PowerCube 500 (T672E-150G1)
V200R001C23

用户手册

文档版本 03

发布日期 2022-12-07

华为技术有限公司

版权所有 © 华为技术有限公司 2022。 保留一切权利。

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

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暗示的声明或保证。

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： https://e.huawei.com

前言

概述

本文档针对PowerCube 500的解决方案介绍、部件介绍、预防性维护、告警故障处理和部件更换等方面做了详细的描述。

本文图片仅供参考，具体结构以实物为准。

产品版本

与本文档相对应的产品版本如下所示。

产品名称	产品版本
PowerCube 500	V200R001C23
eSight	V300R010C00

读者对象

本文档（本指南）主要适用于以下工程师：

- 硬件安装工程师
- 安装调测工程师
- 现场维护工程师
- 系统维护工程师
- 销售工程师

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。

版权所有 © 华为技术有限公司

符号	说明
危险	表示如不避免则将会导致死亡或严重伤害的具有高等级风险的危害。
警告	表示如不避免则可能导致死亡或严重伤害的具有中等级风险的危害。
注意	表示如不避免则可能导致轻微或中度伤害的具有低等级风险的危害。
须知	用于传递设备或环境安全警示信息。如不避免则可能会导致设备损坏、数据丢失、设备性能降低或其它不可预知的结果。 “须知”不涉及人身伤害。
说明	对正文中重点信息的补充说明。 “说明”不是安全警示信息，不涉及人身、设备及环境伤害信息。

修订记录

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

文档版本 03(2022-12-07)

网络模块更新为T672E-P，支持SFP GPON和GE光模块上行。

文档版本 02(2020-02-07)

增加DO口的说明。

文档版本 01 (2020-01-02)

第一次正式发布。

版权所有 © 华为技术有限公司

目 录

 版权所有 © 华为技术有限公司

 版权所有 © 华为技术有限公司

 版权所有 © 华为技术有限公司

 版权所有 © 华为技术有限公司

 版权所有 © 华为技术有限公司

1 安全注意事项

1.1 通用安全

声明

在安装、操作和维护设备时，请先阅读本手册，并遵循设备上标识及手册中所有安全注意事项。

手册中的“须知”、“注意”、“警告”和“危险”事项，并不代表所应遵守的所有安全事项，只作为所有安全注意事项的补充。本公司不承担任何因违反通用安全操作要求或违反设计、生产和使用设备安全标准而造成的责任。

本设备应在符合设计规格要求的环境下使用，否则可能造成设备故障，由此引发的设备功能异常或部件损坏、人身安全事故、财产损失等不在设备质量保证范围之内。

安装、操作、维护设备时应遵守当地法律法规和规范。手册中的安全注意事项仅作为当地法律法规和规范的补充。

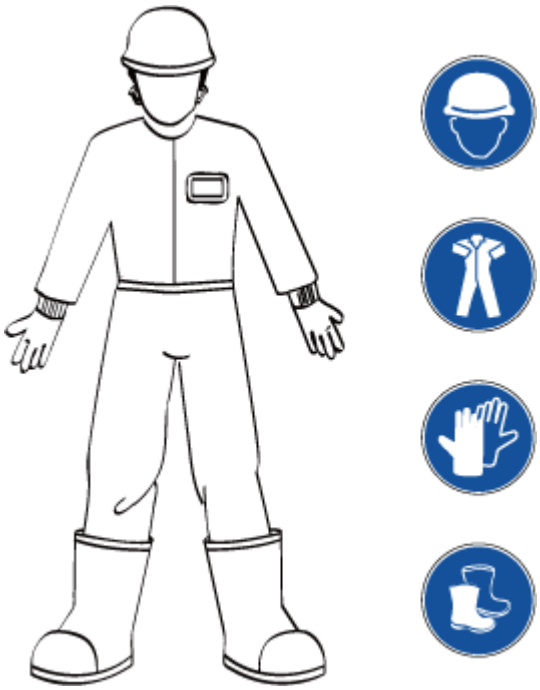
发生以下任一情况时，本公司不承担责任。

- 不在本手册说明的使用条件中运行。
- 安装和使用环境超出相关国际或国家标准中的规定。
- 未经授权擅自拆卸、更改产品或者修改软件代码。
- 未按产品及文档中的操作说明及安全警告操作。
- 非正常自然环境（不可抗力，如地震、火灾、暴风等）引起的设备损坏。
- 客户自行运输导致的运输损坏。
- 存储条件不满足产品文档要求引起的损坏。

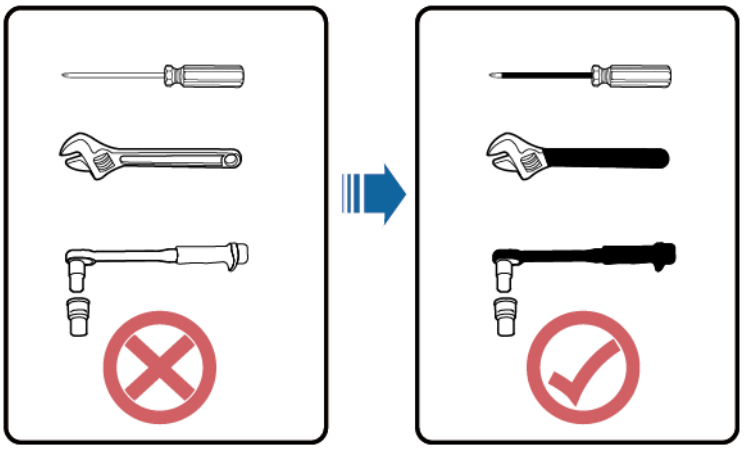
常规要求

- 安装、操作和维护时严禁佩戴手表、手链、手镯、戒指、项链等易导电物体，以免被电击灼伤。
- 安装、操作和维护过程中必须使用专用的防护用具，如佩戴绝缘手套，佩戴护目镜、穿安全服、戴安全帽、穿安全鞋等，如下图所示。

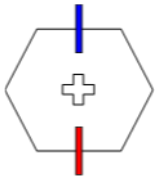
版权所有 © 华为技术有限公司



- 使用的工具手柄需要做绝缘防护处理，或使用绝缘工具，如下图所示。



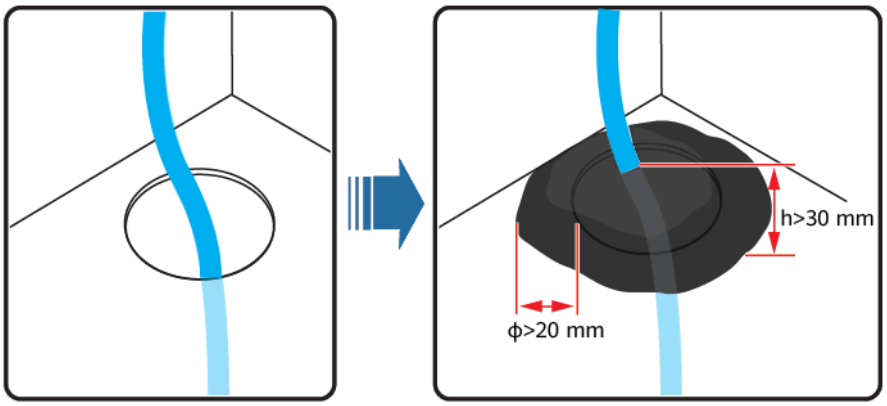
- 安装、操作和维护必须按照指导书的步骤顺序来进行。
- 应采用力矩扳手固定螺丝，并采用红蓝标识进行双重检查。安装人员确认螺丝拧紧后，在螺丝上涂蓝色标识；检查人员确认拧紧后，涂红色标识（画线标识需要跨越螺丝边缘，标识样例如下图所示）。



- 安装、操作、维护机柜时，需先清理干净机柜顶部的积水、冰雪或其他杂物，再打开机柜门，以免杂物掉入柜内。
- 严禁在雷电、雨、雪、六级大风等恶劣天气下安装、使用和操作室外设备、线缆（包括但不限于搬运设备、操作设备和线缆、插拔连接到户外的信号接口、高空作业、室外安装等）。

版权所有 © 华为技术有限公司

- 接触任何导体表面或端子之前应测量接触点的电压，确认无电击危险。
- 应确保所有槽位均有单板或者假面板在位。防止单板上危险电压和能量造成伤害的风险，保证风道正常，控制电磁干扰，并且规避背板、底板、单板落尘或其他异物。
- 安装完设备，应清除设备区域的空包装材料，如纸箱、泡沫、塑料、扎线带等。
- 如发生火灾，应撤离建筑物或设备区域并按下火警警铃，或者拨打火警电话。任何情况下，严禁再次进入燃烧的建筑物。
- 请勿停用保护装置和忽略手册、设备上的警告、警示与预防措施。及时更换因长期使用而变得不清晰的危险标志。
- 除了对设备进行操作的人员，其他人员请勿接近本设备。
- 走线孔均需做密封处理，用防火泥封堵已走线的走线孔，使用机柜自带的盖子封堵未走线的走线孔，正确的防火泥封堵施工标准如下图所示。



- 禁止用水、酒精或油等溶剂清洗机柜内部及外部的电气零部件。

人身安全

- 在设备操作过程中，如发现可能导致人身伤害或设备损坏的故障时，应立即终止操作，向负责人进行报告，并采取行之有效的保护措施。
- 为避免电击危险，禁止将安全特低电压（SELV）电路连接到通信网络电压（TNV）电路上。
- 设备未完成安装或未经专业人员确认，请勿给设备上电。

符号声明

为保障人身和设备安全，在安装、操作和维护设备时，请遵循设备上标识的安全注意事项。

符号	说明
	裸露高压部件的标识，此标识警告操作人员与电网供电电压直接接触，或者通过潮湿的物品或潮气间接地与电网电压接触将是致命的。该标识粘贴在危险电压处，或者维护时可能移走的电源保护盖上面。

版权所有 © 华为技术有限公司

符号	说明
	过热警示标识，此标识贴在可能出现高温引起烫伤的设备表面，警告使用者在操作、维护时不要随意触摸，请佩戴防烫手套进行操作，以免发生烫伤。
 或 	保护接地标识，此标识贴在保护接地端子附近，在设备和外部接地网络相连接的端子旁边使用。设备接地线从保护接地端子处连到外部接地排。
	等电位连接标识，此标识用于等电位连接端子，即设备内部各个等电位端子旁边。
	静电标识，在任何静电敏感区域使用此标识。看到此标识的情况下，请佩戴防静电手套或者手环后，再对设备进行操作。
 或	电容有危险能量。断开所有电源1分钟后方可打开机箱。
	海拔说明标识，仅适用于海拔2000米以下地区安全使用。
	非热带气候说明标识，仅适用于非热带气候条件下安全使用。
 或	风扇盒上/运动部件上的标识，该标识丝印或者贴在风扇盒面板上，警告操作人员不要用手指靠近。“严禁在风扇旋转时接触扇叶！”
 或	看说明书标签，此标识在设备端口处无法表达清楚用途时使用。指导使用者参考说明书中的内容。举例，可以在下面情况时使用看说明书标签，但不局限于如下场景： 1. 对于多电源设备，在电源附近使用，替代多电源标识。意思是：此设备有多路电源输入，设备断电时必须断开所有电源输入。 2. 对于有多个输出接口，在输出接口附近使用。请参考说明书中电源输出的额定值、配置参数信息进行连接。 3. 对于有多个槽位，在槽位信息附近使用。请参考说明书中槽位信息的说明，对单板的限制以及使用条件。

版权所有 © 华为技术有限公司

1.2 人员要求

- 负责安装维护设备的人员，必须先经严格培训，了解各种安全注意事项，掌握正确的操作方法。
- 只允许有资格的专业人员或已培训人员安装、操作和维护设备。
- 只允许有资格的专业人员拆除安全设施和检修设备。
- 对设备进行操作的人员，包括操作人员、已培训人员、专业人员应该有当地国家要求的特种操作资质，如高压操作、登高、特种设备操作资质等。

说明

- 专业人员：拥有培训或操作设备经验，能清楚设备安装、操作、维护过程中潜在的各种危险来源和危险量级的人。
- 已培训人员：经过相应的技术培训而且具有必要经验的人员，能意识到在进行某项操作时可能给他带来的危险，并能采取措施将对他自身或其他人员的危险减至最低限度。
- 操作人员：除已培训人员、专业人员以外的可能接触到设备的操作人员。

1.3 电气安全

接地要求

- 设备保护接地与金属壳体的接地螺钉应具备可靠的电气连接（接地电阻不大于0.1欧姆）。
- 需接地的设备，安装时，必须首先安装保护地线；拆除设备时，必须最后拆除保护地线。
- 禁止破坏接地导体。
- 禁止在未安装接地导体时操作设备。
- 对于使用三芯插座的设备，必须确保三芯插座中的接地端子与保护地连接。

交、直流操作要求

危险

- 电源系统的供电电压为危险电压，直接接触或通过潮湿物体间接接触可能会带来电击危险。
- 不规范、不正确的操作，可能会引起火灾或电击等意外事故。
- 禁止带电安装、拆除电源线。电源线芯在接触导体的瞬间，会产生电弧或电火花，可导致火灾或人身伤害。

- 若设备的电源输入为永久连接，则应在设备外部装上易于接触到的断开装置。
- 设备电气连接之前，如可能碰到带电部件，必须断开设备前级对应的分断装置。
- 如果设备粘贴了“大漏电流”标志，在连接交流输入电源之前，必须先将设备机壳的保护接地端子接地，以防止设备的漏电流对人体产生电击。
- 安装、拆除电源线之前，必须先关闭电源开关。

版权所有 © 华为技术有限公司

- 连接电源线之前，必须先确认电源线标签标识正确再进行连接。
- 接通电源之前，必须确保设备线缆已连接正确。
- 若设备有多路输入，应断开设备所有输入，待设备完全下电后方可对设备进行操作。

布线要求

- 线缆在高温环境下使用可能造成绝缘层老化、破损，线缆与发热器件或热源区域外围之间的距离至少为30mm。
- 设备进、出风口不允许有线缆经过。
- 线缆应满足VW-1阻燃等级要求。
- 同类线缆应绑扎在一起，不同类线缆至少分开30mm布放，禁止相互缠绕或交叉布放。
- 所有线缆应绑扎牢靠，绑扎后的线缆应相互紧密靠拢，外观平直整齐，无外皮损伤。
- 如果交流输入线缆从柜顶接入机柜，需在柜外U型折弯后进入机柜。
- 线缆弯曲半径要求：不小于线缆直径的5倍。
- 电源线布放过程中，严禁出现打圈、扭绞现象。如发现电源线长度不够时，须重新更换电源线，严禁在电源线中做接头或焊点。

防静电要求

- 安装、操作和维护设备时，请遵守静电防护规范，应穿防静电工作服，佩戴防静电手套和腕带。
- 手持单板时，必须持单板边缘不含元器件的部位，禁止用手触摸元器件。
- 拆卸下来的单板必须用防静电包材进行包装后，方可储存或运输。

1.4 安装环境要求

- 在设备运行时，请勿遮挡通风口或散热系统，以防止高温起火。
- 安装场所内应避免有酸性、碱性或其他腐蚀性气体。
- 请勿将设备靠近热源或裸露的火源，如电暖器、微波炉、烤箱、热水器、炉火、蜡烛或其他可能产生高温的地方。否则将使外壳熔化或者设备受热，并导致火灾。
- 设备应安装在远离液体的区域，禁止安装在水管、出风口等易产生冷凝水的位置下方；禁止安装在空调口、通风口、机房出线窗等易漏水位置下方，以防止液体进入设备内部造成设备故障或短路。
- 设备安装到机柜前，首先确定机柜已被固定好，避免机柜因重心不稳，出现倾斜倒塌，致使安装人员被砸伤，设备摔坏等问题。
- 禁止将设备置于易燃、易爆气体或烟雾的环境中，禁止在该环境下进行任何操作。

高空安装

在距离地面2米以上进行的作业，都属于高空作业。

遇以下情况之一者，应停止在高空作业：

版权所有 © 华为技术有限公司

- 钢管雨水未干，以及可能发生危险的其他情况。当上述情况过后，必须经公司安全主任和有关技术人员检查各种作业设备，确认同意后方可作业。
- 高空作业时，必须满足当地高空操作法规的要求。
- 必须经过相关培训，获取相关合格证方可上岗，进行高空作业。
- 高空作业前，应仔细检查登高工具和安全用具，如安全帽、安全带、梯子、跳板、脚手架、起重设备等，如有不符合要求的应立即改进或拒绝高空作业。
- 做好安全防护工作，佩戴安全帽、安全带或腰绳，系在牢固结实的结构件上，严禁挂在移动的不牢固的物体上或有锋利棱角的金属上，防止挂钩滑脱发生坠落事故。

危险

- 高空作业现场，应划出危险禁区，设置明显标志，严禁无关人员进入。
- 携带好操作器械及工具，防止工具坠落砸伤他人。
- 严禁高空作业人员从高空向地面抛掷物件，严禁从地面向高空抛掷物件，应采用强索、吊篮、高架车或吊车等传送物件。
- 应尽量避免上、下层同时进行作业。如无法避免时，上下层之间必须设专用防护棚或采取其他防护措施，且上层严禁堆放工具、物料。
- 高空作业的沿口、孔洞处，应设护栏和标志，防止失足踏空。
- 高空作业区的下方地面，严禁堆放脚手架，跳板，其他杂物。地面人员严禁在高空作业区的正下方停留或通行。
- 高空作业的脚手架、跳板、工作台等，必须事先进行安全检查鉴定，保证结构牢固、脚手架严禁超负荷。
- 工作竣工拆卸脚手架时，应由上而下分层进行，严禁上下层同时拆卸，当拆除某一部分的时候，应防止其它部份发生倒塌。
- 严禁在高空作业时嬉笑打闹，严禁在高空作业区睡觉。

- 现场负责人、安全员如发现高处作业施工人员不按规定作业者，应立即提出，责其改正；否则须停止其作业。
- 作业人员违反高空作业安全规定不听劝阻而造成事故的由本人负责，监护人员应承担一定责任。

1.5 机械安全

吊装安全

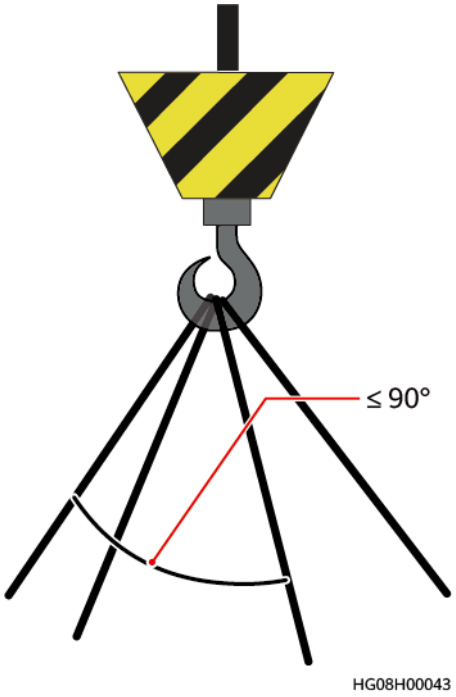
危险

吊装重物时，严禁在吊臂、吊装物下方走动。

- 进行吊装作业的人员需经过相关培训，合格后方可上岗。
- 吊装工具需经检验，工具齐全方可使用。

版权所有 © 华为技术有限公司

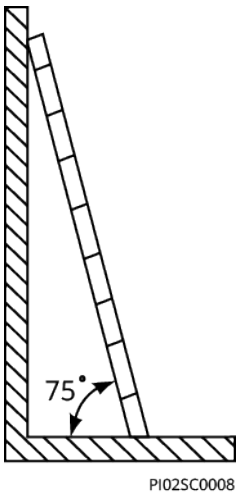
- 吊装作业之前，确保吊装工具牢固固定在可承重的固定物或墙上。
- 在吊装过程中，确保两条缆绳间的夹角不大于90°，如下图所示。



- 吊装时，禁止拖拽钢丝绳、吊具，禁止使用硬物撞击。

梯子使用安全

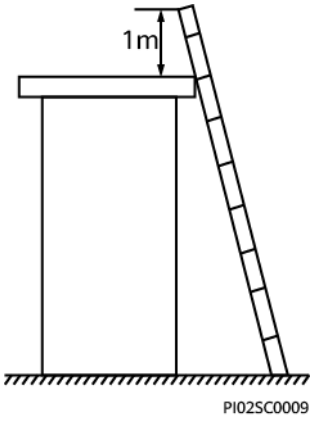
- 当可能涉电登高操作时，应使用木梯或玻璃钢梯。
- 使用人字梯时拉绳必须牢固，作业时必须有人扶住梯子。
- 使用梯子前，请确认梯子完好无损，梯子承载重量符合要求，严禁超重使用。
- 使用梯子时应将宽的梯脚朝下或在梯子的底部采用保护措施，以防滑倒。
- 梯子应放在稳固的地方。梯子的倾斜度以75°为宜，可使用角尺测量，如下图所示。



爬梯时，请注意如下动作，以减少危险并确保安全。

版权所有 © 华为技术有限公司

- 保持身体平稳。
- 作业人员脚站立的最高高度不应超过梯子从上向下数的第4个台阶。
- 若要爬上屋顶，超出屋檐的梯子的垂直高度至少为1米，如下图所示。



- 确保身体重心不偏离梯架的边沿。

钻孔安全

在墙面、地上钻孔时需要考虑如下安全注意事项：

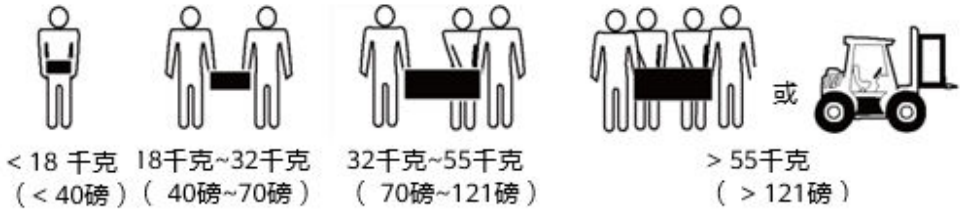
须知

严禁在设备上钻孔。钻孔会破坏设备的电磁屏蔽性能、内部器件和线缆，钻孔所产生的金属屑进入设备会导致电路板短路。

- 钻孔时应佩戴护目镜和保护手套。
- 钻孔过程中应对设备进行遮挡，严防碎屑掉入设备内部，钻孔后应及时打扫、清理碎屑。

搬运重物安全

- 搬运重物时，应做好承重的准备，避免被重物压伤或扭伤。



- 用手搬运设备时，应佩戴保护手套，以免受伤。
- 移动或抬起设备时，应握住设备手柄或托住设备底边，而不应握住设备内已安装模块（如电源模块，风扇模块或单板）的手柄。

1.6 电池安全

若系统未配置电池，无需查阅此章节内容。

版权所有 © 华为技术有限公司

电池的安装、操作和维护之前，请阅读电池厂家提供的说明书。本手册中的安全注意事项仅作为重点提醒事项，更多的安全注意事项请参考电池厂家提供的说明书。

基本要求

在进行电池作业之前，必须仔细阅读操作的安全注意事项，并掌握电池的正确连接方法。

危险

- 请勿将电池暴露在高温环境或发热设备的周围，如日照、火源、变压器、取暖器等。电池过热可能引起爆炸。
- 严禁焚烧电池，否则可能引起爆炸。
- 严禁拆解、改装或破坏电池（如插入异物、浸入水或其它液体中），以免引起电池漏液、过热、起火或爆炸。
- 更换电池时，必须使用同型号或同类型的电池，若电池更换不当可能会导致电池爆炸。
- 请勿将金属物导体与电池两极对接，或接触电池的端点，以免导致电池短路，以及因电池过热而引起的烧伤等身体伤害。

电池安装、操作和维护过程中，为确保安全，应注意：

- 请勿佩戴手表、手链、手镯、戒指等含有金属的物体。
- 应佩戴护目镜、橡胶手套，穿防护服，预防电解液外溢所造成的危害。如电池漏液，请勿使皮肤或眼睛接触到漏出的液体，若接触到皮肤或眼睛上，应立即用清水冲洗，并到医院进行医疗处理。
- 请使用专用绝缘工具。
- 搬运电池时，应按照电池要求的方向搬运，严禁倒置、倾斜。
- 安装、维护等操作时，电池回路应保持断开状态。
- 禁止跌落、挤压或穿刺电池。避免让电池遭受外部大的压力，从而导致电池内部短路和过热。
- 请按当地法律法规处理废旧电池，请勿将电池作为生活垃圾处理。电池处置不当可能会导致电池爆炸。
- 严禁使用已经损坏的电池。
- 严禁让儿童或宠物吞咬电池 ，以免对其造成伤害或导致电池爆炸。
- 电池在使用、充电或保存过程中有变色、变形、异常发热等异常现象，应停止使用并更换新电池。
- 在规定温度范围内，电池可正常按照允许的充放电参数工作。超出规定温度范围，将会影响电池的充放电性能及安全。

电池安装规范

电池安装操作前，为确保安全，应注意遵从以下基本预防措施：

- 电池安装位置应选择通风、干燥、阴凉环境，远离热源、易燃、潮湿环境，并做好防火措施。

版权所有 © 华为技术有限公司

- 电池应水平摆放、固定。
- 电池安装过程注意正负极，严禁将同一支或同一组串电池的正负极短接，否则会引起电池短路。
- 电池组在完成安装前，至少留下一断点，避免形成回路，在检查确认后再闭合断点完成安装。
- 安装过程中，连接电池的线缆端子应做好绝缘保护，切勿触碰机柜等金属部件。
- 电池线缆或铜排安装须按照标准力矩拧紧，否则电池螺栓虚连将导致连接压降过大，甚至在电流较大时大量发热将电池烧毁。
- 请定期检查电池连接端子螺钉，确认拧紧，无松动。

电池短路防护

⚠ 危险

电池短路会产生瞬间大电流并释放大量能量，可能造成人身伤害以及财产损失。

- 在允许的情况下，首先断开工作中的电池连接，再进行其他作业。
- 为避免电池短路，电池不允许在线维护。

易燃气体防护

须知

- 严禁使用未封闭的铅酸电池。
- 铅酸电池应确保可燃性气体（如氢气）排放措施正常，避免导致燃烧或腐蚀设备。

铅酸电池在工作中会释放出可燃性气体，摆放电池的地方应保持通风并做好防火措施。

电池漏液处理规范

须知

电池温度过高会导致电池变形、损坏及电解液溢出。

当电池温度超过60℃时，应检查是否有电解液溢出。如有电解液溢出，应及时处理。

电解液溢出会对设备造成潜在的危害，溢出的电解液会腐蚀金属物体及单板，导致单板损坏。

⚠ 警告

在有电解液溢出时，应及时做好液体的吸收和中和。在移开、搬动漏液电池时，应注意电解液可能带来的伤害。

版权所有 © 华为技术有限公司

如发现电解液溢出，请按照电池生产厂家指导操作，或者采用碳酸氢钠（$NaHCO_3$）、碳酸钠（Na_2CO_3）中和，吸收电解液。

锂电池场景

锂电池操作的安全注意事项参考铅酸电池，另外还需要注意如下事项。

⚠ 警告

更换电池的型号不正确会有爆炸的危险。

- 仅可使用厂商推荐的相同或相似型号的电池更换。
- 搬运锂电池时，禁止倒置、倾斜和碰撞。
- 安装、维护等操作时，锂电池回路要保持断开状态。
- 当环境温度低于工作温度下限时禁止充电（0℃禁止充电），否则会造成锂电池内部短路。
- 禁止将锂电池投入火源。
- 维护完成时，应将废旧的锂电池返回维护处。

版权所有 © 华为技术有限公司

2 解决方案概述

2.1 定位

PowerCube 500一体化视频站点，广泛应用于平安城市、公路、高速沿线、园区、景区等场景。该方案通过一体化集成设计，解决了视频站点的传输、供电、快速部署等一系列问题，并通过远程网管等智能管理手段，极大地减少站点故障率以及运维投入，提升了整个视频站点的在线率。

2.2 特点

简单部署

- 12V DC、24V AC 、220V AC（选配）输出。
- 体积小，重量轻，一站式抱杆或挂墙安装。

高可靠性

- IP55高防护等级；
- -40 ℃ ~+45 ℃ 宽温度适应（太阳辐射：1120W/m^2）。
- GPON/EPON自适应接入，同时支持SFP GPON或者GE上行。
- 支持type C双归属业务保护。

智能管理

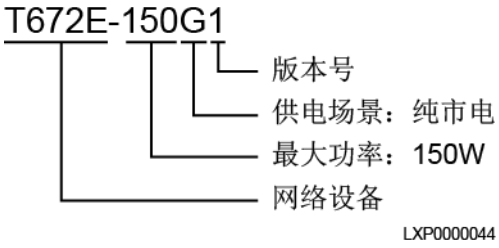
- 远程网管，高效管理。

2.3 型号说明

功能模块T672E-150G1的型号说明如下图所示。

版权所有 © 华为技术有限公司

图 2-1 功能模块型号说明



2.4 场景配置

图 2-2 应用场景

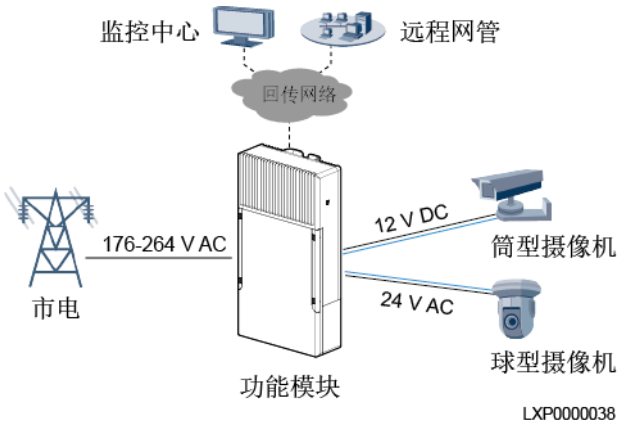


表 2-1 系统配置

项目	内容
功能模块	T672E-150G1
视频监控	12V DC、24V AC接口最大总输出功率144W。

版权所有 © 华为技术有限公司

3 部件介绍

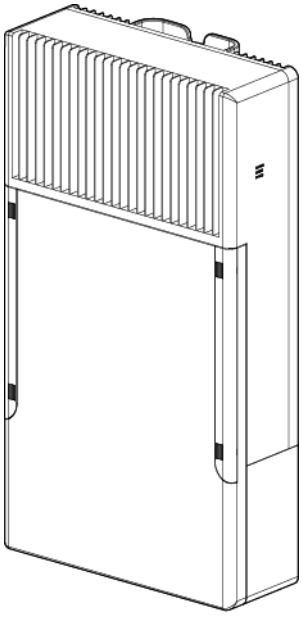
3.1 功能模块

功能

功能模块T672E-150G1集功率单元（整流、配电）和网络设备于一体，将交流电转换成稳定的12V DC和24V AC，支持故障告警和实时监控数据上报给上级网管。

外观

图 3-1 功能模块的外观



版权所有 © 华为技术有限公司

指示灯

图 3-2 功能模块指示灯

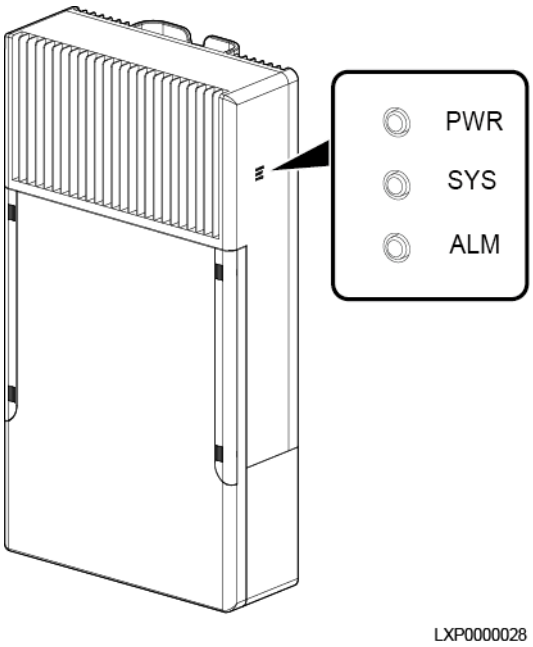


表 3-1 功能模块指示灯说明

指示灯	状态	说明
PWR	常亮（绿色）	设备供电正常，且与内部电源通信正常。
	常灭	设备未供电。
	常亮（橙色）	设备供电正常，但与内部电源通信不正常。
SYS	常灭	系统未运行。
	常亮（绿色）	系统正常运行。
	闪烁（红色）	设备注册后不正常运行，或温度异常告警。
ALM	常灭	无交流输入或设备供电正常。
	常亮（红色）	设备供电异常。

版权所有 © 华为技术有限公司

⚠ 注意

1. 功能模块配置的32A/2P交流输入空开，是为了匹配功率单板20KA的交流防雷器。
2. 功能模块的交流前级输入空开和线缆选型推荐参考：

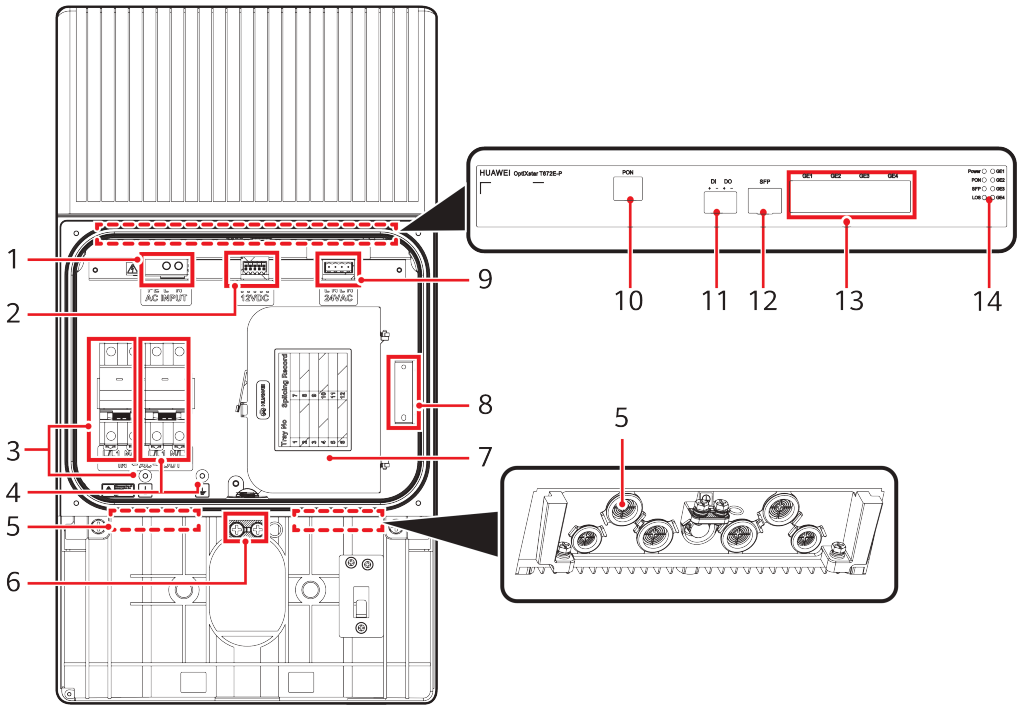
- 在不考虑交流防雷，功能模块配置32A/2P交流输入空开与10A/2P交流输出空开的情况下，则功能模块的交流前级输入空开应选不小于20A，线缆铜导体截面积应选不小于2mm^2，线材耐温不小于70℃；
- 在不考虑交流防雷，功能模块配置32A/2P交流输入空开未配置交流输出空开的情况下，则功能模块的交流前级输入空开应选不小于10A，线缆铜导体截面积应选不小于1mm^2，线材耐温不小于70℃;
- 在考虑交流防雷，功能模块配置32A/2P交流输入空开与10A/2P交流输出空开的情况下，则功能模块的交流前级输入空开应选不小于32A/2P（即对应功能模块交流输入空开的规格），线缆铜导体截面积应选不小于4mm^2（即对应功能模块内部交流输入线缆的规格），线材耐温不小于70℃；
- 在考虑交流防雷，功能模块配置32A/2P交流输入空开未配置交流输出空开的情况下，则功能模块的交流前级输入空开应选不小于32A/2P（即对应功能模块交流输入空开的规格），线缆铜导体截面积应选不小于4mm^2（即对应功能模块内部交流输入线缆的规格），线材耐温不小于70℃；

  以上线缆数据仅供参考，该数据是以线缆长度50m为限。线缆铜导体截面积需要根据实际的供电距离、导体的内阻计算压降，在满足功能模块工作电压和通流量的条件下，适当调整铜导体截面积大小。

版权所有 © 华为技术有限公司

面板

图 3-3 面板介绍（正视图）



（1）交流输入端子	（2）12V直流供电接口	（3）交流输入空开及接地螺丝（选配）
（4）交流输出空开及接地螺丝（选配）	（5）出线口	（6）接地螺丝
（7）盘纤盒（选配）	（8）门磁传感器	（9）24V交流供电接口
（10）PON接口	（11）开关量接口	（12）SFP接口
（13）GE1~GE4接口	（14）Power/PON/SFP/LOS/GE1~GE4指示灯	-

表 3-2 网络模块指示灯说明

指示灯	状态	说明
Power	常亮	电源接通
	常灭	电源断开
PON	如下表所示	
SFP	常亮	当前ONU GPON SFP模块或者GE SFP模块正在使用当中
	熄灭	当前ONU SFP模块没有使用
LOS	如下表所示	

版权所有 © 华为技术有限公司

指示灯	状态	说明
GE1～GE4	常亮	以太网连接正常
	闪烁（绿色）	以太网接口有数据传输
	常灭	以太网连接未建立

PON和LOS两个指示灯的状态共同说明ONU连接和注册到OLT（Optical Line Terminal）的情况，详细说明如下表所示。

表 3-3 PON 和 LOS 指示灯说明

状态编号	指示灯状态		说明
	PON	LOS	
1	快闪（2Hz）	常灭	PON终端正在与上层设备建立连接
2	常亮	常灭	PON终端与上层设备已经建立连接
3	常灭	慢闪（0.5Hz）	PON终端没接光纤或无光信号
4	常灭	常亮	PON终端被上层设备禁用或发光异常，请联系服务提供商
5	慢闪（0.5Hz）	慢闪（0.5Hz）	PON终端硬件故障

业务接口（OptiXstar T672E）

表 3-4 接口说明

接口	说明
PON	上行GPON/EPON自适应接入，接口类型为SC/UPC。
SFP	支持SFP GPON或者GE光模块接入。
DI	连接门磁、红外感应等装置。
DO	连接外部告警装置。 **说明** DO口：默认断开（低电平），告警状态从断开变为闭合（高电平），闭合后高电平可持续时间为3秒。
GE1~GE4	RJ45接口，可连接摄像头等设备，支持10Mbit/s或100Mbit/s或1000Mbit/s接口速率自适应，支持MDI/MDI-X自动配置。

版权所有 © 华为技术有限公司

供电接口

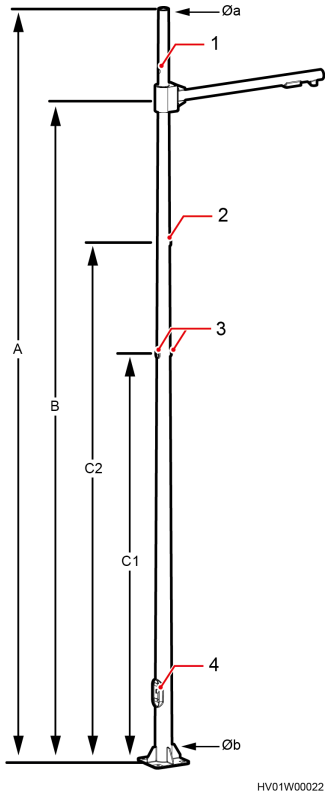
表 3-5 接口说明

接口类型	丝印	说明
AC交流输入接口	L/N/PE	连接市电交流输入。
12V直流供电接口	12V DC	用于筒型摄像机供电。
24V交流供电接口	24V AC	用于球型摄像机供电。
220V AC空开（选配）	220V AC IN、220V AC OUT	连接市电交流输入并提供一路交流输出。

3.2 立杆

外观

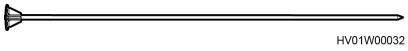
图 3-4 立杆



（1）客户端设备走线孔　　（2）走线孔（预留）

（3）功能模块走线孔　　（4）维护窗口

图 3-5 避雷针



版权所有 © 华为技术有限公司

规格参数

表 3-6 立杆规格参数

项目	立杆
尺寸	• 杆总高度A=6.8m • 悬臂高度B=6m • 走线孔（预留）高度C2=4.7m • C2位置杆直径=108mm • 功能模块走线孔高度C1=3.7m • C1位置杆直径=117mm • 上直径Øa=90mm，下直径Øb=150mm
立杆重量	约110kg
避雷针尺寸	1.5m
防风等级	风速40m/s（美标）
防腐等级	C类环境

3.3 视频监控

视频监控主要包括球型摄像机与筒型摄像机、传输设备和信号处理等，相关内容请参考对应的文档资料，文档资料下载路径：http://support.huawei.com/enterprise/

版权所有 © 华为技术有限公司

4 关键特性

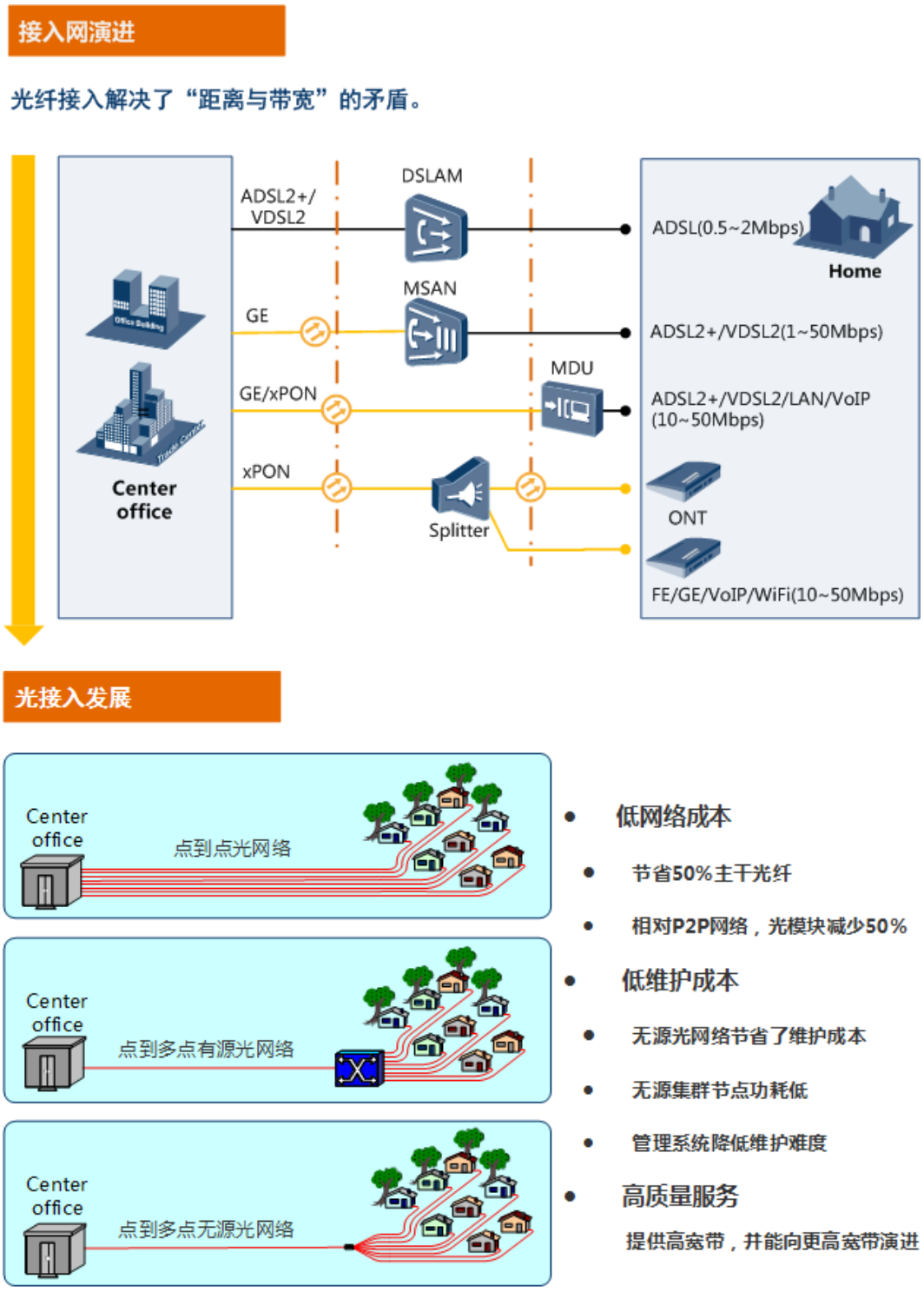
本文档对产品的关键特性进行了简单描述，使读者对产品特性有一定初步了解。

4.1 GPON

GPON（Gigabit Passive Optical Network）是PON（Passive Optical Network）技术中的一种，是由ITU-T G.984.x系列标准规范的千兆比特PON。设备采用GPON接入时，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。

4.1.1 GPON 引入背景

版权所有 © 华为技术有限公司



4.1.2 GPON 介绍

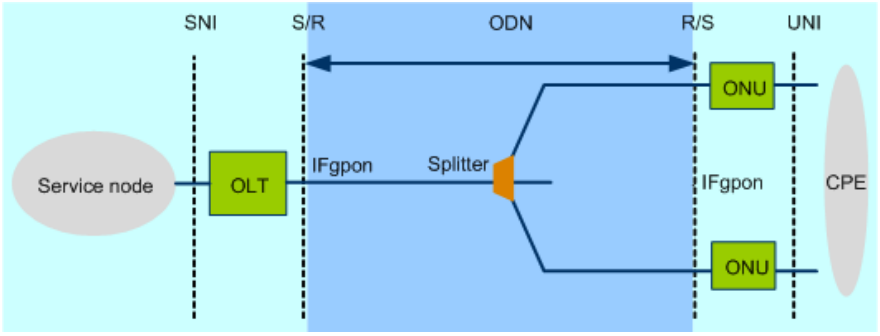
什么是 GPON

PON（Passive Optical Network）是一种点到多点（P2MP）结构的无源光网络，主流的PON技术包括BPON(Broadband Passive Optical Network)、EPON（Ethernet Passive Optical Network）和GPON几种技术。BPON由于采用ATM封装模式，主要用于ATM业务承载，但是随着ATM技术已经过时，BPON技术也随之消失。EPON是以太

版权所有 © 华为技术有限公司

网无源光网络技术。GPON是吉比特无源光网络技术，是目前应用范围最广的光接入主流技术。是由ITU-T G.984.x系列标准定义的千兆比特PON。GPON网络结构如图4-1所示。

图 4-1 GPON 网络结构



IFgpon: GPON Interface	SNI: Service Node Interface
UNI: User to Network Interface	CPE: Customer Premises Equipment

- OLT（Optical Line Terminal）是放置在局端的终结PON协议的汇聚设备。
- ONU（Optical Network Unit）是位于客户端的给用户提供各种接口的用户侧单元或终端，OLT和ONU通过中间的无源光网络ODN连接起来进行互相通信。
- ODN（Optical Distribution Network）是由光纤、一个或多个无源分光器等无源光器件组成，在OLT和ONU间提供光通道，起着连接OLT和ONU的作用，具有很高的可靠性。

说明

无源意味着ODN里面没有光放大器和再生器等器件，节省了室外有源设备维护成本。

为什么选择 GPON

随着宽带业务的普及和光进铜退的趋势，运营商对业务的传输距离、带宽、可靠性和低运营成本提出越来越高的要求。GPON的以下特点满足了这些要求：

- 更远的传输距离：采用光纤传输，接入层的覆盖半径最大可达60km。可以解决双绞线“距离和带宽的矛盾”。
- 更高的带宽：每端口最大下行速率2.5Gbit/s，最大上行速率1.25Gbit/s。满足用户对高带宽业务的需求，如高清电视、实况转播等。
- QoS（Quality of Service）提供灵活的全业务体验：提供区分用户和用户业务的流量控制，保证多用户的多业务带宽，为不同的用户业务提供差异化服务。
- 分光特性：局端单根光纤经分光后引出多路到户光纤，支持1:128分光比，节省主干光纤资源，降低运营维护成本。

版权所有 © 华为技术有限公司

4.1.3 GPON 基本概念

GEM 帧

GEM（GPON Encapsulation Mode）帧是GPON技术中最小的业务承载单元，是最基本的数据结构。所有的业务都要封装在GEM帧中在GPON线路上传输，通过GEM Port标识。

- 每个GEM Port由一个唯一的Port ID来标识，由OLT进行全局分配，即每个GPON端口下的每个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（Virtual Path Identifier）/VCI（Virtual Channel Identifier）标识。

GEM帧结构如图4-2所示。

图 4-2 GEM 帧结构

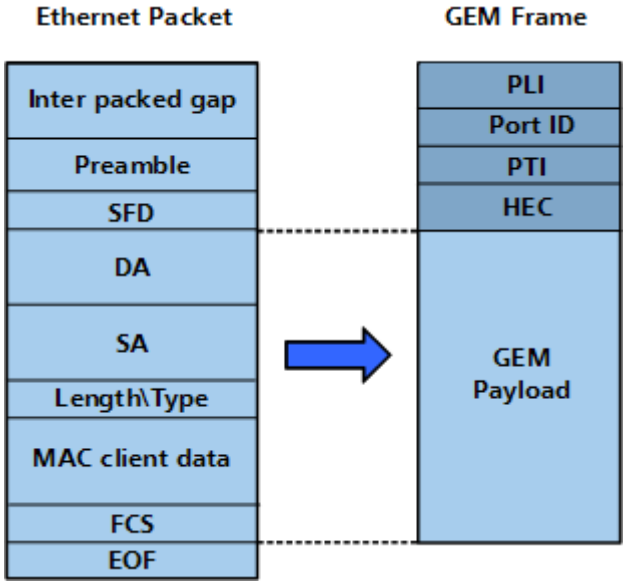
PLI、Port ID、PTI和HEC（Header Error Check）构成GEM header，即GEM帧头，主要用于区别不同的GEM Port中的数据。各字段的具体含义如下：

- PLI：表示数据净荷的长度
- Port ID：唯一标明不同的GEM Port
- PTI：净荷类型标识，主要是为了标识目前所传送的数据的状态和类型，如是否是OAM（Operation, Administration and Maintenance）消息，是否已经将数据传送完毕等信息
- HEC：提供前向纠错编码功能，保证传输质量
- Fragment Payload：表示用户数据帧片段

以以太网业务在GPON中的映射方式为例，更直观地了解GEM帧的作用。如图4-3所示。

版权所有 © 华为技术有限公司

图 4-3 以太帧映射到 GEM 帧



- GPON系统对以太网帧进行解析，将数据部分直接映射到GEM Payload中去进行传输。
- GEM帧会自动封装头信息。
- 映射的格式清晰，兼容性好。

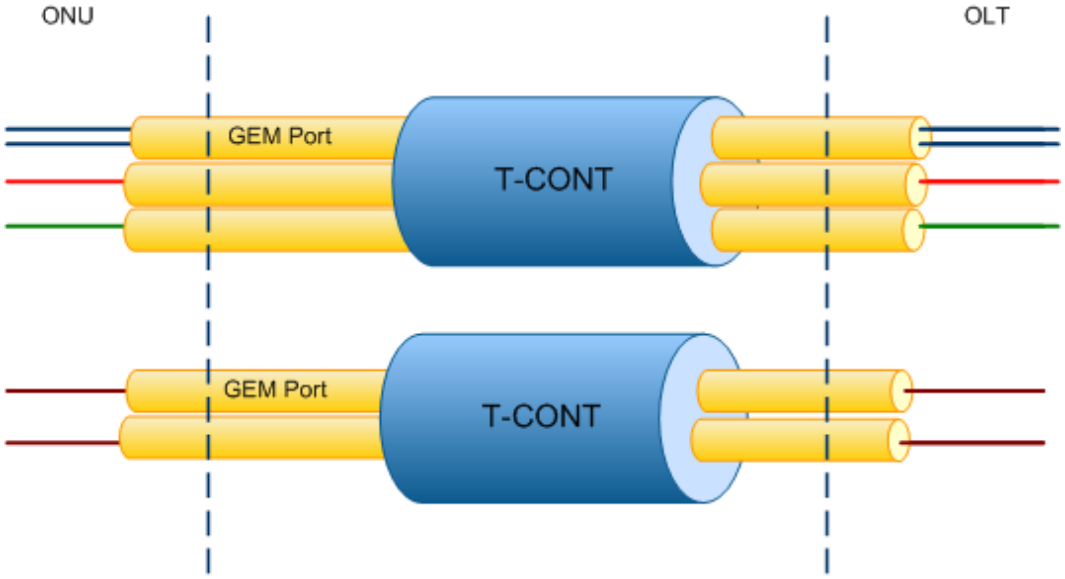
T-CONT

T-CONT（Transmission Container）是GPON上行方向承载业务的载体，所有的GEM Port都要映射到T-CONT中，由OLT通过DBA（Dynamic Bandwidth Allocation）调度的方式上行。T-CONT是DBA实现的基础，通过ONU对T-CONT的带宽申请、OLT对T-CONT的授权，实现整个GPON系统上行业务流的DBA。

T-CONT是GPON系统中上行带宽最基本的控制单元。每个T-CONT由Alloc-ID来唯一标识。Alloc-ID由OLT每个GPON端口分配，即OLT同一GPON端口下的ONU不存在Alloc-ID相同的T-CONT。

版权所有 © 华为技术有限公司

图 4-4 T-CONT 结构



T-CONT包括五种不同的类型，可根据不同类型的业务选择不同类型的T-CONT。每种T-CONT带宽类型有特定的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/最大带宽，最大带宽，混合方式（对应表4-1的Type1到Type5）。

说明

表4-1中的X表示固定带宽值、Y表示保证带宽值、Z表示最大带宽值，-表示不涉及。

表 4-1 五种 T-CONT 类型

带宽类别	Type1	Type2	Type3	Type4	Type5
Fixed BW（固定带宽）	X	-	-	-	X
Assured BW（保证带宽）	-	Y	Y	-	Y
Maximum BW（最大带宽）	Z=X	Z=Y	Z>Y	Z	Z≥ X + Y

版权所有 © 华为技术有限公司

带宽类别	Type1	Type2	Type3	Type4	Type5
应用说明	• 固定带宽是完全预留给特定ONU或者ONU的特定业务，即使在ONU没有上行业务流的情况下，这部分带宽也不能为其他ONU使用。 • 固定带宽主要用于对业务质量非常敏感的业务，如：TDM、VoIP等。	• 保证带宽就是保证在ONU需要使用带宽时可获得的带宽。当ONU的实际业务流量未达到保证带宽时，设备的DBA机制应能够将其剩余带宽分配给其他ONU的业务。 • 由于需要DBA机制控制分配，其实时性比固定带宽要差。	• **Type3**类型为保证带宽+最大带宽的组合类型，在保证用户有一定带宽的同时，还允许用户有一定带宽的抢占，但总和是不会超过用户配置的最大带宽。 • 此带宽类型主要应用于VoIP业务。	• 最大带宽是在ONU使用带宽时可获得的带宽上限值，最大程度地满足ONU使用的带宽资源。 • 最大带宽类型常用于IPTV、高速上网等业务。	**Type5**类型为固定带宽+保证带宽+最大带宽的组合类型，既给用户预留其他用户不能抢占的固定带宽资源，又确保在需要使用带宽时可获得的保证带宽，同时允许用户有一定带宽的抢占，但总和是不会超过用户配置的最大带宽。

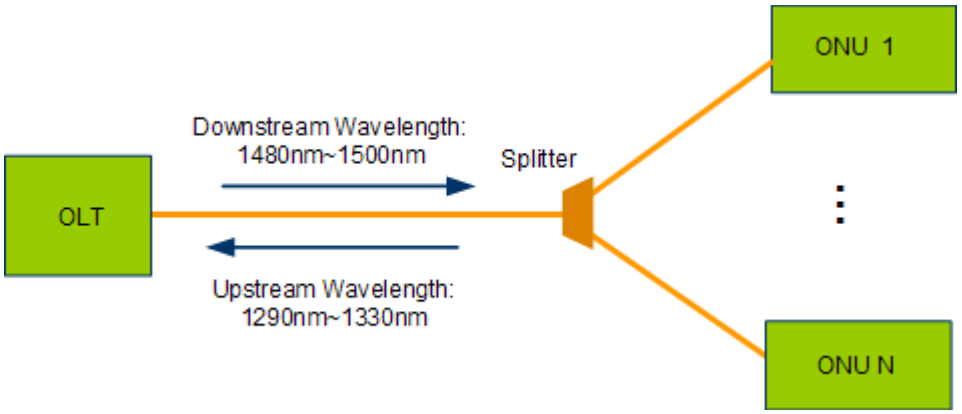
4.1.4 GPON 系统概述

GPON 系统介绍

GPON网络工作原理如**图4-5**所示。

版权所有 © 华为技术有限公司

图 4-5 GPON 网络工作原理

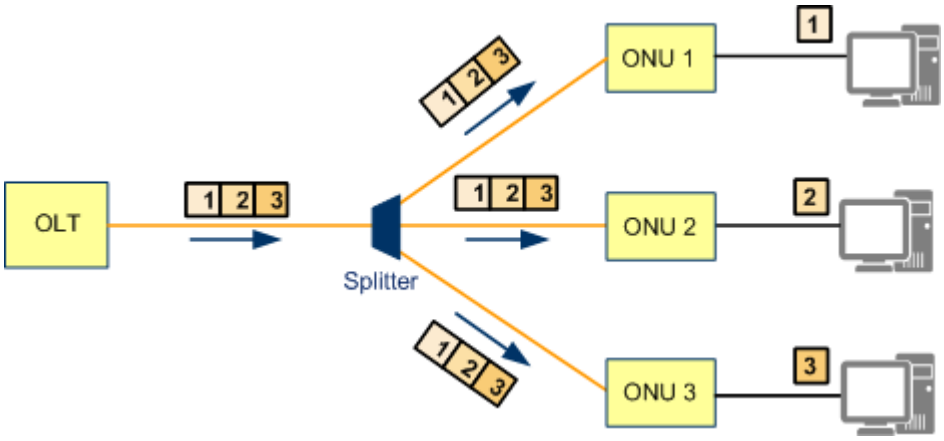


- GPON网络采用单根光纤将OLT、分光器和ONU连接起来，上下行采用不同的波长进行数据承载。上行采用1290nm~1330nm范围的波长，下行采用1480nm~1500nm范围的波长。
- GPON系统采用波分复用的原理通过上下行不同波长在同一个ODN网络上进行数据传输，下行通过广播的方式发送数据，而上行通过TDMA的方式，按照时隙进行数据上传。

GPON 下行传输

所有数据从OLT端广播到所有的ONU上，ONU再选择接收属于自身的数据，将其他数据直接丢弃。具体原理如图4-6所示。

图 4-6 GPON 下行通信原理



主要特征：

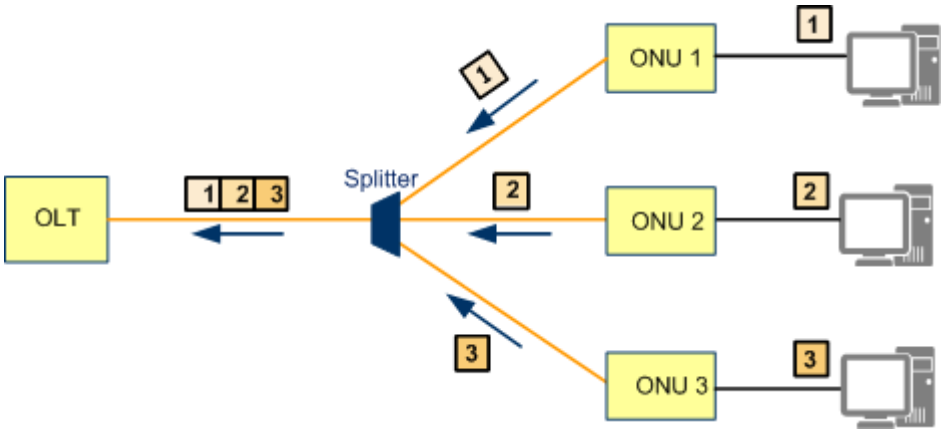
- 点对多点广播式传输。
- 所有的ONU都能收到相同的数据，但是通过gemport ID来区分不同的ONU的数据，ONU通过过滤来接收属于自己的数据。
- 用户接收属于自己的数据包，丢弃不属于自己的数据包。

版权所有 © 华为技术有限公司

GPON 上行传输

ONU在向OLT发送数据时只能在OLT提前许可的时隙内发送数据，这样就可以保证每个ONU都按照要求按次序发送数据，避免了上行数据冲突，如图4-7所示。

图 4-7 GPON 上行通信原理



主要特征：

- 时分复用（Time Division Multiple Access）。
- 数据在属于自己的时隙里传输。
- 光信号在分光器处进行耦合。
- 通过测距实现冲突检测与避免。

4.1.5 GPON 系统原理

4.1.5.1 业务复用原理

GEM Port和T-CONT将PON网络分为虚拟的连接，实现业务复用。

- 一个GEM Port可以承载一种业务，也可以承载多种业务。GEM Port承载业务后先要映射到T-CONT单元进行上行业务调度。每个ONU支持多个T-CONT，并可以根据不同的业务类型选择不同类型的T-CONT。
- 一个T-CONT可以承载多个GEM Port，也可以承载一个GEM Port，根据用户的具体的规划而定。

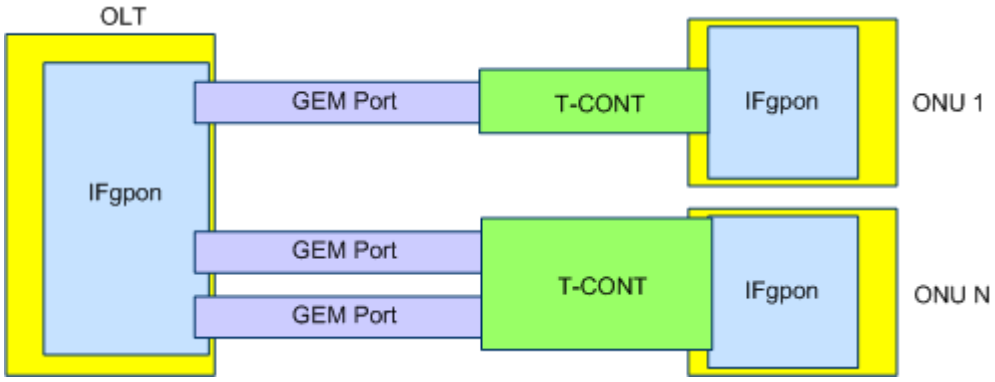
业务映射关系

- 上行方向：
  - 根据配置的Service port和GEM port映射规则，以太帧被发送到对应的GEM port，GEM port将以太帧封装进GEM PDU，并根据GEM port和T-CONT队列映射规则将GEM PDU放入对应的T-CONT队列中。T-CONT队列在其上传时隙中将GEM PDU发送至OLT。
  - OLT接收GEM PDU后提取出以太帧，并根据配置的Service port映射规则将以太帧从指定的上行端口发送出去。

    GPON上行业务映射关系如图4-8所示。

版权所有 © 华为技术有限公司

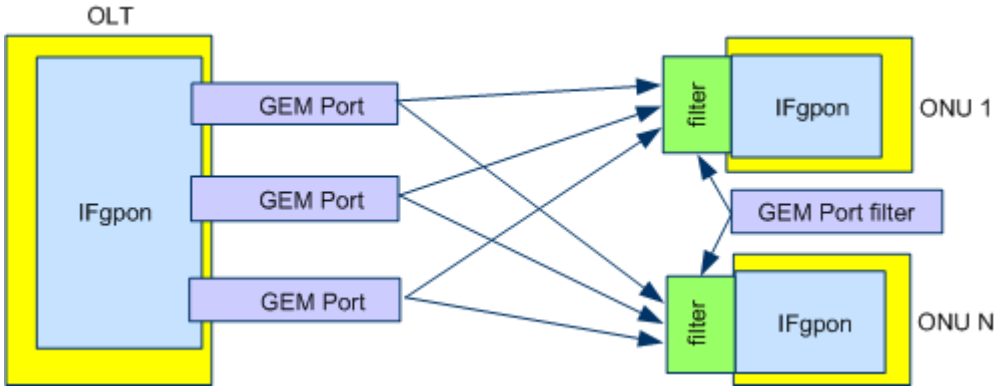
图 4-8 GPON 业务映射关系（上行）



- 下行方向：
  - 根据配置的Service port映射规则，以太帧被发送到GPON业务处理模块，GPON业务处理模块将以太帧封装进GEM PDU后通过GPON端口下行。
  - 包含GEM PDU的GTC帧广播给该GPON端口下所有的ONU设备。
  - ONU根据GEM PDU头部的GEM port ID进行数据过滤，只保留属于该ONU的GEM port并解封装后将以太帧从ONU的业务接口送入用户设备中。

    GPON下行业务映射关系如图4-9所示。

图 4-9 GPON 业务映射关系（下行）

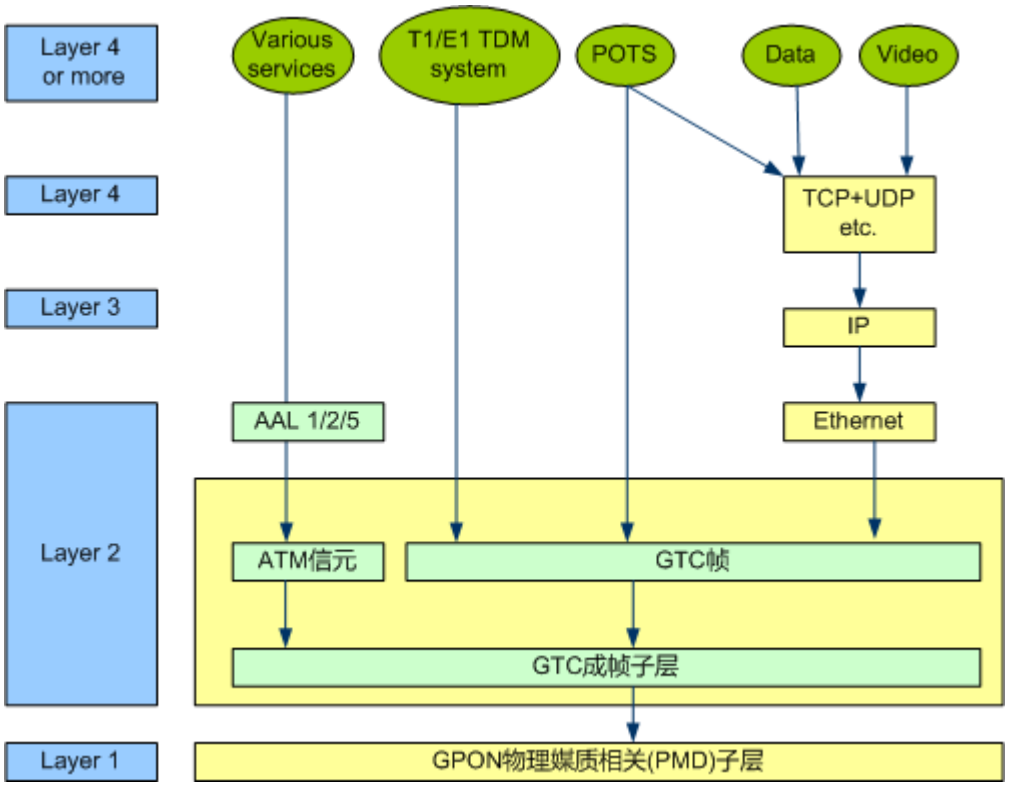


4.1.5.2 GPON 系统协议栈

ITU-T G.984.3标准定义了一套全新的帧结构，将传统的语音、视频及以太网报文作为GPON帧的净荷。GPON协议栈系统结构如图4-10所示。

版权所有 © 华为技术有限公司

图 4-10 GPON 协议栈系统结构



GPON系统协议栈主要由物理媒质相关（PMD）层和GPON传输汇聚（GTC）层组成。

PMD层

GPON的PMD层对应OLT和ONU之间的GPON接口，具体参数值决定了GPON系统的最大传输距离和最大分光比。

GTC层

GTC层封装ATM信元和GEM帧两种格式的净荷，通常GPON系统采用GEM帧封装模式。GEM帧可以承载以太、POTS、E1、T1多种格式的信元。

GTC层是GPON的核心层，主要完成上行业务流的媒质接入控制和ONU注册。以太帧净荷或者其他内容封装在GEM帧中，打包成GTC帧，按照物理层定义的接口参数转换为物理01码进行传输，在接收端按照相反的过程进行解封装，接收GTC帧，取出GEM帧，最终把以太净荷或者其他封装的内容取出以达到传输数据的目的。

GTC层按结构可分为GTC成帧子层和TC适配子层。

- 在TC适配子层，包括ATM适配器、GEM TC适配器和OMCI适配器。ATM适配器、GEM TC适配器通过VPI/VCI或者GEM Port ID识别OMCI通道。OMCI适配器可以和ATM适配器、GEM TC适配器交换OMCI通道数据并传送到OMCI实体上。此外，DBA控制模块为通用功能模块，负责完成ONU报告和所有的DBA控制功能。
- 在GTC成帧子层，GTC帧可分为GEM块、PLOAM块和嵌入式OAM。GPON成帧子层包括三个功能：
  - 复用和解复用：PLOAM和GEM部分根据帧头指示的边界信息复用到下行TC帧中，并可以根据帧头指示从上行TC帧中提取出PLOAM和GEM部分。

版权所有 © 华为技术有限公司

- 帧头生成和解码：下行帧的TC帧头按照格式要求生成，上行帧的帧头会被解码。同时直接封装在GTC帧头的嵌入式OAM信息被终结，并用于直接控制该子层。
- 基于Alloc-ID的内部路由功能：根据Alloc-ID的内部表示为来自或者送往GEM TC适配器的数据进行路由。

GTC层按功能可分为C/M平面和U平面。

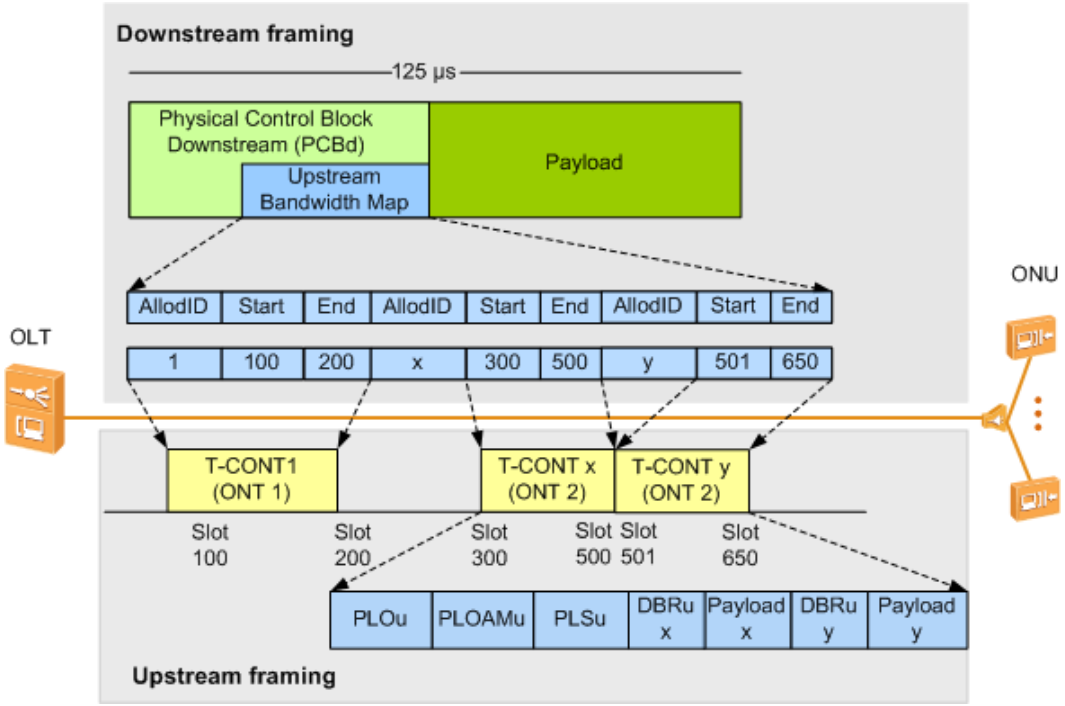
- C/M控制管理平面的协议栈包括三部分：嵌入式OAM，PLOAM（物理层OAM），OMCI（ONT管理控制接口）。嵌入式OAM和PLOAM通道负责管理PMD和GTC子层的功能，OMCI为更高子层管理提供统一的系统。嵌入式OAM通道位于GTC帧的帧头，主要功能包括：带宽确认、交换、动态带宽分配信令等。PLOAM通道是一个格式化的消息系统，在GTC帧中占据专有空间，主要用于承载那些不通过嵌入式OAM发送的PMD和GTC管理信息。OMCI通道用于管理业务。
- U平面内的业务流用业务流类型（ATM、GEM）及其端口ID或VPI来标识。端口ID用于识别GEM业务流，VPI用于识别ATM业务流。在T-CONT（传输容器）中通过可变的时隙控制来实现带宽分配和QoS控制。

4.1.5.3 GPON 帧结构

GPON 帧结构

GPON系统帧结构如图4-11所示。

图 4-11 GPON 帧结构



GPON 上行帧

上行帧长固定为125us，每个上行帧包含了一个或者多个T-CONT传送的内容。每个GPON端口下对于所有ONU都是共享上行带宽。

版权所有 © 华为技术有限公司

- 按照BWmap的要求，ONU必须在属于自己的时隙范围内进行上行数据发送。
- ONU会报告自身需要发送的数据状态通过上行帧发送到OLT，OLT通过DBA方式分配好上行时隙定期每帧发送更新。

图4-11中的GPON上行帧由PLOu、PLOAMu、PLSu、DBRu和Payload字段构成，具体含义如表4-2所示：

表 4-2 GPON 上行帧字段说明

字段名称	字段描述	含义
PLOu：Physical Layer Overhead upstream	上行物理层开销	帧定位、同步和标明此帧是哪个ONU的数据。
PLOAMu：PLOAM upstream	上行数据的PLOAM消息	上报ONU的维护、管理状态等管理消息（不是每帧都有，可以不发，但是需要协商）。
PLSu	功率级别序列	用于ONU调整光口光功率（不是每帧都有，可以不发，但是需要协商）。
DBRu：Dynamic Bandwidth Report upstream	上行动态带宽报告	上报T-CONT的状态，为了给下一次申请带宽，完成ONU的动态带宽分配（不是每帧都有，可以不发，但是需要协商）。
Payload	数据净荷	可以是DBA状态报告也可以是数据帧。如果是数据帧的话，可以分为GEM header和Frame。

GPON 下行帧

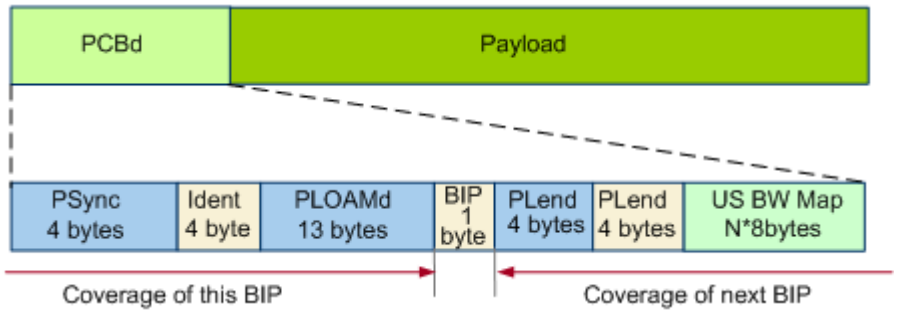
下行帧长固定为125us，下行帧由物理控制块（PCBd，Physical Control Block downstream）和Payload组成，OLT以广播的方式向ONU发送，每个ONU都会收到整个PCBd，然后会根据相关的信息执行动作。PCBd主要包括物理帧头控制字和上行带宽许可BWmap（Bandwidth Map）。

- 帧头控制字主要是用来做帧定界、时钟同步和FEC等信息。
- BWmap字段主要是通知每个ONU的上行带宽分配情况。确定每个ONU的所属T-CONT的上行开始时隙和结束时隙，确保所有ONU能按照OLT统一规定的时隙发送数据，避免数据冲突。

图4-11中的PCBd帧结构如图4-12所示。

版权所有 © 华为技术有限公司

图 4-12 PCBd 结构



PCBd里包含：帧同步信息，物理层OAM，BIP校验字段等。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。PCBd帧由PSync、Ident、PLOAMd、BIP、PLend和US BW Map字段构成，具体含义如表4-3所示：

表 4-3 PCBd 字段说明

字段名称	字段描述	含义
PSync	物理同步域即帧同步信息	ONU可以通过它找到每一帧的开始。
Ident	识别域	用于指示帧结构的大小顺序。
PLOAMd (PLOAM downstream)	下行数据的PLOAM消息	上报ONU的维护、管理状态等管理消息（不是每帧都有，可以不发，但是需要协商）。
BIP	比特间插奇偶校验	对前后两帧BIP字段之间的所有字节（不包括前导和定界）做奇偶校验，用于误码监测。
PLend	下行净荷长度	指定BWmap字段的长度。
US BW Map (Upstream Bandwidth 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。BWmap标识了各个T-CONT传送的起止时刻。

4.1.5.4 OMCI

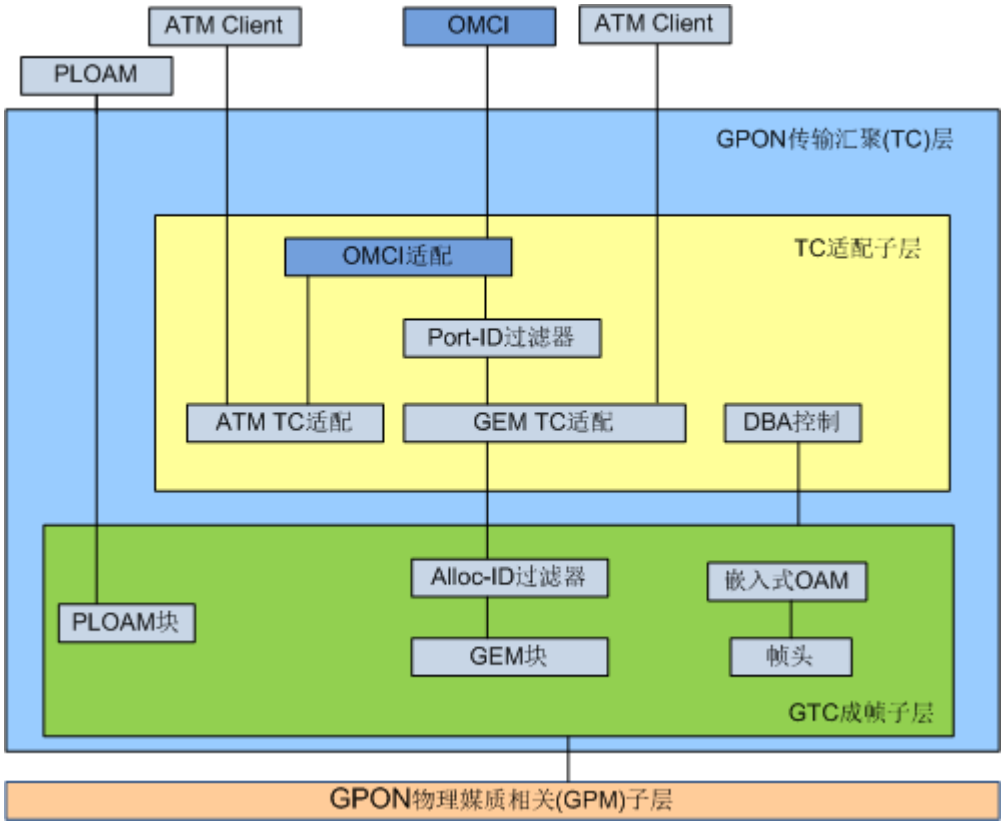
基本概念

OMCI（ONU Management and Control Interface）是ITU-T G.984.4标准中定义的一种配置传输通道，通过在OLT和ONT之间建立专有的ATM PVC或者GEM Port传输OMCI消息，用于提供标准的发现ONU能力，并对其进行管理和控制的方法。

版权所有 © 华为技术有限公司

OMCI 在 GPON 协议栈中的位置

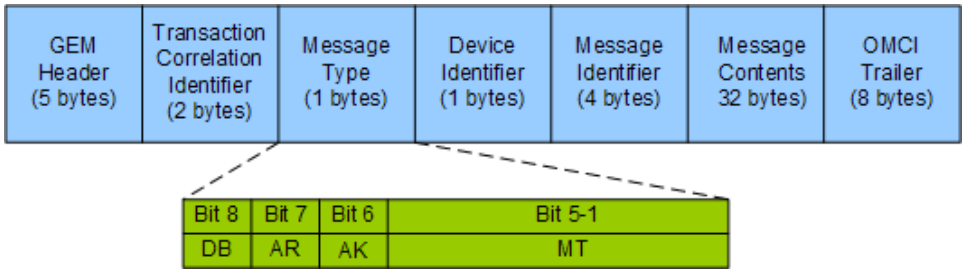
图 4-13 GPON 协议栈



OMCI 消息格式

OMCI具有严格的大小控制和内容格式定义，消息格式固定为53个字节，其中OMCI原始数据单元为48个字节。具体定义如图4-14所示。

图 4-14 OMCI 消息定义



- GEM Header：GEM头信息，包含GEM净荷长度、GEM portID、PTI（Payload Type Indicator）和HEC（Header Error Control）。
- Transaction Correlation Identifier：事务相关标识，一组对应请求和响应的消息中该字段值要一致。该字段的最高位表示该OMCI消息的优先级，0表示低优先级，1表示高优先级。

版权所有 © 华为技术有限公司

- Message type:
  - DB: Destination Bit：固定为0。
  - AR: Acknowledge Request：指示该OMCI消息是否需要对端回应(1：需要回应；0：不需要回应)。
  - AK: Acknowledgement：指示该OMCI是否是回应消息(1: 是；0: 否。)
  - MT: Message Type：指示消息类型，共支持32种消息类型，主要消息类型有：Create、Delete、Set、Get、MIB upload。在协议G.984.4中采用编码4到28，其余的预留。
- Device identifier：DeviceID值固定为0xA。
- Message Identifier：两个字节的实体ID，两个字节的实例ID。
- Message Contents：报文净荷。
- OMCI trailer：两字节固定为0，两字节为报文长度0x28，四字节CRC位。

OMCI 的管理功能

OLT通过OMCI来控制ONT。协议允许OLT进行下列动作：

- 建立和释放与ONT之间的连接
- 管理ONT的UNI
- 向OSS请求配置信息和性能统计
- 向网管自动上报事件，如链路故障

OMCI协议在OLT控制器和ONT控制器之间的GEM连接上运行，该连接在ONT初始化时建立。OMCI协议是异步的：OLT上的控制器是“主”，ONT上的控制器是“从”。一个OLT控制器通过在不同的控制信道上使用多个协议实例来控制多个ONT。

OMCI在下面几个方面对ONT进行管理：

- 配置管理：提供了控制、识别、从ONT收集数据和向ONT提供数据的功能。
- 故障管理：支持有限的故障管理功能，大多数操作仅限于进行故障指示。
- 性能管理：主要是性能监控。
- 安全管理：使能/去使能下行加密功能、全光纤保护倒换能力管理。

4.1.6 GPON 关键技术

GPON关键技术包括：

- 测距
- 突发光电技术
- DBA
- FEC
- 线路加密技术

4.1.6.1 测距

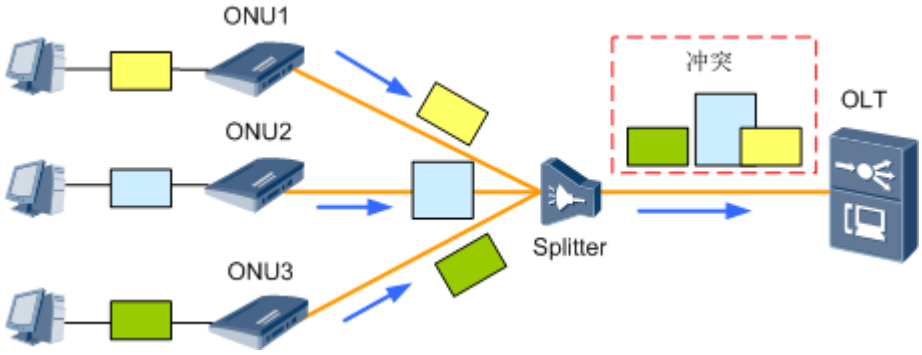
为什么要测距（Ranging）

对OLT而言，各个不同的ONU到OLT的逻辑距离不相等，光信号在光纤上的传输时间不同，到达各ONU的时刻不同。同时，OLT与ONU的环路时延（RTD：Round Trip

版权所有 © 华为技术有限公司

Delay）也会随着时间和环境的变化而变化。因此在ONU以TDMA方式（也就是在同一时刻，OLT一个PON口下的所有ONU中只有一个ONU在发送数据）发送上行信元时可能会出现碰撞冲突，如图4-15所示。为了保证每一个ONU的上行数据在光纤汇合后，插入指定的时隙，彼此间不发生碰撞，且不要间隙太大，OLT必须对每一个ONU与OLT之间的距离进行精确测定，以便控制每个ONU发送上行数据的时刻。

图 4-15 无测距的信元传输



测距原理

测距的过程如下：

- OLT在ONU第一次注册时就会启动测距功能，获取ONU的往返延迟RTD（Round Trip Delay），计算出每个ONU的物理距离。
- 根据ONU的物理距离指定合适的均衡延时参数（EqD：Equalization Delay）。

说明

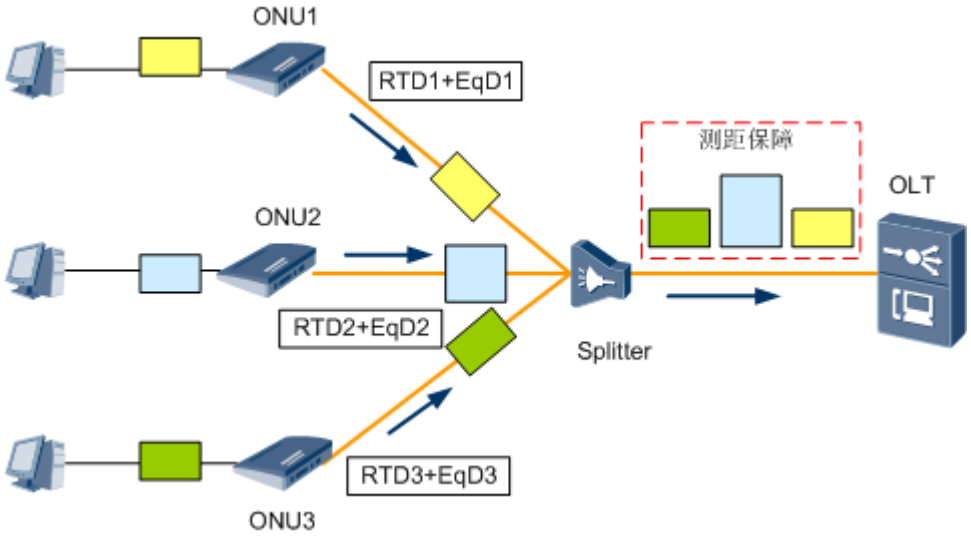
OLT在测距的过程需要开窗，即Quiet Zone，暂停其他ONU的上行发送通道。OLT开窗通过将BWmap设置为空，不授权任何时隙来实现。

测距结果

通过RTD和EqD，使得各个ONU发送的数据帧同步，保证每个ONU发送数据时不会在分光器上产生冲突。相当所有ONU都在同一逻辑距离上，在对应的时隙发送数据即可，从而避免上行信元发生碰撞冲突。

版权所有 © 华为技术有限公司

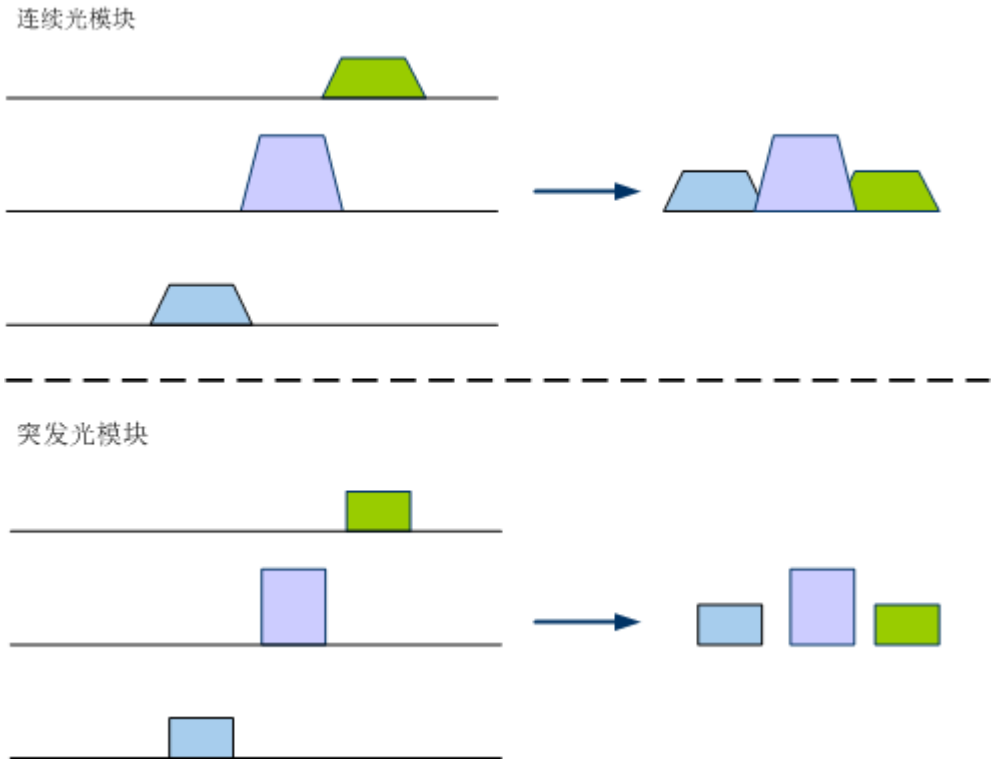
图 4-16 有测距的信元传输



4.1.6.2 突发光电技术

GPON上行方向采用时分复用的方式工作，每个ONU必须在许可的时隙才能发送数据，不属于自己的时隙必须瞬间关闭光模块的发送信号，才不会影响其他ONU的正常工作。对于OLT侧上行接收来讲，必须要根据时隙进行突发接收每个ONU的上行数据，因此，为了保证GPON系统的正常工作，ONU侧的光模块必须支持突发发送功能（如图4-17所示），OLT侧的光模块必须支持突发接收功能（如图4-18所示）。

图 4-17 ONU 侧突发发送功能示意



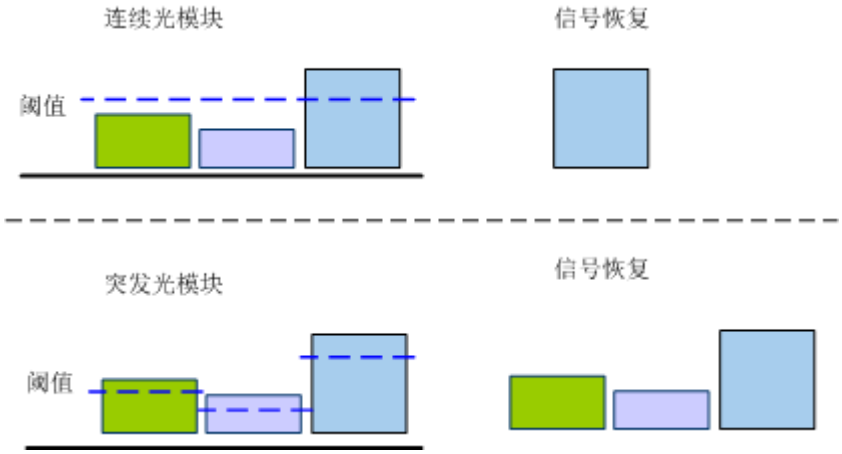
版权所有 © 华为技术有限公司

测距保证不同ONU发送的信元在OLT端互不冲突，但测距精度有限，一般为正负1bit，不同ONU发送的信元之间会有几bits的防护时间（但不是比特的整数倍），如果ONU侧的光模块不具备突发发送功能，则会导致发送信号出现叠加，信号会失真。

说明

GPON下行是按照广播的方式将所有数据发送到ONU侧，因此，要求OLT侧的光模块必须连续发光，ONU侧的光模块也是连续接收方式工作，所以无需光模块具有突发发送/接收功能。

图 4-18 OLT 侧突发接收功能示意



- 由于每个ONU到OLT的距离不同，所以光信号衰减对于每个ONU来讲都是不同的，所以就可能导致OLT在不同时隙接收到的报文的功率电平是不同的。
- 如果OLT侧的光模块不具备光功率突变的快速处理，则会导致距离较远、光功率衰减较大的ONU光信号到达OLT的时候，由于光功率电平小于阈值恢复出错误的信号（高于阈值电平才认为有效，低于阈值电平则无法正确恢复）。动态调整阈值功能可以在OLT按照收光信号的强弱动态调整收光功率的阈值以保证所有ONU的信号可以完整恢复。

4.1.6.3 DBA

在GPON系统中，OLT通过向ONU发送授权信号来控制上行数据流。PON结构需要一个有效的TDMA机制控制上行流量，这样来自多个ONU的数据包在上行过程中不会发生碰撞。然而，使用基于碰撞的机制需要在PON的无源ODN里管理QoS，这在物理上是不可能实现的，或者需要承受效率的严重损失。

鉴于这些问题，管理上行GPON流量的机制一直是GPON流量管理标准化过程中的首要关注焦点。这便促使ITU-T G.984.3标准的发展，该标准定义了用于管理上行PON流量的动态带宽分配（DBA，Dynamically Bandwidth Assignment）协议。

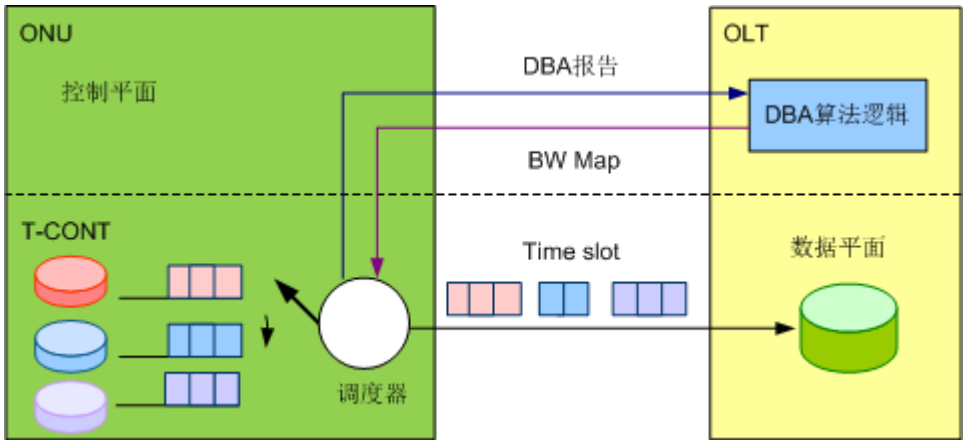
DBA对PON的拥塞进行实时监控，OLT根据拥塞和当前带宽利用情况，以及配置情况进行动态的带宽调整。DBA可以实现以下功能：

- 可以提高PON端口的上行线路带宽利用率
- 可以在PON口上增加更多的用户
- 用户可以享受到更高带宽的服务，特别适用于对带宽突变比较大的业务

DBA原理如图4-19所示。

版权所有 © 华为技术有限公司

图 4-19 DBA 原理



- OLT内部DBA模块不断收集DBA报告信息，进行计算，并将计算结果以BW Map的形式下发给各ONU。
- 各ONU根据BW Map信息在各自的时隙内发送上行突发数据，占用上行带宽。这样就能保证每个ONU可以根据实际的发送数据流量动态调整上行带宽，提升了上行带宽的利用率。

还有一种带宽分配方式，即静态带宽分配，也可以称为固定带宽分配，指每个ONU占用的带宽是固定的，OLT会根据每个ONU的SLA（包括带宽、时延的指标）周期性的为每个ONU分配固定长度的授权。

- 一般来说OLT采取轮询的机制，在每个轮询周期里面，各ONU的固定带宽可能不相同，但同一个ONU在不同的周期里面固定带宽的大小应该是相同的，授权大小只和ONU的SLA有关，和ONU的上行业务流量情况无关，即使ONU上行没有流量，这部分带宽也会固定分配给ONU。
- 这种静态带宽分配的方法简单、易实现，比较适合承载TDM等业务流量固定的业务，但不能根据ONU上的流量情况实时调整上行带宽，承载突发性比较强的IP业务时的带宽利用率比较低。

4.1.6.4 FEC

在工程实践中并不存在理想的数字信道，数字信号在各种媒质的传输过程中就会产生误码和抖动，从而导致线路的传输质量下降。

为解决此问题，需要引入纠错机制。实用的纠错码是靠牺牲带宽效率来换取可靠性，同时也增加了通信设备的复杂度。纠错技术是一种差错控制技术，按照应用场景和侧重点不同，可以分为两类:

- 检错码：重在发现误码，比如奇偶监督编码。
- 纠错码：要求能自动纠正差错，比如BCH码、RS码、汉明码。

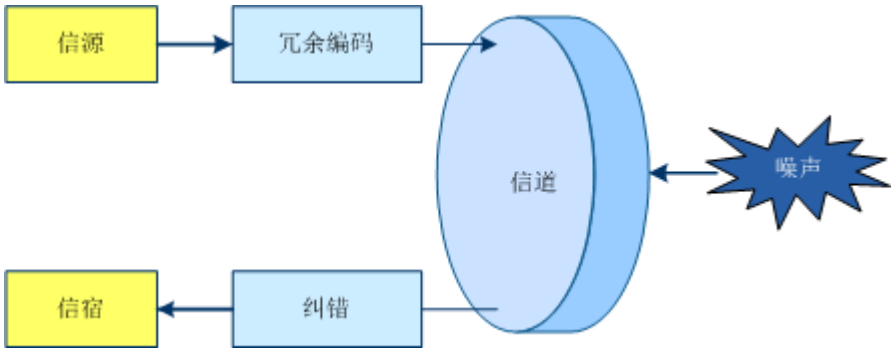
二者没有本质区别，只是应用场合不同而侧重的性能参数不同。FEC属于后者。

FEC的全称是前向纠错，一种数据编码的技术，数据的接收方可以根据编码检查传输过程中的误码。前向是指纠错过程是单方向的，不存在差错的信息反馈。

通过在发射端对信号进行一定的冗余编码，并在接收端根据纠错码对数据进行差错检测，如发现差错，由接收方进行纠正。常见的FEC技术有汉明码、RS编码以及卷积码等。FEC原理如图4-20所示。

版权所有 © 华为技术有限公司

图 4-20 FEC 原理图



GPON采用的FEC算法是RS（255，239）算法，完全遵从ITU-T G.984.3的要求。FEC码字长255字节，由239字节的正常数据和16字节的冗余开销构成。考虑多帧尾碎片开销，GPON系统开启FEC后，系统带宽降低为原吞吐量的90%左右。GPON在传输层使用FEC算法，大约可以将线路传输的10^{-3}误码降低到10^{-12}。

FEC的特点及应用：

- 无需重传，实时性高
- FEC启动后，能够容忍线路上更大的噪声，但是有额外的带宽开销（用户需要根据实际情况在传输质量和带宽间做出选择）
- 适合于数据到达对端后通过自身来查验并纠正的业务，不适合于查验有重传机制的业务
- 可用于网络状况较差时的数据传输，如：在工程使用中，ONT距离远，线路质量差，导致光功率预算裕量不足或线路误码率高，推荐开启FEC
- 可用于要求时延较小的业务（因为此时如果采用重传，则时延会增大）

4.1.6.5 线路加密技术

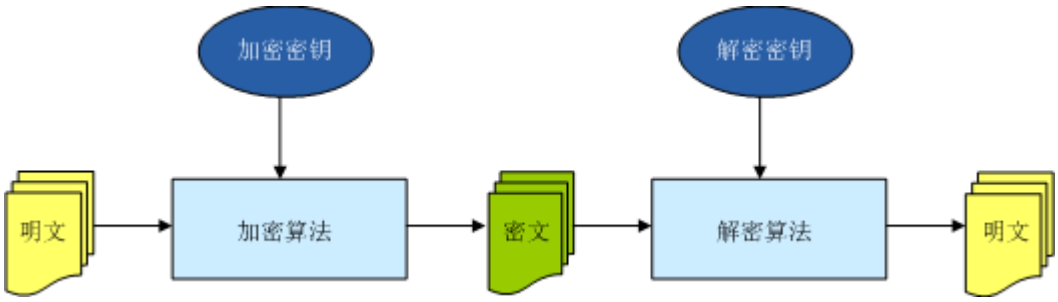
GPON系统中下行数据采用广播的方式发送到所有的ONU上，这样非法接入的ONU可以接收到其他ONU的下行数据，存在安全隐患。

GPON系统采用线路加密技术解决这一安全问题。GPON系统采用AES-128加密算法将明文传输的数据报文进行加密，以密文的方式进行传输，提高安全性。在安全性能要求高的场景，建议打开加密功能。

- GPON系统中使用的加密算法，不会增加额外开销，而且对带宽效率无影响。
- GPON系统中使用的加密功能开启，不会导致传输时延加大。

线路加解密过程如图4-21所示。

图 4-21 线路加解密过程



版权所有 © 华为技术有限公司

密钥更换

GPON系统定期的进行AES密钥交换和更新，提高了线路数据的可靠性。

1. OLT发起密钥更换请求，ONU响应并将生成的新的密钥发给OLT。
2. OLT收到新的密钥后，进行密钥切换，使用新的密钥对数据进行加密。
3. OLT将使用新密钥的帧号通过相关的命令通知ONU。
4. ONU收到使用新密钥的帧号后，在相应的数据帧上切换校验密钥。

说明

- 由于PLOAM（Physical Layer OAM）消息的长度有限，密钥分两部分发给OLT，并重复发送三次。如果OLT没有收到三次传送中的任意一次，OLT将重新发送密钥更换请求，直到三次收到相同的密钥为止。
- OLT使用相关的命令通知ONU使用新密钥的帧号，这个命令会重复发送三次。只要ONU收到一次，ONU就在相应的数据帧上切换校验密钥。

4.1.7 GPON 终端认证及管理

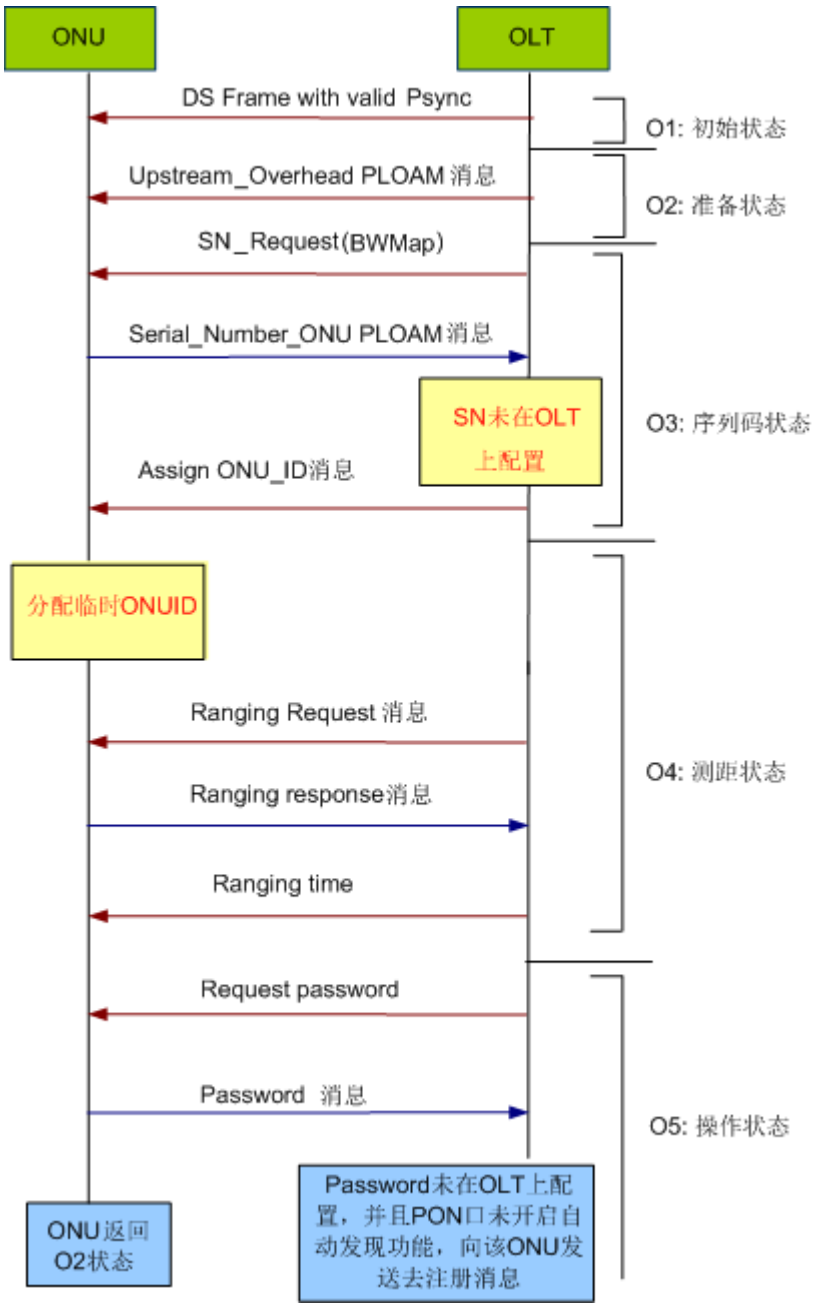
GPON终端认证是指OLT基于上报的认证信息对ONU合法性进行认证，拒绝非法ONU的接入。在GPON系统中，只有通过认证的合法ONU才能接入PON系统，ONU认证上线后才可以传输数据。

4.1.7.1 终端认证（ONU 未预配置）

OLT上未预配置的ONU的注册流程如图4-22所示。

版权所有 © 华为技术有限公司

图 4-22 未预配置 ONU 注册流程图



- OLT向ONU发送SN（Serial Number）请求。
- ONU响应OLT的SN请求。
- OLT收到ONU的SN回应消息后，分配一个临时ONU ID给该ONU。
- ONU进入操作阶段后，OLT会向ONU发送Password请求。ONU向OLT回应Password，该Password未在OLT上配置。
  - 如果OLT的PON口未开启自动发现功能，则OLT向ONU发送去注册消息，ONU重新向OLT发送注册请求。
  - 如果OLT的PON口开启了自动发现功能，则会向主机命令行或者网管上报ONU自动发现告警。该ONU经过确认后才会正常上线。

版权所有 © 华为技术有限公司

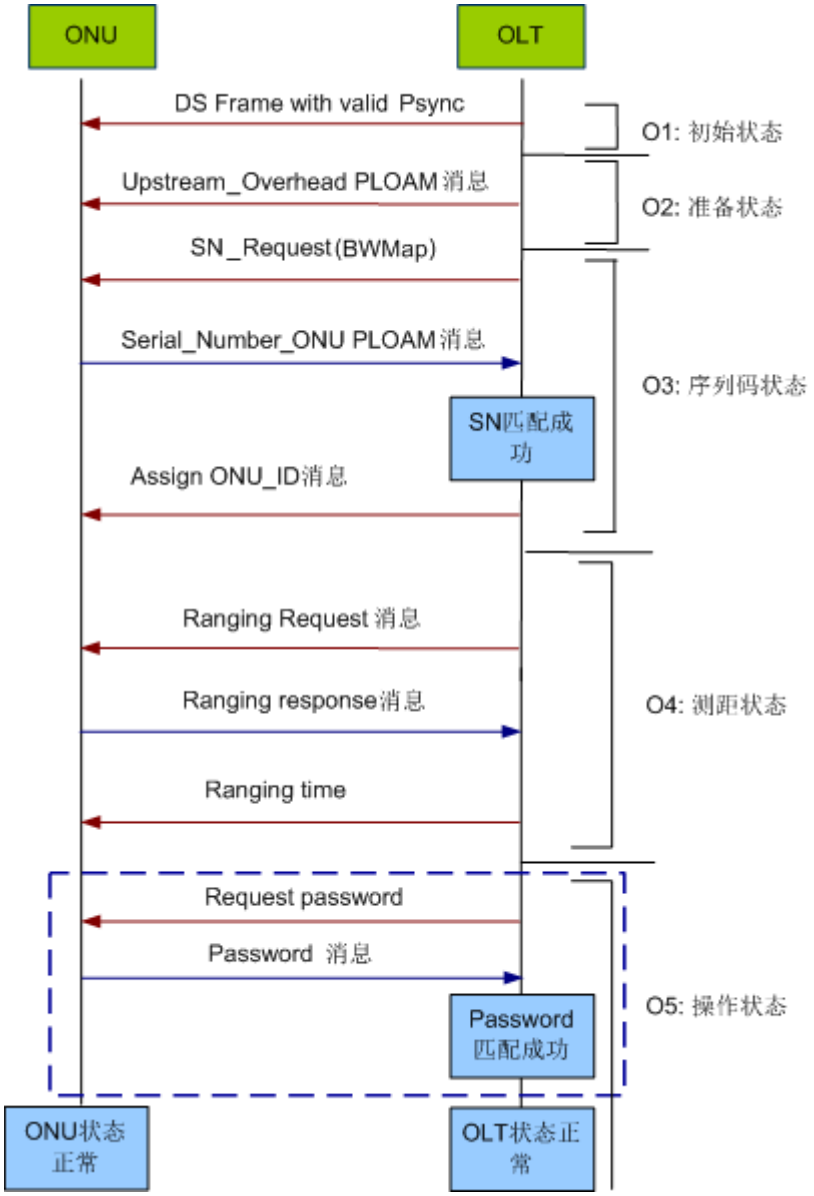
4.1.7.2 终端认证（ONU 已预配置）

对OLT上已经预配置的ONU的认证方式，包括SN、SN+Password和Password。

SN 和 SN+Password 认证

SN认证是指OLT只对ONU的序列码进行匹配的一种认证方式。SN+Password认证方式要同时匹配SN和Password。认证过程如图4-23所示。

图 4-23 SN/SN+Password 认证流程



说明

对于SN认证方式的ONU，认证流程中无需Password步骤。

版权所有 © 华为技术有限公司

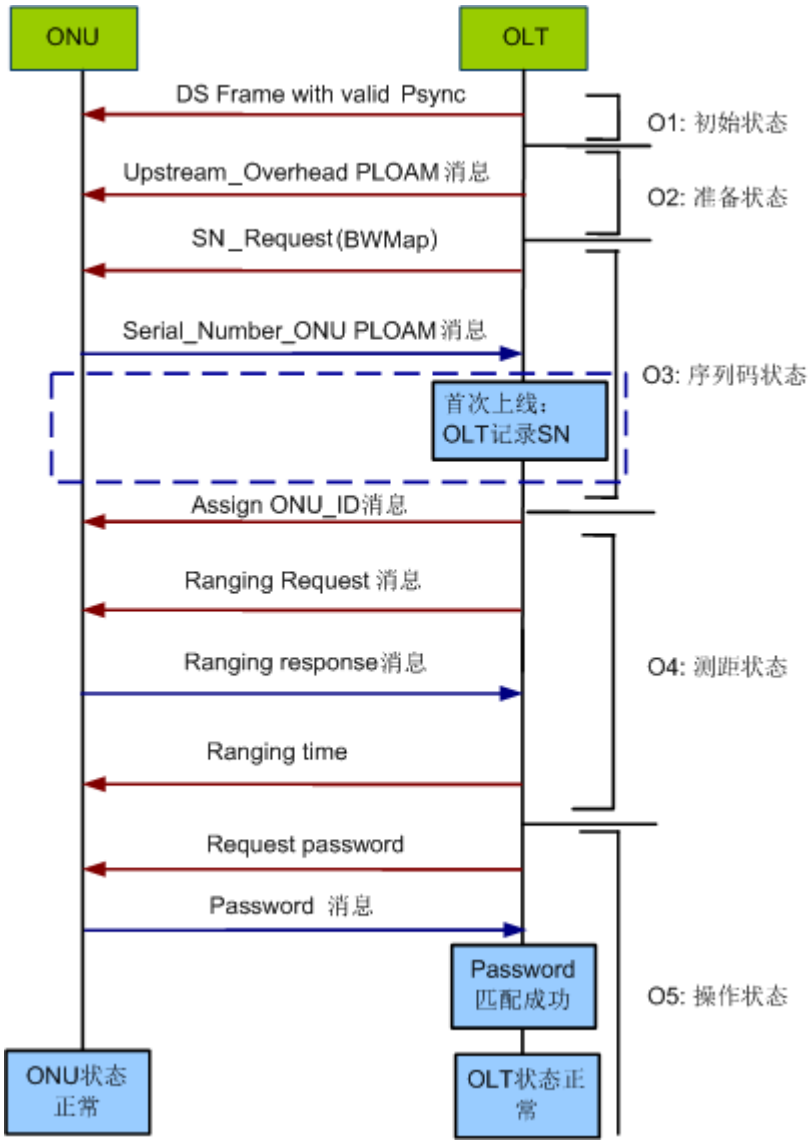
- OLT收到ONU的序列码回应消息后，判断OLT上是否有相同SN的ONU在线。如果有相同SN的ONU在线，则向主机命令行和网管上报SN冲突告警；否则，直接给ONU分配指定的ONUID。
- ONU进入操作状态后:
  - 对于SN认证方式的ONU，OLT不进行Password请求，直接为该ONU配置用于承载OMCI消息的GEM Port后让ONU上线，配置方法可以由OLT自动配置，使得承载OMCI的GEM Port与ONUID相同，并向主机命令行或者网管上报ONU上线告警。
  - 对于SN+Password认证方式的ONU，OLT会向ONU进行Password请求，并将ONU回应的Password与本地配置的Password进行比较，如果Password与本地配置相同，则直接为ONU配置用于承载OMCI消息的GEM Port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，则向主机命令行或者网管上报Password错误告警。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

首先预添加Password认证方式的ONU，然后在PON口下接入该ONU。ONU进行Password认证时，如果ONU的SN或者Password与OLT上已在线ONU的冲突，则将该ONU进行去注册处理，不会对在线ONU造成影响。Password认证有两种模式，Once-on和Always-on。

版权所有 © 华为技术有限公司

图 4-24 Password 认证流程



说明

Always-on模式认证流程时，ONU首次上线时OLT无需记录SN。

Once-on模式的应用场景

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。选择Once-on模式时，可以设置aging-time。设置了aging-time后，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，并且一旦ONU认证成功后，就不允许再修改SN。

在Once-on模式下，

- ONU首次认证是基于Password认证的，认证过程如图4-24所示。
- ONU非首次认证时，可以根据命令行配置选择SN认证或者SN + Password认证，认证过程如图4-23所示。

版权所有 © 华为技术有限公司

说明

对于Once-on模式认证的ONU，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。

Always-on模式的应用场景

运营商为用户分配Password后，用户可以更换使用相同Password不同SN的ONU，在更换ONU后不需要通知运营商。Always-on模式下，对用户接入上线时间无限制，即无论什么时候接入ONU，只要ONU的Password正确，ONU都可以上线。

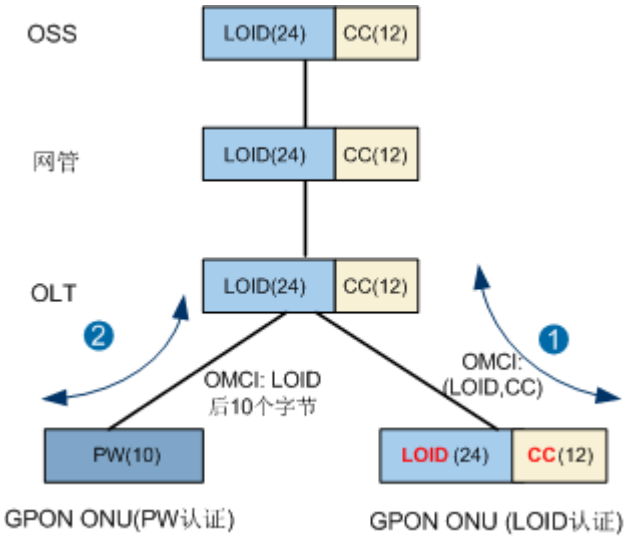
- ONU首次上线时使用Password认证，认证上线成功后，OLT根据用户的SN和Password，生成SN + Password绑定表项。认证过程如图4-24所示。
- ONU非首次上线时，
  - 如果ONU的SN和Password与首次上线成功ONU的SN以及Password相同，则使用SN + Password认证，认证过程如图4-23所示。
  - 如果用户使用相同Password不同SN的ONU，则根据Password进行认证，认证上线成功后，更新SN + Password绑定表项。认证过程如图4-24所示。

4.1.7.3 终端认证（中国电信标准）

LOID（Logical ONU ID）+ CC（CheckCode）认证方式是由中国电信的CTC2.1标准定义的一种认证方式。LOID为24个字节，CC为12个字节，其中CC为可选字节。不选CC时，则为LOID-AUTH认证方式。中国电信在此基础上扩展出新GPON OMCI（Optical network terminal Management and Control Interface）实体，支持LOID+CC认证方式。

OSS系统使用GPON LOID+CC认证流程如图4-25所示。

图 4-25 GPON LOID+CC 认证流程图



LOID+CC认证过程为：

版权所有 © 华为技术有限公司

1. OLT先去ONU获取LOID+CC（ONU的LOID+CC通过WEB界面进行配置），如果匹配则认证通过。
2. 如果认证不匹配，则OLT再去获取ONU的PW（Password）。然后与LOID的后10字节匹配，如果匹配则认证通过。

说明

- 在规划时需要保证LOID的后10字节不能重复。
- 如果使用LOID认证，则流氓ONU排查功能不可用。
- 如果用户输入的LOID/CC的实际长度小于24字节/12字节，则在实际的ONU_ID/CC后面填ASCII码的“NUL”（十六进制数为0x00）以补足24字节/12字节。

4.1.7.4 终端管理

GPON系统的ONU管理通过PLOAM（Physical Layer OAM）和OMCI消息进行管理。

PLOAM协议在ITU-T G.984.3中定义，主要是用来交互GPON物理层和TC层的管理维护信息，如DBA信息，DBRu等信息。

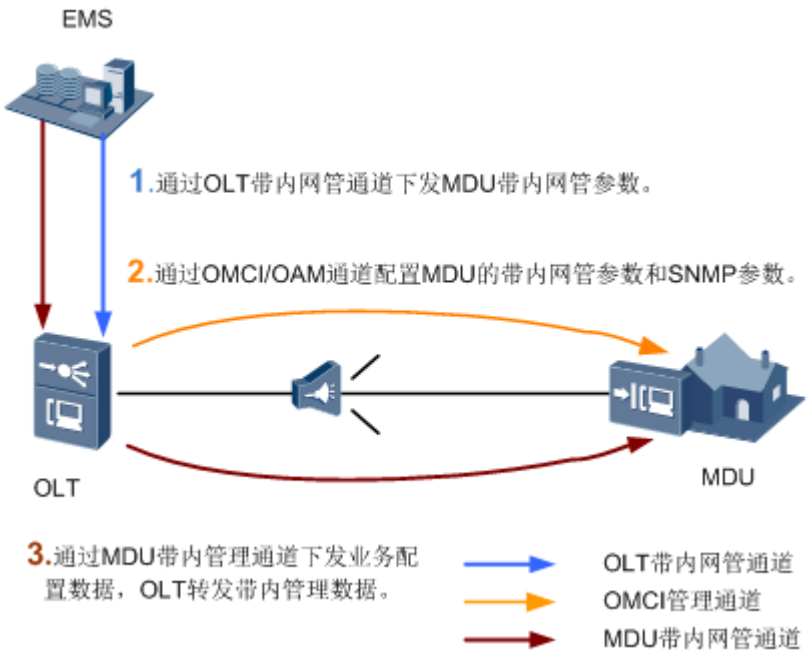
GPON系统的ONU(包括MDU和ONT)管理主要通过OMCI消息进行管理，支持离线部署、即插即用、自动业务发放。OMCI的管理功能参见**4.1.5.4 OMCI**。

- OMCI消息主要用于业务层次的管理维护，如设备的硬件能力发现、各种告警维护信息和业务能力配置等。
- OMCI支持对ONU的离线配置，由于ONU本地不需要保存配置信息，所以便于业务发送。

MDU 管理

MDU管理通道配置流程如**图4-26**所示。

图 4-26 MDU 管理通道配置流程



版权所有 © 华为技术有限公司

1. 网管通过OLT带内网管通道下发MDU带内网管参数到OLT。
2. OLT通过OMCI/OAM通道配置MDU的带内网管参数和SNMP参数。建立MDU带内网管通道。
3. 网管通过MDU带内管理通道下发业务配置数据。MDU带内管理通道建立后，网管直接通过SNMP通道对其进行配置和管理，OLT只需转发MDU带内管理数据，不再需要处理相关配置。

4.1.8 长发光 ONU 检测

概述

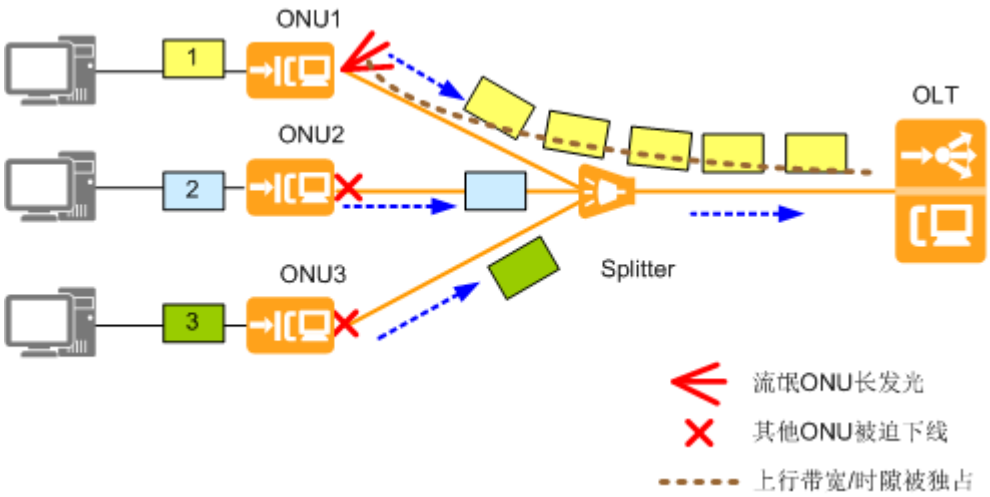
PON遵循P2MP（point-to-multipoint）的网络架构，上行方向采用TDMA（time division multiple access，时分复用）方式，ONU必须按照OLT分配的时间戳向上行方向发送数据才能保证数据依次上行到OLT设备而不产生冲突。

不按照分配的时间戳向上行方向发送光信号的ONU叫长发光ONU。长发光ONU又名长发光流氓ONU，指任意时刻都在发光的ONU。

当系统出现长发光ONU时：

- 如果该ONU已上线，会导致同一PON口下其他某个ONU或者所有ONU下线或者频繁上下线。
- 如果该ONU未配置，会导致PON口下其它未配置的ONU不能被正常自动发现。

图 4-27 流氓 ONU 示意图



流氓 ONU 检测机制

长发光ONU检测又名流氓ONU检测，用来检测系统中长发光ONU并进行隔离处理，确保系统正常运行。针对长发光流氓ONU的处理一般分为三个过程：检测、排查、隔离。

图 4-28 长发光流氓 ONU 处理步骤

版权所有 © 华为技术有限公司

- 检测（check）：检测就是定时对PON口进行测试，检查是否存在流氓ONU。检测过程只能判断PON端口下存在长发光流氓ONU，不能定位具体的ONU。

  OLT在PON上行方向开空窗，进行ONU上行光信号的检测，此时如果检测到上行还有收光，则进入长发光ONU排查流程。

- 排查（detect）：排查过程就是确定具体哪个ONU是流氓ONU的过程。

  OLT下发指令逐个打开ONU光模块的上行发光，检测是否有上行光信号，并判断当打开某个ONU后是否会导致其它ONU下线，如果某个ONU打开后导致其他的ONU均下线，就说明该ONU为长发光ONU。长发光ONU的检测流程将对该PON口上的所有ONU均检测一遍，确保将所有长发光ONU均检测出来。

- 隔离（isolate）：隔离就对ONU下发指令，关闭ONU光模块的发送电源，消除流氓ONU对PON口下其他ONU的影响。

  一旦ONU光模块上行发光被OLT关断后，这个关断将是永久性的，即ONU复位或掉电重启其光模块的上行发光也是被关断的，除非OLT下发命令重新打开，该机制保障了长发光ONU被彻底隔离。

说明

OLT默认只对流氓ONU做检测，不进行自动排查和隔离。

约束与限制

- OLT对PON线路上行方向发光异常做判断和分析，只能针对非恶意用户识别并隔离流氓ONU；对于人为破坏或不符合规定的ONU，不在本特性解决范围。
- 长发光流氓ONU要求能够解析下行PLOAM、OAM消息并正确响应。
- 仅当ONU支持标准PLOAM消息（GPON：ITU-T G.988或G.984.3）、OAM消息（EPON：CTC3.0），正确进行ONU光模块开关控制，才能保证在OLT判断PON口下存在长发光ONU后，快速定位具体的ONU。当PON口上有未配置的ONU出现长发光状态，会导致PON口下其它未配置的ONU不能被正常自动发现。

4.1.9 参考标准与协议

GPON特性参考标准和协议如下：

标准编号	标准描述
ITU-T G.984.1	General characteristics，主要讲述GPON技术的基本特性和主要的保护方式。
ITU-T G.984.2	Physical Media Dependent (PMD) layer specification ，主要讲述了GPON的物理层参数，如光模块的各种物理参数，包括发送光功率、接收灵敏度、过载光功率等。同时定义了不同等级的光功率预算，如目前最常用的Class B+。
ITU-T G.984.3	Transmission convergence layer specification，主要讲述了GPON的TC层协议，包括上下行的帧结构及GPON的工作原理。

版权所有 © 华为技术有限公司

标准编号	标准描述
ITU-T G.984.4	ONT management and control interface specification，主要讲述GPON的管理维护协议，包括OAM，PLOAM和OMCI协议。
ITU-T G.984.5	Enhancement band，主要讲述GPON的波长规划，为下一代PON预留了相应的波段。
ITU-T G.984.6	Reach extension，主要介绍了几种延长GPON传输距离的Long Reach PON的技术方案。
ITU-T G.988	ONU management and control interface (OMCI) specification。
TR-156	Using GPON Access in the context of TR-101

4.2 EPON

4.2.1 EPON 介绍

定义

EPON网络使用单根光纤两种波长传输双向1.25Gbit/s的数字信号，上行方向采用1310nm波长窗口，下行方向采用1490nm波长窗口。EPON网络由OLT（Optical Line Terminal）、ONU（Optical Network Unit）和ODN（Optical Distribution Network）组成，物理拓扑是点到多点的树形网络，逻辑拓扑是OLT到各个ONU的多个点对点链路。其中，ODN起连接OLT和ONU的作用。

目的

EPON作为PON技术之一，具有高带宽、长距离覆盖、组网灵活、中间网络节点无源等公共特征。应用于宽带接入网，可以提高网络带宽和性能，降低维护成本，是主流运营商青睐的光接入技术。

EPON可以应用在FTTH（Fiber To The Home）、FTTB（Fiber To The Building）、FTTO（Fiber To The Office）和FTTM（Fiber To The Mobility Base Station）的环境中，支持：

- 语音
- 数据
- 视频
- 租用线路
- 分布式业务

版权所有 © 华为技术有限公司

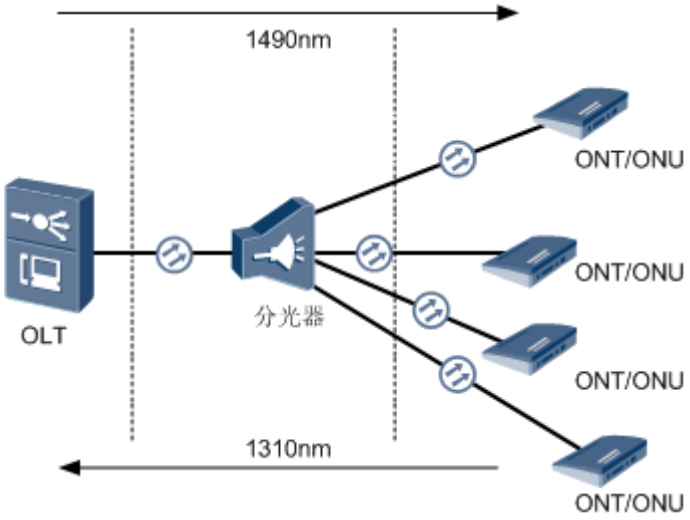
4.2.2 EPON 系统概述

EPON 拓扑结构

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4-29所示。

图 4-29 EPON 物理网络拓扑图



在EPON网络中：

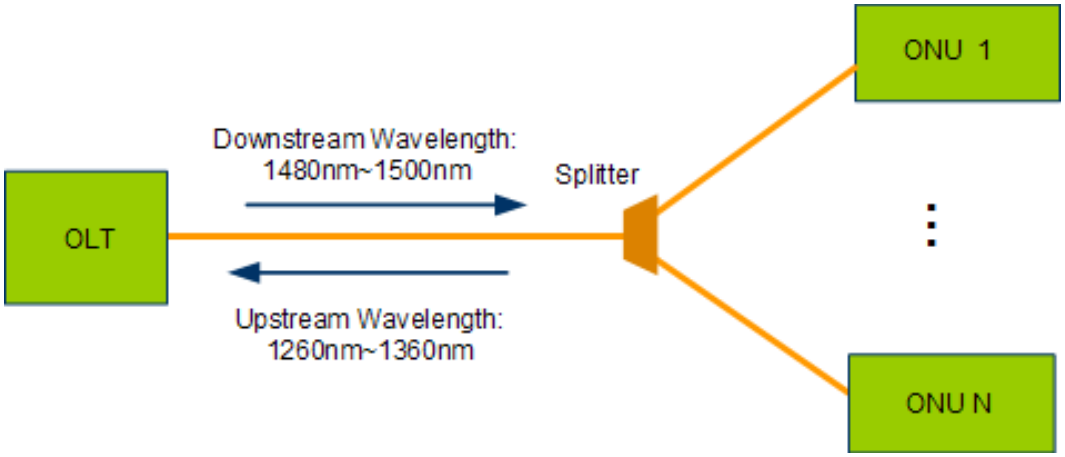
- OLT是放置在局端的终结EPON协议的汇聚设备。
- ONU是位于客户端的给用户提供各种接口的用户侧终端，OLT和ONU通过中间的无源光网络ODN连接起来进行互相通信。
- ODN由光纤、一个或多个无源光分路器等无源光器件组成，在OLT和ONU/ONT间提供光通道，起着连接OLT和ONU/ONT的作用，具有很高的可靠性。

EPON 工作原理

EPON是一种采用点到多点（P2MP）结构的单纤双向光接入网络，EPON系统采用WDM（Wavelength Division Multiplexing）技术，实现单纤双向传输。工作原理如图4-30所示。

版权所有 © 华为技术有限公司

图 4-30 EPON 工作原理

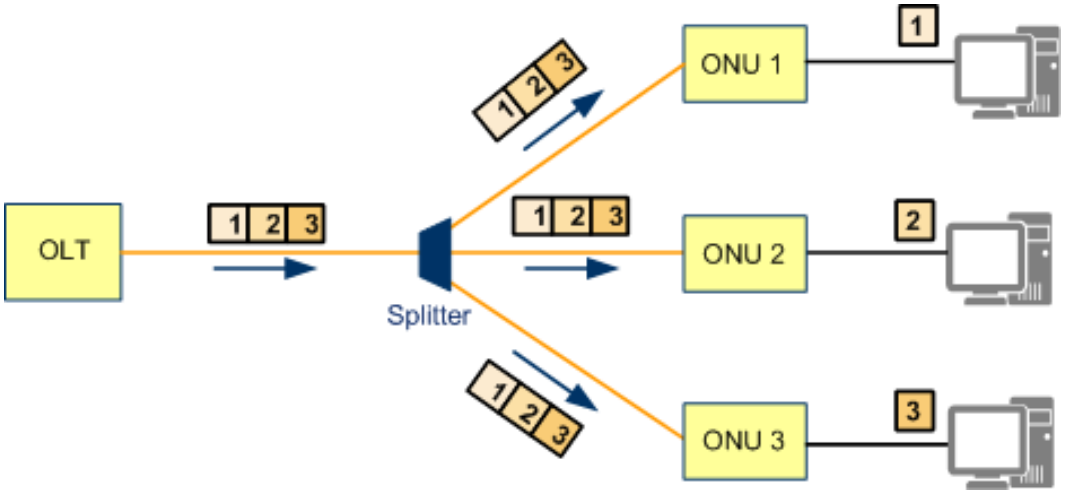


EPON下行数据流采用广播技术，使用1480nm～1500nm波长。上行数据流采用TDMA (Time Division Multiple Access)技术，使用1260nm～1360nm波长。如果采用第三波长方式实现CATV业务的承载，则使用1540nm～1560nm波长。

EPON 下行通信原理

EPON在下行方向采用广播方式，所有的ONU都能收到相同的数据，通过LLID（Logical Link Identifier）来区分不同ONU的数据，ONU过滤广播报文来接收属于自己的数据。下行通信原理如图4-31所示。

图 4-31 EPON 下行通信原理



在逻辑拓扑上，EPON协议为OLT到每个ONU建立一条逻辑链路，以太网数据帧的前导字节承载这个逻辑链路标识，即LLID（Logical Link Identity）。

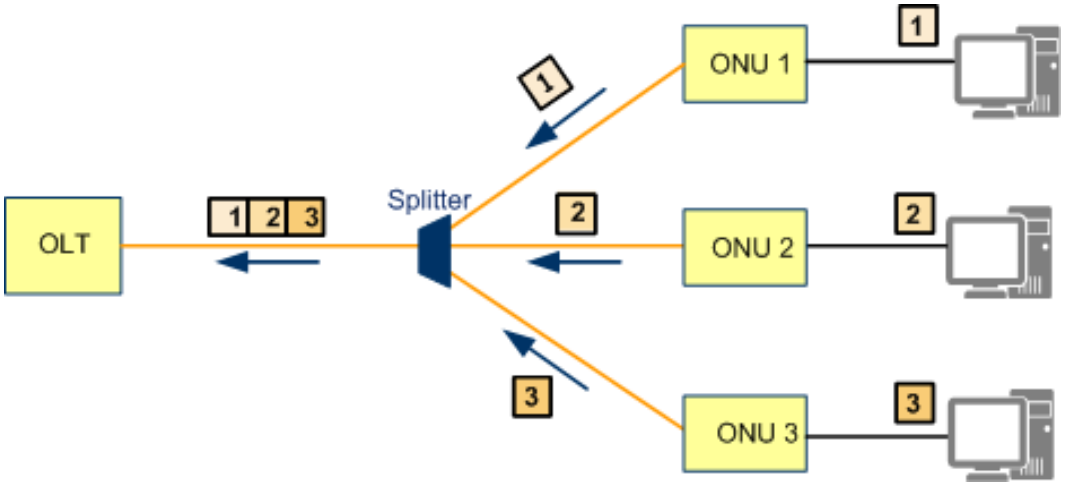
图4-31的结构中，从OLT到ONU的下行数据流被封装为以太网报文，附加相应的LLID，在树状PON网络中发送。在分光器处，流量被分成独立的三组信号广播到各个支路，每一组信号都承载所有ONU的数据。当数据信号到达ONU时，ONU根据LLID选择性接收自身数据。

版权所有 © 华为技术有限公司

EPON 上行通信原理

EPON在ONU到OLT的上行方向上，采用时分多址接入技术（TDMA）分时隙传输上行流量。上行通信原理如图4-32所示。

图 4-32 EPON 上行通信原理



当ONU注册成功后，OLT会根据系统的配置，给ONU分配特定的带宽。在采用动态带宽调整时，OLT会根据指定的带宽分配策略和各个ONU的状态报告，动态的给每一个ONU分配带宽。

带宽对于PON层面来说，就是多少可以传输数据的基本时隙，每一个基本时隙单位时间长度为16ns。在一个OLT端口（PON端口）下面，所有的ONU与OLT PON端口之间时钟是严格同步的，每一个ONU只能够在OLT给他分配的时刻上开始，用分配给它的时隙长度传输数据。通过时隙分配和时延补偿，确保多个ONU的数据信号耦合到一根光纤时，各个ONU的上行包不会互相干扰。

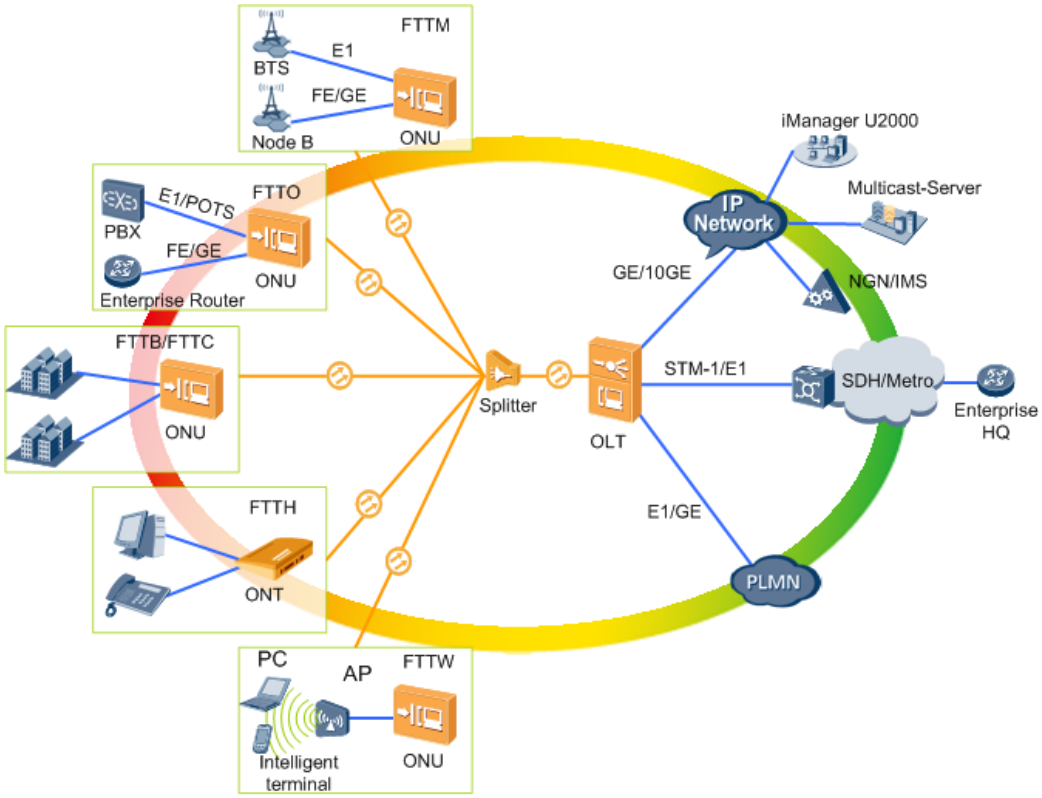
4.2.3 EPON 组网应用

FTTx 组网应用

通过EPON的应用，OLT与ONU（或ONT）可以实现FTTH、FTTO、FTTB、FTTC、FTTM的各种组网应用，如图4-33所示。

版权所有 © 华为技术有限公司

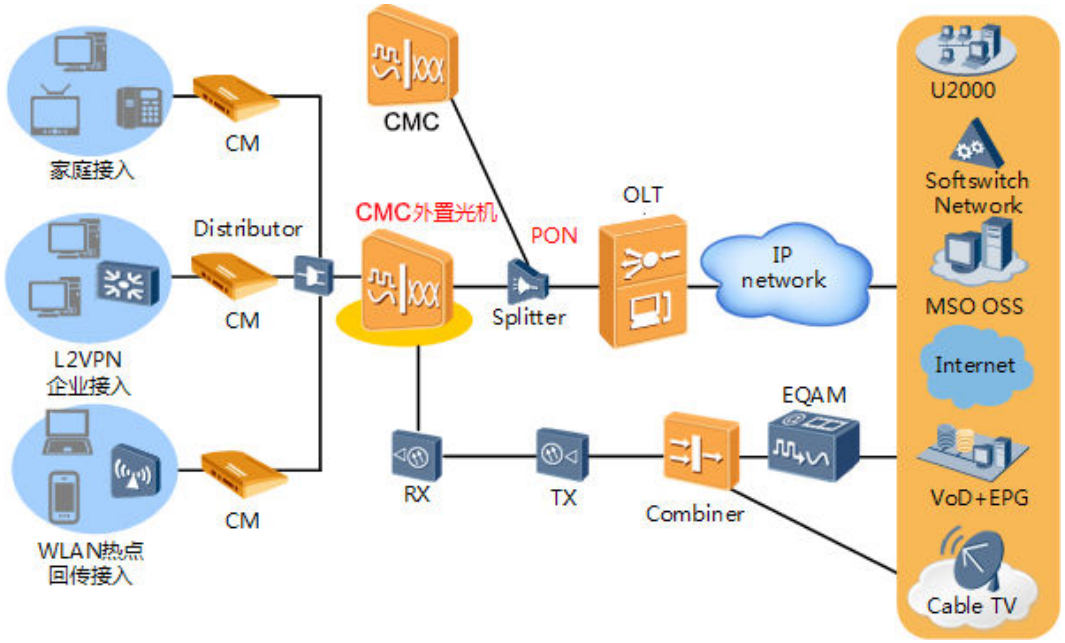
图 4-33 EPON FTTx 组网应用



PON+D-CCAP 组网应用

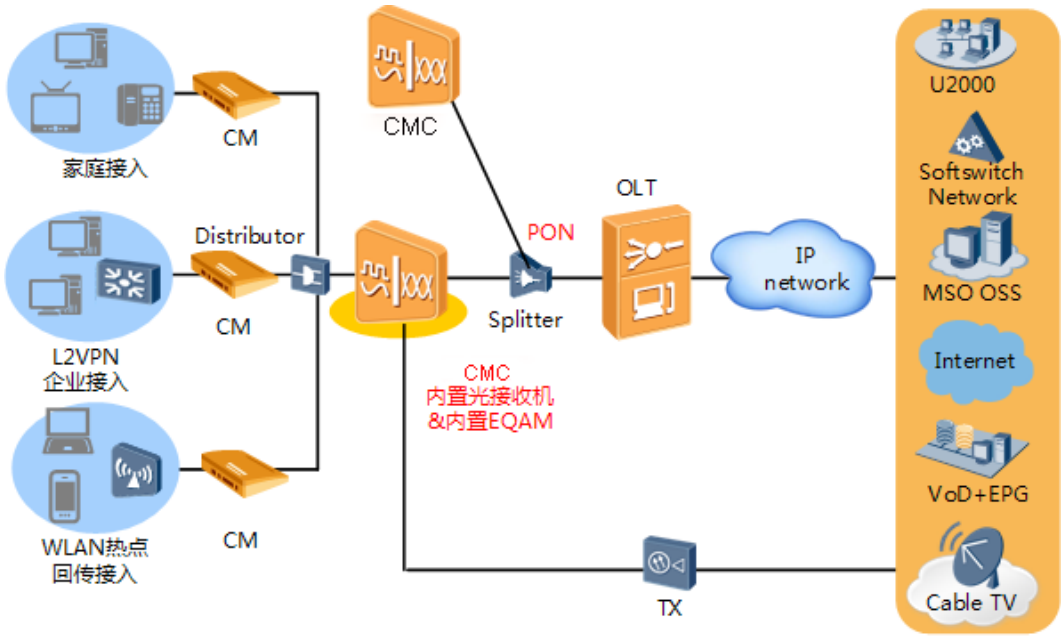
通过PON的应用，OLT与CMC可以实现PON+D-CCAP的组网应用，如图4-34和图4-35所示。

图 4-34 PON+D-CCAP 组网应用（CMC 外置光机）



版权所有 © 华为技术有限公司

图 4-35 PON+D-CCAP 组网应用（CMC 内置光接收机&内置 EQAM）



- 支持为家庭用户提供HSI（High-Speed Internet）、VoD、CATV（Cable TV）、动态语音业务，满足广电多业务发展需求。
- 支持提供企业接入新业务，支持 L2VPN，通过连接交换机实现。
- 支持提供WLAN热点覆盖回传业务，通过连接AP实现。

4.2.4 EPON 系统原理

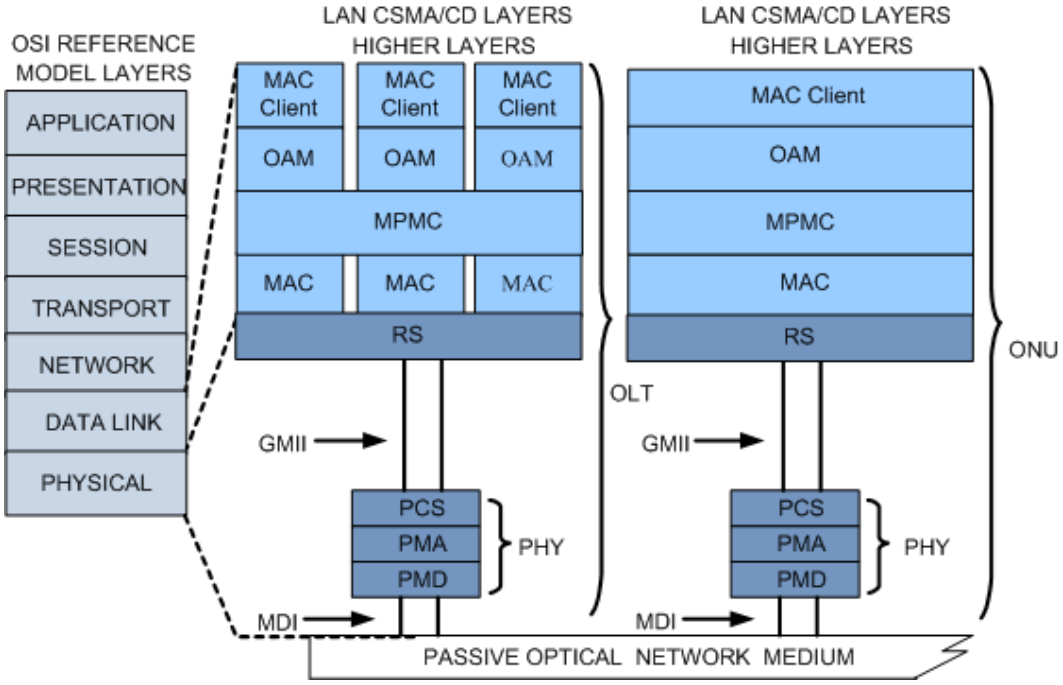
EPON 协议模型

EPON协议最初由IEEE 802.3ah进行定义，现已合并到IEEE 802.3-2005标准文本中。IEEE 802.3-2005协议文本分别从网络架构模型、MPCP(Multi-point Control Protocol)多点控制协议、OAM(Operations, Administration and Maintenance)协议、RS/PCS（Reconciliation Sublayer/Physical Coding Sublayer）子层扩展、PMD（Physical Medium Dependent）层规格参数等方面对EPON进行描述，最终基于原有802.3协议框架扩展了EPON协议，充分利用原有协议资源，降低了协议复杂度。

EPON协议模型如图4-36所示。

版权所有 © 华为技术有限公司

图 4-36 EPON 协议框架模型



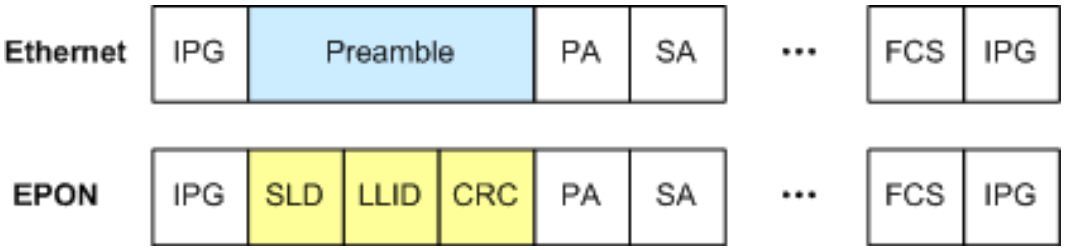
- OAM：Operation Administration Maintenance(运行、管理和维护子层)，定义了EPON各种告警事件和控制处理，使用OAM协议数据单元可对已激活OAM功能的链路进行管理、测试和诊断。
- MPMC：Multi-Point MAC Control(多点MAC控制层)，实现在不同的ONU中分配上行资源、在网络中发现和注册ONU、允许DBA调度，实现点对多点的MAC控制。
- MAC：Media Access Control(媒体访问控制层)，实现对Media的控制。
- RS：Reconciliation Sublayer(调和子层)，实现数据链路层和物理层间的接口，完成外部物理层信号(GMII接口信号)和上层信号之间的适配；同时在EPON系统中完成添加/终结LLID，调和多种数据链路层能够使用统一的物理层接口。
- PCS：Physical Code Sublayer(物理编码子层)，支持在点对多点物理介质中的突发模式，支持FEC算法。
- PMA：Physical Medium Attachment(物理媒质附加子层)，支持时钟恢复，并提供环回测试功能；支持P2MP功能，实现PMD的扩展。
- PMD：Physical Medium Dependent物理媒质相关子层（使用1000BASE-PX 接口），定义了EPON兼容器件的指标，实现PMD服务接口和MDI接口之间的数据收发功能。

EPON 帧格式

EPON帧以802.3帧格式为基础，在此基础上新增LLID，用于在OLT上标识ONU。

版权所有 © 华为技术有限公司

图 4-37 EPON 帧与 Ethernet 帧比较

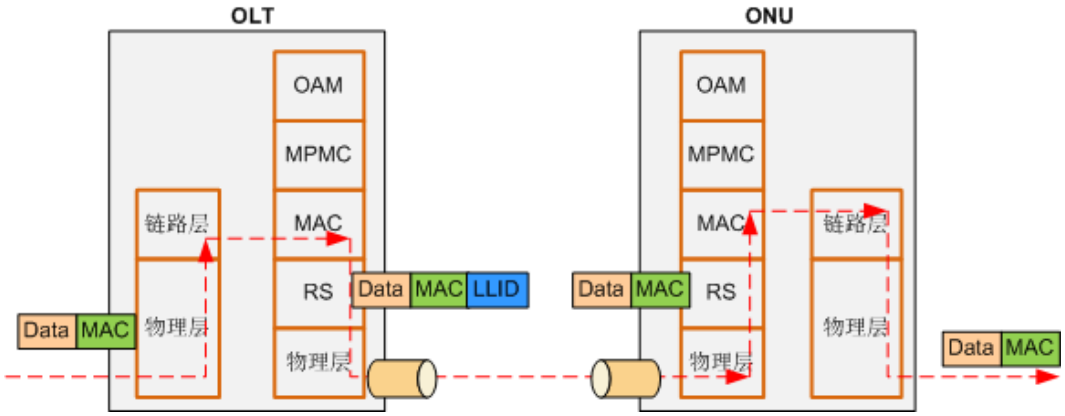


LLID为逻辑链路ID，OLT通过此ID信息与不同的ONU建立点对点逻辑通信链路。EPON标准将以太网帧的前导码做了简单的利用，将LLID信息写入了以太网帧的前导码中，以两个字节来标识，范围为0~0x5FFF。其中0x5FFF来标识广播链路，其他用于单播链路。

EPON 业务流转发

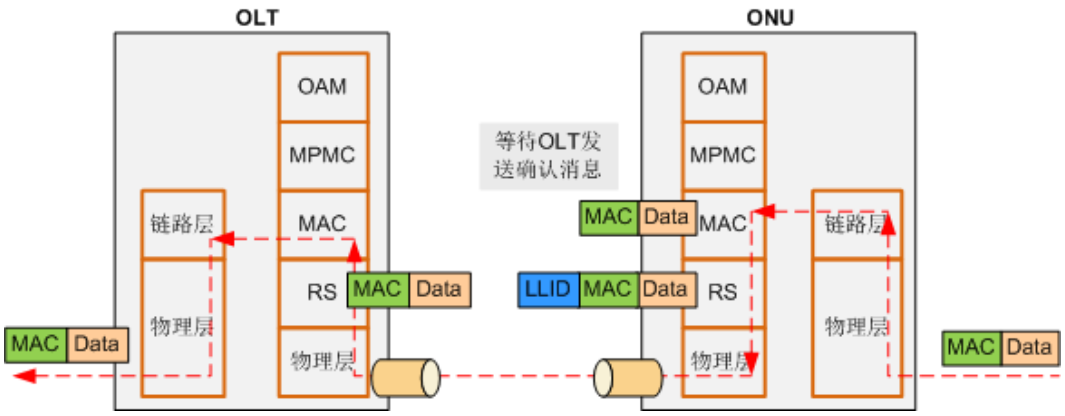
EPON业务流转发过程如图4-38、图4-39所示。

图 4-38 EPON 业务数据流转发过程图（下行）



在下行方向上（OLT->ONU），OLT为每一个发送给ONU的数据包都增加一个唯一的LLID标识，区分不同ONU的数据。在ONU侧通过过滤来接收属于自己的数据。

图 4-39 EPON 业务数据流转发过程图（上行）



版权所有 © 华为技术有限公司

在上行方向上（ONU->OLT），ONU接收到终端用户发送来的数据，此时该数据包不会立刻传递给OLT，而是先放到缓存里。当OLT的MPMC子层发送确认消息后，ONU将该数据包增加LLID标识，然后按照OLT告知的时间点发送。

EPON 管理特征

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。OLT需要对ONU进行业务配置和管理，以便适应多种业务共用接入管道的需求。

OLT通过以太网OAM扩展协议对远端ONU进行配置和管理，并对接兼容其他符合标准的ONU终端。OLT负责存储各ONU的配置数据，在ONU上线后对其进行配置，远端ONU可以实现零配置，减少了业务发放的难度。

OLT通过ONU模板对ONU进行分类管理，以便在业务发放时对ONU进行离线预配置。ONU的带宽控制功能也可通过DBA模板进行配置，OLT通过EPON MAC芯片实现对各个ONU的带宽授权和调度。

OLT使用MAC地址预配置的方式对ONU进行认证，MAC地址匹配的ONU将可以正常注册，使用业务；MAC地址不匹配的ONU将被拒绝，以保证网络安全。OLT时支持ONU自动发现的功能，可记录被拒绝ONU的MAC地址，以便操作员确认后允许其接入EPON网络。

4.2.5 EPON 关键技术

EPON技术主要包括：突发光电技术、测距、DBA（动态带宽分配）和FEC（前向纠错编码）。

突发光电技术

EPON的点对多点（P2MP）的特殊结构和时分多址（TDMA）的接入方式了决定了OUN发送机工作在突发发送的模式下。

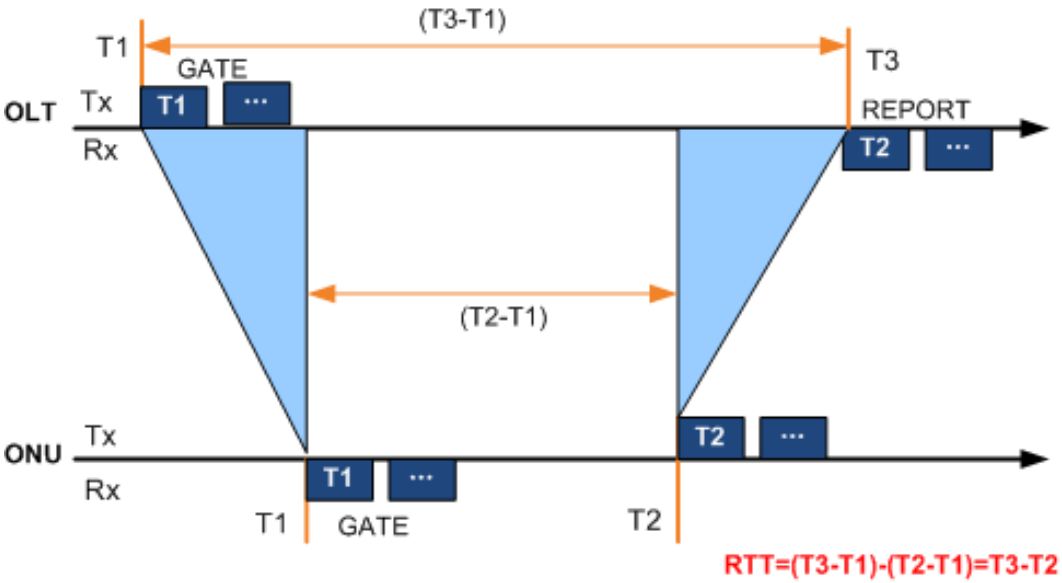
EPON的上行方向采用TDMA的方式工作，每个ONU必须在许可的时隙上才能发送数据，不属于自己的时隙必须关闭光模块的发送信号，才不至于影响其它ONU的正常工作。对于OLT侧上行接收，则要根据时隙进行突发接收每个ONU的上行数据。

测距技术

在EPON系统中主要采用空窗法测量各个ONU到OLT的距离。在OLT和ONU中都有一个记数器，该记数器每传输16比特就增加1，按EPON标称速率1Gbps来计算，则每16ns增加1。测距原理如**图4-40**所示。

版权所有 © 华为技术有限公司

图 4-40 EPON 测距原理



当OLT有MPCP协议数据单元发送时，把记数器的值T1写入控制帧的时戳(TimeStamp)中，ONU一旦收到控制帧后就用时戳中的值替换记数器中的值。当ONU发送MPCP协议数据单元时，把记数器的值T2写入时戳，当OLT收到该帧后其记数器值为T3，用T3减去收到帧的时戳值T2即得到环回时间RTT(Round Trip Time)= (T3-T1)-(T2-T1)=T3-T2。

测距的时机包括：

- 在注册过程中，OLT对新加入的ONU启动测距过程。
- OLT也可以在任何收到MPCP PDU的时候启动测距功能。

OLT使用RTT（Round Trip Time）来调整每个ONU的授权时间。

DBA 技术

DBA（Dynamically Bandwidth Assignment）是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。

DBA算法就是实时地改变EPON的各ONU上行带宽的机制。EPON中如果用带宽静态分配，对数据通信这样的变速率业务很不适合，如按峰值速率静态分配带宽则整个系统带宽很快就被耗尽，带宽利用率很低，而动态带宽分配使系统带宽利用率大幅度提高。

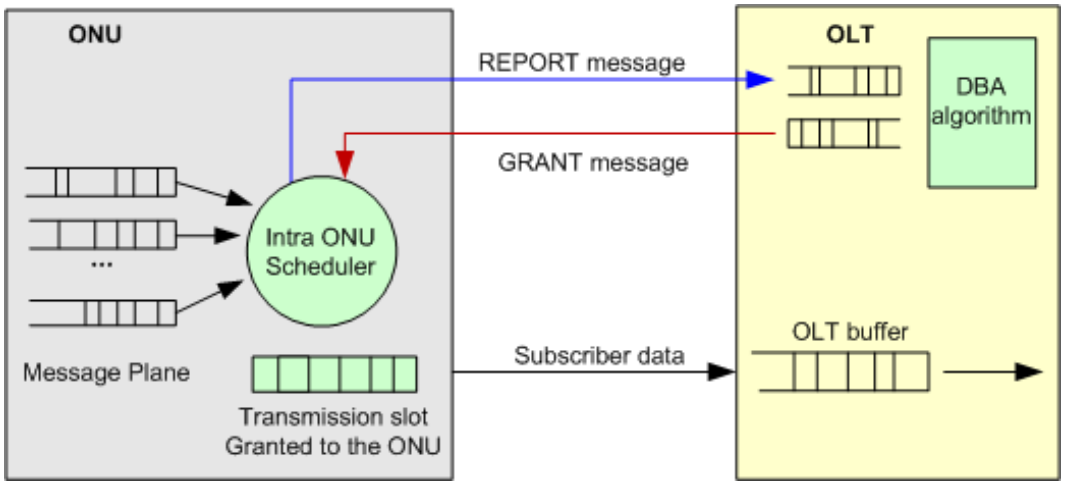
DBA具有如下功能：

- 提高上行带宽的效率
- 允许灵活的SLA策略
- 充分支持增强型业务特性

DBA采用集中控制方式，所有的ONU的上行信息发送，都要向OLT申请带宽，OLT根据ONU的请求按照一定的算法给予带宽（时隙）占用授权，ONU根据分配的时隙发送信息。DBA原理如图4-41所示。

版权所有 © 华为技术有限公司

图 4-41 DBA 原理



在周期n-1，ONU产生报告帧 REPORT，而OLT收集这些报告。在周期n，DBA算法做决定并产生授权，这些授权将在周期n+1有效，即在当前周期里，DBA对前一周期收集到的信息进行计算，并做好下一周期有效的决定。

通过DBA，可以根据ONU突发业务的要求在ONU之间动态调节带宽，从而提高EPON上行带宽效率。

FEC

FEC（Forward Error Correction）的全称是前向纠错编码，主要是为了提高线路的传输质量。FEC算法采用RS（255，239）算法，将所有的下行报文每255Bytes就进行一次FEC编码，确保ONU侧收到数据的准确性。EPON在传输层使用FEC算法可以将线路传输的误码率降低到10E-15，可以避免数据重传，大约可以提升2~3dB的光功率预算。目前EPON系统上行和下行方向均支持FEC功能。

4.2.6 EPON 终端管理

EPON终端管理特性是指EPON OLT通过OAM扩展协议对EPON ONU进行业务配置和管理。操作用户可以通过网管系统或OLT的CLI接口对ONU进行管理和配置，包括端口属性、端口VLAN等。

CTC OAM协议是中国电信定义的对ONU的管理和接口控制协议。该协议定义了OLT和ONU之间交互消息的格式和机制。

OLT通过OAM协议对ONU进行管理和配置，并支持对ONU的离线配置和ONU上线后的配置恢复。通过这种管理机制，ONU本身不需要保存配置信息，有利于业务的发放和对终端的维护。

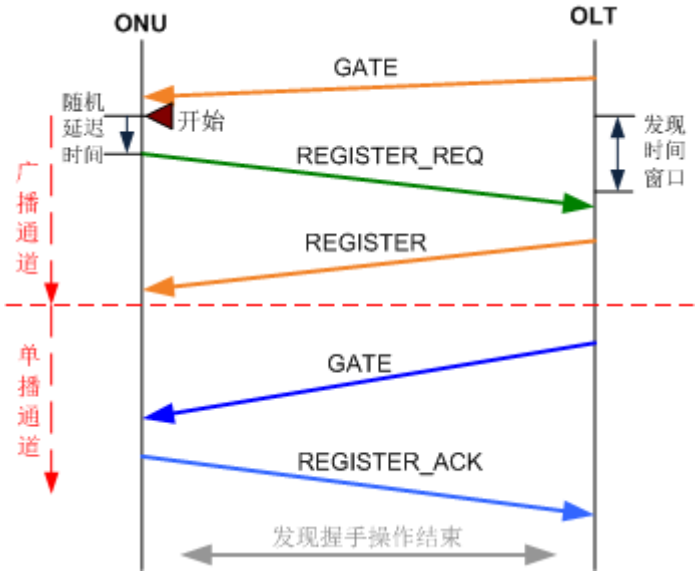
ONU 注册

EPON采用自动发现技术实现ONU向OLT的自动注册。

发现是指新连接或者非在线的ONU接入PON的进程。该进程由OLT发起，它周期性地产生合法的发现时间窗口(Discovery Time Windows)，使OLT可以检测到非在线的ONU。ONU注册过程如图4-42所示。

版权所有 © 华为技术有限公司

图 4-42 ONU 自动注册



ONU自动注册过程如下：

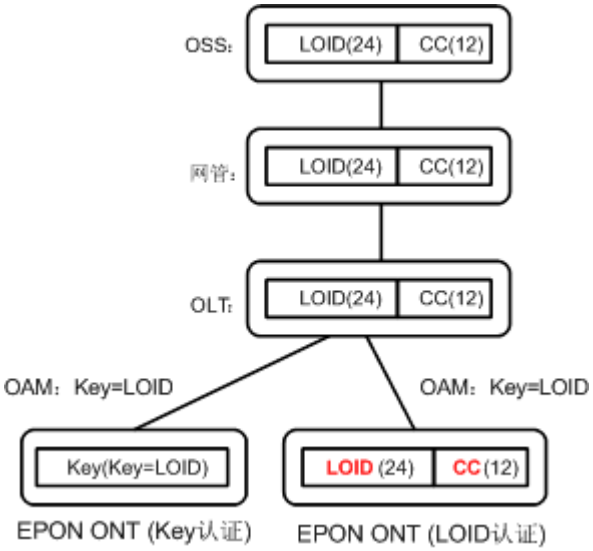
1. OLT通过广播一个发现GATE消息来通知ONU发现窗口的周期。发现GATE消息包含发现窗口的开始时间和长度。
2. 非在线ONU接收到该消息后将等待该周期的开始，然后向OLT发送REGISTER_REQ消息（REGISTER_REQ消息中包括ONU的MAC地址以及最大等待授权（Pending Grant）的数目）。
3. OLT接收到有效的REGISTER_REQ消息后，将注册该ONU，为ONU分配和指定LLID标识并与相应的MAC绑定。OLT向新发现的ONU发送注册(Register)消息，该消息包含ONU的LLID以及OLT要求的同步时间。同时，OLT还对ONU最大等待授权的数目进行响应。

LOID+CC（CheckCode）认证

中国电信的EPON CTC2.1标准中，定义了LOID + Password这种认证方式，是单独的OAM实体，命名为LOID+CC(CheckCode)。EPON LOID+CC认证流程如图4-43所示。

版权所有 © 华为技术有限公司

图 4-43 EPON LOID+CC 认证流程图



认证方式为LOID+CC认证时的认证流程为：

- 在ONT上线过程中，判断此ONT OAM版本号是CTC2.1版本还是CTC2.0版本。
- 如果ONT OAM版本号是CTC2.1：
  - OLT先直接读取LOID+CC信息进行匹配，如果匹配则认证通过。
  - 如果不匹配，再提取Key值（此时Key值当作LOID值）进行匹配判断，如果匹配则也会认证通过。这种情况对应从ONT OAM版本号为CTC2.0升级到CTC 2.1版本的ONT，不改变之前ONT的认证方式。
- 如果ONT OAM版本号是CTC2.0，OLT直接取Key值（此时Key值当作LOID值）后24字节进行匹配判断，如果匹配则此ONU认证通过。

说明

- OLT命令行中的关键字**password-auth**表示密码认证方式，长度为32个字节，对应ONT WEB界面上key认证。中国电信EPON CTC2.1中定义的LOID + Password认证方式，命令行中的关键字为**loid-auth** *loid-value* [**checkcode-auth** *checkcode-value*]，其中**checkcode-auth** *checkcode-value*(CC)对应中国电信的Password。
- 如果用户输入的LOID/CC的实际长度小于24字节/12字节，则在实际的ONU_ID/CC前面填ASCII码的“NUL”（十六进制数为0x00）以补足24字节/12字节。
- 如果ONT WEB界面不支持LOID认证方式，则直接在EPON ONT的Key认证WEB界面中输入LOID值，不够的字节，系统将自动在前面补0。

OAM 协议介绍

EPON终端管理特性主要利用OAM协议，实现OLT对EPON终端的管理。EPON系统支持IEEE802.3-2005中Clause57规定的OAM功能，并支持IEEE802.3-2005中Clause30规定的管理对象、属性和操作。OAM协议定义OLT和ONU之间进行消息交互的报文格式、确认和重传机制，提供一条逻辑上的通信通道。

此外，OAM协议还对ONU的业务模型进行分解抽象，定义了大量的管理实体（Management Entity），以此来描述ONU的内部结构、外部特征、能力范围等。

- 这些管理实体之间有相互的指针和引用关系，形成复杂的拓扑模型，体现数据流和控制流在ONU内部的走向。

版权所有 © 华为技术有限公司

- 各管理实体对应ONU内部的硬件或软件模块，有具体的数据成员，体现本模块的属性参数。
- 数据成员具有不同的属性。其中，只读属性显示了模块的固有特征，可写属性则表明OLT可对该数据成员的参数进行设置。

OLT 与 ONU 的消息交换机制

ONU在上电启动后，会自行生成各种管理实体，对应自身的各个模块。这些管理实体的集合也称为管理实体信息集（Management Information Base，MIB），OLT通过获取各ONU的MIB，可获取ONU的类型和能力集，操作人员也可以了解各ONU的详细信息，以完成业务配置。

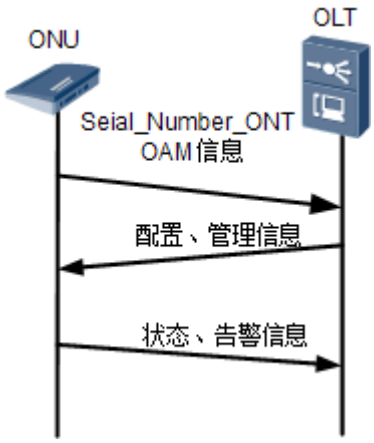
操作人员在OLT的网管或命令行界面上可以对指定的ONU进行配置，例如设置ONU以太网端口的缺省VLAN，将某以太网端口加入指定VLAN等。OLT在解析这些配置命令后，生成的OAM消息将对ONU内部各管理实体的属性进行配置，使之形成指定的拓扑关系。

OLT支持OAM方式配置ONU属性，也支持ONU状态上报到OLT的功能。

- OLT的终端配置管理信息通过OAM通道下发到ONU。
- ONU的状态、告警信息通过OAM通道上报到OLT。

OLT与ONU通过OAM协议实现的消息交换机制示意图如图4-44所示。

图 4-44 OLT 与 ONU 的消息交换机制示意图



OLT与ONU之间建立OAM通道的步骤如下：

1. ONU上线，和OLT交互OAM消息，完成注册过程。
2. OLT通过OAM通道，将终端配置、管理信息下发到ONU。
3. ONU通过OAM通道，将状态、告警信息上报到OLT。

4.2.7 长发光 ONU 检测

版权所有 © 华为技术有限公司

概述

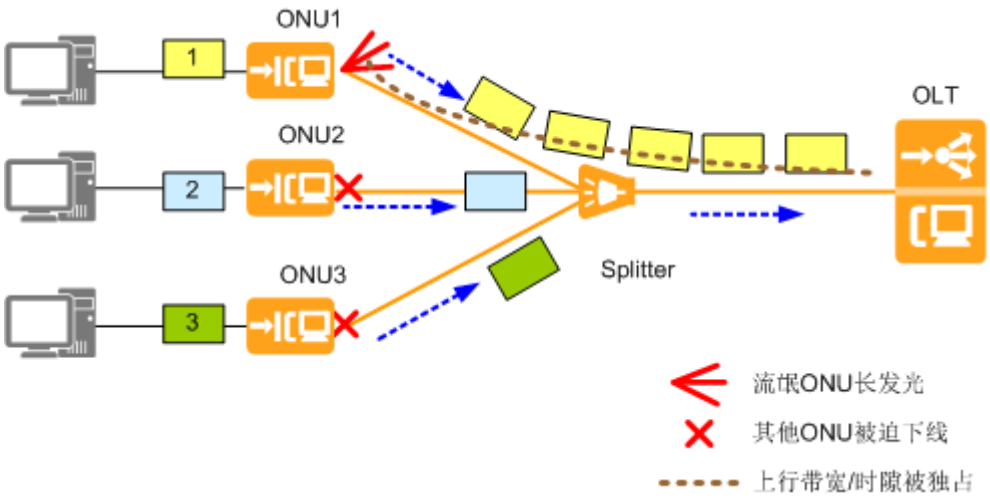
PON遵循P2MP（point-to-multipoint）的网络架构，上行方向采用TDMA（time division multiple access，时分复用）方式，ONU必须按照OLT分配的时间戳向上行方向发送数据才能保证数据依次上行到OLT设备而不产生冲突。

不按照分配的时间戳向上行方向发送光信号的ONU叫长发光ONU。长发光ONU又名长发光流氓ONU，指任意时刻都在发光的ONU。

当系统出现长发光ONU时：

- 如果该ONU已上线，会导致同一PON口下其他某个ONU或者所有ONU下线或者频繁上下线。
- 如果该ONU未配置，会导致PON口下其它未配置的ONU不能被正常自动发现。

图 4-45 流氓 ONU 示意图



流氓 ONU 检测机制

长发光ONU检测又名流氓ONU检测，用来检测系统中长发光ONU并进行隔离处理，确保系统正常运行。针对长发光流氓ONU的处理一般分为三个过程：检测、排查、隔离。

图 4-46 长发光流氓 ONU 处理步骤

- 检测（check）：检测就是定时对PON口进行测试，检查是否存在流氓ONU。检测过程只能判断PON端口下存在长发光流氓ONU，不能定位具体的ONU。

  OLT在PON上行方向开空窗，即在一段时间内，让所有在线的ONU停止发送上行光信号，此时进行ONU上行光信号的检测，此时如果检测到上行还有收光，则进入长发光ONU排查流程。

版权所有 © 华为技术有限公司

- 排查（detect）：排查过程就是确定具体哪个ONU是流氓ONU的过程。

  OLT下发指令逐个打开ONU光模块的上行发光，检测是否有上行光信号，并判断当打开某个ONU后是否会导致其它ONU下线，如果某个ONU打开后导致其他的ONU均下线，就说明该ONU为长发光ONU。长发光ONU的检测流程将对该PON口上的所有ONU均检测一遍，确保将所有长发光ONU均检测出来。

- 隔离（isolate）：隔离就对ONU下发指令，关闭ONU光模块的发送电源，消除流氓ONU对PON口下其他ONU的影响。

  一旦ONU光模块上行发光被OLT关断后，这个关断将是永久性的，即ONU复位或掉电重启其光模块的上行发光也是被关断的，除非OLT下发命令重新打开，该机制保障了长发光ONU被彻底隔离。

说明

OLT默认只对流氓ONU做检测，不进行自动排查和隔离。

流氓 ONU 处理步骤

1. 如果系统中一个ONU已上线，同一PON口下其他ONU下线或者频繁上下线，或者在OLT上产生**0x2e314021 端口下存在非法入侵的流氓ONT**告警，表明系统中可能存在流氓ONU，请根据下面步骤进行排查。

   说明

   也可以使用**display port state**命令查询PON口下是否存在非法入侵的流氓ONT。

2. 使用**anti-rogueont manual-detect**命令，对长发光流氓ONU进行一次性手动检测、排查和隔离。检查系统是否产生**0x2e314022 ONT是流氓ONT**或者**0x2e314021 端口下存在非法入侵的流氓ONT**告警。

   说明

   进行流氓ONU排查时，如果待检测ONU所在端口配置了Type B保护组，为避免排查过程中发生倒换，需要使用**force-switch**命令先对保护组进行强制倒换，再进行排查。如果不确定保护组哪一侧的主干光纤正常，可以先强制倒换到work侧，进行流氓ONU排查。如果work侧没有排查出来，再强制倒换的protect侧，进行流氓ONU排查。排查完成后，需要使用**undo force-switch**命令取消保护组强制倒换。

   - 是，表明该PON口下可能存在长发光流氓ONT。=>**3**
   - 否，表明该PON口下可能存在非长发光流氓ONT。=>**4**

3. 请根据产生的告警进行处理。

   - **0x2e314022 ONT是流氓ONT**，请更换ONU。=>**7**
   - **0x2e314021 端口下存在非法入侵的流氓ONT**。=>**4**

   说明

   产生**0x2e314021 端口下存在非法入侵的流氓ONT**告警，表明PON口下可能存在长发光流氓ONU，且此长发光流氓ONU不支持华为公司定义的扩展PLOAM消息（GPON）或扩展OAM消息（EPON），或者无法控制关闭ONU光模块发送光信号。

4. 使用**ont reset**或者**ont deactivate**命令对PON口下ONU逐个进行复位或者去激活操作。检查其他故障的ONU是否正常上线。

   - 是，表明该ONU为流氓ONU。更换ONU。=>**7**
   - 否。可能由于光模块损坏导致无法使用命令复位或者去激活流氓ONT。=>**5**

5. 对流氓ONU进行手工排查。在分光器处，逐个拔出ONU的上行光纤，检查其他故障的ONU是否正常上线。

版权所有 © 华为技术有限公司

- 是，表明该ONT为流氓ONT。更换ONU。=>**7**
- 否。=>**6**

6. 获取华为技术支持。
7. 故障已清除。

约束与限制

- OLT对PON线路上行方向发光异常做判断和分析，只能针对非恶意用户识别并隔离流氓ONU；对于人为破坏或不符合规定的ONU，不在本特性解决范围。
- 长发光流氓ONU要求能够解析下行PLOAM、OAM消息并正确响应。
- 仅当ONU支持标准PLOAM消息（GPON：ITU-T G.988或G.984.3）、OAM消息（EPON：CTC3.0），正确进行ONU光模块开关控制，才能保证在OLT判断PON口下存在长发光ONU后，快速定位具体的ONU。当PON口上有未配置的ONU出现长发光状态，会导致PON口下其它未配置的ONU不能被正常自动发现。

4.2.8 PON 上行免进站软调

4.2.8.1 介绍

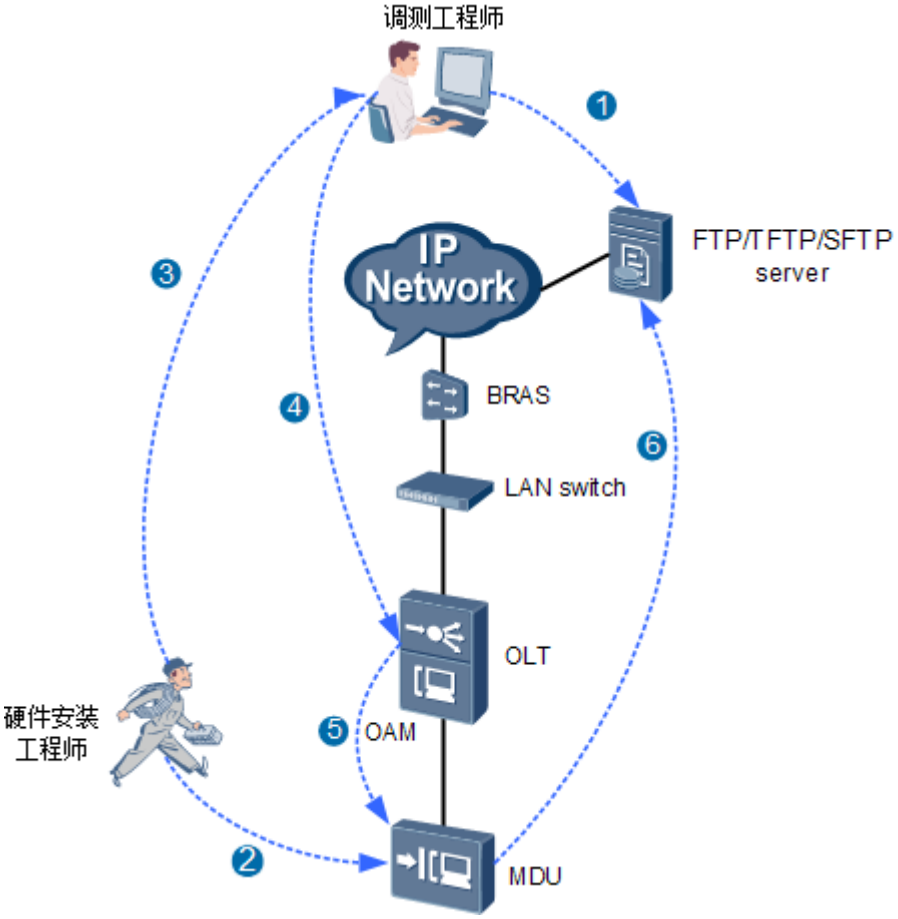
开局部署MDU（Multi-dwelling Unit）设备PON上行组网场景时，为了避免调测工程师到现场调测MDU设备，降低工程部署成本，MDU提供PON上行免软调功能，设备上电后实现MDU设备入网自动业务开局配置和自动软件升级功能，以及MDU设备的自动更换后业务配置自动恢复功能。

4.2.8.2 实现原理

PON上行免进站软调实现原理如**图4-47**所示。

版权所有 © 华为技术有限公司

图 4-47 PON 上行免进站软调原理图



具体实现过程如下:

1. 调测工程师制作预部署策略文件和配置脚本文件，并上载到FTP/TFTP/SFTP Server。

版权所有 © 华为技术有限公司

说明

策略文件命名需要满足xxx.xml，文件内容包括设备类型、主控板类型、配置脚本传输协议、服务器IP地址和配置脚本文件名称。

配置脚本文件的命名为字符串类型。

同一局点的策略文件使用一个即可。例如，某局点策略文件内容如下：

```
<config>
<deploy-version value="1"/>
<product name="MA5XXX">                    //设备类型
<mainboard name="H8XXXXXXX"/>              //主控板类型
<mainboard name="H8XXXXXXX"/>
<mainboard name="H8XXXXXXX"/>
<load>
<transfer-protocol isSupport="1" protocol="ftp" username="user" password="user123" port=""
serveripaddr="10.10.10.10"/>
<init-load-script>
<common-script isSupport="1" value="script.txt"/>
</init-load-script>
</load>
</product>
</config>
```

- protocol：配置脚本的传输协议，可以配置为ftp、sftp和tftp。

  说明

  推荐使用SFTP方式。
- username，password：protocol配置为sftp和ftp时，对应用户名和密码。
- port：如果使用传输协议的默认端口，则不需要配置，否则需要填写对应的端口号
- serveripaddr：服务器IP地址。
- value：配置脚本文件名。传输协议配置为ftp和sftp时文件名中可以包含路径信息。

2. 硬件安装工程师领取MDU，将MDU从库房运往各个站点，进行MDU的硬件安装和上电。

   说明

   设备启动期间，不允许插拔单板。
3. 硬件安装工程师记录MDU的MAC地址、站点信息，上报给调测工程师。
4. 调测工程师通过在OLT上线离线添加ONT、配置ONT的IP地址、相关业务流以及自动部署模板。
5. OLT通过OAM将自动部署策略文件的路径信息传递给MDU。
6. MDU设备上电后接收到自动部署策略文件的路径信息后启动自动部署的流程。

   说明

   MDU设备必须是空数据库，才启用自动部署流程。如果MDU设备已经有配置，则需要使用**erase flash data**命令擦除数据或者使用**load data**命令加载空数据库。
7. MDU设备向FTP/TFTP/SFTP Server请求策略文件并加载，根据自动部署的策略文件的定义，完成自动配置、软件升级。

4.2.9 EPON 配置指导

EPON配置主要包括EPON模板、EPON ONT、EPON端口等的配置。下面介绍具体的配置方法。

背景信息

在模板模式下，对于FTTH场景，MA5800提供了模板方式和简化方式两种配置方式。

版权所有 © 华为技术有限公司

- 模板方式：ONT使用相同的用户侧VLAN，对于所有的ONT绑定相同的业务模板。
- 简化方式：ONT使用不同的用户侧VLAN，此时需要每个ONT建立一个业务模板，配置繁琐。通过简化方式直接对应ONT端口创建业务流，避免大量ONT模板的创建。

配置步骤

4.2.9.1 配置 EPON ONT 模板

EPON ONT模板包括DBA模板、线路模板、业务模板，本任务介绍这些模板的配置。

背景信息

EPON模板方式对EPON ONT配置参数进行分类重组，分为线路模板和业务模板。线路模板主要用于配置DBA相关信息，业务模板主要用于配置ONT的实际能力和与业务相关的参数。

线路模板必须配置，业务模板根据实际业务需求进行选配。相关属性分别在线路模板模式和业务模板模式下进行配置，ONT直接绑定线路模板和业务模板即可。

4.2.9.1.1 配置 DBA 模板

DBA模板描述了xPON的流量参数，通过绑定DBA模板进行动态分配带宽，提高上行带宽利用率。DBA模板可以同时供EPON和GPON使用。

缺省配置

DBA模板相关的缺省配置如表4-4所示。

表 4-4 DBA 模板缺省配置

参数项	缺省值	备注
系统缺省DBA模板号	0～9	使用**display dba-profile all**命令可查询各缺省模板的具体参数值。

操作步骤

步骤1 增加DBA模板。

使用**dba-profile add**命令增加DBA模板。系统缺省有0～9号DBA模板，给出了典型的流量参数值。缺省模板不能被增加或删除。

说明

- T-CONT默认不绑定任何DBA模板，必须进行配置。LLID默认绑定9号DBA模板。
- 在增加DBA模板时，带宽值必须为64的整数倍。如果输入的带宽值不是64的整数倍时，会向下整形为64的倍数。

步骤2 查询DBA模板信息。

版权所有 © 华为技术有限公司

使用**display dba-profile**命令查询DBA模板信息。

----结束

任务示例

举例：增加一个DBA模板，模板类型为type3。规划模板名称为“DBA_100M”，用户要求带宽为100Mbit/s。

```
huawei(config)#dba-profile add profile-name DBA_100M type3 assure 102400 max 102400
huawei(config)#display dba-profile profile-name DBA_100M
```

4.2.9.1.2 配置 EPON ONT 线路模板

配置EPON ONT线路模板，在增加ONT时引用。ONT管理模式为OAM和SNMP，都需要绑定EPON ONT线路模板。

前提条件

已经创建了DBA模板：**4.2.9.1.1 配置DBA模板**。

缺省配置

EPON ONT线路模板相关的缺省配置如**表4-5**所示。

表 4-5 EPON ONT 线路模板缺省配置

参数项	缺省值
LLID绑定的DBA模板	模板号：9
上行FEC开关状态	去使能

操作步骤

步骤1 使用**ont-lineprofile epon**命令增加EPON线路模板，并进入EPON ONT线路模板模式。

ONT管理模式为SNMP和OAM时，都必须配置线路模板。增加EPON ONT线路模板后直接进入EPON ONT线路模板模式，在此模式下可配置与ONT线路相关的属性。

步骤2 绑定DBA模板。

可以使用下面两种方式绑定DBA模板，可以根据实际情况进行二选一，系统支持两种配置方式同时存在。

- 在线路模板中绑定DBA模板。
  适合DBA模板相对固定，并且终端类型单一的场景。
  使用**llid**命令绑定DBA模板。
- 在EPON模式下绑定DBA模板。
  适合DBA模板经常变化，终端类型较多的场景。
  a. 使用**undo llid**命令去绑定系统缺省DBA模板。

版权所有 © 华为技术有限公司

b. 在EPON ONT线路模板配置完成后，进入EPON模式，使用**ont llid**命令绑定DBA模板。

步骤3 配置DBA队列集的队列阈值。

使用**dba-threshold**命令配置DBA队列集的队列阈值。OAM管理的队列阈值，终端会有自己的默认值，采用默认值即可，一般不需要配置。

步骤4 配置上行FEC功能开关。

使用**fec enable**命令使能EPON ONT的上行FEC功能。缺省情况下，ONT FEC开关状态为去使能。

FEC校验是在正常报文中插入冗余数据，使线路具有一定的容错功能，但是会浪费部分带宽资源。使能FEC会增强线路的纠错能力，但是会占用部分带宽，根据实际线路规划确定是否使能FEC功能。

步骤5 使用**commit**命令使模板配置参数生效。必须执行此操作线路模板相关配置才能生效。

说明

如果此模板没有被绑定，则在绑定时所有新配置的参数生效；如果此模板已经被绑定，则所有与其绑定的ONT全部立即生效。

步骤6 使用**quit**命令退回到全局配置模式。

----结束

任务示例

举例：增加一个EPON线路模板，ID为5。LLID绑定DBA模板1。

```
huawei(config)#ont-lineprofile epon profile-id 5
huawei(config-epon-lineprofile-5)#llid dba-profile-id 1
huawei(config-epon-lineprofile-5)#commit
huawei(config-epon-lineprofile-5)#quit
```

举例：修改EPON ONT线路模板5，将LLID绑定的DBA模板由模板1改为模板10。

```
huawei(config)#ont-lineprofile epon profile-id 5
huawei(config-epon-lineprofile-5)#llid dba-profile-id 10
huawei(config-epon-lineprofile-5)#commit
huawei(config-epon-lineprofile-5)#quit
```

4.2.9.1.3 配置 EPON ONT 业务模板

EPON ONT业务模板为采用OAM方式管理的ONT提供了业务配置渠道，采用SNMP管理的ONT（如MDU）的业务配置需要登录到ONT上配置。本章节主要介绍简化方式下ONT业务模板的配置方法。

缺省配置

EPON ONT业务模板相关的缺省配置如表4-6所示。

表 4-6 EPON ONT 业务模板缺省配置

参数项	缺省值
ONT端口的组播模式	CTC

版权所有 © 华为技术有限公司

参数项	缺省值
ONT端口快速离开模式	不关注（即OLT不对其做任何处理）

操作步骤

步骤1 使用**ont-srvprofile epon**命令增加EPON业务模板，并进入EPON ONT业务模板模式。

ONT管理模式为SNMP时，不需要配置业务模板。增加EPON ONT业务模板后直接进入EPON ONT业务模板模式，在此模式下可做如下配置。根据不同的业务需求进行选择配置。

步骤2 上网业务相关配置。

使用**ont-port eth**命令配置ONT的端口能力集。能力集规划ONT支持的各种类型的端口数，ONT的端口能力集必须与ONT实际的能力集保持一致。

步骤3 语音业务相关配置。

说明

ONT的语音业务通过XML下发到网管进行配置，OLT上做透传，只需要使用**service-port**命令创建一条承载语音业务的业务流通道。

使用**ont-port pots**命令配置ONT的端口能力集。能力集规划ONT支持的各种类型的端口数，ONT的端口能力集模板必须与ONT实际的能力集保持一致。

步骤4 组播业务相关配置。

1. 使用**ont-port eth**命令配置ONT的端口能力集。能力集规划ONT支持的各种类型的端口数，ONT的端口能力集模板必须与ONT实际的能力集保持一致。
2. 使用**multicast fast-leave**命令配置ONT端口的快速离开模式。缺省情况下，快速离开模式为不关注。
3. 使用命令**port eth ont-portid multicast-tagstripe { untag | tag }**配置组播数据报文的VLAN Tag处理方式。
   - untag：剥掉下行组播数据报文的VLAN Tag。
   - tag：对下行组播数据报文进行透传。
4. 使用**port multicast-vlan**命令配置ONT端口的组播VLAN。组播VLAN要与OLT侧的组播VLAN一致。

须知

若不配置ONT端口的组播VLAN，下行的组播VLAN数据流会被ONT丢弃。

步骤5 使用**commit**命令使模板配置参数生效。必须执行此操作业务模板相关配置才能生效。

说明

如果此模板没有被绑定，则在绑定时所有新配置的参数生效；如果此模板已经被绑定，则所有与其绑定的ONT全部立即生效。

版权所有 © 华为技术有限公司

步骤6 使用**quit**命令退回到全局配置模式。

----结束

任务示例

举例：增加一个EPON业务模板，ID为200。用于上网业务，ONT支持4个ETH端口。

```
huawei(config)#ont-srvprofile epon profile-id 200
huawei(config-epon-srvprofile-200)#ont-port eth 4
huawei(config-epon-srvprofile-200)#commit
huawei(config-epon-srvprofile-200)#quit
```

举例：增加一个EPON业务模板，ID为20。用于组播业务，ONT支持4个ETH端口。透传组播报文的VLAN Tag，组播VLAN为10。

```
huawei(config)#ont-srvprofile epon profile-id 20
huawei(config-epon-srvprofile-20)#ont-port eth 4
huawei(config-epon-srvprofile-20)#port eth 1 multicast-tagstrip tag
huawei(config-epon-srvprofile-20)#port multicast-vlan eth 1 10
huawei(config-epon-srvprofile-20)#commit
huawei(config-epon-srvprofile-20)#quit
```

4.2.9.2 配置 EPON ONT(模板模式)

MA5800通过ONT为最终用户提供业务，MA5800与ONT的通道打通后，MA5800才能对ONT进行管理，ONT才能正常工作。

前提条件

EPON ONT的模板已经创建：

- 对于ONT，已经完成：**配置EPON ONT线路模板**、**配置EPON ONT业务模板**。
- 对于MDU、ONU，已经完成：**配置EPON ONT线路模板**。

背景信息

MA5800通过OAM（Operation, Administration and Maintenance）协议对EPON ONT进行管理和配置，并支持对ONT的离线配置，ONT上线后的配置恢复。通过这种机制，ONT本地不需要保存配置信息，便于业务发放和终端维护。

在模板模式下，EPON ONT的相关配置集成到业务模板和线路模板中，在增加ONT时，只需要直接与匹配的业务模板和线路模板绑定即可。

EPON ONT相关的缺省配置如**表4-7**所示。

表 4-7 EPON ONT 缺省配置

参数项	缺省值
EPON端口的ONT自动发现功能	去使能
增加ONT后ONT的状态	激活
ONT端口的缺省VLAN	1

版权所有 © 华为技术有限公司

说明

光接入产品支持KEY认证，KEY认证即密码认证。密码认证与MAC认证的区别在于，密码认证是通过创建用户名和密码的形式进行认证的，而MAC认证是通过设备的MAC地址进行认证的。

操作步骤

步骤1 使用**interface epon**命令进入EPON模式。

步骤2 增加EPON ONT。

1. 使用**port portid ont-auto-find**命令使能ONT自动发现功能。使能自动发现ONT功能后，可根据系统上报的信息增加ONT。缺省情况下，EPON端口的ONT自动发现功能为去使能。

   说明

   自动发现的ONT处于自动发现状态，执行确认或增加操作后才能正常工作。

2. 使用**ont add**命令离线增加ONT；或使用**ont confirm**命令确认自动发现的ONT。

   增加或确认ONT时，系统提供MAC地址认证、密码认证、LOID+CHECKCODE认证三种认证方式：

   - MAC地址认证：OLT检测ONT上报的MAC地址，如果与OLT配置一致则通过认证，ONT正常上线。该方式需要提前记录所有ONT的MAC地址，不适用于大批量增加ONT的场景。一般用于确认自动发现的ONT。
   - 密码认证：OLT检测ONT上报的密码，如果与OLT配置一致则通过认证，ONT正常上线。该方式一般用于大批量增加ONT的场景，只需要规划ONT的密码，不需要手工记录ONT的MAC地址。该方式提供always-on和once-on两种发现模式。
     - always-on：第一次认证使用密码认证，认证通过后，不会自动匹配MAC地址，后续每一次认证也都使用密码认证。该模式有利于后续的维护，更换ONT不需要修改配置，输入正确的密码即可。缺点是安全性不高，如果其它用户知道密码，就能非法享有业务权限。
     - once-on：第一次认证使用密码认证，认证通过后，自动匹配MAC地址，后续每一次认证使用MAC地址+密码方式，只有ONT的密码和MAC地址都匹配时才能上线。该模式安全性较高，但在需要更换ONT或密码误修改时，需要重新进行配置，增加了后续维护工作量。
   - LOID+CHECKCODE认证：由某运营商标准定义的一种认证方式。LOID为24个字节，CHECKCODE为12个字节，其中CHECKCODE为可选字节。采用24字节还是36字节由规划决定，全网统一。OLT将判断ONT上报的LOID+CHECKCODE是否与配置一致，如果一致则认证通过；如果不一致，再获取ONT的Password，如果与LOID的后10字节匹配，则ONT也能认证通过，兼容老的Password认证方式的ONT。

   离线增加ONT适用于批量开局场景：预先将所有的ONT增加到OLT设备上，完成ONT的业务发放。当用户需要开通业务时，只需安装人员把ONT带到用户家，完成相关配置，ONT上线认证通过后即可完成业务的开通。一般使用密码认证或LOID+CHECKCODE认证方式确认ONT。

   确认自动发现的ONT适用于小批量增加ONT的场景：当用户需要开通业务时，只需安装人员把ONT带到用户家，在ONT上线状态正常后，逐个增加ONT。一般使用MAC地址认证方式确认ONT。

 版权所有 © 华为技术有限公司

说明

- 如果ONU是作为独立网元，由网管通过SNMP管理模式直接管理，选择SNMP管理模式。这种模式下，只需要在OLT上配置EPON线路参数，和管理通道参数。只需要绑定线路模板。
- 如果ONU不作为独立网元管理，它的所有配置都由OLT通过OAM协议进行管理，选择OAM管理模式。这种模式下，需要在OLT上配置ONU需要的所有参数。需要绑定线路模板和业务模板。
- 对于ONT管理模式一般配置为OAM模式。需要绑定线路模板和业务模板。

3. 使用**ont ipconfig**命令配置ONT的IP地址。不能与别的VLAN接口IP地址同一网段。

   对于作为独立网元管理的ONU，配置ONT的IP地址时需要同时配置管理VLAN；对于支持语音业务的ONT，需要配置ONT的IP地址用于语音业务，此时不需要配置管理VLAN。

4. （可选）当ONT管理模式为SNMP时，需要配置ONT的SNMP管理参数，步骤如下：

   a. 使用**ont snmp-profile**命令为ONT绑定SNMP模板。

      配置前需要保证已经使用**snmp-profile add**命令增加了SNMP模板。

   b. 使用**ont snmp-route**命令配置网管服务器的静态路由。即配置下一跳IP地址。

步骤3 配置ONT端口的缺省VLAN（Native VLAN）。

使用**ont port native-vlan**命令配置ONT端口的缺省VLAN。缺省情况下，ONT端口的缺省VLAN为1。

- 如果用户（例如PC）上报到ONT的报文为Untag，则在ONT上打上端口的缺省VLAN，再上报到OLT。
- 如果用户上报到ONT的报文为Tag，需要配置ONT的端口VLAN与用户的Tag一致，在ONT上不会打上端口的缺省VLAN，报文带着用户Tag上报到OLT。

步骤4 激活ONT。

使用**ont activate**命令激活ONT。ONT只有处于激活态才能传送业务。

增加ONT之后，ONT默认为激活状态，此步骤在ONT为去激活状态时才需要配置。

步骤5 查询ONT状态。

使用**display ont info**命令查询ONT运行状态、ONT配置状态和ONT匹配状态。

----结束

任务示例

举例：离线增加5个ONT，使用密码认证方式，提前规划ONT的password为0100000001-0100000005，为便于后续ONT更换维护，密码认证的发现模式为always-on，绑定和ONT匹配的线路模板10和业务模板10。

```
huawei(config)#interface epon 0/2
huawei(config-if-epon-0/2)#ont add 0 password-auth 0100000001 always-on oam ont-lineprofile-id 10 ont-srvprofile-id 10
huawei(config-if-epon-0/2)#ont add 1 password-auth 0100000002 always-on oam ont-lineprofile-id 10 ont-srvprofile-id 10
huawei(config-if-epon-0/2)#ont add 2 password-auth 0100000003 always-on oam ont-lineprofile-id 10 ont-srvprofile-id 10
huawei(config-if-epon-0/2)#ont add 3 password-auth 0100000004 always-on oam ont-lineprofile-id 10
```


版权所有 © 华为技术有限公司

```
ont-srvprofile-id 10
huawei(config-if-epon-0/2)#ont add 4 password-auth 0100000005 always-on oam ont-lineprofile-id 10
ont-srvprofile-id 10
```

举例：增加ONT，由OLT通过OAM协议对其进行管理。根据系统自动上报ONT的MAC地址00E0-FC00-3E47确认此ONT，绑定和ONT匹配的线路模板1和业务模板1。

```
huawei(config)#interface epon 0/2
huawei(config-if-epon-0/2)#port 0 ont-auto-find enable
huawei(config-if-epon-0/2)#ont confirm 0 mac-auth 00E0-FC00-3E47 oam ont-lineprofile-id 1 ont-
srvprofile-id 1
```

举例：增加ONU，作为独立网元进行管理。已知ONU的MAC地址为00E0-FC00-C9FE，绑定和ONT匹配的线路模板2。并为其配置网管参数，管理VLAN为31。

```
huawei(config)#snmp-profile add profile-id 1 v2c public private 10.10.5.53 161 huawei
huawei(config)#interface epon 0/2
huawei(config-if-epon-0/2)#ont add 0 2 mac-auth 00E0-FC00-C9FE snmp ont-lineprofile-id 2
huawei(config-if-epon-0/2)#ont ipconfig 0 2 ip-address 10.20.20.20 mask 255.255.255.0 gateway
10.20.20.1 manage-vlan 31
huawei(config-if-epon-0/2)#ont snmp-profile 0 2 profile-id 1
huawei(config-if-epon-0/2)#ont snmp-route 0 2 ip-address 10.20.20.19 mask 255.255.255.0 next-hop
10.20.20.100
```

4.2.9.3 配置 EPON ONT(简化方式)

MA5800通过ONT为最终用户提供业务，MA5800与ONT的通道打通后，MA5800才能对ONT进行管理，ONT才能正常工作。

前提条件

EPON ONT的模板已经创建：

- 对于ONT，已经完成：**配置EPON ONT线路模板**、**配置EPON ONT业务模板**。
- 对于MDU、ONU，已经完成：**配置EPON ONT线路模板**。

背景信息

MA5800通过OAM（Operation, Administration and Maintenance）协议对EPON ONT进行管理和配置，并支持对ONT的离线配置，ONT上线后的配置恢复。通过这种机制，ONT本地不需要保存配置信息，便于业务发放和终端维护。

在模板模式下，EPON ONT的相关配置集成到业务模板和线路模板中，在增加ONT时，只需要直接与匹配的业务模板和线路模板绑定即可。

EPON ONT相关的缺省配置如**表4-8**所示。

表 4-8 EPON ONT 缺省配置

参数项	缺省值
EPON端口的ONT自动发现功能	去使能
增加ONT后ONT的状态	激活

版权所有 © 华为技术有限公司

说明

光接入产品支持KEY认证，KEY认证即密码认证。密码认证与MAC认证的区别在于，密码认证是通过创建用户名和密码的形式进行认证的，而MAC认证是通过设备的MAC地址进行认证的。

操作步骤

步骤1 使用**interface epon**命令进入EPON模式。

步骤2 增加EPON ONT。

1. 使用**port portid ont-auto-find**命令使能ONT自动发现功能。使能自动发现ONT功能后，系统会上报自动发现的ONT的MAC地址和密码，可根据系统上报的信息增加ONT。缺省情况下，EPON端口的ONT自动发现功能为去使能。

   说明

   自动发现的ONT处于自动发现状态，执行确认或增加操作后才能正常工作。

2. 使用**ont add**命令离线增加ONT；或使用**ont confirm**命令确认自动发现的ONT。

   说明

   - 如果ONU是作为独立网元，由网管通过SNMP管理模式直接管理，选择SNMP管理模式。这种模式下，只需要在OLT上配置EPON线路参数，和管理通道参数。只需要绑定线路模板。
   - 如果ONU不作为独立网元管理，它的所有配置都由OLT通过OAM协议进行管理，选择OAM管理模式。这种模式下，需要在OLT上配置ONU需要的所有参数。需要绑定线路模板和业务模板。
   - 对于ONT管理模式一般配置为OAM模式。需要绑定线路模板和业务模板。

3. 使用**ont ipconfig**命令配置ONT的IP地址。不能与别的VLAN接口IP地址同一网段。

   对于作为独立网元管理的ONU，配置ONT的IP地址时需要同时配置管理VLAN；对于支持语音业务的ONT，需要配置ONT的IP地址用于语音业务，此时不需要配置管理VLAN。

4. 当ONT管理模式为SNMP时，需要配置ONT的SNMP管理参数，步骤如下：

   a. 使用**ont snmp-profile**命令为ONT绑定SNMP模板。

      配置前需要保证已经使用**snmp-profile add**命令增加了SNMP模板。

   b. 使用**ont snmp-route**命令配置网管服务器的静态路由。即配置下一跳IP地址。

步骤3 激活ONT。

使用**ont activate**命令激活ONT。ONT只有处于激活态才能传送业务。

增加ONT之后，ONT默认为激活状态，此步骤在ONT为去激活状态时才需要配置。

----结束

任务示例

举例：增加ONT，由OLT通过OAM协议对其进行管理。根据系统自动上报ONT的MAC地址00E0-FC00-3E47确认此ONT，绑定和ONT匹配的线路模板1和业务模板1。

```
huawei(config)#interface epon 0/2
huawei(config-if-epon-0/2)#port 0 ont-auto-find enable
huawei(config-if-epon-0/2)#ont confirm 0 mac-auth 00E0-FC00-3E47 oam ont-lineprofile-id 1 ont-srvprofile-id 1
```


版权所有 © 华为技术有限公司

举例：增加ONU，作为独立网元进行管理。已知ONU的MAC地址为00E0-FC00-C9FE，绑定和ONT匹配的线路模板1。并为其配置网管参数，管理VLAN为31。

```
huawei(config)#snmp-profile add profile-id 1 v2c public private 10.10.10.10 161 huawei
huawei(config)#interface epon 0/2
huawei(config-if-epon-0/2)#ont add 0 2 mac-auth 00E0-FC00-C9FE snmp ont-lineprofile-id 2
huawei(config-if-epon-0/2)#ont ipconfig 0 2 ip-address 10.20.20.20 mask 255.255.255.0 gateway 10.20.20.1 manage-vlan 31
huawei(config-if-epon-0/2)#ont snmp-profile 0 2 profile-id 1
huawei(config-if-epon-0/2)#ont snmp-route 0 2 ip-address 10.10.10.10 mask 255.255.255.0 next-hop 10.20.20.1
```

4.2.9.4 配置 EPON 端口

EPON光口必须打开后才能正常工作并承载业务，本任务打开EPON光口，并配置端口的相关属性。

缺省配置

EPON用户端口相关的缺省配置如表4-9所示。

表 4-9 EPON 用户端口缺省配置

参数项	缺省值
EPON光口	打开
可注册ONT的最大距离	20km

操作步骤

步骤1 使用**interface epon**命令进入EPON模式。

步骤2 配置光口开关。

- 使用**port portid laser-switch on**命令或使用**undo shutdown**命令配置打开光口激光器。缺省情况下，光口激光器为打开，光口可用，此步骤无需配置。
- 不需要使用的光口，使用**port portid laser-switch off**命令或使用**shutdown**命令配置关闭光口激光器。

须知

执行此操作前，请确认该PON口没有承载业务。

步骤3 配置ONT可注册的最大距离。

使用**port portid range**命令配置EPON端口可注册ONT的最大距离。缺省值为20km。ONT接入的实际距离大于配置的可注册的最大距离，则不允许注册。

----结束

任务示例

举例：配置EPON端口0/2下可注册ONT的最大距离为15km。

版权所有 © 华为技术有限公司

```
huawei(config)#interface epon 0/2
huawei(config-if-epon-0/2)#port 0 range max-distance 15
```

4.2.10 配置上行 EPON 端口属性

上行EPON端口支持查询端口统计信息、设置光模块电源开关、设置光模块接收光功率告警门限值等。

前提条件

如果在离线方式下配置MA5612，使用**port mode**命令配置端口模式后才能配置端口属性。

操作步骤

- 设置向OLT注册的验证密码。

  使用**password**（EPONNNI模式）命令设置当前设备用作EPON ONU时，通过password认证方式向OLT注册使用的密码。

  使用**loid(eponnni)**命令设置ONU通过LOID+CHECKCODE认证方式向OLT注册使用的认证码。

  说明

  当使用双EPON上行时，0/0/0端口不支持设置，只能设置0/0/1端口。设置完成后，两个端口参数相同。

  当使用双EPON上行时，0/0/1端口不支持设置，只能设置0/0/2端口。设置完成后，两个端口参数相同。

  使用**epon mac address**命令设置ONU通过MAC地址认证方式向OLT注册使用的认证码。

- （可选）设置光模块告警门限值。

  使用**optical-module threshold**（EPONNNI模式）或命令设置光模块告警门限值。

- 设置PON上行光模块的发光模式。

  使用**laser**（EPONNNI模式）或命令设置光模块的发光模式为auto、on、off。

  - auto：光口自动发光模式，此时端口正常工作，保证业务的正常运行。
  - on：光口长发光模式，需要检测光口发光功率时，设置为on。测试完成后，光口发光模式自动切换为auto。
  - off：光口关闭模式，一般用于测试或故障定位场景。

  须知

  设置为off时，不仅影响业务，还会造成onu下线。因此请确认该上行端口没有承载业务。

- 查询端口统计信息。

  使用**display epon-port statistic**命令查询当前PON端口流量信息及线路状况。

----结束

版权所有 © 华为技术有限公司

任务示例

举例：设置PON端口向OLT注册的验证密码，光模块接收光功率告警门限的下限为5dBm，上限为50dBm，并设置PON上行光模块的发光模式为正常发光。

```
huawei(config-if-gponnni-0/9/0)#password huawei-user123
huawei(config-if-eponnni-0/9/0)#optical-module threshold rx-power lower-limit 5 upper-limit 50
huawei(config-if-eponnni-0/9/0)#laser auto
huawei(config-if-eponnni-0/9/1)#password huawei-user123
huawei(config-if-eponnni-0/9/1)#optical-module threshold rx-power lower-limit 5 upper-limit 50
huawei(config-if-eponnni-0/9/1)#laser auto
```

4.2.11 EPON 参考标准和协议

EPON技术参考以下标准和协议：

- IEEE 802.3ah：Amendment to IEEE 802.3-2002
- IEEE 802.3-2005 Local and metropolitan area networks - specific requirements Part 3
- 中国电信EPON设备技术要求 V2.1

4.3 二层转发

宽带二层特性介绍的是链路层协议，包含多个子特性。本章将对其子特性分别加以介绍。

4.3.1 MAC 地址管理

MAC地址管理是二层网络管理的一项基本功能。

4.3.1.1 介绍

定义

MAC地址管理特性是二层管理特性的一项基本特性，包括MAC地址学习开关和MAC地址老化。

MAC地址学习开关

MAC地址学习开关通过配置，控制ONU是否学习MAC地址。系统默认学习MAC地址，GPON设备可以通过配置关闭MAC地址学习，EPON设备目前不支持通过配置关闭MAC地址学习。

MAC地址老化

MAC地址老化是指在ONU二层转发过程中，系统定时检查自动学习到的MAC地址，如果在老化时间内，没有发送或接收任何携带该源MAC地址的报文，对应的MAC地址就会从MAC地址表中删除。GPON设备可以通过配置修改MAC地址老化时间。

目的

MAC地址学习开关

控制ONU基于MAC或者基于VLAN转发。

MAC地址老化

版权所有 © 华为技术有限公司

规定MAC地址老化主要是避免把MAC地址资源耗尽。

受益

运营商受益

- 打开MAC地址学习开关可以避免大量冗余报文转发。
- 通过MAC地址老化设置可以把长期不使用的MAC删除，避免资源浪费，为更多的用户提供服务。

4.3.1.2 原理描述

MAC 地址学习开关

GPON系统通过OMCI协议进行MAC地址学习开关配置，ONU通过LAN Switch芯片实现MAC学习使能和关闭功能。当MAC地址学习使能时，ONU自动学习转发报文MAC地址与端口对应关系，并且在转发时根据MAC找到对应出端口；当MAC地址学习关闭时，ONU不会学习转发报文的MAC地址与端口对应关系，报文转发根据VLAN转发。

MAC 地址老化

GPON系统通过OMCI协议进行MAC地址老化时间配置，ONU通过LAN Switch芯片实现MAC地址老化时间功能。有数据转发时芯片自动学习MAC地址与端口的对应关系，如果有相同MAC地址报文转发时，芯片自动更新老化时间，如果在规定时间内没有该MAC地址的报文转发，芯片就自动删除该MAC地址。

4.3.1.3 参考标准和协议

- 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

4.3.2 VLAN

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。

4.3.2.1 介绍

定义

VLAN（Virtual Local Area Network）即虚拟局域网，是将一个物理的LAN在逻辑上划分成多个广播域（多个VLAN）的通信技术。VLAN内的主机间可以直接通信，而VLAN间的主机不能直接互通。

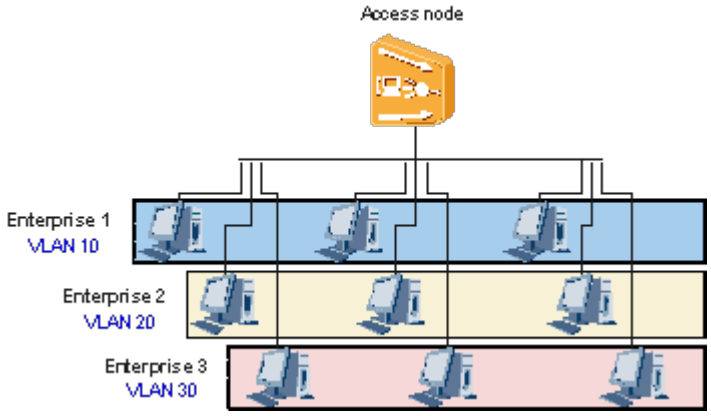
目的

将广播报文限制在一个VLAN内，避免了广播风暴对带宽的浪费。同时由于VLAN间的主机不能直接互通，因此提高了网络安全性。

版权所有 © 华为技术有限公司

例如，同一个写字楼的不同企业客户，若建立各自独立的LAN，企业的网络投资成本很高；若共用写字楼已有的LAN，又会导致企业信息安全无法保证。利用VLAN技术就能解决这个问题。

图 4-48 VLAN 应用示意图



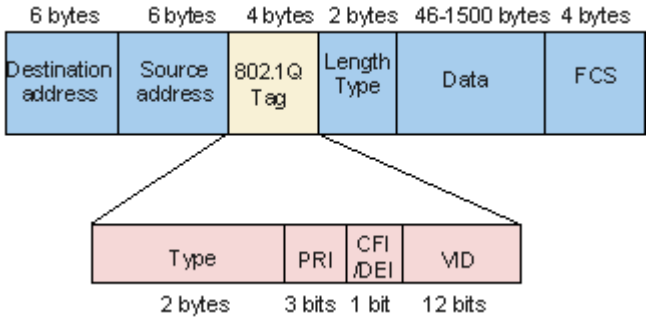
不同企业的用户属于不同的VLAN，各企业客户可以共享LAN设施，同时由于VLAN间的主机不能互通，保证各企业的网络信息安全。

4.3.2.2 基本概念

VLAN 产生后的 802.1Q 帧格式

IEEE 802.1Q标准对以太帧格式进行了修改，在源MAC地址字段和协议类型字段之间加入4字节的802.1Q Tag，如下图所示。

图 4-49 VLAN 产生后的 802.1Q 帧格式



802.1Q Tag包含4个字段，其含义如下：

- Type

  长度为2字节，表示帧类型。取值为0x8100时表示802.1Q Tag帧。如果不支持802.1Q的设备收到这样的帧，会将其丢弃。

- PRI

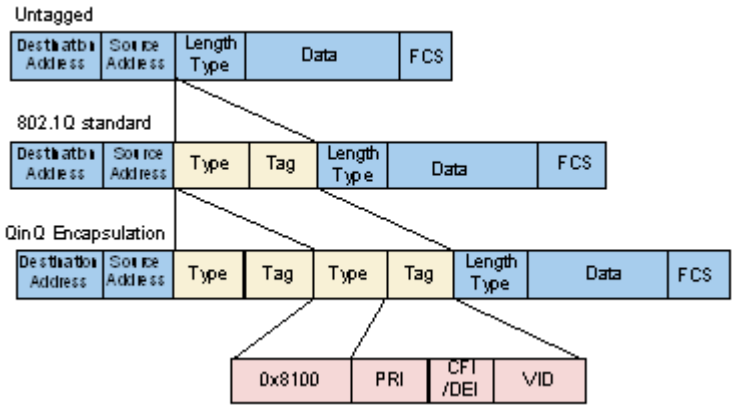
  长度为3比特，表示帧的优先级（Priority），取值范围为0～7，值越大优先级越高。网络阻塞时，优先发送优先级高的数据帧。

版权所有 © 华为技术有限公司

- CFI/DEI：长度为1比特。
  - CFI表示MAC地址是否是经典格式（Canonical Format Indicator）。CFI为0说明是经典格式，CFI为1表示为非经典格式。用于区分以太网帧、FDDI（Fiber Distributed Digital Interface）帧和令牌环网帧。在以太网中，CFI的值为0。
  - DEI：DEI（Drop Eligible Indicator）位，在802.1ad协议中表示丢弃优先级，用来标识报文的颜色。
- VID：VLAN ID，长度为12比特，表示该帧所属的VLAN。

PRI、CFI、VID三个字段又被统称为VLAN tag，它是VLAN通信的依据。不含802.1Q Tag的帧又叫Untagged帧。QinQ封装的802.1Q帧有双层802.1Q Tag。它们的帧结构对比如下图所示。

图 4-50 Untagged 帧、标准 802.1Q 帧、QinQ 封装的 802.1Q 帧结构图

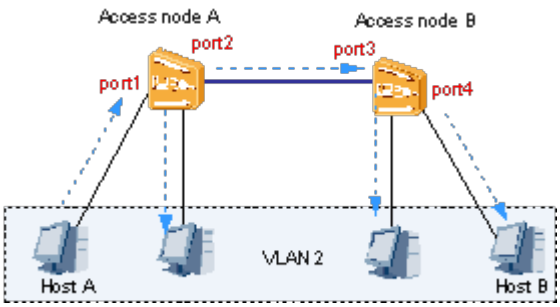


4.3.2.3 VLAN 通信原理

VLAN 内通信原理

同一个VLAN内的用户彼此可以互通。接入节点主要靠识别以太帧中的VLAN tag来进行。在下图的网络中，VLAN 2中有四台主机，下面以Host A和Host B通信过程为例说明VLAN内的通信原理。

图 4-51 VLAN 内通信原理图示



1. Host A发出的以太帧首先到Access node A的port1。

版权所有 © 华为技术有限公司

2. Access node A的port1为该以太帧加上VLAN tag（VID字段填入该端口所属的VLAN 2）。
3. Access node A将以太帧发往除port1外所有属于VLAN 2的端口。
4. Access node A的port2将以太帧发往Access node B（通过port3接收）。
5. Access node B识别出以太帧中的VLAN tag（属于VLAN 2），于是将该以太帧发往Access node B上所有属于VLAN 2的端口。
6. Access node B的port4将该以太帧发给Host B。

VLAN 间通信原理

划分VLAN后，不同VLAN的主机之间不能直接进行二层通信。如果VLAN间的主机要通信，需要建立IP路由。

为了保证第一次数据流通过路由表正常转发，路由表中必须有正确的路由表项。因此必须在三层交换机上部署三层接口并部署路由协议，实现三层路由可达。VLANIF接口（也称为VLAN三层接口）由此产生。

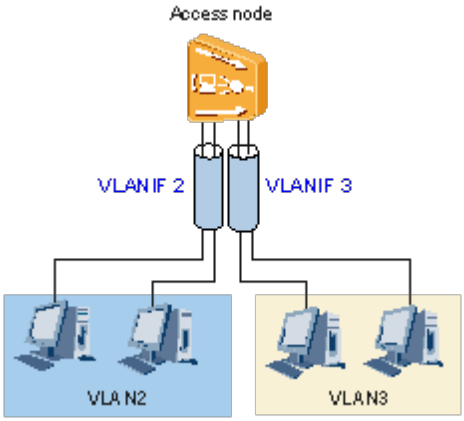
VLANIF接口是三层逻辑接口，可以配置IP地址。

说明

三层交换技术是将路由技术与交换技术合二为一的技术，在交换机内部实现了路由，提高了网络的整体性能。三层交换机通过路由表传输第一个数据流后，会产生一个MAC地址与IP地址的ARP表。当目的IP对应的ARP表项存在时，直接根据ARP表项找到出端口，并进行目的MAC地址，源MAC地址，VLAN的切换。

在下图所示的网络中，Access node上划分了2个VLAN：VLAN 2和VLAN 3。此时可在交换机上创建2个VLANIF接口（VLANIF 2和VLANIF 3），并为它们配置IP地址和路由，实现VLAN 2与VLAN 3内主机间的通信。

图 4-52 VLAN 间通信原理图示



4.3.2.4 原理描述

VLAN操作特性是二层管理特性的一项基本特性，包括VLAN标记、VLAN过滤、VLAN切换、VLAN透传和QinQ。

VLAN 标记

VLAN标记指ONU对接收到的上行以太网帧加上一个端口默认VLAN Tag；对于下行以太网帧，ONU剥掉其VLAN Tag。对于ONU下挂设备不支持VLAN处理时，可以将该端

版权所有 © 华为技术有限公司

口配置成VLAN标记模式，ONU对该设备接入的所有报文标记成端口默认VLAN。VLAN标记功能通过灵活的接入方式，可以支持untag设备接入，丰富运营商接入方式。

表 4-10 VLAN 标记功能对报文的处理策略

方向	以太网包是否有Tag	处理方式
上行	有VLAN Tag	按照VLAN过滤功能处理。
	无VLAN Tag	打上新的VLAN Tag（主要参数是VID），转发。
下行	有VLAN Tag	按照VLAN过滤功能处理。
	无VLAN Tag	丢弃。

VLAN 过滤

VLAN过滤指ONU以太端口对接收到的以太帧进行检查，如果报文携带的VLAN Tag属于端口配置的VLAN列表就允许报文通过，否则丢弃报文。通过VLAN过滤功能，对VLAN进行限定，避免非法VLAN接入，对局域网进行限定和隔离，避免无效数据对上层设备的冲击。

表 4-11 VLAN 过滤功能对报文的处理策略

方向	以太网包是否有Tag	处理方式
上行	有VLAN Tag	如果报文所带的VLAN ID属于该端口的“允许通过VLAN”，则向上转发。 如果报文所带的VLAN ID不属于该端口的“允许通过VLAN”，则丢弃。
	无VLAN Tag	将untagged报文打上缺省VLAN Tag，并转发。
下行	有VLAN Tag	如果报文所带的VLAN ID属于该端口的“允许通过VLAN”，则向下转发。 如果报文所带VLAN ID为“缺省VLAN”，则剥离VLAN标签后向下转发。 如果报文所带的VLAN ID不属于该端口的“允许通过VLAN”，则丢弃。
	无VLAN Tag	丢弃。

VLAN 切换

如果接收到的上行以太网帧的VLAN在以太端口的VLAN切换列表中，则将该VLAN转换为对应的网络侧VLAN并转发；如果不在列表中，则丢弃。对于untagged报文，则打上缺省VLAN。通过此功能，用户接入的VLAN信息和运营商规划的VLAN信息不一致时，可以通过VLAN切换实现业务衔接。

版权所有 © 华为技术有限公司

表 4-12 VLAN 切换功能对报文的处理策略

方向	以太网包是否有Tag	处理方式
上行	有VLAN Tag	如果其原有Tag的VID在对应端口的VLAN Translation列表中有对应的entry（等于其输入VID），则按照该表项将VID转换为对应的VID（输出VID），并转发。 如果其VID在对应端口的VLAN Translation列表中没有对应的entry，则丢弃。
	无VLAN Tag	将untagged报文打上缺省VLAN Tag，并转发。
下行	有VLAN Tag	如果其原有Tag的VID在对应端口的VLAN Translation列表中有对应的entry（等于其输出VID），则按照该表项将VID转换为对应的VID（输入VID），并转发。 如果其原有Tag的VID为缺省VID，则剥除Tag并转发。 如果其VID在对应端口的VLAN Translation列表中没有对应的entry，则丢弃。
	无VLAN Tag	丢弃。

VLAN 透传

VLAN透传指ONU对接收到上行的以太网帧不作任何处理（无论以太网帧是否带VLAN Tag）透明的向OLT转发；对于下行的以太网帧也是透明转发的方式。以太口接收到的VLAN个数超过以太口的VLAN个数限制时，推荐使用VLAN透传。通过VLAN透传功能，运营商可以开展管道运营业务，运营商只提供传输通道，不关注传输内容。

表 4-13 VLAN 透传功能对报文的处理策略

方向	以太网包是否有Tag	处理方式
上行	有VLAN Tag	对以太网包不作任何改变（保留原VLAN Tag），转发。
	无VLAN Tag	对以太网包不作任何改变，转发。
下行	有VLAN Tag	对以太网包不作任何改变（保留原VLAN Tag），转发。
	无VLAN Tag	对以太网包不作任何改变，转发。

QinQ

QinQ指ONU对接收到上行的以太网帧的处理方式是无论以太帧是否带VLAN Tag都增加一层外层VLAN Tag；对于下行的以太网帧剥离一层VLAN Tag。ONU不对下挂设备的VLAN信息感知，使用外层VLAN进行转发。通过QinQ功能，运营商可以开展VPN业务，连接企业的不同分支机构。

版权所有 © 华为技术有限公司

表 4-14 QinQ 功能对报文的处理策略

方向	以太网包是否有Tag	处理方式
上行	有VLAN Tag	对以太包增加一层VLAN Tag，转发。
	无VLAN Tag	对以太包增加一层VLAN Tag，转发。
下行	有VLAN Tag	对以太包剥离一层VLAN Tag，转发。
	无VLAN Tag	转发。

4.3.2.5 参考标准和协议

本特性的参考标准与协议清单如下：

表 4-15 VLAN 特性参考标准和协议

文档	描述
IEEE 802.1Q	IEEE standards for Local and metropolitan area networks-Virtual Bridged Local Area Networks
IEEE 802.1ad	Virtual Bridged Local Area Networks Amendment 4: Provider Bridges
RFC3069	VLAN Aggregation for Efficient IP Address Allocation

4.4 QoS

QoS即服务质量（Quality of Service），是为了满足用户的带宽、时延、抖动、丢包率等应用需求的实现技术。

4.4.1 QoS 概述

定义

QoS：Quality of Service（服务质量）是指网络通信过程中，允许用户业务在带宽、时延、抖动和丢包率等方面获得可预期的服务水平。衡量QoS的指标如下：

- 带宽：指一个连接的理论传输容量。
- 时延：指信息从一个网络节点发送出去到另一个网络节点接收到的时间。较大的时延将影响实时业务（比如IP电话）的质量。
- 抖动：指时延的变化。抖动能够严重影响多媒体业务（比如视频点播）的质量。
- 丢包率：在网络传输过程中丢失报文的百分比。

目的

- 为用户提供带宽保证

版权所有 © 华为技术有限公司

- 调控IP网络的流量
- 减少报文的丢失率
- 设置报文的优先级
- 避免和管理网络拥塞
- 为不同的用户业务提供差异化服务

4.4.2 QoS 服务模型

QoS 服务模型

在网络中实施QoS时，有如下表所示的三种模型可选。其中，ONU上的QoS模型基于差分服务模型。后续在不加说明的情况下，QoS的描述均是基于差分服务模型。

类别	特点	应用
Best-Effort Service（尽力而为服务模型）	简单地尽最大努力转发，不提供任何服务或传送保证，耗尽带宽才丢弃。 简单、单一的服务模型，也是IP网络缺省的服务模型。	大多数数据业务，如email等。
Integrated Service（综合服务模型）	基于资源预留，应用程序通过RSVP信令协议通知网络预留带宽，网络中的每个单元要为特定数据流预留带宽。	由于存在如下严重问题，目前未有大规模应用。 ● 要求端到端支持RSVP ● 可扩展性差 ● 协议报文开销大
Differentiated Service（差分服务模型）	基于优先级，网络识别每条流并提供相应质量的服务。分类和标记是该模型的前提和基础。	报文处理过程简单，易于扩展，广泛应用于如下业务： ● VoD ● 流媒体 ● VoIP ● 电视会议 ● 专线

差分服务模型的 QoS 组件

在实施差分服务模型时，需要考虑四个基本的QoS组件，这些组件相互组合，可以设计出完整的QoS策略。

版权所有 © 华为技术有限公司

名称	解释
流分类和优先级标记	DiffServ的基本思想是流分类，然后对不同的类标记不同的优先级。 流分类：将数据分为不同的类别，分类并不修改原来的数据包。 优先级标记：将数据标记上不同的优先级，标记会修改原来的数据包。
流量监管和整形	服务供应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。 流量监管（Policing）：丢弃超出了服务合同规定部分的报文。 流量整形（Shaping）：缓存超出了服务合同规定部分的报文，等待允许时继续发送。
拥塞管理	是指系统发生拥塞时，如何进行管理和控制数据传输的先后顺序。
拥塞避免	是指系统发生拥塞时，主动丢弃报文，通过调整网络的流量来解除网络过载的一种流控机制。

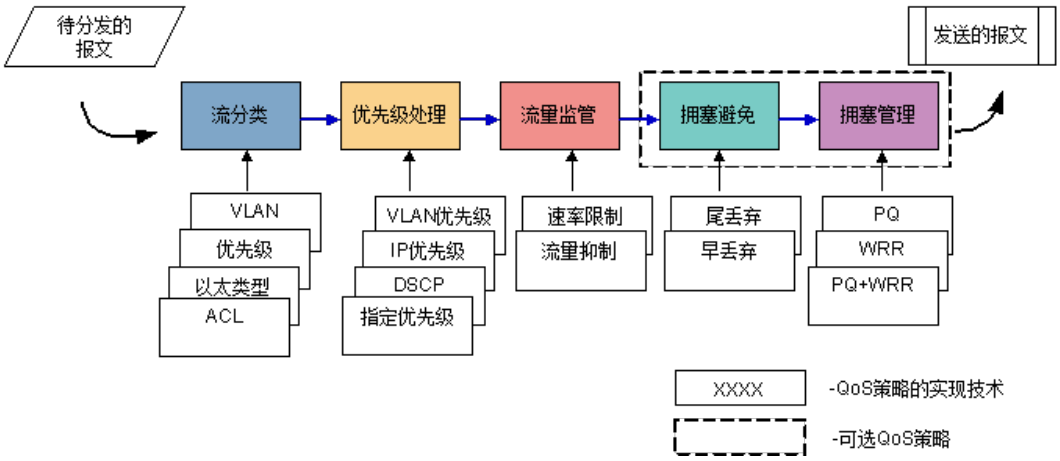
4.4.3 QoS 方案

QoS 方案

ONU采用差分服务模型，其QoS方案如图4-53所示，从图中可以看出：

- 待分发的报文经过了流分类、优先级处理、流量监管、拥塞避免和拥塞管理等QoS策略后，从出端口转发出去。
- 拥塞避免和拥塞管理策略是可选的，如果接口上不存在拥塞，则无需部署此QoS策略。
- 每种QoS策略支持多种实现技术（详见各QoS策略的介绍）。

图 4-53 ONU 支持的 QoS 方案



版权所有 © 华为技术有限公司

QoS 策略

QoS策略如下表所示。

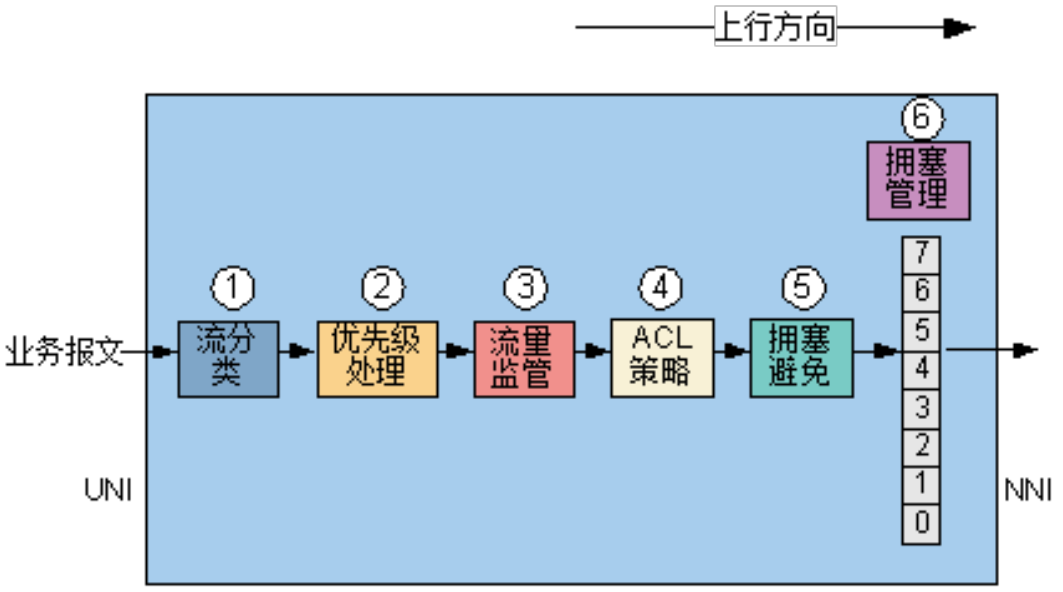
QoS策略	备注
流分类 流分类（基于ACL） 优先级处理 优先级处理（基于ACL） 流量监管 流量监管（基于ACL） 拥塞避免 拥塞管理	• 流分类仅作用在上行方向。 • 拥塞避免和拥塞管理作用在出端口方向。 • 基于ACL的流分类、优先级处理和流量监管请参考“4.4.10 ACL策略”。

4.4.4 QoS 处理流程

QoS 处理通用流程-上行方向

上行方向的处理流程如图4-54所示。

图 4-54 上行方向 QoS 流程



报文从用户侧端口进入，在设备上进行如下QoS处理：

版权所有 © 华为技术有限公司

步骤	QoS策略	举例
1	流分类：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。	上网、语音和IPTV业务，有不同的QoS需求，可以为其规划不同的VLAN和/或优先级，达到区分业务的目的。
2	优先级处理：对业务流的优先级进行标记或重标记，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。	将上网、语音和IPTV业务的优先级分别标记为0、5、4。
3	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。	将上网业务的保证速率限制在8Mbps，峰值限制在10Mbps。报文速率在保证速率和峰值之间时，将该部分报文标记为黄色；报文速率超过峰值时，直接丢弃此部分报文。
4	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。	设定ACL规则，只允许匹配上网和语音业务VLAN的报文通过，丢弃非法的业务报文。
5	拥塞避免：出端口的入队列发生拥塞时，提前丢弃不符合要求的报文，避免拥塞加剧。	基于优先级进行早丢弃，设置上网业务（优先级为0）的早丢弃门限为30%，则入队列时如果队列中有30%的报文为上网报文时，后续的上网报文将被丢弃。
6	拥塞管理：出端口的出队列发生拥塞时，通过适当的队列调度机制，可以优先保证高优先级报文的QoS参数。	采用严格优先级队列调度，发生拥塞时，语音业务（优先级5）首先得到调度，保证业务的实时性；上网业务（优先级0）最后才得到调度。

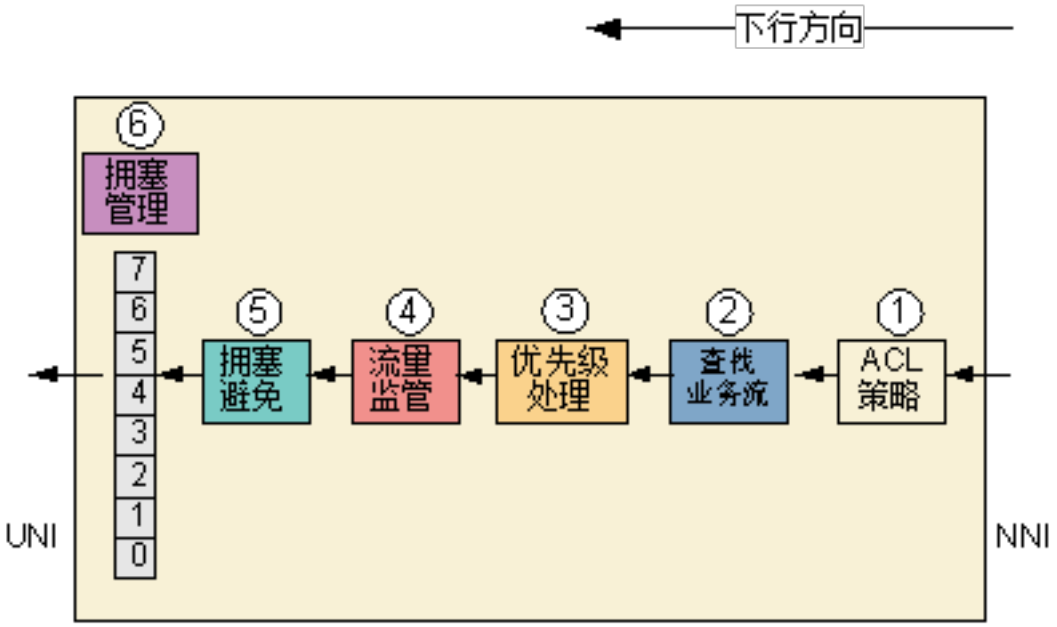
QoS 处理通用流程-下行方向

下行方向的QoS处理流程如图4-55所示，可以看出相对上行方向，下行方向的处理流程有如下的差异：

- 在下行方向上无流分类处理，而是基于转发模式（VLAN+MAC或SVLAN+CVLAN）查找业务流。

版权所有 © 华为技术有限公司

图 4-55 下行方向 QoS 流程



4.4.5 流分类

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。

4.4.5.1 介绍

流

流，也称业务流或数据流，是具有某种共同特征的报文的集合。比如，用户的上网业务报文就可以视为一条流，语音业务报文则可以视为另外一条流。

在ONU中，流也称为service-port（业务虚端口）。

流分类

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。

比如，要为同一用户提供上网、语音和IPTV业务，则需要将业务报文分成三条流，以示区分。

目的

流分类的目的是支持多业务应用，即区分业务流，为用户的不同业务提供差异化的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（Committed Access Rate，承诺访问速率）限速、优先级标记、队列调度等。

版权所有 © 华为技术有限公司

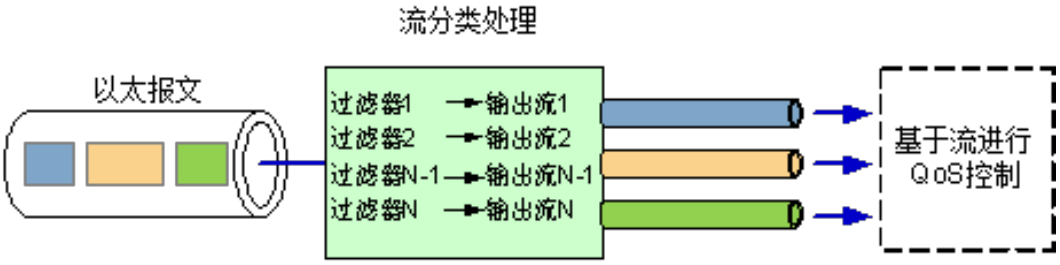
4.4.5.2 实现原理

流分类处理过程

流分类处理过程如图4-56所示。流分类是在分类器中完成的，一个流分类器由过滤器（即分类规则，详见表4-16）和输出流表示；不同业务的以太报文进入设备后，通过流分类被区分为不同的业务流，然后基于业务流进行差异化QoS控制。

流分类的对象是以太报文，对于非以太接口，系统会将其报文进行分段和重组，还原成以太网帧，然后再进行流分类。也就是说，流分类基于逻辑端口，认为这些端口发送和接收的都是以太网帧。

图 4-56 流分类处理过程



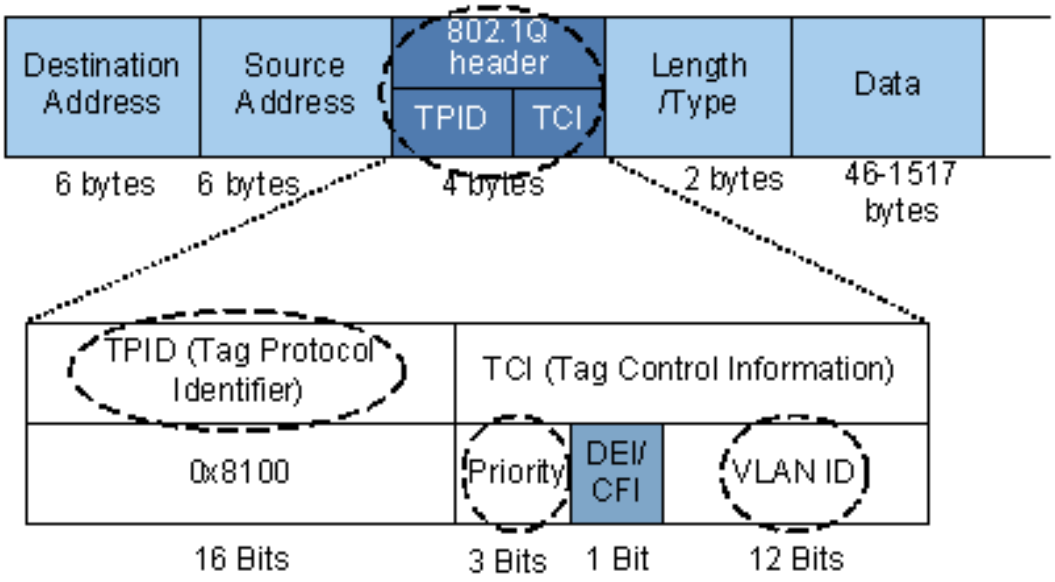
报文只有在上行方向才会进行流分类，同时进行报文的MAC地址学习，并根据VLAN+MAC记录业务流索引；下行方向则基于“VLAN+MAC”查找业务流。

流分类方式及应用

流分类是依据以太报文的特征对用户业务进行区分的。通常根据以太报文帧头（如图4-57所示）的三个域及其组合来进行流分类。

- VLAN
- 优先级
- 以太类型

图 4-57 以太 802.1Q 帧结构



版权所有 © 华为技术有限公司

详细的流分类规则如表4-16所示。

表 4-16 流分类规则

流分类规则	应用场景
基于VLAN(VLAN ID，优先级，以太类型)	当各业务的CVLAN不同时，可以通过CVLAN进行流分类。 比如，上网业务CVLAN为100，语音业务CVLAN为200。
基于CVLAN+以太类型	无法通过上述基于VLAN的流分类方式区分业务的情况下，可以使用条件组合进行区分。 比如，各业务的业务VLAN相同，优先级也相同，此时可以通过“CVLAN+以太类型”进行区分。
基于CVLAN+优先级	
基于Other-all	当系统中同时存在普通业务和透传业务（Transparent LAN Service）时，可以通过Other-all方式区分两者。 比如，系统中同时有上网业务（VLAN 100）和其它透传业务，当只需要区分两者，但不关注具体的透传业务时，则可以让透传业务匹配到Other-all的流。

说明

CVLAN是指用户VLAN（Customer VLAN），通常用来表征不同的用户，在业务流中亦称内层VLAN。

报文的匹配关系

- 如果配置了Other-all业务流，则报文最后才匹配Other-all。
- 如果不存在Other-all业务流，则各条业务流是平等的，无先后顺序。
- 如果进入的报文不匹配任何业务流，报文将被丢弃。

4.4.6 优先级标记

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

4.4.6.1 介绍

定义

标记/重标记报文的优先级，让设备/网络依据此标记对报文按约定的方式进行处理。其中，

- 通常在设备/网络的入口上进行标记，在设备/网络的内部进行重标记。
- 优先级包含了常规意义的转发优先级，以及丢弃优先级（比如通过以太报文的DEI（Discard Eligibility Indicator）位来标识报文的颜色），两者本质都是为后续QoS处理提供依据。

版权所有 © 华为技术有限公司

目的

优先级处理是设备/网络对报文进行调度处理的基础和依据。在设备/网络产生拥塞后可根据优先级进行调度。

4.4.6.2 基本概念

设备处理的优先级主要包含了VLAN优先级（802.1p优先级）和IP优先级。

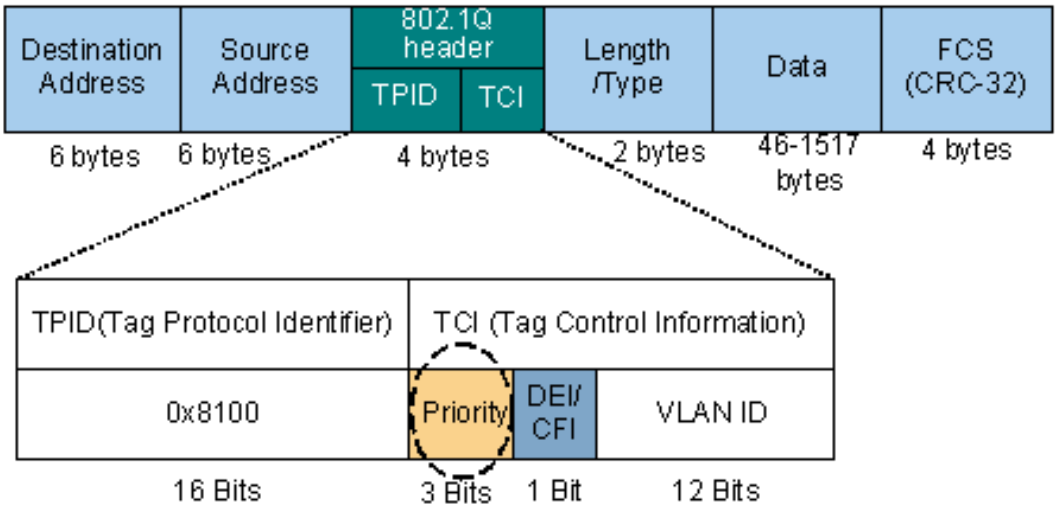
VLAN 优先级

VLAN优先级，亦称802.1p优先级，是在链路层定义的报文优先级，即CoS（Class of Service），使用了VLAN Tag里面的三个比特（在以太网帧的位置如图4-58所示），它由IEEE 802.1Q文档定义。

Priory字段就是802.1p优先级，它由3个bit组成，这3位指明以太网帧优先级；一共有8种优先级，取值范围为0～7，优先级的顺序是0最低，7最高，主要用于当设备端口阻塞时，优先发送哪个数据包。

图中的DEI（Drop Eligible Indicator）位，在802.1ad协议中表示丢弃优先级，用来标识报文的颜色；如，0标识绿色，1标识黄色，在使能了基于颜色的丢弃策略时，发生拥塞时黄色报文会被优先丢弃。

图 4-58 802.1Q 帧格式



IP 优先级

在IP协议定义中，DSCP和ToS在IP头中占用相同的1个字节的域，IP承载网设备根据识别填充的是DSCP或ToS，根据系统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）是IP头里面的报文分类（不直接指明优先级，而是指明报文分类，由设备决定哪些类别优先级比较高），ToS字段有8个bit，包括3 bit的IP precedence字段，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为1。如果所有4 bit均为0，则意味着是一般服务。

DSCP（Differentiated Services Code Point）在RFC2474中定义，它是基于IPv4的ToS（Type of Service）和IPv6的流量类型（Traffic Class）重新定义的产物。

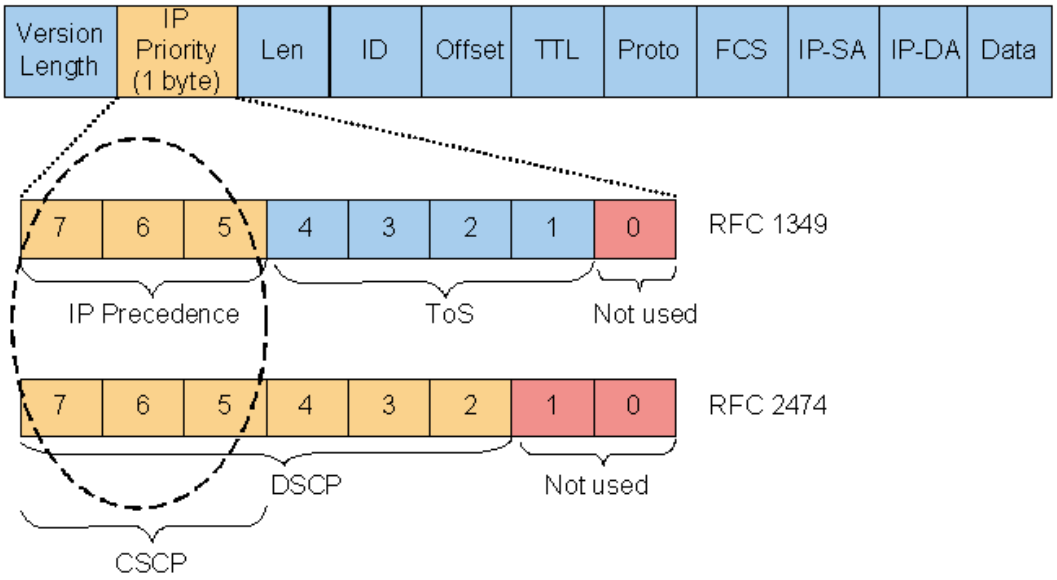
版权所有 © 华为技术有限公司

说明

IPv6报文头中的TC（Traffic Class）字段与IPv4报文头中的IP优先级字段作用相同。本节以IPv4为例介绍IP优先级。

如图4-59所示，DS字段的高6位（bit7～bit2）用作区分服务代码点DSCP（DS CodePoint），低2位（bit1、bit0）是保留位。DS字段的高3位（bit 7-6-5）是类选择代码点（Class Selector CodePoint，CSCP），它表示了一类DSCP。

图 4-59 IPv4 报文头格式



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定义了如下标准的PHB：

- 类选择器CS（Class Slector）
- 加速转发EF（Expedited Forwarding）
- 确保转发AF（Assured Forwarding）
- 尽力而为BE（Best-Effort）

每种PHB的组成如表4-17所示。

表 4-17 PHB 及组成

PHB	前三位（bit 7-6-5）	后三位（bit 4-3-2）
CS	aaa【备注】	000
BE	000	000
EF	101	110
AF	bbb【备注】	cc0【备注】

版权所有 © 华为技术有限公司

备注：a、b、c均表示某bit的值，取值为0或者1。其中：

- aaa有8种组合：000–111，对应十进制数0-7。此3bit可与IP precedence互相映射。
- bbb有4种组合：001、010、011和100，对应十进制数1-4。
- cc有3种组合：01-11，对应十进制数1-3。

常用DSCP用法及优先级对应关系如表4-18所示。

表 4-18 常用 DSCP 用法及优先级对应关系

DSCP类型	IPv4优先级/MPLS EXP/802.1P优先级	DSCP（二进制）	应用
BE	0	0	Internet
AF1	1	001 010	Leased Line
AF1	1	001 100	Leased Line
AF1	1	001 110	Leased Line
AF2	2	010 010	IPTV VoD
AF2	2	010 100	IPTV VoD
AF2	2	010 110	IPTV VoD
AF3	3	011 010	IPTV Broadcast
AF3	3	011 100	IPTV Broadcast
AF3	3	011 110	IPTV Broadcast
AF4	4	100 010	NGN/3G Singaling
AF4	4	100 100	NGN/3G Singaling
AF4	4	100 110	NGN/3G Singaling
EF	5	101 110	NGN/3G voice
CS6	6	110 000	Protocol
CS7	7	111 000	Protocol

4.4.6.3 实现原理

优先级处理包含了内外层优先级的拷贝和指定。

外层（或单层）优先级的处理

外层（或单层）优先级的处理如图4-60所示，外层优先级的来源有多种：

- 拷贝入报文的外层优先级（user-cos）

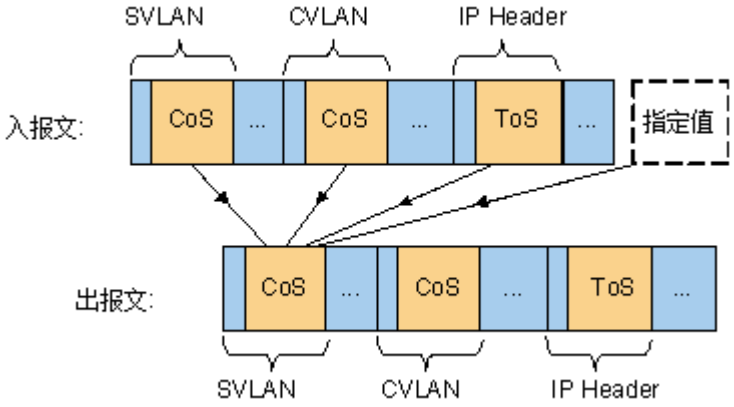
版权所有 © 华为技术有限公司

- 拷贝入报文的内层优先级（user-inner-cos）
- 拷贝入报文的IP ToS优先级（user-tos）
- 指定报文的优先级（prival）

说明

业务流的下行方向目前不支持拷贝user-tos。

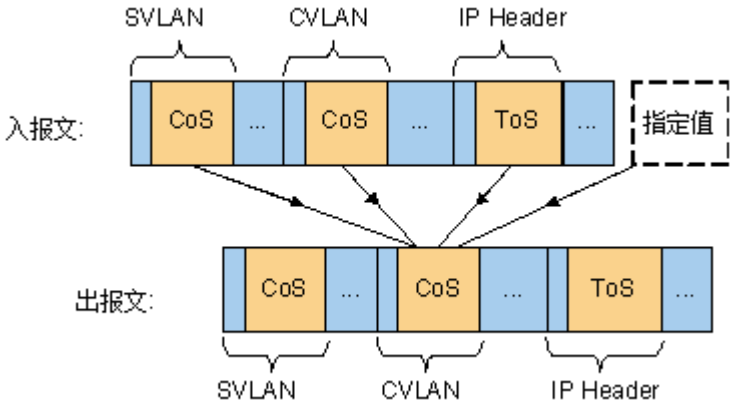
图 4-60 外层（或单层）优先级处理



内层优先级的处理

内层优先级的处理策略如图4-61所示，可以看出，内层优先级的来源和外层优先级完全一致。

图 4-61 内层优先级处理



4.4.7 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。

版权所有 © 华为技术有限公司

4.4.7.1 介绍

定义

流量监管又称流量策略（Traffic Policy），通过测量业务流的速率，限制进出某一网络的某一业务流的流量与突发，在报文满足一定的条件下，如某个业务流的报文流量过大，流量监管就可以选择丢弃报文，或标记报文的颜色（重新设置报文的优先级）等。

流量监管的常见实现技术是CAR（Committed Access Rate，承诺访问速率），在PON组网中，还会通过**4.1.6.3 DBA**（Dynamic Bandwidth Allocation，动态带宽分配）技术对ONU的上行流量进行监管。

目的

对运营商来说，流量监管是非常必要的。

- 为保证客户进入的流量符合SLA（Service Level Agreement）。
- 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。

4.4.7.2 基本概念

流量监管的基本概念如**图4-62**所示；基本概念的解释如**表4-19**所示。

图 4-62 流量监管基本概念

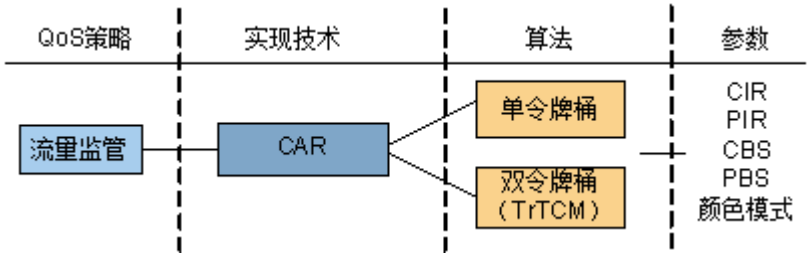


表 4-19 基本概念的解释

概念	解释
CAR	Committed Access Rate，承诺访问速率。是实现特定报文流量的常用技术。广泛应用于针对以太端口、xDSL端口及xPON端口的限速。 CAR通常是通过令牌桶算法来实现的。
GTS	Generic Traffic Shaping，通用流量整形。采用令牌桶技术来控制流量，对于不符合流量特征的报文进行缓冲后传输。
令牌桶	令牌桶（Token Bucket）是一个存放令牌的容器，是用来控制数据流量的工具。令牌桶允许数据的突发性传输，同时又能控制流量。令牌桶分为单桶和双桶。 原理：一个报文只有在令牌桶中存在相应大小的令牌时才能通过；报文通过后，令牌桶减少相应大小的令牌。

版权所有 © 华为技术有限公司

概念	解释
TrTCM	Two Rate Three Color Marker，双速率三色标记。在IETF的RFC2698中定义。根据两种速率（即峰值信息速率（PIR）和保证信息速率（CIR））及其相关突发尺寸，通过标记报文的DEI位，将报文标记为绿色、黄色或者红色。
DEI	Drop Eligible Indicator，丢弃标记，802.1ad协议中为以太报头中的1bit的字段，复用自802.1Q协议中的CFI。用来标识报文的颜色。
CIR	Committed Information Rate，即保证信息速率。单位：bps。
PIR	Peak Information Rate，即峰值信息速率。这是系统空闲时用户可获得的最大带宽。单位：bps。
CBS	Committed Burst Size，即保证突发度。此参数用于描述令牌桶C的容量，即在按CIR转发数据时允许转发的最大突发IP包尺寸。单位：byte。
PBS	Peak Burst Size，即峰值突发度。此参数用于描述令牌桶P的容量，即在按PIR转发数据时允许转发的最大突发IP包尺寸。单位：byte。
颜色模式	TrTCM算法中定义了色盲（color-blind）和色敏（color-aware）模式，前者不关注报文原来的颜色，后者关注。

4.4.7.3 实现原理-CAR

单令牌桶原理

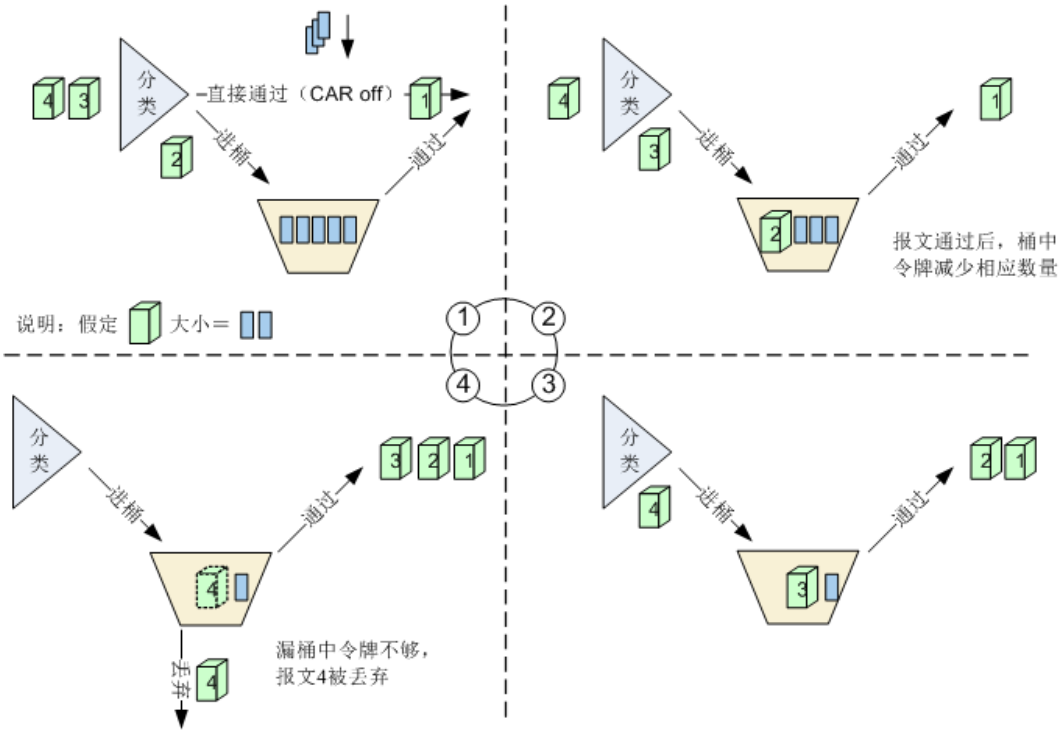
单令牌桶的原理：一个报文只有在令牌桶中存在相应大小（字节）的令牌时才能通过，报文通过后，令牌桶减少相应大小的令牌。

1. 首先报文被分类，如果报文是某类限定了流量参数的报文，则进入令牌桶中进行处理（图中的报文2、3、4），否则报文直接通过，不限速（如**图4-63**中的报文1）。
2. 如果令牌桶中有足够的令牌可以用来发送报文，则报文可以通过，可以被继续发送下去。如**图4-63**中的报文2和3。
3. 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。如**图4-63**中的报文4。
4. 系统按设定的速度恒定的向桶中放置令牌，等到桶中生成了新的令牌，报文才可以继续被发送。

当令牌桶中充满令牌的时候，桶中所有的令牌代表的报文都可以被发送，这样可以允许数据的突发性传输。当令牌桶中没有令牌的时候，报文将不能被发送，只有等到桶中生成了新的令牌，报文才可以发送，这就可以限制报文的流量只能是小于等于令牌生成的速度，达到限制流量的目的。

版权所有 © 华为技术有限公司

图 4-63 单令牌桶原理图（图中以顺时针方向来表示处理过程）



上图中报文1、2、3、4表示不同的报文编号，每个报文在令牌桶中经过时会消耗与自身同等大小的令牌，为简便描述，这里假定每个报文大小相等。

双令牌桶（TrTCM）原理

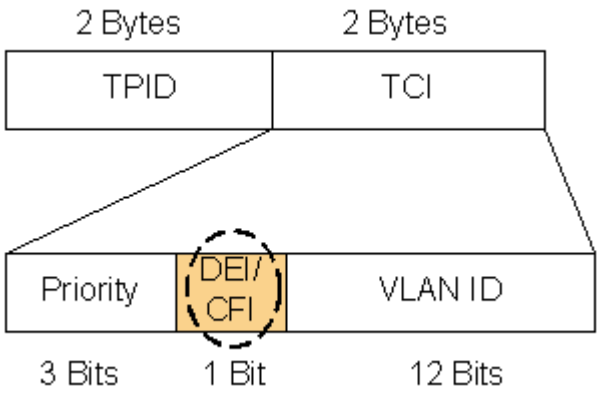
双速率三色标记（TrTCM）算法在RFC2698中定义，可用于流量监管（Policing）和标记（Marking），以进行更有效的带宽管理。它在静态规划带宽的基础上，能够保证用户的基本带宽（CIR，保证信息速率），并允许在网络空闲时让用户获得额外带宽服务（PIR，峰值信息速率），提高网络资源的利用率。

TrTCM实现原理：

- 采用双令牌桶P桶和C桶，其最大尺寸分别为PBS和CBS（PBS >CBS），初始情况下两个令牌桶都是满的。
- 报文通过后，每个令牌桶减少相应大小的令牌。
- 每秒钟分别向两个桶放入PIR、CIR数量的令牌（PIR>=CIR），但桶内的令牌总数不能超过该桶的最大尺寸。
- 根据令牌桶内令牌情况，通过标识报文的DEI位（如图4-64所示）对报文进行颜色标记（绿色、黄色、红色），标记的颜色主要是为后续的拥塞避免和拥塞管理提供报文处理依据。

版权所有 © 华为技术有限公司

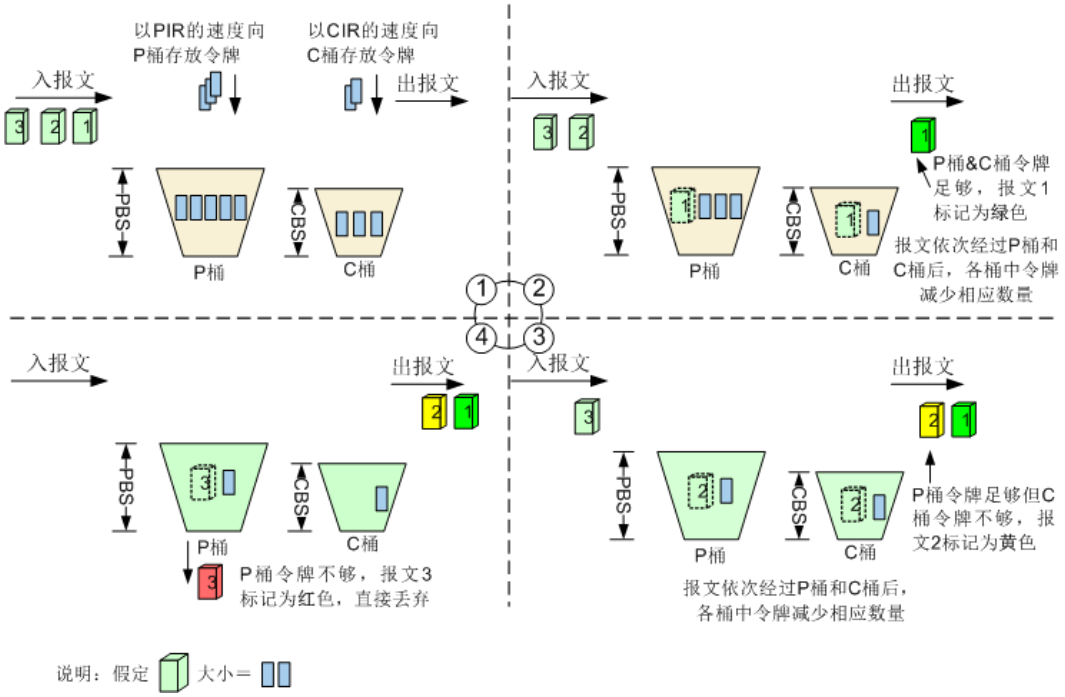
图 4-64 802.1ad 标准的 DEI 位（复用 802.1Q 的 CFI 位）



如图4-65所示。

1. 当报文速率≤CIR时，将报文标识为绿色（DEI置0），允许通过。如图中的报文1。
2. 当CIR＜报文速率＜PIR时，将报文标识为黄色（DEI置1），允许通过。如图中的报文2。
3. 当报文速率＞PIR时，将报文标识为红色，直接丢弃。如图中的报文3。

图 4-65 双令牌桶原理（图中以顺时针方向来表示处理过程）



上图中报文1、2、3表示不同的报文编号，每个报文在令牌桶中经过时会消耗与自身同等大小的令牌，为简便描述，这里假定每个报文大小相等。

版权所有 © 华为技术有限公司

流量监管的分类

ONU支持多种流量监管方式。

- 基于业务流的限速
- 流量抑制

流量监管方式	说明	令牌桶算法
基于业务流的限速	配置业务流的时候，通过绑定上下行流量模板进行限速。 如果业务流不需要限速，也可以配置流量模板为car-off，默认不限速。 同一单板或端口，基于业务流的限速和基于Port+CoS的限速不能同时生效。 配置命令： ● **service-port** ● **traffic table ip**	TrTCM
流量抑制	对广播、未知多播、未知单播报文在入口方向进行抑制，防止这类报文占用过多的网络资源，造成网络拥塞。 配置命令：**traffic-suppress**	-

4.4.8 拥塞避免

4.4.8.1 介绍

定义

拥塞避免，是指通过监视网络资源（如队列或内存缓冲区）的使用情况，在系统发生拥塞时，主动丢弃报文，通过调整网络的流量来解除网络过载的一种流控机制。

拥塞避免的实质是解决报文如何入队列及入队列前如何进行丢弃的问题。

目的

通过一定的丢弃算法来避免拥塞加剧，同时又可充分利用网络带宽。

4.4.8.2 基本概念

拥塞避免是采用报文丢弃算法来实现的，ONU支持如下的丢弃算法。

- 尾丢弃（Tail Drop）
- 加权随机早期检测（Weighted Random Early Detection，WRED）

4.4.8.3 实现原理

ONU支持如下的拥塞避免算法：

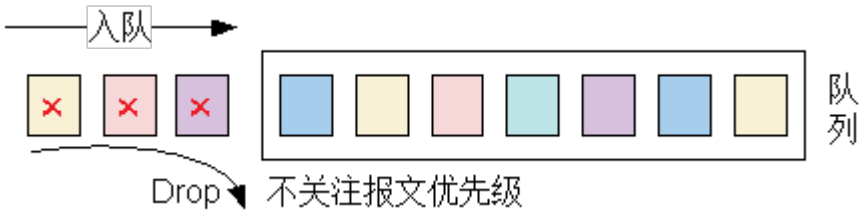
版权所有 © 华为技术有限公司

- 尾丢弃
- WRED

尾丢弃

当接口发生完全拥塞时（队列的长度达到规定的最大长度（队列深度）），总是将最后到达的数据包丢弃，直到没有拥塞为止。如图4-66所示。

图 4-66 尾丢弃



尾丢弃是所有队列的固有动作，无需配置也无法配置。

基于颜色的 WRED

系统通过流量监管trTCM算法可以给报文标识上不同的颜色（黄色和绿色，红色的报文则直接丢弃），在入端口队列时基于颜色设置该队列中黄色和绿色报文的丢弃下限和丢弃上限，当队列中的黄色报文比率小于报文丢弃下限时，不丢弃报文；当队列中黄色报文的比率在报文丢弃下限和报文丢弃上限之间时，队列开始随机丢弃黄色报文。并且黄色报文的比率越大，被随机丢弃的概率越高。

可通过**wred-profile**命令配置黄、绿色报文的丢弃下限（**low-limit**）和丢弃上限（**high-limit**），以及丢弃上限的丢弃率（**discard-probability**）。

某时刻报文丢弃率 =（该时刻报文缓存区使用率 － 丢弃下限）÷（丢弃上限 － 丢弃下限）× 丢弃上限的丢弃率

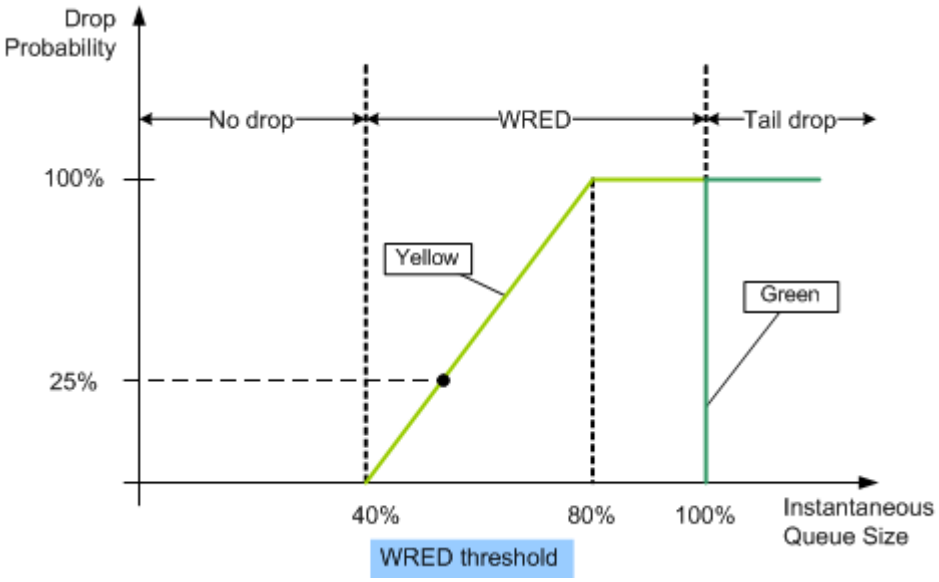
入端口上的8个队列可通过**queue-wred**命令绑定对应的WRED模板，以实现不同队列上黄、绿色报文的灵活丢弃。

如图4-67所示，设置黄色报文丢弃下限为40%，丢弃上限为80%，丢弃上限的报文丢弃率为100%；绿色报文不早丢弃（**wred-profile**命令）。

- 当队列中的黄色报文数<队列深度的40%时，队列不会丢弃报文，黄、绿色报文可以继续入队。
- 当队列中的黄色报文数≥队列深度的40%时，后续入队列的黄色报文被按照此刻的丢弃率（如图中某时刻丢弃率为25%）进行部分丢弃，绿色报文和部分黄色报文可以继续入队。
- 当队列中的黄色报文数≥队列深度的80%时，后续入队列的黄色报文被直接丢弃。绿色报文可以继续入队。
- 当队列中的报文数=队列深度的100%时，队列进行尾丢弃，所有后达的报文被直接丢弃。

版权所有 © 华为技术有限公司

图 4-67 基于颜色的 WRED



说明

上图中的黄线为丢弃率曲线。

4.4.9 拥塞管理

4.4.9.1 介绍

定义

在报文到达的速度超过接口发送报文的速度时，接口就发生了拥塞。拥塞管理是指设备/网络在发生拥塞时，如何进行管理和控制。

拥塞管理使用的是队列技术，本质上是为了解决报文的出队列问题。

目的

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。

4.4.9.2 基本概念

拥塞管理是采用队列技术实现的，ONU支持如下的队列技术：

- PQ（Priority Queue）
- WRR（Weighted Round Robin）
- PQ+WRR

版权所有 © 华为技术有限公司

表 4-20 基本概念的解释

概念	解释	备注
PQ	优先级队列，采用严格优先级（Strict Priority）调度算法，共8个优先级，高优先级报文得到优先调度。	关键业务的报文能够得到优先处理。
WRR	加权轮询调度，按配置权重进行队列调度。	保证每个队列都得到一定的服务。
PQ +WRR	严格优先级调度和加权轮询调度的组合，队列优先调度部分高优先级报文，然后按权重调度其余的报文。	既保证了高优先级业务，在有带宽剩余时又能调度低优先级业务。
入队优先级	报文进入队列时的优先级，它决定了报文进入哪个队列。	入队优先级有多种来源，取值为0-7。
队列缓存	也称队列深度，决定了队列处理突发报文的能力。队列缓存表示该队列存储缓冲区域越大，处理突发报文的能力也就越强，丢包越少，但同时也导致报文时延越大。	-

4.4.9.3 实现原理

报文在入队前及队列中的处理步骤为：

1. 分类–详见**4.4.5.2 实现原理**。
2. 入队–按照报文的优先级和队列之间的映射关系进入不同的队列。
3. 调度–报文进入队列后按照该队列的调度技术进行调度。

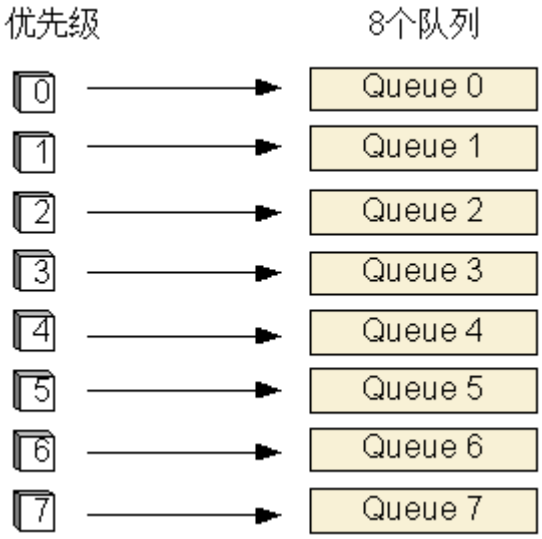
入队

在经过了优先级处理之后，报文按照优先级和队列之间的映射关系进入不同的队列。缺省情况下，优先级和队列之间存在着固定的映射关系，如**图4-68**所示。

队列ID的值越大，其报文转发的优先级就越高，所以，在所有8个队列中，ID为7的队列优先级最高。

版权所有 © 华为技术有限公司

图 4-68 优先级和队列之间的缺省映射关系



系统也支持优先级和队列的灵活映射，可以通过**cos-queue-map**命令映射报文的802.1p优先级到任意一个队列中，即：允许一个队列同时包含多个802.1p优先级，又允许一个队列不包含任何802.1p优先级。

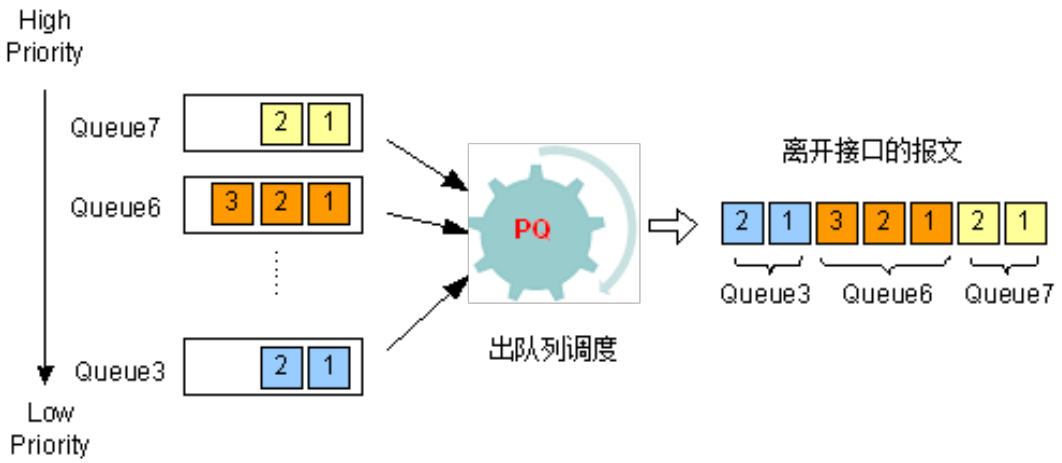
由于优先级与队列的映射关系是全局配置，一般情况下如果无特殊需求，请不要自行设置，使用系统缺省值即可。

调度-PQ

优先级队列（Priority Queue）将队列分为高优先队列、中优先队列、正常优先队列和低优先队列，它们的优先级依次降低。如图4-69所示，在报文出队的时候，PQ首先让高优先队列中的报文出队并发送，直到高优先队列中的报文发送完，然后发送中优先队列中的报文，同样，直到发送完，然后是正常优先队列和低优先队列。

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 4-69 PQ 调度机制



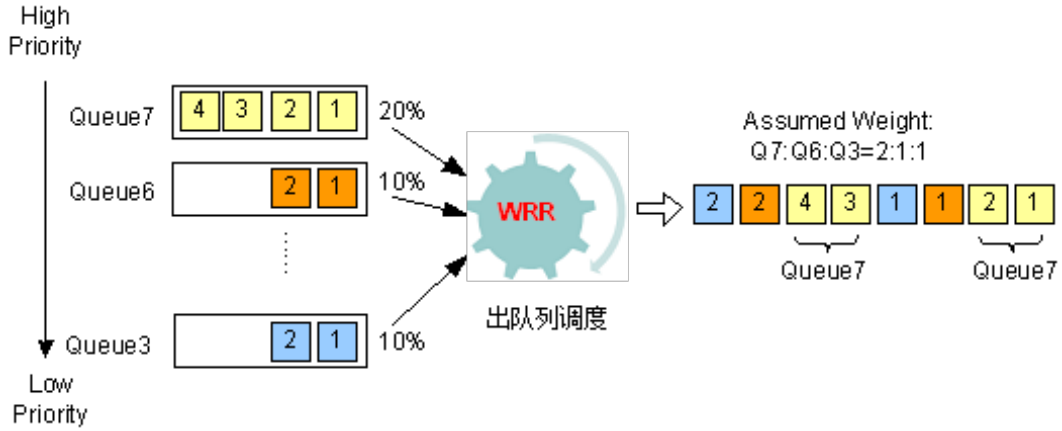
版权所有 © 华为技术有限公司

调度-WRR

加权轮询调度WRR（Weighted Round Robin）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。如图4-70所示，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。

WRR调度模式是在队列之间按照一定的权重轮流调度，保证每个队列都得到一定的服务。当某一队列为空时，可以立即切换到下一个队列进行调度，充分利用带宽资源。

图 4-70 WRR 调度机制

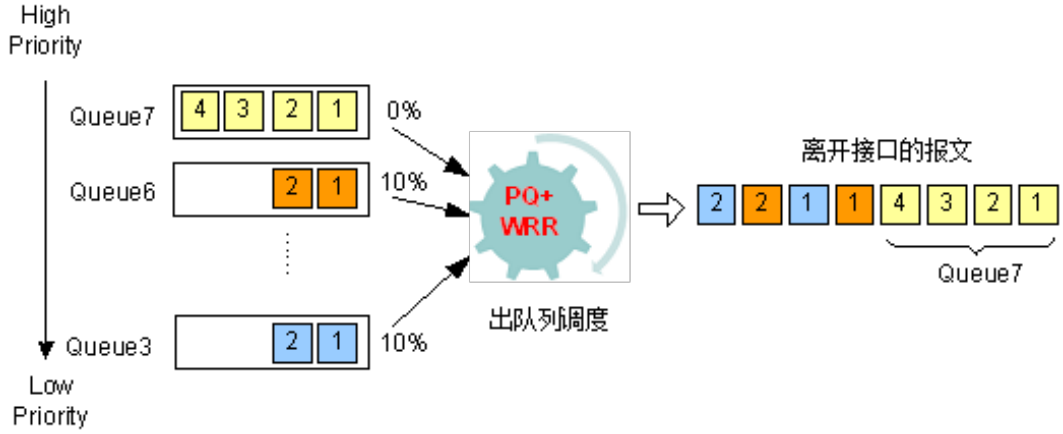


调度-PQ+WRR

PQ+WRR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。如图4-71所示，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能使低优先级业务得到处理。

图 4-71 PQ+WRR 调度机制



版权所有 © 华为技术有限公司

4.4.10 ACL 策略

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。

4.4.10.1 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，提高系统的安全性。

4.4.10.2 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：

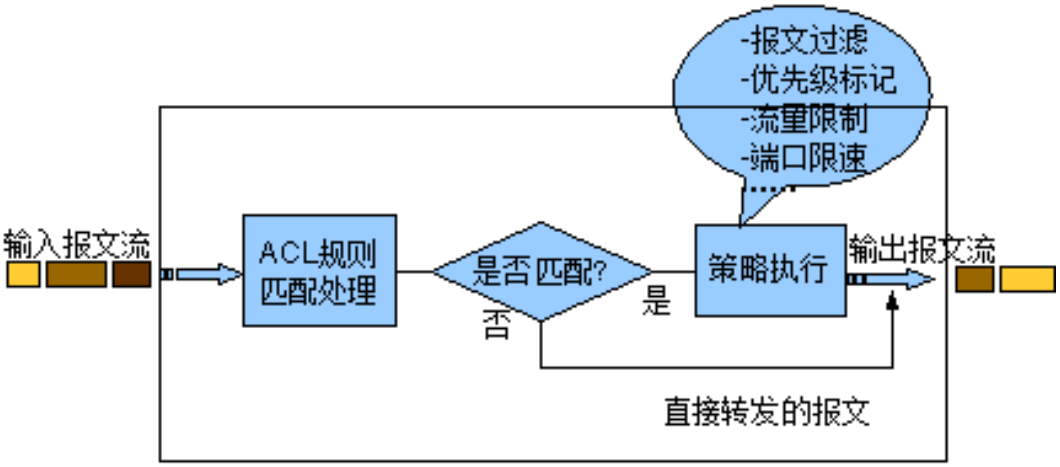
- 如果匹配规则，则执行QoS策略处理，包括报文过滤、优先级标记、流量限制、流量统计、报文镜像，在完成策略执行处理后再转发输出报文流。
  - 报文过滤：按照匹配ACL规则匹配的结果确定是否丢弃报文。
  - 优先级标记：对匹配ACL规则的数据包进行优先级标记，标记内容包括802.1p等。
  - 流量限制：对匹配访问ACL规则的数据包进行流量限制。
  - 流量统计：对匹配ACL规则的数据包进行流量统计。
  - 报文镜像：对匹配访问控制列表的数据包进行流镜像，可以将匹配ACL的报文流拷贝输出到其他端口。

  说明

  根据业界惯例，出于保障网络运营和服务的目的，镜像功能可能涉及获取个人数据和个人用户通信内容（产品本身不对这些数据进行存储、解析或处理）。本公司无法单方采集或存储个人数据和用户通信内容，建议运营商只有在所适用法律法规允许的目的和范围内方可启用相应的功能。在使用、存储用户个人数据和通信内容的过程中，您应采取足够的措施以确保用户的个人数据和通信内容受到严格保护。
- 否则，按照ACL规则的定义，不匹配规则的报文将被直接转发。

版权所有 © 华为技术有限公司

图 4-72 ACL 规则过滤处理原理图



4.5 IPv6

IPv6（Internet Protocol Version 6）是网络层协议的第二代标准协议，也被称为IPng（IP Next Generation）。

4.5.1 为什么引入 IPv6

定义

IPv6是IETF（Internet Engineering Task Force，Internet工程任务组）设计的一套规范，是IPv4（Internet Protocol Version 4）的升级版本。IPv6和IPv4之间最显著的区别就是IP地址长度从原来的32位升级为128位。IPv6以其简化的报文头格式、充足的地址空间、层次化的地址结构、灵活的扩展头、增强的邻居发现机制将在未来的市场竞争中充满活力。

目的

以IPv4为核心技术的Internet获得巨大成功，促使IP技术得到广泛应用。同时，随着因特网的迅猛发展，IPv4设计的不足也日益明显，主要有以下几点：

- IPv4地址空间不足

  IPv4地址采用32比特标识，理论上能够提供的地址数量是43亿。但由于地址分配的原因，实际可使用的数量不到43亿。另外，IPv4地址的分配也很不均衡：美国占全球地址空间的一半左右，而欧洲则相对匮乏；亚太地区则更加匮乏。与此同时，移动IP和宽带技术的发展需要更多的IP地址。IPv4地址资源紧张直接限制了IP技术应用的进一步发展。

  针对IPv4的地址短缺问题，也曾先后出现过几种解决方案。比较有代表性的是CIDR(Classless Inter-Domain Routing)和NAT(IP Network Address Translator)。但是CIDR和NAT都有各自的弊端和不能解决的问题，由此推动了IPv6的发展。

- 骨干设备维护的路由表的表项数量过大

  由于IPv4发展初期的分配规划问题，造成许多IPv4地址分配不连续，不能有效聚合路由。日益庞大的路由表耗用大量的内存，对设备成本和转发效率产生影响，这一问题促使设备制造商不断升级其产品，以提高路由寻址和转发性能。

版权所有 © 华为技术有限公司

- 不易进行自动配置和重新编址

  由于IPv4地址只有32比特，并且地址分配不均衡，导致在网络扩容或重新部署时，经常需要重新分配IP地址。因此需要能够进行自动配置和重新编址以减少维护工作量。

- 不能解决日益突出的安全问题

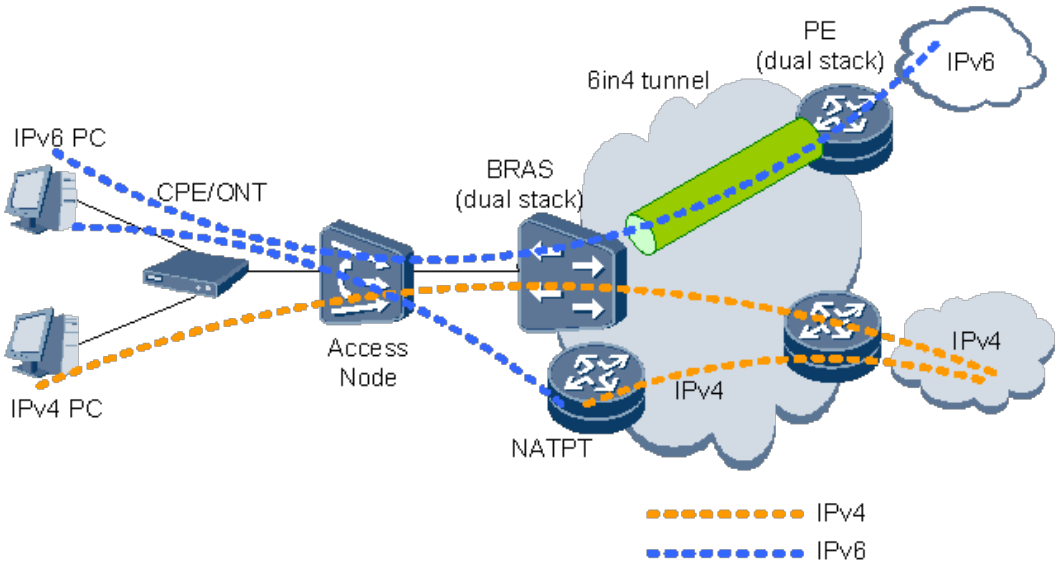
  随着因特网的发展，安全问题越来越突出。IPv4协议制定时并没有仔细针对安全性进行设计，因此固有的框架结构并不能支持端到端的安全。IPv6可以提供端到端的安全特性。

IPv6技术从根本上解决了IP地址短缺的问题；且易于部署，能够兼容当前的各种应用，方便用户的平滑过渡；同时可实现与IPv4网络的共存和互通。由于IPv4存在以上弊端和不足，IPv6技术的优越性显而易见，因此IPv6技术得以迅猛发展。

4.5.2 IPv6 网络部署

IPv6主要是解决全球IPv4地址空间不足而引入的技术，在IPv4网络向IPv6网络过渡的初期，IPv4网络已被大量部署，而IPv6网络只是散布在世界各地的一些孤岛。初期IPv6部署如图4-73所示。

图 4-73 IPv6 初期网络部署



现网IPv4 BRAS逐步升级支持双栈，双栈BRAS提供6in4隧道或专用链路将IPv6流量传递到IPv6网络。

双栈BRAS提供NAT-PT(Network Address Translator - Protocol Translator)功能，支持IPv6用户访问IPv4网络。

接入设备支持IPv6报文感知，IPv6地址分配（DHCPv6），以及IPv6 ACL安全控制等。

4.5.3 IPv6 实现原理

IPv6基本功能主要包括IPv6邻居发现、IPv6路径MTU发现。邻居发现和Path MTU发现机制均是基于ICMPv6协议报文实现的。

版权所有 © 华为技术有限公司

4.5.3.1 IPv6 的特点

- 128位地址结构，提供充足的地址空间

  近乎无限的IP地址空间是部署IPv6网络最大的优势。和IPv4相比，IPv6的地址比特数是IPv4的4倍（从32位扩充到128位）。128位地址可包含约43亿×43亿×43亿×43亿个地址节点，足已满足任何可预计的地址空间分配（IPv4 理论上能够提供的上限是43 亿个，而IPv6 理论上地址空间的上限是43亿×43亿×43亿×43亿个）。

- 层次化的地址结构

  IPv6的地址空间采用了层次化的地址结构，利于路由快速查找，同时借助路由聚合，可减少IPv6路由表的大小，提高路由设备的转发效率。

- 地址自动配置

  IPv6协议内置支持通过地址自动配置方式使主机自动发现网络并获取IPv6地址，大大提高了内部网络的可管理性。使用自动配置，用户设备（如移动电话、无线设备）可以即插即用 而无需手工配置或使用专用服务器（如DHCP Server）。IPv6支持有状态地址配置（Stateful Address Autoconfiguration）和无状态地址配置（Stateless Address Autoconfiguration）。

  - 对于有状态地址配置，主机通过服务器获取地址信息和配置信息。
  - 对于无状态地址配置，主机自动配置地址信息，地址中带有本地路由设备通告的前缀和主机的接口标识。如果链路上没有路由设备，主机只能自动配置链路本地地址，实现与本地节点的互通。

- 源/目的地址选择

  当网络管理者需要指定和预知系统发送报文的源/目的地址时，可以定义一组地址选择规则，这些规则构成地址选择策略表。该表类似于路由表，使用最长匹配原则查找规则。地址选择的结果是由源地址和目的地址共同决定的。

  依次根据以下规则进行源地址选择，规则的编号越小，优先级越高。

  a. 源地址和目的地址相同
  b. 合适的生效范围
  c. 避免使用已经废弃的地址
  d. 家乡地址（home address）
  e. 出接口地址
  f. 源地址的*label*值和目的地址的*label*值相同
  g. 最长匹配原则

  说明

  备选的源地址可以限定为配置在出接口上的单播地址，如果在出接口上没有找到和目的地址具有相同*label*值和范围的源地址，则可以选择其他接口上具有相同*label*值和范围的地址作为源地址。

  依次根据以下规则进行目的地址选择，规则的编号越小，优先级越高。

  a. 避免使用不可用的目的地址
  b. 合适的生效范围
  c. 避免使用已经废弃的地址
  d. 家乡地址（home address）
  e. 目的地址的*label*值和源地址的*label*值相同
  f. 较高的*precedence*值

版权所有 © 华为技术有限公司

g. 在本地转发报文，不需要使用6over4或6to4隧道
h. 更小的生效范围
i. 最长匹配原则
j. 遵循原来的顺序

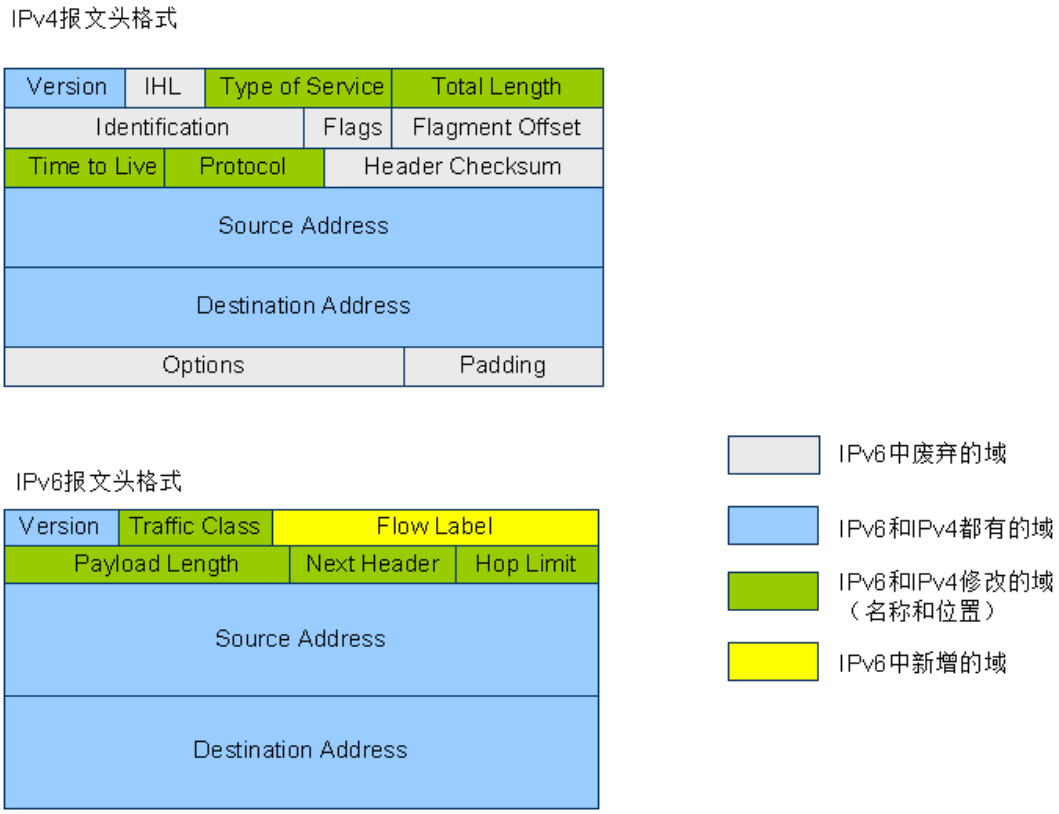
- 支持QoS

  IPv6报头的新字段定义了流量应该被如何标识和处理。通过报文头里的流标签（Flow Label）字段完成流量标识，允许路由设备对某一流中的报文进行识别并提供特殊处理。

- 灵活、简洁的可扩展报文头

  IPv6 和IPv4 报文头格式对比如图4-74所示。IPv6和IPv4相比，去除了IHL（Internet Header Length）、identifiers、Flags、Fragment Offset、Header Checksum、 Options、Paddiing域，只增了流标签域，因此IPv6报文头的处理较IPv4大大简化，提高了处理效率。另外，IPv6为了更好支持各种选项处理，提出了扩展头的概念，新增选项时不必修改现有结构就能做到，理论上可以无限扩展，体现了优异的灵活性。

图 4-74 IPv6 和 IPv4 报文头格式对比



4.5.3.2 IPv6 地址

IPv6 地址的书写格式

IPv6的128位IP地址有以下两种表示形式。

- X:X:X:X:X:X:X:X

版权所有 © 华为技术有限公司

  - 在这种形式中，IPv6的128位地址被分为8组，每组的16位用4个十六进制字符（0～9，A～F）来表示，组和组之间用冒号（:）隔开。其中每个“X”代表一组十六进制数值。比如下面这个IPv6地址：

    2031:0000:130F:0000:0000:09C0:876A:130B

    为了书写方便，每组中的前导“0”都可以省略，所以上述地址可写为：

    2031:0:130F:0:0:9C0:876A:130B。
  - 另外，地址中包含的连续两个或多个均为0的组，可以用双冒号“::”来代替，这样可以压缩IPv6地址书写时的长度，所以上述地址又可以进一步简写为：

    2031:0:130F::9C0:876A:130B。

    在一个IPv6地址中只能使用一次双冒号“::”，否则当计算机将压缩后的地址恢复成128位时，无法确定每段中0的个数。
- X:X:X:X:X:X:d.d.d.d

  分为如下两种类型：
  - IPv4兼容IPv6地址。地址格式为：0:0:0:0:0:0:IPv4-address，其高阶96bits均为0，其低阶32bits是一个IPv4地址。该IPv4地址必须是IPv4网络中可达的IPv4地址，且不能是组播地址、广播地址、环回地址或未指定的地址（0.0.0.0）。
  - IPv4映射IPv6地址。地址格式为：0:0:0:0:0:FFFF:IPv4-address。该地址用来将IPv4节点的地址表示为IPv6地址。

    其中IPv4兼容IPv6地址用于配置IPv6 over IPv4隧道。

    其中“X”代表高阶的六组数字，用十六进制数来表示每组的16比特。“d”代表低阶的四组数字，用十进制数表示每组的8比特。后边的部分（d.d.d.d）其实就是一个标准的IPv4地址。

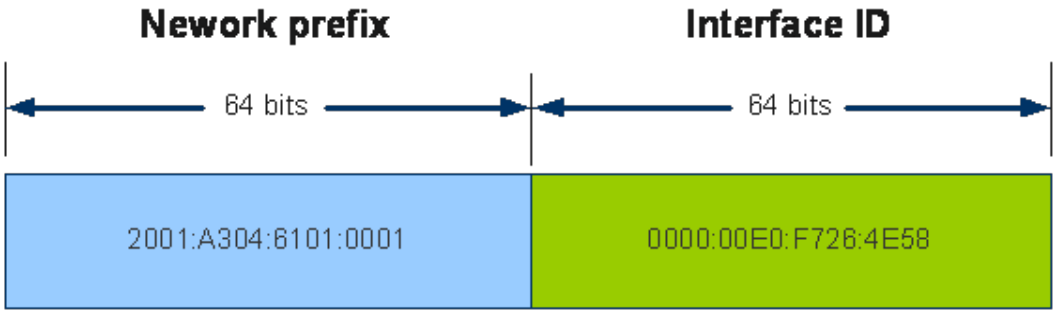
IPv6 地址的结构

一个IPv6地址可以分为如下两部分：

- 网络前缀：n比特，相当于IPv4地址中的网络ID
- 接口标识：128-n比特，相当于IPv4地址中的主机ID

地址2001:A304:6101:1::E0:F726:4E58 /64的构成如图4-75所示。

图 4-75 地址 2001:A304:6101:1::E0:F726:4E58 /64 的构成示意图



版权所有 © 华为技术有限公司

IPv6 的地址分类

IPv6主要有三种地址：

- 单播地址（Unicast）：唯一标识一个接口，类似于IPv4的单播地址。发送到单播地址的数据包将被传输到此地址所标识的唯一接口。

  单播地址还可以分为四种，如表4-21所示。

  表 4-21 IPv6 单播地址类型

地址类型	二进制前缀	IPv6前缀标识
链路本地单播地址	1111111010	FE80::/10
环回地址	00...1 (128 bits)	::1/128
未指定地址	00...0 (128 bits)	::/128
全球单播地址	其他	-

  表中各类地址的意义如下：

  - 链路本地单播地址：用于邻居发现协议和无状态自动配置进程中链路本地上节点之间的通信。使用链路本地地址作为源或目的地址的数据包不会被转发到其他链路上。使用链路本地前缀FE80::/10(1111 1110 10)和IEEE EUI-64格式的接口标识符（EUI-64可来源于EUI-48）可在任意接口对其进行自动配置。
  - 环回地址0:0:0:0:0:0:0:1或::1，不会被分配给任何接口。它的作用与在IPv4中的127.0.0.1相同，即节点将IPv6报文发送给自己。
  - 未指定地址（::），不能被分配给任何节点，也不能作为目的地址。在主机初始化且没有取得自己的地址时，未指定地址可以用在IPv6报文的源地址字段，例如重复地址探测时，NS（Neighbor Solicitation）报文的源地址就是未指定地址。
  - 全球单播地址等同于IPv4公网地址。用于可以聚合的链路，最后提供给网络服务提供商。这种地址类型的结构允许路由前缀的聚合，从而满足全球路由表项的数量限制。地址包括运营商管理的48位路由前缀和本地站点管理的16位子网ID，以及64位接口ID。如无特殊说明，全球单播地址包括站点本地单播地址。

- 任播地址（Anycast）：用来标识一组接口（通常这组接口属于不同的节点）。发送到任播地址的数据包被传输给此地址所标识的一组接口中距离源节点最近的一个接口（最“近”的一个，是指根据路由协议的距离度量）。

  应用场合：当移动主机需要与它的“home”子网上的移动代理之一通信时，它将用该子网路由设备的任播地址。

  具体地址规定：任播地址没有独立的地址空间，它们可使用任何单播地址的格式。因此，需要一种语法来区别任播地址和单播地址。

- 组播地址（Multicast）：用来标识属于不同节点的一组接口，类似IPv4的组播地址。发送到组播地址的数据包被传输给此地址所标识的所有接口。

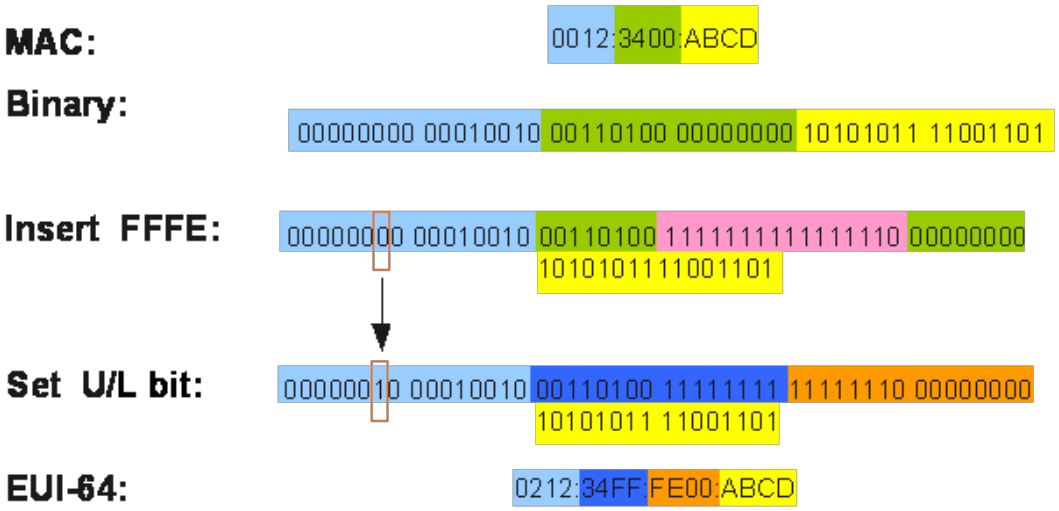
  IPv6不包括广播地址，广播地址的功能均由组播地址来提供。

版权所有 © 华为技术有限公司

IEEE EUI-64 格式的接口标识符

IPv6地址中的64位接口标识符（Interface ID）用来标识链路上的唯一接口。这个地址是从接口的链路层地址（如MAC地址）变化而来的。IPv6地址中的接口标识符是64位，而MAC地址是48位，因此需要在MAC地址的中间位置插入十六进制数FFFE（1111 1111 1111 1110）。然后将U/L位（从高位开始的第7位）设置为“1”，这样就得到了EUI-64格式的接口ID。具体转换过程如图4-76。

图 4-76 MAC 地址到 EUI-64 格式的转换过程

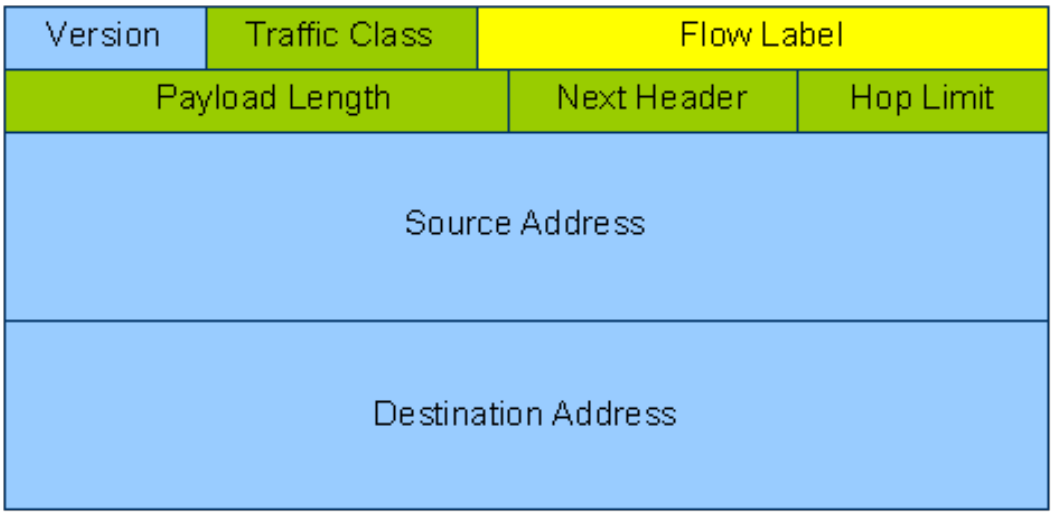


4.5.3.3 IPv6 报文格式

IPv6 报文基本头格式

IPv6报文基本头格式如图4-77所示。

图 4-77 IPv6 报文基本头格式



版权所有 © 华为技术有限公司

- Version：

  4比特。值为6表示IPv6报文。

- Traffic Class：

  8比特。类似于IPv4中的TOS域。

- Flow Label：

  20比特。IPv6中新增。流标签可用来标记特定流的报文，以便在网络层区分不同的报文。转发路径上的路由器可以根据流标签来区分流并进行处理。由于流标签在IPv6报文头中携带，转发路由器可以不必根据报文内容来识别不同的流，目的节点也同样可以根据流标签识别流。

- Payload Length：

  16比特。以字节为单位的IPv6载荷长度，也就是IPv6报文基本头以后部分的长度（包括所有扩展头部分）。

- Next Header：

  8比特。用来标识当前头（基本头或扩展头）后下一个头的类型。此域内定义的类型与IPv4中的协议域值相同。基本头中的Next Header或扩展头中的Next Header链接成一条链，这一机制下处理扩展头更高效，转发路由器只处理必须处理的选项头，提高了转发效率。

- Hop Limit：

  8比特。和IPv4中的TTL字段类似。每个转发此报文的节点把此域值减1，如果此域值减到0则丢弃。

- Source Address：

  128比特。报文的源地址。

- Destination Address：

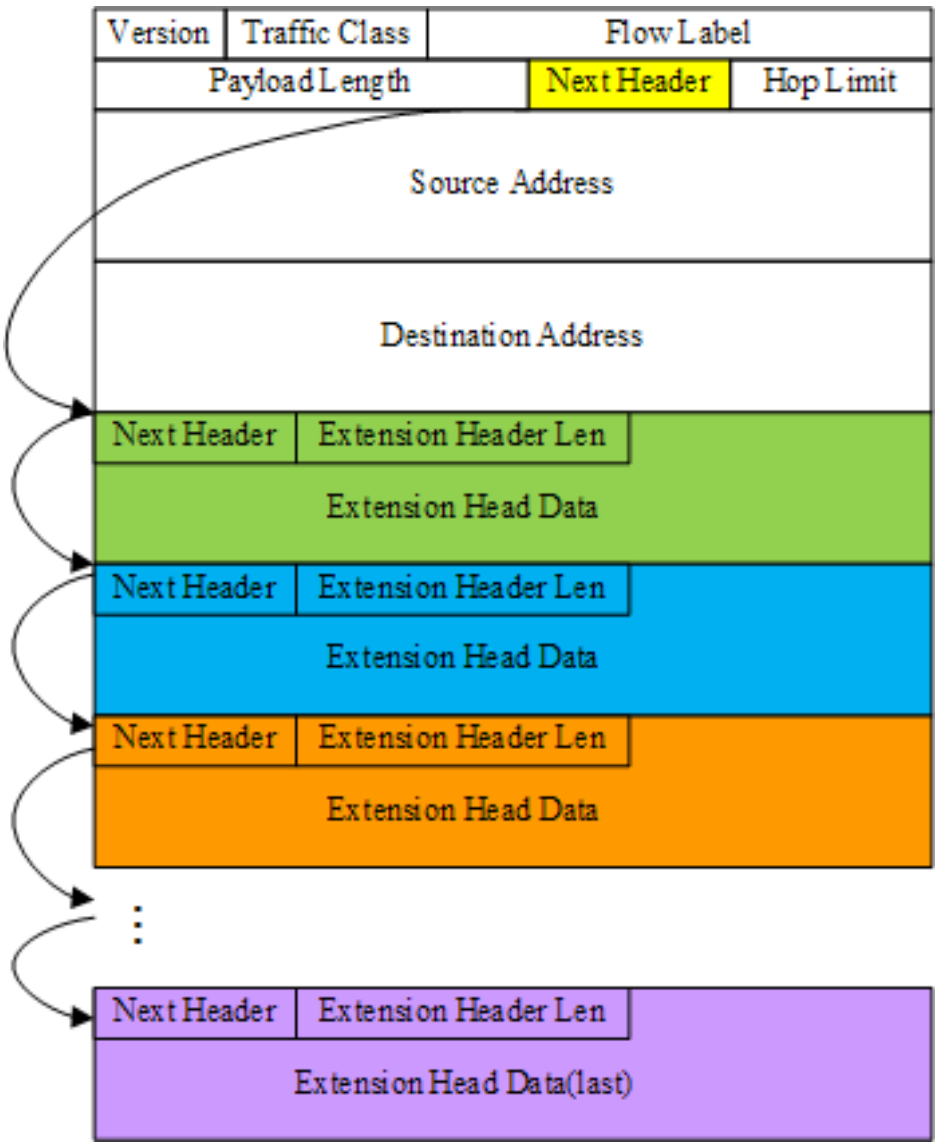
  128比特。报文的目的地址。

IPv6 报文扩展头格式

IPv6报文扩展头格式如**图4-78**所示。

 版权所有 © 华为技术有限公司

图 4-78 IPv6 报文扩展头格式



IPv6选项字段是通过形成链式结构的扩展头支持的。IPv6基本头后面可以有0到多个扩展头。

IPv6扩展头排列顺序如下：

- 逐跳选项头（Hop-by-Hop Options Header）

  值为0（在IPv6 基本头中定义）。用于路由告警与Jumbo帧。此扩展头被转发路径所有节点处理。
- 目的选项头（Destination Options Header）

  值为60。只可能出现在两个位置：
  - 路由头前

    这时此选项头被目的节点和路由头中指定的节点处理。

 版权所有 © 华为技术有限公司

- 上层头前（任何ESP选项后）
  此时只能被目的节点处理。

- 路由头（Routing Header）
  值为43。用于源路由选项和Mobile IPv6。
- 分片头（Fragment Header）
  值为44。此选项头在源节点发送的报文超过Path MTU（源和目的之间传输路径的MTU）时对报文分片时使用。
- 验证头（Authentication Header）
  值为51。提供报文验证、完整性检查。定义和IPv4中相同。
- 封装安全载荷头（ESP Header）
  值为50。提供报文验证、完整性检查和加密。定义和IPv4中相同。
- 上层头（Upper-layer Header）
  上层协议头，如TCP/UDP/ICMP等。

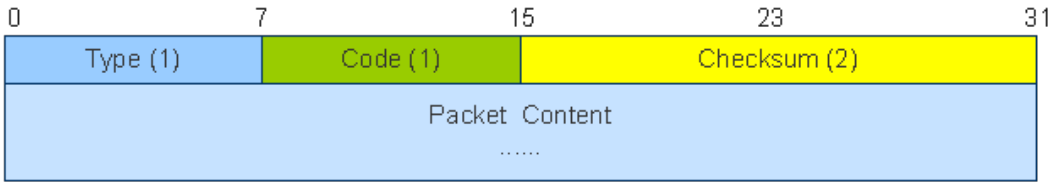
目的选项头最多出现两次（一次在路由头前，一次在上层协议头前），其它选项头最多出现一次。

但IPv6节点必须能够处理选项头（逐跳选项头除外，它固定只能紧随基本头之后）的任意出现位置和任意出现次数，以保证互通性。

4.5.3.4 ICMPv6

ICMPv6（Internet Control Message Protocol for the Internet Protocol Version 6）是IPv6的基础协议之一，具有差错报文和信息报文两种，用于IPv6节点报告报文处理过程中的错误和信息。ICMPv6报文的报文格式如图4-79所示。

图 4-79 ICMPv6 报文格式



报文中各个字段的解释如下：

- Type字段表明消息的类型，0至127表示差错报文类型，128至255为消息报文类型。
- Code字段表示此消息类型细分的类型。
- Checksum表示ICMPv6报文的校验和。

ICMPv6 错误报文的分类

- 目的不可达错误报文
  在IPv6节点转发IPv6报文过程中，发现目的地址不可达时，就会向发送报文的源节点发送ICMPv6目的不可达错误报文。同时报文中会携带引起该错误报文的具体原因。目的不可达错误报文又细分为以下几种：

版权所有 © 华为技术有限公司

  - 没有到目的地的路由
  - 地址不可达
  - 端口不可达
- 数据包过大错误报文

  在IPv6节点转发IPv6报文过程中，发现报文超过出接口的链路MTU时，则向发送报文的源节点发送ICMPv6数据包过大错误报文，其中携带出接口的链路MTU值。数据包过大错误报文是Path MTU发现机制的基础。
- 时间超时错误报文

  在IPv6报文收发过程中，当设备收到Hop Limit值等于0的数据包，或者当设备将HopLimit值减为0时，会向报文的源节点发送ICMPv6超时错误报文。对于分段重组报文的操作，如果超过定时时间，也会产生一个ICMPv6超时报文。
- 参数错误报文

  当目的节点收到一个IPv6报文时，会对报文进行有效性检查，如果发现以下问题会向报文的源节点回应一个ICMPv6参数错误差错报文。
  - IPv6基本头或扩展头的某个域有错误
  - IPv6基本头或扩展头的NextHeader值不可识别
  - 扩展头中出现未知的选项

ICMPv6 信息报文的分类

请求信息（Echo Request）和应答信息（Echo Reply）。可以利用ICMPv6信息报文实现网络故障诊断、PMTU发现和邻居发现等功能。在两节点的互通性检测中，收到Echo Request报文的节点向源节点回应Echo Reply报文，实现两节点间报文的收发。

4.5.3.5 Path MTU

网络上的 MTU 问题

从源地址到目的地址可能会经过具有不同MTU值的接口，其中最小的MTU值即为该路径的Path MTU。

- 由于IPv6报文在传输过程中不允许在中间节点分片转发，所以在转发过程中经常会出现报文长度大于路径IPv6 MTU的情形，这就需要源节点不断的进行重传，降低了传输的效率。
- 如果在源节点使用最小链接IPv6 MTU（1280字节）作为分片的最大长度，在大多数情况下，路径的IPv6 MTU是大于最小链接的IPv6 MTU的，一个节点发出的分片远小于路径IPv6 MTU，这是对网络资源的一种浪费。

为了解决上述问题，提出了Path MTU发现协议。

Path MTU 的工作原理

PMTU发现协议描述了一种动态发现任意路径的PMTU的方法。当一个IPv6节点发送大量数据到另一节点时，数据通过一系列IPv6分片传送。当这些分片具有从源节点到信宿节点能够成功传送所允许的最大长度时，此时认为它达到理想状态，这个分片长度被称为Path MTU。

一个源节点开始会假设一个路径的PMTU是路径中第一跳的已知的IPv6 MTU，如果从那个路径发出的报文太大以至于不能沿着路径转发，中间节点将丢弃此报文并返回一

 版权所有 © 华为技术有限公司

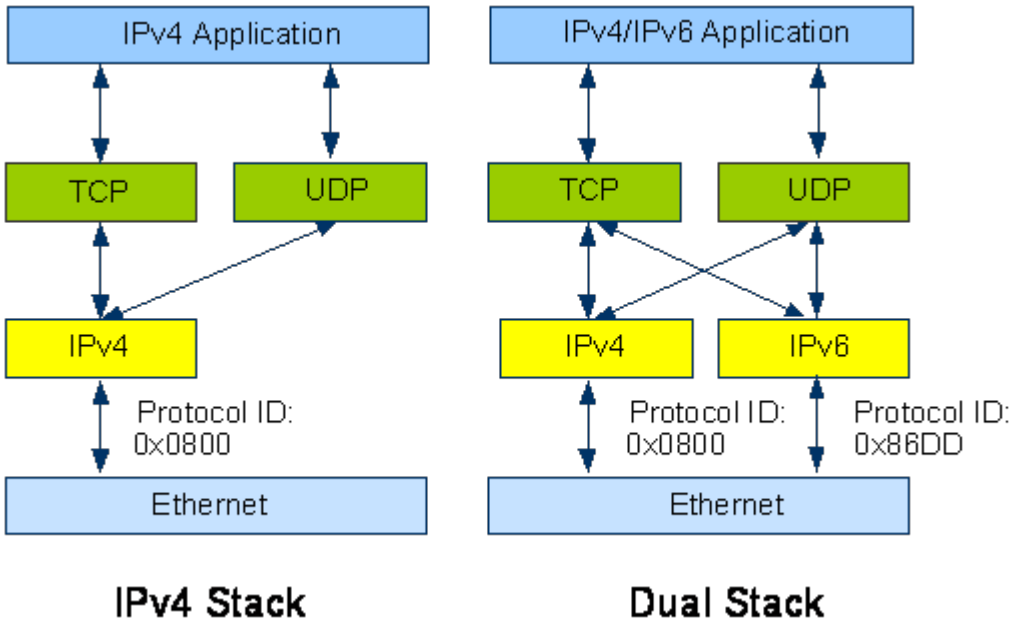
个ICMPv6数据过大差错报文给源节点，根据数据过大消息中的IPv6 MTU值来设置此路径的PMTU值。

当节点学习到的PMTU值小于或者等于实际的PMTU时，PMTU的发现过程结束。注意在PMTU发现过程结束之前，可能会出现反复发送报文和收到报文太大消息，这是因为可能会不断发现更远的路径链路有更小的IPv6 MTU。

4.5.3.6 双协议栈

对于IPv6节点来说，兼容IPv4的最直接有效的办法就是保留一个完整的IPv4协议栈，这样的节点即为双协议栈节点。单协议栈和双协议栈结构示例如图4-80所示。

图 4-80 单协议栈与双协议栈结构（以太网）



双协议栈具有以下特点：

- 多种链路协议支持双协议栈

  多种链路协议（如以太网）支持双协议栈。图中的链路层是以太网，在以太网帧上，如果协议ID字段的值为0x0800，表示网络层收到的是IPv4报文，如果为0x86DD，表示网络层是IPv6报文。

- 多种应用支持双协议栈

  多种应用支持双协议栈。上层应用（如DNS）可以选用TCP或UDP作为传输层的协议，但优先选择IPv6协议栈，而不是IPv4协议栈作为网络层协议。

4.5.3.7 TCP6

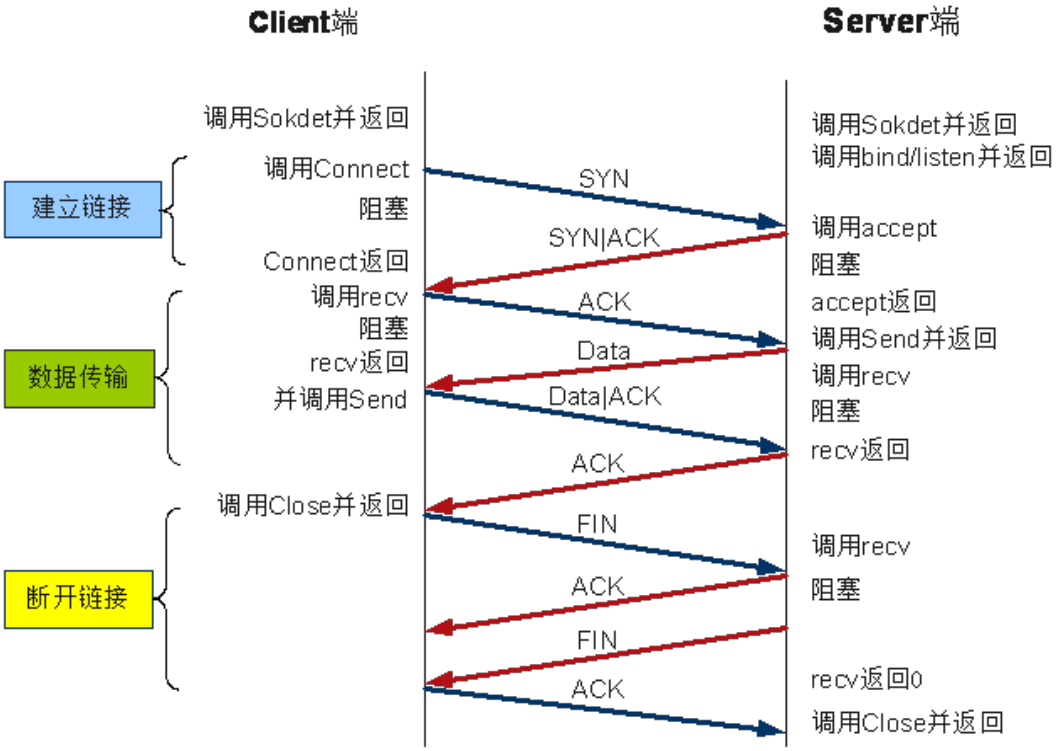
TCP6提供了在两个端点的进程间建立虚电路的机制，一个TCP6虚连接如同在系统间承载数据的全双工电路。由于TCP6中提供了进程间数据的可靠传输，因此被称为可靠协议，它还提供了根据当前网络状态来优化传输性能的机制。在所有数据均可收到和确认的情况下，传输速率可以逐渐增加。

版权所有 © 华为技术有限公司

TCP6通常用于交互式应用，如WEB之类。TCP6使用了“三次握手”机制来建立虚电路，所有的虚电路都需使用“四次握手”拆除。这种连接方式可以提供多种校验和及其他可靠性功能，但是增加了使用TCP6的开销并导致其效率低于UDP6。

如图4-81表示了TCP6连接建立和拆除的过程。

图 4-81 TCP6 连接建立和拆除过程示意图



4.5.3.8 UDP6

UDP6是用来在互连网络环境中提供包交换的计算机通信协议。有如下特点：

- 只使用源和目的信息，主要用于简单的请求/响应式结构。
- 不可靠，即没有任何控制能确定UDP6数据报是否已被接收。
- 无连接，即在主机间传输数据时，不需要任何类型的虚电路。

UDP6的无连接特性使得UDP6可以向广播地址发送数据；而TCP6则不同，它要求特定的源地址和目的地址。

4.5.3.9 RawIP6

RawIP6较为简单，只填充IPv6首部的有限几个字段，允许应用进程提供自己的IPv6首部。

RawIP6类似于UDP6：

- 不可靠，即没有任何控制能确定RawIP6数据报是否已被接收。
- 无连接，即在主机间传输数据时，不需要任何类型的虚电路。

版权所有 © 华为技术有限公司

RawIP6相比UDP6的区别在于，RawIP6允许应用程序直接通过Socket接口操作IP层。对于许多需要跟下层直接交互的应用来说，非常方便。

4.5.3.10 IPv6 邻居发现

邻居发现ND（Neighbor Discovery）是确定邻居节点之间关系的一组消息和进程。邻居发现协议替代了IPv4的ARP（Address Resolution Protocol）、ICMP路由器发现（Router Discovery）和ICMP重定向（Redirect）消息，并提供了其他功能。

对于一个节点而言，当其配置一个IPv6地址之后，首先会确定此地址是否可用、不冲突。当一个节点是主机时，路由器需要通知主机向特定目的地址转发报文的理想下一跳地址；当一个节点是路由器时，需要发布自己的地址、地址前缀和其他配置参数以指导主机进行参数配置。在IPv6报文转发过程中，节点需要确定邻居节点的链路层地址和其可达性。IPv6邻居发现机制提供了5种不同类型的ICMPv6报文。

- 路由器请求报文RS（Router Solicitation）：主机启动后，通过RS报文向路由设备发出请求，路由设备则会以RA报文响应。
- 路由器通告报文RA（Router Advertisement）：路由设备周期性的发布RA报文，其中包括前缀和一些标志位的信息。
- 邻居请求报文NS（Neighbor Solicitation）：IPv6节点通过NS报文可以得到邻居的链路层地址，检查邻居是否可达，也可以进行重复地址检测。
- 邻居通告报文NA（Neighbor Advertisement）：NA报文是IPv6节点对NS报文的响应，同时IPv6节点在链路层变化时也可以主动发送NA报文。
- 重定向报文（Redirect）：路由设备发现报文的入接口和出接口相同时，可以通过重定向报文通知主机选择另外一个更好的下一跳地址。

IPv6邻居发现协议主要包括以下功能：

地址冲突检测功能

在IPv6网络中，LLA链路本地地址用于同一链路的相邻节点间通信，如单条链路上没有路由器时主机间的通信。链路本地地址可用于邻居发现，且总是自动配置的。地址冲突检测DAD（Duplicate address detect）是确定LLA地址是否可用的一种探测机制。具体执行过程如下：

1. 当一个节点配置了IPv6地址，为了查看该地址是否被其他邻居节点所使用，会即时发送邻居请求报文来确定其可用性。
2. 当其他邻居节点收到该报文后会查找本地的IPv6地址中是否存在相同的IPv6地址，若存在会回应一个邻居通告报文给源节点，并携带此IPv6地址信息。
3. 源节点收到邻居的回应报文则认为该IPv6地址已被邻居使用。反之，如果源节点发出的邻居请求报文没有收到相应的回应报文，则表示配置的IPv6地址是可用的。

邻居发现功能

邻居发现功能和IPv4中的ARP功能类似，主要实现对邻居地址的解析和邻居可达性的探测，依赖于邻居请求和邻居通告报文完成。

当一个节点需要得到同一本地链路上另外一个节点的链路层地址时，就会发送ICMPv6类型为135的邻居请求报文。此报文类似于IPv4中的ARP请求报文，不过使用组播地址而不使用广播地址，只有被请求节点的最后24比特和此组播地址相同的节点才会收到此报文，减少了广播风暴的可能。目的节点在响应报文中填充其链路层地址。

版权所有 © 华为技术有限公司

邻居请求报文也用来在邻居的链路层地址已知时，验证邻居的可达性。IPv6邻居通告报文是对IPv6邻居请求报文的响应。收到邻居请求报文后，目的节点通过在本地链路上发送ICMPv6类型为136的邻居通告报文进行响应。收到邻居通告后，源节点和目的节点可以进行通信。当一个节点的本地链路上的链路层地址改变时也会主动发送邻居通告报文。

路由器发现功能

路由器发现功能用来定位邻居路由设备，同时学习和地址自动配置有关的前缀和配置参数。IPv6路由发现由下面两种机制实现：

- 路由器请求

  当主机没有配置单播地址时（例如系统刚启动），就会发送路由器请求报文RS。路由器请求报文有助于主机迅速进行自动配置而不必等待IPv6路由设备的周期性路由器通告报文。IPv6路由器请求也是ICMPv6报文，类型为133。

- 路由器通告

  每个IPv6路由设备的接口在配置了IPv6 RA去抑制的前提下会周期发送路由器通告报文。在本地链路上收到IPv6节点的路由器请求报文后，路由设备也会回应路由器通告报文。IPv6路由器通告报文发送到所有节点多播地址（FF02::1）或发送路由器请求报文节点的IPv6单播地址。路由器通告为ICMPv6报文，类型为134，包含以下内容：

  - 是否使用地址自动配置
  - 标记支持的自动配置类型（无状态或有状态自动配置）
  - 一个或多个本地链路前缀（本地链路上的节点可以使用这些前缀完成地址自动配置）
  - 通告的本地链路前缀的生存期
  - 发送路由器通告的路由设备是否可作为缺省路由设备，如果可以，还包括此路由设备可作为缺省路由设备的时间（用秒表示）
  - 和主机相关的其它信息，如跳数限制、主机发起的报文可以使用的最大MTU

    本地链路上的IPv6节点接收路由器通告报文，并用其中的信息得到更新的缺省路由设备、前缀列表以及其它配置。

地址自动配置功能

通过使用路由器通告报文和针对每一前缀的标记，路由设备可以通知主机如何进行地址自动配置。例如，路由设备可以指定主机是使用有状态（DHCPv6）地址配置还是无状态地址自动配置进行地址配置。

对于无状态地址自动配置而言，当主机收到路由器通告报文后，使用其中的前缀信息和本地接口ID自动形成IPv6地址，同时还可以根据其中的默认路由设备信息设置默认路由设备。

重定向功能

重定向报文用来通知主机去往目的地的理想下一跳IPv6地址。和IPv4类似，IPv6路由设备发送重定向报文的目的仅限于把报文重新路由到更合适的路由设备。收到重定向报文的节点随后会把后续报文发送到更合适的路由设备。路由设备只针对单播流发送重定向报文，重定向报文只发送给引起重定向的报文的节点（主机），并被处理。

版权所有 © 华为技术有限公司

默认路由器优先级和路由信息

在邻居发现协议的RA报文中，定义了默认路由器优先级和路由信息两个字段，帮助主机在发送报文时选择合适的转发路由器。

当主机所在的链路中存在多个路由器时，主机需要根据报文的目的地址选择转发路由器。在这种情况下，路由器通过发布默认路由器优先级和特定路由信息给主机，提高主机根据不同的目的地选择合适的转发路由器的能力。

主机收到包含路由信息的RA报文后，会更新自己的路由表。当主机向其他设备发送报文时，通过查询该列表的路由信息，选择合适的路由发送报文。

主机收到包含默认路由器优先级信息的RA报文后，会更新自己的默认路由器列表。当主机向其他设备发送报文时，如果没有路由可选，则首先查询该列表，然后选择本链路内优先级最高的路由器发送报文；如果该路由器故障，主机根据优先级从高到低的顺序，依次选择其他路由器。

4.5.4 参考标准和协议

本特性的参考资料清单如下：

文档	描述
RFC1887	An Architecture for IPv6 Unicast Address Allocation
RFC1981	Path MTU Discovery for IP version 6
RFC2375	IPv6 Multicast Address Assignments
RFC2460	Version 6 of the Internet Protocol (IPv6)， also sometimes referred to as IP Next Generation or IPng
RFC2461/ RFC4861	Neighbor Discovery for IP Version 6 (IPv6)
RFC2462/ RFC4862	IPv6 Stateless Address Auto configuration
RFC2463/ RFC4443	Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification
RFC2464	Transmission of IPv6 Packets over Ethernet Networks
RFC2466	Management Information Base for IP Version 6 ICMPv6 Group
RFC2711	IPv6 Router Alert Option
RFC2893	Transition Mechanisms for IPv6 Hosts and Routers
RFC3315	DHCPv6 snooping
RFC3484	Default Address Selection for Internet Protocol Version 6 (IPv6)Section 2.1
RFC3493	Basic Socket Interface Extensions for IPv6

版权所有 © 华为技术有限公司

文档	描述
RFC3633	IPv6 Prefix Options for Dynamic Host Configuration Protocol(DHCP) version 6
RFC3736	Stateless Dynamic Host Configuration Protocol (DHCP) Service for IPv6
RFC3849	IPv6 Address Prefix Reserved for Documentation
RFC4001	Textual Conventions for Internet Network Addresses
RFC4007	IPv6 Scoped Address Architecture
RFC4191	Default Router Preferences and More-Specific Routes
RFC4193	Unique Local IPv6 Unicast Addresses
RFC4213	Basic Transition Mechanisms for IPv6 Hosts and Routers
RFC4214	Intra-Site Automatic Tunnel Addressing Protocol(ISATAP)
RFC4429	Duplicate Address Detection
RFC4282	A Model of IPv6/IPv4 Dual Stack Internet Access Service
RFC2373/ RFC3513/ RFC4291	Internet Protocol Version 6 (IPv6) Addressing Architecture
RFC4862/ RFC5006	Router Advertisement (RA) filtering
RFC6221	DHCPv6 LDRA

4.6 组网保护

介绍系统实现的各种组网保护特性的功能。

4.6.1 Ring check

Ring check主要用于检测用户侧、网络侧的环网，并消除用户侧的环网。

4.6.1.1 介绍

定义

Ring check特性是通过设备周期性发送Ring check报文，监控用户侧、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，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，使合法用户不被干扰。

目的

Ring check用于快速定位用户侧、网络侧环网，并根据需要消除用户侧环网。

版权所有 © 华为技术有限公司

- 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

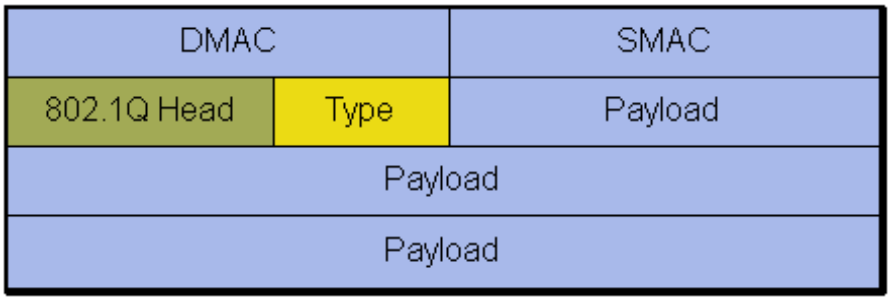
Ring check特性通过去激活环路端口，保证合法用户不被干扰，获得良好的网络服务。

4.6.1.2 原理描述

Ring check 报文格式

环网检测是通过设备在用户侧、网络侧周期性发送Ring check报文，监控用户侧、网络侧收到的Ring check报文来检测运营商网络是否形成环路。其报文格式如图4-82所示。

图 4-82 Ring check 报文格式



- DMAC为广播MAC 地址，值为ff-ff-ff-ff-ff-ff，SMAC为发送设备的桥MAC地址。
- 802.1Q Head根据用户侧流属性，自动选择是否填写。
- Type为私有以太网类型，可配置。
- 报文内容Payload为私有，无需配置。

实现原理

当用户侧、网络侧环网检测功能打开后，定时向用户侧、网络侧发送私有的Ring check报文，用户侧、网络侧同时捕获环网检测报文。

- 对于从网络侧捕获到本设备用户侧、网络侧发送的环网检测报文，则上报告警给网络管理系统。
- 对于从用户侧捕获到用户侧、网络侧发送的环网检测报文，上报告警给网络管理系统，并将收到该报文的端口去激活，实现环网消除。

版权所有 © 华为技术有限公司

说明

系统故障排除后，端口需要一定时间才能自动激活。若希望端口能快速激活，建议采用先手动去激活端口，再激活端口的方式。

- 环网检测每秒最多可以检测12条状态UP的业务流。假设系统中存在8000条状态UP的业务流，那么如果有环网产生，最多需要过8000/12=666.67秒后才能检测出来。

4.7 系统安全

首先介绍防止恶意用户对系统攻击的解决方案，然后分别阐述各子特性。

4.7.1 防御用户侧 IP/ICMP 攻击

接入设备能够识别并丢弃终端用户发送的目的IP地址为系统IP地址（包含设备管理IP地址和三层Vlanif接口IP地址等其他地址）的IP报文或ICMP（Internet Control Message Protocol）报文，防御用户侧发起的IP/ICMP攻击。

4.7.1.1 什么是用户侧 IP/ICMP 攻击

用户侧 IP 攻击

正常用户发送的报文，一般目的IP地址不会是接入设备的管理IP地址（部分运营商特殊规划除外）。恶意用户伪造目的IP地址为管理IP地址的IP报文，对接入设备发起攻击。常见的IP攻击的方式是：恶意用户在短时间内发送大量报文向接入设备请求回应，试图让接入系统由于负担过重而不能处理合法的任务。IP攻击也可认为是DoS攻击的一种。

通过识别和丢弃用户端口收到的目的IP地址为管理IP地址的IP报文，可以防御恶意用户发起的IP攻击，简称防IP攻击。

用户侧 ICMP 攻击

ICMP（Internet Control Message Protocol）是TCP/IP协议族的一个子协议，用于在IP主机、路由器之间传递控制消息（例如PING、trace route）。在定位故障时，可以从对端设备向接入设备发送ICMP报文来检测网络的连通性、路由是否可达等。

一般情况下，只需要让上级设备和级联设备PING接入设备，不需要让用户终端PING接入设备，避免恶意用户PING通并发现接入设备，进而发起攻击。

通过识别和丢弃用户端口收到的目的IP地址为管理IP地址的ICMP报文，可以防御恶意用户发起的ICMP攻击，简称防ICMP攻击。

4.7.1.2 防御用户侧 IP/ICMP 攻击实现原理

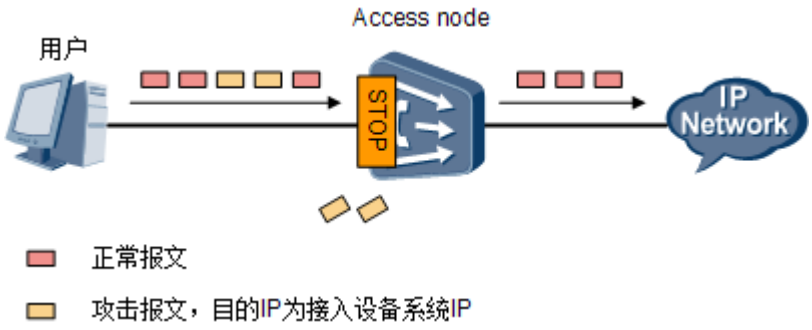
接入设备可以识别并丢弃目的IP为系统IP地址的IP报文、ICMP报文，防御用户发起的IP/ICMP攻击，原理如图4-83所示。

说明

系统IP地址指目的IP地址是接入设备IP地址（配置的三层Vlanif接口的IP地址）。

版权所有 © 华为技术有限公司

图 4-83 防 IP/ICMP 攻击示意图



如上图所示，接入设备可实现：

- 正常报文被转发。
- 目的IP地址为接入设备系统IP地址的攻击报文被丢弃。

4.7.2 源路由过滤

源路由过滤特性通过识别并丢弃带源路由选项的IP报文，防止恶意用户利用源路由选项的原理对网络进行攻击。

4.7.2.1 为什么引入源路由过滤

源路由过滤特性是为了解决源路由选项带来的问题。因此要理解源路由过滤特性，首先得了解源路由选项。

什么是源路由选项

IPv4网络的IP报头中定义了两个选项用于指定发送报文的路由：严格源路由选项、松散源路由选项。

- 当包含严格源路由选项时，报文必须严格按照选项指定的路由器按顺序逐跳转发。
- 当包含松散源路由选项时，报文必须经过选项指定的路由器按顺序转发，但指定的路由器之间可以经过其他的路由器。

源路由选项的作用

通过在报文中加入源路由选项，用户可以指定他所发送的数据包沿途经过的部分或者全部路由器，有选择性地将数据包发往不同目的地址。可用于测试某特定网络的吞吐率、也可以在指定信任的网络中传输数据。例如：让一个IP报文明确的经过三台路由器R1、R2、R3，则可以在严格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。

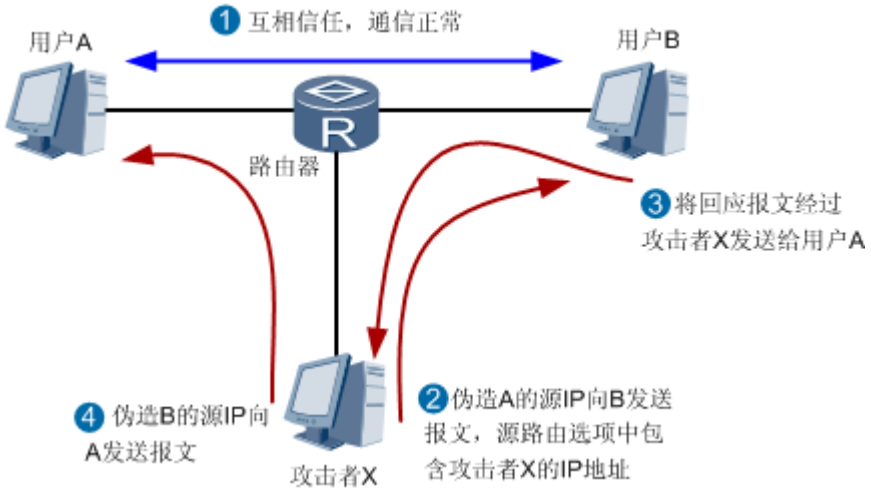
当对端设备接收到包含源路由选项的报文时，一般会在回应报文中也包含对应的源路由选项。回应报文源路由选项中的路由器顺序是反过来的，这样回应报文会沿着同样的转发路径转发回来。

版权所有 © 华为技术有限公司

源路由选项带来的问题

在安全的网络中，用户可以通过源路由选项指定报文的转发路径，对数据流向进行管理。但是在不安全的网络中，源路由选项给恶意用户提供了攻击网络、窃取他人通信数据的可能性。过程如图4-84所示。

图 4-84 利用源路由选项原理发起攻击



1. 用户A和用户B相互信任，正常通信。
2. 攻击者X向用户B发送含有源路由选项的报文。其中，源IP伪造成用户A的源IP，源路由选项中包含攻击者X的IP地址。
3. 用户B收到攻击者X发送的报文之后，从源IP判断该报文是用户A发送的。用户B按照接收报文的源路由选项，将回应报文经过攻击者X发送给用户A。
4. 攻击者X收到用户B的报文后，伪造成用户B的源IP对用户A发送报文。同时，攻击者X还可以通过修改源路由选项让该报文通过指定的路径转发给用户A，以掩盖攻击者X的真正位置。

解决办法

恶意用户在进行网络攻击时，一般把源路由选项作为IP地址欺骗的辅助手段使用，接入设备可通过以下方式防御。

- 源路由过滤：把用户发送的IP报文中含有源路由选项字段的报文过滤掉。
- 防御IP地址欺骗：防止恶意用户伪造合法用户的IP地址。

4.8 应用安全

本章包含接入设备支持的所有应用安全特性。某些应用安全特性和命令可能在部分产品型号不支持，详细支持情况请参考“特性规格”。

4.8.1 802.1X 认证

IEEE 802.1X标准是一种基于端口的网络接入控制协议。

版权所有 © 华为技术有限公司

4.8.1.1 介绍

定义

IEEE 802.1X标准（以下简称802.1X）是一种基于端口的网络接入控制（Port Based Network Access Control）协议。“基于端口的网络接入控制”是指在局域网接入设备的端口这一级对所接入的用户设备进行认证和控制。连接在端口上的用户设备如果能通过认证，就可以访问局域网中的资源；如果不能通过认证，则无法访问局域网中的资源。

4.8.1.2 基本概念

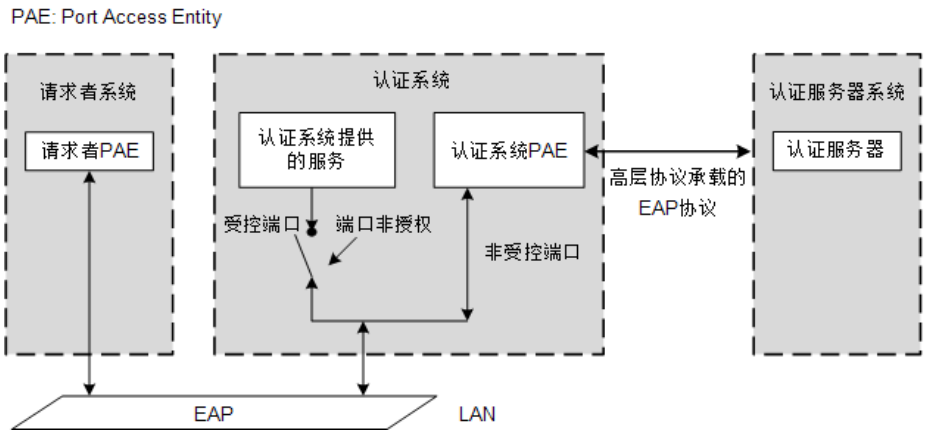
802.1X 的体系结构

802.1X对基于端口的网络接入控制进行了定义，其主要思路是：

- 接入设备提供对接入端口（物理端口或逻辑端口）进行认证控制的功能。
- 在端口通过认证之前，端口处于关闭状态，连接在该端口上的用户无法获取网络资源。
- 如果用户能够通过认证，则端口打开，用户可以正常访问网络。

802.1X系统定义了三个功能实体：请求者系统、认证系统和认证服务器系统。802.1X体系结构如图4-85所示。

图 4-85 802.1X 体系结构图



- 请求者系统：一般为一个用户终端系统，该终端系统通常要安装一个802.1X客户端软件，用户通过启动这个客户端软件发起802.1X协议的认证过程。为支持基于端口的接入控制，客户端系统需支持EAPoL（Extensible Authentication Protocol Over LAN）协议。
- 认证系统：一般为支持802.1X协议的网络设备，如OLT设备，该设备对应于不同用户的端口（可以是物理端口，也可以是逻辑端口，如用户MAC、VLAN、IP等）。物理端口分为2种类型：受控端口（Controlled Port）和非受控端口（Uncontrolled Port）。非受控端口始终处于双向连通状态，不需要进行认证。受控端口存在2种状态：非授权状态（unauthorized）和授权状态（authorized）。受控端口的状态决定了客户端是否能接入网络，端口初始状态一般为非授权，在该状态下，除802.1X报文和DHCP广播报文外，不允许任何业务流通过该端口。当客户端通过认证，则端口状态切换到授权状态，允许客户端通

版权所有 © 华为技术有限公司

过该端口进行正常通讯。受控端口可配置为双向受控、仅输入受控两种方式，以适应不同的应用环境。

- 认证服务器：通常为RADIUS服务器，该服务器可以存储有关用户的信息，比如用户名、密码等。当用户通过认证后，认证服务器会把用户的相关认证信息传递给认证系统，由认证系统构建动态的访问控制列表。认证系统和认证服务器之间通过RADIUS协议进行通信。

4.8.1.3 802.1X 认证实现原理

认证方式

POL设备运行802.1X协议，担任认证者角色，接收用户的认证请求，并将用户的认证信息发送给RADIUS服务器进行认证，如果RADIUS服务器认证通过，则打开认证端口。

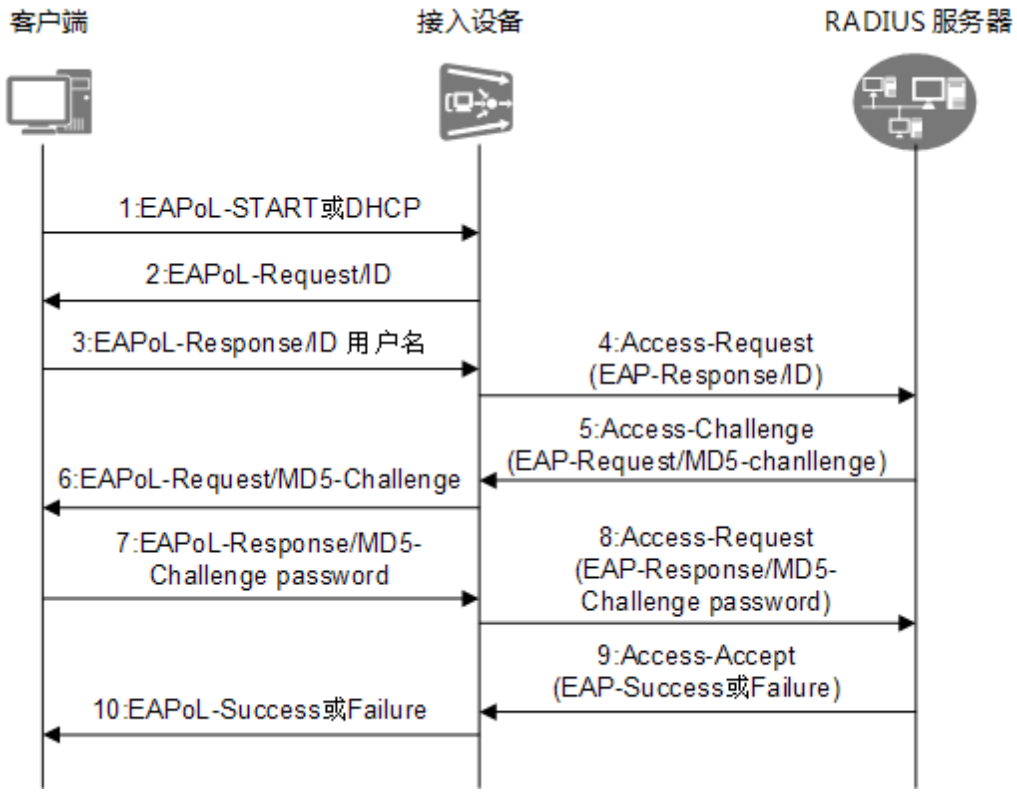
POL设备支持802.1X远程认证，远程认证包括远端终结认证和远端中继认证两种方式:

- 远端中继认证：ONU设备则将EAP报文封装到RADIUS协议相应的属性中，发送到RADIUS服务器认证，这种方式下RADIUS服务器需要处理EAP报文。
- 远端终结认证：ONU设备从EAP报文中提取用户的认证消息，封装到RADIUS协议相应的属性中，发送到RADIUS服务器认证。

认证过程

- 以认证服务器为Radius服务器为例，EAP远端中继认证过程如图4-86所示。此处的接入设备指ONU。

图 4-86 EAP 远端中继认证过程



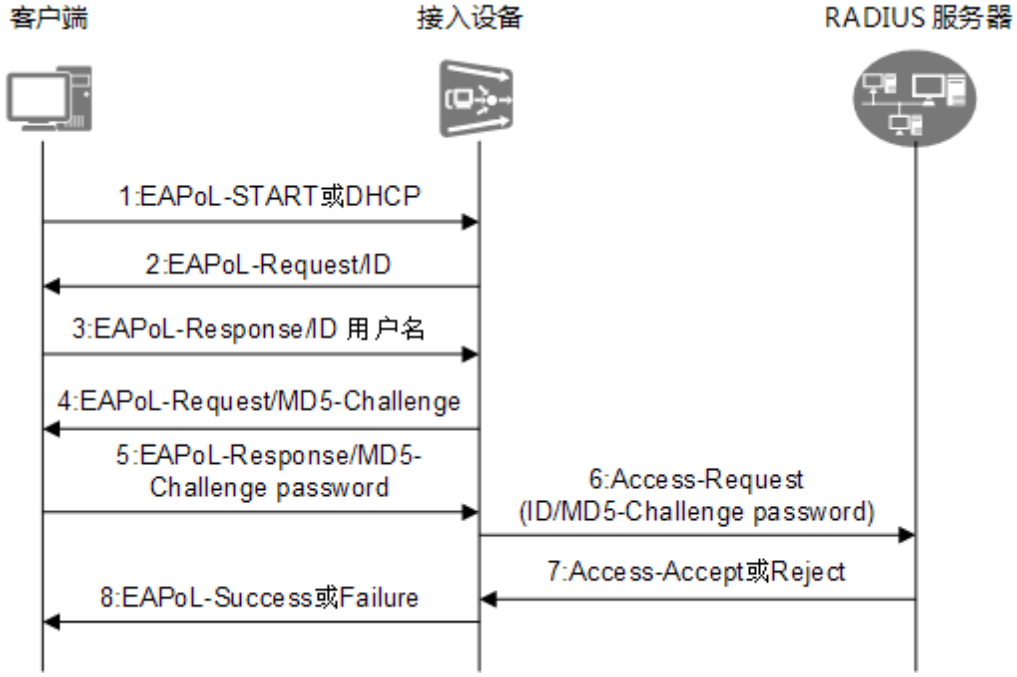
版权所有 © 华为技术有限公司

a. 用户有上网需求时打开802.1X客户端，输入用户名和口令，发起连接请求EAPoL-Start，开始启动一次认证过程。
b. 接入设备收到请求认证报文EAPoL-Start后，发出一个请求报文EAPoL-Request/Identity，要求客户端发送用户输入的用户名信息。
c. 客户端将用户名信息通过报文EAPoL-Response/Identity发送给接入设备。
d. 接入设备收到客户端送上来的报文EAP-Response/Identity后，将EAP-Response/Identity封装到RADIUS报文中（RADIUS Access-Request报文），发送给RADIUS Server处理。
e. RADIUS服务器收到RADIUS Access-Request 报文后，解析出包含有用户信息的EAPoL-Response/Identity报文，随机生成一个加密字并生成携带此加密字的报文EAP-Request/MD5-Challenge，然后将该报文封装在RADIUS报文中发送给接入设备。
f. 接入设备从RADIUS报文中解析出EAPoL-Request/MD5-Challenge，然后发送给客户端。
g. 客户端收到加密字EAPoL-Request/MD5-Challenge报文后，用该加密字对口令进行加密处理，生成EAPoL-Response/MD5-Challenge password报文发送给接入设备。
h. 接入设备收到加密口令EAP-Response/MD5-Challenge password报文后，将EAP-Response/MD5-Challenge password封装到RADIUS报文中（RADIUS Access-Request报文），发送给RADIUS Server处理。
i. Radius服务器收到RADIUS Access-Request报文后，解析出包含有加密口令的EAPoL-Response/MD5-Challenge password，根据用户名信息在数据库中查找对应的口令信息，用加密字对口令信息进行加密处理得到自己的加密口令，和收到的加密口令信息进行对比，根据认证结果的不同生成EAP-Success或Failure，然后封装到RADIUS Access-Accept报文中，发送给接入设备。
j. 接入设备从RADIUS报文中解析出EAP-Success或Failure，然后发送给客户端。同时，根据认证结果进行端口授权状态的修改。
k. 接入设备定期与客户端交互握手报文，检测用户是否意外下线。
l. 客户端可以发送EAPoL-Logoff报文给接入设备，主动终止已认证状态，接入设备将端口状态从授权状态变成未授权状态。

- EAP远端终结认证过程如**图4-87**所示。

 版权所有 © 华为技术有限公司

图 4-87 EAP 远端终结认证过程



a. 用户有上网需求时打开802.1X客户端，输入用户名和口令，发起连接请求EAPoL-Start报文，开始启动一次认证过程。

b. 接入设备收到请求认证EAPoL-Start后，发出一个请求报文EAPoL-Request/Identity，要求客户端发送用户输入的用户名信息。

c. 客户端将用户名信息通过报文EAPoL-Response/Identity送给接入设备。

d. 接入设备收到客户端送上来的EAPoL-Response/Identity报文后，随机生成一个加密字，并将此加密字通过报文EAPoL-Request/MD5-Challenge交给客户端。

e. 客户端收到加密字EAPoL-Request/MD5-Challenge报文后，用该加密字对口令进行加密处理，生成EAPoL-Response/MD5-Challenge password报文送给接入设备。

f. 接入设备收到加密口令EAPoL-Response/MD5-Challenge password后，对用户名、加密口令、加密字等认证信息重新封装成标准的Radius报文（RADIUS Access-Requeset报文），送给Radius服务器进行处理。

g. Radius服务器收到认证信息（RADIUS Access-Requeset报文）后，根据收到的用户名信息在数据库中查找对应的口令信息，用收到的加密字对口令信息进行加密处理得到自己的加密口令。然后和收到的加密口令信息进行对比，根据认证结果的不同生成RADIUS Access-Accept或Reject报文，发送给接入设备

h. 接入设备根据收到的RADIUS Access-Accept或Reject报文，生成EAP-Success或Failure报文发送给客户端。同时，根据认证结果进行端口授权状态的修改。

i. 接入设备定期与客户端交互握手报文，检测用户是否意外下线。

j. 客户端可以发送EAPoL-Logoff报文给接入设备，主动终止已认证状态，接入设备将端口状态从授权状态变成未授权状态。

版权所有 © 华为技术有限公司

4.8.1.4 802.1X 在 POL 上的应用

802.1X 认证

POL设备在基于802.1X基本的认证方式上，考虑不同应用场景，通过配置多种VLAN为客户提供差异化的接入方式。

支持802.1X认证的基本VLAN包括：

- GuestVLAN：当端口802.1X功能开启，但还未启动认证时，端口的所有业务都使用GuestVLAN。此VLAN主要应用于部分终端没有802.1X终端软件，需要通过GuestVLAN来下载802.1X拨号软件或者访问受限的WEB页面。
- RestrictVLAN：当端口802.1X功能开启，而且端口已启动802.1X认证，但认证被服务器Reject后，此端口下的所有业务都走RestrictVLAN。用户认证失败，只能受限访问指定的资源。

在POL（Passive Optical LAN）场景下，考虑用户迁移——如移动办公、酒店等用户应用，通过配置DynamicServiceVLAN及CriticalVLAN为移动或临时客户接入设备设计了更为灵活的访问策略，极大提升了网络的容错性及灵活性。

- DynamicServiceVLAN：动态的业务VLAN。当端口802.1X功能开启并认证通过，Radius协议通过指定的属性字段给用户分配的动态业务VLAN。端口下的所有业务都走Radius服务器分配的动态业务VLAN。
- CriticalVLAN：紧急VLAN。当端口802.1X功能开启，但进行认证时发现Radius服务器无法连接上（路由不可达或者连接超时）时，端口下所有业务使用CriticalVLAN。

802.1X只支持EAP触发，支持远程终结认证和远程中继认证两种认证方式。

802.1X支持VOICE VLAN用户不认证。

MAC 旁路认证（MAB：MAC-Bypass）

在某些802.1X进行网络访问控制的组网下，存在一些不支持802.1X的终端，比如打印机、网络摄像头等设备。这些设备无法安装802.1X客户端，无法进行802.1X认证，需要MAC旁路认证来适应这些终端的访问要求。

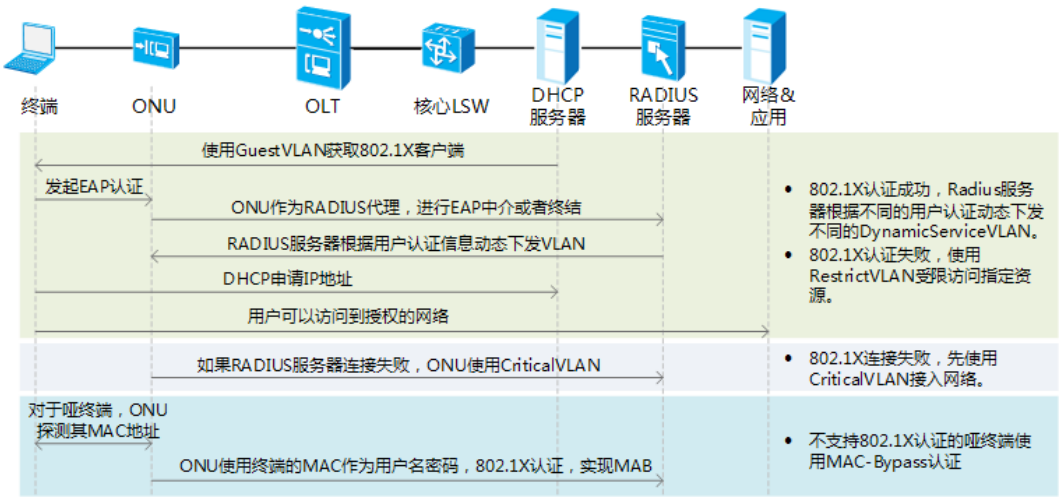
设备开启MAC旁路认证后，对端口下学习到的MAC地址直接进行MAC认证，将用户MAC地址作为用户名、密码，通过RADIUS协议到RADIUS服务器认证，认证成功后，直接开启端口的802.1X状态。

MAB是802.1X的补充，同样基于端口配置，支持DHCP和ARP触发，且只支持远程终结认证方式。MAB开关与802.1X端口级开关的关系为：开启了802.1X开关，同时开启MAB，则端口优先进行802.1X认证，超时后才进行MAB认证；当关闭802.1X开关，但开启MAB时，则无需等802.1x认证超时即进行MAC认证；关闭MAB开关，不影响802.1X开关状态。

POL场景下典型的组网如**图4-88**所示。

版权所有 © 华为技术有限公司

图 4-88 802.1X 认证 POL 场景组网图



4.8.2 DHCP Option82

本章从特性介绍、原理描述方面对DHCP option 82进行描述。

4.8.2.1 什么是 DHCP Option82

定义

DHCP Option82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。

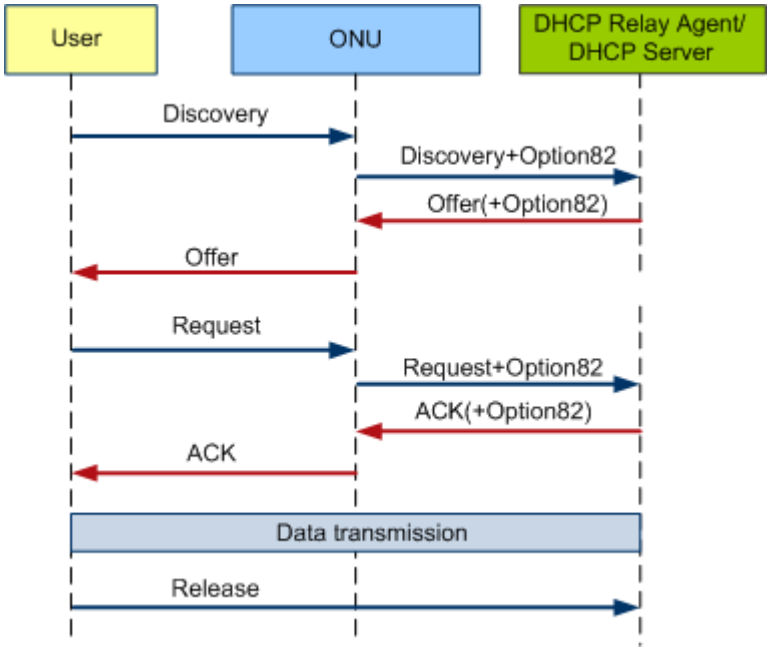
4.8.2.2 DHCP Option82 的报文格式与交互过程

基本原理

DHCP Option82功能启动时，DHCP过程如图4-89所示。

版权所有 © 华为技术有限公司

图 4-89 开启 Option82 功能的 DHCP 过程



在用户请求配置阶段，ONU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。

使能DHCP Option82后，接入设备会修改用户发送的DHCP报文的XID，使得DHCP client发送的DHCP报文中的XID与DHCP server接收到的DHCP报文中的XID不同。通常情况下，DHCP server不校验XID，因此不会影响业务。如果运营商超出协议范围在DHCP client发送报文的XID中嵌入信息用于DHCP server校验，则可能导致校验失败，影响业务。

说明

XID是协议定义的DHCP报文字段，相当于DHCP报文的编号。

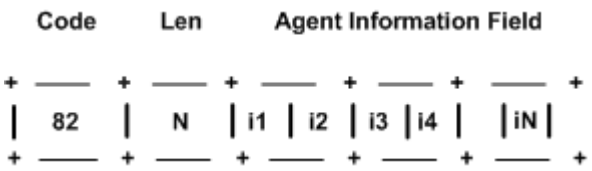
DHCP Option82 报文格式

对于DHCP Option82特性，仅需要关注DHCP报文中的Option82字段，本文仅对Option82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4-90所示。

图 4-90 DHCP Option82 字段报文格式



版权所有 © 华为技术有限公司

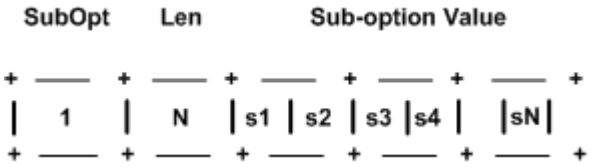
DHCP Option82报文各字段具体含义，如表4-22所示。

表 4-22 DHCP Option82 报文字段含义

字段	含义
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4-91所示。

图 4-91 DHCP Option82 sub-option 格式



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

为了满足不同客户的需求，设备支持不同Option82的信息格式。

4.8.3 PITP

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

4.8.3.1 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。

版权所有 © 华为技术有限公司

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。

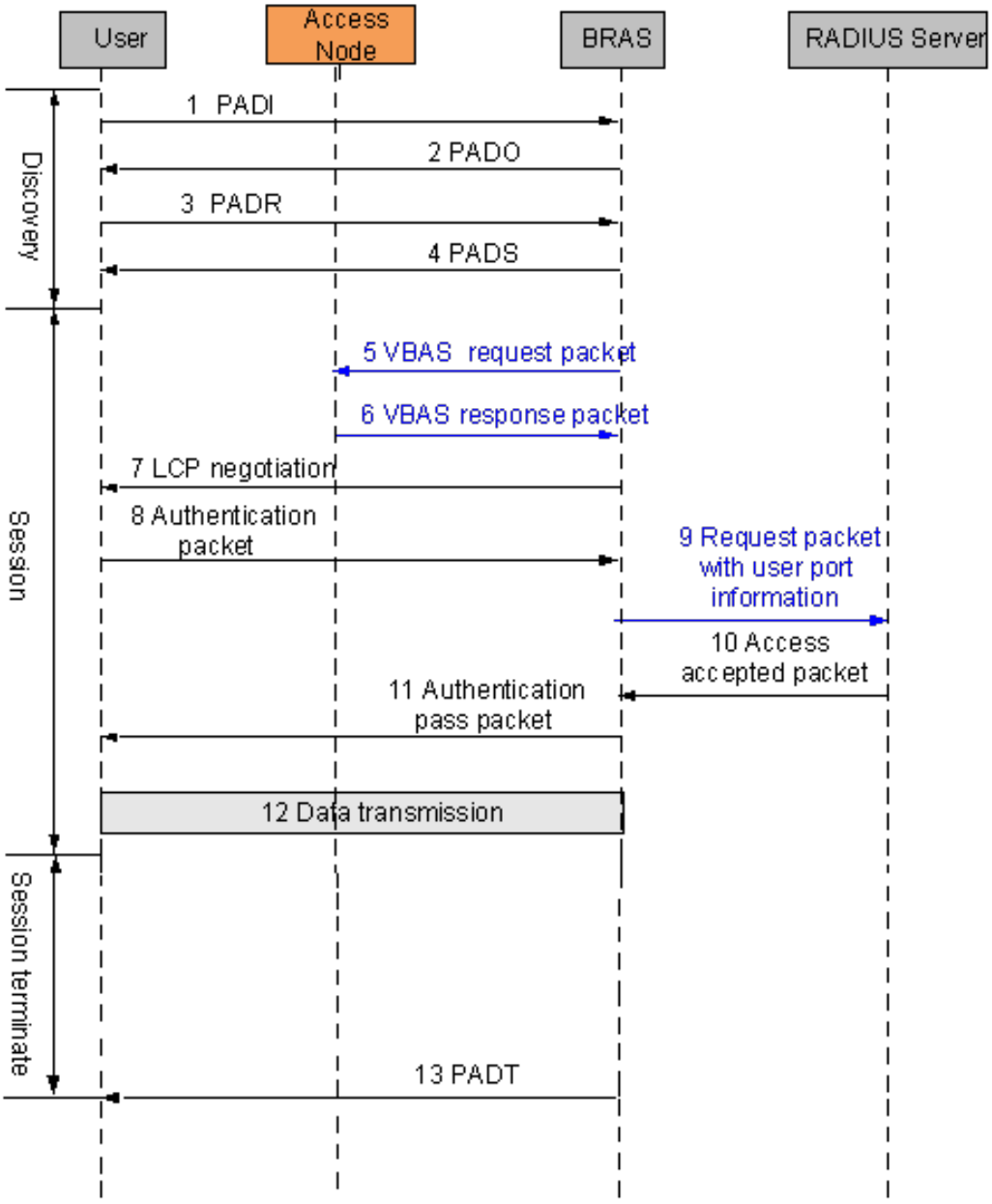
用户受益：PITP通过用户物理信息与用户帐号绑定认证，避免用户帐号密码被盗。

4.8.3.2 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4-92所示。

图 4-92 启动 V 模式功能的 PPPoE 拨号过程



版权所有 © 华为技术有限公司

说明

- PADI：PPPoE Active Discovery Initiation，发现阶段初始化报文。
- PADO：PPPoE Active Discovery Offer，发现阶段响应报文。
- PADR：PPPoE Active Discovery Request，发现阶段请求报文。
- PADS：PPPoE Active Discovery session-confirmation，发现阶段会话确认报文。
- PADT：PPPoE Active Discovery Terminate，发现阶段会话终止报文。

PITP V模式（又称为VBAS方式）是指在接入用户与BRAS设备进行PPPoE协商的过程中，BRAS设备主动向ONU发送VBAS请求报文，要求ONU上报接入用户的物理端口信息。ONU通过VBAS响应报文，将端口信息发送给BRAS设备。

PITP V模式认证分为三个阶段，发现阶段（Discovery）、会话阶段（Session）和会话中断阶段（Session terminate）。

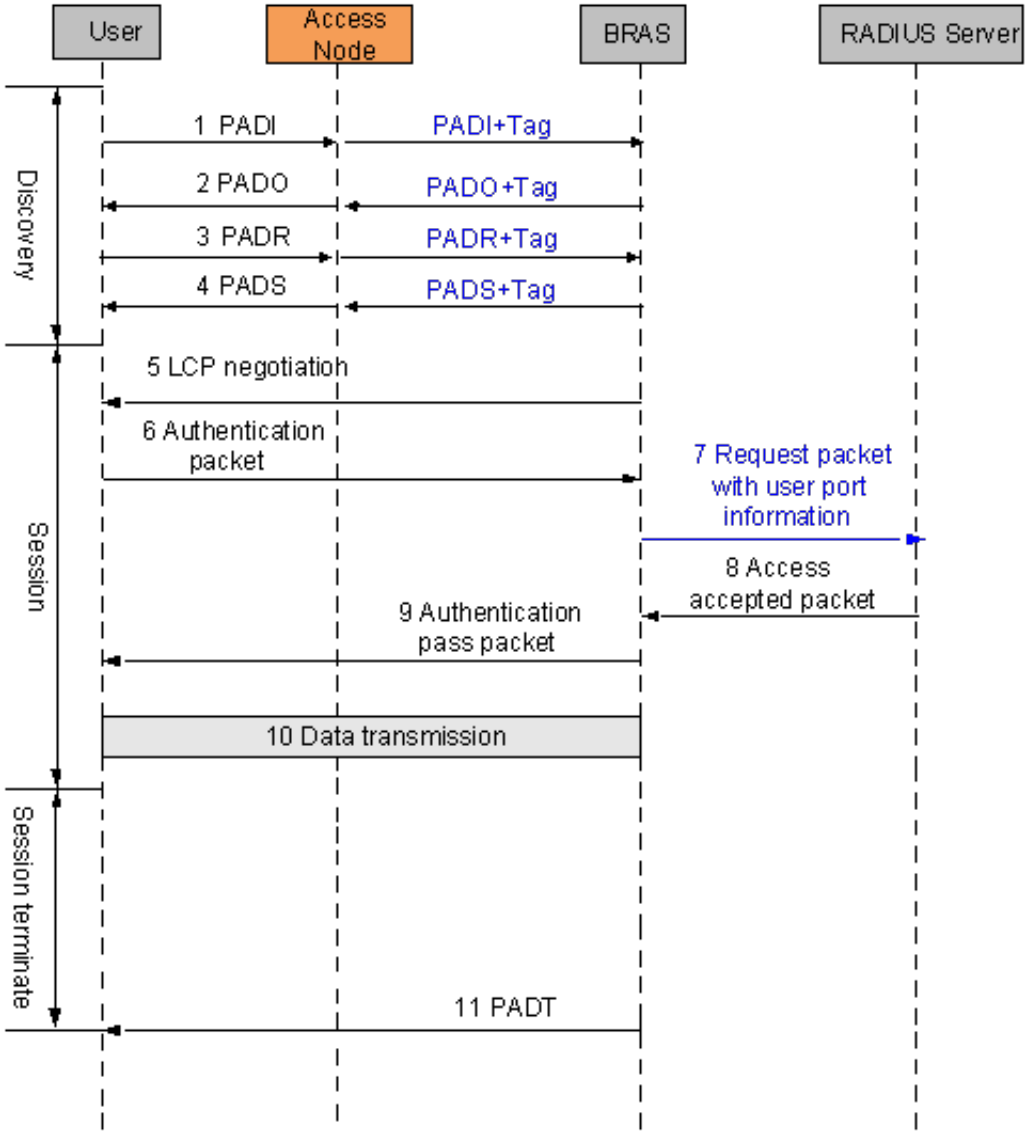
- 发现阶段：带有VBAS功能时，在PPPoE发现阶段的处理并没有什么不同。PPPoE发现阶段结束时，BRAS设备向ONU发送VBAS请求报文。ONU根据VBAS请求查询端口物理信息，并通过VBAS响应报文发送给BRAS设备。BRAS设备解析VBAS响应报文，获取到接入端口的物理信息。
- 会话阶段：当BRAS设备向RADIUS Server发起接入请求包时，就可以将其掌握的端口物理信息同用户的帐号密码一并提供给RADIUS Server。RADIUS Server可以通过这些信息共同决定是否接收接入请求。如果帐号和端口物理信息匹配的话，则允许接入，否则拒绝接入，认证通过后开始数据传输。
- 会话中断阶段：PADT报文主要是用来终止一个PPPoE会话，可以在会话开始之后的任意时间内发送。它可以由BRAS或用户发起，ONU上不添加Tag信息到PADT报文。

P 模式实现原理

启动PITP P模式后，PPPoE拨号过程如图4-93所示。

版权所有 © 华为技术有限公司

图 4-93 启动 P 模式功能的 PPPoE 拨号过程



PITP P模式（又称为PPPoE+模式）。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。

PITP P模式认证分为三个阶段，发现阶段（Discovery）、会话阶段（Session）和会话中断阶段（Session terminate）。

- 发现阶段：在PPPoE发现阶段，ONU在上行的PADI和PADR报文中添加Vendor TAG，并剥离下行PADO和PADS报文中的Vendor TAG。BRAS设备收到的PPPoE发现阶段报文是带有Vendor TAG的，通过解析Vendor TAG的内容，就可以获取到接入端口的物理信息。
- 会话阶段：当BRAS设备向RADIUS Server发起接入请求包时，就可以将其掌握的端口物理信息同用户的帐号密码一并提供给RADIUS Server。RADIUS Server可以通过这些信息共同决定是否接收接入请求。如果帐号和端口物理信息匹配的话，则允许接入，否则拒绝接入，认证通过后开始数据传输。

版权所有 © 华为技术有限公司

- 会话中断阶段：PADT报文主要是用来终止一个PPPoE会话，可以在会话开始之后的任意时间内发送。它可以由BRAS或用户发起，ONU上不添加Tag信息到PADT报文。

4.9 MAC 地址安全防护手段

针对恶意用户通过伪造MAC地址来试图干扰网络通信的问题，接入设备提供了多种防护手段。合理利用这些手段，可以在不同场景下防御恶意用户对MAC地址发起的攻击。

不同产品型号支持的防护手段有区别，具体请参考“特性规格”。

4.9.1 MAC 地址安全问题

当接入设备工作在VLAN+MAC转发模式下时，常见的MAC地址安全问题包括三种：仿冒用户MAC地址、仿冒网络设备MAC地址、MAC地址表耗尽。

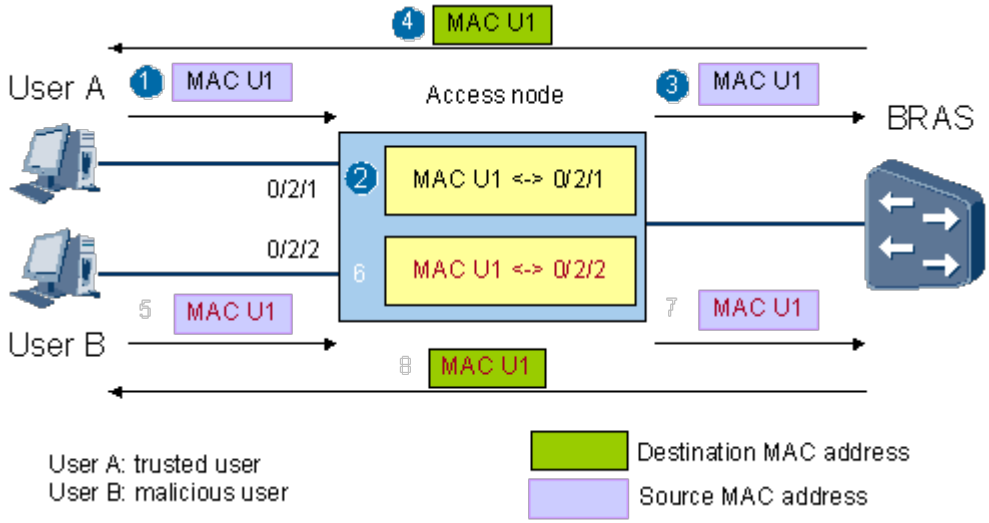
接入设备支持多种转发模式。当接入设备工作在VLAN+MAC转发模式下时（即VLAN转发模式为vlan-mac模式），报文根据VLAN和MAC地址表项进行转发。VLAN只能由手工配置生成，一般不容易被恶意用户篡改。设备的MAC地址表项既可以由手工配置（即静态MAC地址表项），也可以由设备学习生成（即动态MAC地址表项）。手工配置的静态MAC地址表项一般不容易被恶意用户篡改，因此设备学习的动态MAC地址表项就成为恶意用户攻击的主要对象。在VLAN+MAC转发模式下，恶意用户最常见的一种攻击手段就是利用接入设备的动态MAC地址学习机制，仿冒正常用户或网络设备的源MAC地址对设备的MAC地址表项发起攻击，试图干扰正常的网络通信。常见的MAC地址安全问题包括以下三种：

- 仿冒用户MAC地址
- 仿冒网络设备MAC地址
- MAC地址表耗尽

仿冒用户 MAC 地址

恶意用户通过仿冒正常用户的源MAC地址接入到网络中，占用正常用户的网络资源，导致正常用户网络中断。以PPPoE拨号上网为例，原理如图4-94所示。

图 4-94 仿冒用户 MAC 地址



版权所有 © 华为技术有限公司

1. 正常用户User A发送PPPoE拨号报文，源MAC地址为MAC U1。
2. 接入设备从User A发送的报文中，学习到源MAC地址与端口的对应关系（MAC U1 <-> 0/2/1），记录在MAC地址表中。
3. 接入设备将User A的拨号报文转发给BRAS。
4. BRAS认证通过后，接入设备按照MAC地址表中的对应关系（MAC U1 <-> 0/2/1），将BRAS发送的目的MAC地址为MAC U1的报文从0/2/1端口转发给User A。User A正常通信。
5. 恶意用户User B发送PPPoE拨号报文，源MAC地址仿冒成User A的源MAC地址（即MAC U1）。
6. 接入设备从User B发送的报文中，学习到源MAC地址与端口的对应关系（MAC U1 <-> 0/2/2），刷新MAC地址表中MAC U1对应的表项。这时，系统MAC地址表中MAC U1从0/2/1端口迁移到0/2/2端口。
7. 接入设备将User B仿冒的拨号报文转发给BRAS。
8. BRAS认证通过后，接入设备按照MAC地址表中的对应关系（MAC U1 <-> 0/2/2），将BRAS发送的目的MAC地址为MAC U1的报文通过0/2/2端口转发给User B。

User B仿冒User A的源MAC地址进行通信，占用User A的通信资源，导致User A的通信被中断。原本发送给User A的报文被转发给User B，User B窃取User A的通信数据。

仿冒网络设备 MAC 地址

恶意用户通过仿冒接入网上层设备的MAC地址，试图窃取所有转发至该上层设备的通信数据。原理如下：

1. 恶意用户发送源MAC地址为接入网上层设备MAC地址的报文。
2. 接入设备在收到恶意用户仿冒的报文后，按照MAC地址动态学习机制刷新MAC地址表。系统MAC地址表中上层设备MAC地址从上行端口迁移到恶意用户所在的用户端口。
3. 接入设备将其他用户发送给上层设备的报文转发到恶意用户所在端口。

在未使能二层互通的情况下，用户端口间是二层隔离的，不能进行二层转发。因此，其他用户发往该上层设备的报文会被丢弃，导致通信中断。

MAC 地址表耗尽

恶意用户通过仿冒大量不同源MAC地址报文，对接入设备进行攻击，干扰网络通信。原理如下：

1. 恶意用户仿冒大量不同源MAC地址报文。
2. 接入设备从恶意用户发送的报文中学习到大量的垃圾表项，消耗系统MAC地址表资源。
3. MAC地址表资源被耗尽后，接入设备无法学习新的MAC地址，导致其他用户的正常通信报文只能作为未知单播报文处理。
4. 根据未知单播转发策略，用户报文被广播或丢弃。
   - 当设备使能未知单播抑制时，报文被丢弃，导致部分用户无法上网。
   - 当设备未使能未知单播抑制时，报文被广播，导致消耗大量转发带宽，影响通信质量。

版权所有 © 华为技术有限公司

4.9.2 静态 MAC 地址过滤

为了防止用户仿冒接入网上层网络设备的MAC地址，或者一些知名的MAC地址，可以将这些MAC地址配置为要过滤的MAC地址，禁止带有这些源MAC地址或目的MAC地址的报文通过设备。静态MAC地址过滤分为静态源MAC地址过滤和静态目的MAC地址过滤。

静态源 MAC 地址过滤

通过将上层设备的MAC地址手工添加到接入设备的静态源MAC地址过滤表项，可以保护该上层设备的MAC地址不能被用户作为发送报文的源MAC地址，防御恶意用户发起的仿冒上层设备MAC地址的攻击。当用户的IP地址通过手工静态配置，而非动态获取时，最常用的一种防御仿冒网络设备MAC地址的方式就是静态源MAC地址过滤。

源MAC地址过滤的基本原理是：在设备中建立源MAC地址过滤表项，丢弃用户端口收到的源MAC地址为该表项中的所有报文。静态源MAC地址过滤就是把上层设备的源MAC地址通过手工配置方式，增加到源MAC地址过滤表项中。

通过配置上行端口的静态MAC地址也可以防御仿冒网络设备MAC地址。与配置上行端口的静态MAC地址相比，静态源MAC地址过滤的优缺点如下。

- 与静态MAC地址相比，静态源MAC地址过滤不能指定对应的业务流和端口。这既是优点又是缺点。
  - 优点：配置之前不需要知道上级设备与上行端口的对应关系，减少了配置工作量。配置之后上级设备与上行端口的对应关系可以灵活变化。
  - 缺点：静态源MAC地址过滤只能限制用户不能使用上级设备的MAC地址作为发送报文的源MAC地址，但一个上行端口的上级设备却可以使用另一个上行端口的上级设备的MAC地址作为发送报文的源MAC地址，保护能力略微弱一点。不过通常情况下，上行端口是可信任的，这个缺点影响不大。
- 与静态MAC地址相比，接入设备支持的静态源MAC地址过滤数量要少得多。不过一般来说上级设备的数量不多，所以上级设备的MAC地址数量也不多，这个缺点影响也不大。
- 与静态MAC地址相比，静态源MAC地址过滤是全局生效，不能基于VLAN配置是否进行源MAC地址过滤。

综合上面的优缺点，静态源MAC地址过滤比静态MAC地址更适用于防御仿冒网络设备MAC地址。

静态目的 MAC 地址过滤

通过将接入网上层设备的MAC手工配置为目的MAC地址过滤，可以保护该上层设备的MAC地址不能被用户作为发送报文的目的MAC地址，避免恶意用户发送单播报文访问上层设备。

4.9.3 防御 MAC 地址漂移

MAC地址漂移是指：某个端口的源MAC地址老化之前，设备从另一个端口学习到该源MAC地址，并刷新MAC地址表中源MAC地址和物理端口的对应关系，这就好像是MAC地址从一个端口漂移到另一个端口。为应对恶意用户利用MAC地址漂移原理仿冒其他用户或上层设备的MAC地址，接入设备支持防御MAC地址漂移特性，简称防MAC漂移。

MAC地址漂移是关于MAC地址学习的一个术语。当设备从端口A接收到某个源MAC地址的报文时，如果MAC地址表中记录该MAC地址对应端口B，设备会将MAC地址表中

版权所有 © 华为技术有限公司

该MAC地址对应的端口从端口B修改为端口A。这就好像MAC地址从端口B飘移到了端口A，因此把此现象称为MAC地址漂移。

MAC地址漂移分为四种类型：

- 用户侧端口之间漂移
- 从用户侧端口漂移到网络侧端口
- 从网络侧端口漂移到用户侧端口
- 网络侧端口之间漂移

说明

用户侧端口是指用户端口和级联端口，网络侧端口是指上行端口。

为了防御恶意用户利用MAC地址漂移原理，仿冒其他用户或上层网络设备的MAC地址，接入网设备支持防御MAC地址漂移特性，简称为防MAC漂移。

POL设备主要支持防御MAC地址从网络侧端口漂移到用户侧端口。

当设备开启防MAC漂移特性时，从端口A接收到某个源MAC地址的报文后，设备会检查MAC地址表中是否已存在该MAC地址。如果MAC地址表中记录端口B对应该MAC地址，则设备根据端口类型等判断是否允许该MAC地址从端口B漂移到端口A。对于禁止漂移的情况，在MAC地址老化之前，设备会丢弃从端口A接收到的含有该源MAC地址的报文。

4.10 LLDP

LLDP（Link Layer Discovery Protocol，链路层发现协议）是IEEE 802.1ab中定义的一种标准的链路层发现方式。当网管需要管理不同厂商和网络的设备时，在所有的设备上部署LLDP，邻居间就可以交互设备信息。网管通过读取这些设备信息，来实时获取全网拓扑和设备间的物理连接关系等详细信息，从而帮助用户实时监控网络状态，定位网络故障。LLDP-MED（LLDP for Media Endpoint Devices，媒体节点发现协议）是LLDP协议的扩展，是终端设备（如IP电话）和网络设备（如交换机）之间的LLDP交互。

4.10.1 介绍

介绍LLDP-MED的产生背景及应用价值。

随着大规模组网需求的出现，网络设备种类日益繁多，各自的配置错综复杂，用户对网管能力的要求也越来越高，例如自动获取相连设备的拓扑状态、检测设备间的配置冲突等。

现阶段很多网管都使用自动发现（Automated Discovery）功能来获取网络拓扑的变化，但是绝大多数的网管最多只能分析到网络层的拓扑结构。这样的拓扑结构只能帮助用户获取到网络中有关设备增加或删除的基本事件，无法确定设备通过哪些接口跟其他设备相连，即无法说明设备的具体位置。虽然各厂家也有一些私有的协议用于发现设备之间的邻接信息，但是不利于全网拓扑的生成。

LLDP的出现有效解决了上述问题。LLDP（Link Layer Discovery Protocol，链路层发现协议）是IEEE 802.1ab中定义的第二层发现（Layer 2 Discovery）协议。LLDP提供了一种标准的链路层发现方式，可以将本端设备的主要能力、管理地址、设备标识、接口标识等信息封装到LLDP报文中传递给邻居节点。邻居节点在收到这些信息后，将其以标准MIB（Management Information Base，管理信息库）的形式保存起来，供网管查询及判断链路的通信状况。

版权所有 © 华为技术有限公司

LLDP能够准确发现网络中的设备有哪些接口，以及设备之间相互连接的具体信息。网管通过对各网元上LLDP本端信息和LLDP邻居信息的读取和整合，可以清晰的显示出整个网络拓扑，设备间的物理连接关系等详细信息。这些信息能够帮助网络管理员快速定位网络故障、实时监控网络状态，有效提升了网络的安全性和稳定性。

LLDP-MED通过在网络设备和IP电话之间添加和交换特定TLV（Type Length Value）消息来实现LLDP功能。LLDP的TLV信息包括机架和端口标识、系统名称、系统功能、系统描述及其它属性信息。LLDP-MED的TLV消息中增加了PoE（Power over Ethernet）、联网策略以及紧急电话服务的终端位置及清单等信息。

4.10.2 基本概念

介绍LLDP相关的基本概念，便于更深刻的了解LLDP的工作原理。

LLDP MIB

LLDP和MIB（Management Information Base，管理信息数据库）是密不可分的。LLDP协议规定设备的每个接口上都有四个MIB，其中最主要的两个为LLDP本地MIB（LLDP Local System MIB）和LLDP远端MIB（LLDP Remote System MIB），分别存储着本端设备和邻居节点的状态信息，包括设备ID、接口ID、系统名称、系统描述、接口描述、设备能力和网络管理地址。

LLDP Agent

LLDP协议规定设备的每个接口上都有一个LLDP Agent，用于管理设备的LLDP操作。LLDP Agent主要完成如下功能：

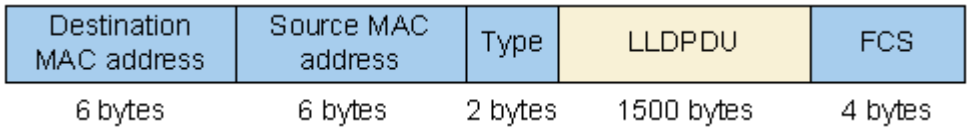
- 维护LLDP本地MIB的信息。
- 向邻居节点发送LLDP报文，通告本端设备的状态信息。
- 识别并解析收到的邻居节点发送的LLDP报文，维护LLDP远端MIB的信息。
- LLDP本地MIB或LLDP远端MIB的信息发生变化时，向NMS发送LLDP告警。

与IEEE 802.1ab-2009相比，不支持一个端口多个LLDP Agent，只支持一个端口一个LLDP Agent。

LLDP 报文

封装了LLDP数据单元LLDPDU（LLDP Data Unit）的以太网报文称为LLDP报文，其封装格式有两种：Ethernet II和SNAP（Subnetwork Access Protocol，子网访问协议）。目前设备支持的封装格式为Ethernet II，该封装格式的LLDP报文结构如下图所示：

图 4-95 LLDP 报文结构



LLDP报文中相关字段的解释如下表所示：

版权所有 © 华为技术有限公司

字段	说明
Destination MAC address	目的MAC地址，为固定的组播MAC地址0x0180-C200-000E。该地址是IEEE 802.1ab-2005规定的。
Source MAC address	源MAC地址，使用设备MAC地址。
Type	报文类型，固定为0x88CC。
LLDPDU	LLDP数据单元，LLDP信息交换的主体。
FCS（Frame Check Sequence）	帧校验序列。

LLDPDU

LLDPDU是封装在LLDP报文中的数据单元。设备先将本地信息封装成TLV（Type-Length-Value）格式，再由若干个TLV组合成一个LLDPDU，封装在LLDP报文中进行传送。用户可以根据需要将多种不同的TLV组合到LLDPDU中，设备根据这些不同的TLV来通告自己的状态信息，学习邻居节点的状态信息。

图 4-96 LLDPDU 结构

LLDP协议规定每个LLDPDU固定以Chassis ID TLV、Port ID TLV和Time to Live TLV开始，以End of LLDPDU TLV为结束，这四个TLV为必选的TLV，其他则为可选TLV。

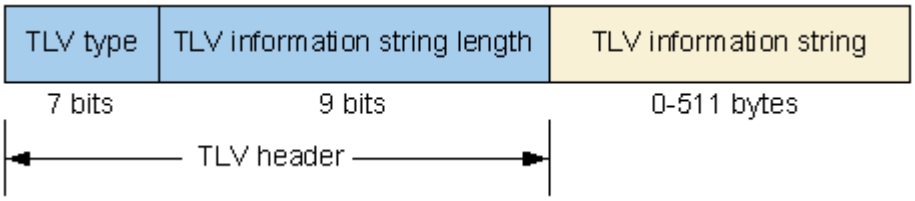
LLDPDU有两种类型：

- Normal LLDPDU：普通的LLDPDU，提供本端设备信息与邻居信息。
- Shutdown LLDPDU：去使能端口LLDP能力时发送，用于通知对端快速清除邻居信息。不包括可选TLV，且TTL TLV值为0。

TLV

TLV是组成LLDPDU的最小单元，表示一个对象的类型、长度和信息。每个TLV代表设备的一种信息，例如设备ID、接口ID、管理地址等，分别对应Chassis ID TLV、Port ID TLV、Management Address TLV等固定的TLV。

图 4-97 TLV 结构



版权所有 © 华为技术有限公司

LLDP可以封装的TLV类型包括两大类：基本TLV和组织特定TLV。后者包括802.1组织和802.3组织定义的TLV，将来可能有更多组织定义的TLV。

表 4-23 TLV 列表

TLV名称	TLV类型	说明
End of LLDPDU TLV	0	标识LLDPDU结束。
Chassis ID TLV	1	标识设备的桥MAC地址。
Port ID TLV	2	标识LLDPDU发送端的接口名，采用IF-MIB叶子ifName的值。
Time To Live TLV	3	标识本设备信息在邻居节点上的存活时间。
Port Description TLV	4	标识接口的描述信息 采用IF-MIB的iftable表中的ifDescr叶子的值。
System Name TLV	5	标识设备的名称，可以通过**sysname**命令配置。
System Description TLV	6	标识设备描述信息，可以通过**system sys-info description**命令配置。
System Capabilities TLV	7	标识设备支持的功能，以及哪些功能被使能。
Management Address TLV	8	标识管理地址。
Reserved	9-126	保留，用作特殊用途。
组织特定TLV（Organizationally Specific TLV）	127	通过不同的OUI（Organizationally Unique Identifier ）字段代表不同的组织，详细说明请参见LLDP协议。

LLDP-MED

LLDP-MED以IEEE的802.1AB LLDP为基础。LLDP是IEEE的邻居发现协议，其它组织可以对其进行扩展。从网络设备查明的信息，如交换机和无线接入点，可以帮助进行故障分析，并允许管理系统准确地了解网络拓扑结构。

电讯工业协会TIA标准草案：Link Layer Discovery Protocol-Media Endpoint Discovery（LLDP-MED）使得端点与网络基础设施之间的信息共享变得更加容易。这些数据可以简化端点的部署，进一步简化管理，同时推动企业网络对E911的支持。

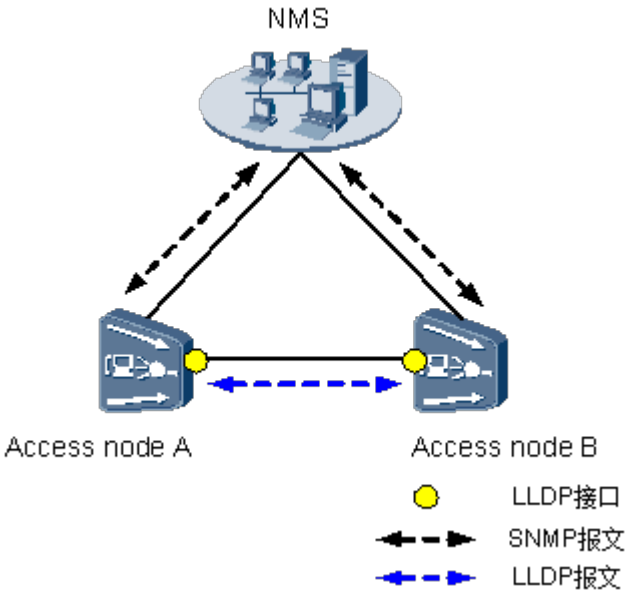
4.10.3 原理描述

结合LLDP的基本组网图，介绍网管通过LLDP协议获取设备信息和网络拓扑的过程。

版权所有 © 华为技术有限公司

LLDP 工作过程

图 4-98 LLDP 基本组网图



如图所示，Access node A和Access node B支持LLDP，NMS收集设备信息的过程如下：

1. Access node A将本端的状态信息封装成LLDP报文，发送给邻居设备Access node B。
2. Access node B解析接收到的LLDP报文，并将该报文中Access node A的信息存储到自己的远端MIB数据库中，供NMS提取拓扑信息使用。
3. 同样，Access node B也将本端的状态信息封装成LLDP报文发送给Access node A。
4. Access node A解析接收到的LLDP报文，并将该报文中Access node B的信息存储到自己的远端MIB数据库中，供NMS提取拓扑信息使用。
5. NMS通过与Access node A和Access node B交互SNMP报文，从两者的MIB数据库中提取本地信息和邻居信息，进行整合分析，最终发现整网的拓扑结构。

从以上过程可以看出：

- 在NMS上建立整个网络的拓扑，需要NMS管理范围内的所有设备都支持LLDP。
- 每台设备只能发现和自己直接相连的设备信息，因此NMS需要收集网络中所有设备上报的本地信息和邻居信息，才能得到全网拓扑。

LLDP 接口工作模式

LLDP接口有如下工作模式：

- Tx/Rx：既发送又接收LLDP报文。
- Tx：只发送不接收LLDP报文。
- Rx：只接收不发送LLDP报文。

版权所有 © 华为技术有限公司

- Disable：既不发送也不接收LLDP报文。

当接口的LLDP工作模式发生变化时，接口将对协议状态机进行初始化操作。为了避免接口工作模式频繁改变而导致接口不断执行初始化操作，设备支持配置接口初始化延迟时间，当接口工作模式改变时延迟一段时间再执行初始化操作。

LLDP 报文的发送机制

使能LLDP功能后，设备会周期性地向邻居节点发送LLDP报文。在以下三种情况下，为了让其它设备尽快发现本设备，设备支持快速发送机制，即会立即发送一个LLDP报文。

- 设备发现一个新邻居，即接收到一个新的LLDP报文且本地没有保存该报文的发送方设备信息。
- 设备的LLDP状态由去使能变为使能。
- 设备的接口状态由Down变为Up。

LLDP 报文的接收机制

设备收到LLDP报文时，会对报文及其携带的TLV信息进行有效性检查。通过有效性检查后，保存邻居信息，并根据LLDPDU中携带的Time To Live TLV值设置邻居信息在本地设备上的老化时间。如果接收到的LLDPDU中的TTL值等于零，将立刻老化掉该邻居信息。

LLDP-MED 工作过程

如下图所示，IP话机通过RJ45接口连接到ONU，并发送LLDP报文到ONU。ONU收到LLDP报文后，解析其设备类型，如果设备类型为话机类型，则发送LLDP报文到IP话机，在LLDP报文中携带LLDP-MED的TLV。

图 4-99 LLDP-MED 工作过程图

4.10.4 组网应用

传统基于铜线的企业局域网，正面临POL（Passive Optical LAN，无源光局域网）的改造挑战，LLDP-MED功能可以实现语音业务识别和二层转发配置下发，从而支撑无源光局域网的部署和实施。

无源光局域网相对于传统基于铜线的企业局域网的优势：

- 更节能、节省管线空间、机房配套等，成本更低。
- 光纤架构演进性更好
- 光纤有更长的传输距离
- 运维方便

LLDP-MED功能为无源光局域网终端设备的业务管理和维护诊断提供了技术支持，具体应用场景如下。

版权所有 © 华为技术有限公司

企业园区上网业务

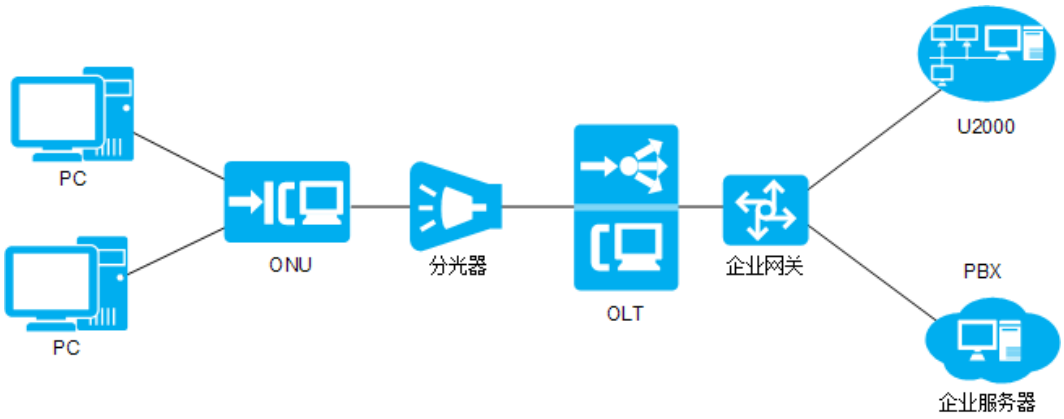
如图4-100所示的组网方式下，通过带POE功能的ONU连接会议终端、IP电话、PC，以及Wifi瘦AP、打印机等。

光网络终端提供1~24以太端口连接办公桌面，提供单个或者多个用户的上网接入功能，光网络终端提供L2转发功能；光网络终端通过OMCI进行管理；用户通过802.1x功能进行认证接入。

光网络终端通过PON网络连接OLT，OLT提供L2/L3转发功能。

企业服务器负责网络的管理，用户接入的认证功能。

图 4-100 企业园区上网业务组网



企业园区（酒店接入）场景

在如图4-101所示的组网方式下，光网络终端提供接口分别接入Wifi瘦AP、机顶盒、PC、IP话机。

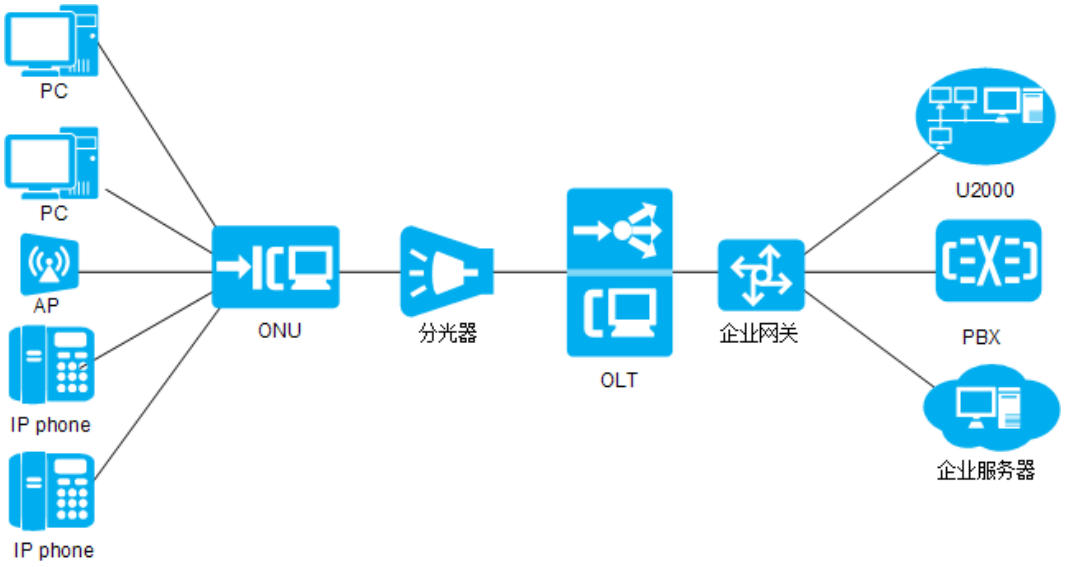
光网络终端提供4个以太端口用于酒店房间接入；对于酒店接入场景：一个接口连接Wifi瘦AP，一个接口连接IPTV机顶盒，一个接口用户连接PC，提供上网接入功能，另外一个接口用于连接IP话机，提供语音接入功能；接IP话机的接口需要提供POE功能；上层设备通过LLDP-MED向IP话机下发业务配置。

光网络终端通过PON网络连接OLT，OLT提供L2/L3转发功能。

企业服务器负责网络的管理，用户接入的认证功能。

版权所有 © 华为技术有限公司

图 4-101 企业园区（酒店接入）场景组网



4.10.5 参考标准和协议

本特性参考的标准和协议如下：

- IEEE 802.1ab-2009
- 目的MAC地址参考IEEE 802.1ab-2005

版权所有 © 华为技术有限公司

5 预防性维护

5.1 功能模块

维护人员需根据当地实际情况制定维护周期，推荐维护周期为半年一次。

表 5-1 功能模块维护

编号	维护项	状态异常的可能原因	推荐的处理方法
1	PWR指示灯是否绿色常亮	• 常灭：网络模块未上电 • 常亮（橙色）：网络模块供电正常，但网络模块与电源模块通信不正常	1. 检查网络模块的电源输入及网络模块内部电源线缆连接状况。 2. 更换网络模块。
2	SYS指示灯是否绿色常亮	• 常灭：网络模块未运行 • 闪烁（红色，2Hz）：网络模块没有激活；或者网络模块有故障，故障可恢复。	1. 检查光纤线路是否正常。 2. 登录到网管，根据具体告警类型做出对应的告警处理（参考**6.1 eSight告警故障处理**）。 3. 更换功能模块。
3	ALM指示灯是否常灭	常亮（红色）：设备供电异常	1. 根据具体告警类型做出对应的告警处理（参考**6.1 eSight告警故障处理**）。 2. 更换功能模块。

5.2 立杆

维护人员需根据当地实际情况制定维护周期，推荐维护周期为半年一次。

版权所有 © 华为技术有限公司

表 5-2 立杆维护项目表

维护项	检查项	检测方法	维护条件	处理方法
外观	检查杆件是否变形/倾斜。	目测	杆件变形/倾斜	• 变形需更换杆件。 • 地基倾斜需调整地基。
	检查立杆是否腐蚀、生锈。	目测	立杆腐蚀、生锈	除锈后重新喷漆。 **说明** 油漆色号是RAL 9016

版权所有 © 华为技术有限公司

6 设备维护

6.1 eSight 告警故障处理

表 6-1 告警及故障处理

告警名称	告警解释	可能原因	处理方法
交流停电	交流停电	• 交流停电。 • 取电处交流空开断开。 • 取电线缆老化，短路或断路异常。	1. 测量交流输入电压，查看是否无交流输入。 • 是，处理电网故障； • 否，下一步。 2. 查看交流输入空开是否断开。 • 是，检修交流配电，排除故障后闭合空开； • 否，联系华为技术支持。
交流输入过压	交流输入过压	• 交流输入电压高于264V AC。 • 功率模块交流检测回路故障。	1. 测量交流输入电压是否异常。 • 是，查找异常原因并及时排除，防止高压损坏功率模块； • 否，联系华为技术支持。

版权所有 © 华为技术有限公司

告警名称	告警解释	可能原因	处理方法
交流输入欠压	交流输入欠压	• 交流输入电压低于176V AC。 • 线缆松脱。	1. 测量交流输入电压是否异常。 • 是，处理电网故障； • 否，下一步。 2. 检查接线是否正常。 • 是，联系华为技术支持； • 否，修复异常接线。
12V DC输出保护	12V DC输出保护	• 输出过功率。 • 输出短路。 • 12V DC输出高于16V DC。 • 环境过温。	1. 查看12V DC输出口是否短路或负载是否过功率。 • 是，让输出口不短路或减轻负载； • 否，下一步。 2. 在正午测试功率模块表面温度，要求小于45℃。 • 是，联系华为技术支持； • 否，增加遮阳罩。
24V AC输出保护	24V AC输出保护	• 输出过功率。 • 输出短路。 • 24V AC输出高于30V AC。 • 环境过温。	1. 查看24V AC输出口是否短路或负载是否过功率。 • 是，让输出口不短路或减轻负载； • 否，下一步。 2. 在正午测试功率模块表面温度，要求小于45℃。 • 是，联系华为技术支持； • 否，增加遮阳罩。
53V DC输出保护	53V DC输出保护	• 输出过功率。 • 输出过流。 • 53V DC输出高于57V DC。 • 环境过温。	1. 查看53V DC输出口是否短路或负载是否过功率。 • 是，让输出口不短路或减轻负载； • 否，下一步。 2. 在正午测试功率模块表面温度，要求小于45℃。 • 是，联系华为技术支持； • 否，增加遮阳罩。
24V AC模块故障	24V AC模块故障	功率模块中子单元“24V AC模块硬件”故障。	更换功率模块。

版权所有 © 华为技术有限公司

告警名称	告警解释	可能原因	处理方法
53V DC模块故障	53V DC模块故障	功率模块中子单元“53V DC模块硬件”故障。	更换功率模块。
AC模块故障	AC模块故障	功率模块中子单元“AC模块硬件故障”。	更换功率模块。
AC模块保护	AC模块保护	交流输入电压不在工作范围内，或PFC模块保护。	1. 测量交流输入电压是否异常（正常范围176V AC~264V AC）。 ● 是，处理电网故障； ● 否，联系华为技术支持。
过温保护	过温保护	环境过温。	1. 查看功能模块工作环境温度是否大于45℃。 ● 是，增加遮阳罩； ● 否，联系华为技术支持。
交流避雷器故障	交流避雷器故障	● 模块接地异常。 ● 站点总接地点异常。 ● 交流避雷器自身故障。	1. 检查站点交流输入到供电设备是否架空走线或设备用于高速路且配电箱到设备距离超过1.5Km。 ● 是，站点需要增加B级防雷器； ● 否，下一步。 2. 检测功能模块接地点连接是否正常。 ● 是，下一步； ● 否，确保接地连接正常。 3. 检测站点接地阻抗是否小于10Ω。 ● 是，下一步； ● 否，修复站点总接地阻抗并降低到10Ω以下。 4. 检查交流避雷器是否故障。 ● 是，更换交流避雷器； ● 否，联系华为技术支持。

版权所有 © 华为技术有限公司

告警名称	告警解释	可能原因	处理方法
模块升级失败	功率模块升级失败	• 升级过程中功率模块掉电。 • 升级过程中功率模块通信失败。	1. 检查是否掉电。 • 是，保证功率模块正常上电； • 否，下一步。 2. 功率模块通信是否正常，在保证通信正常的情况下，继续升级并查看是否产生告警。 • 是，更换功率模块。 • 否，完毕。
ONT信号丢失	ONT信号丢失	• ONT掉电； • 光纤损坏。	• 检查网络模块的电源输入及内部电源线缆连接状况。 • 检查光纤连接状况及光纤损坏情况。

版权所有 © 华为技术有限公司

告警名称	告警解释	可能原因	处理方法
PON端口存在环网	当用户PON端口环网检测功能使能时，设备定时向用户PON端口发送环网检测报文。如果设备从某个用户PON端口或者网络PON端口收到对应报文，就认为用户PON端口发生了环网。对用户侧接收到的报文，设备将本设备上形成环网的ONT去激活，同时系统产生此告警；对网络侧或级联侧接收到的报文，不产生此告警。	PON端口形成环网。	检查用户侧网络拓扑结构，消除环网条件，检查ONT是否已经去激活；如果去激活，就将ONT重新激活。
ONT位相摆动(DOWi)	ONT上行帧出现在非预期的位置上，测距距离发生变化	• 温度变化等原因导致了光纤长度变化； • ONT硬件故障。	• 更换分支光纤； • 复位该ONT。

 版权所有 © 华为技术有限公司

告警名称	告警解释	可能原因	处理方法
ONT帧丢失(LOFi)	当GPON端口连续从ONT收到多个无效的定界符时，系统产生此告警。	• 光通路质量差； • ONT异常。	• 检查光纤连接, 确保光纤连接紧密； • 清洁光纤接头； • 光纤老化、弯折或损坏时更换光纤； • 复位或更换ONT。
ONT下行信号失败(SF)	当ONT检测到其下行信号失败，ONT的下行误码率超出门限时，系统产生此告警。	• 光通路质量差； • ONT异常。	• 检查光纤连接, 确保光纤连接紧密； • 清洁光纤接头； • 光纤老化、弯折或损坏时更换光纤； • 复位或更换ONT。
GPON ONT掉电(DGi)	当OLT接收到ONT的掉电消息时，系统产生此告警。	ONT供电异常。	检查ONT电源，保证ONT电源正常工作。
保护组倒换失败	保护组倒换失败，相关业务中断	• OLT没有收到PON段层踪迹消息； • OLT收到的PON段层踪迹消息错误。	• 检查并更换ONT • 检查光纤连接, 确保光纤连接正确
ONT以太端口信号丢失	ONT以太端口没有信号，业务中断	ONT以太网端口没有信号。	确保ONT对应以太网口有插网线并且网线没有松动
ONT是流氓ONT	ONT光模块常发光，ONT是流氓ONT	ONT光模块常发光。	• 隔离ONT； • 替换ONT。
ONT温度超出告警阈值	ONT温度过高或过低, ONT无法正常工作	• ONT异常； • ONT外部环境温度过高或过低。	• 复位或更换ONT； • 使ONT处于正常室温或通风环境下。
ONT以太端口检测到环路	ONT以太端口检测到环路	• ONT以太端口间存在环路； • ONT以太端口下的网络存在环路。	• 检查并断开ONT以太端口间存在的环路； • 检查并断开ONT以太端口下网络存在的环路。

版权所有 © 华为技术有限公司

告警名称	告警解释	可能原因	处理方法
ONT性能统计值超出告警门限	ONT在性能统计周期内, 性能统计值超出告警门限, 有可能影响业务质量	• 发送丢包事件阈值不合适； • 线路连接故障。	• 检查发送丢包事件阈值设置是否合适； • 检查线路连接, 确保线路连接正常。
ONT掉电(DGi)	OLT接收到ONT的掉电消息时发生此告警	供电线缆未插好。	检查网络模块的电源输入及内部电源线缆连接状况。

版权所有 © 华为技术有限公司

告警名称	告警解释	可能原因	处理方法
PON端口存在环网	当用户PON端口环网检测功能使能时，设备定时向用户PON端口发送环网检测报文。如果设备从某个用户PON端口或者网络PON端口收到对应报文，就认为用户PON端口发生了环网。对用户侧接收到的报文，设备将本设备上形成环网的ONT去激活，同时系统产生此告警；对网络侧或级联侧接收到的报文，不产生此告警。	设备的两个PON端口存在环网。	• 按照组网规划，检查网络拓扑结构，保证设备业务端口之间、业务端口与上行口之间无环路后，再使用display ont info命令检查ONT是否被去激活，查询参数“Control Flag”是否是“deactive”； • 使用ont activate命令将ONT重新激活。检查系统是否产生恢复告警。
ONT DI端口状态变化	ONT机柜门打开时，系统产生此告警。	ONT机柜门被打开。	检查ONT机柜门，确保ONT机柜门处于正常关闭状态。

6.2 ONU Web 维护

ONU支持通过Web界面进行业务维护。

版权所有 © 华为技术有限公司

如何登录 Web 界面

步骤1 设置个人计算机的IP地址与ONU的管理IP地址在同一网段。例如：

- IP地址：192.168.18.100
- 子网掩码：255.255.255.0

说明

ONU管理IP 地址和子网掩码的出厂缺省值为：

- IP地址：192.168.18.1
- 子网掩码：255.255.255.0

步骤2 在浏览器地址栏输入ONU的管理IP地址，然后按回车键，浏览器弹出登录窗口。

步骤3 在登录窗口中输入用户名和密码（默认用户名为**Epadmin**，默认密码为**adminEp**），选择Web界面语言，然后单击登录。密码验证通过后，即可访问Web界面。

- 登录Web 界面后，如果5分钟之内未执行任何操作，超时退出，系统自动返回登录状态。
- 连续三次用户名和密码输入错误，系统将被锁定，一分钟后自动解锁。

----结束

 版权所有 © 华为技术有限公司

7 部件更换

危险

- 更换功能模块，需要负载断电，需取得客户同意。请做好减少断电时间的保证措施。
- 更换功能模块，需断开前级输入空开。

前提条件

- 准备好工具和材料：劳保手套、刀头宽度2毫米一字螺丝刀、刀头宽度3毫米一字螺丝刀、刀头大小6毫米十字螺丝刀、绝缘胶带、防水胶带和防火泥等。
- 备好新的功能模块。

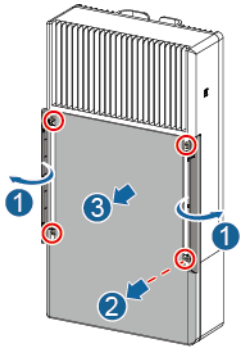
操作步骤

步骤1 戴上劳保手套。

步骤2 断开功能模块的交流前级输入空开。

步骤3 拆除旧功能模块的前面板。

图 7-1 拆除前面板



LXP0000029

步骤4 记录功能模块上的线缆连接位置，并依次取下各接口线缆，做好绝缘防护。

版权所有 © 华为技术有限公司

步骤5 拆除旧的功能模块。

图 7-2 拧松螺钉

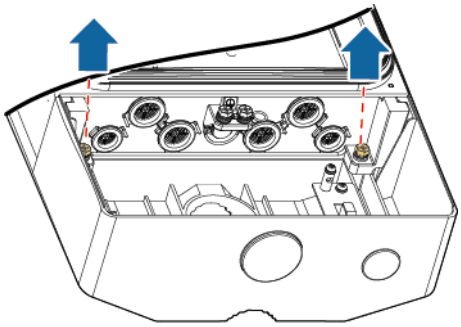


图 7-3 拆除模块

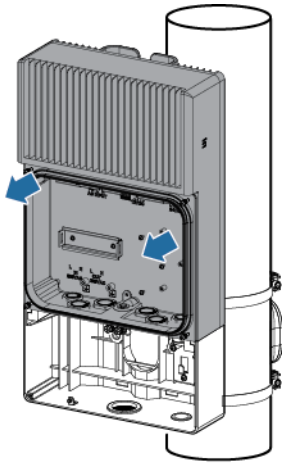
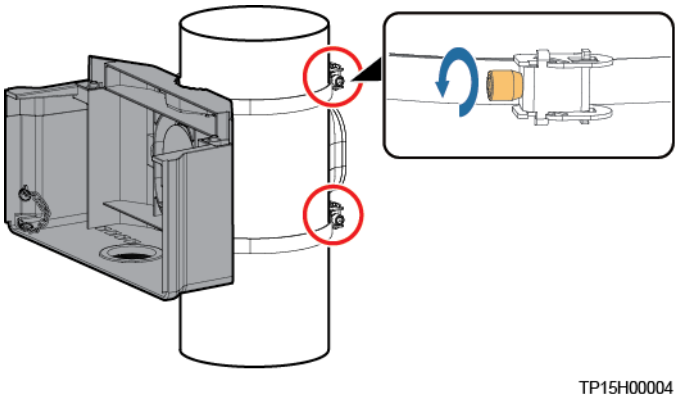


图 7-4 拆除底座（可根据实际情况选择是否拆除底座）



步骤6 安装新的功能模块。

步骤7 根据记录的信息将线缆连接到功能模块上。

步骤8 使用防水胶带和防火泥对线缆接口进行处理。

步骤9 闭合功能模块的交流前级输入空开。

版权所有 © 华为技术有限公司

步骤10 脱下劳保手套。

----结束

后续处理

将拆除下来的部件包装好返回华为当地库房。

 版权所有 © 华为技术有限公司

A 技术指标

表 A-1 系统应用环境条件

项目	规格
工作温度	–40℃～+45℃，太阳辐射：1120W/m^2
储存温度	–40℃～+70℃
相对湿度	5% RH～95% RH
大气压	70kPa～106kPa
海拔要求	–150m～4000m （在2000m～4000m环境下高温降额，每升高200m，工作温度降低1℃）
设备运行环境	C类环境
其他要求	没有导电尘埃和腐蚀性气体、没有爆炸危险 灰尘度、腐蚀性物质、有害生物、霉菌等指标应符合ETSI EN 300 019-1-4（V2.2.1） Class 4.1要求

表 A-2 功能模块指标

项目	规格
尺寸（高×宽×深）	550mm×300mm×105mm（外框尺寸，不包含外凸部分）
重量	≤9kg
防护等级	IP55
安规设计	CE认证
平均无故障时间（MTBF）	25万小时

版权所有 © 华为技术有限公司

项目	规格	
交流输入	输入制式	单相三线制输入
	工作电压范围	176V AC～264V AC
	频率	45Hz～66Hz，额定值为50Hz/60Hz
	功率因数	≥0.96 T_a=25℃，V_{in}=220V AC，仅54.5V输出100%负载
	THD	≤10% T_a=25℃，V_{in}=220V AC，仅54.5V输出100%负载
	输入电流	最大值2.5A
12V DC直流输出	输出电压	13.2V DC
	输出功率	72W
	纹波+噪声	≤400mV
24V AC交流输出	输出电压	25.2V AC，50Hz
	输出功率	72W
	稳压精度	≤±5%
12V DC、24V AC接口最大总输出功率144W。		
功能模块供电后自身最大功耗27.5W。		

表 A-3 EMC 指标

项目	规格	
电磁干扰（EMI）	传导干扰（CE）	交流电源输入端口：Class A，满足CISPR 32 **说明** 此为A级产品，在生活环境中，该产品可能会造成无线电干扰。在这种情况下，可能需要用户对其干扰采取切实可行的措施。
	辐射干扰（RE）	壳体端口：Class A，满足CISPR 32
	谐波电流（Harmonic）	交流电源输入端口：IEC 61000-3-2，A类设备要求
	电压闪烁和波动（Flicker）	交流电源输入端口：IEC 61000-3-3，A类设备要求

版权所有 © 华为技术有限公司

项目	规格	
电磁敏感度（EMS）	静电放电抗扰性（ESD）	IEC 61000-4-2 壳体端口：接触放电6kV（B级），空气放电8kV（B级）
	电快速脉冲群抗扰性（EFT）	IEC 61000-4-4 ● 壳体输入端口：2kV（判据B） ● 壳体输出端口：1kV（判据B）
	辐射抗扰性（RS）	IEC 61000-4-3 壳体端口：频率范围为80MHz-6000MHz，采用80%AM（1kHz）调制，场强10V/m。
	传导抗扰性（CS）	IEC 61000-4-6 ● 壳体输入端口：0.15MHz～80MHz：10V ● 壳体输出端口：0.15MHz～80MHz：10V
	浪涌抗扰性（SURGE）	EN61000-4-5 ● 交流电源输入端口：（判据B）差模6kV，共模6kV，1.2/50μs ● 12V DC直流输出端口：（判据B）差模±2kV，共模±4kV，1.2/50μs ● 24V AC交流输出端口：（判据B）差模±2kV，共模±6kV，1.2/50μs
	防雷	● 交流电源输入端口：共模±20kA，差模±20kA，8/20us冲击电流波形，正负各五次 ● 12V DC输出端口：共模±5kA、差模±3kA，8/20us冲击电流波形，正负各五次。
	电源跌落抗扰度（DIP）	满足IEC 61000-4-11标准要求 ● 电压中断（减小>95%），持续时间10ms，性能等级B ● 电压跌落（减小30%），持续时间500ms，性能等级C ● 电压中断（减小>95%），持续时间5000ms，性能等级C

版权所有 © 华为技术有限公司

B 运用环境说明

表 B-1 运用环境说明

分类	环境定义
A类	指温湿度受控的室内（包括有人居住的房间）。
B类	指温湿度不受控的房间内，一般的室外环境（包括只有简单遮蔽（如遮阳棚）、湿度偶然会达到100%的情况）。
C类	指海洋上环境，或者污染源附近的陆地室外和只有简单遮蔽（如遮阳棚）的环境。（污染源附近是指在以下半径范围内的区域：距离盐水（如海洋、盐水湖）3.7公里，冶炼厂、煤矿、热电厂等重污染源3公里，化工、橡胶、电镀等中等污染源2公里，食品、皮革、采暖锅炉等轻污染源1公里。）
D类	指距离海岸边500m以内的环境。属于C类环境中的一种特定场景。

版权所有 © 华为技术有限公司

C 缩略语

A		
APS	Automatic Protection Switching	自动保护倒换
C		
CAN	Controller Area Network	控制区域网络
COM	cluster communication port	串行通信端口
D		
DI	digital input	数字量输入
DO	digital output	数字量输出
E		
ERPS	Ethernet Ring Protection Switching	以太网环保护
G		
GE	Gigabit Ethernet	千兆以太网
GPON	gigabit-capable passive optical network	千兆比特无源光网络
L		
LAG	link aggregation group	链路聚合组
M		
MAC	Media Access Control	媒体接入控制

版权所有 © 华为技术有限公司

MDI	Medium Dependent Interface	媒介依赖接口
N		
NMS	network management system	网络管理系统
P		
PoE	power over Ethernet	以太网供电
Q		
QoS	Quality of Service	服务质量
S		
SEP	Smart Ethernet Protection	智能以太保护协议
V		
VLAN	virtual local area network	虚拟局域网
W		
WLAN	wireless local area network	无线局域网

版权所有 © 华为技术有限公司