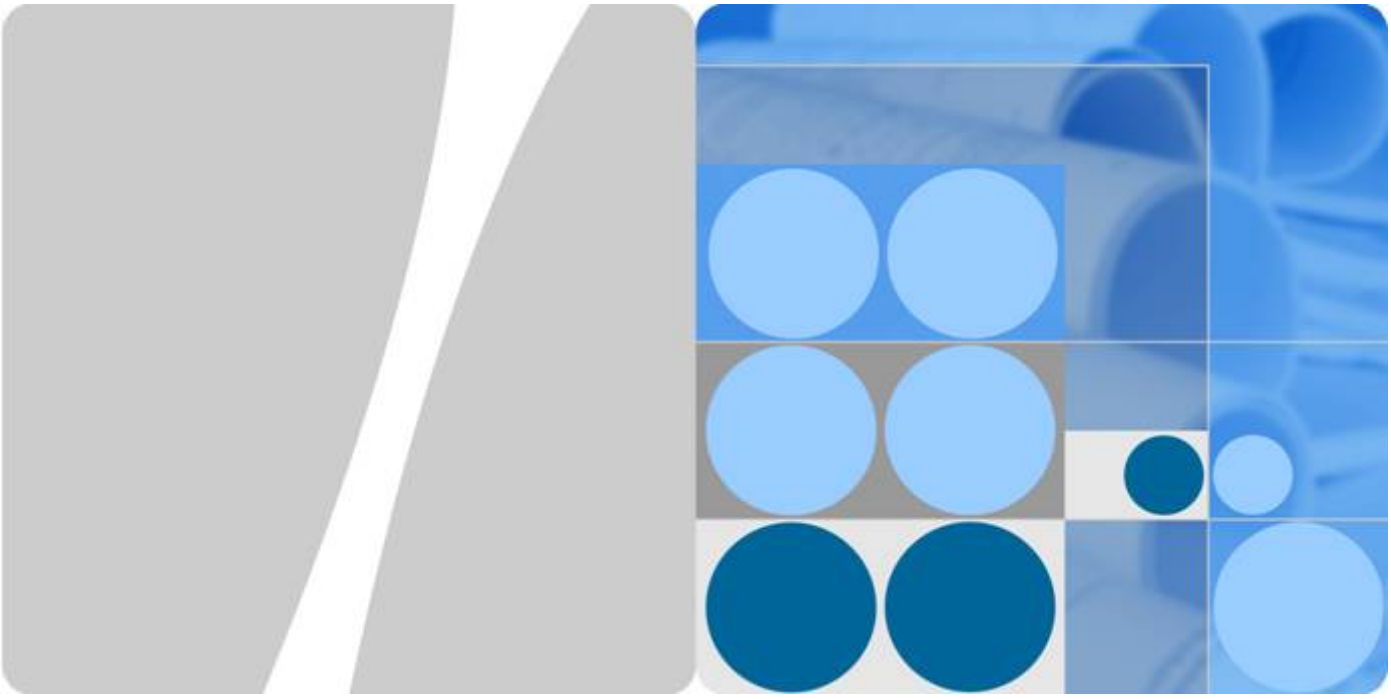


SmartAX MA5631 EoC 局端设备

V800R308C02

特性描述

文档版本　02

发布日期　2011-08-05

华为技术有限公司

商标声明


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

注意

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

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

华为技术有限公司

地址： 深圳市龙岗区坂田华为总部办公楼 邮编：518129

网址： http://www.huawei.com

客户服务邮箱： support@huawei.com

客户服务电话： 4008302118

前 言

读者对象

本文档针对 MA5631 的关键特性，分别详细介绍其子特性。

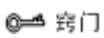
本文档能指导读者了解各类特性的定义、设备实现该特性的目的、设备对特性规格的支持情况以及与特性密切相关的参考资料，帮助读者全面了解特性，较深层次地理解各特性在 MDU 上的实现原理。

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 (2011-08-05)

相对产品版本 V800R308C02 文档版本 01 (2011-04-15)的变更如下。

修改：

- **1.4 原理描述**(调制 EoC)

文档版本 01 (2011-04-15)

第一次正式发布版本。

目 录

1 调制 EoC

关于本章

EoC 可以划分为两类：无源 EoC（即基带 EoC）和有源 EoC（即调制 EoC）。

1.1 介绍

定义

EoC（Ethernet over Coaxial cable）电缆接入技术是下一代广播电视网的关键技术之一，即基于同轴电缆，通过各种数字调制技术来承载以太网业务和其他各种综合业务，实现下一代广播电视网的用户宽带接入。利用该技术进行有线电视网络宽带、双向化改造，可以有效发挥有线电视网频带宽、成本低、易普及的优势，有利于推进三网融合。

基带 EoC 直接把以太网的基带信号通过无源器件耦合到同轴电缆中传输。由于采用简单的信号耦合，基带 EoC 存在抗干扰能力差、对阻抗匹配要求高等问题，实际使用中适应性比较差。

调制 EoC 是利用调制技术如 OFDM（Orthogonal Frequency Division Multiplexing）、QAM（Quadrature Amplitude Modulation）等将数据信号调制到能在 CATV（Cable TV）同轴网传输的某一频段上，然后将 CATV 信号和调制后的数据信号混合传输，下行方向传输 CATV 和数据调制信号，上行方向传输数据调制信号。

目的

MA5631 支持的 optiCable 方案（即 PON+EoC 方案）属于调制 EoC 技术范畴，几乎无需改造 Cable 网，带宽相对较高，且后续扩展性好。

1.2 参考标准和协议

本特性的参考资料清单如下：

- IEEE P1901
- HomePlug AV

1.3 可获得性

版本支持

表 1-1 调制 EoC 特性的版本支持

产品	支持版本
MA5631	V800R308C02

硬件要求

MA5631 必须配置 EoC 局端模块。

1.4 原理描述

调制 EoC 技术低频段有 HomePlug AV/BPL、HomePNA 等，高频段有 MoCA 和 WiFi 等。

MA5631 支持 Homeplug AV 技术。HomePlug AV 标准由家庭插电联盟制定。HomePlug AV 技术具有高带宽、抗干扰能力强等优点。

HomePlug AV 技术在物理层采用具有高级前向纠错、通道预估和自适应能力的 OFDM，而在 MAC 层则综合使用具有 QoS 保证的 TDMA（Time Division Multiple Access）时分多址有序接入和 CSMA（Carrier Sense Multiple Access）竞争接入两种方式，并通过 ARQ（Automatic Repeat Request）来保障可靠传送。

MoCA、HomePNA、HomePlug AV 和 WiFi 的对比如**表 1-2** 所示。

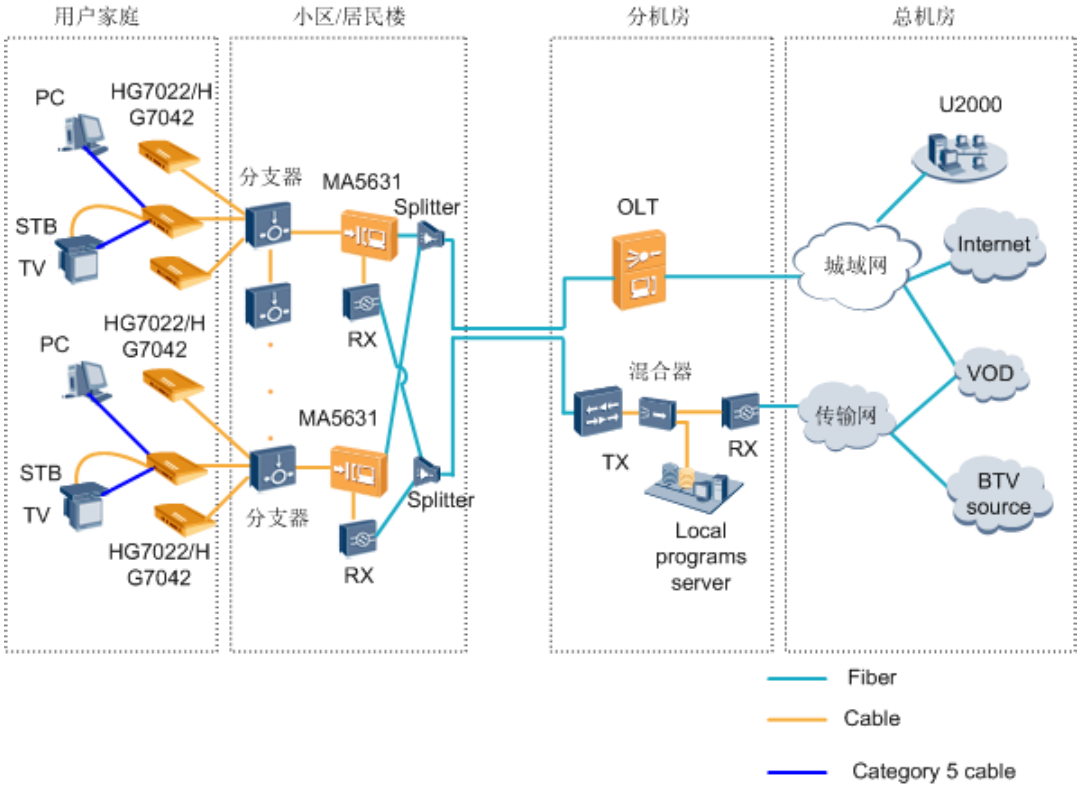
表 1-2 EoC 技术对比

比较项	MoCA	HomePNA	HomePlug AV	WiFi Over Cable
传输频宽	800MHz ～ 1500MHz	4MHz ～ 28MHz	7.5MHz ～ 65MHz	2.4GHz
动态范围	70dB	70dB	75dB	70dB
调制	OFDM TDMA/ TDD	QAM，FDQAM	OFDM	BPSK/QPSK/ QAM
安全	DES	AES	128AES	802.11i/WEP
QoS	802.1p	私有	802.1p	803.11e
信号衰减	大	小	小	大
技术标准	MoCA 1.0	ITU G.9954，HPNA 3.0	HomePlug AV（IEEE P1901）	IEEE 802.11g/n

MA5631 支持 optiCable 方案的组网应用，可提供高带宽，支持 HSI、IPTV 等业务，满足广电多业务的发展需求。P2MP 的结构，适合用户密集分布的情况，建设成本低。

组网如**图 1-1** 所示。MA5631 为 EoC 局端设备，HG7022/HG7042 的全称为 EchoLife HG7022/HG7042，是 EoC 终端设备。

图 1-1 optiCable 方案组网图



MA5631 采用 GPON 上行，GPON 信号和光接收机上行传输的 CATV 信号分别在两根光纤上传输。

1.5 术语与缩略语

缩略语

缩略语	全称
ARQ	Automatic Repeat Request（自动重传请求）
TDMA	Time Division Multiple Access（时分多址）
CSMA	Carrier Sense Multiple Access（载波检测多址）
OFDM	Orthogonal Frequency Division Multiplexing（正交频分复用）
QAM	Quadrature Amplitude Modulation（正交幅度调制）
EoC	Ethernet over Coaxial Cable（基于同轴电缆以太网承载技术）
CATV	Cable TV（有线电视）

2 CNU 管理

关于本章

MA5631 和 EoC 终端设备一起可以实现 HSI、IPTV 等业务，可以满足广电多业务的发展需求。

2.1 介绍

定义

目前有线电视网覆盖用户超过 1 亿户，绝大多数用户的网络都没有进行双向改造，这样的网络仅能满足单向的广播电视节目传输，无法开展双向交互等增值型业务。

针对广电双向网络改造和家庭宽带接入应用，MA5631 提出了 optiCable 方案（即 PON +EoC 融合的方案，MA5631 为 ONU 与 EoC 局端融合一体化的设备）。

CNU（Coaxial Network Unit）即 EoC 终端设备。MA5631 和 CNU 一起可以实现 HSI、IPTV 等业务，可以满足广电多业务的发展需求。

目的

CNU 网络侧提供 RF 接口，采用 Cable 上行，用户侧提供以太网接口和 RF 接口，用于宽带和有线电视接入。采用 EoC 技术可以很好地利用原有的同轴电缆接入网资源，减少投资、节省资源。

2.2 规格

系统支持的 CNU 的规格如下：

- 支持 EchoLife HG7022/HG7042 EoC 终端。
- 最多支持 256 个 CNU 和 256 个 CNU 线路模板。
- 每个 EoC 端口可以管理 64 个 CNU。
- 支持 64 个 CNU 成员的黑名单。

系统支持对 CNU 做如下操作：

- 离线添加 CNU。
- 删除系统中已经确认的 CNU。
- 修改 CNU 的认证信息。
- 自动发现和自动确认 CNU。
- 通过命令行或网管查询 CNU 信息。
- 激活、去激活 CNU。
- 批量升级 CNU。
- 对 CNU 的每一个端口进行环回操作，以定位线路故障位置。
- 配置 CNU 加载信息，指定需要加载文件的加载方式、服务器 IP 地址、用户名、密码、文件类型、文件名称。
- 查询 CNU 加载信息。
- 选择和查询 CNU 加载对象。

2.3 参考标准和协议

本特性的参考资料清单如下：

- ITU-T G.1010: End-user multimedia QoS categories
- NSCRTV-EPONEOC-MOD-EOC-MIB.pdf

2.4 可获得性

版本支持

表 2-1 CNU 管理特性的版本支持

产品	支持版本
MA5631	V800R308C02

硬件要求

MA5631 必须配置 EoC 局端模块才能管理 CNU。

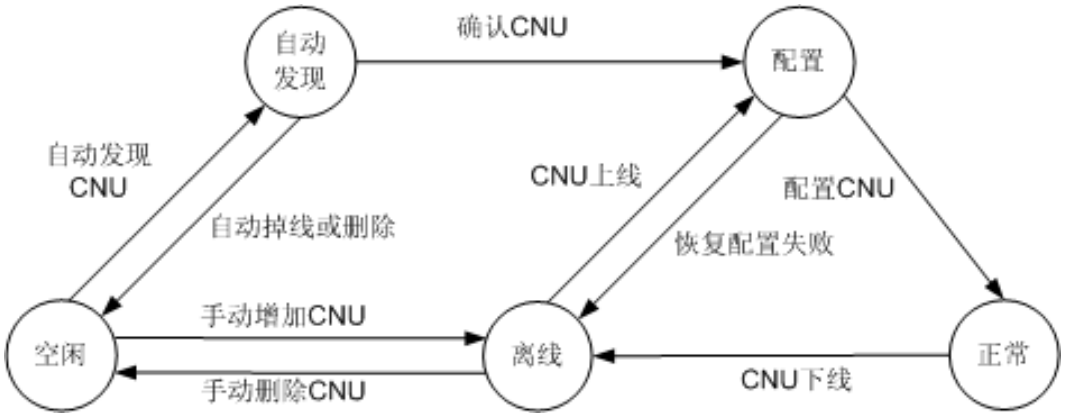
2.5 原理描述

2.5.1 CNU 状态管理

CNU 有自动发现、离线、正常、配置四种状态。

CNU 状态迁移如图 2-1 所示。

图 2-1 CNU 状态迁移图



说明

当 EoC 端口连接的 CNU 数量小于 128 时，EoC 端口的状态为空闲。

CNU 有如下几种状态：

- 自动发现：当 MA5631 检测到 CNU 连接上线请求，且 MA5631 暂无与该 CNU 匹配的认证信息，CNU 进入自动发现状态。自动发现的 CNU 不可配置，不能进行业务传输，系统不分配 CNU ID。
- 离线：离线增加 CNU 后，CNU 处于离线状态。或者当正常状态的 CNU 与 MA5631 通信中断后（如 CNU 故障、掉电等），CNU 状态切换成离线状态。
- 配置：当 CNU 连接上线时，如 MA5631 已经配置了和此 CNU 认证信息匹配的 CNU，或者已确认自动发现的 CNU，则下发此 CNU 的配置数据。
- 正常：自动发现的 CNU 在确认、配置完毕后，状态变为正常。

说明

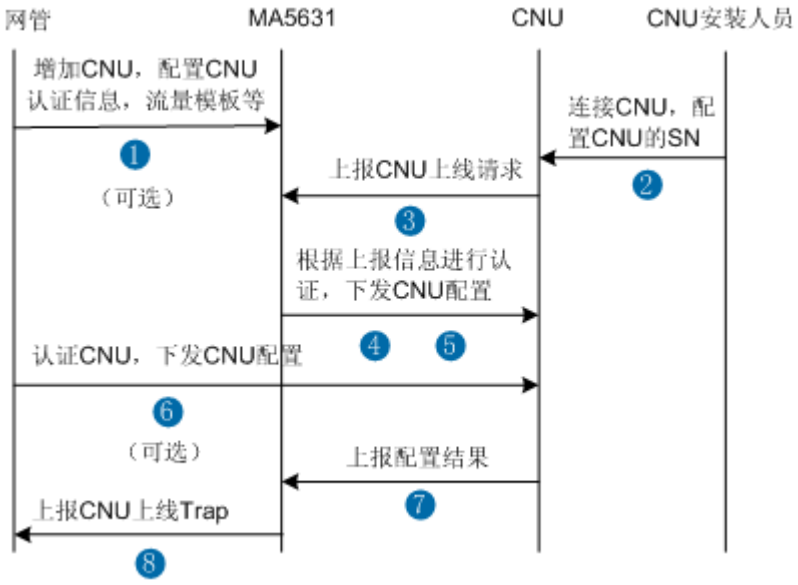
通过命令行和网管仅可以查看到 CNU 处于自动发现、离线或正常状态。

2.5.2 CNU 认证

CNU 认证通过后，才可以对 CNU 进行配置。

CNU 认证流程如图 2-2 所示。

图 2-2 CNU 认证流程图



CNU 认证流程如下：

1. （可选）在网管或 CLI 上添加 CNU，配置 CNU 认证信息、线路模板、CNU ID 和 CNU 的描述信息等。

   说明

   必须配置 CNU 的认证信息，包括 MAC 地址或 SN 信息，其他数据的配置是可选的。
2. 安装人员上门安装 CNU，将 CNU 和 PC 连接好后，通过专用软件设置 CNU 的 SN（必须保证同一台 MA5631 下连接的 CNU 的 SN 信息唯一）。
3. CNU 向 MA5631 上报上线请求，包括 CNU 的 MAC 地址和 SN 信息。
4. MA5631 查询 CNU 上报的 MAC 地址和 SN 是否在黑名单中。如在，强制 CNU 下线，否则，进一步查询上报信息是否与已上线 CNU 的冲突。

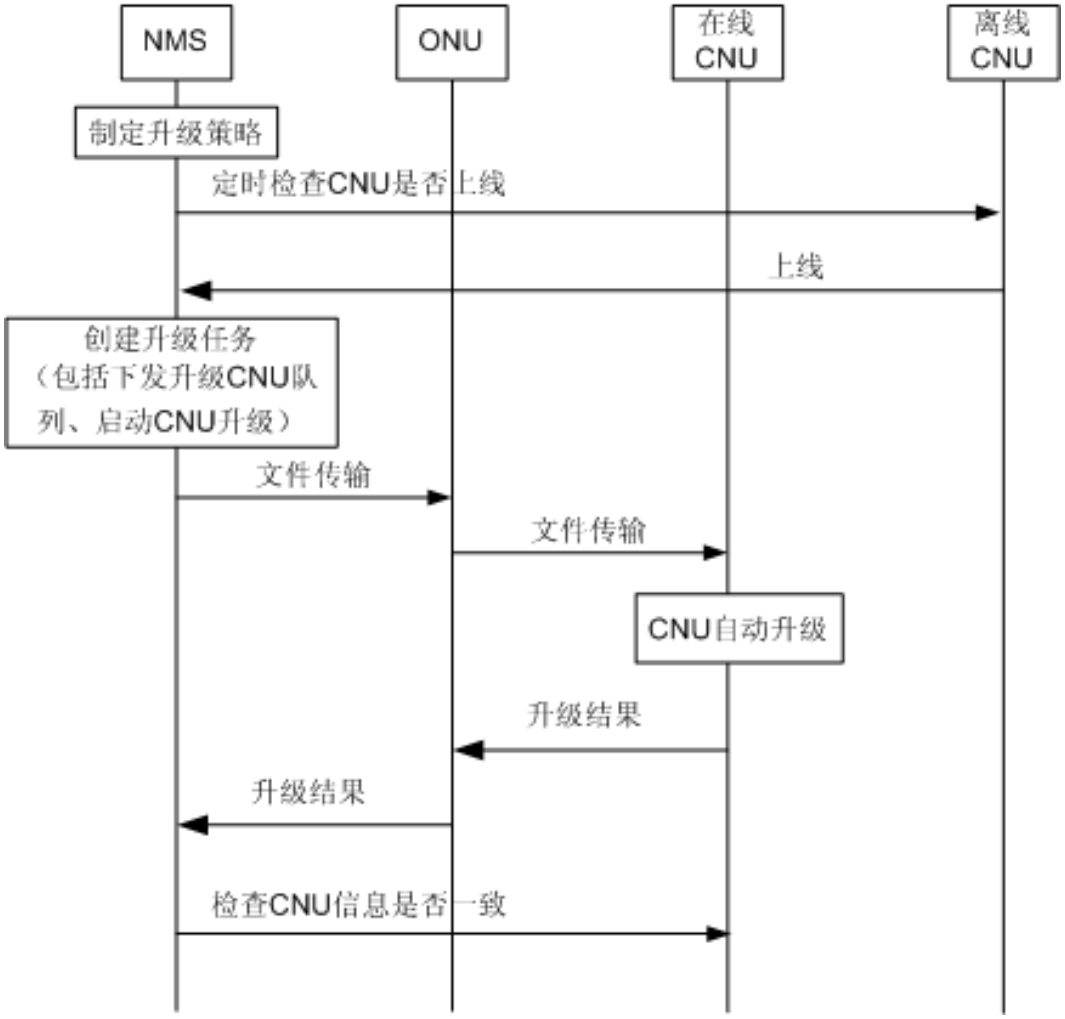
5. 如 CNU 上报的信息与已上线 CNU 的冲突，MA5631 上报告警，并强制该 CNU 下线。如不冲突，MA5631 向 CNU 下发配置数据。
6. （如未执行步骤 1，需执行此步骤）通过 CLI 或者网管可以查询到 CNU 处于自动发现状态。通过 CLI 或网管对 CNU 进行认证，认证通过后向 CNU 下发配置数据。
7. CNU 上数据配置完毕后向 MA5631 上报配置结果。
8. MA5631 向网管上报 CNU 上线的 Trap 报文。

2.5.3 CNU 批量升级

可以通过网管选择符合条件的 CNU，将其加入到 MDU 设备下的加载队列，然后启动 CNU 升级，来完成 CNU 批量升级。

CNU 批量升级流程如图 2-3 所示。

图 2-3 CNU 批量升级流程图



网管上的操作：

1. 制定升级策略。

2. 设置升级加载信息。
3. 创建升级任务，添加升级队列，启动或者停止升级。

网管通过 MIB 接口对 ONU 的操作：

设置加载信息，添加升级队列，启动和停止升级的 MIB 接口，处理配置消息。

ONU 上的操作：

向在线 CNU 传输升级文件，上报 CNU 加载结果给网管，管理 CNU。

2.6 术语与缩略语

缩略语

缩略语	全称
CNU	Coaxial Network Unit（同轴电缆宽带接入网接入端（调制解调）设备）
EoC	Ethernet over Coaxial Cable（基于同轴电缆以太网承载技术）
MDU	Multi Dwelling Unit（多住户单元）
ONU	Optical Network Unit（光网络单元）

3 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。

3.1 介绍

MA5631 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 3-1 所示：

表 3-1 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 MA5631 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。

3.2 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 3-2 所示：

表 3-2 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

3.3 可获得性

版本支持

表 3-3 上行特性的版本支持

产品	支持版本
MA5631	V800R308C02

3.4 三模自适应

上行端口的三模自适应，即 MA5631 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。

3.4.1 介绍

定义

上行端口的三模自适应，即 MA5631 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。

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。

3.4.2 规格

MA5631 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

3.4.3 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。

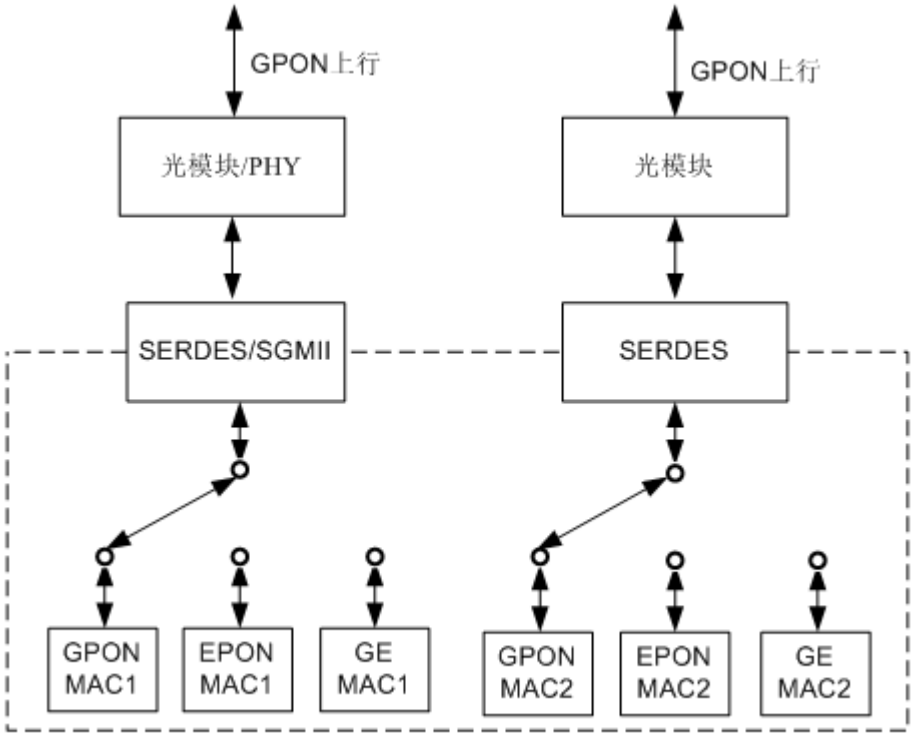
当扣板上行端口插入相应的光模块和光纤，上行端口状态由 DOWN 状态切换为 UP 状态后，芯片软件程序自动启动三模检测，对于 GE/EPON/GPON 三种模式自适应原理介绍如下。

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 3-1 所示。

图 3-1 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。

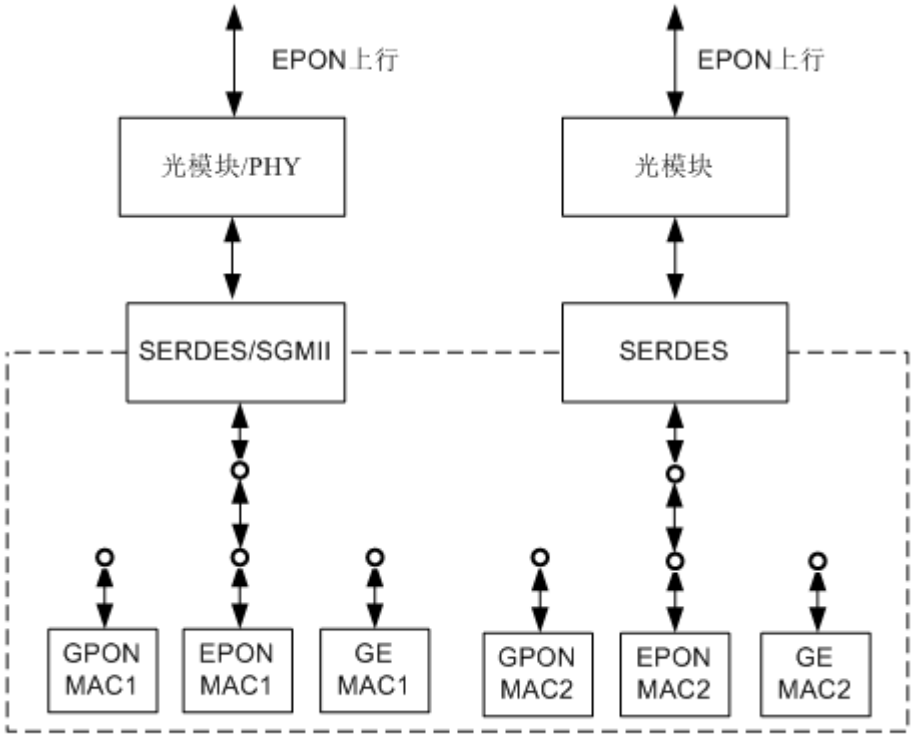
GPON 模式切换到 EPON 模式：GPON MAC 无法同步（有 LOS/LOF），则跳转到 EPON 模式。

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 3-2 所示。

图 3-2 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。

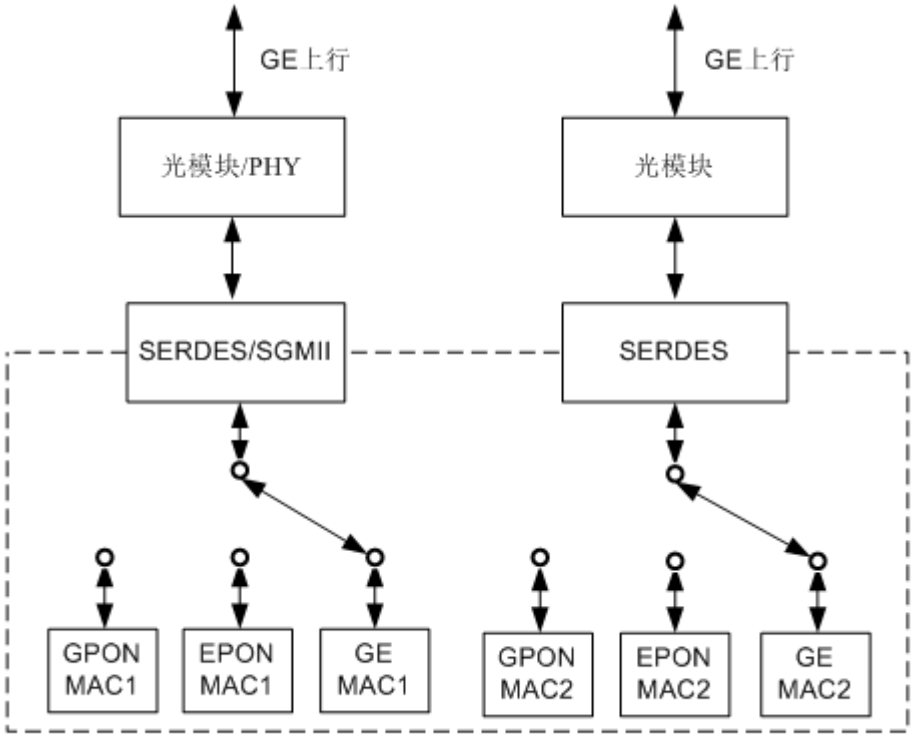
EPON 模式切换到 GE 模式：EPON PCS 子层可以同步，但正确帧数不增加，CRC8 错误帧数增加；或者正确帧数和 CRC8 错误帧数都不增加（GE 链路无数据的情况）。则跳转到 GE 模式。

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 3-3 所示。

图 3-3 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。

3.5 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。

3.5.1 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

MA5631 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。

3.5.2 规格

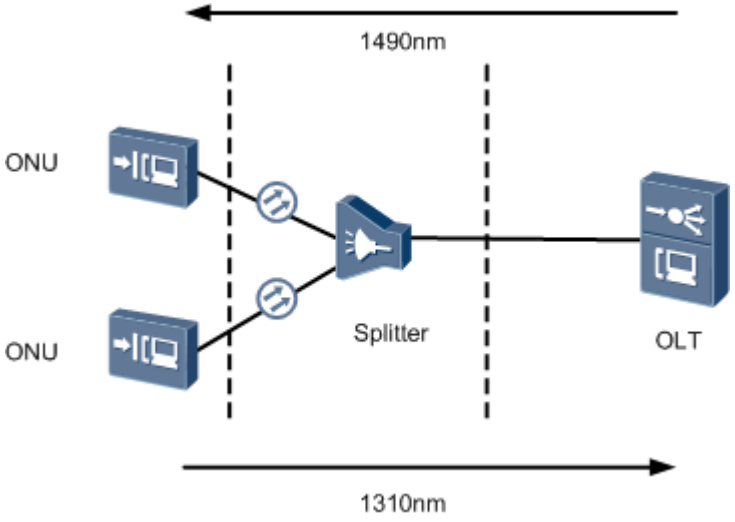
- 支持一个 EPON 上行端口，下行速率 1.25Gbit/s，上行速率 1.25Gbit/s。
- 支持最远 20km 的传输距离。
- EPON 光接口采用单模光模块，支持单纤双向的数据传输。
- 支持 EPON 光模块长发光的检测和防护。
- 支持 EPON Type D 和 Type B 保护倒换。

3.5.3 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 3-4 所示：

图 3-4 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 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）》。

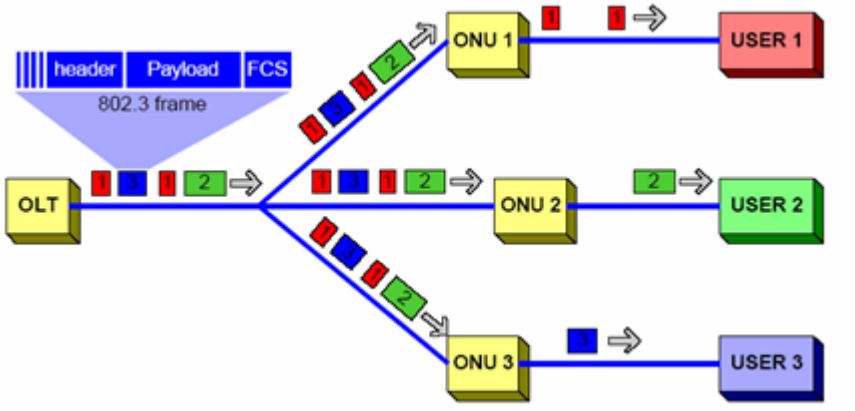
EPON 作为新型光接入技术，与传统的 xDSL 技术相比，不仅传输介质和带宽速率不相同，而且接入网络的管理维护模式也相应的发生变化。

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 3-5 所示。

图 3-5 EPON 下行传输

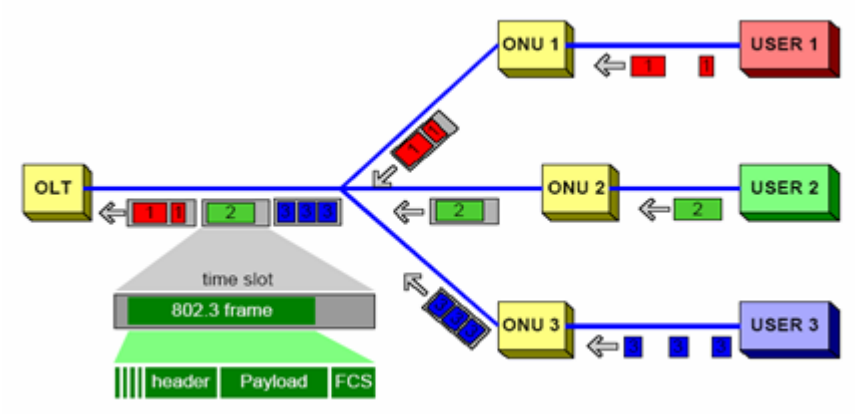


EPON 下行数据流采用广播技术，各 ONU 只接收属于自己的数据。

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 3-6 所示。

图 3-6 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

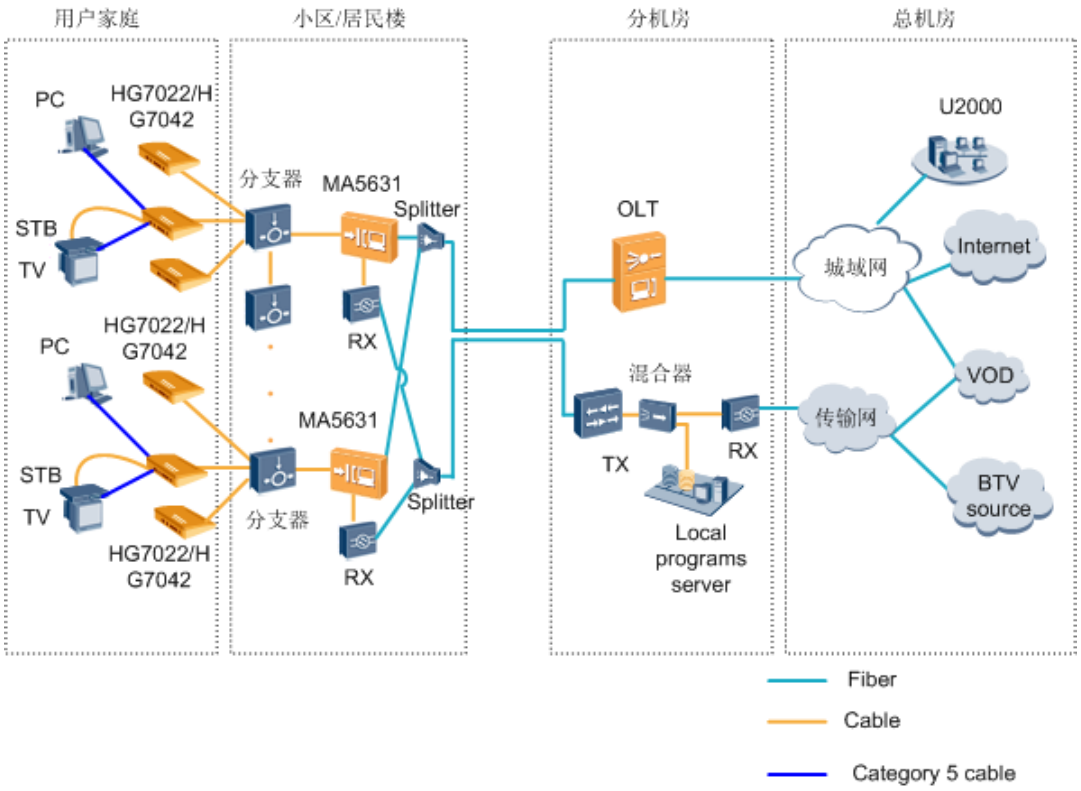
由于 EPON 上行数据流采用 TDMA 技术，各 ONU 在分配的特定时隙内发送数据，这样的话，ONU 会由于距离不通而产生一定的时延，造成到达 OLT 的数据冲突。

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。

3.5.4 组网应用

MA5631 支持 EPON+EoC 的组网应用，可提供高带宽，支持 HSI、IPTV 等业务，满足广电多业务的发展需求。P2MP 的结构，适合用户密集分布的情况，建设成本低。组网如图 3-7 所示。

图 3-7 EPON+EoC 组网图



3.6 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。

3.6.1 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。

3.6.2 规格

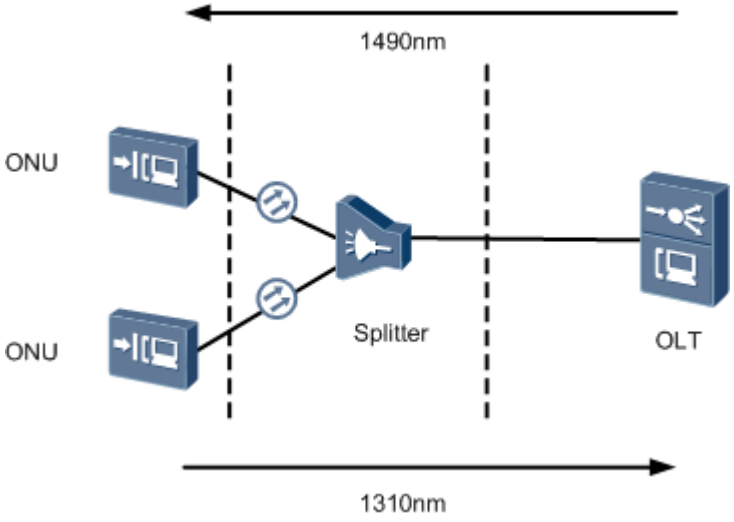
- GPON 接口支持 T-CONT Type1 ～ 5 类型：支持最多 32 个 T-CONT，Alloc-ID 范围 0 ～ 4095。T-CONT 最小分配带宽为 64kbit/s，最大为 1.2Gbit/s，最小粒度为 64kbit/s。
- GPON 接口支持最多 1024 个 GEM Port，GEM Port ID 范围是 0 ～ 1023。
- GPON 接口支持基于业务流的 VLAN ID、802.1p、VLAN ID+802.1p 到 GEM Port 的映射配置，其中 VLAN ID 支持全范围，业务流到 GEM Port 的映射无限制。
- GPON 接口每个 T-CONT 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 GPON Type B 保护。
- 当设备掉电后，支持通过 PLOAM/OMCI 消息上报 Dying Gasp 告警。
- 当分光比为 1:32，支持最大物理距离 20km；当分光比为 1:64，支持最大物理距离 10km。
- 支持最大逻辑距离 60km。

3.6.3 原理描述

系统原理

GPON 系统原理结构如图 3-8 所示：

图 3-8 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：

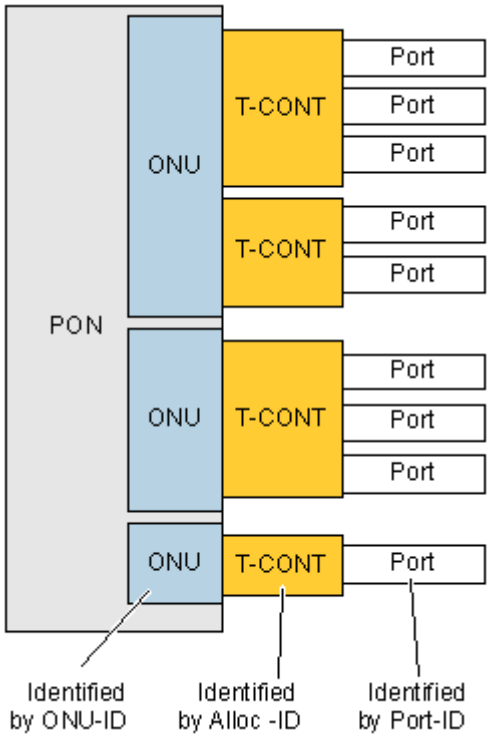
- 下行数据流采用广播技术，各 ONU 只接收属于自己的数据，传输速率是 2.4Gbit/s。
- 上行数据流采用 TDMA 技术，各 ONU 在分配的特定时隙内发送数据，传输速率 1.2Gbit/s。

工作原理

GPON 主要由物理层，TC 成帧子层，TC 封装适配层组成。

MA5631 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 3-9 所示。

图 3-9 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 3-4 的 Type1 到 Type5）。

表 3-4 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 3-10，图 3-11 所示。

图 3-10 GPON 下行帧结构

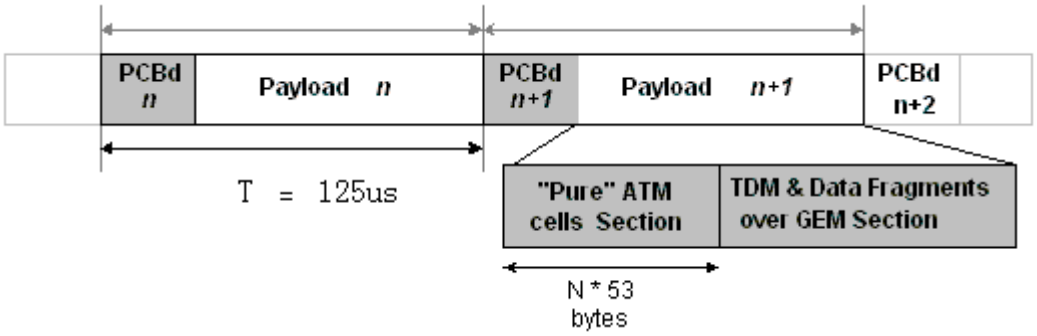
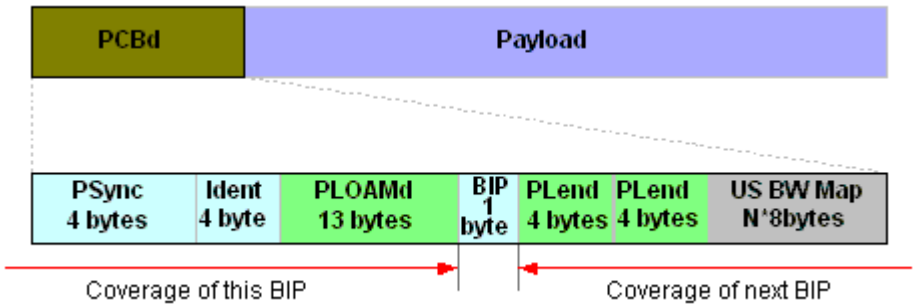


图 3-11 PCBd 结构



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。

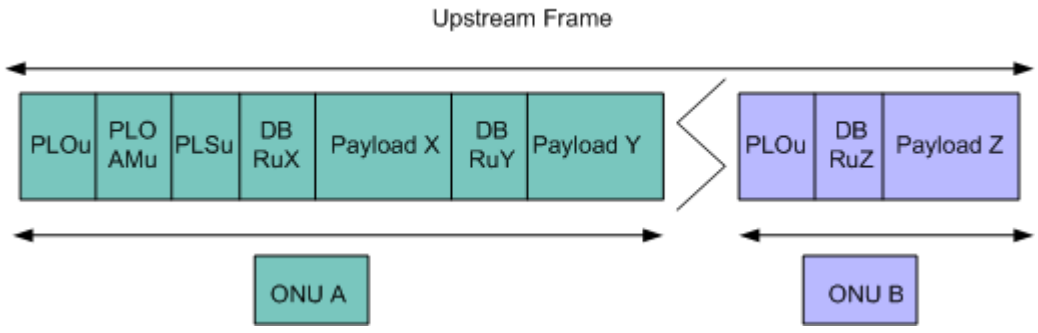
PCBd 里包含：帧同步信息，物理层 OAM，BIP 校验字段等等。其中 US BW Map（上行带宽映射）是 OLT 发送给每个 T-CONT 的各自的上行传输带宽映射。这正是通过下行帧的 PCBd 里的带宽映射字段来完成。从而实现 MAC 控制功能。

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 3-12 所示。

图 3-12 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 帧和 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：

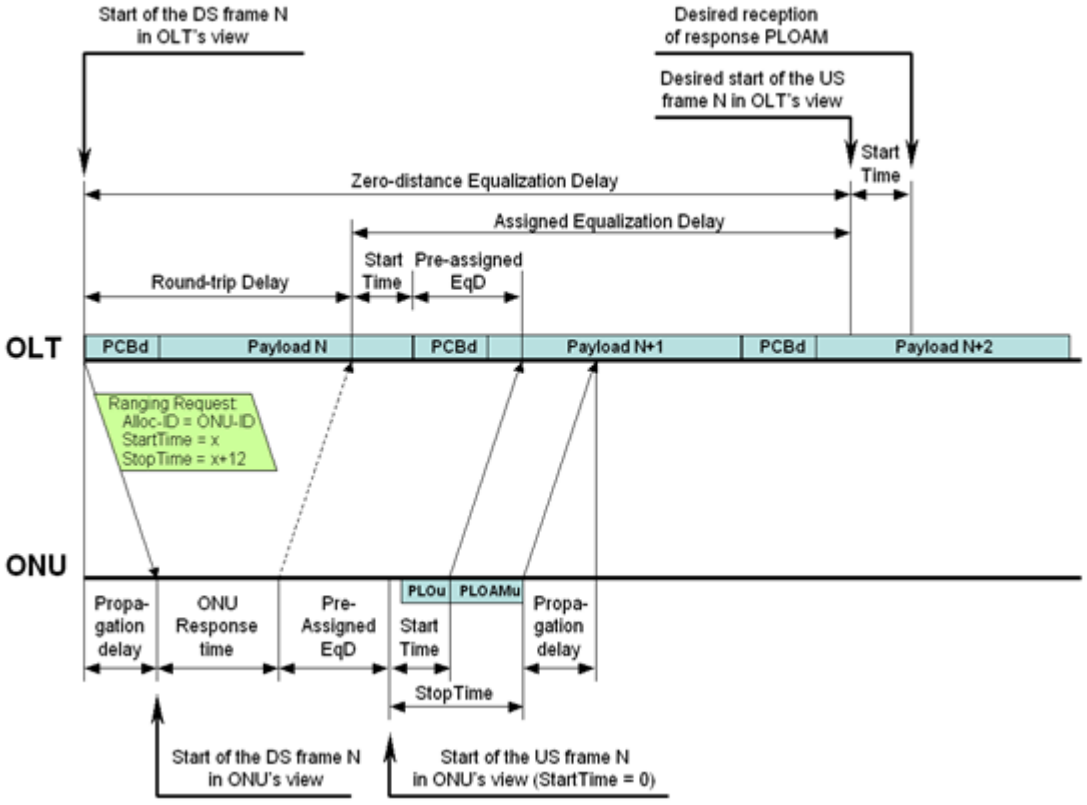
- ONU 根据 OLT 的需求调节发送光功率级别。
- OLT 发现一个新 ONU 的序列号。
- OLT 分配一个 ONU-ID 给 ONU。
- OLT 测量从 ONU 发来的上行数据的相位。
- OLT 通知 ONU 补偿延时时间。
- ONU 根据通报值调节发送相位。

GPON 的测距方法

对于 GPON 系统来说，ONU 发送数据到 OLT 是采用 TDMA 方式的。也就是在同一时刻，OLT 一个 PON 口下的所有 ONU，只有一个 ONU 在发送数据。否则，会发生传输的数据冲突。为避免这种冲突，所有 ONU 发送数据的时间必须由 OLT 控制。由于 OLT 与其相连接的 ONU 距离不同，信号在光纤中的延时（RTD：Round Trip Delay）也不同，因此，必须测出每个 ONU 与 OLT 的逻辑距离，以便计算出每个 ONU 的补偿延时（EqD：Equalization Delay）。每个 ONU 以下行数据相位为基准，根据所分配的补偿延时（EqD）对上行数据延时发送，使各 ONU 上行数据不冲突。

测距的方法是：OLT 通过测距（Ranging）过程获取 ONU 的均衡时延（RTD：Round Trip Delay），然后通过计算得出每个 ONU 的补偿延时（EqD：Equalization Delay），使得所有 ONU 的 Teqd=RTD+EqD 相等。Teqd 又称补偿循环往返延时，其值是系统预先设置的，会大于等于逻辑距离最远的 ONU 的 RTD。测距方法如图 3-13 所示。

图 3-13 GPON 测距方法



- Pre Assigned EqD：ONU 预置的默认 EqD。
- Zero-distance Equalization Delay：就是系统设置的 Teqd。
- Assigned Equalization Delay：就是 ONU 正常工作时的 EqD。

3.7 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）
GPON	Gigabit-capable Passive Optical Network（千兆比特无源光网络）

缩略语	全称
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）

4 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。

4.1 介绍

4.2 参考标准和协议

4.3 可获得性

4.4 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。

4.5 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。

4.6 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。

4.7 二层转发策略
MDU 支持两种二层转发策略，一种是根据 VLAN 转发报文，即 SVLAN ＋ CVLAN 转发，另一种是根据报文的 VLAN 信息和 MAC 地址进行转发，即：VLAN ＋ MAC 转发。

4.8 术语与缩略语

4.1 介绍

MA5631 提供的宽带二层特性如表 4-1 所示：

表 4-1 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。
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	MDU 支持两种二层转发策略，一种是根据 VLAN 转发报文，即 SVLAN ＋ CVLAN 转发，另一种是根据报文的 VLAN 信息和 MAC 地址进行转发，即：VLAN ＋ MAC 转发。

4.2 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 4-2 所示：

表 4-2 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
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

4.3 可获得性

版本支持

表 4-3 二层特性的版本支持

产品	支持版本
MA5631	V800R308C02

其他

设置二层转发模式为 SVLAN ＋ CVLAN 转发的约束条件为：

- VLAN 不能为保留 VLAN。
- 如果为 Standard VLAN，则该 VLAN 属性必须为 QinQ。
- 如果为 Smart VLAN，则该 VLAN 属性必须为 Stacking 或 QinQ。
- VLAN 上未建立 Service port。
- VLAN 上未启动 PPPoE 单 MAC 功能。
- VLAN 上未启动防御 MAC 地址欺骗功能。

4.4 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。

4.4.1 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。

4.4.2 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（默认为 600）。
- 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 CNU 功能。

4.4.3 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。
- 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。

4.5 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。

4.5.1 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

  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 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 管理使运营商可以灵活地规划业务。

4.5.2 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 4093 个 VLAN。
- 系统支持基于端口划分的 VLAN。
- 支持 Stacking VLAN。

4.5.3 原理描述

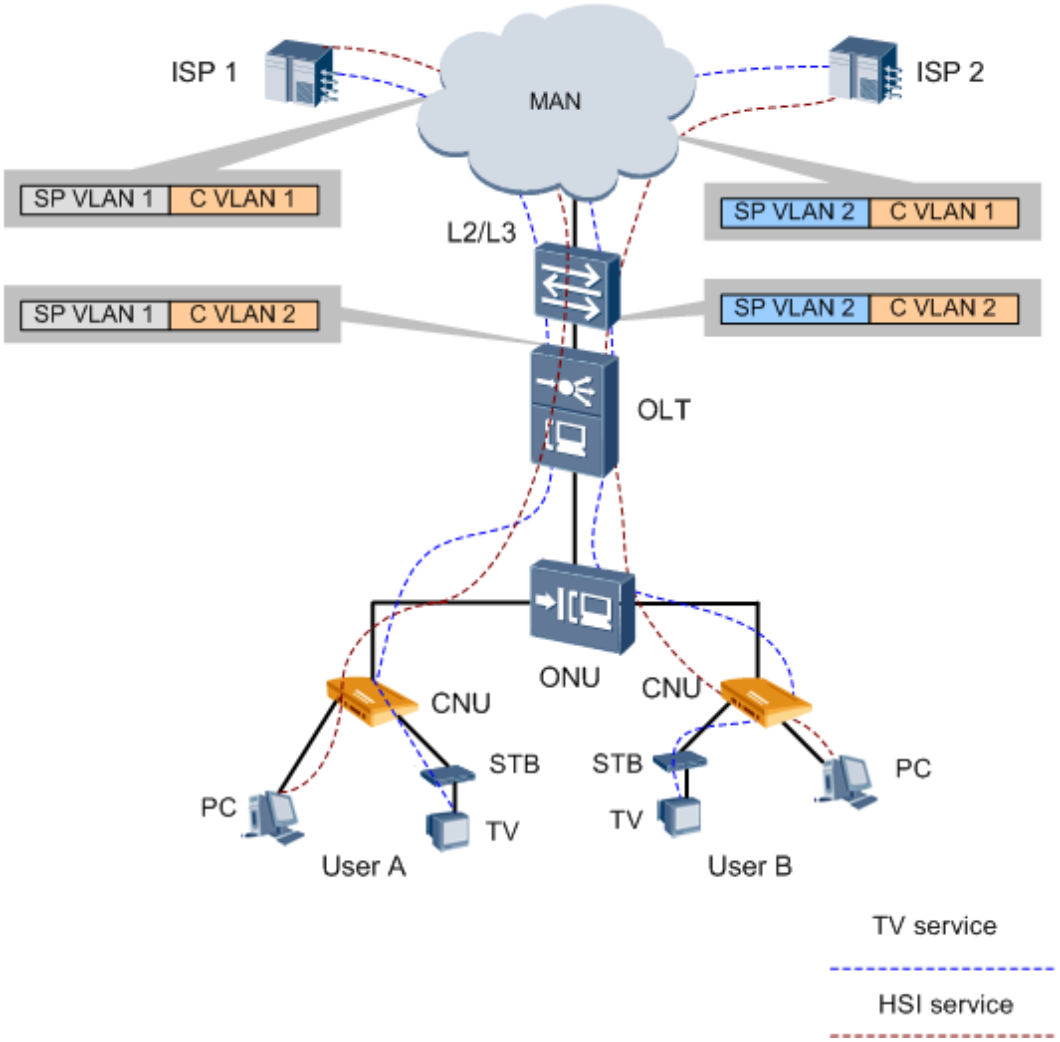
Stacking VLAN

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 4-1 所示。

图 4-1 Stacking 业务示意图



ONU 通过不同 VLAN Stacking 将用户 A 接入 ISP1，用户 B 接入 ISP2。业务的处理过程如下：

1. 用户上行发送 Untagged 报文，经过 CNU 后到达 MDU。
2. ONU 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。
   - 用户 A 的报文外层统一封装 SP VLAN1，内层封装对应的 Customer VLAN。
   - 用户 B 的报文外层统一封装 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，根据内层标签区分用户的不同业务。

4.6 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。

4.6.1 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。

4.6.2 规格

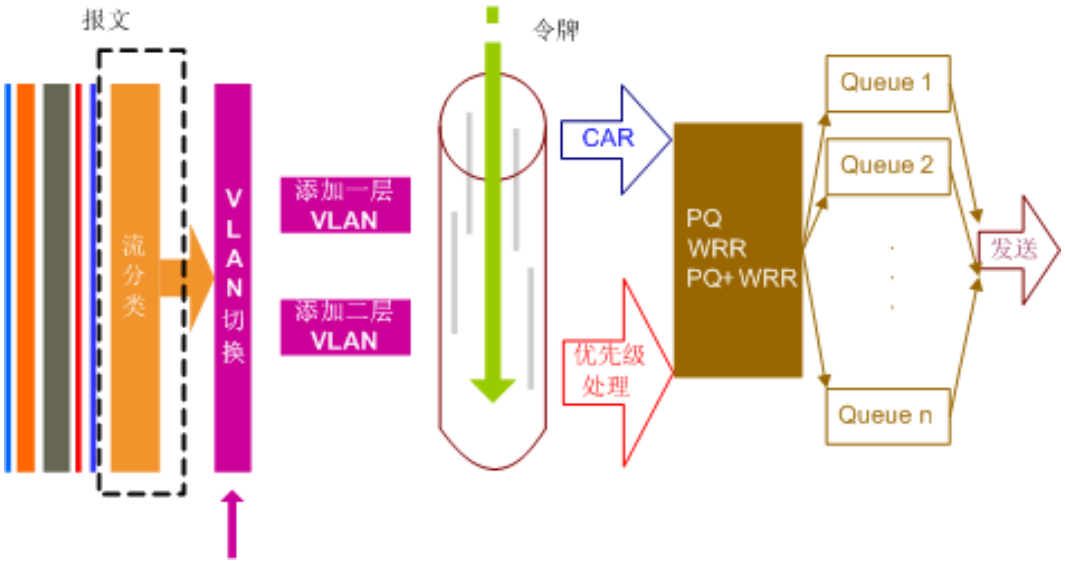
VLAN 切换特性的相关规格如下：

- 支持添加一层 VLAN。
- 支持添加两层 VLAN。

4.6.3 原理描述

如图 4-2 所示，报文进行流分类后需要进行 VLAN 切换。

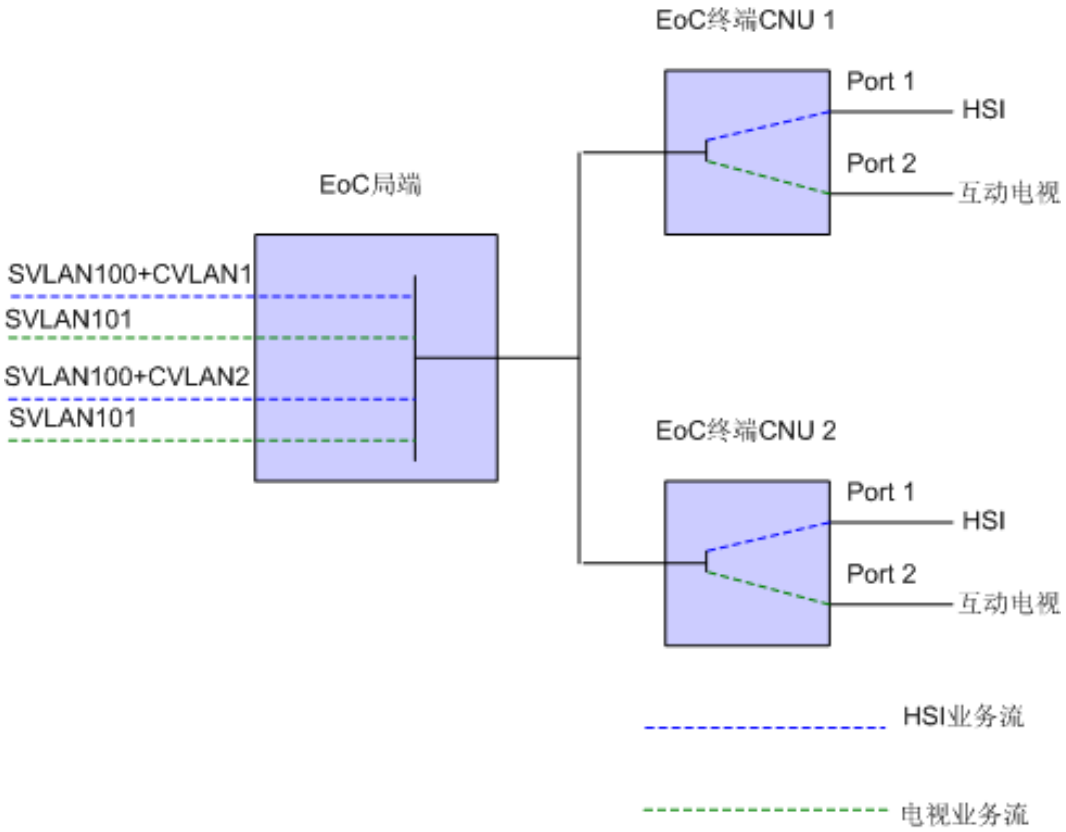
图 4-2 MDU 中 QoS 处理整体模型-VLAN 切换



MA5631 支持端到端建流，支持的 VLAN 切换策略为：untagged->SVLAN 或 SVLAN +CVLAN。

从 CNU 到 MA5631 的 VLAN 切换如图 4-3 所示。CNU 用户侧的 HSI 和互动电视业务流不带 VLAN tag。MA5631 上做 VLAN 切换，为这两条业务流打上 SVLAN tag 或 SVLAN+CVLAN 两层 tag，然后再向 OLT 传送带 VLAN tag 的业务流。

图 4-3 VLAN 切换



4.7 二层转发策略

MDU 支持两种二层转发策略，一种是根据 VLAN 转发报文，即 SVLAN ＋ CVLAN 转发，另一种是根据报文的 VLAN 信息和 MAC 地址进行转发，即：VLAN ＋ MAC 转发。

4.7.1 介绍

定义

MDU 支持两种二层转发策略，一种是根据 VLAN 转发报文，即 SVLAN ＋ CVLAN 转发，另一种是根据报文的 VLAN 信息和 MAC 地址进行转发，即：VLAN ＋ MAC 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。

4.7.2 原理描述

VLAN+MAC 转发

VLAN+MAC 地址转发是指报文进入单板时，系统自动学习 VLAN、源 MAC 地址和入端口的对应关系；向外转发时，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。

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。

4.8 术语与缩略语

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）

5 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。

5.1 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	流分类指根据用户以太报文特征和一定规则，对报文进行分类，从而区分不同的业务，进行不同的处理和提供不同的服务。
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（Service Level Agreement），明确各种服务参数。为了保证用户流量能够符合 SLA，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。

5.2 QoS 整体模型

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。

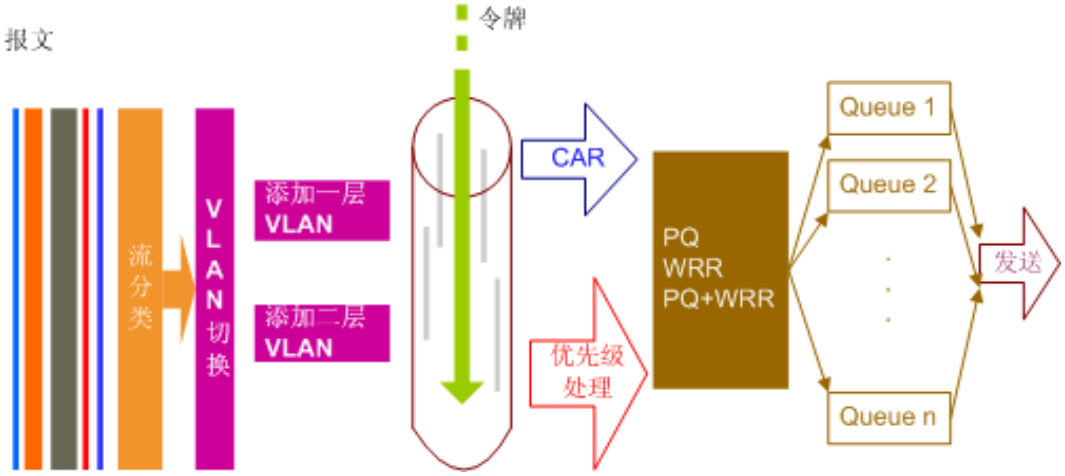
DiffServ 模型由许多在网络节点上实现的功能实体组成，包括每一跳转发行为集合、流分类功能、流量调节功能。其中流量调节功能又包括测量（metering）、标记（marking）、整形（shaping）和监管（policing）。DiffServ 模型只在网络的边界节点上实现复杂的分类和调节功能。通过在 IPv4 和 IPv6 包头的 DS 域做适当的优先级标记（IP Precedence），把业务流聚类为行为集合 BA（Behavior Aggregate），然后根据所做的标记，采取不同的转发行为。

MDU 中实现 QoS 的技术主要有如下几个方面：

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

MDU 的 QoS 整体模型如图 5-1 所示：

图 5-1 QoS 整体模型



MDU 的 QoS 处理过程包括：

- 流分类：根据用户以太报文的特征对用户业务进行区分，针对不同的业务实现不同的 QoS 保证。
- 优先级处理：针对不同的业务流设置优先级处理策略，在设备上产生拥塞或者上行网络产生拥塞时可根据优先级进行调度。
- 流量监管：流量监管用于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。从而使端口达到一个相对稳定的速率，避免给下一级设备造成冲击。通常使用 CAR 来限制某类报文的流量。
- 拥塞管理：拥塞管理是针对出端口报文进行管理，通过队列调度实现不同的优先级报文进行不同的优先级队列调度，达到设备流量管理的目的。如常用的 PQ，WRR 等算法。
- ACL 策略：通过配置的一系列匹配规则对特定的数据包进行过滤，并对识别出来的对象根据预先设定的策略允许或禁止相应的数据包通过。ACL 过滤数据包过程是在为 QoS 处理做准备，与 QoS 策略共同提高系统的安全性。

5.3 可获得性

版本支持

表 5-1 QoS 特性的版本支持

产品	支持版本
MA5631	V800R308C02

5.4 流分类策略

流分类指根据用户以太报文特征和一定规则，对报文进行分类，从而区分不同的业务，进行不同的处理和提供不同的服务。

5.4.1 介绍

定义

流分类指根据用户以太报文特征和一定规则，对报文进行分类，从而区分不同的业务，进行不同的处理和提供不同的服务。

目的

流分类的目的是区分业务流，为用户的各种业务提供不同的 QoS 保证。系统基于业务流完成业务映射，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、队列调度等。

5.4.2 规格

流分类策略的相关规格如下：

系统最大支持的业务流数量为 2000。

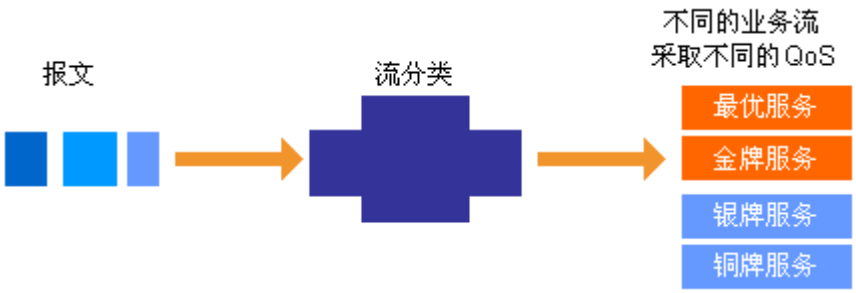
5.4.3 原理描述

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，提供不同的 QoS 服务。

流分类处理过程如图 5-2 所示。

图 5-2 流分类处理过程



5.5 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。

5.5.1 介绍

定义

MA5631 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。

5.5.2 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。

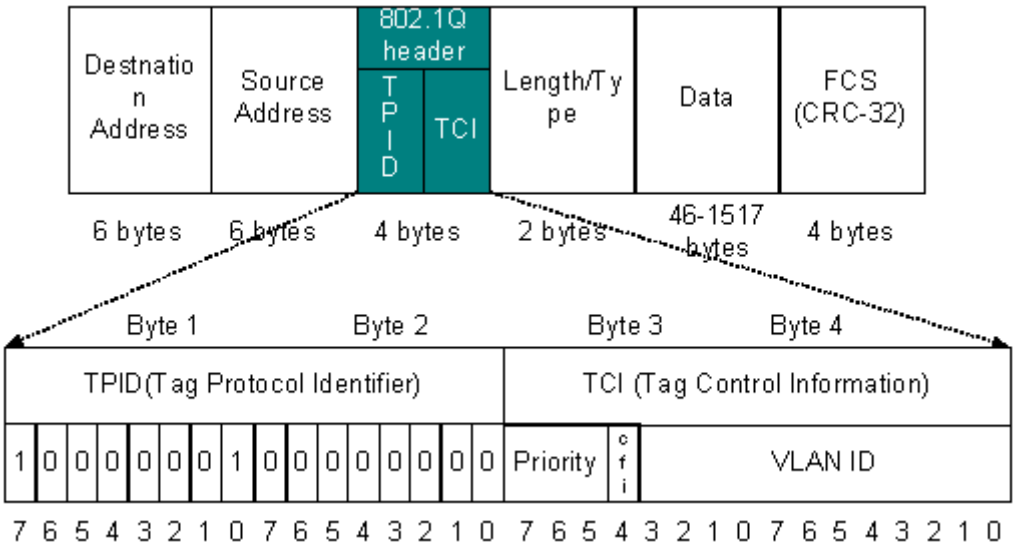
5.5.3 原理描述

优先级处理可以按照一定规则对 802.1p 优先级重新标记。优先级处理为队列调度做准备。MA5631 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。

802.1p 优先级和 IP 优先级

1. 802.1p 优先级

图 5-3 802.1Q 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。

2. TOS

   在 IP 协议定义中，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 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 MxU 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。

SVLAN 优先级处理原则

MA5631 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 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。

5.6 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（Service Level Agreement），明确各种服务参数。为了保证用户流量能够符合 SLA，需要对用户流量进行监管。

5.6.1 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。

5.6.2 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。

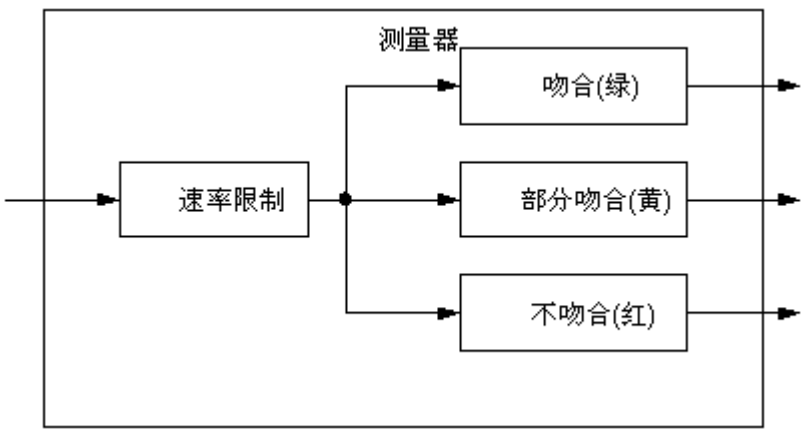
5.6.3 原理描述

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（Committed Access Rate）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。

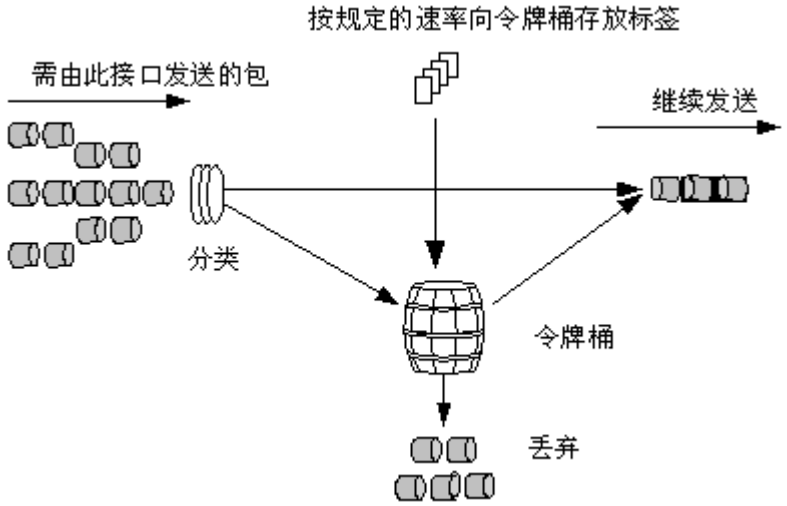
为了测量客户的实际流量，首先需要做的是基于时间的流量测量，通过实际流量与 SLA 的吻合水平，决定采用何种策略，比如是否丢弃，或者着色。

图 5-4 一个测量器的例子



CAR 是流量控制的最常用的测量和丢弃工具。CAR 利用令牌桶 TB（Token Bucket）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，并减少令牌数；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 5-5 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。

5.7 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。

5.7.1 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。

5.7.2 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 5-2 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 5-2 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。

5.7.3 原理描述

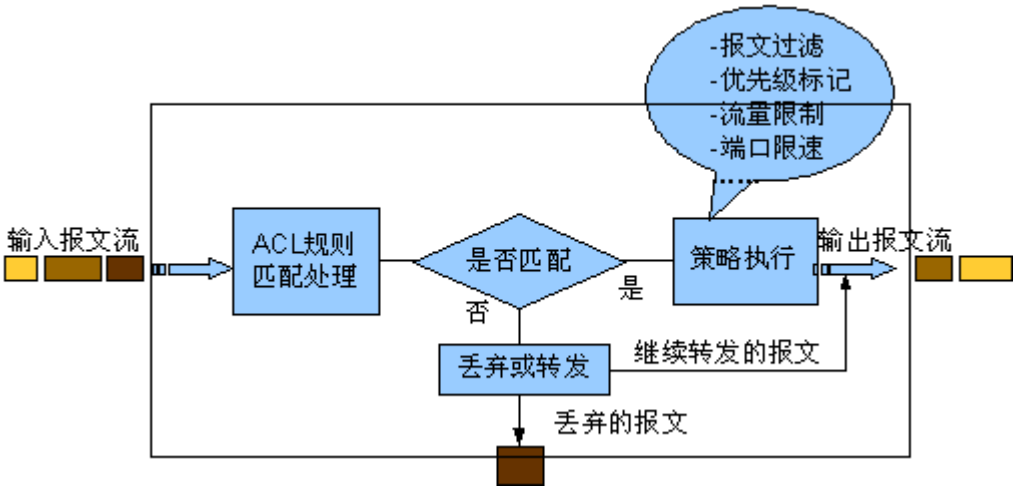
系统对输入的报文流将按照 ACL 所定义的规则进行匹配处理：

- 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 5-6 ACL 规则过滤处理原理图



5.8 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。

5.8.1 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。

5.8.2 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。

5.8.3 原理描述

MA5631 设备产生拥塞时采用队列调度的方式处理拥塞。

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
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

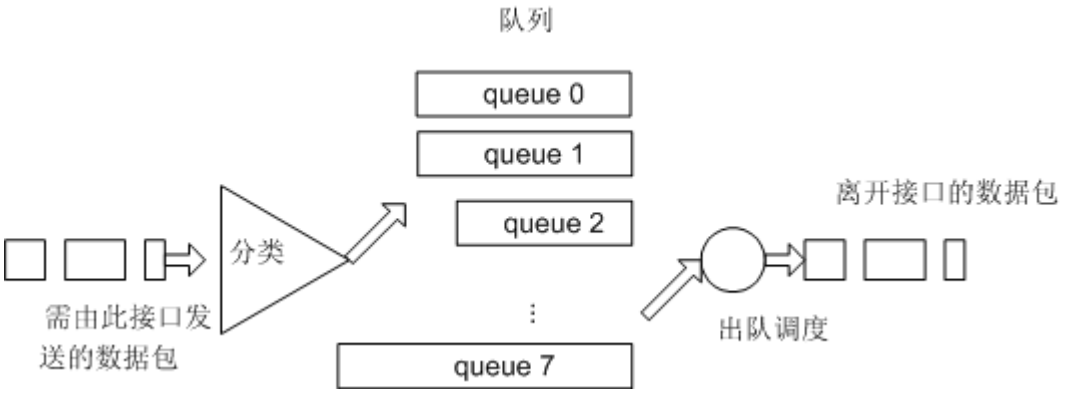
PQ

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。

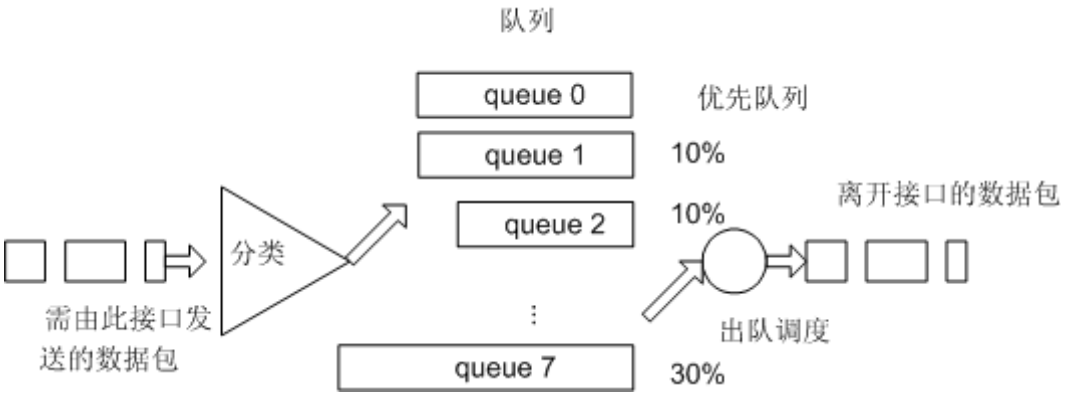
图 5-7 优先队列（Priority Queuing, PQ）



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 5-8 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。

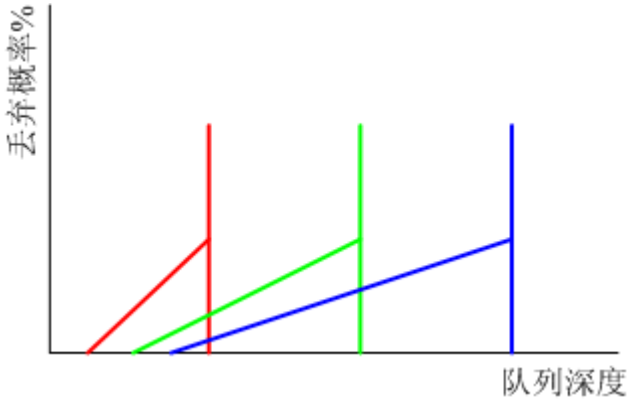
WRED

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 5-9 WRED 队列丢弃管理



拥塞管理

- MA5631 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。

- MA5631 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。

5.9 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）
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）

6 组网保护

关于本章

介绍系统实现的各种组网保护特性。

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 环网检测
介绍环网检测特性的定义、目的、规格和原理。

6.8 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。
环网检测特性	环网检测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，MxU 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

6.3 可获得性

版本支持

表 6-1 组网特性的版本支持

产品	支持版本
MA5631	V800R308C02

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。

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

MA5631 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

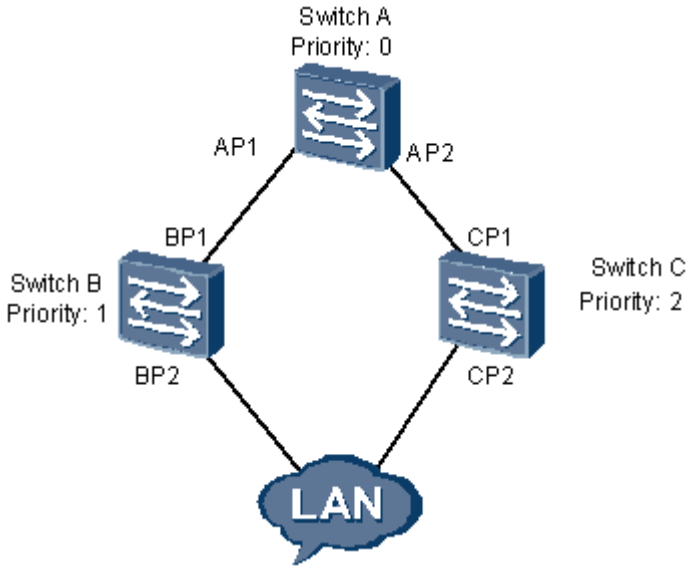
STP 基本原理

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。

MA5631 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。

  MA5631 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 MA5631 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

MA5631 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，如所示，介绍手工链路聚合的实现原理。

MA5631 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，MA5631 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，MA5631 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。

MA5631Switch 之间通过 LACP 协议交互聚合组信息如所示。

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。
  MA5631 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

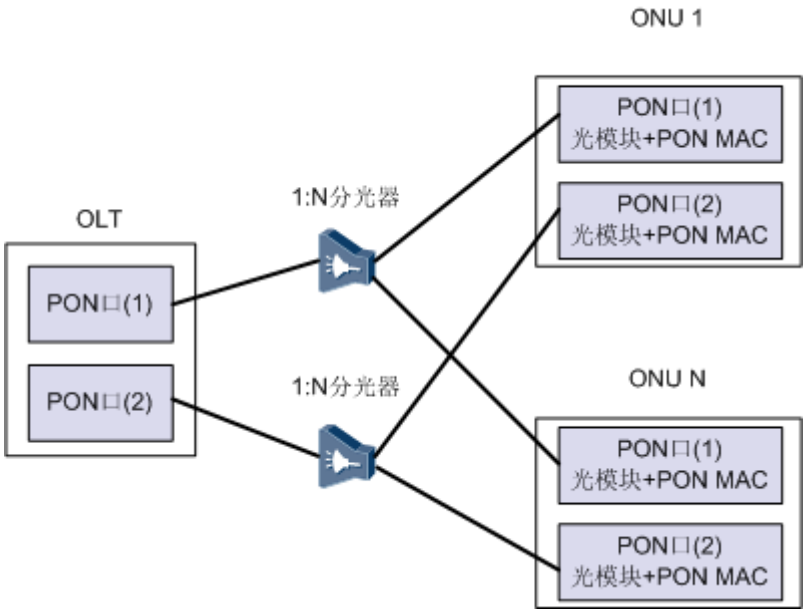
- 要求符合中国电信 CTC2.1 标准中有关 TYPE D 保护倒换的具体要求，倒换交互协议上兼容 CTC2.1 要求的 OAM 扩展消息，二层转发业务在倒换时的中断时间小于 50ms。满足光链路保护倒换准则，即输入光信号丢失或输入通道信道劣化触发自动倒换。
- 只支持主备保护倒换工作模式。
- 要支持此特性，与 MA5631 对接的对端 OLT 设备必须支持此特性，目前只有 MA5600T 支持 EPON TYPE D 保护倒换功能。
- 由于 MA5631 只有两个上行 PON 端口，默认为一个保护组，不需要用户设置保护组，并且不支持用户对保护组操作，只提供查询 PON 端口主备状态和保护倒换原因的功能。

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 MA5631 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 6-2 所示。

图 6-2 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 环网检测

介绍环网检测特性的定义、目的、规格和原理。

6.7.1 介绍

定义

环网检测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环网检测报文，检测运营商网络是否形成环路。如果网络中有环路产生，MA5631 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

环网检测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

环网检测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。

6.7.2 规格

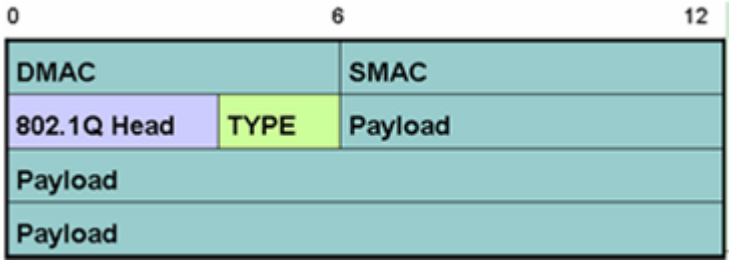
- 支持使能或去使能环网检测特性。
- 支持用户端口自环检测、用户端口之间的环路检测、用户端口和网络侧端口之间的环路检测。
- 支持环网检测特性协议类型可配置。

6.7.3 原理描述

实现原理

环网检测特性是通过设备在用户端口周期性发送环网检测报文，监控用户侧和网络侧收到的环网检测报文，检测运营商网络是否形成环路。其报文格式如图 6-3 所示。

图 6-3 环网检测报文格式



- 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。

环网检测过程

- 系统使能环网检测特性后，定时向用户端口发送自定义的广播报文，每秒发送 16 个环网检测报文。并且只对流状态为 Up 的流索引发送环网检测报文。
- 通过设备在用户端口周期性发送环网检测报文，实时监控用户侧和网络侧收到的环网检测报文，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，由系统自动或用户手动去激活形成环路的用户端口或 CNU，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，手动激活用户端口或 CNU。系统也支持配置重新自动激活时间，即超过重新自动激活时间后，系统自动激活用户端口或 CNU。
- 用户端口或 CNU 重新激活后，系统自动对用户端口或 CNU 进行环网检测。

6.8 术语与缩略语

术语

表 6-2 组网保护特性术语表

术语	解释
手工链路聚合	完全由用户手工创建聚合组，手工增删成员端口，不运行 LACP 协议，聚合组内成员端口有 down 和 up 两种物理状态。
VLAN 映射表	VLAN 和生成树的对应关系表。
多生成树域（MSTR）	由交换网络中的多台交换机以及它们之间的网段所构成，这些交换机都启动了 MSTP、具有相同域名，具有相同 VLAN 到生成树映射配置，具有相同 MSTP 修订级别配置，并且物理上直接相连。
内部生成树（IST）	内部生成树，是多生成树域内的一棵生成树，它和公共生成树共同构成整台交换机网络的生成树，是公共和内部生成树在一个多生成树域中的片段。

术语	解释
公共生成树（CST）	公共生成树连接交换网络内所有多生成树域的单生成树。如果把每个多生成树域看作是一个“交换机”，公共生成树就是这些“交换机”通过 STP 协议、RSTP 协议计算生成的一棵生成树。
公共和内部生成树（CIST）	由 IST 和 CST 共同构成，是连接一个交换网络内所有交换机的单生成树。
多生成树实例（MSTI）	一个多生成树域内可以通过 MSTP 生成多棵生成树，各棵生成树之间彼此独立。每棵生成树都称为一个 MSTI，即多生成树实例。

缩略语

表 6-3 组网保护特性缩略语表

缩略语	全称
STP	Spanning Tree Protocol（生成树协议）
MSTP	Multiple Spanning Tree Protocol（多生成树协议）
IST	Internal Spanning Tree（内部生成树）
CST	Common Spanning Tree（公共生成树）
CIST	Common and Internal Spanning Tree（公共和内部生成树）
MSTI	Multiple Spanning Tree Instance（多生成树实例）
LACP	Link Aggregation Control Protocol（链路聚合控制协议）

7 用户安全

关于本章

首先从介绍、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
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

版本支持

表 7-1 用户安全特性的版本支持

产品	支持版本
MA5631	V800R308C02

涉及网元

PITP 与 RAIO 共同配合使用，需要 MA5631、BRAS 和 RADIUS Server 配合完成。对这些网元的要求如表 7-2 所示。

表 7-2 PITP 特性对网元要求

MA5631	BRAS	RADIUS Server
√	√	√

DHCP Option82 与 RAIO 共同配合使用，需要 MA5631、DHCP 中继代理或者 DHCP 服务器配合完成。

表 7-3 DHCP Option82 特性对网元要求

MA5631	DHCP 中继代理或者 DHCP 服务器
√	√

防御 MAC Spoofing、防御 IP Spoofing 和用户隔离特性只涉及 MA5631 设备，不涉及其他网元。

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

- 仅用户口支持 PITP、DHCP Option82，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

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，可实现对用户帐号与接入位置信息的绑定认证，避免用户帐号的盗用与漫游。

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：

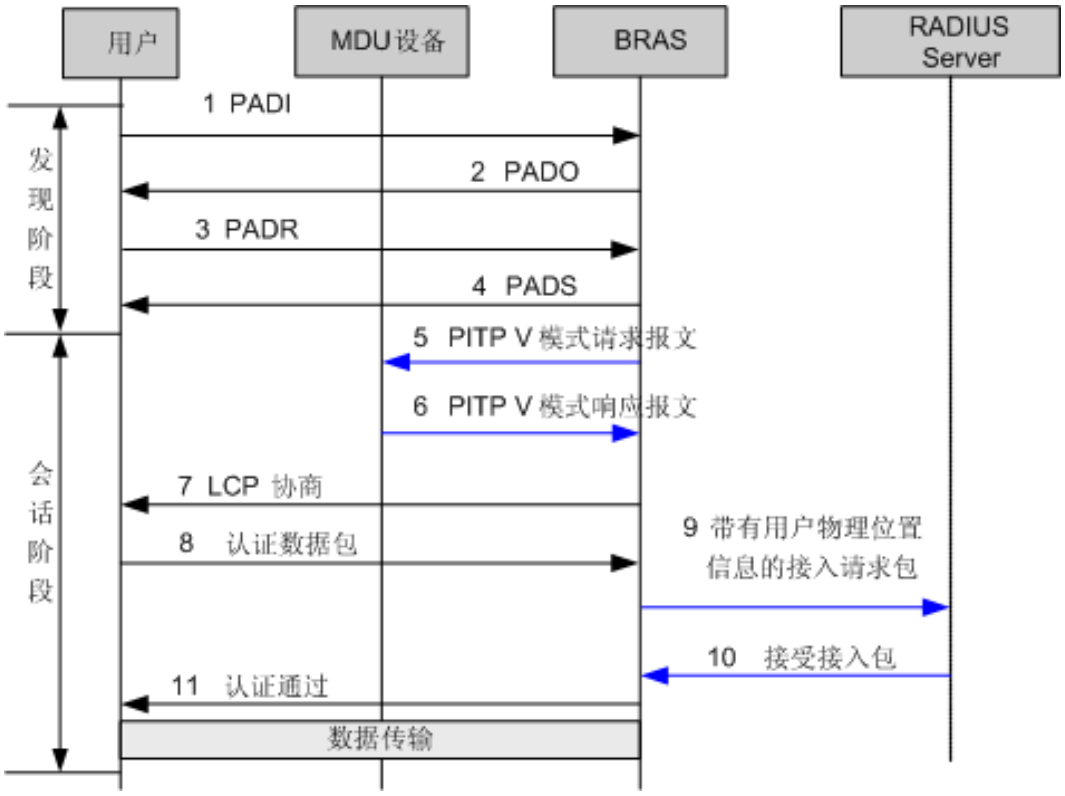
- PITP 支持两种模式：PITP P 模式 PITP V 模式。
- PITP 开关分为两级：系统级开关和 VLAN 级开关。只有两个级别的开关同时开启，接入设备才会向 BRAS 提供用户物理位置信息。
- PITP 系统级开关缺省关闭，VLAN 级开关缺省开启。

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



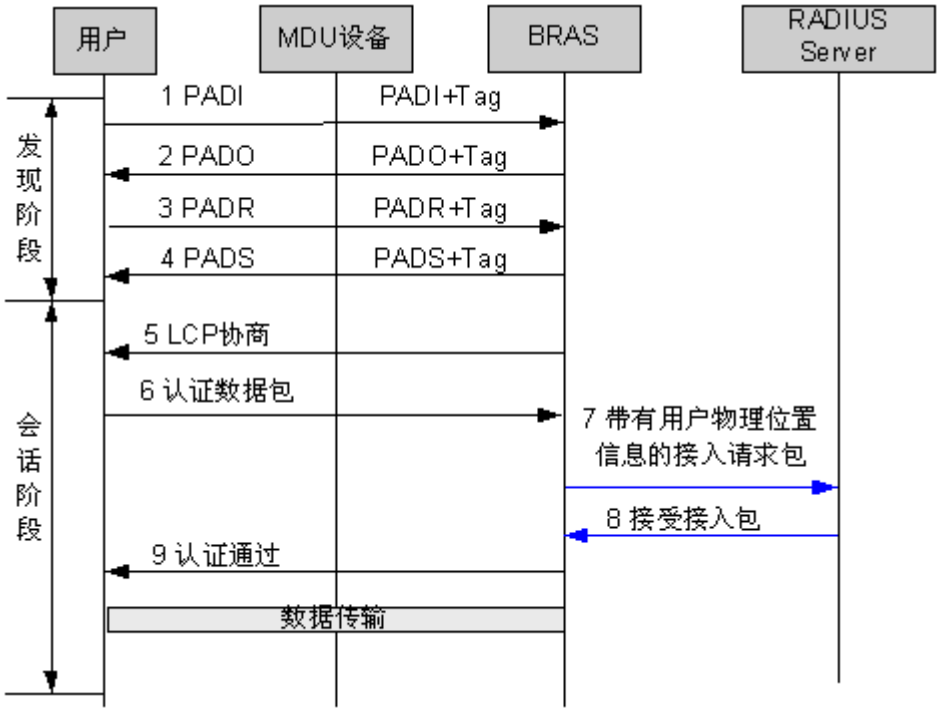
PITP V 模式的三个过程为：

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

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

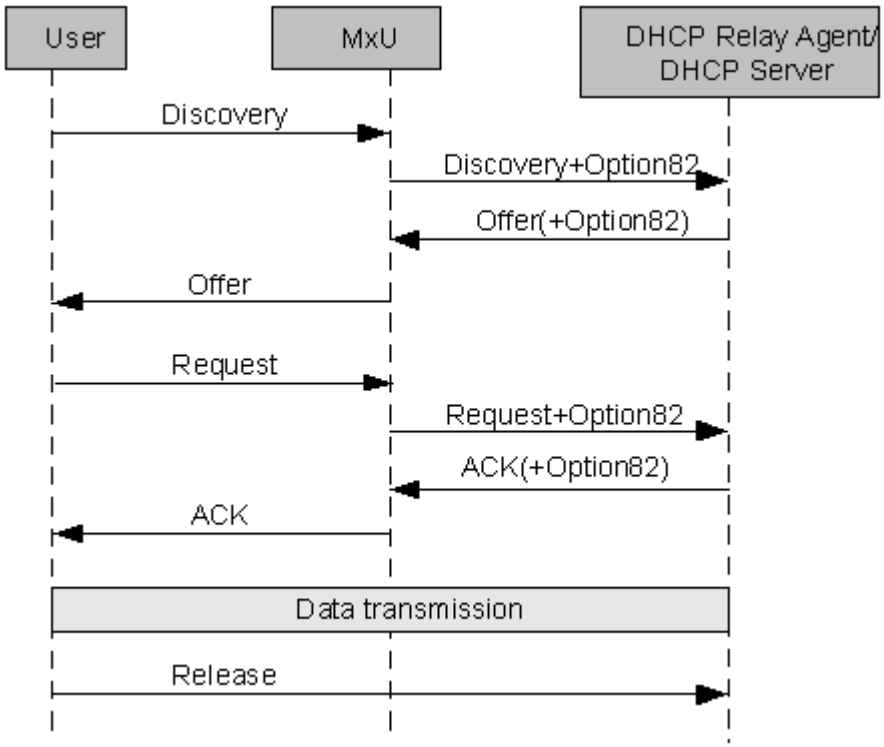
DHCP Option82 开关分为两级：全局级和 VLAN 级。只有各个级别开关全部打开，系统才会在上行的 DHCP 报文中添加 Option82 信息。

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。

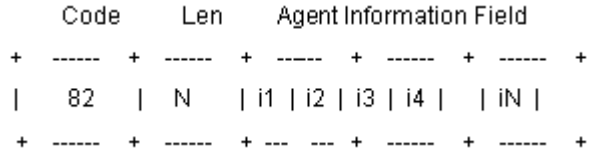
DHCP Option82 报文格式

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



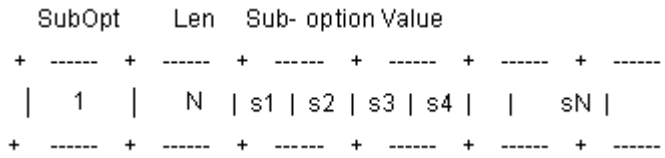
DHCP Option82 报文各字段具体含义，如表 7-4 所示。

表 7-4 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

RAIO 工作模式包括：Common、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 7-5** 所示。

表 7-5 不同接入方式的 CID 格式

接入方式	CID 格式
EoC 接入方式	设备名 eoc 框号/槽号/子槽/端口号：cnunid

- 当设备名字段为缺省名字“MA5631”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“MA5631”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 MA5631 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 eoc 0/12/0/49：0
- RID ---------> NULL（不填）

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
eoc	EoC 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

关键字	描述	可订宽度	最大宽度
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		
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 （对应于 eoc 接入方式）	AXPI 对应于网络侧的 vlanid。	Yes	4
axci （对应于 eoc 接入方式）	网络侧 VLAN 的属性为 stacking 时： 如果用户所在业务虚端口承载的业务是根据用户侧的 VLAN ID 进行区分的，AXCI 为用户侧的 VLAN ID。 如果不是根据用户侧的 VLAN ID 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 时： 如果用户所在业务虚端口承载的业务是根据用户侧的 VLAN ID 进行区分的，AXCI 为用户侧的 VLAN ID。 如果不是根据用户侧的 VLAN ID 进行区分，AXCI 固定为 4096。	Yes	5
cnuid	EoC 线路上的 CNU ID。	Yes	4

- 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“-”
%	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，VLAN ID－2，则自定义的 CID 字符串：anid eoc slot/port:vlanid，最终生成的字符串为：“mxu01 eoc 3/15：vlan2”。

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 1024 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 1024。
  - 每条业务流最多可以绑定 8 个 MAC 地址（最多可以支持 2000 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 1024 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 1024。
  - 最多允许 2000 条业务流绑定 IP 地址，每条业务流最多绑定 8 个 IP 地址。

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

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

8.5 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。

8.6 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。

8.7 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。
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。

8.2 可获得性

版本支持

表 8-1 系统安全特性的版本支持

产品	支持版本
MA5631	V800R308C02

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

- 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，可以通过防御 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。
- 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：将发起 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 DoS 攻击出现或消失时上报相应的告警或恢复告警。
- 支持基于业务流的防 DoS 攻击。
- 支持基于框号/槽号/端口号+CNU ID 查询 DoS 攻击黑名单。

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 CNU 用户端口每秒持续送交 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 CNU 用户端口发生了 DoS 攻击。
- CNU 用户端口发生 DoS 攻击时，系统将该 CNU 用户端口加入黑名单，并禁止该 CNU 用户端口上携带相同 MAC 地址的协议报文发送到 CPU。
- 系统检测到 CNU 用户端口在一定时间内没有 DoS 攻击时，将该 CNU 用户端口从黑名单中删除，允许该 CNU 用户端口的报文发送到 CPU。

8.4 MAC 地址过滤

首先介绍 MAC 地址过滤，然后对其原理进行阐述。

8.4.1 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。

8.4.2 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。

8.4.3 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。

8.5 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。

8.5.1 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。

8.5.2 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。

8.5.3 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。

8.6 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。

8.6.1 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。

8.6.2 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。

8.6.3 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。

8.7 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
首先介绍管理用户帐号/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

特性名称	特性简介
管理系统用户帐号/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 SFTP 加密的方式。
安全事件日志	针对系统安全相关的事件进行记录。
SNMP 管理	网管与设备间交互采用 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

版本支持

表 9-1 操作维护安全特性的版本支持

产品	支持版本
MA5631	V800R308C02

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。
- 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

首先介绍管理用户帐号/口令子特性，然后对其原理进行阐述。

9.4.1 介绍

定义

帐号/口令管理是指用户通过命令行接口 CLI（Command Line Interface）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，用户模板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。

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/trace/msg-emulate/ntp/radius）。

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

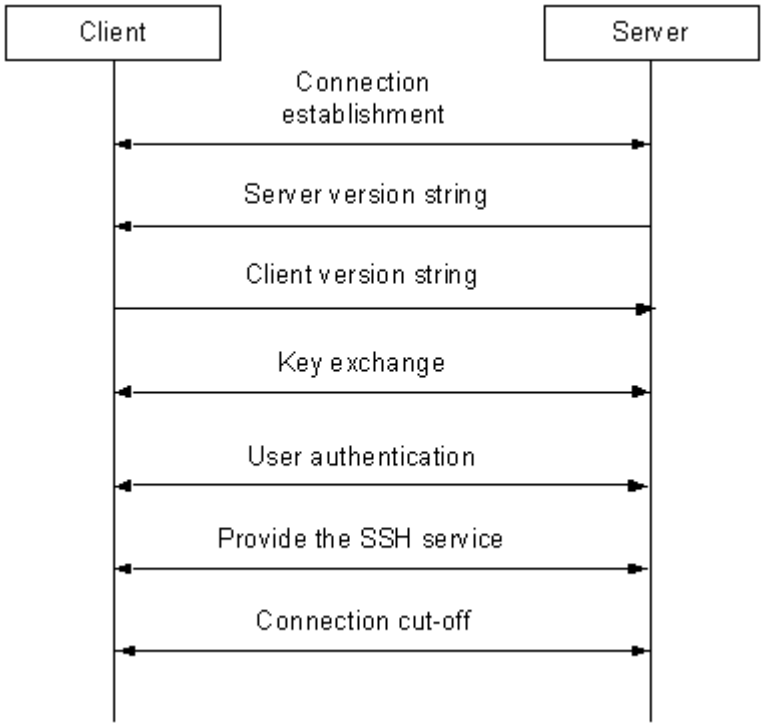
实现原理

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和退出。

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。

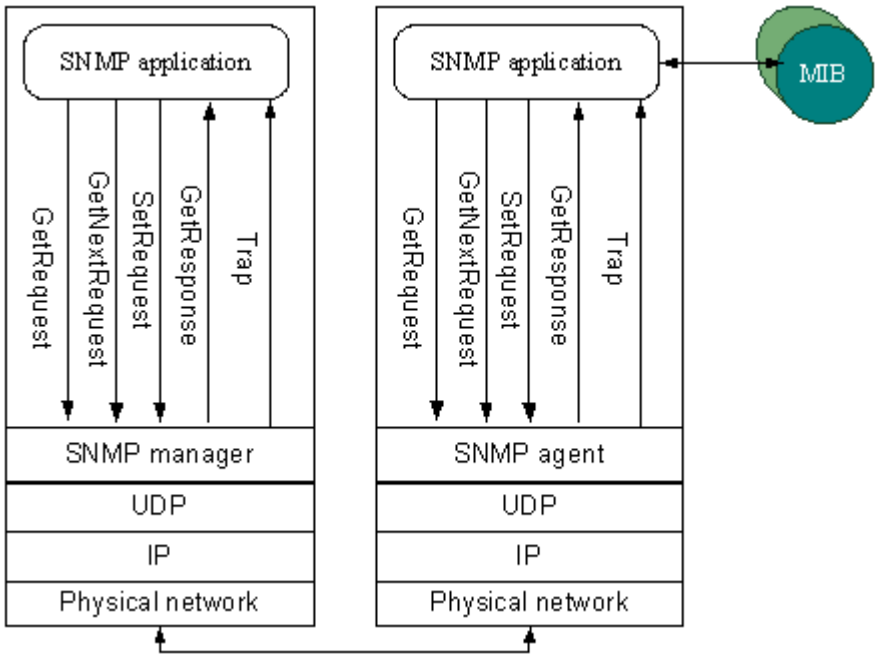
9.10.3 原理描述

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）
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

OAM 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

特性名称	特性简介
GPON 认证	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。
EPON 认证	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。
PPPoE 拨号业务仿真	指通过在 MA5631 上模拟 PPPoE 客户端的 PPPoE 拨号行为，得到 PPPoE 拨号结果。

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

版本支持

表 10-1 OAM 特性的版本支持

产品	支持版本

MA5631	V800R308C02

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。

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

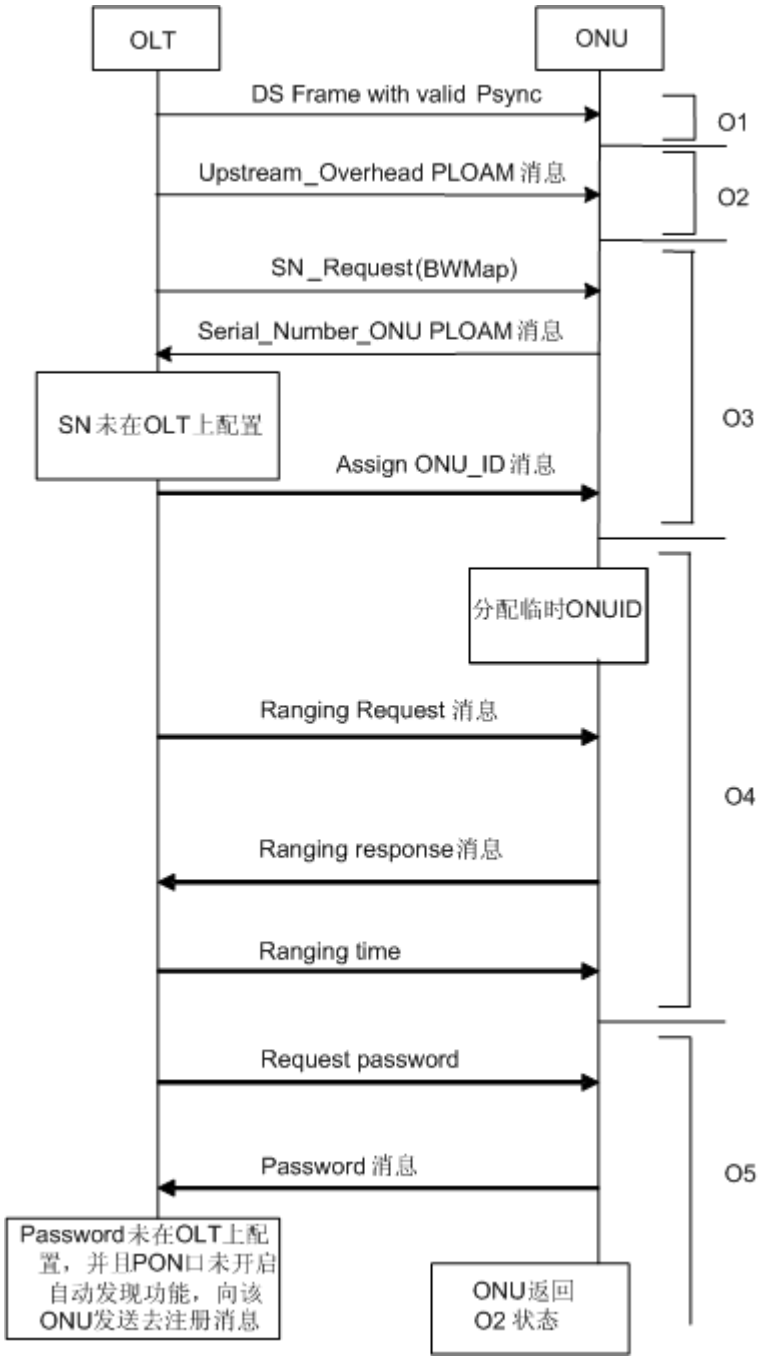
GPON ONU 的认证方式支持三种：

- 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 帐号后，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

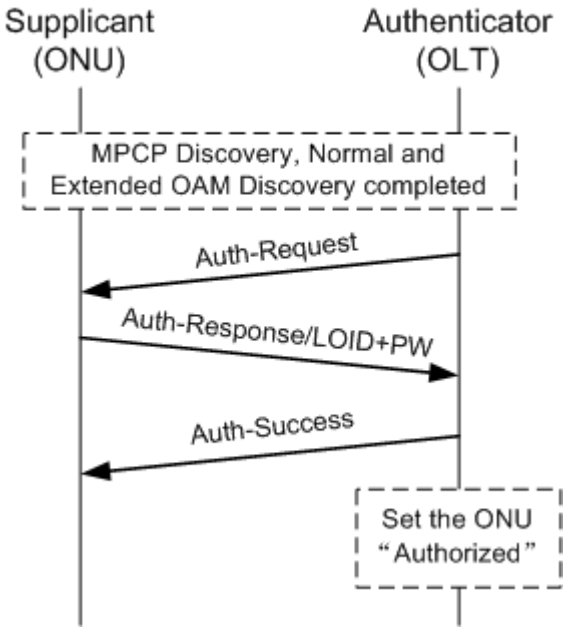
EPON 认证方式支持三种：MAC 地址认证、逻辑标识认证、password 认证。

- 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 帐号后，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 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。

10.6.1 介绍

定义

PPPoE 拨号业务仿真通过在 MA5631 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 MA5631 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。

10.6.2 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。

10.6.3 原理描述

介绍该特性的实现原理。

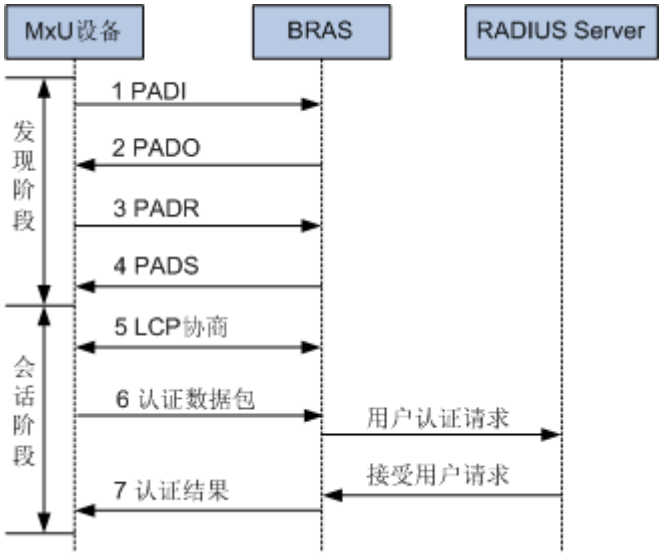
实现原理

- PPPoE 拨号业务仿真特性是指在 MA5631 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 10-3 所示。

图 10-3 PPPoE 业务仿真过程



启动 PPPoE 拨号业务仿真后，MA5631 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 MA5631 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 MA5631 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。

10.7 术语与缩略语

术语

表 10-2 OAM 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，ONU 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 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。可通过 no-aging 和 aging-time 设置规定时间。
aging-time	当 ONU 为 Once-on 模式时，对超时时间进行设置，要求 ONU 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。

缩略语

表 10-3 OAM 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 NTP

关于本章

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 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（Internet Control Message Protocol）时间戳报文演变而来，主要是从准确性和强壮性方面进行了特殊的设计。

目的

NTP 用来在整个网络内发布精确时间。

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

MA5631 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。

11.2 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

11.3 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”

11.4 可获得性

版本支持

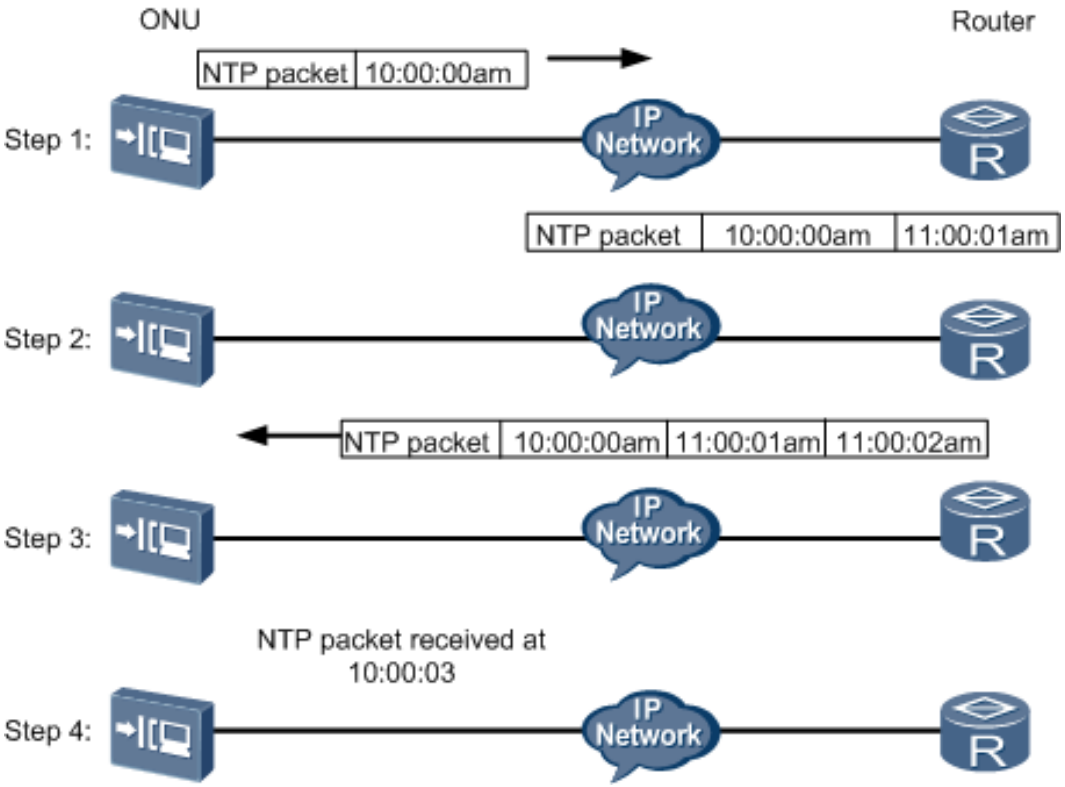
表 11-1 NTP 特性的版本支持

产品	支持版本
MA5631	V800R308C02

11.5 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. MA5631 发送一个 NTP 消息包给路由器，该消息包带有它离开 MA5631 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 MA5631 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，MA5631 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）；
- MA5631 相对 Router 的时间差 Offset=（（T2-T1）+（T3-T4））/2。

综上所述，MA5631 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。