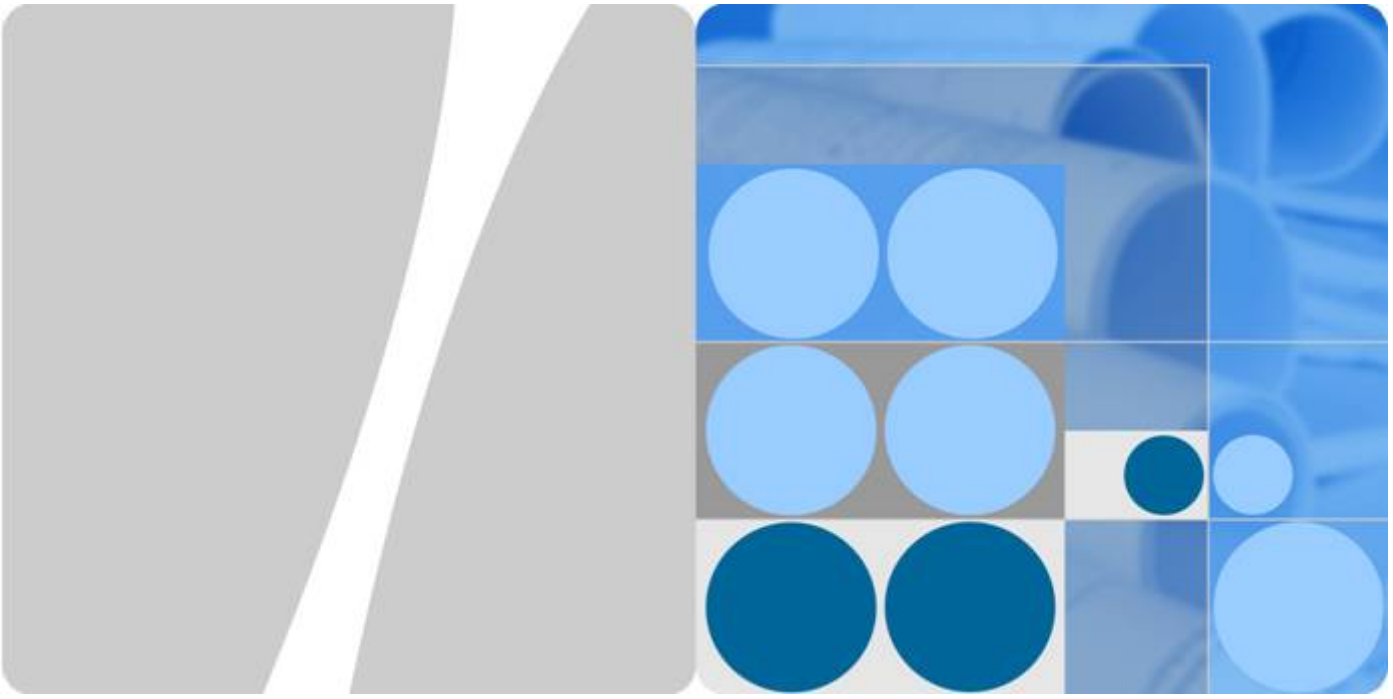


SmartAX MA5620/MA5626 远端光接入单元

V800R308C00

特性描述

文档版本　02

发布日期　2010-10-30

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： 0755-28560000 4008302118

客户服务传真： 0755-28560111

前 言

读者对象

本文档针对 MA5620/MA5626 的关键特性，分别详细介绍其子特性。

本文档能指导读者了解各类特性的定义、设备实现该特性的目的、设备对特性规格的支持情况以及与特性密切相关的参考资料，帮助读者全面了解特性，较深层次地理解各特性在 MDU 上的实现原理。

本文档（本指南）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 （2010-10-30）

相对于版本 01（2010-07-20）的变化如下：

优化了本文档的结构和内容。

文档版本 01 （2010-07-20）

第一次正式发布版本。

目 录

插图目录

表格目录

1 上行接口

关于本章

上行接口用于业务的上行，包含多个子特性。本章对其子特性分别加以介绍。

上行端口的三模自适应，即 MA5620/MA5626 设备可自动进行 GE/EPON/GPON 三种模式的适配。用户在整个适应过程中仅需插入相应的光模块并连接好光纤，整个模式的适应过程完全由设备自动完成。

EPON（Ethernet Passive Optical Network）上行是指上行口为 EPON 接口。通过 EPON 上行在一条光纤上传输汇聚的数据、视频和语音数据。

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（GPON Encapsulation Mode）功能，能够传输任何类型的数据。

1.1 介绍

MA5620/MA5626 通过上行接口进行业务上行，上行接口特性包含的子特性如表 1-1 所示：

表 1-1 上行接口子特性表

特性名称	特性简介
EPON	EPON（Ethernet Passive Optical Network）上行是指上行口为 EPON 接口。通过 EPON 上行在一条光纤上传输汇聚的数据、视频和语音数据。
GPON	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（GPON Encapsulation Mode）功能，能够传输任何类型的数据。
三模自适应	上行端口的三模自适应，即 MA5620/MA5626 设备可自动进行 GE/EPON/GPON 三种模式的适配。用户在整个适应过程中仅需插入相应的光模块并连接好光纤，整个模式的适应过程完全由设备自动完成。

1.2 参考标准与协议

上行特性各子特性对应的参考标准与协议如表 1-2 所示：

表 1-2 上行特性子特性参考标准与协议表

特性名称	参考标准与协议
EPON	● IEEE802.3ah 标准 ● 《中国电信 EPON 设备技术要求 V2.1》
GPON	● 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
三模自适应	无

1.3 可获得性

上行特性及其子特性能够正常使用需要的硬件和 License 支持情况如表 1-3 所示：

表 1-3 上行特性对应的硬件和 License 支持情况

特性名称	版本支持	License 支持
EPON	没有限制	无需 License 许可
GPON	没有限制	无需 License 许可
三模自适应	MA5620/MA5626V800R308C00 新开发硬件支持	无需 License 许可

1.4 三模自适应

上行端口的三模自适应，即 MA5620/MA5626 设备可自动进行 GE/EPON/GPON 三种模式的适配。用户在整个适应过程中仅需插入相应的光模块并连接好光纤，整个模式的适应过程完全由设备自动完成。

1.4.1 介绍

定义

上行端口的三模自适应，即 MA5620/MA5626 设备可自动进行 GE/EPON/GPON 三种模式 GE/EPON/GPON 多种模式的适配。用户在整个适应过程中仅需插入相应的光模块并连接好光纤，整个模式的适应过程完全由设备自动完成。

目的

实际组网应用中，为了适应不同的网络，需要更换不同的上行扣板硬件或不同上行设备，在用户 GE/EPON/GPON 三种模式进行混合建网的场景下，需要进行多种硬件的备货，安装和备件维修储备都非常复杂，通过 GE/EPON/GPON 三种模式自适应，可以有效的解决上面提到的问题。

受益

运营商受益

- 在 GE/EPON/GPON 三种模式上行混建的网络中，硬件可以统一备货、统一安装。
- 维修备件仅需一种，无需多种维修备件的储备。

1.4.2 规格

MA5620/MA5626 提供两个三模自适应的上行端口，两个上行端口可以适配成以下组合：

- GE+EPON
- GE+GPON

- GE+GE
- EPON+EPON
- GPON+GPON

1.4.3 原理描述

三模自适应使用华为最新的 ASIC 芯片实现的特性，该芯片中内置了 2 个 GE 接口的 MAC 地址，2 个 EPON 接口的 MAC 地址，2 个 GPON 接口的 MAC 地址。

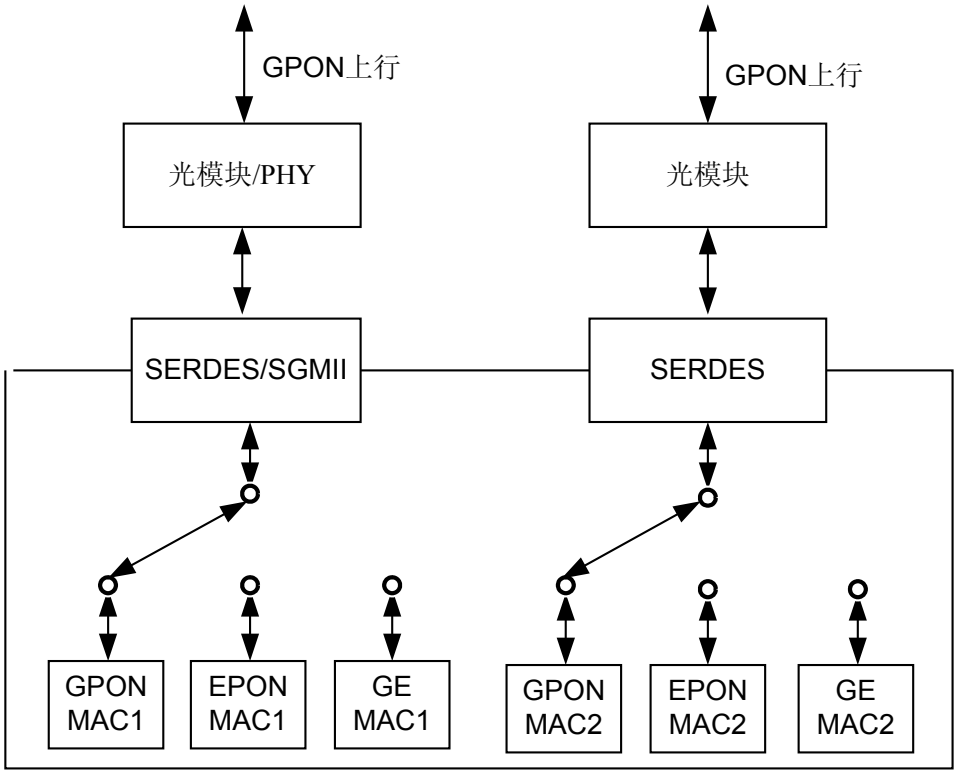
当扣板上行端口插入相应的光模块和光纤，上行端口状态由 DOWN 状态切换为 UP 状态后，芯片软件程序自动启动三模检测，对于 GE/EPON/GPON 三种模式自适应原理介绍如下。

GPON 模式

ASIC 芯片实现 GPON 上行原理

ASIC 芯片实现 GPON 上行原理如图 1-1 所示。

图 1-1 ASIC 芯片实现 GPON 上行原理图



软件自适应原理

如果 GPON MAC 可以同步（无 LOS/LOF），则认为是 GPON 线路。

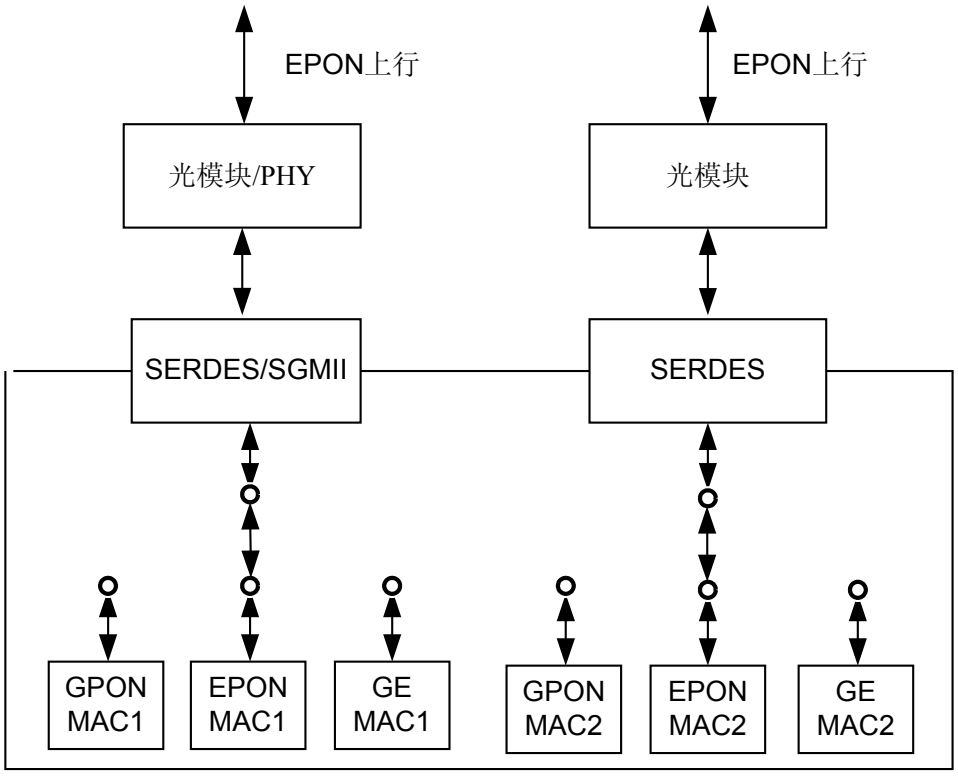
GPON 模式切换到 EPON 模式：GPON MAC 无法同步（有 LOS/LOF），则跳转到 EPON 模式。

EPON 模式

ASIC 芯片实现 EPON 上行原理

ASIC 芯片实现 EPON 上行原理如图 1-2 所示。

图 1-2 ASIC 芯片实现 EPON 上行原理图



软件自适应原理

EPON PCS 子层同步，且接收的正确帧数不断增加，CRC8 错帧不增加。则认为是 EPON 线路。

EPON 模式切换到 GPON 模式：EPON PCS 子层无法同步，则跳转到 GPON 模式。

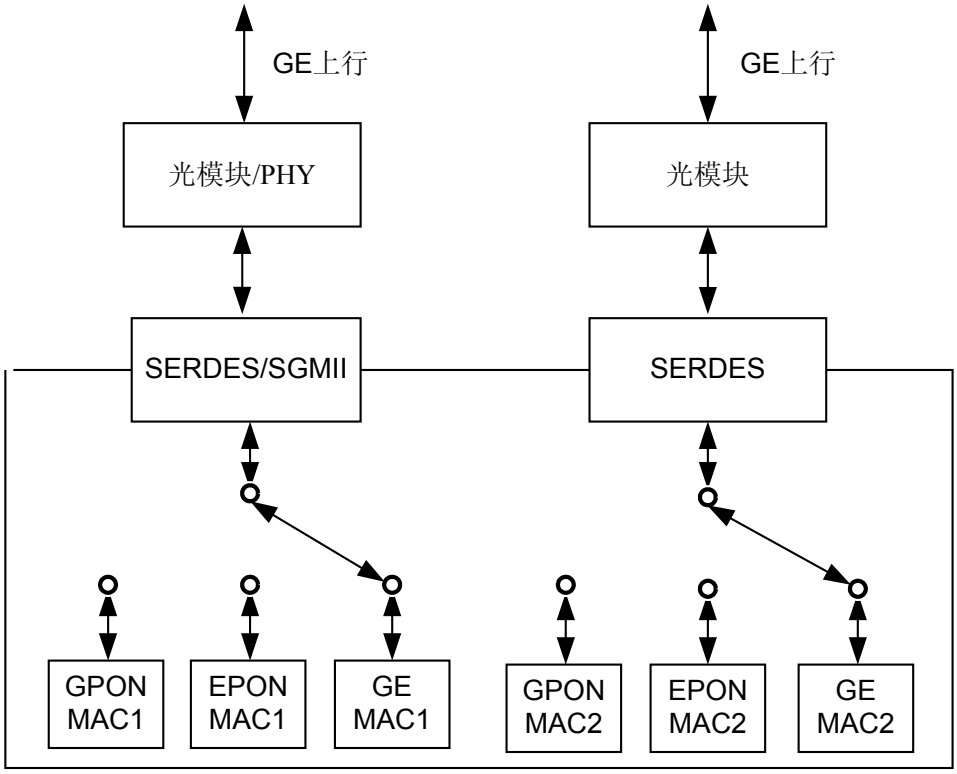
EPON 模式切换到 GE 模式：EPON PCS 子层可以同步，但正确帧数不增加，CRC8 错误帧数增加；或者正确帧数和 CRC8 错误帧数都不增加（GE 链路无数据的情况）。则跳转到 GE 模式。

GE 模式

ASIC 芯片实现 GE 上行原理

ASIC 芯片实现 GE 上行原理如图 1-3 所示。

图 1-3 ASIC 芯片实现 GE 上行原理图



软件自适应原理

GE 端口链路可以 UP，并且 FCS 没有错误，则认为是 GE 模式。

GE 模式切换到 EPON 模式：GE 端口链路可以 UP，能够接收到帧且接收到的帧全部 FCS 错误，则跳转到 EPON 模式。

GE 模式切换到 GPON 模式：GE 端口链路无法 UP，则跳转到 GPON 模式。

1.5 EPON

EPON（Ethernet Passive Optical Network）上行是指上行口为 EPON 接口。通过 EPON 上行在一条光纤上传输汇聚的数据、视频和语音数据。

1.5.1 介绍

定义

无源光网络（PON）技术是一种点到多点的光纤接入技术。一般其下行采用 TDM 广播方式、上行采用 TDMA（时分多址接入）方式。所谓“无源”，是指 ODN 中不含有任

何有源电子器件及电子电源，全部由光分路器（Splitter）等无源器件组成，因此其管理维护的成本较低。

EPON（Ethernet Passive Optical Network）是 PON 技术中的一种，由 IEEE802.3 EFM（Ethernet for the First Mile）提出。EPON 是一种采用点到多点（P2MP）网络结构、无源光纤传输方式、基于高速以太网平台和 TDM 时分 MAC 媒体访问控制方式、提供多种综合业务的宽带接入技术。

典型的 EPON 接入系统由三部分组成：

- OLT（Optical Line Terminal）系统
- ONU（Optical Network Unit）或 ONT（Optical Network Termination）
- ODN（Optical Distribution Network）

其中 ODN 起连接 OLT 和 ONU/ODN 的作用。

目的

MA5620/MA5626 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。

1.5.2 规格

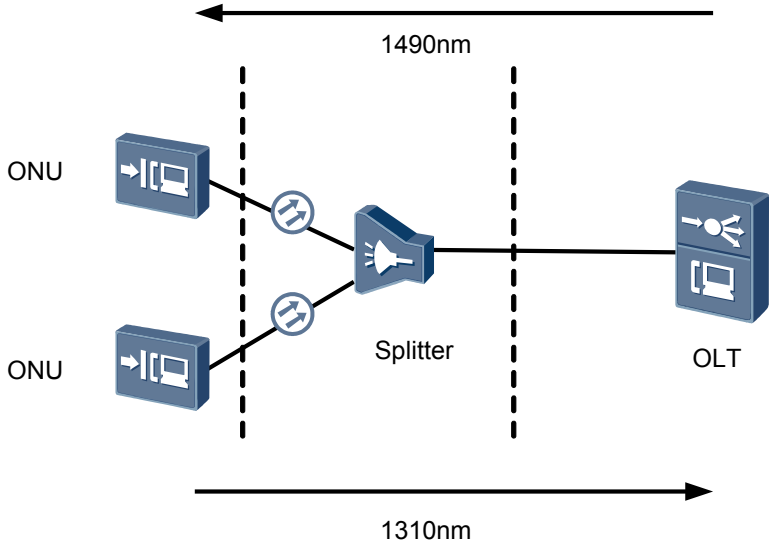
- 支持一个 EPON 上行端口，下行速率 1.25Gbit/s，上行速率 1.25Gbit/s。
- 支持最远 20km 的传输距离。
- EPON 光接口采用单模光模块，支持单纤双向的数据传输。
- 使用的光纤接头类型是 SC/PC。
- 支持 EPON 光模块长发光的检测和防护。
- 支持 EPON Type D 和 Type B 保护倒换。

1.5.3 原理描述

系统原理

EPON 标准是众多 TDM-PON 标准之一，具有 TDM-PON 网络的基本特征：树状拓扑网络由 OLT、ONU 和 ODN（Optical Distribution Network）三部分组成，ODN 又分为主干光纤、分光器、支路光纤等无源光部件，整体拓扑如图 1-4 所示：

图 1-4 EPON 网络物理拓扑图



EPON 采用单纤波分复用的光传输方式，遵从上行 1310nm、下行 1490nm 的波长分配，OLT 与 ONU/ONT 之间进行单纤双向数据传送。

为了分离同一根光纤上多个用户来去方向的信号，采用以下两种复用技术：

- 下行数据流采用广播技术，各 ONU 只接收属于自己的数据，传输速率是 1.25Gbit/s。
- 上行数据流采用 TDMA 技术，各 ONU 在分配的特定时隙内发送数据，传输速率 1.25Gbit/s。

EPON 遵循 CTC EPON 设备技术要求规范《中国电信 EPON 设计技术要求（V2.1）》。

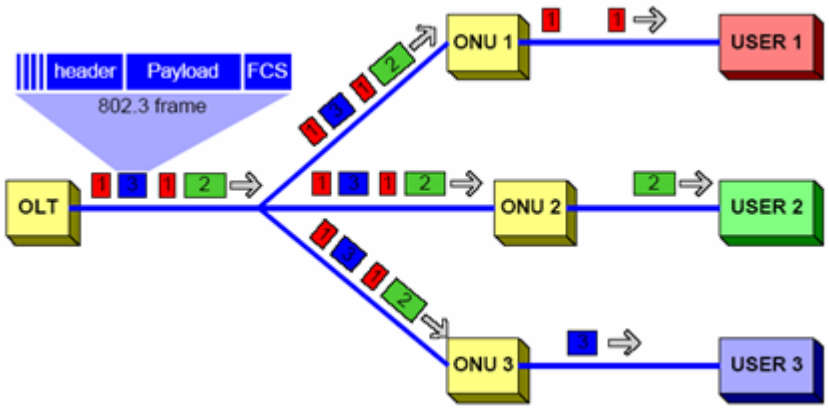
EPON 作为新型光接入技术，与传统的 xDSL 技术相比，不仅传输介质和带宽速率不相同，而且接入网络的管理维护模式也相应的发生变化。

工作原理

EPON 的下行传输

EPON 的下行数据（OLT 至 ONU）采用 802.3 帧格式进行广播，如图 1-5 所示。

图 1-5 EPON 下行传输

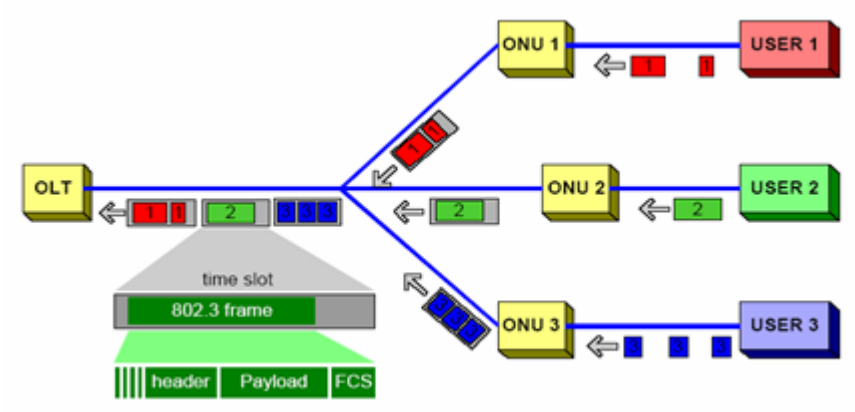


EPON 下行数据流采用广播技术，各 ONU 只接收属于自己的数据。

EPON 的上行传输

EPON 的上行数据流（ONU 至 OLT）采用 TDMA 技术，各 ONU 在分配的特定时隙内发送数据，如图 1-6 所示。

图 1-6 EPON 上行传输



ONU 在规定的时隙内发送以太网帧到 OLT，由 MPCP 协议完成上行数据流的管理。

EPON 关键技术

DBA

DBA（Dynamically Bandwidth Assignment 动态带宽分配），一种能在微秒或毫秒级的时间间隔内完成对上行带宽的动态分配的机制。

EPON 上行传输是多个 ONU 时分复用上行带宽，DBA 技术可以实现根据 ONU 上行突发流量需要，通过在 ONU 之间动态调整带宽提高了 EPON 上行带宽的有效性。

测距

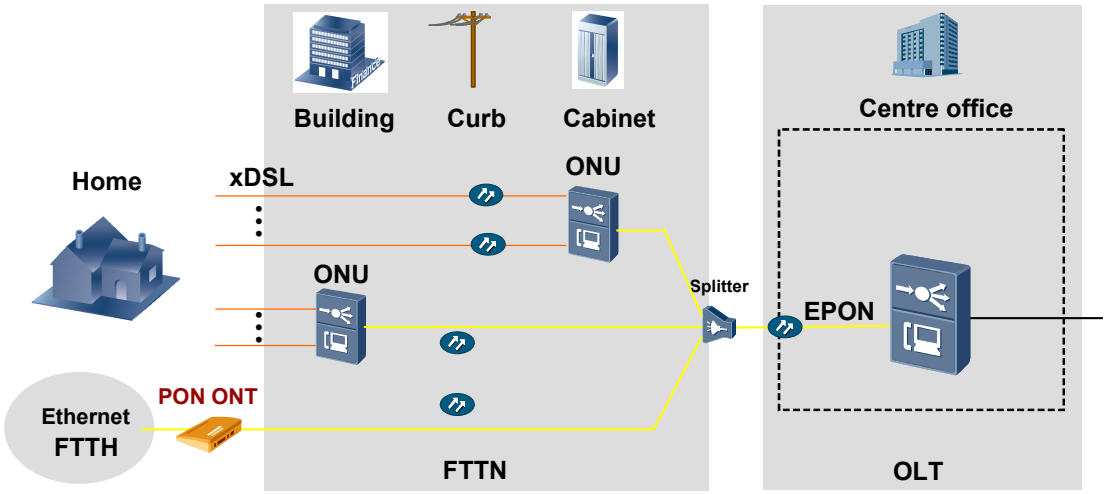
由于 EPON 上行数据流采用 TDMA 技术，各 ONU 在分配的特定时隙内发送数据，这样的话，ONU 会由于距离不通而产生一定的时延，造成到达 OLT 的数据冲突。

通过测距补偿因 ONU 距离不同而产生的时延差异，从而保证上行数据不会发生冲突。

EPON 组网应用

EPON 上行主要运用于 FTTx 组网中，如 FTTC、FTTB、FTTH，组网如图 1-7 所示。

图 1-7 FTTX 组网图



1.6 GPON

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（GPON Encapsulation Mode）功能，能够传输任何类型的数据。

1.6.1 介绍

定义

GPON 是一种点到多点（P2MP）结构的无源光网络。

典型的 GPON 接入系统由三部分组成：

- OLT（Optical Line Terminal）系统
- ONU（Optical Network Unit）或 ONT（Optical Network Termination）
- ODN（Optical Distribution Network）

其中 ODN 起连接 OLT 和 ONU/ODN 的作用。

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），下行速率可达 1.2Gbit/s 或 2.4Gbit/s，上行速率可达 155Mbit/s、622Mbit/s、1.2Gbit/s 或 2.4Gbit/s。

目的

GPON 采用无源光传输技术，主要应用在 FTTH（Fiber To The Home）、FTTB（Fiber To The Building）的环境中，支持语音、数据、视频、租用线路和分布式业务在内的多种业务。

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。

1.6.2 规格

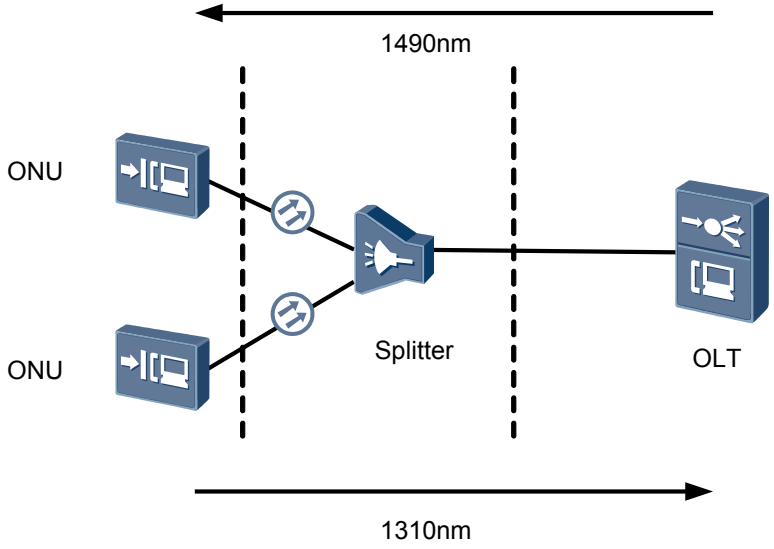
- GPON 接口支持 T-CONT Type1 ～ 5 类型：支持最多 32 个 T-CONT，Alloc-ID 范围 0~4095。T-CONT 最小分配带宽为 64kbit/s，最大为 1.2Gbit/s，最小粒度为 64kbit/s。
- GPON 接口支持最多 1024 个 GEM Port，GEM Port ID 范围是 0 ～ 1023。
- GPON 接口支持基于业务流的 VLAN ID、802.1p、VLAN ID+802.1p 到 GEM Port 的映射配置，其中 VLAN ID 支持全范围，业务流到 GEM Port 的映射无限制。
- GPON 接口每个 T-CONT 最多支持优先级队列无限制，支持 SP/SP+WRR/WRR 的调度方式，缺省为 SP。
- 支持 GPON 光模块长发光的检测和防护。
- 支持查询 GPON 光模块参数：温度、偏置电流、电压和接收光功率。
- 支持设置 GPON 光模块接收光功率告警上下限设置。
- 支持 PON Type B 保护。
- 当设备掉电后，支持通过 PLOAM/OMCI 消息上报 Dying Gasp 告警。
- 支持最大物理距离 20km，最大逻辑距离 60km。

1.6.3 原理描述

系统原理

GPON 系统原理结构如图 1-8 所示：

图 1-8 GPON 系统原理结构图



GPON 采用单纤波分复用的光传输方式，遵从 ITU-T G.984.2 规定的上行 1310nm、下行 1490nm 的波长分配，OLT 与 ONU 之间进行单纤双向数据传送。

为了分离同一根光纤上多个用户来去方向的信号，采用以下两种复用技术：

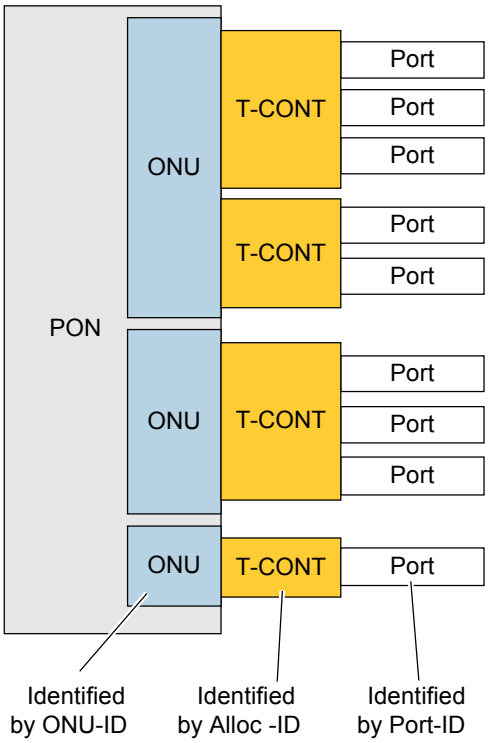
- 下行数据流采用广播技术，各 ONU 只接收属于自己的数据，传输速率是 2.4Gbit/s。
- 上行数据流采用 TDMA 技术，各 ONU 在分配的特定时隙内发送数据，传输速率 1.2Gbit/s。

工作原理

GPON 主要由物理层，TC 成帧子层，TC 封装适配层组成。

MA5620/MA5626 作为 ONU 应用时，上行到 OLT。OLT 和 ONU 之间传送 GPON GEM（G-PON Encapsulation Method）帧，GEM 帧通过 GEM Port-ID 标识，上行方向由 T-CONT 承载，如图 1-9 所示。

图 1-9 GPON 复用结构（GEM 方式）



T-CONT

GPON 使用 T-CONT 实现业务汇聚，T-CONT 是 GPON 系统中上行业务流最基本的控制单元。

一个 T-CONT 对应一种带宽类型的业务流。每种带宽类型有自己的 QoS 特征，QoS 特征主要体现在带宽保证上，分为固定带宽，保证带宽，保证/非保证带宽，尽力转发，混合方式（对应表 1-4 的 Type1 到 Type5）。

表 1-4 可用 T-CONT 类型

带宽类别	延迟敏感	分配方式	T-CONT 类型				
			Type 1	Type 2	Type 3	Type 4	Type 5
Fixed	Yes	Provisioned	Yes	No	No	No	Yes
Assured	No	Provisioned	No	Yes	Yes	No	Yes
Non-assured	No	Dynamic	No	No	Yes	No	Yes
Best-effort	No	Dynamic	No	No	No	Yes	Yes

每个 T-CONT 由 Alloc-ID 来唯一标识，Alloc-ID 的范围为 0 ～ 4095。Alloc-ID 由 OLT 进行全局分配，即 OLT 下的每个 ONU 不能使用 Alloc-ID 重复的 T-CONT。

GEM Port

每个 T-CONT 由一个或者多个 GEM Port 组成，每个 GEM Port 承载一种业务流。一个 T-CONT 可以承载一个或者多个 GEM Port 的不同业务流。

每个 GEM Port 由一个唯一的 Port-ID 来标识，Port-ID 的范围为 0 ～ 4095，并且由 OLT 进行全局分配，即 OLT 下的每个 ONU 不能使用 Port-ID 重复的 GEM Port。

GEM Port 标识的是 OLT 和 ONU 之间的业务虚通道，即承载业务流的通道，类似于 ATM 虚连接中的 VPI/VCI 标识。

GPON 的下行传输

采用 2.488Gbit/s 下行速率，下行帧长为 38880 bytes，每 125us 一帧。如图 1-10，图 1-11 所示。

图 1-10 GPON 下行帧结构

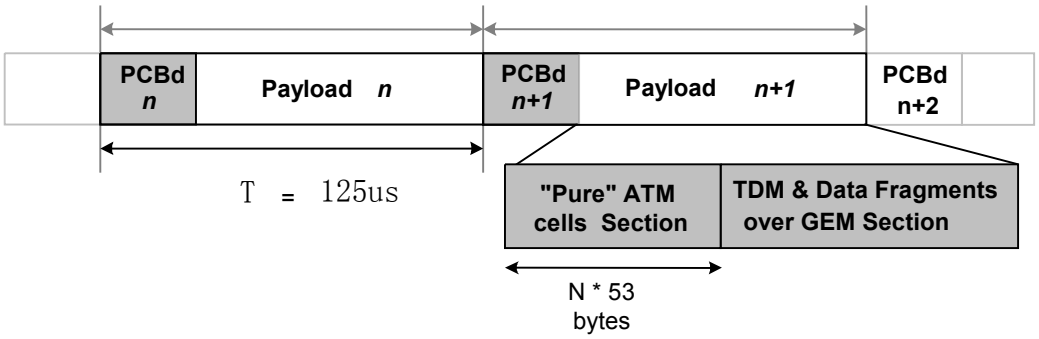
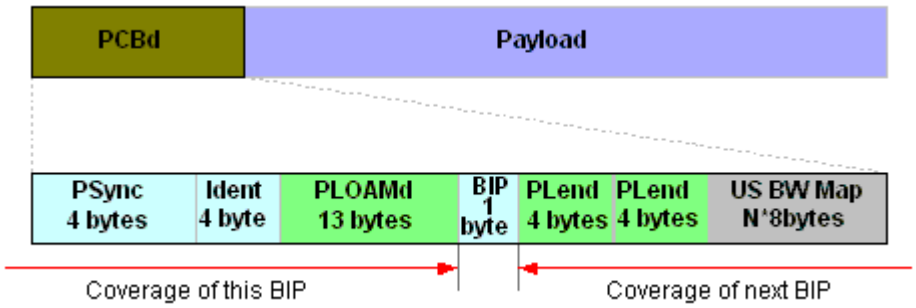


图 1-11 PCBd 结构



OLT 以广播的方式向 ONU 发送 PCBd，每个 ONU 都会收到整个 PCBd，然后会根据相关的信息执行动作。

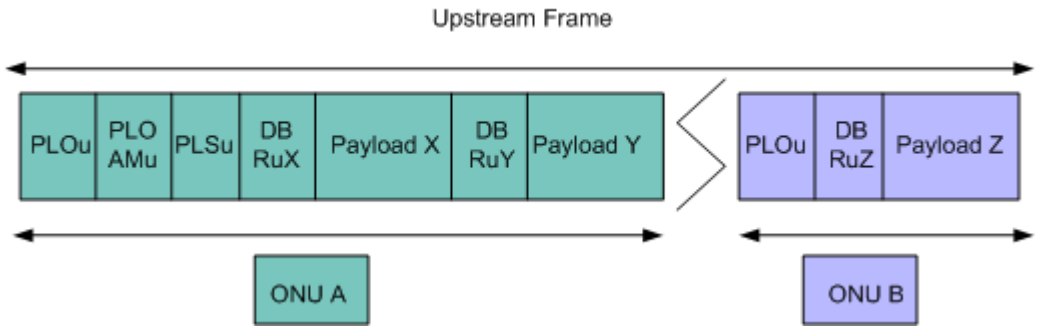
PCBd 里包含：帧同步信息，物理层 OAM，BIP 校验字段等等。其中 US BW Map（上行带宽映射）是 OLT 发送给每个 T-CONT 的各自的上行传输带宽映射。这正是通过下行帧的 PCBd 里的带宽映射字段来完成。从而实现 MAC 控制功能。

由于 GPON 上行方向采用时分复用，如果多个 ONU 同一时刻发送上行数据，则会产生冲突。GPON 里使用的机制是 OLT 在下行帧里通告，每个 ONU 所能使用的上行传输时隙。

GPON 的上行传输

各个 GPON 速率下上下行帧长度都相同。每个上行帧包含了一个或者多个 T-CONT 传送的内容。而下行帧里的 BWmap 标识了各个 T-CONT 传送的起止时刻。如图 1-12 所示。

图 1-12 GPON 上行帧结构



每次一个 ONU 从另一个 ONU 那里接过 PON 的媒介访问权时，它都必须先发送一份 PLOu 数据。如果一个 ONU 分配了两个连续的 Alloc－ID（即一个的结束时间比另一个的开始时间小 1），则 ONU 应该抑止发送第二个 Alloc－ID 的 PLOu 数据。上行帧净荷区段可能包含三种内容:ATM 信元；GEM 帧；DBA 报告。

GPON 的激活

GPON 里激活过程由 OLT 控制。ONU 根据 OLT 发出的消息进行响应。

激活过程概括如下：

- ONU 根据 OLT 的需求调节发送光功率级别。
- OLT 发现一个新 ONU 的序列号。
- OLT 分配一个 ONU-ID 给 ONU。
- OLT 测量从 ONU 发来的上行数据的相位。
- OLT 通知 ONU 补偿延时时间。
- ONU 根据通报值调节发送相位。

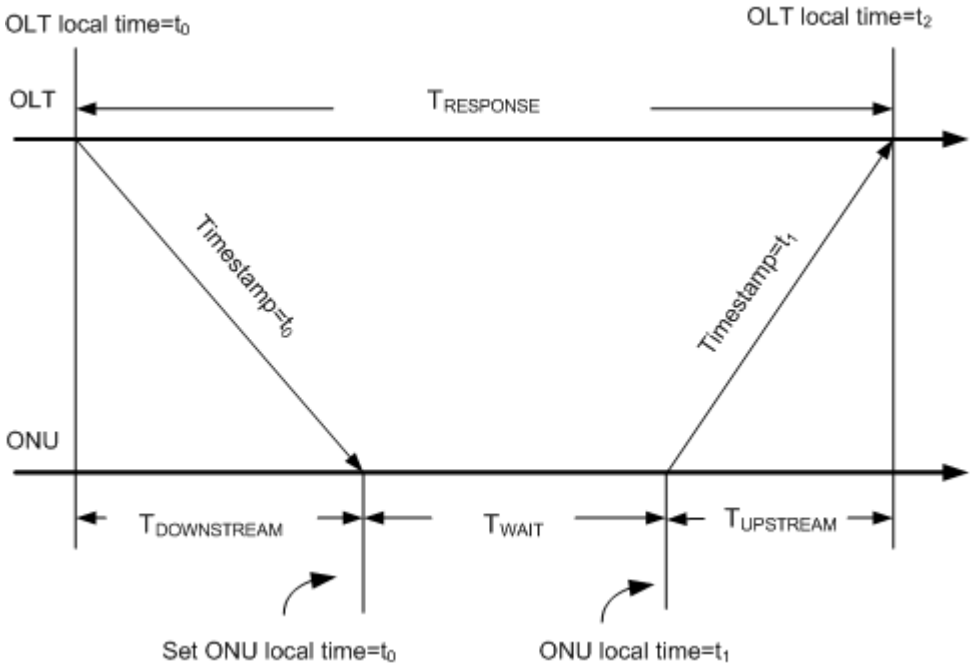
GPON 的测距方法

为了让所有 ONU 逻辑上与 OLT 的距离相同，使 ONU 的上行传输相位能够真正与分配的时隙相符。所有 ONU 在传输时都必须进行时延补偿，这是通过测距来完成的。

测距的方法如下：如图 1-13 所示。

- 基本公式为：EqD(n) = Teqd － Rtd(n) 其中 Teqd 为固定值，是指该 GPON 系统可能的最大时延（比如最大 OLT,ONU 距离为 20km,则 Teqd 为 200 ＋ 50 ＝ 250us），而 RTD 是 OLT 测量出的每个 ONU 的往返传输时延。
- 为了测量 RTD，OLT 会发送一个测距请求消息给 ONU，ONU 再响应该消息。
- RTD 的时间是：从传输下行测距请求消息的第一个比特或者字节到接收到的测距响应消息的最后一个比特或者字节之间的时间。

图 1-13 GPON 测距方法



- $T_{DOWNSTREAM}$= 下行传输时延
- $T_{UPSTREAM}$= 上行传输时延
- T_{WAIT}= ONU 处的等待时间 = t1 - t0
- $T_{RESPONSE}$= OLT 的响应时间 = t2 - t0
- Rtd = $T_{DOWNSTREAM}$ + $T_{UPSTREAM}$= $T_{RESPONSE}$ - T_{WAIT} = (t2 - t0) - (t1 - t0) = t2 - t1

1.7 术语与缩略语

术语

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。
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。
GEM Port	每个 T-CONT 由一个或者多个 GEM Port 组成，每个 GEM Port 承载一种业务流。一个 T-CONT 可以承载一个或者多个 GEM Port 的不同业务流。 每个 GEM Port 由一个唯一的 Port-ID 来标识，Port-ID 的范围为 0 ～ 4095，并且由 OLT 进行全局分配，即 OLT 下的每个 ONU 不能使用 Port-ID 重复的 GEM Port。 GEM Port 标识的是 OLT 和 ONU 之间的业务虚通道，即承载业务流的通道，类似于 ATM 虚连接中的 VPI/VCI 标识。

缩略语

缩略语	全称
EPON	Ethernet Passive Optical Network（以太网无源光网络）

缩略语	全称
GPON	Gigabit-capable Passive Optical Network（千兆比特无源光网络）
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）
GEM	GPON Encapsulation Mode（GPON 封装模式）
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）

2 二层

关于本章

宽带二层特性是对链路层协议的管理，包含多个子特性。本章将对其子特性分别加以介绍。

2.1 介绍

MA5620/MA5626 提供的宽带二层特性如表 2-1 所示：

表 2-1 宽带二层特性

特性名称	特性简介
MAC 地址管理	MAC 地址管理是二层管理的一项基本功能，包括 MAC 地址老化设置，限制动态 MAC 地址学习数和静态 MAC 地址设置。
Flow Bundle	Flow Bundle 是一个基本的二层管理特性，通过在转发面上引入对 COS（Class of Service 服务等级）的识别，扩展了数据在 MA5620/MA5626 设备内的转发策略，对普通的 VLAN + MAC 和 SVLAN + CVLAN 转发策略进行有效扩展，提高了运营商在业务规划方面的灵活性。
VLAN 管理	VLAN（Virtual Local Area Network）即虚拟局域网，是一种通过将局域网内的设备逻辑地而不是物理地划分成一个个网段，从而实现虚拟工作组的技术，VLAN 管理可以使运营商灵活的规划业务。
VLAN 切换策略	VLAN 切换是指从用户侧 VLAN 到网络侧 VLAN 的变换，灵活的 VLAN 切换策略能够使运营商更加容易的规划网络。
二层转发策略	报文在二层设备上转发一般是根据报文的 VLAN 信息和 MAC 地址进行转发。即：VLAN ＋ MAC 转发。MDU 支持报文根据 VLAN 进行转发，即 SVLAN ＋ CVLAN 转发。
Native TDM	Native TDM 是通过 TDMoGEM 方式将 TDM 帧直接封装到 GPON 的 GEM 帧中，这种方式封装简单，网络开销小，而且链路质量比较好保证。

2.2 参考标准和协议

二层特性以及子特性对应的参考标准与协议如表 2-2 所示：

表 2-2 二层特性以及子特性参考标准与协议

特性名称	参考标准与协议
MAC 地址管理	无
Flow Bundle	TR-101

特性名称	参考标准与协议
VLAN 管理	● 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 ● RFC3069：VLAN Aggregation for Efficient IP Address Allocation
VLAN 切换策略	无
二层转发策略	无
Native TDM	● ITU-T G.984.1 General characteristics for Gigabit-capable Passive Optical Networks (GPON) ● 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 ● ITU-T G.984.4 Gigabit-capable Passive Optical Networks (GPON): ONT management and control interface specification

2.3 可获得性

宽带二层特性能够正常使用需要的支持情况如表 2-3 所示：

表 2-3 宽带二层特性对应的 License 支持情况

特性名称	License 支持
MAC 地址管理	无需 License 许可即可正常使用。
Flow Bundle	无需 License 许可即可正常使用。
VLAN 管理	在 VLAN Stacking 授权状态为允许时，才可以修改 vlan 属性为 Stacking。
VLAN 切换策略	无需 License 许可即可正常使用。
二层转发策略	无需 License 许可即可正常使用。
Native TDM	无需 License 许可即可正常使用。

2.4 MAC 地址管理

MAC 地址管理是二层管理的一项基本功能，包括 MAC 地址老化设置，限制动态 MAC 地址学习数和静态 MAC 地址设置。

2.4.1 介绍

定义

MAC 地址管理是二层管理的一项基本功能，包括 MAC 地址老化设置，限制动态 MAC 地址学习数和静态 MAC 地址设置。

目的

- MAC 地址老化设置

  成功配置 MAC 地址老化时间后，系统定时检查老化的动态 MAC 地址，如果在老化时间的 0.75 ～ 1 倍时长范围内没有发送/接收任何携带该源 MAC 地址的报文，对应的 MAC 地址就会从 MAC 地址表中删除。
- 限制动态 MAC 地址学习数

  端口的动态 MAC 地址学习数支持手工设置。当学习到的 MAC 地址达到配置的最大动态 MAC 地址学习数后，用户端口不再对新 MAC 地址进行学习。
- 静态 MAC 地址设置

  需要在端口接入某指定 MAC 地址的设备时，MDU 直接根据静态 MAC 进行数据转发。

受益

运营商受益

- 限制动态 MAC 地址学习数可以限制进入网络的 MAC 地址数量，减少网络设备的负担。
- 静态 MAC 地址设置可以防止 MAC 地址漂移。

用户受益

设置业务端口的静态 MAC 地址后，如果同时设置动态 MAC 最大学习数为 0，则端口只接收已配置的静态 MAC 的用户数据，实现 MAC 地址绑定功能。这样能够提高用户的安全性。

2.4.2 规格

本特性的相关规格如下：

- 系统 MAC 地址学习数为 4K。
- 系统支持设置静态 MAC 地址的最大数为：1024 个。
- 支持动态 MAC 地址老化时间设置（10s ～ 1000000s）。
- 支持 MAC 动态、静态 MAC 地址查询。
- 支持设置业务虚端口的最大 MAC 地址学习数（默认不限制）。
- 支持查询属于特定业务虚端口的 MAC 地址的信息。
- 支持根据 MAC 地址定位端口功能。

2.4.3 原理描述

MAC 地址老化设置

- 设置老化时间太短会造成动态 MAC 地址过早地被删除。当设备收到未知目的地址的数据包时，将广播这个数据包到同一 VLAN 内的所有端口。这种不必要的广播会影响运行性能。
- 设置过长的老化时间会导致设备无法根据网络的变化更新地址表，新的 MAC 地址学习不到，造成报文找不到目的地址而被广播。
- 动态 MAC 地址定期老化可以释放 MAC 地址表资源，避免学习不到新的 MAC 地址。
- 配置的老化时间只对动态 MAC 地址起作用，对静态 MAC 地址表项不起作用。

限制 MAC 地址学习数

- 业务通道最大的动态 MAC 地址学习数，不影响手工添加的静态 MAC 地址个数。
- 设置用户端口的静态 MAC 地址后，如果同时设置动态 MAC 最大学习数为 0，则端口只接收已配置的静态 MAC 的用户数据，实现 MAC 地址绑定功能。

静态 MAC 地址设置

- 对指定业务流或对包含在指定 VLAN 中的上行端口增加静态 MAC 地址时，如果该业务通道或上行端口已经存在相同的动态 MAC 地址，系统将会覆盖原有的动态 MAC 地址；如果存在相同的静态 MAC 地址，则配置不成功。
- 静态配置的 MAC 地址不要包含在已配置的 MAC 地址池中。在配置静态 MAC 地址表项之前，可以通过 display mac-pool 这个命令来查看 MAC 地址池中是否包含欲配置的静态 MAC 地址。
- 包含在不同 VLAN 中的同一个上行端口可以配置相同的静态 MAC 地址。
- 系统只支持增加单播 MAC 地址，且增加的 MAC 地址不能为系统的 MAC 地址。
- 删除 MAC 地址时，既可以删除静态 MAC 地址，又可以删除动态 MAC 地址。

2.5 Flow Bundle

Flow Bundle 是一个基本的二层管理特性，通过在转发面上引入对 COS（Class of Service 服务等级）的识别，扩展了数据在 MA5620/MA5626 设备内的转发策略，对普通的 VLAN + MAC 和 SVLAN + CVLAN 转发策略进行有效扩展，提高了运营商在业务规划方面的灵活性。

2.5.1 介绍

定义

Flow Bundle 是一个基本的二层管理特性，是普通的 VLAN + MAC 和 SVLAN + CVLAN 转发策略的有效扩展。

目的

Flow Bundle 通过在转发面上引入对 COS 的识别，扩展了数据在 ONU 设备内的转发策略，在原来 VLAN + MAC 和 SVLAN + CVLAN 转发的基础上，细分出 VLAN + MAC + COS、SVLAN + CVLAN + COS 等转发策略。主要应用于如下场景：

- VLAN 汇聚的场景，如 N:1 VLAN。

受益

运营商受益：

通过在转发面上引入对 COS 的识别，扩展了数据在 MA5620/MA5626 设备内的转发策略，对普通的 VLAN + MAC 和 SVLAN + CVLAN 转发策略进行有效扩展，提高了运营商在业务规划方面的灵活性。

2.5.2 规格

MA5620/MA5626 的 Flow Bundle 规格如下：

- 支持每个用户端口一个 Flow Bundle ID，无需用户手动创建。
- 支持创建业务流时指定 Flow Bundle 参数。

2.5.3 原理描述

Flow Bundle 通过在转发面上引入对 COS 的识别，扩展了数据在 MA5620/MA5626 设备内的转发策略，在原来 VLAN + MAC 和 SVLAN + CVLAN 转发的基础上，细分出 VLAN + MAC + COS、SVLAN + CVLAN + COS 等转发策略。

对网络设备的假设

Flow Bundle 实现基于 COS 的转发，依赖于上层网络设备送往接入设备的报文携带正确的 COS 值，即在 AN 上对某一业务定义了其 COS 值，要求上层网络设备与之一致。

也就是说，在接入设备仅实现二层硬件转发的情况下，Service Flow Bundle 模型要求同一个用户的数据报文和控制报文要么携带相同的优先级（走相的业务流），要么携带不同的优先级（走不同的业务流），否则可能无法正确转发。

如果接入设备的 CPU 参与某些协议报文的交互，则可以根据业务流进行记录和转发，下行同一条业务流上的协议报文，控制报文携带的优先级不一定要和数据报文携带的优先级一致。

Flow Bundle 的基本原理

上行方向的业务

MA5620/MA5626 设备某用户端口下的多条业务流，通过 Flow Bundle 汇聚到一个 VLAN 上行，并从用户端口学习到的 ARL 表中获得 Flow Bundle 标识。

说明

如果转发策略为 SVLAN + CVLAN 转发模式，则静态配置 ARL 表。

下行方向的业务

下行业务流根据 SVLAN + SMAC/S + C 查找到用户端口，再通过 Flow Bundle 表，根据 COS 值查找到业务流并进行转发。

2.6 VLAN 管理

VLAN（Virtual Local Area Network）即虚拟局域网，是一种通过将局域网内的设备逻辑地而不是物理地划分成一个个网段，从而实现虚拟工作组的技术，VLAN 管理可以使运营商灵活的规划业务。

2.6.1 介绍

定义

VLAN（Virtual Local Area Network）即虚拟局域网，是一种通过将局域网内的设备逻辑地而不是物理地划分成一个个网段，从而实现虚拟工作组的技术。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
  - Standard VLAN 中的各个端口是互通的标准以太网口，各个端口在逻辑上是对等的。
  - 相同 Standard VLAN 里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。
- Smart VLAN
  - 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。
- MUX VLAN
  - 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。
  - 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。
- VLAN 模板配置
  - 在 VLAN 模板中设置防 MAC spoofing，BPDU 透传，Rip 透传，VTP-CDP 透传，OSPF 透传，DHCP option82，PITP 设置，报文的二层转发模式，VMAC 等。
  - 将 VLAN 与模板绑定，VLAN 内业务的配置生效。VLAN 的模板配置起到了简化配置的作用。
- QinQ VLAN
  - QinQ VLAN 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。

- 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 专线业务，在一定程度上拓展私网的地域广度。

- VLAN Stacking

  VLAN Stacking 是对 802.1Q 标识的堆叠。为 Untagged 的用户报文添加两层 802.1Q 格式的 VLAN Tag，或将 Tagged 的用户报文切换成两层 802.1Q 格式的报文。报文带着两层 VLAN Tag 穿越服务商的骨干网络，到达 BRAS 使用双层 VLAN 进行认证，或者到 BRAS 设备后剥离外层 VLAN，而根据内层标签来标识用户。

目的

Standard VLAN 主要用于级联。MDU 产品支持以太网级联组网，多级接入设备间可以通过 GE/FE 接口实现级联，有效延长网络覆盖距离，并可以满足用户容量比较大的场合的需求。

Smart VLAN 主要用于减少对系统 VLAN 数量的占用和隔离用户。

QinQ VLAN 主要用于实现私网 VLAN 在公网透传，达到二层 VPN 的应用效果。

VLAN Stacking 可以标识用户和业务。另一方面，有些 BRAS 设备需要对双层 VLAN 进行认证。所以要求上行到 BRAS 的报文带双层 VLAN，这种情况需要设备支持 VLAN Stacking。

受益

运营商受益

VLAN 管理给运营商都带来了明显的收益：

- VLAN 管理可以使运营商灵活的规划业务。

2.6.2 规格

VLAN 管理特性的相关规格如下：

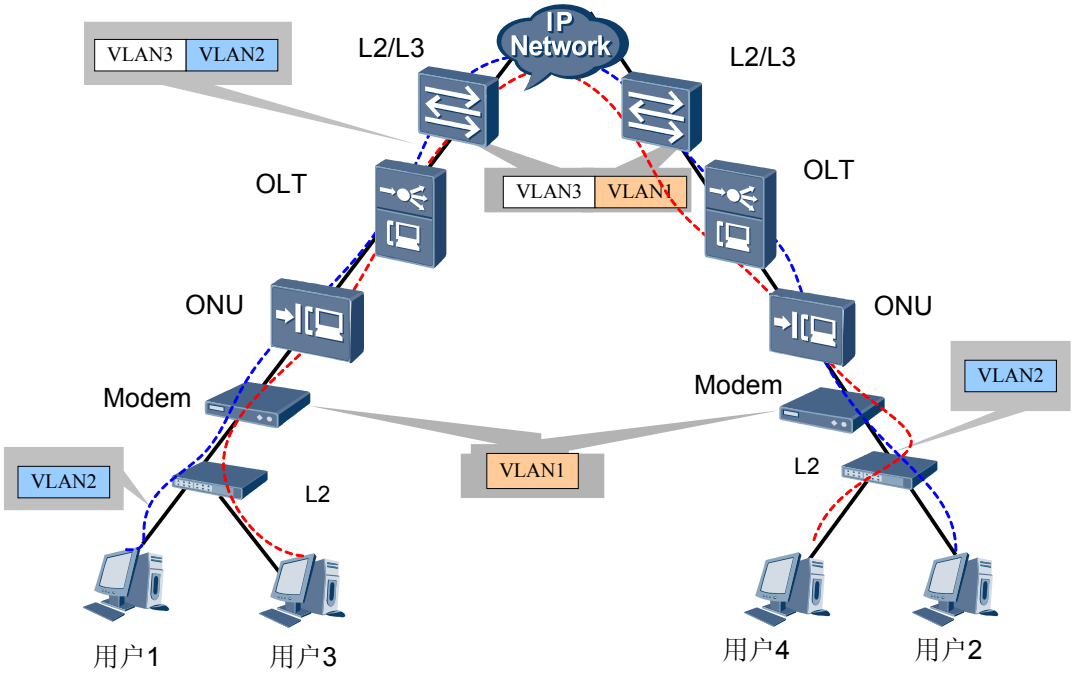
- 支持 Smart VLAN，MUX VLAN 和 standard VLAN。
- 支持 4000 个 VLAN。
- 系统支持基于端口划分的 VLAN。
- 支持 QinQ、Stacking VLAN。

2.6.3 原理描述

QinQ VLAN

QinQ VLAN 的业务处理过程如图 2-1 所示。

图 2-1 QinQ 业务示意图



MDU 通过 QinQ VLAN 可以在不同地域间的同一私网（VLAN1 或 VLAN2）内实现用户之间的互连。用户业务报文的处理过程如下：

1. PC 用户上行发送 Untagged 报文。
2. 二层 LAN Switch 为该报文加上 PC 用户在私网中的 VLAN Tag（VLAN1 或 VLAN2），并上行发送到 MDU。
3. MDU 为报文统一加上公网 VLAN Tag（VLAN3），并继续传送到上层网络。
4. 上层网络设备根据公网 VLAN Tag（VLAN3）传送报文。
5. 对端的 MDU 接收到这些报文后，剥离其公网 VLAN Tag（VLAN3），并将其传给同侧的 LAN Switch。
6. LAN Switch 识别并剥离私网 VLAN Tag（VLAN1 或 VLAN2），将 Utagged 报文转发给该私网 VLAN 中的用户。

   如上所述，通过 QinQ VLAN 即可实现了 VLAN1 内用户 1 和用户 2 之间的互通，或者 VLAN2 内用户 3 和用户 4 之间的互通。

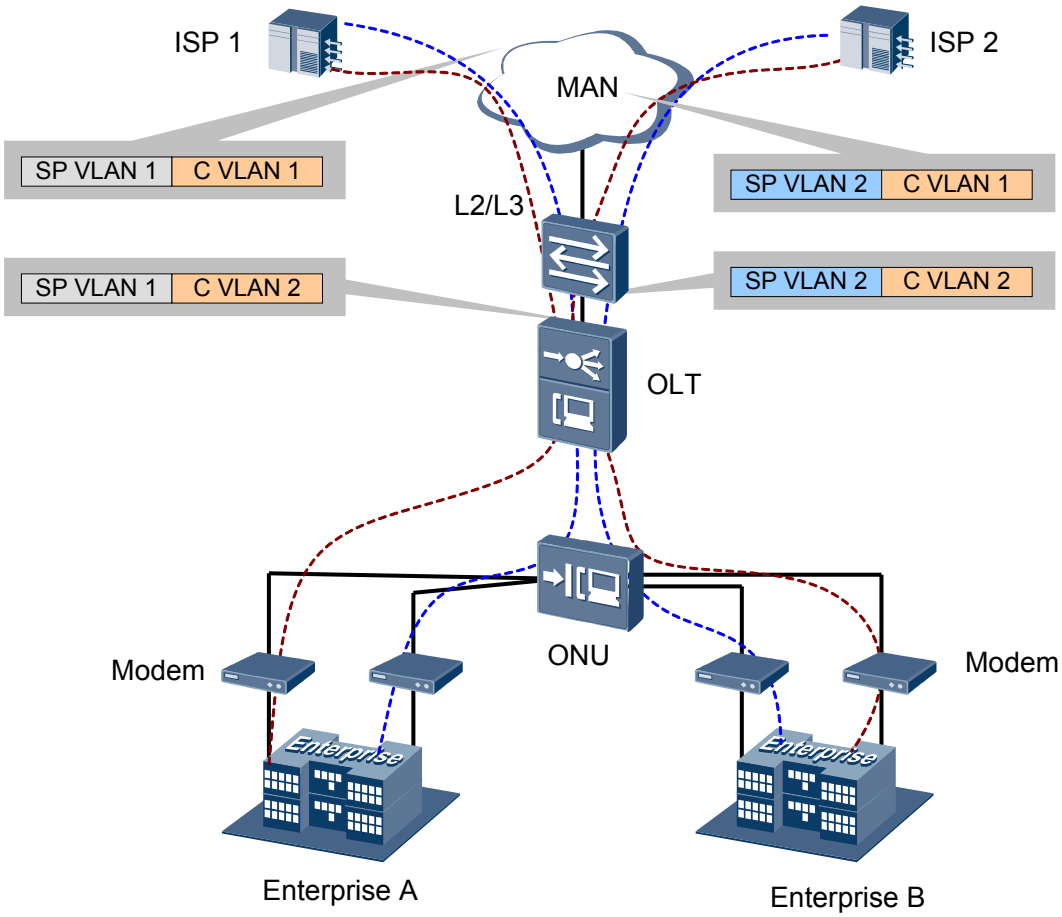
Stacking VLAN

如果 VLAN Stacking 应用于 VLAN 数目的扩展或标识用户，则需要 BRAS 配合实现。

如果 VLAN Stacking 用于提供专线批发业务，则要求上层网络工作于二层模式，直接根据 VLAN 和 MAC 转发。

MDU 实现的 VLAN Stacking 业务处理过程如图 2-2 所示。

图 2-2 Stacking 业务示意图



MDU 产品通过不同 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. 用户上行发送 Untagged 报文，经过 Modem 后到达 MDU。
2. MDU 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 Customer VLAN。
   - 企业 B 的用户报文外层统一封装 SP VLAN2，内层封装对应的 Customer VLAN。
3. 交换城域网设备根据 SP VLAN 转发报文到不同的 ISP。
4. ISP1 和 ISP2 设备接收到报文后剥离 SP VLAN，根据内层标签区分企业内的不同类用户。

2.7 VLAN 切换策略

VLAN 切换是指从用户侧 VLAN 到网络侧 VLAN 的变换，灵活的 VLAN 切换策略能够使运营商更加容易的规划网络。

2.7.1 介绍

定义

VLAN 切换是指从用户侧 VLAN 到网络侧 VLAN 的变换。

目的

VLAN 的规划是网络规划的一部分。灵活的 VLAN 切换策略能够使运营商更加容易的规划网络，用 VLAN 对用户或者业务加以标识，标识方法更加灵活。

受益

运营商受益

提高了运营商在业务规划方面的灵活性。

2.7.2 规格

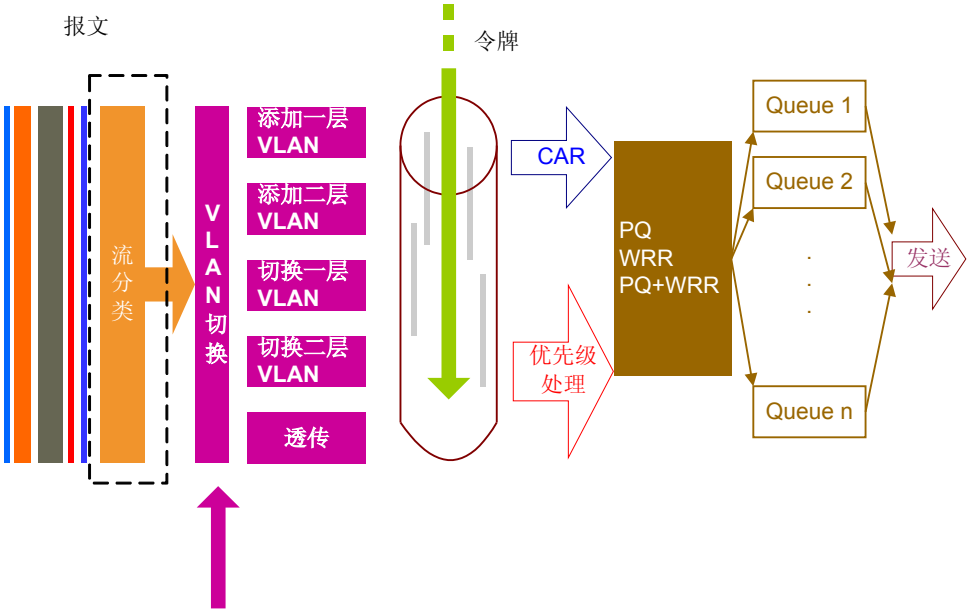
VLAN 切换特性的相关规格如下：

- 支持添加一层 VLAN。
- 支持添加两层 VLAN。
- 支持切换一层 VLAN。
- 支持透传 VLAN。
- 支持 N：1VLAN 切换。
- 支持用户带 VLAN tag 报文进行 1:1VLAN 切换。

2.7.3 原理描述

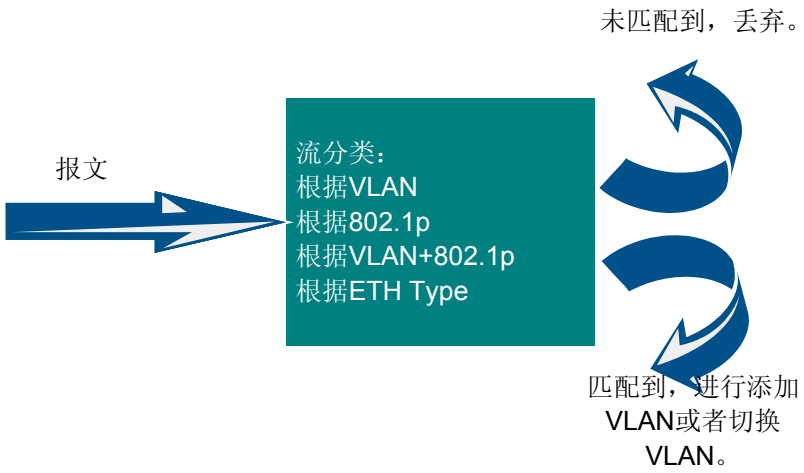
请参考**图 2-3**，报文进行流分类后需要进行 VLAN 切换。

图 2-3 MDU 中 QoS 处理整体模型-VLAN 切换



当报文被某一条流规则匹配到之后，设备会根据规则对报文进行添加 VLAN 或者切换 VLAN。如果报文没有匹配到流规则，那么此报文将被丢弃。如图 2-4 所示。

图 2-4 报文匹配



多业务流 VLAN 切换策略如表 2-4 所示。

表 2-4 多业务流 VLAN 切换策略

VLAN 类型	流类型	上行报文是否带 Tag	报文如何处理
QinQ	other-all	tag	打一层 SVLAN

VLAN 类型	流类型	上行报文是否带 Tag	报文如何处理
		untag	打一层 SVLAN
	user-8021p	tag	报文 tag 优先级 =user-802.1p，打一层 tag
		untag	丢弃
	user-vlan(tag)	tag	报文 tag=uservlan，则打一层 SVLAN，不相等则丢弃。
		untag	打一层 SVLAN
	user-vlan(untag)	tag	丢弃
		untag	打一层 SVLAN
	user encap(ipoe/pppoe)	tag	报文业务类型=配置的报文封装类型，则打一层 SVLAN。
		untag	报文业务类型=配置的报文封装类型，则打一层 SVLAN。
Stacking	other-all	无法配置	
	user-vlan(tag)	tag	报文 tag=uservlan，则进行 CVLAN 到 SVLAN 的切换。报文上行所带的 VLAN 为 Stacking VLAN+内层 VLAN。
		untag	丢弃
	user-8021p	tag	报文 tag 优先级 =user-802.1p，剥离用户 Tag 后添加两层上行 Tag
		untag	丢弃
	user-vlan(untag)	tag	丢弃
		untag	把报文打一层 label，再打一层 SVLAN。
	user encap(ipoe/pppoe)	tag	报文业务类型=配置的报文封装类型，则把报文的 tag 切换成一层 label，再打一层 VLAN。

VLAN 类型	流类型	上行报文是否带 Tag	报文如何处理
		untag	报文业务类型=配置的报文封装类型，则把报文打一层 label，再打一层 SVLAN。
Common	other-all	无法配置	
	user-8021p	tag	报文 tag 优先级=user-802.1p，剥离用户 Tag 后添加一层上行 Tag
		untag	丢弃
	user-vlan(tag)	tag	报文 tag=uservlan，切换成 SVLAN，不相等则丢弃。
		untag	丢弃
	user-vlan(untag)	tag	丢弃
		untag	打一层 SVLAN
	user encap(ipoe/pppoe)	tag	报文业务类型=配置的报文封装类型，则切换成 SVLAN。
		untag	报文业务类型=配置的报文封装类型，则打一层 SVLAN。
Transparent	other-all	tag	透传
		untag	透传

VLAN 类型：在 MDU 设备上配置 VLAN 的类型。

流类型：在 MDU 设备上配置业务流的类型。

上行报文是否带 tag：向上行发送的报文带 tag 的情况。untag 为上行报文不带 tag。tag 为上行报文带 tag。

报文如何处理：设备对报文的处理动作。

2.8 二层转发策略

报文在二层设备上转发一般是根据报文的 VLAN 信息和 MAC 地址进行转发。即：VLAN ＋ MAC 转发。MDU 支持报文根据 VLAN 进行转发，即 SVLAN ＋ CVLAN 转发。

2.8.1 介绍

2.8.1 介绍

定义

报文在二层设备上转发一般是根据报文的 VLAN 信息和 MAC 地址进行转发。即：VLAN ＋ MAC 转发。MDU 支持报文根据 VLAN 进行转发，即 SVLAN ＋ CVLAN 转发。

目的

SVLAN+CVLAN 转发使 MDU 设备的二层转发不再依赖于 MAC 地址学习，从而解决如下问题：

1. 解决 MAC 地址空间不足。
2. 解决动态 MAC 地址老化，引起未知单播的出现；未知单播进行广播时带来安全问题。
3. 解决 MAC 地址欺骗和攻击的安全性问题。

2.8.2 规格

转发策略的相关规格如下：

- 支持 VLAN ＋ MAC 转发。
- 支持 SVLAN+CVLAN 转发。

2.8.3 原理描述

VLAN+MAC 转发

通常 Lanswitch 的转发原理为基于 VLAN ＋ MAC 转发。VLAN+MAC 转发是指，报文进入 Lanswitch 时，Lanswitch 自动学习 VLAN、源 MAC 地址和入端口的对应关系；在向 Lanswitch 外转发时，根据 VLAN 和目的 MAC，查找对应的出端口，从找到的端口发送出去。

VLAN+MAC 转发机制中，对于广播 MAC 地址或者未知单播 MAC 地址，会在 VLAN 内进行广播，即将报文复制多份，从该 VLAN 内的每个端口发送一份。

SVLAN+CVLAN 转发

SVLAN+CVLAN 双层 VLAN 是对 VLAN 的扩展。一方面增大了 VLAN 的表示范围，另一方面往往用 S 和 C 表示不同的含义，比如 S 表示业务，C 表示用户。这样，每个 SVLAN+CVLAN 就可以唯一对应一个用户业务，使 SVLAN+CVLAN 转发成为可能。

SVLAN+CVLAN 转发是指根据 SVLAN+CVLAN 两层 VLAN ID 组成二层转发映射关系，能够找到唯一对应一个出端口（或业务虚端口）就可以完成基于 VLAN 的转发。

说明

因为 MUX VLAN 中只能建立一条业务流，所以 Common 属性的 MUX VLAN 也可以支持基于 VLAN 进行转发。而 Smart VLAN 必须为 QinQ 或者 Stacking 属性，QinQ 属性的 Smart VLAN 也可以支持基于 SVLAN+CVLAN 进行转发。

SVLAN+CVLAN 转发表项不需要动态学习，在创建业务流时，系统自动创建静态的转发表项。根据转发表项上行报文找到相应的上行口发送，下行报文找到对应的业务虚端口进行发送。

2.9 术语与缩略语

术语

术语	解释
用户板	在本文中，指接入用户业务的单板
S+C 转发	根据报文中以太网头部的两层 VLAN 进行转发，外层为 S-tag，内层为 C-tag

缩略语

缩略语	全称
ONU	Optical Network Unit（光网络单元）
COS	Class of Service（服务等级）
ONT	Optical Network Terminal（光网络终端）

3 QoS

关于本章

QoS 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，向用户的业务提供端到端的质量保证，包括多个子特性，本章将对其子特性分别加以介绍。

3.1 介绍

QoS 特性是向用户的业务提供端到端的质量保证，其子特性介绍如下：

特性名称	特性介绍
流分类策略	流分类的结果是区分业务流，系统基于业务流完成业务映射和并为后续的 QoS 动作做准备。
优先级处理	不同的业务流可以根据优先级处理的策略，设置业务流内外层 VLAN 的优先级或者信任用户侧优先级。
流量管理（流量监管）	服务提供商在向客户提供特定的服务前，一般都要订立服务合同（SLA），明确各种服务参数。为了保证用户流量能够符合 SLA，那么需要对用户流量进行监管。
ACL 策略	ACL 策略是指根据预先设定的策略允许或禁止相应的数据包通过。
拥塞管理	当系统产生拥塞时，系统必须通过一系列的 QoS 活动来处理拥塞的报文。这一系列的活动就是拥塞管理。

3.2 可获得性

QoS 特性能够正常使用需要的 License 支持情况如下所示：

接入特性	License 支持
流分类策略	无需 License 许可。
优先级处理	无需 License 许可。
流量管理（流量监管）	无需 License 许可。
ACL 策略	ACL 策略特性是可选特性，只有获得 License 许可才能获得该特性的服务。
拥塞管理	无需 License 许可。

3.3 流分类策略

流分类的结果是区分业务流，系统基于业务流完成业务映射和并为后续的 QoS 动作做准备。

3.3.1 介绍

定义

MDU 产品进行的流分类是根据用户以太报文的特征对用户业务进行区分的技术。

目的

流分类的结果是区分业务流，系统基于业务流完成业务映射和并为后续的 QoS 动作做准备。比如用户 VLAN 到网络 VLAN 的切换、上下行 CAR 限速、优先级标记、入队列等等。

受益

为用户的各种业务提供 QoS 保证。

3.3.2 规格

流分类策略的相关规格如下：

- 支持基于以太网报文协议类型进行流分类。
- 支持基于用户侧 VLAN 进行流分类。
- 支持基于以太网 802.1P 进行分类。
- 每个以太网 UNI 端口最大支持的业务流数量为 280。
- 系统支持的最大的业务流数量为 512。

3.3.3 原理描述

MDU 的 QoS 模型

IETF 定义的 DiffServ（Differentiated Services Architecture）是一种可以在 Internet 上实现可扩展的业务区分模型。DiffServ 模型可以采用少量的成熟的构件构造出多种结构，提供不同 QoS 级别的服务，能够支持多种应用需求，满足组播和语音等要求实时性较高的需求。

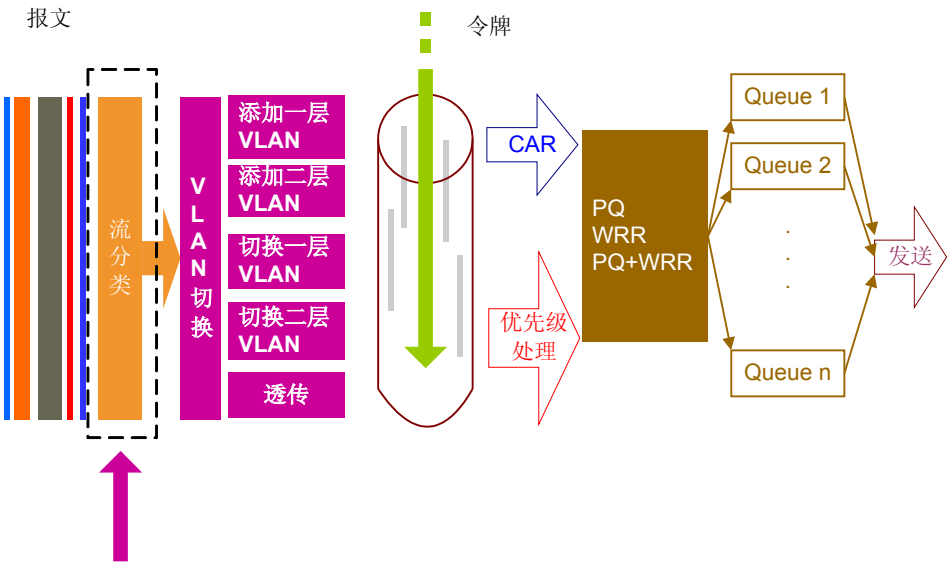
DiffServ 模型由许多在网络节点上实现的功能实体组成，包括每一跳转发行为集合、流分类功能、流量调节功能。其中流量调节功能又包括测量（metering）、标记（marking）、整形（shaping）、和监管（policing）。DiffServ 模型只在网络的边界节点上实现复杂的分类和调节功能。通过在 IPv4 和 IPv6 包头的 DS 域做适当的优先级标记（IP Precedence），把业务流聚类为行为集合（BA，Behavior Aggregate），然后根据所做的标记，采取不同的转发行为。

MDU 中实现 QoS 的技术主要有如下几个方面：

- 分类和标记（Classifciation and Marking）
- 流量监管和整形（Traffic Policing and Shaping）
- 队列调度（Queuing）

MDU 的 QoS 处理整体模型如图 3-1 所示：

图 3-1 MDU 中 QoS 处理整体模型-流分类



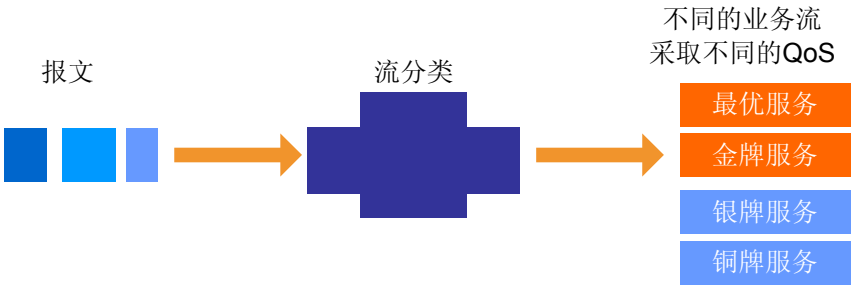
流分类

MDU 产品进行的流分类是根据用户以太报文的特征对用户业务进行区分的技术，主要是为了支持多业务应用，并对每一个用户的每一种业务（一条业务流）提供 QoS 保证。

报文进入 MDU 设备后，先进行流分类，然后对不同的流，提供不同 QoS 服务。

流分类处理过程如图 3-2 所示。

图 3-2 流分类处理过程



3.4 优先级处理

不同的业务流可以根据优先级处理的策略，设置业务流内外层 VLAN 的优先级或者信任用户侧优先级。

3.4.1 介绍

定义

MA5620/MA5626 的优先级处理主要体现在能够灵活的对报文进行 VLAN 优先级重标记以及信任用户侧的 CoS 优先级和 ToS 优先级。

目的

不同的业务流可以根据优先级处理的策略，设置业务流内外层 VLAN 的优先级或者信任用户侧优先级。在本设备上产生拥塞或者上行网络产生拥塞后可根据优先级进行调度。

3.4.2 规格

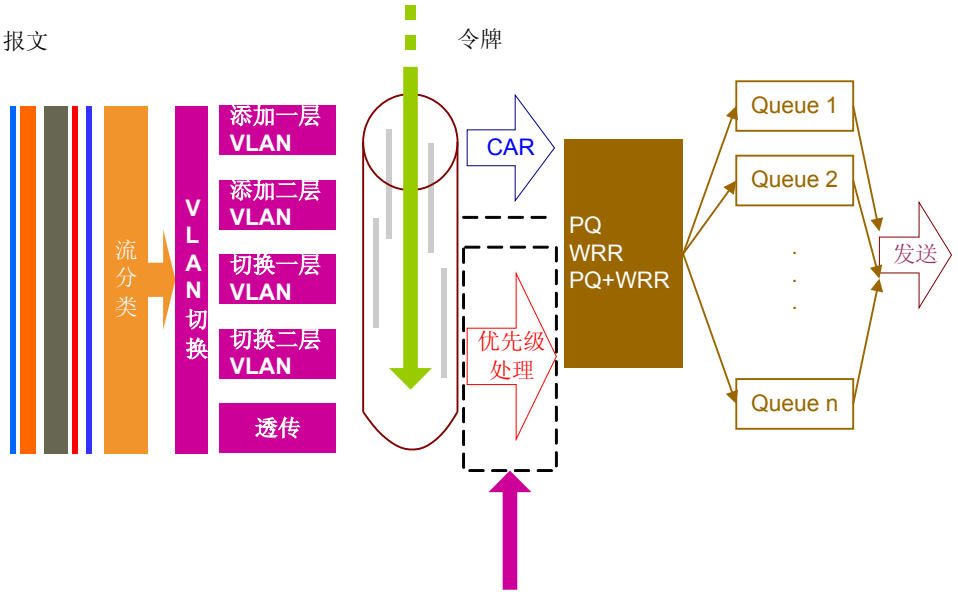
本特性的相关规格如下：

- 支持基于流量模板的 802.1P Remark，支持的 Remark 方式：配置指定、拷贝源报文 802.1P、拷贝源报文 ToS 值。
- 支持对匹配 ACL 策略的报文指定优先级，可配置指定 ToS、802.1P 值。
- 支持用户侧 CoS 优先级到网络侧优先级的拷贝。
- 支持用户侧 ToS 优先级到网络侧优先级的拷贝。
- 支持设置网络侧 CoS 优先级。
- 支持通过 ACL 设置 CoS 优先级。

3.4.3 原理描述

优先级处理可以按照一定规则对 802.1p 优先级重新标记。优先级处理为 MA5620/MA5626 的队列调度做准备。MA5620/MA5626 的队列调度是按照外层 VLAN 的优先级进入队列。同时优先级处理也为上层网络的调度做准备。请参考 MA5620/MA5626 的 QoS 整体模型：

图 3-3 MA5620/MA5626 的 QoS 整体模型

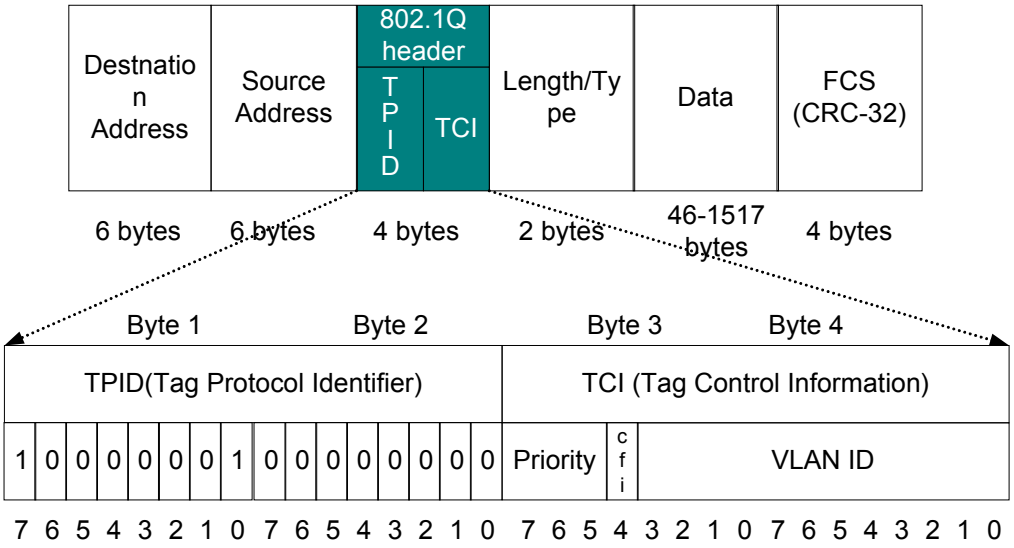


报文的优先级包括：802.1p 优先级和 IP 优先级。

802.1p 优先级和 IP 优先级

1. 802.1p 优先级

图 3-4 802.1Q 帧格式



802.1Q 定义的以太网帧结构如上图所示，这 4 个字节的 802.1Q 标签头包含如下内容：

- TPID—Tag Protocol Identifier：2 个字节的标签协议标识，它的值是 8100。
- TCI—Tag Control Information：2 个字节的标签协议标识，TPID 是 IEEE 定义的新的类型表明这是一个加了 802.1Q 标签的本文。
- TCI 划分成 3 个域：
  - VLAN Identified（ VLAN ID ）: 这是一个 12 位的域，指明 VLAN 的 ID 一共 4096 个每个支持 802.1Q 协议的主机发送出来的数据包都会包含这个域以指明自己属于哪一个 VLAN。
  - Canonical Format Indicator（ cfi ） 这一位主要用于总线型的以太网与 FDDI、令牌环网交换数据时的帧格式。
  - Priority ：3 位，指明帧的优先级一共有 8 种优先级主要用于当交换机阻塞时优先发送哪个数据包。

MA5620/MA5626 的本端媒体 IP 和信令 IP，根据组网需要，可配置到同一个 VLAN 中，也可以配置到不同的 VLAN 中。同时还可以分别为媒体 IP 和信令 IP 配置一个 802.1P 优先级（范围：0 ～ 7），默认情况下，媒体和信令 IP 的优先级为 6。

2. DSCP/TOS

在 IP 协议定义中，DSCP 和 TOS 在 IP 头中占用相同的域（1 个字节），IP 承载网设备根据识别填充的是 DSCP 或 TOS，根据设置进行相应调度和转发，保证不同业务的 QoS。但目前 MDU 不支持 DSCP。

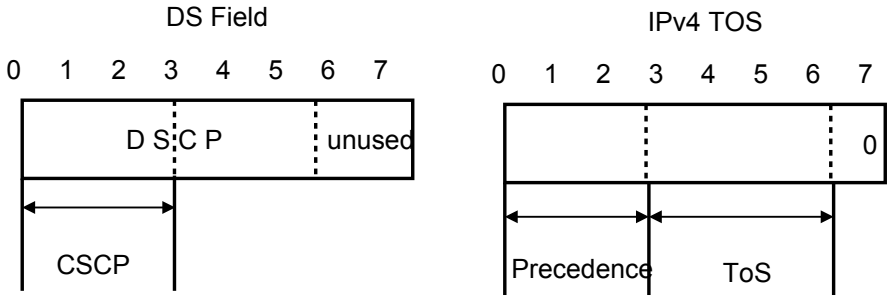
服务类型（TOS：Type of Service）字段包括一个 3 bit 的优先权子字段（现在已被忽略），4 bit 的 TOS 子字段和 1 bit 未用位（必须置为 0）。4 bit 的 TOS 分别代

表：最小时延、最大吞吐量、最高可靠性和最小费用。4 bit 中只能置其中 1 bit。如果所有 4 bit 均为 0，那么就意味着是一般服务。

DSCP 标识是基于 Ipv4 的 ToS（Type of Service）和 IPv6 的流量类型（Traffic Class）进行定义。

如图 3-5 所示，DS 字段的低 6 位（0 ～ 5 位）用作区分服务代码点 DSCP（DS CodePoint），高 2 位（6、7 位）是保留位。DS 字段的低 3 位（0 ～ 2 位）是类选择代码点 CSCP（Class Selector CodePoint），它表示了一类 DSCP。

图 3-5 DSCP 标识



其中，DSCP 用于在网络中每个节点上选择相应的 PHB（Per-Hop Behavior）。PHB 是 DS 节点作用于数据流聚合的外部可见行为的描述。目前，IETF 定义了三种标准的 PHB：加速转发 EF（Expedited Forwarding）、确保转发 AF（Assured Forwarding）和尽力而为 BE（Best-Effort）。

SVLAN 优先级处理原则

MA5620/MA5626 产品对外层的 VLAN 优先级支持三种优先级处理方式：

- 信任 user-cos

  将业务流的外层 VLAN 优先级设置为用户侧的 VLAN 优先级。
- 信任 user-tos

  将业务流的外层 VLAN 优先级设置为用户侧 IP 报文的 tos 优先级。
- 信任本地优先级

  可配置业务流的外层 VLAN 优先级。

上行报文均支持三种优先级处理方式。但下行报文只支持信任 user-cos 和本地优先级，不支持信任 user-tos。

CVLAN 优先级处理原则

当 VLAN 的属性为 QinQ 时，内层 VLAN 为用户侧带上来的 VLAN，优先级不会改变。

当 VLAN 的属性为 Stacking 时，可以设置内层 VLAN 的优先级，如果不配置，内层 VLAN 优先级则取默认值 0。

3.5 流量管理（流量监管）

服务提供商在向客户提供特定的服务前，一般都要订立服务合同（SLA），明确各种服务参数。为了保证用户流量能够符合 SLA，那么需要对用户流量进行监管。

3.5.1 介绍

定义

服务提供商在向客户提供特定的服务前，一般都要订立服务合同（SLA），明确各种服务参数。为了保证用户流量能够符合 SLA，那么需要对用户流量进行监管。

目的

流量监管主要目的如下：

- 为保证客户进入的流量符合 SLA。
- 用来调节出去的流量，平抑突发流量，保证服务质量。
- 通过报文抑制来控制广播报文速率。

3.5.2 规格

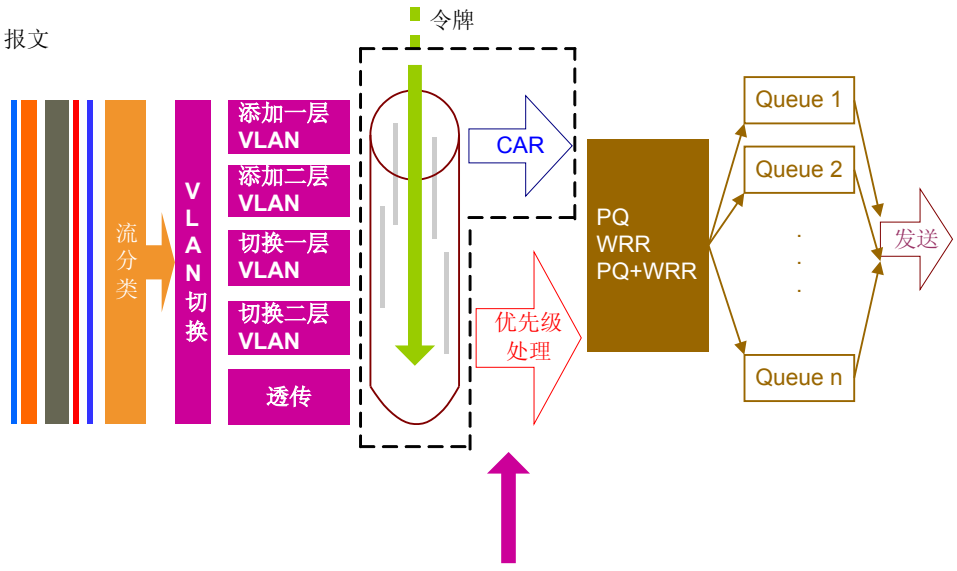
本特性的相关规格如下：

- 支持基于业务流的流量限速。
- 支持基于端口的双向流量限速。
- 支持 trTCM。基于业务流进行流量管理时，IP 流量模板中的 CIR、CBS、PIR、PBS，按照 trTCM 算法 Color-Blind 模式进行流量管理。

3.5.3 原理描述

请参考 MA5620/MA5626 的 QoS 整体模型：

图 3-6 MA5620/MA5626 的 QoS 整体模型

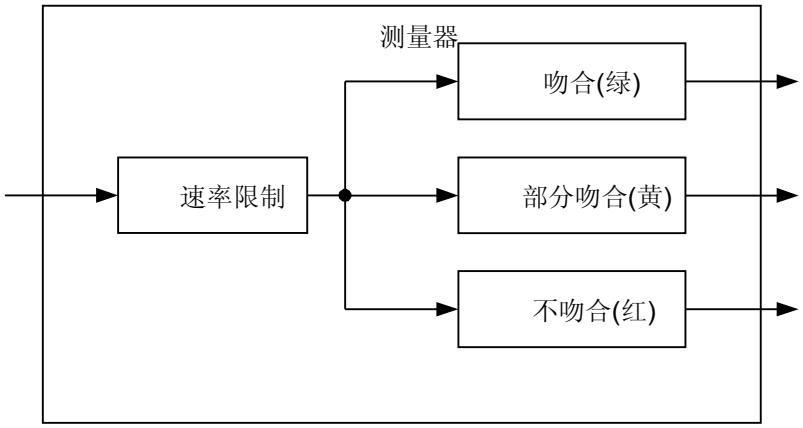


流量监管

流量监管又称流量策略（Traffic Policing），其典型作用是限制进入某一网络的某一连接的流量与突发。在报文满足一定的条件时，如某个连接的报文流量过大，监管就可以对该报文采取不同的处理动作，例如丢弃报文，或标记报文的颜色（重新设置报文的优先级）等。通常的用法是使用 CAR 来限制某类报文的流量，例如限制 HTTP 报文不能占用超过 50%的网络带宽。

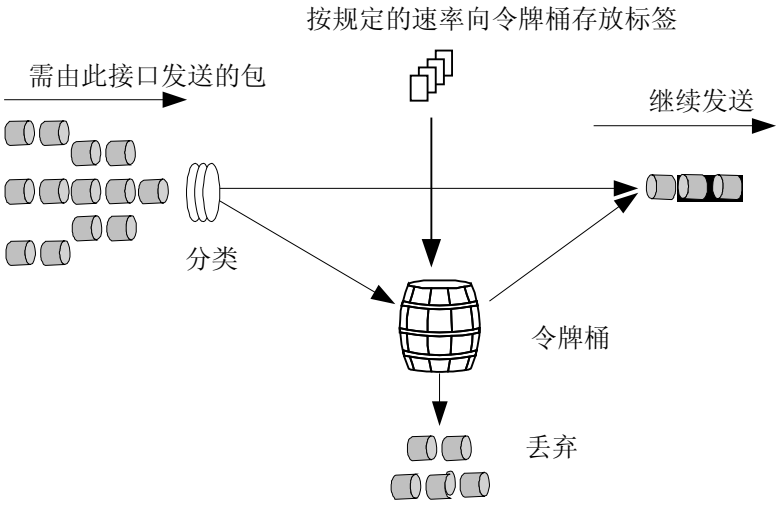
为了测量客户的实际流量，首先需要做的是基于时间的流量测量，通过实际流量与 SLA 的吻合水平，决定采用何种策略，比如是否丢弃，或者着色。

图 3-7 一个测量器的例子



CAR（Committed Access Rate）是流量控制的最常用的测量和丢弃工具。CAR 利用令牌桶（Token Bucket, TB）进行流量控制，其基本原理是：每隔一定时间，向令牌桶添加一定数目的令牌；每个报文的发送都需要使用和报文长度相应的令牌，如果令牌桶中有足够的令牌，则允许报文通过，并将令牌数减少；如果令牌桶中的令牌不满足报文的发送条件，则报文被丢弃。

图 3-8 Token Bucket



CAR 可以为不同类别的报文设置不同的流量特性和标记特性，即首先对报文进行分类，然后不同类别的报文有不同的流量特性和标记特性，此外 CAR 的策略还可以进行串联处理。例如可以对所有的报文限制一个总的流量，然后在总的流量中再限制部分报文的流量符合某个流量特性。

在实际应用中 CAR 不仅可以用来进行流量控制，还可以进行报文的标记（mark）或重新标记（remark），即 CAR 可以设置报文的优先级，达到标记报文的目的。例如当报文符合流量特性的时候可以设置报文的优先级为 5，当报文不符合流量特性的时候可以丢弃，也可以设置报文的优先级为 1 并继续进行发送，这样后续的处理可以尽量保证不丢弃优先级为 5 的报文。在网络不拥塞的情况下也发送优先级为 1 的报文。当网络拥塞时首先丢弃优先级为 1 的报文。

基于流的流量监管

基于流的流量管理的目的是对每条业务流的流量进行监控。业务流可以绑定流量模板，通过流量模板来定义业务流的 CAR 值。

基于端口的流量监管

1. 对于 ETH 端口，可以通过 line-rate 命令对指定出端口的上行速率和下行速率分别进行限制。

报文抑制功能

报文抑制是指广播、多播、未知单播报文的抑制，通常情况下，广播、多播、未知单播报文是在 VLAN 内广播的，对这类报文的抑制，目的是为了防止这类报文占用过多的网络资源，造成网络拥塞。

通过 traffic-suppress 配置广播、未知多播和未知单播流量抑制等级。流量抑制等级配置成功后，如果开启端口的流量控制开关，系统将按照流量抑制等级对应的流量对该端口的流量进行限制。

3.6 ACL 策略

ACL 策略是指根据预先设定的策略允许或禁止相应的数据包通过。

3.6.1 介绍

定义

ACL（Access Control List）策略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。

3.6.2 规格

- ACL 编号在 2000 ～ 4999 之间，最多允许定义 256 条规则，系统中最多可创建 8 条 ACL，每条 ACL 下最多设置 32 条规则。各种类型 ACL 说明如表 3-1 所示。
- 系统可以激活的 ACL 有效规则条数不超过 256 条。
- 支持 ACL 时间段的设置，最多支持 256 个时间段配置。
- 支持针对端口下发基于 ACL 的包过滤，可下发的基于 ACL 包过滤条数不超过 256。
- 支持基于 ACL 规则的报文的过滤、镜像、优先级映射/修改、带宽控制、允许/禁止访问等动作。

表 3-1 ACL 分类列表

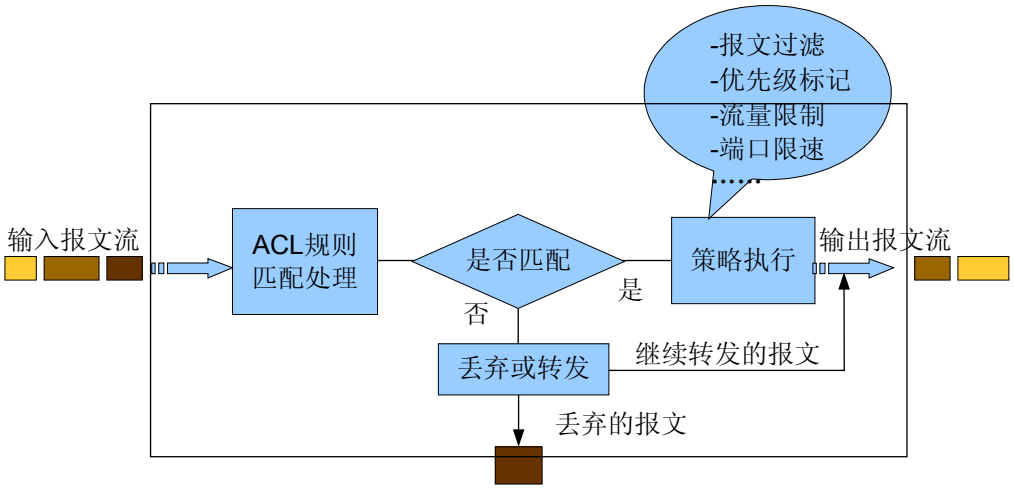
项目	数字取值范围	特点
基本 ACL	2000 ～ 2999	只能根据三层源 IP 和 fragment 字段制定规则，对数据包进行相应的分析处理。
高级 ACL	3000 ～ 3999	可以根据数据包的源地址信息、目的地址信息、IP 承载的协议类型(包括的报文类型有 gre、icmp、ip、ipinip、tcp、udp)、针对协议的特性，例如 TCP 的源端口、目的端口，ICMP 协议的类型、code 等内容定义规则。 利用高级 ACL 可以定义比基本 ACL 更准确、更丰富、更灵活的规则。
链路层 ACL	4000 ～ 4999	可以根据源 MAC 地址、源 VLAN ID、二层协议类型、目的 MAC 地址等链路层信息制定规则。

3.6.3 原理描述

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：

- 如果匹配规则，则交 QoS 进一步策略动作执行处理，包括报文过滤、优先级标记、流量限制、流量统计、报文镜像，在完成策略执行处理后再转发输出报文流。
  - 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、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。
  - 流量统计：对匹配 ACL 规则的数据包进行流量统计。
  - 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。
- 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 3-9 ACL 规则过滤处理原理图



3.7 拥塞管理

当系统产生拥塞时，系统必须通过一系列的 QoS 活动来处理拥塞的报文。这一系列的活动就是拥塞管理。

3.7.1 介绍

定义

当系统产生拥塞时，系统必须通过一系列的 QoS 活动来处理拥塞的报文。这一系列的活动就是拥塞管理。通常拥塞管理是通过队列调度来实现的。

目的

区分业务的优先级，并在系统拥塞时优先处理优先级高的报文。

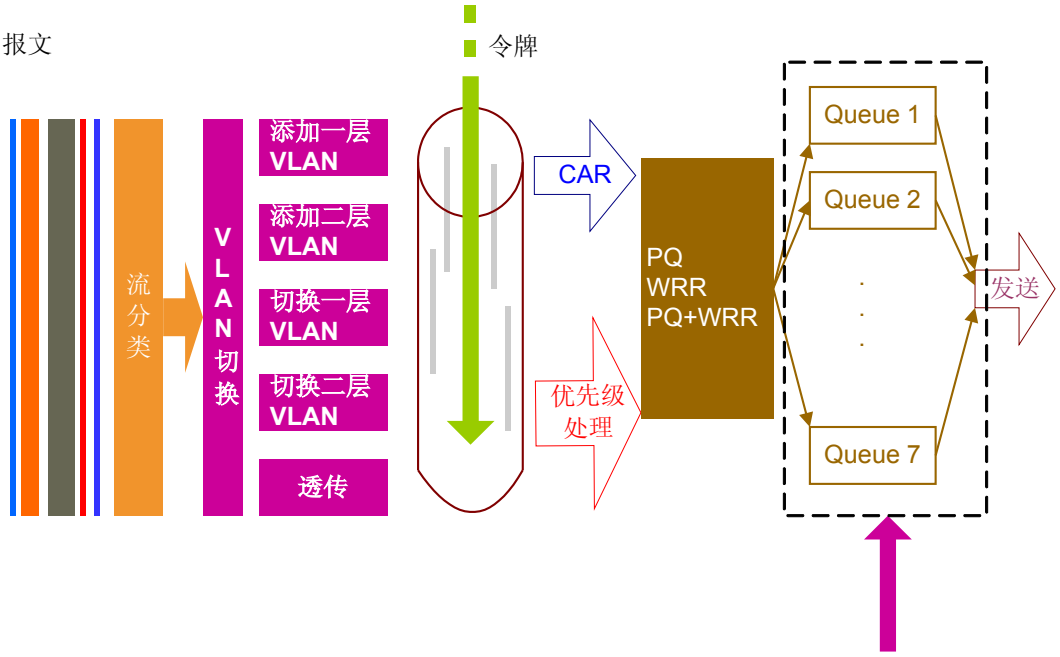
3.7.2 规格

本特性的相关规格如下：

- 支持全局按照百分比设置各队列深度。
- 支持 PQ，WRR，PQ ＋ WRR 三种调度方式。默认的调度方式为 PQ 调度。
- 支持设置 WRR 队列权重。
- 支持 WRED 模板配置，支持对不同颜色的报文分别设置丢弃门限和丢弃概率。
- 支持不同优先级的队列绑定不同的 WRED 模板。

3.7.3 原理描述

MA5620/MA5626 设备产生拥塞时采用队列调度的方式处理拥塞，请参考 MA5620/MA5626 的 QoS 整体框架：



Queuing 技术

队列调度机制是 QoS 中非常重要的一个技术，是为了实现拥塞管理。在出接口发生拥塞时，通过适当的队列调度机制，可以优先保证某种类型的报文的 QoS 参数，例如带宽、时延、抖动等。这里所说的队列是指出队列，其作用是在接口有能力发送报文之前先将报文在内存中保留下来，直到接口可以继续发送报文；所以队列调度机制都是在出端口发生拥塞情况下产生作用，另外一个主要作用就是将报文重新排序，FIFO（First In First Out Queueing 先进先出的排队策略）除外。

和队列调度相关的功能或特征包括如下内容：

特性	定义	可影响的 QoS 参数
分类 classification	检查报文并决定将其放入到那个队列的能力	无
丢弃策略 drop policy	定义了设备丢弃报文的规则，常用的丢弃策略有尾部丢弃、修改的尾部丢弃例如 WFQ 采用的丢弃策略、WRED 等	丢包
单一队列内的调度方式	在一个队列内，报文有可能被重新排序，在大多数情况下都是采用的 FIFO	带宽、时延、抖动、丢包
队列之间的调度方式	定义了从哪个队列拿包放到发送队列	带宽、时延、抖动、丢包

特性	定义	可影响的 QoS 参数
队列数目	报文可以被分类细化的程度	无
队列长度	单一队列可以存储的最大报文数目	丢包、时延

常用的队列调度机制包括 PQ、WRR、PQ+WRR，其基本特点对比如下：

队列调度机制	调度方式
PQ	严格优先级调度
WRR	加权优先级调度
PQ+WRR	PQ 和 WRR 混合调度

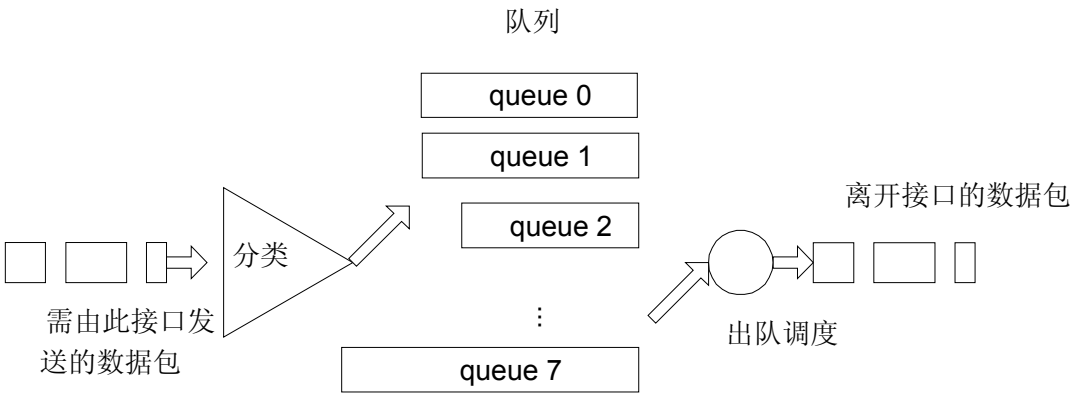
PQ

优先队列（Priority Queuing, PQ）对报文进行分类，然后按报文的类别将报文送入相应的队列。

在报文到达接口后，首先对报文进行分类，然后按照报文所属的类别让报文进入所属队列的尾部，在报文发送时，按照优先级，总是在所有优先级高的队列发送完毕后，再发送低优先级队列中的报文。这样在每次发送报文时，总是将优先级高的报文先发出去，保证了属于较高优先级队列的报文有非常低的时延，其报文的丢失率和通过率这两个性能指标在网络拥塞时也可以有一定的保障。

这样，分类时属于较高优先级队列的报文将会得到优先发送，而较低优先级的报文将会在发生拥塞时被较高优先级的报文抢先，使得关键业务的报文能够得到优先处理，非关键业务（如 E-Mail）的报文在网络处理完关键业务后的空闲中得到处理，既保证了关键业务的优先，又充分利用了网络资源。

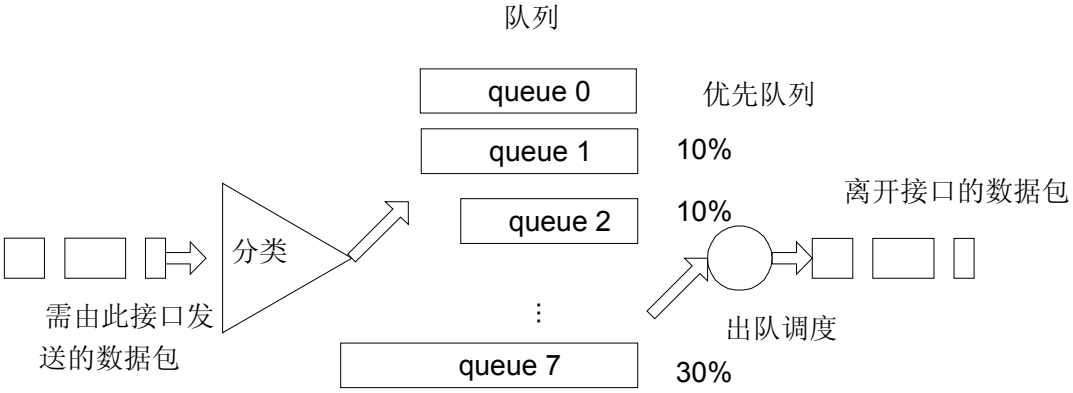
图 3-10 优先队列（Priority Queuing, PQ）



WRR

加权轮询算法（Weighted Round Robin, WRR）对报文进行分类，然后按报文的类别将报文进入相应的队列。WRR 队列可以按用户的定义分配它们能占用接口带宽的比例，在报文出队的时候，WRR 按定义的带宽比例分别从队列中取一定量的报文在接口上发送出去。

图 3-11 加权轮询算法（Weighted Round Robin, WRR）



PQ + WRR

WRR+PQ 调度模式是 WRR 与 PQ 两种调度模式的混合。当队列的权重存在 0 值时，队列调度模式为 PQ+WRR 调度模式。在这种模式下，系统先按 PQ 模式调度权重为 0 的队列，再按 WRR 模式调度权重非 0 的队列。这种调度方式更加灵活，可以配置必须保证的业务进行 PQ 调度，当带宽有剩余时，对优先级低的业务进行 WRR 调度。一方面保证了高优先级业务，一方面在有带宽剩余的情况下不至于使低优先级业务无法开展。

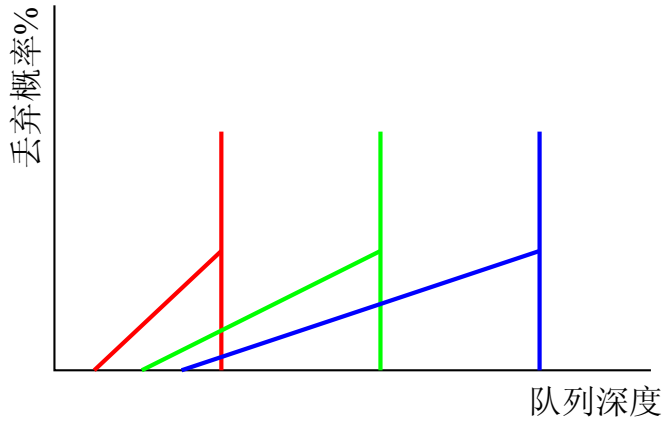
WRED

加权随机早期检测（WRED）采用随机丢弃策略，避免了尾部丢弃而引起的带宽震荡，用户可以设置队列不同颜色报文的低丢弃门限、高丢弃门限和丢弃概率。

- 当队列的长度在低丢弃门限和高丢弃门限之间时，WRED 开始根据颜色随机丢弃报文，队列的长度越长，丢弃的概率越高。
- 当队列的长度达到高门限时，丢弃到来的所有报文，通过开始丢弃数据包的过程，WRED 能有助于避免出现不受控的丢失数据包，不受控的丢失数据包可能会对应用性能带来重大影响。

WRED 可以为不同的优先级报文设置不同的低丢弃门限、高丢弃门限和丢弃概率，从而对不同优先级的报文提供不同的丢弃策略。

图 3-12 WRED 队列丢弃管理



拥塞管理

- MA5620/MA5626 上行方向的调度策略：

用户报文在 UNI 侧进行业务流分类，并对业务流进行 CAR、优先级标记等 QOS 动作之后，按照 QOS 策略分别进入 8 个队列，在 8 个队列之间进行调度，可支持 PQ、WRR、PQ+WRR 队列调度模式。队列调度完成后，报文被送到上行接口。

- MA5620/MA5626 下行方向的调度策略：

下行的报文先进行业务流分类，并对业务流进行 CAR、优先级标记等 QOS 动作之后，按照 QOS 策略分别进入 8 个队列，在 8 个队列之间进行调度，可支持 PQ、WRR、PQ+WRR 队列调度模式。队列调度完成后，报文被送到 UNI 接口。

3.8 术语与缩略语

术语

术语	解释
保证带宽	为用户提供保证通过的带宽，用户在此带宽范围内的流量都可以通过。
突发带宽	允许用户超过保证带宽的流量，用户在此带宽范围内的流量在端口还有剩余带宽时可以通过。

缩略语

缩略语	全称
ONT	Pseudo Wire Emulation Edge-to-EdgeOptical Network Termination（光网络终端）
ODN	Optical Distribution Network （光纤网络）

缩略语	全称
CIR	Committed Information Rate （承诺信息速率）
PIR	Peak Information Rate（峰值信息速率）
CAR	Committed Access Rate（承诺接入速率）
CP	Content Provider（内容提供商）
TrTCM	two rate three color marker （双速率三色标）
PQ	Priority Queuing（优先级队列）
WRR	Weighted Round Robin（加权轮询算法）
WRED	Weighted Random Early Detection（加权随机早期检测）
COS	Class of Service（服务等级）

4 组播

关于本章

组播是指信源将信息发向所有网络节点的某个确定子集的点到多点的通信形式，组播特性包含多个子特性。本章将对其子特性分别加以介绍。

组播 CAC（Connection Admission Control）控制是以用户线路带宽为依据对用户点播新节目进行控制。

4.12 术语与缩略语

4.1 介绍

定义

组播是指信源将信息发向所有网络节点的某个确定子集的点到多点的通信形式。

受控组播，即网络设备通过对用户加入或请求报文的识别，进行相应的权限控制，确定申请者是否有相应的权限观看节目，从而在接入设备完成组播业务的控制和转发。

目的

MA5620/MA5626 采用组播技术为运营商提供 IPTV 业务。

通过受控组播的引入，在网络设备上完成组播用户的管理和控制，满足运营商发放宽带视频业务的需求，使组播业务“可运营、可管理”。

组播技术的核心思想就是把报文复制工作尽可能的放到离接收者最近的地方来完成，减少网络上的组播数据流量。

4.2 参考标准和协议

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

4.3 可获得性

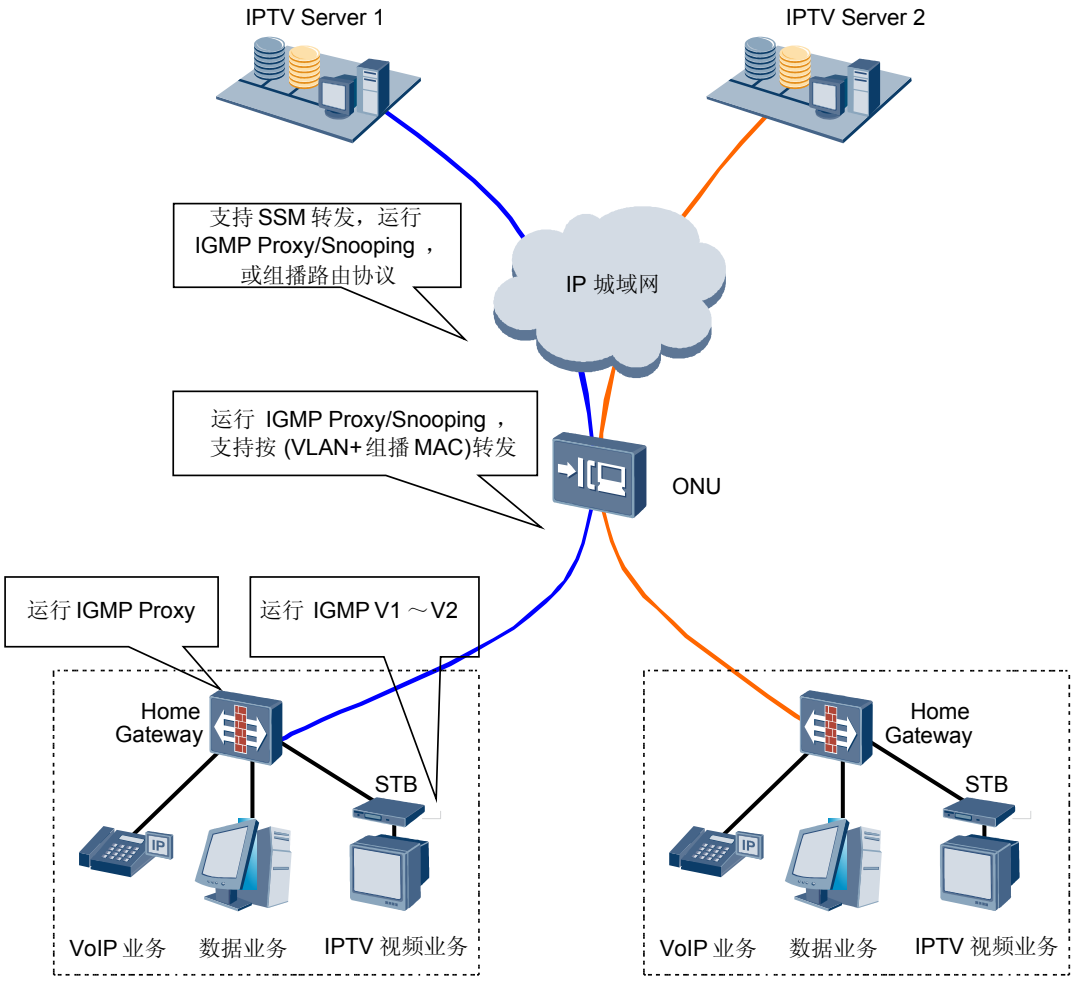
License 支持

- MA5620/MA5626 可以接入的组播用户数量受 License 控制，只有获得了 License 许可后才能获得该特性的服务。
- MA5620/MA5626 接入用户可以点播的组播节目数量受 License 控制，只有获得了 License 许可后才能获得该特性的服务。

4.4 原理描述

目前业界对接入设备的组播应用采用二层转发，MA5620/MA5626 于（VLAN+组播 MAC）进行数据转发。典型树形组网应用如图 4-1 所示。

图 4-1 组播典型的树形组网



在环形组网中，运行 MSTP 协议的设备通过一定的算法实现路径冗余，同时将环路网络动态地修剪成无环路的树型网络。

4.5 IGMP Snooping

IGMP Snooping 是一种运行在链路层的组播约束机制，用于管理和控制组播。本特性从介绍和原理描述方面进行描述。

4.5.1 介绍

定义

IGMP 监听(IGMP Snooping)是一种运行在链路层的组播约束机制，用于管理和控制组播组，并能有效地抑制组播数据在二层网络中扩散。

目的

采用 IGMP Snooping 实现二层组播管理，从而有效抑制组播数据在二层网络的广播。

4.5.2 规格

MA5620/MA5626 支持以下 IGMP Snooping 特性规格：

- 支持 IGMP V2/V3 Snooping

  IGMP V3 按照 TR101 的描述仅支持 Include 模式的报文。
- 支持 IGMP Snooping over IPoE。
- 支持 IGMP Snooping over PPPoE。
- 实现查询器功能，支持通用查询和特定查询机制。
- 实现报告器功能，响应上层路由器的查询。
- 支持 SSM 转发。
- 支持树型和环形组网。
- 支持 Snooping Report Proxy 功能。
- 支持 Snooping Leave Proxy 功能。

4.5.3 原理描述

- 组播用户上下线处理流程

  IGMP Snooping 工作模式下，MA5620/MA5626 将组播用户的加入和离开报文在切换为上行 VLAN 后，转发至上层路由器。

  MA5620/MA5626 设备在 IGMP Snooping 模式下充当查询器，在接收到组播路由器查询报文时，触发发送查询报文，在设定的周期内没有响应，则删除本地组播转发表项；组播路由器在设定的周期内未收到用户的响应报文，则删除路由器的转发表项。

  上层路由器收到用户的 Leave 报文后，发送特定组查询，若在设定的周期内没有收到该用户的响应报文，将该用户从组播组中删除。
- Snooping Report Proxy 和 Leave Proxy

  用户上线，在收到用户对节目的第一个请求报文时，将用户报文切换成组播 VLAN 转发至组播路由器；该节目的后续加入请求，不再转发至组播路由器。

  用户下线时，只有该节目的最后一个用户的 Leave 报文，会被转发至组播路由器，告知上层设备不再转发相应的组播流。

  在 Report Proxy 启用的情况下，响应组播路由器的查询。
- IGMP Snooping over PPPoE

  在 PPPoE 用户既需要 BRAS 验证，又需要接收组播节目的场景下，需要 MA5620/MA5626 备支持 IGMP Snooping over PPPoE。该特性满足 TR101 关于“IGMP

ECHO”功能的定义，除了转发用户 PPPoE 封装的 IGMP 报文到 BRAS 设备，同时 MA5620/MA5626 构造一份 IPoE 的 IGMP 报文转发到组播路由器。

4.6 IGMP Proxy

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中继转发。本特性从介绍和原理描述方面进行描述。

4.6.1 介绍

定义

组播代理（IGMP Proxy）即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中继转发。

- 从组播用户的角度看，该设备是一台组播路由器，完成 IGMP 协议中路由器部分的功能。
- 从组播路由器来看，接入设备是一个组播用户。

目的

采用 IGMP Proxy，使二层设备具备组播业务能力；同时屏蔽了用户频繁的加入和离开报文，减少了网络侧的组播报文流量。

4.6.2 规格

MA5620/MA5626 支持以下 IGMP Proxy 特性规格：

- 支持 IGMP V2/V3 Proxy

  IGMP V3 按照 TR101 的描述只支持 Include 模式的报文。
- 实现查询器功能，支持通用查询和特定查询机制。
- 实现报告器功能，响应上层路由器的查询。
- 支持 SSM 转发。
- 支持 IGMP 主机功能，对上层组播路由器发送加入和离开报文。
- 支持树型和环形组网。

4.6.3 原理描述

在 IGMP Proxy 工作模式下，用户上下线的处理流程如下：

1. 组播用户点播一个视频节目，向 MA5620/MA5626 发送 IGMP 请求报文，申请加入该节目。

2. MA5620/MA5626 接到请求报文后，如果该用户是第一个观看此节目的用户，MA5620/MA5626 向上层路由器发送请求报文申请该节目流下发到 MA5620/MA5626；如果已存在节目流，直接向该用户转发。
3. MA5620/MA5626 定期向所有在线的 IGMP 用户发送通用组查询报文。若在设定的周期内没有收到组播用户的响应报文，则认为该用户已离开该组播组，并将其从组播组中删除；如果是该节目的最后一个用户，MA5620/MA5626 设备还向上行组播路由器发送 Leave 报文。
4. MA5620/MA5626 接收上层组播路由器的查询报文，并向其回应相应的报告报文。

4.7 组播 VLAN 管理

组播 VLAN 定义了组播节目和用户等受控组播的重要内容。本特性从介绍和原理描述方面进行描述。

4.7.1 介绍

定义

组播 VLAN 定义了组播节目和用户等受控组播的重要内容。

目的

通过把组播 VLAN 出租给 ISP，客户达到管理 ISP 的目的。

4.7.2 规格

MA5620/MA5626 支持以下组播 VLAN 管理特性规格：

- 系统最大支持 32 个组播 VLAN。
- 每个组播 VLAN 可以选择不同的工作模式：Proxy、Snooping。
- 每个组播 VLAN 可以选择不同的 IGMP 协议版本：IGMP V2、IGMP V3。
- 每个组播 VLAN 支持不同的节目创建模式：静态配置节目、动态生成节目。
- 每个组播 VLAN 可以指定组播上行端口。

4.7.3 原理描述

工作模式

组播 VLAN 主要用于支持不同 ISP 的组网模式，基于每个 VLAN 配置 IGMP Proxy 或者 IGMP Snooping 工作模式。

对于 IGMP V3，用户的加入报文可能携带属于多个 VLAN 的节目。

- 如果 VLAN 的工作模式为 IGMP Proxy，用户原始报文将会被切分多个报文从相应的组播 VLAN 发送。
- 如果 VLAN 的工作模式为 IGMP Snooping，为了避免一个 Report 报文中的多条记录对应不同 Snooping 模式的组播 VLAN（这种情况下的转发将造成 IGMP 报文泛洪），系统只处理 IGMP Report 报文的第一条记录或丢弃。

IGMP 协议版本

基于每个 VLAN 配置 IGMP 的版本，主要目的是保证版本的兼容。组播 VLAN 的 IGMP 版本支持 V2 和 V3，缺省为 V3。

- IGMP V3：兼容 IGMP V2/V1，V2 兼容 V1，反向则不支持兼容。
  - 基于目前业务应用情况，MA5620/MA5626 持 IGMP V3 终端接入，兼容 IGMP V2 报文处理，但不支持 IGMP V1。
  - 对于 IGMP V3 终端，通过发送 IGMP V2 的查询报文强制将终端转换为 IGMP V2 模式。
- IGMP V2：只支持 IGMP V2。

节目创建模式

MA5620/MA5626 支持以下两种节目创建模式。

- 静态节目
  - 对于用户通过 IGMP 请求加入的组播组，根据组播组地址以及源 IP（只对 IGMP V3）为索引查找节目表。
  - 如果匹配，允许从该组播 VLAN 到用户端口的组播转发；上行的 IGMP 也将通过该组播 VLAN 进行转发。
- 动态节目
  - 根据用户加入请求报文，提取组播地址动态生成节目。
  - 动态生成节目，不提供用户侧和网络侧 CAC 带宽控制功能和预览和预加入功能。

组播用户

按 TR101 的描述，组播用户必须是组播 VLAN 的成员，才能点播该 VLAN 的节目。

4.8 节目管理

节目管理是指管理节目的各种属性，包括节目带宽、预览等参数，实现节目的可控。本特性从介绍和原理描述方面进行描述。

4.8.1 介绍

定义

节目管理是指管理节目的各种属性，包括节目带宽、预览等参数，实现节目的可控。

目的

定义受控节目的属性。

4.8.2 规格

MA5620/MA5626 支持以下节目管理特性规格：

- 支持预览参数设置。
- 支持静态节目的预加入功能。
- 支持静态节目的优先级设置。
- 支持静态节目的带宽设置。
- 支持组播节目的分级管理，即属于不同组播等级的用户可以享用的带宽、可以同时观看的节目数各不相同。

4.8.3 原理描述

节目预览

节目预览是通过控制用户观看节目的次数、时长、间隔等，使用户对节目有基本的了解，但又无权限完整的观看一个节目。

具有预览权限的用户上线后，会受预览时长的约束，在预览时长到期后，MA5620/MA5626 设备对用户进行下线处理。在预览间隔后的时间里，用户才能再次点播该节目。用户一天内点播该节目的次数受预览次数的限制。

节目预加入

节目预加入功能是指在没有用户加入的情况下，MA5620/MA5626 备作为用户向组播路由器发送加入报文，把组播流事先引到 MA5620/MA5626 设备，缩短用户点播节目的等待时间。

节目优先级

MA5620/MA5626 设备在转发相应的组播流时，在用户端口，按相应的优先级进行调度，目的是保证节目质量。

节目带宽

用户侧 CAC 和网络侧 CAC，都是利用该用户或该上行口的在线节目的累加带宽作为是否允许加入新节目的依据。如果用户在线节目的累加带宽与新节目的带宽之和超过设定的 CAC 值，则不允许新节目加入。

4.9 用户管理

用户管理是指定义合法的组播用户，在用户上线时进行鉴权，并进行 CAC 带宽校验。本特性从介绍和原理描述方面进行描述。

4.9.1 介绍

定义

定义合法的组播用户，在用户上线时进行鉴权，并进行 CAC 带宽校验。

目的

控制接入，防止非法的用户观看受控的节目。

4.9.2 规格

MA5620/MA5626 支持以下用户管理特性规格：

- 支持分别定义组播用户的 IGMP 协议承载通道和组播业务承载通道。
- 系统支持最多 256 个权限模板。
- 系统支持最多 32 个组播预览模板。
- 一个组播用户最大可以绑定 64 个权限模板。
- 支持用户快速离开。
- 一个用户同时观看的最大节目数为 16 个。

4.9.3 原理描述

组播 CAC 控制

组播 CAC 控制是以用户线路带宽为依据对用户点播新节目进行控制。用户点播新节目后，从 MA5620/MA5626 备获知新节目带宽，MA5620/MA5626 看用户线路带宽是否满足增加新节目带宽需求。如果满足，允许用户点播该节目，否则拒绝用户点播该节目。

快速离开模式

快速离开是指设备收到 IGMP Leave 后不经过查询，直接将用户从组播组中删除。

IGMP 协议承载通道

IGMP 协议承载通道包括以下各类型的参数：

- user-encap，包括：PPPoE、IPoE

- user-VLAN
- user-802.1p

视频承载通道

缺省情况下，IGMP 协议承载通道与组播流的承载通道默认是同一个，为了保持灵活性，可以在指定 IGMP 协议承载通道时，同时指定视频承载通道。

如果不指定，则使用协议承载通道作为组播流的承载通道。

视频承载通道包括以下类型的参数：

- user-encap，包括：PPPoE、IPoE
- user-VLAN
- user-802.1p

组播权限

组播权限在权限模板中定义，通过用户绑定不同的权限模板，达到权限控制的目的。

权限模板中包含的权限为：禁止、预览、观看、空闲；其权限优先级按上述顺序默认依次变低。该优先级系统管理员可配置。

4.10 动态可控组播

动态可控组播简化了 EPON 系统中组播业务的管理和维护，从而节约了成本，提高了业务开展的效率。

4.10.1 介绍

定义

动态可控组播是应用在 OLT+ONU 的 EPON 系统下的一种可控组播，即，OLT 利用扩展的 EPON OAM 消息实现对 ONU 上组播业务的控制和管理，整个系统中，组播业务的控制和管理集中在 OLT 上，ONU 只需按照 OLT 的扩展 OAM 消息实现组播数据报文的转发控制，而无需实现复杂的组播业务的控制和管理，例如：对组播用户进行权限配置和鉴权。

目的

在组播业务时，需要在最靠近用户的设备上对组播权限进行控制，在 EPON 系统中则为 ONU 设备。但在 OLT+ONU 的 EPON 系统中，OLT 是布置在局端的设备，ONU 是布置在远端小区，楼道或者用户家中的设备，一个 OLT 可以接入大量的 ONU 设备，这样在 ONU 上进行组播权限管理非常不方便，配置量大，且一旦组播节目进行增加或更新，需要对所有 ONU 进行更新，这样效率非常低。

动态可控组播中将组播权限管理上移到 OLT 设备集中管理，简化了 ONU 上的配置，提高了管理维护的效率。

受益

动态可控组播简化了 EPON 系统中组播业务的管理和维护，从而节约了成本，提高了业务开展的效率。

4.10.2 规格

MA5620/MA5626 支持如下可控组播规格：

- 系统支持最多 256 个权限模板。
- 系统支持最多 32 个组播预览模板。
- 一个组播用户最大可以绑定 64 个权限模板。
- 一个用户同时观看的最大节目数为 16 个。

4.10.3 原理描述

在动态可控组播模式下，OLT 上进行组播用户的权限管理，如：组播节目、组播权限模板、组播用户、组播用户绑定的权限模板；而 ONU 上不进行任何组播用户和权限管理的配置。

OLT 利用 ONU 上的 LLID 和上行的 IGMP Report 报文携带的 VLAN ID 进行组播用户的识别，这个 VLAN ID 由 ONU 负责添加。OLT 识别出 ONU 上的组播用户后，基于 OLT 上已配置的此组播用户的组播权限模板进行权限控制，组播视频流将通过 OLT 转发到 ONU，再由 ONU 转发到申请的用户。

动态可控组播模式下，报文处理流程如下：

1. 组播用户发起 IGMP 加入报文，申请组播节目。
2. ONU 收到 IGMP 加入报文后，向 IGMP 加入报文添加 VLAN ID 后，将报文发送到 OLT。
3. OLT 收到来自 ONU 的 IGMP 加入报文后，根据 ONT ID 和报文中 VLAN ID，查找组播用户和组播用户对应的权限。
4. OLT 根据权限模板的定义，首先在本地创建此组播用户的转发表项，并向上行组播路由器申请组播节目视频流，同时向 ONU 发送扩展的组播控制 OAM 报文，通知 ONU 添加此组播用户的组播转发表。
5. ONU 根据 OAM 消息，配置此组播用户在本地的转发表。

可见，在这种模式下，组播权限配置和控制统一由 OLT 完成，OLT 是组播权限管理的主体，ONU 只负责对用户发出的 IGMP 协议报文添加标识组播用户的 VLAN ID 后发送到 OLT，同时执行 OLT 通过 OAM 消息下发的组播表项添加处理。OLT 本身还要支持 IGMP Proxy 功能，与上行的组播路由器配合，实现组播业务流的动态申请和转发。

4.11 组播 CAC

组播 CAC（Connection Admission Control）控制是以用户线路带宽为依据对用户点播新节目进行控制。

4.11.1 介绍

定义

组播 CAC 控制是以用户线路带宽为依据对用户点播新节目进行控制。用户点播新节目后，从设备上获知新节目带宽，设备查看用户线路带宽是否满足增加新节目带宽需求。如果满足，允许用户点播该节目，否则拒绝用户点播该节目。

目的

通过组播 CAC 控制，可以在理论上保证用户观看的节目带宽是符合实际带宽的需求的。因为如果线路带宽不满足节目需求的话，用户是不能点播对应节目的。

4.11.2 规格

MA5620/MA5626 支持以下组播 CAC 特性规格：

- 组播 CAC 功能全局开关控制。
- 支持组播用户最大带宽的设置。
- 支持用户已使用带宽的查询。
- 支持节目带宽管理。

4.11.3 原理描述

组播 CAC 由接入设备完成。

- 对于 GPON 端口：不但要根据用户的可用带宽与组播节目带宽，还要根据 GPON 端口的组播带宽来决定用户是否可以加入某个组播节目。
  - 当启用组播带宽管理时（组播 CAC 使能），如果用户请求加入某个组播节目时，系统将先匹配 GPON 端口的组播带宽。
  - 如果 GPON 端口的组播带宽够用，则再检查用户剩余带宽（用户配置的可用带宽-用户已在线节目带宽之和）与新要求的组播节目带宽进行比较。
  - 当 PON 端口带宽与用户剩余带宽都足够时，则将用户加入组播组，如果剩余带宽不够，则不响应用户请求。
  - 这样一来，可以保证用户观看的节目是满足带宽需求的。

  说明
  如果不使能组播的带宽管理功能（去使能组播 CAC），则系统不对组播节目的带宽做任何保证。当带宽得不到保证时，用户可以看到视频画面，只不过画面会出现马赛克、延迟等现象。

4.12 术语与缩略语

缩略语

缩略语	全称
IGMP	Internet Group Management Protocol（因特网组管理协议）
CAC	Connection Access Control（连接允许控制）

缩略语	全称
BRAS	Broadband Remote Access Server（宽带接入服务器）

5 语音

关于本章

本章主要介绍语音相关的特性。

5.1 介绍

5.2 规格

5.3 参考标准和协议

5.4 可获得性

5.5 H.248 语音特性
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。

5.6 SIP 语音特性
首先对 SIP 协议进行介绍，然后详细介绍 SIP 协议的原理。

5.7 语音关键特性
首先对语音关键特性进行简介，由于包含的子特性是比较多也比较零散的，因此主要是在原理描述部分分别详细阐述各子特性的原理。

5.8 语音线路接口特性
本章节介绍与语音接口相关的特性，包括振铃、Z 接口基本特性及增强特性。

5.9 语音测试及维护特性
语音测试及维护特性，包括内外线测试、仿真呼叫测试、导通测试、RTCP（Real-time Transport Control Protocol）统计等维护特性。

5.10 语音可靠性
主要介绍语音可靠性相关的特性，包括双归属组网、高可靠性传输（SCTP）及语音 QoS。

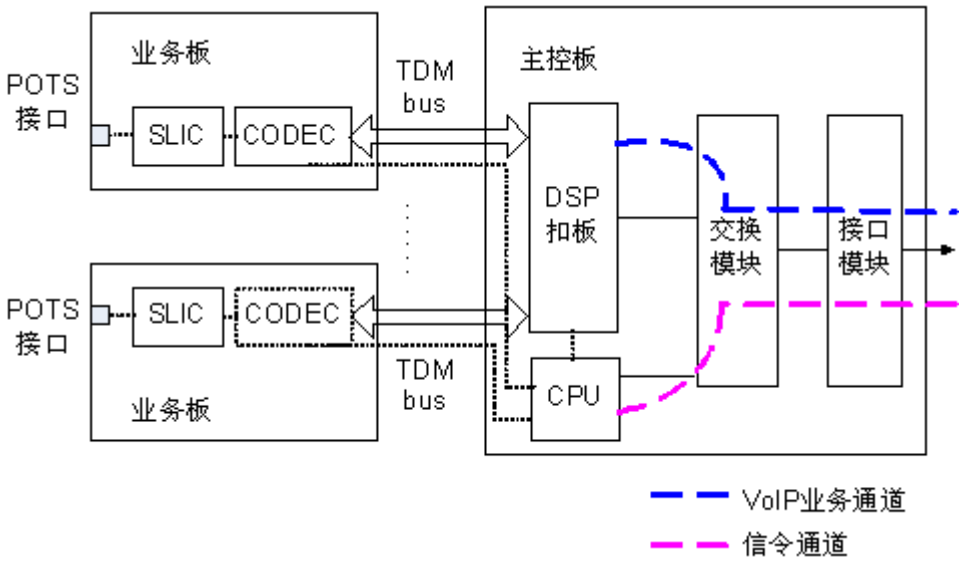
5.11 术语与缩略语

5.1 介绍

随着数据、语音、视频业务的三网合一，作为 FTTB 建设模型中的 MDU 接入设备，MA5620 不仅能够提供宽带业务（包括数据和视频直播、点播等业务），还能利用内置语音模块直接通过双绞线接入为终端用户提供高质量的语音业务。

MDU 语音整体方案示意图如图 5-1 所示。

图 5-1 MDU 语音整体方案示意图



其中，SLIC（Subscriber Line Interface Circuit）是用户线路接口电路的缩写，主要用途是用于向电话馈电、发送语音频率，生成振铃和检测用户摘机、挂机等信号，完成模拟信号的处理；CODEC 的作用主要是完成模拟信号及数字信号之间的转换；DSP 主要作用是处理音频（如语音编码、回声消除、DTMF 的生成与检测），完成数字信号到 VoIP 包的转换。

VoIP 业务通道及信令通道分别如图 5-1 中虚线所标示。各业务板上的语音业务通过 TDM 总线汇聚到主控板上的 DSP 扣板，DSP 扣板完成系统内所有语音业务的集中处理。CPU 完成所有语音信令相关的处理，包括信令报文的封装及解析、用户摘挂机处理、用户端口振铃等指令控制，同时完成对业务板的控制及管理。

Centrex 是“Central Office Exchange Service”的简称，即中心局交换业务，是指在相同企业中的用户可以配置在同一个 Centrex 群中，方便进行短号互拨及相关新业务的处理。在较多中小企业中，网关以解决话音业务为主，如果企业 1 与企业 2 分别为公司的总部和分部，通过定义一个基本用户群，可以实现 IP Centrex 功能。在 PSTN 及 NGN 组网下，交换机或软交换是支持 Centrex 群相关功能的，可以进行短号互拨及相关新业务。在 IMS 组网下，需要网关兼容支持该业务，支持群内呼叫及出群呼叫。同时在 IMS 的控制下，可以支持和 Centrex 群相关的新业务。

5.2 规格

- 支持 H.248、SIP 语音协议。
- 支持最大 24 个语音用户。
- 支持 VoIP/FoIP/MoIP，支持的业务具体如表 5-1 所示。

表 5-1 可支持的语音业务列表

类型	业务
SIP 基本呼叫业务	SIP 业务
	SIP 呼叫保持业务
	SIP 三方业务
	SIP 呼叫等待业务
	SIP 会议业务
	SIP 呼叫转移业务
	SIP 注册管理
	SIP 传真业务
	SIP Modem 业务
	SIP 主叫号码显示业务
	SIP 话费信息通知和显示业务（仅支持通话结束时的计费通知）
	SIP 留言灯业务
	SIP 恶意呼叫跟踪业务
	SIP Ua Profile 订阅
	计费业务
	区别振铃
H.248 业务	POTS 普通业务

类型	业务
	POTS 新业务： ● 支持主叫控制业务 ● 支持被叫控制业务 ● 支持双方控制业务 ● 支持互不控制业务 ● 支持呼叫等待业务 ● 支持呼叫转移业务 ● 支持呼叫前转业务 ● 支持同组代答业务 ● 支持指定代答业务 ● 支持三方通话业务 ● 支持会议呼叫业务 ● 主叫号码显示业务
	FoIP： ● 支持自切换传真 ● 支持 T.30 透传传真 ● 支持 T.38 传真 ● 支持传真参数的配置，支持 V2、V3 传真流程
	MoIP： ● 支持 Modem 透传方式 ● 支持自切换 Modem 流程 ● 支持软交换控制的 Modem 流程 ● 支持缓存上报模式 ● 支持立即上报模式 ● 支持低速 Modem ● 支持高速 Modem
	计费业务
	留言灯业务
	区别振铃
	话费立显
	DTMF 传输

- 支持 G.711a/μ 编解码，打包时长：10ms，20ms 和 30ms。
- 支持 G.729 编解码，打包时长：10ms，20ms 和 30ms。
- 支持 RFC2833、RFC2198、回音检测（EC）、静音检测（VAD）、双音多频（DTMF）、Modem 质量增强等语音特性。

- 支持内外线测试、呼叫仿真测试、导通测试。
- 支持 RTCP 统计、H.248 性能统计、呼叫统计。
- 支持远程抓包、E2E 信令分析。
- 支持 H.248 和 SIP 双归属。
- 支持 RFC2833 加密，支持 H.248 鉴权。
- 支持设置报文 802.1p 优先级（媒体和信令可分开设置），支持 ToS。
- 支持 8K Byte 长的 digital MAP。
- 支持 Centrex 功能，包括：
  - 支持配置数图模式直接拨出 Centrex。
  - 支持配置数图模式二次拨出 Centrex。
  - 支持用户配置出群数据直接拨出 Centrex。
  - 支持用户配置出群数据二次拨出 Centrex。
  - 支持订阅出群数据直接拨出 Centrex。
  - 支持订阅出群数据二次拨出 Centrex。
  - 支持 Profile 配置是否上报出群字冠。

5.3 参考标准和协议

与 Centrex 特性相关的参考标准和协议：

- ETSI TS 182 024 V2.1.1
- ETSI TS 181 019 V2.0.0
- ETSI TS 181 005 V2.4.1
- ETSI TR 102 647 V1.2.1
- ETSI TR 184 005 V1.1.1
- ETSI TR 181 003 V1.1.1
- ETSI TS 102 477 V1.1.1
- ETSI TS 102 478 V1.1.1

与其它语音特性相关的参考标准和协议：

- ITU-T G.711、ITU-T G.729、ITU-T G.723
- ITU-T G.168、ITU-T G.131、ITU-T G.161
- ITU-T Q.24、ITU-T G.107
- RFC 2833: RTP Payload for DTMF Digits,Telephony Tones and Telephony Signals
- RFC 3611
- RFC 3525 H.248 协议
- RFC 3262: Reliability Of Provisional Responses in the Session Initiation Protocol (SIP)
- RFC 3263: SIP Locating SIP Servers

5.4 可获得性

软件上，语音特性包含在基本软件包中；硬件上，需配置语音业务板及 DSP 扣板。

涉及网元

语音特性需要 NGN 或者 IMS 等核心网网络中的设备配合支持。

Centrex 业务特性需要 IMS 支持 Centrex 群配置及相关功能的使用。

版本支持

表 5-2 语音特性最低版本支持

产品	支持版本
MA5620	V800R308

5.5 H.248 语音特性

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。

5.5.1 介绍

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：

- 支持更多类型的接入技术；H248 标准化方面做得更完善和健全。
- 能够支持更大规模的网络应用，而且更便于对协议进行扩充，因而灵活性更强。
- H.248 消息可以基于 UDP/SCTP 等多种协议承载。

5.5.2 原理描述

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

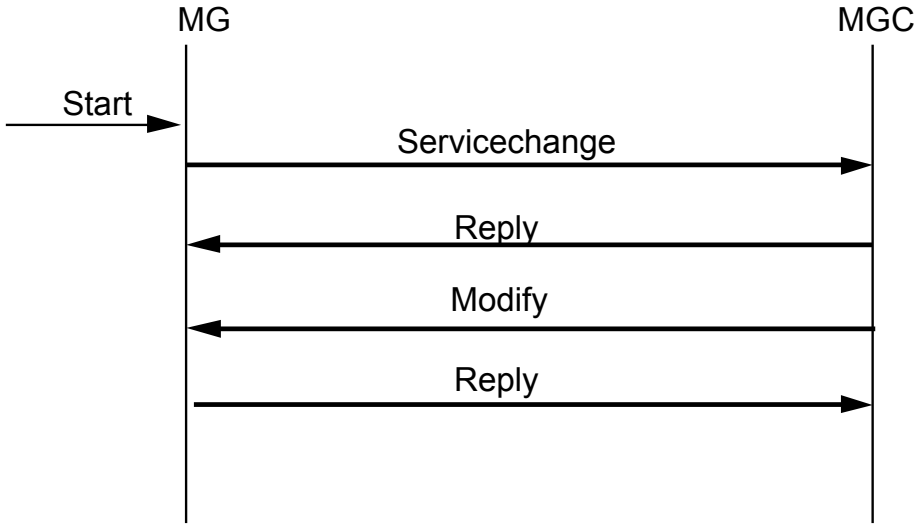
MG 通过 ServiceChangeRequest 命令通知 MGC 某一个或者某一组用户将进入或者退出服务，此命令交互成功后直接影响到端点状态改变为“InService”或者“out of service”。同时，MGC 也可以通过主动发送 ServiceChangeRequest 命令使 MG 上的某一个或者某一组端点进入或者退出服务。

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 5-2 所示。

图 5-2 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）。

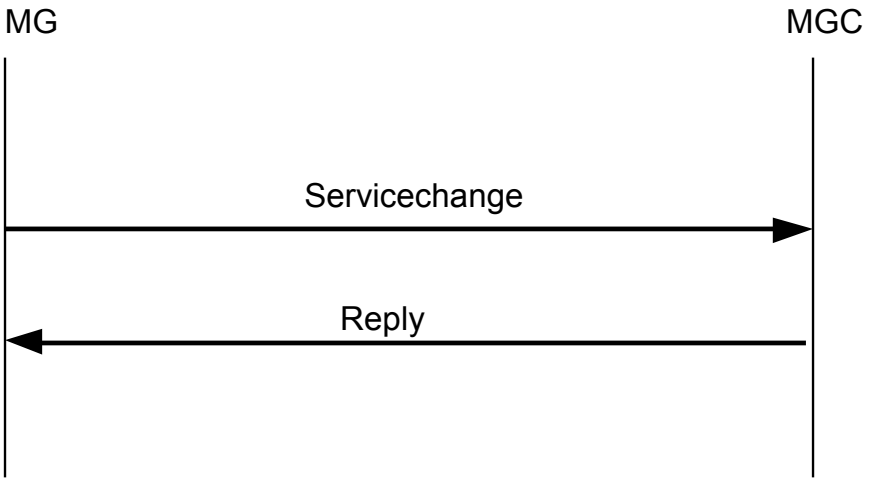
当从第一次 MG 向 MGC 发起心跳开始，在配置的接口心跳时间长度内（譬如发送 3 次心跳消息），如果没有收到 MGC 的心跳响应，将会把接口状态置为“等待响应”态。之后 MG 会一直向 MGC 发起注册，如果配置了双归属，将会在在两个 MGC 之间轮询

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 5-3 所示。

图 5-3 网关主动注销流程图

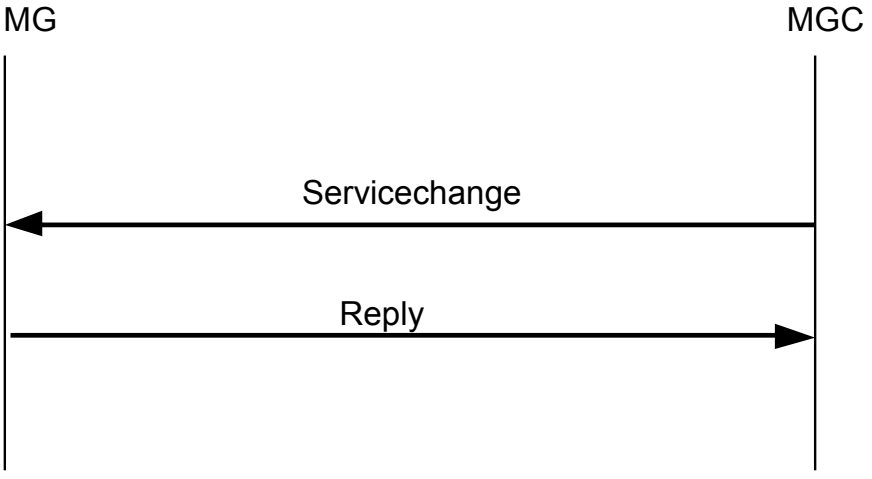


流程说明：

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 5-4 所示。

图 5-4 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。

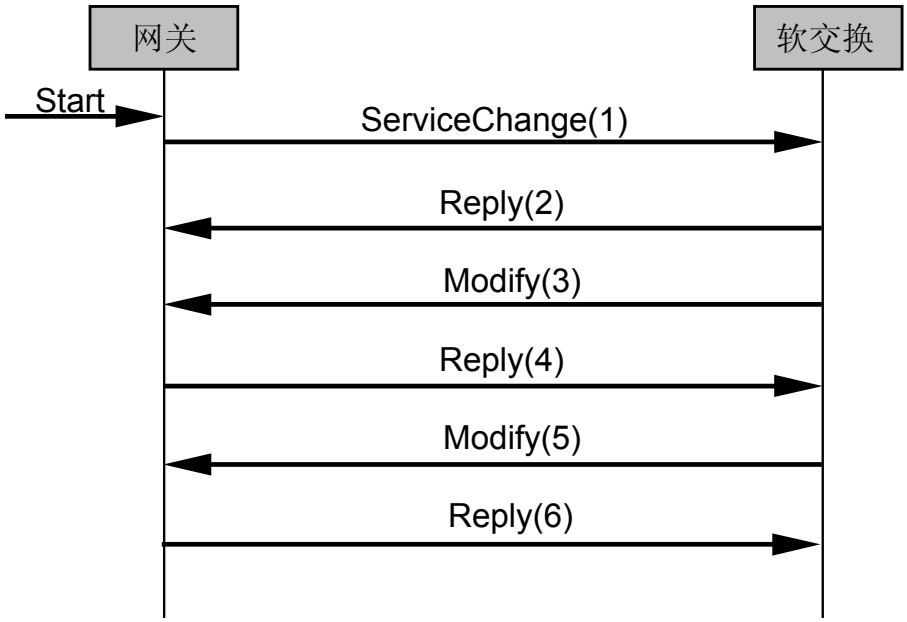
H.248 接口鉴权机制

鉴权是媒体网关控制器（MGC）为了验证识别 MG（即 MDU）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 5-5 所示。

图 5-5 鉴权流程图



鉴权流程如下：

1. 网关（此处指 MDU 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。

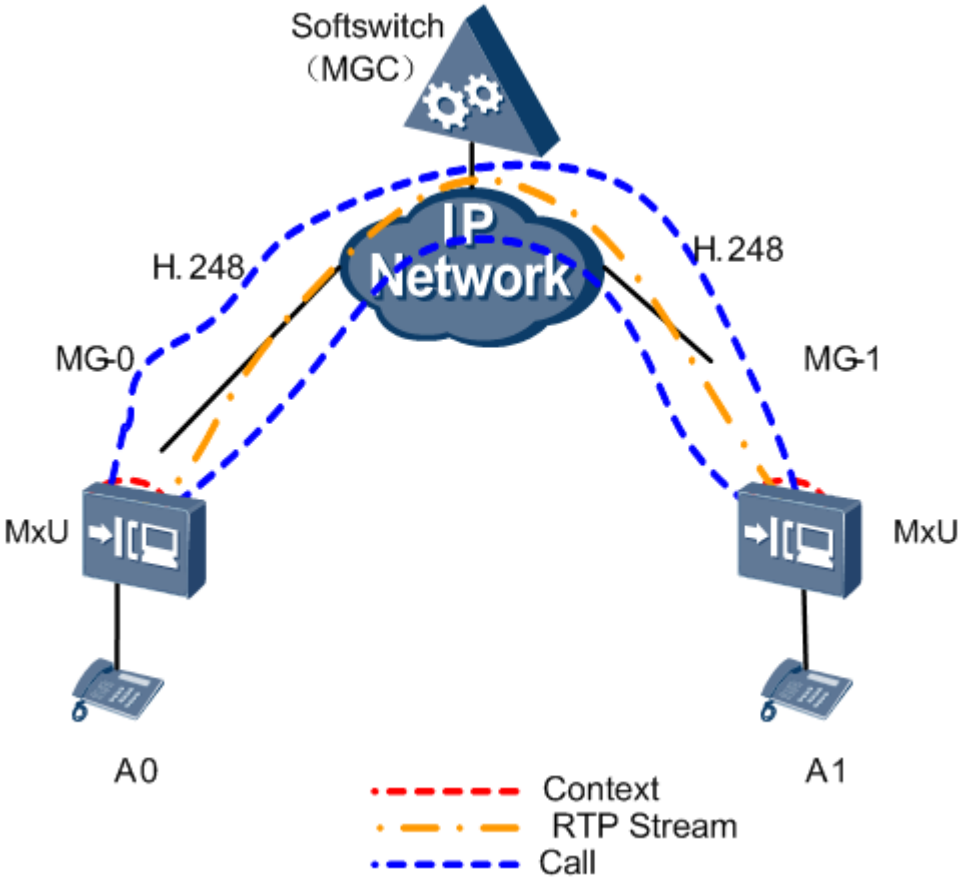
6. 网关对软交换进行应答。

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 5-6 所示。

图 5-6 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 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。

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 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。
6. 回音检测（EC）、静音检测（VAD）和工作模式的设置如下：
   (1) 低速 Modem：EC 为 ON，VAD 为 OFF，DSP 工作模式为 Modem 方式。
   (2) 高速 Modem：EC 为 OFF，VAD 为 OFF，DSP 工作模式为 Modem 方式。
7. Modem 结束后，如果继续进行通话，由于没有 Modem 结束事件，DSP 工作模式不会自动从 Modem 模式切换到语音工作模式，所以通话质量可能会有影响。

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。

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 和自切换下的 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. 在网关和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

自切换下的 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。

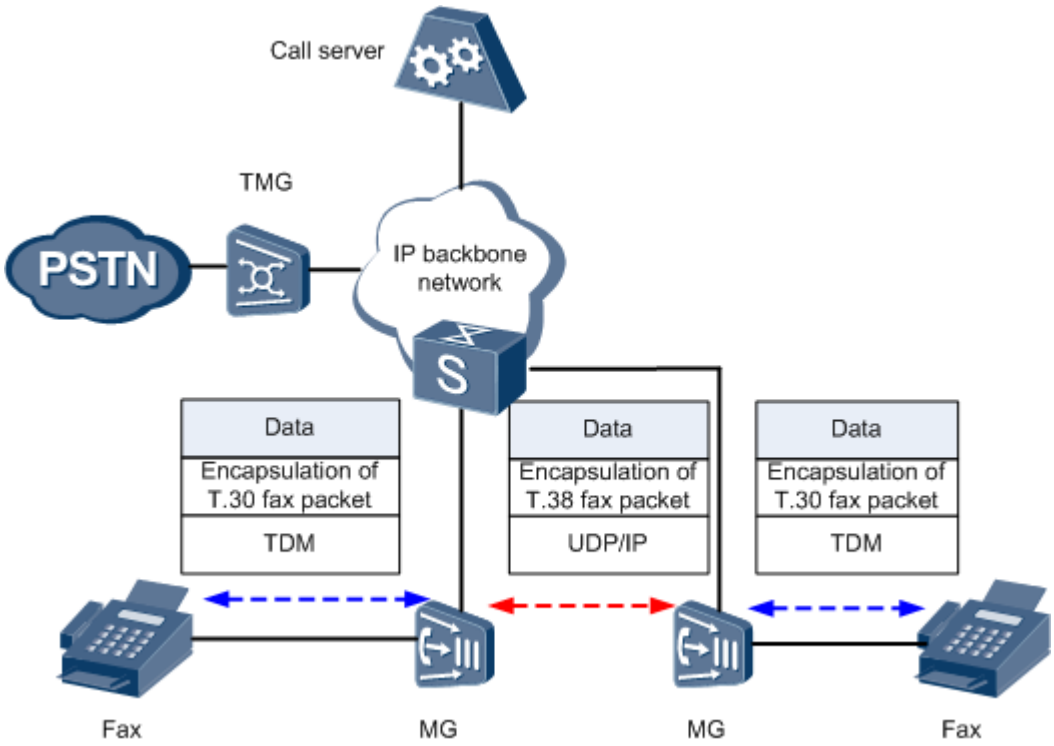
传真常用协议

分组语音网络中实现传真涉及到两个传真常用协议：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 网络的丢报、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 5-7 所示。

图 5-7 T.38 传真的实现原理图



5.6 SIP 语音特性

首先对 SIP 协议进行介绍，然后详细介绍 SIP 协议的原理。

5.6.1 介绍

定义

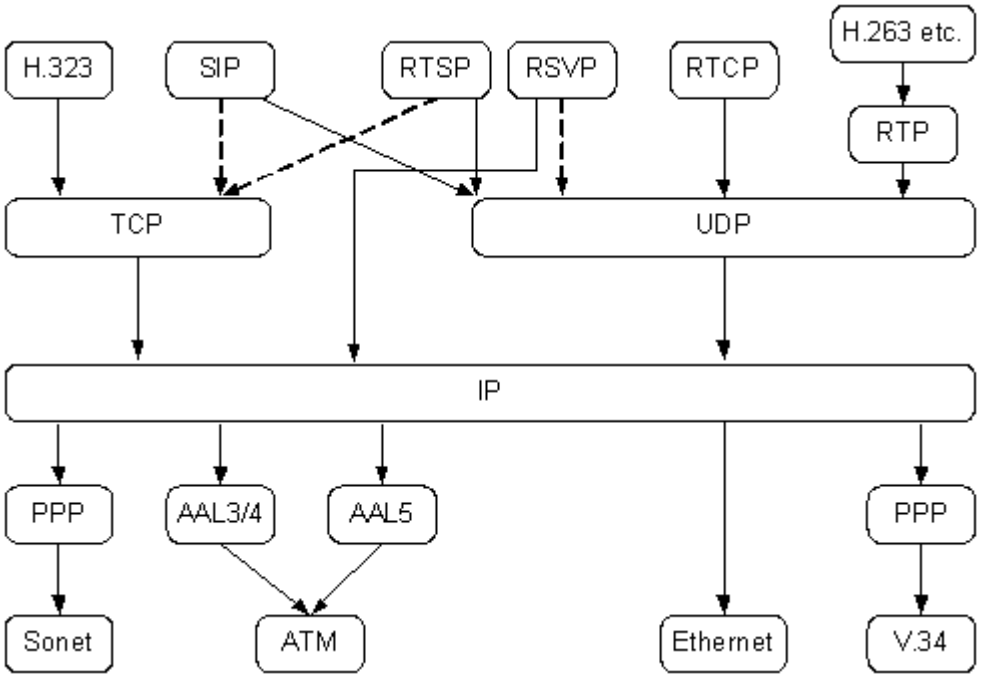
SIP（Session Initiation Protocol）协议是一个用于建立，更改和终止多媒体会话或呼叫的应用层协议。多媒体会话可以是多媒体会议，远程教学，因特网电话等各种应用。SIP 协议可用于发起会话，也可以用于邀请成员加入已经用其它方式建立的会话。SIP 协议透明地支持名字映射和重定向服务，便于实现 ISDN，智能网以及个人移动业务。一旦建立会话，媒体流将使用 RTP 协议在承载层中直接传送。

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 5-8 所示。

图 5-8 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 协议也可以和其它呼叫建立和信令协议配合。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 可以用来确定被叫通过 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-weight signaling），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。

5.6.2 原理描述

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

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 5-3 所示。

表 5-3 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
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 5-4 所示。

表 5-4 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。

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 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。

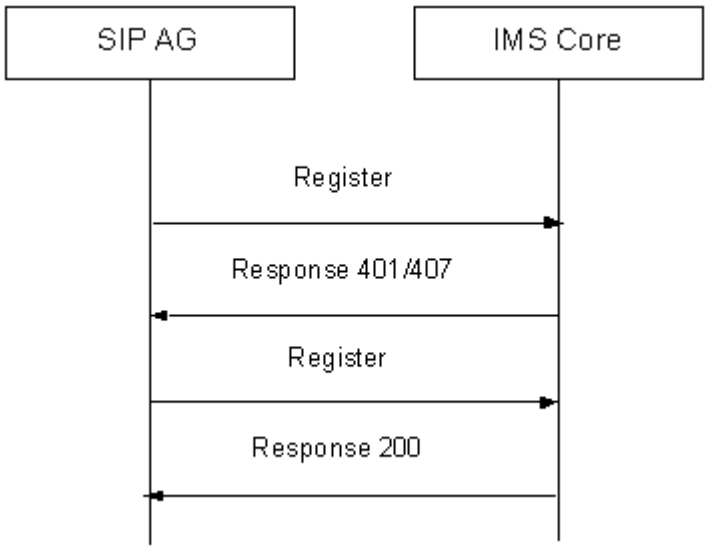
无安全性连接的注册流程

图 5-9 无安全性连接的注册流程图

如图 5-9 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，判断该用户是否在 IMS 已配置，若配置 OK，回应 RESPONSE 200 给 SIP AG

安全性连接的注册流程

图 5-10 安全性连接的注册流程图



如图 5-10 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。

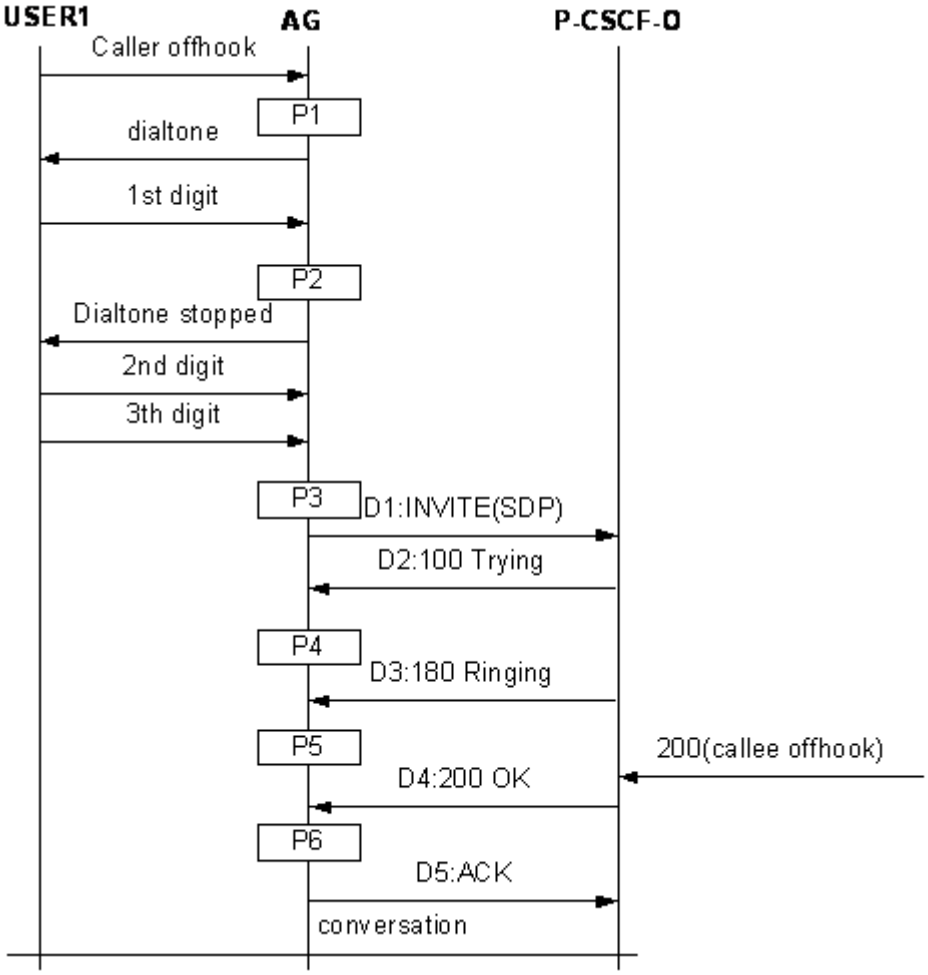
IMS Core 回复 401/407，其中包含密钥及加密方式等信息，SIP AG 用此密钥加密该用户的用户名和密码，重新构造 REGISTER 请求消息发送给 IMS，IMS 解密后判断用户名和密码是否正确，若正确回复 200。

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 5-11 所示。

图 5-11 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：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 给主叫用户停回铃音，流模式改为双向。接着，构造 ACK 消息发送到 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：

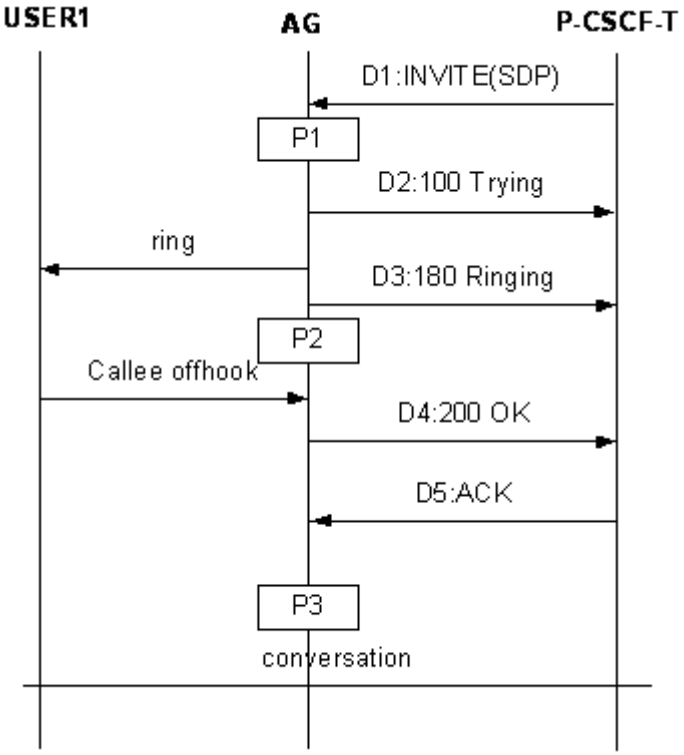
- 若主叫有数据但未注册，则拒绝主叫呼叫，回复 403。
- 若没有用户数据，则拒绝主叫呼叫，回复 404。

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 5-12 所示。

图 5-12 SIP 协议的 VoIP 被叫流程图



- P1：AG 收到 P-CSCF 过来的 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（如果使用 TEL-URI，实际上可以不要这个头域，根据 TEL-URI 上的电话号码即可找到被叫用户）。找到被叫后，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：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：

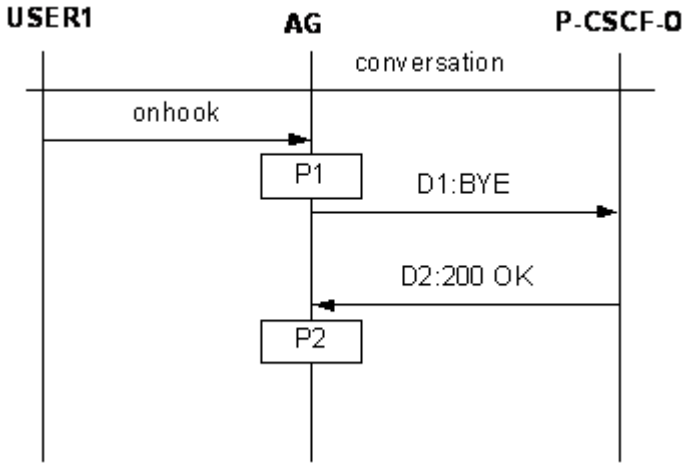
- 若被叫用户有数据但未注册，则拒绝主叫呼叫，回复 403。
- 若没有被叫用户数据，则拒绝主叫呼叫，回复 404。

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 5-13 所示

图 5-13 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，释放分配给该用户的 DSP 资源。
- P2：AG 收到 P-CSCF 的 200 消息。

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，和对端进行传真方式的协商。

实际上，根据速率的不同，传真还可以分为低速传真和高速传真两种。不过高速传真是不能使用 T.38 的，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

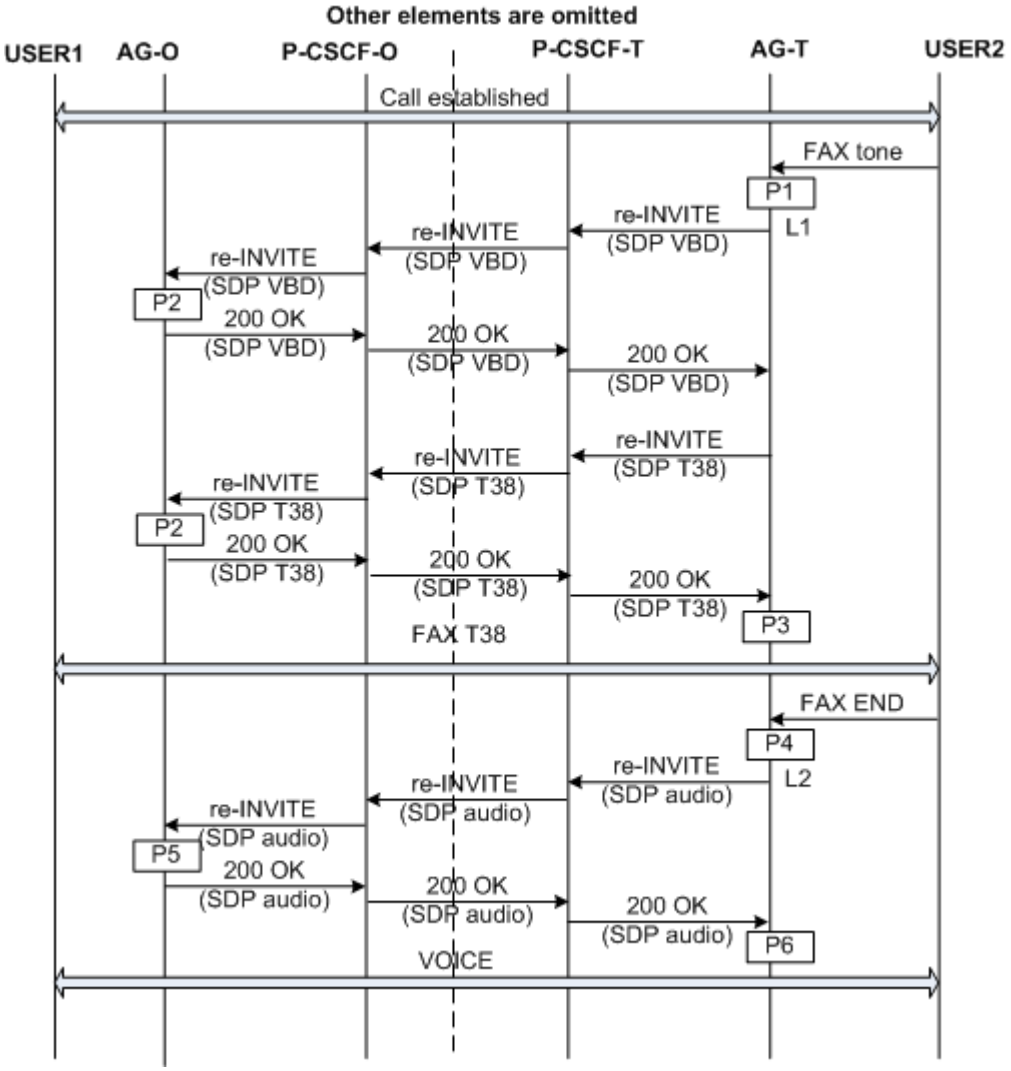
目前协商透传传真有三种方式。

- 第一种是以 a=fax 表示，由中国电信提出的 g711 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 g711 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，则根据参数配置来确定。

流程如图 5-14 所示。

图 5-14 FAX 协商切换透传流程图



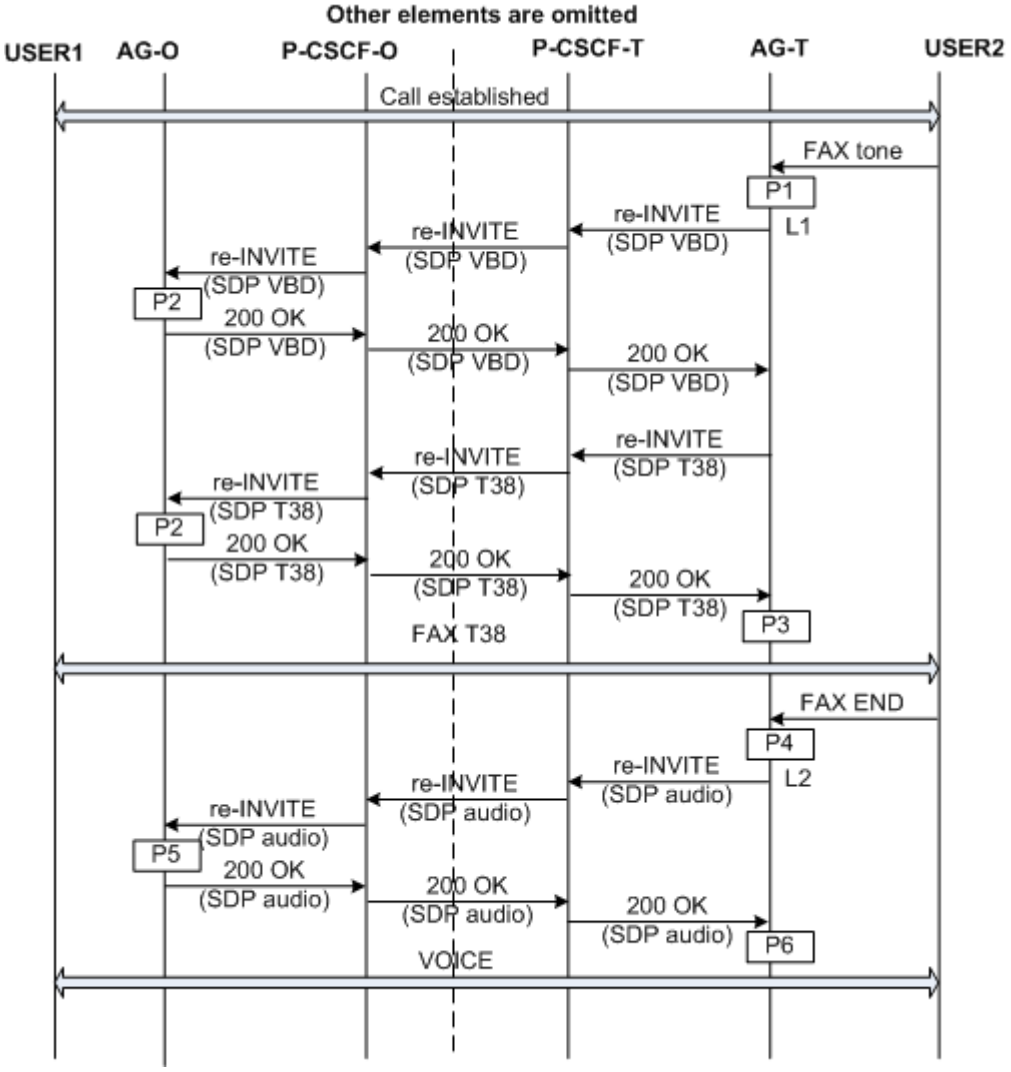
- P1：AG-T 先检测到 FAX 音，发送 re-INVITE 消息到主叫用户所在的 AG（AG-O）。
- L1：re-INVITE 消息携带的 SDP 消息可能有三种。在 AG 中，需要配置使用哪种 FAX 的透传协商流程。协商的发起方根据配置来使用不同的 a 参数，协商的接受方则需要兼容三种方式，即收到的 re-INVITE 消息里，无论使用哪种 a 参数，都可以完成协商流程。
  - 第一种是 draft-ietf-sipping-realtimefax-01.txt 提出的 g711 透传 FAX/MODEM 的方式。
  - 第二种是中国电信提出的 g711 透传 FAX/MODEM 的方式。
  - 第三种是 V.152 定义的 VBD 方式。
- P2：AG-O 收到 re-INVITE 消息。然后构造 200 消息给 AG-T。
- P3：AG-T 收到 200 OK 消息，则也使用 FAX 方式来打开 DSP 通道。
- P4：AG-T 收到传真结束信号，发送 re-INVITE 消息到 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，也也会为语音模式。

FAX 协商切换 T.38 流程

FAX 协商切换 T.38 流程如图 5-15 所示。

图 5-15 FAX 协商切换 T.38 流程图



- P1：AG-T 先检测到 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 消息给 AG-T。
- P3：AG-T 收到 200 OK 消息，则也使用 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 消息到 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，也也会为语音模式。

说明

如果对端设备不支持 T.38，则流程如下边的图 5-16 和图 5-17 所示。

图 5-16 FAX 协商切换 T.38 流程图（对端不支持 T .38 的情况 1 ）

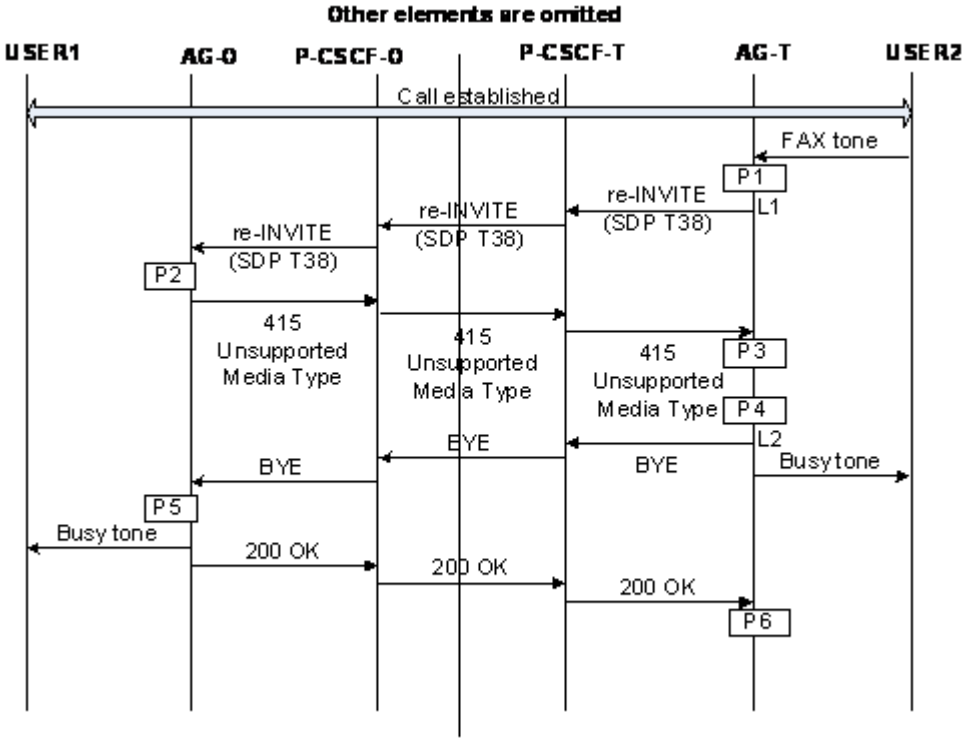
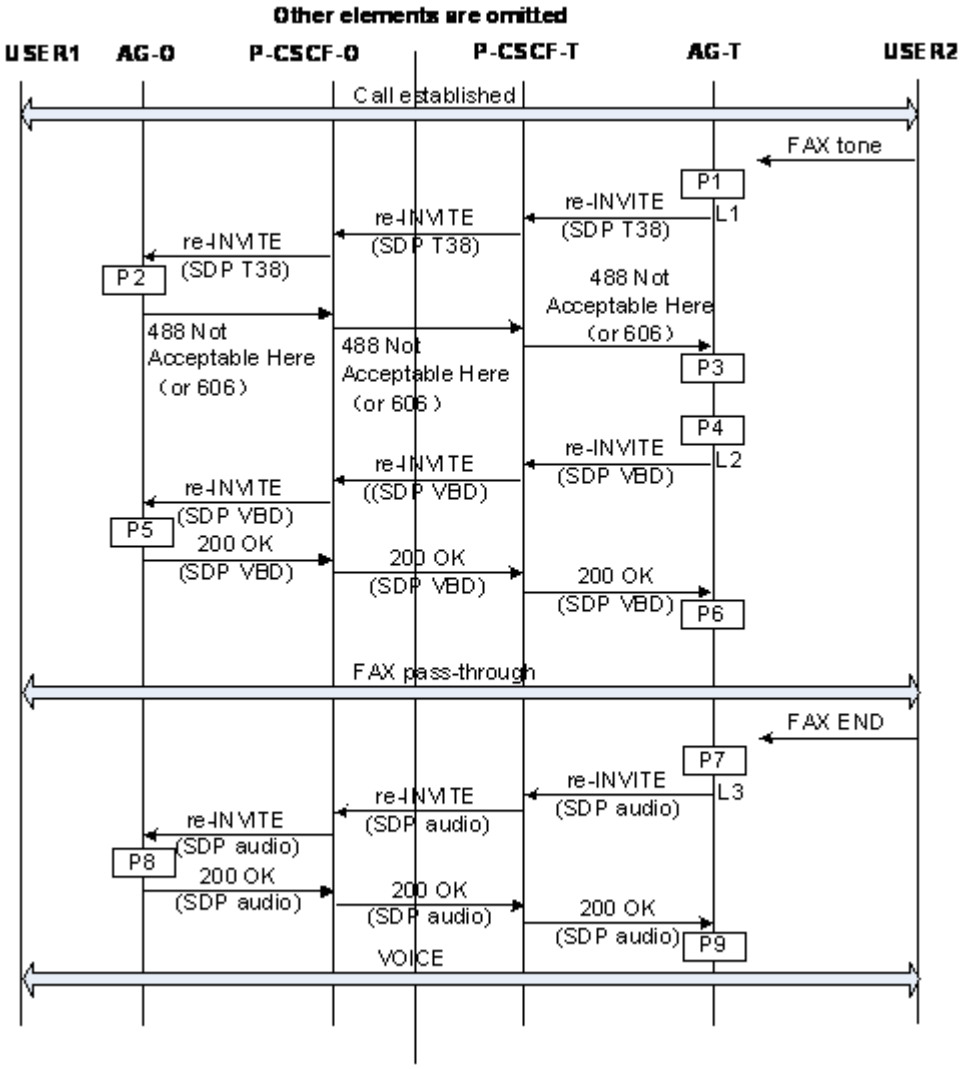


图 5-17 FAX 协商切换 T.38 流程图（对端不支持 T .38 的情况 2 ）



如果 AG-O 不支持 T.38，则可能回 415 Unsupported Media Type，AG-T 收到 415 响应，则发送 BYE，释放当前的呼叫。如果 AG-O 不支持 T.38，则会回 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。

MDU 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 G711 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 G711 的语音包。这就要求 DSP 芯片可以在 G.729 或者其他编解码方式下，可以接收 G711 的包。当然了，DSP 检测 IP 侧的传真音并上报是必须的。

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，只不过收到 FAX 音后，使用 T.38 模式打开 DSP 通道，而不是使用 FAX 透传模式。

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：

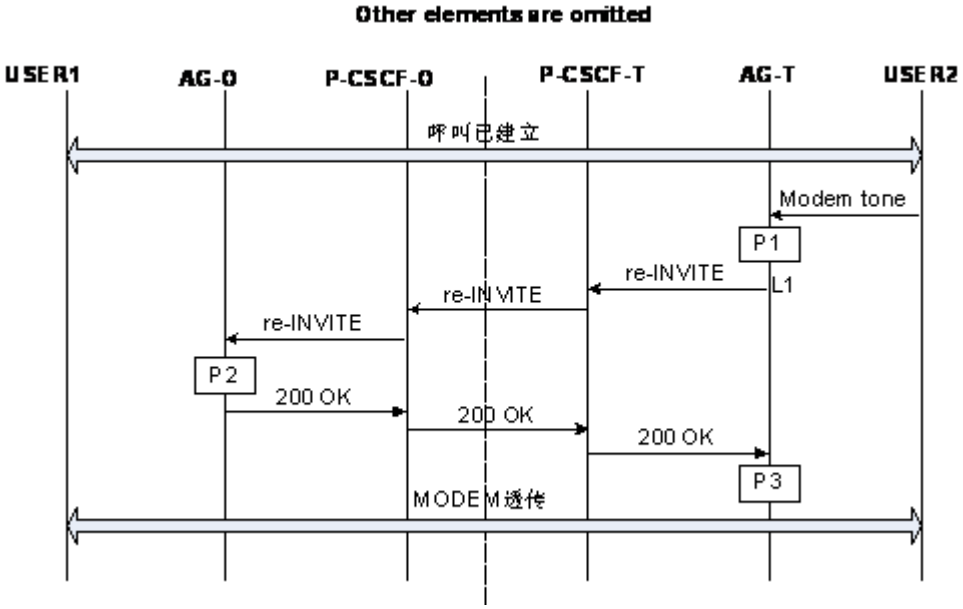
- 第一种是以 a=Modem 表示。这是由中国电信提出的 g711 透传 Modem 的方式。
- 第二种是以 a=silenceSupp:off 表示。这是 draft-ietf-sipping-realtimefax-01.txt 提出的 g711 透传 Modem 的方式。
- 第三种是 VBD 的方式，表示方式 a=gpmd:99 vbd=yes。这是 V.152 定义的 VBD 方式。

具体采用哪种方式进行传真，则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 5-18 所示。

图 5-18 MODEM 协商切换流程图



- P1：AG-T 先检测到 MODEM 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 中，需要配置使用哪种 MODEM 的透传流程。
- P2：AG-O 收到 re-INVITE 消息。然后构造 200 消息给 AG-T。

- P3：AG-T 收到 200 OK 消息，则也使用 FAX 或者 MODEM 方式来打开 DSP 通道。

MODEM 自切换

MODEM 自切换是说 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。目前我们的 DSP 芯片已经支持 RFC2198 方式下的 MODEM，不过只能支持一个冗余包。

5.7 语音关键特性

首先对语音关键特性进行简介，由于包含的子特性是比较多也比较零散的，因此主要是在原理描述部分分别详细阐述各子特性的原理。

5.7.1 介绍

定义

语音关键特性是指为提供高质量语音服务所采用的一系列技术，例如语音编解码、回声消除（Echo Canceller）、语音动态检测(VAD)等技术。

目的

提供高质量的语音服务。

5.7.2 原理描述

编解码/打包时长

介绍编解码/打包时长。

介绍

编解码是语音的核心技术。编码是 DSP 将 TDM 的语音数据进行编码，组成分组报文发送到 IP 网络上。解码是 DSP 将收到的网络的语音分组报文进行解码，并播放到 TDM 侧。

常用的编解码类型有 G.711a、G.711μ、G.729、G.723.1Low、G.723.1High。其中 G.711a、G.711μ 是无损伤的编码。G.729、G.723.1Low、G.723.1High 是有损伤的压缩编码，压缩编码所占的带宽小，但是语音质量差、延时大（G.711 话音质量最好，但需要 64K 的带宽，G.723 占用的带宽小，话音质量就有损耗）。

打包时长可以理解为 DSP 组装语音分组报文的时间间隔，不同编码支持的打包时长不同。编码方式如表 5-5 所示。

表 5-5 编码方式比较表

编码方式	编码速率（kbit/s）	报文大小（包括 RTP 头、UDP 头、IP 头和以太网头在内）
G.711a/μ	64	20 毫秒打包，214bytes
G.729	8	20 毫秒打包，74bytes
G.723.1High	6.3	30 毫秒打包，78bytes
G.723.1Low	5.3	30 毫秒打包，74bytes

版本支持情况

支持 64 路 G.711a、G.711μ 或 32 路 G.729，不支持 G.723.1。

Echo Canceller（回声消除）

介绍 Echo Canceller（回声消除）。

介绍

Echo Canceller 即回声消除。

回声（Echo）包括声学回声和线路回声：

- 声学回声

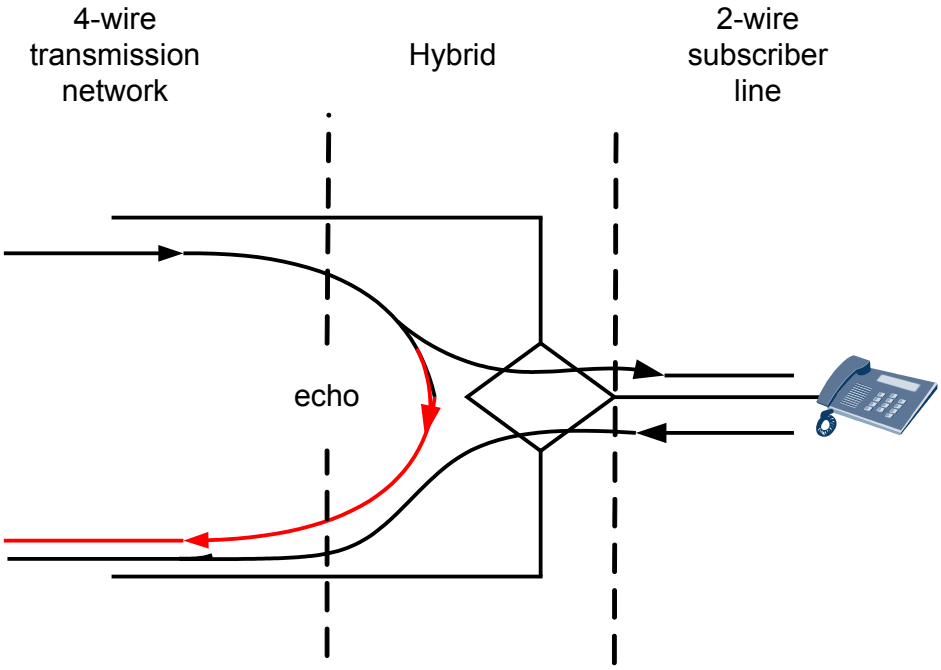
  声学回声是指声音遇到障碍物反射回来产生的回音，如通话时将一侧话机的话筒放在桌面上另一侧说话的人通常能听到自己的声音，是因为听筒的声音经桌面反射到话筒中导致的，这就是声学回声。由于无法判别是正常语音还是声学回声，目前 VOIP 的 DSP 都不支持声学回声的消除。

- 线路回声

  线路回声是由于用户板的二四线转换引起的，因为二四线转换线圈的阻抗无法做到完全匹配，通常说的回声消除就是指线路回声的消除。

线路回声产生如图 5-19 所示。

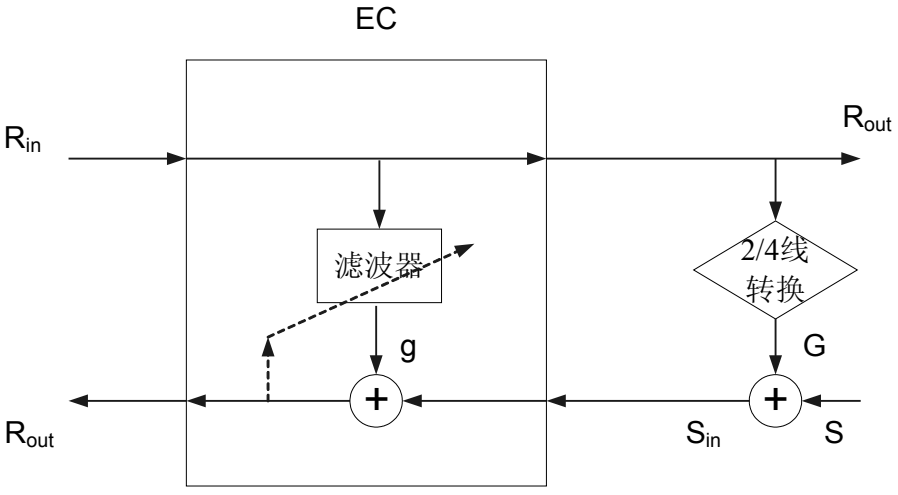
图 5-19 线路回声产生原理图



在传统的 PSTN 中由于时延小，人的说话声音和回声几乎同时传入人耳，所以感觉不到回声的存在。在 VoIP 中由于时延较大，人的说话声音传入人耳后，过一段时间回声才传入人耳，人就能够特别明显的感觉到回声的存在，ITU-T G.131 和 ITU-T G.161 指出当回波延时超过 25 毫秒时，回声可以被人感觉出来。

EC（Echo Canceller）回声消除，实现原理如图 5-20 所示。

图 5-20 EC （Echo Canceller）回声消除原理图



Rin 为从远端接收到的语音，作为滤波器的输入得到了模拟的回声 g，Rin 在 2/4 线转换为回声 G，S 为近端语音，即本端话筒输入的声音，近端语音和回声叠加成了 EC 的发送输入信号 Sin，EC 用输入的 Sin 信号减去模拟的回声 g 就得到了输出信号 Sout，即：

Sin = S + G

Sout = Sin － g = S + G － g

因为 G ≈ g，所以 Sout ≈ S

版本支持情况

支持 EC 的开/关配置，支持 64ms 的 EC 尾长延时。

NLP（非线性处理器）

介绍 NLP（非线性处理器）的基本原理。

介绍

NLP （NoLinear Processor）即非线性处理器。EC 由于种种原因不能将回波完全抵消，即存在残留回波。为提高 EC 性能，在残留回波功率小到一定程度后，对其进行某种非线性处理，可以进一步减小残留回波功率。一种简单的方法是用静音替代残余回波，即当残余回波信号小于一定门限时，强制残余回波信号为 0 。

版本支持情况

支持 NLP 的开/关配置（基于用户端口）。

影响

FoIP MoIP 时需要关闭 NLP 功能。

VAD（语音动态检测）

介绍 VAD（语音动态检测）的基本原理。

介绍

VAD （Voice Activity Detector）即语音动态检测。其用途在于减小网络带宽的消耗。

话机的输入信号分为语音和静音两类，VAD 检测就是用来区分语音和静音的，主要的检测方法就是通过信号的能量进行判断。

VAD 通常与静音压缩绑定使用。例如：配置 VAD ON，DSP 检测是语音信号时才会打 RTP 包发送到远端，若是静音，DSP 不会向 IP 侧发送 RTP 包，只有当背景噪声变化时 DSP 会给远端发送一个静音标识（Silence ID）包通知远端，远端 DSP 根据 SID 中带的信息产生背景噪声，即在静音时能够节省网络带宽。

一次通话有效的语音大约为 40%，在网络资源紧张的运营环境下使能 VAD 能够大大减小网络带宽的消耗。

版本支持情况：

支持 VAD 的开/关配置，支持 SID 包发送和接收。

PLC（丢包补偿）

介绍 PLC（丢包补偿）的基本原理。

介绍

PLC（Packet Loss Concealment）即丢包补偿。

网络或设备出现丢包会影响语音质量，在实际环境中丢包是很难避免的，通过 PLC 对丢失的信号进行补偿可以减少丢包对语音质量的影响，提高 FoIP 及 MoIP 在丢包情况下的成功率。

PLC 的补偿有三种方式：对丢失的包用静音来补偿、用丢失的包的前一个包来补偿、通过丢失包的前后包的能量计算出一个近似的包来补偿（G.711 Appendix I），三种补偿算法对丢包语音质量的提升依次由低到高，对 DSP 资源的消耗依次由低到高。

版本支持情况

支持 PLC 开关设置和 G.711 Appendix I 补偿配置。默认支持用丢失的包的前一个包来补偿的方式。

JB（去抖动缓冲）

介绍 JB（去抖动缓冲）的基本原理。

介绍

JB（Jitter Buffer）即去抖动缓冲。

由于网络侧传输无 QOS 保证，远端匀速发送的数据包到达近端时的时间间隔并不均匀，甚至可能发生了乱序，从而导致语音质量下降。Jitter buffer（去抖动缓冲）用来消除 IP 侧抖动，其最基本的思想是以增加时延换取数据包的正确顺序并降低丢包率。

JB 分为：动态 JB 和静态 JB。

在一次通话过程中可能某段时间的网络抖动小或没有、某段时间的网络抖动很大，动态 JB 可以根据网络抖动的大小调整缓冲的深度，确保在抖动小时缓冲引入的时延小，在抖动大时有足够的缓冲深度来消除抖动。在 FoIP/MoIP 等数据业务时需要使用静态 JB，因为 JB 调整可能导致丢包，且丢包对数据业务影响很大。

版本支持情况

支持动态 JB 和静态 JB，支持的 JB 最大调整深度为 150ms。

DTMF（双音多频）

介绍 DTMF（双音多频）的基本原理。

介绍

DTMF（Dual Tone Multi Frequency）双音多频用两个频率的音叠加来表示号码，如表 5-6 所示。

表 5-6 双音多频对应数字表

单位:Hz	1209	1336	1477	1633
697	1	2	3	A

770	4	5	6	B
852	7	8	9	C
941	*	0	#	D

话机拨号时将对应的号码转换为双频的叠加音，DSP 通过检测双音多频来检测用户拨的号码。

支持 DTMF 相关功能有：DTMF 擦除、DTMF 透传、DTMF 的 2833 传输、RFC2198 冗余 2833，DTMF 擦除是 DSP 检测 DTMF 后将 DTMF 信号从 RTP 媒体流中擦除掉，DTMF 透传是 DSP 检测 DTMF 后 RTP 媒体流中仍保留 DTMF 信号，DTMF 的 2833 传输是 DSP 检测 DTMF 后将 DTMF 信号从 RTP 媒体流中擦除掉，并用 RFC2833 来传输 DTMF 信息。

版本支持情况

支持 DTMF 的检测和发送。

支持 DTMF 相关功能的配置（基于设备）。

Tone（放音）

介绍设备对用户放音的基本原理。

介绍

在主控板 FLASH 中保存有语音文件（通常文件名：voice.efs），语音文件中有一个区域对 DSP 支持的放音类型进行了描述，该描述包含了以下内容：信号音类型，频率，持续时间，强度。在系统初始化完成后，放音参数被配置到 DSP 参数中，当需要给用户放音时 DSP 通过读取这些信息，实时产生出给用户播放的信号音。

语音文件包括参数音、波形音、Announcement。

参数音是简单音，如：拨号音、忙音、回铃音等，将参数音的频率、能量、持续时间、节拍等属性下发给 DSP，由 DSP 来产生。

波形音也是拨号音、忙音、回铃音等简单音，实现方法是事先将拨号音、忙音、回铃音等简单音进行录音，将录音数据转换成 PCM 数据存放在 POTS 板中，POTS 板循环地向某个 TDM 时隙放某种音的数据，当某个用户需要听时就将该用户对应的时隙连到 POTS 板的放音时隙上。优选参数音，在 DSP 故障或没有 DSP 资源时再使用波形音。

Announcement 是告示音，如“用户忙，请稍后再拨”的提示音，实现方法是将需要播放的语音进行录音，将录音数据存放在 DSP 内，当某个用户需要听语音提示时 DSP 就将事先录制的语音数据播放给用户听。

版本支持情况

- 支持参数音、波形音和 Announcement 的播放。
- DSP 可以存放 1Mbytes 的 Announcement 语音数据。
- 支持 64 路播放 Announcement。

Fax/Modem 质量增强

介绍传真和 Modem 在 IP 网络中质量增强的基本原理。

介绍

IP 网络替换 PSTN 网络后，VOIP 下的 FAX、MODEM 使用也越来越普遍，需要我们 AG 设备能够提供比拟 PSTN 网络的应用效果。目前媒体网关对 FAX、Modem 的应用多采用 VBD（voice band data）透传方式，而透传对承载网络有较大的依赖性，网络质量的下降会直接导致业务失败。

Fax/Modem 质量增强特性主要应对于 IP 网络质量较差的情况，改善 Fax/Modem 业务的接通率和在线时长。例如在商场或银行等使用 MODEM 连接 POS 终端场景下，使用此特性可以提高 Modem 稳定性和在线时长，减少因网络质量引起的断线。

Fax/Modem 质量增强特性主要包括 RFC2198 智能启动和 10ms 打包功能。使能该特性后，当检测到网络丢包后，自动启动 RFC2198 和 10ms 打包功能。

RFC2198 标准利用了数据流冗余机制减少网络丢包对业务质量产生的影响，在网络平均连续丢包率较低的情况下，接收方可以根据后续包中的冗余数据对丢失的包进行重组和恢复。采用 RFC2198 中描述的音频冗余机制可以用于恢复数据包中丢失的事件和 RFC2833 的方式处理 RTP 包中传送双音多频数字 dual-tone multifrequency （DTMF）信号。

10ms 打包比 20ms 打包承载信息少，如果有丢包现象对业务的影响比较小。

表 5-7 是采用增强特性前后测试数据对比，很明显可以看出使用增强特性可以明显改善业务稳定性。

表 5-7 增强特性前后测试数据

Modem 型号	打包时长	网络丢包率（随机丢包）	在线时长
T336CX	20ms	0.10%	22Hour
		0.50%	1.5Hour
		1.00%	基本不可用
		1.00%（rfc2198）	12.5Hour
	10ms	0.10%	>24Hour
		0.50%	22.5Hour
		1.00%	5.5Hour
		1.00%（rfc2198）	24Hour

版本支持情况

支持 Fax/Modem 质量增加特性。

RFC2833 加密

介绍 RFC2833 加密技术的背景和基本原理。

背景介绍

在 NGN 网络中，语音和 DTMF 信号被封装成 IP 包的方式在 IP 网络中传送。DTMF 信息在语音的 RTP 报文中以两种方式传送，一种是 DTMF 的双频信号在 RTP 媒体流中传送，另外是用 RFC2833 来传送 DTMF 信息，并将 RTP 媒体流中的 DTMF 双频信号擦除，以下将分别介绍这两种方式。

- 当 DTMF 信号在 NGN 网络中以媒体流的方式传送时，发送侧的媒体网关（MG）只是简单测量声音波段信号的频率成分并将这些信息通过 RTP 报文发送到接收侧的媒体网关（MG）。在这种模式下，收发端的媒体网关将 DTMF 信号按照话音信号来处理，无需鉴别 DTMF 信号。语音信号的损伤可能会导致接收侧网关无法检测出媒体流中的 DTMF 信号，所以在网络质量差或采用 G.723.1/G.729 等压缩编码时不建议使用这种 DTMF 传送方式。
- 当 DTMF 信号在 NGN 网络中以 RFC2833 方式传送时，发送侧的媒体网关（MG）必须得有数字信号处理器和相应的算法，用于检测 DTMF 信号，并将它们译为号码承载在 RFC2833 报文中，接收侧的媒体网关（MG）识别 RFC2833 报文中的 DTMF 信号，并且采取相应处理。

无论采用那种方式传送 DTMF 信号都是在 IP 网络中以明文传送，由于 IP 网络的开放性，网络黑客容易截获 IP 报文，通过分析 IP 包，黑客很容易获取 IP 报文中承载的语音和 DTMF 信息。由于电话银行的客户信息是承载在 DTMF 中，如果没有对二次拨号的 DTMF 报文进行加密传送，电话银行的用户信息容易被黑客截取导致泄密，引起严重的后果。

技术概述

RFC2833 描述了在 RTP 数据包中传送双音多频（DTMF）信号、其它电话信号音和电话事件的方法。

当采用 RFC2833 传送 DTMF 信号方式时，网关识别 DTMF 信号音并将它们译为对应的号码数字，并将号码数字按 RFC2833 的格式组成包发送。接收端根据接收到的 RFC2833 包中的号码数字还原 DTMF 信号音。

RFC2833 加密的实现

在软交换上配置了网关的 RFC2833 加密功能，软交换将密钥下发给收发两侧的网关，网关又将密钥下发给 DSP。发送侧网关的 DSP 检测到 DTMF 号码，将媒体流中的 DTMF 信号擦除，组 RFC2833 包，根据下发的密钥对 RFC2833 包的内容进行加密，接收侧网关的 Dsp 根据下发的密钥对收到 RFC2833 的内容进行解密，并从解密的内容中获取 DTMF 信息，进行 DTMF 信号音的还原。

采用华为公司专利算法加密采用 HNC1（NGN Cipher Version1）算法，支持 128/256 位秘钥。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。

通过 RFC2833 加密功能确保了 DTMF 信息传送的安全性，但是需要与华为的 Softx3000 配合使用。

RTCP XR（传输控制协议扩展协议）

简单介绍传输控制协议扩展协议的基本原理。

介绍

RTCP 是 RTP 的传输控制协议，对应某个 RTP 会话，启动了 RTCP 功能，每过一个间隔时间，一端会将发送 RTP 数目的信息和接收 RTP 数目的信息通过 RTCP 包发送给对方，对端就可以知道这段间隔应该要收的包数，与实现收的包数目进行比较就得到了网络的丢包情况。

RTCP XR 是 RTCP 的扩展，增加了模拟线路能量、噪声能量、语音评分（R-factor、Mos）等信息。

版本支持情况

目前不支持 RTCP XR。

Centrex 业务

介绍 Centrex 业务的背景和基本原理。

背景介绍

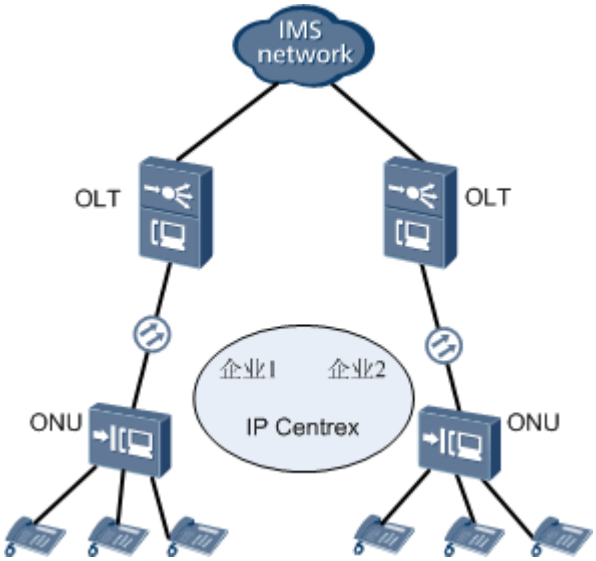
Centrex 是“Central Office Exchange Service”的简称，即中心局交换业务，是指在相同企业中的用户可以配置在同一个 Centrex 群中，方便进行短号互拨。

在较多中小企业中，网关以解决话音业务为主，如果企业 1 与企业 2 分别为公司的总部和分部，通过定义一个基本用户群，可以实现 IP Centrex 功能。在 PSTN 及 NGN 组网下，交换机或软交换是支持 Centrex 群相关功能的，可以进行短号互拨及相关新业务。在 IMS 组网下，需要网关兼容支持该业务，支持群内呼叫及出群呼叫。同时在 IMS 的控制下，可以支持和 Centrex 群相关业务。

原理描述

IP Centrex 业务组网图如下图所示：

图 5-21 IP Centrex 业务组网图



在相同或不同位置的企业用户 1 和 2，可以通过 Centrex 群功能联系在一起，实现短号互拨及相关的新业务，主要由 IMS 控制实现。

目前，我们可以支持 Centrex 出群呼叫功能，可以通过本地配置、匹配出群数图或向 IMS 订阅的方式实现，可以支持直接出群，或二次拨号出群。下面就相关功能作简单介绍。

- 支持配置数图模式直接拨出或二次拨出 Centrex 功能，采用用户配置的直接出群数图或二次拨号出群数图（为避免冲突，这两种数图不能同时存在）实现，在主叫用户摘机等输入条件启动数图时，首先数图模块要装载数图文件中的直接出群（或二次拨号）、普通、紧急与 SCC 数图进行匹配。若已经匹配了出群数图，由数图模块删除出群数图与 SCC，重新匹配正常数图（普通、紧急数图）；最后上报带出群字冠的号码给业务模块处理；业务模块根据 profile 决定是否将出群字冠一起通过 INVITE 消息发送给 IMS，从而实现直拨出群呼叫功能。
- 支持用户配置出群数据直接拨出或二次拨出 Centrex 功能，采用用户配置出群数据实现时，需要先配置好用户 Centrex 数据；然后在主叫用户摘机等输入条件启动数图时，首先读取该用户业务权限数据，根据 Centrex 数据动态生成并下发 Centrex 数图；数图模块除了装载 Centrex 数图外，还需要一起装载数图文件中的普通、紧急与 SCC 数图进行匹配。若已经匹配了出群数图，由数图模块删除出群数图与 SCC，重新匹配正常数图（普通、紧急数图）；最后上报带出群字冠的号码给业务模块处理；业务模块根据 profile 决定是否将出群字冠一起通过 INVITE 消息发送给 IMS，从而实现直拨出群呼叫功能。由于出群数图是根据用户 Centrex 数据动态生成，所以只对该用户产生作用，不影响其它用户的拨号处理。
- 支持订阅出群数据直接拨出或二次拨出 Centrex 功能，在用户发送 Uaprofile 订阅功能时(显式或隐式订阅)，IMS 通过 NOTITY 消息下发 Uaprofile 值，其中包含了用户的 Centrex 数据(包括群号、出群字冠、出群方式)；在主叫用户摘机等输入条件启动数图时，首先读取该用户业务权限数据，根据 Centrex 数据动态生成并下发 Centrex 数图；之后的流程同上面的配置数据出群业务。

处理优先级从高到低为：订阅方式的出群、用户配置的出群、配置数图文件方式的出群。

5.8 语音线路接口特性

本章节介绍与语音接口相关的特性，包括振铃、Z 接口基本特性及增强特性。

5.8.1 介绍

定义

语音接口特性是指在系统在语音接口上所实现的相关特性，包括振铃、Z 接口基本特性及增强特性。

目的

提供符合标准的语音接口，其具有可靠的防护能力，智能的节能功能。

5.8.2 原理描述

振铃

介绍振铃的实现机制。

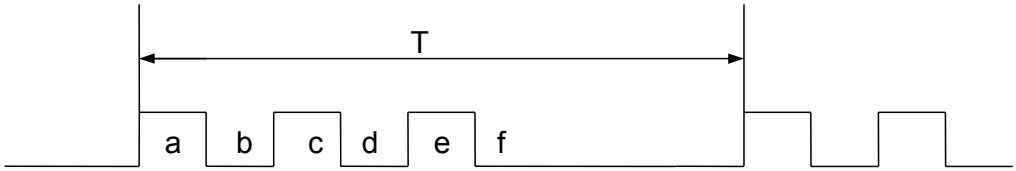
振铃信号由用户板产生，当前系统已经预置 13 种振铃模式，同时还支持 16 种自定义振铃模式。预制的振铃模式如表 5-8 所示。

表 5-8 预制的振铃模式表

模式编号	模式说明
0	Normal Ring 1:4
1	Special Ring 1:2
2	Special Ring 0.4:0.2:0.4:4
3	Long Ring
4	Special Ring 1.2:2
5	HK Ring 1:3
6	HK CNTRX 0.4:0.2:0.4:0.2:0.4:3.0
8	HK DN-A 0.4:0.2:0.4:3.0
9	HK ACB 0.4:0.2
10	HK Reminder (ringing for 0.4 second)
11	HK DN-B 1.2:3
12	CNTRX_IN 0.4:0.2:0.4:0.2:0.4:2.6
13	Egyptian long distance Ring 2:1

自定义的振铃模式允许配置 16 种自定义振铃，自定义振铃最大支持 3 段振铃的配置，如图 5-22 所示，其中，a，c，e 为振铃段，b，d，f 为间歇期，每段振铃和间歇期最大支持时长为 25.5s。

图 5-22 自定义的振铃模式配置示意图



接口防护

介绍接口防护的基本原理。

介绍

由于用户单板通过用户电缆和用户终端对接，而用户电缆在实际布防时候存在各种情况，例如有的地下布放，有的架空走线，有的布放可能和市交流供电平行。这些情况都会致用户线可能会遭受雷击，电力线碰触，电力线感应等等导致用户线上出现比较大的电压，而这些电压会将用户单板端口直接打坏而导致失效。用户单板的防护能力就是为了解决类似问题。

版本支持情况

完全满足 ITU K20/K45 的需求，而且华为内部制定的防护标准要高于 ITU K20/K45 的需求。例如 ITU 规定的无一级防护的端口过电压一般要求是满足 1500V 即可，而华为的单板一般上都可以满足 4000V 的测试。

参考标准和协议

ITU K20/K45

语音线路接口

介绍语音线路接口特性。

语音线路接口标准

语音线路接口的标准主要涉及有几个：

- ITU－Q552，主要是涉及 Z 接口传输指标。
- ETSI 的 ES 201970，主要定义了语音接口的一些基本硬件特性。
- 《yd751－电话交换设备入网检查方法》，主要是中国定义的关于语音接口的标准。

由于语音技术发展的历史比较长，基本上每个国家都有自己单独的标准，上述 3 个标准一般是涉及单板的基本特性，而针对不同国家需求可能需要定做一些特性，例如英国 BT 就有其单独的标准，其中一些需求是比较特别的，需要特殊的单板才能够满足需求。

Z 接口基本特性

MDU 的语音接口单板支持的 Z 接口基本特性简单总结如下：

- B－battery feeding（馈电）
  - 馈电，就是为话机等终端提供电压和电流保证终端正常工作。
  - MA5620 的单板挂机下的电压一般是 48V。摘机下支持恒流馈电，可以支持 20mA，25mA，30mA 三种馈电电流，馈电电流可以根据需要进行配置。
  - 端口的摘机馈电可以自动进行调整，当环路距离比较短的时候，端口保持恒流馈电，当环路距离比较长的时候，端口会根据设定的门限值自动调整环路电流，这样设计可以保证既满足相关标准要求，同时可以保证端口的功耗达到最优。
  - 对于 25mA 馈电电流，在－48V 的供电环境下，可以保证 1200 欧姆环阻内电流不小于 25mA，在 1800 欧姆环阻下馈电电流会大于 18mA 以上。
- R－Ringing（振铃）
  - 振铃，就是为话机提供铃流，通过话机发出响声提醒用户有电话接入。MA5620 单板按照平衡振铃特性设计。

- 平衡振铃概念是相对于传统的非平衡振铃概念来的。传统的非平衡振铃一般有 2 种：1）用户线的 A 线是 0V，B 线是－48V 直流电压叠加了 65Vrms 交流信号。2）用户线的 A 线是-48V，B 线是 65Vrms 交流信号。平衡振铃是用户线 A 线有交流信号，B 线也有交流信号，A 线和 B 线交流信号频率相同，相位相反，是差分信号。平衡振铃的频率是可以配置的，提供 16Hz，25Hz，50Hz 三种。
- 铃流幅度最大可以支持到 65Vrms。可以支持在 1400 欧姆线路电阻（0.4mm 线径大约 5KM），终端阻抗小到 4000 欧姆情况下终端的铃流幅度大于 35Vrms。同时提供 50Vrms 铃流幅度的配置，这种配置主要针对短环路的应用（1KM 之内），这种情况可以大大降低端口振铃的功耗。
- 单板提供的直流偏置可以达到 20V，可以保证在比较长的距离下达到可靠的截铃。
- 单板支持铃流的断续比可配置，完全可以满足全球所有需求。

- O－over voltage protection（过电压保护）

  过电压保护，也就是满足接口防护特性。
- S－Supervision（监控）

  监控，指的是单板检测话机的状态，例如话机是否摘机，是否挂机，是否振铃状态下摘机等等。通过检测来确认终端状态，终端状态检测是一些呼叫的基础。
- C－Codec/Decode（编码/解码）

  编码/解码，就是单板完成用户线模拟信号到数字信号的转换，并按照 A/U 标准对信号进行压缩。
- H－Hybrid circuit（混合电路）

  混合电路，指的是单板实现模拟 2 线接口到数字 4 线接口的转换，同时实现与用户线阻抗的平衡匹配。
- T－Test（测试功能）。

  测试特性可以参照**语音测试及维护特性**的介绍。

接口阻抗，传输指标以及增益

MDU 语音接口单板可以通过配置支持各种接口阻抗需求以及增益的设置。

目前一般提供 8 种通用的接口阻抗可配置。主要有：

- 200+680//100nf－－中国定义的
- 200+560//100nf－－中国定义的
- 600Ω－－一种比较通用的
- 150+510//47nf－－俄罗斯的
- 220+820//115nf－－德国等使用比较广的
- 220+820//120nf－－使用比较广的
- 900Ω－－使用比较少的一种
- 270+750//150nf－－ETSI 推荐的使用比较广的

接口传输增益也是可配置的，发送增益一般支持＋ 5db ～－6db，接收增益可以支持 0db ～－12db，增益可以按照 0.5db 步长进行配置。

单板的传输指标完全满足 ITU-Q522 的测试需求。对于某些接口阻抗不在上述 8 种之外的需求，可以通过单独的定制软件来支持。

收号

MDU 的语音接口单板支持脉冲收号。

老式的话机一般式按照脉冲的形式进行拨号，新的话机一般是 DTMF 拨号，但是大都支持兼容脉冲拨号模式。

单板脉冲收号可以支持的范围是：8PPS ～ 12PPS，断续比 50％～ 80％范围，而且脉冲号的间隔默认的配置是 240ms。

对于 DTMF 收号，由系统的 DSP 完成，不属于用户单板的功能范围。

计费信号

单板可以支持三种计费方式：反极计费（polarity reverse），12/16KC 计费和脉冲计费（Counter impulse delivery）。

- 反极：指将用户线 AB 线间电压翻转，一些终端设备通过检测这种翻转来计费。
- 12/16KC：指单板向终端发送一定宽度的 12000HZ/16000HZ 的正弦交流信号。
- 脉冲计费：指单板可以向终端发送一定的脉冲信号。

单板所有端口可以支持反极特性。既可以支持快速的反极（反极时间一般在 3ms 之内），以适应一些话机对反极时间的要求，同时也支持慢反极特性，反极时间可以达到 80ms，可以大大降低反极期间对线路干扰，对同一线路上传输 DSL 具有很好的兼容性。

单板支持 12/16KC 计费。12/16KC 的幅度可以进行配置，最大可以支持到 200 欧姆下 4.5Vrms（可以选择的配置幅度有 0.45Vrms，0.775Vrms，1Vrms，1.5Vrms，2Vrms，2.5Vrms，3Vrms，3.5Vrms，4Vrms 和 4.5Vrms）。同时 KC 信号的断续比也是可以进行配置的，默认的配置是 make：100ms，Break 300ms。Make 时间和 Break 时间别可以支持的范围都是 20ms ～ 500ms。

单板支持脉冲发送计费。脉冲发送的一些特性是可以进行配置的，可配置的参数有脉冲宽度，以及每分钟发送脉冲的个数。

锁定端口降电流特性

当端口长时间摘机而不通话的情况下，单板可以将端口的电流下降到 12mA 以下，以降低端口的功耗。

短环路馈电

单板在线路距离比较短的情况下使用低压供电，降低端口的功率，而当线路距离加长时候会自动切换到比较高的低压供电，满足使用要求。

断电特性

针对未放号端口，可以将这些端口的馈电切断，以降低端口的功耗。

挂机传输，摘机传输

单板支持挂机传输功能，以及摘机传输功能。这些功能主要支持的特性如：来电显示，固网短信等等。

REN

REN 就是 Ringer Equivalence Number，指一个端口可以并接的话机数量。MDU 一般允许一个端口并接话机的数量最大 4 ～ 5 部。

5.9 语音测试及维护特性

语音测试及维护特性，包括内外线测试、仿真呼叫测试、导通测试、RTCP（Real-time Transport Control Protocol）统计等维护特性。

5.9.1 介绍

定义

语音测试及维护特性，包括内外线测试、仿真呼叫测试、导通测试、RTCP 统计等维护特性。

目的

为 MDU 语音特性提供完备的测试及维护功能。

5.9.2 原理描述

内外线测试

介绍内外线测试的具体内容。

语音业务，线路维护部分是很重要的部分，业务发放前或业务发放后出现话路质量问题、呼叫故障时，需要先测试用户线路质量，判断是用户线路问题还是设备问题，MDU 提供的线路测试功能可以协助客户简单、快速判断线路问题。

外线测试，是测试设备到用户话机这一段的电气指标。

内线测试，是 POTS 用户板内部的提供的电气指标。

具体的测试指标项如**表 5-9** 所示。

表 5-9 测试指标项

类型	测试项
外线测试	A->地 交流电压
	B->地 交流电压
	A->B 交流电压
	A->地 直流电压
	B->地 直流电压

类型	测试项
	A->B 直流电压
	A->地 绝缘电阻
	B->地 绝缘电阻
	A->B 绝缘电阻
	A->B 环阻
	A->B 反极性电阻
	A->地 电容
	B->地 电容
	A->B 电容
内线测试	数字电压
	供电低电压（负）
	供电高电压（负）
	供电正电压
	环路电流
	馈电电压
	振铃电压
	频率
	A 线对地电压
	B 线对地电压

外线测试和内线测试完成后，设备会综合各测试指标给一个最终测试结论，说明内线、外线正常，或具体故障原因，用于指导维护人员后续的维护。内外线测试结论如**表 5-10** 所示。

表 5-10 内外线测试结论列表

类型	结论
外线测试	正常
	碰电力线
	A 线它混
	B 线它混
	AB 线双它混

类型	结论
	A 线地气
	B 线地气
	AB 双地气
	自混（小电阻）
	自混（自碰线）
	A 对地漏电
	B 对地漏电
	双线对地漏电
	AB 线间漏电
	断线（双线）
	未挂机
	未知结论
内线测试	正常
	异常

考虑到各国或不同运营商的布线或网络特征不一样，MDU 提供各项指标的判据阀值设置，上面外线测试的结论就是依据各项判据阀值计算比较所得，如果维护人员不修改，则使用默认值。

当需要判断是否为局内断线、局外断线、局内自混和局外自混时，需要获取机框校准值。通过获取机框校准值，自动获取模拟用户端口外线断线和自混情况下的校准值，进行外线测试，能够准确的得出是否为局内断线、局外自混等结论。

在做内外线测试时，可能会碰到用户正在使用电话，测试时为了不影响用户的正常使用，MDU 提供“遇忙不测”和“遇忙强测”2 个选项供维护人员明确使用。

仿真呼叫测试

介绍仿真呼叫测试的实现机制。

随着 MDU 设备的规模布放，MDU 不仅数量具大，而且 MDU 靠近用户，布放场地复杂，偏远，一旦出现问题，需要有远程定位手段进行定位，快速区分用户数据配置或设备问题，在用户开局前，仿真测试也可用来模拟实际业务，进行测试。

仿真呼叫测试功能是模拟用户呼叫功能，可避免人员去现场操作定位。呼叫仿真包括主叫仿真和被叫仿真，可以模拟 MDU 上语音用户端口做主叫和被叫的应用场景，通过人工配合的方式使用。

所谓主叫仿真，就是设备端口模拟用户摘机、拨号、通话、挂机的过程。

1. 维护人员需设置一个端口为主叫仿真端口。

2. 设置要拨打的电话号码后，启动仿真测试。
3. 在设备端口模拟用户摘机，并在检测到拨号音后，模拟话机产生配置的用户号码。
4. 测试人员在被叫侧（仿真拨打的电话号码）配合，如果能听到电话振铃（说明信令接续成功）；维护人员人工摘机，如果能听到主叫侧发送的 DTMF 号码，说明媒体通路是正常的。

所谓被叫仿真，就是设备端口模拟用户端口做被叫的情况。

1. 在设备上设置用户端口为被叫仿真端口。
2. 启动测试，维护人员在远端使用任一电话拨打该仿真用户电话。
3. MDU 设备上该被叫仿真端口在检测到铃流时，模拟用户摘机（在摘机前，如果主叫端听到回铃音，说明信令通路正常），并设置远端环回。这时，主叫侧维护人员拨通被叫并且听到被叫发送的 DTMF 号码，说明媒体通路正常。

说明

在仿真测试过程中，请确保仿真终端处于挂机状态。

导通测试

介绍导通测试的实现机制。

为了减少去现场的次数，减少成本，设备安装时，在 POTS 业务发放前，对设备 POTS 业务部分的硬件和配置数据进行全面的测试是非常必要的，导通测试针对这种场景进行全面的测试和验证，测试执行可以在近端执行，也可以在远端执行，遍历所有端口的测试。

测试主要包括 2 部分：

设备硬件测试：未开展语音业务的设备，为了后续支持语音业务预留能力，需要在设备开始应用的时候，测试语音模块的硬件没有问题。

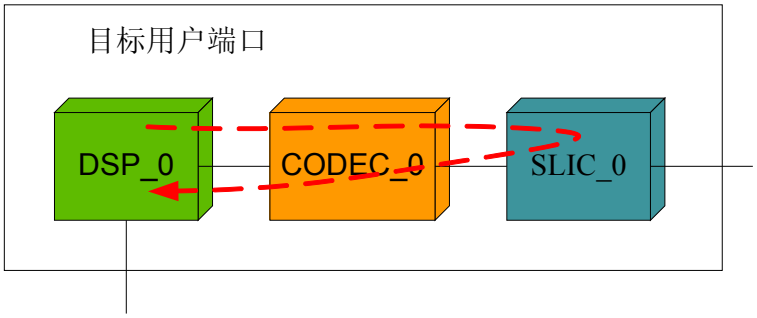
设备业务测试：开展语音业务的设备，验证设备下的用户可以开展语音，测试设备上用户开展语音业务的能力。

设备硬件测试能够覆盖的内容包括：

- 摘机的检测；（设备硬件）
- 挂机的检测；（设备硬件）
- 用户端口振铃、截铃的检测；（设备硬件）
- 话路通道的检测；（设备硬件）

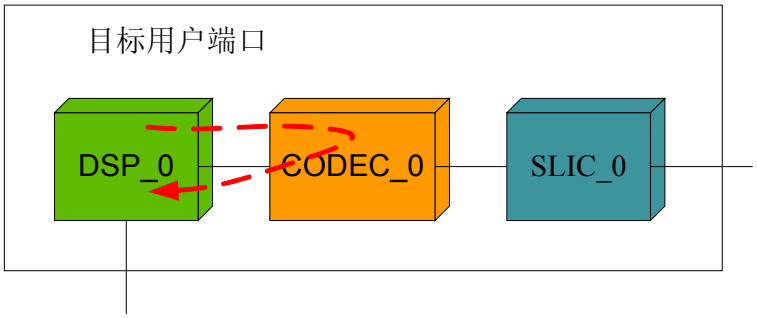
前 3 项主要是 POTS 板检测和控制功能，也是最基本功能，后一项通过业务环回，测试芯片对业务处理的功能，它主要包括以下 3 种环回测试。

图 5-23 SLIC 环回测试原理图



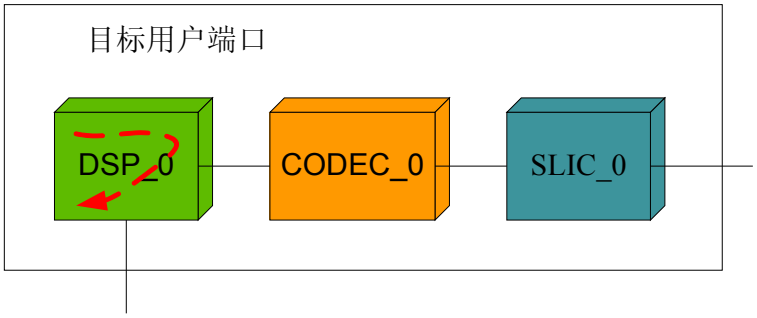
SLIC 环回测试，设置 POTS 某一端口与某一 DSP Channel 时隙相连，然后 DSP 向 TDM 侧产生 DTMF 验证码，通过 DSP 接收检测 TDM 侧的 DTMF，验证 DSP、Codec、SLIC 通路是否正常。如图 5-23 所示。

图 5-24 Codec 环回测试原理图



Codec 环回测试，设置 Codec 向网络侧环回（远端环回），然后 DSP 向 TDM 侧产生 DTMF 验证码，通过 DSP 接收检测 TDM 侧环回的 DTMF，验证 DSP 到 Codec 的通路是否正常。如图 5-24 所示。

图 5-25 DSP TDM 侧环回测试原理图



DSP TDM 侧环回测试，设置 DSP Channel 时隙由 TDM 向 IP 侧环回，然后 DSP 向 TDM 侧产生 DTMF 验证码，DSP 接收 TDM 侧的 DTMF，验证 DSP 的 TDM 侧发送和接收功能。如图 5-25 所示。

设备业务测试能够覆盖的内容包括：

- 设备接口数据测试，包括设备上的配置的 MG 接口数据，协议参数，Call Server 参数等信令相关数据。
- 用户端口数据测试，包括设备上的用户数据、电话号码等用户数据。

业务测试的基本原理类似呼叫仿真，只是主叫和被叫都由设备进行仿真，设备上的一个端口呼叫另一个端口（因此要配置电话号码），每个端口进行轮询呼叫，环回，检测。

以上导通测试项覆盖设备的每个端口，维护人员可选择只进行硬件测试或业务测试，测试完成后显示具体的测试结果。

RTCP 统计

介绍 RTCP 统计的基本原理。

遵循 H.248 协议，软交换可以在用户通话过程中和通话结束时，查询用户的 RTCP 统计信息，统计信息包括：发送 RTP 包总数，发送 RTP 包字节总数，接收 RTP 包总数，接收 RTP 包字节总数，发送丢包总数，接收丢包总数，网络抖动，网络环路时延等数据。

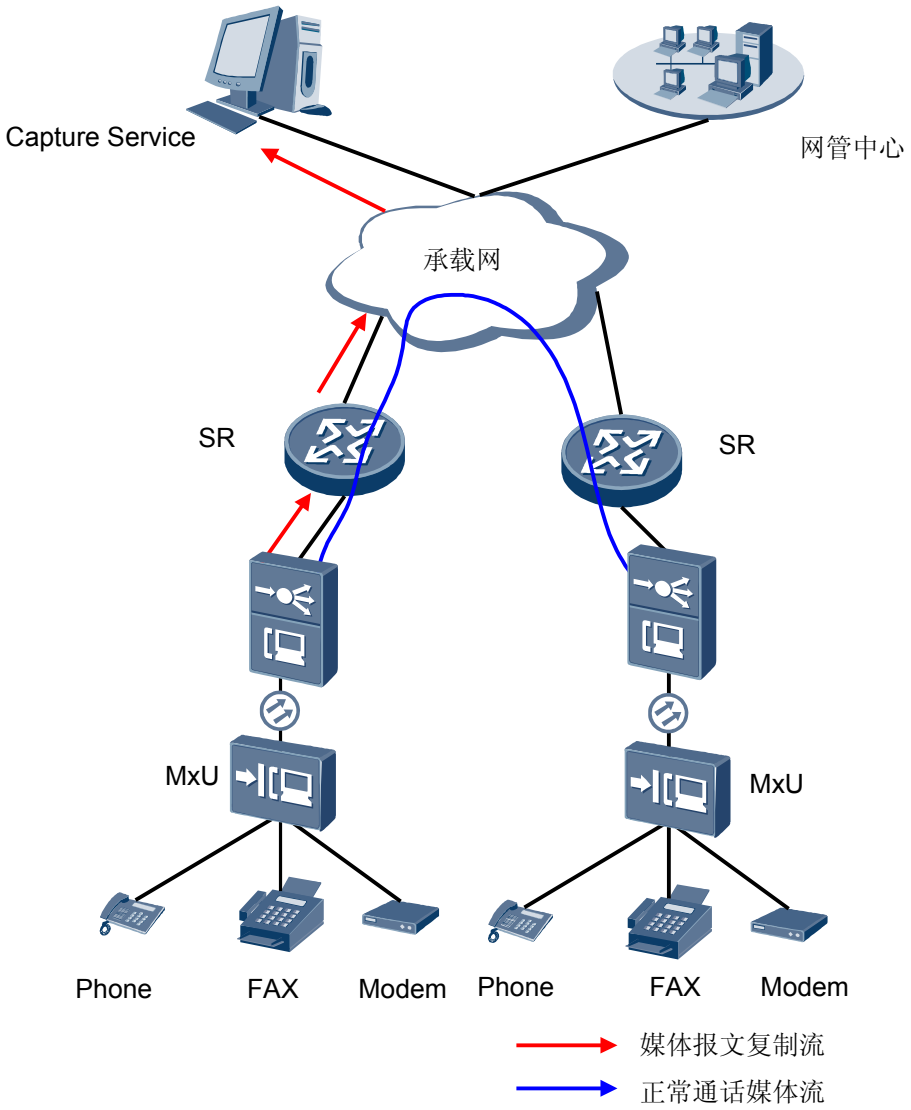
MDU 实时统计数据，在软交换下发信令查询时，上报给软交换。软交换或 OSS 系统可根据这些统计数据进行质量监控方面的管理。

远程抓包

介绍远程抓包的目的以及实现原理。

MDU 到网上运行后，远程抓包功能是一项非常重要的维护手段，如出现通话质量差、Fax/Modem 业务成功率低等问题时，需要捕获原始的媒体报文信息进行定位，MDU 的远程抓包特性不仅可以避免维护人员去现场抓包，还能根据问题现象进行有针对性、快速及时启动抓包等功能，不仅大大降低成本，还能快速捕获故障数据，缩短故障定位时间。

图 5-26 远程抓包原理示意图



MDU 远程抓包的组网如图 5-26 所示。基本原理是，MDU 将指定用户端口的媒体流复制一份，然后添加 MAC/IP/UDP 等头发送到指定的服务器上，在服务器上通过专用工具接收 UDP 报文，并剥离复制时添加的 MAC/IP/UDP 头，还原成原始数据。MDU 媒体报文的复制功能在语音 DSP 芯片上完成，主控板 CPU 不参与，因此远程抓包不仅对正常业务的通话没有影响，对主控系统也没有任何影响。

远程抓包的服务器可以指定，可以在网管上集成，也可以是专门的服务器或者 PC 机，因此在启动远程抓包功能前要先配置服务器的相关数据（如 IP）。

远程抓包的启动有以下形式：

- 指定用户的端口信息，如框/槽/端口号、TID 等。

  这种情况下，只要该用户发起呼叫并通话，远程抓包功能就会启动远程抓包，将通话的全过程跟踪下来。这种形式适用于某一用户端口申报过问题，但重现概率低的问题，或者某一特定业务出现问题（如 Fax/Modem）。

- 通过按键操作，及时启动抓包功能。

  这种情况的应用场景是，当 2 个用户正在通话过程中发现质量变差，可通过按一特殊键（如 911*#），MDU 检测到这一特殊号码后，及时启动抓包功能，可以快速捕获第一手数据。该按键号码需要预先在设备上配置好，否则该功能无法启动激活。MDU 支持最大同时 2 路的抓包功能。

TOOLBOX 功能

介绍华为网管信令跟踪工具 ToolBox。

背景信息

ToolBox 是华为网管信令跟踪工具，也是华为公司提供的维护工具，可以对各接入产品（如 MD5500、UA5000、AMG5000、MDU）设备进行语音信令跟踪。

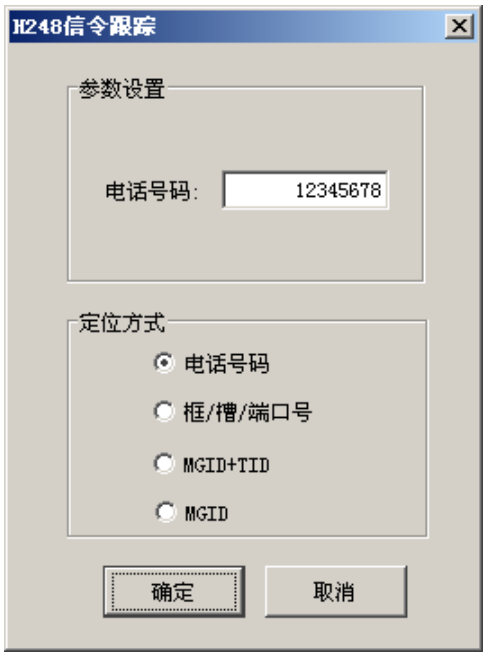
设备支持的信令包括：V5 信令跟踪（包括：二层消息跟踪、消息跟踪、端口信令跟踪）、H.248 信令跟踪、IUA 信令跟踪、Q.921 信令跟踪、DPNSS 信令跟踪、DASS2 信令跟踪、SIP 信令跟踪、Q931 信令跟踪等能力。MDU 支持 H.248、SIP 协议，因此可在 Toolbox 上执行对这 2 种协议的信令跟踪，跟踪信令可用于各种呼叫问题定位，隔离呼叫问题。

Toolbox 可按照用户端口进行跟踪，下面举例 H248 的信令跟踪操作步骤。

操作步骤

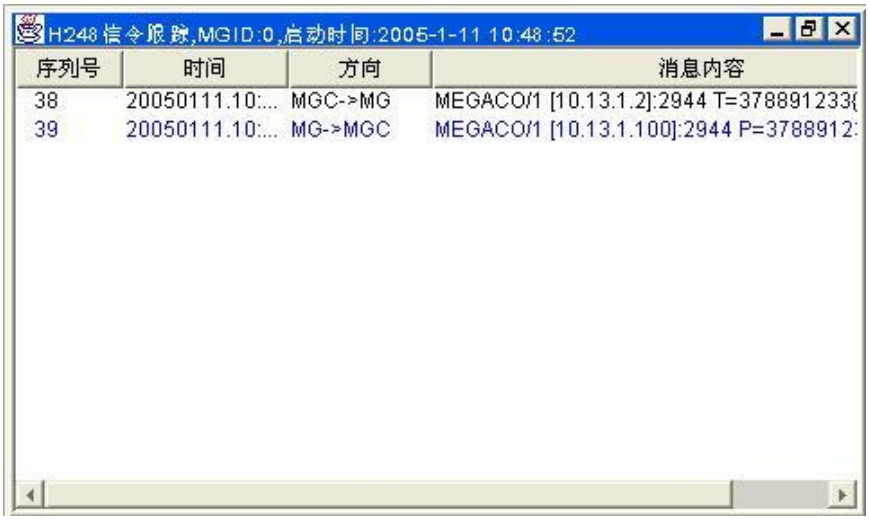
步骤 1 选择主菜单“跟踪/H248 信令跟踪”，弹出对话框如图 5-27 所示。

图 5-27 “跟踪/H248 信令跟踪”对话框



步骤 2 在定位方式中选择“电话号码”，在参数设置中输入电话号码，单击“确定”按钮，弹出消息跟踪窗口如图 5-28 所示。

图 5-28 消息跟踪窗口



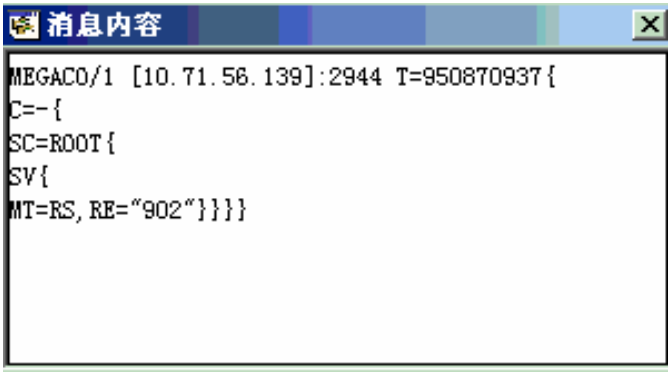
步骤 3 方式中选择“框/槽/端口号”，输入待跟踪端口的框、槽、端口号，单击“确定”按钮，弹出如步骤 2 所示的消息跟踪窗口。

步骤 4 在定位方式中选择 MGID+TID，输入 MGID 和 TID，单击确定按钮，弹出如步骤 2 所示的消息跟踪窗口。

步骤 5 在定位方式中选择“MGID”，输入 MGID，单击确定>按钮，弹出如步骤 2 所示的消息跟踪窗口。

步骤 6 通过鼠标双击某一行或直接在此行上按回车键，可以打开消息内容解释窗口，如图 5-29 所示。

图 5-29 消息内容解释窗口



步骤 7 在消息跟踪窗口中，单击鼠标右键，在弹出快捷菜单中：

- 选择“暂停”，使当前的滚动窗口停止滚动，以便查询信息。
- 选择“恢复”，使当前暂停的窗口恢复滚动。
- 选择“保存”，在弹出的对话框中，输入文件名称，单击“保存”按钮，可将当前窗口的记录保存成文本文件（以*.txt 结尾）。

- 选择“清除”，清除当前滚动窗口的信息。
- 选择“统计”，在弹出的窗口中，选择分类统计类型，及相关参数，单击“确定”，弹出分类查询消息跟踪窗口。

步骤 8 关闭消息跟踪窗口，可结束消息跟踪。

----结束

Qos 告警

介绍 Qos 告警的定义和用途。

网络的质量对语音有很大的影响，在通话过程中，MDU 设备可实时监控网络质量，当网络质量低于预先设置的阀值时，MDU 会给出相应告警，提示客户关注网络质量。

Qos 告警功能提供 3 个指标的监控，丢包、环路时延和抖动。用户可根据自己的网络情况设置相应的值，在用户呼叫通话时，MDU 统计丢包、环路时延和抖动数据，并与设定阀值比较，超出阀值时，给出告警。当监控的网络指标低于阀值时，给出恢复告警。

Qos 告警可实时发现网络异常，在出现用户投诉时，也可供参考，定位是网络还是设备问题。

5.10 语音可靠性

主要介绍语音可靠性相关的特性，包括双归属组网、高可靠性传输（SCTP）及语音 QoS。

5.10.1 介绍

定义

语音可靠性相关的特性，包括双归属组网、高可靠性传输及语音 QoS。

目的

保证 MDU 语音高可靠性。

5.10.2 原理描述

H.248 双归属

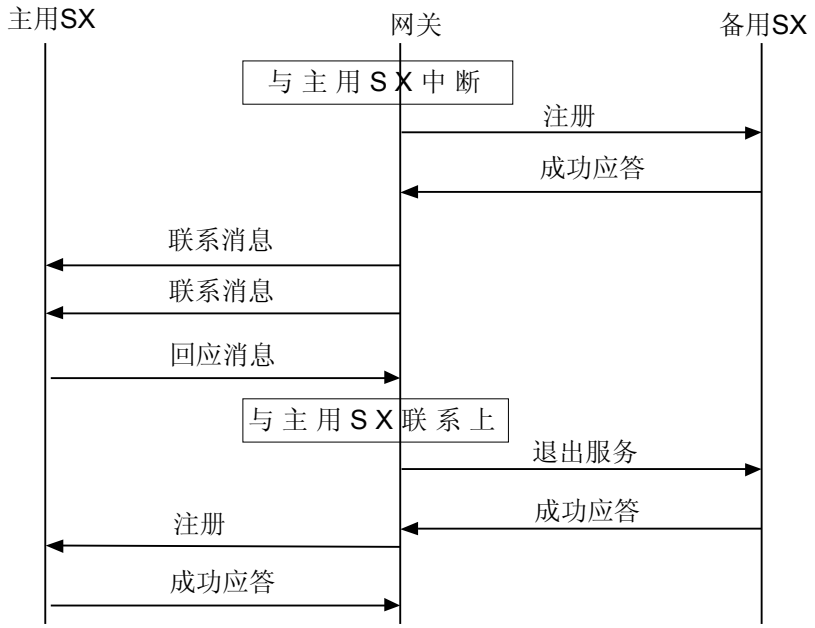
介绍通过 H.248 协议实现 MG 到软交换设备双归属的实现原理。

双归属为 NGN 整网解决方案，当主用软交换故障或 MG 到主用软交换的链路发生故障时，要求 MG 能迅速切换到备用软交换上，这样软交换和 MG 下的用户呼叫都不会受到影响。

双归属需要在一台 MG 上配置 2 台软交换数据，但一台软交换主用，一台软交换备用，MG 与软交换之间通过心跳进行检测。

双归属工作流程如图 5-30 所示。

图 5-30 双归属工作流程图



1. 网关通过心跳消息检测到与主用软交换联系中断。
2. 网关注册到备用软交换上。
3. 网关同时定时给主用软交换发送心跳探测消息（周期和普通心跳周期一样），如果收到响应则说明主用软交换恢复正常了，进入步骤 4，没有收到响应则一直发。
4. 向备用软交换发退出服务，等待响应。
5. 收到备用软交换的响应，则向启动向主用软交换注册的流程。如果注册三次不成功的话，则又转为向备用软交换注册，同原来的流程。

另外，不同的运营商可能会选择不同的双归属策略：

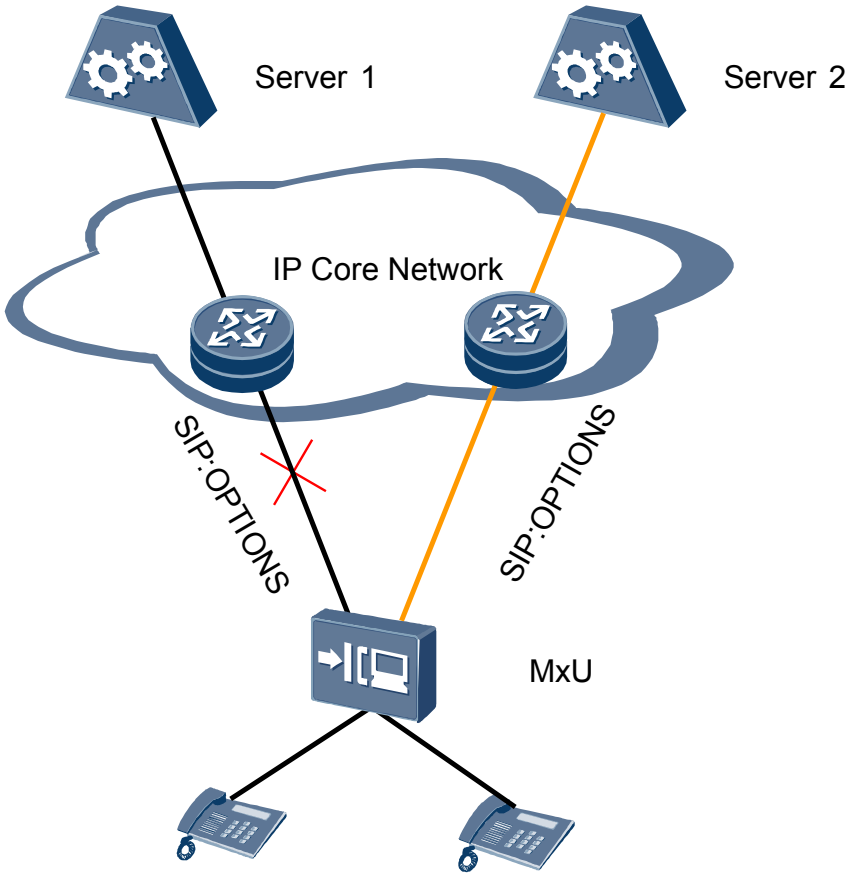
1. 当原主用软交换恢复正常时，MG 自动切换回主用软交换。
2. 不自动回切，不论注册到主用还是备用软交换上，只要注册到的软交换工作正常，则一直使用这个软交换。MDU 通过配置支持上面两种策略，默认是策略 2。

SIP 双归属

介绍 SIP 双归属的实现原理。

SIP 双归属组网如图 5-31 所示。

图 5-31 呼叫释放流程图



SIP 双归属流程与 H.248 双归属工作流程类似，MDU 对代理服务器实时检测，当主用代理服务器故障时，切换到备用代理服务器。切换前呼叫能够正确释放，切换后呼叫能够正常发起。

H248/SIP over SCTP

介绍 H248/SIP 协议承载在 SCTP 协议上的原理。

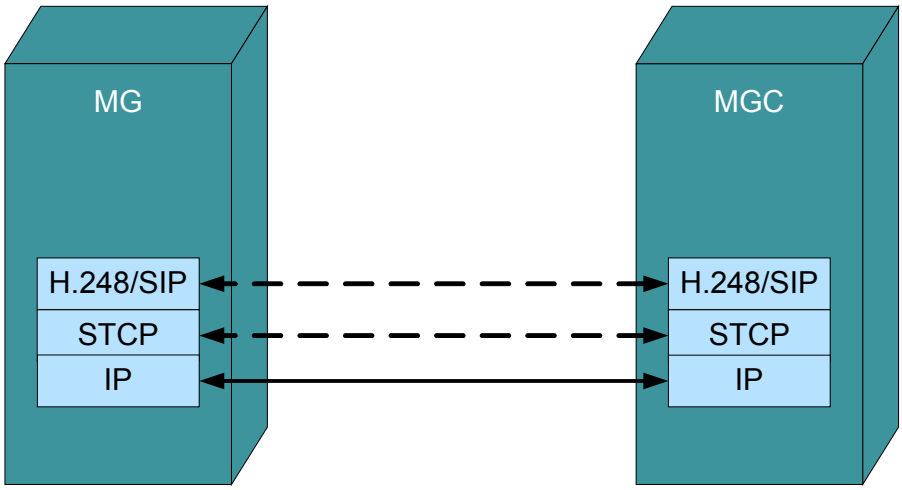
H.248/SIP 协议，目前大多数设备都是通过 UDP 承载，H.248.4 推荐使用 SCTP 承载 H.248 协议，通过 SCTP 实现应用层面消息的重传。

和 UDP 相比，SCTP 具备的优势包括：

1. 可靠：能够快速、可靠传递消息。
2. 多归属：所谓多归属，就是支持多 IP 地址，通过实现一个端点有多个 IP 地址，就可以支持一个端点使用多个物理网口，这样来提高端点的可靠性。
3. 具备拥塞控制功能：SCTP 的拥塞控制过程和 TCP 的非常相似。
4. 心跳机制：提供网络层面的心跳机制。
5. 安全：通过 4 次握手和 COOKIE 机制，有效防止 DoS 攻击。

如图 5-32 架构所示，网络层使用 IP 协议，传输层使用 SCTP 协议，应用层使用 H.248/SIP 协议。

图 5-32 H.248/SIP Over SCTP 协议架构图



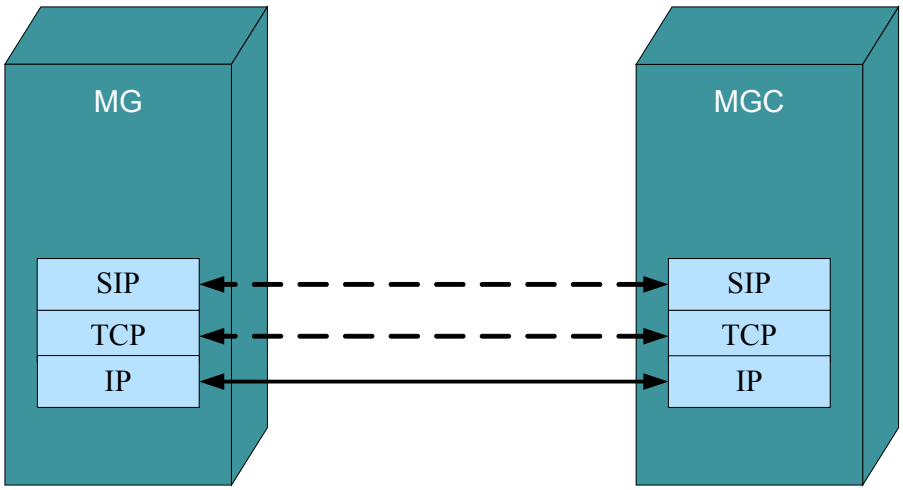
SIP over TCP

介绍 SIP 承载在 TCP 协议上的基本原理。

有的运营商要求支持基于 TCP 传送 SIP 信令，一方面是 SIP 报文比较大，使用 TCP 解决 SIP 报文的分包问题，另一方面则是解决可靠性传输的问题。

如图 5-33 架构所示，网络层使用 IP 协议，传输层使用 TCP 协议，应用层使用 SIP 协议。

图 5-33 SIP over TCP 协议架构图



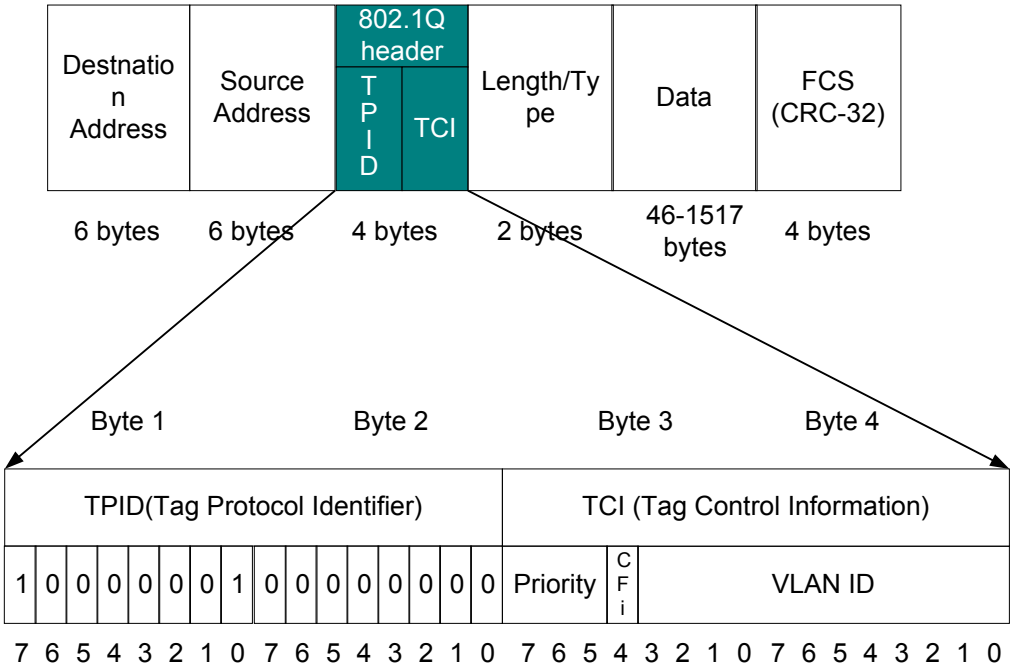
语音 QoS

介绍语音 QoS 的实现机制，主要是优先级的识别。

语音通话的特点是实时性要求高，延时小，呼叫接续快，因此语音的报文一般要求有较高优先级的转发，而路由器在做报文转发时是通过报文设置的 VLAN 优先级（遵循 802.1P）、DSCP/TOS 进行区分转发。但目前 MDU 不支持 DSCP。

802.1p 优先级（媒体和信令可分开设置）

图 5-34 802.1Q 帧格式



802.1Q 定义的以太网帧结构如图 5-34 所示，这 4 个字节的 802.1Q 标签头包含如下内容：

- TPID—Tag Protocol Identifier：2 个字节的标签协议标识，它的值是 8100。
- TCI—Tag Control Information：2 个字节的标签协议标识，TPID 是 IEEE 定义的新的类型表明这是一个加了 802.1Q 标签的本文。TCI 中划分成如下 3 个域：
  - VLAN Identified（ VLAN ID ）：这是一个 12 位的域，指明 VLAN 的 ID 一共 4096 个每个支持 802.1Q 协议的主机发送出来的数据包都会包含这个域以指明自己属于哪一个 VLAN。
  - Canonical Format Indicator（cfi）：这一位主要用于总线型的以太网与 FDDI、令牌环网交换数据时的帧格式。
  - Priority：3 位，指明帧的优先级一共有 8 种优先级主要用于当交换机阻塞时优先发送哪个数据包。

MDU 的本端媒体 IP 和信令 IP，根据组网需要，可配置到同一个 VLAN 中，也可以配置到不同的 VLAN 中。同时还可以分别为媒体 IP 和信令 IP 配置一个 802.1P 优先级（范围：0 ～ 7），默认情况下，媒体和信令 IP 的优先级为 6。

DSCP/TOS

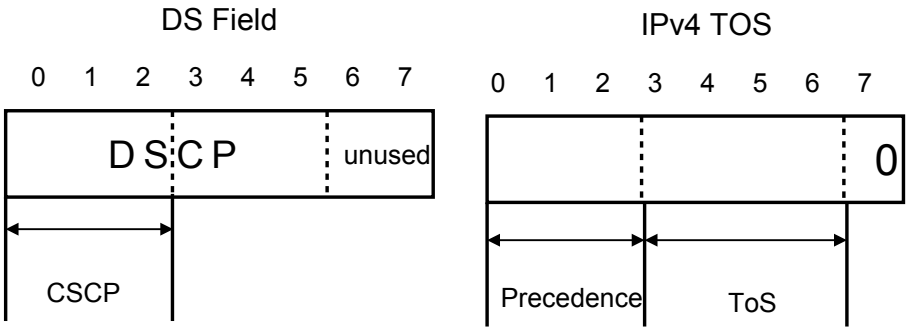
在 IP 协议定义中，DSCP 和 TOS 在 IP 头中占用相同的域（1 个字节），IP 承载网设备根据识别填充的是 DSCP 或 TOS，根据设置进行相应调度和转发，保证不同业务的 QoS。

服务类型（TOS：Type of Service）字段包括一个 3 bit 的优先权子字段（现在已被忽略），4bit 的 TOS 子字段和 1bit 未用位（必须置为 0）。4bit 的 TOS 分别代表：最小时延、最大吞吐量、最高可靠性和最小费用。4bit 中只能置其中 1bit。如果所有 4bit 均为 0，那么就意味着是一般服务。

DSCP 标识是基于 IPv4 的 ToS（Type of Service）和 IPv6 的流量类型（Traffic Class）进行定义。

如图 5-35 所示，DS 字段的低 6 位（0 ～ 5 位）用作区分服务代码点 DSCP（DS CodePoint），高 2 位（6、7 位）是保留位。DS 字段的低 3 位（0 ～ 2 位）是类选择代码点 CSCP（Class Selector CodePoint），它表示了一类 DSCP。

图 5-35 DSCP 标识格式



其中，DSCP 用于在网络中每个节点上选择相应的 PHB（Per-Hop Behavior）。PHB 是 DS 节点作用于数据流聚合的外部可见行为的描述。目前，IETF 定义了三种标准的 PHB：加速转发 EF（Expedited Forwarding）、确保转发 AF（Assured Forwarding）和尽力而为 BE（Best-Effort）。

5.11 术语与缩略语

术语

无

缩略语

表 5-11 缩略语

缩略语	全称
VoIP	Voice over IP（在 IP 协议上传送语音）

缩略语	全称
PPP	Point-To-Point Protocol（点到点协议）
RTP	Real-time Transport Protocol（实时传输协议）
UDP	User Datagram Protocol（用户数据报协议）
LCP	Link Control Protocol（链路控制协议）
NCP	Network Control Protocol（网络控制协议）
PAP	Password Authentication Protocol（口令验证协议）
CHAP	Challenge-Handshake Authentication Protocol（挑战握手验证协议）
AS	Application Server（应用服务器）
SOC	Switching order command（切换码）
ECT	Explicit Communication Transfer（呼叫转移）
DC	Double Communication（双通话）
CFU	Call Forwarding Unconditional（无条件前转）
CFNR	Call Forwarding No Reply（无应答呼叫前转）
CFB	Call Forwarding Busy（遇忙无条件前转）
VSP	Voice Service Plane（语音业务平台）
IMS	IP Multimedia Subsystem（IP 多媒体子系统）
VMIF	Visual Multiple Interface（虚拟多接口）

6 组网

关于本章

介绍系统实现的各种组网特性的功能。

6.1 介绍

6.2 参考标准和协议

6.3 可获得性

6.4 MSTP
MSTP 是多生成树协议，兼容 STP。

6.5 以太网链路聚合
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，来提供更高的带宽和链路安全性。

6.6 EPON Type D 保护倒换
从概念、规格、可获得性和原理描述方面对 EPON TYPE D 保护倒换特性进行介绍。

6.7 ETH OAM
OAM 泛指监控，是诊断网络故障的手段。

6.8 Ring Check
介绍 Ring Check 特性的定义、目的、规格和原理。

6.9 术语与缩略语

6.1 介绍

特性名称	特性简介
MSTP	MSTP（Multiple Spanning Tree Algorithm and Protocol）可以快速收敛，也能使不同 VLAN 的流量沿各自的路径分发，从而为冗余链路提供了更好的负载分担机制。
以太网链路聚合	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，并提供更高的带宽和链路安全性。
EPON TYPE D 保护倒换特性	EPON TYPE D 保护是 EPON 光纤系统的全保护，包括 OLT 侧 PON 口、ONU 侧 PON 口、主干光纤、光分光器和分支光纤等。通过 OLT 双 PON 口、ONU 双 PON 口、主干光纤、光分路器和配线光纤均双路冗余，实现 PON 光纤线路故障时满足 50ms 内保护倒换要求。
Ethernet OAM 特性	OAM 泛指监控，是诊断网络故障的手段。以太网作为一种局域网技术以其丰富的带宽，低廉的成本，易于即插即用，支持多点操作等特点被广泛应用。但随着以太网技术逐渐由运营商网络向城域、广域网扩展，网络的管理和维护工作也显得越来越重要。而目前以太网没有电信级管理能力，不能检测二层网络故障。Ethernet OAM 提供了端到端的故障检测手段，可以对以太网进行监控、诊断和故障检查。
Ring Check 特性	Ring Check 特性是通过设备在用户端口周期性发送 Ring Check 报文，监控用户侧和网络侧收到的 Ring Check 报文，检测运营商网络是否形成环路。如果网络中有环路产生，MDU 设备通过去激活形成环路的用户端口，并上报告警给网络管理系统，以保证设备的正常运转，其他合法用户不被干扰。

6.2 参考标准和协议

MSTP 特性的相关参考标准和协议如下：

- IEEE Std 802.1d, 1998 Edition, Spanning Tree Protocol
- IEEE Std 802.1w-2001, Rapid Spanning Tree Protocol
- IEEE Std 802.1s-2002, Multiple Spanning Tree Protocol

以太网链路聚合特性相关的参考标准和协议如下：

- IEEE 802.3-2002

Ethernet OAM 特性参考标准和协议如下：

- IEEE 802.1ag-2007 VLAN Amendment 5 Connectivity Fault Management
- WT-156v17 - Straw
- IEEE 802.3ah：Operations, Administration, and Maintenance (OAM)

6.3 可获得性

License 支持

Ethernet CFM OAM 特性和 Ethernet EFM OAM 特性都是 MA5620/MA5626 的可选特性，只有获得了 License 许可后才能获得该特性的服务。

版本支持

表 6-1 组网特性的版本支持

产品	支持版本
MA5620/MA5626	V800R308

特性依赖

由于协议机制的差异，RSTP 和 MSTP 在快速迁移的配合上有如下的限制：

建议运行 MSTP 协议的网桥作为上游，运行 RSTP 的网桥作下游，否则网络拓扑结构发生变化时可能无法实现端口的快速迁移。

以太网链路聚合特性有如下限制：

相同类型的端口（包括端口类型、工作模式和速率）才能配置聚合组。

硬件要求

用户接口中只有以下接口支持 Ethernet OAM 特性：

- ETH 接入用户接口。
- 上行口中仅 GE、GPON 接口。

6.4 MSTP

MSTP 是多生成树协议，兼容 STP。

6.4.1 介绍

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。

MSTP（Multiple Spanning Tree Algorithm and Protocol）协议兼容 STP（Spanning Tree Protocol），并且可以弥补 STP 的缺陷。

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 倍的 Forward delay 的时间延迟，端口才能迁移到转发状态。

MSTP 既可以快速收敛，也能使不同 VLAN 的流量沿各自的路径分发，从而为冗余链路提供了更好的负载分担机制。

MSTP 设置 VLAN 映射表（即 VLAN 和生成树的对应关系表）把 VLAN 和生成树联系起来。同时它把一个交换网络划分成多个域，每个域内形成多棵生成树，生成树之间彼此独立。

MSTP 将环路网络修剪成为一个无环的树型网络，避免报文在环路网络中的增生和无限循环，同时还提供了数据转发的多个冗余路径，在数据转发过程中实现 VLAN 数据的负载均衡。

6.4.2 规格

MA5620/MA5626 支持的 MSTP 的规格如下：

- 支持符合 IEEE std 802.1s 的 MSTP 协议。
- 支持 BPDU（Bridge Protocol Data Unit）保护功能。
- 支持 Root 保护功能。
- 支持环路保护功能。

6.4.3 原理描述

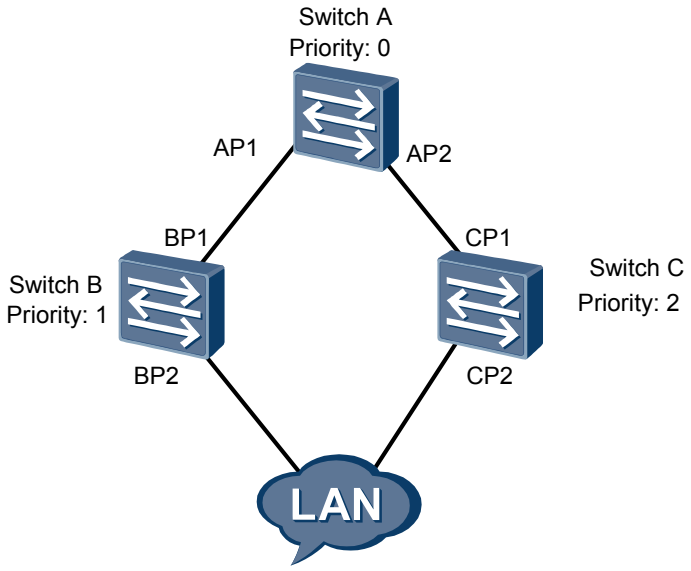
STP 基本原理

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的计算。

指定端口和指定网桥的相关说明如下：

- 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 6-1 指定网桥和指定端口示意图



如图 6-1 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生成树的树根。
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。

重新计算得到的新配置消息不能立刻传遍整个网络，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。

因此，STP 采用了一种状态迁移的机制，即在根端口和指定端口重新开始数据转发之前需要经历一个中间状态，该中间状态经过 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能够传遍整个网络。

STP 缺陷

- 当拓扑变化或者链路故障时，端口从阻塞状态切换到转发状态时，需要两倍的 Forward Delay 延时，所以，在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。

- 整个桥接网络应用一个单一的生成树实例。当网络规模较大的时候，可能需要更长的收敛时间，也可能很频繁的发生拓扑的改变。

MSTP 基本原理

MSTP 可以弥补 STP 和 RSTP 的缺陷，既可以快速收敛，也能使不同 VLAN 的流量沿各自的路径分发，从而为冗余链路提供了更好的负载分担机制。

MSTP 设置 VLAN 映射表（即 VLAN 和生成树的对应关系表），把 VLAN 和生成树联系起来。同时，MSTP 把一个交换网络划分成多个域，每个域内形成多棵生成树，生成树之间彼此独立。每个网桥内允许运行多棵生成树，在不同的生成树上转发不同 VLAN 的报文。

MSTP 将整个二层网络划分为多个 MST 域，各个域之间通过计算生成 CST（Common Spanning Tree）；域内则通过计算生成多棵生成树，每棵生成树都被称为是一个多生成树实例。其中实例 0 被称为 IST（Internal Spanning Tree），其他的多生成树实例为 MSTI（Multiple Spanning Tree Instance）。MSTP 同 RSTP 一样，使用配置消息进行生成树的计算，只是配置消息中携带的是网桥上 MSTP 的配置信息。

- CIST 生成树的计算
  - 通过“配置消息”的比较在整个网络中选择一个优先级最高的网桥作为 CIST 的树根。
  - 在每个 MST 域内 MSTP 通过计算生成 IST；同时 MSTP 将每个 MST 域作为单台网桥对待，通过计算在域间生成的 CST。
  - CST 和 IST 构成了整台网桥网络中连接所有网桥的 CIST。
- MSTI 的计算

  在 MST 域内，MSTP 根据 VLAN 和生成树实例的映射关系，针对不同的 VLAN 生成不同的生成树实例，即 MSTI。每棵生成树独立进行计算，计算过程与 RSTP 计算生成树的过程类似。

MSTP 具体实现

MSTP 同时兼容 STP、RSTP。STP、RSTP 两种协议报文都可以被运行 MSTP 的网桥识别并应用于生成树计算。

MA5620/MA5626 除了提供 MSTP 的基本功能外，还从用户的角度出发，提供了许多特殊功能，例如 Root 保护功能、BPDU 保护功能、环路保护功能。

- BPDU 保护功能

  对于接入层设备，接入端口一般直接与用户终端（如 PC 机）或文件服务器相连。此时，接入端口被设置为边缘端口，以实现这些端口的快速迁移；当这些端口接收到配置消息（BPDU 报文）时，系统会自动将这些端口设置为非边缘端口。在重新计算生成树后，将引起网络拓扑的震荡。

  在正常情况下，这些端口不会收到生成树协议的配置消息。如果有人伪造配置消息恶意攻击网桥，就会引起网络震荡。BPDU 保护功能可以防止这种网络攻击。

  MA5620/MA5626 启动了 BPDU 保护功能以后，如果边缘端口收到了配置消息，系统就将这些端口 Shutdown，同时通知网管。被 Shutdown 的端口只能由网络管理人员恢复。

  推荐用户在配置了边缘端口的 MA5620/MA5626 配置 BPDU 保护功能。

- Root 保护功能

  由于维护人员的错误配置或网络中的恶意攻击，网络中的合法根网桥有可能会收到优先级更高的配置消息，这样，当前根网桥会失去根网桥的地位，引起网络拓扑结构的错误变动。这种不合法的变动，会导致原来应该通过高速链路的流量被牵引到低速链路上，导致网络拥塞。

  Root 保护功能可以防止这种情况的发生。

  对于设置了 Root 保护功能的端口，端口角色只能保持为指定端口。一旦这种端口上收到了优先级高的配置消息，即其将被选择为非指定端口时，这些端口的状态将被设置为侦听状态，不再转发报文（相当于将此端口相连的链路断开）。当在足够长的时间内没有收到更优的配置消息时，端口会恢复原来的正常状态。

- 环路保护功能

  网桥的根端口和其他阻塞端口的状态依靠不断接收上游网桥发送的 BPDU 来维持。

  但是，如果链路拥塞或者单向链路故障，这些端口会收不到上游网桥的 BPDU。此时，网桥会重新选择根端口。根端口将转变为指定端口，而阻塞端口将迁移到转发状态，因而交换网络中将产生环路。

  环路保护功能会抑制这种环路的产生。

  被环路保护的端口在重新收到 BPDU 报文（除 TCN 报文）后，会进行正常的报文处理，选择角色，重新设置端口的转发状态，不会一直是阻塞状态。

  在启动了环路保护功能后，根端口的角色如果发生变化就会设置它为 Discarding 状态，阻塞端口会一直保持在 Discarding 状态，不转发报文，因而不会在网络中形成环路。

说明

三种保护功能是互斥的。

6.5 以太网链路聚合

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，来提供更高的带宽和链路安全性。

6.5.1 介绍

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，来提供更高的带宽和链路安全性。

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。

IEEE 802.3ad 是关于以太网链路聚合的标准。按照链路聚合的配置方式分为：

- 手工链路聚合

- 静态链路聚合
- 动态链路聚合

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，则系统无法发现。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：

- 易于管理和使用；
- 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。

6.5.2 规格

MA5620/MA5626 支持以下以太网链路聚合特性规格：

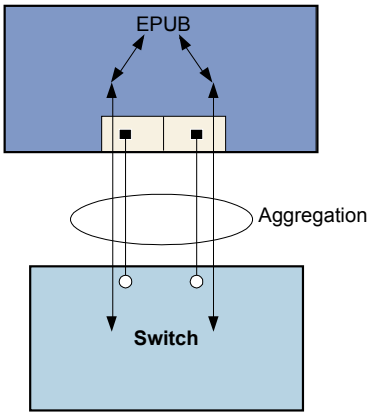
- 系统优先级：0 ～ 65535。
- 端口优先级：0 ～ 32767。
- LACP 交互短周期时间：1s ～ 10s，缺省值：1s。
- LACP 交互长周期时间：20s ～ 40s，缺省值：30s。

6.5.3 原理描述

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，以主控板的两个端口进行聚合为例，如图 6-2 所示，介绍手工链路聚合的实现原理。

图 6-2 手工链路聚合图



MA5620/MA5626 的两个上行端口加入了一个聚合组（Link Aggregation Group），对端 Switch 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，MA5620/MA5626 与 Switch 之间的流量就会分担到两条链路上。

但是如果其中一个端口故障或者对应的链路故障，MA5620/MA5626 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。

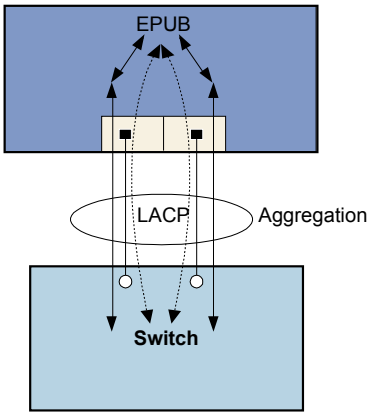
在静态链路聚合中，LACP 主要完成以下功能：

- 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。

MA5620/MA5626Switch 之间通过 LACP 协议交互聚合组信息如图 6-3 所示。

图 6-3 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，提高了链路聚合的安全性，支持以下聚合链路状态的检测：

- 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

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。
  MA5620/MA5626 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

6.6 EPON Type D 保护倒换

从概念、规格、可获得性和原理描述方面对 EPON TYPE D 保护倒换特性进行介绍。

6.6.1 介绍

定义

EPON TYPE D 保护是 EPON 光纤系统的全保护，包括 OLT 侧 PON 口、ONU 侧 PON 口、主干光纤、光分光器和分支光纤等。通过 OLT 双 PON 口、ONU 双 PON 口、主干光纤、光分路器和配线光纤均双路冗余，实现 PON 光纤线路故障时满足 50ms 内保护倒换要求。

目的

随着 EPON 系统应用越来越广泛，FTTB、FTTC、FTTH，需要对 PON 光纤线路做到全保护。TYPE B 保护只能做到主干光纤保护，TYPE D 保护可以对主干光纤、光分路器和分支光纤都做到保护。

6.6.2 规格

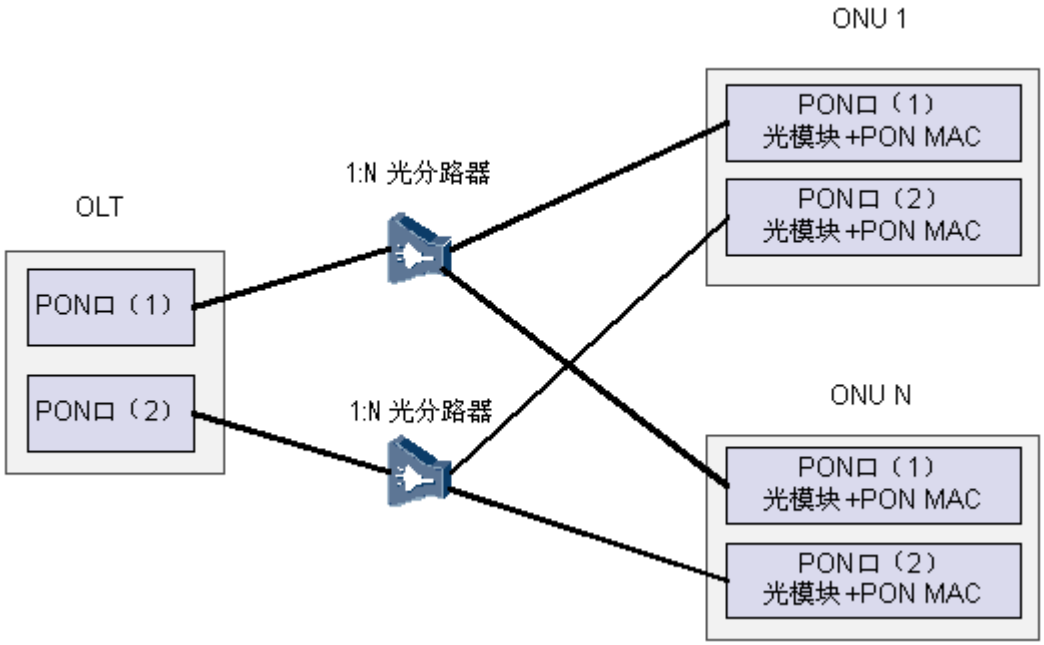
- 要求符合中国电信 CTC2.1 标准中有关 TYPE D 保护倒换的具体要求，倒换交互协议上兼容 CTC2.1 要求的 OAM 扩展消息，二层转发业务在倒换时的中断时间小于 50ms。满足光链路保护倒换准则，即输入光信号丢失或输入通道信道劣化触发自动倒换。
- 只支持主备保护倒换工作模式。
- 要支持此特性，与 MA5620/MA5626 对接的对端 OLT 设备必须支持此特性，目前只有 MA5600T 支持 EPON TYPE D 保护倒换功能。
- 由于 MA5620/MA5626 只有两个上行 PON 端口，默认为一个保护组，不需要用户设置保护组，并且不支持用户对保护组操作，只提供查询 PON 端口主备状态和保护倒换原因的功能。

6.6.3 原理描述

在 2009 年 4 月份修订的《中国电信 EPON 设备技术要求 V2.1》文档中，针对 EPON 线路，共提出四种保护倒换方式。其中 Type D 是 MA5620/MA5626 所要实现的保护倒换方式。

EPON Type D 保护倒换方式下，OLT 双 PON 口，ONU 双 PON 口，主干光纤、光分路器和配线光纤均双路冗余。EPON Type D 保护倒换连接图如图 6-4 所示。

图 6-4 EPON Type D 保护倒换连接图



EPON Type D 保护倒换连接中，对 OLT，分光器和 ONU 的要求如下：

- OLT：主、备用的 OLT PON 端口 PON 口（1）和 PON 口（2）均处于工作状态（即 ONU 同时在两个 PON 口上完成 MPCP 注册、标准和扩展的 OAM 发现）。OLT 应保证主用 PON 端口的业务信息能够同步备份到备用 PON 端口，使得保护倒换过程中，备用 PON 端口能维持 ONU 的业务属性不变，不用进行 ONU 的初始化配置和业务属性配置。
- 分光器：使用 2 个 1:N 分光器。
- ONU：采用不同的 PON MAC 芯片和不同光模块。ONU 应能保证主用 PON 端口的业务信息能够同步备份到备用 PON 端口，使得 PON 口在保护倒换过程中，ONU 能维持本地业务属性不变。

EPON TYPE D 保护倒换的实现原理

ONU 和 OLT 均检测链路状态，并根据链路状态决定是否倒换。

- 如果 OLT 检测到主用 PON 口的光链路故障后，OLT 自动切换到备用的光链路，并采用备用的光链路通过扩展的 OAM 消息（Active PON_IF AdminState 属性）配置 ONU 主用的 PON 端口。
- 如果 ONU 检测到主用 PON 口的链路故障后，ONU 自动切换到备用光链路，并采用备用的光链路进行扩展的 OAM 事件通告（Alarm ID=0x000C，PON_IF Switch），告知 ONU 的 PON 端口已经进行了切换以及切换的原因。

对于 EPON Type D 保护倒换，当满足下列条件之一时，必须进行光链路保护倒换。

- 输入光信号丢失。
- 输入通道信道劣化：包括输入光信号功率过高或过低和误码率越限两种。目前设备不支持误码率越限情况下的 EPON Type D 保护倒换。

6.7 ETH OAM

OAM 泛指监控，是诊断网络故障的手段。

以太网作为一种局域网技术以其丰富的带宽，低廉的成本，易于即插即用，支持多点操作等特点被广泛应用。但随着以太网技术逐渐由运营商网络向城域、广域网扩展，网络的管理和维护工作也显得越来越重要。而目前以太网没有电信级管理能力，不能检测二层网络故障。

Ethernet OAM 提供了端到端的故障检测手段，可以对以太网进行监控、诊断和故障检查。

6.7.1 介绍

Ethernet CFM OAM 定义

Ethernet CFM（Connectivity Fault Management） OAM 在 IEEE 802.1ag（2007）中定义为“连接故障管理”，用于在全以太网内提供一种端到端的故障检测和诊断手段。

MD 定义

- MD（Maintenance Domain）：维护域。指被 CFM 管理的网络范围，有可能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成若干个维护集，每个维护集对应维护域上的一个业务实例（Service Instance, SI），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（Maintenance Point, MP）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 entity Point)：维护实体端点。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。

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。

说明

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。

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。

Ethernet EFM OAM 定义

OAM 提供了网络操作员监控网络健康状况和快速定位故障链路位置及故障情况的能力。

Ethernet EFM（Ethernet in the First Mile）OAM 由 IEEE 的 EFM 工作组在 IEEE 802.3ah Clause 57 中定义，是 Ethernet OAM 的一个重要组成部分。Ethernet EFM OAM 提供了监控链路的机制，例如远端故障指示（Remote Defect Indication，RDI）和远端环回控制等，是一种数据链路层的机制，可以作为高层应用的补充机制。

OAMPDU 报文定义

Ethernet EFM OAM 除了具备远端故障指示和远端环回的功能之外，还有一种 OAM 发现机制，是一种高层管理应用的扩展机制。以太网链路上相邻的两个实体之间通过交换以下几种 OAMPDU 报文实现上述功能。

- Information OAMPDU 报文：用于向对端发送 OAM 状态信息，包括本端的 OAM 能力、Multiplexer 和 Parser 的状态、本端对对端 OAM 状态的满足情况等等。其中，OAM 能力是指：
  - 是否支持单向数据传输，因为该能力直接决定了是否可以支持 RDI。
  - 是否支持发送变量查询响应，即是否支持查询本端信息。
  - 是否支持远端环回，即是否支持远端设置本端处于环回状态。
  - 是否支持解析链路事件，即能否处理对端发送的链路事件。

  Information PDU 报文中还包含了 OUI(Organizationally Unique Identifier)域和 Vendor Specific Information 域，通过这两个域，可以知道对端的供应商信息。
- Event Notification OAMPDU 报文：用于通知对端在本端发生了特定的事件，这些事件是形如一段事件内接收到多少错误帧，错误帧门限是多少等。

- Variable Request OAMPDU 报文：用于向对端查询一个或者多个 MIB 变量，如正确收发的帧数等。
- Variable Response OAMPDU 报文：用于在收到 Variable Request OAMPDU 报文后，向对端返回一个或者多个 MIB 变量。
- Loopback Control OAMPDU 报文：用于控制对端的环回状态。对端处于环回状态时，其接收的数据帧，除 OAMPDU 报文外，都会被环回到本端。

6.7.2 规格

Ethernet CFM OAM 特性的规格：

- 支持最多 8 个 MD（Maintenance Domain, MD）。
- 每个 MD 下支持最多 128 个维护集 MA（Maintenance Association, MA）。
- 所有 MD 下支持最多 128 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 1s、10s、1m、10m。

Ethernet EFM OAM 特性的规格：

- 系统默认为 active 模式。
- 支持收发和处理 Information OAMPDU 报文，以进行 OAM 发现过程和获得终端供应商信息。
- 支持解析接收的 Event Notificaiton OAMPDU 报文。
- 支持发送和响应 Loopback Control OAMPDU 报文，即支持发起和响应远端环回。
- 不支持发送和响应 Variable Request OAMPDU 报文，即不支持远端 MIB 变量查询功能。

6.7.3 可获得性

License 支持

Ethernet CFM OAM 特性和 Ethernet EFM OAM 特性都是 MA5620/MA5626 的可选特性，只有获得了 License 许可后才能获得该特性的服务。

硬件支持

用户接口中只有以下接口支持 Ethernet OAM 特性：

- ETH 接入用户接口。
- 上行口中仅 GE、GPON/EPON 接口支持本特性。

6.7.4 Ethernet CFM OAM 原理描述

介绍 Ethernet CFM OAM 特性的实现原理。

说明

本特性中，除非特别说明，MEP 代指 MA5620/MA5626 设备端口。

CFM 诊断、故障检测的手段包括：

- 连续性检查（Continuity Check，CC）
- 环回检测（Loopback，LB）
- 链路跟踪（Linktrace，LT）

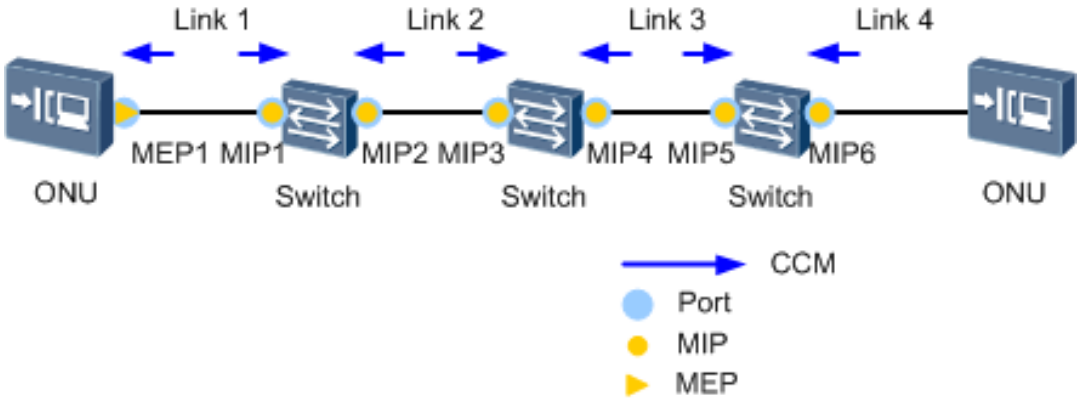
连续性检查（CC）原理

为了保证两台 MA5620/MA5626 的连通性，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 MA5620/MA5626-1 和 MA5620/MA5626-2 互相配置成远端。

- MA5620/MA5626-1：假设在 ETH 接入端口配置 MEP1，如图 6-5 所示，MEP1 需要朝硬件、逻辑方向发送报文，则 MEP1 配置为 UP MEP。
- MA5620/MA5626-2：假设在 GIU 上行端口配置 MEP2，如图 6-5 所示，MEP2 需要朝汇聚方向发送报文，则 MEP2 配置为 Down MEP。

连续性检查（CC）原理如图 6-5 所示。

图 6-5 连续性检查（CC）原理图



连续性检查（CC）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-MA5620/MA56261 和-MA5620/MA56262 之间的网络出现故障。
5. MA5620/MA5626-2 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：

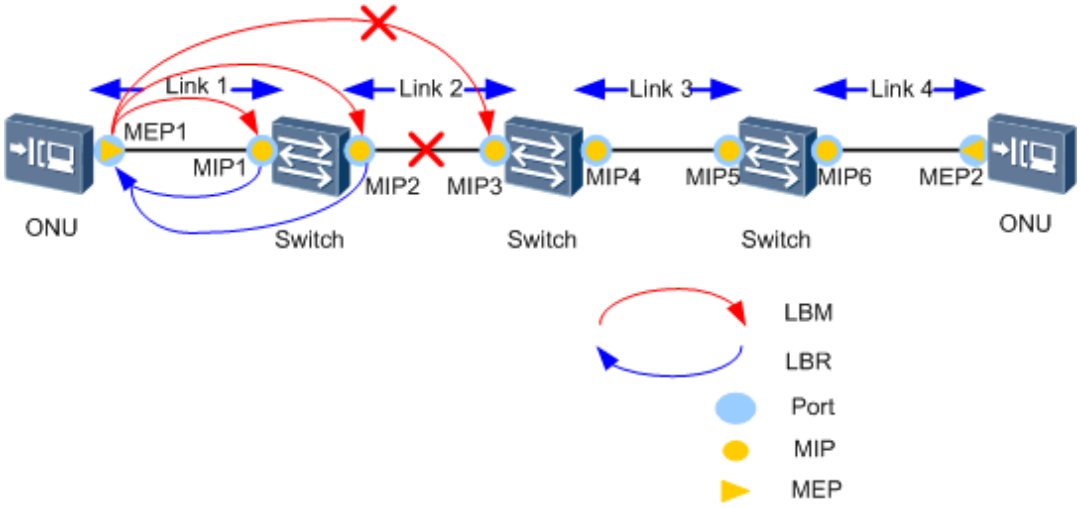
- CC 超时告警：低层交换链路故障，导致 MEP 不能收到 CCM,此时 MEP 的预期远端的 RMEP 定时器超时告警。
- 交叉链接告警：MEP 接受到的 CCM 中 MA 的 ID 和本地配置不符合。
- 收到错误报文告警：MEP 收到的 CCM 中的 MEP 的 ID 和本端口的 MEP 不符合。
- 远端 MEP 端口、接口告警：MEP 收到的 CCM 中包含 Port，Interface TLV。
- 远端 RDI 告警：收到的 CCM 中 RDI 设置为 1。

环回检测（LB）原理

环回检测消息（LBM，LBR）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（LB）原理如图 6-6 所示。

图 6-6 环回检测（LB）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 6-6 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. MA5620/MA5626-1 可以判断 MIP2 和 MIP3 之间的链路故障，即链路 2 故障。

说明

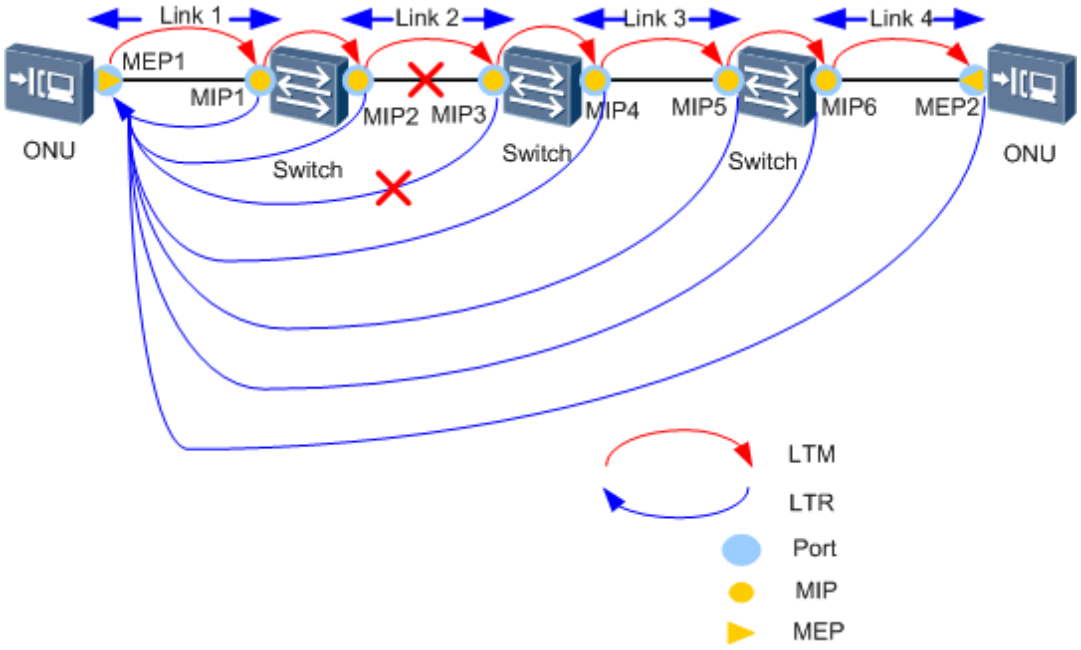
环回检测（LB）是一种手段，只要知道 MA5620/MA5626-1 和 MA5620/MA5626-2 之间所有 MIP（或 MEP）的 MAC 地址，诊断路径可以自由安排。

链路跟踪（LT）原理

链路跟踪消息（LTM，LTR）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（LTM）的 MEP 响应链路跟踪消息（LTR），并转发 LTM，直到到达目的 MIP（或 MEP）。

链路跟踪（LT）原理如图 6-7 所示。

图 6-7 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 LTR，发起 MEP 将会得到 MA 上所有 MIP 的 MAC 地址和相对发起 MEP 的位置，以及出现故障的链路位置区间。链路跟踪（LT）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 6-7 所示，当 MIP2 和 MIP3 之间的链路 2 故障时，MEP1 向 MEP2 发送 LTM，只能收到 MIP1、MIP2 返回的 LTR，不能收到 MIP3 返回的 LTR，从而判断出故障位置。

6.7.5 Ethernet EFM OAM 原理描述

介绍 Ethernet EFM OAM 特性的实现原理。

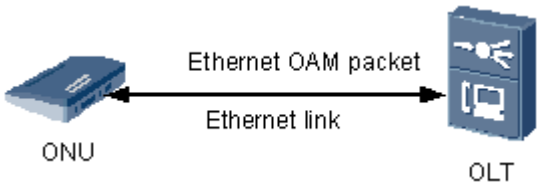
Ethernet EFM OAM 的主要功能有：

- 远端故障管理：如果 ONU 和 OLT 之间的以太链路支持单向传输，即一个方向故障时另一个方向还可以传输数据，则接收故障的一端可以向对端发送特殊的 OAMPDU 报文通知本端故障。
- 远端环回：本端通过发送特殊的 OAMPDU 报文，使对端进入环回状态。对端进入环回状态后，本端发到对端的报文中，除了 OAMPDU 报文之外，其他报文都被原封不动的环回回来。

远端故障管理原理

Ethernet EFM OAM 特性的应用组网如图 6-8 所示。

图 6-8 Ethernet EFM OAM 应用组网图



说明

EFM OAM 报文仅在链路上相邻的两个实体之间进行交换，不会被转发到该链路之外。

Ethernet EFM OAM 特性的远端故障管理功能的原理描述如下：

1. 本端 OLT 和对端 ONU 同时使能 Ethernet EFM OAM 功能；
2. 当对端 ONU 发生了严重事件，包括链路故障、其它未定义的严重事件时，会发送 Event Notification OAMPDU 报文通知本端 OLT；
3. 本端 OLT 收到该报文并进行解析后，上报告警消息给主机。

远端环回原理

说明

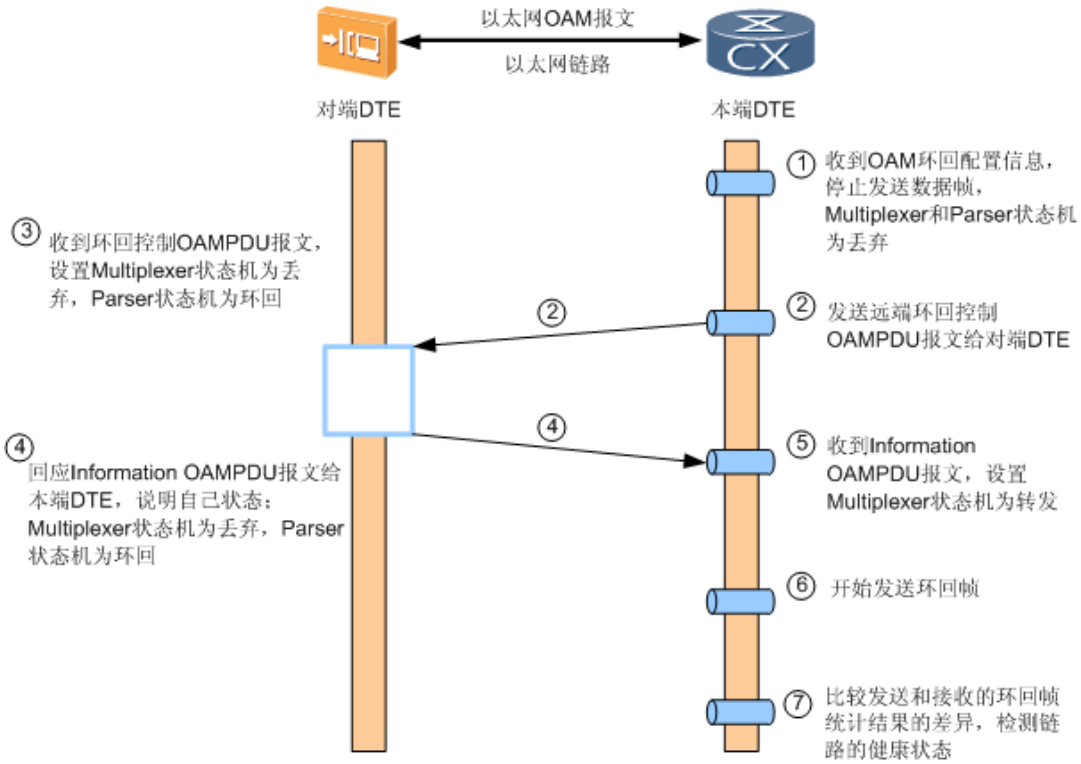
- 远端环回功能是 IEEE802.3ah 协议定义的被远端控制的数据链路层的环回模式。该功能主要用于定位故障的具体区域和进行链路质量测试，质量检测包括报文的吞吐量、误码率、时延、抖动等，同时该端口下需要配置有业务流。
- 对端 DTE 支持远端环回功能是开启远端环回功能的必要条件，只有对端 DTE 支持，才能正常启动远端环回功能。

注意

当开启远端环回功能时，与该 DTE 相连的所有用户的业务都将处于中断状态，所以要谨慎使用该功能。

Ethernet EFM OAM 特性的远端环回功能实现原理如图 6-9 所示。

图 6-9 Ethernet EFM OAM 远端环回原理图



Ethernet EFM OAM 特性的远端环回功能的原理描述如下：

1. 本端 DTE 收到 OAM 环回配置信息，停止发送数据帧，Multiplexer 和 Parser 状态机为丢弃；
2. 本端 DTE 发送远端环回控制 OAMPDU 报文给对端 DTE；
3. 对端 DTE 收到远端环回控制 OAMPDU 报文后，设置其 Multiplexer 状态机为丢弃，Parser 状态机为环回；
4. 对端 DTE 回应 Information OAMPDU 报文给本端 DTE，告知其状态为：Multiplexer 状态机为丢弃，Parser 状态机为环回；
5. 本端 DTE 收到 Information OAMPDU 报文后，设置其 Multiplexer 状态机为转发；
6. 本端 DTE 开始向对端 DTE 发送环回帧；

   说明

   当链路以及对端 DTE 正常情况下，对端 DTE 会将环回帧原封不动地环回给本端 DTE。
7. 本端 DTE 分析本端 DTE 发送 MAC 地址帧报文和对端 DTE 环回 MAC 地址帧报文，通过比较前后统计结果的差异，可以确定链路的时延、误码率等质量问题，从而可以检测链路的健康状态。

6.8 Ring Check

介绍 Ring Check 特性的定义、目的、规格和原理。

6.8.1 介绍

定义

Ring Check 特性是通过设备在用户端口周期性发送 Ring Check 报文，监控用户侧和网络侧收到的 Ring Check 报文，检测运营商网络是否形成环路。如果网络中有环路产生，MA5620/MA5626 设备通过去激活形成环路的用户端口，并上报告警给网络管理系统，以保证设备的正常运转，其他合法用户不被干扰。

目的

- 防止单个用户端口自环。
- 防止不同用户端口之间形成环路。
- 防止用户侧端口和网络侧端口形成环路。

受益

运营商受益

Ring Check 特性通过检测运营商网络，并上报告警给网络管理系统，使得运营商可以在最短的时间内获取到网络异常信息，快速排除故障，恢复网络正常运行。

用户受益

Ring Check 特性通过去激活环路端口，保证合法用户不被干扰，获得良好的网络服务。

6.8.2 规格

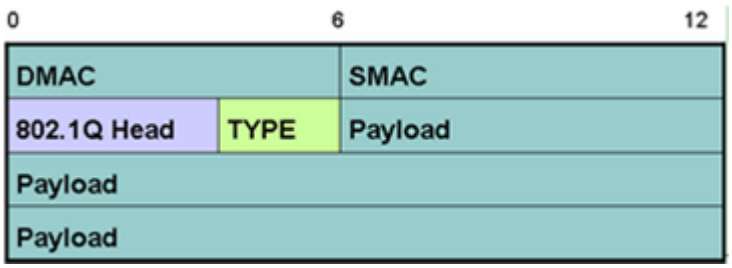
- 支持使能或去使能 Ring Check 特性。
- 支持用户端口自环检测、用户端口之间的环路检测、用户端口和网络侧端口之间的环路检测。
- 支持 Ring Check 特性协议类型可配置。

6.8.3 原理描述

实现原理

Ring Check 特性是通过设备在用户端口周期性发送 Ring Check 报文，监控用户侧和网络侧收到的 Ring Check 报文，检测运营商网络是否形成环路。其报文格式如图 6-10 所示。

图 6-10 Ring Check 报文格式



- DMAC 为广播 MAC 地址，SMAC 为桥 MAC 地址。
- 802.1Q Head 可以根据用户侧流属性，自动选择是否填写，无需用户配置。
- TYPE 为私有以太网类型，用户可配置。
- 报文内容 Payload 为私有，用户无需关注。

Ring Check 过程

- 系统使能 Ring Check 特性后，定时向用户端口发送自定义的广播报文，每秒发送 16 个 Ring Check 报文。并且只对流状态为 Up 的流索引发送 Ring Check 报文。
- 通过设备在用户端口周期性发送 Ring Check 报文，实时监控用户侧和网络侧收到的 Ring Check 报文，检测运营商网络是否形成环路。
- 当检测到运营商网络形成环路时，上报告警给网络管理系统，并去激活形成环路的用户端口从而保证设备的正常运转，保证其他合法用户不被干扰。
- 网络管理员排查了故障以后，重新激活用户端口，系统会对激活的用户端口重新自动进行监控。

6.9 术语与缩略语

术语

表 6-2 组网特性术语表

术语	解释
CFM	CFM（Connectivity Fault Management）是端到端的以太网连接故障管理，是实现 Ethernet OAM 的主要协议，可以将 CFM 理解为 OAM 的一个子集。
维护实体	维护实体（Maintenance Entities，ME）是网络中可维护的设备，更确切地说是网络中的桥设备，即可过 VLAN+MAC 进行二层转发的设备。
维护域	维护域（Maintenance Domain, MD）是桥接设备和维护级别的组合。
维护集	在维护域下可以划分成若干个维护集（Maintenance Association, MA）。每个维护集对应维护域上的一个通常用 VLAN 来标识的业务实例（Service Instance, SI），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。
维护节点	MA 由维护节点（Maintenance Point, MP）组成。MP 定义在桥接设备的端口上，即 MP 是桥端口，VLAN，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）。设备在每个 MA 中可配置一个 MEP，且该 MEP 是 MA 的边缘节点。MEP 关联一个设备的一个端口。

术语	解释
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（Remote Maintenance association End Point）。
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 MA5620/MA5626 上行 GIU 端口为 MEP，如果定义 GIU 端口只能朝上行方向（汇聚层）发送报文，则该端口就是 Down MEP；如果定义 GIU 端口只能朝下行方向（朝向硬件、逻辑等）发送报文，则该端口就是 UP MEP。
EFM	EFM（Ethernet in the First Mile）是定义用户接入部分的以太网物理层规范，以及接入部分的以太网 OAM，主要用于最后一公里的链路检测，是链路级的 OAM，可以将 EFM 理解为 OAM 的一个子集。
OAM 能力发现	以太网 OAM 的 Discovery 过程来发现对端 DTE 的能力，包括 OAM 的配置信息、OAM 模式信息、OAMPDU 信息、OUI 信息等。
远端故障管理	提供了一种诊断对端 DTE 的能力，当对端 DTE 故障或者不可用导致流量中断时，会通过 OAMPDU 的 flag 域向本端发送通知消息。
远端环回	通过命令控制对端 DTE 进入环回状态。EFM 的远端环回功能主要用于故障定位和链路性能测试。在远端环回模式下可以通过查询、比较本端和对端的统计报文来实现。
Multiplexer 状态机	IEEE802.3ah 定义的一种状态机，用于对报文发送的控制。
Parser 状态机	IEEE802.3ah 定义的一种状态机，用于对报文接收的控制。

缩略语

表 6-3 组网特性缩略语表

缩略语	全称
OAM	Operations Administration and Maintenance（操作管理维护）
STP	Spanning Tree Protocol（生成树协议）
CFM	Connectivity Fault Management（连接故障管理）
MD	Maintenance Domain（维护域）
MA	Maintenance Association（维护集）

缩略语	全称
MEP	Maintenance End Point（维护实体端点）
RMEP	Remote Maintenance association End Point（远端维护实体端点）
MIP	Maintenance Intermediate Point（维护实体中间点）
CC	Continuity Check（连续性检查）
LB	Loopback（环回）
LT	Linktrace（链路跟踪）
TLV	Type、Length、Value（类型、长度、值）
EFM	Ethernet in the First Mile（最后一英里以太网）
OAMPDU	OAM Protocol Data Unit（操作管理维护协议数据单元）
OUI	Organizationally Unique Identifier（组织唯一标识）
RDI	Remote Defect Indication（远端故障指示）
DTE	Digital Terminal Equipment（数字终端设备）

7 用户安全

关于本章

首先从介绍、总体规格、可获得性等方面对用户安全特性进行介绍，然后分别阐述各子特性。

7.1 介绍

7.2 参考标准和协议

7.3 可获得性

7.4 PITP （PITP P 模式，PITP V 模式）
首先介绍 PITP 协议（包含：PITP P 模式，PITP V 模式），然后对规格和原理进行阐述。

7.5 DHCP Option82
DHCP Option82 是一种用户安全机制，在用户发起的 DHCP 请求报文的 Option82 字段中，添加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。本特性从介绍、原理描述和参考信息方面进行描述。

7.6 RAIO
首先介绍 RAIO 协议，然后对其规格和原理进行阐述。

7.7 防御 MAC Spoofing
首先介绍防御 MAC Spoofing 的含义，然后对其规格和原理进行阐述。

7.8 防御 IP Spoofing
首先介绍防御 IP Spoofing 的含义，然后对其规格和原理进行阐述。

7.9 用户隔离
首先介绍用户隔离，然后对其规格和原理进行阐述。

7.10 术语与缩略语

7.1 介绍

用户安全是指保证接入用户的安全的机制，分为 PITP、DHCP Option82、RAIO、防御 MAC Spoofing、防御 IP Spoofing 和用户隔离特性。

特性名称	特性简介
PITP	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。
DHCP Option82	在用户发起的 DHCP 请求报文的 Option82 字段中，添加用户物理信息，以配合上层认证服务器进行用户认证。
RAIO	RAIO（Relay Agent Information Option）是 PITP 和 DHCP Option82 功能使能时，设备向 BRAS 或 DHCP Server 提供的用户物理信息，如设备上的框/槽/端口等。
防御 MAC Spoofing	系统防御用户伪造 MAC 地址进行攻击的特性。
防御 IP Spoofing	系统防御用户伪造 IP 地址进行攻击的特性。
用户隔离	通过 MuX VLAN 限制不同 VLAN 间的用户之间互访，通过 Smart VLAN 限制同一 VLAN 内的用户之间互访，从而达到不同层面用户隔离的目的。

7.2 参考标准和协议

PITP

符合 TR101。

RAIO

符合 TR101。

7.3 可获得性

涉及网元

PITP 与 RAIO 共同配合使用，需要 MA5620/MA5626、BRAS 和 RADIUS Server 配合完成。对这些网元的要求如表 7-1 所示。

表 7-1 PITP 特性对网元要求

MA5620/MA5626	BRAS	RADIUS Server
√	√	√

DHCP OPTION82 与 RAIO 共同配合使用，需要 MA5620/MA5626、DHCP 中继代理或者 DHCP 服务器配合完成。

表 7-2 DHCP OPTION82 特性对网元要求

MA5620/MA5626	DHCP 中继代理或者 DHCP 服务器
√	√

- RAIO 一般配合 PITP 和 DHCP Option82 使用。
- 防御 MAC Spoofing、防御 IP Spoofing 和用户隔离特性只涉及 MA5620/MA5626 设备，不涉及其他网元。

License 支持

- PITP 特性是 MA5620/MA5626 的可选功能，只有获得 License 许可才能获得该特性的服务。
- DHCP Option82 特性是 MA5620/MA5626 的可选功能，只有获得 License 许可才能获得该特性的服务。

特性依赖

- 系统全局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。
- PITP V 模式协议类型不能设置为已知的以太网协议类型，否则存在冲突。需要设置为不和已知协议冲突的类型。
- 向 BRAS 提供的接入用户物理信息由 RAIO（Relay Agent Info Option）工作模式决定。
- MUX VLAN 和 Smart VLAN 在系统内可以共存。

其他

- PITP、DHCP Option82 支持用户端口，对用户接入方式无要求。
- RAIO 配合 PITP 和 DHCP Option82 使用，为 PITP 和 DHCP Option82 提供用户物理信息格式。

7.4 PITP （PITP P 模式，PITP V 模式）

首先介绍 PITP 协议（包含：PITP P 模式，PITP V 模式），然后对规格和原理进行阐述。

7.4.1 介绍

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 PITP P 模式和 PITP V 模式。

- PITP 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。
- PITP P 模式则是接入设备在 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。

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物理位置信息，BRAS 设备获取用户接入位置信息后，可实现对用户账号与接入位置信息的绑定认证，避免用户账号的盗用与漫游。

受益

运营商受益：通过提供高可靠性的业务，提升自我品牌和价值。

用户受益：PITP 通过用户物理信息与用户帐号绑定认证，避免用户帐号密码被盗。

7.4.2 规格

该特性的相关规格如下：

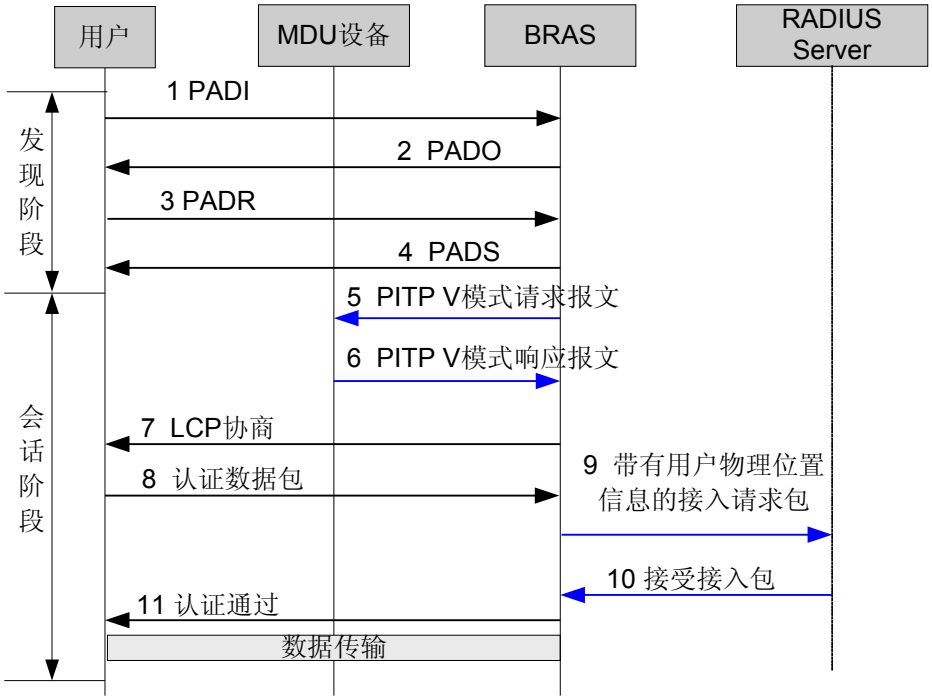
- PITP 支持两种模式：PITP P 模式 PITP V 模式。
- PITP 开关分为两级：系统级开关和 VLAN 级开关。只有两个级别的开关同时开启，接入设备才会向 BRAS 提供用户物理位置信息。
- PITP 系统级开关缺省关闭，VLAN 级开关缺省开启。

7.4.3 原理描述

V 模式实现原理

启动 PITP V 模式后，PPPoE 拨号过程如图 7-1 所示。

图 7-1 启动 V 模式功能的 PPPoE 拨号过程



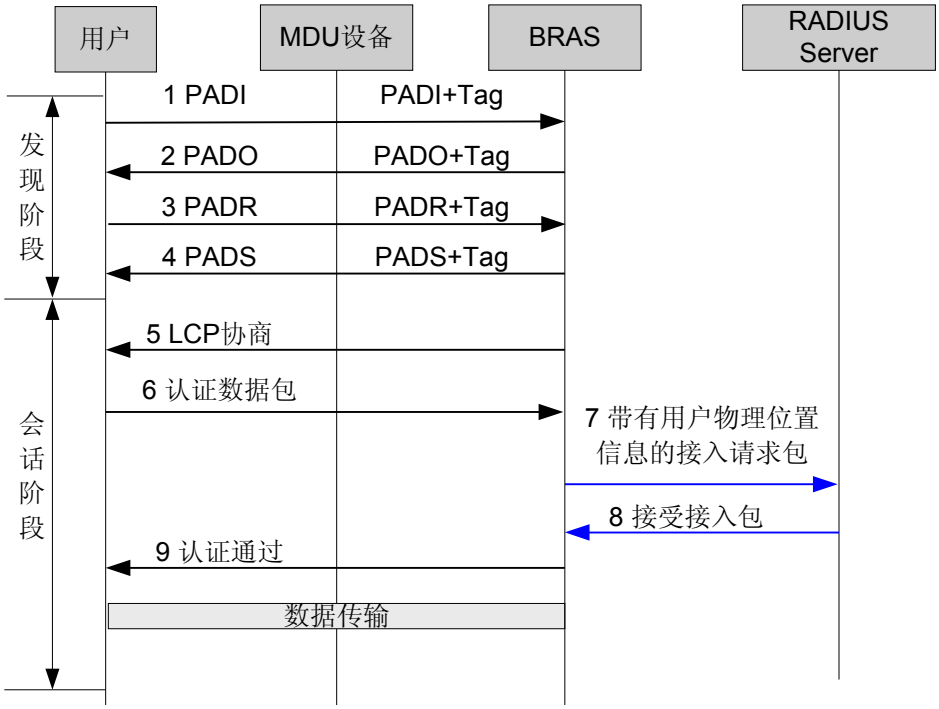
PITP V 模式的三个过程为：

1. 在 PPPoE 发现阶段结束后，由 BRAS 向接入设备发送 PITP 请求报文，请求用户所在的物理位置信息。
2. 设备收到 PITP 请求报文后，根据请求报文中的用户 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 PITP 响应报文，该响应报文中包含接入用户的物理位置信息。否则不应答。

P 模式实现原理

启动 PITP P 模式后，PPPoE 拨号过程如图 7-2 所示。

图 7-2 启动 P 模式功能的 PPPoE 拨号过程



启动 PITP P 模式功能后，在 PPPoE Discovery 阶段，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。

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

- 在 PPPoE Discovery 阶段，MDU 和 BRAS 之间交互的 PPPoE 报文中都携带了用户物理位置信息。MDU 负责在收到来自用户的 PPPoE 报文后插入用户物理信息，然后转发给 BRAS；收到来自 BRAS 的带用户物理位置信息的 PPPoE 报文后，剥离该信息，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 MDU 的 PPPoE 报文中携带的用户物理位置信息提取出来，放到认证请求报文中，为服务器认证提供用户物理信息。

7.5 DHCP Option82

DHCP Option82 是一种用户安全机制，在用户发起的 DHCP 请求报文的 Option82 字段中，添加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。本特性从介绍、原理描述和参考信息方面进行描述。

7.5.1 介绍

7.5.2 规格

7.5.3 原理描述

7.5.1 介绍

定义

DHCP Option82 与 PPPoE+类似，作为一种用户安全机制，在用户发起的 DHCP 请求报文的 Option82 字段中，添加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。

7.5.2 规格

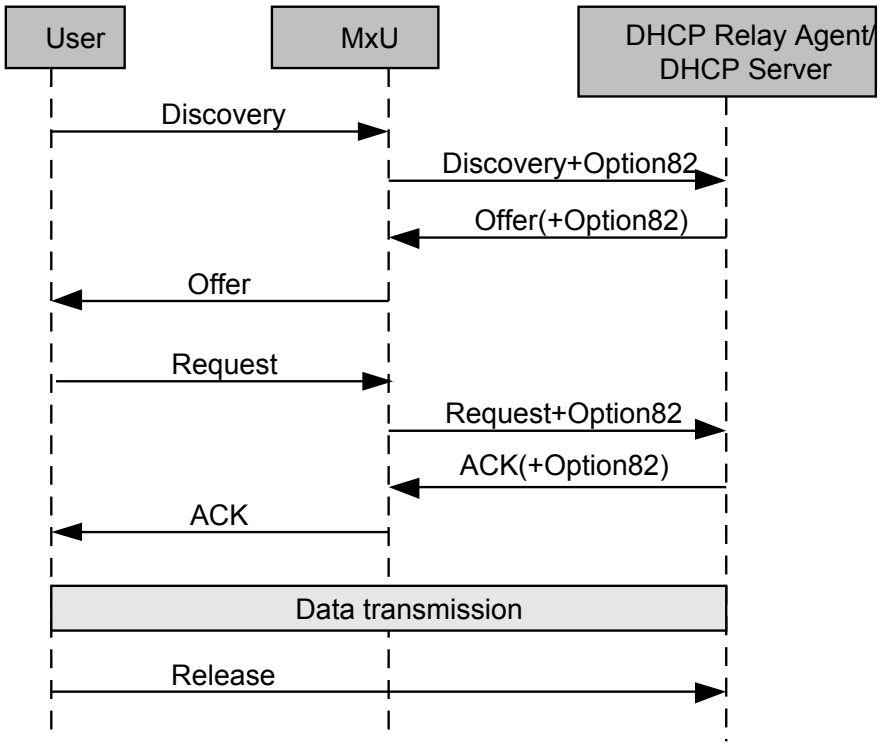
DHCP Option82 开关分为三级：全局级和 VLAN 级。只有各个级别开关全部打开，系统才会在上行的 DHCP 报文中添加 Option82 信息。

7.5.3 原理描述

基本原理

DHCP Option82 功能启动时，DHCP 过程如图 7-3 所示。

图 7-3 启动 Option82 功能的 DHCP 过程



DHCP Option82 的原理与 PPPoE+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。

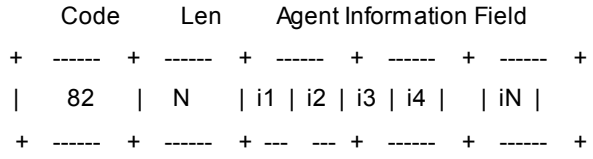
DHCP Option82 报文格式

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 7-4 所示。

图 7-4 DHCP Option82 字段报文格式



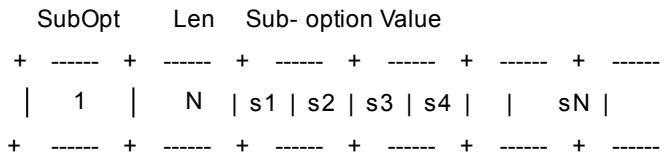
DHCP Option82 报文各字段具体含义，如表 7-3 所示。

表 7-3 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，其长度由字段 Len 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 7-5 所示。

图 7-5 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 PPPoE+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 **7.6 RAIO**。

7.6 RAIO

首先介绍 RAIO 协议，然后对其规格和原理进行阐述。

7.6.1 介绍

定义

RAIO（Relay Agent Information Option）是指在 PITP 和 DHCP Option82 功能使能时，设备通过 PITP 应答报文（PITP V 模式）、PPPoE Discovery 报文（PITP P 模式）和 DHCP 报文（DHCP Option82）向 BRAS 或 DHCP Server 提供的用户物理信息，如设备上的框/槽/端口等。

目的

RAIO 的目的在于设备向 BRAS 或者 DHCP Server 提供用户的物理位置信息，与 PITP、DHCP Option82 配合使用来实现用户帐号的安全。

受益

运营商受益：为运营商提供灵活的的个性化需求，方便运营商合理网络规划。

用户受益：通过用户物理信息与用户帐号绑定认证，避免用户帐号密码被盗。

7.6.2 规格

该特性的相关规格如下：

RAIO 工作模式包括：Common、Port-userlabel、Service-port-userlabel、User-defined。

7.6.3 原理描述

Common 模式实现原理

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 7-4** 所示。

表 7-4 不同接入方式的 CID 格式

接入方式	CID 格式
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“MA5620/MA5626”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“MA5620/MA5626”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 MA5620/MA5626 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）

Port-userlabel 模式实现原理

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

Service-port-userlabel 模式实现原理

CID 支持 ETH 接入。RID 中携带用户所在的流描述信息。

RAIO 字段具体格式如表 7-5 所示。

表 7-5 Service-port-userlabel 模式下的 RAIO 字段

字段	接入方式	CID 格式
CID	ETH	基于 VLAN 的多业务：<Access-Node-Identifier> eth slot/port：flowpara 其他：<Access-Node-Identifier> eth slot/port：vlanid
RID	-	description-of-flow-label（流描述信息）

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 7-6 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 7-6 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
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
Bslot	BRAS 槽位号	Yes	4
Bsubslot	BRAS 子槽号	Yes	4
Bporttype	BRAS 接入方式	Yes	4
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		

关键字	描述	可订宽度	最大宽度
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	ETH AXPI 对应于网络侧的 vlanid	Yes	4
AXCI	ETH 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	Yes	5
UpRate	xDSL 线路上行激活速率，以 kbit/s 为单位	Yes	6
DnRate	xDSL 线路下行激活速率，以 kbit/s 为单位	Yes	6

- 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 VPI 与 Gemport，或同时出现 ETH 与 VCI 都是不合法的。
- 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 7-7 所示。

表 7-7 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“-”

分隔符	表示符号
%	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。

User-defined 模式 RAIO 字段格式举例：

系统名称－MxU01，槽号－3，端口号－15，VPI－0，VCI－35，优先级－6，则自定义的 CID 字符串：anid atm slot/port：vpi.vci%priority，最终生成的字符串为：“mxu01 atm 3/15：0.35%6”。

7.7 防御 MAC Spoofing

首先介绍防御 MAC Spoofing 的含义，然后对其规格和原理进行阐述。

7.7.1 介绍

定义

MAC Spoofing 攻击指恶意用户伪造 MAC 地址发送报文进行网络攻击。恶意用户可以通过伪造正常用户的 MAC 地址，破坏正常用户的业务；或者向系统发送大量含有不同 MAC 地址的伪造报文，破化系统正常工作，甚至导致系统瘫痪。

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

目的

为了保护系统和运营商网络的正常运营，对于通过 PPPoE 和 DHCP 上线流程进入运营商网络的正常用户，系统动态 MAC 地址绑定，仅允许有限的、安全的 MAC 地址通过正常的 PPPoE 和 DHCP 上线流程进入运营商网络，禁止不信任的 MAC 地址进入运营商网络。

对于不经过 PPPoE 或者 DHCP 上线流程进入运营商网络的正常用户，通过静态 MAC 地址绑定，仅允许有限的、安全的 MAC 地址进入运营商网络。

受益

运营商受益：防御 MAC Spoofing 通过动态 MAC 地址绑定或者静态 MAC 地址绑定，保护运营商的网络不被攻击。

用户受益：防御 MAC Spoofing 通过动态 MAC 地址绑定或者静态 MAC 地址绑定，提高用户业务的安全性。

7.7.2 规格

该特性的相关规格如下：

- 静态绑定：系统支持 1K 个静态 MAC 地址的绑定，对每条业务流上可以绑定的 MAC 地址没有限制。
- 动态绑定：
  - 支持系统级开关。
  - 系统支持动态绑定的 MAC 地址总数为 1K。
  - 每条业务流最多可以绑定 8 个 MAC 地址（最多可以支持 256 条业务流）

7.7.3 原理描述

实现原理

- 动态 MAC 地址绑定防御 MAC Spoofing
  1. 系统关闭用户的动态 MAC 地址学习功能，监控用户的 PPPoE 和 DHCP 上线下线流程，在用户的上线过程中，动态获取用户的 源 MAC 地址，设置用户的 源 MAC 地址与用户端口或者业务流的绑定关系。
  2. 只允许源 MAC 地址为已经绑定到端口或者业务流的 MAC 地址的业务 报文通过设备
  3. 在用户的下线过程中，解除用户的源 MAC 地址与用户端口或者业务流的绑定关系。
- 静态 MAC 地址绑定防御 MAC Spoofing

  系统关闭用户的动态 MAC 地址学习功能，通过网管或者命令行接口，设置用户的源 MAC 地址与用户端口或者业务流的绑定关系。

7.8 防御 IP Spoofing

首先介绍防御 IP Spoofing 的含义，然后对其规格和原理进行阐述。

7.8.1 介绍

定义

IP Spoofing 攻击指恶意用户伪造 IP 地址发送报文进行网络攻击。恶意用户可以通过伪造正常用户的 IP 地址，破坏正常用户的业务。

防御 IP Spoofing 攻击特性指系统防御用户伪造 IP 地址进行攻击的特性。

目的

为了保护运营商网络的正常运营，对于通过 DHCP 上线流程进入运营商网络的正常用户，系统动态 IP 地址绑定，仅允许安全的 IP 地址通过正常的 DHCP 上线流程进入运营商网络，禁止不信任的 IP 地址进入运营商网络。

对于不经过 DHCP 上线流程进入运营商网络的正常用户，通过静态 IP 地址绑定，仅允许安全的 IP 地址进入运营商网络。

受益

运营商受益：防御 IP Spoofing 通过动态 IP 地址绑定或者静态 IP 地址绑定，保护运营商的网络不被攻击。

用户受益：防御 IP Spoofing 通过动态 IP 地址绑定或者静态 IP 地址绑定，提高用户业务的安全性。

7.8.2 规格

该特性的相关规格如下：

- 静态绑定：系统支持 1K 个静态 IP 地址的绑定，每条业务流上可以绑定 8 个 IP 地址。
- 动态绑定：
  - 支持系统级开关和 VLAN 级开关。
  - 系统支持动态绑定的 IP 地址总数为 1K。
  - 最多允许 512 条业务流绑定 IP 地址，每条业务流最多绑定 8 个 IP 地址。
- 支持基于 VLAN 的防御 IP Spoofing 特性。

7.8.3 原理描述

实现原理

- 动态 IP 地址绑定防御 IP Spoofing
  - 系统关闭用户的动态 IP 地址学习功能，监控用户的 DHCP 上线下线流程，在用户的上线过程中，动态获取用户的源 IP 地址，设置用户的源 IP 地址与用户业务流绑定。
  - 只允许源 IP 地址为已经绑定到业务流的 IP 地址的业务报文通过设备。
  - 在用户的下线过程中，解除用户的源 IP 地址与用户业务流的绑定关系。
- 静态 IP 地址绑定防御 IP Spoofing

  通过网管或者命令行接口，设置用户的源 IP 地址与用户业务流的绑定关系。

7.9 用户隔离

首先介绍用户隔离，然后对其规格和原理进行阐述。

7.9.1 介绍

定义

MDU 支持 MUX VLAN 和 Smart VLAN，MUX VLAN 将用户业务划分在不同的虚拟局域网（VLAN）内，各 VLAN 之间的业务是隔离的，从而限制不同 VLAN 间的用户之间互访。

在同一 Smart VLAN 内，不同的用户端口之间也是隔离的，从而限制同一 VLAN 内的用户之间互访。

目的

通过将用户业务流或者用户端口划分在不同的 VLAN，或者通过 Smart VLAN 隔离 VLAN 内的业务流或者用户端口，以限制用户之间的相互访问，保障用户的业务安全。

受益

运营商受益：通过提供高安全性的业务，提升自我品牌和价值。

用户受益：享受高安全性的网络。

7.9.2 规格

该特性的相关规格如下：

- 支持 MUX VLAN
- 支持 Smart VLAN

7.9.3 原理描述

实现原理

MUX VLAN 通过将用户业务流或者用户端口划分在不同的 VLAN 实现用户间的隔离。

Smart VLAN 通过隔离 VLAN 内的业务流或者用户端口，以限制用户之间的相互访问。

7.10 术语与缩略语

术语

无

缩略语

表 7-8 用户安全特性缩略语表

缩略语	全称
PITP	Policy Information Transfer Protocol（策略信息传输协议）
DHCP	Dynamic Host Configuration Protocol（动态主机配置协议）
RAIO	Relay Agent Information Option

8 系统安全

关于本章

首先从概述、总体规格、可获得性等方面对系统安全特性进行介绍，然后分别阐述各子特性。

8.1 介绍

8.2 可获得性

8.3 防御 DoS 攻击
首先介绍 DoS 攻击及防御，然后对其原理进行阐述。

8.4 防御 ICMP/IP 攻击
首先介绍防御 ICMP/IP 攻击，然后对其原理进行阐述。

8.5 源路由过滤
首先介绍源路由过滤，然后对其原理进行阐述。

8.6 MAC 地址过滤
首先介绍 MAC 地址过滤，然后对其原理进行阐述。

8.7 防火墙黑名单功能
首先介绍防火墙黑名单功能，然后对其原理进行阐述。

8.8 允许/拒绝访问地址段
首先介绍允许/拒绝访问地址段，然后对其原理进行阐述。

8.9 业务过载控制
介绍业务过载控制特性的定义、目的及原理。

8.10 1:1 VMAC
VMAC 是指虚拟 MAC，1:1 VMAC 是指设备用唯一的虚拟 MAC 来替换单个用户的 MAC，用户 MAC 与设备 VMAC 的对应关系是 1:1。

8.11 术语与缩略语

8.1 介绍

特性名称	特性简介
防御 DoS 攻击	指系统对用户发送的协议报文进行限制性接收的防御攻击措施。
防御 ICMP/IP 攻击	指系统丢弃从用户侧发给设备本身的 ICMP 报文、IP 报文。
源路由过滤	指系统把用户发送的 IP 报文中含有路由选项字段的报文过滤掉。
MAC 地址过滤	针对用户报文携带的源 MAC 地址或目的 MAC 地址对报文进行过滤。
防火墙黑名单功能	系统过滤掉所有源 IP 地址在黑名单上的业务报文。
防火墙功能	系统根据 ACL（Access Control List）进行数据包过滤。
允许/拒绝访问地址段	系统支持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。
1:1 VMAC	VMAC（Virtual MAC）即虚拟 MAC 地址，由 MA5620/MA5626 采用虚拟 MAC 地址代替终端用户源 MAC 地址。

8.2 可获得性

涉及网元

设备操作维护安全主要是针对设备本身的安全管理，不涉及其他网元。

License 支持

无需获得 License 许可即可获得设备操作维护安全特性的服务。

特性依赖

- 由于 ICMP/IP 报文是由主机 CPU 进行过滤，因此如果短时间内出现大流量的报文攻击，会导致系统的 CPU 占用率过高，这种情况下，可以通过防 DoS 攻击手段来防范。
- 防 ICMP/IP 攻击打开时，会导致用户无法 ping 通设备的三层接口，也不能从用户侧 telnet 设备。
- 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）。
- 对报文源 IP 地址进行检查或进行 ACL 匹配，对系统性能没有明显的影响。
- 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。
- MAC 地址过滤是硬件过滤，对系统性能无影响。

- 如果用户的 IP 地址在不允许的 IP 地址段内，则不允许用户登录，因此需要事先将配置允许访问系统的 IP 地址网段。

8.3 防御 DoS 攻击

首先介绍 DoS 攻击及防御，然后对其原理进行阐述。

8.3.1 介绍

定义

DoS（Denial of Service）攻击指恶意用户发送大量的协议报文攻击系统，导致系统无法处理正常用户的服务请求，即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协议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，可能引起系统无法处理正常用户的服务请求，甚至导致系统瘫痪。

为了保护系统，将系统接收的用户协议报文数量限制在规定的范围内。对于超出规定范围的报文，作为非法报文丢弃；对发起 DoS 攻击的用户加入黑名单，并拒绝接收该用户的协议报文。对于黑名单用户，系统管理员可以强制该用户下线。

受益

运营商受益：防御 DoS 通过对发起 DoS 攻击的用户加入黑名单，保护运营商的网络不被攻击。

用户受益：提高用户业务的安全性，使用户享受稳定、安全的业务。

8.3.2 规格

该特性的相关规格如下：

- 支持防御 DoS 攻击特性开启和关闭，缺省关闭。
- 支持的黑名单个数为设备支持的用户端口数。
- 支持 DoS 攻击出现/消失时发出告警/告警恢复。

8.3.3 原理描述

实现原理

防御 DoS 攻击功能的实现原理如下：

1. 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）。
2. 开启防御 DoS 攻击控制开关时，根据下面的流程判断是否发生 DoS 攻击及是否已经停止攻击：
   - 系统对每个用户端口送交 CPU 的协议报文个数进行监测，如果发现报文数量超出用户正常业务的报文平均数目，则认为该端口发生了 DoS 攻击。
   - 用户端口发生 DoS 攻击时，系统将该用户端口加入黑名单，并禁止该端口的协议报文发送到 CPU。
   - 系统检测到用户端口在一定时间内没有 DoS 攻击时，将用户端口从黑名单中删除，允许该端口的报文发送到 CPU。

8.4 防御 ICMP/IP 攻击

首先介绍防御 ICMP/IP 攻击，然后对其原理进行阐述。

8.4.1 介绍

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。这种攻击也可认为是 DoS 攻击的一种。

如果恶意用户短时间内用大量的 ICMP 消息（如 ping）和 IP 报文向接入系统不断请求回应，致使接入系统负担过重而不能处理合法的任务。

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。

8.4.2 规格

支持通过命令行或网管打开或关闭防御 ICMP/IP 攻击特性开关。

支持通过命令行或网管查询防御 ICMP/IP 攻击特性开关配置情况。

8.4.3 原理描述

实现原理

如果接入用户向接入设备发出的 ICMP/IP 报文的目的 IP 地址为系统的 IP 地址，则该 ICMP/IP 报文将被丢弃。

8.5 源路由过滤

首先介绍源路由过滤，然后对其原理进行阐述。

8.5.1 介绍

定义

带源路由选项的 IP 报文明确指明了报文的传输路径。例如：让一个 IP 报文明确的经过三台路由器 R1、R2、R3，则可以在源路由选项中指明这三个路由器的接口地址；这样不论三台路由器上的路由表如何，这个 IP 报文就会依次经过 R1、R2、R3。

这些带源路由选项的 IP 报文在传输的过程中，其源地址不断改变，目标地址也不断改变。因此，通过合适的设置源路由选项，攻击者便可以伪造一些合法的 IP 地址，而蒙混进入网络。

源路由过滤特性是指把用户发送的 IP 报文中含有路由选项字段的报文过滤掉。

目的

源路由过滤特性的目的就是通过识别并丢弃带源路由选项的 IP 报文，防止恶意用户伪造 IP 报文对运营商网络进行攻击。

受益

运营商受益：可以防止恶意用户伪造 IP 报文对运营商网络进行攻击。

8.5.2 规格

支持通过命令行或网管设置源路由选项报文过滤功能。

支持通过命令行或网管查询源路由选项报文过滤功能。

8.5.3 原理描述

实现原理

MDU 在使能源路由过滤功能后，MDU 系统将丢弃接入用户发送的带源路由选项的 IP 报文。

8.6 MAC 地址过滤

首先介绍 MAC 地址过滤，然后对其原理进行阐述。

8.6.1 介绍

定义

MAC 地址过滤指对用户报文携带的源 MAC 地址或目的 MAC 地址进行过滤。

目的

MAC 地址过滤特性支持配置禁止用户携带的源 MAC 地址或目的 MAC 地址，主要是为了防止恶意用户假冒网络设备 MAC 地址对运营商网络的攻击。

8.6.2 规格

该特性的相关规格如下：

- 系统支持 4 个源 MAC 地址的过滤。
- 系统支持 4 个目的 MAC 地址的过滤。

8.6.3 原理描述

实现原理

MAC 地址过滤功能主要是针对源 MAC 地址和目的 MAC 地址进行过滤，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源地址。
2. 用户报文上行时，系统检查该报文的源 MAC 地址，如果检查到的源 MAC 地址和已经配置的网络侧设备的 MAC 地址相同，则系统将丢弃该用户报文。
3. 为了防止用户攻击网络侧设备，可以将网络侧设备的 MAC 地址设置为要过滤的目的地址。

8.7 防火墙黑名单功能

首先介绍防火墙黑名单功能，然后对其原理进行阐述。

8.7.1 介绍

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 地址在黑名单上的业务报文，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。

受益

运营商受益：运营商可以自行设定黑名单屏蔽有恶意行为的 IP 地址用户对系统的攻击。

8.7.2 规格

该特性的相关规格如下：

- 支持手动配置 1024 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。

8.7.3 原理描述

实现原理

防火墙黑名单功能的实现原理如下：

1. 如果用户报文的源 IP 地址为防火墙黑名单中的 IP 地址，则该报文被丢弃。
2. 对于匹配 ACL 规则的报文，如果 ACL 规则拒绝这类报文访问，则报文将被丢弃；如果 ACL 规则允许这类报文访问，则无论报文 IP 地址是否在黑名单列表中，报文都可以通过。

8.8 允许/拒绝访问地址段

首先介绍允许/拒绝访问地址段，然后对其原理进行阐述。

8.8.1 介绍

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

系统支持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，以防止非法 IP 地址段的用户登录系统，维护系统的安全。

受益

运营商受益：可以防止非法 IP 地址的用户登录系统，维护系统的安全。

8.8.2 规格

该特性的相关规格如下：

- 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。
- 对于任何类型的 IP 报文，都支持设置允许访问地址段功能。
- 最多可以配置 8 条允许访问的 IP 地址段，源 IP 地址不在允许的 IP 地址范围内的报文将不允许访问系统。

8.8.3 原理描述

实现原理

当用户以 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，以决定是否允许用户登录。

1. 如果用户的 IP 地址在允许的 IP 地址段内，则允许用户登录。
2. 如果用户的 IP 地址在不允许的 IP 地址段内，则不允许用户登录。

8.9 业务过载控制

介绍业务过载控制特性的定义、目的及原理。

8.9.1 介绍

定义

过载控制特性用于防止设备系统资源被过度的消耗，如：CPU 资源，以保证在业务量过大时，设备不会因 CPU 或其他资源过载而导致业务中断或网管脱管，且在系统过载时，在一定的范围内，优先保证高优先级的关键业务质量。如：语音的 119 呼叫等。

同时，对窄带业务来说，在大流量业务输入下，不同 VAG 之间以及不同 ISDN 单板或端口之间的业务量保持相对的平衡，不相互影响，某个 VAG、ISDN 单板或端口的流量冲击不会影响其他 VAG、ISDN 单板或端口业务。

目的

在 MA5620/MA5626 设备中，当业务突发大流量时将直接导致系统 CPU 占用率或业务资源上升，如果不区分不同流量的优先级，系统将无法正常处理业务，从而导致系统业务中断，因此需要对上报到 CPU 的报文按照一定的优先级规则进行过滤，当 CPU 占有率达到阀值时，对低优先级报文进行丢弃以及高优先线级的业务优先处理。

支持业务过载控制特性之后，可以对上报到 CPU 的报文进行过滤控制，防止恶意攻击以及瞬间业务过载，提高设备的安全性以及可靠性。

8.9.2 规格

无。

8.9.3 原理描述

系统中上报到 CPU 的各种流量必须设定合理的优先级，这些流量包括：内部管理报文、网络拓扑管理报文、业务报文（包括语音和宽带业务）等。优先级的规划，是提供差异控制的基础。其中控制面业务报文的优先级与转发面的相同，由运营商统一规划，包括用户侧上行的流量和网络侧下行的流量。所以对于控制面，只要能区分对待内部管理报文与其它流量，在 CPU 占有率超过一定门限时，限制低优先级的业务流量，就能保证系统的稳定性。

系统中可能的流量类型如下：

- 内部管理报文，包括板间握手、高层协议、加载报文。
- MSTP、LACP 等链路层网络管理协议报文。
- 路由、BFD、ETH OAM 等协议报文。
- SNMP、ANCP、TELNET、NTP 报文。
- VoIP、IPTV、专线业务报文。

业务流量的优先级依赖运营商的规划，内部管理报文默认始终为最高优先级 7，其他报文优先级采用与队列的映射，为了灵活满足不同用户的需要，支持按协议设置优先级，系统默认按流配置优先级。

为了实现对各类优先级流量的区别对待，系统过载控制特性必须实现多优先级队列管理功能，其中队列调度机制主要是依据 WRR 算法和漏桶算法实现。

WRR 算法原理

在 RR（Round Robin）的基础上为每个队列赋予了一个权值（队列的权值总和为 100），同时为每个队列维护一个计数器。在每次轮循时，计数器为非零的队列可以允许发送一个消息。计数器的计算方法为：初值为权值，每发送一个消息就减一，如果队列没有得到调度也减一，当所有队列的计数器为零时，则都重置为权值。WRR 算法能提供很好的公平性，且同时以较为平滑的方式调度输出业务。

漏桶算法原理

设计一个具有漏桶特性的缓冲器，如果用一个底部开有小孔的桶接水，那么不论向里倒水的速度是否变化，水从孔中流出的速度都是恒定的，只有桶空了，水的流出速率才变为零。如果不顾桶的大小，以太高的速度向里倒水，水就会从上沿溢出。这样的原理可用于对于进入系统的突发业务量的突发性进行调节，即可对违约的高突发业务量进行丢弃或标识。

实现上，漏桶可被设计为一个计数器，每当收到一个报文时计数值加 1，同时计数值与阈值 N 之间的差值按一个适当的速率 a 减少。在计数值达到设定的阈值 N 时到达的报文将被丢弃或被标识。

漏桶的两个控制参数是漏出速率 a 和缓冲区容量 N，当前漏率 a 是根据 CPU 占用率动态可调的。当 CPU 占有率高于设定的目标值时，开始调低漏率 a，这样报文到达的速度被快速的抑制。CPU 占有率没有达到目标值时，调高漏率 a，容量 N 保持不变。

业务过载处理

系统在实现 WRR 调度的同时，也根据系统漏桶过载状态判断是否从当前队列读取报文。考虑实现的合理性，上报到 CPU 的流量对于管理报文队列和 VoIP 报文采用 PQ 调度；对于语音队列根据 CPU 占有率动态分配系统漏率，采用单独的漏桶进行控制；其余队列采用 WRR 调度。

8.10 1:1 VMAC

VMAC 是指虚拟 MAC，1:1 VMAC 是指设备用唯一的虚拟 MAC 来替换单个用户的 MAC，用户 MAC 与设备 VMAC 的对应关系是 1:1。

8.10.1 介绍

定义

VMAC（Virtual MAC）即虚拟 MAC 地址，由 MA5620/MA5626 采用虚拟 MAC 地址代替终端用户源 MAC 地址。1:1 VMAC 是指对每个用户 MAC 地址，MA5620/MA5626 都替换一个唯一的虚拟 MAC 地址。

目的

典型的二层转发模型中以 MAC 地址标识一台设备，然而，因为这些设备并非都直接由操作员进行控制，它们的 MAC 地址不可信。已经出现了一些相关网络设备用于控制 MAC 地址冲突的问题，但是，这仅仅只能解决部分问题：

- MAC 地址唯一性只能在网元级别进行保证，而不能贯穿于整个网络。
- 网元可以检测出冲突的 MAC 地址，但是不能区分合法用户和恶意用户。

VMAC 提供了一个完善的解决方案，用操作员定义的 MAC 地址（可控的 MAC 地址）替换设备的 MAC 地址。启用 VMAC 功能使二层转发模型从以下两个方面有所提升：

- 安全性：

  用操作员定义的 MAC 地址替换设备的 MAC 地址，确保了整个网络 MAC 地址的唯一性。自然避免了 MAC 地址冲突带来的相关问题。
- 可量测性：

通过保证整个网络 MAC 地址的唯一性，操作员可以选择使用相同的 VLAN 来将多个 DSLAM 与边缘路由器进行连接。因此，操作员可以扩大共享相同子网的设备数量，从而提高 IP 地址池的分配效率。

受益

运营商受益

- 提高安全性。通过运营商设备分配的可信的虚拟 MAC 来替换终端用户源 MAC 地址，阻止用户的不可信任 MAC 进入运营商网络，以达到防止 MAC 地址欺骗的目的。
- 标识用户。虚拟 MAC 地址的编码可以包含用户地址或其它信息（比如框号/槽位号/端口号），在运营商网络中根据该 MAC 地址可以直接定位到用户。

用户受益

避免 MAC 地址冲突和恶意用户的 MAC 欺骗攻击。

8.10.2 规格

本特性的相关规格如下：

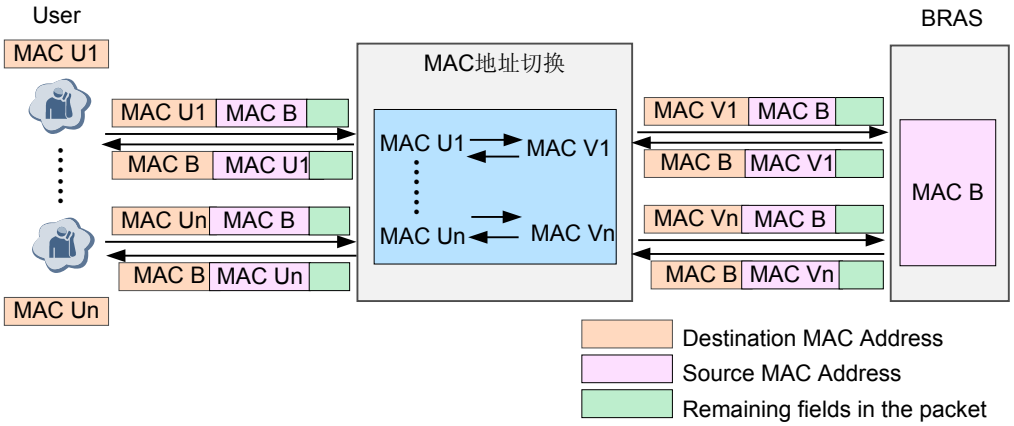
- 每端口支持 VMAC 最大数为 8 个。
- 支持 VMAC 的全局使能开关。
- 支持基于 VLAN 使能 VMAC 特性。

8.10.3 原理描述

PPPoE/IPoE 支持的 1:1 VMAC 原理

用户 MAC 除存在于 MAC 头中的源 MAC 地址外，还存在于数据域中。MA5620/MA5626 对其以太网首部中的以太网源地址和数据域中的以太网源地址均进行替换。

图 8-1 PPPoE/IPoE 支持的 1:1 VMAC 处理流程图



PPPoE/IPoE 支持的 1:1 VMAC 具体流程如图 8-1 所示，其转换的具体处理流程为：

- 上行方向：
  - 当 MA5620/MA5626 收到一个新的用户 MAC(MAC U1)，就添加 1 个新用户 MAC 和 VMAC 的对应表项，MAC U1 对应 MAC V1；当 MA5620/MA5626 收

到的用户 MAC 已分配 VMAC，则仅改写老化标志，使用系统分配的 VMAC；如果此用户 MAC 没分配 VMAC，且 VMAC 表项已满，则学习不成功，丢弃此报文。

- 用户已经分配到 VMAC(MAC V1)，报文中以太头中的源 MAC 地址(MAC U1)替换成系统自动分配的 VMAC 地址。
- VMAC 的替换原则同样应用于控制层协议（ARP、DHCP、ETHOAM），这些协议报文净荷里的 UMAC(MAC U1)也需要替换为 VMAC(MAC V1)。

- 下行方向：
  - 以太网报文中的目的 MAC 为 VMAC（MAC V1），通过 VLAN+VMAC 进行 ARL 表查询，得到出端口信息后，最后查询 VMAC 表，将 VMAC 替换成 UMAC（MAC U1）。
  - VMAC 的替换原则同样应用于控制层协议（ARP、DHCP、ETHOAM），这些协议报文净荷里的 VMAC(MAC V1)也需要替换为 UMAC(MAC U1)。

对于不使用的 VMAC，根据 MAC 地址老化机制进行释放。

1:1 VMAC 地址老化机制

1:1 VMAC 地址老化机制有两种，可以通过命令行配置进行选择：

- 基于 ARL 表的 MAC 地址老化机制：

  根据配置的 MAC 地址老化时间，系统定时检查老化的动态 MAC 地址，如果在老化时间的 1 ～ 2 倍时长范围内没有发送或接收到任何携带该 VMAC 地址的报文，对应的 VMAC 地址就会自动释放，可以分配给其它用户。

- 基于 DHCP 的老化机制：

  如果 DHCP 服务器收到客户端发送的 IP 地址释放请求，在租期内没有收到 DHCP 客户端的续租请求，则会释放 IP 地址，对应的用户 MAC 地址和 VMAC 地址才会相应老化；否则对应的用户 MAC 和 VMAC 都不会老化。

8.11 术语与缩略语

缩略语

缩略语	全称
ACL	Access Control List（访问控制列表）
DoS	Denial of Service（拒绝服务）
ICMP	Internet Control Message Protocol（Internet 控制消息协议）
MAC	Media Access Control（媒体访问控制子层协议）
SSH	The Secure Shell（安全外壳）
SNMP	Simple Network Management Protocol（简单网络管理协议）

9 操作维护安全

关于本章

首先从概述、总体规格、可获得性等方面对操作维护安全特性进行介绍，然后分别阐述各子特性。

9.1 介绍

9.2 参考标准和协议

9.3 可获得性

9.4 管理系统用户帐号/口令
首先介绍管理用户账号/口令子特性，然后对其原理进行阐述。

9.5 远程连接安全
首先介绍远程连接安全子特性，然后对其原理进行阐述。

9.6 独立安全管理员
首先介绍独立安全管理员子特性，然后对其原理进行阐述。

9.7 文件传输加密策略
首先介绍文件传输加密策略子特性，然后对其原理进行阐述。

9.8 远程管理连接加密
首先介绍远程管理连接加密子特性，然后对其原理进行阐述。

9.9 安全事件日志
首先介绍安全事件日志加密子特性，然后对其原理进行阐述。

9.10 SNMP 管理
首先介绍 SNMP 协议子特性，然后对其原理进行阐述。

9.11 术语与缩略语

9.1 介绍

设备操作维护安全主要包含了管理用户账号/口令、远程连接安全、独立安全管理员、文件传输加密策略、远程管理连接加密、安全事件日志以及 SNMP 协议。

特性名称	特性简介
管理用户账号/口令	针对设备管理用户名和密码安全采用的加密以及防攻击等安全措施。
远程连接安全	对用户登录设备连接的进行一系列防火墙功能以及设备服务端口的关闭功能。
独立安全管理员	针对系统管理员与安全管理员权限分离，只有安全管理员才能进行设备安全相关的功能的配置。
文件传输加密策略	针对设备和外部服务器之间的文件传送采用 SSH 进行加密的传输方式。
远程管理连接加密	终端连接到设备上进行操作维护管理时，设备与终端的报文采用 SSH 加密的方式。
安全事件日志	针对对系统安全相关的事件进行记录。
SNMP 协议	网管与设备间交互采用的 SNMP 协议标准。

9.2 参考标准和协议

远程管理连接加密

- RFC4254：The Secure Shell (SSH) Connection Protocol
- RFC4253：The Secure Shell (SSH) Transport Layer Protocol
- RFC4252：The Secure Shell (SSH) Authentication Protocol
- RFC4251：The Secure Shell (SSH) Protocol Architecture

SNMP 协议

本特性的参考协议清单如下：

1. SNMPv1
   - RFC1157：Simple Network Management Protocol (SNMP)
2. SNMPv2c
   - RFC1905：Protocol Operations for Version 2 of the Simple Network Management Protocol (SNMPv2)
3. SNMPv3
   - RFC2570：Introduction to Version 3 of the Internet-standard Network Management Framework (Status=3DINFORMATIONAL)

- RFC2571：An Architecture for Describing SNMP Management Frameworks
- RFC2572：Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)
- RFC2573 ：SNMP Applications
- RFC2574：User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)
- RFC2575 ：View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)

9.3 可获得性

涉及网元

设备操作维护安全主要是针对设备本身的安全管理，不涉及其他网元。

特性依赖

- 修改密码时，密码要求遵守当前系统的要求。
- 系统管理员不可以进行安全管理员的合并操作。
- 注册安全命令的增量接口中，用户模板不允许为“security”。
- 隐藏命令的增量接口，用户模式名不允许为“security”。

9.4 管理系统用户帐号/口令

首先介绍管理用户账号/口令子特性，然后对其原理进行阐述。

9.4.1 介绍

定义

账号/口令管理是指用户通过 CLI 接口（Command Line Interface，命令行接口）接入到设备时所采用的用户身份验证措施。

目的

用户通过 CLI 接口接入到设备时，设备通过用户名及口令的匹配认证，来保证设备管理和维护的安全。

9.4.2 规格

该特性的相关规格如下：

- 支持安全管理员与系统管理员分离与统一。

- 支持用户绑定用户模板，用户模版可以配置用户名和密码的有效期，用户可登录的时间段。
- 用户的权限分为四个级别：超级用户级、管理者级、操作员级和普通用户级。
- 用户名和密码最小长度限制：普通用户支持 6 ～ 15 个字符串，root 和 security 用户支持 8 ～ 15 个字符串。
- 密码复杂度限制：密码中至少有一个字符和一个数字。
- 支持用户长时间闲置时自动锁定用户名；闲置时间的长短由用户配置。
- 支持用户名和密码的有效时间由用户配置。
- 用户名过期会被删除，密码过期后需重新设置。
- 支持同一用户名连续登录失败 N 次，锁定该用户名的登录。N 是用户可配置的限制次数，默认值为 3 次。
- 同一 IP 地址连续登录失败 N 次，会锁定该 IP 的用户登录，N 是用户可配的限制次数，默认为 3 次。

9.4.3 原理描述

实现原理

通过 CLI 接口登录系统时，用户必须输入用户名及口令进行匹配认证。通过这种匹配对用户身份进行验证，从而保障系统维护的安全。

9.5 远程连接安全

首先介绍远程连接安全子特性，然后对其原理进行阐述。

9.5.1 介绍

定义

远程连接安全是指通过 IP 防火墙或者关闭系统的相关服务端口，来防止非法用户对设备进行攻击或者防止非法操作。

目的

通过 IP 防火墙或者关闭服务端口，防止非法用户的攻击，保证设备的运行安全。

9.5.2 规格

该特性的相关规格如下：

- IP 防火墙支持配置 Telnet/SSH/SNMP3 种协议允许接入设备的 IP 地址范围，3 种协议各可以配置 10 个 IP 地址范围段。

- IP 防火墙支持配置 Telnet/SSH/SNMP3 种协议拒绝接入设备的 IP 地址范围，3 种协议各可以配置 10 个 IP 地址范围段。
- 支持关闭系统默认打开的服务端口（dBWin/Telnet//NTP/RADIUStrace/Telnet proxy/msg-emulate）。
- 支持配置系统远程命令行登录会话的数目（包含 Telnet/SSH/本地串口），配置的范围为 1 ～ 9。默认值为 9。

9.5.3 原理描述

实现原理

IP 防火墙功能是通过限制合法的 IP 地址范围以及访问协议的允许登录访问设备，或者通过限定不符合地址范围以及访问协议要求的操作用户将被拒绝访问设备。

系统服务关闭是通过关闭系统的默认的服务的监听端口，防止恶意对端口进行扫描或者攻击。

9.6 独立安全管理员

首先介绍独立安全管理员子特性，然后对其原理进行阐述。

9.6.1 介绍

定义

独立安全管理员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。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，此时系统管理员只有安全查询权限，没有安全设置权限。

合并是指把分开了的操作权限合并，由系统管理员执行。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。

9.6.2 规格

该特性的相关规格如下：

- 支持通过命令行分离安全模式。
- 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。
- 支持安全模式的 MIB（设置、查询）。
- 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。
- 用户登录时，提示该用户上次登录的时间等信息。
- 支持 root 用户或者安全管理员登录时，显示最近的多个登录错误的记录。
- 安全管理员登录时，系统提示安全信息。

9.6.3 原理描述

实现原理

1. 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。
2. 安全模式分离时，会执行两个操作。
   - 生成一个安全管理员用户。
   - 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。
3. 安全模式合并时，则会执行三个操作。
   - 解隐藏非安全模板下的安全配置命令。
   - 从用户表中删除安全管理员。
   - 该用户下线。

   说明：

   网管进行合并操作时不允许安全管理员在线，所以不需要上面第三步的操作。

   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。

9.7 文件传输加密策略

首先介绍文件传输加密策略子特性，然后对其原理进行阐述。

9.7.1 介绍

定义

文件传输加密策略是指使用 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。使用 SSH 协议加强了 SFTP 的安全性，从而提高文件在传输过程中的安全性。

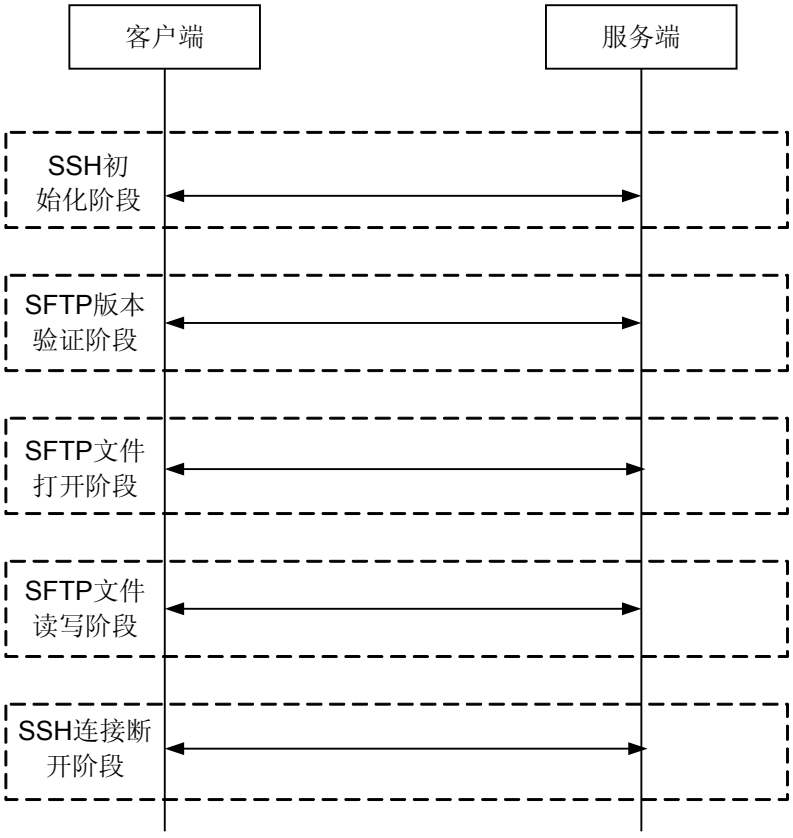
9.7.2 原理描述

实现原理

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 9-1 所示。

图 9-1 SFTP 的文件传输流程



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：

4. 在 SFTP 阶段进行 SFTP 的版本验证。
5. 打开本地和远程文件。
6. 进行相应的读数据操作。
7. 在读数据完成后，关闭打开的文件。

9.8 远程管理连接加密

首先介绍远程管理连接加密子特性，然后对其原理进行阐述。

9.8.1 介绍

定义

远程管理连接加密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。

9.8.2 规格

该特性的相关规格如下：

- 支持 SSH 1.x 协议和 SSH 2.0 协议。
- 用户以 SSH 方式登录时支持 Radius 认证。
- 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。
- SSH 登录支持 AES，DES，3DES，BLOWFISH 四种加密算法。

9.8.3 原理描述

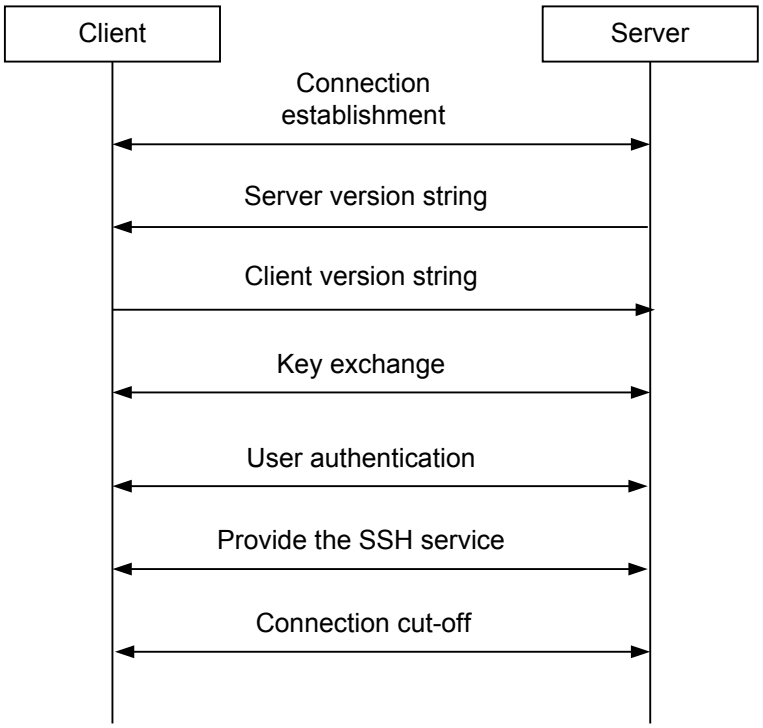
实现原理

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。

SSH 协议在客户端和服务器端的交互流程如图 9-2 所示。

图 9-2 SSH 交互流程



9.9 安全事件日志

首先介绍安全事件日志加密子特性，然后对其原理进行阐述。

9.9.1 介绍

定义

安全事件日志是指对系统安全相关的事件进行记录。目前支持两个安全事件，维护类用户状态改变事件和用户锁定事件。维护类用户状态改变包括用户登录、登出和非法登录。

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特定安全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。

9.9.2 规格

该特性的相关规格如下：

- 系统默认支持三个安全事件。系统支持的运行事件不属于安全事件记录特性的范围。
- 支持查询安全事件列表。
- 支持命令行修改安全事件级别。
- 支持 MIB 查询安全事件和修改安全事件级别。

9.9.3 原理描述

实现原理

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、事件类别、事件级别、事件默认级别等，其中可定制的为事件级别。

对于安全事件，事件级别的变化影响安全事件的记录。只有事件级别高于等于次要时才记录对应的安全日志。

9.10 SNMP 管理

首先介绍 SNMP 协议子特性，然后对其原理进行阐述。

9.10.1 介绍

定义

SNMP（Simple Network Management Protocol）是一种广泛使用的网络管理协议，由 IETF（Internet Engineering Task Force）开发。至今，SNMP 发展经历了 SNMPV1、SNMPV2 以及 SNMPV3。

SNMP 保证管理信息在任意两点间传送，便于网络管理员在网络上的任何节点检索信息、进行修改、寻找故障，并完成故障诊断、容量上报和报告生成。

目的

提供网络设备的一种管理方法。

SNMP 相对简单，被管对象为简单变量，属性少，易于扩展，可自定义 MIB 接口。SNMP 独立于被管理设备，可适用于任何 TCP/IP 网络，以及其它类型网络。

9.10.2 规格

该特性的相关规格如下：

- 支持 SNMP V1、SNMP V2c、SNMP V3 版本 Server 端。
- 支持 MIB 树静态注册。
- 持 SNMP Get 请求处理。
- 支持 SNMP Get Next 请求处理。
- 支持 SNMP Set 请求处理。
- 支持团体名管理、团体名校验。
- 支持基于用户的安全模型（USM）。
- 支持基于视图的访问控制模型（VACM）。
- 支持 Trap 源地址配置。
- 支持 Trap 发送开关控制。
- 支持 System Group 信息配置。
- 支持 SNMP 报文统计。
- 支持动态增加删除 MIB 子树。
- 支持 SNMP 产品规格配置。
- 支持 SNMP MIB 增量开发。
- 如果网管下发 Get Next 报文给某个正在执行命令行操作的模块，系统会返回错误，通知网管数据同步失败。
- SNMP 支持的最大报文大小为 17940byte。
- 支持修改 SNMP V3 用户密钥。
- 支持配置 Trap 目的主机 MIB 接口。配置 SNMP 引擎 ID 通过 sysName 生成。
- SNMP V3 支持 2 种加密算法：AES 和 DES。

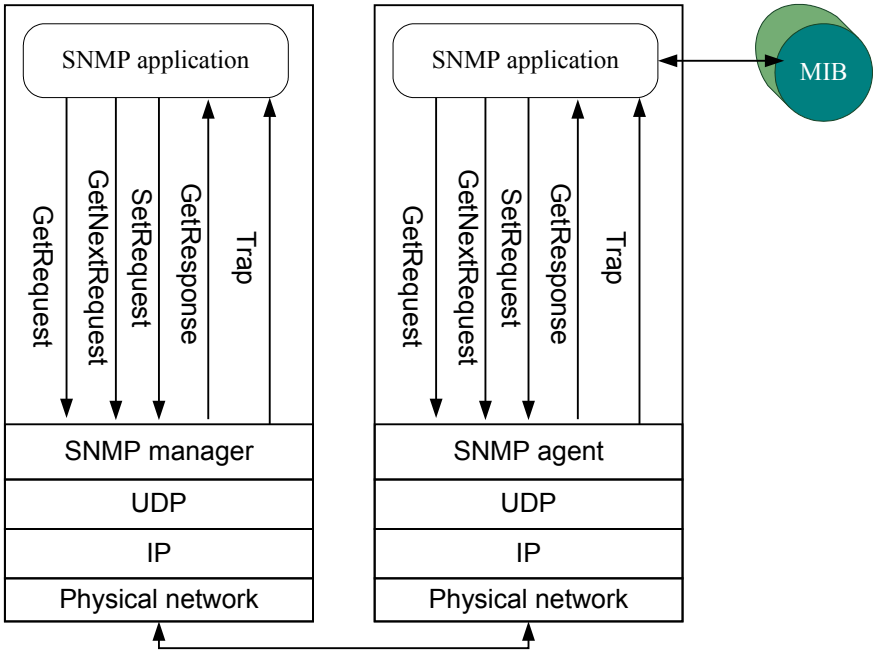
9.10.3 原理描述

实现原理

SNMP 管理模型基于 Client/Server 架构，SNMP 实体又分为 Manager 和 Agent。

SNMP 网络管理框架如图 9-3 所示。

图 9-3 SNMP 网络管理框架



SNMP 属于应用层的协议，承载在 UDP 之上。

1. SNMP 管理信息库（MIB）

   MIB 即 Management Information Base，管理信息库，它是所有被管理对象的抽象集合。管理信息库按树形结构组织，称为 MIB 树。每个被管理对象对应树形结构的一个叶子接点，称为一个 object 或一个 MIB。

   MIB 树是棵静态树，也就是说，MIB 树形结构在设备启动时完成初始化，以后 Manager 只是检索或修改每个被管对象的内容。网管通过读写 MIB 中的被管对象实现对设备的管理。

2. SNMP 报文类型

   Get Request：获取指定对象信息的请求。

   GetNext Request：获取指定对象的下一对象信息的请求。

   Set Request：对指定对象进行配置的请求。

   Get Response：以上三种请求，代理都通过发送 GetResponse 消息回应答。

   Trap：Trap 由 Agent 产生，将被管理设备的异常事件报告给网管。

   当设备出错告警，设备的重要数据被用户/控制台/其他网管改变，代理通过发送 Trap 通知网管。

   当 SNMPManager 接收到 Trap 后，可产生相应的动作，如轮询检测（polling）来诊断故障，采取恢复措施，修改网管的相关数据库。

3. SNMP V3 基于用户的安全模型（USM）

   SNMPV1、V2c 版本缺乏安全机制来保障。SNMP V3 版本支持了基于用户的安全模型（USM），可以避免篡改和伪装攻击。

   USM 安全模型主要负责验证 SNMP 消息在网络传输过程中是否被修改；验证 SNMP 消息是否为其所宣称的用户所发出的；监测过时 SNMP 消息以及提供 SNMP 消息的保密机制。

USM 模型由三个模块组成：

认证模块（authentication module）：数据来源认证。

定时模块（timeliness module）：防止消息延迟或多余应答。

加密模块（privacy module）：防止消息内容泄露。

4. SNMP V3 基于视图的访问控制模型（VACM）

SNMP 引擎的访问控制子系统负责检查对一个特殊对象进行的访问是否被允许。VACM 则是 SNMPV3 下默认的访问控制模型。由以下几部分组成：

- 组 Groups

组是一系列的由零个或多个映射组成。组定义了所有属于该组对于 securityName 的访问权限。

- 安全级别 securityLevel

不同的访问权限由不同的安全级别来定义。

- 背景环境（上下文）Contexts

SNMP 背景环境是一系列受 SNMP 实体访问的管理信息。

- MIB 视图和视图族 MIB Views and View Families

对于一个给定的背景环境下只对应一个可供访问的 MIB 视图。

视图子树（View Subtree）：一系列的具有共同 ASN.1 OBJECT IDENTIFIER 前缀的 MIB 对象实例。

- 访问策略 Access Policy

读视图（read-view）。

写视图（write-view）。

通告视图（notify-view）。

9.11 术语与缩略语

术语

术语	解释
USM	在 SNMP 协议中，定义了一种 USM（User-based Security Model，基于用户的安全模型）模型来实现安全子系统。USM 在 消息级别上操作，使用 DES 的 CBC 加密，使用 HMAC 来鉴别，并且包含及时性功能来仿真延时和 重播攻击。另外，USM 还包含密钥管理能力，并提供了密钥本地化和密钥更新功能。

缩略语

缩略语	全称
AES	Advanced Encryption Standard（高级加密标准）
CLI	Command Line Interface（命令行接口）

缩略语	全称
DES	Data Encryption Standard（数据加密标准）
MIB	Management Information Base（管理信息库）
SSH	The Secure Shell（安全外壳）
SNMP	Simple Network Management Protocol（简单网络管理协议）

10 OAM

关于本章

O&M 特性即操作与维护特性，是属于设备运维管理的范畴，对设备日常的正常运作、设备网络拓扑管理、故障定位和设备升级维护起着举足轻重的作用。本章将对其子特性加以介绍。

10.1 介绍

操作与维护特性属于设备运维管理的范畴，对设备日常的正常运作、设备网络拓扑管理、故障定位和设备升级维护起着举足轻重的作用。

本章针对 MA5620/MA5626 的操作与维护特性从定义、目的、规格、原理描述、参考资料方面，详细介绍了设备对各子特性的支持能力，帮助读者全面深层次的了解设备的操作与维护的特性。

操作与维护的特性主要包括远程操作与用户管理、版本与数据管理、设备异常管理。

10.2 参考标准和协议

本特性的参考资料清单如下：

- ITUT.G.984.3 Gigabit-capable Passive Optical Networks (G PON): Transmission convergence layer specification
- IEEE 802.3ah：Carrier Sense Multiple Access withCollision Detection (CSMA/CD) access method and physical layer specifications
- 中国电信 EPON 设计技术要求（V2.1）
- IETF RFC0854 Telnet Protocol Specification
- IETF RFC0793 Transmission Control Protocol
- ITU-T X.733
- ITU-T G.984.3
- IEEE 802.3ah
- WT-147 Draft Version 1.2----Layer2 Control Mechanism for Broadband Multi-Service Architecture，29 May 2006，DSL Forum
- RFC 3292----General Switch Management Protocol （GSMP）V3，June 2002
- draft-ietf-ancp-framework-11
- draft-ietf-ancp-protocol-06
- TR101：Technical Report DSL Forum TR-101 Migration to Ethernet-Based DSL Aggregation April 2006
- RFC2516：A Method for Transmitting PPP Over Ethernet（PPPoE）

10.3 可获得性

涉及网元

GPON 认证特性需要 OLT 和 ONU 的配合才能完成。OLT 和 ONU 需要兼容 G.984 标准。

EPON 认证特性需要 OLT 和 ONU 的配合才能完成。

- MAC 地址认证需要 OLT 和 ONU 兼容 IEEE 802.3ah。
- 逻辑标识认证需要 OLT 和 ONU 兼容中国电信 EPON 设技术要求（V2.1）。
- Password 认证需要 OLT 和 ONU 兼容华为私有 OAM 协议。

版本支持

表 10-1 O&M 特性的版本支持

产品	支持版本
MA5620/MA5626	V800R308

硬件要求

支持 GPON 认证特性，涉及的 OLT 侧单板：SCUx 和 GPBx。涉及的 ONU 侧设备：ONU 系列的任何 GPON 上行扣板或单板。

支持 EPON 认证特性，涉及的 OLT 侧单板：SCUx 和 EPBx。涉及的 ONU 侧设备：ONU 系列的任何 EPON 上行扣板或单板。

10.4 GPON 认证

GPON 认证是指 OLT 基于 ONU 的 SN 或 password 对 ONU 合法性进行认证，拒绝非法 ONU 的接入。

10.4.1 介绍

定义

GPON 认证是指 OLT 基于 ONU 的 SN 或 password 对 ONU 合法性进行认证，拒绝非法 ONU 的接入。

目的

在 GPON 系统中，只有通过认证的合法 ONU 才能接入 GPON 系统，这样可以满足运营商实现灵活的、便于维护的管理方式。

受益

运营商受益

- SN 认证和 password 认证可以防止非法 ONU 随意接入 GPON 系统。如果出现非法或重复的 SN 认证和 password 认证，系统会上报告警。
- password 认证可以方便用户更换 ONU 设备，只需要在 ONU 设置原有 password，而不需要修改 OLT 及网管侧的配置，就可以上线配置恢复正常工作，简化设备更换流程。

10.4.2 规格

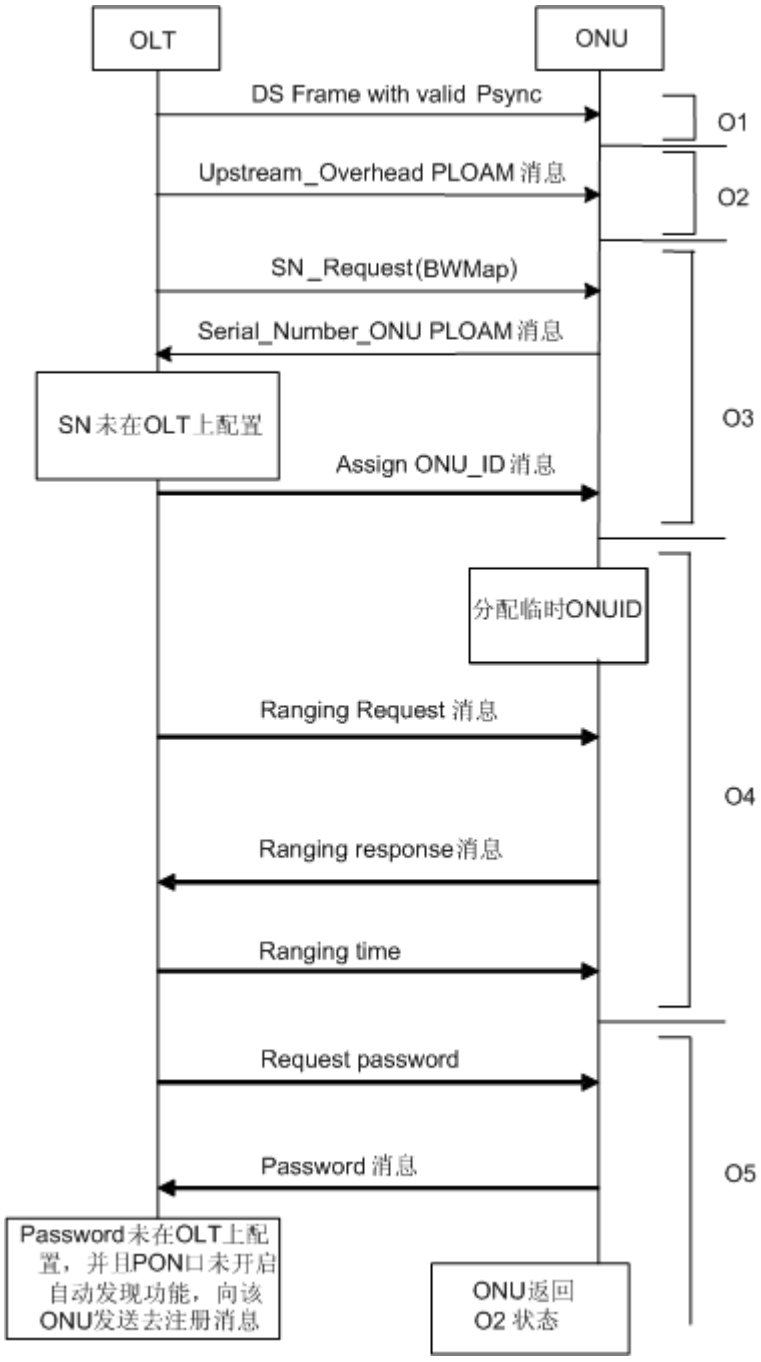
GPON ONU 的认证方式支持三种：

- SN 认证
- SN+password 认证
- password 认证

10.4.3 原理描述

GPON ONU 的认证方式包括：SN 认证、SN ＋ Password 认证和 Password 认证。ONU 认证上线后就可以传输数据了，ONU 对下行数据是根据 gemport 进行选择接收的。各个 ONU 监测接收到的数据帧的 gemport，以决定是否接收该帧，如果该帧所包含的 gemport 与 ONU 自身的 gemport 相同或者为 gemport（默认为 4095，支持修改，设置范围为 4000 ～ 4095），则接收该数据帧；否则作丢弃处理。ONU 的认证部分主要是针对 OLT 上已经预配置的 ONU 而言，对于在 OLT 上未预配置 ONU 的处理参照图 10-1。

图 10-1 图 1 未预配置 ONU 注册流程图



- SN 和 SN ＋ Password 认证

  首先 ONU 在 OLT 上预配置为 SN 认证或者 SN ＋ Password 认证，在 PON 口下接入该 ONU，该 ONU 注册上线过程与未预配置 ONU 的注册流程差异体现在：

  - OLT 收到 ONU 的序列码回应消息后，如果发现该 ONU 已经配置，则判断 OLT 上是否有相同 SN 的 ONU 在线，如果有相同 SN 的 ONU 在线，则向主机命令行和网管上报 SN 冲突告警；否则，直接分配用户指定的 ONUID 给该 ONU。
  - ONU 进入操作状态后，对于 SN 认证方式的 ONU，OLT 不进行 Password 请求，直接为该 ONU 配置用于承载 OMCI 消息的 gemport（目前我司的做法是，

承载 OMCI 的 gemport 与 ONUID 相同，由 OLT 自动配置）后让 ONU 上线，并向主机命令行或者网管上报 ONU 上线告警。对于 SN ＋ Password 认证的 ONU，OLT会向 ONU 进行 Password 请求，并将 ONU 回应的 Password 与本地配置的 Password 进行比较，如果 Password 与本地配置相同，则判断 OLT 上是否有相同 SN ＋ Password 认证的 ONU 在线，如果有相同 SN ＋ Password 认证的 ONU 在线，则向主机命令行或者网管上报 Password 冲突告警，否则直接为 ONU 配置用于承载 OMCI 消息的 gemprot 后让 ONU 上线，并向主机命令行或者网管上报 ONU 上线告警；如果 Password 与本地配置不同，即使 PON 口开启了 ONU 自动发现功能，也不会上报 ONU 自动发现，OLT 发送 Deactivate_ONU-ID PLOAM 消息去注册该 ONU。

- Password 认证

  Password 认证有两种模式，Always-on 和 Once-on。首先预添加 Password 认证方式的 ONU，然后在 PON 口下接入该 ONU，Password 认证之前的处理与未预配置 ONU 的注册流程相同。

  - 选择 Once-on 模式时，可以选择设置使用 aging-time，范围为 1 ～ 168h，设置为 aging-time 时，ONU 必须在设定的时间范围内注册上线，否则一旦 ONU 的实际注册上线时间超过了设置的时间，就不允许该 ONU 注册上线。选择 Always-on 模式，任何时间都可以接入 ONU 进行注册上线。

    Once-on 认证方式下要求 ONU 在规定的时间内认证，超出该时间就不允许认证，并且一旦 ONU 认证成功后就不允许再修改 SN，也就是说，对于 Once-on 认证模式，只有首次认证是基于 Password 认证的，非首次认证时，使用的是 SN ＋ Password 认证。Once-on 的应用场景是运营商为用户分配 Password 账号后，要求用户在规定时间上线，并且上线后就不允许再更换 ONU，如果有更换 ONU 的需求，需要通知运营商进行处理。

  - Always-on 认证方式下，对用户接入上线时间无限制，首次上线时使用 Password 认证，认证上线成功后 OLT 根据用户的 SN 和 Password，生成 SN ＋ Password 绑定表项。非首次上线时，如果 ONU 的 SN 和 Password 与首次上线成功 ONU 的 SN 以及 Password 相同，则使用 SN ＋ Password 认证；如果用户更换相同 Password，不同 SN 的 ONU，则根据 Password 进行认证，认证上线成功后，更新 SN ＋ Password 的绑定表项。因此对于 Always-on 认证模式，无论什么时候接入 ONU，只要 ONU 的 Password 正确都可以上线。应用场景为，运营商为用户分配 Password 后，用户可以随意更换使用相同 Password，不同 SN 的 ONU，在更换 ONU 后不需要通知运营商。

  ONU 进行 Password 认证时，如果 GPON 单板软件发现该 ONU 的 SN 或者 Password 与 OLT 上已在线 ONU 冲突，则将该 ONU 进行去注册处理，并向主机命令行和网管上报 SN 冲突或者 Password 冲突，但不会对在线 ONU 造成任何影响；对于 Password 认证失败的处理参照未预配置 ONU 的注册处理流程，在此不再进行重复阐述。

  对于 Once-on 模式认证的 ONU，在 GPON 单板配置恢复完成后，单板软件启动注册超时定时器，在 ONU 注册超时时间到达之前，如果 GPON 单板复位了，ONU 注册超时时间清零，重新开始计算。在 ONU 注册时间超时或者 ONU 首次注册成功之前，ONU 的发现状态为 ON，只有当 ONU 的发现状态为 ON 时才允许 ONU 注册上线。在 ONU 注册时间超时或者首次注册成功后，OLT 会将 ONU 的发现状态设置为 OFF。对于注册时间超时的 ONU，不允许该 ONU 注册上线，需要在局端清除掉该 ONU 的注册时间超时标志后才能上线；对于首次注册成功后的 ONU，允许该 ONU 再次注册上线。ONU 的注册时间超时后，单板会向主机命令行和网管上报告警，ONU 的发现状态设置支持系统主备倒换和配置恢复。

10.5 EPON 认证

EPON 认证是指 OLT 基于 ONU 的 MAC 地址或逻辑标识或 password 对 ONU 合法性进行认证，拒绝非法 ONU 的接入。

10.5.1 介绍

定义

EPON 认证是指 OLT 基于 ONU 的 MAC 地址或逻辑标识或 password 对 ONU 合法性进行认证，拒绝非法 ONU 的接入。

目的

在 EPON 系统中，只有通过认证的合法 ONU 才能接入 EPON 系统，这样可以满足运营商实现灵活的、便于维护的管理方式。

受益

运营商受益

- MAC 地址认证、逻辑标识认证和 password 认证可以防止非法 ONU 随意接入 PON 系统。
- 逻辑标识认证和 password 认证可以方便用户更换 ONU 设备，只需要在 ONU 设置原有 password，而不需要修改 OLT 及网管侧的配置，就可以上线配置恢复正常工作,简化设备更换流程。

10.5.2 规格

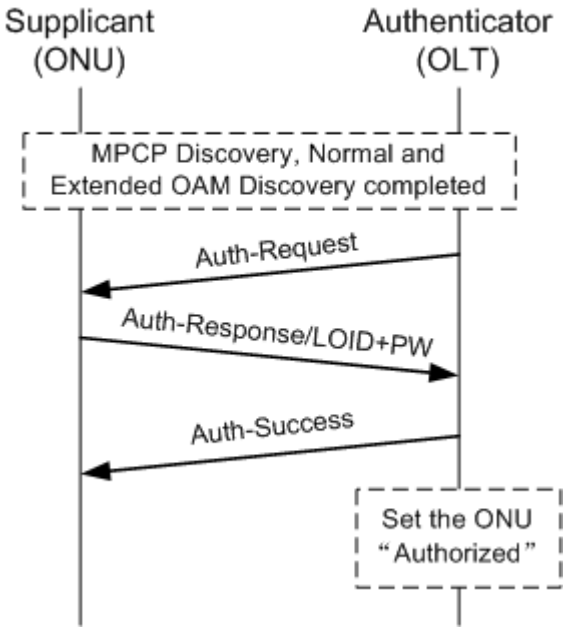
EPON 认证方式支持三种：MAC 地址认证、逻辑标识认证、password 认证。

- MAC 认证符合 CTC EPON 标准要求，认证 MAC 为 ONU 的 MAC 地址，长度为 6 个字节。
- 逻辑标识认证符合 CTC EPON 2.1 标准要求：LOID+password，LOID 的长度为 24 字节，password 的长度为 12 字节。
- password 认证是华为私有 OAM 协议支持的认证方式，password 长度为 32 字节。

10.5.3 原理描述

EPON ONU 的认证方式包括：MAC 地址认证、逻辑标识认证和 Password 认证。ONU 在完成 MPCP 注册后，开始 MAC 地址认证、逻辑标识认证或者 Password 认证，整个认证过程由单板和终端配合完成的。**图 10-2** 是基于逻辑标识的 ONU 认证的流程。

图 10-2 基于逻辑标识的 ONU 认证的流程（认证成功）



- MAC 地址认证

  对于 MAC 地址认证，如果主机发现新发现 ONU 的 MAC 地址与 OLT 上已经在线 ONU 的 MAC 地址相同，则上报 MAC 地址冲突告警，并将该 ONU 进行去注册处理，对在线 ONU 不会造成任何影响；如果 EPON 单板软件发现新注册 ONU 的 MAC 地址没有配置，则判断 PON 口是否已经开启 ONU 自动发现功能，如果自动发现已经开启，则向 OLT 上报 ONU 自动发现，否则将该 ONU 进行去注册处理。

- 逻辑标识认证和 Password 认证

  逻辑标识认证和 Password 认证的过程完全一样，下面以 Password 认证为例进行描述。

  - 选择 Once-on 模式时，可以选择设置使用 aging-time 或者 no-aging。使用 aging-time 时，必须设置 Password 的超时时间，设置范围为 1 ～ 168h，设置为 aging-time 时，ONU 必须在设定的时间范围内注册上线，否则一旦 ONU 的实际注册上线时间超过了设置的时间，就不允许该 ONU 注册上线；使用 no-aging 时，Password 永不超时，用户可以在任意时刻首次接入该 ONU 注册上线。选择 Always-on 模式时，用户可以在任意时刻接入 ONU 进行注册上线。

    Once-on 认证方式下要求 ONU 在规定的时间内认证，超出该时间就不允许认证，并且一旦 ONU 认证成功后就不允许再修改 MAC，也就是说，对于 Once-on 认证模式，只有首次认证是基于 Password 认证的，非首次认证时，使用的是 MAC ＋ Password 认证。Once-on 的应用场景是运营商为用户分配 Password 账号后，要求用户在规定时间上线，并且上线后就不允许再更换 ONU，如果有更换 ONU 的需求，需要通知运营商处理。

  - Always-on 认证方式下，无论用户是首次注册认证，还是非首次注册认证，都是使用 Password 进行认证。也就是说无论什么时候，用户使用相同 Password，不同 MAC 的终端都可以上线。应用场景为，运营商为用户分配 Password 后，用户可以随意更换使用相同 Password，不同 MAC 的 ONU，在更换 ONU 后就不需要通知运营商。

  ONU 进行 Password 认证时，如果主机发现该 ONU 的 MAC 地址与 OLT 上已在线 ONU 相同上报 MAC 冲突，但不会对在线 ONU 造成任何影响，并将该 ONU 进行

去注册处理；如果主机发现该 ONU 的 Password 与相同 PON 口下已在线 ONU 相同，OLT 上报 ONU 自动发现信息；对于 Password 认证失败的 ONU，OLT 下发去注册消息进行去注册处理；如果单板软件基于注册 ONU 的 Password 查表失败，则判断 PON 口是否开启自动发现功能，如果 PON 口开启了自动发现，则上报 ONU 自动发现告警，否则去注册该 ONU。

对于 Once-on 模式认证的 ONU，在 EPON 单板配置恢复完成后，单板软件启动注册超时定时器，在 ONU 注册超时时间到达之前，如果 XPON 单板复位了，ONU 注册超时时间清零，重新开始计算。在 ONU 注册时间超时或者 ONU 首次注册成功之前，ONU 的发现状态为 ON，只有当 ONU 的发现状态为 ON 时才允许 ONU 注册上线。在 ONU 注册时间超时或者首次注册成功后，OLT 会将 ONU 的发现状态设置为 OFF。对于注册时间超时的 ONU，不允许该 ONU 注册上线，需要在局端清除掉该 ONU 的注册超时标志后才能上线；对于首次注册成功后的 ONU，允许该 ONU 再次注册上线。ONU 的注册时间超时后，单板会向主机命令行和网管上报告警，ONU 的发现状态设置支持主备倒换和配置恢复。

10.6 POE

从概念、规格、可获得性和原理描述方面对 PoE 特性进行介绍。

10.6.1 介绍

定义

PoE 全称为 Power Over Ethernet，是指通过 10BASE-T、100BASE-TX、或 1000BASE-T 以太网网络供电，其可靠供电的距离最长可达 100 米。

目的

通过 PoE 特性，可以有效的解决远程终端（IP 电话、无线 AP、便携设备充电器、刷卡机、摄像头、数据采集设备等）的集中式电源供电问题。这些终端不再需要考虑取电的问题，在接入网络的同时就可以实现对设备的集中供电和集中备电。

受益

运营商受益

通过 PoE 特性，对远程终端设备进行供电，可以有效的缓解设备布放的取电问题。

10.6.2 规格

PoE 特性的相关规格如下：

- 支持 PSE 模式下板级供电管理方式配置，可以设置为手动模式和自动模式，默认为自动模式。
- 支持 PSE 模式 PD 设备检测兼容性方式配置功能，默认 PD 设备兼容性检测功能为禁止状态。

- 支持 PSE 模式下设备过温保护配置功能，系统温度超过阈值，关闭所有端口供电功能。
- 支持 PSE 模式下端口最大功率为 30W，默认值为 15.4W。
- 支持端口供电优先级配置功能，提供三种类型的优先级：Critical、High、Low。

10.6.3 原理描述

PoE 的基本原理

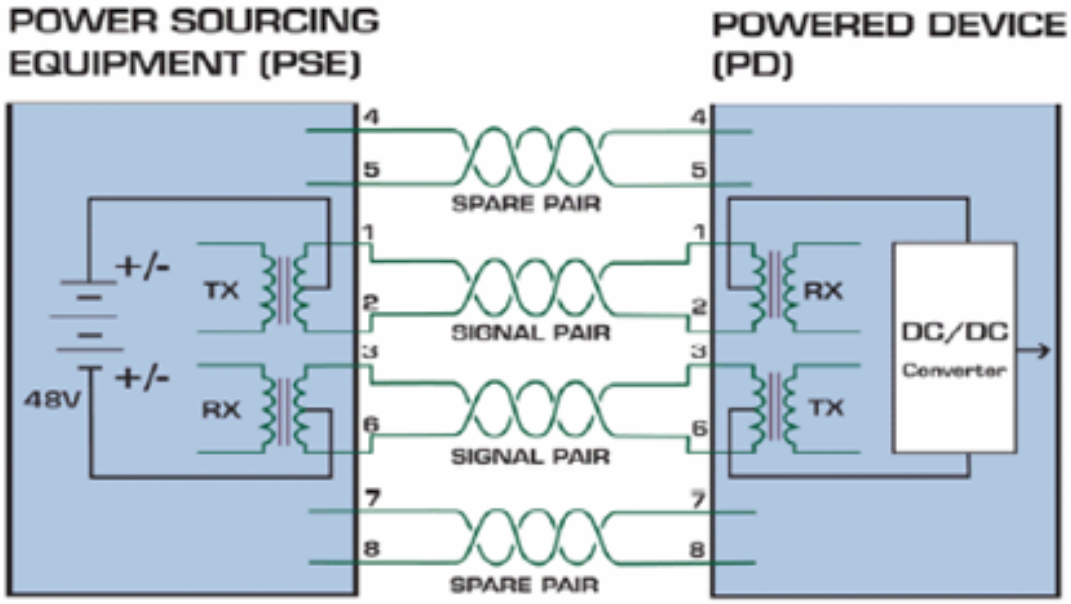
PoE 特性是通过以太网线双绞线完成对网络设备的供电，一般一套 PoE 系统需要两种设备配合完成，即 PSE 设备和 PD 设备。PSE（Power Sourcing Equipment）设备是提供电源的设备，PSE 在通过在业务端口(RJ-45 端口)耦合上 48V 直流电源，直接驱动以太网双绞线。PD（Powered device）设备是通过以太网双绞线上获取电能的受电设备。

MA5626 8 路反向 POE 设备是遵从 IEEE802.3at 标准的 Type1 PD 设备，要求线缆的环路直流电阻小于 40ohm。一般的 5 类网线都可以满足要求，但是不排除非标准线缆直流电阻过大，导致 MA5626 8 路反向 POE 设备的输入电压不满足 IEEE802.3at 标准，设备不能正常工作。

根据 IEEE 802.3af 规定，PSE 设备有两种方式向 PD 设备供电其说明如下：

1.通过数据线对（1/2，3/6）供电，即模式 A（Alternative A），图 10-3 所示：

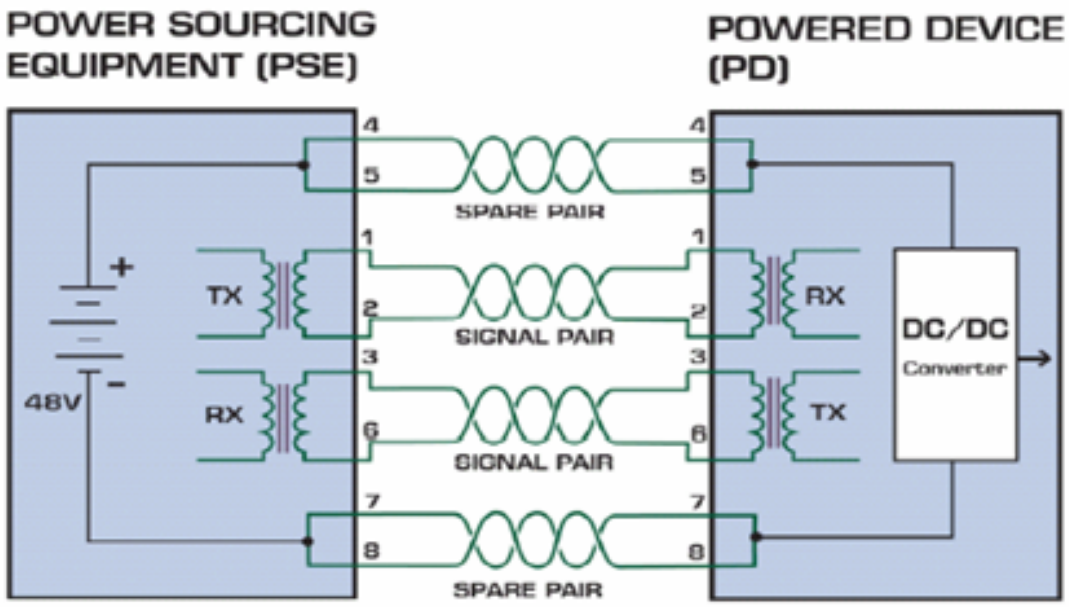
图 10-3 模式 A 供电示意图



PSE 可通过数据线对给 PD 供电。由于 DC 和数据频率互不干扰，所以可以在同一对线同时传输电流和数据。其实，对电缆来说可以看作一种“复用”。可以把 1，2 链接形成正（或负）极，把 3，6 链接形成负（或正）极。

2.通过空闲线对（4/5，7/8）供电，即模式 B（Alternative B），图 10-4 所示：

图 10-4 模式 B 供电示意图



4，5 链接形成正极，7，8 链接形成负极。由 PSE 给 PD 供电。

说明

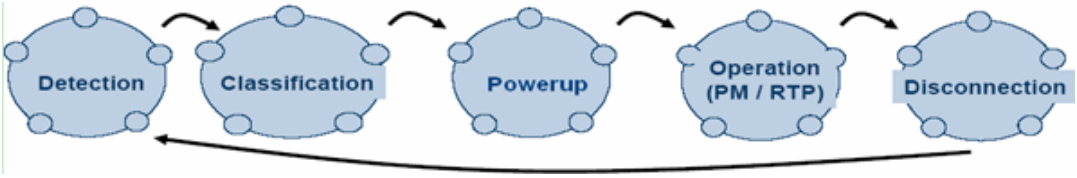
一般来说，标准的 PD 设备必须支持两种受电方式，但 PSE 设备只需支持其中一种，EPWA 单板支持数据线对供电。

PoE 供电流程

以太网供电系统要能与传统的网络系统兼容，要求必须符合 IEEE 802.3af/IEEE 802.3at 标准。标准规定在一定的时间内，供电设备必须完成对终端网络设备的检测和分级，然后决定是否对其供电以及输出多少功率。这一规定可以保障不兼容的网络设备不至于受到 48 电源的破坏，所以供电设备的主要功能是检测是否有兼容的设备（PD）连接入系统或从系统中断开，并对受电设备进行分级，以提供相应功率的电源或切断电源。

PoE 按照 IEEE 802.3af/IEEE 802.3at 标准实现，标准中规定 PSE 设备和 PD 设备对接时，其供电的流程如下图所示：

图 10-5 PoE 供电流程图



供电过程主要包括以下几个步骤：

1. Detection（检测）：PSE 设备检测 PD 设备是否存在。

PSE 通过检测端口的电源输出线对之间的电阻值和电容值来判断 PD 是否存在。此阶段端口输出电压为 2.8V ～ 10V,电压极性与－48V 输出一致。PD 存在的特征：

- 直流阻抗在 19K ～ 26.5Kohm 之间；
- 容值不超过 150nF。

只有检测到合法的 PD，PSE 才会进行下一步的操作。

2. Classification(功率分级)：PSE 确定 PD 功耗。

   PSE 通过检测电源输出电流来确定 PD 功率等级，不同的功率等级对应不同的功率。此阶段端口输出电压大小为 15.5V ～ 20.5V。电压极性与-48V 输出一致。

3. Powerup（上电）：PSE 给 PD 供电。

   当检测到端口下挂设备属于合法的 PD 设备时（符合检测中描述的 PD 存在特征），并且 PSE 完成对此 PD 的分类，PSE 开始按照 PD 功率等级对该设备进行供电，输出-48V 的电压。

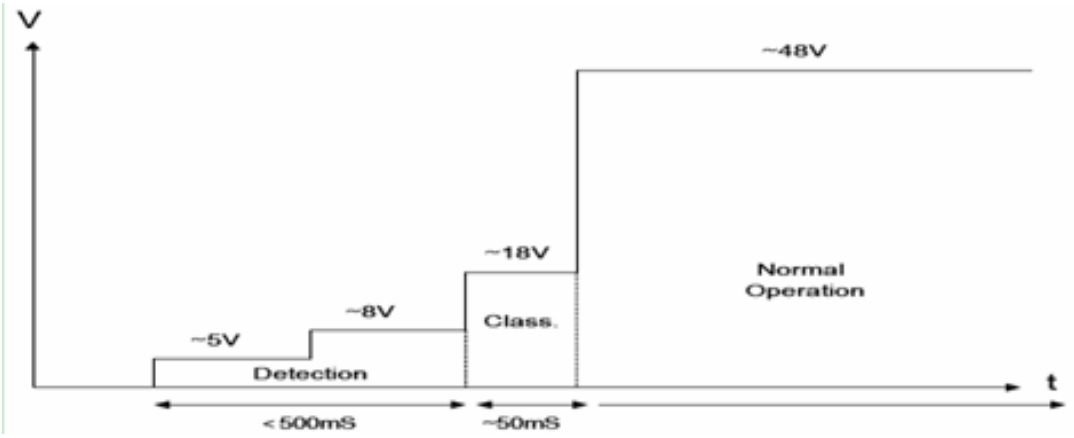
4. RTP & Power management，实时监控，电源管理。

   在此阶段，PSE 在进行供电的同时会实时检测 PD 设备是否断开。

5. Disconnection PD 断开处理。

   如果 PD 断开，PSE 将关闭端口输出电压。端口状态返回到 Detection。对于 PSE 供电系统，其整个供电过程理想的输出电压波形如下图所示：

图 10-6 PoE 供电过程电压变化图



10.7 PPPoE 拨号业务仿真

介绍 PPPoE 拨号业务仿真特性的定义、目的、规格、原理以及相关的术语和缩略语。

介绍该特性的实现原理。

10.7.1 介绍

定义

PPPoE 拨号业务仿真通过在 MA5620/MA5626 上模拟 PPPoE 客户端的 PPPoE 拨号行为，得到 PPPoE 拨号结果。根据结果可以验证 MA5620/MA5626 与 BRAS 以及 RADIUS Server 的连通性，也可以检查 PPPoE 用户名和用户密码正确与否，主要用于远程故障定位和远程验收。

目的

- 用于远程故障定位，免现场维护。
- 用于远程验收，降低设备安装成本。

受益

运营商受益

通过远程故障定位和远程验收，可以极大地节省运营商的运营成本 OPEX（Operating Expenditures），提升用户满意度。

用户受益

如果用户 PPPoE 业务出现异常，运营商可以远程快速定位问题原因，在最短时间内使用户的业务恢复正常。

10.7.2 规格

- 支持 PPPoE 用户名、用户密码、用户流索引、认证方式和拨号超时时间的配置。
- 支持通过命令行和网管查询 PPPoE 拨号仿真结果，支持仿真过程结束自动上报结果。
- 支持通过命令行或网管停止 PPPoE 业务仿真过程。
- 支持绑定了 MUX VLAN 或 Smart VLAN 的业务虚端口的 PPPoE 拨号业务仿真，且 VLAN 属性不能配置为 QinQ。

10.7.3 原理描述

介绍该特性的实现原理。

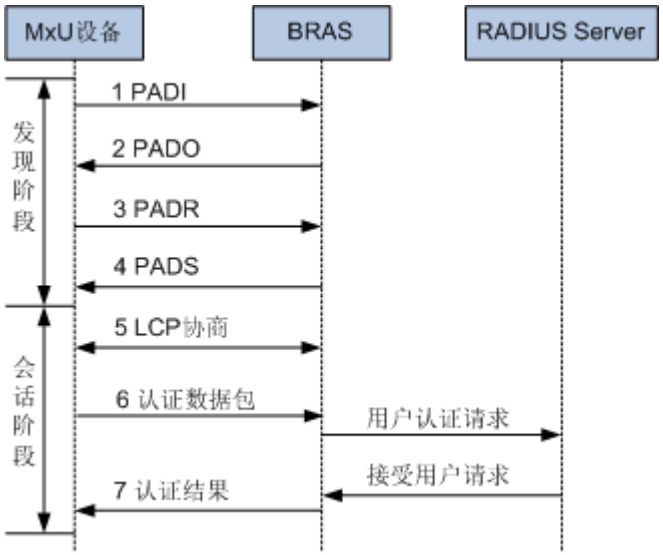
实现原理

- PPPoE 拨号业务仿真特性是指在 MA5620/MA5626 设备上模拟用户终端发起 PPPoE 拨号过程，通过分析 PPPoE 拨号成功/失败的结果，验证网络连通性和检测网络故障，也可以检查 PPPoE 用户名和用户密码正确与否，如果网络存在故障，能够迅速定位出故障在网络侧还是用户侧。 PPPoE 拨号业务仿真特性主要用于远程故障定位和远程验收。
- 通过用户界面输入需要仿真用户的业务流索引，由设备进行 PITP、VLAN 和 MAC 地址等与业务流相关的报文信息封装；同时需要通过用户界面输入 PPPoE 用户名、用户密码、认证方式和拨号超时时间。
- PPPoE 拨号业务仿真同时支持通过命令行和网管下发配置参数，进行业务仿真，支持通过命令行和网管查询 PPPoE 业务仿真结果，支持仿真过程结束自动上报结果。

业务仿真过程

PPPoE 拨号业务仿真过程如图 10-7 所示。

图 10-7 PPPoE 业务仿真过程



启动 PPPoE 拨号业务仿真后，MA5620/MA5626 模拟 PPPoE 客户端，发起 PPPoE 拨号过程，并配合上层服务器进行用户认证，与普通 PPPoE 拨号过程完全相同。

PPPoE 拨号业务仿真与普通 PPPoE 拨号过程主要区别如下：

1. PPPoE 拨号业务仿真过程由 MA5620/MA5626 发起，普通 PPPoE 拨号一般由 PC、Modem 或者家庭网关发起。
2. PPPoE 拨号业务仿真报文的 MAC 地址为 MA5620/MA5626 设备的桥 MAC 地址，普通 PPPoE 拨号的 MAC 地址一般为 PC、Modem 或者家庭网关的 MAC 地址。

10.8 术语与缩略语

术语

表 10-2 O&M 特性术语表

术语	解释
逻辑标识认证	逻辑标识认证是一种 EPON ONU 的认证方法，逻辑标识包括 LOID（LOID－－Logical ONU ID）和 Password 两部分，其中 Password 用于对 LOID 的校验。
Always-on	Always-on 是密码认证的一种发现模式，这种发现模式是指用户通过 Password 认证通过后，ONT 的 MAC 修改后，仍然可以上线。
Once-on	Once-on 是密码认证的一种发现模式，这种发现模式要求 ONT 在规定的时间内认证，超出该时间就不允许认证，并且一旦 ONT 认证成功后就不允许再修改 MAC。可通过 no-aging 和 aging-time 设置规定时间。

术语	解释
aging-time	当 ONT 为 Once-on 模式时，对超时时间进行设置，要求 ONT 在规定的时间内密码认证，超出该时间就不允许认证。
Gemport	在 TCONT 中使用 Gemport index 标识业务流。
无级调速	通过占空比调整机框风扇转速，全速时占空比为 100%，停止时为 0%。
占空比	描述机框风扇转速的快慢，全速时占空比为 100%，即全速时机框风扇以 100%的速率转动。

缩略语

表 10-3 O&M 特性缩略语表

缩略语	全称
PPPoE	Point-to-Point Protocol over Ethernet（以太网承载 PPP 协议）

11 时钟

关于本章

介绍 MA5620/MA5626 的时钟特性。

11.1 NTP
NTP 用于在分布式时间服务器和客户端之间进行时间同步。

11.2 系统时钟
介绍系统时钟的定义、原理、及时钟同步的具体应用。

11.3 术语与缩略语

11.1 NTP

NTP 用于在分布式时间服务器和客户端之间进行时间同步。

11.1.1 介绍

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（Time Protocol）和 ICMP 时间戳报文（ICMP Timestamp Message）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。

MA5620/MA5626 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。

11.1.2 规格

NTP 特性规格如下：

- 支持 NTP Version3
- 支持 NTP 客户端/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 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

11.1.3 参考标准和协议

本特性的参考资料清单如下：

- RFC1305.txt，“Network Time Protocol (Version 3) Specification，Implementation and Analysis”

11.1.4 可获得性

版本支持

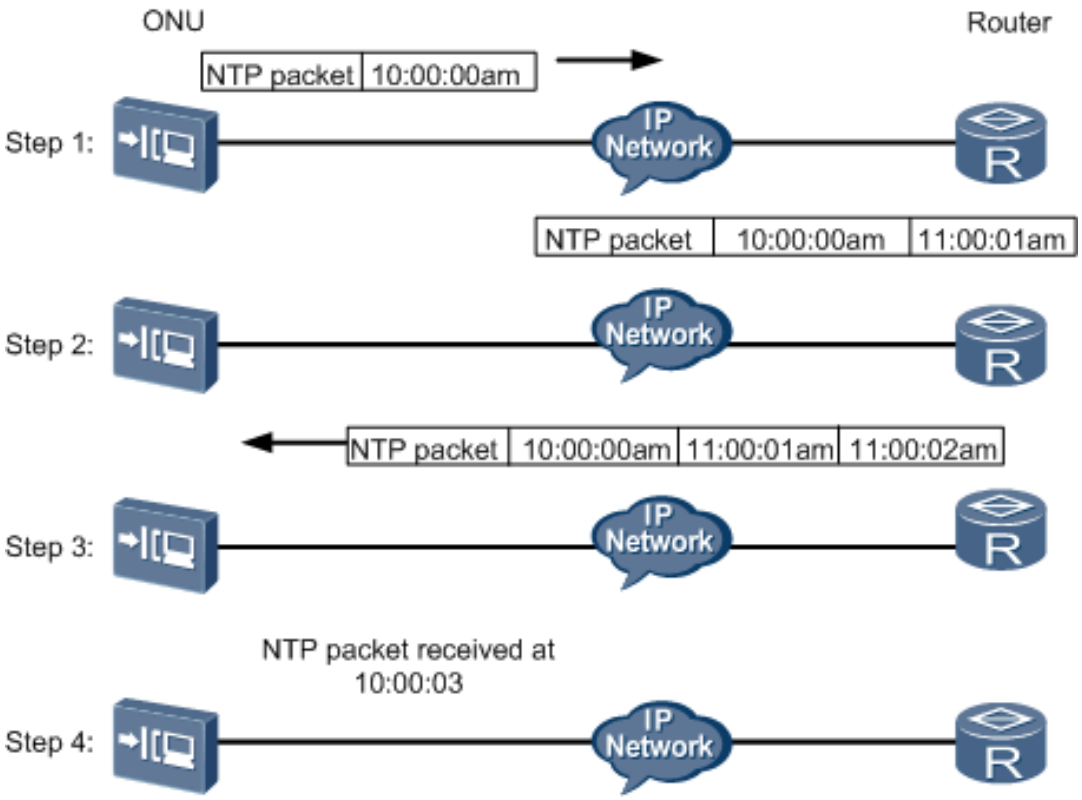
表 11-1 版本支持

产品	版本
MA5620/MA5626	V800R308
U2000	V100R002C01

11.1.5 原理描述

NTP 的工作原理如图 11-1 所示，工作过程如下：

图 11-1 NTP 工作原理图



1. MA5620/MA5626 发送一个 NTP 消息包给路由器，该消息包带有它离开 MA5620/MA5626 时的时间戳，假设该时间戳为 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，假设该时间戳为 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，假设该时间戳为 11:00:02am（T3）。
4. 当 MA5620/MA5626 接收到该响应消息包时，加上一个新的时间戳，假设该时间戳为 10:00:03am（T4）。

至此，MA5620/MA5626 已经拥有足够的信息来计算的两个重要参数：

- NTP 消息来回一个周期的时延 Delay=（T4-T1）-（T3-T2）；
- MA5620/MA5626 相对 Router 的时间差 Offset=（（T2-T1）+（T3-T4））/2。

综上所述，MA5620/MA5626 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。

11.2 系统时钟

介绍系统时钟的定义、原理、及时钟同步的具体应用。

介绍 MA5620/MA5626 支持时钟的几种常用的应用场景。

11.2.1 介绍

IP 化是未来网络和业务的发展趋势，在接入网从传统网络过渡到以 IP 为基础的以太承载网络目前还存在很多困难，一个关键技术是解决新网络对传统 TDM 业务的承载。传统 TDM 有两个主要的应用：语音业务和时钟同步业务。

在传统的通讯网络结构中，固网的 TDM 业务主要是语音业务。如果承载网络两端的时钟不一致，长期积累后会造成滑码。ITU-T 在 G.823 中定义了对固网 TDM 业务的需求和测试标准，称为 G.823 TRAFFIC 接口标准。

通讯网络对时钟频率最苛刻的需求体现在无线应用上，不同基站之间的频率必须同步在一定精度之内，否则基站切换时会出现掉线。目前的无线技术存在多种制式，不同制式下对时钟的承载有不同的需求。

- 以 GSM/WCDMA 为代表的欧洲标准采用的是异步基站技术，此时只需要做频率同步，精度要求 0.05ppm（或者 50ppb），需要由承载网络为它提供时钟。传统的解决方案是采用 PDH/SDH 来提供，IP 化后，需要 IP 网络提供。
- 而以 CDMA/CDMA2000 代表的同步基站技术，需要做时钟的相位同步（也叫时间同步）。

不同制式对时钟和时间的要求如**表 11-2** 所示。

表 11-2 不同制式对时钟和时间的要求表

无线制式	时钟频率精度要求	时钟相位同步要求
GSM	0.05ppm	NA
WCDMA	0.05ppm	NA
TD-SCDMA	0.05ppm	3us
CDMA2000	0.05ppm	3us
WiMax FDD	0.05ppm	NA
WiMax TDD	0.05ppm	1us
LTE	0.05ppm	倾向于采用时间同步

当前的时钟技术主要有以下几类：

- 同步以太时钟
- GPON/EPON/GE 线路时钟
- 1588V2 时钟

目的

用来保证通信设备与通信网的时钟同步。

11.2.2 规格

MA5620/MA5626 支持以下几种时钟：

- 同步以太时钟
- xDSL 线路时钟
- BIS 时钟
- GPON/EPON/GE 线路时钟
- 1588V2 时钟

MA5620/MA5626 支持以下时钟处理功能：

- 支持以太同步恢复时钟作为系统时钟，通过以太接口下传。
- 下行以太接口发送时钟默认采用系统时钟，时钟模式不可更改，且时钟的传递是单向的。
- 系统最大支持定义 10 个时钟源。
- 支持时钟源配置不同的优先级，并可以根据优先级选择相应的时钟源。
- 支持多个时钟源手动切换和自动切换。

11.2.3 参考标准和协议

表 11-3 时钟特性参考标准和协议

时钟特性标准	标准描述
ITU-T G.823（The control of jitter and wander within digital networks which are based on the 2048 kbit/s hierarchy）	ITU-T G.823 描述了 2048 kbit/s 同步体系 PDH 接口的抖动和漂移，这里主要指 E1 接口，对于 1544 kbit/s 体系则需满足 G.824 要求。 G.823 定义了 traffic 接口和 synchronization 接口要求。traffic 接口指标是满足业务传送的基本需求，如果 E1 接口要求传递同步时钟则需满足 synchronization 接口要求。Synchronization 接口的抖动和频漂特性要求比 traffic 接口严格。 G.823 定义的指标项目： ● Output Jitter（输出抖动） ● Output wander（输出频漂） ● Input Jitter and Wander tolerance（输入噪声容限）
ITU-T G.8261（Timing and Synchronization aspects in Packet Networks）	G.8261 针对包传送网络分别定义了 CES 和同步以太网的频漂预算，其指标要求基本等同于 TDM 网络的 G.823。MA5620/MA5626 的同步以太网时钟特性需满足 G.8261。
ITU-T G.8262（Timing characteristics of synchronous Ethernet equipment slave clock (EEC)）	G.8262 定义了同步以太网时钟体系的指标要求，其指标定义等同于 TDM 网络的 G.813 和 G.812。

11.2.4 可获得性

版本支持

产品	支持版本
MA5620/MA5626	V800R308
U2000	V100R002C01

11.2.5 原理描述

MA5620/MA5626 系统时钟结构分为：系统时钟源、系统锁相环电路、系统时钟输出三个部分。

时钟源

介绍系统支持的各种时钟源。

MA5620/MA5626 系统支持以下几类时钟源：GE 上行接口线路时钟源、xDSL 上行接口线路时钟源、BITS 时钟源、GPON/EPON 上行接口线路时钟源和内部时钟源。

GE 线路时钟源

- 支持跟踪上行 GE 线路时钟，通过物理层的同步，从线路码流恢复的时钟可作为系统时钟源。
- 不支持恢复以太接入单板的线路时钟作为系统时钟源。

xDSL 线路时钟源

支持跟踪上行 xDSL 线路时钟，通过物理层的同步，从线路码流恢复的时钟可作为系统时钟源。

BITS 时钟源

跟踪 BITS 输入时钟源，支持 2.048MHz、E1 和 T1 时钟信号输入模式。

GPON/EPON 线路时钟源

支持跟踪上行 GPON/EPON 线路时钟，通过物理层的同步、从线路码流恢复的时钟可作为系统时钟源。

内部时钟源

MA5620/MA5626 支持内部时钟源。

IEEE1588 V2 报文恢复时钟源

MA5620/MA5626 支持 IEEE1588 V2 特性，作为 SLAVE 设备能够通过报文时戳交互获得 MASTER 设备的时间和频率。通过 1588 报文恢复的频率时钟质量可满足 G.813、G.8262 规格，可作为系统时钟源。

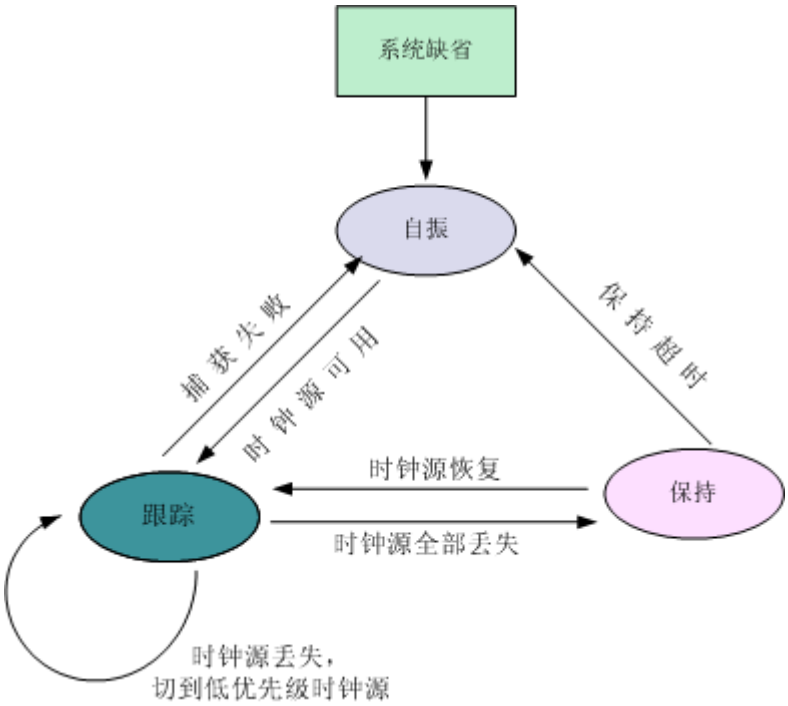
时钟源切换

介绍系统时钟源切换的原理。

MA5620/MA5626 采用人工配置优先级的方式进行时钟源切换，暂不支持 SSM 选源。系统最多可配置 10 个外部时钟源，每个时钟源分配不同的优先级，同时只能选择一个时钟源作为参考时钟，即最高优先级时钟源。当系统跟踪的时钟源出现故障时，系统自动选择次高优先级时钟源作为系统参考。

时钟源状态迁移过程如图 11-2 所示。

图 11-2 时钟源状态迁移图



11.2.6 应用场景

介绍 MA5620/MA5626 支持时钟的几种常用的应用场景。

同步以太时钟应用

介绍同步以太时钟的应用场景。

传统以太网应用没有考虑同步需求，各以太网接口采用+/-100ppm 的本地自振作为发送参考，各网元发送参考时钟彼此独立，精度不够理想。同步以太网是一种采用以太网链路码流恢复时钟的技术，完成以太网之间的同步关系，实现方式类似 SDH/PDH 网络同步方式。在发送方向使用高精度系统时钟作为发送参考，在接收端恢复并提取这个时钟，收发过程由 PHY 层独立完成。

同步以太时钟主要应用场景如图 11-3 所示。

图 11-3 MA5620/MA5626 同步以太应用场景

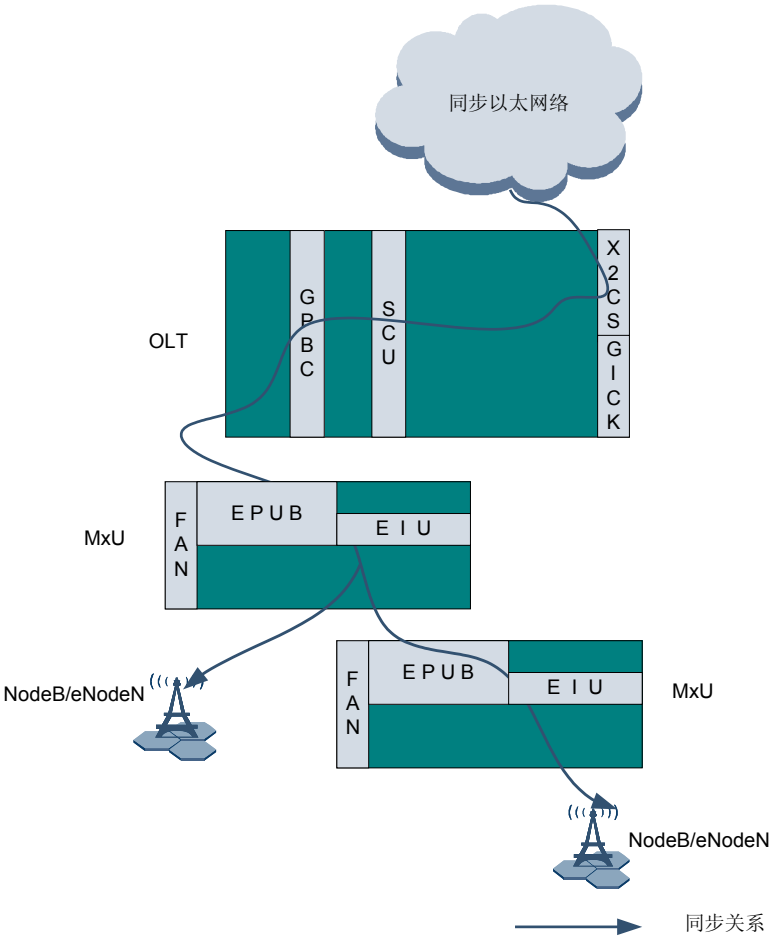


图 11-3 中的场景主要用于 3G 通信网络。

图 11-3 中，时钟同步实现过程如下：

1. MA5620/MA5626 设备的系统时钟选择上行以太端口的线路恢复时钟，从而实现对上级设备的时钟同步。
2. MA5620/MA5626 通过 GE 将系统时钟下发。

图 11-3 中同步以太网应用对 MA5620/MA5626 接入设备的系统硬件配置要求如下：

- MA5620/MA5626 支持 GE 上行，支持 GE 接入。

图 11-3 中同步以太网应用配置注意要点：

- 在 MA5620/MA5626 设备上配置上行接口的线路时钟为系统时钟源，选择同步以太线路时钟作为系统时钟。
- MA5620/MA5626 的上行接口、接入接口的发送时钟默认为系统时钟，且不可更改，不需要额外设置。

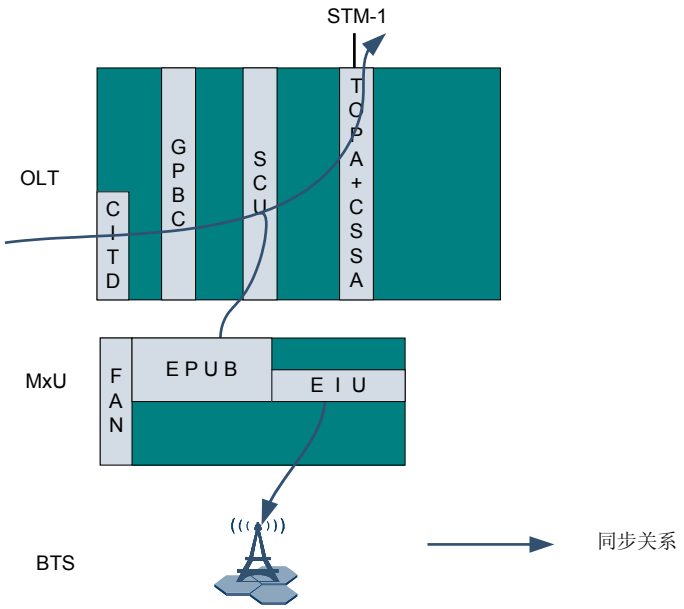
GPON 线路时钟应用

介绍 GPON 线路时钟的应用场景。

当 MA5600T TOPA 的 E1 端口发送时钟采用系统时钟，GPBD 的 PON 口线路发送时钟默认为系统时钟时，MA5620/MA5626 可通过 GPON 口同步 MA5600T 系统时钟。

GPON 线路时钟应用场景如图 11-4 所示。

图 11-4 GPON 线路时钟应用场景



上图中，时钟同步实现过程如下：

1. MA5620/MA5626 的系统时钟选择上行 GPON 端口的线路恢复时钟，从而实现对上级设备的时钟同步。
2. 设置 MA5620/MA5626 GPON 端口的线路恢复时钟为系统时钟。

GPON 线路时钟应用场景中 MA5620/MA5626 设备的系统硬件配置：

- MA5620/MA5626 采用 GPON 上行。
- 时钟配置：满足 G.813 要求。

GPON 线路时钟同步配置要点：

- 配置 MA5600T 系统时钟源，如选择 STM-1 线路时钟作为系统时钟。
- MA5600T 的 PON 端口发送时钟默认为系统时钟。
- MA5620/MA5626 设置系统时钟选定为上行端口的线路时钟，可通过提取 PON 线路时钟同步于上级 MA5600T 时钟。
- MA5620/MA5626 下级的 BTS 直接连接到 MA5620/MA5626 上的时钟输出接口，获取时钟。

11.3 术语与缩略语

术语

术语	解释
Frequency accuracy	频率准确度是指信号的实际输出频率与理想时钟源的频率偏离程度，一般用相对频率偏差来表示。例如：若标称频率为f0，实际频率为 f，则频率准确度为（f-f0）/f0，单位一般用ppm 或者 ppb 来表示。
Pull-in and pull-out ranges	在非锁定情况下，当输入时钟频率靠近中心频率的某个范围内时，时钟锁相环会从自振或保持状态转入锁定状态，这个范围值称为牵引入范围（PULL IN）。 在锁定情况下，当输入时钟频率偏离中心频率的某个范围时，时钟锁相环会转入保持状态，这个范围值称为牵引出范围(PULL OUT)，牵引出范围不考虑输入频率的反复变化。
Wander generation	漂移产生是指当时钟锁定一个没有漂动的理想信号时，输出信号的漂动的大小。它反映了时钟系统跟踪理想信号时对输入理想源劣化的程度。该指标通常用 MTIE 和 TDEV 来衡量。
Jitter output	时钟输出抖动是指设备在跟踪理想基准定时信号时，设备的输出时钟产生的抖动。
Wander tolerance/Jitter tolerance	漂移/抖动容限用于衡量系统对输入时钟源漂移、抖动的容忍能力。
Noise transfer	噪声传递反映了时钟对于输入漂动的滤除能力。当给定一个带有较大幅度漂动的输入信号时，经过锁相环系统的低通特性，输出信号应该具有较小的漂动。
Long-term phase transient response (Holdover)	当设备长期跟踪外部时钟源，并且已经记录了保持数据，当外部时钟源丢失时，设备会根据记录的保持数据提供系统时钟，即进入保持状态。保持能力考察时钟系统在参考源丢失后一段时间内的频漂稳定能力。

缩略语

缩略语	全称
PDH	Plesiochronous Digital Hierarchy（准同步数字体系）
STM	Synchronous Transfer Mode（同步传输模式）
SDH	Synchronous Digital Hierarchy（同步数字体系）
PRC	Primary Reference Clock（基准参考钟）
LPR	Local Primary Referenc（区域基准钟）

缩略语	全称
SSU	Synchronization Supply Unit（同步供给单元）
SEC	SDH Equipment Clock（SDH 设备时钟）
EEC	Ethernet Equipment Clock（以太网设备从时钟）
GPS	Global Positioning System（全球定位系统）
TIE	Time Interval Error（时间间隔误差）
MTIE	Maximum Time Interval Error（最大时间间隔误差）
CES	Circuit Emulation Service（电路仿真业务）
SSM	Synchronization Status Message（同步状态信息）
GE/FE	Gigabit Ethernet/Fast Ethernet（千兆/百兆以太网）
BITS	Building Integrated Timing Supply（通信楼综合定时供给系统）
NTR	Network Time Recover（网络时钟恢复）
CBU	Cellular Backhaul Unit（基站回传单元）