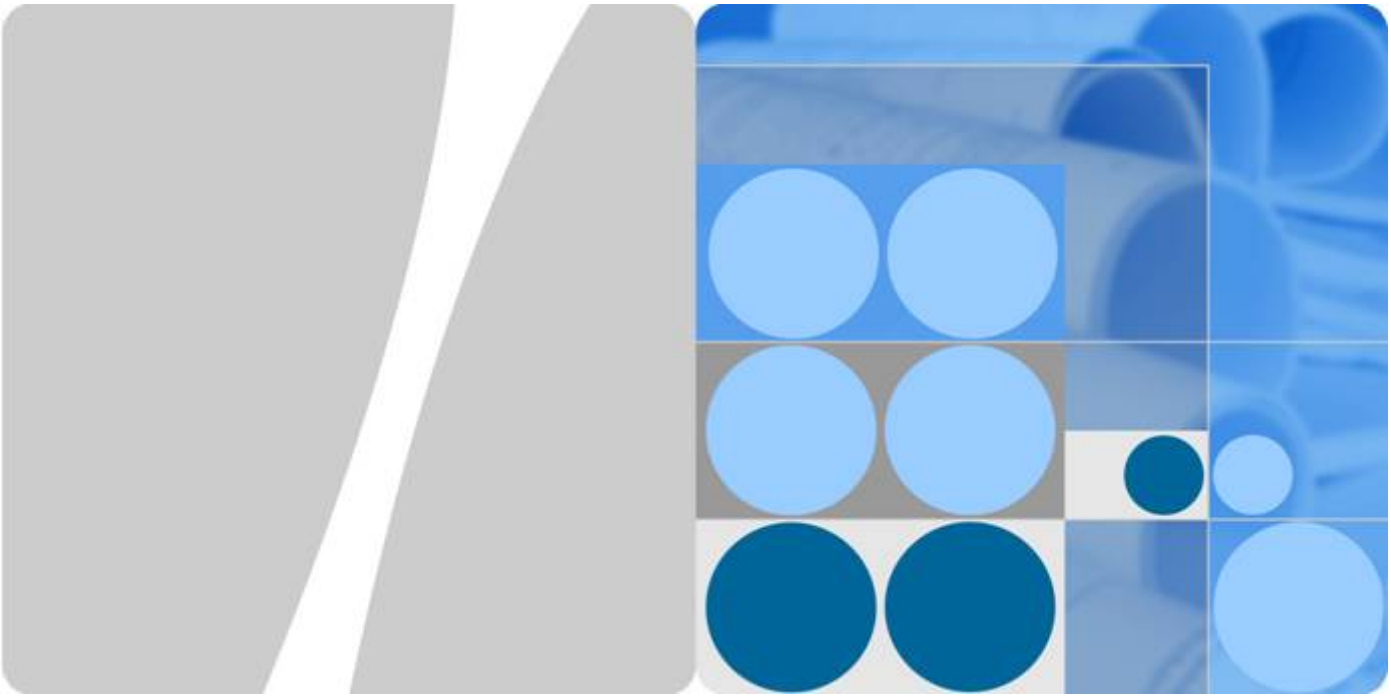


SmartAX MA5631 EoC 局端设备

V800R308C02

配置指南

文档版本　02

发布日期　2011-08-05

华为技术有限公司

商标声明


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

注意

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

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

华为技术有限公司

地址： 深圳市龙岗区坂田华为总部办公楼 邮编：518129

网址： http://www.huawei.com

客户服务邮箱： support@huawei.com

客户服务电话： 4008302118

前 言

读者对象

本文档针对 MA5631 的重点业务，从配置实例介绍了业务的配置过程。主要包括如下方面的具体内容：目的、组网图、数据规划、前提条件、注意事项、配置流程、操作步骤和操作结果。

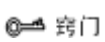
阅读本文档能指导用户掌握 MA5631 设备重点业务的配置过程。

本文档（本指南）主要适用于以下工程师：

- 安装调测工程师
- 系统维护工程师
- 数据配置工程师

符号约定

在本文中可能出现下列标志，它们所代表的含义如下。

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

命令行格式约定

格式	意义
粗体	命令行关键字（命令中保持不变、必须照输的部分）采用**加粗**字体表示。
斜体	命令行参数（命令中必须由实际值进行替代的部分）采用*斜体*表示。
[ ]	表示用“[ ]”括起来的部分在命令配置时是可选的。
{ x | y | ... }	表示从两个或多个选项中选取一个。
[x | y | ...]	表示从两个或多个选项中选取一个或者不选。
{ x | y | ... } *	表示从两个或多个选项中选取多个，最少选取一个，最多选取所有选项。
[x | y | ...] *	表示从两个或多个选项中选取多个或者不选。

图形界面元素引用约定

格式	意义
“”	带双引号“”的格式表示各类界面控件名称和数据表，如单击“确定”。
>	多级菜单用“>”隔开。如选择“文件 > 新建 > 文件夹”，表示选择“文件”菜单下的“新建”子菜单下的“文件夹”菜单项。

修订记录

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

文档版本 02 （2011-08-05）

相对于版本 V800R308C02 文档版本 01 （2011-04-15）的变化如下：

修改：

- **7 配置 EoC 宽带业务示例（OLT 使用 EPON 接入方式）**
- **8 配置 EoC 宽带业务示例（OLT 使用 GPON 接入方式）**
- **3.11.1.1 配置基于业务流的流量管理**

文档版本 01 （2011-04-15）

第一次正式发布版本。

目 录

1 部署网络设备

关于本章

按照规划完成各个站点 MA5631 的部署，实现网络中的网管、OLT、MA5631、CNU 的相互通信。

1.1 网络设备部署概述
网络设备部署包括 MA5631 的数据规划、离线部署（通过网管或者通过 OLT 的 CLI 命令）、MA5631 的安装、MA5631 的绑定、CNU 的安装。完成网络设备部署后，即可以远程对 MA5631 配置业务。

1.2 部署网络设备实例
通过实例介绍在有网管和无网管的场景下网络设备的部署。

1.1 网络设备部署概述

网络设备部署包括 MA5631 的数据规划、离线部署（通过网管或者通过 OLT 的 CLI 命令）、MA5631 的安装、MA5631 的绑定、CNU 的安装。完成网络设备部署后，即可以远程对 MA5631 配置业务。

有网管场景下的网络设备部署中所包括活动的详细介绍如**表 1-1** 所示。

表 1-1 有网管场景下的设备部署活动表

活动	说明
MA5631 的数据规划	使用网管提供的“预部署规划表单”进行数据规划，并最终生成“资源部署表单”。
离线部署 MA5631	通过网管导入“资源部署表单”，实现对 MA5631 的预部署。
MA5631 的安装	硬件安装工程师到库房领取 MA5631 设备后到目的地进行安装，完成安装并确认设备无硬件问题后，将 MA5631 设备类型、业务端口信息与 MA5631 SN 序列号（或者 MAC 地址）返回给调测工程师。
MA5631 绑定	● 使用 EPON 上行时，通过网管绑定 MA5631 的 IP 地址与 MAC 地址。 ● 使用 GPON 上行时，通过网管绑定 MA5631 的 IP 地址与 SN。
CNU 的安装	硬件安装工程师到库房领取 CNU 设备后到目的地进行安装，完成安装并确认设备无硬件问题后，将 CNU 设备类型、业务端口信息与 CNU SN 序列号（或者 MAC 地址）返回给调测工程师。

无网管场景下的网络设备部署中所包括活动的详细介绍如**表 1-2** 所示。

说明

无网管的场景下通过 OLT 增加 ONU 有两种方法:

- 方法一:
  1. 安装 MA5631 并正常上电。
  2. 在 EPON 或 GPON 模式下使用 **port** *portid* **ont-auto-find** 命令使能 ONU 自动发现功能。
  3. OLT 自动发现 MA5631。
  4. 在 EPON 或 GPON 模式下使用 **ont confirm** 命令确认自动发现的 MA5631。
  5. 安装 CNU 并正常上电。
  6. MA5631 自动发现 CNU。
  7. 在 EoC 模式下使用 **cnu confirm** 命令确认自动发现的 CNU。
- 方法二:
  1. 在 EPON 或 GPON 模式下使用 **ont add** 命令在 OLT 上离线添加 MA5631。
  2. 安装 MA5631 并正常上电。
  3. 在 EoC 模式下使用 **cnu add** 命令在 MA5631 上离线添加 CNU。
  4. 安装 CNU 并正常上电。

本文档选取第一种方法进行部署。

表 1-2 无网管场景下的设备部署活动表

活动	说明
MA5631 的数据规划	根据实际 FTTx 业务规划和配套的 OLT 版本，完成 OLT、MA5631 的数据规划。
MA5631 的安装	硬件安装工程师到库房领取 MA5631 设备后到目的地进行安装，完成安装并确认设备无硬件问题后，将 MA5631 设备类型、业务端口信息与 MA5631 SN 序列号（或者 MAC 地址）返回给调测工程师。
部署 MA5631	通过 OLT 的 CLI 命令使能 PON 端口的自动发现功能，确认自动发现的 MA5631 后，使用预先配置的模板增加 MA5631。
配置 MA5631 的业务	通过 OLT Telnet 登录 MA5631 的管理 IP 地址后，就可以对 MA5631 进行业务配置。
CNU 的数据规划	根据实际 FTTx 业务规划，完成 CNU 的数据规划。
CNU 的安装	硬件安装工程师到库房领取 CNU 设备后到目的地进行安装，完成安装并确认设备无硬件问题后，将 CNU 设备类型、业务端口信息与 CNU SN 序列号（或者 MAC 地址）返回给调测工程师。
部署 CNU	MA5631 确认自动发现的 CNU 后，使用预先配置的模板增加 CNU。
配置 CNU 的业务	在 EoC 局端模块上实现对 CNU 的业务配置。

1.2 部署网络设备实例

通过实例介绍在有网管和无网管的场景下网络设备的部署。

前提条件

- 网络设备和线路正常。
- OLT 上主控板及 EPON 业务板、GPON 业务板状态正常。

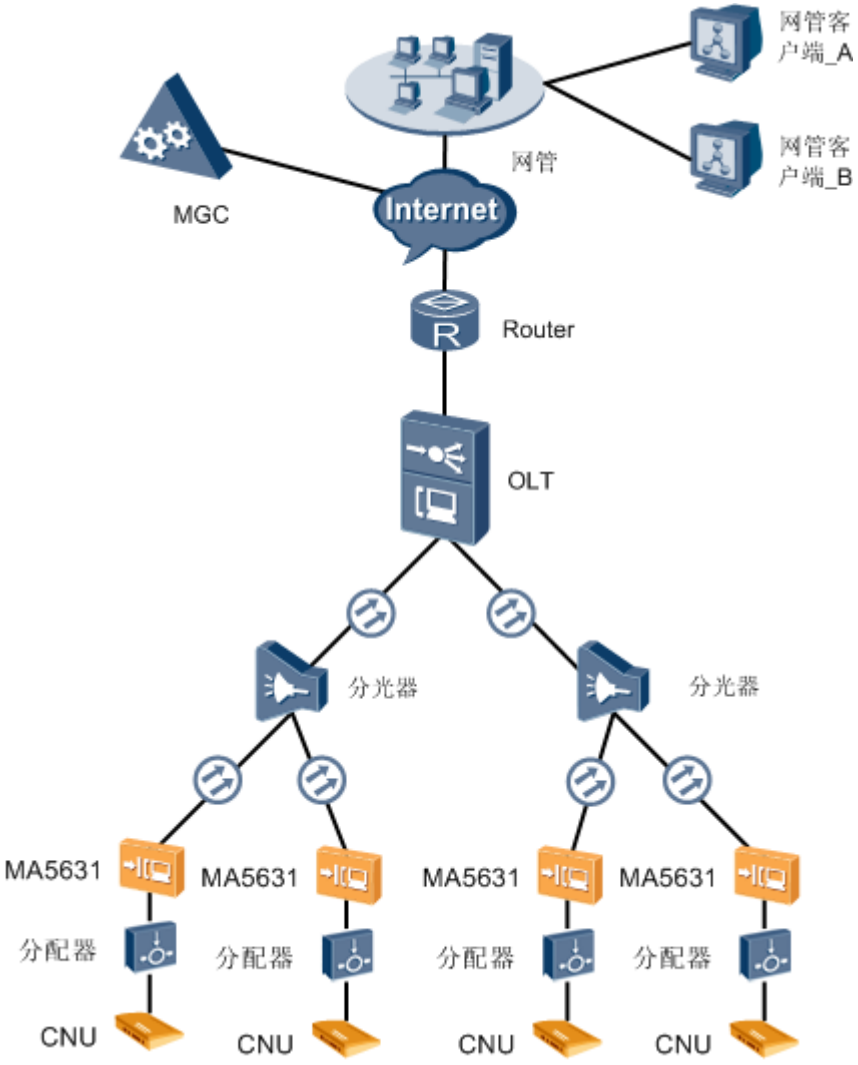
背景信息

当 MA5631 使用 EPON 上行时，使用 MAC 地址认证；使用 GPON 上行时，使用 SN 认证。

有网管的场景

有网管的场景下部署网络设备的组网图如图 1-1 所示。

图 1-1 有网管的场景下网络设备组网图



有网管的场景下部署网络设备的流程如下：

1. 调测工程师根据用户的 FTTx 数据规划，制作“预部署规划表单”并生成“资源部署表单”。
2. 调测工程师通过网管导入“资源部署表单”，实现对 MA5631 的预部署。
3. 硬件安装工程师领取 MA5631，将 MA5631 从库房运往各个站点，进行 MA5631 的硬件安装、打线、上电。
4. 硬件安装工程师完成 MA5631 的安装上电后观测 MA5631 运行情况。

   MA5631 设备有 RUN 灯和 LINK/ACT 灯：

   - RUN 灯常亮，说明 EoC 模块电源正常供电；
   - LINK/ACT 灯闪烁，说明 EoC 模块与 MA5631 主板之间传输数据；
   - LINK/ACT 灯长亮，说明 EoC 模块与 MA5631 主板连接正常。
5. 硬件安装工程师观察 RUN 灯和 LINK/ACT 灯闪烁，确认 MA5631 运行无问题，记录 MA5631 的 SN（或者 MAC 地址），上报给调测工程师。
6. 调测工程师将 MA5631 的 SN（或者 MAC 地址）、MA5631 的管理 IP 地址、物理位置建立对应关系，并通过网管绑定 MA5631 的 IP 地址和 SN（或者 MAC 地址）。
7. MA5631 上电后自动注册，OLT 将 MA5631 的管理通道参数（管理 VLAN、IP 地址、SNMP 参数）下发给 MA5631，OLT 向网管上报 Trap，告知网管有 MA5631 上线。
8. 调测工程师在网管上收到 OLT 上报的 MA5631 上线 Trap。

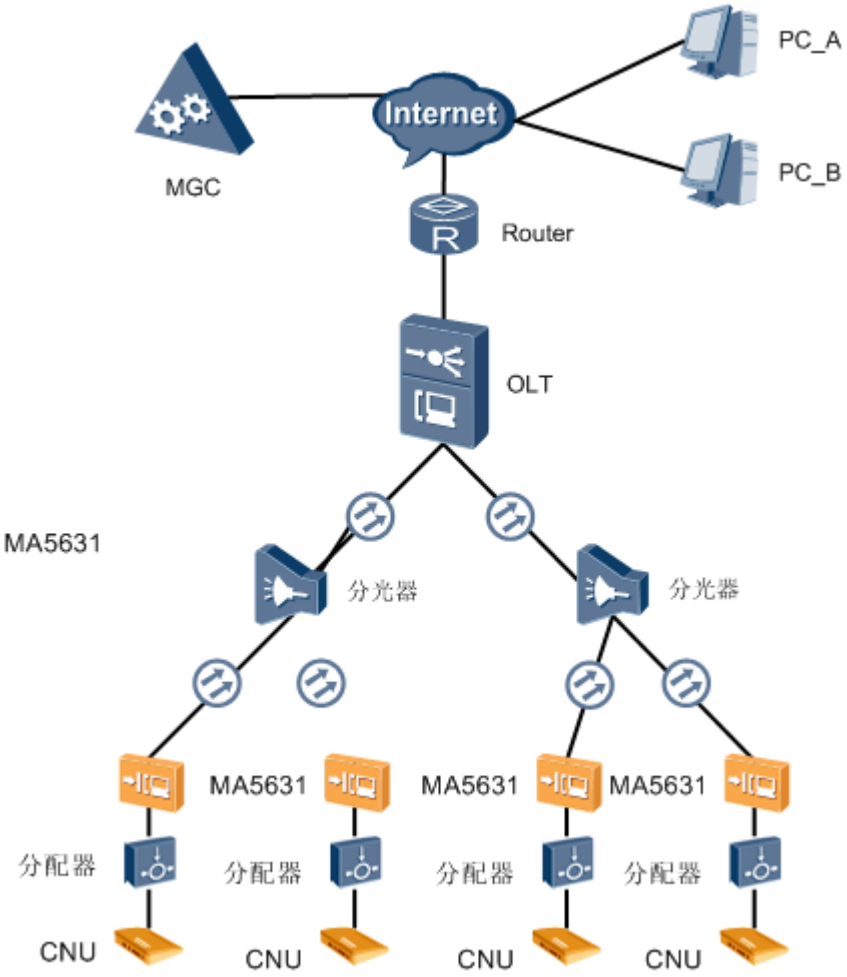
   当成功收到 MA5631 上线 Trap 时，即表示已经成功打通了 MA5631 的管理通道，之后，就可以通过网管远程对 MA5631 进行业务配置。
9. 硬件安装工程师完成 CNU 的安装上电后观测 CNU 运行情况。

   - CABLE 灯常亮，说明 CNU 与 EoC 模块连接正常；
   - CABLE 灯闪烁，说明 CNU 与 EoC 模块之间传输数据；
10. 硬件安装工程师观察 CABLE 灯闪烁，确认 CNU 运行无问题，记录 CNU 的 SN（或者 MAC 地址），上报给调测工程师。
11. CNU 上电后自动注册，注册成功后，可以对其进行业务配置。

无网管的场景

无网管的场景下部署网络设备的组网图如**图 1-2** 所示。

图 1-2 无网管的场景下网络设备组网图



无网管的场景下部署网络设备的流程如下：

1. 调测工程师根据 FTTx 业务规划和配套的 OLT 版本，完成 OLT、MA5631 的数据规划。
2. 硬件安装工程师领取 MA5631，将 MA5631 从库房运往各个站点，进行 MA5631 的硬件安装、打线、上电。
3. 硬件安装工程师完成 MA5631 的安装上电后观测 MA5631 运行情况。

   MA5631 设备有 RUN 灯和 LINK/ACT 灯：

   - RUN 灯常亮，说明 EoC 模块电源正常供电；
   - LINK/ACT 灯闪烁，说明 EoC 模块与 MA5631 主板之间传输数据；
   - LINK/ACT 灯长亮，说明 EoC 模块与 MA5631 主板连接正常。
4. 硬件安装工程师观察 RUN 灯和 LINK/ACT 灯闪烁，确认 MA5631 运行无问题，记录 MA5631 的 SN（或者 MAC 地址），上报给调测工程师。
5. 调测工程师根据 OLT、MA5631 的数据规划，完成在 OLT 侧的数据配置。
6. 调测工程师开启 OLT 的自动发现 MA5631 功能。

7. 调测工程师根据 OLT、MA5631 的数据规划及硬件安装工程师上报的 SN（或者 MAC 地址）在 OLT 中添加 MA5631。
8. 调测工程师通过 OLT 配置 MA5631 的管理 IP 地址。
9. 调测工程师通过 OLT Telnet 登录 MA5631 的管理 IP 地址，对 MA5631 进行业务配置。
10. 硬件安装工程师完成 CNU 的安装上电后观测 CNU 运行情况。
    - CABLE 灯常亮，说明 CNU 与 EoC 模块连接正常；
    - CABLE 灯闪烁，说明 CNU 与 EoC 模块之间传输数据；
11. 硬件安装工程师观察 CABLE 灯闪烁，确认 CNU 运行无问题，记录 CNU 的 SN（或者 MAC 地址），上报给调测工程师。
12. 调测工程师根据 CNU 的数据规划及硬件安装工程师上报的 SN（或者 MAC 地址）在 MA5631 上添加 CNU。
13. 调测工程师添加 CNU 正常上线后，可对 CNU 进行业务配置。

2 配置前检查

关于本章

在进行业务配置前，需要先对 MA5631 软件版本、单板状态进行检查，以保证业务的正常运行。

2.1 检查软件版本

检查当前运行的软件版本是否符合现场开局的要求。

前提条件

已经成功登录 MA5631 设备。具体操作步骤请参见“3.1 配置操作控制台”。

操作步骤

- 通过 MA5631 设备进行检查。
  1. 在普通用户模式下，使用 **display language** 命令检查系统支持的多语种信息和系统版本是否符合现场开局的需要。
  2. 在普通用户模式下，使用 **display version** 命令检查当前运行的主机软件版本、补丁版本是否符合现场开局的需要。
- 通过 iManager U2000 进行检查。
  1. 在“工作台”主界面，双击  ，进入“主拓扑”界面，点击  。
  2. 在弹出的“查找”对话框中，“查找类别”下拉列表中选择“网元”，输入需要查询的 MA5631 设备相关信息，单击“查找”。
  3. 在网元查找结果中，选择需要查询的 MA5631 设备，单击“定位”，选择“定位到网元面板”在“设备详细信息”页签中查看“设备版本”和“已激活补丁”相关信息是否符合现场开局的需要。

----结束

操作结果

- 主机软件版本、补丁版本符合现场开局的需要。
- 如果不符合，请及时联系华为技术有限公司客户服务中心，必要时进行主机软件的升级。升级操作请参见“MA5631 升级指导书”。

2.2 检查主控板和 EoC 局端模块状态

检查主控板和 EoC 局端模块是否与数据规划一致，以及运行状态是否正常。

操作步骤

- 通过 MA5631 设备进行检查。
  1. 使用 **display board** 命令检查主控板和 EoC 局端模块是否满足数据规划（即主控板类型、主控板所在槽位、EoC 局端模块类型和 EoC 局端模块所在槽位是否与数据规划一致），及主控板和 EoC 局端模块的状态。
     - 如果没有缺少 EoC 局端模块，且 EoC 局端模块状态正常，则操作结束。
     - 如果缺少数据规划中对应的 EoC 局端模块，插入对应 EoC 局端模块并使用 **board confirm** 命令确认处于自动发现态的 EoC 局端模块。再使用 **display board** 命令查询 EoC 局端模块的状态。
- 通过 iManager U2000 进行检查。

1. 在“工作台”主界面，双击  ，进入“主拓扑”界面，点击  。
2. 在弹出的“查找”对话框中，“查找类别”下拉列表中选择“单板”，输入需要查询的单板相关信息，单击“查找”。
3. 在单板查找结果中，选择需要查询的 MA5631 设备单板，单击“定位到单板”，查看 MA5631 设备单板是否满足数据规划（即单板类型、单板所在槽位是否与数据规划一致），及单板的状态。

----结束

操作结果

- 在 MA5631 设备上查询，主控板的状态（Status）主用正常，显示为“Active_normal”；EoC 局端模块的状态（Status）正常，显示为“Normal”。
- 在 iManager U2000 上进行查询，MA5631 设备的主控板和 EoC 局端模块状态正常，显示为  。

3 基础配置

关于本章

基础配置主要包括一些常用配置和公共配置，以及业务配置中的预配置。基础配置之间没有明显的逻辑关系，可以根据实际需要进行配置。

3.1 配置操作控制台
介绍 3 种通过操作控制台对 MA5631 进行维护管理的方法。

3.2 配置网管
MA5631 设备提供与“Huawei iManager U2000 网管系统”（简称 U2000）对接的功能，管理员可以通过 U2000 对设备进行维护和管理。MA5631 设备支持通过带内、带外方式与 U2000 对接。下面分别介绍基于 SNMP V1/V2c/V3 协议配置带内、带外网管的方法。

3.3 配置上行端口属性
MA5631 设备支持通过 EPON、GPON、GE 上行接口与 OLT 设备对接，通过配置上行端口属性使系统与上行设备通讯正常。

3.4 配置 EoC 局端模块线路模板
本任务配置 EoC 局端模块线路模板。

3.5 配置 VLAN
配置 VLAN 为配置业务的基础，在进行业务配置前需要保证 VLAN 已经按照实际规划完成配置。

3.6 配置 VLAN 业务模板
VLAN 相关配置集中在 VLAN 业务模板中，VLAN 与业务模板绑定后所有属性立即生效，提高配置效率。

3.7 配置 NTP 时间
配置 NTP 协议，使网络内所有设备的时钟基本保持一致，从而使设备能够提供基于统一时间的多种应用（如网络管理系统、网络计费系统）。

3.8 配置用户安全
配置保护操作用户和接入用户的安全机制，以防止用户帐号被盗和漫游或恶意用户的攻击。

3.9 配置系统安全
配置设备系统的网络安全和保护措施，以防止系统受到恶意攻击等威胁。

3.10 配置 ACL 进行报文过滤

介绍了 MA5631 设备中 ACL 分类、ACL 规则及其相关配置。

3.11 配置 QoS

通过 MA5631 设备中 QoS（Quality of Service）的相关配置操作，向用户的业务提供端到端的质量保证。

3.12 配置 H831VESC 监控

MA5631 可以通过内置的虚拟环境监控单元 H831VESC 来监控设备所处的环境状态，以下介绍 H831VESC 的配置方法。

3.1 配置操作控制台

介绍 3 种通过操作控制台对 MA5631 进行维护管理的方法。

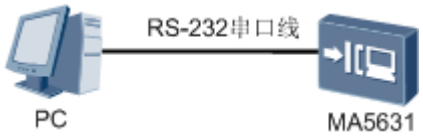
3.1.1 配置本地串口方式

操作控制台通过串口与 MA5631 设备相连并登录到 MA5631 设备，实现对设备的本地维护管理。

组网图

本地串口方式配置组网如图 3-1 所示。

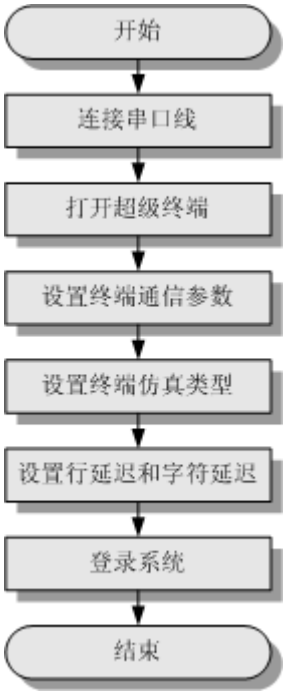
图 3-1 本地串口方式配置组网图



配置流程

本地串口方式配置流程如图 3-2 所示。

图 3-2 本地串口方式配置流程图



操作步骤

步骤 1 连接串口线。

将计算机串口通过标准的 RS-232 串口线与 MA5631 的主控板上的维护串口 CONSOLE 相连接，如图 3-1 所示。

步骤 2 打开超级终端。

1. 新建连接。

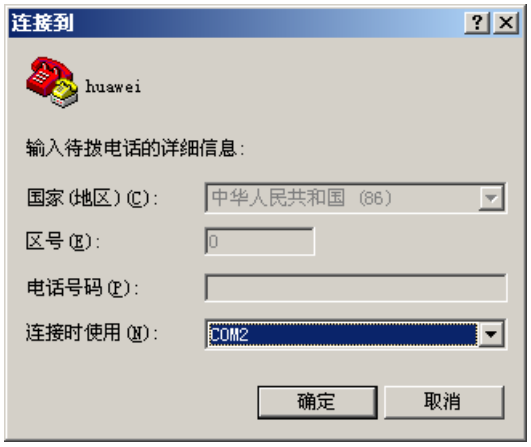
   在计算机上选择“开始 > 程序 > 附件 > 通讯 > 超级终端”，打开“连接描述”对话框，输入连接名称，如图 3-3 所示，单击“确定”。

图 3-3 新建连接

2. 设置串口。

   选择计算机上与 MA5631 实际连接的标准字符终端或 PC 终端串口号，可以选择“COM1”或者“COM2”，这里以“COM2”为例，如图 3-4 所示。单击“确定”按钮。

图 3-4 选择连接使用串口



步骤 3 设置终端通信参数。

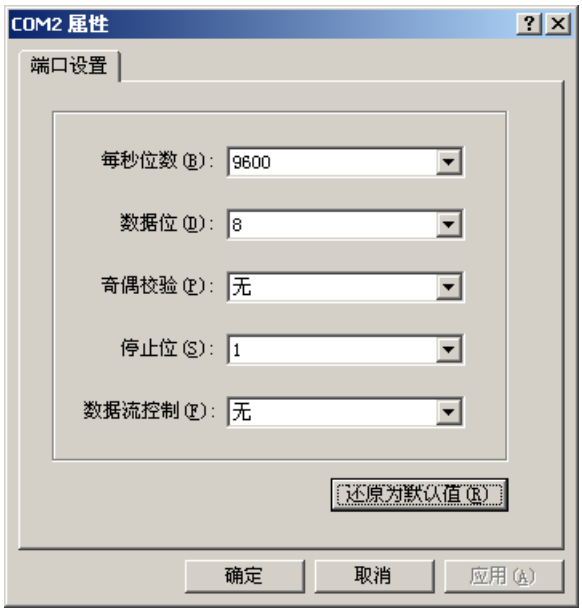
在出现的“COM2 属性”对话框中设置参数，如图 3-5 所示。这里设置为：

- 波特率为 9600bit/s
- 数据位为 8
- 奇偶校验为无
- 停止位为 1
- 数据流控制为无

说明

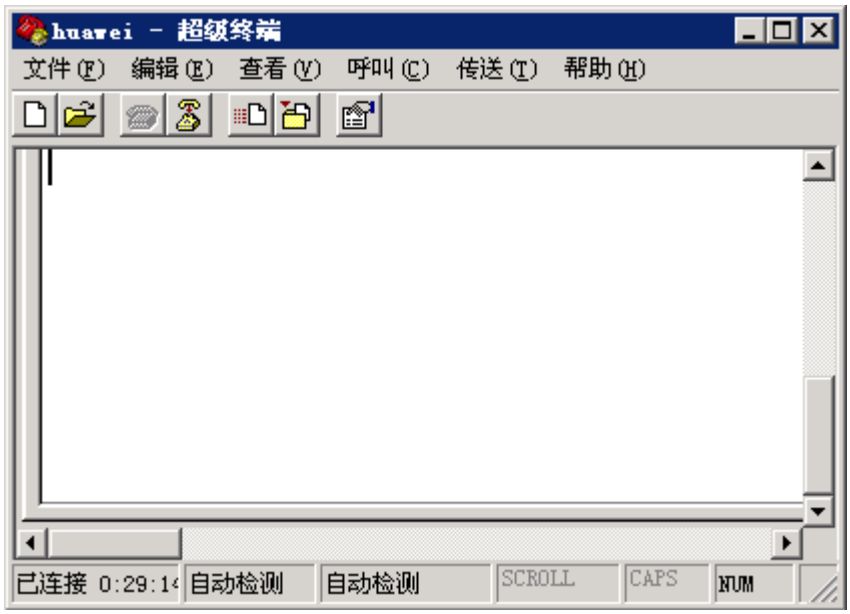
- 超级终端波特率的设置必须与 MA5631 系统的串口波特率参数一致。MA5631 默认串口波特率为 9600bit/s。
- 如果登录后超级终端界面输入字符出现乱码，一般是由于终端的波特率设置与 MA5631 系统的波特率设置不一致导致，可尝试使用其他波特率登录系统。系统支持的波特率包括 9600bit/s、19200bit/s、38400bit/s、57600bit/s、115200bit/s。

图 3-5 超级终端参数设置图



单击“确认”按钮后出现超级终端界面，如图 3-6 所示。

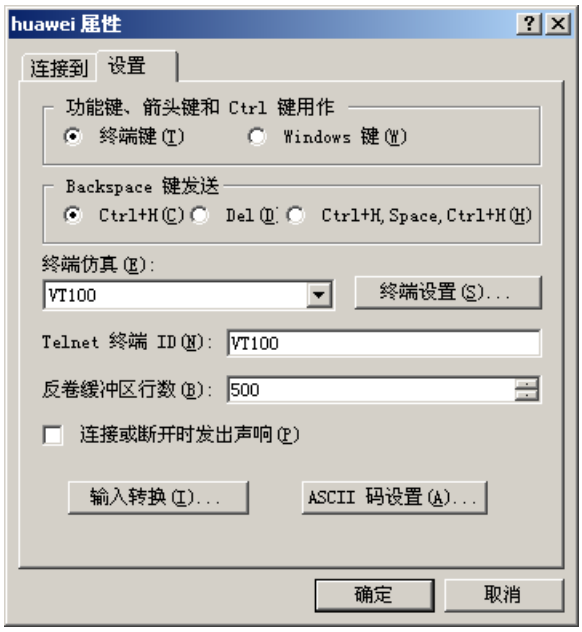
图 3-6 超级终端界面图



步骤 4 设置终端仿真类型。

在超级终端界面中选择“文件 > 属性”，在弹出的对话框的“设置”页签中选择“终端仿真”为“VT100”或“自动检测”，其他选项使用缺省值，单击“确定”保存。如图 3-7 所示。

图 3-7 终端仿真类型设置



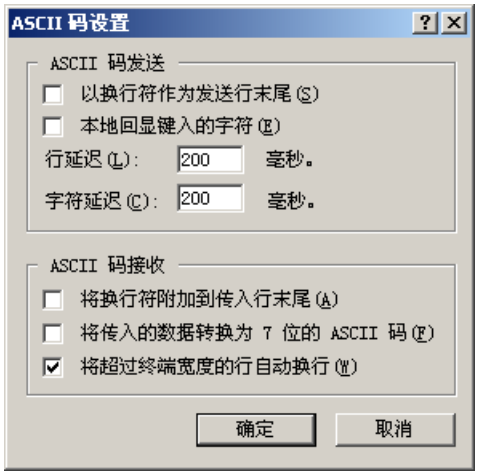
步骤 5 设置行延迟和字符延迟。

单击“ASCII 码设置”按钮，在弹出的对话框中，设置 ASCII 码发送“行延迟”为 200ms，“字符延迟”为 200ms，其他选项使用缺省值，单击“确定”保存。如图 3-8 所示。

说明

- 系统缺省“行延迟”为 0，“字符延迟”设置为 0。
- 当向超级终端粘贴文本时“字符延迟”将控制每个字符的发送速度。“行延迟”将控制每行的间隔时间。延迟时间太短将会造成缺漏字符的现象，若粘贴文本时显示不正常，请注意修改此值。

图 3-8 ASCII 码设置



----结束

操作结果

在超级终端界面中敲击回车键，出现输入用户名的提示符。根据提示输入用户名和密码进行用户注册（系统缺省的超级用户名为：**root**，密码为：**mduadmin**），直到出现命令行提示符。CLI(Command Line Interface)使用的基本信息，请参见“CLI 操作特点”。

若登录不成功，请单击操作界面上的图标后再单击图标。若还无法登录，请回到步骤 1 检查参数设置或物理连接是否正确，确认设置正确后再重新登录。

3.1.2 配置带外管理接口方式

操作控制台通过 MA5631 的带外管理接口登录到 MA5631 并进行维护管理。

前提条件

- 已经通过本地串口方式登录系统。具体配置过程请参见 3.1.1 配置本地串口方式。
- 已经正确配置操作控制台 IP 地址。

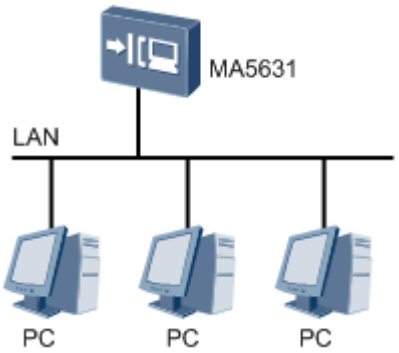
说明

以下操作中在 MA5631 设备上的配置需要通过本地串口配置完成。

组网图—局域网方式

Telnet 方式通过局域网进行带外管理配置组网如图 3-9 所示。

图 3-9 Telnet 方式通过局域网进行带外管理配置组网图



在此配置组网图中，MA5631 设备维护网口的 IP 地址与操作控制台的 IP 地址在同一网段；也可以将操作控制台的网口与 MA5631 设备主控板的维护网口直接连接，对设备进行带外管理。

数据规划—局域网方式

Telnet 方式通过局域网进行带外管理数据规划如表 3-1 所示。

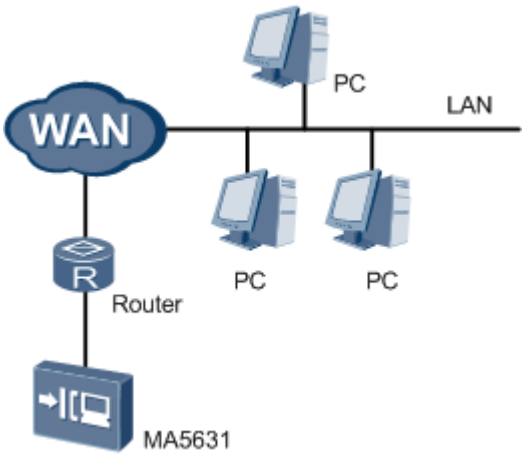
表 3-1 Telnet 方式通过局域网进行带外管理数据规划表

配置项	数据
MA5631 维护网口	IP 地址：10.10.20.2/24
操作控制台网口	IP 地址：10.10.20.3/24

组网图—广域网方式

Telnet 方式通过广域网进行带外管理配置组网如图 3-10 所示。

图 3-10 Telnet 方式通过广域网进行带外管理配置组网图



在此配置组网图中 MA5631 通过维护网口，接入到广域网中，操作控制台可远程对 MA5631 进行维护、管理。

数据规划—广域网方式

Telnet 方式通过广域网进行带外管理数据规划如表 3-2 所示。

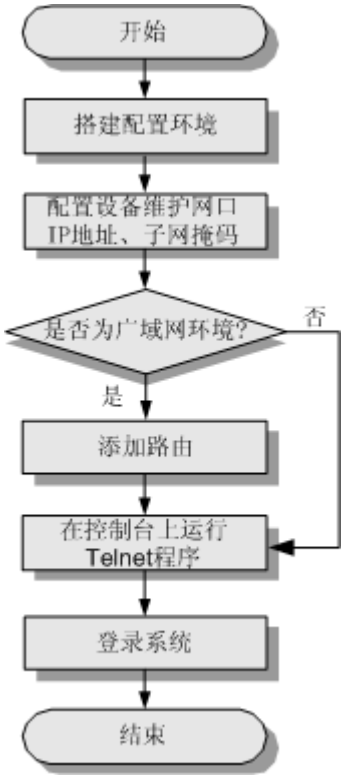
表 3-2 Telnet 方式通过广域网进行带外管理数据规划表

配置项	数据
MA5631 维护网口	IP 地址：10.10.20.2/24
操作控制台网口	IP 地址：10.10.21.3/24
路由器接 MA5631 侧的接口	IP 地址：10.10.20.254/24

配置流程

Telnet 方式通过带外管理接口登录配置流程如图 3-11 所示。

图 3-11 Telnet 方式通过带外管理接口登录配置流程图



操作步骤

步骤 1 搭建配置环境。

根据实际需要和条件，如图 3-9 或图 3-10 所示搭建配置环境。

步骤 2 在 Meth 模式下，使用 **ip address** 命令配置 MA5631 设备维护网口 IP 地址、子网掩码。

说明

维护网口的 IP 地址默认为 10.11.104.2，子网掩码为 255.255.255.0，可以根据实际组网规划设置维护网口的 IP 地址。

```
huawei(config)#interface meth 0
huawei(config-if-meth0)#ip address 10.10.20.2 24
```

步骤 3 添加路由。

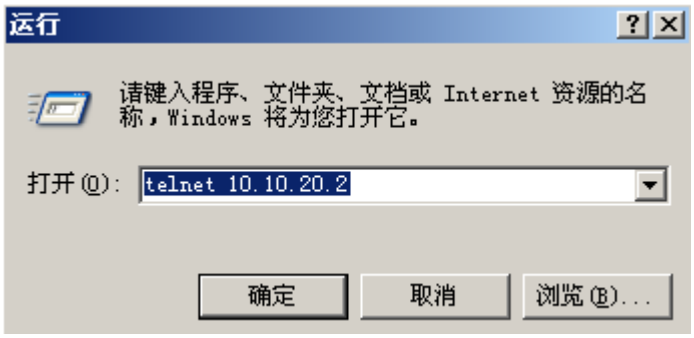
- 如果如图 3-9 所示搭建局域网本地管理环境，不需要添加路由。
- 如果如图 3-10 所示搭建广域网远程管理环境，需要使用 **ip route-static** 命令添加下一跳路由。

```
huawei(config-if-meth0)#quit
huawei(config)#ip route-static 10.10.21.0 24 10.10.20.254
```

步骤 4 在控制台上运行 Telnet 程序。

在控制台上选择“开始>运行”，在“打开”地址栏里输入 **telnet 10.10.20.2**（10.10.20.2 为 MA5631 维护网口 IP 地址），如图 3-12 所示（以 Windows 操作系统为例）。单击“确定”运行 Telnet 应用程序，弹出远程登录的对话框。

图 3-12 运行 Telnet 程序界面



步骤 5 登录 MA5631 系统。

在弹出的远程登录对话框中输入用户名和密码。系统缺省的超级用户名为：**root**，密码为：**mduadmin**。成功登录系统后会给出提示信息，如下所示。

```
>>User name:root
>>User password:


  Huawei Integrated Access Software (MA5631).

  Copyright(C) Huawei Technologies Co., Ltd. 2002-2010. All rights reserved.
```

----结束

操作结果

用户登录系统后，可以对 MA5631 设备进行维护、管理。CLI 使用的基本信息，请参见“CLI 操作特点”。

3.1.3 配置带内管理接口方式（PON 上行）

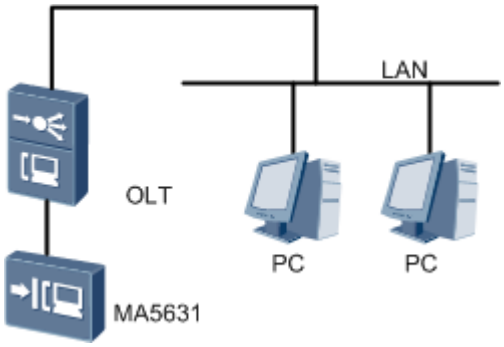
通过本任务实现操作控制台通过 OLT 登录到 MA5631 设备并进行维护管理。

前提条件

- MA5631 设备与 OLT 设备物理连接正常。
- 已经正确配置操作控制台 IP 地址。

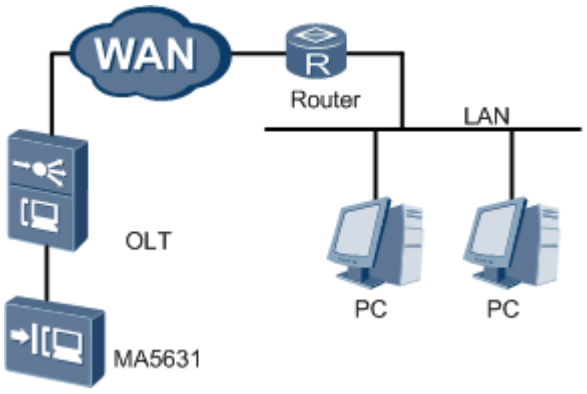
组网图—局域网方式

图 3-13 通过局域网方式 PON 上行进行带内管理配置组网图



组网图—广域网方式

图 3-14 通过广域网方式 PON 上行进行带内管理配置组网图



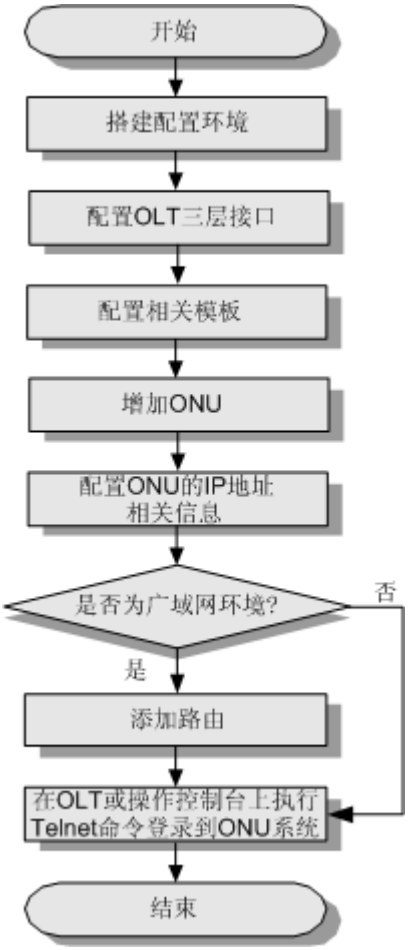
配置流程

MA5631 设备通过 PON 上行方式带内管理配置流程如图 3-15 所示。

说明

PON 上行方式下 MA5631 设备和 OLT 设备对接，实现带内管理。所需配置均在 OLT 上进行，本文档仅给出 OLT 设备的配置流程，具体的配置过程请参见 OLT 对应配置手册。

图 3-15 通过 PON 上行方式带内管理配置流程图



操作结果

用户通过 OLT 或操作控制台登录 MA5631 系统后，可以对其进行配置。CLI 使用的基本信息，请参见“CLI 操作特点”。

3.1.4 配置带内管理接口方式（GE 上行）

通过本任务实现操作控制台通过 MA5631 设备的上行端口（带内管理接口）以 Telnet 方式登录到 MA5631 设备并进行维护和管理。

前提条件

- 已经通过本地串口方式登录系统。具体配置过程请参见 **3.1.1 配置本地串口方式**。
- 已经正确配置操作控制台 IP 地址。

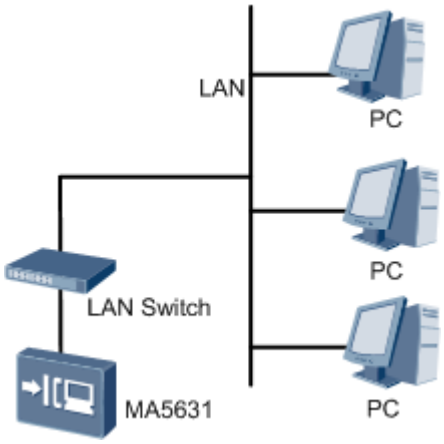
说明

以下操作中在 MA5631 设备上的配置需要通过本地串口配置完成。

组网图—局域网方式

Telnet 方式通过局域网进行带内管理配置组网如图 3-16 所示。

图 3-16 Telnet 方式通过局域网进行带内管理配置组网图



数据规划—局域网方式

Telnet 方式通过局域网进行带内管理数据规划如表 3-3 所示。

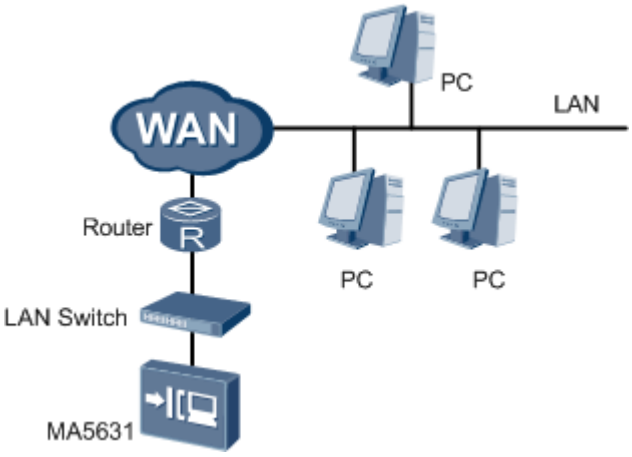
表 3-3 Telnet 方式通过局域网进行带内管理数据规划表

配置项	数据
MA5631 上行端口	● VLAN ID：30 ● 端口号：0/0/0 ● IP 地址：10.10.20.2/24
操作控制台网口	IP 地址：10.10.20.3/24

组网图—广域网方式

Telnet 方式通过广域网进行带内管理配置组网如图 3-17 所示。

图 3-17 Telnet 方式通过广域网进行带内管理配置组网图



数据规划—广域网方式

Telnet 方式通过广域网进行带内管理数据规划如**表 3-4** 所示。

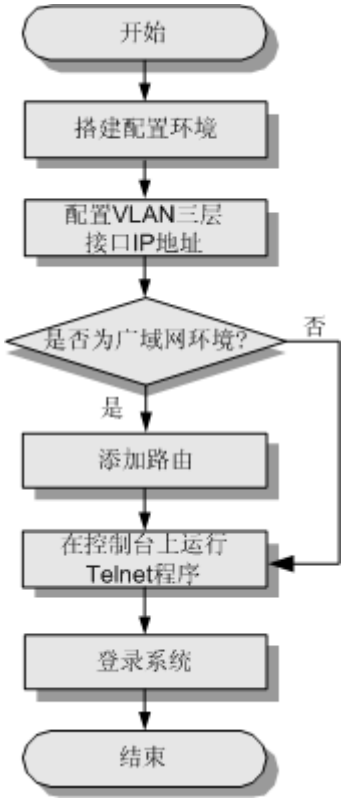
表 3-4 Telnet 方式通过广域网进行带内管理数据规划表

配置项	数据
MA5631 上行端口	● VLAN ID：30 ● 端口号：0/0/0 ● IP 地址：10.10.20.2/24
操作控制台网口	IP 地址：10.10.21.3/24
LAN Switch 接路由器侧接口	IP 地址：10.10.20.3/24

配置流程

Telnet 方式通过带内管理接口登录配置流程如**图 3-18** 所示。

图 3-18 Telnet 方式通过带内管理接口登录配置流程图



操作步骤

步骤 1 搭建配置环境。

根据实际需要和条件，如图 3-16 或图 3-17 所示搭建配置环境。

步骤 2 配置 VLAN 三层接口 IP 地址。

1. 使用 **vlan** 命令创建 VLAN。

```
huawei(config)#vlan 30 smart
```

2. 使用 **port vlan** 命令添加上行端口。

```
huawei(config)#port vlan 30 0/0 1
```

3. 在 VLANIF 模式下，使用 **ip address** 命令设置 VLAN 三层接口的 IP 地址和子网掩码。

```
huawei(config)#interface vlanif 30
huawei(config-if-vlanif30)#ip address 10.10.20.2 255.255.255.0
```

步骤 3 添加路由。

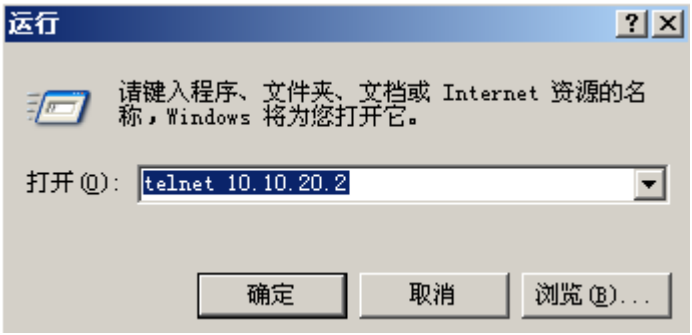
- 如果如图 3-16 所示搭建局域网本地管理环境，不需要添加路由。
- 如果如图 3-17 所示搭建广域网远程管理环境，需要使用 **ip route-static** 命令添加下一跳路由。

```
huawei(config-if-vlanif30)#quit
huawei(config)#ip route-static 10.10.21.0 24 10.10.20.3
```

步骤 4 运行 Telnet 程序。

在控制台上选择“开始>运行”，在“打开”地址栏里输入 **telnet 10.10.20.2**（10.10.20.2 为 MA5631 设备 VLAN 三层接口 IP 地址），如图 3-19 所示（以 Windows 操作系统为例）。弹出远程登录的对话框。

图 3-19 运行 Telnet 程序界面



步骤 5 登录 MA5631 系统。

在弹出的远程登录对话框中输入用户名和密码。系统缺省的超级用户名为：**root**，密码为：**mduadmin**。成功登录系统后会给出提示信息，如下所示。

```
>>User name:root
>>User password:


  Huawei Integrated Access Software (MA5631).

  Copyright(C) Huawei Technologies Co., Ltd. 2002-2010. All rights reserved.
```

----结束

操作结果

用户登录系统后，可以对 MA5631 设备进行维护、管理。CLI 使用的基本信息，请参见“CLI 操作特点”。

3.2 配置网管

MA5631 设备提供与“Huawei iManager U2000 网管系统”（简称 U2000）对接的功能，管理员可以通过 U2000 对设备进行维护和管理。MA5631 设备支持通过带内、带外方式与 U2000 对接。下面分别介绍基于 SNMP V1/V2c/V3 协议配置带内、带外网管的方法。

3.2.1 配置网管（基于 SNMP V1 协议）

基于 SNMP V1 协议时，MA5631 设备支持带内、带外两种组网方式与网管连接。

前提条件

- 采用带外组网方式与网管对接，已配置通信端口-维护网口。详细操作请参见 **3.1.2 配置带外管理接口方式**。
- 采用 PON 上行带内组网方式与网管对接，已配置通信端口-PON 上行端口。详细操作请参见 **3.1.3 配置带内管理接口方式（PON 上行）**。

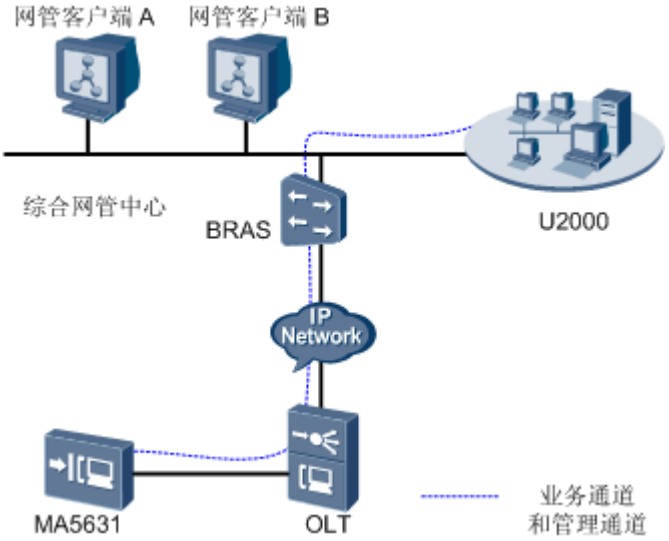
- 采用 GE 上行带内组网方式与网管对接，已配置通信端口-GE 上行端口。详细操作请参见 **3.1.4 配置带内管理接口方式（GE 上行）**。

组网图-带内网管组网方式

如**图 3-20** 所示，SNMP 协议在业务通道上传送，业务通道和管理通道相同，通过上行端口实现带内网管管理。

- MA5631 设备可以采用 GPON/EPON 上行接口。
- MA5631 设备与 U2000 之间采用静态路由。

图 3-20 带内网管组网示意图

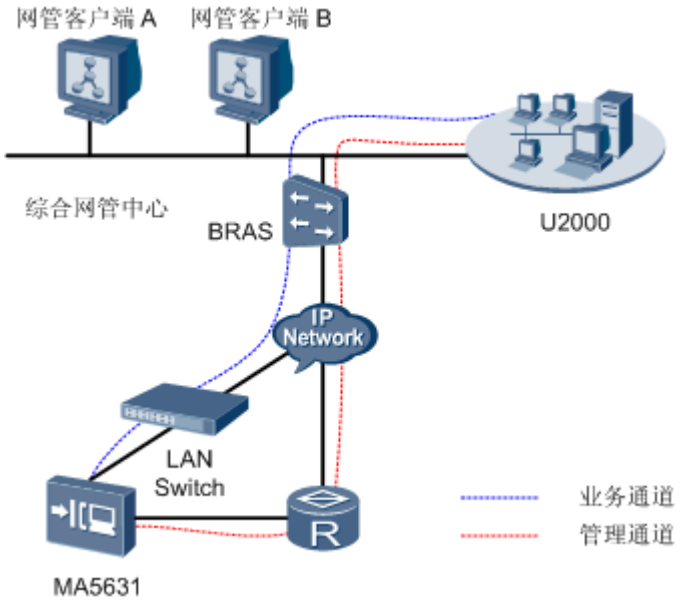


组网图-带外网管组网方式

如**图 3-21** 所示，SNMP 协议在管理通道上传送，业务通道和管理通道分离，通过维护网口实现带外网管管理。

- MA5631 设备与 U2000 之间采用静态路由。

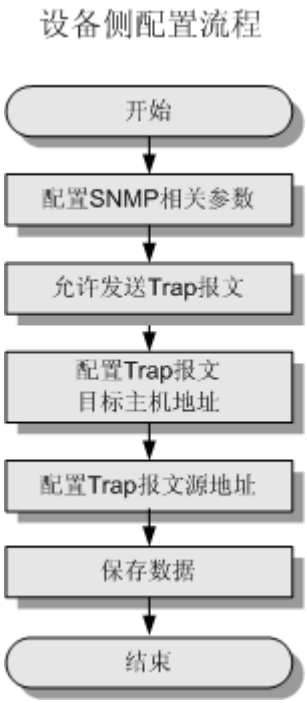
图 3-21 带外网管组网示意图



配置流程

配置网管管理的流程如图 3-22 所示。

图 3-22 配置网管的流程图



操作步骤

- 设备侧配置过程。

1. 配置 SNMP 相关参数。

(1) 配置团体名和访问权限。

使用 **snmp-agent community** 命令配置团体名和访问权限。

说明

读团体名为 **public**，写团体名为 **private**。

读团体名、写团体名的配置与 U2000 侧的配置相同。

```
huawei(config)#snmp-agent community read public
huawei(config)#snmp-agent community write private
```

(2) （可选）设置管理员信息。

使用 **snmp-agent sys-info** 命令设置 SNMP Agent 管理员联系信息、物理位置信息。

管理员联系方式为 HW-075528780808、设备位置信息为 Shenzhen_China。

```
huawei(config)#snmp-agent sys-info contact HW-075528780808
huawei(config)#snmp-agent sys-info location Shenzhen_China
```

(3) 设置 SNMP 版本信息。

使用 **snmp-agent sys-info** 命令设置支持的 SNMP 协议版本。

```
huawei(config)#snmp-agent sys-info version v1
```

说明

SNMP 版本的配置要与 U2000 侧的配置相同。

2. 允许发送 Trap 报文。

使用 **snmp-agent trap enable** 命令使能设备对网管发送 Trap 报文的功能。

```
huawei(config)#snmp-agent trap enable standard
```

3. 配置 Trap 报文目标主机地址。

使用 **snmp-agent target-host** 命令用于设置 Trap 报文目的主机的 IP 地址。

设置主机名为 huawei，主机 IP 地址为 10.10.1.10/24（U2000 网管 IP 地址），Trap 报文目的主机参数名为 ABC，SNMP 协议为 V1，参数安全名为 private（参数安全名为 SNMP 团体名）。

```
huawei(config)#snmp-agent target-host trap-hostname huawei address 10.10.1.10 trap-paramsname ABC
huawei(config)#snmp-agent target-host trap-paramsname ABC v1 securityname private
```

4. 配置 Trap 报文源地址。

使用 **snmp-agent trap source** 命令配置 Trap 报文的源地址。

- 带内组网方式连接网管，将上行接口 IP 地址作为发送 Trap 报文的源地址。
- 带外组网方式连接网管，将维护网口 IP 地址作为发送 Trap 报文的源地址。

说明

本例中采用带外组网方式。

```
huawei(config)#snmp-agent trap source meth 0
```

5. 保存数据。

使用 **save** 命令保存数据。

```
huawei(config)#save
```

- 网管侧配置过程。

  说明

  使用带内网管组网方式时，只需要在 MA5631 上进行配置，网管侧可以通过 OLT 自动发现 MA5631，不用执行本步骤。

  使用带外网管组网方式时，需要按照本步骤在网管侧进行配置。

  1. 添加网管至设备的路由。

     配置网管服务器到网段 10.50.1.0/24 的路由网关为 10.10.1.1。

     - 在 solaris 操作系统下

       使用 **route add 10.50.1.0 10.10.1.1** 命令添加路由。

       使用 **netstat -r** 命令查询当前的路由表信息。

     - 在 windows 操作系统下

       使用 **route add 10.50.1.0 mask 255.255.255.0 10.10.1.1** 命令添加路由。

       使用 **route print** 命令查询当前的路由表信息。

     说明

     当带外网管接口的 IP 地址与 U2000 的 IP 地址在同一子网时，无需配置路由信息。

  2. 登录 U2000 系统。
  3. 配置 SNMP 相关参数。

     说明

     系统存在一个名为 default 的缺省模板，在本例中使用此缺省模板。如果需要配置新的模板，请按照以下步骤执行。

     (1) 在主菜单中选择“系统 > 网元通讯参数 > 网元 SNMP 参数模板管理(S)...”。

     (2) 在弹出的“缺省访问协议参数”，选择“SNMP v1 参数”页签，单击“增加”。

     (3) 设置模板名称，其他参数根据规划设置。

     (4) 单击“确定”，完成 SNMP 参数的配置。

  4. 增加设备。

     (1) 在主拓扑视图中单击右键，选择“新建 > 网元”。

     (2) 在弹出的对话框中设置相关参数。

说明

- IP 地址为 MA5631 的管理 IP 地址。
- SNMP 参数根据对接协议的类型进行选择，此处以 SNMP V1 default 模板为例。可以根据实际规划选择对应模板。

(3) 单击“确定”。需要数秒或十几分钟上载设备数据，读取设备相关数据完毕后系统会自动刷新显示该设备图标。

----结束

操作结果

通过 U2000 可以对 MA5631 设备进行维护管理。

配置脚本

配置带外网管（设备侧）的脚本

```
snmp-agent community read public
snmp-agent community write private
snmp-agent sys-info contact HW-075528780808
snmp-agent sys-info location Shenzhen_China
snmp-agent sys-info version v1
snmp-agent trap enable standard
snmp-agent target-host trap-hostname huawei address 10.10.1.10 trap-paramsname ABC
snmp-agent target-host trap-paramsname ABC v1 securityname private
snmp-agent trap source meth 0
save
```

配置带内网管（设备侧）的脚本：上行接口的管理 VLAN ID 为 30

```
snmp-agent community read public
snmp-agent community write private
snmp-agent sys-info contact HW-075528780808
snmp-agent sys-info location Shenzhen_China
snmp-agent sys-info version v1
snmp-agent trap enable standard
snmp-agent target-host trap-hostname huawei address 10.10.1.10 trap-paramsname ABC
snmp-agent target-host trap-paramsname ABC v1 securityname private
snmp-agent trap source vlanif 30
save
```

3.2.2 配置网管（基于 SNMP V2c 协议）

基于 SNMP V2c 协议时，MA5631 设备支持带内、带外两种组网方式与网管连接。

前提条件

- 采用带外组网方式与网管对接，已配置通信端口-维护网口。详细操作请参见 **3.1.2 配置带外管理接口方式**。
- 采用 PON 上行带内组网方式与网管对接，已配置通信端口-PON 上行端口。详细操作请参见 **3.1.3 配置带内管理接口方式（PON 上行）**。
- 采用 GE 上行带内组网方式与网管对接，已配置通信端口-GE 上行端口。详细操作请参见 **3.1.4 配置带内管理接口方式（GE 上行）**。

组网图-带内网管组网方式

如 **3.2.1 配置网管（基于 SNMP V1 协议）**中的“带内网管组网示意图”所示，SNMP 协议在业务通道上传送，业务通道和管理通道相同，通过上行端口实现带内网管管理。

- MA5631 设备可以采用 GPON/EPON 上行接口。
- MA5631 设备与 U2000 之间采用静态路由。

组网图-带外网管组网方式

如 **3.2.1 配置网管（基于 SNMP V1 协议）**中的“带外网管组网示意图”所示，SNMP 协议在管理通道上传送，业务通道和管理通道分离，通过维护网口实现带外网管管理。

- MA5631 设备与 U2000 之间采用静态路由。

配置流程

配置网管管理的流程如 **3.2.1 配置网管（基于 SNMP V1 协议）**中的“配置网管的流程图”所示。

操作步骤

- 设备侧配置过程。
  1. 配置 SNMP 相关参数。
     (1) 配置团体名和访问权限。
     使用 **snmp-agent community** 命令配置团体名和访问权限。
     说明
     读团体名为 **public**，写团体名为 **private**。
     读团体名、写团体名的配置与 U2000 侧的配置相同。

```
huawei(config)#snmp-agent community read public
huawei(config)#snmp-agent community write private
```

     (2) （可选）设置管理员信息。
     使用 **snmp-agent sys-info** 命令设置 SNMP Agent 管理员联系信息、物理位置信息。
     管理员联系方式为 HW-075528780808、设备位置信息为 XA_China。

```
huawei(config)#snmp-agent sys-info contact HW-075528780808
huawei(config)#snmp-agent sys-info location XA_China
```

(3) 设置 SNMP 版本信息。

使用 **snmp-agent sys-info** 命令设置支持的 SNMP 协议版本。

```
huawei(config)#snmp-agent sys-info version v2c
```

说明

SNMP 版本的配置要与 U2000 侧的配置相同。

2. 允许发送 Trap 报文。

使用 **snmp-agent trap enable** 命令使能设备对网管发送 Trap 报文的功能。

```
huawei(config)#snmp-agent trap enable standard
```

3. 配置 Trap 报文目标主机地址。

使用命令用于设置 Trap 报文目的主机的 IP 地址。

设置主机名为 huawei，主机 IP 地址为 10.10.1.10/24（U2000 网管 IP 地址），Trap 报文目的主机参数名为 ABC，SNMP 协议为 V2c，参数安全名为 private（参数安全名为 SNMP 团体名）。

```
huawei(config)#snmp-agent target-host trap-hostname huawei address 10.10.1.10 trap-paramsname ABC
huawei(config)#snmp-agent target-host trap-paramsname ABC v2c securityname private
```

4. 配置 Trap 报文源地址。

使用 **snmp-agent trap source** 命令配置 Trap 报文的源地址。

- 带内组网方式连接网管，将上行接口 IP 地址作为发送 Trap 报文的源地址。
- 带外组网方式连接网管，将维护网口 IP 地址作为发送 Trap 报文的源地址。

说明

本例中采用带外组网方式。

```
huawei(config)#snmp-agent trap source meth 0
```

5. 保存数据。

使用 **save** 命令保存数据。

```
huawei(config)#save
```

- 网管侧配置过程。

说明

使用带内网管组网方式时，只需要在 MA5631 上进行配置，网管侧可以通过 OLT 自动发现 MA5631，不用执行本步骤。

使用带外网管组网方式时，需要按照本步骤在网管侧进行配置。

1. 添加网管至设备的路由。

配置网管服务器到网段 10.50.1.0/24 的路由网关为 10.10.1.1。

- 在 solaris 操作系统下

  使用 **route add 10.50.1.0 10.10.1.1** 命令添加路由。

  使用 **netstat -r** 命令查询当前的路由表信息。

- 在 windows 操作系统下

  使用 **route add 10.50.1.0 mask 255.255.255.0 10.10.1.1** 命令添加路由。

  使用 **route print** 命令查询当前的路由表信息。

说明

当带外网管接口的 IP 地址与 U2000 的 IP 地址在同一子网时，无需配置路由信息。

2. 登陆 U2000 系统。
3. 配置 SNMP 相关参数。

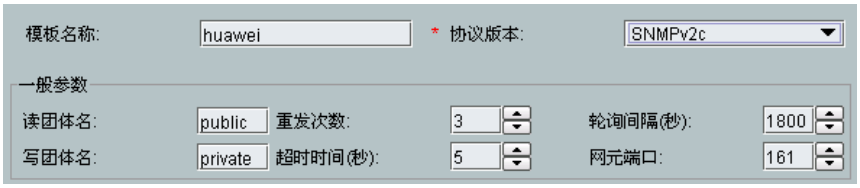
说明

系统存在一个名为 default 的缺省模板，在本例中使用此缺省模板。如果需要配置新的模板，请按照以下步骤执行。

(1) 在主菜单中选择“系统 > 网元通讯参数 > 网元 SNMP 参数模板管理(S)...”。

(2) 在弹出的“缺省访问协议参数”，选择“SNMP v2 参数”页签，单击“增加”。

(3) 设置模板名称，其他参数根据规划设置。

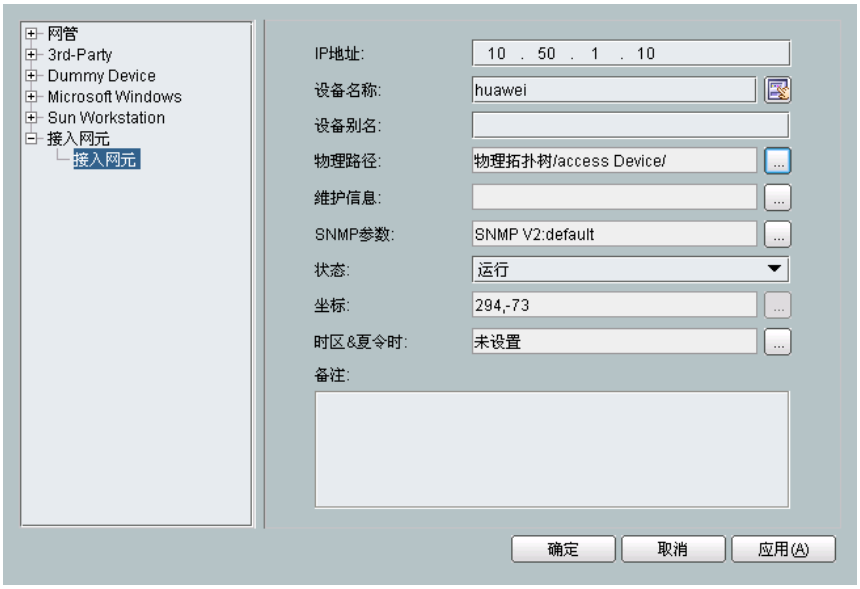


(4) 单击“确定”，完成 SNMP 参数的配置。

4. 增加设备。

(1) 在主拓扑视图中单击右键，选择“新建 > 网元”。

(2) 在弹出的对话框中设置相关参数。



说明

- IP 地址为 MA5631 的管理 IP 地址。
- SNMP 参数根据对接协议的类型进行选择，此处以 SNMP V2c default 模板为例。可以根据实际规划选择对应模板。

(3) 单击“确定”。需要数秒或十几分钟上载设备数据，读取设备相关数据完毕后系统会自动刷新显示该设备图标。

----结束

操作结果

通过 U2000 可以对 MA5631 设备进行维护管理。

配置脚本

配置带外网管（设备侧）的脚本

```
snmp-agent community read public
snmp-agent community write private
snmp-agent sys-info contact HW-075528780808
snmp-agent sys-info location Shenzhen_China
snmp-agent sys-info version v2c
snmp-agent trap enable standard
snmp-agent target-host trap-hostname huawei address 10.10.1.10 trap-paramsname ABC
snmp-agent target-host trap-paramsname ABC v2c securityname private
snmp-agent trap source meth 0
save
```

配置带内网管（设备侧）的脚本：上行接口的管理 VLAN ID 为 30

```
snmp-agent community read public
snmp-agent community write private
snmp-agent sys-info contact HW-075528780808
snmp-agent sys-info location Shenzhen_China
snmp-agent sys-info version v2c
snmp-agent trap enable standard
snmp-agent target-host trap-hostname huawei address 10.10.1.10 trap-paramsname ABC
snmp-agent target-host trap-paramsname ABC v2c securityname private
snmp-agent trap source vlanif 30
save
```

3.2.3 配置网管（基于 SNMP V3 协议）

基于 SNMP V3 协议时，MA5631 设备支持带内、带外两种组网方式与网管连接。

前提条件

- 采用带外组网方式与网管对接，已配置通信端口-维护网口。详细操作请参见 **3.1.2 配置带外管理接口方式**。
- 采用 PON 上行带内组网方式与网管对接，已配置通信端口-PON 上行端口。详细操作请参见 **3.1.3 配置带内管理接口方式（PON 上行）**。
- 采用 GE 上行带内组网方式与网管对接，已配置通信端口-GE 上行端口。详细操作请参见 **3.1.4 配置带内管理接口方式（GE 上行）**。

组网图-带内网管组网方式

如 **3.2.1 配置网管（基于 SNMP V1 协议）**中的“带内网管组网示意图”所示，SNMP 协议在业务通道上传送，业务通道和管理通道相同，通过上行端口实现带内网管管理。

- MA5631 设备可以采用 GPON/EPON 上行接口。
- MA5631 设备与 U2000 之间采用静态路由。

组网图-带外网管组网方式

如 **3.2.1 配置网管（基于 SNMP V1 协议）**中的“带外网管组网示意图”所示，SNMP 协议在管理通道上传送，业务通道和管理通道分离，通过维护网口实现带外网管管理。

- MA5631 设备与 U2000 之间采用静态路由。

配置流程

配置网管管理的流程如 **3.2.1 配置网管（基于 SNMP V1 协议）**中的“配置网管的流程图”所示。

操作步骤

- 设备侧配置过程。

1. 配置 SNMP 相关参数。

(1) 配置 SNMP 用户、组和视图。

用户名为 user1，组名为 group1，用户鉴别模式为 MD5，鉴权密码为 authkey123，用户加密模式为 des56，加密密码为 prikey123，读、写视图名都为 hardy，视图包含 internet 子树。

```
huawei(config)#snmp-agent usm-user v3 user1 group1 authentication-mode md5
authkey123 privacy-mode des56 prikey123
huawei(config)#snmp-agent group v3 group1 privacy read-view hardy write-view hardy
huawei(config)#snmp-agent mib-view hardy include internet
```

(2) （可选）设置管理员信息、设备信息。

使用 **snmp-agent sys-info** 命令设置 SNMP Agent 管理员联系信息、物理位置信息。

管理员联系方式为 HW-075528780808、设备位置信息为 Shenzhen_China。

```
huawei(config)#snmp-agent sys-info contact HW-075528780808
huawei(config)#snmp-agent sys-info location Shenzhen_China
```

(3) （可选）配置 SNMP 实体引擎 ID。

使用 **snmp-agent local-engineid** 配置 SNMP 环境引擎 ID 为 0123456789。

说明

SNMP 环境引擎 ID 配置需要与 U2000 侧的配置相同。

```
huawei(config)#snmp-agent local-engineid 0123456789
  Info: Modify the local-engineid will disable the configured SNMPv3 user, all
users must be reconfigured, proceed? (y/n)[n]:y
```

(4) 设置 SNMP 版本信息。

使用 **snmp-agent sys-info** 命令设置支持的 SNMP 协议版本。

```
huawei(config)#snmp-agent sys-info version v3
```

说明

SNMP 版本的配置要与 U2000 侧的配置相同。

2. 允许发送 Trap 报文。

使用 **snmp-agent trap enable** 命令使能设备对网管发送 Trap 报文的功能。

```
huawei(config)#snmp-agent trap enable standard
```

3. 配置 Trap 报文目标主机地址。

使用 **snmp-agent target-host** 命令用于设置 Trap 报文目的主机的 IP 地址。

主机名为 huawei，主机 IP 地址为 10.10.1.10/24（U2000 网管 IP 地址），Trap 报文目的主机参数名为 ABC，SNMP 协议为 V3，参数安全名为 user1（SNMP 协议版本为 V3 时，参数安全名为 USM 用户名），对报文认证并加密。

```
huawei(config)#snmp-agent target-host trap-hostname huawei address 10.10.1.10 trap-paramsname ABC
huawei(config)#snmp-agent target-host trap-paramsname ABC v3 securityname user1 privacy
```

4. 配置 Trap 报文源地址。

   使用 **snmp-agent trap source** 命令配置 Trap 报文的源地址。

   - 带内组网方式连接网管，将上行接口 IP 地址作为发送 Trap 报文的源地址。
   - 带外组网方式连接网管，将维护网口 IP 地址作为发送 Trap 报文的源地址。

   说明

   本例中采用带外组网方式。

```
huawei(config)#snmp-agent trap source meth 0
```

5. 保存数据。

   使用 **save** 命令保存数据。

```
huawei(config)#save
```

- 网管侧配置过程。

1. 添加网管至设备的路由。

   配置网管服务器到网段 10.50.1.0/24 的路由网关为 10.10.1.1。

   - 在 solaris 操作系统下

     使用 **route add 10.50.1.0 10.10.1.1** 命令添加路由。

     使用 **netstat -r** 命令查询当前的路由表信息。

   - 在 windows 操作系统下

     使用 **route add 10.50.1.0 mask 255.255.255.0 10.10.1.1** 命令添加路由。

     使用 **route print** 命令查询当前的路由表信息。

   说明

   当带外网管接口的 IP 地址与 U2000 的 IP 地址在同一子网时，无需配置路由信息。

2. 登陆 U2000 系统。
3. 配置 SNMP 相关参数。

   (1) 在主菜单中选择“系统 > 网元通讯参数 > 网元 SNMP 参数模板管理(S)...”。

   (2) 在弹出的“缺省访问协议参数”，选择“SNMP v3 参数”页签，单击“增加”。

   (3) 设置模板名称，其他参数根据规划设置。

(4) 在“数据加密协议”和“授权认证协议”处选择相应的协议类型后，单击参数后的[...]，在弹出的“设置密码”对话框中设置“数据加密协议”和“授权认证协议”的密码，单击“确定”。

说明

“设备用户”、“环境引擎 ID”、“数据加密协议”及密码、“授权认证协议”及密码需要与 MA5631 设备侧的配置相同。可以使用 **display snmp-agent usm-user** 命令查询 MA5631 设备侧的设备用户、数据加密协议和授权认证协议；使用 **display snmp-agent local-engineid** 命令查询 MA5631 设备侧的环境引擎 ID。

(5) 单击“确定”，完成 SNMP 参数的配置。

4. 增加设备。

(1) 在主拓扑视图中单击右键，选择“新建 > 网元”。

(2) 在弹出的对话框中设置相关参数。

说明

- IP 地址为 MA5631 的管理 IP 地址。
- SNMP 参数根据对接协议的类型进行选择，此处以 SNMP V3:huawei 模板为例。可以根据实际规划选择对应模板。

(3) 单击“确定”。需要数秒或十几分钟上载设备数据，读取设备相关数据完毕后系统会自动刷新显示该设备图标。

----结束

操作结果

通过 U2000 可以对 MA5631 设备进行维护管理。

配置脚本

配置带外网管（设备侧）的脚本

```
snmp-agent usm-user v3 user1 group1 authentication-mode md5 authkey123 privacy-mode des56 prikey123
snmp-agent group v3 group1 privacy read-view hardy write-view hardy
snmp-agent mib-view hardy include internet
snmp-agent sys-info contact HW-075528780808
snmp-agent sys-info location Shenzhen_China
snmp-agent local-engineid 0123456789
snmp-agent sys-info version v3
snmp-agent trap enable standard
snmp-agent target-host trap-hostname huawei address 10.10.1.10 trap-paramsname ABC
snmp-agent target-host trap-paramsname ABC v3 securityname user1 privacy
snmp-agent trap source meth 0
save
```

配置带内网管（设备侧）的脚本：上行接口的管理 VLAN ID 为 30

```
snmp-agent usm-user v3 user1 group1 authentication-mode md5 authkey123 privacy-mode des56 prikey123
snmp-agent group v3 group1 privacy read-view hardy write-view hardy
snmp-agent mib-view hardy include internet
snmp-agent sys-info contact HW-075528780808
snmp-agent sys-info location Shenzhen_China
snmp-agent local-engineid 0123456789
snmp-agent sys-info version v3
snmp-agent trap enable standard
snmp-agent target-host trap-hostname huawei address 10.10.1.10 trap-paramsname ABC
snmp-agent target-host trap-paramsname ABC v3 securityname user1 privacy
snmp-agent trap source vlanif 30
save
```

3.3 配置上行端口属性

MA5631 设备支持通过 EPON、GPON、GE 上行接口与 OLT 设备对接，通过配置上行端口属性使系统与上行设备通讯正常。

3.3.1 配置上行以太网端口属性

通过本任务对指定的以太网端口进行属性配置，使系统与上行设备通讯正常。

前提条件

如果在离线方式下配置 MA5631，使用 **port mode** 命令配置端口模式后才能配置端口属性。

背景信息

MA5631 需要与上行设备使用以太网端口对接，因此需要注意端口属性的一致性。

缺省配置

以太网端口属性的系统缺省值如**表 3-5** 所示。

表 3-5 以太网端口属性缺省值

参数项	缺省值（光口）	缺省值（电口）
端口自协商模式	关闭	打开
端口速率	GE 光口为 1000Mbit/s。	不能进行配置 **说明** 去使能端口自协商模式后，可以对端口速率进行配置。
双工模式	全双工	不能进行配置 **说明** 去使能端口自协商模式后，可以对端口双工模式进行配置。
网线适应方式	不支持	GE 电口为 normal 方式
流量控制	关闭	关闭

操作步骤

- 配置以太网端口物理属性。
  1. （可选）设置以太网端口自协商模式。

     使用命令 **auto-neg** 对以太网端口自协商模式进行设置。可以对自协商模式进行使能或者去使能：
     - 当使能自协商模式后，端口自动和对接端口协商以太网端口的端口速率和工作模式。
     - 当去使能自协商模式后，端口的速率和工作模式处于强制模式（使用默认或命令行设置的速率和工作模式）。
  2. （可选）设置以太网端口速率。

     使用命令 **speed** 设置以太网端口速率，当端口速率配置成功后，可以使端口以设定的速率工作。进行配置时的注意事项：
     - 配置原则是互连的两个设备对应端口的端口速率应一致，以避免无法通讯的问题。
     - 需要去使能自协商模式。
  3. （可选）配置以太网端口双工模式。

     使用命令 **duplex** 配置以太网端口双工模式。端口双工状态可以为半双工、全双工、自协商三种模式，进行配置时的注意事项：
     - 配置原则是互连的两个设备对应端口双工状态应一致，以避免无法通讯的问题。
     - 需要去使能自协商模式。
  4. （可选）配置以太网端口的网线适应方式。

     使用命令 **mdi** 配置以太网端口的网线适应方式，使之与实际使用的网线匹配。网线适应方式有以下几种：
     - **normal**：指定以太网端口的网线适应方式为使用直通网线。这时与该以太网端口实际连接的网线类型必须为直通网线。

- **across**：指定以太网端口的网线适应方式为使用交叉网线。这时与该以太网端口实际连接的网线类型必须为交叉网线。

- 使用 **flow-control** 命令开启以太网端口的流量控制。
- 使用命令 **mirror port** 配置以太网端口镜像。

----结束

任务示例

举例：以太网端口 0/0/1 为光口，设置其属性为：端口速率 1000Mbit/s，全双工模式，支持流量控制，不支持自协商模式。

```
huawei(config)#interface eth 0/0
huawei(config-if-eth-0/0)#auto-neg 1 disable
huawei(config-if-eth-0/0)#speed 1 1000
huawei(config-if-eth-0/0)#duplex 1 full
huawei(config-if-eth-0/0)#flow-control 1
```

3.3.2 配置上行 PON 端口属性

上行 PON 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 MA5631，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** 命令设置当前设备作为 PON ONU 时向 OLT 注册使用的密码。

- 设置光模块接收光功率告警门限值。

  使用 **optical-module threshold**（EPONNNI 模式）或 **optical-module threshold**（GPONNNI 模式）命令设置光模块接收光功率告警门限值，设置成功后光模块的接收光功率超过设置门限的上下限时会产生告警，及时上报光功率异常。

- 设置 PON 上行光模块的发光模式。

  使用 **laser**（EPONNNI 模式）或 **laser**（GPONNNI 模式）命令设置光模块的发光模式为正常发光、长发光或不发光。

  - 为使 PON 上行光模块正常工作，必须将其发光模式设置为正常发光。
  - 将 PON 上行光模块的发光模式设置为不发光时，请确认该 PON 上行端口没有承载业务。
  - 将 PON 上行光模块的发光模式设置为长发光时，可以测试上行发光功率。

- 查询端口统计信息。

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

----结束

任务示例

举例：设置 GPON 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-0/0/1)#password
{ passwordvalue<S><Length 1-10> }:huawei

  Command:
          password huawei
huawei(config-if-gponnni-0/0/1)#optical-module threshold rx-power lower-limit 5 upper-limit 50
{ <cr>|bias<K>|temperature<K>|tx-power<K>|voltage<K> }:

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

3.4 配置 EoC 局端模块线路模板

本任务配置 EoC 局端模块线路模板。

背景信息

EoC 局端模块线路模板可以直接被绑定。

操作步骤

步骤 1 配置 EoC 模块线路模板。

在全局配置模式或 EoC 模式下，使用 **cbat line-profile add** 命令配置 EoC 模块线路模板。

- 缺省情况下 EoC 局端模块线路模板的配置为：
  - 不限制发送功率。
  - 频谱不开槽。
  - EoC 局端模块线路模板名称缺省模板名称为 cbat-lineprofile_x，其中“x”使用实际模板编号代替。
- 频谱开槽频段中的子载波和未包含在发送频段中的子载波数目之和不能大于 200。

步骤 2 绑定 EoC 端口与 EoC 模块线路模板。

使用 **port cbat-line-profile** 命令将配置完成的 EoC 模块线路模板与 EoC 端口进行绑定。

说明

EoC 端口成功绑定新的 EoC 模块线路模板后，会立即引起 EoC 端口的复位，该端口下所有 CNU 将重新上线，请谨慎使用此命令。

----结束

任务示例

举例：添加一个 EoC 局端模块线路模板，模板编号为 2，并与 EoC 端口 0/1/0 进行绑定。其中模板参数规划如下：

- 线路发送功率为 200dB
- 子载波索引范围为 300-2800

- 频谱开槽频段为 420-450

```
huawei(config-if-eoc-0/1)#cbat line-profile add 2 power 200 start-sub-carrier 300
end-sub-carrier 2800 carriermask enable 420-450
huawei(config-if-eoc-0/1)#port cbat-line-profile 0 profile-id 2
```

3.5 配置 VLAN

配置 VLAN 为配置业务的基础，在进行业务配置前需要保证 VLAN 已经按照实际规划完成配置。

前提条件

规划的 VLAN ID 未被占用。

应用环境

不同类型的用户对 VLAN 的应用不一样，具体应用情况如表 3-6 所示。

表 3-6 VLAN 应用及规划

用户类型	应用场景	VLAN 规划
● 住宅用户 ● 商业用户的上网业务	N:1 场景，即单层 VLAN 上行，多个用户的业务汇聚到同一个 VLAN。	VLAN 类型：Smart VLAN 属性：Common
	1:1 场景，即双层 VLAN 上行，外层 VLAN 用于标识业务，内层 VLAN 用于标识用户。	VLAN 类型：Smart VLAN 属性：Stacking
商业用户的透传业务	只适用于商业用户的透传业务。	VLAN 类型：Smart VLAN 属性：QinQ

缺省配置

VLAN 的缺省配置如表 3-7 所示。

表 3-7 VLAN 缺省配置

参数项	缺省值	备注
系统缺省 VLAN	VLAN ID：1 类型：Smart VLAN	-
系统缺省保留 VLAN	VLAN 范围：4079 ～ 4093	可使用 **vlan reserve** 命令修改系统的保留 VLAN。

参数项	缺省值	备注
新建 VLAN 缺省属性	Common	-
VLAN 转发模式	VLAN+MAC	-

操作步骤

步骤 1 创建 VLAN。

使用 **vlan** 命令创建 VLAN，不同类型的 VLAN 应用于不同的场景。

表 3-8 VLAN 类型及应用场景

VLAN 类型	配置命令	VLAN 描述	应用场景
Standard VLAN	单个增加 VLAN：**vlan *vlanid* standard**	标准 VLAN。 一个 Standard VLAN 只包含多个上行端口，VLAN 中的以太网端口可相互通信，VLAN 间的以太网端口相互隔离。	只适用于以太网端口。应用于网管通信、设备级联等。
Smart VLAN	单个增加 VLAN：**vlan *vlanid* smart**	一个 Smart VLAN 中可包含多个上行端口和多个业务虚端口，且同一个 Smart VLAN 包含的业务虚端口相互隔离。VLAN 间的业务虚端口也相互隔离。一个 VLAN 可接入多个用户，减少了对 VLAN 数量的占用。	应用于 GE 接入业务，如小区接入。
MUX VLAN	单个增加 VLAN：**vlan *vlanid* mux**	一个 MUX VLAN 可包含多个上行端口，但只包含一个业务虚端口，VLAN 间的业务虚端口相互隔离。VLAN 与接入用户存在一对一的映射关系，因此可根据 VLAN 区分不同的接入用户。	应用于 GE 接入业务，如用 VLAN 来区分用户。

说明

- 批量增加 VLAN ID 连续的 VLAN 使用 **vlan *vlanid* to *end-vlanid*** 命令。
- 批量增加 VLAN ID 非连续的 VLAN 使用 **vlan *vlan-list*** 命令。

步骤 2 （可选）配置 VLAN 属性。

VLAN 创建后，缺省属性为 Common，使用 **vlan attrib** 命令配置 VLAN 属性。

根据 VLAN 的规划情况进行选配。

表 3-9 VLAN 属性及应用场景

VLAN 属性	配置命令	VLAN 类型	VLAN 描述	应用场景
Common	创建 VLAN 后默认属性为 Common。	可以是 Standard VLAN、Smart VLAN 和 MUX VLAN。	具有 Common 属性的 VLAN 可作为普通的二层 VLAN 或创建三层虚接口使用。	用于 N:1 接入场景。
VLAN Stacking	配置单个 VLAN 的属性：**vlan attrib** ***vlanid*** **stacking**	只能为 Smart VLAN 或 MUX VLAN。	具有 Stacking 属性的 VLAN 报文包含有 MA5631 分配的内、外两层 VLAN 标签。上层 BRAS 设备可根据两层标签进行双 VLAN 认证，增加接入用户的数量。在二层工作模式的上层网络中，还可以直接通过外层 VLAN+MAC 进行报文转发，为 ISP（Internet Service Provider）提供批发业务功能。	用于 1:1 接入场景，可用于批发业务或 VLAN ID 扩展。 VLAN Stacking 需要使用 **stacking label** 命令配置业务虚端口的标签。 MA5631 支持通过 **stacking outer-ethertype** 命令设置系统 VLAN Stacking 支持的外层以太网协议类型；通过 **stacking inner-ethertype** 命令设置系统 VLAN Stacking 支持的内层以太网协议类型。为了实现设备与其它厂商的设备对接，使用命令将外层/内层以太网协议类型设置为与对接设备一致。

说明

- 批量配置 ID 连续的 VLAN 属性使用 **vlan attrib** ***vlanid*** **to** ***end-vlanid*** 命令。
- 批量配置 ID 非连续的 VLAN 属性使用 **vlan attrib** ***vlan-list*** 命令。

步骤 3 （可选）配置 VLAN 的描述信息。

使用 **vlan desc** 命令配置 VLAN 的描述信息。为了方便维护，可以增加 VLAN 的描述信息，VLAN 描述信息一般为 VLAN 的用途、相关业务信息等。

----结束

任务示例

举例：创建 VLAN 50，VLAN 属性为 Stacking，用于 VLAN ID 扩展。为 VLAN 50 增加业务虚端口，索引值为 100，CNU ID 为 1，物理端口为 1-4，接收方向采用流量表项 9，发送方向采用流量表项 9。VLAN Stacking 的外层 VLAN Tag 50 用于标识接入设备，内层 VLAN Tag 10 用于标识该设备接入的用户。增加 VLAN 的描述信息以方便维护。

```
huawei(config)#vlan 50 smart
huawei(config)#vlan attrib 50 stacking
huawei(config)#service-port 100 vlan 50 eoc 0/1/0 cnu 1 eth 1-4 multi-service
user-vlan untagged inbound traffic-table index 9 outbound traffic-table index 9
huawei(config)#stacking label vlan 50 baselabel 10
huawei(config)#vlan desc 50 description stackingvlan/label10
```

3.6 配置 VLAN 业务模板

VLAN 相关配置集中在 VLAN 业务模板中，VLAN 与业务模板绑定后所有属性立即生效，提高配置效率。

背景信息

- 欲绑定 VLAN 业务模板的 VLAN 已经创建。
- PITP、DHCP、防 IP Spoofing 功能、防 MAC Spoofing 各功能，只有当所有开关都打开时才会生效。

操作步骤

步骤 1 创建 VLAN 业务模板。

使用 **vlan service-profile** 命令创建 VLAN 业务模板或者进入 VLAN 业务模板配置模式。当模板不存在时，创建 VLAN 业务模板并进入该业务模板配置模式。当模板已存在时，直接进入该业务模板配置模式。

步骤 2 配置 VLAN 业务模板参数。

VLAN 业务模板中包含了 VLAN 相关的配置，用户可根据实际需要进行配置。

- 使用 **packet-policy** 命令配置 VLAN 中未知组播报文转发策略，支持转发（forward）和丢弃（discard）两种策略。
- 使用 **dhcp option82** 命令配置 DHCP Option82 特性的使能状态。
- 使用 **pitp** 命令配置 PITP 功能，实现对用户帐号与接入端口的绑定认证。
- 使用 **security anti-ipspoofing** 命令配置防 IP Spoofing 功能，使能防 IP Spoofing 功能后，系统将自动实现 IP 地址与用户的动态绑定。只有当用户报文的源 IP 地址与绑定的 IP 地址一致时，才允许通过设备上行，否则将丢弃。
- 使用 **security anti-macspoofing** 命令配置防 MAC Spoofing 功能，使能防 MAC Spoofing 功能后，系统将自动实现 MAC 地址与业务流的动态绑定。只有当业务流的源 MAC 地址与绑定的 MAC 地址一致时，才允许通过设备上行，否则将丢弃。

- 系统缺省的转发模式为 VLAN+MAC，无需配置。

说明

配置完成后必须使用 **commit** 命令进行提交才能使配置生效。

步骤 3 绑定 VLAN 与 VLAN 业务模板。

使用 **vlan bind service-profile** 命令将配置完成的 VLAN 业务模板与 VLAN 进行绑定。

----结束

任务示例

举例：增加 VLAN 业务模板，索引号为 3，并与 VLAN 100 进行绑定。其中模板参数规划如下：

- 支持未知组播报文转发
- 使能 DHCP Option82 功能
- 使能 PITP 功能
- 使能防 IP Spoofing 功能

其余参数使用缺省值。

```
huawei(config)#vlan service-profile profile-id 3
huawei(config-vlan-srvprof-3)#packet-policy multicast forward
huawei(config-vlan-srvprof-3)#dhcp option82 enable
huawei(config-vlan-srvprof-3)#pitp enable
huawei(config-vlan-srvprof-3)#security anti-ipspoofing enable
huawei(config-vlan-srvprof-3)#commit
huawei(config-vlan-srvprof-3)#quit
huawei(config)#vlan bind service-profile 100 profile-id 3
```

3.7 配置 NTP 时间

配置 NTP 协议，使网络内所有设备的时钟基本保持一致，从而使设备能够提供基于统一时间的多种应用（如网络管理系统、网络计费系统）。

背景信息

NTP 协议简介：

- NTP（Network Time Protocol，网络时间协议）是由 RFC 1305 定义的时间同步协议，用来在分布式时间服务器和客户端之间进行时间同步。它定义了协议实现过程中所使用的结构、算法、实体和协议。
- NTP 是从时间协议（TIME PROTOCOL）和 ICMP 时间戳报文（ICMP TIMESTAMP MESSAGE）演变而来，主要是从准确性和强壮性方面进行了特殊的设计。
- NTP 基于 UDP 报文进行传输，使用的 UDP 端口号为 123。
- 对于运行 NTP 的本地系统，既可以接受来自其他时钟源的同步，又可以作为时钟源同步其他的时钟，并且可以和其他设备互相同步。

NTP 协议主要应用于需要网络中所有主机或路由器时钟保持一致的场合，比如：

- 在网络管理中，对从不同路由器采集来的日志信息、调试信息进行分析时，需要以时间作为参照依据。
- 计费系统要求所有设备的时钟一致。

- 完成某些功能，如定时重启网络中的所有路由器，要求所有路由器的时钟保持一致。
- 多个系统协同处理同一个比较复杂的事件时，为保证正确的执行顺序，多个系统必须参考同一时钟。
- 在备份服务器和客户机之间进行增量备份时，要求备份服务器和所有客户机之间的时钟同步。

对于网络中的各设备来说，如果依靠管理员手工输入命令来修改系统时钟是不可能的，这不但工作量巨大，而且也不能保证时钟的精确性。但通过配置 NTP，可以很快将网络中设备的时钟同步，同时也能保证很高的精度。

NTP 协议支持四种工作模式：广播模式、组播模式、单播服务器模式和对等体模式。MA5631 设备支持 NTP 协议的全部四种工作模式。

缺省配置

网络时钟的缺省配置如表 3-10 所示。

表 3-10 网络时钟的缺省配置表

参数项	缺省值
身份验证功能	去使能
NTP 验证密钥	无
允许建立的最大 NTP 同步连接数	100
时钟层数	16

3.7.1 （可选）配置 NTP 身份验证功能

配置 NTP 的身份验证功能，在一些对安全性要求较高的网络中，可以选择启用身份验证功能来提高网络的安全性，防止未授权的用户对时钟进行修改。

前提条件

在配置 NTP 验证功能之前，需完成 MA5631 设备的网络接口和路由协议的配置，使服务器端和客户端的网络层可达。

背景信息

在一些对安全性要求较高的网络中，运行 NTP 协议时需要启用验证功能。配置 NTP 验证功能可以分为配置客户端的 NTP 验证和配置服务器端的 NTP 验证两个部分。

注意事项

- 如果客户端没有使能 NTP 验证功能，不论服务器端是否使能 NTP 验证，客户端均可以与服务器端同步。
- 如果使能了 NTP 验证功能，应同时配置可信的密钥。

- 服务器端的配置和客户端的配置应保持一致。
- 在客户端已配置 NTP 验证的情况下，服务器端只要配置了与客户端相同的验证密钥，客户端就能通过验证。此时服务器端不需要使能 NTP 验证功能，也不必声明该密钥是可信的。
- 客户端只会同步到提供可信密钥的服务器，如果服务器提供的密钥不是可信的密钥，那么客户端不会与其同步。
- 配置 NTP 的身份验证功能流程是“开始－使能 NTP 验证功能－配置 NTP 验证密钥－声明可信的密钥－结束”。

操作步骤

步骤 1 使用 **ntp-service authentication enable** 命令使能 NTP-service 身份验证功能。

步骤 2 使用 **ntp-service authentication-keyid** 命令设置 NTP 验证密钥。

步骤 3 使用 **ntp-service reliable authentication-keyid** 命令指定密钥是可信的。

----结束

任务示例

举例：启动 NTP 的身份验证功能，配置验证密钥为 aNiceKey、密钥编号为 42，最后将 42 号密钥配置为可信密钥。

```
huawei(config)#ntp-service authentication enable
huawei(config)#ntp-service authentication-keyid 42 authentication-mode md5 aNiceKey
huawei(config)#ntp-service reliable authentication-keyid 42
```

3.7.2 配置广播模式 NTP

配置 MA5631 采用 NTP 广播模式进行时钟的同步。配置完成后服务器端周期性从指定端口广播时钟同步报文，MA5631 作为客户端侦听来自服务器的广播消息包，根据收到的广播消息包对本地时钟进行同步。

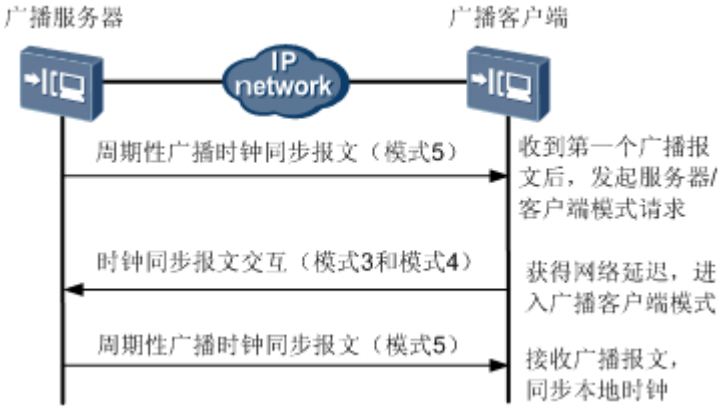
前提条件

在配置 NTP 广播模式之前，需完成 MA5631 设备的网络接口和路由协议的配置，使服务器端和客户端的网络层可达。

背景信息

在广播模式中，服务器端周期性地向广播地址 255.255.255.255 发送时钟同步报文，报文中的 Mode 字段设置为 5（广播模式）。客户端侦听来自服务器的广播报文。当客户端接收到第一个广播报文后，客户端与服务器交互 Mode 字段为 3（客户模式）和 4（服务器模式）的 NTP 报文，以获得客户端与服务器间的网络延迟。之后，客户端就进入广播客户端模式，继续侦听广播报文的到来，根据到来的广播报文对系统时钟进行同步。如图 3-23 所示。

图 3-23 NTP 广播模式



注意事项

1. 广播模式下，需要同时配置 NTP 服务器端和客户端。
2. 同步设备的时钟层数必须小于或等于被同步设备的时钟层数，否则，不能进行时钟同步。

操作步骤

- 配置广播客户端主机。
  1. （可选）配置 NTP 身份验证功能。

     建议在一些对安全性要求较高的网络中，运行 NTP 协议时启用验证功能。服务器端的配置和客户端的配置应保持一致。

     (1) 使用 **ntp-service authentication enable** 命令使能 NTP-service 身份验证功能。

     (2) 使用 **ntp-service authentication-keyid** 命令设置 NTP 验证密钥。

     (3) 使用 **ntp-service reliable authentication-keyid** 命令指定密钥是可信的。
  2. 增加 VLAN 的三层虚接口。

     (1) 使用 **vlan** 命令创建 VLAN。

     (2) 使用 **port vlan** 命令将上行口加入到 VLAN 中，使带 VLAN 的用户报文通过上行端口上行。

     (3) 使用 **interface vlanif** 命令从全局配置模式创建 VLAN 接口并进入 VLANIF 模式，以便配置虚拟的三层接口。

     (4) 使用 **ip address** 命令配置 VLAN 接口 IP 地址和子网掩码，让 VLAN 中的 IP 报文能够参与三层转发。
  3. 使用 **ntp-service broadcast-client** 命令设置主机为 NTP 广播客户端。

----结束

任务示例

举例：配置 MA5631 作为 NTP 客户端，通过 VLAN 2 的三层接口 IP 地址 10.10.10.20/24 侦听来自服务器的广播消息包，并与广播服务器端的时钟进行同步。

```
huawei(config)#vlan 2 standard
huawei(config)#port vlan 2 0/0 0
```

```
huawei(config)#interface vlanif 2
huawei(config-if-vlanif2)#ip address 10.10.10.20 24
huawei(config-if-vlanif2)#ntp-service broadcast-client
huawei(config-if-vlanif2)#quit
```

3.7.3 配置组播模式 NTP

配置 MA5631 采用 NTP 组播模式进行时钟的同步。配置完成后服务器端从指定端口周期性组播时钟同步报文，MA5631 作为客户端侦听来自服务器的组播消息包，根据收到的组播消息包对本地时钟进行同步。

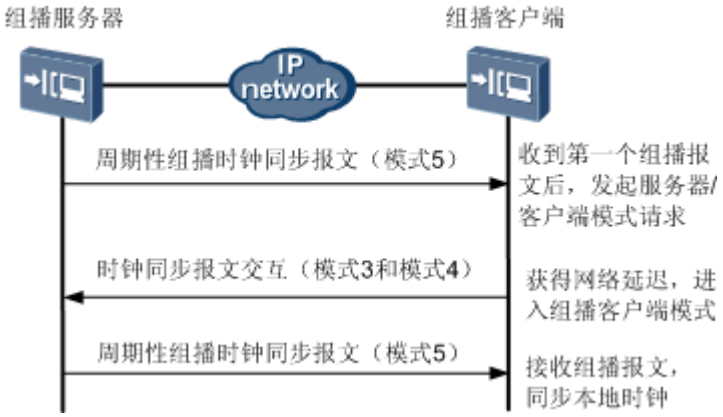
前提条件

在配置 NTP 组播模式之前，需完成 MA5631 设备的网络接口和路由协议的配置，使服务器端和客户端的网络层可达。

背景信息

在组播模式中，服务器端周期性地向用户配置的组播地址（若用户没有配置组播地址，则使用默认的 NTP 组播地址 224.0.1.1）发送时钟同步报文，报文中的 Mode 字段设置为 5（组播模式）。客户端侦听来自服务器的组播报文。当客户端接收到第一个组播报文后，客户端与服务器交互 Mode 字段为 3（客户模式）和 4（服务器模式）的 NTP 报文，以获得客户端与服务器间的网络延迟。之后，客户端就进入组播客户模式，继续侦听组播报文的到来，根据到来的组播报文对系统时钟进行同步。如图 3-24 所示。

图 3-24 NTP 组播模式



注意事项

1. 组播模式下，需要同时配置 NTP 服务器端和客户端。
2. 同步设备的时钟层数必须小于或等于被同步设备的时钟层数，否则，不能进行时钟同步。

操作步骤

- 配置组播客户端主机。
  1. （可选）配置 NTP 身份验证功能。

     建议在一些对安全性要求较高的网络中，运行 NTP 协议时启用验证功能。服务器端的配置和客户端的配置应保持一致。

(1) 使用 **ntp-service authentication enable** 命令使能 NTP-service 身份验证功能。

(2) 使用 **ntp-service authentication-keyid** 命令设置 NTP 验证密钥。

(3) 使用 **ntp-service reliable authentication-keyid** 命令指定密钥是可信的。

2. 增加 VLAN 的三层虚接口。

(1) 使用 **vlan** 命令创建 VLAN。

(2) 使用 **port vlan** 命令将上行口加入到 VLAN 中，使带 VLAN 的用户报文通过上行端口上行。

(3) 使用 **interface vlanif** 命令从全局配置模式创建 VLAN 接口并进入 VLANIF 模式，以便配置虚拟的三层接口。

(4) 使用 **ip address** 命令配置 VLAN 接口 IP 地址和子网掩码，让 VLAN 中的 IP 报文能够参与三层转发。

3. 使用 **ntp-service multicast-client** 命令设置主机为 NTP 组播客户端。

----结束

任务示例

举例：配置 MA5631 作为 NTP 客户端，通过 VLAN 2 的三层接口 IP 地址 10.10.10.20/24 侦听来自服务器的组播消息包，并与组播服务器端的时钟进行同步。

```
huawei(config)#vlan 2 standard
huawei(config)#port vlan 2 0/0 0
huawei(config)#interface vlanif 2
huawei(config-if-vlanif2)#ip address 10.10.10.20 24
huawei(config-if-vlanif2)#ntp-service multicast-client
huawei(config-if-vlanif2)#quit
```

3.7.4 配置单播服务器模式 NTP

配置 MA5631 作为 NTP 客户端向网络中的 NTP 服务器进行时间同步。

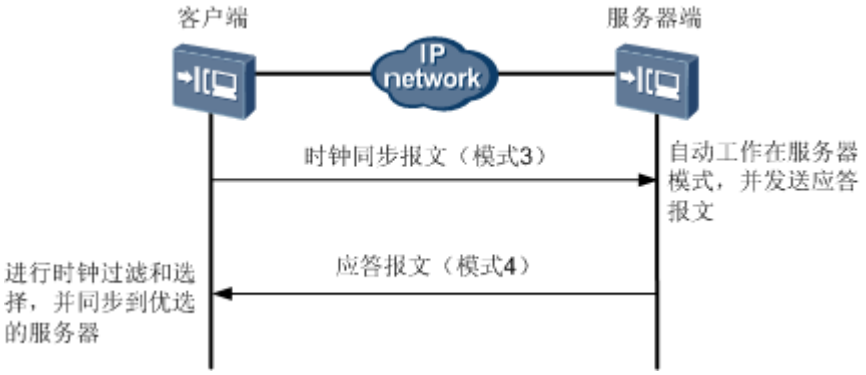
前提条件

在配置 NTP 客户端或服务器模式之前，需完成 MA5631 设备的网络接口和路由协议的配置，使服务器端和客户端的网络层可达。

背景信息

在客户端/服务器模式中，客户端向服务器发送时钟同步报文，报文中的 Mode 字段设置为 3（客户模式）。服务器端收到报文后会自动工作在服务器模式，并发送应答报文，报文中的 Mode 字段设置为 4（服务器模式）。客户端收到应答报文后，进行时钟过滤和选择，并同步到优选的服务器。如**图 3-25** 所示。

图 3-25 NTP 客户端/服务器模式



注意事项

1. 当设备采用客户端/服务器模式时，只需在客户端进行配置，服务器端不需进行配置。
2. 同步设备的时钟层数必须小于或等于被同步设备的时钟层数，否则，不能进行时钟同步。

操作步骤

步骤 1 配置 VLAN 的三层虚接口。

1. 使用 **vlan** 命令创建 VLAN。
2. 使用 **port vlan** 命令将上行口加入到 VLAN 中，使带 VLAN 的用户报文通过上行端口上行。
3. 使用 **interface vlanif** 命令从全局配置模式创建 VLAN 接口并进入 VLANIF 模式，以便配置虚拟的三层接口。
4. 使用 **ip address** 命令配置 VLAN 接口 IP 地址和子网掩码，让 VLAN 中的 IP 报文能够参与三层转发。

步骤 2 使用 **ntp-service unicast-server** 命令配置 NTP 单播服务器模式，并指定作为本地时间服务器的远程服务器 IP 地址和本地收发 NTP 消息时的接口。

说明

- 此命令中的 *ip-address* 是一个单播地址，不能为广播地址、组播地址或本地时钟的 IP 地址。
- 通过 *source-interface* 参数指定 NTP 报文的源接口后，NTP 报文的源 IP 地址将被设置为指定接口的主 IP 地址。
- 服务器端只有当其时钟被同步后，才能作为时间服务器去同步其他设备。
- 当服务器端的时钟层数大于或等于客户端的时钟层数时，客户端将不会向其同步。
- 可以通过多次执行 **ntp-service unicast-server** 命令配置多个服务器，客户端依据时钟优选来选择最优的时钟源。

步骤 3 （可选）配置 ACL 规则。

过滤通过三层接口的报文，只允许来自时钟服务器的 IP 报文访问该三层接口，禁止其它非授权访问。建议在对系统安全性比较高的场合使用 ACL 规则。

1. 使用 **acl** *adv-acl-numbe* 命令创建告警访问控制列表。

2. 使用 **rule** 命令根据数据包的源地址信息/目的地址信息/IP 承载的协议类型/协议的特性制定流规则，允许或禁止符合条件的数据包通过。
3. 使用 **packet-filter** 命令为指定端口配置 ACL 过滤规则，并使之生效。

----结束

任务示例

举例：NTP 服务器的 IP 地址：10.20.20.20/24，配置 MA5631 设备（VLAN 2 的三层接口 IP 地址 10.10.10.10/24，网关：10.10.10.1）作为客户端，客户端通过 VLAN 接口向服务器发送同步时钟请求报文，服务器端响应请求报文进行时钟同步；同时配置 ACL 规则，只允许来自时钟服务器的 IP 报文访问该三层接口。

```
uawei(config)#vlan 2 standard
huawei(config)#port vlan 2 0/0 0
huawei(config)#interface vlanif 2
huawei(config-if-vlanif2)#ip address 10.10.10.10 24
huawei(config-if-vlanif2)#quit
huawei(config)#ntp-service unicast-server 10.20.20.20 source-interface vlanif 2
huawei(config)#acl 3010
huawei(config-acl-adv-3010)#rule deny ip source any destination 10.10.10.10 0.0.0.0
huawei(config-acl-adv-3010)#rule permit ip source 10.20.20.20 0.0.0.0 destination 10.10.10.10
0.0.0.0
huawei(config-acl-adv-3010)#quit
huawei(config)#packet-filter inbound ip-group 3010 port 0/0/0
```

3.7.5 配置对等体模式 NTP

配置 MA5631 采用 NTP 对等模式进行时钟同步的配置。在对等体模式中，只需要在主动对等体端进行配置，被动对等体端无需配置。对等体模式下，主动对等体和被动对等体可以互相同步，层数高的对等体被层数低的对等体同步。

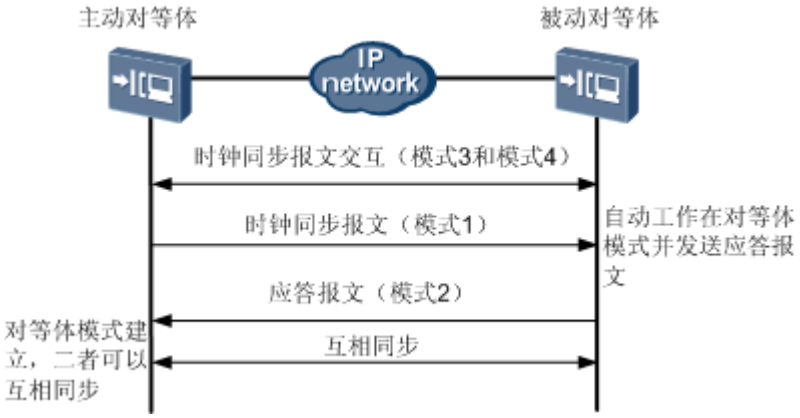
前提条件

在配置 NTP 对等体模式之前，需完成 MA5631 设备的网络接口和路由协议的配置，使服务器端和客户端的网络层可达。

背景信息

在对等体模式中，主动对等体和被动对等体之间首先交互 Mode 字段为 3（客户端模式）和 4（服务器模式）的 NTP 报文。之后，主动对等体向被动对等体发送时钟同步报文，报文中的 Mode 字段设置为 1（主动对等体），被动对等体收到报文后自动工作在被动对等体模式，并发送应答报文，报文中的 Mode 字段设置为 2（被动对等体）。经过报文的交互，对等体模式建立起来。主动对等体和被动对等体可以互相同步。如果双方的时钟都已经同步，则以层数小的时钟为准。如图 3-26 所示。

图 3-26 NTP 对等体模式



注意事项

1. 对等体模式下，只需要在主动对等体端进行 NTP 模式的配置。
2. 对等体之间是根据它们的时间层数，而不是根据是否处于主动对等体地位来决定如何进行时钟同步。

操作步骤

步骤 1 配置 NTP 主动对等体。

1. 使用 **ntp-service refclock-master** 命令设置本地时钟作为 NTP 主时钟，并指定 NTP 主时钟所处的层次数。
2. 使用 **ntp-service unicast-peer** 命令配置 NTP 对等体模式，并指定作为本地对等体的远程服务器 IP 地址和本地收发 NTP 消息时的接口。

   说明

   - 此命令中的 *ip-address* 是一个单播地址，不能为广播地址、组播地址或参考时钟的 IP 地址。
   - 通过 *source-interface* 参数指定 NTP 报文的源接口后，NTP 报文的源 IP 地址将被设置为指定接口的主 IP 地址。

步骤 2 配置 VLAN 的三层虚接口。

1. 使用 **vlan** 命令创建 VLAN。
2. 使用 **port vlan** 命令将上行口加入到 VLAN 中，使带 VLAN 的用户报文通过上行端口上行。
3. 使用 **interface vlanif** 命令从全局配置模式创建 VLAN 接口并进入 VLANIF 模式，以便配置虚拟的三层接口。
4. 使用 **ip address** 命令配置 VLAN 接口 IP 地址和子网掩码，让 VLAN 中的 IP 报文能够参与三层转发。

----结束

任务示例

举例：配置一台 MA5631 设备作为 NTP 主动对等体（VLAN 2 接口 IP 地址：10.10.10.10/24），时钟层数设置为 4，网络中 NTP 被动对等体的 IP 地址为

0.10.10.20/24，等体通过 VLAN 2 的三层接口向被动对等体发送同步时钟请求报文，被动对等体响应请求报文，时钟层数高的对等体将被时钟层数低的对等体同步。

```
huawei(config)#ntp-service refclock-master 4
huawei(config)#ntp-service unicast-peer 10.10.10.20 source-interface vlanif 2
huawei(config)#vlan 2 standard
huawei(config)#port vlan 2 0/0 0
huawei(config)#interface vlanif 2
huawei(config-if-vlanif2)#ip address 10.10.10.10 24
huawei(config-if-vlanif2)#quit
```

3.8 配置用户安全

配置保护操作用户和接入用户的安全机制，以防止用户帐号被盗和漫游或恶意用户的攻击。

背景信息

用户安全包括：

- PITP：为上层的认证服务器提供接入用户物理位置信息，BRAS 设备获取用户端口信息后，可实现对用户账号与接入端口的绑定认证，避免用户账号的盗用与漫游。
- DHCP Option82：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，避免用户账号的盗用与漫游。
- IP 地址绑定：将 IP 地址与业务虚端口绑定，用于用户认证，保证认证的安全性。
- MAC 地址绑定：将 MAC 地址与业务虚端口绑定，防止非法用户接入。
- 防御 MAC Spoofing：系统防御用户伪造 MAC 地址进行攻击的措施。
- 防御 IP Spoofing：系统防御用户伪造 IP 地址进行攻击的措施。

用户安全相关的缺省配置如表 3-11 所示。

表 3-11 用户安全缺省配置

参数项	缺省值	备注
PITP	全局开关：关闭 基于 VLAN 的开关：打开	只有所有开关全部打开时，才能使能 PITP 功能。
DHCP Option82	全局开关：关闭 基于 VLAN 的开关：打开	只有所有开关全部打开时，才能使能 DHCP Option82 功能。
防御 IP Spoofing	全局开关：关闭 基于 VLAN 的开关：关闭	只有所有开关全部打开时，才能使能防御 IP Spoofing 功能。
防御 MAC Spoofing	全局开关：关闭 基于 VLAN 的开关：关闭 业务虚端口开关：打开。缺省情况下，可绑定的最大 MAC 地址数为 8。	只有所有开关全部打开时，才能使能防御 MAC Spoofing 功能。

3.8.1 配置 PITP 的防盗号和漫游

PITP（Policy Information Transfer Protocol）主要用于用户 PPPoE 拨号上网，在接入设备和 BRAS（Broadband Remote Access Server）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，防止用户帐号的盗号和漫游。

背景信息

PITP 用于向 BRAS 设备提供用户端口的信息。BRAS 设备获取用户端口信息后，可实现对用户帐号与用户端口的绑定认证，避免用户帐号的盗用与漫游。包括 PPPoE+模式（PITP P 模式）和 VBAS 模式（PITP V 模式）。

- PPPoE+方式：PPPoE+方式是指在接入用户与 BRAS 进行 PPPoE 协商的过程中，设备直接在 PPPoE 报文中添加 TAG 标识，将接入用户的端口信息传送给 BRAS。
- VBRAS 方式：VBRAS 方式是指在接入用户与 BRAS 进行 PPPoE 协商的过程中，BRAS 主动向设备发送 VBRAS 请求报文，要求设备上报接入用户的物理端口信息。设备通过 VBRAS 响应报文，将端口信息发送给 BRAS。

PITP 可应用于 MA5631 单网元组网和 MA5631 级联组网场景。

- 单网元组网场景：两台 PC（PC1 和 PC2）接入 MA5631 的不同端口进行拨号上网。
- MA5631 级联组网场景：两台 PC（PC1 和 PC2）接入不同的设备（PC1 接入 MA5631，PC2 通过级联设备接入 MA5631）进行拨号上网。

两种场景下的原理类似，PC1 使用自己的帐号拨号上网，BRAS 设备把用户的帐号与 MA5631 设备上报的 PC1 用户所在的物理网络位置绑定。当 PC2 用户拨号上网时，如果盗用 PC1 的帐号，在认证时 BRAS 会发现帐号信息与物理位置信息不匹配，从而拒绝用户上线。

缺省配置

PITP 相关的缺省配置如表 3-12 所示。

表 3-12 PITP 相关缺省配置

参数项	缺省值
PITP 功能	全局开关：关闭 基于 VLAN 的开关：打开
PITP Sub-option90 功能	关闭
是否允许用户侧 PPPoE 报文携带 vendor Tag 信息	否

操作步骤

步骤 1 配置 RAIO（Relay Agent Information Option），在使用 PITP 功能前，必须完成 RAIO 的配置。

- 使用 **raio-mode *mode* pitp-pmode** 命令配置 PITP P 模式下的 RAIO 模式。
- 使用 **raio-mode *mode* pitp-vmode** 命令配置 PITP V 模式下的 RAIO 模式。

P 模式，支持所有的 RAIO 模式；V 模式，暂时只支持 common、userdefine 模式。

user-defined：用户自定义模式，在这种模式下，需要使用 **raio-format** 命令配置 RAIO 的格式。RAIO 格式也需要根据 PITP 的工作模式选择对应的关键字。

- 使用 **raio-format pitp-pmode** 命令配置 PITP P 模式下的 RAIO 格式。
- 使用 **raio-format pitp-vmode** 命令配置 PITP V 模式下的 RAIO 格式。

用户自定义格式配置 CID 和 RID，不选择接入方式，则配置的格式对所有的接入方式生效；选择接入方式，则配置的格式只对此接入方式生效。PITP V 模式下的 CID 和 RID 的格式相同。

- CID：Circuit ID，用于标识设备的属性信息。
- RID：Remote ID，用于标识用户的接入信息。

其他模式下，RAIO 格式固定，不需要手工配置。

步骤 2 配置 PITP 功能开关。

PITP 一共有两级开关，只有当所有开关都打开时，此功能才生效。

1. 配置全局开关：使用 **pitp enable pmode** 命令使能全局 PITP P 模式功能。缺省为关闭。

   在 V 模式下，需要使用 **pitp vmode ether-type** 命令将协议类型设置为与 BRAS 一致。再使用 **pitp enable vmode** 命令使能全局 PITP V 模式功能。

   说明

   PITP V 模式的以太网协议类型必须在 PITP V 模式功能关闭时配置。

2. （可选）配置 VLAN 级开关：

   a. 使用 **vlan service-profile** 命令创建 VLAN 业务模板并进入 VLAN 业务模板模式。

   b. 使用 **pitp enable** 命令使能 VLAN 的 PITP 功能，缺省为打开。

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

   d. 使用 **quit** 命令退出 VLAN 业务模板模式。

   e. 使用 **vlan bind service-profile** 命令为 VLAN 绑定步骤 2.2.a 配置的 VLAN 业务模板。

步骤 3 配置 PITP 的可选属性。

- 使用 **pitp permit-forwarding service-port** 命令配置业务虚端口上是否允许用户侧 PPPoE 报文携带 vendor Tag 信息。系统缺省关闭此功能。

  系统将设备名以及框、槽、端口号等信息以 Tag 方式加入到 PPPoE+上行的 PADI 和 PADR 报文中，生成新的报文。如果打开此功能，则将带 Tag 的报文进行转发；如果关闭此功能，则将带 Tag 的报文丢弃。

  在 OLT+MA5631 组网时的 PITP 应用需要注意以下事项：

  1. 当只在 OLT 上使能 PITP 时，则只能带 OLT 的 PON 端口信息。
  2. 当只在 MA5631 上使能 PITP 时，则只能带 MA5631 的用户端口信息。
  3. 如果在 OLT 和 MA5631 上都使能了 PITP，则需要通过 OLT 上的一个开关（使用 **pitp permit-forwarding service-port** 命令）选择这条流带哪个的标签：
     - 当使能了这个开关时，则只能带 OLT 的 PON 端口信息。

- 当去使能（disable）这个开关时，这个业务虚端口的用户是不能拔号的，也就是说 PADI 报文（P 模式）无法发送出去。

- 使用 **raio sub-option 0x90** 命令配置 Sub-option90 的开关。此开关缺省关闭。

  PPPoE+支持 Sub-option90 子选项线路参数上报（包括链路类型及封装信息等），根据需要进行选配。只在 P 模式下配置才生效，VBAS 模式下不支持线路参数上报。

----结束

任务示例

举例：使能 VLAN ID 为 30 的业务流的 PITP P 模式功能。规划如下：

- RAIO 模式为用户自定义。
- EoC 的 CID 格式为 eoc（接入方式） 机框号/槽位号/端口号/cnuid。

```
huawei(config)#raio-mode user-defined pitp-pmode
huawei(config)#raio-format pitp-pmode cid eoc anid eoc frame/slot/port/cnuid
huawei(config)#raio-format pitp-pmode rid eoc plabel
huawei(config)#pitp enable pmode
huawei(config)#vlan service-profile profile-id 1
huawei(config-vlan-srvprof-1)#pitp enable
huawei(config-vlan-srvprof-1)#commit
huawei(config-vlan-srvprof-1)#quit
huawei(config)#vlan bind service-profile 30 profile-id 1
```

举例：将 VBRAS 报文的以太网协议类型配置为与上层 BRAS 一致，即为 0x8500。使能 VLAN ID 为 30 的业务流的 PITP V 模式功能。RAIO 模式为 common。

```
huawei(config)#raio-mode common pitp-vmode
huawei(config)#pitp enable vmode
huawei(config)#vlan service-profile profile-id 1
huawei(config-vlan-srvprof-1)#pitp enable
huawei(config-vlan-srvprof-1)#commit
huawei(config-vlan-srvprof-1)#quit
huawei(config)#vlan bind service-profile 30 profile-id 1
```

3.8.2 配置 DHCP 的防盗号和漫游

DHCP 通过在用户发起的 DHCP 请求报文的 Option82 字段中，添加用户的物理位置信息，提高用户认证安全性，可防止用户帐号的盗号和漫游。

背景信息

Option82 字段中包括 CID（Circuit ID）、RID（Remote ID）以及 sub-option90（可选）字段，提供用户的机框号、槽位号、端口号等信息。

MA5631 可以工作在 DHCP 二层转发模式，可以配置 DHCP Option82 防盗号和漫游。

DHCP Option82 相关的缺省配置如表 3-13 所示。

表 3-13 DHCP Option82 相关缺省配置

参数项	缺省值
DHCP Option82 功能	全局开关：去使能 基于 VLAN 的开关：使能
dhcp sub-option7 功能	去使能

参数项	缺省值
dhcp sub-option90 功能	去使能

操作步骤

步骤 1 配置 RAIO。在使用 DHCP 功能前，必须完成 RAIO 的配置。

使用 **raio-mode** 命令配置 RAIO 的模式。

- 对应模式需要选择 **dhcp-option82**。
- 在用户自定义模式 **user-defined** 下，需要使用 **raio-format** 命令配置 RAIO 的格式，对应的模式需要选择 **dhcp-option82**。用户自定义格式主要配置 CID 的 RID，不选择接入方式，则配置的格式对所有的接入方式生效；选择接入方式，则配置的格式只对此接入方式生效。RAIO 的输入格式的详细介绍请参考 **raio-format** 命令。
  - CID，Circuit ID，用于标识设备的属性信息。
  - RID：Remote ID，用于标识用户的接入信息。
- 其他模式下，RAIO 格式固定，不需要手工配置。

步骤 2 （可选）配置业务虚端口上是否允许用户侧 DHCP 报文携带 Option82 信息。

- 使用 **dhcp-option82 permit-forwarding service-port** 命令配置业务虚端口上是否允许用户侧 DHCP 报文携带 Option82 信息。

  系统将设备名以及框、槽、端口号等信息加入到 DHCP 报文的 Option82 字段中，生成新的报文。如果使能此功能，则将带 Tag 的报文进行转发；如果去使能此功能，则将带 Tag 的报文丢弃。

步骤 3 配置 DHCP Option82 功能开关。

使用 **dhcp option82** 命令配置端口的 DHCP Option82 功能。DHCP Option82 全局开关缺省去使能。

DHCP Option82 一共有两级开关，只有所有开关都使能时，此功能才生效。

1. 配置全局开关：使用 **dhcp option82** 命令进行配置，缺省为去使能。
2. 配置 VLAN 级开关：
   a. （可选）使用 **vlan service-profile** 命令创建 VLAN 业务模板并进入 VLAN 业务模板模式。
   b. 使用 **dhcp option82** 命令进行配置，缺省为使能。
   c. 使用 **commit** 命令使模板配置参数生效。必须执行此操作 VLAN 业务模板相关配置才能生效。
   d. 使用 **quit** 命令退出 VLAN 业务模板模式。
   e. 使用 **vlan bind service-profile** 命令为 VLAN 绑定步骤 3.2.a 配置的 VLAN 业务模板。

----结束

任务示例

举例：使能 DHCP Option82 功能。数据规划如下：

- RAIO 模式为用户自定义。
- EoC 的 CID 格式为 eoc（接入方式） 机框号/槽位号/端口号/cnuid。
- RID 格式都为端口的标签。

```
huawei(config)#raio-mode user-defined dhcp-option82
huawei(config)#raio-format dhcp-option82 cid eoc anid eoc frame/slot/port/cnuid
huawei(config)#raio-format dhcp-option82 rid eoc splabel
huawei(config)#dhcp option82 enable
```

3.8.3 配置防 IP 地址攻击

配置 IP 地址绑定和防御 IP Spoofing，以防止恶意用户伪造合法用户的 IP 地址对设备或合法用户进行攻击。

背景信息

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

IP Spoofing 功能主要是动态触发 IP 地址绑定功能，从而防止非法用户盗用合法用户的 IP 地址。防 IP Spoofing 开关开启时，用户上线后会绑定 IP 地址，则此用户端口上不允许用户使用其他 IP 地址上线，同时不允许其他端口用户仿冒此 IP 地址上线。

操作步骤

- 配置 IP 地址绑定。

  使用 **bind ip** 命令配置 IP 地址绑定。

  当只希望指定的某些 IP 地址访问系统，以防止非法用户盗用合法用户的 IP 地址时，配置 IP 地址绑定。

- 配置防御 IP Spoofing。

  防御 IP Spoofing 一共有两级开关，只有两级开关都打开时，此功能才生效。

  - 全局开关：使用 **security anti-ipspoofing** 命令进行配置，缺省为关闭。
  - 基于 VLAN 的开关：

    1. 使用 **vlan service-profile** 命令创建 VLAN 业务模板并进入 VLAN 业务模板模式。
    2. 使用 **security anti-ipspoofing** 命令进行配置，缺省为打开。
    3. 使用 **commit** 命令使模板配置参数生效。必须执行此操作 VLAN 业务模板相关配置才能生效。
    4. 使用 **quit** 命令退出 VLAN 业务模板模式。
    5. 使用 **vlan bind service-profile** 命令为 VLAN 绑定步骤 1 配置的 VLAN 业务模板。

  说明

  如果在用户已经上线的情况下，再使能防御 IP Spoofing，此时系统中是没有绑定这些已上线用户的 IP 地址的，这样将导致这部分用户下线，需要重新上线；只有在使能防御 IP Spoofing 功能后上线的用户的 IP 地址才可以被绑定。

----结束

任务示例

举例：绑定 IP 地址 10.1.1.245 与索引号为 2 的业务虚端口，即该端口只允许源 IP 地址为 10.1.1.245 的报文通过。

```
huawei(config)#bind ip service-port 2 10.1.1.245
```

举例：使能业务 VLAN 为 10 的防御 IP Spoofing 功能。

```
huawei(config)#security anti-ipspoofing enable
huawei(config)#vlan service-profile profile-id 2
huawei(config-vlan-srvprof-2)#security anti-ipspoofing enable
  Info: Please use the commit command to make modifications take effect
huawei(config-vlan-srvprof-2)#commit
huawei(config-vlan-srvprof-2)#quit
huawei(config)#vlan bind service-profile 10 profile-id 2
```

3.8.4 配置防 MAC 地址攻击

配置 MAC 地址绑定和防御 MAC Spoofing，以防止恶意用户伪造合法用户的 MAC 地址对设备或合法用户进行攻击。

背景信息

MAC 地址绑定是指将 MAC 地址绑定到业务虚端口，限制该业务虚端口上只有特定 MAC 地址的用户才可以接入到网络。MA5631 不支持直接绑定 MAC 地址的配置，而是通过设置端口静态 MAC 地址表项和端口 MAC 地址最大学习数为 0，从而实现端口与 MAC 地址绑定的功能。

防御 MAC Spoofing 功能主要是防止非法用户伪造合法用户的 MAC 地址，目的是保证合法用户的业务不受影响，主要应用于 PPPoE 接入和 DHCP 接入用户。

操作步骤

- 配置 MAC 地址绑定。
  1. 使用 **mac-address static** 命令配置静态 MAC 地址绑定。
  2. 使用 **mac-address max-mac-count** 命令配置 MAC 地址最大学习数为 0。

     MAC 地址最大学习数用于限制同一帐号下可学习到的最大 MAC 地址数，即限制同一帐号下可上网的最大 PC 数。
- 配置防御 MAC Spoofing。

  说明

  为保障设备安全，建议开启此功能。

  防御 MAC Spoofing 功能共有三级开关，只有当三级开关都打开时，此功能才生效。
  - 全局开关：使用 **security anti-macspoofing** 命令进行配置，缺省为关闭。
  - VLAN 级开关：
    1. 使用 **vlan service-profile** 命令创建 VLAN 业务模板并进入 VLAN 业务模板模式。
    2. 使用 **security anti-macspoofing** 命令进行配置，缺省为关闭。
    3. 使用 **commit** 命令使模板配置生效。必须执行此操作 VLAN 业务模板相关配置才能生效。
    4. 使用 **quit** 命令退出 VLAN 业务模板模式。

5. 使用 **vlan bind service-profile** 命令为 VLAN 绑定步骤 1 配置的 VLAN 业务模板。

- 业务虚端口级开关：使用 **security anti-macspoofing max-mac-count** 命令配置业务虚端口上能够绑定的最大 MAC 地址数。缺省情况下，可绑定的最大 MAC 地址数为 8。

说明

如果在用户已经上线的情况下，开启防御 MAC Spoofing 开关，系统没有绑定该用户的 MAC 地址，用户业务会中断，需要下线后重新上线；如果在开启防御 MAC Spoofing 开关后，用户才拨号上线，这时用户的 MAC 地址才被绑定。

----结束

任务示例

举例：配置索引号为 1 的业务虚端口的静态 MAC 地址为 1010-1010-1010，而且该端口的 MAC 地址最大学习数为 0，即该端口只允许源 MAC 地址为 1010-1010-1010 的报文通过，从而达到端口与 MAC 地址绑定的目的。

```
huawei(config)#mac-address static service-port 1 1010-1010-1010
huawei(config)#mac-address max-mac-count service-port 1 0
```

举例：使能 VLAN 10 的防御 MAC Spoofing 功能，配置此 VLAN 创建的索引号为 2 的业务流上可绑定的最大 MAC 地址数为 7。

```
huawei(config)#security anti-macspoofing enable
huawei(config)#vlan service-profile profile-id 3
huawei(config-vlan-srvprof-3)#security anti-macspoofing enable
  Info: Please use the commit command to make modifications take effect
huawei(config-vlan-srvprof-3)#commit
huawei(config-vlan-srvprof-3)#quit
huawei(config)#vlan bind service-profile 10 profile-id 3
huawei(config)#security anti-macspoofing max-mac-count service-port 2 7
```

3.9 配置系统安全

配置设备系统的网络安全和保护措施，以防止系统受到恶意攻击等威胁。

背景信息

系统安全特性的配置是为了防止来自于网络侧或用户侧的非法报文对 MA5631 设备的攻击，从而保证 MA5631 设备在网络上稳定运行。系统安全配置包括：

- ACL 包过滤防火墙
- 黑名单
- 防 DoS 攻击
- MAC 地址过滤
- 用户侧环网检测
- 允许/拒绝访问地址段

系统安全相关的缺省配置如表 3-14 所示。

表 3-14 系统安全缺省配置

参数项	缺省值
防火墙黑名单	去使能
防 DoS 攻击	去使能
用户侧环网检测	去使能

3.9.1 配置防火墙

配置系统防火墙可以对访问设备管理接口的报文进行控制，防止未授权的操作用户通过带内或带外方式入侵系统。

背景信息

防火墙包括：

- 黑名单：使用黑名单功能可以将特定 IP 地址发送来的报文屏蔽，其最主要的一个应用特色是可以动态地进行黑名单表项的添加或删除。当防火墙根据报文的行为特征察觉到特定 IP 地址的攻击企图之后，即可主动添加黑名单表项，从而将该 IP 地址发送过来的报文过滤掉。
- ACL 包过滤防火墙：通过配置 ACL 实施数据包的过滤。当用户需要限制某个端口只可以通过某类型的报文，一般使用 ACL 报文过滤功能来实现。

  例如：用户需要一个端口只允许源 IP 为 1.1.1.1 的报文在下行方向通过，其它报文不能通过，则需要做如下配置：

  1. 配置一条 ACL 规则 rule1，允许源 IP 为 1.1.1.1 的报文通过。
  2. 配置一条 ACL 规则 rule2，禁止所有报文通过。
  3. 使用 **firewall packet-filter** 命令，在下行方向先绑定 rule2，再绑定 rule1。

     说明

     在 MA5631 中，激活 ACL 有两种方式，两种激活方式对于同一 ACL 中的子规则的执行优先级不同：

     - 使用 **firewall packet-filter** 命令激活 ACL，主要用于网管。对于同一 ACL 中的子规则的执行优先级由软件完成，同一 ACL 中的子规则的执行优先级是先配置的优先级高。
     - 使用 **packet-filter** 命令激活 ACL。对于同一 ACL 中的子规则的执行优先级由硬件完成，同一 ACL 中子规则的执行优先级是后配置的优先级高。

注意

为保障设备安全，必须配置防火墙，对访问设备管理接口的报文进行控制。

操作步骤

- 配置防火墙黑名单。

  有两种方式：使用 ACL 规则配置防火墙黑名单功能和通过增加不信任报文的源 IP 地址配置防火墙黑名单功能。这两种方式可以二选一，也可以共同作用。

当两种方式共同作用时，防火墙黑名单功能的优先级比 ACL 规则的优先级要高，即系统首先检查防火墙黑名单，再匹配 ACL 规则。

说明

防火墙黑名单功能只对来自用户侧的报文有效。

- 使用高级 ACL 规则配置防火墙黑名单功能。
  1. 使用 **acl** 命令创建 ACL。使能防火墙黑名单功能同时应用的 ACL 只能是高级 ACL，所以 ACL 的范围为 3000 ～ 3999。
  2. 使用 **rule(adv acl)**命令创建高级 ACL 规则。
  3. 使用 **quit** 命令退回到全局配置模式。
  4. 使用 **firewall blacklist enable acl-number *acl-number*** 命令使能防火墙黑名单功能。
- 通过增加不信任报文的源 IP 地址配置防火墙黑名单功能。
  1. 使用 **firewall blacklist item** 命令在黑名单中增加不信任报文的源 IP 地址。
  2. 使用 **firewall blacklist enable** 命令使能防火墙黑名单功能。

- 配置防火墙（基于 ACL 进行报文过滤）。
  1. 使用 **acl** 命令创建 ACL。配置防火墙包过滤的 ACL 只能是基本和高级 ACL，所以，ACL 的范围为 2000 ～ 3999。
  2. 对于不同的 ACL 需要使用不同的命令创建规则。
     - 基本 ACL 规则：使用 **rule(basic acl)**命令。
     - 高级 ACL 规则：使用 **rule(adv acl)**命令。
  3. 使用 **quit** 命令退回到全局配置模式。
  4. 使用 **firewall enable** 命令使能防火墙黑名单功能。默认去使能。
     如果需要基于基本 ACL 对接口进行报文过滤，需要使能这个功能。
  5. 使用 **firewall packet-filter** 命令在接口上应用防火墙包过滤规则。

----结束

任务示例

举例：将 IP 地址 192.168.10.18 加入到防火墙黑名单，老化时间为 100 分钟。

```
huawei(config)#firewall blacklist item 192.168.10.18 timeout 100
huawei(config)#firewall blacklist enable
```

举例：将 10.10.10.0 网段的 IP 地址加入防火墙黑名单，绑定 ACL 3000。

```
huawei(config)#acl 3000
huawei(config-acl-adv-3000)#rule deny ip source 10.10.10.0 0.0.0.255 destination
 10.10.10.20 0
huawei(config-acl-adv-3000)#quit
huawei(config)#firewall blacklist enable acl-number 3000
```

举例：防止 172.16.25.0 网段的用户访问 IP 地址为 172.16.25.28 的设备维护网口。

```
huawei(config)#acl 3001
huawei(config-acl-adv-3001)#rule 5 deny icmp source 172.16.25.0 0.0.0.255 destin
ation 172.16.25.28 0
huawei(config-acl-adv-3001)#quit
huawei(config)#firewall enable
huawei(config)#interface meth 0
huawei(config-if-meth0)#firewall packet-filter 3001 inbound
 ACL applied successfully
```

3.9.2 配置防对系统的恶意攻击

通过使能防 DoS 攻击、防 ICMP/IP 攻击，以及配置源路由过滤和 MAC 地址过滤，防止恶意用户对系统的攻击，提高系统的安全性。

背景信息

防止恶意用户对系统的攻击有以下几种措施，根据实际需求进行配置。

- 防 DoS 攻击：对用户发送的控制报文进行限制性接收的防御攻击。
- 源 MAC 地址过滤：把用户发送的报文中带有某些源 MAC 的报文过滤掉。
- 用户侧环网检测：对组网中出现的用户侧环网进行检测，以便对环网进行处理，防止环网对业务造成影响。

操作步骤

- 配置防御 DoS 攻击。

  使用 **security anti-dos enable** 命令使能防御 DoS 攻击功能。使能防 DoS 攻击后，系统收到攻击报文，会把用户端口加入黑名单。去使能 DoS 攻击后，系统将删除黑名单。

  应用场景：两台 PC（PC1 和 PC2）通过 MA5631 接入网络，如果其中非法用户（PC1）发送大量协议控制报文，冲击 MA5631 系统 CPU，则会导致 MA5631 设备 CPU 占有率过高，而不能正常处理同设备下其它用户（如 PC2）的业务。需要通过使能防 DoS 攻击功能，屏蔽攻击端口，使 MA5631 设备免受攻击。

- 配置 MAC 地址过滤。

  使用 **security mac-filter** 命令配置 MAC 地址过滤。

  主机动态学习到的 MAC 地址与使用 **security mac-filter source** 命令静态配置的源 MAC 地址共享单板上的 4 条源 MAC 地址表项。静态配置的 MAC 地址表项比动态学习到的 MAC 地址表项优先级高。

  应用场景：为了防止用户假冒网络侧设备的 MAC 地址，或者一些知名的 MAC 地址，可以将网络侧设备的 MAC 地址设置为要过滤的地址。

- 配置用户侧环网检测。

  使用 **ring check enable** 命令使能用户侧环网检测功能。该功能缺省为去使能。

> **注意**
>
> 为保障设备安全，建议开启此功能。

----结束

任务示例

举例：使能系统防御 DoS 攻击功能和用户侧环网检测功能。

```
huawei(config)#security anti-dos enable
huawei(config)#ring check enable
```

3.9.3 配置防非法用户登录

只有配置的允许访问设备的地址段才能访问设备，配置的拒绝访问设备的地址段不能访问设备，以防止非法 IP 地址段的用户登录系统，维护系统的安全。

背景信息

每种防火墙允许添加 10 条地址段信息。

增加一个地址段时，不允许首地址和已有的首地址重复。

删除一个地址段时，只需要输入此地址段的首地址。

操作步骤

- 配置防非法用户通过 Telnet 方式登录设备。
  1. 使用 **sysman firewall telnet enable** 命令使能 Telnet 协议的防火墙功能。系统缺省防火墙处于去使能状态。
  2. 使用 **sysman ip-access telnet** 命令配置允许通过 Telnet 协议访问设备的 IP 地址段。

     注意

     为了保障设备安全，必须遵循最小授权原则，配置允许访问的地址段，且仅在其中增加必要的管理网段 IP 地址，其余 IP 地址不允许访问设备管理接口。
  3. 使用 **sysman ip-refuse telnet** 命令配置拒绝 Telnet 访问设备的 IP 地址段。

     说明

     允许访问的地址段和拒绝访问的地址段最好不重复，只有在允许访问地址段且不在拒绝访问地址段的 IP 地址才能访问设备。
- 配置防非法用户通过 SSH 方式登录设备。
  1. 使用 **sysman firewall ssh enable** 命令使能 SSH 协议的防火墙功能。系统缺省防火墙处于去使能状态。
  2. 使用 **sysman ip-access ssh** 命令配置允许通过 SSH 方式访问设备的 IP 地址段。

     注意

     为了保障设备安全，必须遵循最小授权原则，配置允许访问的地址段，且仅在其中增加必要的管理网段 IP 地址，其余 IP 地址不允许访问设备管理接口。
  3. 使用 **sysman ip-refuse ssh** 命令配置拒绝通过 SSH 方式访问设备的 IP 地址段。

     说明

     允许访问的地址段和拒绝访问的地址段最好不重复，只有在允许访问地址段且不在拒绝访问地址段的 IP 地址才能访问设备。
- 配置防非法用户通过 SNMP 方式（网管）登录设备。

1. 使用 **sysman firewall snmp enable** 命令使能 SNMP 协议的防火墙功能。系统缺省防火墙处于去使能状态。
2. 使用 **sysman ip-access snmp** 命令配置允许通过 SNMP 方式访问设备的 IP 地址段。

注意

为了保障设备安全，必须遵循最小授权原则，配置允许访问的地址段，且仅在其中增加必要的管理网段 IP 地址，其余 IP 地址不允许访问设备管理接口。

3. 使用 **sysman ip-refuse snmp** 命令配置拒绝通过 SNMP 方式访问设备的 IP 地址段。

说明

允许访问的地址段和拒绝访问的地址段最好不重复，只有在允许访问地址段且不在拒绝访问地址段的 IP 地址才能访问设备。

----结束

任务示例

举例：使能系统的 Telnet 协议防火墙，只允许 134.140.5.1 ～ 134.140.5.254 地址段的用户通过 Telnet 方式登录设备。

```
huawei(config)#sysman firewall telnet enable
huawei(config)#sysman ip-access telnet 134.140.5.1 134.140.5.254
```

举例：使能系统的 SSH 协议防火墙，只允许 133.7.22.1 ～ 133.7.22.254 地址段的用户通过 SSH 方式登录设备。

```
huawei(config)#sysman firewall ssh enable
huawei(config)#sysman ip-access ssh 133.7.22.1 133.7.22.254
```

举例：使能系统的 SNMP 协议防火墙，只允许 10.10.20.1 ～ 10.10.20.254 地址段的用户通过 SNMP 方式登录设备。

```
huawei(config)#sysman firewall snmp enable
huawei(config)#sysman ip-access snmp 10.10.20.1 10.10.20.254
```

3.10 配置 ACL 进行报文过滤

介绍了 MA5631 设备中 ACL 分类、ACL 规则及其相关配置。

背景信息

ACL（Access Control List），即访问控制列表，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。ACL 过滤报文流过程是在为进行 QoS 或用户安全的配置做准备。

ACL 分类如**表 3-15** 所示。

表 3-15 ACL 分类列表

类别	取值范围	特点
基本 ACL	2000 ～ 2999	只能根据三层源 IP 制定规则，对数据包进行相应的分析处理。
高级 ACL	3000 ～ 3999	根据数据包的源 IP 地址信息、目的 IP 地址信息、IP 承载的协议类型、针对协议的特性（例如 TCP 的源端口、目的端口、ICMP 消息的类型）等内容制定规则。 利用高级 ACL 制定比基本 ACL 更准确、更丰富、更灵活的规则。
链路层 ACL	4000 ～ 4999	根据源 MAC 地址、VLAN ID、二层协议类型、目的 MAC 地址等链路层信息制定规则，对数据包进行相应的分析处理。

当一条报文流到达，与两条以上的流规则相匹配，系统匹配顺序如下：

- 同一条 ACL 内的子规则，如果同时激活，默认先配置的规则较后配置的规则具有更高的执行优先级。
- 同一条 ACL 内的子规则，如果是逐条单独激活，则后激活的规则较先激活的规则具有更高的执行优先级。
- 不同的 ACL 间下发的子规则，后激活的子规则较先激活的子规则具有更高的执行优先级。

注意事项

由于 ACL 在使用上灵活多变，所以在配置上给出以下建议：

- 建议在任何一条 ACL 的子规则里，首先定义一条普遍适用的规则，例如 permit any 或者 deny any，使任何报文都有一条流规则与之匹配，就能确认没有特别标识报文的默认规则是转发还是过滤。
- 激活后的 ACL 规则会占用到硬件资源，与协议模块（例如 DHCP，IPoA 等）功能共享硬件资源，因为这部分硬件资源较为有限，因此会存在资源不足的情况。为了避免因为 ACL 规则占用相关硬件资源，而造成其他业务功能启动失败的情况，建议用户在配置数据时先启动协议模块，然后再激活 ACL。如果出现启动某个协议模块失败的情况，处理思路如下：
  1. 首先考虑是否是因为 ACL 占用资源过多而导致启动失败。
  2. 如果确认是 ACL 问题，可以去激活或者删除一部分不重要或者暂时不使用的 ACL 配置后，再来进行协议模块的配置和启用。

3.10.1 配置基本 ACL 进行报文过滤

配置基本 ACL 适用于当设备需要根据源 IP 地址对数据包进行流分类的场景。

背景信息

基本 ACL 的编号取值范围为：2000 ～ 2999。

基本 ACL 只能根据三层源 IP 制定规则，对数据包进行相应的分析处理。

操作步骤

步骤 1 （可选）设置时间段。

使用 **time-range** 创建生效时间段，可以在创建 ACL 规则时引用。

步骤 2 创建基本 ACL。

使用 **acl***basic-acl-number* 创建基本 ACL 并且进入该 ACL 模式。ACL 序号的取值只能在 2000 到 2999 之间。

步骤 3 配置基本 ACL 子规则。

在 acl-basic 模式下，使用 **rule** 命令创建基本 ACL 子规则，主要参数：

- *rule-id*：ACL 规则 ID，当需要创建指定 ID 号的 ACL 规则时使用此参数。
- **permit**：允许符合条件的数据包通过的关键字。
- **deny**：丢弃符合条件的数据包的关键字。
- **time-range**：该 ACL 规则生效时间段的关键字。

步骤 4 激活 ACL。

ACL 配置完成后，只是生成了 ACL 控制列表，并不能实际生效，还需要配合其他命令激活 ACL 才能够生效。比较常见的如：

- 使用 **packet-filter** 命令激活 ACL。
- 执行 QoS 操作，请参考**配置基于 ACL 的流量管理**。

----结束

任务示例

举例：每周五的 00:00 到 12:00，MA5631 的端口只能接收来自 2.2.2.2 的数据包，其他数据包将被丢弃。

```
huawei(config)#time-range time1 00:00 to 12:00 fri
huawei(config)#acl 2000
huawei(config-acl-basic-2000)#rule permit source 2.2.2.2 0.0.0.0 time-range time1
huawei(config-acl-basic-2000)#rule deny time-range time1
huawei(config-acl-basic-2000)#quit
huawei(config)#packet-filter inbound ip-group 2000 port
huawei(config)#save
```

3.10.2 配置高级 ACL 进行报文过滤

当设备需要根据数据包的源 IP 地址信息、目的 IP 地址信息、IP 承载的协议类型、协议的特性（例如 TCP 的源端口、目的端口、ICMP 消息的类型）对数据包进行流分类时使用。

背景信息

高级 ACL 的编号取值范围为：3000 ～ 3999。

高级 ACL 支持根据以下信息对报文进行流分类：

- 协议类型
- 源 IP 地址
- 目的 IP 地址
- 源端口号（UDP 或者 TCP 报文的源端口）

- 目的端口号（UDP 或者 TCP 报文的目的端口）
- ICMP 报文的类型
- precedence 值：数据包的优先级字段
- ToS（Type of Service）值：数据包的服务类型字段

操作步骤

步骤 1 （可选）设置时间段。

使用 **time-range** 创建生效时间段，可以在创建 ACL 规则时引用。

步骤 2 创建高级 ACL。

使用 **acl***adv-acl-number* 创建高级 ACL 并且进入 acl-adv 模式，ACL 序号的取值只能在 3000 到 3999 之间。

步骤 3 配置高级 ACL 规则。

在 acl-adv 模式下，使用 **rule** 创建 ACL 规则，主要参数：

- *rule-id*：ACL 规则 ID，当需要创建指定 ID 号的 ACL 规则时使用此参数。
- **permit**：允许符合条件的数据包通过的关键字。
- **deny**：丢弃符合条件的数据包的关键字。
- **time-range**：该 ACL 规则生效时间段的关键字。

步骤 4 激活 ACL。

ACL 配置完成后，只是生成了 ACL 控制列表，并不能实际生效，还需要配合其他命令激活 ACL 才能够生效。比较常见的如：

- 使用 **packet-filter** 命令激活 ACL。
- 执行 QoS 操作，请参考**配置基于 ACL 的流量管理**。

----结束

任务示例

举例：MA5631 的用户板置于 1 槽位，属于一个 VLAN，该 VLAN 具有三层 IP 地址（10.10.10.101）。现在不允许从用户侧发起对设备上 VLAN 接口的 ICMP 操作（如 ping 操作）和 telnet 操作。

```
huawei(config)#acl 3001
huawei(config-acl-adv-3001)#rule 1 deny icmp destination 10.10.10.101 0
huawei(config-acl-adv-3001)#rule 2 deny tcp destination 10.10.10.101 0 destination-port eq telnet
huawei(config-acl-adv-3001)#quit
huawei(config)#packet-filter inbound ip-group 3001 rule 1 port 0/1/0
huawei(config)#packet-filter inbound ip-group 3001 rule 2 port 0/1/0
huawei(config)#save
```

3.10.3 配置链路层 ACL 进行报文过滤

当设备需要根据源 MAC 地址、VLAN ID、二层协议类型、目的 MAC 地址等链路层信息进行流分类时使用。

背景信息

链路层 ACL 的编号取值范围为：4000 ～ 4999。

链路层 ACL 支持根据以下链路层的信息进行分类：

- 以太网承载的协议类型
- 802.1p 优先级
- VLAN ID 信息
- 源 MAC 地址
- 目的 MAC 地址

操作步骤

步骤 1 （可选）设置时间段。

使用 **time-range** 创建生效时间段，可以在创建 ACL 规则时引用。

步骤 2 创建链路层 ACL。

使用 **acl***link-acl-number* 创建链路层 ACL 并且进入 acl-link 模式。ACL 序号的取值只能在 4000 到 4999 之间。

步骤 3 配置链路层 ACL 规则。

在 acl-link 模式下，使用 **rule** 命令创建链路层 ACL 规则，主要参数：

- *rule-id*：ACL 规则 ID，当需要创建指定 ID 号的 ACL 规则时使用此参数。
- **permit**：允许符合条件的数据包通过的关键字。
- **deny**：丢弃符合条件的数据包的关键字。
- **time-range**：该 ACL 规则生效时间段的关键字。

步骤 4 激活 ACL。

ACL 配置完成后，只是生成了 ACL 控制列表，并不能实际生效，还需要配合其他命令激活 ACL 才能够生效。比较常见的如：

- 使用 **packet-filter** 命令激活 ACL。
- 执行 QoS 操作，请参考**配置基于 ACL 的流量管理**。

----结束

任务示例

举例：创建一条允许源 MAC 地址为 2222-2222-2222、目的 MAC 地址为 00e0-fc11-4141、VLAN ID 为 12、COS 值为 1、类型为 0x8863（pppoe-control 消息）的数据包通过的规则。

```
huawei(config)#acl 4001
huawei(config-acl-link-4001)#rule 1 permit type 0x8863 cos 1 source 12
2222-2222-2222 0000-0000-0000 destination 00e0-fc11-4141 0000-0000-0000
huawei(config-acl-basic-4001)#quit
huawei(config)#save
```

3.11 配置 QoS

通过 MA5631 设备中 QoS（Quality of Service）的相关配置操作，向用户的业务提供端到端的质量保证。

背景信息

QoS 是通过一系统的配置，实现为不同的业务提供不同的服务质量。对于 QoS 来说，没有统一的业务模型，所以需要事先做好全网业务的 QoS 规划，然后制定配置方案。

在 MA5631 系统中，QoS 实现的关键点主要是以下内容：

- 流量管理

  通过流量管理的配置，可以实现对用户业务或者针对端口的流量限速。

- 队列调度

  对于已经执行流量管理的业务报文来说，通过队列调度的配置，可以将业务报文置于不同的优先级队列中，实现系统内的 QoS 保证。

除以上关键点之外，MA5631 还支持基于 ACL 的流量管理。

对于用户有灵活需求来实现业务流的 QoS 保障的场景，可以通过 ACL 实现灵活的流分类（请参考“**配置 ACL**”）,然后再对流进行 QoS 动作。

3.11.1 配置流量管理

介绍在 MA5631 上配置流量管理的方法。

概述

MA5631 支持对进入系统或者送出系统的业务流量进行流量管理。

说明

业务流分类的配置方法，请参考 **5.3 创建业务流**。

此外，MA5631 可以针对以太网端口进行限速、可以针对进入系统的广播报文及未知报文（多播、单播）进行流量抑制。

3.11.1.1 配置基于业务流的流量管理

本节介绍基于业务流的流量管理方法。当配置业务虚端口时需要引用 IP 流量模板，并通过模板中定义的流量参数对通过该业务虚端口的流量进行管理。

背景信息

基于业务流的流量管理是首先通过定义 IP 流量模板，然后在创建业务流时引用 IP 流量模板来实现的。

- 系统中存在 7 个缺省的 IP 流量模板，模板 ID 为 0 ～ 6。可以使用 **display traffic table ip** 命令查询这些缺省流量模板的流量参数。
- 建议优先选择缺省的流量模板。只有当缺省的流量模板不能满足用户需求时再配置新的 IP 流量模板。

IP 流量模板中定义的流量参数如**表 3-16** 所示。

表 3-16 IP 流量模板中定义的流量参数列表

配置项	配置参数及说明
双速率三色流量管理参数	CIR：保证信息速率（Committed Information Rate）。 CBS：保证突发量（Committed Burst Size）。 PIR：峰值信息速率（Peak Information Rate）。 PBS：峰值突发量（Peak Burst Size）。 **说明** ● CIR 为必选参数，其它三个参数为可选参数。若只配置 CIR 参数，系统将根据公式计算出其它三个参数值，建议只配置 CIR 参数。 ● 系统根据以上参数，对业务报文标记颜色。红色报文直接丢弃，其他两种颜色的报文则在其 VLAN 标签的 DEI 字段进行标记，黄色标记为 1，绿色标记为 0。
优先级策略	优先级策略有以下三种： ● user-cos：将用户报文外层 VLAN 中的 802.1p 优先级拷贝到上行报文 VLAN 的 802.1p 优先级中。 ● user-inner-cos：将用户报文内层 VLAN（CTag）中的 802.1p 优先级拷贝到上行报文 VLAN 的 802.1p 优先级中。 ● user-tos：将用户报文的 ToS 优先级拷贝到上行报文 VLAN 的 802.1p 优先级中。
调度策略	调度策略有以下两种，只对下行方向的报文有效： ● Tag-In-Package：系统根据报文自带的 802.1p 优先级进行调度。 ● Local-Setting：即本地优先级。系统将根据业务流绑定的流量模板中指定的 802.1p 优先级进行调度。

说明

本文出现的“上行”，是指从用户侧到网络侧的方向；“下行”，是指从网络侧到用户侧的方向。

操作步骤

步骤 1 使用 **display traffic table ip** 查询系统是否存在合适的模板。

检查系统中存在的模板是否和规划好的流量管理参数、优先级策略、调度策略符合，如有合适的流程模板直接通过模板号选择即可。如果不符合，则需要创建新的 IP 流量模板。

步骤 2 使用 **traffic table ip** 命令配置流量模板。

这条命令的具体配置和各个参数说明请参考对应链接中命令参考的详细描述，下面仅对配置过程中涉及关键信息进行简单介绍：

- 流量管理的参数至少必须输入 **CIR** 参数并且赋值。
- 必须输入 **priority** 关键字对报文的外层 802.1p 优先级进行设置。优先级策略的设置有以下 2 种情况：
  - 输入 0－7 之间的数值，为报文指定优先级。

- 使用 user-cos、user-inner-cos 或者 user-tos 这三种从用户侧报文优先级进行拷贝的方法，则还需要输入默认报文的 802.1p 优先级（0－7 之间的数值）。如果用户侧报文没有带优先级时，上行报文的优先级为指定的默认报文的 802.1p 优先级。

- （可选）输入 **inner-priority** 关键字对报文的内层 802.1p 优先级（即报文 CTag 的 802.1p 优先级）进行设置。优先级策略的设置有以下 2 种情况：
  - 输入 0－7 之间的数值，为报文指定优先级。
  - 使用 user-cos、user-inner-cos 或者 user-tos 这三种从用户侧报文优先级进行拷贝的方法，则还需要输入默认报文的 802.1p 优先级（0－7 之间的数值）。如果用户侧报文没有带优先级时，上行报文的优先级为指定的默认报文的 802.1p 优先级。
- 必须输入 **priority-policy** 关键字为下行报文选择调度策略，调度策略请参见**表 3-16**。

步骤 3 使用 **service-port** 绑定适合的流量模板。

说明

创建业务流时，流分类的优先级与流量模板中的优先级保持一致。当修改业务流所绑定的流量模板时，**tx-cttr** 流量模板中的优先级仅仅在队列调度时有效，而流分类的优先级仍然为创建业务流时的优先级。

这条命令的具体配置和各个参数说明请参考对应链接中命令参考的详细描述，下面仅对配置过程中涉及关键信息进行简单介绍：

- 必须输入 **rx-cttr** 和 **tx-cttr** 参数并且赋值：
  - **rx-cttr**：连接接收方向（即从网络侧到用户接入侧）流量索引值。当需要设置连接接收方向流量模板时，使用此参数。
  - **tx-cttr**：连接发送方向（即从用户接入侧到网络侧）流量索引值。当需要设置发送方向流量模板时，使用此参数。
- （可选）输入 **traffic-table** 关键字增加或修改业务虚端口引用的流量模板。
- （可选）输入 **user-encap** 关键字选择用户侧业务封装类型：
  - 当用户侧封装类型为 IPoE 时，选择 ipoe。
  - 当用户侧封装类型为 PPPoE 时，选择 pppoe。

----结束

任务示例

举例：增加一个索引号为 9 的 IP 流量模板：CIR 为 2048Kbit/s，指定上行报文 802.1p 优先级为 6，下行报文调度策略为 tag-In-Package。

```
huawei(config)#traffic table ip index 9 cir 2048 priority 6 priority-policy tag-In-Package
  Create traffic descriptor record successfully
  ------------------------------------------------
  TD Index              : 9
  TD Name               : ip-traffic-table_9
  Priority              : 6
  Copy Priority         : -
  CTAG Mapping Priority: -
  CTAG Default Priority: 0
  Priority Policy       : tag-pri
  CIR                   : 2048 kbps
  CBS                   : 67536 bytes
  PIR                   : 4096 kbps
  PBS                   : 133072 bytes
  Color Mode            : color-blind
  Referenced Status     : not used
-------------------------------------------------
huawei(config)#display traffic table ip index 9
  ------------------------------------------------
```

```
TD Index             : 9
TD Name              : ip-traffic-table_9
Priority             : 6
Copy Priority        : -
CTAG Mapping Priority: -
CTAG Default Priority: 0
Priority Policy      : tag-pri
CIR                  : 2048 kbps
CBS                  : 67536 bytes
PIR                  : 4096 kbps
PBS                  : 133072 bytes
Color Mode           : color-blind
Referenced Status    : not used
-----------------------------------------------
```

3.11.1.2 配置 EoC 局端上行端口限速

通过本任务对 EoC 局端上行端口进行流量限制。

操作步骤

步骤 1 在全局配置模式下，使用 **line-rate** 命令配置对 EoC 局端上行端口进行流量限制。

主要配置参数如下：

- inbound：表示端口的输入方向。
- outbound：表示端口的输出方向。
- target-rate：限制端口的速率，单位为 kbit/s。
- port：取值为机框号/槽位号/端口号。

步骤 2 使用 **display qos-info line-rate port** 命令查询 EoC 局端上行端口流量限制配置值。

----结束

任务示例

举例：设置 EoC 局端上行端口 0/0/0 限速为 6400kbit/s。

```
huawei(config)#line-rate outbound 6400 port 0/0/0
huawei(config)#display qos-info line-rate port 0/0/0

line-rate:
port 0/0/0:
  Outbound:
      line rate: 6400 Kbps
```

3.11.1.3 配置基于用户的限速

通过本任务对指定的 CNU 用户进行速率限制。

前提条件

系统已经配置 CNU。

背景信息

- CNU 限速仅对 CNU 生效。
- 超过指定速率的流量将被丢弃。

操作步骤

步骤 1 在全局配置模式或 EoC 模式下，使用 **cnu line-profile add** 命令增加 CNU 的线路模板时设置其线路上行最大速率，进行限速。

主要参数：

max-transmit-rate-us-value：线路上行最大速率限制值。以 64kbit/s 为粒度进行限制，如果输入的值不是 64 的整倍数，则自动向上进行调整。

步骤 2 在全局配置模式下，使用 **display cnu line-profile** 查询 CNU 线路模板的速率限制配置值。

----结束

任务示例

举例：创建一个模板号为 2 的 CNU 线路模板，线路上行最大速率为 64000kbit/s。

```
huawei(config)#cnu line-profile add 2 rate 64000
huawei(config)#display cnu line-profile 2
  ---------------------------------------------------------------------------
  Profile-ID                    :2
  Profile-name                  :cnu-line-profile_2
  Transmit power(0.1dBm)        :-
  Max up rate(Kbps)             :64000
  bind-times                    :0
  ---------------------------------------------------------------------------
```

3.11.2 配置队列调度

通过配置队列调度为不同优先级的业务提供不同的调度策略，确保不同业务均能得到相应的服务质量。

背景信息

MA5631 根据视频业务（优先级一般为 4）、高速上网业务（优先级一般为 0）配置队列调度策略。当出现拥塞时，系统能在保证高优先级的业务流得到及时处理的同时，也确保低优先级业务的质量。

3.11.2.1 配置队列调度模式

通过本任务配置队列调度方式，确保在发生阻塞时高优先级队列中的报文得到及时处理。

背景信息

MA5631 支持三种队列调度模式：严格优先级调度 PQ（Strict-Priority Queue）、加权轮循调度 WRR（Weighted Round Robin）和 PQ+WRR 调度。

- 严格优先级调度 PQ

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

  缺省情况下系统采用严格优先级调度 PQ 方式。

- 加权轮循调度 WRR

系统支持 8 个优先级队列的加权轮循调度，每个队列有一个加权值（由高到低依次为 w7、w6、w5、w4、w3、w2、w1、w0）。加权值表示获取资源的比重。加权轮循队列调度是在队列之间轮流调度，保证每个队列都得到一定的服务时间。

队列权重与实际队列的对应关系如表 3-17 所示。

表 3-17 队列权重与实际队列的对应关系表

队列号	配置权重	实际队列权重（支持 8 个队列的端口）	实际队列权重（支持 4 个队列的端口）
7	W7	W7	-
6	W6	W6	-
5	W5	W5	-
4	W4	W4	-
3	W3	W3	W7+W6
2	W2	W2	W5+W4
1	W1	W1	W3+W2
0	W0	W0	W1+W0

Wn：表示队列 n 的权重。各队列权重之和必须等于 0 或者 100（队列权重为 255 的除外）。其中，0 表示使用严格优先级队列调度模式；255 表示不使用该队列。

- PQ+WRR 混合调度
  - 系统支持部分队列进行 PQ 调度，部分队列进行 WRR 调度。当指定 WRR 值为 0 时表示该队列进行 PQ 调度。
  - 进行 PQ 调度的队列应是高优先级的队列。
  - 参与轮询调度的各队列权重之和必须等于 100。

操作步骤

步骤 1 使用 **queue-scheduler** 命令配置队列调度方式。

步骤 2 使用 **display queue-scheduler** 命令查询队列调度方式配置信息。

----结束

任务示例

举例：设置队列调度方式为加权轮循调度，8 个队列的权重分别为 10 、10、20、20、10、10、10、10。

```
huawei(config)#queue-scheduler wrr 10 10 20 20 10 10 10 10
huawei(config)#display queue-scheduler
  Queue scheduler mode : WRR
  ---------------------------------
  Queue  Scheduler Mode  WRR Weight
  ---------------------------------
      0  WRR                     10
```

```
    1  WRR                    10
    2  WRR                    20
    3  WRR                    20
    4  WRR                    10
    5  WRR                    10
    6  WRR                    10
    7  WRR                    10
---------------------------------
```

举例：设置队列调度模式为 PQ+WRR 调度，6 个 WRR 调度的队列的权值分别为 20、20、10、30、10、10。

```
huawei(config)#queue-scheduler wrr 20 20 10 30 10 10 0 0
huawei(config)#display queue-scheduler
  Queue scheduler mode : WRR
---------------------------------
Queue  Scheduler Mode  WRR Weight
---------------------------------
    0  WRR                    20
    1  WRR                    20
    2  WRR                    10
    3  WRR                    30
    4  WRR                    10
    5  WRR                    10
    6  PQ                     --
    7  PQ                     --
---------------------------------
```

3.11.2.2 配置队列与 802.1p 优先级的映射关系

配置队列与 802.1p 优先级的映射关系，使系统能根据配置的映射关系将不同优先级的报文分配到指定的队列中。此配置增强了向队列分配报文的灵活性。

背景信息

- 此配置为系统级配置，对所有业务板有效。
- 缺省情况下，队列与 802.1p 优先级的映射关系如表 3-18 所示。

表 3-18 队列与 802.1p 优先级的映射关系表

队列号	实际队列号（支持 8 个队列的端口）	实际队列号（支持 4 个队列的端口）	802.1p 优先级
7	7	3	7
6	6	3	6
5	5	2	5
4	4	2	4
3	3	1	3
2	2	1	2
1	1	0	1
0	0	0	0

操作步骤

步骤 1 使用 **cos-queue-map** 命令配置 802.1p 优先级与队列的映射关系。

步骤 2 使用 **display cos-queue-map** 命令查询 802.1p 优先级与队列映射关系。

----结束

任务示例

举例：配置 802.1p 优先级 0 映射到队列 0，802.1p 优先级 1 映射到队列 2，其它优先级全部映射到队列 6。

```
huawei(config)#cos-queue-map cos0 0 cos1 2 cos2 6 cos3 6 cos4 6 cos5 6 cos6 6 cos7
6
huawei(config)#display cos-queue-map
  CoS and queue map:
  ------------------------
  CoS             Queue ID
  ------------------------
    0                    0
    1                    2
    2                    6
    3                    6
    4                    6
    5                    6
    6                    6
    7                    6
  ------------------------
```

3.11.3 配置早丢弃

介绍早丢弃的配置过程，适用于对队列中的报文进行丢弃设置。

背景信息

早丢弃是指当系统发生拥塞时，对进入队列的报文进行丢弃的行为。此过程发生在流量管理之后。MA5631 支持基于颜色的早丢弃：

MA5631 根据 IP 流量模板里的参数，能够实现基于报文颜色的早丢弃，当入队拥塞时丢弃黄色报文。

操作步骤

步骤 1 增加 WRED（Weighted Random Early Detection，加权随机早期检测）模板。

使用 **wred-profile** 命令增加 WRED 模板。

步骤 2（可选）查询 WRED 模板信息。

使用 **display wred-profile** 命令查询 WRED 模板信息配置是否正确。

步骤 3 设置队列绑定 WRED 模板。

使用 **queue-wred** 命令设置队列绑定 WRED 模板。

----结束

任务示例

举例：增加 WRED 模板 0，设置绿色报文不丢弃，黄色报文丢弃阈值低门限为 50，丢弃阈值高门限为 80，报文丢弃率为 100。报文队列绑定 WRED 模板，队列 0 绑定 WRED 模板0。

```
huawei(config)#wred-profile index 0 green low-limit 100 high-limit 100 discard-probability 0
yellow
low-limit 50 high-limit 80 discard-probability 100
huawei(config)#display wred-profile all
  Command:
          display wred-profile all
 ------------------------------------------------------------------
  WRED profile index: 0
            Low-limit(%)    High-limit(%)    Discard-probability(%)
  Green:             100              100                         0
  Yellow:             50               80                       100
  Queue ID: -
 ------------------------------------------------------------------
huawei(config)#queue-wred queue0 0
```

3.11.4 配置基于 ACL 的流量管理

通过配置 ACL 可以根据用户的需求灵活地实现流分类，当这种基于 ACL 的流分类动作完成后，可以针对这些业务流进行 QoS 动作。

3.11.4.1 配置对匹配 ACL 规则的流量进行限制

通过本任务对通过指定端口匹配 ACL 规则的流量进行限制，并对超过限制的流量进行相应处理。

前提条件

相关 ACL 及其子规则已经完成配置，并且需要限制流量的端口正常工作。

背景信息

- 仅对访问控制列表中动作为 permit 的规则有效。
- 所限制的速率必须是 64kbit/s 的整数倍。

操作步骤

步骤 1 使用 **traffic-limit** 命令对通过指定端口匹配 ACL 规则的流量进行限制。

当端口接收流量超过限制值时直接丢弃。

步骤 2 使用 **display qos-info traffic-limit port** 命令查询指定端口的流量控制信息。

----结束

任务示例

举例：对端口 0/0/0 接收到的匹配 ACL 2001 的流规则的报文流进行限速（限速为 512Kbit/s）。

```
huawei(config)#traffic-limit inbound ip-group 2001 512 port 0/0/0
huawei(config)#display qos-info traffic-limit port 0/0/0
traffic-limit:
```

```
port 0/0/0:
 Inbound:
   Matches: Acl 2001 rule 5     running
     Target rate: 512 Kbps
     Exceed action: drop
```

3.11.4.2 配置对匹配 ACL 规则的流量标记优先级

通过本任务对通过指定端口匹配 ACL 规则的流量标记优先级，使该流量能得到与指定优先级相匹配的服务。可标记的优先级类型有 ToS、802.1p。

前提条件

相关 ACL 及其子规则已经完成配置，并且需要标记优先级的端口正常工作。

背景信息

仅对访问列表中动作为 permit 的规则有效。

操作步骤

步骤 1 使用 **traffic-priority** 命令对通过指定端口匹配 ACL 规则的流量标记优先级。

步骤 2 使用 **display qos-info traffic-priority port** 查询设置的优先级。

----结束

任务示例

举例：将端口 0/0/0 接收到的匹配 ACL 规则 2001 的流量标记优先级。其中本地优先级为 0。

```
huawei(config)#traffic-priority inbound ip-group 2001 local-precedence 0 port 0/0/0
huawei(config)#display qos-info traffic-priority port 0/0/0

traffic-priority:
port 0/0/0:
 Inbound:
   Matches: Acl 2001 rule 5  running
     Priority action: local-precedence 0
```

3.11.4.3 配置对匹配 ACL 规则的流量进行统计

通过本任务对匹配 ACL 规则的流量进行统计，以便对该流量进行分析、监控。

前提条件

相关 ACL 及其子规则已经完成配置，并且需要流量统计的端口正常工作。

背景信息

仅对访问列表中动作为 permit 的规则有效。

操作步骤

步骤 1 使用 **traffic-statistic** 命令对通过指定端口匹配 ACL 规则的流量进行统计。

步骤 2 使用 **display qos-info traffic-statistic port** 查询通过指定端口匹配 ACL 规则的流量统计信息。

----结束

任务示例

举例：对端口 0/0/0 接收到的匹配 ACL 2001 规则的流量进行统计。

```
huawei(config)#traffic-statistic inbound ip-group 2001 port 0/0/0
huawei(config)#display qos-info traffic-statistic port 0/0/0

traffic-statistic:
port 0/0/0:
 Inbound:
   Matches: Acl 2001 rule 5     running
     0 packet
```

3.11.4.4 配置对匹配 ACL 规则的流量进行镜像

通过本任务将通过某端口且匹配 ACL 规则的流量镜像到指定端口上。镜像操作不会影响镜像源端口上流量的接收与发送。用户可以对通过镜像目的端口的流量进行分析，实现对镜像源端口上流量的监控。

前提条件

相关 ACL 及其子规则已经完成配置，并且需要流镜像的端口正常工作。

背景信息

- 仅对访问列表中动作为 permit 的规则有效。
- 镜像目的端口不能是聚合端口。
- 系统只支持一个镜像目的端口，并且镜像目的端口只能是上行端口。

操作步骤

步骤 1 使用 **traffic-mirror** 命令对通过指定端口匹配 ACL 规则的流量进行镜像操作。

步骤 2 使用 **display qos-info traffic-mirror port** 命令查询指定端口匹配 ACL 规则的流镜像信息。

----结束

任务示例

举例：将端口 0/0/1 下接收到的匹配 ACL 规则 2001 的流量镜像到端口 0/0/0。

```
huawei(config)#traffic-mirror inbound ip-group 2001 port 0/0/1 to port 0/0/0
huawei(config)#display qos-info traffic-mirror port 0/0/1

traffic-mirror:
port 0/0/1:
 Inbound:
   Matches: Acl 2001 rule 5     running
   Mirror to: port 0/0/0
```

3.12 配置 H831VESC 监控

MA5631 可以通过内置的虚拟环境监控单元 H831VESC 来监控设备所处的环境状态，以下介绍 H831VESC 的配置方法。

背景信息

- H831VESC 为 MA5631 设备主控板内置虚拟环境监控单元，主控板上的 ALARM 口通过环境监控电缆和外置传感器相连。
- H831VESC 的 EMU ID 与机框连接的从节点号由系统默认配置，用户无法自行修改。
- 对于 H831VESC，系统支持 4 个数字量，用户均可自行定义。其中：
  - 数字量 0 名称默认为烟雾。
  - 数字量 1 名称默认为机柜门。
  - 数字量 2 名称默认为防雷器。
  - 数字量 3 名称默认为配线架。

  系统缺省数字量的默认有效电平均为高电平。

操作步骤

步骤 1 查询 H831VESC 状态。

使用 **display emu** 命令查询环境监控单元的运行状态。

步骤 2 配置数字量参数。

使用 **esc digital** 命令设置环境监控单元数字量的有效电平、标识该数字量的名称、数字量的告警索引等参数。

步骤 3 查询 H831VESC 环境信息。

使用 **display esc environment info** 命令查询环境量信息。

步骤 4 保存数据。

使用 **quit** 命令退出 H831VESC 模式后，使用 **save** 命令保存数据。

----结束

操作结果

配置完成后，H831VESC 正常工作，且对 MA5631 所设置的数字监控量进行监控。当实际监控数字量的电平和系统配置有效电平不一致时，MA5631 将上报故障告警。

任务示例

举例：配置环境监控单元 H831VESC，参数规划如表 3-19 所示。

表 3-19 H831VESC 配置数据规划表

配置项	数据	备注
数字量参数	数字量 ID：0	-
	数字量 0 的有效电平：低电平	使用低电平来代表有效电平，低电平时主机不上报告警。
	数字量 0 的名称：Smoke	根据实际需要配置数字量参数。此处为监控烟感的监控数字量，对烟感的状态进行监控。
	数字量 0 的自定义告警索引：0	当设备所在环境存在烟雾时，主机将上报告警。
	数字量 ID：1	-
	数字量 1 的有效电平：高电平	使用高电平来代表有效电平，高电平时主机不上报告警。
	数字量 1 的名称：Door	根据实际需要配置的数字量来设置。此处为门禁的监控数字量，对门禁的状态进行监控。
	数字量 1 的自定义告警索引：1	当机柜门被打开时，主机将上报告警。
	数字量 ID：2	-
	数字量 2 的有效电平：低电平	使用低电平来代表有效电平，低电平时主机不上报告警。
	数字量 2 的名称：Arrester	根据实际需要配置数字量参数。此处为防雷模块的监控数字量，对防雷模块的状态进行监控。
	数字量 2 的自定义告警索引：2	当防雷模块故障时，主机将上报告警。
	数字量 ID：3	-
	数字量 3 的有效电平：低电平	使用低电平来代表有效电平，低电平时主机不上报告警。
	数字量 3 的名称：Wiring	根据实际需要配置的数字量来设置。此处为配线架的监控数字量，对配线架的状态进行监控。
	数字量 3 的自定义告警索引：3	当配线架故障时，主机将上报告警。

```
huawei(config)#display emu 0

  EMU ID: 0
  ------------------------------------------------------------------------
  EMU name     : H831VESC
  EMU type     : H831VESC
```

```
  Used or not : Used
  EMU state   : Normal
  Frame ID    : 0
  Subnode     : 1
  COM port    : RS232
  ---------------------------------------------------------------------------
huawei(config)#interface emu 0
huawei(config-if-h831vesc-0)#esc digital 0 available-level low-level digital-alarm 0 name Smoke
huawei(config-if-h831vesc-0)#esc digital 1 available-level high-level digital-alarm 1 name Door
huawei(config-if-h831vesc-0)#esc digital 2 available-level low-level digital-alarm 2 name Arrester
huawei(config-if-h831vesc-0)#esc digital 3 available-level low-level digital-alarm 3 name Wiring
huawei(config-if-h831vesc-0)#display esc environment info

  EMU ID: 0                          ESC environment state
  -------------------------Digital environment info--------------------------
  ID Name               State  Value |ID Name               State  Value
  0  Smoke              Alarm  1     |1  Door               Normal 1
  2  Arrester           Alarm  1     |3  Wiring             Alarm  1
  ---------------------------------------------------------------------------
huawei(config-if-h831vesc-0)#quit
huawei(config)#save
```

4 配置 CNU 管理

关于本章

在 MA5631 上对 CNU 的管理、CNU 运行相关的功能进行配置。一个 EoC 局端模块最多支持配置 64 个 CNU。MA5631 一共可支持 256 个 CNU。

4.1 （可选）配置 CNU 线路模板
通过本任务完成对 CNU 线路模板的配置。配置的 CNU 线路模板可以根据需要绑定到 CNU 上，进行 CNU 流量管理。

4.2 配置通过自动发现方式增加 CNU
本任务介绍确认自动发现的 CNU 的方法。

4.3 配置通过离线方式增加 CNU
本任务配置通过离线方式增加 CNU。

4.4 （可选）配置 CNU 端口属性
通过本任务对指定的以太网端口进行属性配置，使 CNU 与 MA5631 设备通讯正常。

4.1 （可选）配置 CNU 线路模板

通过本任务完成对 CNU 线路模板的配置。配置的 CNU 线路模板可以根据需要绑定到 CNU 上，进行 CNU 流量管理。

操作步骤

步骤 1 配置 CNU 线路模板。

在全局配置模式或 EoC 模式下，使用 **cnu line-profile add** 命令配置 CNU 线路模板。

步骤 2 在使用 **cnu add** 命令添加或者使用 **cnu confirm** 命令确认 CNU 时，可以将 CNU 线路模板绑定到对应的 CNU。

----结束

任务示例

举例：添加一个 EoC 局端模块线路模板，模板编号为 2，并与 CNU 进行绑定。其中模板参数规划如下：

- 线路发送功率为 100dB
- 线路上行最大速率为 64000kbit/s

```
huawei(config-if-eoc-0/1)#cnu line-profile add 2 rate 64000 power 100
huawei(config-if-eoc-0/1)#cnu confirm 0 all lineprofile-id 2
```

4.2 配置通过自动发现方式增加 CNU

本任务介绍确认自动发现的 CNU 的方法。

背景信息

EoC 局端、CNU 安装完毕正常上电后，启动 CNU 自动发现功能。

操作步骤

步骤 1 对自动发现的 CNU 进行确认，分为三种情况：

- 使用 **cnu auto confirm** 使能 CNU 自动确认功能对同一 EoC 模块下的所有自动发现 CNU 或指定的自动发现 CNU 进行确认。前提条件是必须将 CNU 和 EoC 模块正常连接并上电。
- 使用 **cnu confirm** ***portid*** **all** 命令对同一 EoC 模块下的所有自动发现 CNU 进行确认。
- 使用 **cnu confirm** ***portid cnuid*** 命令对同一 EoC 模块下指定的自动发现 CNU 进行确认。
- 在使用 **cnu confirm** 命令确认 CNU 时有以下参数可选配置。
  - **lineprofile-id**：CNU 线路模板编号。通过指定 CNU 线路模板编号来为 CNU 绑定线路模板。
  - **lineprofile-name**：CNU 线路模板名称。通过指定 CNU 线路模板名称来为 CNU 绑定线路模板。

- **desc**：CNU 的描述信息。可选参数，建议为每个 CNU 都增加位置、时间等相关描述信息，有利于对 CNU 的管理和维护。
- **alarm-switch**：设置 CNU 告警上报控制开关。此参数可选，不输入时，默认告警关闭。

说明

批量确认 CNU 时，默认均以 MAC 认证方式进行认证；单个确认 CNU 时，必须通过命令行指定认证方式。

步骤 2 可以使用 **cnu cancel** 命令删除处于自动发现状态的 CNU。

步骤 3 使用 **cnu blacklist** 命令增加或删除 CNU 到黑名单中。增加到黑名单中的 CNU 不再自动发现，不允许上线。

----结束

任务示例

举例：确认 EoC 局端模块端口 0/1/0 下自动发现的 CNU。具体数据规划如下：

- CNU ID 为 0
- CNU MAC 地址为 00B0-5240-0003
- 绑定线路模板 1
- 增加 CNU 描述信息为 huaweicnu
- CNU 告警上报控制开关采用默认关闭

```
huawei(config-if-eoc-0/1)#cnu confirm 0 0 mac-auth 00B0-5240-0003 lineprofile-id
 1 desc huaweicnu
```

4.3 配置通过离线方式增加 CNU

本任务配置通过离线方式增加 CNU。

背景信息

CNU 安装完毕正常上电前，可以在 EoC 局端模块上离线增加 CNU，在 CNU 不在线的情况下对业务进行配置。CNU 上线后，配置数据通过 MME 消息管理协议下发到 CNU，完成配置过程。

操作步骤

步骤 1 离线增加 CNU。

使用 **cnu add** ***portid cnuid*** 命令增加 CNU。在使用 **cnu add** 命令增加 CNU 时有以下参数可选配置。

- **lineprofile-id**：CNU 线路模板编号。通过指定 CNU 线路模板编号来为 CNU 绑定线路模板。
- **lineprofile-name**：CNU 线路模板名称。通过指定 CNU 线路模板名称来为 CNU 绑定线路模板。
- **desc**：CNU 的描述信息。可选参数，建议为每个 CNU 都增加位置、时间等相关描述信息，有利于对 CNU 的管理和维护。

- **alarm-switch**：设置 CNU 告警上报控制开关。此参数可选，不输入时，默认告警关闭。

----结束

任务示例

举例：在 EoC 局端模块端口 0/1/0 下离线增加 CNU。具体数据规划如下：

- CNU ID 为 0
- CNU SN 为 hwhw-12341234
- 绑定线路模板 1
- 增加 CNU 描述信息为 huaweicnu
- CNU 告警上报控制开关采用默认关闭

```
huawei(config-if-eoc-0/1)#cnu add 0 0 sn-auth hwhw-12341234 lineprofile-id 1
desc huaweicnu
```

4.4 （可选）配置 CNU 端口属性

通过本任务对指定的以太网端口进行属性配置，使 CNU 与 MA5631 设备通讯正常。

背景信息

CNU 使用以太网端口对接时需要注意与对接设备端口属性的一致性。

缺省配置

以太网端口属性的系统缺省值如表 4-1 所示。

表 4-1 以太网端口属性缺省值

参数项	缺省值
端口自协商模式	打开
端口速率	不支持设置 1000Mbit/s
双工模式	全双工
激活开关	打开
流量控制	关闭

操作步骤

- 配置 CNU 的端口属性。

  在 EoC 模式下，使用 **cnu port attribute** 命令配置 CNU 上的以太网端口属性，主要参数：

  - **auto-neg**：CNU 以太网端口自协商模式。可以对自协商模式进行使能或者去使能：

  - 当使能自协商模式后，端口自动和对接端口协商以太网端口的端口速率和工作模式。
  - 当去使能自协商模式后，端口的速率和工作模式处于强制模式（使用默认或命令行设置的速率和工作模式）。
- **speed**：CNU 以太网端口速率。当端口速率配置成功后，可以使端口以设定的速率工作。进行配置时的注意事项：
  - 配置原则是互连的两个设备对应端口的端口速率应一致，以避免无法通讯的问题。
  - 需要去使能自协商模式。
- **duplex**：CNU 以太网端口双工模式。端口双工状态可以为半双工、全双工模式，进行设置时的注意事项：
  - 设置原则是互连的两个设备对应端口双工状态应一致，以避免无法通讯的问题。
  - 需要去使能自协商模式。
- **operational-state**：CNU 以太网端口的激活开关。
- **flow-control**：CNU 以太网端口的流量控制。当以太网端口的流量比较大，需要对其进行控制时，使用此参数，以避免造成网络拥塞，丢失数据包。

----结束

任务示例

举例：设置 CNU 以太网端口属性为：端口速率 100Mbit/s，全双工模式，支持流量控制，不支持自协商模式，以太网端口的激活开关打开。

```
huawei(config)#interface eoc 0/1
huawei(config-if-eoc-0/1)#cnu port attribute 0 1 eth 1 auto-neg off
huawei(config-if-eoc-0/1)#cnu port attribute 0 1 eth 1 speed 100
huawei(config-if-eoc-0/1)#cnu port attribute 0 1 eth 1 duplex full
huawei(config-if-eoc-0/1)#cnu port attribute 0 1 eth 1 flow-control on
huawei(config-if-eoc-0/1)#cnu port attribute 0 1 eth 1 operational-state on
```

5 配置 EoC 宽带业务

关于本章

介绍 EoC 宽带业务的相关配置操作。

背景信息

配置宽带业务前，CNU 必须已经和 EoC 模块正常连接，CNU 的相关配置可参见**配置 CNU 管理**。

5.1 配置 VLAN
配置 VLAN 为配置业务的基础，在进行业务配置前需要保证 VLAN 已经按照实际规划完成配置。

5.2 配置上行端口
将带某一特定 VLAN 的用户报文通过上行端口上行，需要将上行端口加入到 VLAN 中。

5.3 创建业务流
业务流用于打通用户侧与网络侧的业务通道，要开通业务，必须配置业务流。

5.1 配置 VLAN

配置 VLAN 为配置业务的基础，在进行业务配置前需要保证 VLAN 已经按照实际规划完成配置。

前提条件

规划的 VLAN ID 未被占用。

应用环境

不同类型的用户对 VLAN 的应用不一样，具体应用情况如表 5-1 所示。

表 5-1 VLAN 应用及规划

用户类型	应用场景	VLAN 规划
● 住宅用户 ● 商业用户的上网业务	N:1 场景，即单层 VLAN 上行，多个用户的业务汇聚到同一个 VLAN。	VLAN 类型：Smart VLAN 属性：Common
	1:1 场景，即双层 VLAN 上行，外层 VLAN 用于标识业务，内层 VLAN 用于标识用户。	VLAN 类型：Smart VLAN 属性：Stacking
商业用户的透传业务	只适用于商业用户的透传业务。	VLAN 类型：Smart VLAN 属性：QinQ

缺省配置

VLAN 的缺省配置如表 5-2 所示。

表 5-2 VLAN 缺省配置

参数项	缺省值	备注
系统缺省 VLAN	VLAN ID：1 类型：Smart VLAN	-
系统缺省保留 VLAN	VLAN 范围：4079 ～ 4093	可使用 **vlan reserve** 命令修改系统的保留 VLAN。
新建 VLAN 缺省属性	Common	-
VLAN 转发模式	VLAN+MAC	-

操作步骤

步骤 1 创建 VLAN。

使用 **vlan** 命令创建 VLAN，不同类型的 VLAN 应用于不同的场景。

表 5-3 VLAN 类型及应用场景

VLAN 类型	配置命令	VLAN 描述	应用场景
Standard VLAN	单个增加 VLAN：**vlan *vlanid* standard**	标准 VLAN。 一个 Standard VLAN 只包含多个上行端口，VLAN 中的以太网端口可相互通信，VLAN 间的以太网端口相互隔离。	只适用于以太网端口。应用于网管通信、设备级联等。
Smart VLAN	单个增加 VLAN：**vlan *vlanid* smart**	一个 Smart VLAN 中可包含多个上行端口和多个业务虚端口，且同一个 Smart VLAN 包含的业务虚端口相互隔离。VLAN 间的业务虚端口也相互隔离。一个 VLAN 可接入多个用户，减少了对 VLAN 数量的占用。	应用于 GE 接入业务，如小区接入。
MUX VLAN	单个增加 VLAN：**vlan *vlanid* mux**	一个 MUX VLAN 可包含多个上行端口，但只包含一个业务虚端口，VLAN 间的业务虚端口相互隔离。VLAN 与接入用户存在一对一的映射关系，因此可根据 VLAN 区分不同的接入用户。	应用于 GE 接入业务，如用 VLAN 来区分用户。

说明

- 批量增加 VLAN ID 连续的 VLAN 使用 **vlan *vlanid* to *end-vlanid*** 命令。
- 批量增加 VLAN ID 非连续的 VLAN 使用 **vlan *vlan-list*** 命令。

步骤 2 （可选）配置 VLAN 属性。

VLAN 创建后，缺省属性为 Common，使用 **vlan attrib** 命令配置 VLAN 属性。

根据 VLAN 的规划情况进行选配。

表 5-4 VLAN 属性及应用场景

VLAN 属性	配置命令	VLAN 类型	VLAN 描述	应用场景
Common	创建 VLAN 后默认属性为 Common。	可以是 Standard VLAN、Smart VLAN 和 MUX VLAN。	具有 Common 属性的 VLAN 可作为普通的二层 VLAN 或创建三层虚接口使用。	用于 N:1 接入场景。
VLAN Stacking	配置单个 VLAN 的属性：**vlan attrib *vlanid* stacking**	只能为 Smart VLAN 或 MUX VLAN。	具有 Stacking 属性的 VLAN 报文包含有 MA5631 分配的内、外两层 VLAN 标签。上层 BRAS 设备可根据两层标签进行双 VLAN 认证，增加接入用户的数量。在二层工作模式的上层网络中，还可以直接通过外层 VLAN+MAC 进行报文转发，为 ISP（Internet Service Provider）提供批发业务功能。	用于 1:1 接入场景，可用于批发业务或 VLAN ID 扩展。 VLAN Stacking 需要使用 **stacking label** 命令配置业务虚端口的标签。 MA5631 支持通过 **stacking outer-ethertype** 命令设置系统 VLAN Stacking 支持的外层以太网协议类型；通过 **stacking inner-ethertype** 命令设置系统 VLAN Stacking 支持的内层以太网协议类型。为了实现设备与其它厂商的设备对接，使用命令将外层/内层以太网协议类型设置为与对接设备一致。

说明

- 批量配置 ID 连续的 VLAN 属性使用 **vlan attrib *vlanid* to *end-vlanid*** 命令。
- 批量配置 ID 非连续的 VLAN 属性使用 **vlan attrib *vlan-list*** 命令。

步骤 3 （可选）配置 VLAN 的描述信息。

使用 **vlan desc** 命令配置 VLAN 的描述信息。为了方便维护，可以增加 VLAN 的描述信息，VLAN 描述信息一般为 VLAN 的用途、相关业务信息等。

----结束

任务示例

举例：创建 VLAN 50，VLAN 属性为 Stacking，用于 VLAN ID 扩展。为 VLAN 50 增加业务虚端口，索引值为 100，CNU ID 为 1，物理端口为 1-4，接收方向采用流量表项 9，发送方向采用流量表项 9。VLAN Stacking 的外层 VLAN Tag 50 用于标识接入设备，内层 VLAN Tag 10 用于标识该设备接入的用户。增加 VLAN 的描述信息以方便维护。

```
huawei(config)#vlan 50 smart
huawei(config)#vlan attrib 50 stacking
huawei(config)#service-port 100 vlan 50 eoc 0/1/0 cnu 1 eth 1-4 multi-service
user-vlan untagged inbound traffic-table index 9 outbound traffic-table index 9
huawei(config)#stacking label vlan 50 baselabel 10
huawei(config)#vlan desc 50 description stackingvlan/label10
```

5.2 配置上行端口

将带某一特定 VLAN 的用户报文通过上行端口上行，需要将上行端口加入到 VLAN 中。

前提条件

- MA5631 设备与 OLT 对接成功。
- MA5631 设备已经**配置 VLAN**。

操作步骤

步骤 1 增加 VLAN 上行端口。

使用 **port vlan** 命令将上行端口加入到 VLAN 中。

步骤 2 （可选）配置上行端口属性。

为了与上层设备正常对接，缺省的上行口属性不能满足需求时需要配置。具体配置请参考 **3.3 配置上行端口属性**。

----结束

任务示例

举例：将上行端口 0/0/0 加入到 VLAN 100 中。

```
huawei(config)#port vlan
{ vlan-list<S><Length 1-256>|vlanid<U><1,4093> }:100
{ frame/slot<S><Length 1-15>|to<K> }:0/0
{ portlist<S><Length 1-256> }:1

  Command:
          port vlan 100 0/0 1
```

5.3 创建业务流

业务流用于打通用户侧与网络侧的业务通道，要开通业务，必须配置业务流。

背景信息

业务流可以承载单业务也可以承载多业务。

操作步骤

步骤 1 创建流量模板。

使用 **traffic table ip** 命令创建流量模板。系统中存在 7 个缺省的流量模板，模板 ID 为 0 ～ 6。

创建业务流之前，先使用 **display traffic table** 命令确认系统中是否有已经满足需求的流量模板。如果没有，必须先根据应用需求创建流量模板。关于流量模板的详细介绍请参考“3.11.1.1 配置基于业务流的流量管理”。

步骤 2 创建业务流。

可以创建单个业务流，也可以批量创建业务流，根据需要进行二选一。

- 使用 **service-port** 命令创建业务流。
  - 基于用户侧 VLAN 的多业务流：

    选择 **multi-service user-vlan untagged inbound outbound**。
    - **untagged**：用户侧报文不带标签。
    - **inbound**：连接发送方向（即从用户接入侧到网络侧）。
    - **outbound**：连接接收方向（即从网络侧到用户接入侧）。

  说明

  - 系统支持按照索引值创建业务流，一个索引值对应一个业务流，并且不需要输入大量的流参数，简化了业务流的配置。在创建业务流时，*index* 为可选配置，指业务流的索引值。如果不设置该索引值，系统自动分配一个最小的数字。
  - 引用的流量模板即为操作步骤**步骤 1** 中创建的流量模板。
- 使用 **multi-service-port** 命令批量增加业务流。

步骤 3 配置业务流的属性，根据需要进行选配。

- 使用 **service-port desc** 命令配置业务流的描述信息。为了方便维护，可以增加业务流的描述信息，描述信息一般为业务流的用途、相关业务信息等。
- 使用 **service-port *index* adminstatus** 命令配置业务流的管理状态。缺省情况下，业务流为激活状态。

  业务的开通基于两级开关，端口级和业务流级。如果要为某用户开通业务，则必须激活用户的接入端口和对应的业务流。
- 使用 **mac-address max-mac-count service-port** 命令配置业务流的最大 MAC 地址学习数，以限制同一帐号下可上网的最大 PC 数。

----结束

任务示例

举例：商业用户要求开通 8192Kbit/s 的上网业务，为了后续业务扩展，MA5631 通过 EoC 模块为此用户提供上网业务，基于用户侧 VLAN 来区分用户，业务侧 VLAN 为 50，用户侧 VLAN 属性为 untagged。查询后发现系统中没有合适的流量模板。需要立即为用户开通上网业务。为了方便维护，增加业务流的描述信息。

```
huawei(config)#display traffic table ip from-index 0
{ <cr>|to-index<K> }:

  Command:
          display traffic table ip from-index 0
  ------------------------------------------------------------------------
   TID CIR(kbps) CBS(bytes) PIR(kbps) PBS(bytes) Pri Copy-policy    Pri-Policy
```

```
  ------------------------------------------------------------------------
    0       512      18384      1024      36768   6 -              tag-pri
    1      1024      34768      2048      69536   0 -              tag-pri
    2      2048      67536      4096     135072   0 -              tag-pri
    3      4096     133072      8192     266144   4 -              tag-pri
    4      8192     264144     16384     528288   4 -              tag-pri
    5     16384     526288     32768    1024000   4 -              tag-pri
    6       off        off       off        off   0 -              tag-pri
  ------------------------------------------------------------------------
  Total Num : 7
huawei(config)#traffic table ip index 9 cir 8192 priority 4 priority-policy loca
l-Setting
  Create traffic descriptor record successfully
  ------------------------------------------------
  TD Index             : 9
  TD Name              : ip-traffic-table_9
  Priority             : 4
  Copy Priority        : -
  CTAG Mapping Index   : -
  CTAG Default Priority: 0
  Priority Policy      : local-pri
  CIR                  : 8192 kbps
  CBS                  : 264144 bytes
  PIR                  : 16384 kbps
  PBS                  : 526288 bytes
  Color Mode           : color-blind
  Referenced Status    : not used
  ------------------------------------------------
huawei(config)#service-port 6 vlan 50 eoc 0/1/0 cnu 1 eth 1-4 multi-service user-vlan
 untagged inbound traffic-table index 9 outbound traffic-table index 9
huawei(config)#service-port desc 6 description HW_eoc/VlanID:50/uservaln:untagged
```

6 配置组网保护

关于本章

MA5631 提供了冗余或备份机制，通过冗余或备份实现了系统的高度可靠性和自愈能力，保证在突发意外出现时，最大程度保全运营商提供的业务和客户网络的稳定性，使损失降到最低。

背景信息

在电信级运营中，为了保证系统在某些意外和灾难性事件发生时仍然正常工作，一般采用增加冗余（备份）设备或部件的方式来提高整个系统的可靠性。

6.1 配置 MSTP
介绍 MSTP 协议在 MA5631 设备中的相关配置。

6.2 配置以太网上行端口链路聚合
端口聚合是将 MA5631 的两个 GE 上行端口聚合在一起，通过负荷分担的工作方式提高传输带宽。当聚合的某个 GE 端口或 GE 链路故障时，设备通过另一个 GE 端口传输业务，提高传输可靠性。

6.1 配置 MSTP

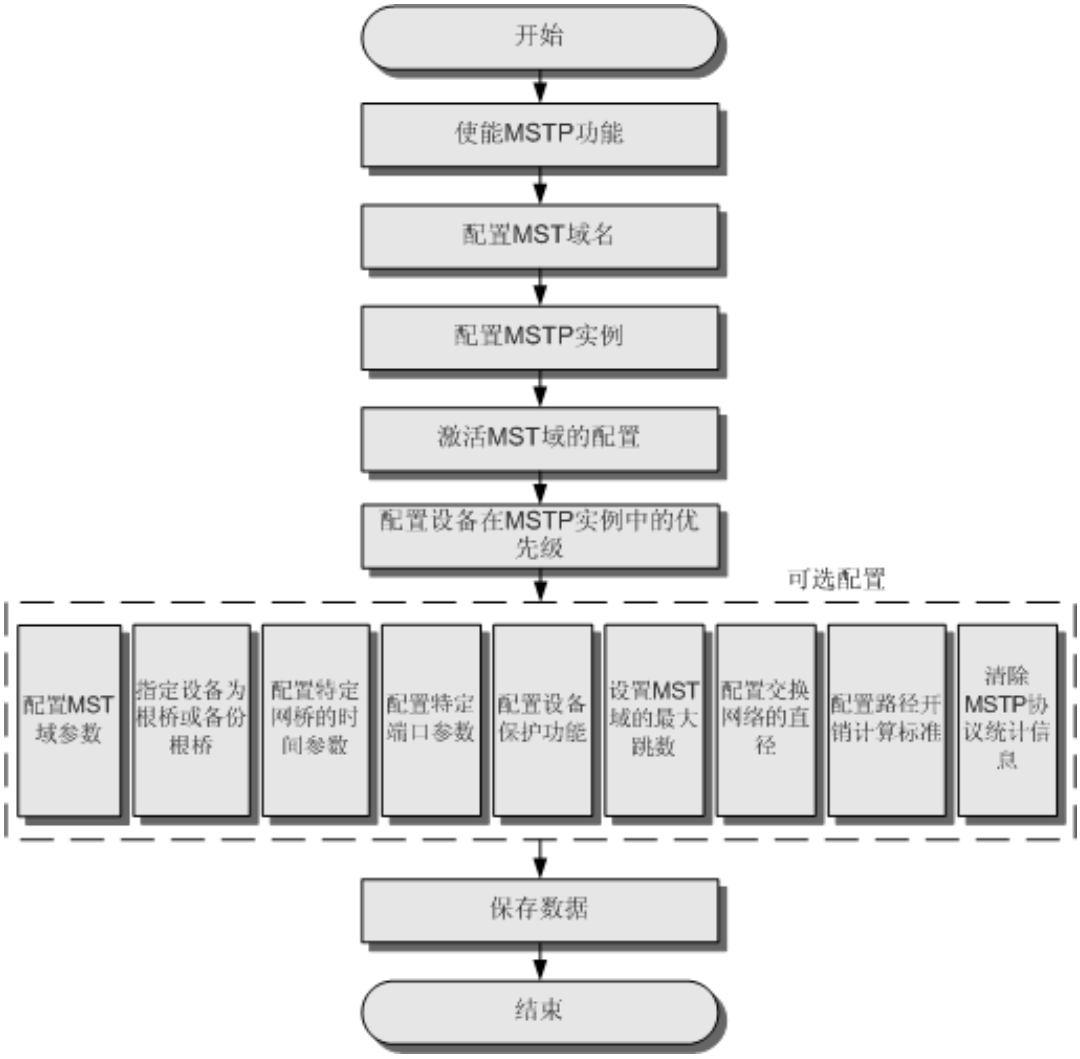
介绍 MSTP 协议在 MA5631 设备中的相关配置。

背景信息

- MSTP（Multiple Spanning Tree Protocol，多生成树协议）应用于冗余网络，弥补 STP 和 RSTP 的缺陷，它既可以快速收敛，也能使不同 VLAN 的流量沿各自的路径分发，从而为冗余链路提供了更好的负载分担机制。
- MSTP 将环路网络修剪成为一个无环的树型网络，避免报文在环路网络中的增生和无限循环，同时还提供了数据转发的多个冗余路径，在数据转发过程中实现 VLAN 数据的负载均衡。

MSTP 配置流程如图 6-1 所示。

图 6-1 MSTP 配置流程图



操作步骤

步骤 1 使能 MSTP 功能。

- 缺省情况下，设备上的 MSTP 功能处于去使能状态。
- 在 MSTP 功能使能后，设备会根据用户配置的协议模式来决定是在 STP 兼容模式下运行或者是在 MSTP 模式运行。
- MSTP 功能使能后，MSTP 根据收到的配置消息（即 BPDU 报文）动态维护相应 VLAN 的生成树状态；MSTP 功能去使能后，如果去使能 BPDU 报文透传功能，MSTP 设备将成为透明桥，将不再维护生成树的状态。

1. 使用 **stp enable** 命令或 **stp port enable** 命令使能网桥或端口的 MSTP 功能。
2. 使用 **display stp** 命令或 **display stp port** 命令查询网桥或端口的 MSTP 功能是否已经使能。

步骤 2 配置 MST 域名。

1. 使用 **stp region-configuration** 命令进入 MST 域模式。
2. 使用 **region-name** 命令配置 MST 域的名称。
3. 使用 **check region-configuration** 命令查询当前 MST 域的参数配置信息。

步骤 3 配置 MSTP 实例。

配置 VLAN 映射表（即 VLAN 和生成树的对应关系表），把 VLAN 和生成树联系起来。

- 缺省情况下，所有 VLAN 均映射到 CIST，即实例 0 上。
- 一个 VLAN 只能映射到同一个实例上，如果将一个已经设置映射的 VLAN 重新映射到一个不同的实例上时，则自动取消原来的映射关系。
- 一个 MSTP 实例中最大允许配置 10 个 VLAN 段。

1. 使用 **stp region-configuration** 命令进入 MST 域模式。
2. 使用 **instance vlan** 命令映射指定 VLAN 到指定 MSTP 实例。
3. 使用 **check region-configuration** 命令查询当前 MST 域的参数配置信息。

步骤 4 激活 MST 域的配置。

1. 使用 **stp region-configuration** 命令进入 MST 域模式。
2. 使用 **active region-configuration** 命令激活 MST 域的配置。
3. 使用 **display stp region-configuration** 命令查询 MST 域已生效的参数配置信息。

步骤 5 配置设备在 MSTP 实例中的优先级。

1. 使用 **stp priority** 命令配置设备在指定生成树实例中的优先级。
2. 使用 **display stp** 命令查询当前设备上 MSTP 的配置信息。

步骤 6 其它可选配置。

- 配置 MST 域参数。
  - 使用 **stp md5-key** 命令设定域配置 MD5 加密算法的 MD5-KEY 值。
  - 在 MSTP 域模式下，使用 **vlan-mapping module** 命令按模映射所有 VLAN 到指定的 MSTP 实例。
  - 在 MSTP 域模式下，使用 **revision-level** 命令配置设备的 MSTP 修订级别。
  - 使用 **reset stp region-configuration** 命令恢复 MST 域所有配置参数为缺省值。

- 指定设备为根桥或备份根桥。
  - 使用 **stp root** 命令指定当前设备作为指定生成树实例的根桥或备份根桥设备。
- 配置特定网桥的时间参数。
  - 使用 **stp timer forward-delay** 命令配置特定网桥的 Forward Delay 时间。
  - 使用 **stp timer hello** 命令设置特定网桥的 Hello Time 时间。
  - 使用 **stp timer max-age** 命令设置特定网桥的 Max Age 时间。
  - 使用 **stp time-factor** 命令设置特定网桥的超时时间因子。
- 配置特定端口参数。
  - 使用 **stp port transmit-limit** 命令设定当前端口在 Hello Time 时间内配置消息报文的发送数目。
  - 使用 **stp port edged-port enable** 命令将端口配置为边缘端口。
  - 使用 **stp port cost** 命令设置端口在指定生成树实例中的路径开销。
  - 使用 **stp port port-priority** 命令设置特定端口的优先级。
  - 使用 **stp port point-to-point** 命令设定与端口相连的链路是否是点到点链路。
- 配置设备保护功能。
  - 使用 **stp bpdu-protection enable** 命令使能设备的 BPDU 保护功能。
  - 使用 **stp port loop-protection enable** 命令启动端口的环路保护功能。
  - 使用 **stp port root-protection enable** 命令使能端口的 Root 保护功能。
- 设置 MST 域的最大跳数。
  - 使用 **stp max-hops** 命令配置 MST 域的最大跳数。
- 配置交换网络的直径。
  - 使用 **stp bridge-diameter** 命令配置交换网络的直径。
- 配置路径开销计算标准。
  - 使用 **stp pathcost-standard** 命令配置路径开销计算标准。
- 清除 MSTP 协议统计信息。
  - 使用 **reset stp statistics** 命令清除设备的 MSTP 统计信息。

----结束

任务示例

配置 MSTP 参数，具体参数信息如下：

- 使能 MSTP 功能。
- 启动 0/0/0 端口的 MSTP 功能。
- 设置 MSTP 协议的运行模式为 MSTP 兼容模式。
- 配置 MST 域参数：
  - 配置 MD5 加密算法的 MD5-KEY 为 0x11ed224466。
  - 配置 MST 域名为 huawei-mstp-bridge。
  - 映射 VLAN2 ～ VLAN10、VLAN12 ～ VLAN16 到 MSTP 实例 3。
  - 按模 2 将所有的 VLAN 分别映射到相应的 MSTP 实例中。
  - 配置设备的 MSTP 修订级别为 100。
- 配置 MST 域的最大跳数为 10。

- 手工激活 MST 域的配置。
- 设备在指定生成树实例 2 中的优先级为 4096。
- 指定当前设备为 MSTP 实例 2 的根桥设备。
- 配置交换网络的直径为 6。
- 路径开销计算标准为 IEEE 802.1t 标准方法。
- 配置特定网桥的时间参数：
  - 特定网桥的 Forward Delay 时间为 2000 厘秒。
  - 特定网桥的 Hello Time 时间为 1000 厘秒。
  - 特定网桥的 Max Age 时间为 3000 厘秒。
  - 特定网桥的超时时间因子为 6。
- 配置特定端口参数：
  - 端口在每个 Hello Time 时间内最大发送数目为 16。
  - 端口 0/0/0 为边缘端口。
  - 端口在指定生成树实例中的路径开销为 1024。
  - 端口的优先级为 64。
  - 与 0/0/0 端口相连的链路为点对点链路。
- 使能设备的 BPDU 保护功能。

```
huawei(config)#stp enable
  Change global stp state may active region configuration,it may take several
minutes,are you sure to change global stp state? [Y/N][N]y
huawei(config)#stp port 0/0/0 enable
huawei(config)#stp mode mstp
huawei(config)#stp md5-key 11ed224466
huawei(config)#stp region-configuration
huawei(stp-region-configuration)#region-name huawei-mstp-bridge
huawei(stp-region-configuration)#instance 3 vlan 2 to 10 12 to 16
huawei(stp-region-configuration)#vlan-mapping module 2
huawei(stp-region-configuration)#revision-level 100
huawei(stp-region-configuration)#active region-configuration
  STP actives region configuration,it may take several minutes,are you sure to
active region configuration? [Y/N][N]y
huawei(stp-region-configuration)#quit
huawei(config)#stp instance 2 priority 4096
huawei(config)#stp instance 2 root primary
huawei(config)#stp max-hops 10
huawei(config)#stp bridge-diameter 6
huawei(config)#stp pathcost-standard dot1t
huawei(config)#stp timer forward-delay 2000
huawei(config)#stp timer hello 1000
huawei(config)#stp timer max-age 3000
huawei(config)#stp time-factor 6
huawei(config)#stp port 0/0/0 transmit-limit 16
huawei(config)#stp port 0/0/0 edged-port enable
huawei(config)#stp port 0/0/0 instance 0 cost 1024
huawei(config)#stp port 0/0/0 instance 0 port-priority 64
huawei(config)#stp port 0/0/0 point-to-point force-true
huawei(config)#stp bpdu-protection enable
```

6.2 配置以太网上行端口链路聚合

端口聚合是将 MA5631 的两个 GE 上行端口聚合在一起，通过负荷分担的工作方式提高传输带宽。当聚合的某个 GE 端口或 GE 链路故障时，设备通过另一个 GE 端口传输业务，提高传输可靠性。

前提条件

- 网络设备和线路正常。
- MA5631 上层设备的接口 VLAN 与上行口配置的 VLAN 相对应。

背景信息

- 两个聚合端口上的以太网端口属性配置应完全一致。
- 聚合端口上不能存在静态 MAC，可以使用 **display mac-address** 命令进行查询。
- 聚合端口不能为镜像目的端口。

操作步骤

步骤 1 配置以太网端口聚合。

使用命令 **link-aggregation** 设置以太网端口聚合。

步骤 2 查询聚合组信息。

使用 **display link-aggregation all** 命令查询以太网聚合端口的端口类型、端口数目和端口的工作模式等信息。

----结束

操作结果

在 ETH 模式下，使用 **shutdown** 命令去激活 0/0/0 或者 0/0/1 端口，PC 仍可以通过 PPPoE 拨号软件拨号上网。

任务示例

举例：MA5631 设备通过 GE 上行，将两个上行端口 0/0/0 和 0/0/1 配置为端口聚合组，聚合组中各成员端口按源 MAC 地址分发报文，工作模式为 LACP 静态聚合。

```
huawei(config)#link-aggregation 0/0 0-1 ingress workmode lacp-static
huawei(config)#display link-aggregation all
  ------------------------------------------------------------------------------
  Master port  Link aggregation mode  Port NUM  Work mode  Max link number
  ------------------------------------------------------------------------------
  0/0/0        ingress                       2  lacp-static             -
  ------------------------------------------------------------------------------
  Total: 1 link aggregation(s)
```

7 配置 EoC 宽带业务示例（OLT 使用 EPON 接入方式）

通过示例介绍 EoC 宽带业务的配置方法。本示例中 ONU 使用 MA5631。

前提条件

配置宽带业务前，CNU 必须已经和 EoC 局端正常连接，CNU 的相关配置可参见**配置 CNU 管理**。

业务需求

CNU 使用 HG7022（2 个 LAN 口），CNU 的端口 1 接 PC 提供上网业务，端口 2 接机顶盒提供互动电视的回传通道，基于端口区分业务。OLT 上不做 VLAN 切换，直接透传。

- 用户通过 PPPoE 拨号方式上网。
- 使用 PITP 来防止用户帐号的盗号和漫游。

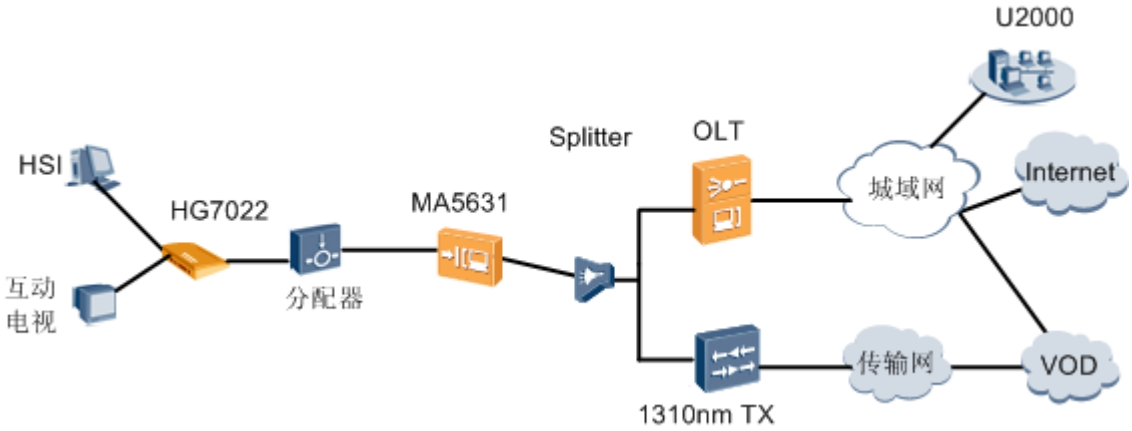
  说明

  若采用 DHCP 拨号方式，也可以配置防盗号和漫游，具体配置方法请参见**配置 DHCP 的防盗号和漫游**。

组网图

EoC 宽带业务应用组网如**图 7-1** 所示。

图 7-1 EoC 宽带业务应用组网图



数据规划

OLT 侧数据规划如表 7-1 所示，ONU 侧数据规划如表 7-2 所示。

表 7-1 EoC 宽带业务配置数据规划-OLT 侧

配置项	数据
VLAN	带内管理 VLAN 8，类型为 Smart 业务 VLAN 100，类型为 Smart，属性为 Common 业务 VLAN 101，类型为 Smart，属性为 Common
IP 地址	带内管理 IP 地址：192.168.50.1/24
EPON 业务板	端口：0/3/1 ONU ID：1 ONU 认证方式：MAC
DBA 模板	模板 ID：20 类型：type3 保证带宽：30Mbit/s 最大带宽：100Mbit/s
ONU 线路模板	模板 ID：20，LLID 绑定 ID 为 20 的 DBA 模板
ONU 管理模式	SNMP

表 7-2 EoC 宽带业务配置数据规划-ONU 侧

配置项	数据
VLAN	带内管理 VLAN 8，类型为 Smart，将 EPON 上行口 0/0/0 加入到 VLAN 中 HSI 业务 VLAN 100，类型为 Smart，属性为 Stacking，将 EPON 上行口 0/0/0 加入到 VLAN 中 互动电视业务 VLAN 101，类型为 Smart，属性为 Common，将 EPON 上行口 0/0/0 加入到 VLAN 中
IP 地址	带内管理 IP 地址：192.168.50.2/24

操作步骤

步骤 1　OLT 侧配置：

1. 创建业务 VLAN 并配置其上行口。

   业务 VLAN 为 100，101，类型为 Smart VLAN，属性为 Common，将上行端口 0/19/0 加入到 VLAN 100，101 中。

   ```
   huawei(config)#vlan 100-101 smart
   huawei(config)#vlan attrib 100 common
   huawei(config)#vlan attrib 101 common
   huawei(config)#port vlan 100-101 0/19 0
   ```

2. （可选）配置上行链路聚合。

   本示例以单上行端口为例，当多个上行端口时可配置上行链路聚合。具体请参考**配置以太网上行端口链路聚合**。

3. 配置 EPON ONU 模板。

   EPON ONU 模板包括 DBA 模板、线路模板和业务模板。

   - DBA 模板：DBA 模板描述了 EPON 的流量参数，LLID 通过绑定 DBA 模板进行动态分配带宽，提高上行带宽利用率。
   - 线路模板：线路模板主要描述了 LLID（Logic Link ID）和 DBA 模板的绑定关系。
   - 业务模板：业务模板为采用 OMCI 方式管理的 ONT 提供了业务配置渠道。

   a. 配置 DBA 模板。

      可以先使用 **display dba-profile** 命令查询系统中已存在的 DBA 模板。如果系统中现有的 DBA 模板不能满足需求，则需要执行 **dba-profile add** 命令来添加。

      模板的 ID 为 20，类型为 Type3，保证带宽为 30M，最大带宽为 100Mbit/s。

      ```
      huawei(config)#dba-profile add profile-id 20 type3 assure 30720 max 102400
      ```

   b. 配置 ONU 线路模板。

      模板 ID 为 20，LLID（Logic Link ID）的 DBA 模板 ID 为 20。去使能 FEC 功能（默认），不进行流量限速（默认）。

说明

1) 可以根据需要使用 **fec enable** 命令使能 FEC 功能，以提高 OLT 和 ONU 之间数据传输的可靠性。

2) 可根据需要使用 **llid ont-car** 命令对 ONU 的上行流量进行限速。

```
huawei(config)#ont-lineprofile epon profile-id 20
huawei(config-epon-lineprofile-20)#llid dba-profile-id 20
```

配置完成使用 commit 命令使配置的参数生效。

huawei(config-epon-lineprofile-20)#**commit**

huawei(config-epon-lineprofile-20)#**quit**

4. OLT 上添加 ONU。

ONU 通过光纤连接到 OLT 的 EPON 接口，需要先在 OLT 上成功添加 ONU 后，才能进行业务配置。

a. 增加 ONU。

ONU 通过分光器接在 EPON 端口 0/3/1 下，ONU ID 为 1，使用 MAC 地址认证，MAC 地址为 0018-82D6-D178，管理模式为 SNMP，绑定的线路模板 ID 为 20。

增加 ONU 有两种方式，请根据实际情况进行选择。

- 离线增加 ONU：在已经获悉 ONU 的密码或者序列号的情况下，可以使用 **ont add** 命令离线增加 ONU。
- 自动发现 ONU：在 ONU 的密码或序列号未知的情况下，先在 EPON 模式下使用 **port ont-auto-find** 命令使能 EPON 端口的 ONU 自动发现功能。然后使用 **ont confirm** 命令确认 ONU。

通过离线方式增加 ONU 的配置如下：

```
huawei(config)#interface epon 0/3
huawei(config-if-epon-0/3)#ont add 1 1 mac-auth 0018-82D6-D178 snmp ont-lineprofile-id
20 desc MA5631_0/3/1/1_lineprofile20
```

通过自动发现方式增加 ONU 的配置如下：

```
huawei(config)#interface epon 0/3
huawei(config-if-epon-0/3)#port 1 ont-auto-find enable
huawei(config-if-epon-0/3)#display ont autofind 1
   //该命令会显示通过分光器接入到该EPON端口的所有ONU的信息


   ---------------------------------------------------------------------------
   Number              : 1
   F/S/P               : 0/3/1
   Ont Mac             : 0018-82D6-D178
   Password            : 00000000000000000000000000000000
   VenderID            : HWTC
   Ontmodel            : MA5631
   Ont SoftwareVersion : V800R308C02
   OntHardwareVersion  : MA5631
   Ont autofind time   : 2010-03-20 10:20:45
   ---------------------------------------------------------------------------
huawei(config-if-epon-0/3)#ont confirm 1 ontid 1 mac-auth 0018-82D6-D178 snmp ont-
lineprofile-id
 20 desc MA5631_0/3/1/1_lineprofile20
```

说明

如果一个端口下有多个同类型的 ONU，且绑定的线路模板或业务模板（对于 ONT 来说）相同，可以通过批量确认自动发现的 ONU 的方式批量增加 ONU，以简化操作、提高配置效率。如，上面的命令也可以修改为：huawei(config-if-epon-0/3)#**ont confirm 1 all mac-auth snmp ont-lineprofile-id 20 desc MA5631_0/3/1_lineprofile20**。

5. 确认 ONU 状态为正常上线。

   增加 ONU 后，请使用 **display ont info** 命令查询 ONU 的当前状态，确保 ONU 的“Control flag”为“active”、“Run State”为“online”、“Config state”为“normal”。

```
huawei(config-if-epon-0/3)#display ont info 1 1
  ------------------------------------------------------------------------
  F/S/P                : 0/3/1
  ONT-ID               : 1
  Control flag         : active    //说明ONU已经激活
  Run state            : online    //说明ONU已经正常在线
  Config state         : normal    //说明ONU配置恢复状态正常
...//省略了后面的回显。
```

   当出现 ONU 配置状态失败、ONU 无法 up 等情况时，建议参考上面的描述检查 ONU 的状态。

   - 如果“Control flag”为“deactive”，需要在 EPON 端口模式下使用 **ont activate** 命令激活 ONU。
   - 如果出现 ONU 无法 up，即“Run state”为“offline”，可能是物理线路中断，也可能是光模块损坏，需要从物料和线路两方面排查。
   - 如果出现 ONU 配置状态失败，即“Config state”为“failed”，则说明配置的 ONU 能力集超出了 ONU 实际支持的能力，需要在诊断模式下使用 **display ont failed-configuration** 命令查看配置失败项及原因，根据具体情况进行修改。

6. 配置 OLT 到 ONU 的管理通道。

   a. 配置 OLT 的带内管理 VLAN 和 IP 地址。

      为了能在 OLT 上远程登录到 ONU 上配置 ONU 相关内容，需要在 OLT 上配置 OLT 和 ONU 的带内管理 VLAN 及 IP 地址。

      管理 VLAN 为 8，并配置带内管理 IP 地址为 192.168.50.1/24。

```
huawei(config-if-epon-0/3)#quit
huawei(config)#vlan 8 smart
huawei(config)#interface vlanif 8
huawei(config-if-vlanif8)#ip address 192.168.50.1 24
huawei(config-if-vlanif8)#quit
```

   b. 配置 ONU 的带内管理 VLAN 和 IP 地址。

      配置 ONU 的静态 IP 地址为 192.168.50.2/24，管理 VLAN 为 8（同 OLT 的管理 VLAN）。

```
huawei(config)#interface epon 0/3
huawei(config-if-epon-0/3)#ont ipconfig 1 1 ip-address 192.168.50.2 mask 255.255.255.0
manage-vlan 8
```

   c. 配置带内管理业务流。

      管理业务流索引为 0，管理 VLAN 为 8，用户侧 VLAN 为 8。OLT 上对带内业务流不限速，因此直接使用索引为 6 的缺省流量模板，如果需要使用业务流限速，可以使用 **traffic table ip** 命令配置流量模板并在业务流中引用。

```
huawei(config)#service-port vlan 8 epon 0/3/1 ont 1 multi-service user-vlan 8
inbound traffic-table index 6 outbound traffic-table index 6
```

7. 确认 OLT 和 ONU 之间的管理通道已经打通。

   - 可以在 OLT 上通过 **ping** ***192.168.50.2*** 命令验证到 ONU 的连通性，应该能收到来自 ONU 的 ICMP ECHO-REPLY 响应报文。
   - 可以通过 **telnet** ***192.168.50.2*** 命令登录到 ONU 上进行 ONU 侧的相关配置。

8. 创建业务流。

   HSI 业务流索引为 1，业务 VLAN 为 100。互通电视业务流索引为 2，业务 VLAN 为 101。对上下行报文的流量限速在 MDU 上控制，在 OLT 上不作限速。因此直接使用索引为 6 的缺省流量模板，如果需要使用业务流限速，可以使用 **traffic table ip** 命令配置流量模板并在此引用。

   用户侧 VLAN 需要和 ONU 的上行 VLAN 保持一致。

```
huawei(config)#service-port 1 vlan 100 epon 0/3/1 ont 1 inbound traffic-table
index 6 outbound traffic-table index 6
huawei(config)#service-port 2 vlan 101 epon 0/3/1 ont 1 inbound traffic-table
index 6 outbound traffic-table index 6
```

9. 配置队列调度。

   采用 3PQ+5WRR 队列调度方式。队列 0－4 采用 WRR 方式，权重分别为 10、10、20、20、40；队列 5－7 采用 PQ 方式。业务优先级为 4，采用 WRR 方式。

   队列调度是全局配置，在 OLT 上只需要配置一次，配置完成后全局有效，后续在配置其它业务时也无需重复配置。

```
huawei(config)#queue-scheduler wrr 10 10 20 20 40 0 0 0
```

   配置队列与 802.1p 优先级的映射关系，优先级 0－7 分别映射到队列 0－7。

   对于只支持 4 个队列的单板，802.1p 优先级与队列 ID 之间的映射关系为：优先级 0、1 映射到队列 1；优先级 2、3 映射到队列 2；优先级 4、5 映射到队列 3；优先级 6、7 映射到队列 4。

```
huawei(config)#cos-queue-map cos0 0 cos1 1 cos2 2 cos3 3 cos4 4 cos5 5 cos6 6 cos7 7
```

10. 保存数据。

```
huawei(config)#save
```

步骤 2 ONU 侧配置：

说明

由于已经创建了管理 VLAN 和管理 IP 地址，所以可以在 OLT 上通过 **telnet** ***192.168.50.2*** 命令进入到 ONU 侧进行配置；也可以通过串口直接登录到 ONU 进行配置。

1. 登录 ONU 进行配置。

   在 OLT 上 telnet ONU 的管理 IP 地址登录设备。用户名：root（缺省），密码：mduadmin（缺省）。

```
huawei(config)#telnet 192.168.50.2
{ <cr>|service-port<U><0,4294967295> }:

  Command:
          telnet 192.168.50.2
  Press CTRL_] to quit telnet mode
  Trying 192.168.50.2 ...
  Connected to 192.168.50.2 ...
>>User name:root
>>User password:     //控制台上不显示
```

2. 创建业务 VLAN。

   HSI 业务 VLAN 100，类型为 Smart，属性为 Stacking，并将上行口 0/0/0 加入 VLAN。互动电视业务 VLAN 101，类型为 Smart，属性为 Common，并将上行口 0/0/0 加入 VLAN。

```
huawei(config)#vlan 100-101 smart
huawei(config)#vlan attrib 100 stacking
huawei(config)#vlan attrib 101 common
huawei(config)#port vlan 100-101 0/0 0
```

3. 配置流量模板。

   您可以使用 **display traffic table ip** 命令查询系统中已存在的流量模板。如果系统中现有的流量模板不能满足需求，则需要执行 **traffic table ip** 来添加。本例中采用默认流量模板。

```
huawei(config)#display traffic table ip from-index 0
{ <cr>|to-index<K> }:

  Command:
          display traffic table ip from-index 0
  ------------------------------------------------------------------------------
   TID CIR(kbps) CBS(bytes) PIR(kbps) PBS(bytes) Pri Copy-policy    Pri-Policy
  ------------------------------------------------------------------------------
     0       512      18384      1024      36768   6 -             tag-pri
     1      1024      34768      2048      69536   0 -             tag-pri
     2      2048      67536      4096     135072   0 -             tag-pri
     3      4096     133072      8192     266144   4 -             tag-pri
     4      8192     264144     16384     528288   4 -             tag-pri
     5     16384     526288     32768    1024000   4 -             tag-pri
     6       off        off       off        off   0 -             tag-pri
  ------------------------------------------------------------------------------
  Total Num : 7
```

4. 创建业务流并绑定流量模板。

   HSI 数据业务进行 VLAN 切换，外层 SVLAN 标识 OLT+PON 口+业务，内层 CVLAN 标识 CNU+ONU（ONUID）。

```
huawei(config)#service-port 1 vlan 100 eoc 0/4/0 cnu 0 eth 1 multi-service user-vlan untagged inbound traffic-table index 3 outbound traffic-table index 3
huawei(config)#stacking label service-port 100 2
```

   互动电视回传业务进行 CVLAN－>SVLAN 切换，SVLAN 标识业务。

```
huawei(config)#service-port 2 vlan 101 eoc 0/4/0 cnu 0 eth 2 multi-service user-vlan untagged inbound traffic-table index 4 outbound traffic-table index 4
```

5. 配置用户帐号安全。

   使用 PITP P 模式来防止用户帐号的盗号和漫游。

```
huawei(config)#pitp enable pmode
```

   说明

   关于 PITP 帐号安全，更详细的信息，请参考**配置 PITP 的防盗号和漫游**。

6. 保存数据。

```
huawei(config)#save
```

----结束

操作结果

- CNU 端口 1 上的用户可实现高速上网业务
- CNU 端口 2 上的用户可实现互动电视业务。

说明

CNU 不管是两口的还是四口的，各 LAN 口用户都可以根据需要接入上网业务或者互动电视业务。配置过程都和上述配置类似。

配置脚本

OLT 侧:

```
vlan 100-101 smart
vlan attrib 100 common
vlan attrib 101 common
port vlan 100-101 0/19 0
```

```
vlan 8 smart
interface vlanif 8
ip address 192.168.50.1 24
quit
dba-profile add profile-id 20 type3 assure 30720 max 102400
ont-lineprofile epon profile-id 20
llid dba-profile-id 20
commit
quit
interface epon 0/3
port 1 ont-auto-find enable
ont confirm 1 ontid 1 mac-auth 0018-82D6-D178 snmp ont-lineprofile-id
 20 desc MA5631_0/3/1/1_lineprofile20
ont ipconfig 1 1 ip-address 192.168.50.2 mask 255.255.255.0 manage-vlan 8
quit
service-port 0 vlan 8 epon 0/3/1 ont 1 multi-service user-vlan 8
service-port 1 vlan 100 epon 0/3/1 ont 1 inbound traffic-table
index 6 outbound traffic-table index 6
service-port 2 vlan 101 epon 0/3/1 ont 1 inbound traffic-table
index 6 outbound traffic-table index 6
queue-scheduler wrr 10 10 20 20 40 0 0 0
cos-queue-map cos0 0 cos1 1 cos2 2 cos3 3 cos4 4 cos5 5 cos6 6 cos7 7
save
```

ONU 侧:

```
vlan 100-101 smart
vlan attrib 100 stacking
vlan attrib 101 common
port vlan 100-101 0/0 0
vlan service-profile profile-id 1
vlan service-profile profile-id 2
commit
quit
vlan bind service-profile 100 profile-id 1
vlan bind service-profile 101 profile-id 2
service-port 1 vlan 100 eoc 0/4/0 cnu 0 eth 1 multi-service user-
vlan untagged inbound traffic-table index 3 outbound traffic-table index 3
stacking label service-port 100 2
service-port 2 vlan 101 eoc 0/4/0 cnu 0 eth 2 multi-service user-
vlan untagged inbound traffic-table index 4 outbound traffic-table index 4
pitp enable pmode
save
```

8 配置 EoC 宽带业务示例（OLT 使用 GPON 接入方式）

通过示例介绍 EoC 宽带业务的配置方法。本示例中 ONU 使用 MA5631。

前提条件

配置宽带业务前，CNU 必须已经和 EoC 局端正常连接，CNU 的相关配置可参见**配置 CNU 管理**。

业务需求

CNU 使用 HG7022（2 个 LAN 口），CNU 的端口 1 接 PC 提供上网业务，端口 2 接机顶盒提供互动电视的回传通道，基于端口区分业务。OLT 上不做 VLAN 切换，直接透传。

- 用户通过 PPPoE 拨号方式上网。
- 使用 PITP 来防止用户帐号的盗号和漫游。

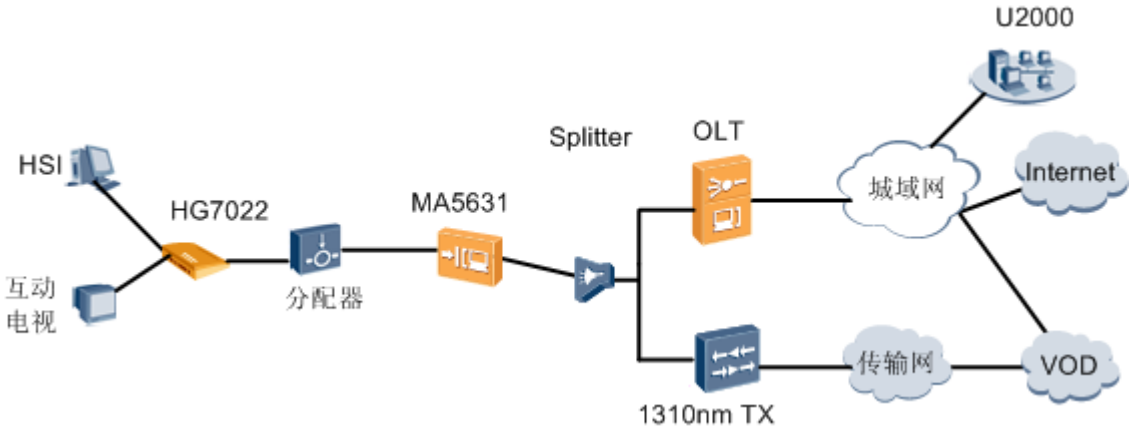
  说明

  若采用 DHCP 拨号方式，也可以配置防盗号和漫游，具体配置方法请参见**配置 DHCP 的防盗号和漫游**。

组网图

EoC 宽带业务应用组网如**图 8-1** 所示。

图 8-1 EoC 宽带业务应用组网图



数据规划

OLT 侧数据规划如表 8-1 所示，ONU 侧数据规划如表 8-2 所示。

表 8-1 EoC 宽带业务配置数据规划-OLT 侧

配置项	数据
VLAN	带内管理 VLAN 8，类型为 Smart 业务 VLAN 100，类型为 Smart，属性为 Common 业务 VLAN 101，类型为 Smart，属性为 Common
IP 地址	带内管理 IP 地址：192.168.50.1/24
GPON 业务板	端口：0/3/1 ONU ID：1 ONU 认证方式：SN ONU SN：48575443E6D8B541
DBA 模板	模板名称：PrivateLine 类型：type3 保证带宽：20Mbit/s 最大带宽：50Mbit/s
ONU 线路模板	模板 ID：10，绑定名称为 PrivateLine 的 DBA 模板 GEM Port ID：0、1、2 T-CONT ID：5
ONU 管理模式	SNMP

表 8-2 EoC 宽带业务配置数据规划-ONU 侧

配置项	数据
VLAN	带内管理 VLAN 8，类型为 Smart，将 GPON 上行口 0/0/0 加入到 VLAN 中 HSI 业务 VLAN 100，类型为 Smart，属性为 Stacking，将 GPON 上行口 0/0/0 加入到 VLAN 中 互动电视业务 VLAN 101，类型为 Smart，属性为 Common，将 GPON 上行口 0/0/0 加入到 VLAN 中
IP 地址	带内管理 IP 地址：192.168.50.2/24

操作步骤

步骤 1　OLT 侧配置：

1. 创建业务 VLAN 并配置其上行口。

   业务 VLAN 为 100，101，类型为 Smart VLAN，属性为 Common，将上行端口 0/19/0 加入到 VLAN 100，101 中。

   ```
   huawei(config)#vlan 100-101 smart
   huawei(config)#vlan attrib 100 common
   huawei(config)#vlan attrib 101 common
   huawei(config)#port vlan 100-101 0/19 0
   ```

2. （可选）配置上行链路聚合。

   本示例以单上行端口为例，当多个上行端口时可配置上行链路聚合。具体请参考**配置以太网上行端口链路聚合**。

3. 配置 GPON ONU 模板。

   GPON ONU 模板包括 DBA 模板、线路模板、业务模板和告警模板。

   - DBA 模板：DBA 模板描述了 GPON 的流量参数，T-CONT 通过绑定 DBA 模板进行动态分配带宽，提高上行带宽利用率。
   - 线路模板：线路模板描述了 T-CONT 和 DBA 模板的绑定关系、业务流的 QoS 模式、GEM Port 与 ONU 侧业务的映射关系等。
   - 业务模板：业务模板为采用 OMCI 方式管理的 ONT 提供了业务配置渠道。
   - 告警模板：告警模板设置一系列告警门限参数，用于对激活的 ONT 线路进行性能统计监控，当某个统计量达到告警门限时，就通知主机，并向日志主机和网管发送告警信息。

   a. 配置 DBA 模板。

      可以先使用 **display dba-profile** 命令查询系统中已存在的 DBA 模板。如果系统中现有的 DBA 模板不能满足需求，则需要执行 **dba-profile add** 命令来添加。

      模板的名称为 PrivateLine，类型为 Type3，保证带宽为 20Mbit/s，最大带宽为 50Mbit/s。

      ```
      huawei(config)#dba-profile add profile-name PrivateLine type3 assure 20480 max 51200
      ```

   b. 配置 ONU 线路模板。

      模创建索引号为 10 的 GPON ONU 线路模板，并将 ID 为 5 的 T-CONT 和名称为 PrivateLine 的 DBA 模板绑定。这样，T-CONT 可以依据 DBA 模板中的不同配置，提供灵活的动态带宽分配方案。

```
huawei(config)#ont-lineprofile gpon profile-id 10
huawei(config-gpon-lineprofile-10)#tcont 5 dba-profile-name PrivateLine
```

增加索引为 0 的 GEM Port 用于承载管理业务流，索引为 1 的 GEM Port 用于承载 HSI 的业务流，索引为 2 的 GEM Port 用于承载互动电视的业务流，GEM Port 0、1 和 2 均绑定到 T-CONT 5。QoS 模式为 priority-queue（默认），队列优先级为 3。

说明

1) 如果需要修改系统缺省的 QoS 模式，请使用 **qos-mode** 命令配置 QoS 模式为 gem-car 或者 flow-car，并且使用 gem add 命令配置此 GEM Port 绑定的流量模板索引。

2) QoS 模式采用 PQ 时，默认的队列优先级为 0；QoS 模式采用 flow-car 时，默认绑定的流量模板索引为 6（不限速）；QoS 模式采用 gem-car 时，默认绑定的流量模板索引为 6（不限速）。

huawei(config-gpon-lineprofile-10)#**gem add 0 eth tcont 5 priority-queue 3**

huawei(config-gpon-lineprofile-10)#**gem add 1 eth tcont 5 priority-queue 3**

huawei(config-gpon-lineprofile-10)#**gem add 2 eth tcont 5 priority-queue 3**

配置 GEM Port 与 ONU 侧业务的映射模式为 VLAN 方式（默认），并将管理 VLAN 8 的业务流映射到索引为 0 的 GEM Port，将 HSI 业务 VLAN 100 的业务流映射到索引为 1 的 GEM Port，将互动电视业务 VLAN 101 的业务流映射到索引为 2 的 GEM Port。

```
huawei(config-gpon-lineprofile-10)#mapping-mode vlan
huawei(config-gpon-lineprofile-10)#gem mapping 0 0 vlan 8
huawei(config-gpon-lineprofile-10)#gem mapping 1 1 vlan 100
huawei(config-gpon-lineprofile-10)#gem mapping 2 2 vlan 101
```

配置完成使用 **commit** 命令使配置的参数生效。

```
huawei(config-gpon-lineprofile-10)#commit
huawei(config-gpon-lineprofile-10)#quit
```

（可选）配置告警门限模板。

- 系统缺省的 GPON 告警门限模板 1，其中各告警域值为 0，即不上报告警。
- 本实例中采用缺省的告警门限模板，无需配置。
- 当需要配置告警门限值参数，用于对激活的 ONU 线路进行性能统计监控时，使用 **gpon alarm-profile add** 命令配置 GPON 告警门限模板。

4. OLT 上添加 ONU。

ONU 通过光纤连接到 OLT 的 GPON 接口，需要先在 OLT 上成功添加 ONU 后，才能进行业务配置。

a. 增加 ONU。

ONU 通过分光器接在 GPON 端口 0/3/1 下，ONU ID 为 1，序列号为 48575443E6D8B541，管理模式为 SNMP，绑定的线路模板 ID 为 10。

增加 ONU 有两种方式，请根据实际情况进行选择。

- 离线增加 ONU：在已经获悉 ONU 的密码或者序列号的情况下，可以使用 **ont add** 命令离线增加 ONU。
- 自动发现 ONU：在 ONU 的密码或序列号未知的情况下，先在 GPON 模式下使用 **port ont-auto-find** 命令使能 GPON 端口的 ONU 自动发现功能。然后使用 **ont confirm** 命令确认 ONU。

通过离线方式增加 ONU 的配置如下：

```
huawei(config)#interface gpon 0/3
huawei(config-if-gpon-0/3)#ont add 1 1 sn-auth 48575443E6D8B541 snmp ont-lineprofile-id
 10 desc MA5631_0/3/1/1_lineprofile10
```

通过自动发现方式增加 ONU 的配置如下：

```
huawei(config)#interface gpon 0/3
huawei(config-if-gpon-0/3)#port 1 ont-auto-find enable
huawei(config-if-gpon-0/3)#display ont autofind 1
   //该命令会显示通过分光器接入到该GPON端口的所有ONU的信息


   ---------------------------------------------------------
   Number              : 1
   F/S/P               : 0/3/1
   Ont SN              : 48575443E6D8B541
   Password            :
   VenderID            : HWTC
   Ont Version         : MA5631
   Ont SoftwareVersion : V800R308C02
   Ont EquipmentID     : SmartAX MA5631
   Ont autofind time   : 2010-03-10 11:20:16
   ---------------------------------------------------------
huawei(config-if-gpon-0/3)#ont confirm 1 ontid 1 sn-auth 48575443E6D8B541 snmp ont-
lineprofile-id
 10 desc MA5631_0/3/1/1_lineprofile10
```

说明

如果一个端口下有多个同类型的 ONU，且绑定的线路模板或业务模板相同，可以通过批量确认自动发现的 ONU 的方式批量增加 ONU，以简化操作、提高配置效率。如，上面的命令也可以修改为：huawei(config-if-gpon-0/3)**#ont confirm 1 all sn-auth snmp ont-lineprofile-id 10 desc MA5631_0/3/1_lineprofile10**。

5. 确认 ONU 状态为正常上线。

   增加 ONU 后，请使用 **display ont info** 命令查询 ONU 的当前状态，确保 ONU 的“Control flag”为“active”、“Run State”为“online”、“Config state”为“normal”。

```
huawei(config-if-gpon-0/3)#display ont info 1 1
  -------------------------------------------------------------------------
  F/S/P                : 0/3/1
  ONT-ID               : 1
  Control flag         : active    //说明ONU已经激活
  Run state            : online    //说明ONU已经正常在线
  Config state         : normal    //说明ONU配置恢复状态正常
...//省略了后面的回显。
```

   当出现 ONU 配置状态失败、ONU 无法 up 等情况时，建议参考上面的描述检查 ONU 的状态。

   - 如果“Control flag”为“deactive”，需要在 GPON 端口模式下使用 **ont activate** 命令激活 ONU。
   - 如果出现 ONU 无法 up，即“Run state”为“offline”，可能是物理线路中断，也可能是光模块损坏，需要从物料和线路两方面排查。
   - 如果出现 ONU 配置状态失败，即“Config state”为“failed”，则说明配置的 ONU 能力集超出了 ONU 实际支持的能力，需要在诊断模式下使用 **display ont failed-configuration** 命令查看配置失败项及原因，根据具体情况进行修改。

     说明

     如果 ONT 只支持 4 个队列，此时 gem add 命令中的 priority-queue 参数取值 4-7 将无效，会导致 Config state 为 failed。

6. 配置 OLT 到 ONU 的管理通道。

   说明

   只有 OLT 通过 SNMP 协议对 ONU 进行远程管理时需要配置管理通道，OLT 通过 OMCI 协议对 ONU 进行远程管理时不需要配置。

a. 配置 OLT 的带内管理 VLAN 和 IP 地址。

为了能在 OLT 上远程登录到 ONU 上配置 ONU 相关内容，需要在 OLT 上配置 OLT 和 ONU 的带内管理 VLAN 及 IP 地址。

管理 VLAN 为 8，并配置带内管理 IP 地址为 192.168.50.1/24。

```
huawei(config-if-gpon-0/3)#quit
huawei(config)#vlan 8 smart
huawei(config)#interface vlanif 8
huawei(config-if-vlanif8)#ip address 192.168.50.1 24
huawei(config-if-vlanif8)#quit
```

b. 配置 ONU 的带内管理 VLAN 和 IP 地址。

配置 ONU 的静态 IP 地址为 192.168.50.2/24，管理 VLAN 为 8（同 OLT 的管理 VLAN）。

```
huawei(config)#interface gpon 0/3
huawei(config-if-gpon-0/3)#ont ipconfig 1 1 static ip-address 192.168.50.2 mask
255.255.255.0 vlan 8
```

c. 配置带内管理业务流。

管理业务流索引为 0，管理 VLAN 为 8，GEM Port ID 为 0，用户侧 VLAN 为 8。OLT 上对带内业务流不限速，因此直接使用索引为 6 的缺省流量模板，如果需要使用业务流限速，可以使用 **traffic table ip** 命令配置流量模板并在业务流中引用。

```
huawei(config)#service-port 0 vlan 8 gpon 0/3/1 ont 1 gemport 0 multi-service
user-vlan 8 rx-cttr 6 tx-cttr 6
```

7. 确认 OLT 和 ONU 之间的管理通道已经打通。

- 可以在 OLT 上通过 **ping** ***192.168.50.2*** 命令验证到 ONU 的连通性，应该能收到来自 ONU 的 ICMP ECHO-REPLY 响应报文。
- 可以通过 **telnet** ***192.168.50.2*** 命令登录到 ONU 上进行 ONU 侧的相关配置。

8. 创建业务流。

HSI 业务流索引为 1，业务 VLAN 为 100，用户侧 VLAN 为 100。互通电视业务流索引为 2，业务 VLAN 为 101，用户侧 VLAN 为 101。对上下行报文的流量限速在 MDU 上控制，在 OLT 上不作限速。因此直接使用索引为 6 的缺省流量模板，如果需要使用业务流限速，可以使用 **traffic table ip** 命令配置流量模板并在此引用。

用户侧 VLAN 需要和 ONU 的上行 VLAN 保持一致。

```
huawei(config)#service-port 1 vlan 100 gpon 0/3/1 ont 1 gemport 1 multi-service
user-vlan 100 rx-cttr 6 tx-cttr 6
huawei(config)#service-port 2 vlan 101 gpon 0/3/1 ont 1 gemport 2 multi-service
user-vlan 101 rx-cttr 6 tx-cttr 6
```

9. 配置队列调度。

采用 3PQ+5WRR 队列调度方式。队列 0－4 采用 WRR 方式，权重分别为 10、10、20、20、40；队列 5－7 采用 PQ 方式。业务优先级为 4，采用 WRR 方式。

队列调度是全局配置，在 OLT 上只需要配置一次，配置完成后全局有效，后续在配置其它业务时也无需重复配置。

```
huawei(config)#queue-scheduler wrr 10 10 20 20 40 0 0 0
```

配置队列与 802.1p 优先级的映射关系，优先级 0－7 分别映射到队列 0－7。

对于只支持 4 个队列的单板，802.1p 优先级与队列 ID 之间的映射关系为：优先级 0、1 映射到队列 1；优先级 2、3 映射到队列 2；优先级 4、5 映射到队列 3；优先级 6、7 映射到队列 4。

```
huawei(config)#cos-queue-map cos0 0 cos1 1 cos2 2 cos3 3 cos4 4 cos5 5 cos6 6 cos7 7
```

10. 保存数据。

```
huawei(config)#save
```

步骤 2 ONU 侧配置：

说明

由于已经创建了管理 VLAN 和管理 IP 地址，所以可以在 OLT 上通过 **telnet *192.168.50.2*** 命令进入到 ONU 侧进行配置；也可以通过串口直接登录到 ONU 进行配置。

1. 登录 ONU 进行配置。

   在 OLT 上 telnet ONU 的管理 IP 地址登录设备。用户名：**root**（缺省），密码：**mduadmin**（缺省）。

```
huawei(config)#telnet 192.168.50.2
{ <cr>|service-port<U><0,4294967295> }:

  Command:
          telnet 192.168.50.2
  Press CTRL_] to quit telnet mode
  Trying 192.168.50.2 ...
  Connected to 192.168.50.2 ...
>>User name:root
>>User password:      //控制台上不显示
```

2. 创建业务 VLAN。

   HSI 业务 VLAN 100，类型为 Smart，属性为 Stacking，并将上行口 0/0/0 加入 VLAN。互动电视业务 VLAN 101，类型为 Smart，属性为 Common，并将上行口 0/0/0 加入 VLAN。

```
huawei(config)#vlan 100-101 smart
huawei(config)#vlan attrib 100 stacking
huawei(config)#vlan attrib 101 common
huawei(config)#port vlan 100-101 0/0 0
```

3. 配置流量模板。

   您可以使用 **display traffic table ip** 命令查询系统中已存在的流量模板。如果系统中现有的流量模板不能满足需求，则需要执行 **traffic table ip** 来添加。本例中采用默认流量模板。

```
huawei(config)#display traffic table ip from-index 0
{ <cr>|to-index<K> }:

  Command:
          display traffic table ip from-index 0
  ------------------------------------------------------------------------------
   TID CIR(kbps) CBS(bytes) PIR(kbps) PBS(bytes) Pri Copy-policy    Pri-Policy
  ------------------------------------------------------------------------------
     0       512      18384      1024      36768   6 -             tag-pri
     1      1024      34768      2048      69536   0 -             tag-pri
     2      2048      67536      4096     135072   0 -             tag-pri
     3      4096     133072      8192     266144   4 -             tag-pri
     4      8192     264144     16384     528288   4 -             tag-pri
     5     16384     526288     32768    1024000   4 -             tag-pri
     6       off        off       off        off   0 -             tag-pri
  ------------------------------------------------------------------------------
  Total Num : 7
```

4. 创建业务流并绑定流量模板。

   HSI 数据业务进行 VLAN 切换，外层 SVLAN 标识 OLT+PON 口+业务，内层 CVLAN 标识 CNU+ONU（ONUID）。

```
huawei(config)#service-port 100 vlan 100 eoc 0/4/0 cnu 0 eth 1 multi-service user-
vlan untagged inbound traffic-table index 3 outbound traffic-table index 3
huawei(config)#stacking label service-port 100 2
```

   互动电视回传业务进行 CVLAN－>SVLAN 切换，SVLAN 标识业务。

```
huawei(config)#service-port 101 vlan 101 eoc 0/4/0 cnu 0 eth 2 multi-service user-vlan untagged inbound traffic-table index 4 outbound traffic-table index 4
```

5. 配置用户帐号安全。

   使用 PITP P 模式来防止用户帐号的盗号和漫游。

   ```
   huawei(config)#pitp enable pmode
   ```

   说明

   关于 PITP 帐号安全，更详细的信息，请参考**配置 PITP 的防盗号和漫游**。

6. 保存数据。

   ```
   huawei(config)#save
   ```

----结束

操作结果

- CNU 端口 1 上的用户可实现高速上网业务
- CNU 端口 2 上的用户可实现互动电视业务。

说明

CNU 不管是两口的还是四口的，各 LAN 口用户都可以根据需要接入上网业务或者互动电视业务。配置过程都和上述配置类似。

配置脚本

OLT 侧:

```
vlan 100-101 smart
vlan attrib 100 common
vlan attrib 101 common
port vlan 100-101 0/19 0
vlan 8 smart
interface vlanif 8
ip address 192.168.50.1 24
quit
dba-profile add profile-name PrivateLine type3 assure 20480 max 51200
ont-lineprofile gpon profile-id 10
tcont 5 dba-profile-name PrivateLine
gem add 0 eth tcont 5 priority-queue 3
gem add 1 eth tcont 5 priority-queue 3
gem add 2 eth tcont 5 priority-queue 3
mapping-mode vlan
gem mapping 0 0 vlan 8
gem mapping 1 1 vlan 100
gem mapping 2 2 vlan 101
commit
quit
interface gpon 0/3
port 1 ont-auto-find enable
display ont autofind 1
ont confirm 1 ontid 1 sn-auth 48575443E6D8B541 snmp ont-lineprofile-id
 10 desc MA5631_0/3/1/1_lineprofile10
ont ipconfig 1 1 static ip-address 192.168.50.2 mask 255.255.255.0 vlan 8
ont alarm-profile 1 1 profile-id 1
service-port 0 vlan 8 gpon 0/3/1 ont 1 gemport 0 multi-service
user-vlan 8 rx-cttr 6 tx-cttr 6
service-port 1 vlan 100 gpon 0/3/1 ont 1 gemport 1 multi-service
user-vlan 100 rx-cttr 6 tx-cttr 6
service-port 2 vlan 101 gpon 0/3/1 ont 1 gemport 2 multi-service
user-vlan 101 rx-cttr 6 tx-cttr 6
queue-scheduler wrr 10 10 20 20 40 0 0 0
cos-queue-map cos0 0 cos1 1 cos2 2 cos3 3 cos4 4 cos5 5 cos6 6 cos7 7
save
```

ONU 侧:

```
vlan 100-101 smart
vlan attrib 100 stacking
vlan attrib 101 common
port vlan 100-101 0/0 0
vlan service-profile profile-id 1
vlan service-profile profile-id 2
commit
quit
vlan bind service-profile 100 profile-id 1
vlan bind service-profile 101 profile-id 2
service-port 100 vlan 100 eoc 0/4/0 cnu 0 eth 1 multi-service user-
vlan untagged inbound traffic-table index 3 outbound traffic-table index 3
stacking label service-port 100 2
service-port 101 vlan 101 eoc 0/4/0 cnu 0 eth 2 multi-service user-
vlan untagged inbound traffic-table index 4 outbound traffic-table index 4
pitp enable pmode
save
```

A 缩略语

A		
AG	Access Gateway	接入网关
B		
BRAS	Broadband Remote Access Server	宽带接入服务器
C		
CAR	Committed Access Rate	允许访问速率
CIR	Committed Information Rate	保证信息速率
CLI	Command Line Interface	命令行接口
D		
DHCP	Dynamic Host Configuration Protocol	动态主机配置协议
DHCP option82	DHCP relay agent option 82	DHCP 中继代理选项
E		
EPON	Ethernet Passive Optical Network	以太网无源光网络
F		
FTP	File Transfer Protocol	文件传输协议
G		

GE	Gigabit Ethernet	千兆以太网
GEM	GPON Encapsulation Method	GPON 封装模式
GPON	Gigabit-capable Passive Optical Networks	吉比特无源光网络
I		
IP	Internet Protocol	因特网协议
IPoA	Internet Protocol Over ATM	承载于 ATM 网的 IP 报文
IPoE	IP over Ethernet	承载于以太网的 IP 报文
L		
LAN	Local Area Network	局域网
M		
MAC	Medium Access Control	介质访问控制
N		
NMS	Network Management System	网络管理系统
O		
OLT	Optical Line Terminal	光线路终端
ONT	Optical Network Terminal	光网络终端
ONU	Optical Network Unit	光网络单元
P		
PITP	Policy Information Transfer Protocol	策略信息传送协议
PON	Passive Optical Network	无源光网络
PPPoA	Point-to-Point Protocol Over ATM	承载于 ATM 网的 PPP 报文
PPPoE	Point-to-Point Protocol Over Ethernet	承载于以太网的 PPP 报文
Q		
QoS	Quality of Service	服务质量

R

RFC	Remote Feature Control	远端功能控制

S

SNMP	Simple Network Management Protocol	简单网管协议
SSH	Secure Shell	安全外壳
STB	Set Top Box	机顶盒
STP	Spanning Tree Protocol	生成树协议

T

T-CONT	Transmission Container	传输容器
TCP/IP	Transmission Control Protocol/ Internet Protocol	传输控制协议/互联网协议
TFTP	Trivial File Transfer Protocol	简单文件传输协议

U

UDP	User Datagram Protocol	用户数据报协议

V

VLAN	Virtual LAN	虚拟局域网