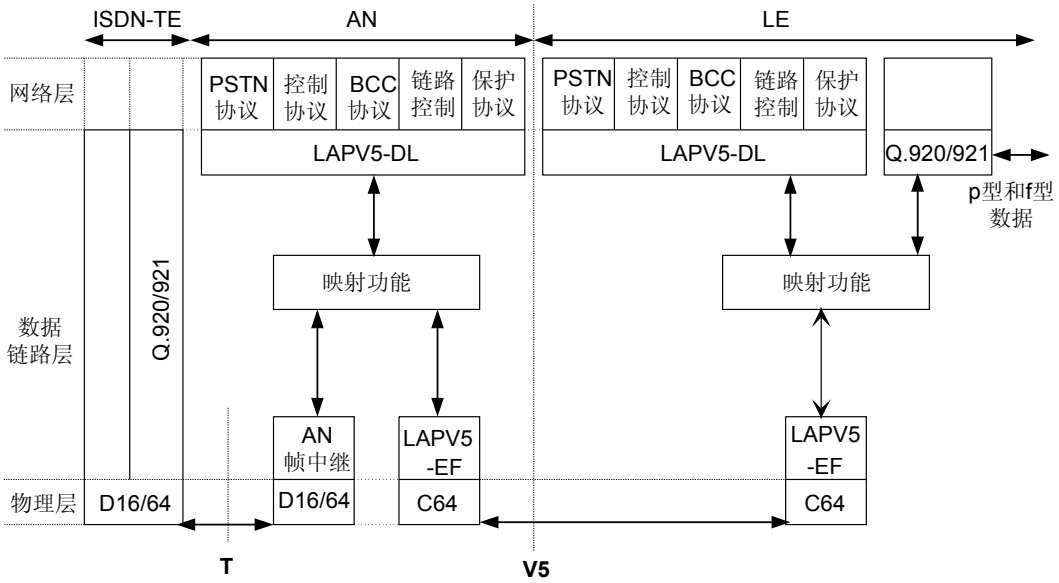
V5 接口个数受 License 控制。

43.3 原理描述

介绍该特性的实现原理。

V5.2 协议的原理如图 43-1 所示。

图 43-1 V5.2 协议原理结构图



- V5 接口的第一层－物理层

  V5 接口物理层帧结构应符合 CCITT 建议 G.704 和 G.706。帧由 32 个时隙（TS0 ～ TS31）组成；其中 TS0 用于帧定位和校验，TS16 作为通信通路（C 通路）可用于传送 PSTN 信令、ISDN 的 D 通路信息，其他时隙作为承载通道，对于没有被用于物理 C 通道的 16 时隙，也可以作为承载通道用于传输业务。如果 TS16 已全部占用，但还有 PSTN 信令等需要传输时，TS15 和 TS31 也可用作物理 C 通道传输信令。

- V5 接口的第二层－数据链路层

  V5 接口数据链路层即 LAPV5 分为两个子层：封装功能子层（LAPV5－EF）和数据链路子层（LAPV5－DL），用于管理 AN 与 LE 之间的二层逻辑链路。

  V5 的每个物理 C 通道承载了一个逻辑 C 通道，每个逻辑 C 通道有多个 C 路径构成。每个 C 路径都各自独立的建立一条二层链路用于 C 路径的信息交互，因此在每个物理 C 通道上就需要区分每个 C 路径的二层链路。通过 LAP-EF 功能将每个 C 路径映射到一个地址上，相当于对每个 C 路径分配一个地址，并将这个地址映射到 LAP-DL 上，这样三层就可以根据映射过来的地址区分不同的 C 路径，进行处理。

  各协议在 AN 和 LE 间是一一对应的，其中 V5.1 仅包含 PSTN 协议和控制协议。

- V5 接口的第三层－网络层

  V5 接口支持面向消息的协议：PSTN 信令协议、控制协议、链路控制协议、承载通路连接（BBC）协议、保护协议，对于交换机侧第三层还包括对 Q931 协议的处理部分。

  - PSTN 协议常用的消息包括 Establish、Establish Ack，signal、Signal ack、Disconnect、Disconnect Complete、Status 和 Protocol Parameter，可以看到除了用于三层确认的消息外，PSTN 协议本质上就是在交换机和接入网之间传递用户端口的线路信息。
  - 控制协议主要包含端口控制协议和公共控制协议，其中端口控制协议用于完成对端口状态的维护和管理，包括端口阻塞，端口解阻塞。 而公共控制协议则主要完成对 V5 接口启动的控制，主要包括 VID 核实、PSTN 重启动、端口状态加速同步。
  - 链路控制协议用于 V5.2 接口的多链路管理，包括链路阻塞，链路解阻塞、链路身份标识消息，其中链路身份标识用于 AN 和 LE 双方唯一确认一条对接 2M 是否正常的交互流程。
  - BCC 协议包括 分配、分配完成、分配拒绝、审计、审计完成、解除分配、解除分配完成等消息，主要用于承载通道的分配和释放。
  - 保护协议用于 V5.2 接口中对接口的主次链路进行保护，当其中主用的 C 通路故障时，可以马上切换到备用的 C 通路上进行保护；主用包括保护切换请求、保护切换命令、保护切换响应。

- V5 的用户管理

  每个 V5 用户分配一个地址，该地址在同一个接口下唯一，用于在 LE 和 AN 中唯一标识一个用户，通过 PSTN 协议完成用户端口状态上报和线路信息的上报，通过与 BCC 协议交互完成用户时隙资源的分配和管理。

- V5 接口的链路管理

  一个 V5.2 接口最多可以有 16 条 2M，每个链路分配一个链路 id，用于在 LE 和 AN 两侧对应一条 2M 链路，通过链路控制协议，可以对进行链路身份标识规程，避免 2M 链路接线时出现交叉的情况。

- V5 的接口管理

通过控制协议的交互，可以完成接口的复位、PSTN 重启动、加速同步等操作，完成接口的对接和启动。 AN 侧还提供了关闭 V5 接口的功能。

- V5 的逻辑 C 通道管理
  - V5.1：最多支持 3 条逻辑 C 通道，除 TS16 时隙用于承载控制协议 C 路径和 PSTN 协议 C 路径外，其他两个时隙 TS15、TS31 可以用来承载 ISDN 业务的 C 路径。
  - V5.2： 1 条 2M 链路的 V5.2 接口和 V5.1 接口是很相似的，其不同之处在于资源分配的不同； 对于多条 2M 链路的 V5.2 接口，必须配置保护协议和主次链路，除了主次链路的 TS16 时隙外一主次链路逻辑 C 通路构成保护组 1，其他链路的物理 C 通路共同组成保护组 2，共有 3 个保护组 2 备用，其余均为保护组 2 主用 C 通道。

43.4 参考信息

介绍与该特性相关的参考信息。

本特性的参考资料清单如下：

- ITU-T G.964V-Interfaces at the Digital Local Exchange (LE) – V5.1-Interface (Based on 2048 kbit/s) for the Support of Access Network (AN)
- ITU-T G.965V-Interfaces at the Digital Local Exchange (LE) – V5.2-Interface (Based on 2048 kbit/s) for the Support of Access Network (AN)
- YDN 021-1996 本地数字交换机和接入网之间的 V5.2 接口技术规范
- YDN 020-1996 本地数字交换机和接入网之间的 V5.2 接口技术规范

44 R2 协议

关于本章

介绍 R2 协议的定义、目的、规格、原理以及参考的术语、缩略语和相关协议标准。

44.1 介绍
介绍该特性的定义、目的、规格和约束条件。

44.2 可获得性
介绍该特性需要的硬件支持和 License 支持。

44.3 原理描述
介绍该特性的实现原理。

44.4 参考信息
介绍与该特性相关的参考信息。

44.1 介绍

介绍该特性的定义、目的、规格和约束条件。

定义

R2 信令为随路信令（CAS: Channel Associated Signaling），是基于 E1 数字网络的国际标准信令。R2 信令中 Timeslot 16 被预留用来传递其话音通道的信令。

R2 信令并不统一，ITU-T 的标准 Q.400-Q.490 定义了 R2 信令标准，但不同的国家和地区都有自己的实现方式。

目的

UA5000 将 R2 PBX 接入到 NGN 网络中，实现从 PSTN 网络到 NGN 网络的迁移。

规格

- 支持 R2 PBX 接入
- 支持数字线路信令
- 支持 MFC 方式寄发器信令
- 支持最大 32 个 R2 E1
- 每块 EDT 单板最大支持 16 个 R2 E1 端口

术语

表 44-1 R2 特性术语表

术语	解释
随路信令	信令和话音在同一条话路中传送的信令方式。
线路信令	由线路监视信号组成，在线路设备（中继器）之间传送，控制交换机之间或交换机内部的传输路径，在呼叫持续期间用于建立、维持、释放及监视所选的路由。
记发器信令	在记发器之间传送，由选择信号和一些业务信号组成，为呼叫路由选择及其相应的呼叫处理提供地址信息和一些其它的信息。主要完成主、被叫号码的发送和请求，主叫用户类别、被叫用户状态及呼叫业务类别的传送。

缩略语

表 44-2 R2 特性缩略语表

缩略语	英文全称	中文全称
CAS	Channel Associated Signaling	随路信令

缩略语	英文全称	中文全称
MFC	Multi-frequency Compelled	多频互控
PBX	Private Branch Exchange	小交换机

44.2 可获得性

介绍该特性需要的硬件支持和 License 支持。

硬件支持

- 业务单板：EDT 单板
- 需要 PBX 支持 R2
- 需要软交换支持 R2
- 需要软交换支持 H.248 协议，并支持 H.248 的 R2、CAS 包

License 支持

R2 接口个数受 License 控制。

44.3 原理描述

介绍该特性的实现原理。

44.3.1 R2 原理介绍

介绍 R2 信令的原理。

R2 信令由线路信令和记发器信令两部分组成。

线路信令

线路信令主要用来监视中继线的占用、释放和闭塞状态。线路信令分为模拟线路信令和数字线路信令。UA5000 只支持数字型线路信令，这里重点介绍数字型线路信令。

数字型线路信令采用 2048 kbit/s PCM 的 16 时隙用于传送线路信号。为了传送 30 个话路的线路信号，采用 16 帧组成一个复帧的结构，复帧中第 0 帧的 16 时隙用于复帧同步，第 1 帧的 16 时隙的前 4 个 bit 对应于第 1 话路，后 4 个 bit 对应于第 16 话路，依次类推。数字型线路信令，则通过 PCM 系统的第 16 时隙传输。

记发器信令

寄发器信令在记发器之间传送，由选择信号和一些业务信号组成，主要用于选择路由、选择被叫用户、管理电话网等。记发器信号的传输可采用互控方式（MFC）或非互控方式（MFP）进行。本产品只支持多频互控方式（MFC），这里重点介绍多频互控方式（MFC）。

多频互控记发器信号分前向信号和后向信号两种，采用 120Hz 等差级频。前向信号采用 1380Hz ～ 1980Hz 高频群，按六中取二编码，最多可组成 15 种信号。后向信号采用

780Hz ～ 1140Hz 低频群，按四中取二编码，最多可组成 6 种信号。为了扩充信号容量，前向信号又分为前向 I 组和前向 II 组；后向信号又分为后向 A 组信号和后向 B 组信号。

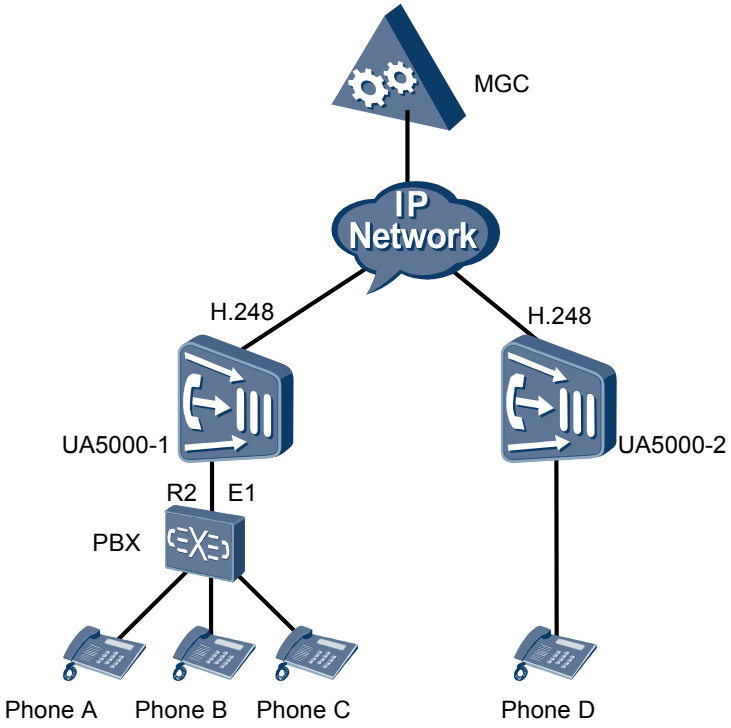
一个互控周期分四个节拍。第一个节拍用户侧发送前向信号；第二个节拍网络侧收到前向信号，回送后向信号；第三个节拍为用户侧收到后向信号，停发前向信号；第四个节拍为网络侧检测到前向信号停发，停发后向信号。

记发器信号为带内信号（频率在话音频带内），因此是通过话音通道进行传输的。

44.3.2 R2 PBX 接入 NGN 组网原理

介绍 PBX 通过 R2 协议接入到 NGN 中的组网原理。

图 44-1 R2 PBX 接入 NGN 网络原理结构图



PBX 通过 R2 接入到 NGN 网中，MG 与 MGC 之间的接口为 H.248；与 PBX 之间的接口为 R2。

为了让 PBX 通过 R2 接入到 NGN 网中，需要 MG 进行 R2 信令和 H.248 信令的相互转换：

- 上行时 UA5000 终结 PBX 的 R2 信令，并把 R2 信令转换成 H.248 信令送给软交换。
- 下行时 UA5000 终结软交换的 H.248 信令，并把 H.248 信令转换成 R2 信令送给 PBX 。

44.4 参考信息

介绍与该特性相关的参考信息。

本特性的参考资料清单如下：

- draft-manyfolks-megaco-caspackage-01.txt
- draft-laha-megaco-cas-mntc-00.txt
- draft-ietf-megaco-r2package-03.txt
- ITU-T H.248.25 Gateway control protocol: Basic CAS packages
- Specifications of Signaling System R2, Q.400 to Q.490, Blue Book, CCITT

45 发夹连接

关于本章

发夹连接（Hairpin Connection）指 MGC 控制下的 MG 内部呼叫，可以直接将同一设备内部的两个用户进行 TDM 时隙和网片 HW（Highway）的连接，无需占用 DSP 资源。

45.1 介绍

介绍该特性的定义、目的、规格和约束条件。

定义

发夹连接指 MGC 控制下的 MG 内部呼叫，可以直接将同一设备内部的两个用户进行 TDM 时隙和网片 HW 的连接，无需占用 DSP 资源。

目的

UA5000 采用发夹连接能减少对 DSP 资源的占用。

规格

发夹连接对资源没有强制性要求，MG 支持的发夹连接数目与实际能支持的用户数目相同。

约束

- 仅支持 H.248 协议下的发夹连接。
- 仅支持软交换控制下的发夹的实现方式。

术语

表 45-1 发夹连接特性术语表

术语	解释
软交换（SoftSwitch）	是电路交换网向分组网演进的核心设备，也是下一代电信网络的重要设备之一，它独立于底层承载协议，主要完成呼叫控制、媒体网关接入控制、资源分配、协议处理、路由、认证、计费等主要功能，并可以向用户提供现有电路交换机所能提供的所有业务以及多样化的第三方业务。
本地连接	在某些网络中，可能经常需要在同一网关内的端点之间建立连接。从一个端点到另一个端点的呼叫进行内部选路，经常称为“发夹”连接；本地连接的建立要比网络连接的建立简单。多数情况下，连接将通过一些本地的互连设备建立，例如，一个 TDM 总线。

缩略语

表 45-2 发夹连接特性缩略语表

缩略语	英文全称	中文全称
HC	Hairpin Connection	发夹连接

缩略语	英文全称	中文全称
TDM	Time Division Multiplex	时分复用
DSP	Digital Signal Processing	数字信号处理器
AG	Access Gateway	接入网关
MG	Media Gateway	媒体网关
MGC	Media Gateway Controller	媒体网关控制器

45.2 可获得性

介绍该特性需要的硬件支持，包括单板和终端。

无需额外硬件支持。

45.3 原理描述

介绍该特性的实现原理。

发夹连接原理结构如图 45-1 所示。

图 45-1 发夹连接原理结构图

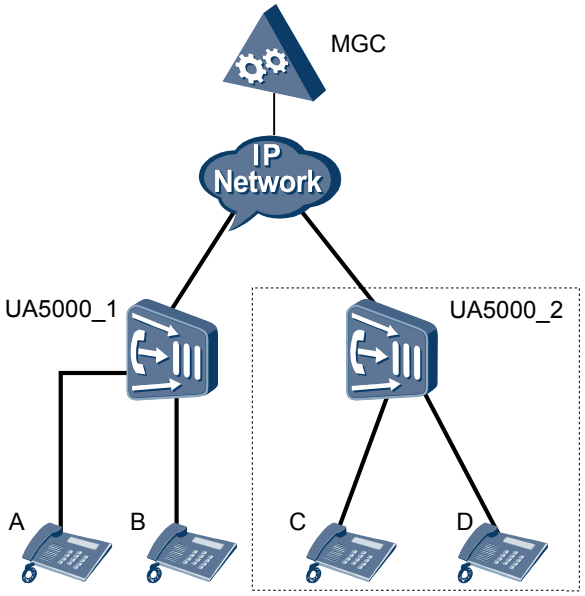


图 45-1 中 UA5000_1 未配置发夹功能，本地连接的两个用户 A、B 通话时，需要分别占用一个编解码 DSP。同时将窄带语音流编码为 IP 报文，送到上行 IP 网络传输。接收方将 IP 报文解码为窄带语音信号。UA5000_2 配置了发夹连接功能，可将本地连接的两个用户 C、D 通过 TDM 时隙和网片 HW 进行连接，用户 C、D 通话时，语音流通过 UA5000_2 直接传输。

45.4 参考信息

介绍与该特性相关的参考信息。

本特性的参考资料清单如下：

- ITU-T H.248.1 Media Gateway Control Protocol
- RFC3435 Media Gateway Control Protocol（MGCP）

46 2198 冗余

关于本章

介绍 2198 冗余特性的定义、目的、规格、原理以及参考的术语、缩略语和相关协议标准。

46.1 介绍
介绍该特性的定义、目的、规格和约束条件。

46.2 可获得性
介绍该特性需要的硬件支持和 License 支持。

46.3 原理描述
介绍该特性的实现原理。

46.4 参考信息
介绍与该特性相关的维护信息。

46.1 介绍

介绍该特性的定义、目的、规格和约束条件。

定义

RFC 2198 是 IETF 组织定义的一种在使用实时传输协议（RTP Version2.0）时对冗余音频数据进行编码的 RTP 负载格式（RTP Payload for Redundant Audio Data）。

目的

RFC 2198 通过冗余发送的方式，提高数据信息传送的可靠性，在网络质量较差的时候可以保证业务质量。

RFC 2198 冗余可用于 RFC 2833 的传送，也可用于透传方式下的 FoIP 业务和 MoIP 业务。

规格

- UA5000 支持 32 个动态负载类型。
- 2833 业务采用 RFC 2198 冗余时，最多支持 3 个冗余包。
- 传真透传业务和 Modem 透传业务采用 RFC 2198 冗余时，仅支持 1 个冗余包。

约束

- 对于 2833 收号业务，传真透传业务和 Modem 透传业务时，需要根据软交换上的配置决定是否启用 UA5000 的 RFC 2198 功能。
- RFC 2198 功能不用于普通语音业务，但是网关需要支持对 RFC 2198 报文的处理。

术语

表 46-1 RFC 2198 特性术语表

术语	解释
块负载类型（block PT）	7 位，表示该块的 RTP 负载类型。
时间戳偏移（timestamp offset）	14 位，本块相对于 RTP 头时间戳的无符号时间戳偏移量。使用无符号偏移则说明冗余数据的发送必须在主数据已经发送之后，因此要从当前时间中减去主数据的发送时间来决定冗余数据所在块的时间戳。
块长度（block length）	10 位，表示对应数据块的字节长度，其中不包括 RTP 头的长度。

缩略语

表 46-2 RFC 2198 特性缩略语表

缩略语	英文全称	中文全称
RTP	Real-time Transport Protocol	实时传输协议
DSP	Digital Signal Processing	数字信号处理器
PT	Payload Type	载荷类型
SDP	Session Description Protocol	会话描述协议
SSRC	Synchronization Source	同步源标识

46.2 可获得性

介绍该特性需要的硬件支持和 License 支持。

硬件支持

无需额外的硬件支持。

License 支持

2198 冗余特性受 License 控制。

46.3 原理描述

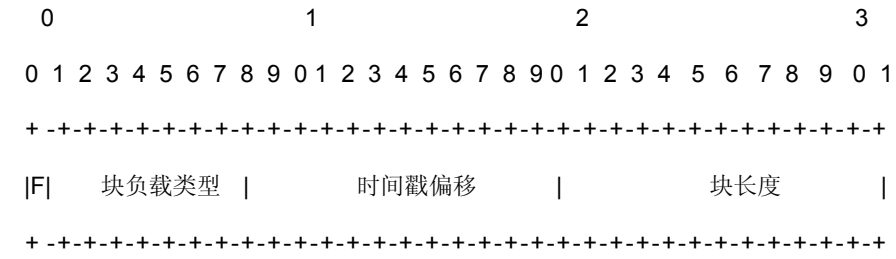
介绍该特性的实现原理。

RTP 应用使用如下冗余编码机制：

- 每个包必须携带一个主编码和一个或多个冗余编码。
- 因为对冗余信息可以采用多种编码形式，每个冗余编码块都必须有一个编码类型标识符。
- 由于可能采用变长编码，每个编码后的块都必须有长度指示符。
- RTP 头提供时间戳字段表示编码数据的创建时间。

一个承载了冗余数据的 RTP 包有一个标准 RTP 头，同时要在负载类型中表示其中含有冗余信息，RTP 头中其它字段与主数据块相关。RFC 2198 冗余负载的格式如图 46-1 所示。

图 46-1 RFC 2198 冗余负载格式



冗余负载在 RTP 头中的位置见**图 46-2** 中蓝色字体部分。

用于普通语音包的例子如下：

m=audio 12345 RTP/AVP 97 8 //2 种 PT 类型，分别是 97 和 8

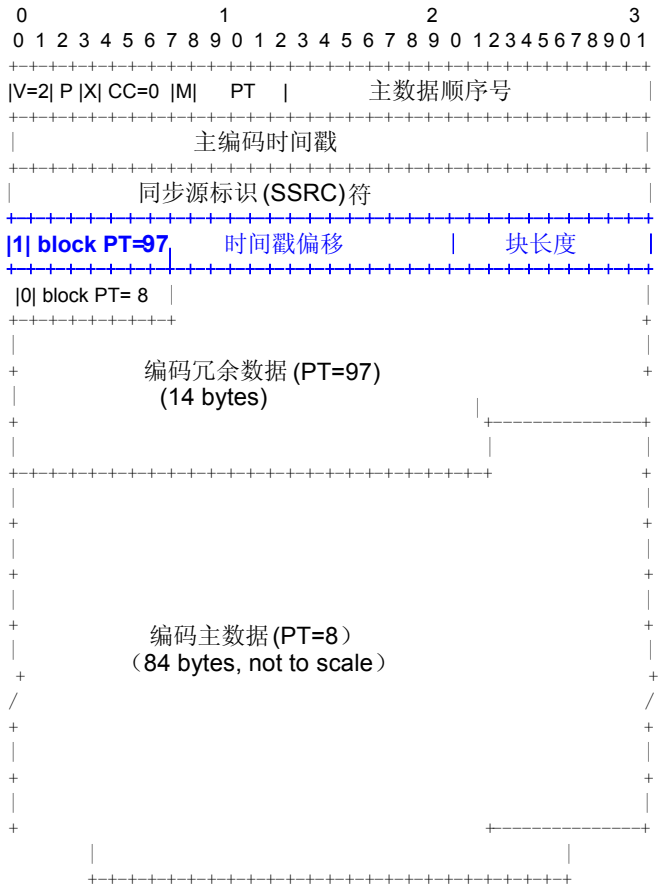
a=rtpmap:97 red/8000/1 //PT=97 表示使用 RFC 2198 冗余方式，red 是 codec

a=fmtp:97 8/8 //说明携带 PT=8 的帧

此时发送的 RTP 包的 PT=97，包里面有多个冗余的语音帧，PT=8。

完整 RTP 包格式如**图 46-2** 所示。

图 46-2 一个完整的冗余负载 RTP 包格式



46.4 参考信息

介绍与该特性相关的维护信息。

本特性的参考资料清单如下：

- International Telecommunication Union, RFC 2198 - “RTP Payload for Redundant Audio Data”
- International Telecommunication Union, RFC 2307 - “Session Description Protocol” RFC2307

47 留言灯

关于本章

介绍留言灯特性的定义、目的、规格、原理以及参考的术语、缩略语和相关协议标准。

47.1 介绍
介绍该特性的定义、目的、规格和约束条件。

47.2 可获得性
介绍该特性需要的硬件支持，包括单板和终端。

47.3 原理描述
介绍该特性的实现原理。

47.1 介绍

介绍该特性的定义、目的、规格和约束条件。

定义

留言灯是指用户可以通过观察话机上的留言灯确定是否有语音留言。

当用户开通留言灯业务并且其话机支持语音留言业务时，如果有人给用户打电话，用户不在电话机旁不能够接听电话，主叫可以在用户的语音信箱中留言，或者给总机留言。用户看到留言灯指示信息后，就可以查询语音信箱或者总机，收听留言。

留言灯功能一般用在酒店或者申请了语音信箱的场合。

目的

留言灯可以提示用户是否有语音留言。

规格

UA5000 本身不提供留言业务，需要在 MGC 设备的配合下提供。

留言灯功能有两种方式：

- 升压方式
- FSK 方式

约束

升压方式的留言灯需要特殊的用户板 VMS 单板。

术语

无。

缩略语

表 47-1 留言灯特性缩略语表

缩略语	英文全称	中文全称
FSK	FSK（Frequency Shift Keying）	频移键控

47.2 可获得性

介绍该特性需要的硬件支持，包括单板和终端。

升压方式需要特殊的 VMS 用户板配合，且话机要能够支持升压方式的留言功能。

FSK 方式需要话机能够支持 FSK 方式的留言功能，不需要特殊的其他硬件配合。

47.3 原理描述

介绍该特性的实现原理。

升压方式

UA5000 在 MGC 的控制下，向指定用户接入的用户板发送打开留言灯消息；用户板提高用户线上的电压，使用户话机上的留言灯点亮。

升压方式是通过话机上的指示灯来提示用户。

FSK 方式

UA5000 在 MGC 的控制下，在指定的用户话路时隙上，通过 FSK（Frequency Shift Keying）方式发送一组特殊的数据给用户话机；支持 FSK 方式的留言灯话机收到此信息后，点亮留言灯，并且会在支持 CID II 的话机屏幕上显示有留言的信息。

FSK 方式可以通过指示灯来提示或话机的屏幕来显示留言信息。

48 端到端信令跟踪

关于本章

介绍端到端信令跟踪特性的定义、目的、规格、原理以及参考的术语、缩略语和相关协议标准。

48.1 介绍
介绍该特性的定义、目的、规格和约束条件。

48.2 可获得性
介绍该特性需要的硬件支持，包括单板和终端。

48.3 原理描述
介绍该特性的实现原理。

48.4 参考信息
介绍该特性相关的参考信息。

48.1 介绍

介绍该特性的定义、目的、规格和约束条件。

定义

端到端（End to End，E2E）信令跟踪系统，所谓端就是指会话中的一个终端，端到端就是包含一个会话从启动建立、线路接续、会话释放等全部过程的信令跟踪，通过 E2E 的信令跟踪可以清楚的获得呼叫的全流程交互。

目的

在测试和定位问题时，E2E 信令跟踪系统可以为运营商和维护人员带来便利。

在端到端信令跟踪系统中，收到任务的网关设备向 FTP 服务器定期上传消息跟踪文件，网管再通过这些文件解析出信令。通过图形界面画出整个端到端的信令交互过程。

端到端信令跟踪系统可以跟踪一个会话的接续过程，因而可以在测试或者问题定位时起到辅助的作用，作为运营商和维护人员维护设备的有力工具。

规格

- 支持 H.248 协议端到端信令跟踪。
- 每个设备最多支持创建 4 个跟踪任务。
- 每个用户端口最多创建两个不同 ID 的跟踪任务（主动跟踪和被动跟踪）。

约束

- 需要软交换支持华为公司自定义的 H.248 端到端信令跟踪包。
- 需要配备华为公司的信令跟踪服务器。

术语

无。

缩略语

表 48-1 端到端信令跟踪特性缩略语表

缩略语	英文全称	中文全称
E2E	End to End	端到端

48.2 可获得性

介绍该特性需要的硬件支持，包括单板和终端。

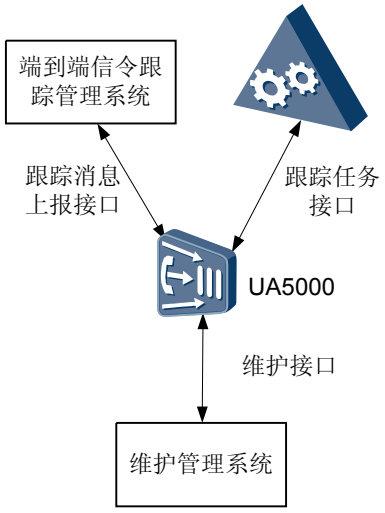
无需额外硬件支持。

48.3 原理描述

介绍该特性的实现原理。

E2E 信令跟踪原理结构如图 48-1 所示。

图 48-1 E2E 信令跟踪原理结构图



端到端信令跟踪系统与跟踪服务器、软交换、维护管理系统等共同完成端到端信令跟踪功能。

- UA5000 通过跟踪任务接口完成软交换下发的任务的启动、取消、校验等活动。
- UA5000 通过跟踪消息上报接口把跟踪消息上报给 E2E 跟踪管理系统。
- UA5000 自身的维护管理系统通过维护接口对任务进行维护和管理。

由软交换对某个端点启动信令跟踪任务（该任务称为主动跟踪任务）。软交换会对跟该端点进行会话的相关端点都下发信令跟踪任务（这些任务称为被动跟踪任务），收到任务的设备将相关端点的交互信令上报到信令跟踪服务器上，网管统一在服务器上获取信令跟踪文件并进行解析。

实现一个跟踪任务的过程如下：

1. 软交换启动跟踪。
2. 网关定时上报跟踪消息。
3. 查询跟踪任务情况。
4. 取消任务。

48.4 参考信息

介绍该特性相关的参考信息。

本特性的参考资料清单如下：

- draft-hw-megaco-calltracepkg-02
- draft-hw-mgcp-calltracepkg-02

49 IUA 链路倒换

关于本章

承载 ISDN 业务的 IUA 链路跟随 H.248 接口联动倒换，可以使 IUA 路径和 H.248 路径同时倒换到同一个管辖域下，保证正常开展呼叫业务。

49.1 介绍

介绍该特性的定义、目的、规格和约束条件等。

定义

承载 ISDN 业务的 IUA 链路跟随 H.248 接口联动倒换，可以使 IUA 路径和 H.248 路径同时倒换到同一个管辖域下。

目的

通过 IUA 链路倒换，提升了 IUA 链路的可靠性，增强了对呼叫的保护能力。

规格

- 支持 ASP 和 MGC 绑定联动倒换配置。
- 支持完全由 Softswitch 控制切换的 MGC 跟随 ASP 切换，两个 ASP 为主备模式。
- 支持完全由 Softswitch 控制切换的 ASP 跟随 MGC 切换，两个 ASP 为主备模式。
- 支持完全由 Softswitch 控制切换的 AS 跟随 MGC 切换，两个 AS 为主备模式。
- 支持完全由 Softswitch 控制切换的 AS 跟随 MGC 切换，两个 AS 为独立模式。
- 支持由 MG 主导的 ASP 跟随 MGC 切换。

约束

不支持 MG 主导的 AS 跟随 MGC 切换。

术语

无。

缩略语

表 49-1 IUA 链路倒换特性缩略语表

缩略语	英文全称	中文全称
AS	Application Server	应用服务器
ASP	Application Server Process	应用服务器进程
ISDN	Integrated Services Digital Network	综合数据业务网络
IUA	ISDN Q.921-User Adaptation	ISDN 用户适配层
MG	Media Gateway	媒体网关
MGC	Media Gateway Controller	媒体网关控制器
SCTP	Stream Control Transmission Protocol	流控制传输协议

缩略语	英文全称	中文全称
SG	Signalling Gateway	信令网关

49.2 可获得性

介绍该特性需要的硬件支持和 License 支持。

硬件支持

无需额外硬件支持。

License 支持

IUA 联动倒换特性是 UA5000 的基本特性，无需获得 License 许可即可获得该特性的服务。

49.3 原理描述

介绍该特性的实现原理。

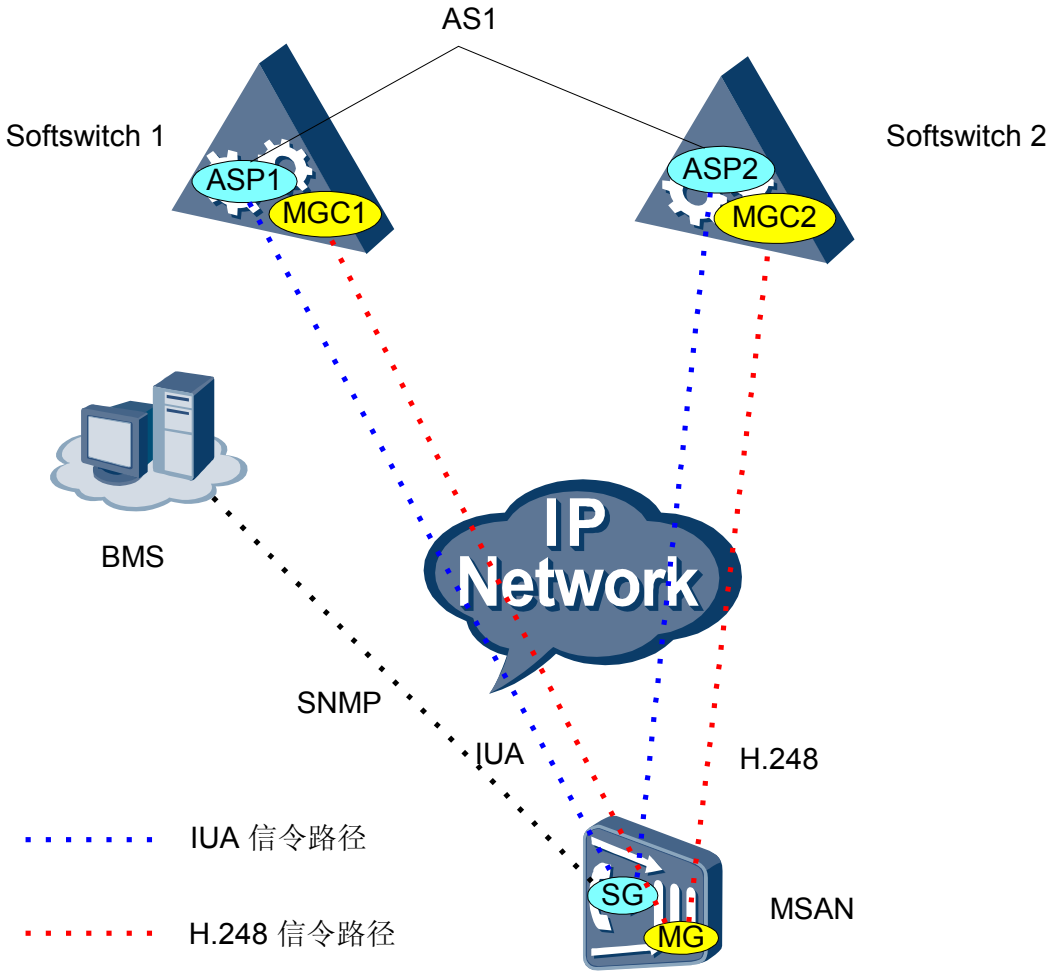
UA5000 目前支持通过信令回程方式实现基于 IP 网络的 ISDN 呼叫业务。在呼叫处理过程中，SG 终结低层的电路交换网(SCN)协议，并且把高层的协议延伸至 MGC。SG 终结 Q.921 协议，并且把 Q.931 协议延伸至 MGC，同时通过 H.248 协议实现 IP 呼叫资源的分配、释放和管理。

因此通过信令回程方式实现基于 IP 网络的 ISDN 呼叫业务在 IP 侧必须包括两条信令路径，一条是 IUA 信令路径，由 SG 和 ASP 共同维护和管理；另外一条是 H.248 信令路径，由 MG 和 MGC 共同维护和管理。

为了提高可靠性和安全性，在实际应用中一般都会配置多个 ASP 和多个 MGC。在标准协议中，这两个路径的管理实体是相互独立的，因此 IUA 链路倒换和 H.248 接口倒换也是相互独立的。两个路径独立倒换后如果不在同一个管辖域下，由于呼叫是统一处理的，就无法协调 IUA 信令和 H.248 信令共同完成呼叫处理。为了解这个问题，必须要实现 IUA 和 H.248 路径的联动倒换，保证 IUA 路径和 H.248 路径同时倒换到同一个管辖域下，保证正常开展呼叫业务。

IUA 链路倒换特性支持的组网如**图 49-1** 和**图 49-2** 所示。

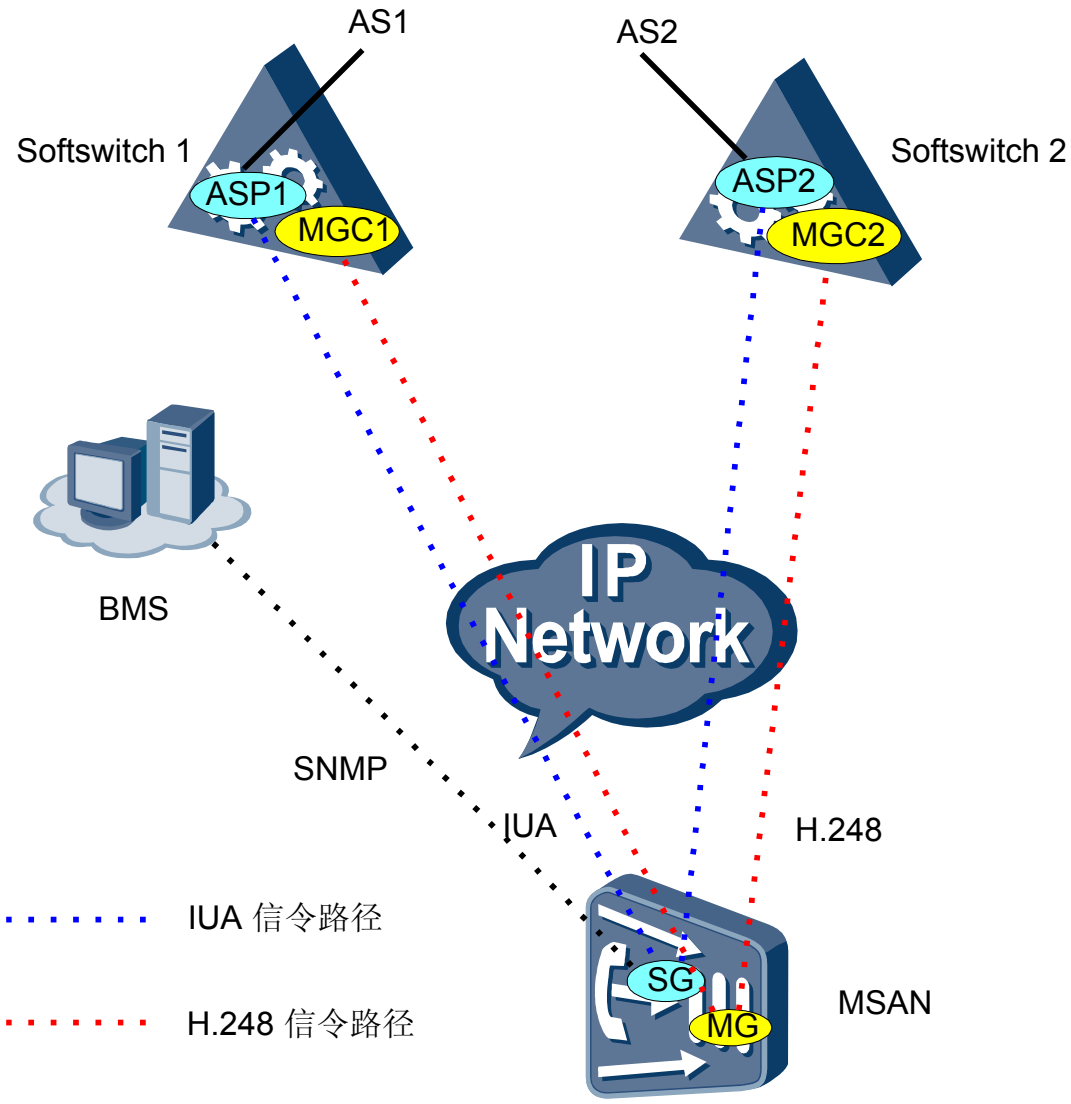
图 49-1 IUA 链路倒换特性支持的组网图 1



说明

UA5000 一个 SG 与一个 AS 对接（两个 ASP 同属于一个 AS，但是两个 ASP 分别在不同的 Softswitch 上）。

图 49-2 IUA 链路倒换特性支持的组网图 2



说明

UA5000 的一个 SG 对接两个 AS（两个 AS 分别在不同的 Softswitch 上）。

支持完全由 Softswitch 控制切换的 MGC 跟随 ASP 切换

说明

对应图 49-1。

由软交换作为控制主导者，AG 按正常 IUA 和 MGC 切换机制执行。在 AG 上不需要做联动倒换的配置。

- MSAN 的 MG 跟 Softswitch 1 的 MGC1 建立偶联关系；MSAN 的 SG 跟 Softswitch 1 的 ASP1 建立偶联关系（激活了 ASP）；MSAN 的 SG 跟 Softswitch 2 的 ASP2 建立偶联关系（没有激活 ASP）。
- 由于 ASP 故障，SG 向 ASP2 发起 NTFY（AS-Pending）；通知 ASP2 AS 处于 Pending 状态（实际上是间接请求 ASP2 激活）；ASP2 向 SG 发送 ASPActive 消

息，SG 向 ASP2 响应 ASPActiveAck 消息；MGC1 向 MG 发送 ServiceChange(903+handoff)要求 MG 切换 MGC 到 MGC2；MG 向 MGC2 发送 ServiceChange(903+handoff)，注册到 MGC2。

- MSAN 的 MG 跟 Softswitch 2 的 MGC2 建立偶联关系；MSAN 的 SG 跟 Softswitch 1 的 ASP1 建立偶联关系（没有激活 ASP）；MSAN 的 SG 跟 Softswitch 2 的 ASP2 建立偶联关系（激活了 ASP）。

支持完全由 Softswitch 控制切换的 ASP 跟随 MGC 切换

说明

对应图 49-1。

由软交换作为控制主导者，AG 按正常 IUA 和 MGC 切换机制执行。在 AG 上不需要做联动倒换的配置。

- MSAN 的 MG 跟 Softswitch 1 的 MGC1 建立偶联关系；MSAN 的 SG 跟 Softswitch 1 的 ASP1 建立偶联关系（激活了 ASP）；MSAN 的 SG 跟 Softswitch 2 的 ASP2 建立偶联关系（没有激活 ASP）。
- MG 向 MGC2 发起 Service Change，向 MGC2 注册；ASP2 向 SG 发送 ASPActive 消息；SG 向 ASP2 响应 ASPActiveAck 消息。
- MSAN 的 MG 跟 Softswitch 2 的 MGC2 建立偶联关系；MSAN 的 SG 跟 Softswitch 1 的 ASP1 建立偶联关系（没有激活 ASP）；MSAN 的 SG 跟 Softswitch 2 的 ASP2 建立偶联关系（激活了 ASP）。

支持完全由 Softswitch 控制切换的 AS 跟随 MGC 切换，AS 为主备模式

说明

对应图 49-2。

由软交换作为控制主导者，AG 按正常 IUA 和 MGC 切换机制执行。在 AG 上不需要做联动倒换的配置。

- MSAN 的 MG 跟 Softswitch 1 的 MGC1 建立偶联关系；MSAN 的 ASP1 跟 Softswitch 1 的 AS1 建立偶联关系（激活了 ASP）；MSAN 的 ASP2 跟 Softswitch 2 的 AS2 建立偶联关系（没有激活 ASP）。
- AS1 检测到 AS1 Down，MGC1 向 MG 发送 ServiceChange(903+handoff)要求 MG 切换 MGC 到 MGC2；MG 向 MGC2 发送 ServiceChange(903+handoff)要求 MG 切换 MGC 到 MGC2；AS2 向 SG2 发 ASP Active。
- MSAN 的 MG 跟 Softswitch 2 的 MGC2 建立偶联关系；MSAN 的 SG1 跟 Softswitch 1 的 AS1 建立偶联关系（没有激活 ASP）；MSAN 的 SG2 跟 Softswitch 2 的 AS2 建立偶联关系（激活了 ASP）。

支持完全由 Softswitch 控制切换的 AS 跟随 MGC 切换，AS 为独立模式

说明

对应图 49-2。

由软交换作为控制主导者，AG 按正常 IUA 和 MGC 切换机制执行。

- MSAN 的 MG 跟 Softswitch 1 的 MGC1 建立偶联关系；MSAN 的 ASP1 跟 Softswitch 1 的 AS1 建立偶联关系（激活了 ASP）；MSAN 的 ASP2 跟 Softswitch 2 的 AS2 建立偶联关系（没有激活 ASP）。

- AS1 检测到 AS1 Down，MGC1 向 MG 发送 ServiceChange(903+handoff)要求 MG 切换 MGC 到 MGC2；MG 向 MGC2 发送 ServiceChange(903+handoff)要求 MG 切换 MGC 到 MGC2；跟 MGC2 绑定的 AS2 设置为主用。
- MSAN 的 MG 跟 Softswitch 2 的 MGC2 建立偶联关系；MSAN 的 ASP1 跟 Softswitch 1 的 AS1 建立偶联关系（没有激活 ASP）；MSAN 的 ASP2 跟 Softswitch 2 的 AS2 建立偶联关系（激活了 ASP）。

支持 MG 主导 ASP 跟随 MGC 切换

说明

对应图 49-1。

由 MG 作为控制主导者，当 MGC 发生了切换，那么 IUA 需要同步切换到跟这个 MGC 绑定的 ASP。

- 在 MG 上需要的配置为：
  - 配置一个链路集，这个链路集对应于 AS1。
  - 配置链路集下链路 1 跟 MGC1 联动倒换，配置自动锁定 IUA 链路。
  - 配置链路集下链路 2 跟 MGC2 联动倒换，配置自动锁定 IUA 链路。
- MSAN 上配置有一个 MG、一个 SG：
  - Softswitch 1 的 ASP1 和 Softswitch 2 的 ASP2 归属一个 AS；ASP1 和 ASP2 互为主备关系。
  - Softswitch 1 的 MGC1 和 Softswitch 2 的 MGC2 互为主备关系。
- MSAN 的 MG 跟 Softswitch 1 的 MGC1 建立偶联关系；MSAN 的 SG 跟 Softswitch 1 的 ASP1 建立偶联关系（激活了 ASP）；MSAN 的 SG 跟 Softswitch 2 的 ASP2 建立偶联关系（没有激活 ASP）。
- 由于 MGC1 故障，MG 向 MGC2 发起 Service Change，向 MGC2 发起注册；MG 将未与 MGC2 绑定的链路 1（对应 ASP1）锁定（Lock）；SG 主动向 ASP2 发起 NTFY（AS-Pending），通知 ASP2 AS 处于 Pending 状态（实际上是间接请求 ASP2 激活）；ASP2 向 SG 发送 ASPActive 消息；SG 向 ASP2 响应 ASPActiveAck 消息。
- MSAN 的 MG 跟 Softswitch 2 的 MGC2 建立偶联关系；MSAN 的 SG 跟 Softswitch 1 的 ASP1（对应 IUA 链路 1）建立偶联关系（没有激活 ASP）；MSAN 的 SG 跟 Softswitch 2 的 ASP2（对应 IUA 链路 2）建立偶联关系（激活了 ASP）。

50 安全管理

关于本章

安全管理特性包括安全的用户管理、安全的文件传输、安全的维护终端连接和操作、安全事件的记录、安全日志和日志的空间调整。每个特性分别从介绍、可获得性、原理描述方面进行描述。

50.1 安全管理特性描述

从介绍、可获得性、原理描述方面概要介绍 UA5000 的安全管理特性。

50.1.1 介绍

介绍安全管理特性的定义、目的及规格等。

定义

软件系统各纬度的安全实现构成了 UA5000 软件系统管理的安全体系，它包括：安全的用户管理、安全的文件传输、安全的维护终端连接和操作、安全事件记录、安全日志和日志的空间调整。

目的

通过安全管理特性维护保证设备安全运行。

规格

- 支持安全管理员与系统管理员分离与统一。
- 支持维护用户绑定模板调整。
- 支持系统日志空间可调整。
- 支持安全日志查询、存储功能。
- 支持系统日志可备份到文件服务器。
- 支持系统日志实时上传 syslog 服务器。
- 支持安全的文件传输。
- 支持安全的维护终端连接和操作。
- 用户密码由 8 ～ 15 个字符组成，区分大小写，密码中至少有一个字符和一个数字。
- 用户名由 6 ～ 15 个字符组成，不区分大小写。
- 支持用户密码安全性规范检查。如果用户三次输入密码错误，系统将锁定该账户。

约束

无。

术语

表 50-1 安全管理特性的术语表

术语	解释
安全模式	标识当前系统的状态，是安全管理员分离还是合并。
安全管理员	与系统管理员并列的系统用户角色，可以执行系统安全管理的操作。

术语	解释
安全命令	执行后可能会对系统的安全造成影响的一类命令，比如：防火墙命令，用户管理命令等。
事件	系统运行过程中发生的某类需提醒用户注意的事情。
安全事件	涉及系统安全的事件。
事件级别	事件级别为事件的属性之一，用于确定该事件是否需要记录日志和发送告警。 目前事件的级别定义为三级： ● major：关键事件，在记录日志的同时发送告警。 ● minor：重要事件，仅记录日志，不发送告警。 ● ignore：可忽略事件，不记录日志，也不发送告警。
安全日志	系统中由于发生了安全事件而记录的日志。
操作日志	由于用户在系统中进行了操作而记录的日志。
公钥	一种在非对称加密算法中使用的解密密钥。

缩略语

表 50-2 安全管理特的缩略语表

缩略语	英文全称	中文全称
SSH	Secure shell	安全 SHELL
FTP	File Transfer Protocol	文件传输协议
SFTP	Secure file transfer protocol	安全文件传输协议

50.1.2 可获得性

介绍安全管理特性的硬件支持和软件支持。

硬件支持

无需额外硬件支持。

License 支持

安全管理特性是 UA5000 的基本特性，无需获得 License 许可即可获得该特性的服务。

50.1.3 原理描述

介绍安全管理特性的原理。

安全的用户管理

通过对安全命令的隐藏和解隐藏来实现对系统管理员权限的修改，通过用户的增加和删除来实现安全管理员的分离和合并。隐藏安全命令后，系统管理员无法使用安全命令，即限制了系统管理员的权限。解隐藏安全命令后，系统管理员可以使用安全命令。

安全的事件记录

事件的发生可能是由于用户的操作引发，也可能是设备状态的反映。记录事件的方式是根据事件的级别记录对应的日志和进行对应告警的上报。

安全日志和日志空间可调整

安全日志是在原有的日志基础上新增的一个类型。原理就是根据执行的命令不同来区分出安全日志。

日志的空间可调整，实质上就是通过程序把实际不连续的空间虚拟成一段连续的空间了来进行读写操作。

安全的文件传输

采用基于 SSH 机制的 SFTP 协议来进行文件的传输。在使用 Password 方式进行客户认证时，要求客户端必须输入用户名和密码进行验证。

安全的维护终端连接和操作

维护终端的数据是通过 TELNET 协议进行传输，安全的维护终端是为了保证传输数据的安全性，在传输前进行 SSH 加密。

50.2 安全的用户管理

安全的用户管理是指在当前系统中新生成一个安全管理员，把原来系统管理员的操作权限分开，系统安全管理的操作由安全管理员执行，其余仍然由系统管理员执行。

50.2.1 介绍

介绍安全用户管理的定义、目的、规格及约束等。

定义

安全的用户管理是指安全管理员的分离和合并。分离是指在当前系统中新生成一个安全管理员，把原来系统管理员的操作权限分开，系统安全管理的操作由安全管理员执行，其余仍然由系统管理员执行。合并是指把分开了的操作权限合并，由系统管理员执行。

分离前后，系统管理员的权限将发生变化，分离前，系统管理员拥有所有的查询和配置权限，包括安全操作；分离后，系统管理员的安全设置权限交给安全管理员，此时它只有安全查询权限，没有安全设置权限。安全管理员合并后，系统管理员重新拥有安全操作的查询和配置权限。

目的

安全管理员分离和合并的方案可以实现不同运营商对安全管理角色的要求。

规格

- 支持安全模式切换命令行。
- 支持安全模式状态的同步。
- 支持旧版本的升级。
- 支持安全命令的增量安装。
- 支持安全命令的增量隐藏/解隐藏。
- 支持用户通过 MIB（Management Information Base）节点设置或查询安全模式开关的状态。
- 安全管理员分离后，支持非安全管理用户修改自己的密码和信息。
- 支持用户模板属性的选择性修改。
- 支持用户模板有效期默认为永久有效。
- 支持用户模板有效期前后空格容错。

约束

- 修改自己的密码时，密码要求遵守当前系统的要求，如：密码长度不能小于 x 个字符。
- 系统管理员不可以进行安全管理员的合并操作。
- 在增量接口模式下增加或隐藏安全命令，用户模板名称不允许为“security”。

50.2.2 可获得性

介绍安全用户管理特性的硬件支持和软件支持。

硬件支持

无需额外硬件支持。

License 支持

安全用户管理特性是 UA5000 的基本特性，无需获得 License 许可即可获得该特性的服务。

50.2.3 原理描述

介绍安全用户管理特性的原理。

安全管理员的合并/分离

安全管理员机制是通过在系统中增加安全模板来实现的。安全管理员可执行的命令在其它模板下注册的同时还要在安全模板下注册。安全模式分离时，会执行两个操作。首先，生成一个安全管理员用户。其次，隐藏非安全模板下的安全配置命令。经过这样的操作，非安全模板下的安全配置命令被隐藏，其他用户无法使用。安全模式只有安全管理员可以进入，执行安全配置命令，这样就实现了安全管理员和系统管理员的权限分离。分离后，安全管理员的初始密码为：Hw!Sec1#_Admin。

安全模式合并时，则会执行三个操作。首先，解隐藏非安全模板下的安全配置命令。其次，从用户表中删除安全管理员，然后该用户下线，MIB 上的合并不允许安全管理员在线，所以也就不需要第三步的操作 ，经过以上几步操作后，非安全模板下的安全配置命

令可见，而安全管理员角色也已不存在，也就实现了安全管理员和系统管理员的权限合并。

安全模式的同步

安全模式的同步采用安全模式标志来完成。安全管理员的分离涉及用户表、安全模式标志、安全配置命令的隐藏/解隐藏。数据库同步机制保证了前两者可以准确同步到备板，对于安全配置命令的隐藏/解隐藏选择在平滑阶段来完成。

50.3 安全的文件传输

安全的文件传输是指使用 SFTP 进行文件传输。本特性从介绍、可获得性、原理描述等方面进行描述。

50.3.1 介绍

介绍安全的文件传输特性的定义、目的及规格等。

定义

安全的文件传输是指使用 SFTP 进行文件传输。SFTP 协议是一个基于 SSH 机制的安全文件传输协议，保证文件传输过程中的安全性。

目的

以往的文件传输协议（如 FTP）的用户验证使用的是明文传输方式，使得报文内容很容易在网络传输中被捕获，造成很大的安全隐患。以 SSH 协议加强了 FTP 的安全性，从而提高文件在传输过程中的安全性。

规格

- SFTP 服务器的用户名长度为 1~40 个字符。
- SFTP 服务器的密码长度为 1~40 个字符。
- SFTP 服务器的端口号从 0~65535。

约束

- 当 SFTP 特性关闭时，SFTP 功能将不可用。
- SFTP 特性依赖于现有 SSH 模块，即必须有 SSH 模块，才可以使用 SFTP 特性。

50.3.2 可获得性

介绍安全文件传输特性的硬件支持和软件支持。

硬件支持

无需额外硬件支持。

License 支持

安全管理特性是 UA5000 的基本特性，无需获得 License 许可即可获得该特性的服务。

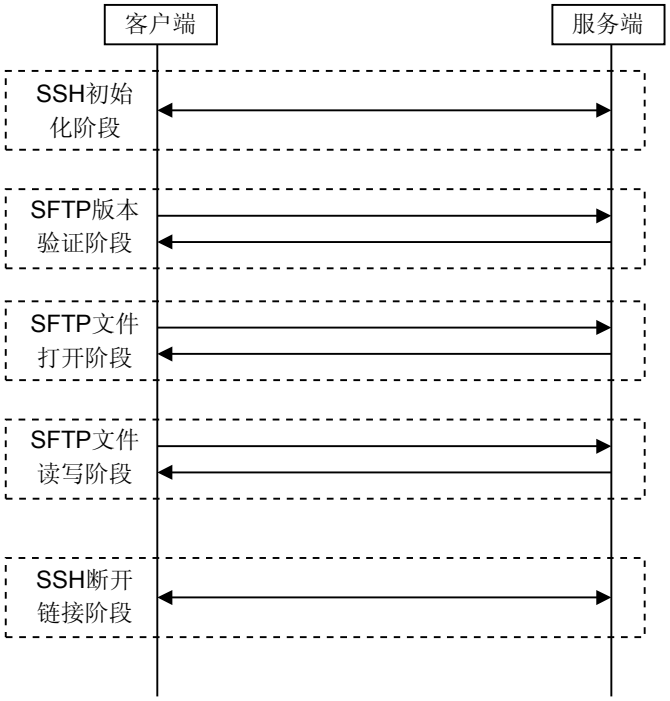
50.3.3 原理描述

介绍安全文件传输特性的原理。

SFTP 是一个基于 SSH 协议的安全文件传输协议，在使用 Password 方式进行客户认证时，要求客户端必须输入用户名和密码进行验证。若不能获得用户名和密码信息，则无法进行文件传输。

SFTP 的文件传输流程如图 50-1 所示。

图 50-1 SFTP 文件传输流程



SFTP 文件上传流程如下:

1. 客户端打开本地需要上传到服务器的文件。
2. 客户端请求打开服务器文件。
3. 根据返回的文件句柄把本地的数据写入到服务器。

SFTP 的下载是在 SSH 验证通过的基础上进行的：

1. 在 SFTP 阶段进行 SFTP 的版本验证。
2. 打开本地和远程文件。
3. 进行相应的读数据操作。
4. 在读数据完成后，关闭打开的文件。

50.4 安全的维护终端连接和操作

安全的维护终端连接和操作是指用户使用终端连接到设备上进行操作维护管理时，所有的操作内容都是安全的，不能被外界所获取。

50.4.1 介绍

介绍安全的维护终端连接和操作特性的定义、目的及规格等。

定义

安全的维护终端连接和操作是指用户使用终端连接到设备上进行操作维护管理时，所有的操作内容都是安全的，不能被外界所获取。

目的

保证用户通过远程终端登录设备后进行维护操作过程中，所有的操作都是安全的，即保证所有的操作的内容都是加密的，外界无法通过网络对维护操作过程中的内容进行监听和修改，保证操作维护过程的安全性。

规格

- 支持 SSH 1.x 协议和 SSH 2.0 协议。
- 支持用户密码认证，用户公钥认证，用户密码和公钥双重认证，用户密码或者公钥认证四种认证方式。

约束

无。

50.4.2 可获得性

介绍安全的维护终端连接和操作特性的硬件支持和软件支持。

硬件支持

无需额外硬件支持。

License 支持

安全的维护终端连接和操作特性是 UA5000 的基本特性，无需获得 License 许可即可获得该特性的服务。

50.4.3 原理描述

介绍安全的维护终端连接和操作特性的原理。

安全的维护终端和普通的维护终端传输数据都使用了 telnet 协议，所不同的是安全维护终端是在对所有的传输数据都使用 SSH 协议加密后，再使用 telnet 协议进行传输。

SSH 协议是一种安全协议，它只提供安全的通道，不提供数据的传输。SSH 协议经过版本协商，密钥交换，算法协商，用户认证等步骤建立了一个安全的通道。任何可以传输数据的协议都可以在此通道内进行数据的传输。安全的维护终端使用的工具提供了 SSH 客户端功能。

50.5 安全的事件记录

安全的事件记录是指对系统安全相关的事件进行记录。

50.5.1 介绍

介绍安全的事件记录特性的定义、目的及规格等。

定义

安全的事件记录是指对系统安全相关的事件进行记录。目前这些事件包括用户登录系统、退出系统、用户非法登录以及用户锁定事件。

目的

为了方便用户管理系统，系统中通过操作日志的方式记录了各个用户在系统上的操作。操作日志仅按时间记录发生的事件。系统运行过程中还会发生很多不是由用户操作引发，但从维护设备和定位故障角度又需记录下来的事件，特别是非命令操作引起的安全事件。安全的事件记录特性提供了将这些事件记录下来的机制，使得用户可以得到更加全面的系统维护信息。

规格

- 系统最多可以支持 64 个事件。
- 系统中默认支持 3 个事件。
- 支持查询事件列表。
- 支持命令行修改事件级别。
- 支持网管查询事件和修改事件级别。

约束

- 当安全日志特性关闭时，所有的安全事件将不可见，而且用户也不能修改安全事件的级别。
- 操作日志不支持通过事件的方式记录，即用户进行操作时只会记录操作日志，不会发送对应的告警。

50.5.2 可获得性

介绍安全事件记录特性的硬件支持和软件支持。

硬件支持

无需额外硬件支持。

License 支持

安全事件记录特性是 UA5000 的基本特性，无需获得 License 许可即可获得该特性的服务。

50.5.3 原理描述

介绍安全事件记录特性的原理。

事件为系统运行过程中发生的某类需提醒用户注意的事情。

事件的属性包括事件 ID、事件名称、事件类型、事件级别、事件默认级别等，其中可定制的为事件级别。事件级别的变化影响对应日志的记录和告警的上报。事件的类型对应于记录的日志类型。

记录事件的方式是根据事件的级别记录对应的日志和进行对应告警的上报。

UA5000 支持的安全事件列表如表 50-3 所示。

表 50-3 UA5000 安全事件列表

事件名称	事件 ID	事件默认级别	日志	告警	备注
用户登录/登出	0x0e100000	major	可定制，默认发送	可定制，默认发送	包括命令行、WEB、XML用户的登录登出。
用户非法登录	0x0e100001	major	可定制，默认发送	可定制，默认发送	尝试登录次数超过设定值的终端登录，包括命令行、WEB、XML等。
用户锁定	0x0e100002	major	可定制，默认发送	可定制，默认发送	非法登录后锁定用户名或IP。

50.6 安全日志和日志空间可调整

日志空间可调整是指系统中在存在多种日志类型的情况下支持通过命令行的方式调整每一类日志最多可以记录的日志的条数。

50.6.1 介绍

介绍安全日志和日志空间可调整特性的定义、目的及规格等。

定义

安全日志是指系统中发生了安全事件后，系统记录的日志。

日志空间可调整是指系统中在存在多种日志类型的情况下，支持通过命令行的方式调整每一类日志最多可以记录的日志的条数。

目的

系统支持安全日志之后，系统中将存在两种日志类型：操作日志和安全日志。

由于存储日志的 SRAM 空间有限，日志进行分类以后各种日志应用不同。在不同的应用中各类日志所需要的 SRAM 存储空间可能不同的，所以系统支持日志空间可调整。通过提供日志空间调整的命令行，用户可以根据实际情况确定每一类日志最多可以记录的条数，从而可以提高 SRAM 空间的利用率。

规格

- 安全日志的默认最大可存储条数为 256 条。
- 操作日志的默认最大可存储条数为 512 条。

约束

安全日志是可选特性。当安全日志特性关闭时，对 SRAM、静态内存基本不占用。无安全日志独立存在，不体现安全事件，日志空间可调整中不体现安全日志，自动上传功能中不体现安全日志。

50.6.2 可获得性

介绍安全日志和日志空间可调整特性的硬件支持。

硬件支持

无需额外硬件支持。

50.6.3 原理描述

介绍安全日志和日志空间可调整特性的原理。

由于每类日志记录的信息不同，要满足用户通过日志记录方便易用的获取到各类信息，日志的格式不能合并为一种。不同日志类型的日志空间的分段中的数据结构是不同的，系统需要维护各类日志的存储信息表。在系统初始化和用户执行日志空间调整命令时，通过各类日志的存储信息表可以实现各类日志的存放。

日志空间调整的前提是各类日志的总空间不变，这样日志空间的调整就是将日志的总空间在各类日志间重新分配。一类日志空间增大，则必然导致其它类日志空间的减少。当某一日志空间增大时，对于已记录的该类日志的处理相对简单，只需要将这些日志记录保留，并转移到新的存储位置。当某类日志空间变小时，如果已记录的该类日志所需要的空间大于调整后该类日志的空间，则需要计算在调整后的该类日志的空间中最多可记录的该类日志的条数，然后将已记录的该类日志中最新的这部分保留，并转移到新的日志空间，最早记录的部分日志将丢失。

为了确保已记录的维护信息的完整性，防止在日志空间调整时丢失部分日志，日志空间调整的命令处理中，将首先进行所有日志的备份，然后才进行日志空间的重新分配。

说明

- 日志空间调整的是日志的存储空间，而不是日志的条目数。由于每类日志单条记录占用的存储空间大小不同，所以减少的日志条数和增加的日志条数不一定相同。
- 日志空间调整过程中，存储空间减少的日志类型可能会丢失部分日志记录。为了保证日志记录的完整性，当系统具有自动备份功能时，在执行空间调整命令之前，请先配置自动备份服务器。这样系统在日志空间调整处理之前将强制进行日志的自动备份，从而避免历史日志记录的丢失。

51 补丁管理

关于本章

补丁是为了对系统软件中的某些缺陷进行修改而发布的独立的软件单元。UA5000 支持软件补丁管理，分别从介绍、可获得性、原理描述方面进行描述。

51.1 介绍
介绍软件补丁特性的定义、目的及规格等。

51.2 可获得性
介绍软件补丁特性的硬件支持和软件支持。

51.3 原理描述
介绍软件补丁特性的原理。

51.1 介绍

介绍软件补丁特性的定义、目的及规格等。

定义

补丁是软件系统和软件工程学中的一个术语。补丁是为了对系统软件中的某些缺陷进行修改而发布的独立的软件单元。从对业务影响方面可以将补丁分为热补丁和冷补丁。

对于一些要求长时间不间断工作的设备，当发现软件有缺陷或新需求时，在不对软件模块进行重新启动并且不中断业务的情况下，用新代码来替换旧代码来解决这些缺陷或者实现新需求。这段新代码就称为热补丁。

通过新文件覆盖或新增文件，重启软件模块来解决缺陷或者实现新需求。这些新文件的集合称为冷补丁。

目的

在设备运行中要求长时间不间断地工作，当解决主机软件问题或新增某些功能时，需要在不中断业务的情况下修改主机软件，即给主机软件打补丁。

规格

- 加载补丁时，补丁会同时加载在主用主控板和备用主控板上。
- 对于热补丁，系统只支持一次回退操作。
- 对于冷补丁，加载完成后，系统不支持回退。

约束

冷补丁的生效与失效需要通过重启系统或者主备倒换实现。

51.2 可获得性

介绍软件补丁特性的硬件支持和软件支持。

硬件支持

无需额外硬件支持。

License 支持

软件补丁特性是 UA5000 的基本特性，无需获得 License 许可即可获得该特性的服务。

51.3 原理描述

介绍软件补丁特性的原理。

补丁实现原理

系统中存在一个补丁区，用于存放加载后的补丁函数。当进行激活等使补丁生效的操作时，系统会根据原函数的地址与补丁区中新函数的地址计算出相对偏移，然后生成相对跳转指令，写入到原函数的起始指令处。

当系统执行到打补丁的函数时，首先调用原函数，执行第一条指令时，会直接跳转到补丁区中的新函数执行，从而实现了补丁生效的操作。

当执行去激活等使补丁失效的操作时，将保存的原函数的第一条指令恢复到原地址，这样补丁区中的新函数不会被调用，从而实现补丁的失效的操作。

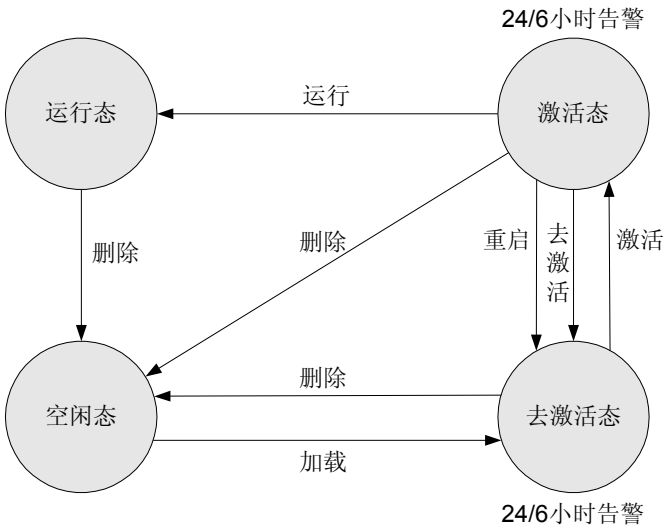
热补丁状态迁移

热补丁的状态包含去激活态、激活态、运行态、空闲态。不同补丁状态的含义如下：

- 去激活态：热补丁还没有生效。
- 激活态：热补丁已经生效，激活态属于一种不稳定状态，系统重启将导致补丁失效。
- 运行态：热补丁已经生效，并且属于一种稳定状态。
- 空闲态：没有热补丁或者热补丁已经删除。

热补丁的不同状态之间的迁移关系如图 51-1 所示。

图 51-1 热补丁状态迁移图



说明

在上图中，24/6 小时告警指统计经过 24/6 小时后，热补丁状态发生变化，由去激活态变为激活态，或由激活态变为运行态。

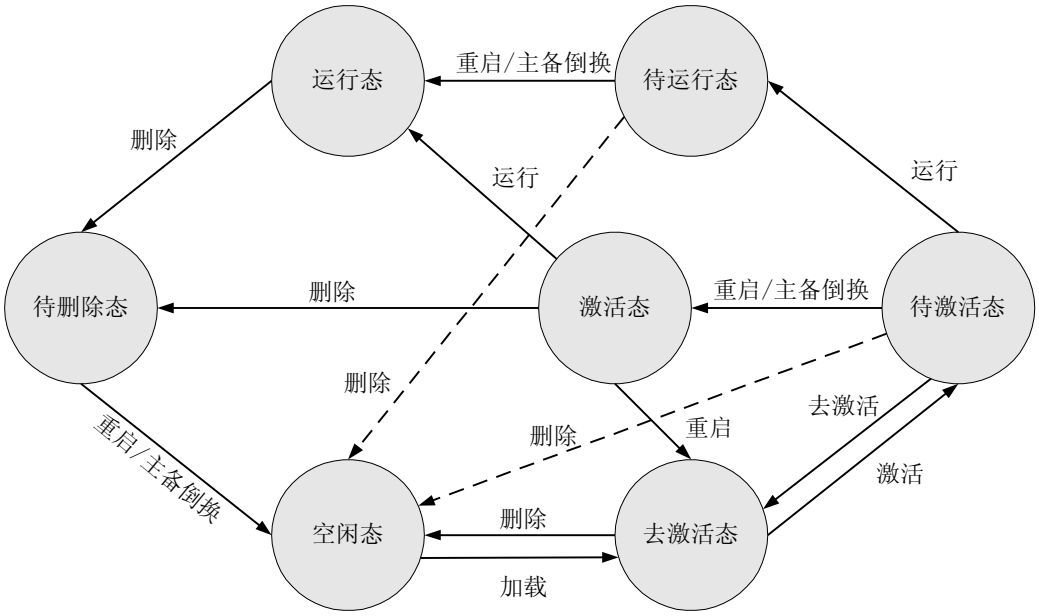
冷补丁状态迁移

冷补丁的状态包含去激活态、待激活态、激活态、待运行态、运行态、待删除态、空闲态。不同补丁状态的含义如下：

- 去激活态：冷补丁还没有生效。
- 待激活态：已经执行了冷补丁激活操作，冷补丁还没有生效，需要重启系统或者主备倒换，才能生效。
- 激活态：冷补丁已经生效，激活态属于一种不稳定状态，存在激活态冷补丁的系统重启将导致补丁失效。冷补丁的激活态不支持去激活态操作。
- 待运行态：已经执行了冷补丁激活、运行的操作，冷补丁还没有生效。需要重启系统或者主备倒换，才能生效。
- 运行态：补丁已经生效，并且属于一种稳定状态。
- 待删除态：已经执行了补丁删除命令，补丁仍然生效，需要重启系统或者主备倒换，才能删除该补丁。
- 空闲态：代表没有补丁或者补丁已经删除。

冷补丁的不同状态之间的迁移关系如图 51-2 所示。

图 51-2 冷补丁状态迁移图



52 设备升级

关于本章

介绍升级不断业务特性和单板软件自动升级特性的定义、目的和原理等。

52.1 升级不断业务
升级不断业务是指在设备进行软件升级时不中断业务或者中断时间在最终用户可以接受的范围内。

52.2 单板软件自动升级
UA5000 支持将单板的 BIOS 文件和单板软件打包加载，单板复位后，单板软件自动加载，从而实现单板软件自动升级。

52.1 升级不断业务

升级不断业务是指在设备进行软件升级时不中断业务或者中断时间在最终用户可以接受的范围内。

52.1.1 介绍

介绍升级不断业务特性的定义、目的及规格等。

定义

升级不断业务是指在设备进行软件升级时不中断业务或者中断时间在最终用户可以接受的范围内。

目的

在传统的设备升级的方式中一般是主备板同时加载高版本的程序和数据，然后同时复位主备板，从而把设备版本过渡到新的版本。在上述的操作过程中，由于同时复位了主备板，导致在设备重启的过程中，业务功能不可用。系统支持升级不断业务后，设备可以平滑的从低版本升级到高版本，降低了升级对用户、业务的影响，降低业务的中断时间或者不中断业务，从而提高了用户的满意度。

规格

无。

约束

升级不断业务特性只能运行在主备硬件设备一致的环境中。

术语

表 52-1 升级不断业务特性术语表

术语	解释
配置数据	系统用户配置的业务数据。

52.1.2 可获得性

介绍升级不断业务特性的硬件支持和 License 支持。

硬件支持

无需额外硬件支持。

License 支持

升级不断业务特性是 UA5000 的基本特性，无需获得 License 许可即可获得该特性的服务。

52.1.3 原理描述

介绍升级不断业务特性的原理。

目前的设备主备同步中把数据分为静态数据和动态数据。

- 静态数据主要是指用户的配置数据，一般是指通过系统配置的数据自动恢复出来的业务数据，不依赖于业务单板是否在位。
- 动态数据是指业务动态变化信息，主要依赖于系统运行起来之后根据单板、端口变化、协议交互而动态生成的数据。

必须在主备主控板均存在的环境下，才可以使能升级不断业务功能。

- 先把备用主控板的软件版本升级到高版本。
- 备用主控板的静态数据通过加载的配置文件或者数据库文件生成，动态数据通过主用主控板同步到备用主控板。
- 在动态数据的同步过程中，由于新旧版本的动态数据存在差异性，主用主控板的动态数据同步到备用主控板时，在同步恢复模块需要把旧版本的同步数据转换成新版本的动态数据。
- 待动态数据同步完成之后，进行主备倒换。这时由于原先的备用主控板变为主用主控板，并且已经存在所有的静态数据和动态数据，用户业务可以正常运行，从而达到升级而不中断业务。
- 动态数据的同步不需要手动操作，但触发升级不断业务需要命令行或者网管设置升级场景。
- 把原先的主用主控板的软件版本升级到高版本，并加载配置文件和数据库文件，生成静态数据。
- 复位原先的主用主控板。

52.2 单板软件自动升级

UA5000 支持将单板的 BIOS 文件和单板软件打包加载，单板复位后，单板软件自动加载，从而实现单板软件自动升级。

52.2.1 介绍

介绍单板软件自动升级特性的定义、目的及缩略语。

定义

当设备上电系统启动后，业务板自动向主控板申请其正常运行需要的相关软件资源（包括 BIOS 文件和单板软件）。业务板接收完资源文件后，在必要的情况下自动复位单板软件，并在单板下次启动时运行刚才接收到的软件资源。

目的

单板软件自动升级降低了手动升级的复杂性，为用户提供了操作简单、可靠的一站式服务。

缩略语

表 52-2 单板软件自动升级特性缩略语表

缩略语	英文全称	中文全称
BIOS	Basic Input Output System	基本输入输出系统

52.2.2 可获得性

介绍单板软件自动升级特性的硬件支持和软件支持。

硬件支持

支持此特性的单板为：

- ADRB、ADRI、CC0VASL、CC0SASL
- CSRI、CSRB
- EDTB、SDL/SDLE、TSSB、TSSC、DSLD/DSLE
- HW 转接板

软件支持

当自动升级过程中，需要从 FTP 服务器下载单板软件时，要求：

- 在 UA5000 上已成功配置下载单板软件所用的 FTP 服务器。

52.2.3 原理描述

介绍单板软件自动升级特性的原理。

单板软件自动升级前的准备流程如下：

1. 将产品所有的程序文件逐一扫描，生成版本配套表文件，将生成版本配套表文件和部分单板软件按照指定的格式封装成一个包文件；
2. 通过加载指令把该包文件加载到主控板，并写入到 FLASH 中；

单板软件自动升级的流程如下：

1. 单板软件自动加载：
   (1) 单板在程序软件启动阶段发起自动加载请求消息（如升级 BIOS 请求）；
   (2) 主控板接收到该消息后，根据版本比较情况，决定单板软件是否需要升级；
      - 当单板软件不需要升级时，主控板通知单板无需升级；
      - 当单板软件需要升级，且主控板 Flash 的软件包中包含所需的单板软件时，主控板直接向单板发送该单板软件；
      - 当单板软件需要升级，但主控板 Flash 的软件包中不包含所需的单板软件时，主控板从 FTP 定制加载服务器下载所需单板软件，并下发给对应单板；

(3) 单板接收完需要的软件资源文件，校验通过后保存至本板 FLASH 中。然后单板根据自己的需要确定是否向主机发送新的软件资源文件的升级请求，直至不再需要任何其他软件资源文件；

(4) 加载结束。

2. 复位单板软件，完成单板软件自动升级。

A 缩略语

A	Attachment Circuit	-
ACL	Access Control List	访问控制列表
ARP	Address Resolution Protocol	地址解析协议
AS	Autonomous System	自治系统
ABR	Area Border Router	区域边界路由器
ANU	Access Network Unit	接入网络单元
ASBR	Autonomous System Boundary Router	自治系统边界路由器
ATM	Asynchronous Transfer Mode	异步转移模式
ATU-C	ADSL transceiver unit,central office end	局端 ADSL 收发器
ATU-R	ADSL transceiver unit, remote end	ADSL 收发器远端终端用户
B		
BPDU	Bridge Protocol Data Unit	桥接协议数据单元
BRAS	Broadband Remote Access Server	宽带接入服务器
C		
CC	Continuity Check Message	连续性检查消息
CE	Customer Edge	-
CFM	Connectivity Fault Management	连接故障管理
CO	Central Office	中心局
CS	Calling Station	呼叫台
CSC	Cell Site Controller	小区控制器

CSPF	Constraint Shortest Path First	最短路径优先算法
D		
DLM	Dynamic Line Management	动态线路管理
DHCP	Dynamic Host Configuration Protocol	动态主机配置协议
DHCP Relay	Dynamic Host Configuration Protocol Relay	DHCP 中继
DHCP option82	DHCP relay agent option 82	DHCP 中继代理选项
DMT	Discrete Multi-Tone	离散多频音线路编码技术/离散多频调制
DSM	Dynamic Spectrum Management	动态频谱管理
E		
EPON	Ethernet Passive Optical Network	以太网无源光网络
F		
FEC	Forwarding Equivalence Class	转发等价类
FTTH	Fiber To The Home	光纤到户
FTTx	Fiber To The x	光纤到户/大楼等
G		
GPON	Gigabit-capable Passive Optical Network	G 比特无源光网络
H		
HDSL	High-speed digital subscriber line	高速数字用户线
I		
ICMP	Internet Control Message Protocol	因特网控制消息协议
IGMP	Internet Group Management Protocol	因特网组管理协议
IP	Internet Protocol	因特网协议
IPoA	Internet Protocol Over ATM	承载于 ATM 网的 IP 报文
IPoE	IP over Ethernet	承载于以太网的 IP 报文

L

LB	Loopback	环回
LT	Linktrace	链路跟踪
TLV	Type、Length、Value	类型、长度、值

M

MA	Maintenance Association	维护关联集
MEP	Maintenance association End Point	维护关联端点
MIP	Maintenance association Intermediate Point	维护关联中间结点
MPLS	Multi-Protocol Label Switch	多协议标记交换
MSTR	Multiple Spanning Tree Regions	多生成树域
MSTI	Multiple Spanning Tree Instance	多生成树实例
MTA	Multifunctional Terminal Adapter	多功能终端适配器

N

NTP	Network Time Protocol	网络时间协议

O

OAM	Operations Administration and Maintenance	操作管理维护
OSPF	Open Shortest Path First	开放最短路径优先
OLT	Optical Line Terminal	光线路终端
ONU	Optical Network Unit	光网络单元
ONT	Optical Network Terminal	光网络终端

P

P2P	Point To Point	点对点
PS	Personal Station	个人电台
PSTN	Public Switched Telephone Network	公共电话交换网
PVC	Permanent Virtual Channel	永久虚通路
PQ	Priority Queuing	优先队列
PTM	Packet Transfer Mode	分组传输模式
PBO	Power Back Off	功率反馈控制

PE	Provider Edge	-
PITP	Policy Information Transfer Protocol	策略信息传送协议
PPPoA	Point to Point Protocol over ATM Adaptation Layer 5	承载于 ATM 网的 PPP 报文
PPPoE	Point-to-Point Protocol over Ethernet	承载于以太网的 PPP 报文
PWE3	Pseudo wire Emulation Edge-to-Edge	-
PW	Pseudo wire	-
PVP	Permanent Virtual Path	永久虚通路
Q		
QinQ	802.1Q in 802.1Q	-
QoS	Quality of Service	服务质量
R		
RAIO	Relay Agent Information Option	中继代理信息选项
RIP	Routing Information Protocol	路由信息协议
RSTP	Rapid Spanning Tree Protocol	快速生成树协议
RRPP	Rapid Ring Protection Protocol	快速环网保护协议
RFI	Radio Frequency Interference	无线频率干扰
S		
SCS	Sub-rate Concentrating Switch	子速率集中交叉
SFTP	Secure File Transfer Protocol	安全文件传输协议
SHDSL	Single-line high speed digital subscriber line	单线对高速数字用户线
SNMP	Simple Network Management Protocol	简单网管协议
SPF	Shortest Path First	最短路径优先算法
SRX	Sub Rate Multiplexer	子速率复用
SSH	Secure Shell	安全外壳
STP	Spanning Tree Protocol	生成树协议
STU-C	SHDSL Transceiver Unit - Central Office end	SHDSL 局端收发单元
STU-R	SHDSL Transceiver Unit - Remote end	SHDSL 远端收发单元

T

TE	Traffic Engeering	流量工程
TEDB	TE DataBase	流量工程数据库
ToS	Type of Service	服务类型
TC-PAM	Trellis Coded Pulse Amplitude Modulation	格栅编码脉冲幅度调制

V

VLAN	Virtual LAN	虚拟局域网
VoIP	Voice over IP	基于 IP 的语音
VP	Virtual Path	虚通路
VBAS	Virtual Broadband Access Server	虚拟宽带接入服务器

W

WRR	Weighted Round Robin	加权循环调度队列

X

xDSL	x Digital Subscriber Line	各类数字用户线