HUAWEI NetEngine 8100 X, NetEngine 8000 X, NetEngine 8000E X 系列 V800R023C00SPC500

配置指南

文档版本 01

发布日期 2023-09-30

华为技术有限公司

商标声明


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

注意

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

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

华为技术有限公司

地址： 深圳市龙岗区坂田华为总部办公楼 邮编：518129

网址： https://www.huawei.com

客户服务邮箱： support@huawei.com

客户服务电话： 4008302118

目 录

1 配置.....1
1.1 接口与链路.....1
1.1.1 接口管理配置.....1
1.1.1.1 接口管理特性描述.....1
1.1.1.1.1 接口管理介绍.....1
1.1.1.1.2 接口管理原理描述.....2
1.1.1.1.3 接口管理应用.....37
1.1.1.2 接口管理配置.....49
1.1.1.2.1 接口管理概述.....49
1.1.1.2.2 接口管理特性限制.....56
1.1.1.2.3 接口基础配置.....57
1.1.1.2.4 物理链路检测配置.....63
1.1.1.2.5 配置 MAC Accounting 功能.....68
1.1.1.2.6 配置 EVC 子接口的精确剪枝功能.....69
1.1.1.2.7 配置接口延迟发出信号.....70
1.1.1.2.8 配置接口统计计数缓存周期.....71
1.1.1.2.9 配置全局接口流量突变告警阈值.....71
1.1.1.2.10 光模块激光器配置.....72
1.1.1.2.11 配置端口的光模块模式.....74
1.1.1.2.12 使能光模块告警门限标准化.....74
1.1.1.2.13 配置光模块禁止告警检测.....75
1.1.1.2.14 管理第三方光模块.....75
1.1.1.2.15 配置 PN 反序模式.....76
1.1.1.2.16 控制接口震荡配置.....76
1.1.1.2.17 逻辑接口配置.....78
1.1.1.2.18 FlexE 接口配置.....81
1.1.1.2.19 端口组配置.....105
1.1.1.2.20 配置接口监控组.....106
1.1.1.2.21 配置去使能板间心跳联动端口状态表功能.....108
1.1.1.2.22 维护接口.....109
1.1.1.2.23 接口管理配置举例.....110
1.1.2 传输告警定制与抑制配置.....117
1.1.2.1 传输告警定制与抑制特性描述.....117

1.1.2.1.1 传输告警定制与抑制介绍 117
1.1.2.1.2 传输告警定制与抑制原理描述 117
1.1.2.1.3 传输告警定制与抑制术语与缩略语 120
1.1.2.2 传输告警定制与抑制配置 121
1.1.2.2.1 传输告警定制与抑制概述 121
1.1.2.2.2 传输告警定制与抑制特性限制 122
1.1.2.2.3 配置传输告警的定制功能 122
1.1.2.2.4 配置传输告警的过滤时间间隔 123
1.1.2.2.5 维护传输告警定制与抑制 124
1.1.3 端口扩展配置 125
1.1.3.1 端口扩展特性描述 125
1.1.3.1.1 端口扩展介绍 125
1.1.3.1.2 端口扩展特性支持说明 127
1.1.3.1.3 端口扩展原理描述 127
1.1.3.1.4 端口扩展应用 138
1.1.3.1.5 端口扩展术语与缩略语 139
1.1.3.2 端口扩展配置 139
1.1.3.2.1 端口扩展特性限制 140
1.1.3.2.2 建立端口扩展系统 140
1.1.3.2.3 AP 的升级和管理 148
1.1.3.2.4 维护端口扩展系统 158
1.1.3.2.5 端口扩展配置举例 159

插图目录

图 1-1 本地环回示意图 9
图 1-2 远端环回示意图 10
图 1-3 接口震荡抑制原理图 15
图 1-4 物理接口震荡抑制示意图 16
图 1-5 标准 Ethernet 与 FlexE 结构 20
图 1-6 FlexE 通用架构 21
图 1-7 捆绑功能 22
图 1-8 通道化功能 22
图 1-9 子速率功能 23
图 1-10 FlexE Shim 机制 23
图 1-11 Calendar 机制 24
图 1-12 开销帧格式 24
图 1-13 时隙表建立 28
图 1-14 时隙表切换实现带宽无损调整 29
图 1-15 时隙表切换具体流程 30
图 1-16 1GE 时隙粒度机制 31
图 1-17 标准 Ethernet 接口切换为 FlexE 模式 31
图 1-18 标准 Ethernet 接口切换为 FlexE 模式后的配置恢复 32
图 1-19 FlexE DCN 模式 33
图 1-20 标准 Ethernet 接口和 FlexE 物理接口对接的模式 34
图 1-21 FlexE 时间同步模式 34
图 1-22 FlexE Mux 功能 35
图 1-23 FlexE Demux 功能 36
图 1-24 接口监控组原理示意图 37
图 1-25 GE 子接口 38
图 1-26 Eth-Trunk 组网图 38
图 1-27 传统 LAG 技术实现接口捆绑 39
图 1-28 FlexE 技术实现接口捆绑 39
图 1-29 FlexE 技术实现 5G 网络分片 40
图 1-30 FlexE Unaware 模式在传输网络映射图 40
图 1-31 FlexE Termination 模式在传输网络映射图 41
图 1-32 FlexE Aware 模式在传输网络映射图 42
图 1-33 信道化接口示意图 42

图 1-34 NULL0 接口防止路由环路示例 45
图 1-35 端口组应用组网图 48
图 1-36 接口监控组应用组网图 49
图 1-37 差分编码模式 58
图 1-38 Mac Accounting 应用场景组网图 68
图 1-39 现网运行 Ethernet 业务场景增加 FlexE 网元 100
图 1-40 现网运行 FlexE 业务场景增加 FlexE 网元 101
图 1-41 现网运行 FlexE 业务场景增加 Ethernet 网元 102
图 1-42 接口监控组典型应用组网图 107
图 1-43 配置 FlexE 接口组网图 111
图 1-44 告警抑制衰减示意图 120
图 1-45 端口扩展特性概念图 126
图 1-46 端口扩展系统示意图 127
图 1-47 控制通道示意图 128
图 1-48 内部转发通道示意图 129
图 1-49 端口扩展系统的数据转发 130
图 1-50 AP 初次上线后的即插即用流程 131
图 1-51 AP 重启上线后的即插即用流程 133
图 1-52 Master 重启后的 AP 即插即用流程 134
图 1-53 AP 下线流程 135
图 1-54 AP 迁移流程 136
图 1-55 端口扩展系统网络管理示意图 137
图 1-56 端口扩展系统作为 PE 节点示意图 138
图 1-57 在端口扩展场景中部署 HQoS 接入 138
图 1-58 端口扩展组网图 140
图 1-59 配置端口扩展系统的典型组网图 159

表格目录

表 1-1 NetEngine 8100 X, NetEngine 8000 X, NetEngine 8000E X 支持的物理接口命令视图和提示符 3
表 1-2 逻辑接口命令视图和提示符 7
表 1-3 控制接口震荡功能 11
表 1-4 control-flap 参数配置建议 12
表 1-5 control-flap 参数取值影响举例 13
表 1-6 逻辑接口列表 16
表 1-7 开销帧字段含义 25
表 1-8 Tunnel 接口支持的隧道类型列表 46
表 1-9 NetEngine 8100 X, NetEngine 8000 X, NetEngine 8000E X 支持的物理接口命令视图和提示符 50
表 1-10 逻辑接口命令视图和提示符 54
表 1-11 控制接口震荡功能 56
表 1-12 接口参数 57
表 1-13 配置接口参数 59
表 1-14 逻辑接口列表 78
表 1-15 不同型号子卡对应的能加入同一 Group 的物理口编号和 port-id 参数的取值范围 85
表 1-16 流程详细描述 131
表 1-17 流程详细描述 133
表 1-18 流程详细描述 134
表 1-19 流程详细描述 135
表 1-20 流程详细描述 136
表 1-21 date 类型的时间格式各部分描述 156

1 配置

1.1 接口与链路

1.1.1 接口管理配置

1.1.1.1 接口管理特性描述

1.1.1.1.1 接口管理介绍

定义

接口是该设备与网络中的其他设备交换数据并相互作用的部件，分为物理接口和逻辑接口两类：

- 物理接口是真实存在、有器件支持的接口。
- 逻辑接口是指能够实现数据交换功能但物理上不存在、需要通过配置建立的接口。

目的

每一个物理接口用于连接通信设备与传输数据的介质（如线缆等），接口与传输数据的介质共同形成为数据端设备提供传送数据的通路。为了达到给数据传送服务的目的，一是要保证数据能在其上正确通过，二是要提供足够的带宽，以减少信道上的拥塞。

逻辑接口指能够实现数据交换功能但物理上不存在的接口，所以逻辑接口并不需要投入额外的硬件资源，大大节省投资成本。

通常，交换设备的接口数比较多，并且很多接口具有相同的配置。如果对这些接口进行逐个配置，不但操作繁琐，而且容易输入错误。为解决此问题，可以创建一个端口组，然后将需要执行相同配置命令的接口加入到该端口组，在端口组视图下配置命令时，系统会自动到端口组绑定的所有成员接口下执行这些命令行，完成接口批量配置。

受益

通过接口管理，用户可以获得如下受益：

- 物理接口与传输介质共同组成传输通道，正确快速传输数据，实现用户正常通信。
- 在不增加硬件投资的情况下，逻辑接口能够实现数据通信。
- 通过端口组，可以完成接口的批量配置，减少单独配置的输入错误，同时大大节省人力。

1.1.1.1.2 接口管理原理描述

基本概念

接口类型

接口是设备与网络中的其他设备交换数据并相互作用的部件，分为物理接口和逻辑接口两类。

- 物理接口

  物理接口是真实存在、有器件支持的接口。物理接口分为两种：

  - 局域网接口：路由器可以通过它与局域网中的网络设备交换数据。
  - 广域网接口：路由器可以通过它与远距离的外部网络设备交换数据。
- 逻辑接口

  逻辑接口是指能够实现数据交换功能但物理上不存在、需要通过配置建立的接口。

接口编号规则

请参见“硬件描述”中硬件指南手册内的“硬件描述 > 单板 > 单板概述 > 单板/子卡槽位号与接口号规则”章节。

接口视图和提示符

NetEngine 8100 X, NetEngine 8000 X, NetEngine 8000E X支持的物理接口的命令视图和提示符如**表1-1**所示，逻辑接口的命令视图和提示符如**表1-2**所示。

表 1-1 NetEngine 8100 X, NetEngine 8000 X, NetEngine 8000E X 支持的物理接口命令视图和提示符

接口名称	命令视图	进入命令	提示符
千兆以太网接口	GE接口视图	在系统视图下键入**interface gigabitethernet** 2/0/0	[~HUAWEI-GigabitEthernet2/0/0]

接口名称	命令视图	进入命令	提示符
10GE接口	10GE接口视图	在系统视图下键入**interface gigabitethernet** 1/0/0 **说明** 通过**display interface brief**命令查看到带有“10G”标识的GigabitEthernet接口为10G带宽的GigabitEthernet接口。	[~HUAWEI-GigabitEthernet1/0/0]
25GE接口	25GE接口视图	在系统视图下键入**interface 25GE** 2/0/0	[~HUAWEI-25GE2/0/0]

接口名称	命令视图	进入命令	提示符
40GE接口	40GE接口视图	在系统视图下键入**interface 40GE** 2/0/0	[~HUAWEI-40GE2/0/0]
100GE接口	100GE接口视图	在系统视图下键入**interface 100GE** 1/0/0	[~HUAWEI-100GE1/0/0]
200GE接口	200GE接口视图	在系统视图下键入**interface 200GE** 1/0/0	[~HUAWEI-200GE1/0/0]
400GE接口	400GE接口视图	在系统视图下键入**interface 400GE** 1/0/0	[~HUAWEI-400GE1/0/0]
1200GE接口	1200GE接口视图	在系统视图下键入**interface 1200GE** 1/0/0	[~HUAWEI-1200GE1/0/0]

接口名称	命令视图	进入命令	提示符
XGigabitEthernet接口	XGigabitEthernet接口视图	在系统视图下键入**interface XGigabitEthernet** 1/0/0	[~HUAWEI-XGigabitEthernet1/0/0]
50GE接口	50GE接口视图	在系统视图下键入**interface 50GE** 1/0/0	[~HUAWEI-50GE1/0/0]
50|100GE接口	50|100GE接口视图 **说明** 该类型接口默认速率是50G，可以切换到100G。	在系统视图下键入**interface 50|100GE** 1/0/0	[~HUAWEI-50|100GE1/0/0]
FlexE-50G接口	FlexE-50G接口视图	在系统视图下键入**interface FlexE-50G** 1/0/0	[~HUAWEI-FlexE-50G1/0/0]

接口名称	命令视图	进入命令	提示符
FlexE-100G接口	FlexE-100G接口视图	在系统视图下键入**interface FlexE-100G** 1/0/0	[~HUAWEI-FlexE-100G1/0/0]
FlexE-400G接口	FlexE-400G接口视图 **说明** 该接口仅在NetEngine 8000 X4和NetEngine 8000 X8设备上支持。	在系统视图下键入**interface FlexE-400G** 1/0/0	[~HUAWEI-FlexE-400G1/0/0]

表 1-2 逻辑接口命令视图和提示符

接口名称	命令视图	进入命令	提示符
子接口	子接口视图	在系统视图下键入**interface gigabitethernet 1/0/0.1**	[~HUAWEI-GigabitEthernet1/0/0.1]
Eth-Trunk接口	Eth-Trunk接口视图	在系统视图下键入**interface eth-trunk 2**	[~HUAWEI-Eth-Trunk2]
VE接口	VE接口视图	在系统视图下键入**interface virtual-ethernet 1/0/0**	[~HUAWEI-Virtual-Ethernet**1/0/0**]
Global-VE接口	Global-VE接口视图	在系统视图下键入**interface global-ve 0**	[~HUAWEI-Global-VE0]
VLANIF接口	VLANIF接口视图	在系统视图下键入**interface vlanif 2**	[~HUAWEI-Vlanif2]

接口名称	命令视图	进入命令	提示符
Loopback接口	Loopback接口视图	在系统视图下键入**interface loopback 2**	[~HUAWEI-LoopBack2]
NULL接口	NULL接口视图	在系统视图下键入**interface null 0**	[~HUAWEI-NULL0]
Tunnel接口	Tunnel接口视图	在系统视图下键入**interface tunnel 2**	[~HUAWEI-Tunnel 2]
NVE接口	NVE接口视图	在系统视图下键入**interface nve 1**	[~HUAWEI-Nve1]
FlexE接口	FlexE接口视图	在系统视图下键入**interface FlexE** 2/0/5	[~HUAWEI-FlexE2/0/5]
PW-VE接口	PW-VE接口视图	在系统视图下键入**interface pw-ve 1**	[~HUAWEI-pw-ve1]
ServiceIf接口	ServiceIf接口视图	在系统视图下键入**interface ServiceIf 1**	[~HUAWEI-ServiceIf1]

常用的链路层协议和接入技术

链路层负责无差错地将数据从一个站点发送到相邻的站点。它从网络层接收数据包，然后将它封装到称为“帧”的数据单元里，再传给物理层，进行传输。

下面介绍NetEngine 8100 X, NetEngine 8000 X, NetEngine 8000E X支持的几种主要的链路层协议。

- Ethernet

  现在的局域网主要是指以太网。以太网是一种广播类型的网络。它因为灵活、简单且易于扩展而被大规模应用

- Trunk

  Trunk技术有如下优点：

  - 增加带宽：接口的带宽是各成员接口带宽的总和。
  - 提高可靠性：当某个成员链路出现故障时，流量会自动的切换到其他可用的链路上，从而提供整个Trunk链路的可靠性。

- PPP

  点到点协议PPP（Point-to-Point Protocol）是在串行链路上封装IP数据报文，既支持数据位为8位且无奇偶校验的异步模式，也支持面向比特的同步链接。

PPP主要包括建立、配置及测试数据链路的链路控制协议（Link Control Protocol）和针对不同网络层协议的网络控制协议（Network Control Protocol）。

最大传输单元 MTU

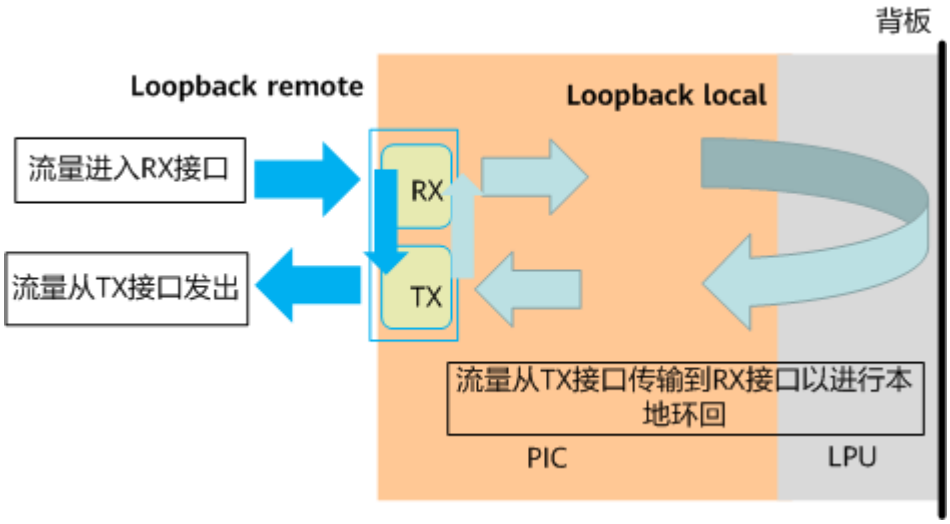
MTU（Maximum Transfer Unit）指在一个物理网络上能够传输的最大的分组字节长度。当同一个网络上的两台设备进行互通时，该网络的MTU非常重要。MTU的大小决定了发送端一次能够发送报文的最大字节数，如果MTU设置的超过了接收端所能够承受的最大值，或者是超过了发送路径上途经的某台设备所能够承受的最大值，这样就会造成报文分片甚至丢弃，加重网络传输的负担。所以设备在进行通信之前必须要把MTU计算明确，才能保证每次发送的报文都能够畅通无阻的到达接收端，确保报文发送一次成功。

- 如果设置强制不分片，IP层在传输数据时可能会出现丢包现象。所以当需要保证网络中的大报文不丢失时，需要对大报文进行强制分片。
- 如果MTU设置过小而报文尺寸较大，可能会造成分片过多，报文被QoS队列丢弃。
- 如果MTU设置过大，可能会造成报文的传输速度较慢。

环回方式介绍

路由器的物理接口支持端口本地环回（**loopback local**）和远端环回（**loopback remote**），两种环回的路径如下图所示。

图 1-1 本地环回示意图



- **loopback local**

  本地环回与插上光模块进行光纤环回的区别是，本地环回的业务流相对光模块进行光纤环回的业务流少经过了Framer的光模块驱动接口电路，因此在转发测试时，只需少数几块板可以插满光模块进行光纤环回以验证Framer的光模块驱动接口电路外，其余的环境都可以采取在端口设置本地环回的方法验证所有接口的转发性能和稳定性，这样也可节约物料。

  重定向是QoS策略的一种类行为，可以用来改变IP报文的下一跳的IP地址和出接口，并应用于具体的接口上，实现接口IP业务改变转发目的的作用。配合端口环

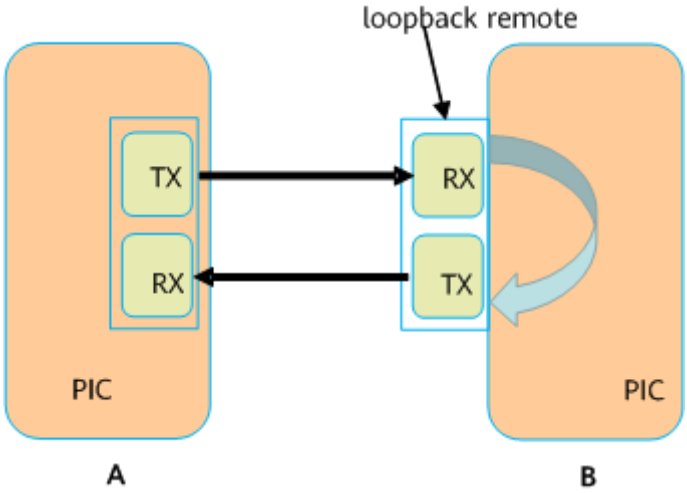
回，就可以实现一个仪器接口遍历所有单板物理接口的转发测试目的。若仅配置**loopback local**，不配置重定向或配置的策略不匹配，系统不会转发报文。

本地环回还可进行功能验证。比如镜像特性，受物料限制，对于观测口可以配置**loopback local**，就可以对流量进行观测，验证功能是否生效。

- **loopback remote**

  远端环回一般进行故障诊断时使用，用于检测物理层，通过子卡计数、接口状态或其他参数来查看物理链路质量。

图 1-2 远端环回示意图



如上图所示，配置**loopback remote**的接口收到对端发送过来的报文，不按照报文的目的地址进行转发，而是直接在接口（不区分二层接口或三层接口）处将收到的报文不做任何处理返回给对端A。

A端收到B端返回的报文处理方式如下：

- 如果A端的接口是三层口，从B端环回的Ping报文由于目的MAC和A端接口MAC不一致，Ping报文会在A端设备内丢弃，但子卡上会有接口计数，通过接口收发计数“Input”和“Output”字段信息判断链路质量。
- 如果A端的接口是二层口，通过该接口是无法成功发送Ping报文。如果通过打流或其他方式由A端向外发送报文，A端收到B端环回后的报文不检查MAC同时根据MAC转发。
  - 如果A端发送报文的目的MAC地址指向对端设备，环回报文会在两台设备间反复环回。
  - 如果A端发送报文的目的MAC地址是广播地址，环回报文在两台设备间反复环回的同时会向广播域广播。

该方式会导致广播风暴，请慎用。

控制接口震荡（control-flap）

网络应用中，由于物理信号干扰、链路层配置错误等原因可能导致设备接口频繁地交替出现Up和Down状态，造成路由协议、MPLS等反复震荡，对设备和网络产生较严重影响，甚至可能造成部分设备瘫痪，网络不可使用。控制接口震荡特性对接口频繁Up、Down事件进行控制，使其小于一定的频率，以减小对设备及网络稳定性的影响。

目前支持两种控制方式。

表 1-3 控制接口震荡功能

功能	功能描述	选择原则
control-flap	对网络层以下接口频繁Up/Down事件进行控制，以减小对设备及网络稳定性的影响。	● 可以指定接口进行配置； ● 从网络层开始抑制向路由管理模块通知接口震荡，是专门针对网络层稳定性的功能配置； ● 用户可以根据业务需求对参数进行精确配置； ● 需要充分理解该算法，才能配置，对用户要求高，命令行易用性差。
damp-interface	对物理层接口频繁Up/Down事件进行控制，以减小对设备及网络稳定性的影响。	● 该功能支持全局性配置也支持指定接口进行配置； ● 从物理层开始抑制，这样一旦接口物理震荡，整个链路层和网络层都能得到有效抑制； ● 从物理层接口震荡进行控制，可以防止上层业务频繁的使能、去使能，引发系统CPU、内存等过度消耗； ● 不需要了解复杂算法，对用户要求低，命令行易用性好。

- control-flap

  控制接口震荡特性（control-flap）对接口频繁Up、Down事件进行控制，使其小于一定的频率，以减小对设备及网络稳定性的影响。

  在接口震荡抑制中，有以下几个概念：

  – 抑制惩罚值和门限

    抑制算法会根据抑制惩罚值对接口进行抑制或解除抑制。

    ▪ 接口抑制惩罚值（penalty value）：根据接口Up/Down的情况由抑制算法计算出来的一个值。抑制惩罚值随接口Up/Down的次数增加，同时按半衰期衰减。

    ▪ 接口抑制门限（suppress）：当接口抑制惩罚值超过此值时，接口被抑制。

- 接口重用门限（reuse）：当接口抑制惩罚值小于此值时，接口抑制被解除。
- 接口抑制惩罚值最大值（ceiling）：接口抑制惩罚值的最大值，当接口抑制惩罚值增加到最大值时便不再增加。

参数取值需保证：接口重用门限（reuse）< 接口抑制门限（suppress）< 接口抑制惩罚值最大值（ceiling）。

– 半衰期

从接口第一次变为Down，半衰期开始计时。设备每秒根据接口实际状态匹配对应的半衰期，如果达到相应状态的半衰期，抑制惩罚值减半。一个半衰期结束后，下一个半衰期开始。

- 接口Up时的半衰期（decay-ok）：当前接口实际状态为Up时，如果距离上个半衰期结束的时间达到此半衰期值，抑制惩罚值减半。
- 接口Down时的半衰期（decay-ng）：当前接口实际状态为Down时，如果距离上个半衰期结束的时间达到此半衰期值，抑制惩罚值减半。

– 接口最大抑制时间：接口被抑制的最长时间，最大抑制时间为30分钟。当接口被抑制的时间达到最大抑制时间后，接口自动解除抑制。

通过对这些参数进行设置，以达到对接口Up/Down事件进行控制的目的。

参数配置时可参考如下建议：

表 1-4 control-flap 参数配置建议

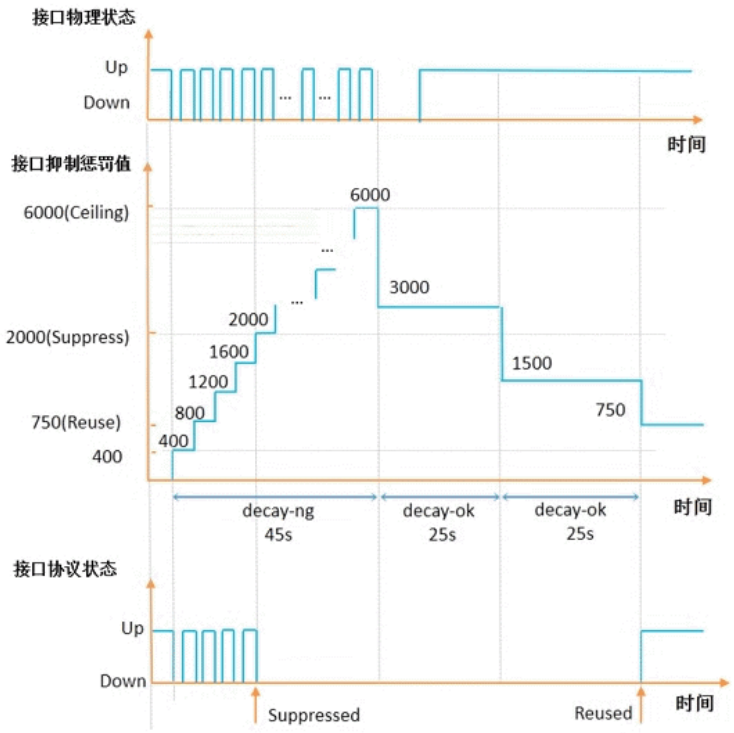
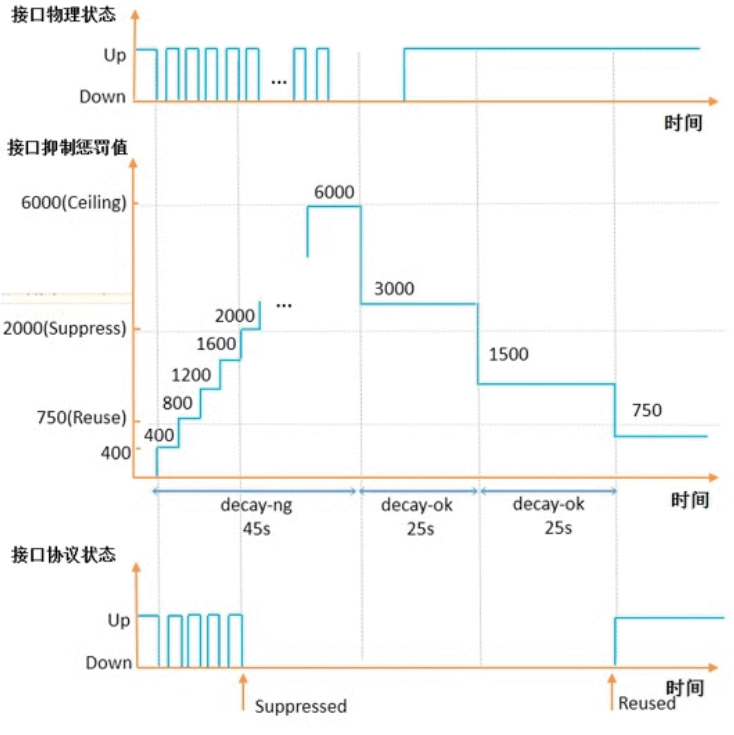
配置目的	参数配置建议			
	suppress	reuse	decay-ok	decay-ng
使接口较晚被抑制	调大	N/A	调小	调小
使接口较早被抑制	调小	N/A	调大	调大
使接口较早解除抑制	N/A	调大	调小	调小
使接口较晚解除抑制	N/A	调小	调大	调大

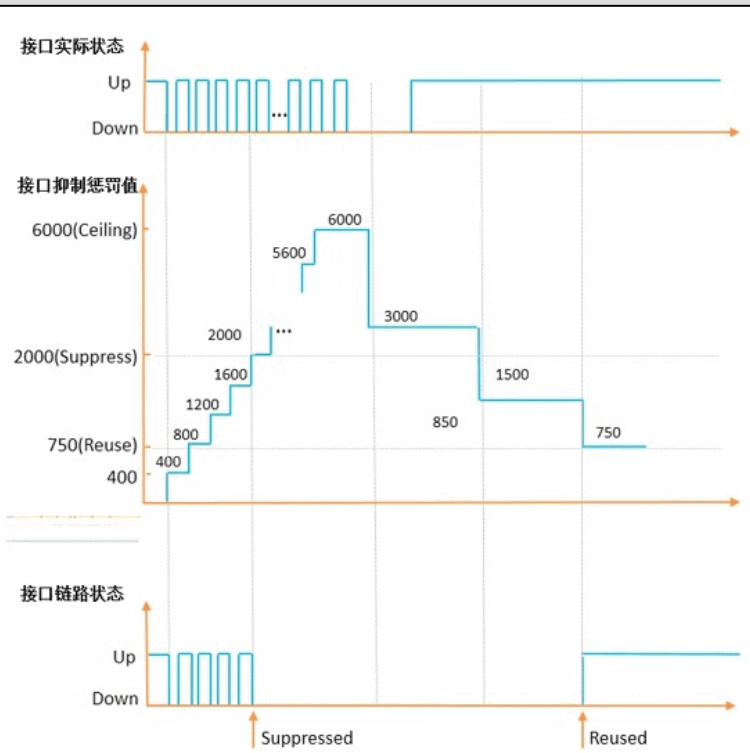
decay-ok和decay-ng可以分别配置：

– 如果接口Up的时间长，且希望接口Up时尽快可用，建议把decay-ok调小。
– 如果接口Down的时间长，且希望接口Down时尽可能的被抑制，建议把decay-ng调大。

举例说明如下：

表 1-5 control-flap 参数取值影响举例

参数	取值变化对接口抑制的影响举例
suppress	
reuse	

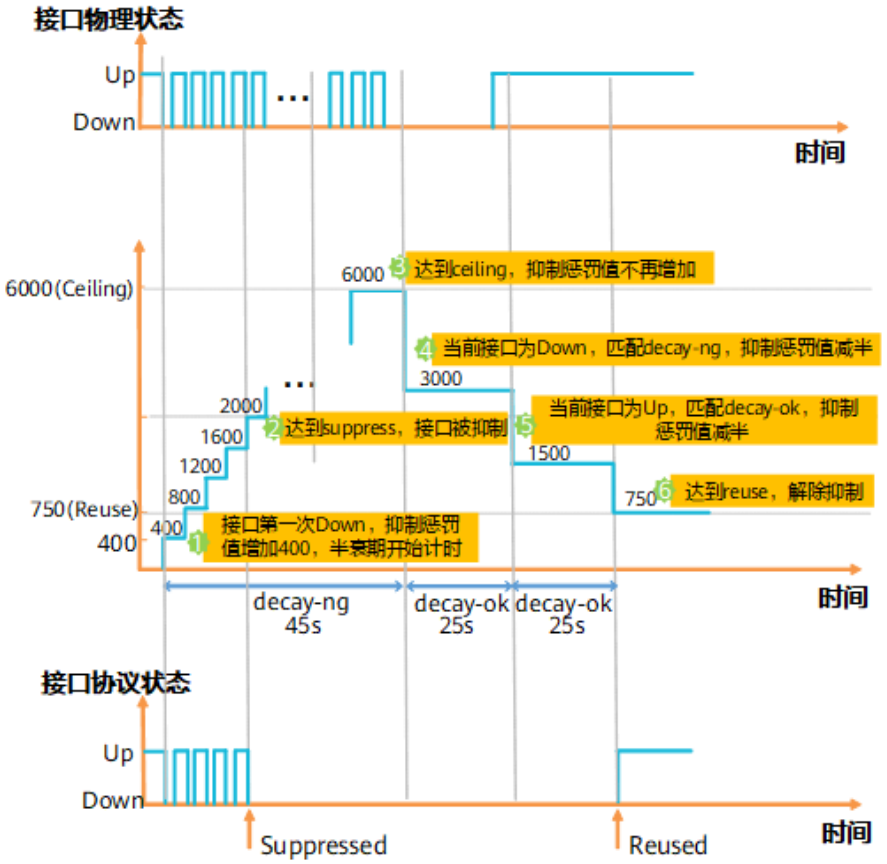
参数	取值变化对接口抑制的影响举例
decay-ok和decay-ng	

接口震荡抑制的原理：

如图1-3所示，接口抑制惩罚值缺省为0，接口实际状态每Down一次，抑制惩罚值增加400。从接口第一次Down开始，半衰期开始计时。每秒根据接口实际状态检查对应的半衰期是否到期。如果达到半衰期，抑制惩罚值减半。一个半衰期结束后，下一个半衰期开始。

- 如果抑制惩罚值超过接口抑制门限数值时，接口被抑制。接口被抑制时，使用**display interface**、**display interface brief**、**display ip interface brief**等命令查看接口的协议状态始终为DOWN(dampening suppressed)，不会再随接口的物理状态震荡。
- 如果抑制惩罚值降到小于接口重用门限数值，接口解除抑制。接口解除抑制后，接口的协议状态恢复为与实际情况一致，不再出现DOWN(dampening suppressed)。
- 如果抑制惩罚值达到ceiling，抑制惩罚值不再增加。

图 1-3 接口震荡抑制原理图



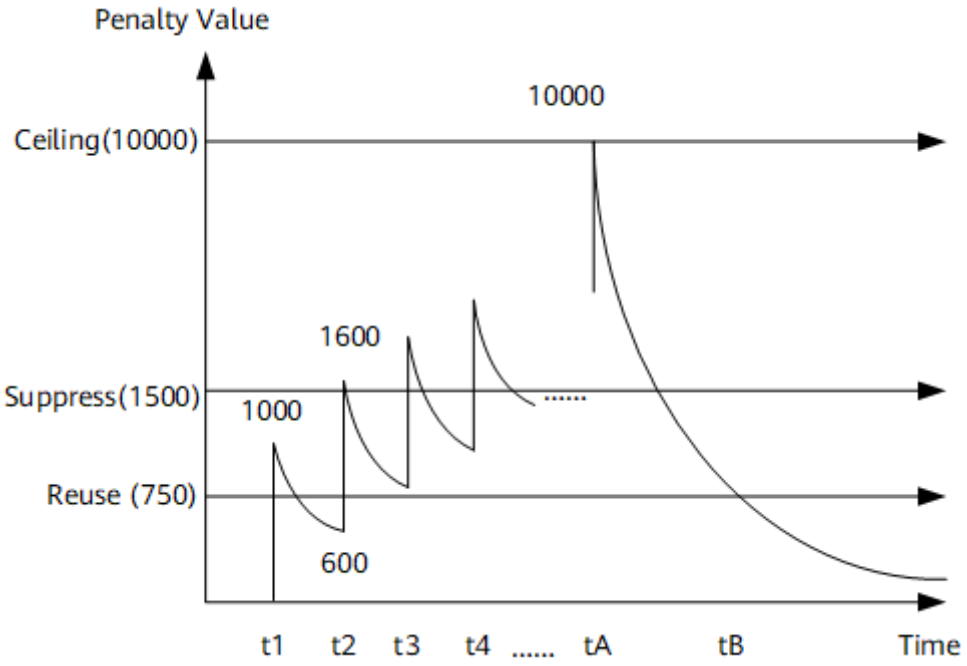
- damp-interface

  在物理状态震荡抑制（damp-interface）中，有以下几个概念：

  - 接口抑制惩罚值（penalty value）：接口抑制惩罚值是根据接口Up/Down的情况由抑制算法计算出来的一个值，其算法的核心是接口抑制惩罚值随接口Up/Down的次数线性增加，同时按指数衰减。
  - 接口抑制门限（suppress）：当接口抑制惩罚值超过此值时，接口被抑制。
  - 接口重用门限（reuse）：当接口抑制惩罚值小于此值时，接口抑制被解除。
  - 接口抑制惩罚值最大值（ceiling）：接口抑制惩罚值的最大值，当接口抑制惩罚值增加到最大值时便不再增加。ceiling = reuse * 2 (MaxSuppressTime/HalfLifeTime)
  - 接口抑制惩罚值半衰期（half-life-period）：接口抑制惩罚值的半衰期。从接口第一次变为Down，开始计算半衰期。如果达到半衰期，抑制惩罚值减半。一个半衰期结束后，下一个半衰期开始。
  - 最长抑制时间（max-suppress-time）：接口被抑制后，最长抑制接口状态的时间。超过该时间后，按照接口当前状态上报。

  以上参数之间的关系可以用图1-4来说明

图 1-4 物理接口震荡抑制示意图



接口状态在t1时刻由于发生Down事件而受到惩罚，惩罚值加1000（设备实际的惩罚值为1，这里的值是设备实际值*1000），之后惩罚值按照半衰期法则进行指数衰减，到t2时，接口再次发生Down事件，惩罚值加1000，达到1600，此时接口发生Up事件，因为惩罚值已经超出suppress值1500，接口状态被抑制。由于接口持续震荡，惩罚值持续增加，tA时刻到达ceiling值10000后惩罚值不再增加。随着时间的推移，惩罚值逐渐降低，在tB时刻已下降到reuse值750，接口抑制状态解除。

说明

Loopback接口、portswitch二层口和NULL接口不支持设置MTU和部署control-flap特性。

逻辑接口

逻辑接口是指能够实现数据交换功能但物理上不存在、需要通过配置建立的接口。下面介绍如下几种常见的逻辑接口。

表 1-6 逻辑接口列表

接口名称	应用场景及特性简介
DCN-Serial接口	全局使能DCN特性后，DCN会自动建立动态的DCN-Serial口。
VE接口（Virtual Ethernet，虚拟以太网接口）	在配置L2VPN接入多个L3VPN时，需要创建VE接口。用于终结L2VPN，接入L3VPN。但普通VE接口不具备全局性，只绑定在一块单板上，当单板出现故障时，会导致业务中断。

接口名称	应用场景及特性简介
Global-VE接口（Global Virtual Ethernet，全局虚拟以太网接口）	全局虚拟以太网接口（Global-VE）是一种具有VE口性质的逻辑接口，主要应用在配置L2VPN接入多个L3VPN时，创建虚拟以太网接口来终结L2VPN并接入L3VPN。 ● 但是与普通VE接口不同的是，普通VE接口只绑定在一块单板上，当单板出现故障时，业务会中断。Global-VE接口分别支持全局L2VE和L3VE，不会因为其中个别单板故障而导致整体业务的中断。 ● Global-VE的环回功能与单板无关，不会因为单板掉电、损坏而影响环回流程，转发的环回流程可以进行优化，转发性能得以保证。 Global-VE接口不依赖于物理接口板，只要设备上电，就可以创建全局虚拟以太网接口。
FlexE接口	标准以太模式下的物理口，带宽是固定的，但通过FlexE技术可以将一个或多个物理口使能为灵活以太模式，加入到一个组中，这个组内的总带宽可以按需灵活分配给组内的逻辑口。 以上描述中，物理口加入的组称为FlexE组（FlexE Group），可共享组内物理口带宽的逻辑口称为FlexE接口（即灵活以太接口，也称FlexE业务接口）。 FlexE接口通过接口带宽隔离，即可以实现业务隔离。相比传统技术，在端口捆绑方面，FlexE能够实现比特级别的捆绑，解决传统Trunk捆绑逐流或逐包哈希不均匀问题；另外，每个FlexE接口都具备独立的MAC地址，不同接口之间的转发资源隔离，可以避免传统逻辑接口如VLAN子接口转发的头阻塞问题。 FlexE接口技术可以满足移动承载、家庭宽带、专线接入等使用大端口综合承载的场景需求，不同类型的业务承载在不同FlexE接口上，并基于FlexE接口配置带宽，达到基于业务控制带宽的目的，满足5G场景网络分片的需求。
VLAN信道化子接口	信道化接口可以通过信道化功能对带宽进行严格隔离。VLAN信道化子接口是指使能了信道化功能的以太物理端口的子接口，不同类型的业务承载在不同信道化子接口上，并基于信道化子接口配置带宽，实现同一物理接口上不同信道化子接口之间的带宽严格隔离，达到基于业务控制带宽的目的，解决不同子接口间业务的带宽抢占的问题。

接口名称	应用场景及特性简介
Loopback接口（环回接口）	目前，支持以下两种类型的环回接口： ● Loopback接口 当用户需要一个接口状态通常是Up的接口的IP地址时，可以选择Loopback接口的IP地址。Loopback接口具有以下优点： – Loopback接口一旦被创建，其物理状态和链路协议状态通常情况下是Up。即使该接口上没有配置IP地址。 – Loopback接口配置IP地址后，就可以对外发布。Loopback接口上可以配置32位掩码的IP地址，以达到节省地址空间的目的。 – Loopback接口不能封装任何链路层协议。数据链路层也就不存在协商问题，其协议状态通常情况下都是Up。 – 对于目的地址不是本地IP地址，出接口是本地Loopback接口的报文，设备会将其直接丢弃。 由于Loopback接口具备如上优点，Loopback接口常用来提高配置的可靠性。Loopback接口通常有两种主要应用： – Loopback接口的IP地址被指定为报文的源地址，可以提高网络可靠性。 – 根据Loopback接口的IP地址控制访问接口和过滤日志等信息，使信息变得简单。 **说明** 在Loopback接口监视接口监控组场景中，Loopback接口可能会联动接口监控组状态变为Down，其他情况下其物理状态和链路协议状态均为Up。 ● InLoopback0接口 系统在启动时，会自动创建一个InLoopback0接口，它是一个特殊而固定的Loopback接口。 InLoopback0接口使用环回地址127.0.0.1/8接收所有发送给本机的数据包。该接口上的IP地址是不可以改变的，也不通过路由协议对外发布。

接口名称	应用场景及特性简介
NULL0接口	NULL0接口类似于一些操作系统中支持的空设备（Null Devices），任何发送到该接口的网络数据报文都会被丢弃。系统自动创建一个NULL0接口。 由于任何到达NULL接口的报文都会被丢弃，可以将需要过滤掉的报文直接发送到NULL0接口，而不必配置访问控制列表。 由于NULL0接口具备如上所述特性，它主要被用在以下两方面： ● 防止路由环路 NULL0接口最典型的使用是用来防止路由环路。例如，在聚合一组路由时，总是创建一条到NULL0接口的路由。 ● 用于过滤流量 NULL0接口提供了过滤流量的一个可选的方法。可以通过将不想要的报文发送到NULL0接口，避免使用访问控制列表。 不能在NULL0接口上配置IP地址，也不能在NULL0接口上封装任何链路层协议。
以太网子接口	以太网子接口是在一个主接口上配置出来的虚拟接口，具有三层特性，可在以太网子接口上配置IP地址，实现VLAN间互通。以太网子接口是在一个主接口上配置出来的虚拟接口，这个主接口可以是物理接口也可以是逻辑接口。子接口共用主接口的物理层参数，又可以分别配置各自的链路层和网络层参数。用户可以禁用或者激活子接口，这不会对主接口产生影响。但主接口状态的变化会对子接口产生影响，特别是只有主接口处于连通状态时子接口才能正常工作。
ETH-Trunk接口	将多个以太网接口捆绑成一个逻辑接口，这个逻辑接口称为Eth-Trunk接口，捆绑在一起的每个以太网接口称为成员接口。Eth-Trunk接口可以实现增加带宽、提高可靠性和负载分担的功能。 基本原理请参见Trunk。
VLANIF接口	VLANIF接口是三层逻辑接口，当二层设备需要与网络层的三层设备通信时，由于二层设备上都是二层口无法配置IP地址，所以可以创建基于VLAN的逻辑接口，即VLANIF接口。VLANIF接口是网络层接口，可以配置IP地址，通过IP地址，该设备即能与网络层的其他设备互相通信。三层交换技术是将路由技术与交换技术合二为一的技术，在交换机内部实现了路由，提高了网络的整体性能。三层交换机通过路由表传输第一个数据流后，会产生一个MAC地址与IP地址的映射表。当同样的数据流再次通过时，将根据此表直接从二层通过而不是通过三层。为了保证第一次数据流通过路由表正常转发，路由表中必须有正确的路由表项。因此必须在三层交换机上部署VLANIF接口并部署路由协议，实现三层路由可达。

接口名称	应用场景及特性简介
Tunnel接口	MPLS TE隧道使用一种虚拟的逻辑接口，即Tunnel接口，进行转发。当应用这些类型的隧道时，必须先创建Tunnel接口。 基本原理请参见**TUNNEL接口应用**。

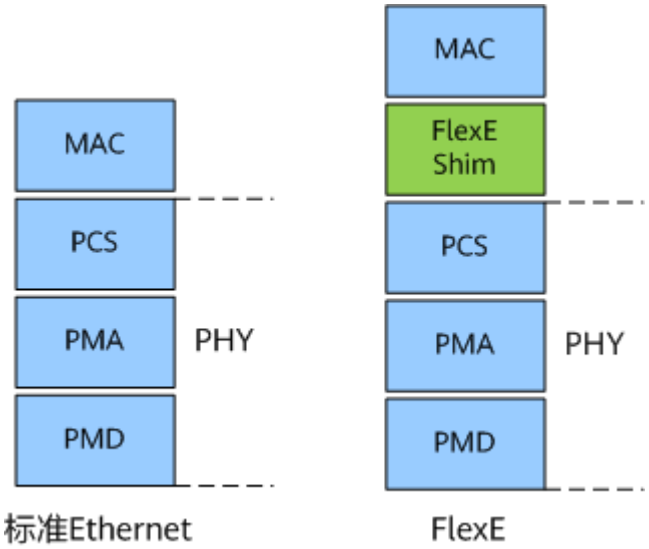
FlexE

?.1. FlexE 介绍

定义

灵活以太网FlexE（Flexible Ethernet）是承载网实现业务隔离承载和网络分片的一种接口技术，在IEEE 802.3定义的标准Ethernet技术基础上，通过在MAC与PHY层之间增加一个FlexE Shim层，实现了MAC与PHY层解耦（其实现如**图1-5**所示），打破两者强绑定的一对一映射关系，实现M个MAC可映射到N个PHY，从而实现了灵活的速率匹配。例如把100GE PHY池化为20个5GE时隙，而业务口可以灵活的从20个5GE时隙资源池中申请独立的带宽资源。

图 1-5 标准 Ethernet 与 FlexE 结构



目的

随着5G的建设，网络发展对移动承载带宽提出更高的需求，同时用户也希望通过统一的网络来承载各种不同的业务，包括家庭宽带业务、专线接入业务、移动承载等，这些需求对电信网络接口也提出了更高的要求。

当前标准Ethernet接口作为电信网络接口时存在以下问题：

- 不支持更加灵活的带宽颗粒度：随着业务与应用场景的多样化，用户希望Ethernet接口可提供更加灵活的带宽颗粒度，而不必受制于IEEE 802.3标准所确定的10-25-40-50-100-200-400GE的阶梯型速率体系。因为IEEE 802.3定义一个新

接口标准的制定过程可能需要数年，无法满足应用变化的诉求，同时也不可能出现一个带宽需求就制定一个接口标准，所以需要寻求其他接口类解决方案。

- 与光传输设备能力相互依赖：IP设备的Ethernet接口能力与光传输设备能力发展并不同步，例如光传输设备没有25/50GE接口，但是在两者组网互联时，又需要光传输网络的链路速率与UNI接口的以太网速率保持严格的匹配。
- 不支持面向多业务承载的增强QoS能力：标准Ethernet接口基于QoS报文优先级调度，会出现长包阻塞短包，导致短包时延变大，业务之间互相影响。

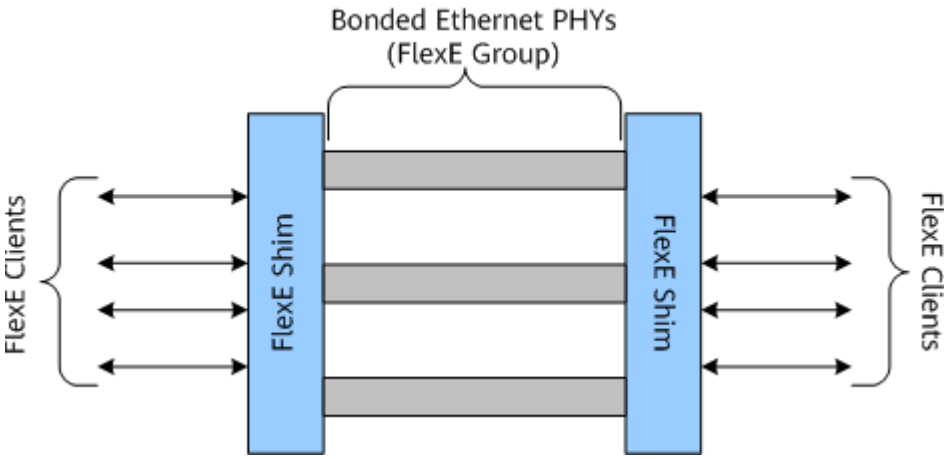
FlexE技术可以解决上述问题：

- 支持更加灵活的带宽颗粒度：FlexE可灵活配置接口速率，这些接口速率可以对应于或不对应于现有IEEE 802.3标准定义的接口速率，满足业务与应用场景的多样化。
- 支持面向多业务承载的增强QoS能力：FlexE在物理层接口上提供通道化的硬件隔离功能，实现硬切片保障业务SLA，各业务独占带宽，业务之间不互相影响，即可在多业务承载条件下实现增强QoS能力。

?.2. FlexE 通用架构

如图1-6所示，FlexE标准定义了Client/Group架构，可以支持任意多个不同子接口（FlexE Client）在任意一组PHY（FlexE Group）上的映射和传输。由于重用了现有IEEE 802.3定义的以太网技术，使得FlexE架构得以在现有以太网MAC/PHY基础上进一步增强。

图 1-6 FlexE 通用架构



FlexE包括FlexE Client、FlexE Shim和FlexE Group，其中：

- FlexE Client：对应于网络中外在观察到的各种用户接口，与现有IP/Ethernet网络中的传统业务接口一致。每个FlexE Client可根据带宽需求灵活配置，支持各种速率的以太网MAC数据流（如10G、40G、n*25G数据流，甚至非标准速率数据流），并通过64B/66B的编码方式将数据流传递至FlexE Shim层。
- FlexE Shim：作为插入标准以太网架构的MAC与PHY(PCS子层)中间的一个额外逻辑层，通过基于时隙分配器Calendar的Slot分发机制实现FlexE技术的核心架构。
- FlexE Group：本质上就是IEEE 802.3标准定义的各种以太网PHY层，默认把PHY的带宽池化为5GE粒度的资源。

?.3. FlexE 功能

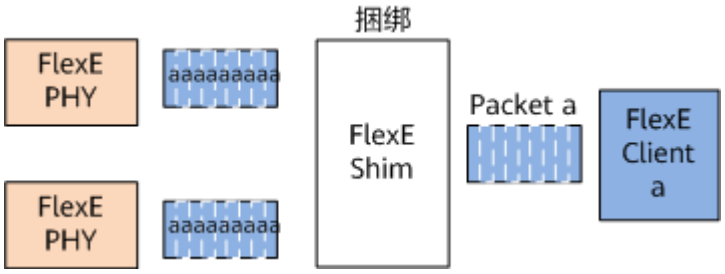
根据FlexE Client与FlexE Group的映射关系，FlexE技术可提供三种主要功能：捆绑、通道化和子速率，满足FlexE Client向上层应用提供各种灵活的带宽而不拘泥于物理PHY带宽。

FlexE以三大功能为基础，实现接口带宽按需分配和硬管道隔离等方案，可应用于IP网络中实现超大带宽接口、5G网络分片和光传输设备对接等场景。

捆绑

如图1-7所示，捆绑指多路PHY一起工作，支持更高速率。例如2路100GE PHY实现200GE MAC速率。

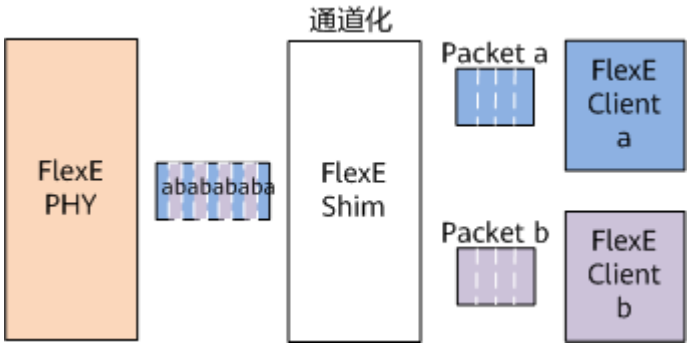
图 1-7 捆绑功能



通道化

如图1-8所示，通道化指多路低速率MAC数据流共享一路或多路PHY。例如在100GE PHY上承载75GE、25GE的2路MAC数据流，或者在三路100GE PHY上复用承载150GE、125GE与25GE的MAC数据流。

图 1-8 通道化功能

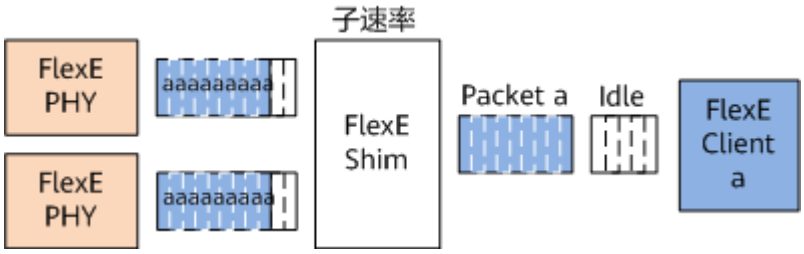


子速率

如图1-9所示，子速率指单一低速率MAC数据流共享一路或多路PHY，并通过特殊定义的Error Control Block实现降速工作。例如在100GE PHY上仅仅承载50GE MAC数据流。

子速率功能在某种意义上是通道化功能的一个子集。

图 1-9 子速率功能



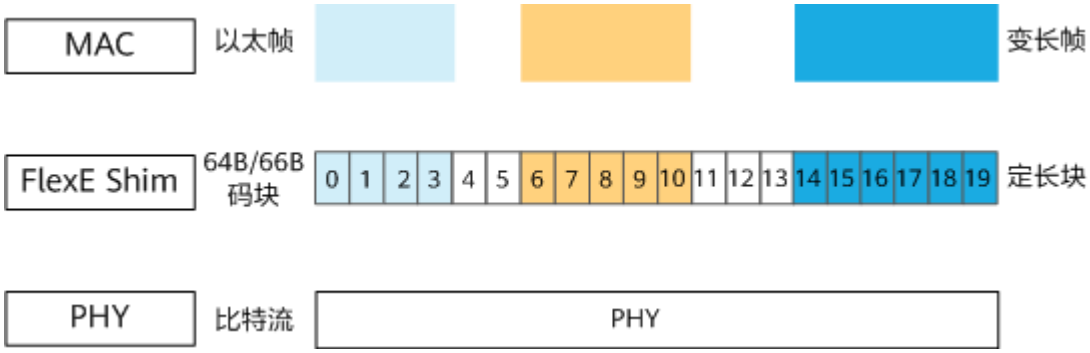
?.4. FlexE Shim

FlexE的核心功能通过FlexE Shim实现，以下内容介绍均以100GE PHY组成的FlexE Group为例。

FlexE Shim 机制

如图1-10所示，FlexE Shim把FlexE Group中的每个100GE PHY划分为20个Slot（时隙）的数据承载通道，其中每个Slot所对应的带宽为5GE，FlexE Client可以按照5GE颗粒的整数倍进行带宽灵活分配。同时把FlexE Client原始数据流中的以太帧以Block原子数据块(即64B/66B编码的数据块)为单位进行切分，这些原子数据块通过FlexE Shim的Calendar机制实现在FlexE Group中的时隙映射和传输，并互相实现严格隔离。

图 1-10 FlexE Shim 机制



Calendar 机制

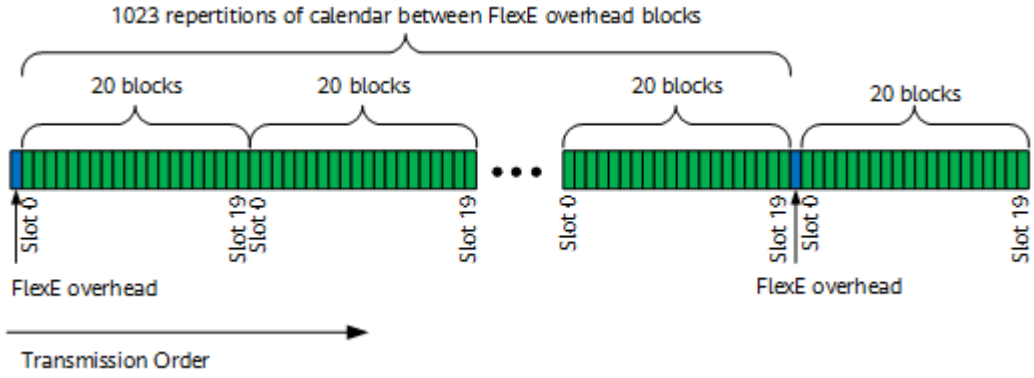
如图1-11所示，FlexE Shim的Calendar机制中，将“20blocks”（对应Slot0到Slot19）作为一个逻辑单元，并进一步将1023个“20blocks”作为Calendar组件，Calendar组件循环往复最终形成了5GE为颗粒度的Slot数据承载通道。

说明

具体到比特流层面，每个64B/66B原子数据块承载在一个Slot时隙中，图1-11中Slot作为承载64B/66B原子数据块的基本逻辑单元，可与Block概念等同。

FlexE技术按照每个FlexE Client所需带宽分配FlexE Group中可用的Slot，形成FlexE Client到一个或多个Slot的映射，再结合Calendar机制实现一个或多个FlexE Client在FlexE Group中的承载。

图 1-11 Calendar 机制



开销帧和开销复帧

为了实现对接的两个FlexE Client之间传递配置、管理信息，实现链路的自动协商，以及建立Client与Group中的Slot映射关系， FlexE Shim定义了开销帧（Overhead Frame）提供带内管理通道。开销帧由图1-11中蓝色的开销块组成，8个开销块组成一个开销帧，每32个开销帧组成一个开销复帧（Overhead MultiFrame）。开销块每隔1023个“20blocks”出现一次，实际上也是一个64B/66B的原子数据块，但每个开销块中所包含的字段是不同的。

开销帧格式如图1-12所示，一个开销帧由8个开销块组成，前3个开销块携带对应时隙与FlexE Client、FlexE Group的映射关系，后5个开销块用来携带管理报文，如DCN、1588v2等。

图 1-12 开销帧格式

Block#	SH		0	...	8	9	10	11	...	16	...	31	32	33	34	35	...	47	...	63
1	1	0	0x4B		C	OMF	RPF	SC	FlexE Group Number				0x5				0x000_0000			
2	0	1	C	FlexE Map		FlexE Instance Number					Reserved									
3	0	1	C	Client Calender A							Client Calender B		CR	CA	Reserved			CRC-16		
4	s	s	Management Channel - Section (two 66B blocks)																	
5	s	s																		
6	s	s	Management Channel - Shim to Shim or Synchronization Messaging Channel																	
7	s	s	Management Channel - Shim to Shim (two or three 66B blocks)																	
8	s	s																		

其中SH是数据经过64B/66B编码后添加的同步头字段，位宽2bit，当值为“10”时表示携带的数据为控制块，值为“01”时表示携带的数据为数据块，值为“00”或“11”时为非法字段；值为“ss”表示同步头有效，可能是“10”或“01”。

开销帧的第1个开销块是控制块，第2和3个开销块是数据块，第4到8个开销块是管理通道和消息同步通道，各字段含义如表1-7所示：

表 1-7 开销帧字段含义

字段名称	位宽（bits）	含义
0x4B	8	表示控制字符，用于接收方向数据同步锁定。
C	1	指示当前使用的Calendar配置，值为“0”表示使用Calendar A，值为“1”表示使用Calendar B，设置两个Calendar用来进行A/B时隙表建立，可实现带宽无损调整。
OMF	1	表示开销复帧指示位，其中一个开销复帧的前16个开销帧在该位的值为“0”，后16个开销帧在该位的值为“1”。
RPF	1	表示远端PHY故障（Remote PHY Fault）指示位。
SC	1	表示同步配置（Synchronization Configuration）指示位，值为“0”表示Shim to Shim管理通道占据开销帧的第6到8个开销块；值为“1”表示Shim to Shim管理通道占据开销帧的第7和8个开销块，6就分配给同步消息通道。
FlexE Group Number	20	表示协议定义的Group ID，需要提前规划。
0x5	4	表示“O”码位，用于接收方向数据同步锁定。
0x000_0000	28	协议暂时未用，全0显示。

字段名称	位宽（bits）	含义
FlexE Map	8*32	表示PHY与Group的映射关系，Bit Map格式，指示FlexE Group中包含的PHY，相应的bit位为“1”表示相应的PHY属于FlexE Group；相应的bit位为“0”表示相应的PHY不属于FlexE Group。以100GE PHY组成的FlexE Group为例，因有32个开销帧组成开销复帧，所以其范围是8*32=256bit，保留0和255，剩下可标记范围是1~254，当一个PHY ID为3时，那么这256个bit中只有第3个bit是1，其他bit都是0。
FlexE Instance Number	8	表示PHY ID，标识该时隙属于哪个PHY，相同Group下的PHY ID不可以重复，不同Group的PHY ID可以重复。
Reserved	N/A	表示保留域，用于将来对该协议实施可能的拓展。
Client Calendar	16*20	表示该时隙对应的Client ID，标识时隙与Client的关系；Calendar A和Calendar B用来进行A/B时隙表建立，可实现带宽无损调整。以100GE PHY组成的FlexE Group为例，其时隙有20个，Client ID占用前20个开销帧的Client Calendar字段。
CR	1	表示时隙表切换请求。
CA	1	表示时隙表切换应答。
CRC-16	16	表示开销帧的CRC校验域，主要是为了避免在存在误码的情况下，破坏时隙配置的内容。开销帧通过CRC保护，计算CRC是用前3个开销块中， 除CRC字段外的有内容的字段进行校验，保留位不计入。

字段名称	位宽（bits）	含义
Management Channel - Section	64	Section管理通道用于在FlexE相邻节点间传递管理消息，例如DCN和LLDP报文。
Management Channel - Shim to Shim	64	Shim to Shim管理通道用于在FlexE端到端节点间传递管理信息，例如DCN和LLDP报文。
Synchronization Messaging Channel	64	同步消息通道用于在FlexE相邻节点间传递时钟报文，例如1588v2报文。

说明

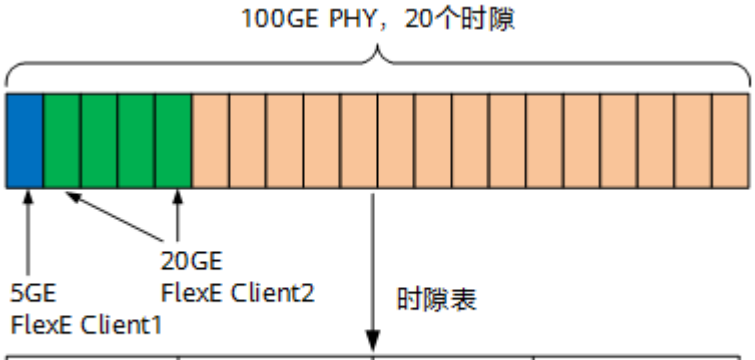
开销帧中的SH、0x4B、0x5和OMF字段组成数据接收方向的同步定帧，用于识别开销帧的第一个开销块，如果SH、0x4B和0x5字段，有5次与预期的位置不匹配，则FlexE开销复帧失锁，开销复帧失锁说明收到的32个开销帧不是同一个开销复帧里的数据，那么恢复出来的时隙信息就存在错误。另外OMF字段，若CRC校验正确，检测到0/1或1/0跳变就锁定，但一帧出现错误就报开销复帧失锁。

时隙表建立

如图1-13所示，以100GE PHY组成的FlexE Group为例，有20个5GE时隙，配置FlexE Client1为5GE带宽，FlexE Client2为20GE带宽，设备会分配对应的时隙（FlexE Client1分配图中蓝色时隙，FlexE Client2分配图中绿色时隙），并通过开销帧中携带的映射关系参数FlexE Group Number、 FlexE Map、 FlexE Instance Number和Client Calendar A/B来建立时隙表，发送端和接收端就按照时隙表的映射关系发送和接收报文。

从时隙表看，两台互联设备接口的Client ID、PHY ID和Group ID参数配置需要一致。

图 1-13 时隙表建立



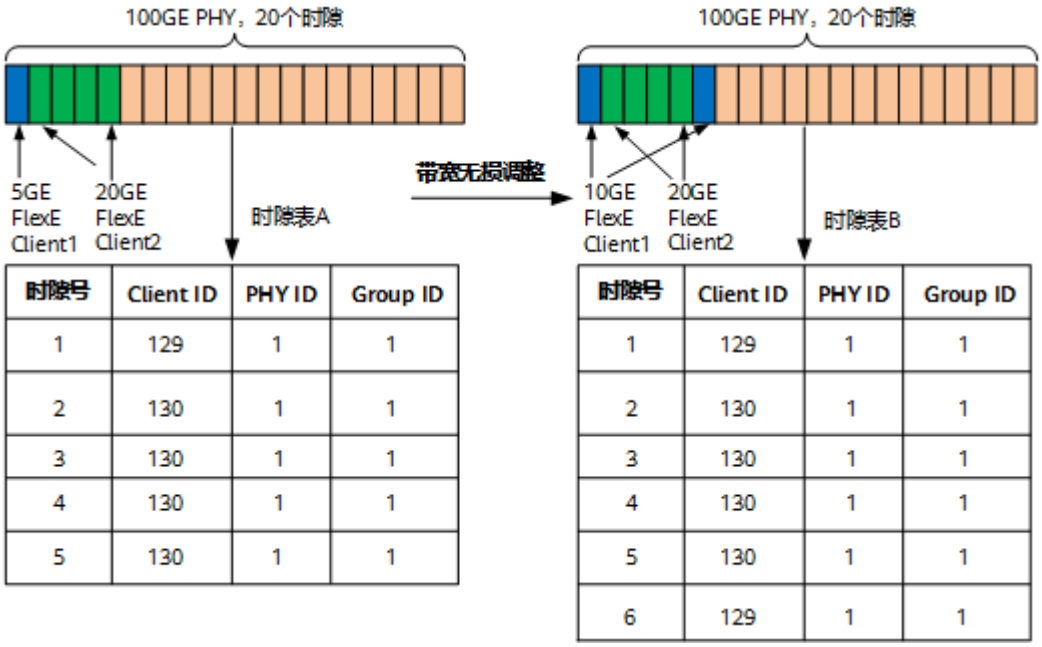
时隙号	Client ID	PHY ID	Group ID
1	129	1	1
2	130	1	1
3	130	1	1
4	130	1	1
5	130	1	1

时隙表切换实现带宽无损调整

每个FlexE Client有两个时隙表，任一时刻只有一个时隙表生效，当FlexE Client带宽发生调整时，需要切换时隙表。

如图1-14所示，将FlexE Client1带宽从5GE调整到10GE，正常采用时隙表A进行收发，时隙表B作为备份，当带宽调整时，会切换为时隙表B，采用时隙B进行收发，实现带宽无损调整。

图 1-14 时隙表切换实现带宽无损调整



时隙号	Client ID	PHY ID	Group ID
1	129	1	1
2	130	1	1
3	130	1	1
4	130	1	1
5	130	1	1

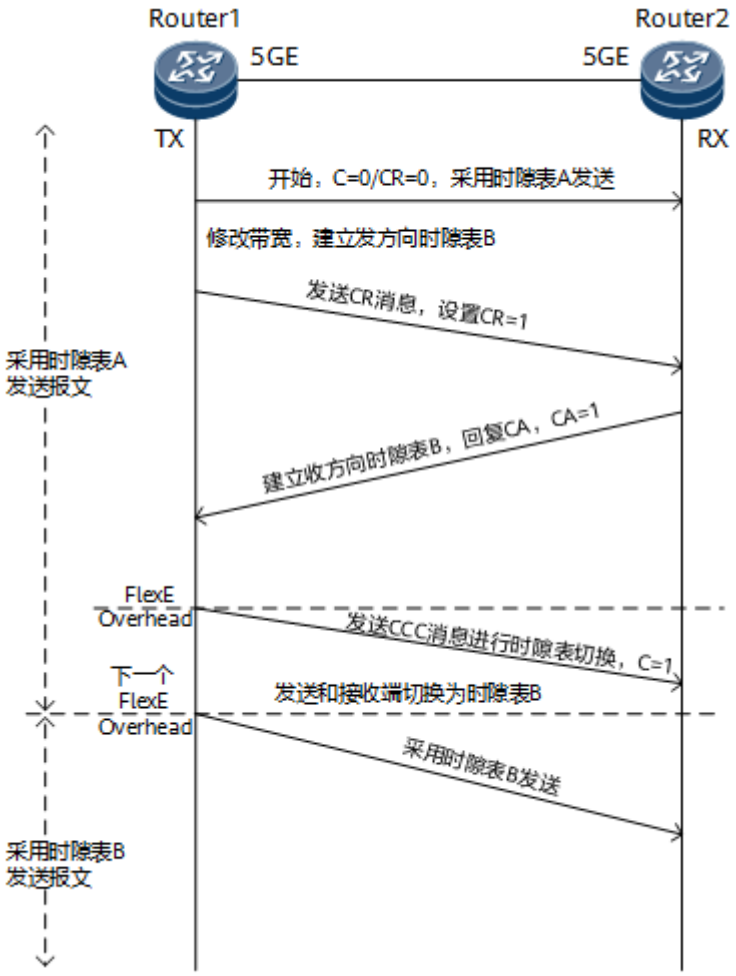
时隙号	Client ID	PHY ID	Group ID
1	129	1	1
2	130	1	1
3	130	1	1
4	130	1	1
5	130	1	1
6	129	1	1

具体流程如下图1-15所示：

1. Router1上的FlexE Client1采用时隙表A，按照5GE带宽正常发送。
2. FlexE Client1调整带宽为10GE后，Router1建立发送方向的时隙表B，并发送CR消息给Router2。
3. Router2收到Router1的CR消息后，建立接收方向的时隙表B，同时回复CA消息给Router1，表示接收端时隙表B建立完成。
4. Router1收到Router2回复的CA消息后，发送时隙表切换的CCC消息给Router2，从这一刻开始，以及下一个时隙周期内，Router1和Router2都采用时隙表A进行收发。
5. Router1发送CCC消息后的下一个时隙周期后，Router1按照时隙表B发送报文，Router2收到下一个时隙周期的开销帧后也切换为时隙表B，同时按照时隙表B接收报文。

同样，Router2上调整FlexE Client1带宽为10GE后，Router1接收方向也修改为时隙表B，最终两端均按照时隙表B进行报文收发。

图 1-15 时隙表切换具体流程



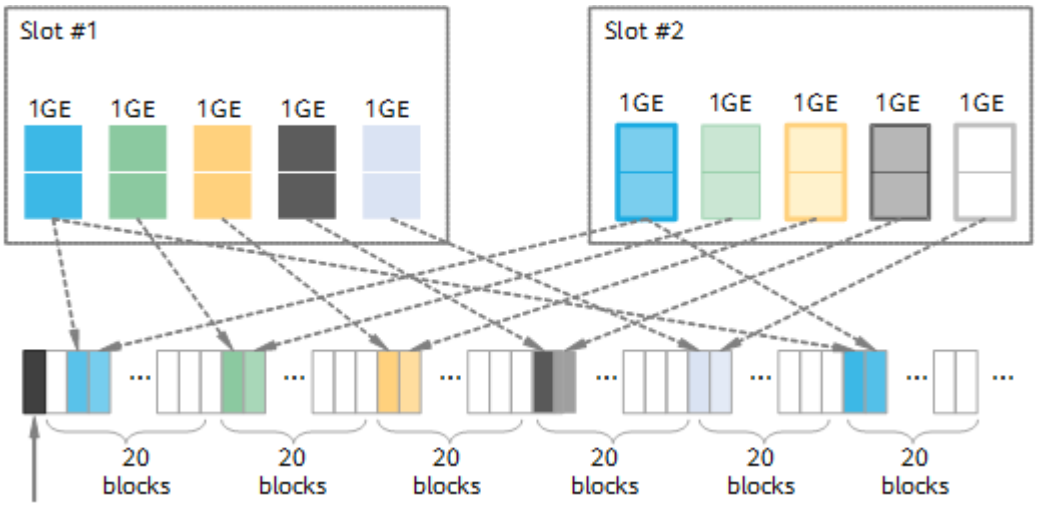
1GE 时隙粒度机制

FlexE标准定义的时隙粒度默认是5GE，但是为了满足5G垂直行业的应用诉求，比如智能电网、MEC等场景，当前设备实现了1GE的时隙粒度，原理如图1-16所示，把5GE时隙从时间维度展宽，5个1GE数据通过时分复用的方式占用一个FlexE标准5GE时隙（5种颜色块交替传送，实现5个1GE子颗粒），实现小颗粒子时隙扩展，同时整体方案兼容FlexE标准定义的主体架构。

说明

1GE时隙粒度是5GE的一个子时隙，只能在一个5GE时隙内生效，超过5GE后必须以5GE粒度为单位。

图 1-16 1GE 时隙粒度机制



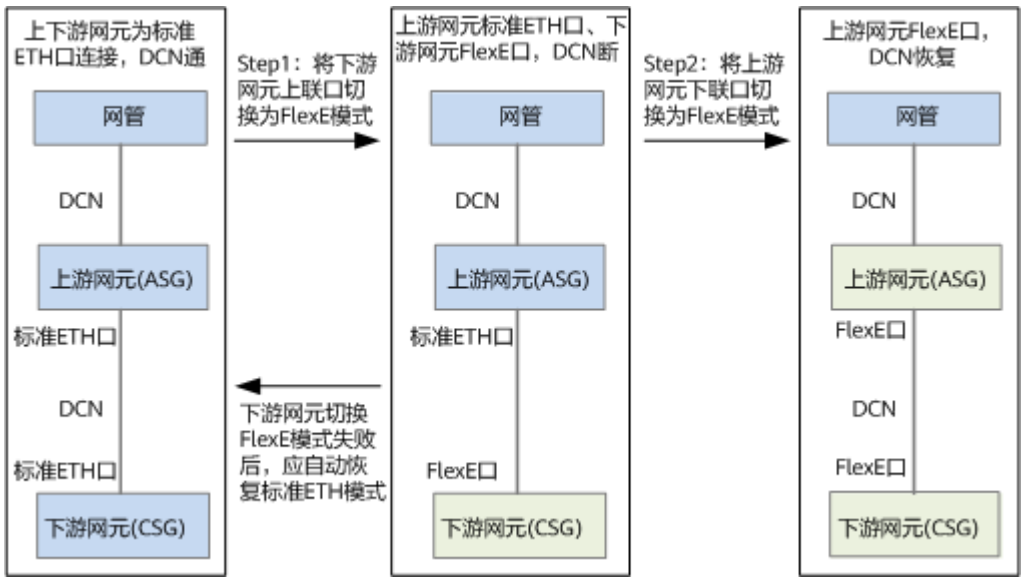
?.5. FlexE 模式切换

如图1-17所示，现网中上下游网元为标准Ethernet接口连接，DCN通，网管可以管理这些设备，接下来需要两步完成标准Ethernet接口切换为FlexE物理接口：

1. 将下游网元上联口切换为FlexE模式。
2. 将上游网元下联口切换为FlexE模式。

两个互联接口切换为FlexE模式后，网管的拓扑上会自动添加该链路连接，同时DCN功能默认使能，网管可以管理这些设备。

图 1-17 标准 Ethernet 接口切换为 FlexE 模式

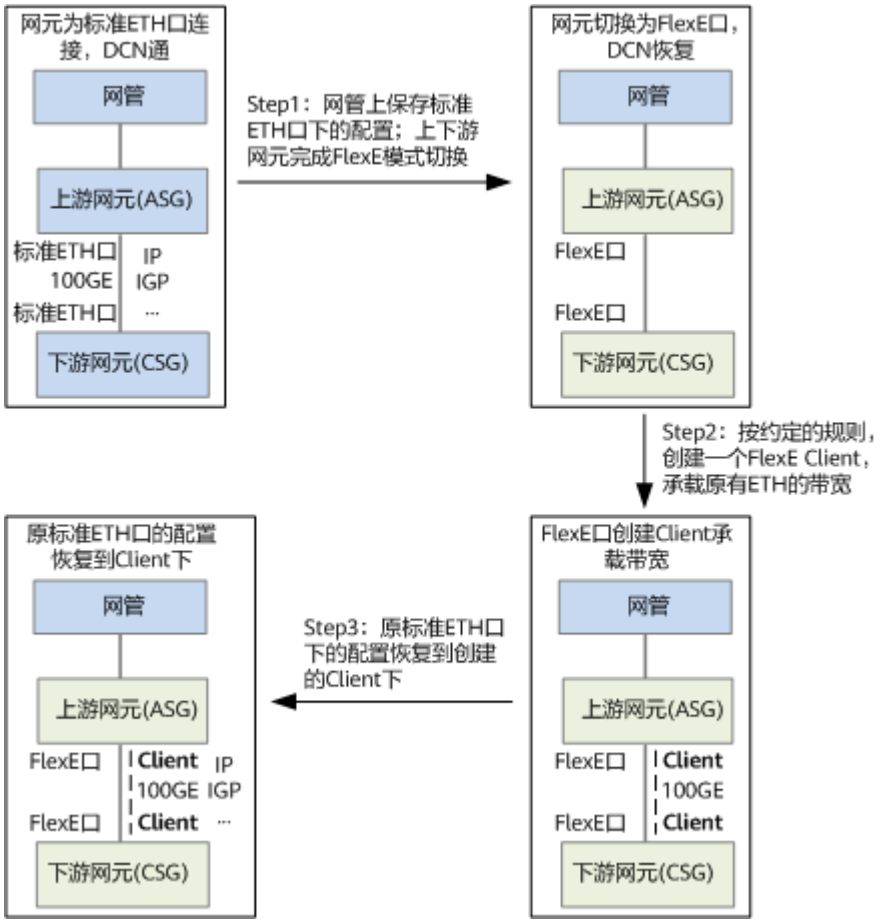


标准Ethernet接口切换为FlexE模式后，原有的标准Ethernet接口会消失，需要按照固定的规则确定一个FlexE Client来承载原有标准Ethernet接口的带宽和配置，实现配置恢复。如图1-18所示，配置恢复的具体步骤如下：

1. 网管上保存标准Ethernet接口下的配置，同时上下游网元完成FlexE模式切换。

2. 按约定的规则，创建一个FlexE Client，承载原有标准Ethernet接口的带宽。
3. 原标准Ethernet接口的配置恢复到创建的FlexE Client下。

图 1-18 标准 Ethernet 接口切换为 FlexE 模式后的配置恢复



FlexE Client带宽的配置有以下两种方式：

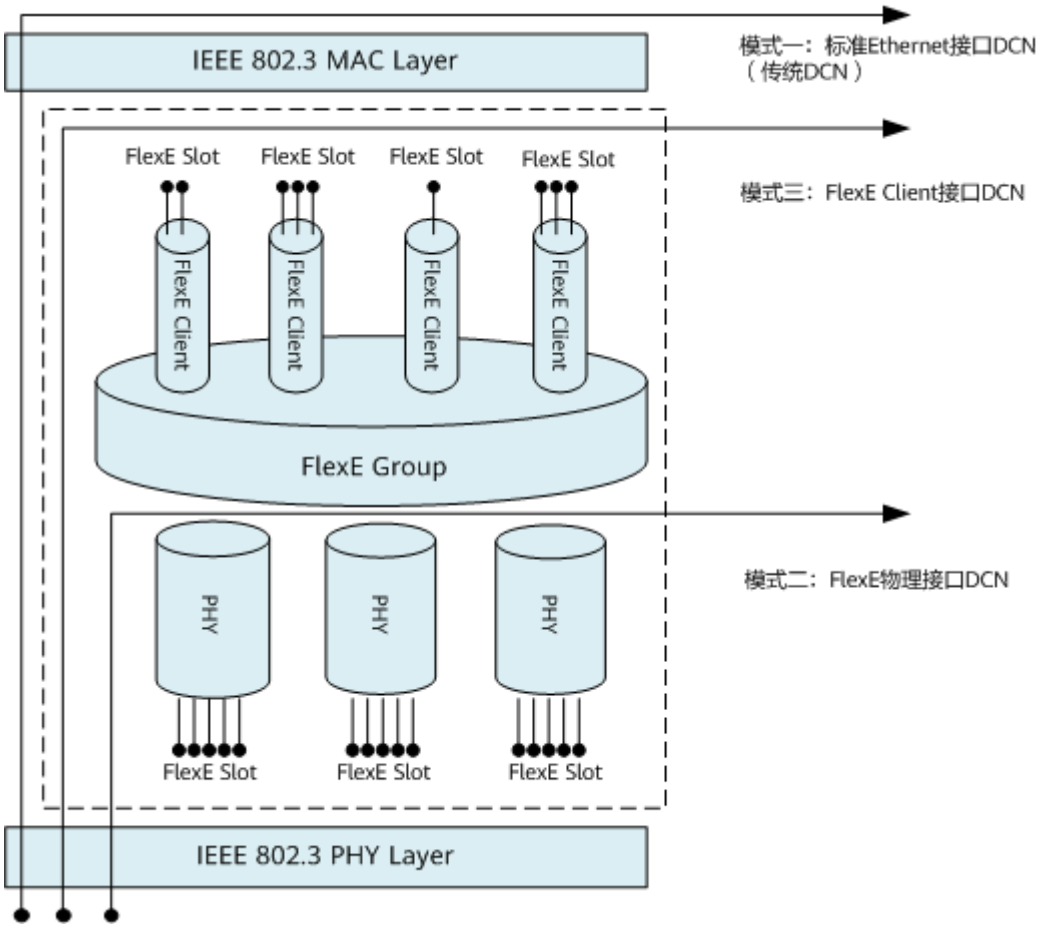
- 默认配置成原有标准Ethernet的整端口带宽，例如100GE接口，选择FlexE Client配置为100G。这种方式适合存量网络改造场景，在进行分片创建前，把标准Ethernet接口切换为同等带宽的FlexE Client，等改造完成后，再按照分片的带宽，调整FlexE Client带宽并创建新的分片接口。
- 配置为默认分片的带宽，其他带宽预留给后续新建的分片使用。例如100GE接口，选择FlexE Client配置为50GE，作为默认分片，另外50GE可以给已规划好的新建网络分片场景使用。

?.6. FlexE DCN 模式

如图1-19所示，标准Ethernet接口的DCN报文是从MAC层提取或下插（模式一）；而FlexE标准定义了OH（OverHead）和Client两种DCN模式，OH的DCN模式是指DCN报文走FlexE的开销时隙（模式二），Client的DCN模式是指DCN报文走FlexE Client（模式三），当前设备两种模式都支持，默认使能OH模式，如果两种模式都使能，即FlexE物理接口和FlexE Client都配置DCN，设备会优先Client模式下的DCN通道。

因此可以看出标准Ethernet接口和FlexE物理接口的DCN无法互通。

图 1-19 FlexE DCN 模式

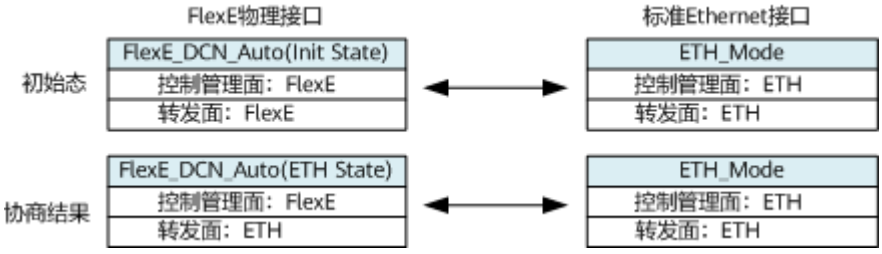


为了实现标准Ethernet接口和FlexE物理接口对接的场景下，设备能被网管管理，FlexE物理接口设计了4种模式，用来实现两者对接时DCN互通功能。

- FlexE_DCN_Auto(Init State)：单板上线默认模式，配置模式为FlexE模式且可基于FlexE物理接口配置业务，底层转发面可与对端FlexE物理接口DCN直通。
- FlexE_DCN_Auto(ETH State)：状态监测到PCS Link Up && Shim LOF后，转发面自协商成标准Ethernet模式以确保与对端DCN互通。
- FlexE_Lock_Mode：FlexE锁定状态，转发面不进行模式协商，规避自协商异常情况。
- ETH_Mode：标准Ethernet模式，不能自协商成FlexE模式。

如**图1-20**所示，标准Ethernet接口和FlexE物理接口对接时，FlexE物理接口初始态为FlexE_DCN_Auto(Init State)模式，开始自协商，标准Ethernet接口为ETH_Mode模式；协商完成后，FlexE物理接口的控制管理面保留FlexE模式，相关配置也保留，但转发面采用标准Ethernet模式转发，实现两者的DCN互通。

图 1-20 标准 Ethernet 接口和 FlexE 物理接口对接的模式



?.7. FlexE 时间同步模式

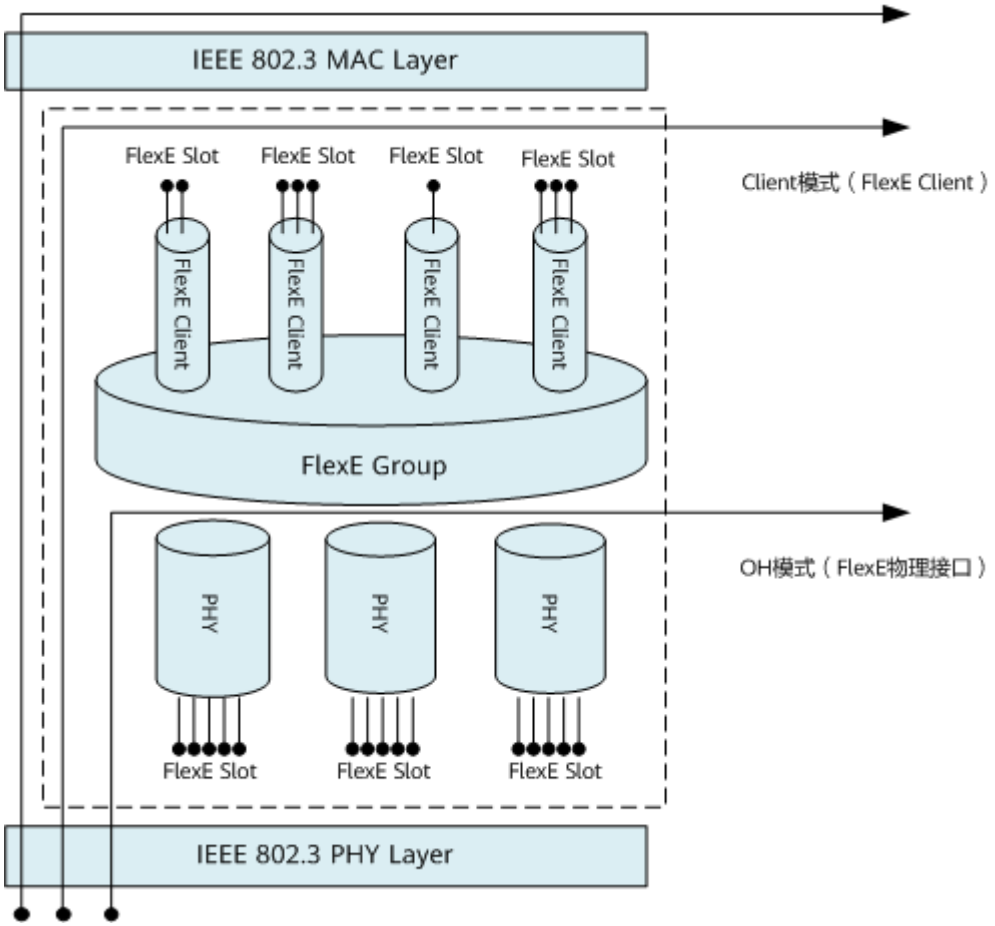
如图1-21所示，FlexE标准定义了两种1588v2报文承载模式：OH（OverHead）模式和Client模式，缺省情况下，1588v2报文通过OH模式承载。

- OH模式：指时钟报文走FlexE的开销时隙，时钟同步的相关配置和标准Ethernet接口下的配置相同。
- Client模式：指时钟报文走FlexE Client，需要在部署时钟业务的FlexE物理接口上绑定承载时钟业务的FlexE接口才能生效。

说明

FlexE链路两端的时间同步模式要一致，不能出现一端是OH模式，另一端是Client模式。

图 1-21 FlexE 时间同步模式

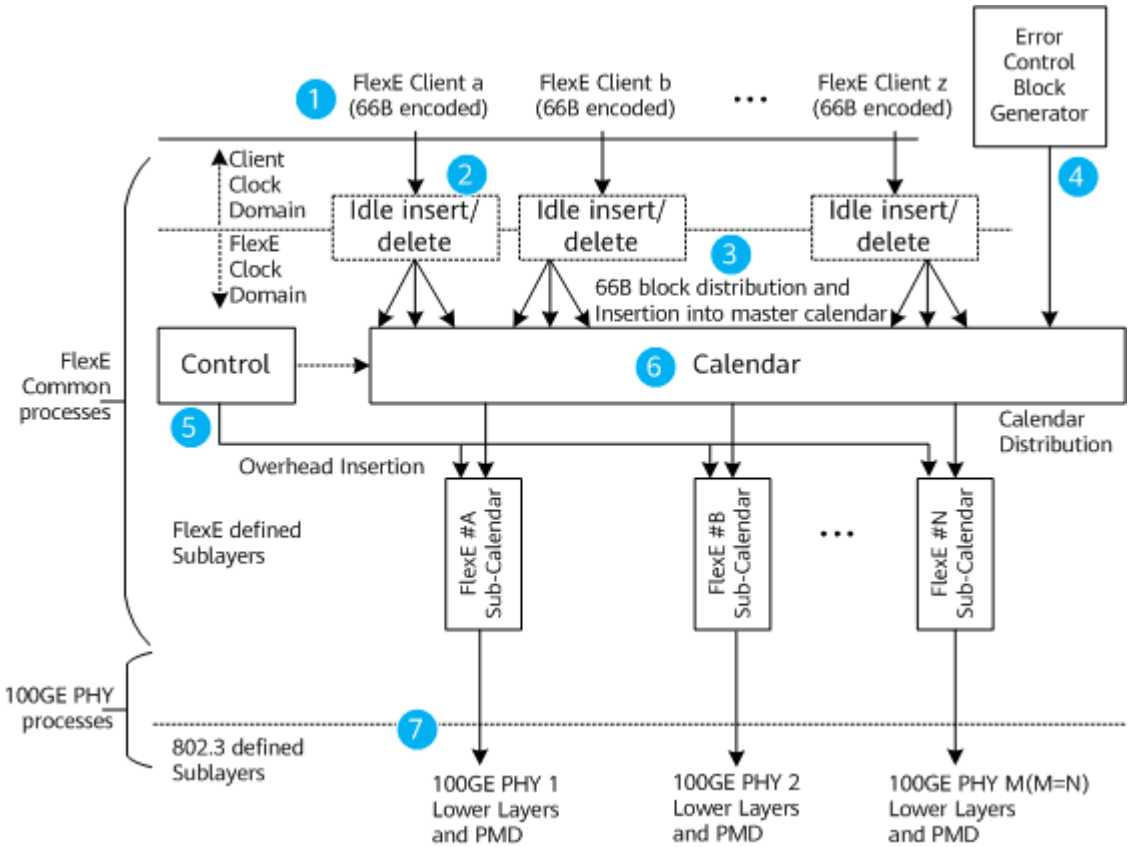


?.8. FlexE Mux

FlexE标准定义的FlexE Mux功能是指接口流量发送方向的FlexE Shim功能，即FlexE Client映射到FlexE Group的发送方向。如图1-22所示，以100GE PHY组成的FlexE Group为例，其工作过程如下：

1. 每个FlexE Client作为64B/66B编码比特流呈现给FlexE Shim。
2. 通过空闲插入/删除的方式实现FlexE Client的速率适配，以匹配FlexE Group的时钟，适配后的FlexE Client速率略小于FlexE Client的标称速率，以便为FlexE Group的PHY上的对齐标记和FlexE开销插入留出空间。
3. 将来自每个FlexE Client的66Bit块按照顺序依次分发和插入时隙分配器Calendar。
4. 生成错误控制块以插入未使用或不可用的时隙，确保这些时隙里的数据不会被认为是有效数据。
5. Control功能是管理每个FlexE Client插入在哪些时隙，并在发送方向为每个PHY插入FlexE开销。
6. Calendar分发负责将Calendar中不同FlexE Client的66Bit块按照TDM时隙分发机制分配到子时隙Sub-Calendar，然后Sub-Calendar把66Bit块轮询调度给FlexE Group中对应的PHY。
7. 每个PHY的66Bit块流通过插入对齐标记被分发到该PHY的PCS通道，PCS以下的层继续按照IEEE 802.3定义的标准Ethernet的规定完整地使用。

图 1-22 FlexE Mux 功能

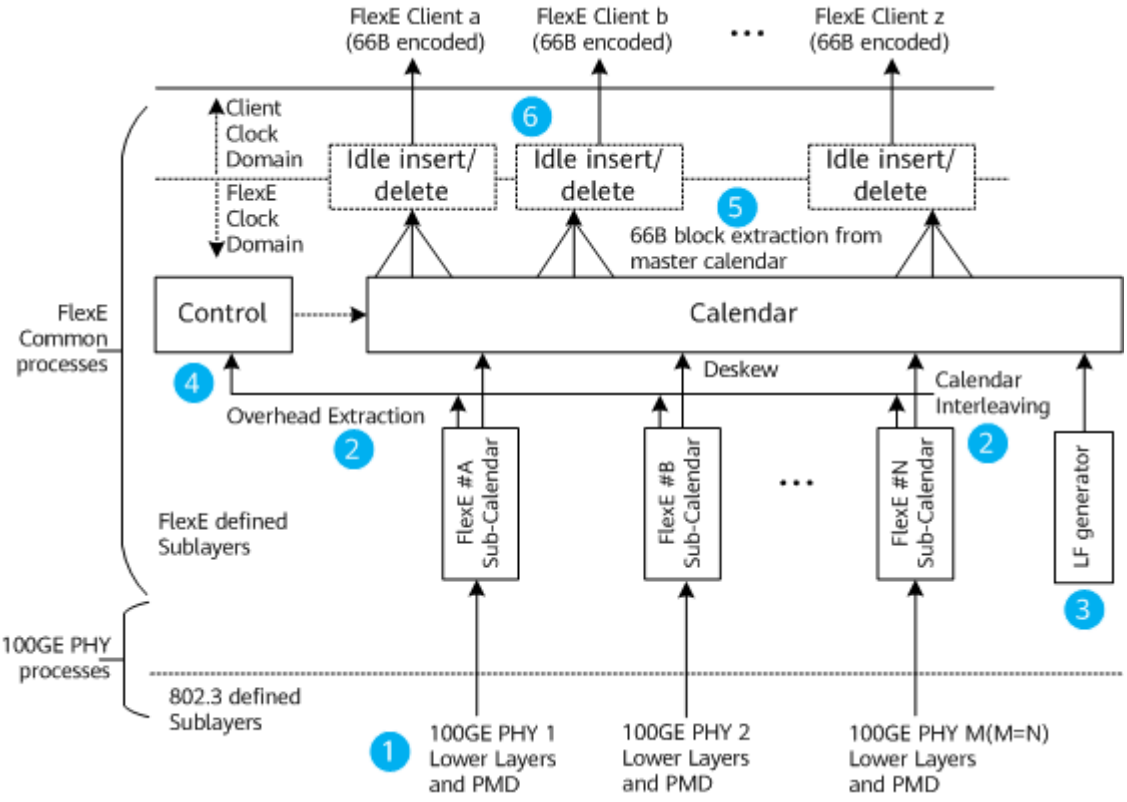


?.9. FlexE Demux

FlexE标准定义的FlexE Demux功能是指接口流量接收方向的FlexE Shim功能，即从FlexE Group中解映射出FlexE Client的接收方向。如图1-23所示，以100GE PHY组成的FlexE Group为例，其工作过程如下：

1. PHY的PCS以下层按照IEEE 802.3定义的标准Ethernet的规定使用，PCS通道完成去偏移，移除对齐标记等动作，将流量送往FlexE Shim。
2. 时隙分配器Calendar对每个FlexE实例的子时隙进行逻辑交织，重新排序并提取出FlexE开销。
3. 当FlexE Group的任一PHY失效，或任一FlexE实例的开销未实现开销帧锁定或开销复帧锁定时，该组内的所有FlexE Client都会产生本端故障LF（Local Fault）。
4. Control功能管理每个FlexE Client在接收方向从每个FlexE实例中提取出哪些时隙。
5. 提取出的时隙，按照66Bit块发送给每个FlexE Client。
6. 通过空闲插入/删除的方式在必要时调整FlexE Client的速率，以适配速率提取66Bit块流到FlexE Client。同样会因为FlexE Group的PHY上的对齐标记和FlexE开销要占用空间，所以适配后的FlexE Client速率略小于FlexE Client的标称速率。

图 1-23 FlexE Demux 功能



端口组

通常，设备的接口数比较多，并且很多接口具有相同的配置。如果对这些接口进行逐个配置，不但操作繁琐，而且容易输入错误。为解决此问题，可以创建一个端口组，然后将需要执行相同配置命令的接口加入到该端口组，在端口组视图下配置命令时，系统会自动到端口组绑定的所有成员接口下执行这些命令行，完成接口批量配置。

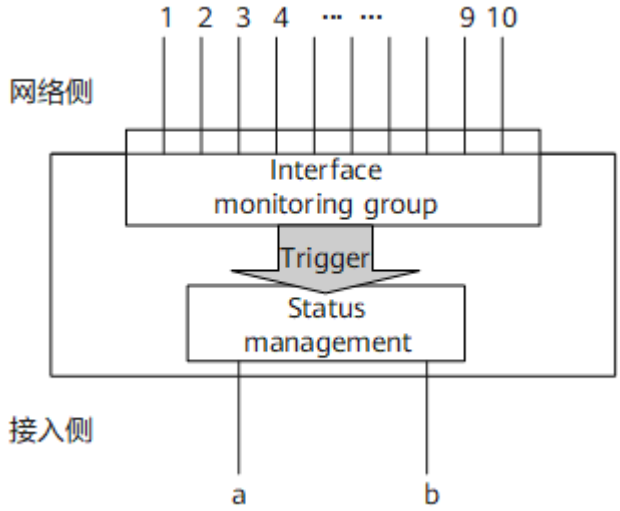
端口组可以分为永久端口组和临时端口组，它们实现的功能基本相同，即都可以将多个接口加入到端口组中，实现在这些接口下批量配置命令。其区别在于：

- 用户退出临时端口组后，该临时端口组被系统自动删除。而永久端口组不会被自动删除，需要通过命令删除。
- 永久端口组的信息可以通过命令查看，而临时端口组的信息无法查看。
- 永久端口组配置会生成配置文件，但是临时端口组配置后不会生成。

接口监控组

网络侧的接口可以加入到一个组中，该组称为接口监控组。每一个接口监控组通过唯一的名称来标识。其中，被监控的网络侧接口为Binding接口，与接口监控组联动的接入侧接口为Track接口，这些接口通过与接口监控组的状态联动，触发自己的状态变化。接口监控组监控该组中的所有Binding接口状态，当该组中超过一定比例的Binding接口状态变为Down时，就会触发对应Track接口的状态变为Down，从而将业务切换到备份链路上；当该组中状态为Down的Binding接口个数小于一定比例时，对应Track接口的状态恢复。

图 1-24 接口监控组原理示意图



如图1-24所示，网络侧有10个Binding接口，用户可以为每个Binding接口设置其权重值，例如所有Binding接口的Down权重均为10；接入侧有4个Track接口，用户可为每个Track接口设置Down的临界权重值，例如Track接口a和b自动触发Down的临界权重值分别为20、80。当监控组中接口状态为Down的Binding接口数量累计达到2个时，系统会自动触发接口a的状态变为Down，当接口状态为Down的Binding接口数量达到8个时，系统会自动触发接口b的状态变为Down；当接口状态为Down的Binding接口数量小于8个时，接口b的状态会自动恢复为Up，当接口状态为Down的Binding接口数量小于2个时，接口a的状态会自动恢复为Up。

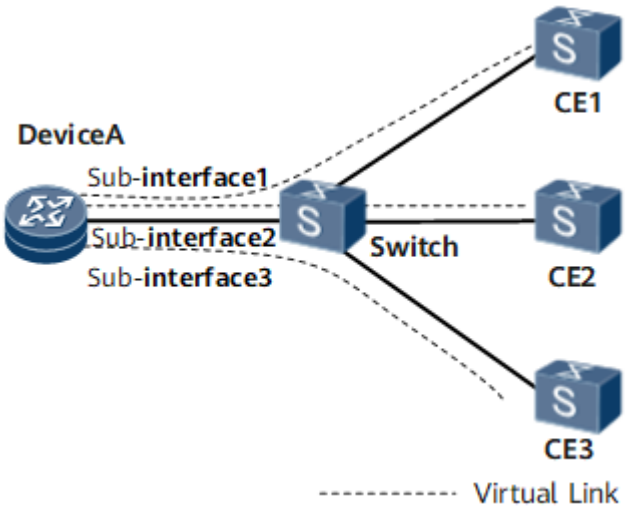
1.1.1.1.3 接口管理应用

子接口应用

如图1-25所示，在DeviceA的物理接口上配置多个子接口。每个子接口可以像物理接口一样配置一个IP地址，使该子接口的IP地址和对端网络的IP地址在同一网段，而各个子接口的IP地址不在同一网段。

这样在逻辑上建立了每个子接口和一个对端网络的连接，使对端网络通过和本地的一个子接口通信，从而和本地网络进行通信。

图 1-25 GE 子接口



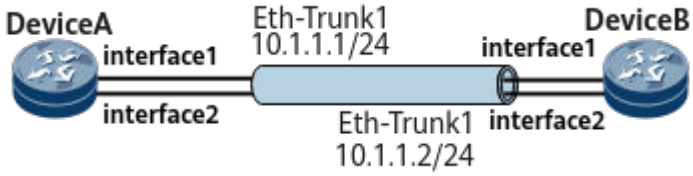
Eth-Trunk 应用

如图1-26所示，DeviceA与DeviceB之间创建Eth-Trunk，将两个全双工1000Mbit/s的接口捆绑成一个Eth-Trunk。DeviceA与DeviceB之间的Eth-Trunk链路最大带宽达到2000Mbit/s。

在Eth-Trunk内启用组内备份，当其中一条链路故障，流量切换到另一条链路，提高链路可靠性。

Eth-Trunk接口将DeviceA和DeviceB之间的流量分担到两条链路上，避免所有流量都走同一条链路而导致网络拥塞。

图 1-26 Eth-Trunk 组网图



FlexE 应用

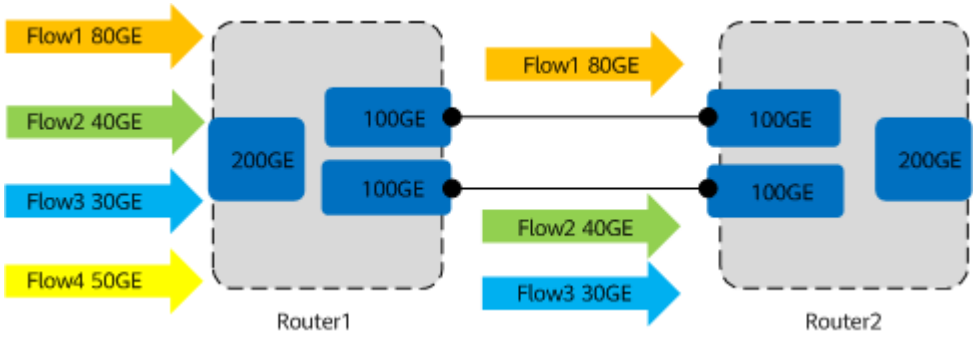
?.1. FlexE 捆绑功能实现超大带宽接口

由于IEEE 802.3标准制定的接口速率都是固定的，且有一定的周期性，无法满足基于灵活带宽组网的需求。可以基于FlexE捆绑技术，通过接口速率组合，构造更大带宽的链路。

传统 LAG 技术实现接口捆绑

如图1-27所示，传统的LAG捆绑技术，通过HASH算法将数据流分发到物理接口，存在负载不均衡，带宽利用率达不到100%。例如将两个100GE物理接口进行传统的LAG捆绑，假设有4组数据流，其中80GE数据流被HASH到上面链路，40GE和30GE数据流被HASH到下面链路，此时50GE数据流不管是被HASH到上面链路还是下面链路，都会出现带宽利用率达不到100%。

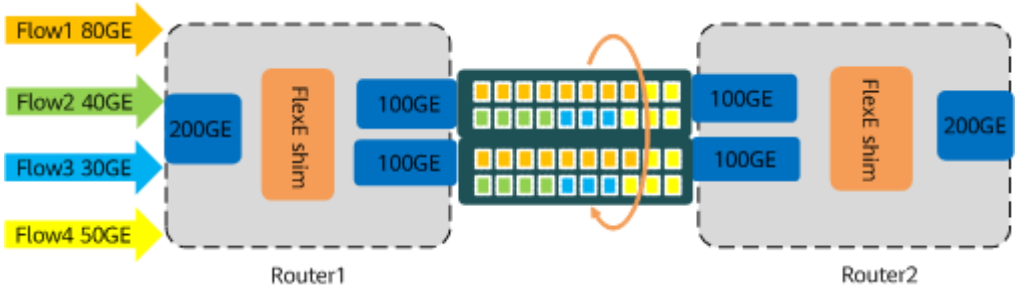
图 1-27 传统 LAG 技术实现接口捆绑



FlexE 技术实现接口捆绑

如图1-28所示，FlexE技术不仅可以捆绑多路物理接口，实现超大带宽接口，而且可以基于时隙调度，把数据流均匀的分发到所有的物理接口，实现带宽利用率100%，保证200GE转发能力。同时用户无需等待新接口标准，利用成熟接口速率，成本更优。

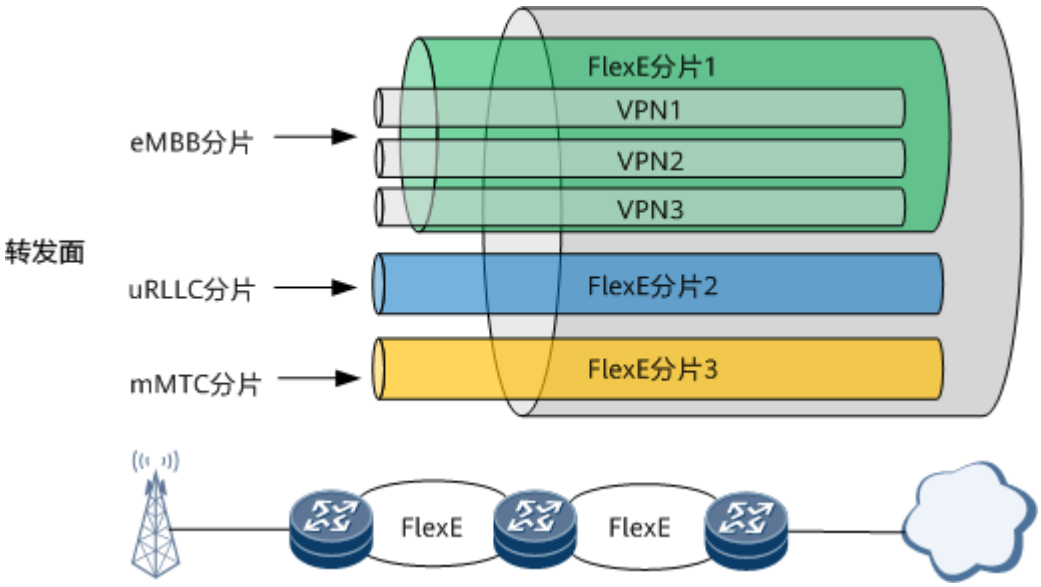
图 1-28 FlexE 技术实现接口捆绑



?.2. FlexE 通道化功能实现 5G 网络分片

5G网络分片包含管理面、控制面和转发面分片，FlexE是实现转发面分片的重要技术。相比标准Ethernet的所有业务共享接口，FlexE的通道化技术提供了接口级不同FlexE Client之间的物理层业务硬隔离，提供不同的业务SLA。如图1-29所示，5G网络中的eMBB、uRLLC和mMTC业务，可以分片实现在同一个IP网络中承载，一网多用。

图 1-29 FlexE 技术实现 5G 网络分片



?.3. FlexE 和光传输设备对接

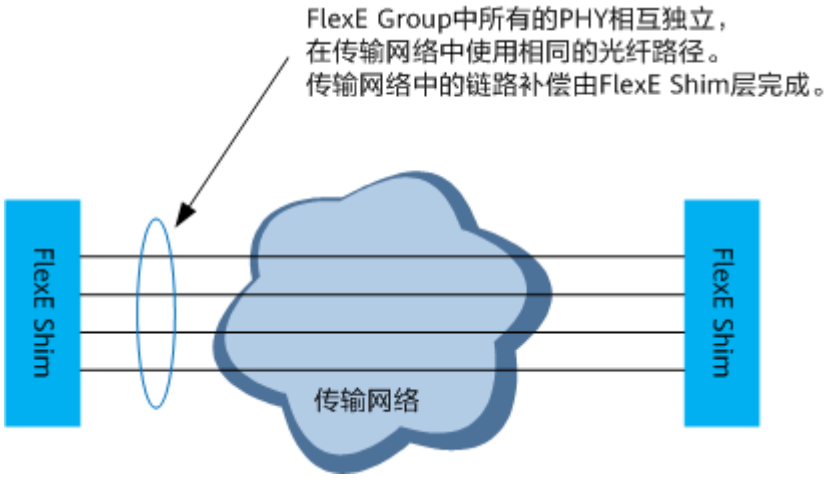
FlexE接口作为路由器与光传输设备之间的UNI接口，可以通过速率灵活匹配实现UNI接口实际承载的数据流带宽与光传输设备NNI接口链路承载的带宽一一对应，从而极大简化路由器的FlexE接口在光传输设备上的映射，降低设备复杂度以及投资成本和维护成本。

FlexE标准定义了三种和光传输设备对接的模式：Unaware、Termination和Aware模式，目前推荐使用Unaware模式。

Unaware 模式

光传输设备承载映射按照Bit透明传输机制实现，如图1-30所示，这种模式适用于以太网速率与彩光波长速率一致的情况，可以充分利旧现有光传输设备，在无需硬件升级的情况下实现对FlexE的承载，并可基于FlexE捆绑技术实现跨光传输网络的端到端超大带宽通道。

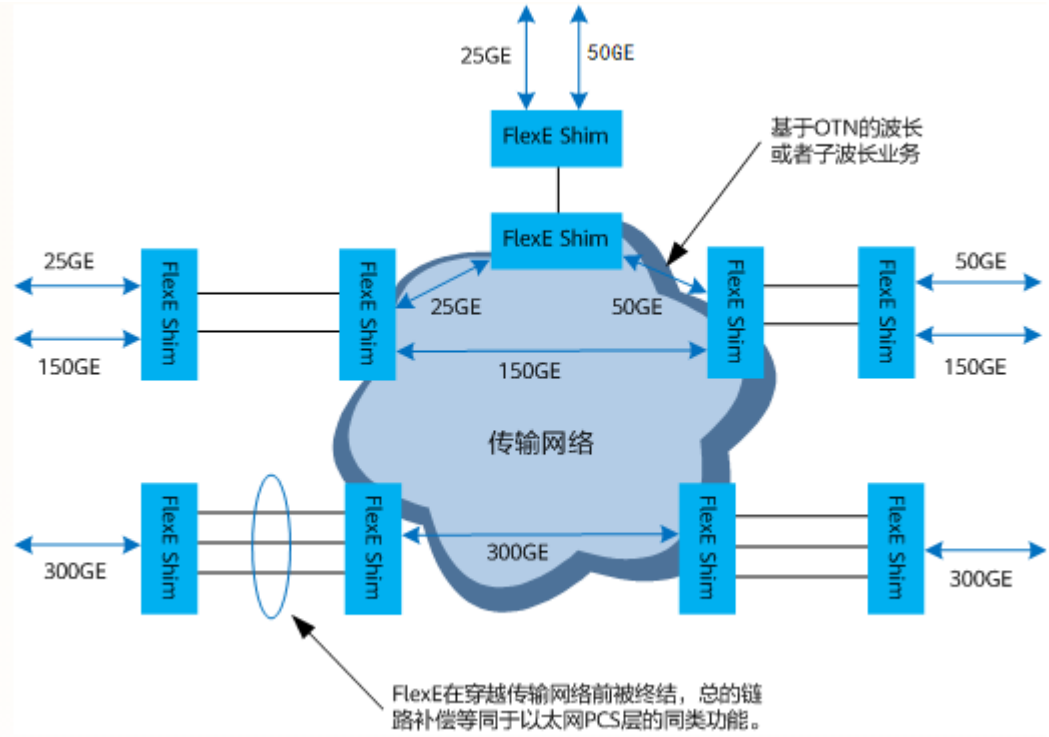
图 1-30 FlexE Unaware 模式在传输网络映射图



Termination 模式

FlexE在光传输设备的入口处终结，光传输网络感知FlexE UNI接口并恢复出FlexE Client数据流，再进一步映射到光传输网络中进行传输承载。如图1-31所示，这种模式与标准Ethernet接口在光传输网络上的承载一致，可以在光传输网络中实现对不同FlexE Client流量的疏导。

图 1-31 FlexE Termination 模式在传输网络映射图

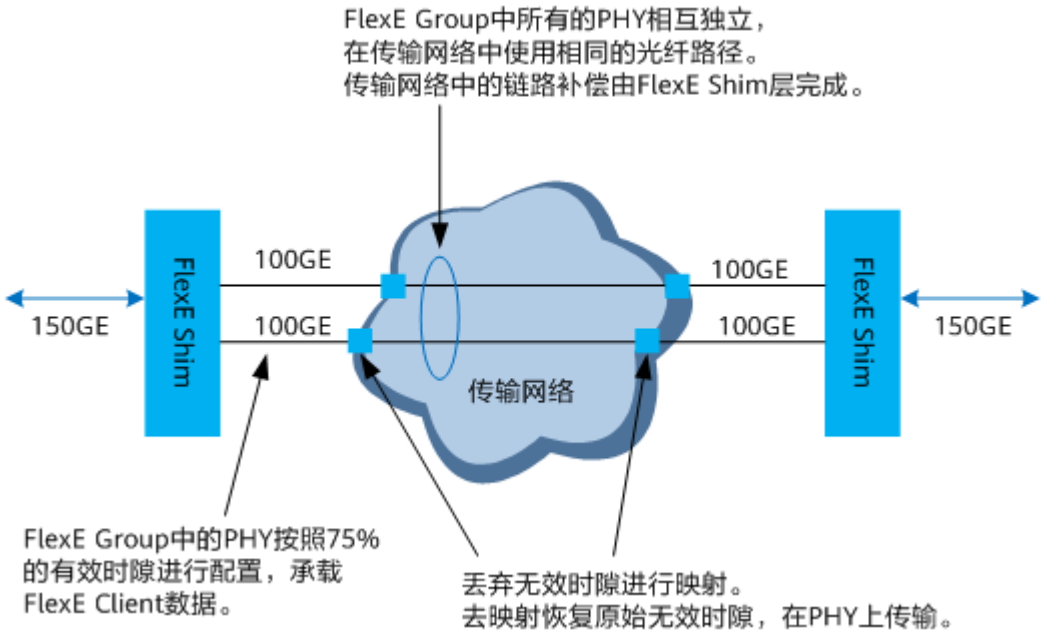


Aware 模式

Aware模式主要利用了FlexE子速率功能，适用于彩光单波长速率小于以太网接口速率的情况。如图1-32所示，路由器和光传输设备之间需要传输150G数据流，此时可以通过捆绑两个100GE PHY组成FlexE Group，然后将该Group的PHY按照75%的有效时隙进行配置，把剩余25%的时隙填充上特殊的Error Control Block数据块，标识为无效时隙。

当作为UNI侧的FlexE接口通过Aware模式在光传输网络中映射时，光传输网络直接丢弃无效时隙，并按照原始数据流带宽提取需要承载的数据，进而映射到速率匹配的光传输设备。光传输设备需要与作为UNI侧的FlexE接口配置保持一致，从而感知FlexE UNI接口并进行承载传输。

图 1-32 FlexE Aware 模式在传输网络映射图



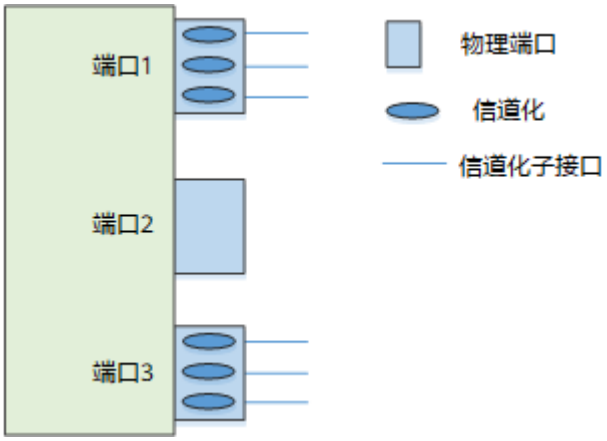
信道化子接口应用

5G网络中承载3大类型的业务：增强移动宽带(eMBB, enhanced Mobile Broadband)、海量机器类通信(mMTC, massive Machine Type Communications)、超高可靠低时延通信(uRLLC, ultra-Reliable and Low-latency Communications)，不同种类的业务希望能够进行分片承载。

为避免不同业务之间相互影响，需要有一种能够隔离不同类型业务的机制。最简单的方式就是基于物理带宽的隔离来区分不同业务。随着路由器大端口的持续演进，短期内没有任何一种类型的业务流量能够独占大端口带宽，因此可以在大速率端口上通过信道化技术来实现不同类型业务的隔离。

不同业务流量可以归属到不同的封装方式的信道化子接口上，每个信道化子接口可以实现独立的HQoS调度，从而实现不同类型业务之间的隔离。如图1-33所示，端口1和端口3表示信道化接口，端口2表示物理接口。

图 1-33 信道化接口示意图



信道化子接口主要应用场景为骨干汇聚网的下行流量隔离和PE网络侧的下行流量隔离。

目前信道化子接口支持以下类型：

- Vlantype Dot1q子接口。
- QinQ终结子接口。

Loopback 接口应用

提高可靠性

- 在IP地址借用中的应用

  当某接口不是长期使用IP地址时，为了节省IP地址，可以配置该接口借用其他接口的IP地址。通常配置为借用Loopback接口的地址，以保持接口的稳定性。

- 在Router ID中的应用

  一些动态路由协议要求路由器必须有Router ID，它是一台路由器在自治系统中的唯一标识。

  例如，OSPF和BGP在没有手工配置Router ID时，系统需要从本地接口的IP地址中选一个最大的IP地址作为Router ID。如果选择的是物理接口的IP地址，当这个物理接口状态变为Down时，系统也不会重新选择Router ID，除非这个被选择的IP地址被删除。

  因为Loopback接口稳定，通常情况下都处于Up状态，建议使用Loopback接口的IP地址作为路由器的Router ID。

- 在BGP中的应用

  为了使BGP会话不受物理接口故障的影响，可将Loopback接口配置成发送BGP报文的源接口。

  在使用Loopback接口作为BGP报文的源接口时，必须注意以下事项：

  – 确认BGP对等体的Loopback接口的地址是可达的。
  – 如果是EBGP连接，还要允许EBGP通过非直连建立邻居关系。

- 在MPLS LDP中的应用

  在MPLS LDP中，为了保持网络的稳定性，通常使用Loopback接口的IP地址作为传输地址。这个Loopback接口的IP地址可以是公网地址。

对信息分类

- 在SNMP中的应用

  为了保障服务器的安全，SNMP trap将Loopback接口的IP地址作为源IP地址，而不是出接口的IP地址。这样可以使用过滤来保护SNMP的管理系统。系统只允许来自Loopback接口IP地址的报文访问SNMP端口，从而使得读写trap信息变得简单。

- 在NTP中的应用

  网络时间协议NTP（Network Time Protocol）可以使所有设备的时间取得同步。NTP可以把Loopback接口的IP地址作为所有从本路由器发出的NTP报文的源地址。

  出于对NTP的安全考虑，NTP将Loopback接口的IP地址（而不是出接口的IP地址）作为源地址。系统只允许Loopback接口地址的报文访问NTP端口。这样可以使用过滤来保护NTP系统。

- 在记录信息方面的应用

  输出网络流量记录时，可以配置网络流量输出时的源IP地址是Loopback接口的IP地址。

  这是从服务器的安全角度考虑的。这样可以使用过滤来保护网络流量收集，因为只允许Loopback接口地址的报文访问指定的端口。

- 在安全方面的应用

  在用户日志服务器端，通过识别日志的源IP地址，可以迅速定位日志信息的来源。建议配置Loopback地址作为日志报文的源IP地址。

- 在HWTACACS中的应用

  配置HWTACACS，使从该路由器始发的报文使用的源地址是Loopback地址。这样可以使用过滤来保护HWTACACS服务器。

  因为这样只允许从Loopback接口的地址发送的报文访问HWTACACS服务器，从而使读写日志变得简单。HWTACACS日志记录中只有Loopback接口的地址，而没有出接口的地址。

- 在RADIUS用户验证中的应用

  配置RADIUS服务器时，使从该路由器始发的报文使用的源IP地址是Loopback接口的IP地址。

  和在HWTACACS中的应用类似，这样配置是从服务器的安全角度考虑的。它可以使用过滤来保护RADIUS服务器和代理。这样只允许Loopback接口地址的报文访问RADIUS服务器的端口，从而使读写日志变得简单。RADIUS日志记录中只有Loopback接口的地址，而没有出接口的地址。

NULL0 接口应用

NULL0接口从不转发任何报文，对于所有发到该接口的报文都直接丢弃，由于它的这个特征，NULL0接口主要被用在以下两方面：

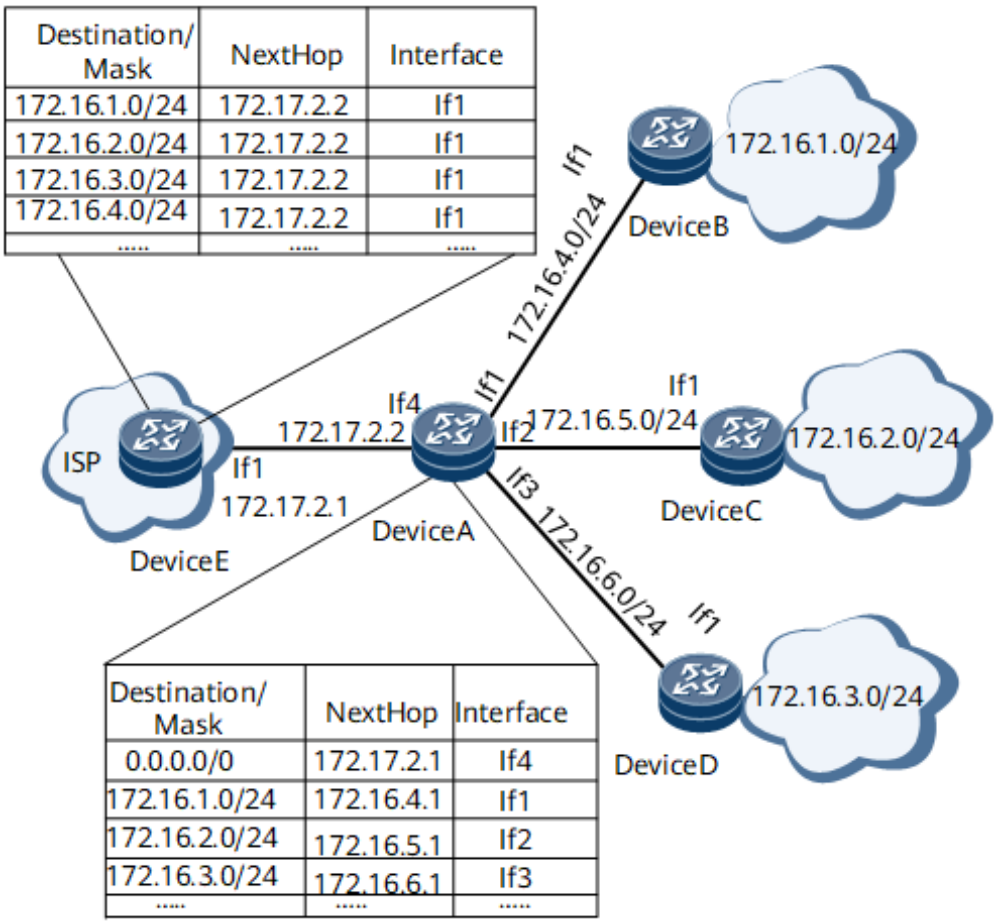
- 防止路由环路

  NULL0接口最典型的使用是用来防止路由环路。例如，在聚合一组路由时，总是创建一条到NULL0接口的路由。

  如**图1-34**所示，DeviceA为多个远端节点提供接入服务。

  DeviceA作为本地网络的网关，本地网络使用一个B类网段地址172.16.0.0/16。DeviceA通过DeviceB、DeviceC和DeviceD分别与三个子网相连。

图 1-34 NULL0 接口防止路由环路示例



正常情况下，DeviceA的路由表应包含三部分路由：

- 到172.16.2.0/24、172.16.3.0/24和172.16.4.0/24三个子网的路由。
- 到DeviceB、DeviceC及DeviceD的网段路由。
- 到ISP网络的缺省路由。

如果ISP侧网络路由器DeviceE接收到目的地址是172.16.10.0/24网段内的报文，则DeviceE会把该报文转发到DeviceA。

如果该报文的目的地址不是DeviceB、DeviceC和DeviceD所连网段的网络地址，DeviceA查找路由表后，会找到缺省路由，然后把该报文发给DeviceE。

因此这些目的地址不是DeviceB、DeviceC和DeviceD所连网段的网络地址，但是172.16.10.0/24网段的网络地址的报文，会在DeviceA和DeviceE之间如此反复被传输，形成路由环路。

在实际应用中，一般会在DeviceA上配置一条到NULL0接口的静态路由。这样，当DeviceA收到目的网段不是本地三个子网的报文后，DeviceA会根据精确匹配原则，找到出接口是NULL0接口的路由，然后把该报文丢弃。

由此可见，在DeviceA上配置一条出接口是NULL0接口的静态路由，可以防止路由环路。

- 用于过滤流量

  NULL0接口提供了过滤流量的一个可选的方法。可以通过将不想要的报文发送到NULL0接口，避免使用访问控制列表。

NULL0接口和访问控制列表都可以用于过滤流量，这两种用法各有裨益。下面对NULL0接口和访问控制列表进行简单比较。

- 如果使用访问控制列表，首先要配置ACL规则，然后将它应用到接口。当路由器收到报文时，要首先查找访问控制列表：
  - 如果是接受，还要查找转发表，再对报文进行转发或丢弃。
  - 如果是拒绝，就直接扔掉。
- NULL0接口的配置简单，只需将不想要的报文的出接口指定为NULL0接口。当路由器收到报文时，直接查找转发表，发现出接口是NULL0接口，则路由器不对报文做任何处理，直接丢弃。

所以对比起来，应用NULL0接口效率高，速度快。比如某路由器不希望收到某个指定目的地址的报文，用NULL0接口实现，只需配置路由。如果用访问控制列表实现，需要先配置一条ACL规则，然后再将这条规则在路由器的相应接口上应用。但是，NULL0接口不能细化流量，它面向的对象是整个路由器。访问控制列表是可以面向接口的。如果细致到需要控制面向接口的流量，NULL0接口就不能满足要求了。

TUNNEL 接口应用

Tunnel接口是一种虚拟的逻辑接口，当应用某些类型的隧道时，必须先创建Tunnel接口。

指定隧道目的地址就是指定对端实际接收报文的接口的IP地址，该地址必须与对端Tunnel接口指定的源地址相同，并且要保证到对端实际接收报文的接口的路由可达。不能对两个或两个以上使用同种封装协议的Tunnel接口配置完全相同的源地址和目的地址。

根据Tunnel接口的用途，可以为Tunnel接口配置不同的封装模式。下面介绍几种常见的Tunnel接口支持的隧道类型。

表 1-8 Tunnel 接口支持的隧道类型列表

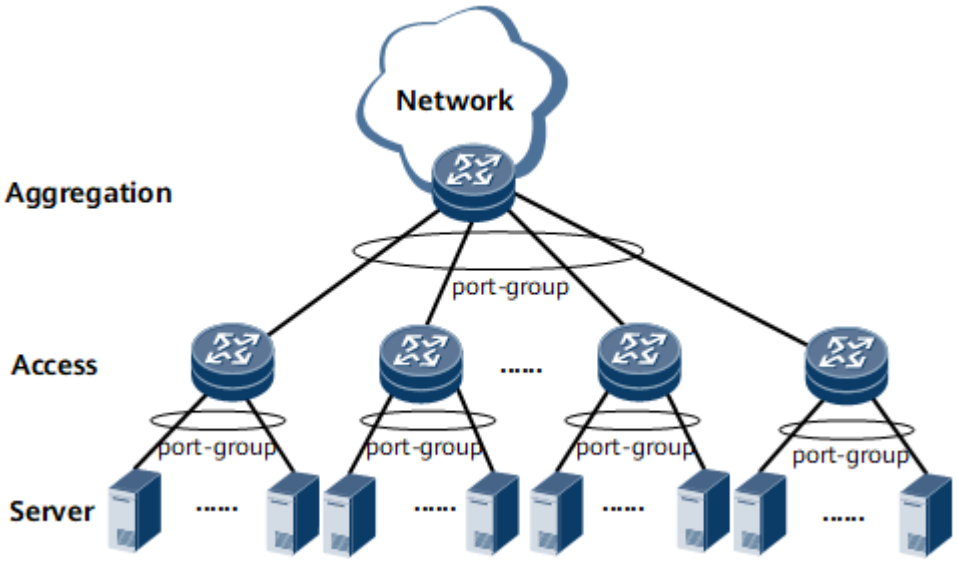
隧道类型	封装协议	应用场景
IPv6 over IPv4隧道	IPv4	IPv6 over IPv4手动隧道是在隧道两端的边界路由设备上通过人工配置而创建的，需要静态指定隧道的源IPv4地址和目的IPv4地址。手动隧道可用于IPv6网络之间的通信，也可在边界路由设备与主机之间配置。手动隧道为点到点模式。
6to4隧道	IPv4	6to4隧道是一种将多个IPv6网络通过IPv4网络互连的机制。6to4隧道与手动隧道的主要区别在于：6to4隧道可以是点到多点的连接，而手动隧道只是点到点的连接，所以6to4隧道并不是成对配置的。

隧道类型	封装协议	应用场景
MPLS TE隧道	MPLS TE隧道是通过一系列协议组件相互配合建立完成的，具体可参见MPLS TE基础-技术概览	通常采用以下两个概念来唯一标识一条MPLS TE隧道： ● 隧道接口：接口类型为Tunnel，接口编号则由“槽位号/卡号/端口号”这种形式来表示。 ● 隧道标识（Tunnel ID）：采用10进制数字来唯一标识一条MPLS TE隧道，以便对隧道进行规划和管理，这个数字称为Tunnel ID。用户在配置MPLS TE的Tunnel接口时需要指定一个ID。
GRE隧道	GRE	GRE提供了将一种协议的报文封装在另一种协议报文中的机制，使报文能够在异种网路中传输，而异种报文传输的通道称为Tunnel。
IPSec隧道	IPSec	将安全策略组应用到Tunnel接口，可以实现对不同的数据流进行不同的安全保护。一个Tunnel接口只能应用一个安全策略组。
IPv4 over IPv6隧道	IPv6	IPv4 over IPv6手动隧道是在隧道两端的边界路由设备上通过人工配置而创建的，需要静态指定隧道的源IPv6地址和目的IPv6地址。手动隧道可用于IPv4网络之间的通信，也可在边界路由设备与主机之间配置。手动隧道为点到点模式。
6RD隧道	IPv4	6RD隧道通过运营商IPv4网络连接IPv6站点，是点到多点的隧道。指定隧道封装类型为6RD模式之前需要创建Tunnel接口。

端口组应用

通常，交换设备的接口数比较多，并且很多接口具有相同的配置。如果对这些接口进行逐个配置，不但操作繁琐，而且容易输入错误。为解决此问题，可以创建一个端口组，然后将需要执行相同配置命令的接口加入到该端口组，在端口组视图下配置命令时，系统会自动到端口组绑定的所有成员接口下执行这些命令行，完成接口批量配置。如图1-35所示，汇聚层和接入层的大量交换设备接口数量多，这些接口很多配置相同，如果都单独配置可能会导致管理成本较高，所以可在这些设备上创建端口组。

图 1-35 端口组应用组网图

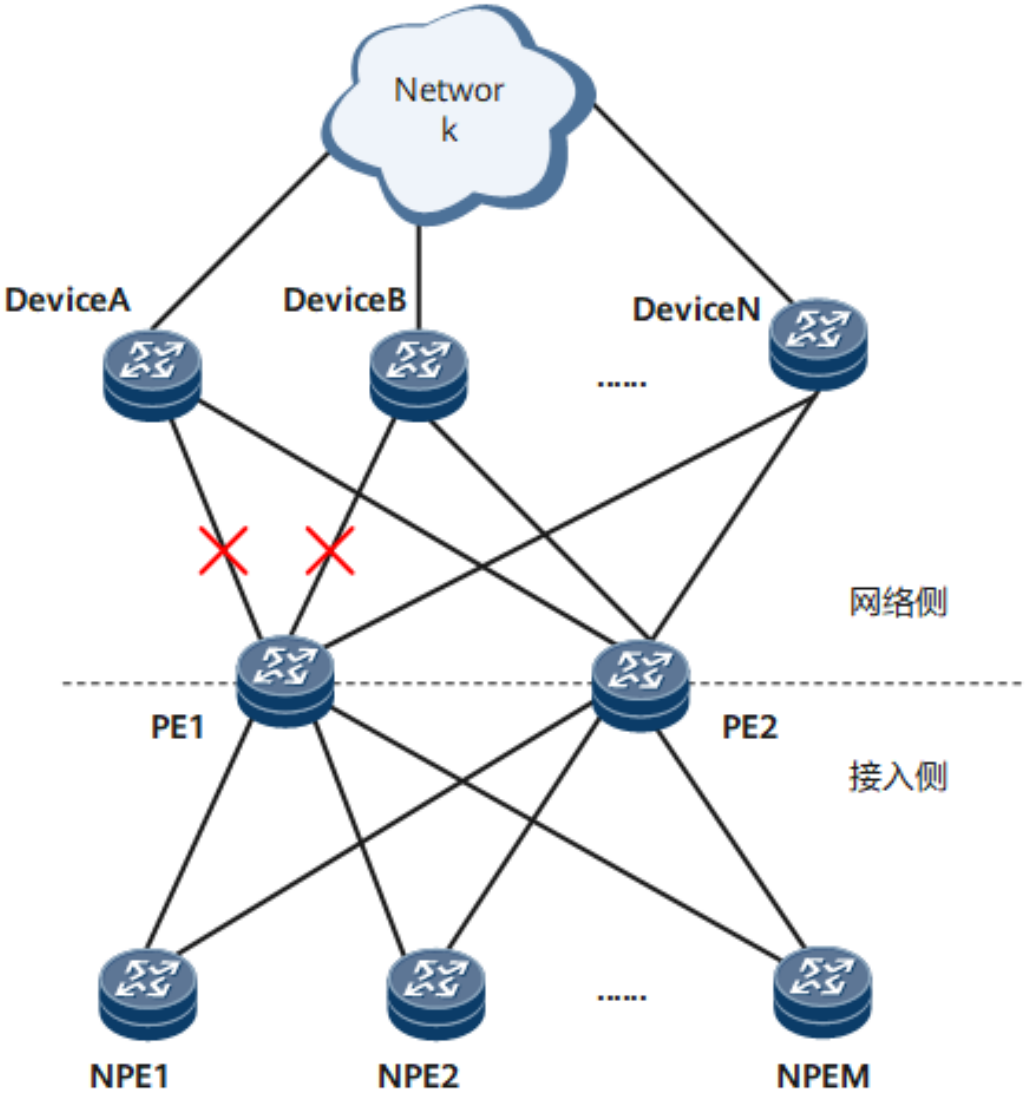


接口监控组应用

网络侧的接口可以加入到一个组中，该组称为接口监控组。每一个接口监控组通过唯一的名称来标识。其中，被监控的网络侧接口为Binding接口，与接口监控组联动的接入侧接口为Track接口，这些接口通过与接口监控组的状态联动，触发自己的状态变化。接口监控组监控该组中的所有Binding接口状态，当该组中超过一定比例的Binding接口状态变为Down时，就会触发对应Track接口的状态变为Down，从而将业务切换到备份链路上；当该组中状态为Down的Binding接口个数小于一定比例时，对应Track接口的状态恢复，链路回切。

如图1-36所示，PE2是PE1的备份设备，M个NPE设备双归属到2个PE设备实现链路负载分担，网络侧PE设备接入到N个路由器。当PE1和RouterA之间、PE1和RouterB之间的链路均故障时，网络侧仅剩余PE1和RouterN之间的链路，NPE设备感知不到该故障的产生，不会将接入侧链路切换到PE2，仍然通过PE1向RouterN发送报文。而由于网络侧可用链路数量减少，因此，可能会造成流量过载。

图 1-36 接口监控组应用组网图



这种情况下，在PE设备上部署接口监控组，将网络侧PE设备的多个接口加入接口监控组中。当网络侧发生链路故障时，通过接口监控组监控网络侧接口的状态，实现一定比例的网络侧接口状态变化时，PE设备接入侧相应接口的状态变化，使接入侧链路发生主备链路切换，从而避免流量过载，保障业务的通畅。

1.1.1.2 接口管理配置

用户通过对接口进行管理，便于更好地实现设备与设备间快速而准确地通信。

1.1.1.2.1 接口管理概述

通过本章节，您可以了解到NetEngine 8100 X, NetEngine 8000 X, NetEngine 8000E X支持的各种物理接口、逻辑接口、接口视图和提示符、常用的链路协议和接入技术等。

接口类型

接口是设备与网络中的其他设备交换数据并相互作用的部件，分为物理接口和逻辑接口两类。

- 物理接口

  物理接口是真实存在、有器件支持的接口。物理接口分为两种：

  - 局域网接口：路由器可以通过它与局域网中的网络设备交换数据。
  - 广域网接口：路由器可以通过它与远距离的外部网络设备交换数据。
- 逻辑接口

  逻辑接口是指能够实现数据交换功能但物理上不存在、需要通过配置建立的接口。

须知

主控板上的管理网口不支持配置转发业务。

接口视图和提示符

NetEngine 8100 X, NetEngine 8000 X, NetEngine 8000E X支持的物理接口的命令视图和提示符如表1-9所示，逻辑接口的命令视图和提示符如表1-10所示。

表 1-9 NetEngine 8100 X, NetEngine 8000 X, NetEngine 8000E X 支持的物理接口命令视图和提示符

接口名称	命令视图	进入命令	提示符
千兆以太网接口	GE接口视图	在系统视图下键入**interface gigabitethernet** 2/0/0	[~HUAWEI-GigabitEthernet2/0/0]

接口名称	命令视图	进入命令	提示符
10GE接口	10GE接口视图	在系统视图下键入**interface gigabitethernet** 1/0/0 **说明** 通过**display interface brief**命令查看到带有“10G”标识的GigabitEthernet接口为10G带宽的GigabitEthernet接口。	[~HUAWEI-GigabitEthernet1/0/0]
25GE接口	25GE接口视图	在系统视图下键入**interface 25GE** 2/0/0	[~HUAWEI-25GE2/0/0]

接口名称	命令视图	进入命令	提示符
40GE接口	40GE接口视图	在系统视图下键入**interface 40GE** 2/0/0	[~HUAWEI-40GE2/0/0]
100GE接口	100GE接口视图	在系统视图下键入**interface 100GE** 1/0/0	[~HUAWEI-100GE1/0/0]
200GE接口	200GE接口视图	在系统视图下键入**interface 200GE** 1/0/0	[~HUAWEI-200GE1/0/0]
400GE接口	400GE接口视图	在系统视图下键入**interface 400GE** 1/0/0	[~HUAWEI-400GE1/0/0]
1200GE接口	1200GE接口视图	在系统视图下键入**interface 1200GE** 1/0/0	[~HUAWEI-1200GE1/0/0]

接口名称	命令视图	进入命令	提示符
XGigabitEthernet接口	XGigabitEthernet接口视图	在系统视图下键入**interface XGigabitEthernet** 1/0/0	[~HUAWEI-XGigabitEthernet1/0/0]
50GE接口	50GE接口视图	在系统视图下键入**interface 50GE** 1/0/0	[~HUAWEI-50GE1/0/0]
50|100GE接口	50|100GE接口视图 **说明** 该类型接口默认速率是50G，可以切换到100G。	在系统视图下键入**interface 50|100GE** 1/0/0	[~HUAWEI-50|100GE1/0/0]
FlexE-50G接口	FlexE-50G接口视图	在系统视图下键入**interface FlexE-50G** 1/0/0	[~HUAWEI-FlexE-50G1/0/0]

接口名称	命令视图	进入命令	提示符
FlexE-100G接口	FlexE-100G接口视图	在系统视图下键入**interface FlexE-100G** 1/0/0	[~HUAWEI-FlexE-100G1/0/0]
FlexE-400G接口	FlexE-400G接口视图 **说明** 该接口仅在NetEngine 8000 X4和NetEngine 8000 X8设备上支持。	在系统视图下键入**interface FlexE-400G** 1/0/0	[~HUAWEI-FlexE-400G1/0/0]

表 1-10 逻辑接口命令视图和提示符

接口名称	命令视图	进入命令	提示符
子接口	子接口视图	在系统视图下键入**interface gigabitethernet 1/0/0.1**	[~HUAWEI-GigabitEthernet1/0/0.1]
Eth-Trunk接口	Eth-Trunk接口视图	在系统视图下键入**interface eth-trunk 2**	[~HUAWEI-Eth-Trunk2]
VE接口	VE接口视图	在系统视图下键入**interface virtual-ethernet 1/0/0**	[~HUAWEI-Virtual-Ethernet**1/0/0**]
Global-VE接口	Global-VE接口视图	在系统视图下键入**interface global-ve 0**	[~HUAWEI-Global-VE0]
VLANIF接口	VLANIF接口视图	在系统视图下键入**interface vlanif 2**	[~HUAWEI-Vlanif2]

接口名称	命令视图	进入命令	提示符
Loopback接口	Loopback接口视图	在系统视图下键入**interface loopback 2**	[~HUAWEI-LoopBack2]
NULL接口	NULL接口视图	在系统视图下键入**interface null 0**	[~HUAWEI-NULL0]
Tunnel接口	Tunnel接口视图	在系统视图下键入**interface tunnel 2**	[~HUAWEI-Tunnel 2]
NVE接口	NVE接口视图	在系统视图下键入**interface nve 1**	[~HUAWEI-Nve1]
FlexE接口	FlexE接口视图	在系统视图下键入**interface FlexE** 2/0/5	[~HUAWEI-FlexE2/0/5]
PW-VE接口	PW-VE接口视图	在系统视图下键入**interface pw-ve 1**	[~HUAWEI-pw-ve1]
ServiceIf接口	ServiceIf接口视图	在系统视图下键入**interface ServiceIf 1**	[~HUAWEI-ServiceIf1]

常用的链路层协议和接入技术

链路层负责无差错地将数据从一个站点发送到相邻的站点。它从网络层接收数据包，然后将它封装到称为“帧”的数据单元里，再传给物理层，进行传输。

下面介绍NetEngine 8100 X, NetEngine 8000 X, NetEngine 8000E X支持的几种主要的链路层协议。

- Ethernet

  现在的局域网主要是指以太网。以太网是一种广播类型的网络。它因为灵活、简单且易于扩展而被大规模应用

- Trunk

  Trunk技术有如下优点：

  - 增加带宽：接口的带宽是各成员接口带宽的总和。
  - 提高可靠性：当某个成员链路出现故障时，流量会自动的切换到其他可用的链路上，从而提供整个Trunk链路的可靠性。

- PPP

  点到点协议PPP（Point-to-Point Protocol）是在串行链路上封装IP数据报文，既支持数据位为8位且无奇偶校验的异步模式，也支持面向比特的同步链接。

PPP主要包括建立、配置及测试数据链路的链路控制协议（Link Control Protocol）和针对不同网络层协议的网络控制协议（Network Control Protocol）。

抑制接口震荡

网络应用中，由于物理信号干扰、链路层配置错误等原因可能导致设备接口频繁地交替出现Up和Down状态，造成路由协议、MPLS等反复震荡，对设备和网络产生较严重影响，甚至可能造成部分设备瘫痪，网络不可使用。控制接口震荡特性对接口频繁Up、Down事件进行控制，使其小于一定的频率，以减小对设备及网络稳定性的影响。

目前支持两种控制方式。

表 1-11 控制接口震荡功能

功能	功能描述	选择原则
control-flap	对网络层以下接口频繁Up/Down事件进行控制，以减小对设备及网络稳定性的影响。	● 可以指定接口进行配置； ● 从网络层开始抑制向路由管理模块通知接口震荡，是专门针对网络层稳定性的功能配置； ● 用户可以根据业务需求对参数进行精确配置； ● 需要充分理解该算法，才能配置，对用户要求高，命令行易用性差。
damp-interface	对物理层接口频繁Up/Down事件进行控制，以减小对设备及网络稳定性的影响。	● 该功能支持全局性配置也支持指定接口进行配置； ● 从物理层开始抑制，这样一旦接口物理震荡，整个链路层和网络层都能得到有效抑制； ● 从物理层接口震荡进行控制，可以防止上层业务频繁的使能、去使能，引发系统CPU、内存等过度消耗； ● 不需要了解复杂算法，对用户要求低，命令行易用性好。

1.1.1.2.2 接口管理特性限制

1.1.1.2.3 接口基础配置

通过了解常见接口类型、各种可配置的接口参数等概念，方便用户对接口进行管理。

应用环境

为了保证网络中各设备间更好地通信，需要物理接口和逻辑接口配合使用，并且根据不同的实际需求对各接口进行参数的配置，如配置描述信息、MTU（Maximum Transfer Unit）值、接口出入带宽利用率的告警阈值、流量统计时间间隔以及使能接口协议状态变化时向网管发送Trap、控制接口震荡等功能。

前置任务

在进行接口基础配置之前，需完成以下任务：

- 设备加电并正常启动。

进入接口视图

根据不同接口的物理特性，需要用不同的命令进入接口。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**interface** *interface-type interface-number*，进入接口视图。

其中，*interface-type*是接口类型，*interface-number*是接口号。

步骤3 （可选）执行命令**commit**，提交配置。

如果接口不是被创建，只是进入接口视图，则不用执行**commit**。

----结束

（可选）配置接口参数

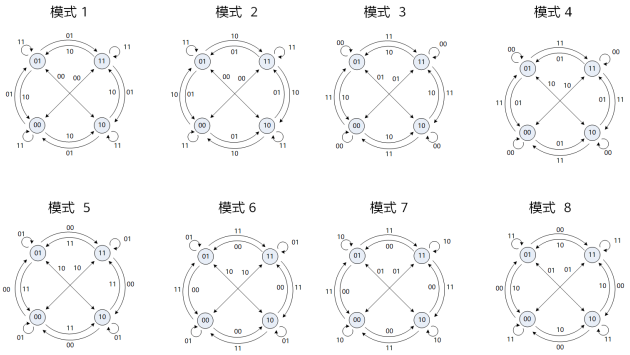
接口下可配置的参数需要根据实际的需求进行配置，包括是否需要配置描述信息、修改MTU值等。

背景信息

接口参数如表1-12所示，请依据实际需要进行相应的选择。

表 1-12 接口参数

参数类型	说明
接口描述信息	当需要维护的接口较多时，需要对接口进行描述，以便能够准确快速地识别接口。
接口MTU值	通过配置接口MTU值，设备会根据接口MTU的大小，对该接口发送的报文进行分片。 **说明** Loopback接口和NULL接口不支持配置MTU。

参数类型	说明
设置网管在MIB上获取的接口带宽	可以通过设置网管在MIB上获取的接口带宽大小来计算接口的带宽利用率。
接口协议状态变化时是否向网管发送Trap	使能接口协议状态变化时主动向网管端发送Trap功能，可以方便网管实时监控接口状态。 但是当接口处于震荡状态时将频繁向网管发送Trap信息，会显著增加网管设备的处理负担。此时可以关闭接口协议状态变化发送Trap的功能。
流量统计时间间隔	设置统计接口流量的时间间隔，可以方便用户统计接口流量和速率。
是否控制接口震荡	控制接口震荡特性对接口频繁Up、Down事件进行控制，使其小于一定的频率，以减小对设备及网络稳定性的影响。 **说明** Loopback接口和NULL接口等不支持使能控制接口震荡功能。
是否调整接口的差分四相相移键控(DQPSK)的模式	100G光接口使用的编码类型为DQPSK，当100G光接口对接时，需要DQPSK的差分编码、解码模式相同才能对接成功。当和其他设备100G光口第一次对接时，如果光口不通，可以调整接口的DQPSK模式。一共有8种差分编码模式，如图1所示。 **图 1-37** 差分编码模式 

参数类型	说明
配置接口MSS值	网络中，NetEngine 8100 X, NetEngine 8000 X, NetEngine 8000E X是用户端和运营商端之间的中间设备。两端在TCP握手过程中，会对后续TCP传输的MSS值进行协商。握手成功后，两端建立了TCP连接，NetEngine 8100 X, NetEngine 8000 X, NetEngine 8000E X即会在两端之间进行TCP报文的转发。由于NetEngine 8100 X, NetEngine 8000 X, NetEngine 8000E X在转发TCP报文时，可能会封装隧道报文头，这样就使得TCP报文长度可能超过两端TCP握手过程中协商出的MSS值，从而造成报文分片，降低传输效率。NetEngine 8100 X, NetEngine 8000 X, NetEngine 8000E X上配置**tcp adjust-mss inbound**命令以后，在两端TCP握手过程中协商MSS值时，会将SYN/SYN+ACK报文中的MSS值与NetEngine 8100 X, NetEngine 8000 X, NetEngine 8000E X上**tcp adjust-mss inbound**命令配置的MSS值进行比较。如果报文中的MSS值大于NetEngine 8100 X, NetEngine 8000 X, NetEngine 8000E X配置的MSS值，则将报文中的MSS值修改为NetEngine 8100 X, NetEngine 8000 X, NetEngine 8000E X配置的MSS值；否则，不做修改。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**interface** *interface-type interface-number*，进入相应的接口视图。

其中，*interface-type*是接口类型，*interface-number*是接口号。

步骤3 配置接口参数，根据需要，可执行如**表1-13**中的一个或多个操作。

表 1-13 配置接口参数

接口参数	操作
配置接口描述信息	执行命令**description** *regular-expression*，配置接口的描述信息。
配置接口MTU值	执行命令**mtu** *mtu*或者执行命令**ipv6 mtu** *mtu*，配置接口的MTU。 执行命令**mtu** *mtu* **spread**或者执行命令**ipv6 mtu** *mtu* **spread**，配置主接口的MTU并且扩散至子接口。 **说明** • 使用**mtu**或者**mtu spread**命令改变接口的最大传输单元MTU后，需要在接口视图下执行命令**shutdown**和**undo shutdown**或只执行命令**restart**，重启接口以保证配置的MTU生效。 • 如果接口上配置的是IPv4属性，请选择**mtu**命令或者**mtu spread**，配置接口上发送IPv4报文时的MTU值。 • 如果接口上配置的是IPv6属性，请选择**ipv6 mtu**或者**ipv6 mtu spread**命令，配置接口上发送IPv6报文时的MTU值。

接口参数	操作
设置接口的配置带宽	执行命令**bandwidth**，设置接口的配置带宽。 **说明** 网管可以通过IF-MIB中的ifSpeed和ifHighSpeed两个节点查看此配置。 默认情况下，业务通常只使用物理带宽作为带宽参数进行协议选路计算，可以通过**bandwidth-config effect service enable**命令将配置带宽作为带宽参数参与协议选路计算。
配置接口协议状态变化时是否向网管发送Trap	执行命令**enable snmp trap updown**，使能接口协议状态变化时向网管发送Trap的功能。 **说明** 默认情况下接口协议状态变化自动向网管设备发送Trap功能是使能的，当接口处于振荡状态时将频繁向网管发送Trap信息，会显著增加网管设备的处理负担。此时可使用**undo enable snmp trap updown**，关闭接口协议状态变化发送Trap的功能。
配置流量统计时间间隔	执行命令**set flow-stat interval** *interval*，配置接口流量统计时间间隔。 **说明** • 若需要配置全局流量统计时间间隔，则直接在系统视图下进行配置，不用执行命令**interface** *interface-type interface-number*。配置全局流量统计时间间隔对所有没有设置接口流量统计时间间隔的接口都有效，方便用户一次配置多个接口。 • 新的时间间隔将在原时间间隔超时后生效。针对逻辑接口，流量显示将在新的时间间隔生效后第二个周期更新。针对物理接口，流量显示立即更新。
配置是否控制接口震荡	执行命令**control-flap** [*suppress reuse ceiling decay-ok decay-ng*]，使能接口的控制接口震荡功能。 *suppress*是接口抑制门限的1000倍，取值范围是1～20000，缺省值是2000，其值必须大于*reuse*值且小于*ceiling*的值。 *reuse*是接口重用门限的1000倍，取值范围是1～20000，缺省值是750，其值必须小于*suppress*的值。 *ceiling*是接口抑制惩罚值的最大值的1000倍，取值范围是1001～20000，缺省值是6000，其值必须大于*suppress*的值。 *decay-ok*是接口UP时，惩罚值半衰期。取值范围是1～900秒，缺省值是54秒。 *decay-ng*是接口Down时，惩罚值半衰期。取值范围是1～900秒，缺省值是54秒。
配置接口MSS值	执行命令**tcp adjust-mss** *mss-value* **inbound**，配置TCP连接中能够给对方发送的最大报文长度MSS值。

步骤4 执行命令**commit**，提交配置。

----结束

打开接口

通常情况下，在设备上电时，初始化并启动各物理接口。

背景信息

说明

该配置过程仅在Admin-VS支持。

操作步骤

- 缺省情况下，接口是打开的。
- 若接口已被关闭，请执行如下操作重新打开接口。
  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**interface** *interface-type interface-number*，进入接口视图。
  c. 执行命令**undo shutdown**，启动接口。
  d. 执行命令**commit**，提交配置。

----结束

（可选）配置接口物理状态变化时向网管发送 Trap

使能接口物理状态变化时主动向网管端发送Trap功能，可以方便网管实时监控接口状态。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**interface** *interface-type interface-number*，进入相应的接口视图。

步骤3 执行命令**enable snmp trap physical-updown**，使能接口物理状态变化时向网管发送Trap的功能。

步骤4 执行命令**commit**，提交配置。

----结束

（可选）配置主接口 IPv4 和 IPv6 分类流量统计

配置主接口的IPv4和IPv6分类流量统计，对所有物理主接口都有效。

背景信息

在需要配置接口IPv4和IPv6分类流量统计的路由器上进行以下配置。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**interface** *interface-type interface-number*，进入指定接口的接口视图。

步骤3 执行命令**statistic enable**，使能指定主接口的IPv4和IPv6分类流量统计功能。

步骤4 执行命令**statistic mode forward**，配置指定接口IPv4和IPv6分类流量统计。

步骤5 （可选）执行命令**statistic accelerate enable**，使能接口的统计加速功能。当主接口使能双栈统计功能时，若想提升主接口转发性能，可以配置此命令。

步骤6 执行命令**commit**，提交配置。

----结束

（可选）配置光放模块的功率锁定和增益锁定功能

配置光放模块的功率锁定和增益锁定，实现光功率的放大。

背景信息

在需要配置光放大模块的功率锁定和增益锁定的路由器上进行以下配置。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 请根据实际情况选择以下配置。

- 执行命令**interface** *interface-type interface-number*，进入指定接口的接口视图。

步骤3 执行命令**work-mode** { **agc** *agc-value* | **apc** *apc-value* }，配置光放模块的增益锁定和功率锁定。

步骤4 执行命令**commit**，提交配置。

----结束

配置光模块的工作模式

通过端口上光模块的工作模式配置实现端口的带宽模式的切换。

背景信息

通过端口光模块的工作模式配置实现端口的带宽模式的切换，增加组网灵活性，减少购置成本。对于不支持工作模式切换的光模块，如果配置该功能，设备会报错，不能成功下发。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**optical-module interface** { *interface-name* | *interface-type interface-number* } **client-mode** { **zr-dwdm** | **zr-single** | **zr-plus** }，配置设备端口上的光模块的工作模式。

步骤3 执行命令**commit**，提交配置。

----结束

（可选）配置端口散列模式

通过端口散列模式配置实现端口的带宽模式的切换。

背景信息

通过端口散列模式配置实现端口的带宽模式的切换，增加组网灵活性，减少购置成本。

说明

VS模式下，该配置过程仅在Admin VS支持。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**port split dimension interface** { { *interface-name1* | *interface-type interface-number1* } [**to** { *interface-name2* | *interface-type interface-number2* }] } &<1–32> **split-type** *split-type*，将端口进行散列命令配置。

步骤3 执行命令**commit**，提交配置。

----结束

检查配置结果

管理接口的相关配置完成后，您可以查看到接口的状态信息、统计信息、控制接口震荡等内容。

操作步骤

- 执行命令**display interface** [*interface-type interface-number*] 可以查看接口的状态信息和统计信息。
- 执行命令**display control-flap interface** *interface-type interface-number*，可以查看接口配置的控制接口震荡特性。
- 执行命令**display counters** [**bit**] [**inbound** | **outbound**] [**interface** *interface-type* [*interface-number*]] [**slot** *slot-id*]，查看接口的流量统计信息。
- 执行命令**display counters** [**bit**] **rate** [**inbound** | **outbound**] [**interface** *interface-type* [*interface-number* | **slot** *slot-id*] | **slot** *slot-id*]，查看接口的流量速率。
- 执行命令**display port split**或**display port split slot**，查看端口的散列能力和散列状态。
- 执行命令**display interface neighbor** [*interface-type interface-number* | **slot** *slot-id* [**card** *card-number*]]，查看设备上物理接口的邻居设备和邻居接口信息。
- 执行命令**display interface description** [*interface-type* [*interface-number*] | **slot** *slot-id* [**card** *card-number*]][**full-name**]，查看接口的描述信息。

----结束

1.1.1.2.4 物理链路检测配置

配置物理链路检测功能，可以避免由于链路上产生大量的错误告警时，使系统处理各种告警而降低性能的情况发生。

应用环境

避免当链路上产生大量的错误告警时，使系统处理各种告警而降低性能。通过设置告警阈值，在超过阈值后将产生告警信息，采取必要的故障处理措施，保证正常业务流量传输。

前置任务

在配置物理链路检测之前，需完成以下任务：

- 路由器上电，自检正常。
- 完成路由器接口物理属性的配置。

配置接口 CRC 错误、SDH 错误、接收错误、发送错误、光模块光功率异常告警功能

本节介绍接口CRC错误、SDH错误、接收错误、发送错误、光模块光功率异常告警功能的配置。

背景信息

使能接口CRC错误、SDH错误、接收错误、发送错误、光模块光功率异常告警功能，当超出设置的阈值，或从阈值以上降到阈值以下时，系统将产生告警信息。通过配置系统处理接口告警的类型，以及告警上送网管的门限值和间隔时间，从而避免由于链路上产生大量的错误告警时，使系统处理各种告警而降低性能的情况发生。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**snmp-agent trap enable port** { **crcexc-error** | **input-error** | **output-error** | **sdh-error-rising** | **optical-module-abnormal** }，使能接口告警功能。

此配置对所有支持此告警的物理端口生效。

请根据实际情况设置接口的告警类型。

- 如果使能接口CRC错误阈值告警，设置阈值告警类型为**crcexc-error**。
- 如果使能接口SDH错误阈值告警，设置阈值告警类型为**sdh-error-rising**。
- 如果使能接口光模块功率异常告警功能，设置告警类型为**optical-module-abnormal**。

VS模式下，该命令仅在Admin VS支持。

步骤3 执行命令**interface** *interface-type interface-number*，进入接口视图。

步骤4 可以根据需要，配置不同类型的接口告警阈值与检测时间间隔。

- 配置出、入带宽利用率的告警阈值：
  - 执行命令**trap-threshold** { **input-rate** | **output-rate** } *bandwidth-in-use* [**resume-rate** *resume-threshold*]，设置接口出、入带宽利用率的告警阈值。

    为了避免告警震荡，*bandwidth-in-use*和*resume-threshold*的取值尽量保持差距。
  - 执行命令**set flow-stat interval** *interval*，配置接口流量统计时间间隔。

新的时间间隔将在原时间间隔超时后生效。针对逻辑接口，流量显示将在新的时间间隔生效后第二个周期更新。针对物理接口，流量显示立即更新。

配置接口流量统计时间间隔只对本接口有效，方便查看某一接口的流量和速率。

说明

可以配置全局流量统计时间间隔对所有没有设置接口流量统计时间间隔的接口都有效，方便用户一次配置多个接口。在系统视图下执行命令**set flow-stat interval** *interval*，接口流量统计时间间隔单位为秒。在接口下的统计时间间隔设置优先级会高于全局下的统计时间间隔设置。

- 配置CRC告警（以太接口支持，以下两种方式任选其一）：
  - 执行命令**trap-threshold crc-error** *threshold* **interval-second** *interval* ，配置在指定时间内CRC错误告警的门限值。
  - 执行命令**trap-threshold crc-error high-threshold** *high-threshold* **low-threshold** *low-threshold* **interval-second** *interval* [**shutdown**]，配置CRC错误告警的高门限值和低门限值以及检测时间间隔。

    说明

    可以在系统视图下执行命令**trap-threshold slot** *slot-id* **card** *card-id* **crc-error high-threshold** *high-threshold* **low-threshold** *low-threshold* **interval-second** *interval*，配置完成后将对该子卡上的所有端口生效。
- 配置SDH告警（10GE WAN接口支持，以下两种方式任选其一）：
  - 执行命令**trap-threshold sdh-error** *threshold* **interval-second** *interval*，配置在指定时间内sdh错误告警的门限值。
  - 执行命令**trap-threshold sdh-error high-threshold** *high-threshold* **low-threshold** *low-threshold* **interval-second** *interval*，配置sdh错误告警的高门限值和低门限值以及检测时间间隔。

    说明

    可以在系统视图下执行命令**trap-threshold slot** *slot-id* **card** *card-id* **sdh-error high-threshold** *high-threshold* **low-threshold** *low-threshold* **interval-second** *interval*，配置完成后将对该子卡上的所有端口生效。
- 配置symbol告警（仅以太接口支持）：
  - 执行命令**trap-threshold symbol-error high-threshold** *high-threshold* **low-threshold** *low-threshold* **interval-second** *interval*，配置symbol错误告警的高门限值和低门限值以及检测时间间隔。

    说明

    可以在系统视图下执行命令**trap-threshold slot** *slot-id* **card** *card-id* **symbol-error high-threshold** *high-threshold* **low-threshold** *low-threshold* **interval-second** *interval*，配置完成后将对该子卡上的所有端口生效。
- 配置接收发送告警（所有以太支持）：
  - 执行命令**trap-threshold** { **input-error** | **output-error** } **high-threshold** *high-threshold* **low-threshold** *low-threshold* **interval-second** *interval*，设置接口input错误告警和output错误告警。

    说明

    可以在系统视图下执行命令**trap-threshold slot** *slot-id* **card** *card-id* { **input-error** | **output-error** } **high-threshold** *high-threshold* **low-threshold** *low-threshold* **interval-second** *interval*，配置完成后将对该子卡上的所有端口生效。

- 配置bip8-sd错误告警（仅40GE/100GE接口支持）：
  - 执行命令**trap-threshold bip8-sd** *bip8-sd*，设置40GE和100GE接口bip8-sd错误告警阈值。
- 配置CRC错包率超门限告警的产生门限和恢复门限:
  - 执行命令**trap-threshold crc-error packet-error-ratio alarm-threshold** *alarm-coefficient-value alarm-power-value* [**resume-threshold** *resume-coefficient-valueresume-power-value*] [**trigger-lsp** | **trigger-section**],配置CRC错包率超门限告警的产生门限和恢复门限。
- 配置CRC错包率算法参数:
  - 执行命令**crc-error packet-error-ratio algorithm-parameter** *sample-window-factor child-window-max-number child-window-alarm-number child-window-resume-number*,设置CRC错包率算法参数。
  - 执行命令**crc-error packet-error-ratio algorithm-parameter realtime-factor** *template-number*,指定接口的CRC误码算法影响因素的模板号。
- 配置CRC错误告警的百分比：
  - 执行命令**trap-threshold crc-error percent** *percent-value*，配置CRC错误告警的百分比。

步骤5 （可选）执行命令**port-alarm down** { **crc-error** | **sdh-error** | **symbol-error** | **input-error** | **output-error** | **bip8-sd** }，使能错误告警联动接口物理DOWN。

说明

- 路由器同时还支持在系统视图下执行命令**port-alarm down slot** *slot-id* **card** *card-id* { **crc-error** | **sdh-error** | **symbol-error** | **input-error** | **output-error** | **bip8-sd** }，该配置将对该子卡上的所有接口都生效。
- 执行联动功能后，可以执行命令**port-alarm clear** { **crc-error** | **sdh-error** | **symbol-error** | **input-error** | **output-error** | **bip8-sd**}，手动清除物理端口的产生的告警。

步骤6 执行命令**commit**，提交配置。

----结束

配置接口接收 PAUSE 帧计数异常告警功能

本节介绍接口接收PAUSE帧计数异常告警功能的配置。

背景信息

连续三个检测时间间隔，当pause-frame错误报文条数达到指定高门限值时，系统将产生告警信息上送到网管系统；连续三个检测时间间隔，当pause-frame错误报文条数降到低门限值以下时，系统才将告警恢复信息上送到网管系统。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**interface** *interface-type interface-number*，进入接口视图。

步骤3 执行命令**trap-threshold pause-frame high-threshold** *high-threshold* **low-threshold** *low-threshold* **interval-second** *interval*，配置接口接收PAUSE帧计数异常告警阈值与检测时间间隔。

步骤4 执行命令**commit**，提交配置。

----结束

配置接口 SDH B1、SDH B2 错误告警功能

当需要基于接口接收的SDH B1、SDH B2错误报文数检测链路质量时，可以配置接口SDH B1、SDH B2错误告警功能。

背景信息

当接口频繁产生大量SDH B1或SDH B2错误报文时，说明链路质量较差，可能无法保证正常业务的流量传输。如果用户想要检测链路的质量，可以使能SDH B1或SDH B2错误告警功能。设备会每隔一段时间检测接口接收的SDH B1或SDH B2错误报文数，当接口接收的SDH B1或SDH B2错误报文数达到一定的门限值，设备将产生告警信息上送到网管系统，通知管理员进行接口维护和故障定位；当接口接收的SDH B1或SDH B2错误报文数下降到一定的门限值，设备将产生告警恢复信息上送到网管系统，通知管理员故障已恢复。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**interface** *interface-type interface-number*，进入接口视图。

步骤3 执行命令**trap-threshold** { **sdh-b1-error** | **sdh-b2-error** } *threshold* **interval-second** *interval*，配置SDH B1、SDH B2错误告警的门限值和检测时间间隔。

步骤4 执行命令**commit**，提交配置。

----结束

配置接口接收坏包字节数越限告警功能

当需要基于接口接收的坏包字节数检测链路质量时，可以配置接口接收坏包字节数越限告警功能。

背景信息

当接口频繁接收大量坏包时，说明链路质量较差，可能无法保证正常业务的可靠传输。如果用户想要检测链路的质量，可以使能接口接收坏包字节数越限告警功能。设备会每隔一段时间检测接口接收坏包字节数，当接口接收坏包字节数达到一定的门限值，设备将产生告警信息上送到网管系统，通知管理员进行接口维护和故障定位；当接口接收坏包字节数下降到一定的门限值，设备将产生告警恢复信息上送到网管系统，通知管理员故障已恢复。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**snmp-agent trap enable port bad-bytes**，使能接口接收坏包字节数越限告警功能。

步骤3 执行命令**interface** *interface-type interface-number*，进入接口视图。

步骤4 执行命令**trap-threshold bad-bytes** *trap-threshold* **interval-second** *interval*，配置接口接收坏包字节数越限告警的门限值和检测时间间隔。

步骤5 执行命令**commit**，提交配置。

----结束

检查配置结果

物理链路检测配置功能完成之后，可以查看接口配置及状态信息。

背景信息

完成物理链路检测功能配置。

操作步骤

- 在接口视图下执行命令**display trap-info**或者在系统视图下执行命令**display trap-info** { *interface-type interface-number* | *interface-name* | **slot** *slot-id* **card** *card-id* }，查看接口告警使能状态、告警门限值、告警时间间隔、告警阻断情况、当前告警状态、当前告警统计计数。
- 接口视图下执行命令**display port-error-info interface** { *interface-type interface-number* | *interface-name* }查看接口的错包或误码告警信息。

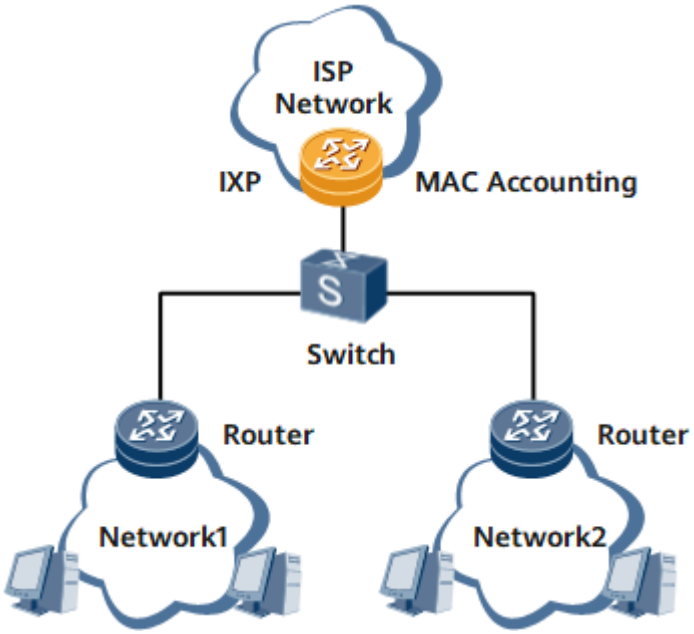
----结束

1.1.1.2.5 配置 MAC Accounting 功能

配置Mac Accounting功能，开启设备按照接口和流量报文MAC进行二三层流量统计的功能。

应用环境

图 1-38 Mac Accounting 应用场景组网图



MAC Accounting功能有两种典型应用场景：

- 当设备作为IXP角色与其它运营商互连，IXP连接的网络是其它运营商提供的网络。当ISP借用其它多个运营商的网络，例如Network1和Network2，这些其它运营商按流量收取ISP的费用。此时可以在IXP的主接口上使能MAC Accounting特性，来查看具体MAC的流量，获取对端某个Router上的具体流量，便于ISP用户分析核对流量。
- 当IXP受到DDOS攻击时，通过MAC Accounting特性可以查看具体MAC地址对应设备的流量，由此可以了解到对端每个Router的具体流量，如果某条线路流量很大，则可以初步确定攻击流量来自何处。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**interface** *interface-type interface-number*，进入用户侧主接口视图。

步骤3 执行命令**mac accounting enable**，使能MAC Accounting功能。

步骤4 执行命令**commit**，提交配置。

----结束

检查配置结果

完成配置后，可以执行**display mac accounting**命令，查看主接口或子接口MAC Accounting统计数据。

当经过一段时间后，如需重新查看MAC Account统计数据，建议先执行**reset mac accounting**命令，清除MAC Accounting统计数据。再执行**display mac accounting**命令查看统计数据，以保证查看的数据准确。

1.1.1.2.6 配置 EVC 子接口的精确剪枝功能

介绍EVC子接口的精确剪枝功能的基本配置。

应用环境

在BD场景中，如果路由器同一主接口下两个子接口，其中一个封装方式为dot1q，另一种封装方式为default，此时如果封装dot1q的子接口上有报文通过，封装default的子接口可能也会转发出一份流量，造成回流的假象。同样，如果路由器上有两个主接口，其中一个主接口配置了一个子接口，并在子接口上指定报文的封转方式为dot1q；另一个主接口下配置了两个子接口，封装方式分别为dot1q和default。此时如果第一个子接口中有流量通过，第二个主接口就同时也会转发出两份流量（两个子接口各转发出去一份）。这种情况就可能会产生流量复制，导致资源浪费，降低了单板的转发效率。为了使报文能够更加准确和精细的从指定的接口转发，可以使能精确剪枝功能。

前置任务

在配置接口的精确剪枝功能之前，需完成路由器接口物理属性的配置。

操作步骤

- 使能全局精确剪枝功能
  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**ethernet egress-strict-filter enable**，使能全局精确剪枝功能。
  c. 执行命令**commit**，提交配置。
- 使能EVC子接口下的流量剪枝功能
  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**interface** *interface-type interface-number.sub-interface-number* **mode l2**，进入EVC子接口视图。
  c. 执行命令**ethernet egress-strict-filter enable**，使能EVC子接口下的精确剪枝功能。
  d. 执行命令**commit**，提交配置。

  说明

  使能EVC子接口下的精确剪枝功能的优先级高于使能全局精确剪枝功能。即在EVC子接口下配置了精确剪枝功能后，无论全局是否使能，系统都会优先按照EVC子接口下的配置生效。

----结束

1.1.1.2.7 配置接口延迟发出信号

配置接口延迟发出信号功能，可有效减少因链路未同步切换或设备未完成配置恢复导致的数据丢失。

应用环境

设备重启或更换单板时，若接口初始化后立即发出信号，可能会因为链路未同步切换或未完成配置恢复等造成数据丢失，这种情况下可以配置接口延迟发出信号功能。

说明

- 接口延迟发出信号功能仅实际的物理接口支持，逻辑接口不支持该功能。
- 在接口上配置延迟发出信号，对已经开始发送信号的接口没有影响，该配置会在接口下次初始化时生效。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**interface** *interface-type interface-number*，进入对应接口视图。

步骤3 执行命令**port-tx-enabling-delay** *port-tx-delay-time*，配置接口延迟发出信号。

步骤4 执行命令**commit**，提交配置。

----结束

检查配置结果

完成配置后，可以执行命令**display port-tx-enabling-delay**查看接口延迟发出信号的延迟时间信息。

1.1.1.2.8 配置接口统计计数缓存周期

通过配置接口统计计数缓存周期，用户可实时获取最新的统计计数。

应用环境

网管获取接口统计计数的方式有get-next模式和get模式。get-next模式下，设备收到网管获取接口统计计数的请求后，会直接从缓存中获取接口统计计数，然后上报网管。默认情况下，缓存中统计计数的刷新周期为50秒。

用户通过MIB表节点ifTable和ifXTable获取接口接收或者发送报文的统计计数时，可以减小缓存周期，从而实现实时获取最新的统计计数。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**snmp-agent**，使能SNMP Agent。

步骤3 执行命令**snmp-agent get-next-cache if-mib age-time** *time-value*，配置网管通过get-next方式获取接口统计计数的缓存周期。

步骤4 执行命令**commit**，提交配置。

----结束

1.1.1.2.9 配置全局接口流量突变告警阈值

配置流量突变告警阈值，可以调整触发接口流量突变告警的接口流量突变百分比。

应用环境

当流量突变并且用户期望感知此情况时，可以配置接口流量突变告警阈值，配置此阈值后，当流量变化百分比超过配置的告警阈值时，设备会上报告警来提醒用户。用户可以根据需要，自行设置流量突变告警阈值，但阈值不要设置的太小，若设置的太小，设备会频繁上报告警。

接口流量变化百分比的公式如下：

接口流量变化百分比 = 当前流量统计周期和上一个流量统计周期的接口速率的差值的绝对值/上一个流量统计周期的接口速率

接口流量统计周期可以通过**set flow-stat interval**命令配置，缺省情况下是300秒。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**set flow-change-ratio** { **input-threshold** | **output-threshold** } **upper-limit** *threshold*，配置接口流量突变告警阈值。

配置此命令后，如果用户打开了流量突变告警开关（通过**snmp-agent trap enable feature-name port trap-name hwinputratechangeoverthresholdnotice**或**snmp-agent trap enable feature-name port trap-name hwoutputratechangeoverthresholdnotice**配置），当流量变化百分比超过配置的告警阈值时，会产生如下两条告警：

- PORT_1.3.6.1.4.1.2011.5.25.157.2.219 hwInputRateChangeOverThresholdNotice
- PORT_1.3.6.1.4.1.2011.5.25.157.2.220 hwOutputRateChangeOverThresholdNotice

步骤3 执行命令**commit**，提交配置。

----结束

1.1.1.2.10 光模块激光器配置

本节介绍打开或关闭光模块激光器发光功能的配置。

应用环境

当线路发生故障时，设备维护人员在进行定位或恢复故障时可能会被光模块发出的激光伤害，这时可以配置自动或手动关闭光模块激光器发光功能，从而确保设备维护人员的人身安全。设备维护人员排除故障后，光模块需要等待一段时间，才能恢复正常工作状态。这时可以配置手动打开光模块激光器发光功能，立即使光模块激光器发光，检测线路是否恢复正常，并恢复正常工作状态。

前置任务

在配置光模块激光器之前，需完成以下任务：

- 路由器上电，自检正常。
- 光模块已在位，且接口没有被shutdown。

配置自动或手动关闭光模块激光器的发光功能

通过配置关闭光模块激光器的发光功能，在线路故障时，可以及时关闭发光功能，避免激光器发光给设备维护人员带来伤害。

背景信息

当线路发生故障时，设备维护人员在进行定位或恢复故障时可能会被光模块发出的激光伤害，这时可以使能光模块激光器自动关闭发光功能，当光模块在感知到线路故障时自动关闭发光功能，或者手动关闭光模块激光器的发光功能，从而确保设备维护人员的人身安全。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**interface** *interface-type interface-number*，进入接口视图。

步骤3 请根据需要，选择其中一种配置：

- 配置自动关闭光模块激光器的发光功能。
  a. 执行命令**laser autoshutdown enable**，使能光模块激光器自动关闭发光功能。
  b. (可选)执行命令**laser auto-shutdown-interval** { **open** *opentime-interval* | **close** *closetime-interval* }，配置光模块激光器自动关闭发光功能的开时间间隔和关时间间隔。

- 配置手动关闭光模块激光器的发光功能。

  执行命令**laser turn-off**，配置手动关闭光模块激光器发光功能。

  须知

  在接口正常工作的状态下，请不要随意执行laser turn-off，执行此命令会将光模块激光器发光功能关闭，接口上的业务会中断。

步骤4 执行命令**commit**，提交配置。

----结束

（可选）配置手动打开光模块激光器发光功能

通过手工打开光模块激光器发光功能，可以及时检测线路故障是否排除。

背景信息

当接口上配置了光模块激光器自动关闭发光功能时，如果线路发生故障，光模块激光器会自动关闭发光功能。设备维护人员排除故障后，光模块需要等待一段时间，才能恢复正常工作状态。这时手动打开光模块激光器发光功能，可以立即使光模块激光器发光，检测线路是否恢复正常，并恢复正常工作状态。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**interface** *interface-type interface-number*，进入接口视图。

步骤3 执行命令**laser turn-on** [**duration** *duration*]，配置手动打开光模块激光器发光功能，并指定激光器自动关闭发光功能后的长开持续时间。

只有执行命令**laser autoshutdown enable**后，配置的长开持续时间才能生效。

步骤4 执行命令**commit**，提交配置。

----结束

检查配置结果

光模块激光器配置功能完成之后，可以查看光模块激光器的状态信息。

前提条件

已完成光模块激光器的所有配置。

背景信息

对激光器发光状态有影响的命令及操作包括：

- 使用命令**laser turn-on**手动打开光模块激光器。
- 使用命令**laser turn-off**手动关闭光模块激光器。
- 使用命令**laser autoshutdown enable**使能激光器自动关闭功能。

- 使用命令**shutdown**关闭接口。

操作步骤

- 在任意视图下执行命令**display laser status**，查看光模块激光器的状态。

----结束

1.1.1.2.11 配置端口的光模块模式

背景信息

当用户需要进行光模块模式切换时，可以通过此配置设置端口的光模块模式。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**interface** *interface-type interface-number*，进入接口视图。

步骤3 执行命令**optical-mode** { **osnr** | **hsen** }，配置光模块为光信噪比模式或高灵敏度模式。

步骤4 执行命令**commit**，提交配置。

----结束

1.1.1.2.12 使能光模块告警门限标准化

通过配置光模块告警门限标准化，使设备上读取出来的光模块门限值符合用户需求。

背景信息

由于系统自动读取光模块厂家设定的门限值并和现网实际收发功率进行比对，如果超出范围，就会打印告警。但是光模块厂家设定的门限值有时不符合用户需求，需要变更告警门限的获取方式。使能光模块告警门限标准化功能后，光模块的门限统一使用标准值，该标准值根据光模块的传输距离和带宽计算得出。

说明

当前版本针对光模块功率的告警有两种类型：warning告警和alarm告警。warning告警是比较轻微的告警，也可认为是预警。根据光模块的不同规格，功率处在预警值也可能正常工作。如果用户对阈值不敏感，配置此命令就可以禁止warning预警检测。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**optical-module alarm-threshold standardization enable**，使能光模块告警门限标准化功能。

步骤3 执行命令**commit**，提交配置。

----结束

1.1.1.2.13 配置光模块禁止告警检测

通过配置光模块禁止告警检测，可以屏蔽光模块功率告警。

背景信息

由于系统自动读取光模块厂家设定的阈值并和现网实际收发功率进行比对，如果超出范围，就会打印告警。而由于现网光纤的光功率通常都大于光模块厂家设定的阈值，而造成告警频繁。鉴于维护的困难，现网光纤上安装衰减器是不可行的。用户可以通过配置此命令，控制设备上某个端口的光模块告警是否使能，比如用户不想收到光模块接收功率高预警，可以关闭光模块接收功率高预警选项，其他告警还是可以正常上报。

说明

当前版本针对光模块功率的告警有两种类型：warning告警和alarm告警。warning告警是比较轻微的告警，也可认为是预警。根据光模块的不同规格，功率处在预警值也可能正常工作。如果用户对阈值不敏感，配置此命令就可以禁止warning预警检测。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**interface** *interface-type interface-number*，进入接口视图。

步骤3 执行命令**port-alarm disable optical-module** { **rx-power-high-warning** | **rx-power-low-warning** | **tx-power-high-warning** | **tx-power-low-warning** | **voltage-high-warning** | **voltage-low-warning** } *，配置光模块禁止告警检测。

步骤4 执行命令**commit**，提交配置。

----结束

1.1.1.2.14 管理第三方光模块

通过配置管理第三方光模块，可以屏蔽第三方光模块非认证告警并且联动端口down功能。

背景信息

当端口中插入第三方非华为公司认证的光模块时，系统会自动上报光模块非认证告警，当用户不想看到此告警时，可以通过配置第三方光模块非认证告警上报功能，屏蔽第三方光模块非认证告警，同时也可以将插入第三方模块的端口配置为down，禁止用户使用。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**transceiver non-certified-alarm disable** ，关闭光模块非认证告警上报。

步骤3 执行命令**transceiver non-certified-alarm port-down enable**，开启插入第三方光模块的端口down功能。

步骤4 执行命令**commit**，提交配置。

----结束

1.1.1.2.15 配置 PN 反序模式

背景信息

当和其他厂商100GE 80KM光模块无法对接时，需要将PN设置成反序模式，这样会引起接口SerDes PN极性反序，造成业务中断，因此配置该功能时请慎重。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**interface** *interface-type interface-number*，进入接口视图。

步骤3 执行命令**optical pn-reverse enable** ，设置PN反序模式，使80KM光模块与其他厂商对接。

步骤4 执行命令**commit**，提交配置。

----结束

1.1.1.2.16 控制接口震荡配置

简单介绍控制接口震荡的基本配置。

应用环境

当接口频繁交替出现Up和Down状态造成路由协议、MPLS（Multiprotocol Label Switching）等反复震荡，影响整个网络的稳定性时，可以配置控制接口震荡特性，减少接口的频繁交替出现Up和Down状态。

抑制接口震荡特性（control-flap）对接口频繁Up、Down事件进行控制，使其小于一定的频率，以减小对设备及网络稳定性的影响。

接口震荡抑制的相关概念和原理请参考**抑制接口震荡**。

前置任务

在配置控制接口震荡之前，需完成路由器接口物理属性的配置。

操作步骤

- 配置control-flap功能：
  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**interface** *interface-type interface-number*，进入接口视图。

     说明

     NULL接口和Loopback接口不支持control-flap特性。
  c. 执行命令**control-flap** [*suppress reuse ceiling decay-ok decay-ng*]，使能接口的control-flap功能。

     *suppress*是接口抑制门限的1000倍，取值范围是1～20000，缺省值是2000，其值必须大于*reuse*值且小于*ceiling*的值。

     *reuse*是接口重用门限的1000倍，取值范围是1～20000，缺省值是750，其值必须小于*suppress*的值。

*ceiling*是接口抑制惩罚值的最大值的1000倍，取值范围是1001～20000，缺省值是6000，其值必须大于*suppress*的值。

*decay-ok*是接口Up时，惩罚值半衰期。取值范围是1～900秒，缺省值是54秒。

*decay-ng*是接口Down时，惩罚值半衰期。取值范围是1～900秒，缺省值是54秒。

d. 执行命令**commit**，提交配置。

- 配置接口的damp-interface功能：
  a. 执行命令**system-view**，进入系统视图。
  b. （可选）执行命令**interface** *interface-type interface-number*，进入某种接口视图。
  c. 执行命令**damp-interface enable**命令使能damp-interface功能。
  d. （可选）执行命令**damp-interface level** { **light** | **middle** | **heavy** | **manual** { *half-life-period suppress reuse max-suppress-time* } }，配置接口的damp-interface功能的抑制级别。
     - **light**：接口震荡轻度抑制，只有接口频繁快速震荡的时候系统才会触发抑制流程。该级别是系统默认抑制级别，主要是针对系统影响最大的接口震荡场景。
     - **heavy**：接口震荡重度抑制，只要系统识别接口状态开始震荡，即使接口状态震荡不是很严重，也会触发接口状态的震荡抑制功能，即接口较容易进入震荡抑制状态。该级别主要是针对接口震荡特别敏感的业务部署场景，防止由于接口震荡导致业务受损以及系统资源紧张。
     - **middle**：接口震荡中度抑制，抑制强度等级介于light和heavy之间。
     - **manual**：当light、middle、heavy三个量级的抑制不能满足需求时，选用此选项手动配置。
  e. （可选）执行命令**damp-interface mode tx-off**，配置当接口为物理震荡抑制状态时关闭发送信号。

     在接口进入物理震荡抑制状态时，如果需要让对端感知本端接口不可用，可以执行本命令关闭发送信号。

     接口关闭发送信号后，对端接口会按照本端接口已经Down的状态进行处理。

     当接口物理震荡抑制状态解除时，本端接口会重新自动开启发送信号，可以让对端接口按照本端接口已经Up的状态进行处理。
  f. 执行命令**commit**，提交配置。

----结束

检查配置结果

完成配置后，可以执行命令来检查功能的配置结果。

执行命令**display control-flap interface** *interface-type interface-number*，可以看到接口配置的控制接口震荡特性。

执行命令**display damp-interface** [**interface** *interface-type interface-number*]，可以查看接口物理状态震荡抑制特性的当前运行状态和统计信息。

1.1.1.2.17 逻辑接口配置

逻辑接口是指能够实现数据交换功能但物理上不存在、需要通过配置建立的接口。

应用环境

逻辑接口的应用环境请参见《NetEngine 8100 X, NetEngine 8000 X, NetEngine 8000E X 特性描述-接口管理》中“逻辑接口”

表 1-14 逻辑接口列表

所属分册	接口名称	配置指南
系统管理	DCN-Serial接口	该接口由系统自动生成，不涉及配置。
接口管理	VE接口（Virtual Ethernet，虚拟以太网接口）	创建L2VE接口 创建L3VE接口
接口管理	Global-VE接口（Global Virtual Ethernet，全局虚拟以太网接口）	**创建全局虚拟以太网接口**
接口管理	Loopback接口（环回接口）	**创建Loopback接口并配置IP地址**
接口管理	NULL0接口	**进入NULL接口视图**
局域网与城域网接入	以太网子接口	配置以太网子接口支持VLAN间的通信
局域网与城域网接入	ETH-Trunk接口	Eth-Trunk接口配置
局域网与城域网接入	VLANIF接口	配置VLANIF接口实现三层互通
MPLS	Tunnel接口	MPLS TE配置

前置任务

在配置逻辑接口之前，需完成以下任务：

- 连接接口并配置接口的物理参数，使接口的物理层状态为Up。

创建全局虚拟以太网接口

全局虚拟以太网接口不依赖于物理接口板，只要路由器上电，就可以创建全局虚拟以太网接口。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**interface global-ve** *ve-number*，创建并进入全局虚拟以太网接口视图。

步骤3 执行命令**commit**，提交配置。

----结束

配置信道化子接口

介绍信道化子接口的配置。

背景信息

为避免不同业务之间相互影响，需要有一种能够隔离不同类型业务的机制。不同业务流量可以归属到不同的Dot1q封装方式的VLAN信道化子接口上，每个信道化子接口可以实现独立的HQoS调度，从而实现不同类型业务之间的隔离。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**interface** *interface-type interface-number.subinterface-number* ，进入指定物理子接口。

步骤3 按照需要配置对应的子接口：

- 对于以太子接口，
  - 执行命令**vlan-type dot1q** *vlanid*，配置子接口的封装方式为Dot1q方式。
  - 执行命令**encapsulation qinq-termination**，**qinq termination pe-vid** *pe-vlanid* **ce-vid** *ce-vlanid*，配置子接口的封装方式为QinQ终结方式。

步骤4 执行命令**quit**，退回系统视图。

步骤5 执行命令**license**，进入License视图。

说明

GE接口无需激活信道化子接口的License。

步骤6 执行命令**active port-slicing slot** *slotid* **card** *cardid* **port** *port-list*，激活设备信道化子接口的License。

步骤7 执行命令**quit**，退回系统视图。

步骤8 执行命令**interface** *interface-type interface-number.subinterface-number* ，进入指定物理子接口。

步骤9 执行命令**mode channel enable**，使能子接口信道化功能。

步骤10 （可选）执行命令**mode channel bandwidth** *bwvalue*，配置信道化子接口的带宽。

步骤11 执行命令**commit**，提交配置。

----结束

创建 Loopback 接口并配置 IP 地址

配置Loopback接口时一般都会为其配置IP地址，利用其一直处于Up状态的特点与其他设备进行通信。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**interface loopback** *loopback-number*，创建并进入Loopback接口。

用户可以创建或删除Loopback接口。Loopback接口一旦被创建，除了在Loopback接口监视接口监控组场景中，Loopback接口可能会联动接口监控组状态变为Down，其他情况下其链路层协议状态将一直是Up。

步骤3 执行命令**ip address** *ip-address* { *mask* | *mask-length* }，配置Loopback接口的IP地址。

步骤4 执行命令**commit**，提交配置。

----结束

进入 NULL 接口视图

系统自动创建一个NULL0接口，不需要手工创建。NULL接口主要用于防止路由环路和过滤流量。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**interface null 0**，进入NULL接口视图。

NULL接口的状态一直是Up，但不能转发数据包，也不能配置IP地址或封装其他协议。

----结束

后续处理

对于NULL接口，主要用于防止路由环路和过滤流量，例如：在系统视图下配置命令**ip route-static 192.168.0.0 255.255.0.0 NULL 0**，当前设备会丢弃所有去往网段192.168.0.1～192.168.255.255的报文。

检查配置结果

配置Global-VE接口、FlexE接口license、 FlexE接口、Loopback接口和NULL接口后，需要检查配置结果，保证配置正确。

前提条件

已经完成Global-VE接口、FlexE接口license、 FlexE接口、Loopback接口或NULL接口的所有配置。

操作步骤

- 使用**display interface global-ve** [*ve-number*]命令查看Global-VE接口的状态信息。
- 使用**display license resource usage port-slicing** { **all** | **slot** *slot-id* } [**active** | **deactive**]命令查看单板上的端口分片License的授权情况。
- 使用**display interface loopback** [*loopback-number*]命令查看Loopback接口的状态信息。

- 使用**display interface null** [**0**]命令查看NULL接口的状态信息。
- 使用**display flexe group information slot** *slot-id* **card** *card-id*命令查看FlexE子卡上的Group信息、加入Group的FlexE物理口信息和Group内时隙分配情况。

----结束

1.1.1.2.18 FlexE 接口配置

FlexE接口就是指FlexE Client，对应于网络中外在观察到的各种用户接口，每个FlexE Client可以灵活的从Group资源池分配带宽，同时可以进行带宽调整。VS模式下，该特性仅在Admin VS支持。

应用环境

随着5G的建设，网络发展对移动承载带宽提出更高的需求，同时用户也希望通过统一的网络来承载各种不同的业务，包括家庭宽带业务、专线接入业务、移动承载等，这些需求对电信网络接口也提出了更高的要求。FlexE技术通过接口带宽隔离，即可以实现业务隔离。FlexE接口之间可以完全隔离互不影响，流量在物理层隔离，业务在同一张物理网络上进行网络分片。

FlexE技术可应用在接入层、汇聚层、核心层，随着5G业务的起步、发展、成熟，其业务量是逐步增长的，承载网可以通过FlexE进行平滑升级。

前提条件

在配置FlexE接口之前，需完成以下任务：

- 设备上电，自检正常。
- 设备上已有支持FlexE功能的单板。
- 激活单板的灵活以太端口License。

激活单板的灵活以太端口 License

如果要配置灵活以太业务，必须先激活单板的灵活以太端口License。

前置任务

在激活单板的灵活以太端口License之前，需要完成以下任务：

1. 执行命令**license active** *file-name*，激活主控板上的License文件。
2. 执行命令**system-view**，进入系统视图。
3. 执行命令**license**，进入License视图。
4. 执行命令**active port-basic slot** *slot-id* **card** *card-id* **port** *port-list*，激活端口基本硬件License。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**license**，进入License视图。

步骤3 执行命令**active port-slicing slot** *slotid* **card** *cardid* **port** *port-list*，激活单板的灵活以太端口License。

步骤4 执行命令**commit**，提交配置。

----结束

配置标准 Ethernet 接口为灵活以太模式

标准Ethernet接口的带宽是固定的，如果需要实现接口带宽可灵活指定，就需要将接口从标准以太模式切换为灵活以太模式。

背景信息

标准Ethernet接口切换为灵活以太模式后，系统会自动创建FlexE物理接口，原先的标准Ethernet接口会被删除，包括该物理接口上的已配置业务也会被同时删除，如果该物理接口是Eth-Trunk成员口，也会被从Eth-Trunk接口中删除。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**flexe enable port** *port-position*，将Ethernet接口从标准以太模式切换为灵活以太模式。

步骤3 执行命令**commit**，提交配置。

----结束

配置 FlexE 物理接口的 PHY Number

为保证对接的两端设备正常通信，用户需要在两端设备的FlexE物理接口上分别配置相同的PHY Number值。

背景信息

不同的FlexE物理接口可以配置相同的PHY Number值，但是具有相同PHY Number值的FlexE物理接口不能加入同一个FlexE Group，且同一个FlexE物理接口只能加入一个FlexE Group。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**interface** *interface-type interface-number*，进入FlexE物理接口视图，例如FlexE-50G 1/1/1接口。

步骤3 执行命令**phy-number** *phy-number*，配置FlexE物理接口的PHY Number值。

步骤4 （可选）执行命令**management-channel mode** { **union** | **section** | **shim-to-shim** | **shim-to-shim-op2** }，配置FlexE物理接口的管理通道模式。

步骤5 （可选）执行命令**down-filter disable**，关闭FlexE物理接口的Down中断抑制功能。

步骤6 执行命令**commit**，提交配置。

----结束

创建 FlexE Group 并绑定 FlexE 物理接口

创建FlexE Group后，用户可以绑定一组FlexE物理接口到Group，按照子时隙粒度，为FlexE Client灵活分配带宽。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**flexe group** *group-index*，创建FlexE Group或者进入指定已创建的FlexE Group视图。

步骤3 （可选）执行命令**description** *text*，配置FlexE Group的描述信息。

为了方便记忆和管理，可以配置此步骤用来对特定的FlexE Group进行详细描述。

步骤4 执行命令**binding interface** *interface-type interface-number*，绑定FlexE物理接口到FlexE Group。

步骤5 （可选）执行命令**padding enable**，使能padding功能。

步骤6 （可选）执行命令**timeslot-negotiation mode disable**，去使能时隙协商模式。

说明

针对FlexE Group中绑定的PHY所在的FlexE卡上配置的是时隙模式，在去使能时隙协商模式前，需要保证当前Group下的FlexE Client没有绑定子时隙。

- 对接设备不支持时隙协商模式时，需要在本端FlexE Group视图下配置时隙协商去使能。
- 对接设备两端的FlexE Group上，要求配置相同的时隙协商模式，否则在执行可靠性操作（如主备倒换、复位子卡、**shutdown**/**undo shutdown**端口等）之后可能导致FlexE接口不up或流量不通。
- 对接设备两端的FlexE Group都配置时隙协商去使能后，两端对应的FlexE Client需要配置完全相同的时隙编号，否则可能导致FlexE接口不up或流量不通。

步骤7 执行命令**commit**，提交配置。

----结束

配置 FlexE Group 的 Group ID

为保证对接的两端设备正常通信，用户需要将两端设备上FlexE物理接口加入的FlexE Group配置相同的Group ID。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**flexe group** *group-index*，创建FlexE Group或者进入指定已创建的FlexE Group视图。

步骤3 执行命令**flexe-groupnum** *group-number*，配置FlexE Group的Group ID值。

步骤4 执行命令**commit**，提交配置。

----结束

（可选）配置 FlexE 卡的子时隙粒度

FlexE卡的子时隙粒度约束着FlexE Client的带宽配置，缺省情况下，FlexE卡的子时隙粒度为5GE。

背景信息

如果FlexE Client需要配置小于5GE的带宽，就需要先配置FlexE卡的子时隙粒度为1GE。

基于不同子时隙粒度的FlexE Client的带宽配置规则如下：

- 当子时隙粒度为默认值5GE时，FlexE Client的带宽值可配置为5GE的整数倍，例如5GE、10GE、15GE等。
- 当子时隙粒度为1GE时，FlexE Client的带宽值可配置为1GE、2GE、3GE和4GE，以及5GE的整数倍。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**set flexe sub-time-slot granula slot** *slotid* **card** *cardid* { **1g** | **5g** }，配置FlexE卡的子时隙粒度。

步骤3 执行命令**commit**，提交配置。

----结束

（可选）配置 FlexE 卡的模式

FlexE卡的模式包括时隙模式和带宽模式，应用中推荐采用带宽模式。

背景信息

- 时隙模式：指在配置FlexE Client时静态指定该Client分配的时隙号。
- 带宽模式：指在配置FlexE Client时只指定需要的带宽，具体对应的时隙由设备自动分配。

说明

缺省情况下，FlexE卡的模式为带宽模式。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**slot** *slot-id*，进入槽位视图。

步骤3 执行命令**flexe config-mode card** *cardid* { **bandwidth** | **timeslot** }，将FlexE卡的模式设置为带宽模式或时隙模式。

步骤4 执行命令**commit**，提交配置。

----结束

创建 FlexE Client 并配置 Client ID 和带宽

FlexE Client对应于外在观察到的用户接口，每个FlexE Client可以灵活的从Group资源池分配带宽，同时可以进行带宽调整。

背景信息

为保证对接的两端设备的FlexE Client正常通信，用户需要将两端设备上FlexE Client的Client ID和带宽配置一致。

表 1-15 不同型号子卡对应的能加入同一 Group 的物理口编号和 port-id 参数的取值范围

型号	能加入同一Group的物理口编号	port-id取值范围
CR8D0E18KBCP	3	1000-3000
	4	1000-3000
	5	1000-3000
	6	1000-3000
	7	1000-3000
	8	1000-3000
	12	1000-3000
	13	1000-3000
	14	1000-3000
	15	1000-3000
	16	1000-3000
	17	1000-3000
CR8D00EKNBC1	0,1,2,3	40-69, 1000-3000
	5,6,8,9	70-99, 1000-3000
	10,11,12,13	100-129, 1000-3000
	15,16,18,19	130-159, 1000-3000
	20,21,22,23	160-189, 1000-3000
	25,26,28,29	190-219, 1000-3000
	30,31,32,33	220-249, 1000-3000
	35,36,38,39	250-279, 1000-3000
CR8D00EKNBC2	0,1,2,3	40-69, 1000-3000
	5,6,8,9	70-99, 1000-3000

型号	能加入同一Group的物理口编号	port-id取值范围
	10,11,12,13	100-129, 1000-3000
	15,16,18,19	130-159, 1000-3000
	20,21,22,23	160-189, 1000-3000
	25,26,28,29	190-219, 1000-3000
	30,31,32,33	220-249, 1000-3000
	35,36,38,39	250-279, 1000-3000
CR8D00EKNBC0	0,1,2,3	40-69, 1000-3000
	5,6,8,9	70-99, 1000-3000
	10,11,12,13	100-129, 1000-3000
	15,16,18,19	130-159, 1000-3000
	20,21,22,23	160-189, 1000-3000
	25,26,28,29	190-219, 1000-3000
	30,31,32,33	220-249, 1000-3000
	35,36,38,39	250-279, 1000-3000
CR8D00EKNBC5	0,1,2,3	40-69, 1000-3000
	5,6,8,9	70-99, 1000-3000
	10,11,12,13	100-129, 1000-3000
	15,16,18,19	130-159, 1000-3000
	20,21,22,23	160-189, 1000-3000
	25,26,28,29	190-219, 1000-3000
	30,31,32,33	220-249, 1000-3000
	35,36,38,39	250-279, 1000-3000
CR8D00EKNBC3	0,1,2,3	40-69, 1000-3000
	5,6,8,9	70-99, 1000-3000
	10,11,12,13	100-129, 1000-3000
	15,16,18,19	130-159, 1000-3000
	20,21,22,23	160-189, 1000-3000
	25,26,28,29	190-219, 1000-3000
	30,31,32,33	220-249, 1000-3000

型号	能加入同一Group的物理口编号	port-id取值范围
	35,36,38,39	250-279, 1000-3000
CR8D00EKNBCP	0,1,2,3	40-69, 1000-3000
	5,6,8,9	70-99, 1000-3000
	10,11,12,13	100-129, 1000-3000
	15,16,18,19	130-159, 1000-3000
	20,21,22,23	160-189, 1000-3000
	25,26,28,29	190-219, 1000-3000
	30,31,32,33	220-249, 1000-3000
	35,36,38,39	250-279, 1000-3000
CR8D00EKNBCQ	0,1,2,3	40-69, 1000-3000
	5,6,8,9	70-99, 1000-3000
	10,11,12,13	100-129, 1000-3000
	15,16,18,19	130-159, 1000-3000
	20,21,22,23	160-189, 1000-3000
	25,26,28,29	190-219, 1000-3000
	30,31,32,33	220-249, 1000-3000
	35,36,38,39	250-279, 1000-3000
CR8D00EKNBCR	0,1,2,3	40-69, 1000-3000
	5,6,8,9	70-99, 1000-3000
	10,11,12,13	100-129, 1000-3000
	15,16,18,19	130-159, 1000-3000
	20,21,22,23	160-189, 1000-3000
	25,26,28,29	190-219, 1000-3000
	30,31,32,33	220-249, 1000-3000
	35,36,38,39	250-279, 1000-3000
CR8D00EENBC1	1,2,4,5	20-49, 1000-3000
	6,7,8,9	50-79, 1000-3000
	11,12,14,15	80-109, 1000-3000
	16,17,18,19	110-139, 1000-3000

型号	能加入同一Group的物理口编号	port-id取值范围
CR8D00EENBC3	1,2,4,5	20-49, 1000-3000
	6,7,8,9	50-79, 1000-3000
	11,12,14,15	80-109, 1000-3000
	16,17,18,19	110-139, 1000-3000
CR8DE8KE8NCS	0	1000-3000
	1	1000-3000
	2	1000-3000
	3	1000-3000
	8	1000-3000
	9	1000-3000
	10	1000-3000
	11	1000-3000
CR8DE8KE8NCR	0	1000-3000
	1	1000-3000
	2	1000-3000
	3	1000-3000
	8	1000-3000
	9	1000-3000
	10	1000-3000
	11	1000-3000
CR8DE8KE8NCV	0	1000-3000
	1	1000-3000
	2	1000-3000
	3	1000-3000
	8	1000-3000
	9	1000-3000
	10	1000-3000
	11	1000-3000
CR8DE8KE8NCW	0	1000-3000

型号	能加入同一Group的物理口编号	port-id取值范围
	1	1000-3000
	2	1000-3000
	3	1000-3000
	8	1000-3000
	9	1000-3000
	10	1000-3000
	11	1000-3000
CR8D00EINBC1（NetEngine 8100 X8）	0,1,2,3	1000-3000
	4,5,6,7	1000-3000
	8,9,10,11	1000-3000
	12,13,14,15	1000-3000
	16,17,18,19	1000-3000
	20,21,22,23	1000-3000
	24,25,26,27	1000-3000
	28,29,30,31	1000-3000
CR8D00EENBC5（NetEngine 8000E X8）	1,2,4,5	20-49,1000-3000
	6,7,8,9	50-79,1000-3000
	11,12,14,15	80-109,1000-3000
	16,17,18,19	110-139,1000-3000
CR8DEANCJXCD	36,37	1000-3000
	38,39	1000-3000
	40,41	1000-3000
	42,43	1000-3000
	44	1000-3000
	45	1000-3000
CR8DEANCJXCE	36,37	1000-3000
	38,39	1000-3000
	40,41	1000-3000
	42,43	1000-3000

型号	能加入同一Group的物理口编号	port-id取值范围
	44	1000-3000
	45	1000-3000
CR8DEANCJXCB	36,37	1000-3000
	38,39	1000-3000
	40,41	1000-3000
	42,43	1000-3000
	44	1000-3000
	45	1000-3000
CR8DEANCJXCC	36,37	1000-3000
	38,39	1000-3000
	40,41	1000-3000
	42,43	1000-3000
	44	1000-3000
	45	1000-3000
GPLI20CQES9	1,2,4,5	20-49, 1000-3000
	6,7,8,9	50-79, 1000-3000
	11,12,14,15	80-109, 1000-3000
	16,17,18,19	110-139, 1000-3000
GPLI20CQE10	1,2,4,5	20-49, 1000-3000
	6,7,8,9	50-79, 1000-3000
	11,12,14,15	80-109, 1000-3000
	16,17,18,19	110-139, 1000-3000
GPLI40CQES7	0,1,2,3	40-69, 1000-3000
	5,6,8,9	70-99, 1000-3000
	10,11,12,13	100-129, 1000-3000
	15,16,18,19	130-159, 1000-3000
	20,21,22,23	160-189, 1000-3000
	25,26,28,29	190-219, 1000-3000
	30,31,32,33	220-249, 1000-3000

型号	能加入同一Group的物理口编号	port-id取值范围
	35,36,38,39	250-279, 1000-3000
GPLI40CQE8	0,1,2,3	40-69, 1000-3000
	5,6,8,9	70-99, 1000-3000
	10,11,12,13	100-129, 1000-3000
	15,16,18,19	130-159, 1000-3000
	20,21,22,23	160-189, 1000-3000
	25,26,28,29	190-219, 1000-3000
	30,31,32,33	220-249, 1000-3000
	35,36,38,39	250-279, 1000-3000
GPLI4KQ24CQES1	0	1000-3000
	1	1000-3000
	2	1000-3000
	3	1000-3000
	8,9,10,11	1000-3000
	13,14,16,17	1000-3000
	18,19,20,21	1000-3000
	23,24,26,27	1000-3000
GPLI4KQ24CQE2	0	1000-3000
	1	1000-3000
	2	1000-3000
	3	1000-3000
	8,9,10,11	1000-3000
	13,14,16,17	1000-3000
	18,19,20,21	1000-3000
	23,24,26,27	1000-3000
GPLI32CQE4（NetEngine 8100）	0,1,2,3	1000-3000
	4,5,6,7	1000-3000
	8,9,10,11	1000-3000
	12,13,14,15	1000-3000

型号	能加入同一Group的物理口编号	port-id取值范围
	16,17,18,19	1000-3000
	20,21,22,23	1000-3000
	24,25,26,27	1000-3000
	28,29,30,31	1000-3000
CR8DEANEJXDM	36,37	1000-3000
	38,39	1000-3000
	40,41	1000-3000
	42,43	1000-3000
	44	1000-3000
	45	1000-3000
CR8DEANEJXD1	36,37	1000-3000
	38,39	1000-3000
	40,41	1000-3000
	42,43	1000-3000
	44	1000-3000
	45	1000-3000
CR8DEANEJXD2	36,37	1000-3000
	38,39	1000-3000
	40,41	1000-3000
	42,43	1000-3000
	44	1000-3000
	45	1000-3000
CR8DEANEJXDN	36,37	1000-3000
	38,39	1000-3000
	40,41	1000-3000
	42,43	1000-3000
	44	1000-3000
	45	1000-3000
CR8D00EENBC7	1,2,4,5	20-49, 1000-3000

型号	能加入同一Group的物理口编号	port-id取值范围
	6,7,8,9	50-79, 1000-3000
	11,12,14,15	80-109, 1000-3000
	16,17,18,19	110-139, 1000-3000
CR8D00EENBC9	1,2,4,5	20-49, 1000-3000
	6,7,8,9	50-79, 1000-3000
	11,12,14,15	80-109, 1000-3000
	16,17,18,19	110-139, 1000-3000
CR8D00EENBC8	1,2,4,5	20-49, 1000-3000
	6,7,8,9	50-79, 1000-3000
	11,12,14,15	80-109, 1000-3000
	16,17,18,19	110-139, 1000-3000
CR8D00EENBCD	1,2,4,5	20-49, 1000-3000
	6,7,8,9	50-79, 1000-3000
	11,12,14,15	80-109, 1000-3000
	16,17,18,19	110-139, 1000-3000
CR8D00EENBCA	1,2,4,5	20-49, 1000-3000
	6,7,8,9	50-79, 1000-3000
	11,12,14,15	80-109, 1000-3000
	16,17,18,19	110-139, 1000-3000
CR8D00EKNBC6	0,1,2,3	40-69, 1000-3000
	5,6,8,9	70-99, 1000-3000
	10,11,12,13	100-129, 1000-3000
	15,16,18,19	130-159, 1000-3000
	20,21,22,23	160-189, 1000-3000
	25,26,28,29	190-219, 1000-3000
	30,31,32,33	220-249, 1000-3000
	35,36,38,39	250-279, 1000-3000
CR8D00EKNBC8	0,1,2,3	40-69, 1000-3000
	5,6,8,9	70-99, 1000-3000

型号	能加入同一Group的物理口编号	port-id取值范围
	10,11,12,13	100-129, 1000-3000
	15,16,18,19	130-159, 1000-3000
	20,21,22,23	160-189, 1000-3000
	25,26,28,29	190-219, 1000-3000
	30,31,32,33	220-249, 1000-3000
	35,36,38,39	250-279, 1000-3000
CR8D00EKNBC7	0,1,2,3	40-69, 1000-3000
	5,6,8,9	70-99, 1000-3000
	10,11,12,13	100-129, 1000-3000
	15,16,18,19	130-159, 1000-3000
	20,21,22,23	160-189, 1000-3000
	25,26,28,29	190-219, 1000-3000
	30,31,32,33	220-249, 1000-3000
	35,36,38,39	250-279, 1000-3000
CR8D00EKNBC9	0,1,2,3	40-69, 1000-3000
	5,6,8,9	70-99, 1000-3000
	10,11,12,13	100-129, 1000-3000
	15,16,18,19	130-159, 1000-3000
	20,21,22,23	160-189, 1000-3000
	25,26,28,29	190-219, 1000-3000
	30,31,32,33	220-249, 1000-3000
	35,36,38,39	250-279, 1000-3000
CR8DE4KEFNC0	0	1000-3000
	1	1000-3000
	2	1000-3000
	3	1000-3000
	8,9,10,11	1000-3000
	13,14,16,17	1000-3000
	18,19,20,21	1000-3000

型号	能加入同一Group的物理口编号	port-id取值范围
	23,24,26,27	1000-3000
CR8DE4KEFNC1	0	1000-3000
	1	1000-3000
	2	1000-3000
	3	1000-3000
	8,9,10,11	1000-3000
	13,14,16,17	1000-3000
	18,19,20,21	1000-3000
	23,24,26,27	1000-3000
CR8DE4KFBNC2	0	1000-3000
	1	1000-3000
	2	1000-3000
	3	1000-3000
	8,9,10,11	1000-3000
	13,14,16,17	1000-3000
	18,19,20,21	1000-3000
	23,24,26,27	1000-3000
CR8DE4KFBNC1	0	1000-3000
	1	1000-3000
	2	1000-3000
	3	1000-3000
	8,9,10,11	1000-3000
	13,14,16,17	1000-3000
	18,19,20,21	1000-3000
	23,24,26,27	1000-3000
CR8DEENBFED1	1,2,4,5	20-49, 1000-3000
	6,7,8,9	50-79, 1000-3000
	11,12,14,15	80-109, 1000-3000
	16,17,18,19	110-139, 1000-3000

型号	能加入同一Group的物理口编号	port-id取值范围
CR8DEENBFED2	1,2,4,5	20-49, 1000-3000
	6,7,8,9	50-79, 1000-3000
	11,12,14,15	80-109, 1000-3000
	16,17,18,19	110-139, 1000-3000
CR8DEANEJYD1	36,37	1000-3000
	38,39	1000-3000
	40,41	1000-3000
	42,43	1000-3000
	44	1000-3000
	45	1000-3000
CR8DEANEJYD2	36,37	1000-3000
	38,39	1000-3000
	40,41	1000-3000
	42,43	1000-3000
	44	1000-3000
	45	1000-3000
CR8DEKNBFED1	0,1,2,3	40-69, 1000-3000
	5,6,8,9	70-99, 1000-3000
	10,11,12,13	100-129, 1000-3000
	15,16,18,19	130-159, 1000-3000
	20,21,22,23	160-189, 1000-3000
	25,26,28,29	190-219, 1000-3000
	30,31,32,33	220-249, 1000-3000
	35,36,38,39	250-279, 1000-3000
CR8DEKNBFED2	0,1,2,3	40-69, 1000-3000
	5,6,8,9	70-99, 1000-3000
	10,11,12,13	100-129, 1000-3000
	15,16,18,19	130-159, 1000-3000
	20,21,22,23	160-189, 1000-3000

型号	能加入同一Group的物理口编号	port-id取值范围
	25,26,28,29	190-219, 1000-3000
	30,31,32,33	220-249, 1000-3000
	35,36,38,39	250-279, 1000-3000
CR8DE4KEFND1	0	1000-3000
	1	1000-3000
	2	1000-3000
	3	1000-3000
	8,9,10,11	1000-3000
	13,14,16,17	1000-3000
	18,19,20,21	1000-3000
	23,24,26,27	1000-3000
CR8DE4KEFND2	0	1000-3000
	1	1000-3000
	2	1000-3000
	3	1000-3000
	8,9,10,11	1000-3000
	13,14,16,17	1000-3000
	18,19,20,21	1000-3000
	23,24,26,27	1000-3000
CR8DE8KE8ND1	0	1000-3000
	1	1000-3000
	2	1000-3000
	3	1000-3000
	8	1000-3000
	9	1000-3000
	10	1000-3000
	11	1000-3000
CR8DE8KE8ND2	0	1000-3000
	1	1000-3000

型号	能加入同一Group的物理口编号	port-id取值范围
	2	1000-3000
	3	1000-3000
	8	1000-3000
	9	1000-3000
	10	1000-3000
	11	1000-3000
CR5D00LFXF70	0	2-21, 1000-3000
	1	22-41, 1000-3000
CR5DEDVE8N72	0,1	8-15, 1000-3000
	2,3	16-23, 1000-3000
	4,5	24-31, 1000-3000
	6,7	32-39, 1000-3000
CR5D00E8NB7R	0,1	8-15, 1000-3000
	2,3	16-23, 1000-3000
	4,5	24-31, 1000-3000
	6,7	32-39, 1000-3000
CR5D00EENB72	0,1	20-39, 1000-3000
	2,3	40-59, 1000-3000
	4	60-69, 1000-3000
	5	70-79, 1000-3000
	6,7	80-99, 1000-3000
	8,9	100-119, 1000-3000
	10,11	120-139, 1000-3000
	12,13	140-159, 1000-3000
	14	160-169, 1000-3000
	15	170-179, 1000-3000
	16,17	180-199, 1000-3000
	18,19	200-219, 1000-3000
CR8D0E5NBCCP	0,1	1000-3000

型号	能加入同一Group的物理口编号	port-id取值范围
	2,3	1000-3000
	4	1000-3000
CR8D0E5NBCDP	0,1	1000-3000
	2,3	1000-3000
	4	1000-3000
CR8DEANBFECP	0,1	1000-3000
	2,3	1000-3000
	4,5	1000-3000
	6,7	1000-3000
	8	1000-3000
	9	1000-3000
CR8DE2KE2NCP	0	1000-3000
	1	1000-3000

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**flexe client-instance** *clientindex* [**flexe-group** *groupIndex* **flexe-type full-function** [**port-id** *portid*]]，创建并进入FlexE Client视图。

步骤3 执行命令**flexe-clientid** *clientid*，配置FlexE Client的Client ID值。

步骤4 配置FlexE Client的带宽。

- 如果FlexE卡的模式为带宽模式，则执行命令**flexe-bandwidth** { **1** | **2** | **3** | **4** | *bandwidth-value* }，配置FlexE Client的带宽。
- 如果FlexE卡的模式为时隙模式，则执行命令**binding interface** *interface-type interface-number* **time-slot** *timeslot-list* [**sub-time-slot** *subtime-slot*]，将一个或多个子时隙绑定到FlexE Client，绑定的时隙即构成FlexE Client的带宽。

步骤5 （可选）执行命令**minimal available bandwidth** *percent*，配置FlexE Client的最小可用带宽比例值。

步骤6 执行命令**commit**，提交配置。

----结束

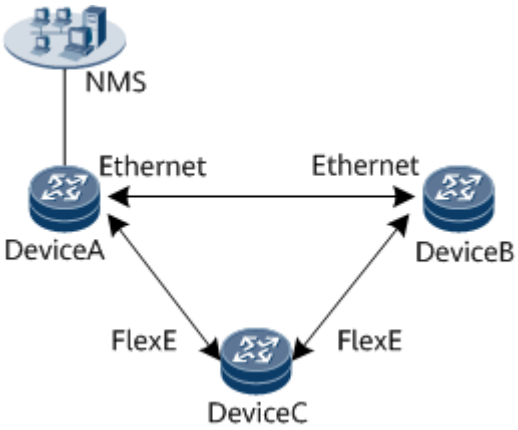
配置 Ethernet 业务场景下增加 FlexE 网元

在现网运行Ethernet业务场景下增加FlexE网元，会涉及到FlexE物理接口与标准Ethernet口对接，如果FlexE物理接口的DCN自协商功能使能，则无需手动干预，两者能够自动连通，网管即可管理到新增网元。

应用环境

如图1-39所示，现网网元DeviceA和DeviceB是标准Ethernet模式，且不支持FlexE物理接口的DCN自协商功能；新增的网元DeviceC为FlexE模式，并支持FlexE物理接口的DCN自协商功能。

图 1-39 现网运行 Ethernet 业务场景增加 FlexE 网元



网元DeviceC加入后，因为命令**undo dcn-auto-negotiation disable**默认使能，即FlexE物理接口的DCN自协商功能默认使能，所以FlexE物理接口的底层工作模式会在10秒左右的时间，自动从FlexE模式切换成标准Ethernet模式，实现DCN连通，网管可以管理到DeviceC。

- 用户如果在20分钟内，针对DeviceC执行如下命令，可立即生效，让DCN持续连通。
  a. 执行命令**force-physical-mode ethernet**，强制切换FlexE物理接口的底层工作模式为标准Ethernet模式。

     说明

     缺省情况下，FlexE物理接口的底层工作模式回切时间是20分钟，即20分钟后会自动从标准Ethernet模式回切成FlexE模式。

  b. 如果需要修改FlexE物理接口的底层工作在标准Ethernet模式的时间或需要让FlexE物理接口的底层工作在标准Ethernet模式不回切，用户可执行如下操作。

     - 执行命令**phyautoclear forcephysicalmode enable** *cleartime*，设置FlexE物理接口的底层工作模式从标准Ethernet模式回切成FlexE模式的时间。
     - 执行命令**phyautoclear forcephysicalmode disable**，取消FlexE物理接口的底层工作模式从标准Ethernet模式回切成FlexE模式。
- 用户如果在20分钟内，针对DeviceC没有执行上述命令，则在第20分钟的时候，DeviceC的FlexE物理接口底层工作模式会从标准Ethernet模式回切成FlexE模式，然后继续等待10秒再进行DCN自协商，实现DCN连通。从而造成DeviceC会暂时脱管10秒左右的时间，如此反复。

如果用户想要修改现网业务为FlexE，请按如下操作步骤执行。

操作步骤

步骤1 在DeviceA上执行命令**flexe enable port** *port-position*，将Ethernet接口从标准以太模式切换为灵活以太模式。由于DeviceC的FlexE物理接口底层工作模式已切换成标准Ethernet模式，此时DeviceA和DeviceC之间DCN不通，DeviceC会脱管。

步骤2 手动修改DeviceA的FlexE物理接口状态，状态的改变会触发与其相连的DeviceC的FlexE物理接口底层模式快速回切成FlexE模式。用户可执行如下操作。

- 在DeviceA上执行命令**laser turn-off**，手动关闭光模块激光器发光功能，然后再执行命令**laser turn-on**，手动打开光模块激光器发光功能。
- 在DeviceA上执行命令**shutdown**，关闭接口，然后再执行命令**undo shutdown**，启动该接口。

完成上述操作后，DeviceC上与DeviceA相连的FlexE物理接口会回切成FlexE模式，两者FlexE对接成功，网管可以继续管理DeviceC。

说明

上述场景中，DeviceB的操作同DeviceA。

----结束

配置 FlexE 业务场景下新增 FlexE 或 Ethernet 网元

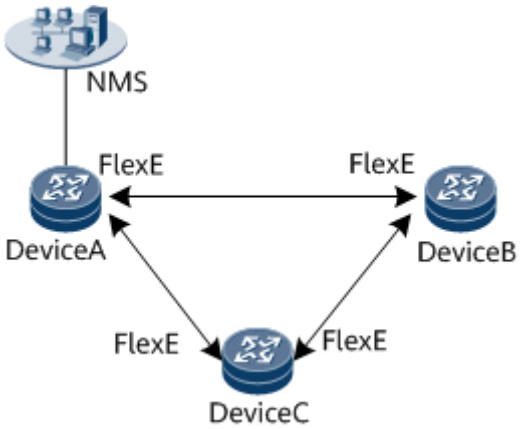
在现网运行FlexE业务场景下增加Ethernet网元，会涉及到FlexE物理接口与标准Ethernet口对接，如果FlexE物理接口的DCN自协商功能使能，则无需手动干预，两者能够自动连通，网管即可管理到新增网元。

应用环境

- 现网运行FlexE业务场景增加FlexE网元

  如图1-40所示，现网网元DeviceA和DeviceB是FlexE模式，新增的网元DeviceC也是FlexE模式。

  图 1-40 现网运行 FlexE 业务场景增加 FlexE 网元

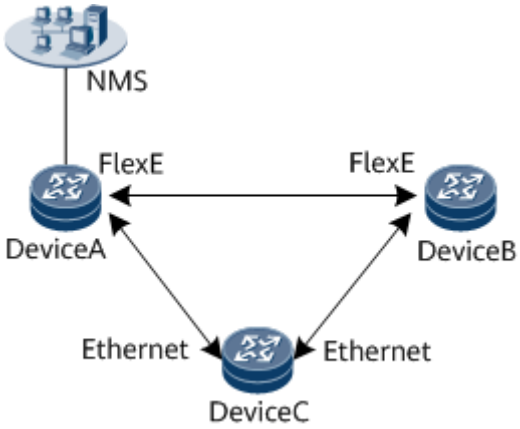
  

  网元DeviceC加入后，因为现网运行的网元和DeviceC都是FlexE模式，所以DeviceC会跟DeviceA和DeviceB直接对接成功，中间也不会出现FlexE物理接口的底层工作模式从FlexE模式自适应成标准Ethernet模式的过程，网管可以直接管理到DeviceC。

- 现网运行FlexE业务场景增加Ethernet网元

  如图1-41所示，现网网元DeviceA和DeviceB是FlexE模式，新增的网元DeviceC是Ethernet模式。

  图 1-41 现网运行 FlexE 业务场景增加 Ethernet 网元

  此种情况有以下几种场景，用户可按如下操作步骤执行相应的操作，确保新增的Ethernet网元能对接成功并被网管管理。

  说明

  下述场景中，DeviceB的操作同DeviceA。

操作步骤

- 如果DeviceA支持FlexE物理接口的DCN自协商功能，DeviceC不支持。

  当DeviceC加入后，由于DeviceA上的命令**undo dcn-auto-negotiation disable**默认使能，即FlexE物理接口的DCN自协商功能默认使能，FlexE物理接口的底层工作模式会在10秒左右的时间，自动从FlexE模式切换成标准Ethernet模式，实现DCN连通，网管可以管理到DeviceC。

  - 用户如果在20分钟内，针对DeviceA执行如下命令，可立即生效，让DCN持续连通。
    i. 执行命令**system-view**，进入系统视图。
    ii. 执行命令**interface** *interface-type interface-number*，进入FlexE物理接口视图，例如FlexE-50G 1/1/1接口。
    iii. 执行命令**force-physical-mode ethernet**，强制切换FlexE物理接口的底层工作模式为标准Ethernet模式。

    说明

    缺省情况下，FlexE物理接口的底层工作模式回切时间是20分钟，即20分钟后会自动从标准Ethernet模式回切成FlexE模式。

    iv. 如果需要修改FlexE物理接口的底层工作在标准Ethernet模式的时间或需要让FlexE物理接口的底层工作在标准Ethernet模式不回切，用户可执行如下操作。
    - 执行命令**phyautoclear forcephysicalmode enable** *cleartime*，设置FlexE物理接口的底层工作模式从标准Ethernet模式回切成FlexE模式的时间。

    - 执行命令**phyautoclear forcephysicalmode disable**，取消FlexE物理接口的底层工作模式从标准Ethernet模式回切成FlexE模式。

  - 用户如果在20分钟内，针对DeviceA没有执行上述命令，则在第20分钟的时候，DeviceA的FlexE物理接口底层工作模式会从标准Ethernet模式回切成FlexE模式，然后继续等待10秒再进行DCN自协商，实现DCN连通。从而造成DeviceC会暂时脱管10秒左右的时间，如此反复。

  如果用户想要现网继续运行FlexE业务，需要做如下操作。

  a. 在DeviceC上执行命令**flexe enable port** *port-position*，将Ethernet接口从标准以太模式切换为灵活以太模式。由于DeviceA的FlexE物理接口底层工作模式已切换成标准Ethernet模式，此时DeviceC和DeviceA之间DCN不通，DeviceC会脱管。
  b. 手动修改DeviceC的FlexE物理接口状态，状态的改变会触发与其相连的DeviceA的FlexE物理接口底层模式快速回切成FlexE模式。用户可执行如下操作。

     - 在DeviceC上执行命令**laser turn-off**，手动关闭光模块激光器发光功能，然后再执行命令**laser turn-on**，手动打开光模块激光器发光功能。
     - 在DeviceC上执行命令**shutdown**，关闭接口，然后再执行命令**undo shutdown**，启动该接口。

  完成上述操作后，DeviceA上与DeviceC相连的FlexE物理接口会回切成FlexE模式，两者FlexE对接成功，网管可以继续管理DeviceC。

- 如果DeviceA支持FlexE物理接口的DCN自协商功能，DeviceC也支持。

  当DeviceC加入后，由于DeviceA上的命令**undo dcn-auto-negotiation disable**默认使能，即FlexE物理接口的DCN自协商功能默认使能，FlexE物理接口的底层工作模式会在10秒左右的时间，自动从FlexE模式切换成标准Ethernet模式，实现DCN连通，网管可以管理到DeviceC。

  因为DeviceC支持FlexE物理接口的DCN自协商功能且默认使能，所以用户想要现网继续运行FlexE业务，就在DeviceC上执行命令**flexe enable port** *port-position*，将Ethernet接口从标准以太模式切换为灵活以太模式即可。

- 如果DeviceA不支持FlexE物理接口的DCN自协商功能，DeviceC支持。

  当DeviceC加入后，用户在DeviceA上执行命令**force-physical-mode ethernet**，强制切换FlexE物理接口的底层工作模式为标准Ethernet模式，实现DeviceC和DeviceA的DCN互通，并让网管可以管理到DeviceC。

  如果用户想要现网继续运行FlexE业务，需要做如下操作。

  a. 在DeviceC上执行命令**flexe enable port** *port-position*，将Ethernet接口从标准以太模式切换为灵活以太模式。因为DeviceC支持FlexE物理接口的DCN自协商功能且默认使能，所以FlexE物理接口的底层工作模式会在10秒左右的时间，自动从FlexE模式切换成标准Ethernet模式。
  b. 在DeviceA上执行命令**undo force-physical-mode**，恢复FlexE物理接口的底层工作模式为FlexE模式。
  c. 手动修改DeviceA的FlexE物理接口状态，状态的改变会触发与其相连的DeviceC的FlexE物理接口底层模式快速回切成FlexE模式。用户可执行如下操作。

     - 在DeviceA上执行命令**laser turn-off**，手动关闭光模块激光器发光功能，然后再执行命令**laser turn-on**，手动打开光模块激光器发光功能。

- 在DeviceA上执行命令**shutdown**，关闭接口，然后再执行命令**undo shutdown**，启动该接口。

完成上述操作后，DeviceC上与DeviceA相连的FlexE物理接口会回切成FlexE模式，两者FlexE对接成功，网管可以继续管理DeviceC。

----结束

（可选）配置 FlexE 物理接口的时间同步模式

FlexE标准定义了两种1588v2报文承载模式：OH（OverHead）模式和Client模式，缺省情况下，1588v2报文通过OH模式承载。

背景信息

- OH模式：指时钟报文走FlexE的开销时隙，时钟同步的相关配置和标准Ethernet接口下的配置相同。
- Client模式：指时钟报文走FlexE Client，需要在部署时钟业务的FlexE物理接口上绑定承载时钟业务的FlexE接口才能生效。

前置任务

不管1588v2报文采用哪种模式承载，首先需要完成1588v2配置，具体配置过程请参见《HUAWEI NetEngine 8100 X, NetEngine 8000 X, NetEngine 8000E X系列路由器配置指南-系统管理》。

在FlexE物理接口下完成1588v2配置后，1588v2报文承载模式即是默认的OH模式，如果用户想把1588v2报文承载模式变成Client模式，可以执行如下步骤。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**interface** *interface-type interface-number*，进入FlexE物理接口视图，例如FlexE-50G 1/0/0接口。

步骤3 执行命令**clock binding flexe interface** *iftype ifnum*，配置FlexE物理接口绑定承载时钟业务的FlexE接口。

步骤4 执行命令**commit**，提交配置。

----结束

检查配置结果

配置FlexE接口后，需要检查配置结果，保证配置正确。

前提条件

已经完成FlexE接口的所有配置。

操作步骤

- 使用**display flexe group information slot** *slot-id* **card** *card-id*命令查看FlexE卡的Group信息。

- 请选择如下命令之一查看FlexE业务口信息、FlexE物理口信息以及绑定FlexE Group中的物理口信息：
  - **display flexe client information** [**interface** { *interface-type interface-number* | *interface-name* }]
  - **display flexe client information** [**index** *clientindex*]
  - **display flexe physical-interface information** [**interface** { *interface-type interface-number* | *interface-name* }]]
- 使用**display interface ethernet brief**命令查看FlexE接口的简要信息。
- 使用**display interface flexe** *interface-number*命令查看FlexE接口的运行状态和统计信息。
- 使用**display lldp neighbor brief**命令查看FlexE接口的LLDP邻居节点的简要信息。

----结束

1.1.1.2.19 端口组配置

端口组实现为多个接口批量配置命令的功能，减少单独配置的输入错误，同时节省人力。

背景信息

端口组可以分为永久端口组和临时端口组，它们实现的功能基本相同，即都可以将多个接口加入到端口组中，实现在这些接口下批量配置命令。其区别在于：

- 用户退出临时端口组后，该临时端口组被系统自动删除；而永久端口组不会被自动删除，需要通过**undo port-group**命令删除。
- 永久端口组的信息可以通过命令**display port-group**查看，而临时端口组的信息无法查看。
- 永久端口组配置会生成配置文件，但是临时端口组配置后不会生成。

操作步骤

- 配置永久端口组：
  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**port-group** *port-group-name*，创建一个永久端口组并进入端口组视图。
  c. 执行命令**group-member** { *interface-type interface-number1* [**to** *interface-type interface-number2*] } &<1-10>，将指定的接口添加到永久端口组中。
  d. 执行命令**commit**，提交配置。
- 配置临时端口组：
  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**port-group group-member** { *interface-type-start interface-number-start* [**to** *interface-type-end* | *interface-number-end*] } &<1-10>，创建一个临时端口组，并将指定的接口添加到临时端口组中。

     说明

     - 永久端口组下，下发**shutdown**或者**undo shutdown**命令，commit之后不保存到配置文件。

c. 执行命令**commit**，提交配置。

----结束

检查配置结果

完成配置后，可以执行命令**display port-group** [**all** | *port-group-name*]查看端口组的状态信息。

1.1.1.2.20 配置接口监控组

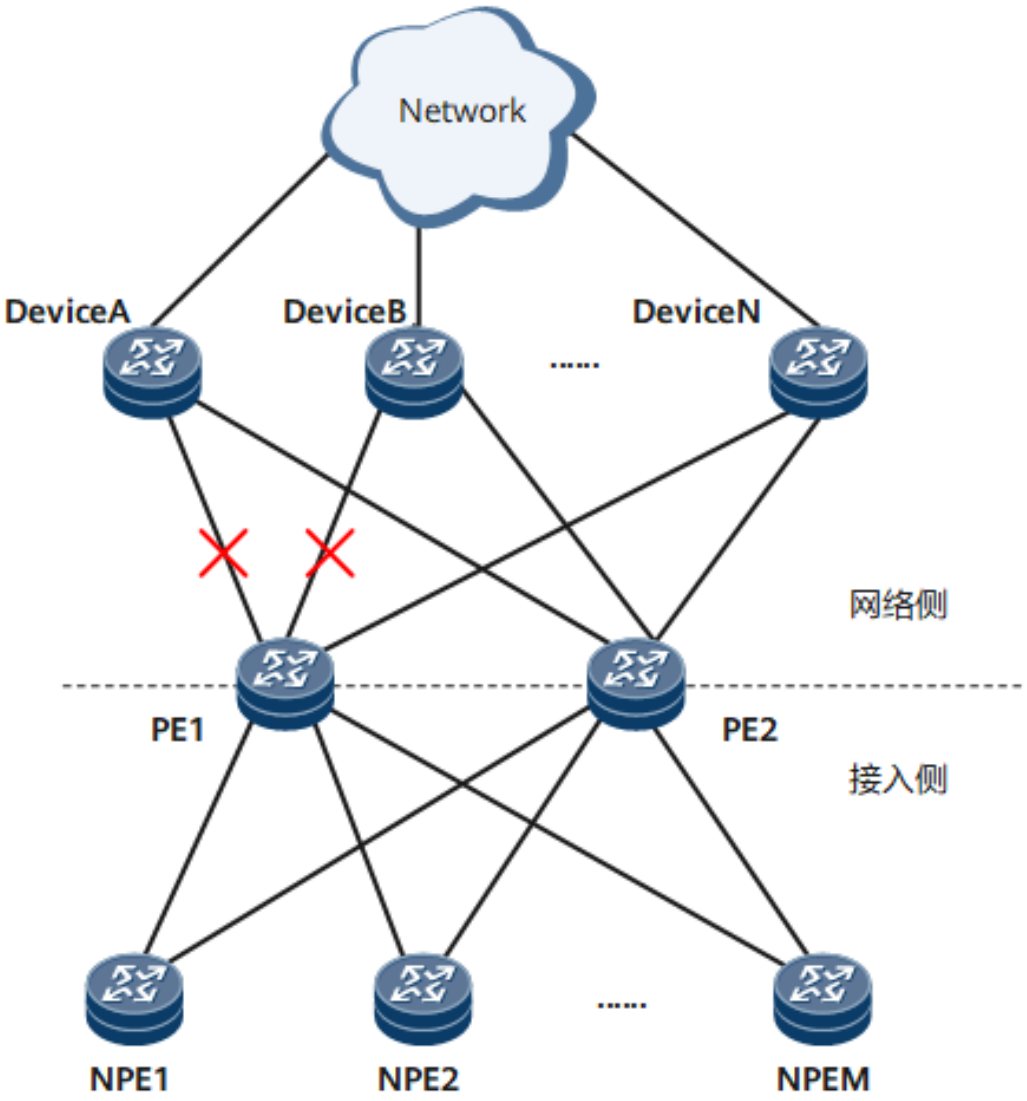
在双机备份的场景中，通过配置接口监控组，根据网络侧接口的状态变化来触发接入侧接口的状态变化，以此达到接入侧主备链路切换的目的。

应用环境

在双机备份的场景中，当网络侧接口故障时，接入侧设备感知不到故障的发生，不会将业务切换到备份链路，可能导致流量过载或者转发不通。在这种情况下，可以配置接口监控组，通过接口监控组管理网络侧接口的状态，使接入侧接口能够及时感知到故障已发生，从而业务及时触发主备链路倒换，避免流量过载或者丢失的情况发生。

如**图1-421**所示，PE2是PE1的备份设备，M个NPE双归属到2个PE设备来实现链路负载分担，网络侧PE设备接入到N个路由器。当PE1和DeviceA之间、PE1和DeviceB之间的链路均故障时，网络侧仅剩余PE1和DeviceN之间的链路，NPE设备感知不到该故障的产生，不会相应切换接入侧链路到PE2，仍然通过PE1向DeviceN发送报文，而由于网络侧可用链路数量的减少，可能会造成流量过载。

图 1-42 接口监控组典型应用组网图



这种情况下，在PE设备上部署接口监控组，将网络侧PE设备的多个接口加入接口监控组中。当网络侧发生链路故障时，通过接口监控组监控网络侧接口的状态，实现一定比例的网络侧接口状态变化时，PE设备接入侧相应接口的状态变化，使接入侧链路发生主备链路切换，从而避免流量过载，保障业务的通畅。

前置任务

在配置接口监控组之前，需完成路由器接口物理属性的配置。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**monitor-group** *monitor-group-name*，创建接口监控组，并进入接口监控组视图。

步骤3 执行命令**binding interface** *interface-type interface-number* [**down-weight** *down-weight-value*]，将接口加入到接口监控组中。

加入接口监控组中的接口称为Binding接口。Binding接口一般是网络侧接口，Track接口一般是接入侧接口。接口监控组通过对Binding接口状态的监控，实现Track接口状态的变化。

重复执行本步骤，可以将多个Binding接口加入同一个接口监控组中。

步骤4 执行命令**quit**，退出接口监控组视图。

步骤5 执行命令**interface** *interface-type interface-number*，进入接入侧指定接口视图。

步骤6 执行命令**track monitor-group** *monitor-group-name* [**trigger-down-weight** *trigger-down-weight-value*]，配置接口监视接口监控组。

监视接口监控组的接口称为Track接口。

重复执行第5步和第6步，可以将多个Track接口监控同一个接口监控组。

当接口监控组中所有Binding接口的Down权重值之和大于或等于Track接口的*trigger-down-weight-value*值时，就会触发对应Track接口的状态变为Down，从而将业务切换到备份链路上；当接口监控组中所有Binding接口的Down权重值之和小于Track接口的*trigger-down-weight-value*值时，对应Track接口的状态恢复为Up，业务回切到主用链路。

步骤7 执行命令**quit**，退出接口视图。

步骤8 执行命令**monitor-group** *monitor-group-name*，进入已创建的接口监控组视图。

步骤9 （可选）执行命令**trigger-up-delay** *trigger-up-delay-value*，配置Track接口延迟恢复Up的时间。

步骤10 执行命令**monitor enable**，启动接口监控组和接口的联动功能。

步骤11 执行命令**commit**，提交配置。

----结束

检查配置结果

执行命令**display monitor-group** [*monitor-group-name*]，查看接口监控组的相关信息。

1.1.1.2.21 配置去使能板间心跳联动端口状态表功能

板间心跳联动端口状态表（PST）功能默认开启，可通过配置去使能板间心跳联动端口状态表功能进行关闭。

应用环境

板间心跳是通过单板间定时发送心跳报文来检测硬件故障的机制。当设备上某单板发生故障时，其他单板可通过板间心跳快速感知此单板故障，从而联动刷新与此故障单板相关的端口状态表为Down，使流量快速切换到非故障链路。若联动功能出现异常时，可以去使能板间心跳联动端口状态表功能。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**pst board-fast-switch disable**，去使能板间心跳联动端口状态表功能。

步骤3 执行命令**commit**，提交配置。

----结束

1.1.1.2.22 维护接口

使用清除统计信息命令，对定位接口故障有帮助。

清除统计信息

当需要统计一定时间内某接口的流量信息，这时必须在统计开始前清除该接口原有的统计信息，使接口重新进行统计。

背景信息

须知

清除计数器信息后，以前的信息将无法恢复，务必仔细确认。

操作步骤

- 在确认需要清除接口的流量统计信息后，请在用户视图下执行命令**reset counters interface**。
- 如果需要清除接口历史保存的峰值速率值，获取后续时间内的峰值速率，请在用户视图下执行命令**reset counters peak-rate interface**。

----结束

监控接口信息

监控接口统计信息，方便用户通过流量和速率分析网络状况。

操作步骤

- 在任意视图下执行命令**monitor interface-statistics** *interface-type interface-number* &<1–5> [**interval** *interval-value* | **times** { *times-value* | **infinity** }] *，监控接口当前的流量统计信息。
- 在任意视图下执行命令**monitor interface-statistics batch** [*interface-type* [*interface-number-begin* [**to** *interface-number-end*]]] [**interval** *interval-value* | **times** { *times-value* | **infinity** }] * [**main**]，批量监控接口当前的流量统计信息。
- 在任意视图下执行命令**monitor interface-information interface** *interface-type interface-number* [**interval** *interval-value* | **times** { *times-value* | **infinity** }] *，监控指定接口的详细信息，包括运行状态和统计信息。
- 在任意视图下执行命令**monitor counters bit** [**rate**] **interface** *interface-type interface-number* [**interval** *interval-value* | **times** { *times-value* | **infinity** }]

*，监控接口的报文个数或报文速率，包括接口入方向/出方向的总字节数以及单播、组播和广播报文总数或报文速率。

----结束

1.1.1.2.23 接口管理配置举例

通过以下举例，您可以了解到接口管理的基本使用。

管理接口示例

通过接口管理示例，您可以了解到如何配置接口的描述信息、MTU、流量统计时间间隔等内容。

组网需求

为了保证网络中各设备间更好地通信，需要物理接口和逻辑接口配合使用，并且根据不同的实际需求对各接口进行参数的配置，如配置描述信息、MTU值、接口出入带宽利用率的告警阈值、流量统计时间间隔以及使能接口协议状态变化时向网管发送Trap、控制接口震荡等功能。

配置思路

采用如下的思路配置接口：

1. 配置接口的描述信息，便于用户识别接口。
2. 配置接口的MTU，保证接口每次发送的报文都能够畅通无阻的到达接收端，确保报文发送一次成功。
3. 配置全局流量统计时间间隔，便于用户统计接口流量和速率。
4. 创建子接口并配置MTU，保证子接口每次发送的报文都能够畅通无阻的到达接收端，确保报文发送一次成功。

数据准备

为完成此配置举例，需要准备如下数据：

- 接口名称
- 接口的描述信息
- 接口的MTU
- 全局流量统计时间间隔
- 子接口的MTU

操作步骤

步骤1 配置接口的描述信息。

```
<HUAWEI> system-view
[~HUAWEI] interface gigabitethernet 2/0/0
[~HUAWEI-GigabitEthernet2/0/0] description for IFM
[*HUAWEI-GigabitEthernet2/0/0] commit
```

步骤2 配置接口MTU。

```
[~HUAWEI-GigabitEthernet2/0/0] mtu 1000
[*HUAWEI-GigabitEthernet2/0/0] commit
```



```
[~HUAWEI-GigabitEthernet2/0/0] quit
```

步骤3 配置全局流量统计时间间隔。

```
[~HUAWEI] set flow-stat interval 100
[*HUAWEI] commit
```

步骤4 创建子接口并配置子接口的MTU。

```
[~HUAWEI] interface gigabitethernet 2/0/0.1
[*HUAWEI-GigabitEthernet2/0/0.1] mtu 800
[*HUAWEI-GigabitEthernet2/0/0.1] commit
```

----结束

配置文件

```
#
set flow-stat interval 100
#
interface Gigabitethernet2/0/0
 description for IFM
 mtu 1000
#
interface Gigabitethernet2/0/0.1
 mtu 800
#
return
```

配置 FlexE 接口示例

本例介绍采用FlexE技术对接的两端设备上的接口配置。

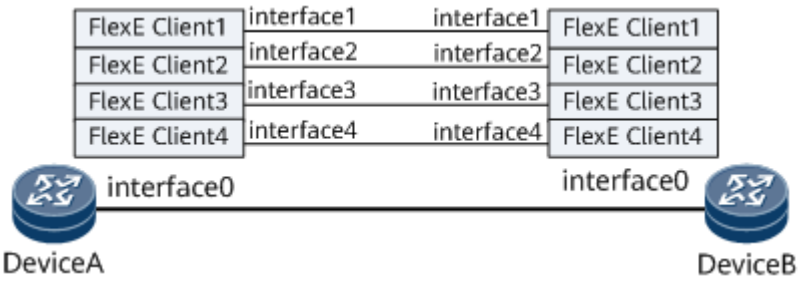
组网需求

如图1-43所示，DeviceA与DeviceB之间通过FlexE技术创建FlexE Client进行通信，不同的FlexE Client配置不同的带宽，满足多样化的业务和应用场景，要求FlexE Client1的带宽为4G，FlexE Client2的带宽为5G，FlexE Client3的带宽为15G，FlexE Client4的带宽为20G。

图 1-43 配置 FlexE 接口组网图

说明

本示例中interface0，interface1，interface2，interface3，interface4分别代表FlexE-50G 1/1/1，FlexE 1/1/129，FlexE 1/1/130，FlexE 1/1/131，FlexE 1/1/132。



配置注意事项

在配置过程中，需注意以下事项：

- 为保证对接的两端设备正常通信，用户需要在两端设备的FlexE物理接口上分别配置相同的PHY Number值。

- 为保证对接的两端设备正常通信，用户需要将两端设备上FlexE物理接口加入的FlexE Group配置相同的Group ID。
- 为保证对接的两端设备的FlexE Client正常通信，用户需要将两端设备上FlexE Client的Client ID和带宽配置一致。

配置思路

配置思路如下：

1. 激活单板的灵活以太端口License。
2. 配置标准Ethernet接口为灵活以太模式。
3. 配置FlexE物理接口的PHY Number。
4. 创建FlexE Group并绑定FlexE物理接口。
5. 配置FlexE Group的Group ID。
6. 配置FlexE卡的子时隙粒度。
7. 创建FlexE Client并配置Client ID和带宽。
8. 配置各接口的IP地址。

数据准备

为完成此配置例，需准备如下的数据：

- FlexE物理接口的PHY Number为5。
- FlexE Group的索引为1。
- FlexE Group的Group ID为2345。
- FlexE卡的子时隙粒度为1G。
- 四个FlexE接口的Port ID为interface1、interface2、interface3和interface4的接口编号最后一位。
- 四个FlexE Client的Client ID为1、2、3、4，分别对应带宽为4G、5G、15G、20G。

操作步骤

步骤1 激活单板的灵活以太端口License。

```
<DeviceA> license active XXXXX.dat
<DeviceA> system-view
[~DeviceA] license
[~DeviceA-license] active port-basic slot 1 card 1 port 1
[*DeviceA-license] active port-slicing slot 1 card 1 port 1
[*DeviceA-license] commit
[~DeviceA-license] quit
```

步骤2 配置标准Ethernet接口为灵活以太模式。

```
[~DeviceA] flexe enable port 1/1/1
Warning: This operation will delete interface 50G1/1/1 and related services. Continue? [Y/N]:y
[*DeviceA] commit
```

步骤3 配置FlexE物理接口的PHY Number。

```
[~DeviceA] interface FlexE-50G 1/1/1
[~DeviceA-FlexE-50G1/1/1] phy-number 5
Warning: The traffic on this interface may be interrupted if the operation is performed. Continue? [Y/N]:y
[*DeviceA-FlexE-50G1/1/1] commit
[~DeviceA-FlexE-50G1/1/1] quit
```


步骤4 创建FlexE Group并绑定FlexE物理接口。

```
[~DeviceA] flexe group 1
[*DeviceA-flexe-group-1] binding interface FlexE-50G1/1/1
```

步骤5 配置FlexE Group的Group ID。

```
[*DeviceA-flexe-group-1] flexe-groupnum 2345
Warning: The traffic on related clients may be interrupted if the operation is performed. Continue? [Y/N]:y
[*DeviceA-flexe-group-1] commit
[~DeviceA-flexe-group-1] quit
```

步骤6 配置FlexE卡的子时隙粒度。

```
[~DeviceA] set flexe sub-time-slot granula slot 1 card 1 1g
[*DeviceA] commit
```

步骤7 创建FlexE Client并配置Client ID和带宽。

```
[~DeviceA] flexe client-instance 1 flexe-group 1 flexe-type full-function port-id 129
[*DeviceA-flexe-client-1] flexe-clientid 1
Warning: The traffic on this interface may be interrupted if the operation is performed. Continue? [Y/N]:y
[*DeviceA-flexe-client-1] flexe-bandwidth 4
[*DeviceA-flexe-client-1] commit
[~DeviceA-flexe-client-1] quit
[~DeviceA] flexe client-instance 2 flexe-group 1 flexe-type full-function port-id 130
[*DeviceA-flexe-client-2] flexe-clientid 2
Warning: The traffic on this interface may be interrupted if the operation is performed. Continue? [Y/N]:y
[*DeviceA-flexe-client-2] flexe-bandwidth 5
[*DeviceA-flexe-client-2] commit
[~DeviceA-flexe-client-2] quit
[~DeviceA] flexe client-instance 3 flexe-group 1 flexe-type full-function port-id 131
[*DeviceA-flexe-client-3] flexe-clientid 3
Warning: The traffic on this interface may be interrupted if the operation is performed. Continue? [Y/N]:y
[*DeviceA-flexe-client-3] flexe-bandwidth 15
[*DeviceA-flexe-client-3] commit
[~DeviceA-flexe-client-3] quit
[~DeviceA] flexe client-instance 4 flexe-group 1 flexe-type full-function port-id 132
[*DeviceA-flexe-client-4] flexe-clientid 4
Warning: The traffic on this interface may be interrupted if the operation is performed. Continue? [Y/N]:y
[*DeviceA-flexe-client-4] flexe-bandwidth 20
[*DeviceA-flexe-client-4] commit
[~DeviceA-flexe-client-4] quit
```

步骤8 配置各接口的IP地址（略）。

步骤9 在DeviceB上，重复操作如上DeviceA的全部步骤，具体配置请参见**配置文件**。

步骤10 检查配置结果

上述配置成功后，在DeviceA和DeviceB上执行**display flexe group information**命令，查看FlexE卡的Group信息。以DeviceA显示为例。

```
[~DeviceA] display flexe group information slot 9 card      1
FlexE Card Info:
============================================================
FlexE Config Mode              : Bandwidth
============================================================

FlexE Group Info:
============================================================
GroupID    Total Bandwidth(M)    Valid Bandwidth(M)
------------------------------------------------------------
1              50000              50000
============================================================

FlexE Group Binding Interfaces Capability:
============================================================
------------------------------------------------------------
GroupID   Interfaces already bound  Interfaces can be bound
------------------------------------------------------------
```



```
1        FlexE-50G1/1/1
------------------------------------------------------------
============================================================

FlexE Phy Info:
============================================================
Port No             : FlexE-50G1/1/1
Active Status       : 1
Cfg Group ID        : 1
Cfg Group No        : 2345
Real TX Group No    : 2345
Real RX Group No    : 2345
Remote Group No     : 2345
Cfg Phy No          : 5
Real TX Phy No      : 5
Real RX Phy No      : 5
Remote Phy No       : 5
============================================================

FlexE Time Slot Info:
============================================================

------------------------------------------------------
port-no             : FlexE-50G1/1/1
ts-num              : 20
sub-ts-num          : 5
------------------------------------------------------
 time-slot-id      ts-port-map
------------------------------------------------------
   0:              [129][129][129][129][130]
   1:              [130][130][130][130][131]
   2:              [131][131][131][131][131]
   3:              [131][131][131][131][131]
   4:              [131][131][131][131][132]
   5:              [132][132][132][132][132]
   6:              [132][132][132][132][132]
   7:              [132][132][132][132][132]
   8:              [132][132][132][132][-]
   9:              [-][-][-][-][-]
  10:              [-][-][-][-][-]
  11:              [-][-][-][-][-]
  12:              [-][-][-][-][-]
  13:              [-][-][-][-][-]
  14:              [-][-][-][-][-]
  15:              [-][-][-][-][-]
  16:              [-][-][-][-][-]
  17:              [-][-][-][-][-]
  18:              [-][-][-][-][-]
  19:              [-][-][-][-][-]
============================================================

FlexE Client Info:
============================================================
------------------------------------------------------
Instance Index           Port Name
------------------------------------------------------
129                      FlexE1/1/129
130                      FlexE1/1/130
131                      FlexE1/1/131
132                      FlexE1/1/132
------------------------------------------------------
============================================================
```

在DeviceA和DeviceB上执行**display interface ethernet brief**命令，查看FlexE接口的简要信息。以DeviceA显示为例。

```
[~DeviceA] display interface ethernet brief
PHY: Physical
*down: administratively down
^down: standby
```



```
(l): loopback
(b): BFD down
(d): Dampening Suppressed
(p): port alarm down
InUti/OutUti: input utility/output utility
Interface                PHY   Auto-Neg Duplex Bandwidth  InUti OutUti Trunk
FlexE1/1/129               up    -       full        4G  0.01%  0.01%    --
FlexE1/1/130               up    -       full        5G  0.01%  0.01%    --
FlexE1/1/131               up    -       full       15G  0.01%  0.01%    --
FlexE1/1/132               up    -       full       20G  0.01%  0.01%    --
FlexE-50G1/1/1              up    -       full       50G     --     --    --
```

在DeviceA和DeviceB上执行**display lldp neighbor brief**命令，查看FlexE接口的LLDP邻居节点的简要信息。以DeviceA显示为例。

```
[~DeviceA] display lldp neighbor brief
Local Intf              Neighbor Dev        Neighbor Intf       Exptime (sec)
--------------------------------------------------------------------------------
FlexE1/1/129              DeviceB           FlexE1/1/129              114
FlexE1/1/130              DeviceB           FlexE1/1/130              114
FlexE1/1/131              DeviceB           FlexE1/1/131              114
FlexE1/1/132              DeviceB           FlexE1/1/132              114
FlexE-50G1/1/1             DeviceB           FlexE-50G1/1/1             95
```

在DeviceA和DeviceB上执行**display interface flexe** *interface-number*命令，查看FlexE接口的运行状态和统计信息。以DeviceA的FlexE1/1/129接口显示为例。

```
[~DeviceA] display interface flexe 1/1/129
FlexE1/1/129 current state : UP (ifindex: 285)
Line protocol current state : UP
Last line protocol up time : 2021-03-11 09:11:24
Link quality grade : GOOD
Description:
Route Port,The Maximum Transmit Unit is 1500
Internet Address is 10.1.1.1/24
IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is 00e0-fc12-3456
Port BW: 4G
Pause Flowcontrol: Receive Enable and Send Enable
Client-id Match State: Match
Last physical up time   : 2021-03-10 15:11:46
Last physical down time : 2021-03-10 15:11:29
Current system time: 2021-03-11 11:36:52
Statistics last cleared:never
    Last 300 seconds input rate: 10031 bits/sec, 1 packets/sec
    Last 300 seconds output rate: 10041 bits/sec, 1 packets/sec
    Input peak rate 125150137 bits/sec, Record time: 2021-03-10 09:25:57
    Output peak rate 125757954 bits/sec, Record time: 2021-03-10 09:25:57
    Input: 7006191780 bytes, 52343200 packets
    Output: 7024402448 bytes, 52482810 packets
    Input:
      Unicast: 52334185 packets, Multicast: 9010 packets
      Broadcast: 5 packets, JumboOctets: 0 packets
      CRC: 0 packets, Symbol: 0 packets
      Overrun: 0 packets, InRangeLength: 0 packets
      LongPacket: 0 packets, Jabber: 0 packets, Alignment: 0 packets
      Fragment: 0 packets, Undersized Frame: 0 packets
      RxPause: 0 packets
    Output:
      Unicast: 52473465 packets, Multicast: 9334 packets
      Broadcast: 11 packets, JumboOctets: 0 packets
      Lost: 0 packets, Overflow: 0 packets, Underrun: 0 packets
      System: 0 packets, Overruns: 0 packets
      TxPause: 0 packets
    Last 300 seconds input utility rate:  0.01%
    Last 300 seconds output utility rate: 0.01%
```

----结束

配置文件

- DeviceA的配置文件

```
#
sysname DeviceA
#
set flexe sub-time-slot granula slot 1 card 1 1g
flexe enable port 1/1/1
#
flexe group 1
 flexe-groupnum 2345
 binding interface FlexE-50G1/1/1
#
flexe client-instance 1 flexe-group 1 flexe-type full-function port-id 129
 flexe-clientid 1
 flexe-bandwidth 4
#
flexe client-instance 2 flexe-group 1 flexe-type full-function port-id 130
 flexe-clientid 2
 flexe-bandwidth 5
#
flexe client-instance 3 flexe-group 1 flexe-type full-function port-id 131
 flexe-clientid 3
 flexe-bandwidth 15
#
flexe client-instance 4 flexe-group 1 flexe-type full-function port-id 132
 flexe-clientid 4
 flexe-bandwidth 20
#
license
 active port-basic slot 1 card 1 port 1
 active port-slicing slot 1 card 1 port 1
#
interface FlexE-50G1/1/1
 undo shutdown
 undo dcn
 phy-number 5
#
return
```

- DeviceB的配置文件

```
#
sysname DeviceB
#
flexe enable port 1/1/1
#
flexe group 1
 flexe-groupnum 2345
 binding interface FlexE-50G1/1/1
#
flexe client-instance 1 flexe-group 1 flexe-type full-function port-id 129
 flexe-clientid 1
 flexe-bandwidth 4
#
flexe client-instance 2 flexe-group 1 flexe-type full-function port-id 130
 flexe-clientid 2
 flexe-bandwidth 5
#
flexe client-instance 3 flexe-group 1 flexe-type full-function port-id 131
 flexe-clientid 3
 flexe-bandwidth 15
#
flexe client-instance 4 flexe-group 1 flexe-type full-function port-id 132
 flexe-clientid 4
 flexe-bandwidth 20
#
license
 active port-basic slot 1 card 1 port 1
 active port-slicing slot 1 card 1 port 1
#
```



```
interface FlexE-50G1/1/1
 undo shutdown
 undo dcn
 phy-number 5
#
return
```

1.1.2 传输告警定制与抑制配置

1.1.2.1 传输告警定制与抑制特性描述

1.1.2.1.1 传输告警定制与抑制介绍

定义

当前电信级网络对IP设备网络可靠性的要求越来越高，因此要求网络中的设备能够快速检测到故障信息。当接口启动快速检测功能后，告警信息上报速度加快，会引起接口的物理层状态频繁在Up和Down之间切换，导致网络反复振荡。因而需要对告警进行过滤和抑制，避免网络频繁振荡。

传输告警抑制功能可以有效实现对告警信号进行过滤和抑制，避免接口的反复振荡。同时提供告警定制功能，使得告警对接口状态变化的影响可以有效控制。

传输告警定制与抑制具体实现的功能如下：

- 传输告警定制：可以定制哪些告警才能够引起接口的物理层状态变化，起到告警过滤效果。
- 传输告警抑制：通过设置门限值，通过一系列算法来抑制网络反复振荡。

目的

用户可以根据需求定制传输告警，从而过滤掉不在定制范围内的传输告警。传输告警抑制功能对定制的告警设定门限值，从而忽略传输链路保护等产生的毛刺。避免网络频繁振荡。

在骨干网或城域网中，IP路由设备要与传输设备进行对接(一般的传输设备有SDH（Synchronous Digital Hierarchy）、SONET（Synchronous Optical Network）等)。当传输设备发生故障时，在IP路由设备上会接收到一些告警，之后传输设备会进行链路倒换，待传输设备的链路正常后会向IP路由设备发出告警清除。传输设备从发生告警到告警消除的保护时间通常是50ms～200ms。从IP路由设备上来看，这通常是一个50ms～200ms内的毛刺。这些毛刺会导致IP路由设备接口状态频繁变化，导致路由设备频繁的进行路由计算，造成路由振荡的情况，对路由设备的性能造成影响。

从网络整体角度来看，希望IP路由设备能够忽略这样的毛刺，不做任何处理。也就是说在传输设备进行维护或者传输设备进行链路保护时，路由设备要通过对传输设备产生的告警采取定制与抑制手段，从而不产生路由振荡，保证路由设备的稳定运行。传输告警定制功能可以使告警对接口的物理层状态的影响得到控制。传输告警抑制功能可以有效实现对特定告警信号进行过滤和抑制，避免接口反复振荡。

在主备倒换过程中，系统可以正常处理传输告警的各种告警信号，传输告警的配置也依然生效。

1.1.2.1.2 传输告警定制与抑制原理描述

基本概念

网络震荡

网络震荡是指当接口启动快速检测功能后，因为告警信息上报速度加快，引起接口的物理层状态频繁在Up和Down之间切换，导致网络反复振荡。

告警毛刺

所谓告警毛刺是指在很短的时间内收到成对的告警产生信号和告警消除信号。即，在很短一段时间内，告警产生了又消失或者消失了又产生的过程称为告警毛刺。

这里所指的“很短的一段时间”是和实际应用场景有关的。对于不同的设备或不同的业务类型要求的时间段也不同。

例如LOS（Loss of Signal）告警产生50ms后又消失，这个告警产生消失的过程就可以称为毛刺。

告警振荡

很短一段时间内，告警产生又消失或者消失又产生，如此反复的过程称为告警振荡。

这里所指的“很短的一段时间”也和实际应用场景有关的。对于不同的设备或不同的业务类型要求的时间段也不同。

例如1秒内LOS告警产生消失交替出现了10次，这个过程就称为告警振荡。

抑制振荡的关键值

- figure of merit：稳定值。给每个告警设置的值。稳定值越大说明该告警越不稳定。
- penalty：惩罚值。当某个接口的某个告警发生振荡时，就给予其惩罚。告警产生信号每到达一次就将其稳定值增加一个惩罚值。告警消除信号每到达一次，稳定值进行一次指数衰减计算。
- suppress：告警抑制门限值。当告警抑制稳定值超过此值时，告警被抑制。它必须小于告警稳定最高上限值，大于告警重用门限值。
- reuse：告警重用门限值。当告警稳定值小于此值时，告警抑制被解除。它必须小于告警抑制门限值。
- ceiling：告警稳定最高上限值。当某告警的产生和消除信息在短时间内频繁出现时，稳定值会非常高。当告警稳定后，稳定值回到reuse门限的时间会非常长，为了避免这么长的时间，故设置了稳定值最高上限。当告警抑制稳定值超过此值时，告警抑制稳定值不再增加。它必须大于告警抑制门限值。
- half-time：半衰期。被抑制的告警每经过一段时间，稳定值便会减少一半，这个时间称为半衰期。
- decay-ok：告警消失时的半衰期。设定当是告警消失信号时，稳定值衰减到1/2所用时间。
- decay-ng：告警产生时的半衰期。设定当是告警产生信号时，稳定值衰减到1/2所用时间。

传输告警的处理过程

对传输设备产生的告警的处理过程如下：

1. 当传输设备产生告警后，根据告警的类型判断是否直接上报系统。
   - 如果告警类型是b3tca、sdbere或sfbere，则需要判断是否达到告警门限值。
     如果达到告警门限值，则上报系统处理。
     如果没有达到告警门限值，则忽略该告警，不做任何处理。
   - 如果是其他告警，产生后直接上报系统处理。
2. 当告警上报到系统时，用户还可以配置是否记录日志。如果使能对某类告警进行记录日志的功能，只要有该类告警的日志，都会被记录下来。
3. 当告警上报到系统后，根据用户定制的告警类型判断是否对接口的物理状态产生影响。
   - 如果用户没有定制某类告警可以影响接口的物理层状态，则该告警被忽略，接口的物理层状态不受影响。
   - 当用户定制了某类告警影响接口的物理层状态，则进入下面的传输告警定制处理过程。

传输告警定制处理过程

当传输设备的告警信号上报到系统后，可以通过传输告警定制功能控制告警对接口的物理层状态的影响。

当用户定制了某类告警可以影响接口的物理层状态后，

- 如果没有配置传输告警过滤功能或传输告警抑制功能，
  - 当告警产生时，接口的物理层状态变为Down。
  - 当告警消失时，接口的物理层状态变为Up。
- 如果配置了传输告警过滤功能或传输告警抑制功能，当有告警信号时，系统会根据过滤或抑制功能的参数处理该告警。

传输告警过滤处理过程

如果用户配置了传输告警定制功能，当告警信号到达后，可以通过传输告警过滤功能判断该告警信号是不是毛刺。

如果告警产生信号与告警消失信号的时间间隔小于过滤定时器的时间，就认为该告警信号是毛刺。

- 当告警信号是毛刺时，该告警信号被忽略，同时不会影响接口的物理层状态。
- 当告警信号不是毛刺时：
  - 如果是告警产生信号，接口的物理层状态变为Down。
  - 如果是告警消失信号，且告警没有被抑制，接口的物理层状态变为Up。

传输告警抑制处理过程

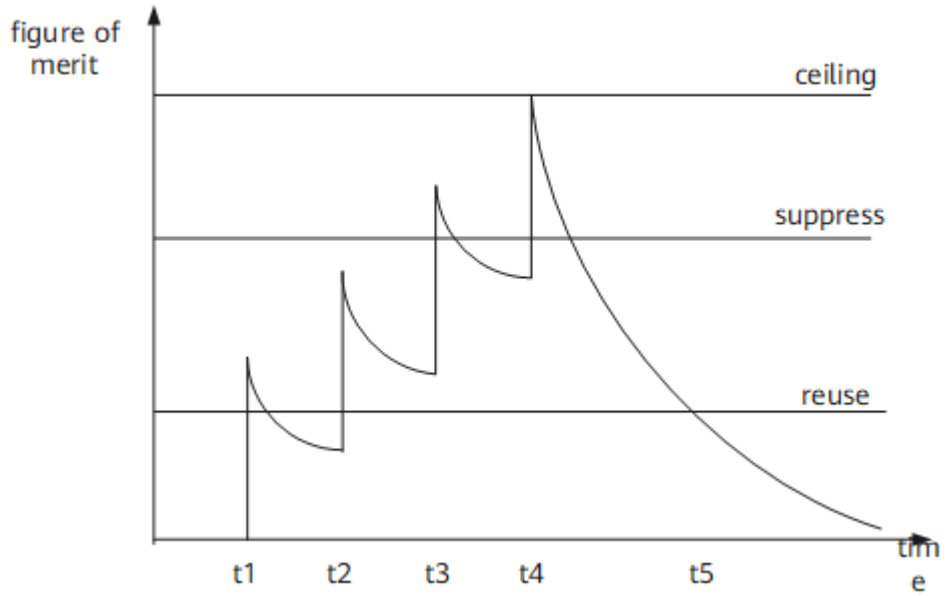
如果用户配置了传输告警定制功能，当告警到达时，可以通过传输告警抑制参数判断如何处理该告警信号。

- 当告警的稳定值小于抑制门限（suppress）值时，
  - 如果没有收到告警产生或消失信号，稳定值会随着时间衰减。
  - 如果收到告警产生信号，接口的物理层状态变为Down。其稳定值增加一个惩罚值。

  - 如果收到告警消失信号，接口的物理层状态变为Up。其稳定值会进行一次指数衰减。
- 当告警的稳定值达到设定的抑制门限时，该告警被抑制。此后该告警的产生或消失信号不会影响接口的物理层状态。
- 如果告警继续频繁产生，稳定值到达最高上限值（ceiling）。此时如果再有告警信号，稳定值也不会再增加。如果没有告警信号到达，则其稳定值会随着时间而衰减。
- 当告警的稳定值下降到重用门限（reuse）时，解除对该告警的抑制。

当告警被解除抑制后，如果再发生该告警，仍按上面的判断过程进行处理。

图 1-44 告警抑制衰减示意图



如图1-44所示，在t1、t2、t3和t4时刻，传输设备发出了告警产生信号。所以在这四个时刻，其稳定值都增加了一个惩罚值。

1. 在t1和t2时刻，其稳定值并没有超过抑制门限，所以这个两个时刻的告警信号都会影响接口的物理层状态。因为是告警产生信号，所以接口的物理状态会变为Down。
2. 在t3时刻，其稳定值已经超出抑制门限，告警被抑制。此时再有告警信号时，不会影响接口的物理层状态。
3. 在t4时刻，其稳定值达到最高上限值。此后如果再有告警上报，稳定值会重新计算，但不会超过最高上限。
4. 在t5时刻下降到重用门限，告警抑制被解除。

1.1.2.1.3 传输告警定制与抑制术语与缩略语

缩略语

缩略语	英文全称	中文全称
SDH	Synchronous Digital Hierarchy	同步数字体系

缩略语	英文全称	中文全称
SONET	Synchronous Optical Network	同步光网络
VRP	Versatile Routing Platform	通用路由平台

1.1.2.2 传输告警定制与抑制配置

配置传输告警特性，可以降低网络中传输告警的频繁发生对网络稳定性的影响。

1.1.2.2.1 传输告警定制与抑制概述

传输告警定制功能可以有效控制告警信号对接口状态变化的影响。传输告警抑制功能可以有效实现对告警信号进行抑制，避免接口的反复振荡。

定义

当前电信级网络对IP设备网络可靠性的要求越来越高，因此要求网络中的设备能够快速检测到故障信息。当接口启动快速检测功能后，告警信息上报速度加快，会引起接口的物理层状态频繁在Up和Down之间切换，导致网络反复振荡。因而需要对告警进行过滤和抑制，避免网络频繁振荡。

传输告警抑制功能可以有效实现对告警信号进行过滤和抑制，避免接口的反复振荡。同时提供告警定制功能，使得告警对接口状态变化的影响可以有效控制。

传输告警定制与抑制具体实现的功能如下：

- 传输告警定制：可以定制哪些告警才能够引起接口的物理层状态变化，起到告警过滤效果。
- 传输告警抑制：通过设置门限值，通过一系列算法来抑制网络反复振荡。

目的

用户可以根据需求定制传输告警，从而过滤掉不在定制范围内的传输告警。传输告警抑制功能对定制的告警设定门限值，从而忽略传输链路保护等产生的毛刺。避免网络频繁振荡。

在骨干网或城域网中，IP路由设备要与传输设备进行对接(一般的传输设备有SDH（Synchronous Digital Hierarchy）、SONET（Synchronous Optical Network）等)。当传输设备发生故障时，在IP路由设备上会接收到一些告警，之后传输设备会进行链路倒换，待传输设备的链路正常后会向IP路由设备发出告警清除。传输设备从发生告警到告警消除的保护时间通常是50ms～200ms。从IP路由设备上来看，这通常是一个50ms～200ms内的毛刺。这些毛刺会导致IP路由设备接口状态频繁变化，导致路由设备频繁的进行路由计算，造成路由振荡的情况，对路由设备的性能造成影响。

从网络整体角度来看，希望IP路由设备能够忽略这样的毛刺，不做任何处理。也就是说在传输设备进行维护或者传输设备进行链路保护时，路由设备要通过对传输设备产生的告警采取定制与抑制手段，从而不产生路由振荡，保证路由设备的稳定运行。传输告警定制功能可以使告警对接口的物理层状态的影响得到控制。传输告警抑制功能可以有效实现对特定告警信号进行过滤和抑制，避免接口反复振荡。

在主备倒换过程中，系统可以正常处理传输告警的各种告警信号，传输告警的配置也依然生效。

1.1.2.2.2 传输告警定制与抑制特性限制

1.1.2.2.3 配置传输告警的定制功能

通过本节可以了解到传输告警定制的应用环境、前置任务和数据准备。

应用环境

当和传输设备相连时，如果网络不稳定，将产生大量的毛刺告警信息，而这些告警信息将导致接口的物理层状态不断地在Up和Down状态之间切换。如果希望能指定哪些告警可以触发接口的物理层状态为Down，可以配置传输告警的定制功能。

前置任务

在配置传输告警的定制功能之前，需完成以下任务：

- 路由器上电，自检正常

配置可以影响接口的物理层状态的告警类型

当和传输设备相连时，如果网络不稳定，将产生大量的毛刺告警信息，而这些告警信息将导致接口的物理层状态不断地在Up和Down状态之间切换。如果希望能指定哪些告警可以触发接口的物理层状态为Down，可以配置传输告警的定制功能。

背景信息

当传输设备的告警信号上报到系统后，可以通过传输告警定制功能控制告警对接口的物理层状态的影响。在全局或者与传输设备相连的接口上进行以下配置。

传输告警过滤时间可以全局配置，也可以在接口下配置。全局配置后，对支持该功能的接口均生效。二者之间的关系如下。

- 配置全局告警定制功能时，若接口有非默认告警定制配置，则接口配置生效。
- 当接口下未配置告警定制功能，则全局配置生效。

说明

VS模式下，全局传输告警定制功能仅在Admin VS支持。

操作步骤

- 配置全局传输告警定制功能。
  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**transmission-alarm down wan** { **auais** | **b1tca** | **b2tca** | **b3tca** | **lais** | **lcd** | **lof** | **lom** | **lop** | **los** | **lrdi** | **lrei** | **oof** | **pais** | **pplm** | **prdi** | **prei** | **puneq** | **rdool** | **rrool** | **sdbere** | **sfbere** | **trool** } *，配置全局10GE WAN接口的告警定制功能，定制这些告警的产生可以触发接口的物理层状态变为Down。
  c. 执行命令**commit**，提交配置。
- 配置接口下传输告警定制功能。
  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**interface** *interface-type interface-number*，进入对应接口视图。

c. 请根据实际情况选择以下配置。

- 如果接口类型为10GE WAN，执行命令**transmission-alarm down { auais | b1tca | b2tca | b3tca | lais | lcd | lof | lom | lop | los | lrdi | lrei | oof | pais | pplm | prdi | prei | puneq | rdool | rrool | sdbere | sfbere | trool }** *，定制这些告警可以影响接口的物理层状态。

说明

- 由于硬件上不同子卡支持的告警类型不同，并不是所有接口都支持这些告警。如果配置了接口不支持的告警类型，则配置失败，并会提示该接口不支持配置哪些告警类型。
- 告警wlnk只支持查看，不支持通过命令行配置。该告警永远是打开状态的，且可以触发接口的物理层状态变为Down。可使用命令**display transmission-alarm**查看wlnk告警的状态和统计信息。

须知

LAIS、LOF和LOS三类告警对链路状态变化提供告警，如果去使能这三类告警会影响业务数据的准确转发，所以建议使能这几类告警。

d. 执行命令**commit**，提交配置。

----结束

1.1.2.2.4 配置传输告警的过滤时间间隔

通过本节可以了解到传输告警过滤时间间隔的应用环境、前置任务和操作步骤。如果告警产生和消失的时间间隔小于该时间间隔，则告警信号就被认为是毛刺，并被过滤掉。否则就是正常的告警信号。

应用环境

当和传输设备相连时，如果网络不稳定，将产生大量的毛刺告警信息，而这些告警信息将导致接口的物理层状态不断地在Up和Down状态之间切换。如果希望这些告警产生和消除的时间间隔在一定时间范围内时忽略这些告警，就需要配置传输告警的过滤时间间隔。

传输告警过滤时间可以全局配置，也可以在接口下配置。全局配置后，对支持该功能的接口均生效。二者之间的关系如下。

- 全局配置后，如果接口下存在传输告警过滤时间的非默认配置，则实际以接口配置为准。
- 当接口视图下未配置传输告警过滤时间时，以全局配置为准。

说明

VS模式下，全局配置传输告警的过滤时间间隔仅在Admin VS支持。

前置任务

在配置传输告警的过滤时间间隔之前，需完成以下任务：

- 路由器上电，自检正常

- 在路由器接口上1.1.2.2.3 配置传输告警的定制功能

说明

对接口使能了传输告警定制功能后，接口使能过滤功能才生效。

操作步骤

- 配置全局告警过滤功能并设置告警过滤时间间隔。
  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**transmission-alarm holdup-timer** *holdup-time*，配置全局告警消除过滤功能并设置过滤消除告警的时间间隔。
  c. 执行命令**commit**，提交配置。
- 配置接口下告警过滤功能并设置告警过滤时间间隔。
  a. 执行命令**system-view**，进入系统视图。
  b. 请根据实际情况选择以下配置。
     - 执行命令**interface** *interface-type interface-number*，进入10GE WAN接口视图。
  c. 执行命令**transmission-alarm holdup-timer** [*holdup-time*]，配置接口下告警消除过滤功能并设置过滤消除告警的时间间隔。
  d. 执行命令**commit**，提交配置。

----结束

检查配置结果

完成配置后，可以执行**display transmission-alarm**命令选择不同的接口检查对应的配置结果。

1.1.2.2.5 维护传输告警定制与抑制

通过本节可以了解维护传输告警抑制中查看误码速率值和清除传输告警的运行信息的相关操作步骤。

查看误码速率值

当发生误码率告警，设备把接口置“down”时，您可以执行如下命令查询当前的误码速率值。

操作步骤

- 查询当前接口的误码速率值，请在所有视图下执行**display transmission-alarm bit-error-rate**命令。

----结束

清除传输告警的运行信息

当需要重新统计接口的传输告警信息时，需要先清除该接口的传输告警运行信息。

背景信息

须知

清除接口上的告警运行信息会导致接口所有告警计数清零。务必仔细确认是否必须执行清除接口告警运行信息的操作。

操作步骤

- 在确认需要清除接口上所有告警的运行统计信息后，请在接口视图下执行**reset transmission-alarm statistics**命令。

----结束

1.1.3 端口扩展配置

1.1.3.1 端口扩展特性描述

1.1.3.1.1 端口扩展介绍

定义

在IP Core网络中，为了满足接入侧和网络侧越来越多的业务部署需求，需要PE设备提供高密度的以太类接口。为了在不增加网络设备投资的情况下支持设备提供高密度以太类接口，华为实现了端口扩展特性。

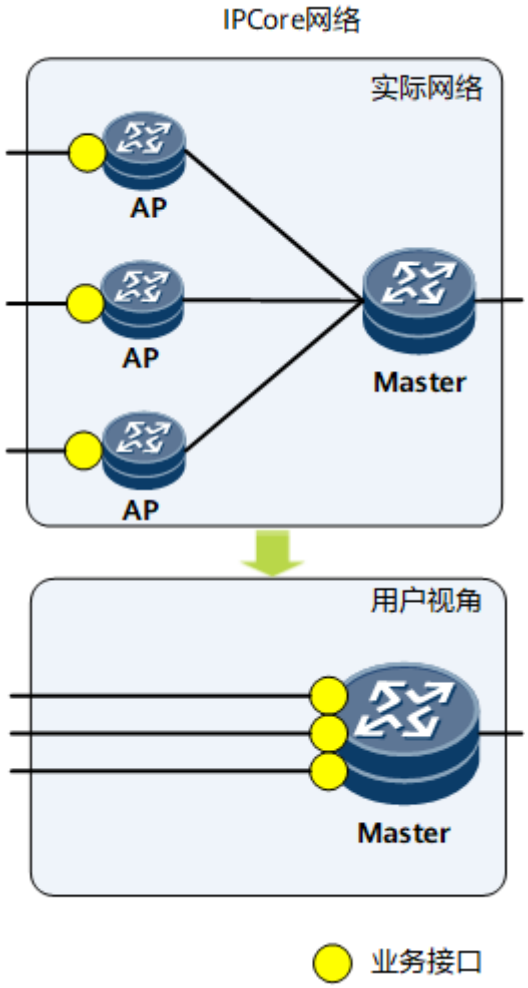
如图1-45所示，端口扩展特性是将一台性能较高的设备设置为Master，将大量的支持以太类接口的低端设备设置为AP，把AP上的以太类接口映射为Master上的端口扩展接口，业务配置只需在Master的端口扩展接口上完成，从而使Master设备具备高密度的以太类接口。

- AP：端口扩展系统的接入节点，可以看作是Master的一个板卡，由Master自动发现并管理。AP接受Master下发的配置和转发表项，对外提供业务外联接口。
- Master：端口扩展系统的控制节点，负责内部隧道建立、业务下发和流量控制，并可以对连接的AP进行管理。

说明

请保证Master和AP设备的软件版本一致。Master和Ap的软件版本不一致可能导致AP上线后业务不可用。

图 1-45 端口扩展特性概念图

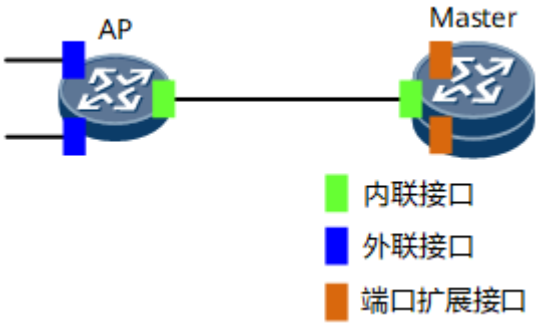


相关概念

端口扩展特性涉及的基本概念如下表所示。

概念	描述
内联接口	用于Master和AP进行互联的接口，使能端口扩展能力。
外联接口	AP上连接系统外部的接口，该接口在Master上有对应的端口扩展接口。
端口扩展接口	Master在本地为AP上的外联接口建立的一个虚拟的映射接口。Master上的一个端口扩展接口对应AP上的一个外联接口。

图 1-46 端口扩展系统示意图



方案价值

采用端口扩展特性可以为用户带来的价值有：

- 减少建网成本

  Master设备使用较少的槽位就可以提供高密度的接口，既充分利用了已有的支持以太类接口的设备（作为AP），又避免购买支持大量以太类接口的设备，显著降低了建网成本。

- 降低运维成本

  控制和管理平面都集中在Master上，部署业务的配置和查询等操作都在Master或网管上完成，用户无需再到AP上进行配置和管理，减少了人员投入，显著降低了网络运维成本。

1.1.3.1.2 端口扩展特性支持说明

特性名称	简要描述
AP即插即用	当AP上线、下线、迁移以及AP或Master重启时，Master自动感知并完成相应的管理动作，无需用户干预。
Trunk内联接口	当需要增加带宽或提升可靠性时，可以将Master和AP之间的Eth-Trunk接口设置为Trunk内联接口。
端口扩展Trunk接口	当AP上的外联接口需要配置Eth-Trunk时，可以在Master上将相应的端口扩展接口加入到普通的Eth-Trunk接口中，作为端口扩展Trunk接口。
端口扩展系统的告警和日志管理	Master和AP各自记录各自产生的告警信息，并独立向网管发送告警信息。 支持在Master上指定syslog服务器，Master和AP各自记录各自产生的日志信息，并独立向指定的syslog服务器发送日志信息。

1.1.3.1.3 端口扩展原理描述

控制平面

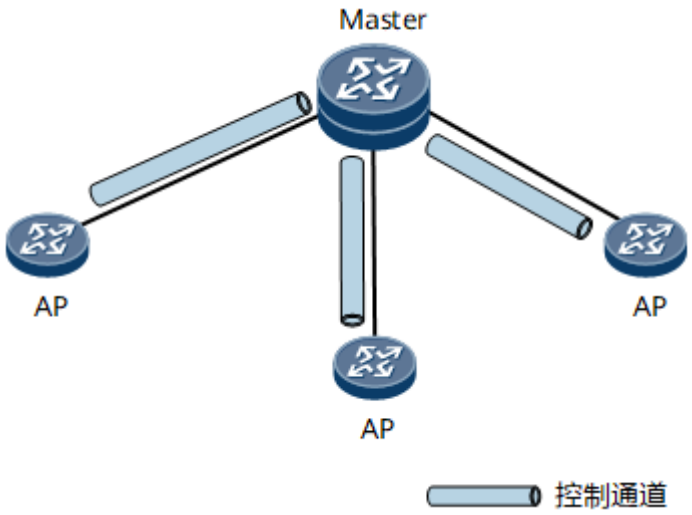
端口扩展系统的控制平面主要包括控制通道和内部转发通道。

控制通道

在端口扩展系统中，由AP向Master发起建立控制通道。如图1-47所示，通过控制通道：

- Master向AP下发转发表项，用于指导数据在Master和AP之间转发。
- AP向Master上报外联接口的相关属性（包括接口物理/协议状态、接口MAC、接口带宽等），用于在Master上通过端口扩展接口查询AP上的外联接口属性。

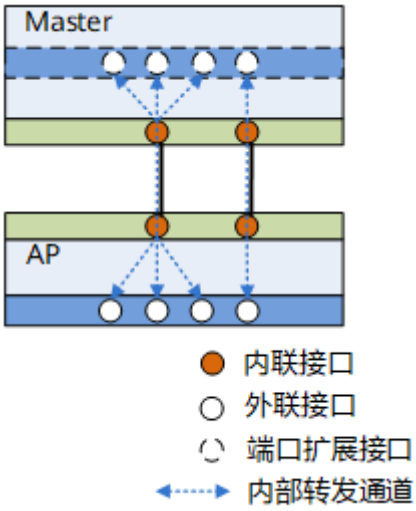
图 1-47 控制通道示意图



内部转发通道

端口扩展系统需要建立内部转发通道，以便转发业务流量。内部转发通道是通过配置建立的，如图1-48所示，先指定Master的内联接口与AP上对应的内联接口建立绑定关系，再指定Master的内联接口与AP的外联接口建立绑定关系。配置之后，Master会创建与AP外联接口对应的端口扩展接口，系统将建立起一条从AP的外联接口开始，经由AP的内联接口、Master的内联接口到Master上的端口扩展接口的双向通道。系统会为这条通道分配一个标签，称为NVTAG，在这条通道内传输的报文会携带NVTAG，用于报文的识别。

图 1-48 内部转发通道示意图



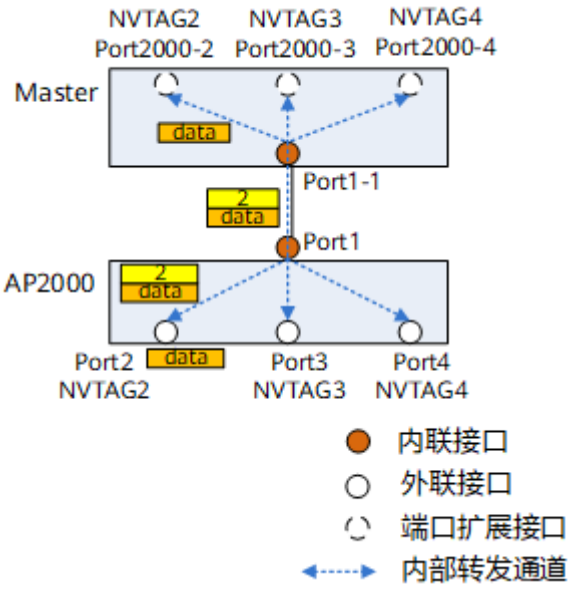
转发平面

在端口扩展系统的转发平面，AP将从外联接口上收到的报文通过内部转发通道发送到Master上，同时AP也通过内部转发通道接收到Master发来的报文，然后通过外联口发送出去。AP只负责数据转发，业务处理都在Master的端口扩展接口上完成。

如图1-49所示，当控制平面配置完成后，Master的Port1-1成为内联口，AP的Port1成为内联口，AP2000的Port2、Port3、Port4成为外联口。同时，Master上会创建三个与AP外联接口对应的端口扩展端口Port2000-2、Port2000-3、Port2000-4，Master会为AP的三个外联接口分配三个NVTAG，该值在Master和AP上都会下发到转发表项中。在Master上，转发表项中记录的是内联接口、端口扩展接口与NVTAG的对应关系；在AP上，转发表项中记录的是内联接口、外联接口和NVTAG的对应关系。

例如：当AP从外联接口(如Port2)接收到数据报文之后，AP根据转发表项打上NVTAG（如NVTAG2）；然后转发到AP的内联接口Port1，最后发送到Master的内联接口Port1-1。Master根据接收到报文的内联接口，以及报文中携带的NVTAG2，可以查找到唯一确定的端口扩展接口（Port2000-2），根据该端口扩展接口上配置的业务进行相应的报文处理。同理，数据报文从Master发送到AP的过程完全类似。

图 1-49 端口扩展系统的数据转发



AP 即插即用

AP的即插即用是指：当AP上线、下线、迁移以及AP或Master重启时，Master自动感知并完成相应的管理动作，无需用户干预。支持AP的即插即用，是端口扩展系统简化网络运维和管理的重要特性。AP的即插即用包含以下几种流程：

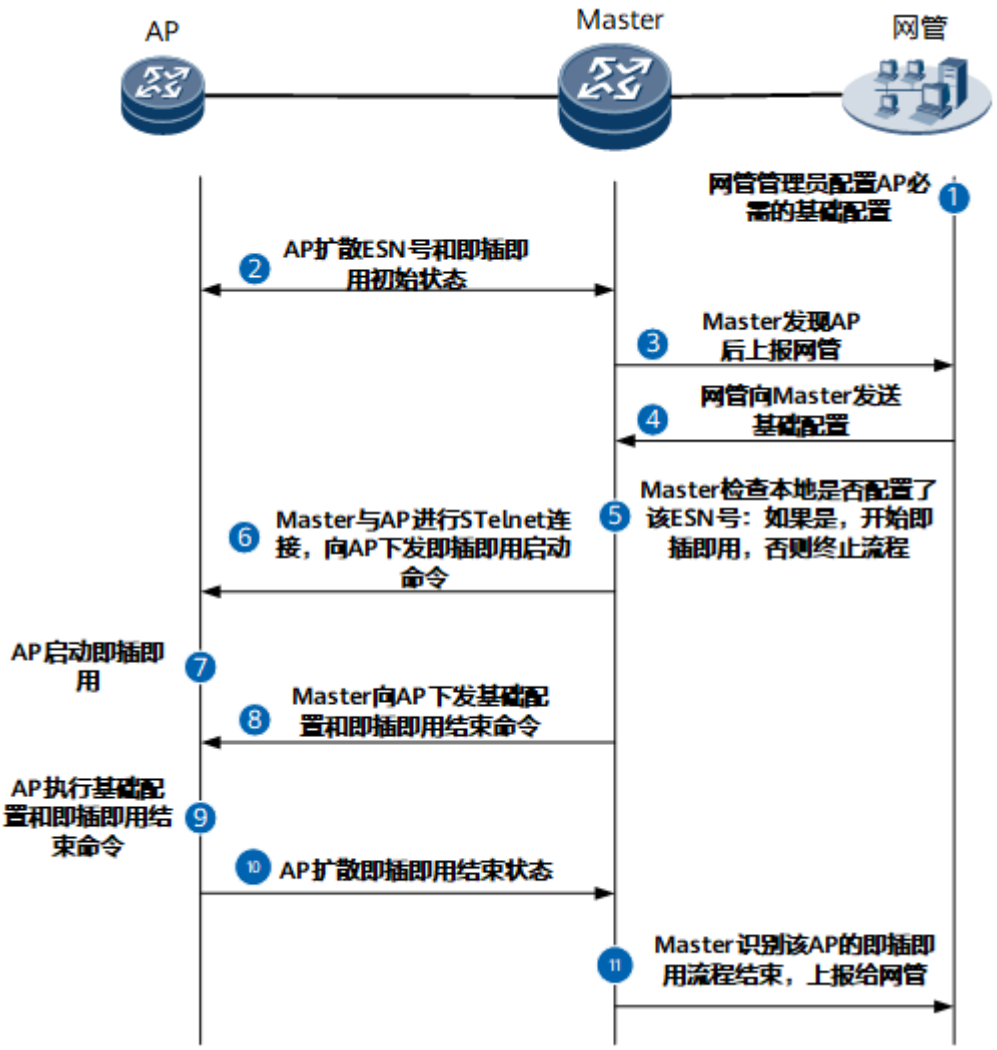
- **AP初次上线**
- **AP重启上线**
- **Master重启**
- **AP下线**
- **AP迁移**

下面分别介绍一下上述AP即插即用流程。

AP 初次上线

AP初次上线后的即插即用流程如**图1-50**所示。

图 1-50 AP 初次上线后的即插即用流程



关于该流程中各步骤的详细描述如表1-16所示。

说明

AP即插即用部署之前，需要先配置Master基础功能（配置端口扩展能力+配置Master角色），并使能Master内联口的DCN功能。

表 1-16 流程详细描述

步骤序号	描述
1	网络管理员在网管上配置AP即插即用必需的基础配置，包括： ● AP的ESN号 ● AP的管理IP地址 ● 在AP上创建一个用户并配置该用户的登录口令、SFTP访问目录

步骤序号	描述
2	AP采用缺省配置启动，并且加载预配置文件，自动使能DCN（Data Communication Network）功能，并在端口扩展系统内通过OSPF扩散自己的ESN号以及即插即用初始状态。
3	Master通过DCN发现AP，并识别AP的即插即用状态为初始状态。Master将发现AP的信息（如ESN号等）上报给网管。
4	网管将AP即插即用必需的基础配置（见步骤1）发送给Master。
5	Master检查本地是否配置了被发现AP的ESN号，如果是，则启动即插即用；如果不是则终止即插即用流程。 **说明** Master要管理哪些AP由用户在Master上配置相应AP的ESN号来控制。
6	Master使用初始用户名和密码与AP建立STelnet连接，并向AP下发即插即用启动命令。
7	AP启动即插即用同时启动定时器等待即插即用过程完成。
8	Master将如下基础配置下发到AP上（包括Master自动生成的配置和网管下发的基础配置）： ● 使能设备的端口扩展能力 ● 将设备角色设置为AP ● AP的管理IP地址 ● 在AP上创建一个用户并配置该用户的登录口令、SFTP访问目录 如果上述基础配置完整，则同时下发即插即用结束命令；如果不完整，则终止即插即用流程。
9	AP自动执行Master发来的基础配置。 如果AP收到了即插即用结束命令，则认为配置完成，终止定时器；如果在定时器超时前未收到即插即用结束命令，则认为基础配置不全，AP将自动重启再次尝试即插即用。
10	AP在端口扩展系统内通过OSPF扩散即插即用结束状态。
11	Master感知到AP的即插即用结束状态，并向网管上报。即插即用流程结束，AP上线成功。

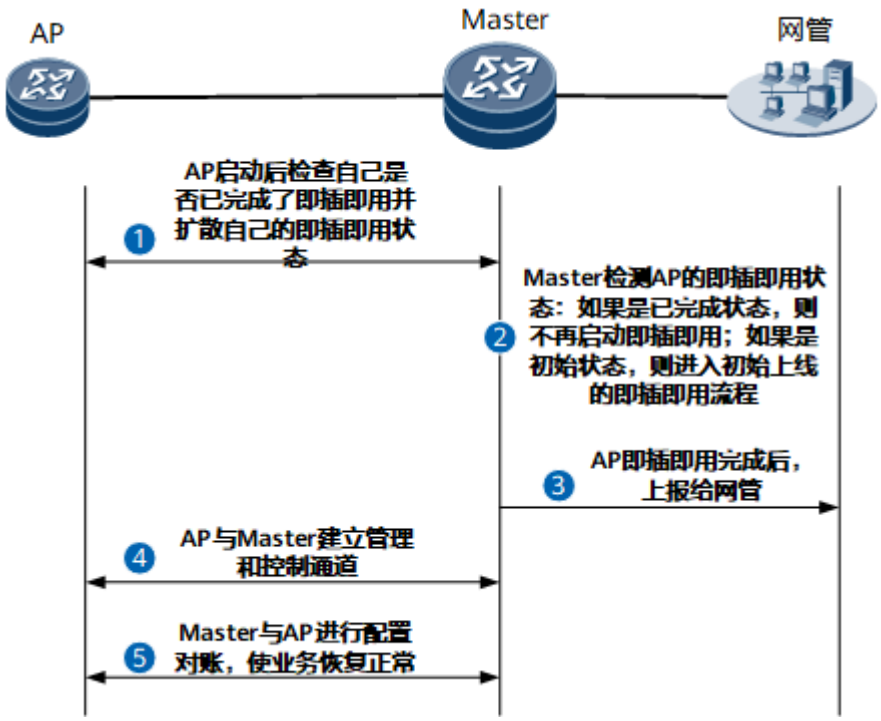
说明

以上描述的是有网管参与的AP即插即用流程。如果网络中无网管，则需要用户预先在Master上完成AP即插即用必需的基础配置（见上表的第1步），其余过程与有网管参与时相同，这里不再赘述。下文介绍的其他流程情况类似。

AP 重启上线

AP重启上线后的即插即用流程如图1-51所示。

图 1-51 AP 重启上线后的即插即用流程



关于该流程中各步骤的详细描述如表1-17所示

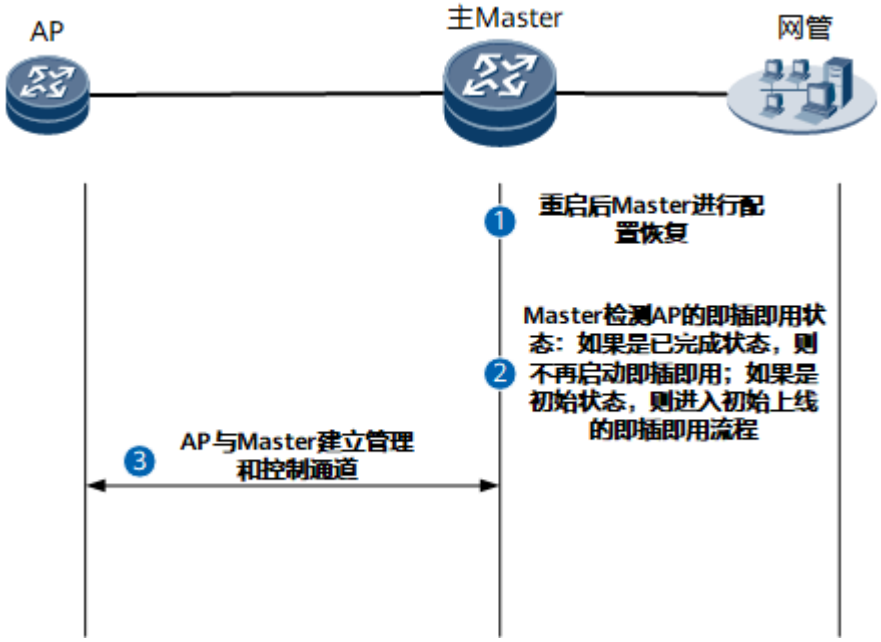
表 1-17 流程详细描述

步骤序号	描述
1	AP重启后读取本地保存的即插即用状态，并在端口扩展系统内通过OSPF扩散自己的即插即用状态。
2	Master通过DCN发现AP，并检测AP的即插即用状态： ● 如果是初始状态，则进入AP初始上线的流程。 ● 如果是已完成状态，则不再启动即插即用。 **说明** 如果AP进行恢复配置的重启，则AP的即插即用状态为已完成状态；如果AP进行清除配置的重启并且加载预配置文件，则AP的即插即用状态为初始状态。
3	Master向网管上报AP已完成即插即用。
4	AP与Master之间建立NETCONF和控制通道。
5	Master通过NETCONF通道与AP进行配置对账，使业务恢复正常。 **说明** 这里的配置对账是指Master与AP之间进行配置比对，以Master的配置为准，检查Master上针对AP的配置是否都已在AP上。如果没有，则通过NETCONF通道将缺少的配置下发给AP。如果AP上存在Master没有的配置，会进行删除。

Master 重启

Master重启后的AP即插即用流程如图1-52所示。

图 1-52 Master 重启后的 AP 即插即用流程



关于该流程中各步骤的详细描述如表1-18所示

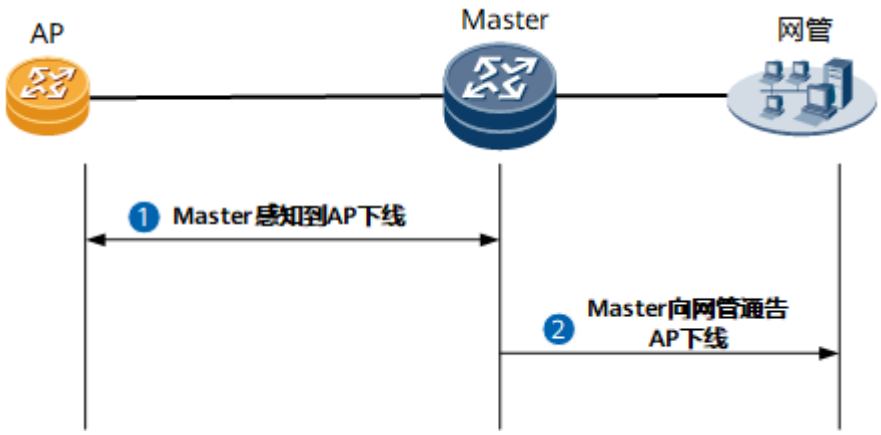
表 1-18 流程详细描述

步骤序号	描述
1	重启完成后，Master进行配置恢复。此时AP上的配置已存在。
2	Master通过DCN发现AP，并检测AP扩散的即插即用状态： ● 如果是初始状态，则进入AP初始上线的流程。 ● 如果是已完成状态，则不再启动即插即用。 **说明** 正常情况下AP的即插即用状态为已完成状态。当AP被清除配置并加载预配置文件时（如清除配置重启等），它的即插即用状态变为初始状态。
3	AP与Master之间建立NETCONF和控制通道。

AP 下线

AP下线的流程如图1-53所示。

图 1-53 AP 下线流程



关于该流程中各步骤的详细描述如表1-19所示

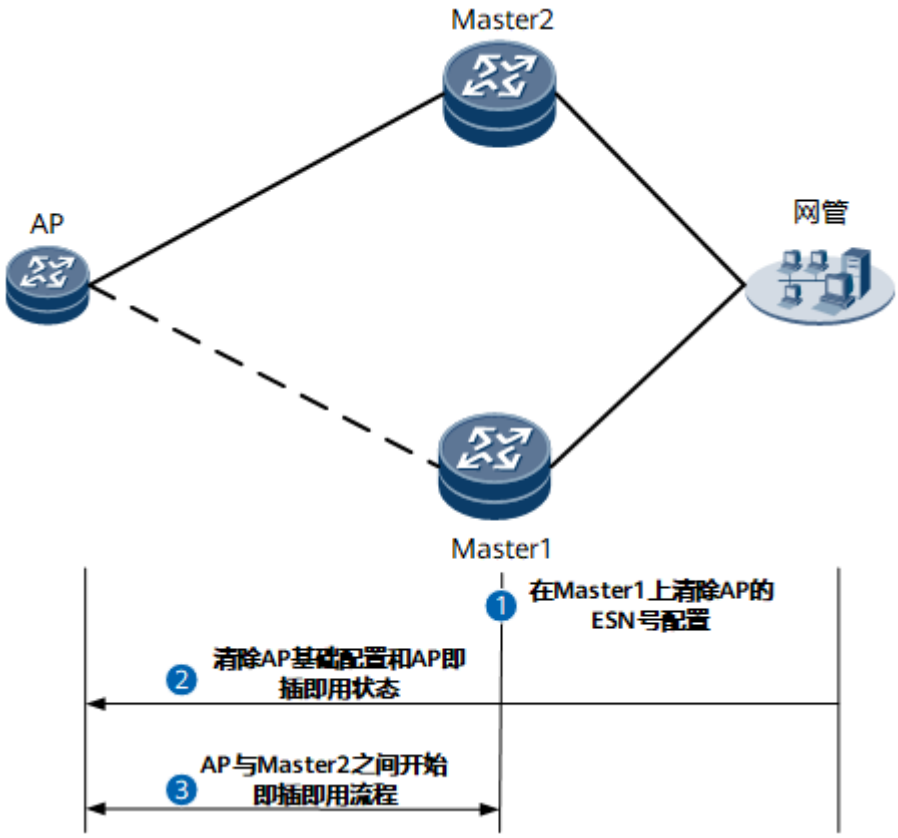
表 1-19 流程详细描述

步骤序号	描述
1	当AP的路由信息在Master的路由表中被删除时，Master感知到AP下线，Master上不做任何处理。
2	Master将下线AP的信息上报给网管。

AP 迁移

AP迁移的流程如图1-54所示，AP从Master1的管理下迁移到Master2的管理下。

图 1-54 AP 迁移流程



关于该流程中各步骤的详细描述如表1-20所示

表 1-20 流程详细描述

步骤序号	描述
1	用户在Master1上清除该AP的ESN号配置。
2	用户通过Master或网管登录到AP上清除基础配置，加载预配置文件，并清除AP的即插即用状态，恢复到初始状态。
3	AP与Master2之间开始即插即用流程，参见AP初始上线的流程。

网络管理

存在网管的场景

在存在网管的场景中，端口扩展系统中的管理通道包括NETCONF通道和SNMP通道，如图1-55所示。

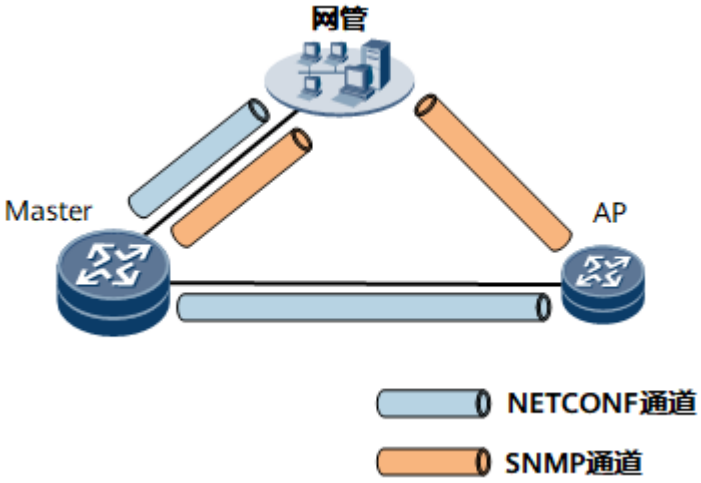
- NETCONF通道

  - Master与AP之间的NETCONF通道：Master向AP发起建立NETCONF通道。通过NETCONF通道，Master可以向AP下发配置，也可以下发查询（如查询AP的外联接口状态等）和维护（如升级软件包、重启AP等）命令。
  - 网管与Master之间的NETCONF通道：用于网管向Master下发配置或查询任务。与Master和AP之间的NETCONF通道连通之后，网管也可以直接向AP下发配置或查询任务。
- SNMP通道

  Master和AP分别与网管建立SNMP通道，用于Master和AP向网管上报告警。

  SNMP通道采用带内管理方案。该方案是指网络管理系统利用被管设备提供的转发路径对网络中的设备实施管理的组网方式。为了实现网管信息的可靠传输，在承载网络内通常通过L3VPN承载。其原理为：Master上通过接口板上的业务口和网管通信，AP到网管的报文是从Master上的接口板进去，再从Master上的接口板转发出去。

图 1-55 端口扩展系统网络管理示意图



网管在端口扩展系统运维和管理工作中的主要作用包括：

- 参与AP即插即用的过程，详情请参见**AP即插即用**。
- 对Master和AP进行日常的配置、维护和信息查询。
- 接收Master和AP上报的告警信息，帮助网络管理员进行故障处理。

不存在网管的场景

当网络中不存在网管时，管理通道只有Master与AP之间的NETCONF通道。用户可以直接在Master上对AP进行管理，方式有以下两种：

- 直接在Master上执行对AP的配置、查询和维护操作，Master通过NETCONF通道下发给AP。
- 先在Master上通过STelnet登录到AP上，然后进行查询和维护操作。

说明

在Master上通过STelnet登录到AP上只能进行查询（如查询AP的外联接口状态等）和维护（如升级软件包、重启AP等）操作。对AP的业务配置，只能在Master上直接执行。

1.1.3.1.4 端口扩展应用

端口扩展在 IPCore 网络中的应用

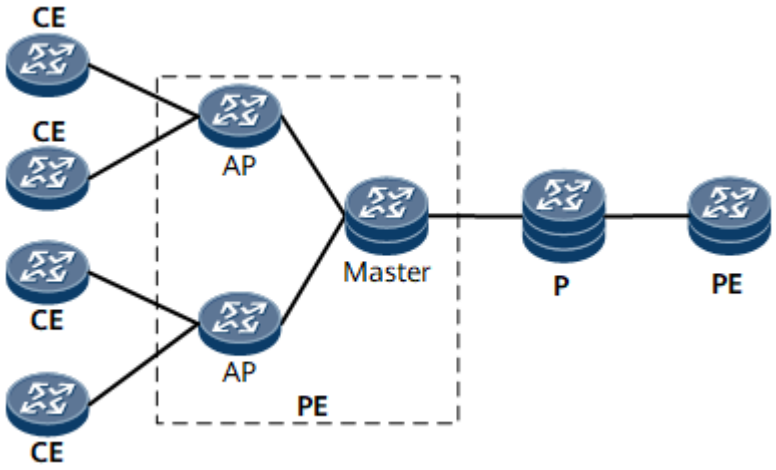
业务描述

在IP Core网络场景下，如果用户的建网预算有限，同时又有较多支持以太类接口的低端设备，就可以只采购很少的高端设备，或对原有的高端设备进行软件升级，作为Master设备。对已有的低端设备进行软件升级，作为AP设备。这样就可以通过建立端口扩展系统来提供高密度以太类接口。

组网描述

在IP Core网络中，端口扩展系统主要作为PE节点，其典型组网如图1-56所示。

图 1-56 端口扩展系统作为 PE 节点示意图



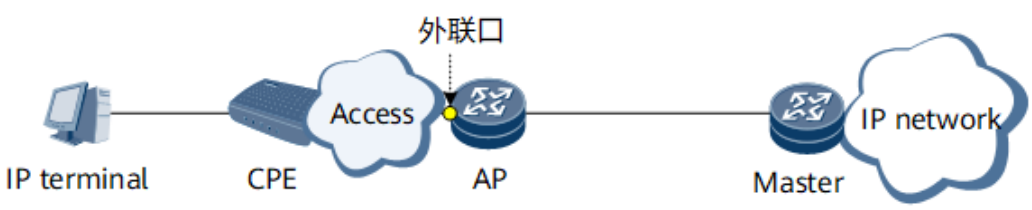
特性部署

1. 指定端口扩展系统的Master和AP。
2. 配置Master和AP之间对应内联接口的绑定关系。
3. 配置Master内联接口与AP上外联接口之间的绑定关系。

端口扩展场景中的 HQoS

如图1-57所示，目前实现的端口扩展场景中的HQoS接入主要是通过路由器下行接口在外联口下配置基于模板的HQoS。基于模板的HQoS配置完成后，在端口扩展接口下完成应用，即可实现端口扩展系统下的HQoS接入。

图 1-57 在端口扩展场景中部署 HQoS 接入



1.1.3.1.5 端口扩展术语与缩略语

术语

术语	解释
Master	端口扩展系统的控制节点，负责端口扩展系统的内部转发隧道建立、业务下发和流量控制，并可以对连接的AP进行管理。
AP	端口扩展系统的接入节点，可以看作是Master的一个板卡，由Master自动发现并管理。AP接受Master下发的配置和转发表项，对外提供业务外联接口。

缩略语

缩略语	英文全称	中文全称
AP	Access Point	接入节点
ESN	Equipment Serial Number	设备序列号
PNP	Plug and Play	即插即用
DCN	Data Communication Network	数据通信网络

1.1.3.2 端口扩展配置

配置端口扩展，可以使设备用较少的槽位提供高密度的以太类接口。

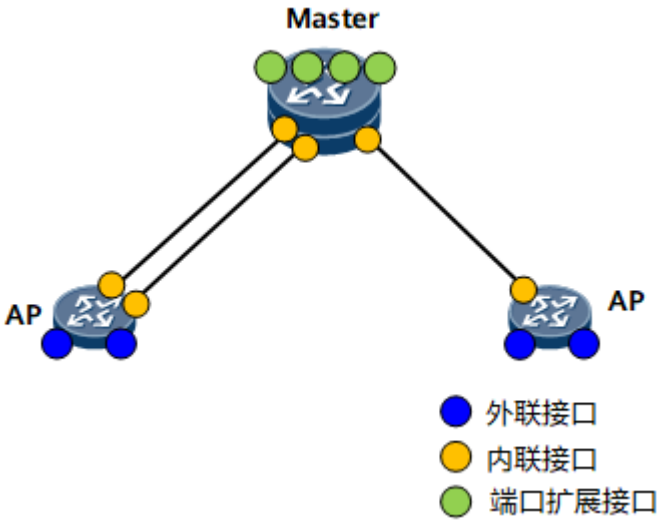
应用场景

说明

该特性仅在Admin-VS支持。

在IP Core网络中，为了满足接入侧和网络侧越来越多的业务部署需求，需要PE设备或P设备提供高密度的以太类接口。此时，可以部署端口扩展系统，将一台性能较高的设备设置为Master，将大量的支持以太类接口的低端设备设置为AP，把AP上的以太类接口映射为Master上的端口扩展接口，业务配置只需在Master的端口扩展接口上完成，从而使Master设备具备高密度的以太类接口。这样既可以充分利用已有的支持以太类接口的设备，又避免购买支持大量以太类接口的设备，显著降低了建网成本。同时，端口扩展系统可以实现AP的即插即用，在一台Master上可以对所有AP进行配置和管理，简化了网络和业务部署，降低了运维难度。端口扩展的典型组网如图1-58所示。

图 1-58 端口扩展组网图



说明

完成端口扩展系统的部署后，在Master上，端口扩展接口支持的业务特性范围与本地的普通以太类接口是基本一致的。

部署指导

为了完整的部署端口扩展系统，并按需开展维护和管理工作，需要在Master上进行以下配置：

1.1.3.2.1 端口扩展特性限制

1.1.3.2.2 建立端口扩展系统

本节介绍建立端口扩展系统的基本配置任务。

背景信息

端口扩展系统由Master和AP两种角色构成。为了简化业务部署、方便运维和管理，端口扩展系统的控制平面在Master上，因此，建立端口扩展系统的基本配置都在Master上完成。同时，AP支持即插即用，Master通过ESN号自动识别AP并管理它，然后通过内部的NETCONF通道将相关的基本配置下发到AP上，用户无需到AP上进行任何配置。

前置任务

在建立端口扩展系统之前，需完成以下任务：

- AP设备需保持默认配置并加载预配置文件。
- 获取AP设备的ESN号。
- 请在Master设备上使能SSH客户端首次认证功能（**ssh client first-time enable**）。

配置 Master 的基本功能

Master是端口扩展系统的主体，建立端口扩展系统需先配置Master。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**virtual-access port-extend**，使能端口扩展能力，并进入端口扩展视图。

步骤3 执行命令**role master**，将当前节点的角色配置为Master。

执行此步骤后：

- 本地的所有物理接口将变成四维接口，例如：GigabitEthernet1/1/0/1，其中第一维为1表示该接口为本地接口。
- 设备将根据本地的特性配置具体情况，自动使能全局BFD能力并创建端口扩展系统内部的IS-IS进程，具体规则如下：

初始情况	子分类	创建的IS-IS进程
不存在任何IS-IS进程	缺省情况	自动创建一个进程号为65534的IS-IS进程。
存在一个或多个IS-IS进程	进程65534被使用	将在65534到1之间查找一个未被占用且离65534最近的进程号作为端口扩展的IS-IS进程号。
	进程65534未被使用	自动创建一个进程号为65534的IS-IS进程。

步骤4 执行命令**admin** *ip-address*，配置Master的管理IP地址。

Master的管理IP地址将通过内部IS-IS扩散给AP，用于与AP建立内部控制和管理通道。执行此步骤后，Master本地将自动生成一个IP地址为*ip-address*的Loopback接口。

步骤5 根据实际情况选择相应的命令，配置Master与AP建立STelnet连接的用户名、密码和备用密码。

- 执行命令**ap default login-user** *user-name* { **login-password** *password* | **slave** *slave-password-value* }*。
- 执行命令**ap default login-user** *user-name* **login-password** 。
- 执行命令**ap default login-user** *user-name* **slave-password** 。

说明

该用户名和密码需要配置成AP的默认用户名和密码。

步骤6 （可选）执行命令**isis authentication-mode hmac-sha256 key-id** *key-id* **cipher** *cipher-text* [**send-only**]，配置IS-IS认证。

为提高端口扩展系统的安全性，需配置**isis authentication-mode**命令，对IS-IS接收的Hello报文、LSP报文以及SNP报文进行一定规则的验证并对发送的上述报文附加认证信息，使只有通过验证或加密的报文才可以在系统中进行转发，避免非法报文给系统带来干扰。

步骤7 （可选）执行命令**control-tunnel authentication keychain** *keychain-name*，配置控制通道的Keychain认证。

AP与Master之间的控制通道用于两者交互控制信息，为了提升控制通道的安全性，可以在Master上执行此步骤，配置Keychain认证。

配置此步骤之前，需要先创建名称为*keychain-name*的Keychain。

步骤8 执行命令**commit**，提交配置。

----结束

在 Master 上配置 AP 的基本功能

AP可以看作是Master的远端板卡，AP的基本功能配置可以在Master上完成。

背景信息

在端口扩展系统中，一个Master可以同时管理多个AP。在Master上重复执行下述步骤，可以为多个AP配置基本功能。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**ap-id** *ap-id*，在Master上配置AP的ID并进入AP视图。

步骤3 执行命令**esn** *esn-number*，配置当前AP的ESN号。

端口扩展系统支持AP即插即用。在AP启动之后，会自动使能DCN（Data Communication Network）功能，并通过内部的OSPF扩散AP的ESN号和PNP（Plug and Play）初始状态；Master在发现AP并识别AP的PNP状态为初始状态之后，查询本地是否配置了对应的ESN号，如果配置了，则启动即插即用流程。ESN号是Master用来唯一识别一个AP的，因此不同AP的ESN号不能相同。

步骤4 （可选）执行命令**sysname** *host-name*，设置AP的主机名。

步骤5 执行命令**commit**，提交配置。

步骤6 执行命令**admin** *ip-address*，配置当前AP的管理IP地址。

AP的管理IP地址用于与Master建立内部控制和管理通道。该配置会在AP的即插即用流程中，由Master下发给AP。然后AP会自动生成一个IP地址为*ip-address*的Loopback接口。

此命令执行后无需提交，立即生效。

----结束

配置端口扩展的认证方案

为了保证端口扩展系统的安全性，必须配置认证方案。

背景信息

为了建立起端口扩展系统，需要在Master与AP之间建立Stelnet、SFTP、NETCONF等通道。为了保证安全性，必须配置登录AP的认证方案。当前认证方案支持的认证模式包括：

- 本地认证：如果当前网络中没有部署HWTACACS服务器，则可以采用本地方式进行认证。本地方式进行认证的优点是速度快，可以降低运营成本；缺点是存储信息量受设备硬件条件限制。
- HWTACACS认证：采用HWTACACS方式进行认证，可以防止非法用户对端口扩展系统的攻击。与本地认证相比，HWTACACS具有更加可靠的传输和加密特性。

请在Master上执行下列操作步骤。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**ap-id** *ap-id*，进入AP视图。

步骤3 执行命令**login-user** *user-name* **login-password** *password*，配置Master登录到AP时所需的用户名和口令。

步骤4 执行命令**commit**，提交配置。

步骤5 执行命令**login-user** *user-name* **sftp-directory** *sftp-directory*，配置Master登录到AP时所需的用户名和SFTP目录。

步骤6 执行命令**authentication-mode** { **hwtacacs** | **local** } *，配置当前认证方案使用的认证模式。

其中**local**表示采用本地认证，**hwtacacs**表示采用HWTACACS认证。缺省情况下采用本地认证。

在一个认证方案中可以同时采用两种认证模式，系统将按照**local**与**hwtacacs**配置的顺序进行认证：

- 当配置的认证方式是先本地认证后HWTACACS认证时

  如果步骤3中的用户名在AP上没有创建，将转入HWTACACS认证。

  如果步骤3中的用户名在AP和HWTACACS服务器都已经创建，本地认证时由于口令错误导致的认证失败，将不再转入HWTACACS认证。
- 当配置的认证方式是先HWTACACS认证后本地认证时

  如果步骤3中的用户名在HWTACACS服务器上没有创建，但是在AP上是存在的，经过HWTACACS认证时，将被认为认证失败，不再转入本地认证。

  只有在HWTACACS认证服务器Down时，才会转入本地认证。

推荐采用先HWTACACS认证后本地认证。

步骤7 根据选择的认证模式，执行相应的操作步骤。

- 如果采用了HWTACACS认证，则需进行如下配置：
  a. 执行命令**hwtacacs**，进入端口扩展HWTACACS视图。
  b. 执行命令**hwtacacs-server shared-key** { **cipher** *cipher-string* | *key-string* }，配置与AP的HWTACACS服务器通信的全局共享密钥。

     设置密钥可以提高Master与AP的HWTACACS服务器通信的安全性。
  c. 执行命令**hwtacacs-server** *ip-address* [*port*] [**shared-key** { *key-string* | **cipher** *cipher-string* }] [**secondary**]，配置AP的主备HWTACACS公共服务器。

     其中：

- 如果不指定**shared-key** { *key-string* | **cipher** *cipher-string* }，则使用全局共享密钥。
- 主用服务器和备用服务器的IP地址必须不同，否则配置失败。

说明

如果采用HWTACACS认证，则需要保证步骤3中**login-user**配置的用户名和口令与HWTACACS服务器上的用户名和口令一致，否则AP功能无法正常使用。

- 如果采用了本地认证，则需进行如下配置：
  a. 执行命令**ap-user**，进入虚拟接入AP-USER视图。
  b. 执行命令**local-user** *user-name* **password cipher** *password*，在AP上创建一个本地用户名并配置登录口令。

说明

如果采用本地认证，则需要保证步骤3中**login-user**配置的用户名和口令与**local-user**配置的用户名和口令一致，否则AP功能无法正常使用。

步骤8 执行命令**commit**，提交配置。

----结束

配置内联接口

为了建立起端口扩展系统，需在Master与AP之间配置内联接口。

背景信息

在端口扩展系统内部，数据流量需要通过AP与Master内联接口之间的内部转发通道进行传输，为了建立起该通道，需要将Master与AP之间物理直连的接口设置为物理内联接口。当需要增加带宽或提升可靠性时，还可以将Master和AP之间的Eth-Trunk接口设置为Trunk内联接口。

说明

物理内联接口和Trunk内联接口都不支持配置具体业务，也不支持创建子接口。

当用户希望查看与Master上的物理内联口相连的AP上的物理内联口时，可以在用户视图下执行**link detect interface** *interface-type interface-number*，触发Master发送LAD报文，然后执行**display link neighbor interface** *interface-type interface-number*命令查看Master和AP之间内联口的邻居信息。

操作步骤

- 配置物理内联接口
  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**interface** *interface-type interface-number*，进入Master与AP之间物理直连的接口视图。
  c. 执行命令**virtual-access enable**，使能接口的端口扩展能力，设置为物理内联接口。

     执行此步骤后，对应的接口将自动使能端口扩展的IS-IS进程，并自动配置**isis circuit-type p2p**命令，将当前接口模拟为P2P类型。

说明

- 如果用户先在当前接口下手动配置**isis enable** *process-id*命令，然后再配置**virtual-access enable**命令，则当前接口不再自动使能端口扩展的IS-IS进程，也不会自动配置**isis circuit-type p2p**命令。此时需要用户确保进程号为*process-id*的IS-IS进程已使能端口扩展能力，并在当前接口下手动配置**isis circuit-type p2p**命令，配置工作量较大。因此，建议用户采用自动配置的方案，不要在配置**virtual-access enable**命令之前手动配置**isis enable** *process-id*命令。
- AP自动上线成功之后，AP上的所有以太接口自动使能端口扩展能力，同时AP会在对应的接口下自动保存**virtual-access enable**的配置，无需用户配置。

d. 执行命令**dcn**命令，使能内联接口的DCN功能。

e. 执行命令**commit**，提交配置。

f. 执行命令**quit**，退回到系统视图。

g. 执行命令**ap-id** *ap-id*，进入AP视图。

h. 执行命令**inner-connect** *ap-interface-type ap-interface-number* **binding** *master-interface-type master-interface-number*，配置AP与Master之间内联接口的绑定关系。

其中

- 参数*ap-interface-type ap-interface-number*指定的是AP上的物理内联接口，*master-interface-type master-interface-number*指定的是Master上的物理内联接口。
- 此步骤配置的接口绑定关系必须与实际物理连接是一致的。

i. 执行命令**commit**，提交配置。

- 配置Trunk内联接口

a. **配置手工负载分担模式Eth-Trunk接口**

其中：

- 配置三层Eth-Trunk接口。
- 在配置向Eth-Trunk接口中加入成员接口时，将Master上与AP直连的物理接口加入到Eth-Trunk中。

b. 执行命令**interface eth-trunk** *trunk-id*，进入Eth-Trunk接口视图。

c. 执行命令**virtual-access enable**，使能Eth-Trunk接口的端口扩展能力，设置为Trunk内联接口。

执行此步骤后，当前Eth-Trunk接口将自动使能端口扩展的IS-IS进程，并自动配置**isis circuit-type p2p**命令，将当前接口模拟为P2P类型。同时，该Eth-Trunk的成员接口自动继承内联接口属性。

说明

如果用户先在Eth-Trunk接口下手动配置**isis enable** *process-id*命令，然后再配置**virtual-access enable**命令，则Eth-Trunk接口不再自动使能端口扩展的IS-IS进程，也不会自动配置**isis circuit-type p2p**命令。此时需要用户确保进程号为*process-id*的IS-IS进程已使能端口扩展能力，并在Eth-Trunk接口下手动配置**isis circuit-type p2p**命令，配置工作量较大。因此，建议用户采用自动配置的方案，不要在配置**virtual-access enable**命令之前手动配置**isis enable** *process-id*命令。

d. 执行命令**commit**，提交配置。

e. 执行命令**quit**，退回到系统视图。

f. 执行命令**ap-id** *ap-id*，进入AP视图。

g. 执行命令**inner-connect** *ap-interface-type ap-interface-number* **binding** *master-interface-type master-interface-number*，配置AP与Master之间内联接口的绑定关系。

其中

- 参数*ap-interface-type ap-interface-numbe*指定的是AP上的物理内联接口，*master-interface-type master-interface-numbe*指定的是Master上Trunk内联接口的成员接口。
- 同一Trunk内联接口的成员接口，只能与同一AP的内联接口绑定。
- 此步骤配置的接口绑定关系必须与实际物理连接是一致的。

执行此步骤之后，AP上会自动完成相应的Trunk内联接口的配置，无需用户配置。

h. 执行命令**commit**，提交配置。

----结束

配置端口扩展接口

通过配置端口扩展接口，可以将AP上的外联接口映射为Master上的虚拟口，达到提升Master端口密度的目的。

背景信息

在端口扩展系统中，AP可以看作是用于扩展Master接口的板卡，接收Master下发的配置和转发表项，并对外提供外联接口。为了提升Master上的接口密度，需要在Master上配置AP的外联接口与Master的内联接口之间的绑定关系，创建相应的端口扩展接口。

当AP上的外联接口需要配置Eth-Trunk时，可以在Master上将端口扩展接口加入到普通的Eth-Trunk接口中，作为端口扩展Trunk接口。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**ap-id** *ap-id*，进入AP视图。

步骤3 执行命令**remote-interface** *ap-interface-type ap-interface-number* [**to** *max-port-number*] **binding** *master-interface-type master-interface-number*，配置AP的外联接口与Master的内联接口之间的绑定关系，并创建相应的端口扩展接口。

其中：

- 参数*ap-interface-type ap-interface-numbe*指定的是AP上的外联接口，*master-interface-type master-interface-numbe*指定的是Master上的物理内联接口或Trunk内联接口。
- 参数*max-port-numbe*指定AP上外联接口的端口编号最大值。配置该参数时，表示配置一组AP外联接口与Master内联接口的绑定关系，并创建一组端口扩展接口。其中，被绑定的外联接口端口编号范围是*ap-interface-number*最后一维数字到*max-port-number*。

端口扩展接口是一种四维接口，它是指定AP的外联接口映射在当前Master上的扩展端口，例如：GigabitEthernet1025/1/0/1，表示该端口扩展接口对应的是AP ID为1025的AP上的外联接口GigabitEthernet1/0/1。通过端口扩展接口，用户可以将AP上的外联接口当作Master本地的接口一样进行各种业务配置。

说明

在AP上线成功后，AP上的所有以太接口都自动使能端口扩展能力，即默认为内联接口。在Master上执行本步骤后，对应AP上的外联接口将自动去使能端口扩展能力，因为同一接口不能既作内联接口又作外联接口。

步骤4 执行命令**commit**，提交配置。

步骤5 （可选）执行命令**quit**，退回到系统视图。

步骤6 （可选）配置端口扩展Trunk接口。根据业务需要，选择执行其中一个配置任务：

- **配置手工负载分担模式Eth-Trunk接口**
- **配置静态LACP模式Eth-Trunk接口**
- **配置手工1:1主备模式Eth-Trunk接口**

在执行上述任务时，需将已创建的端口扩展接口加入到Eth-Trunk接口中。

说明

目前不支持端口扩展接口与本地普通接口加入到同一Eth-Trunk接口中。

----结束

（可选）配置端口扩展系统和外部路由互引

为了便于网管直接管理Master和AP，需要配置端口扩展系统和外部路由互引。

背景信息

端口扩展系统是通过DCN功能来实现AP即插即用的，而DCN网络具有路由隔离的特性，因此，在网管参与管理Master和AP的场景中，需要在Master上配置端口扩展系统与外部的路由互引。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**virtual-access port-extend**，进入端口扩展视图。

步骤3 执行命令**import admin-ip to** { **bgp** [**vpn-instance** *vpn-instance-name*] | **isis** *process-id* [**level-1** | **level-1-2** | **level-2**] | **ospf** *process-id* | **public** }，将Master和AP的管理IP地址路由引入到其他协议的路由中。

此步骤的作用是将端口扩展系统内的路由引入到DCN外部的网络。执行此步骤前，需要根据引入路由协议的类型，在Master上完成相应协议的配置。

说明

当引入路由协议为IS-IS或OSPF时，需要确保网络规划正确，进程号*process-id*没有引入其他路由，否则将配置失败。

步骤4 执行命令**import** { **bgp** [**vpn-instance** *vpn-instance-name*] | **static** [**vpn-instance** *vpn-instance-name*] | **isis** *process-id* | **ospf** *process-id* } **to dcn-ospf** [**route-policy** *route-policy-name*]，将其他协议的路由引入到DCN中。

此步骤的作用是将Master到网管之间的路由引入到端口扩展系统内部的DCN OSPF路由中。执行此步骤前，需要根据被引入路由协议的类型以及采用的路由策略名称，在Master上完成相应协议及路由策略的配置。

步骤5 执行命令**commit**，提交配置。

----结束

检查配置结果

在端口扩展系统建立成功后，可以在Master上查看到AP的基本信息、AP的统计信息、AP接口信息、端口扩展接口信息、NVTAG分配信息等。

前提条件

已经完成建立端口扩展系统的所有配置。

操作步骤

- 使用**display virtual-access ap** [*ap-id*]命令，查看AP的基本信息。
- 使用**display virtual-access ap statistics**命令，查看AP的统计信息。
- 使用**display virtual-access ap-interface** [**ap-id** *ap-id*]命令，查看AP的接口信息。
- 使用**display interface** { *interface-name* | *interface-type interface-number* } **remote**命令，查看外联口对应Master上的端口扩展接口信息。
- 使用**display remote interface** *interface-type interface-number*命令，在Master上查看指定端口扩展接口的信息。
- 使用**display virtual-access bindinfo** [**ap** *ap-id* | **interface** *interface-type interface-number*]命令，在Master上查看内联接口与端口扩展接口的绑定信息。

----结束

1.1.3.2.3 AP 的升级和管理

本节介绍对AP进行升级和管理的相关配置。

背景信息

在端口扩展系统中，控制和管理平面集中在Master上。因此，如下AP的升级和管理配置都可在Master上完成：

- 升级软件包
- 安装补丁
- 重启AP
- 配置AP使用SNMP与网管通信
- 配置AP向syslog服务器发送信息

- 配置AP设备接口的流量统计时间间隔
- 配置AP设备接口的带宽利用率告警阈值
- 配置AP设备信息的时间格式
- 配置AP信息输出方式

配置完成后，Master通过NETCONF通道将上述配置下发到AP上，由AP自动执行。

说明

- 在端口扩展系统软件升级过程中，需先升级AP，然后再逐个升级Master。对Master的升级与普通设备的升级过程相同。
- 请保证Master和AP设备的软件版本一致。Master和Ap的软件版本不一致可能导致AP上线后业务不可用。
- 对于上述升级和管理配置，AP也支持作为独立网元的原有操作方式。

前置任务

在进行AP的升级和管理之前，需完成以下任务：

- **建立端口扩展系统**
- 将升级用的软件包或补丁文件放置在Master或指定服务器上

升级软件包

AP软件包升级可以实现AP设备原有功能的优化、新功能的增加以及解决当前运行版本更新不及时的问题。

操作步骤

步骤1 将用于升级的软件包上传到AP上，有以下几种方式：

软件包来源	AP范围	执行命令
Master	指定范围内的AP	**upgrade download-package** *packagename* **ap-id** { *startapid* [**to** *endapid*] } &<1-10>
	所有AP	**upgrade download-package** *packagename* **all-ap**
指定服务器	指定范围内的AP	**upgrade download-package** *packagename* **server-ip** *ip-address* **server-port** *port-number* **ap-id** { *startapid* [**to** *endapid*] } &<1-10>
	所有AP	**upgrade download-package** *packagename* **server-ip** *ip-address* **server-port** *port-number* **all-ap**

说明

- 执行**upgrade download-package**命令后，需要用户按提示输入SFTP用户名和口令，用于AP与Master或指定服务器之间的SFTP认证。
- 如果软件包来源是指定服务器，则需先配置端口扩展系统与服务器所在网络的路由互引，保证AP与服务器之间的路由互通。
- 为了节省系统的存储空间，用户可以在Master上执行**upgrade delete-package type**命令删除AP上多余的、不再需要使用的软件包。

步骤2 执行命令**display patch-information ap-id** *ap-id*，查看待升级的AP是否存在状态为“Running”的补丁。

步骤3 （可选）执行命令**patch delete all** { **all-ap** | **ap-id** { *startapid* [**to** *endapid*] } &<1-10> }，删除待升级AP上正在运行的补丁文件，直到所有待升级的AP上都没有补丁在运行。

对AP进行软件包升级，必须保证AP上没有正在运行的补丁，否则无法顺利完成系统软件的升级操作。若检查出待升级的AP上存在正在运行的补丁，执行本步操作，否则请跳过此步执行下一步操作。

步骤4 执行命令**startup system-software** *system-file* { **all-ap** | **ap-id** { *startapid* [**to** *endapid*] } &<1-10> }，指定AP在下次启动的系统软件。

其中：

- **all-ap**：配置该Master管理的所有AP下次启动的系统软件。
- **ap-id** { *startapid* [**to** *endapid*] } &<1-10>：配置在指定AP ID范围内的AP下次启动的系统软件。

步骤5 等待一段时间后，执行命令**display startup ap-id** *ap-id*查询设置结果。

----结束

后续处理

为了使更新的软件包立即生效，请进行**AP重启**。

安装补丁

通过为AP安装补丁，可以优化AP的系统功能或增加小型新需求。

操作步骤

步骤1 将补丁文件上传到AP上，有以下几种方式：

补丁文件来源	AP范围	执行命令
Master	指定范围内的AP	**upgrade download-package** *packagename* **ap-id** { *startapid* [**to** *endapid*] } &<1-10>
	所有AP	**upgrade download-package** *packagename* **all-ap**
指定服务器	指定范围内的AP	**upgrade download-package** *packagename* **server-ip** *ip-address* **server-port** *port-number* **ap-id** { *startapid* [**to** *endapid*] } &<1-10>

补丁文件来源	AP范围	执行命令
	所有AP	**upgrade download-package** *packagename* **server-ip** *ip-address* **server-port** *port-number* **all-ap**

说明

- 执行**upgrade download-package**命令后，需要用户按提示输入SFTP用户名和口令，用于AP与Master或指定服务器之间的SFTP认证。
- 如果软件包来源是指定服务器，则需先配置端口扩展系统与服务器所在网络的路由互引，保证AP与服务器之间的路由互通。
- 为了节省系统的存储空间，用户可以在Master上执行**upgrade delete-package type**命令删除AP上多余的、不再需要使用的补丁包。

步骤2 为AP安装补丁有以下两种方式：

- 不中断业务的补丁安装
  a. 执行命令**patch load** *file-name* **all run** { **all-ap** | **ap-id** { *startapid* [**to** *endapid*] } &<1-10> }，为AP加载指定补丁文件。

参数选择	说明
run	补丁加载后处于运行状态，补丁安装已完成。
all-ap	为该Master管理的所有AP加载补丁文件。
ap-id { *startapid* [**to** *endapid*] } &<1-10>	为指定AP ID范围内的AP加载补丁文件。

- 下次启动生效的补丁安装
  a. 执行命令**startup patch** *packagename* **all** { **all-ap** | **ap-id** { *startapid* [**to** *endapid*] } &<1-10> }，指定AP下次启动安装的补丁文件。
  AP重启之后，补丁永久生效。

----结束

后续处理

- 在采用不中断业务的补丁安装方式时：
  - 若补丁安装后，出现异常需要进行补丁包文件的删除，可以执行命令**patch delete all** { **all-ap** | **ap-id** { *startapid* [**to** *endapid*] } &<1-10> }，删除AP的补丁文件。
- 在采用下次启动生效的补丁安装方式时：
  - 若指定下次启动的补丁包文件后，希望取消该文件在下次启动后生效，可以执行命令**reset patch-configure next-startup** { **all-ap** | **ap-id** { *startapid* [**to** *endapid*] } &<1-10> }，清除AP重启后系统启用的补丁包文件。
  - 为了使更新的补丁文件立即生效，请进行**AP重启**。

重启 AP

配置了软件包升级或下次启动生效补丁安装后，重启AP才能使得新的系统软件或补丁及时生效，同时也能快速验证软件包升级或补丁安装是否成功。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**ap-id** *ap-id*，进入相应的AP视图。

步骤3 执行命令**reboot**，重新启动AP。

----结束

配置 AP 使用 SNMP 与网管通信

当需要通过网管统一管理AP时，可以在Master上配置其管理的AP使用SNMP与网管通信。

背景信息

在端口扩展场景中，如果想通过网管统一管理AP，需要在Master的端口扩展视图下配置SNMP功能。配置完成后，只要网管与AP之间的IP路由可达，就可以进行如下交互：

- AP通过Trap向网管上报故障告警。
- AP上记录活动告警，网管可以通过MIB到AP上查询或同步活动告警。

说明

- 在端口扩展系统中，所有的业务配置都在Master上，因此由Master统一上报业务告警。AP独立上报的是自身设备的故障告警。
- Master与网管之间使用SNMP通信，配置过程与普通场景下的配置相同。

请在Master上执行如下操作步骤。

前置任务

在配置AP使用SNMP与网管通信之前，需先完成以下任务：

- **建立端口扩展系统**

  在配置上述任务时，请执行可选任务“**（可选）配置端口扩展系统和外部路由互引**”，使网管与AP之间路由可达。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**virtual-access port-extend**，进入端口扩展视图。

步骤3 执行命令**snmp-agent**，启动SNMP Agent服务。

步骤4 执行命令**snmp-agent sys-info version** { **v1** | **v2c** | **v3** | **all** } *，配置SNMP的协议版本。

步骤5 根据SNMP的协议版本进行配置。建议使用安全性更高的SNMPv3协议版本。

- SNMPv1或SNMPv2协议版本。

  执行命令**snmp-agent community** { **read** | **write** } **cipher** *community-name* [**mib-view** *view-name*]，配置AP设备的读写团体名以及对应的MIB视图。

  团体是NMS和SNMP Agent的集合，用团体名来标志。团体名相当于密码，团体内的设备通信时需要使用团体名来进行认证。只有NMS和SNMP Agent上配置的团体名相同时，才能互相访问。执行此步骤配置AP设备的SNMP团体名，从而实现网管与AP之间的通信。同时还可以通过**snmp-agent community**命令的参数设置团体名可访问的MIB视图等。

- SNMPv3协议版本。

  a. 执行命令**snmp-agent group v3** *group-name* { **authentication** | **privacy** | **noauthentication** } [**read-view** *read-view* | **write-view** *write-view* | **notify-view** *notify-view*]，配置SNMP用户组。

  当网管和设备处在不安全的网络环境中时，比如容易遭受攻击，建议用户配置参数**authentication**或**privacy**，使能数据的认证和加密功能。

  用户可以选择的认证加密模式如下：

  - 不配置**authentication**和**privacy**参数或配置**noauthentication**参数：不认证不加密。适用于网络环境安全，且管理员比较固定的情况下。
  - 配置**authentication**参数：只认证不加密。适用于网络环境安全，但管理员个数多，管理员对设备交叉操作比较频繁的情况下。通过认证可以限制拥有权限的管理员才可以访问该设备。
  - 配置**authentication**和**privacy**参数：既认证又加密。适用于网络环境不太安全，管理员交叉操作多的情况下。通过认证和加密既可以限制特定的管理员访问设备，并且使网络数据以加密形式发送，避免网络数据被窃取，造成关键数据泄露。

  希望网管在指定视图下具有只读权限时（比如级别比较低的管理员），使用**read-view**参数。

  希望网管在指定视图下具有读写权限时（比如级别比较高的管理员），使用**write-view**参数。

  当希望过滤不相关告警并配置被管理设备只向网管发送指定MIB节点的告警信息，使用**notify-view**参数。如果配置了该参数，只有**notify-view**视图下的MIB节点的告警会发送到网管。

  b. 执行命令**snmp-agent usm-userv3** *user-name* [**group** *group-name*]为一个SNMP组添加一个新USM用户。

  c. 执行命令**snmp-agent usm-user**，配置SNMP USM用户的认证方式、加密方式和密码。

  说明

  snmp-agent usm-user命令中的md5、sha、sha2-224、DES56和3DES168算法为弱安全算法，推荐使用其他安全的算法。为避免安全风险，可以执行crypto weak-algorithm disable命令去使能弱安全算法功能。

步骤6 执行命令**snmp-agent target-host host-name** *host-name* **trap address udp-domain** *ip-address* **params securityname cipher** *cipher-name* [[**v1** | **v2c**] | **private-netmanager** | **ext-vb**] *，设置AP发送Trap消息的目的地。

该步骤是设置AP发送的Trap消息的目的网管地址。其中，如果接收Trap的目标主机是华为网管，则请指定关键字**private-netmanager**。如果Trap消息中会携带扩展绑定变量，请指定关键字**ext-vb**。

步骤7 （可选）执行命令**snmp-agent extend error-code enable**，打开AP设备扩展错误码开关。

只有当网管是华为网管，被管理AP设备是华为设备时，才能配置SNMP扩展错误码功能对标准错误码进行扩展，方便用户能够快速准确地定位故障。

步骤8 （可选）执行命令**snmp-agent mib-view** *type view-name oid-tree*，创建MIB视图并限定网管监控和管理的MIB节点。

- 需要网管管理AP上的绝大部分MIB节点，只有一少部分节点不允许网管管理时，或者在现有的MIB视图中希望取消网管对某些节点的访问权限时，使用参数excluded，排除这些MIB节点。
- 需要网管管理AP上的一少部分MIB节点，绝大部分节点不允许网管管理时，或者在现有的MIB视图中添加网管对某些节点的访问权限时，使用参数included，添加这些允许管理的MIB节点。

步骤9 （可选）执行命令**snmp-agent trap enable**，使能AP发送Trap报文。

使能AP向网管发送Trap，可以方便用户定位重要的问题。执行此步骤，可以打开AP上所有模块发送Trap的开关。

步骤10 执行命令**commit**，提交配置。

----结束

配置 AP 向 syslog 服务器发送信息

当需要在Syslog服务器中查看AP的运行信息时，可以在Master上配置其管理的AP向syslog服务器发送信息。

背景信息

AP运行时，系统会实时记录AP运行情况并产生一些信息。启动信息管理功能后，在Master上配置其管理的AP向syslog服务器发送信息，以备存储和查阅，为网络管理员监控AP的运行情况和诊断网络故障提供依据。

请在Master上执行如下操作步骤。

前置任务

在配置AP向syslog服务器发送信息之前，需先完成以下任务：

- **建立端口扩展系统**

  在配置上述任务时，请执行可选任务“**（可选）配置端口扩展系统和外部路由互引**”，使网管与AP之间路由可达。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**virtual-access port-extend**，进入端口扩展视图。

步骤3 执行命令**info-center loghost source** *interface-type interface-number*，配置AP设备向syslog服务器发送信息的源接口信息。

配置成功后，如果AP设备向Syslog服务器发送信息，Syslog服务器就可以通过源接口地址判断信息消息是从哪个AP设备发出的，从而便于Syslog服务器对收到的信息消息检索。

步骤4 执行命令**info-center loghost** *ipv4-address* [{ **local-time** | **utc** } | **facility** *local-number* | **port** *port-number* | **level** *log-level* | **transport** { **udp** | **tcp** }] *，配置当前Master管理的所有AP向指定syslog服务器发送信息。

重复执行此步骤，可以配置AP向多个syslog服务器发送消息，实现Syslog服务器间相互备份的功能。

步骤5 （可选）执行命令**info-center source** { *module-name* | **default** } **channel** { *channel-number* | *channel-name* } [**log** { **state** { **off** | **on** } | **level** *severity* } * | **trap** { **state** { **off** | **on** } | **level** *severity* } * | **debug** { **state** { **off** | **on** } | **level** *severity* } *] *，配置AP向信息通道中输出信息的规则。

步骤6 执行命令**commit**，提交配置。

----结束

配置 AP 设备信息的时间格式

如果用户希望为了适应自身习惯或者本地时间而需要调整AP设备信息的时间格式时，可以进行此配置。

应用环境

为了满足各地不同的时间习惯，用户可以在Master上设置AP设备上信息的时间格式。进行配置后，AP设备上新的信息会按照所设置的时间格式生成。

说明

此配置中的信息指的是日志信息、Trap信息和调试信息。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**virtual-access port-extend**，进入端口扩展视图。

步骤3 配置下列各类信息的时间格式，用户可以根据自己所需的信息选择其中一项或几项进行配置：

- 执行命令**info-center timestamp log** { **boot** | { **date** | **short-date** | **format-date** | **rfc-3339** } [**precision-time** { **tenth-second** | **millisecond** | **second** }] } [**without-timezone**]，配置日志信息的时间格式。
- 执行命令**info-center timestamp trap** { **boot** | { **date** | **short-date** | **format-date** | **rfc-3339** } [**precision-time** { **tenth-second** | **millisecond** | **second** }] } [**without-timezone**]，配置Trap信息的时间格式。
- 执行命令**info-center timestamp debugging** { **boot** | { **date** | **short-date** | **format-date** | **rfc-3339** } [**precision-time** { **tenth-second** | **second** | **millisecond** }] } [**without-timezone**]，配置调试信息的时间格式。

当采用**date**类型时，时间格式各部分介绍如下表所示。

表 1-21 date 类型的时间格式各部分描述

字段	含义	取值
yyyy	年份	4位数字格式。
mm	月份	中文环境：1～12。西文环境：Jan，Feb，Mar，Apr，May，Jun，Jul，Aug，Sep，Oct，Nov，Dec。
dd	日期	中文环境：1～31。西文环境：如果日期的值小于10，则在日期前面补一个空格，例如“ 7”。
hh:mm:ss	本地时间，时:分:秒	hh采用24小时制，取值范围是00～23，mm和ss取值范围都是00～59。

步骤4 执行命令**commit**，提交配置。

----结束

配置 AP 信息输出方式

用户可以通过此配置，使AP上的信息输出到本地文件或显示区，还可以设置文件和显示区的一些属性。

背景信息

AP设备以日志信息的形式实时记录AP运行时出现的各种情况。通过配置信息输出方式，用户可以登录AP设备查看相关日志信息，了解AP的运行情况。

请在Master上执行如下操作步骤。

操作步骤

- 配置信息输出到显示区
  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**virtual-access port-extend**，进入端口扩展视图。
  c. （可选）执行命令**info-center logbuffer size** *buffersize*，配置AP设备上日志信息的显示数目。
  d. 执行命令**info-center source** { *module-name* | **default** } **channel** { *channel-number* | *channel-name* } **log** { **state** { **off** | **on** } | **level** *severity* }*，配置AP向信息通道中输出日志信息的规则。
  e. 执行命令**commit**，提交配置。
- 配置信息输入到文件
  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**virtual-access port-extend**，进入端口扩展视图。
  c. （可选）执行命令**info-center debugfile-name** *file-name*，设置AP的debug日志文件名称。

     在AP上，debug日志默认生成的日志文件名为debug.log的文本文件，此步骤可以配置debug日志文件名称，方便根据特殊要求获取debug日志文件。

d. （可选）执行命令**info-center max-debugfile-number** *max-debugfile-number*，设置AP的日志目录下debug日志文件保存的最大个数。

在AP上debug日志默认生成的日志文件名为debug.log的文本文件，当文件大小超过8M时，日志文件会被压缩成debug_*.log.zip 文件。此步骤可以设置日志目录下debug日志文件保存的最大个数。当ZIP文件总数是超过设置的最大数时，系统会删除时间最久的文件。

e. 执行命令**info-center source** { *module-name* | **default** } **channel** { *channel-number* | *channel-name* } [**log** { **state** { **off** | **on** } | **level** *severity* } * | **trap** { **state** { **off** | **on** } | **level** *severity* } * | **debug** { **state** { **off** | **on** } | **level** *severity* } *] *，配置AP向信息通道中输出信息的规则。

f. 执行命令**commit**，提交配置。

----结束

配置 AP 设备接口的流量统计时间间隔

当需要调整AP设备上外联接口的流量统计时间间隔时，可以在Master上完成相应的配置。

背景信息

AP设备上的外联接口都默认使能流量统计功能，有助于监控接口和业务的运行情况。当需要调整AP设备上外联接口的流量统计时间间隔时，在Master上有以下两种方式配置：

- 配置全局流量统计时间间隔

  在相应的AP视图下执行，完成后配置将下发至对应的AP上，配置生效后，AP设备上未在对应端口扩展接口下配置流量统计时间间隔的外联接口，将统一使用全局的时间间隔。

- 配置指定外联接口的流量统计时间间隔

  在相应的端口扩展接口（包括端口扩展Trunk接口）视图下执行，完成后配置将下发至对应的AP上，并在对应的外联接口上设置接口的流量统计时间间隔。此配置的优先级高于全局配置。

操作步骤

- 配置全局流量统计时间间隔
  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**ap-id** *ap-id*，进入相应的AP视图。
  c. 执行命令**set flow-stat interval** *interval*，设置AP设备上全局流量统计的时间间隔。
  d. 执行命令**commit**，提交配置。
- 配置指定外联接口的流量统计时间间隔
  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**interface** *interface-type interface-number*，进入端口扩展接口或端口扩展Trunk接口视图。
  c. 执行命令**set flow-stat interval** *interval*，设置对应AP上指定外联接口的流量统计时间间隔。

d. 执行命令**commit**，提交配置。

----结束

配置 AP 设备接口的带宽利用率告警阈值

当需要调整AP设备上外联接口的带宽利用率告警阈值，可以在Master上完成相应的配置。

背景信息

通过带宽利用率能够了解AP设备的负载，如果带宽利用率超过一定阈值则表明带宽资源已经难以满足当前的业务需求，需对AP设备进行扩容，或将业务迁移到其他AP设备上。AP设备上外联接口默认的带宽利用率告警阈值为90%，如果带宽利用率超过90%产生告警，此时由于带宽利用率已经接近饱和，从发现到扩容或迁移业务这段时间很可能会造成流量丢失。为了避免上述问题，可以调整AP设备上外联接口的带宽利用率告警阈值，例如：将入带宽的告警阈值设置为80%，这样在入带宽利用率达到80%时通过告警提醒用户及时处理，避免影响业务。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**interface** *interface-type interface-number*，进入端口扩展接口视图。

步骤3 执行命令**trap-threshold** { **input-rate** | **output-rate** } *bandwidth-in-use* [**resume-rate** *resume-threshold*]，设置AP设备上对应外联接口的出、入带宽利用率的告警阈值。

执行此步骤时，需要注意：

- *resume-threshold*需要小于等于*bandwidth-in-use*。
- 若不指定**resume-rate** *resume-threshold*，则系统会自动将恢复告警带宽利用率的阈值设置为与产生告警的带宽利用率阈值相等。
- 为了避免告警震荡，*bandwidth-in-use*和*resume-threshold*的取值尽量保持差距。

步骤4 执行命令**commit**，提交配置。

----结束

1.1.3.2.4 维护端口扩展系统

本节介绍端口扩展系统的维护操作。

清除端口扩展接口统计信息

当您需要统计一定时间内端口扩展接口的流量信息，这时必须在统计开始前清除该接口原有的统计信息，使接口重新进行统计。

背景信息

须知

清除计数器信息后，以前的信息将无法恢复，务必仔细确认。

操作步骤

- 在确认需要清除指定端口扩展接口或端口扩展Trunk接口对应的远端计数或远端MIB计数后，请在用户视图下执行命令**reset counters** [**if-mib**] **interface** { *interface-name* | *interface-type interface-number* } **remote**。

----结束

1.1.3.2.5 端口扩展配置举例

本节介绍部署端口扩展系统示例。

配置端口扩展系统示例

本例描述了建立端口扩展系统的详细配置过程。

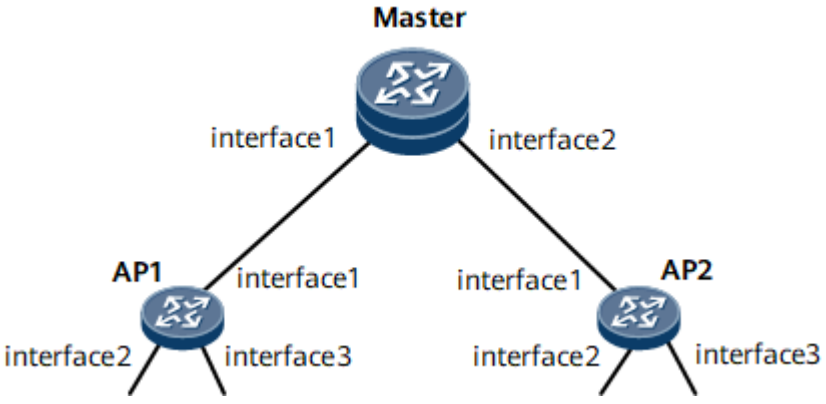
组网需求

端口扩展系统的典型组网如图1-59所示，用于在IP Core网络中提供具备高密度以太类接口的设备。将一台性能较高的设备设置为Master，将大量的支持以太类接口的低端设备设置为AP，把AP上的以太类接口映射为Master上的端口扩展接口，业务配置只需在Master的端口扩展接口上完成，从而使Master设备具备高密度的以太类接口。

图 1-59 配置端口扩展系统的典型组网图

说明

本例中Interface1、Interface2、Interface3分别代表GE1/0/1、GE1/0/2、GE1/0/3。



配置思路

采用如下的思路配置端口扩展系统：

1. 配置Master基本功能。
2. 在Master上配置AP的基本功能。
3. 配置端口扩展的认证方案。
4. 配置内联接口。
5. 配置端口扩展接口。

数据准备

为完成此配置例，需准备如下的数据：

- Master的管理IP地址为1.1.1.1，AP1和AP2的管理IP地址分别为2.2.2.2、3.3.3.3。
- 端口扩展系统的IS-IS认证密钥ID是1，认证密码为YsHsjx_202206。
- Master与AP建立STelnet连接的默认用户名为root，口令为Changeme_123。
- Master与AP1之间的内联接口均为GE1/0/1，Master与AP2之间的内联接口分别为GE1/0/2、GE1/0/1。
- AP1的ID为2000，ESN号（在AP设备上查询）为391092333866236，AP1上的外联接口分别为GE1/0/2和GE1/0/3。
- AP2的ID为2001，ESN号（在AP设备上查询）为391092333000298，AP2上的外联接口分别为GE1/0/2和GE1/0/3。
- Master与AP1、AP2之间采用本地认证方式；Master登录到AP1和AP2所需的用户名为sys-admin，口令为YsHsjx_202207，SFTP目录为cfcard:/；Master在AP1和AP2上创建的本地用户名为sys-admin，口令为YsHsjx_202207。

操作步骤

步骤1 AP设备需保持默认配置

AP首次上线时，Master向AP下发root用户建连，如果：

- AP上线前，用户如果使用STelnet方式首次创建用户登录AP、或者使用串口登录AP时设置串口密码，则AP无法正常上线，需手动恢复空配置并加载预配置文件。以AP1为例，配置如下：

```
<AP1> reset saved-configuration
Warning: The action will delete the saved configuration on the device.
The configuration will be erased to reconfigure.Continue? [Y/N]:y
Warning: Now clearing the configuration on the device.
Info: Succeeded in clearing the configuration on the device.
<AP1> startup default-configuration default-custom_XXX_V***R***C**SPC***.defcfg
Warning: The action will override and update the default configuration file on the device. Continue? [Y/N]:y
...
Info: Succeeded in setting the configuration for booting system.
```

说明

请从华为公司正规渠道获取对应产品版本的预配置文件default-custom_XXX_V***R***C**SPC***.defcfg。

- AP上线后，用户如果修改AP上root用户的密码，则后续AP无法正常与Master建联对账 。

步骤2 配置Master基本功能

```
<Master> system-view
[~Master] ssh client first-time enable
```



```
[~Master] dcn
Warning: This operation will enable DCN function. Continue? [Y/N]:y
Info: The operation may take a few seconds. Please wait for a moment....done.
[*Master] commit
[~Master] virtual-access port-extend
[*Master-virtual-access-portextend] role master
[*Master-virtual-access-portextend] admin 1.1.1.1
[*Master-virtual-access-portextend] ap default login-user root login-password Changeme_123
[*Master-virtual-access-portextend] isis authentication-mode hmac-sha256 key-id 1 cipher
YsHsjx_202206
[*Master-virtual-access-portextend] commit
[~Master-virtual-access-portextend] quit
```

步骤3 在Master上配置AP的基本功能

```
[~Master] ap-id 2000
[*Master-ap2000] esn 391092333866236
[*Master-ap2000] commit
[~Master-ap2000] admin 2.2.2.2
[~Master-ap2000] quit
[~Master] ap-id 2001
[*Master-ap2001] esn 391092333000298
[*Master-ap2001] commit
[~Master-ap2001] admin 3.3.3.3
[~Master-ap2001] quit
```

步骤4 配置端口扩展的认证方案

```
[~Master] ap-id 2000
[~Master-ap2000] login-user sys-admin login-password YsHsjx_202207
[*Master-ap2000] commit
[~Master-ap2000] login-user sys-admin sftp-directory cfcard:/
[~Master-ap2000] ap-user
[~Master-ap2000-ap-user] local-user sys-admin password cipher YsHsjx_202207
[~Master-ap2000-ap-user] quit
[~Master-ap2000] authentication-mode local
[~Master-ap2000] quit
[~Master] ap-id 2001
[~Master-ap2001] login-user sys-admin login-password YsHsjx_202207
[*Master-ap2001] commit
[~Master-ap2001] login-user sys-admin sftp-directory cfcard:/
[~Master-ap2001] ap-user
[~Master-ap2001-ap-user] local-user sys-admin password cipher YsHsjx_202207
[~Master-ap2001-ap-user] quit
[~Master-ap2001] authentication-mode local
[~Master-ap2001] quit
```

步骤5 配置内联接口

```
[~Master] interface GigabitEthernet1/1/0/1
[~Master-GigabitEthernet1/1/0/1] virtual-access enable
[~Master-GigabitEthernet1/1/0/1] dcn
[*Master-GigabitEthernet1/1/0/1] quit
[*Master] interface GigabitEthernet1/1/0/2
[*Master-GigabitEthernet1/1/0/2] virtual-access enable
[*Master-GigabitEthernet1/1/0/2] dcn
[*Master-GigabitEthernet1/1/0/2] quit
[~Master] ap-id 2000
[~Master-ap2000] inner-connect GigabitEthernet1/0/1 binding GigabitEthernet1/1/0/1
[*Master-ap2000] quit
[*Master] ap-id 2001
[*Master-ap2001] inner-connect GigabitEthernet1/0/1 binding GigabitEthernet1/1/0/2
[*Master-ap2001] commit
[~Master-ap2001] quit
```

步骤6 配置端口扩展接口

```
[~Master] ap-id 2000
[~Master-ap2000] remote-interface GigabitEthernet1/0/2 binding GigabitEthernet1/1/0/1
[*Master-ap2000] remote-interface GigabitEthernet1/0/3 binding GigabitEthernet1/1/0/1
[*Master-ap2000] quit
[*Master] ap-id 2001
```



```
[*Master-ap2001] remote-interface GigabitEthernet1/0/2 binding GigabitEthernet1/1/0/2
[*Master-ap2001] remote-interface GigabitEthernet1/0/3 binding GigabitEthernet1/1/0/2
[*Master-ap2001] commit
[~Master-ap2001] quit
```

步骤7 检查配置结果

在Master上执行**display virtual-access ap**命令，可以查看到该Master管理的AP基本信息：

```
[~Master] display virtual-access ap
                        AP Information
-------------------------------------------------------------------------------------------
 AP Esn          : 391092333866236
 AP ID           : 2000          Admin IP      : 2.2.2.2
 Master          : 1.1.1.1
 State           : Online
 Online Time     : 2017-09-30 01:03:56

 AP Esn          : 391092333000298
 AP ID           : 2001          Admin IP      : 3.3.3.3
 Master          : 1.1.1.1
 State           : Online
 Online Time     : 2017-09-30 01:31:26

-------------------------------------------------------------------------------------------
```

在Master上执行**display virtual-access ap-interface**命令，可以查看到该Master管理的AP接口信息：

```
[~Master] display virtual-access ap-interface
                    Ap Interface Information
Total 20 record(s) found:
-------------------------------------------------------------------------------------------
APID  APAdminIP       Interface           IfIndex          State   Type
-------------------------------------------------------------------------------------------
2000  2.2.2.2     GigabitEthernet1/0/1      8              Up      inner
2000  2.2.2.2     GigabitEthernet1/0/2      9              Up      outer
2000  2.2.2.2     GigabitEthernet1/0/3      10             Up      outer
2001  3.3.3.3     GigabitEthernet1/0/1      8              Up      inner
2001  3.3.3.3     GigabitEthernet1/0/2      9              Up      outer
2001  3.3.3.3     GigabitEthernet1/0/3      10             Up      outer
-------------------------------------------------------------------------------------------
```

在Master上执行**display virtual-access bindinfo**命令，可以查看到Master上内联接口与端口扩展接口的绑定信息：

```
[~Master] display virtual-access bindinfo
-------------------------------------------------------------------------------
AP-ID       Inner-interface          Out-interface
-------------------------------------------------------------------------------
2000        GigabitEthernet1/1/0/1       GigabitEthernet2000/1/0/2
2000        GigabitEthernet1/1/0/1       GigabitEthernet2000/1/0/3
2001        GigabitEthernet1/1/0/2       GigabitEthernet2001/1/0/2
2001        GigabitEthernet1/1/0/2       GigabitEthernet2001/1/0/3
```

----结束

配置文件

- AP1的配置文件

```
#
sysname AP1
#
virtual-access
 role ap
 admin 2.2.2.2
```

```
 master admin-ip primary 1.1.1.1
 isis authentication-mode hmac-sha256 key-id 1 cipher %^%#OqaV.B&wk-eu\lD0(u:5ZWFN)r'k:2uIW.-/
9:NU%^%#
#
undo user-security-policy enable
#
ip dcn vpn-instance __dcn_vpn__
 ipv4-family
#
bfd
#
aaa
 local-user sys-admin password irreversible-cipher $1c$VW58EBdUe"$uXfj.2l)I#za`:6tJ,w$U|
([5}MsD#|):rU(cV/+$
 local-user sys-admin service-type ssh
 local-user sys-admin state block fail-times 3 interval 5
 local-user sys-admin user-group manage-ug
 #
 authentication-scheme default0
 #
 authentication-scheme default1
 #
 authentication-scheme default
  authentication-mode local
 #
 authorization-scheme default
 #
 accounting-scheme default0
 #
 accounting-scheme default1
 #
 domain default0
 #
 domain default1
 #
 domain default_admin
  authorization-scheme default
#
isis 65534
 description auto-generated for virtual-access
 is-level level-2
 cost-style wide
 virtual-access enable
 network-entity 00.38ba.33bc.a402.00
 binding interface GigabitEthernet1/0/1 down-weight 10
#
interface GigabitEthernet1/0/1
 undo shutdown
 isis enable 65534
 isis circuit-type p2p
 dcn
 virtual-access enable
#
interface GigabitEthernet1/0/2
 undo shutdown
#
interface GigabitEthernet1/0/3
 undo shutdown
#
interface LoopBack2147483646
 description virtual-access loopback interface
 ip binding vpn-instance __dcn_vpn__
 ip address 2.2.2.2 255.255.255.255
#
interface LoopBack2147483647
 description DCN loopback interface
 ip binding vpn-instance __dcn_vpn__
 ip address 172.16.1.1 255.255.0.0
#
```



```
ospf 65534 vpn-instance __dcn_vpn__
 description DCN ospf create by default
 opaque-capability enable
 hostname
 vpn-instance-capability simple
 area 0.0.0.0
  network 0.0.0.0 255.255.255.255
#
!The DCN function implements the capability of plug-and-play for this device.
!A NE IP address based on the unique NE ID is automatically generated in VPN
!of DCN. It is recommended that the NE IP address be changed to the planned
!one by running the ne-ip X.X.X.X <mask>  command after the device being online.
dcn
 bandwidth ethernet 1024
#
stelnet ipv4 server enable
sftp ipv4 server enable
snetconf ipv4 server enable
stelnet ipv6 server enable
sftp ipv6 server enable
snetconf ipv6 server enable
ssh user sys-admin
ssh user sys-admin authentication-type password
ssh user sys-admin service-type all
ssh user sys-admin sftp-directory cfcard:/
ssh authorization-type default aaa
#
ssh server cipher aes256_gcm aes128_gcm aes256_ctr aes192_ctr aes128_ctr
ssh server hmac sha2_512 sha2_256
ssh server key-exchange dh_group_exchange_sha256
#
ssh server publickey rsa_sha2_256 rsa_sha2_512
#
ssh server dh-exchange min-len 3072
#
ssh client first-time enable
sftp client-source -a 2.2.2.2 -vpn-instance __dcn_vpn__
#
user-interface con 0
#
user-interface vty 0 4
 authentication-mode aaa
 protocol inbound ssh
#
netconf
 idle-timeout 0 0
#
local-aaa-server
#
return
```

- AP2的配置文件

```
#
sysname AP2
#
virtual-access
 role ap
 admin 3.3.3.3
 master admin-ip primary 1.1.1.1
 isis authentication-mode hmac-sha256 key-id 1 cipher %^%#gb0N3W.{o6QZelLT!#yIPjdj/
~Dk8$F&p73~P/x.%^%#
#
undo user-security-policy enable
#
ip dcn vpn-instance __dcn_vpn__
 ipv4-family
#
bfd
#
aaa
```



```
 local-user sys-admin password irreversible-cipher $1c$2"iN;T!PrW$4H+g1J;+D>"[]=$i,Z/4(5"MWJ-Ld
%)']CO`l>Z9$
 local-user sys-admin service-type ssh
 local-user sys-admin state block fail-times 3 interval 5
 local-user sys-admin user-group manage-ug
 #
 authentication-scheme default0
 #
 authentication-scheme default1
 #
 authentication-scheme default
  authentication-mode local
 #
 authorization-scheme default
 #
 accounting-scheme default0
 #
 accounting-scheme default1
 #
 domain default0
 #
 domain default1
 #
 domain default_admin
  authorization-scheme default
#
isis 65534
 description auto-generated for virtual-access
 is-level level-2
 cost-style wide
 virtual-access enable
 network-entity 00.38ba.33bc.a402.00
 binding interface GigabitEthernet1/0/1 down-weight 10
#
interface GigabitEthernet1/0/1
 undo shutdown
 isis enable 65534
 isis circuit-type p2p
 dcn
 virtual-access enable
#
interface GigabitEthernet1/0/2
 undo shutdown
#
interface GigabitEthernet1/0/3
 undo shutdown
#
interface LoopBack2147483646
 description virtual-access loopback interface
 ip binding vpn-instance __dcn_vpn__
 ip address 3.3.3.3 255.255.255.255
#
interface LoopBack2147483647
 description DCN loopback interface
 ip binding vpn-instance __dcn_vpn__
 ip address 172.16.1.2 255.255.0.0
#
ospf 65534 vpn-instance __dcn_vpn__
 description DCN ospf create by default
 opaque-capability enable
 hostname
 vpn-instance-capability simple
 area 0.0.0.0
  network 0.0.0.0 255.255.255.255
#
!The DCN function implements the capability of plug-and-play for this device.
!A NE IP address based on the unique NE ID is automatically generated in VPN
!of DCN. It is recommended that the NE IP address be changed to the planned
!one by running the ne-ip X.X.X.X <mask>  command after the device being online.
```



```
dcn
#
stelnet ipv4 server enable
sftp ipv4 server enable
snetconf ipv4 server enable
stelnet ipv6 server enable
sftp ipv6 server enable
snetconf ipv6 server enable
ssh user sys-admin
ssh user sys-admin authentication-type password
ssh user sys-admin service-type all
ssh user sys-admin sftp-directory cfcard:/
ssh authorization-type default aaa
#
ssh server cipher aes256_gcm aes128_gcm aes256_ctr aes192_ctr aes128_ctr
ssh server hmac sha2_512 sha2_256
ssh server key-exchange dh_group_exchange_sha256
#
ssh server publickey rsa_sha2_256 rsa_sha2_512
#
ssh server dh-exchange min-len 3072
#
ssh client first-time enable
sftp client-source -a 3.3.3.3 -vpn-instance __dcn_vpn__
#
user-interface con 0
#
user-interface vty 0 4
 authentication-mode aaa
 protocol inbound ssh
#
netconf
 idle-timeout 0 0
#
local-aaa-server
#
return
```

- Master的配置文件

```
#
sysname Master
#
virtual-access port-extend
 role master
 admin 1.1.1.1
 ap default login-user root login-password %^%#gOTF'nZ=j7+odk7U&I%>xVl0+h.l8AuNHt2_Y*n~%^
%#
 isis authentication-mode hmac-sha256 key-id 1 cipher %^%#RmQD<'UJ)/Nl3L6*
+L8=*&(P"e4H[B~JbRW!W>3A%^%#
#
rsa peer-public-key 2.2.2.2
 public-key-code begin
 3082010A
  02820101
    009FD60F 4245F341 C86A4717 BB17C282 CE090BB7 12E1A73F FFBF0D44 D51EF073
    49A6CA0D 90077E7C BE173037 2851FDB5 A3390BB9 96EAE330 3F999B47 0A765780
    C21BEA42 9A132975 D3A1D64B DEF6E5C2 4CD6A7F3 909F7574 9B84B0A8 BF744446
    67B00D1D 440DD081 8ABDA172 F995C80C C2953A13 F8D6EECA E835A442 C650A464
    BA4B96A2 15D21EBE DD71D5FC 06F559D9 7DC11AD7 3D538CFC FDD408C8 03AA4B3B
    D93E4764 BBDE5FB8 9A2ACBCF 3E7188EE 81995DC4 5A2C8F63 8994F7DA 0094E410
    96C3F70E 9AFBA22A 273F53A3 D152B245 636419BA 71B03A9A E488BA20 1FC18BFB
    396A66A4 0F325E9C A2F1C0CD 9759E1AA ED9A27E6 68605CE2 D284F541 AAD00ED0
    9F
  0203
    010001
 public-key-code end
 peer-public-key end
#
rsa peer-public-key 3.3.3.3
 public-key-code begin
```



```
 3082010A
  02820101
    00CFEC57 3531F1E0 97D6D719 5A4B3D2D 707EE3DD E3FDF9FA C4B73D47 E6D439B5
    3ED2E12F C63D83B7 E76C9B25 125490F5 30AB7277 3BCCB159 F3C90881 32CCDEDC
    E703EB64 5A46DDD2 969A2368 16CFF8FB DA1628D3 F8989A6B 135B66E5 CDC00157
    68246295 C4670F50 BFD4F1C0 48A2C195 E4243F3A BD6BA3E3 32651930 F8A8E4B5
    3020F373 2A58F15E DFE003B4 1B1ACF80 9E0490C1 BE5A2997 97D8B146 3FB16FF5
    9F26DFF6 F83040AF 012D59EA 943F8AB8 71E21A07 5785537F F6523D9E C3050217
    FD03E7B3 BA72AEEA FD108F6D 644EFABB 7C9F2971 065EE65F DDB61426 6ED5084B
    CC7C99E3 C0B6A4BF 95181DBC E2DF89DD 29A24AD8 51E55CCA 8DB1F130 7CE0798F
    83
  0203
    010001
 public-key-code end
 peer-public-key end
#
rsa peer-public-key 172.16.1.1
 public-key-code begin
 3082010A
  02820101
    009FD60F 4245F341 C86A4717 BB17C282 CE090BB7 12E1A73F FFBF0D44 D51EF073
    49A6CA0D 90077E7C BE173037 2851FDB5 A3390BB9 96EAE330 3F999B47 0A765780
    C21BEA42 9A132975 D3A1D64B DEF6E5C2 4CD6A7F3 909F7574 9B84B0A8 BF744446
    67B00D1D 440DD081 8ABDA172 F995C80C C2953A13 F8D6EECA E835A442 C650A464
    BA4B96A2 15D21EBE DD71D5FC 06F559D9 7DC11AD7 3D538CFC FDD408C8 03AA4B3B
    D93E4764 BBDE5FB8 9A2ACBCF 3E7188EE 81995DC4 5A2C8F63 8994F7DA 0094E410
    96C3F70E 9AFBA22A 273F53A3 D152B245 636419BA 71B03A9A E488BA20 1FC18BFB
    396A66A4 0F325E9C A2F1C0CD 9759E1AA ED9A27E6 68605CE2 D284F541 AAD00ED0
    9F
  0203
    010001
 public-key-code end
 peer-public-key end
#
rsa peer-public-key 172.16.1.2
 public-key-code begin
 3082010A
  02820101
    00CFEC57 3531F1E0 97D6D719 5A4B3D2D 707EE3DD E3FDF9FA C4B73D47 E6D439B5
    3ED2E12F C63D83B7 E76C9B25 125490F5 30AB7277 3BCCB159 F3C90881 32CCDEDC
    E703EB64 5A46DDD2 969A2368 16CFF8FB DA1628D3 F8989A6B 135B66E5 CDC00157
    68246295 C4670F50 BFD4F1C0 48A2C195 E4243F3A BD6BA3E3 32651930 F8A8E4B5
    3020F373 2A58F15E DFE003B4 1B1ACF80 9E0490C1 BE5A2997 97D8B146 3FB16FF5
    9F26DFF6 F83040AF 012D59EA 943F8AB8 71E21A07 5785537F F6523D9E C3050217
    FD03E7B3 BA72AEEA FD108F6D 644EFABB 7C9F2971 065EE65F DDB61426 6ED5084B
    CC7C99E3 C0B6A4BF 95181DBC E2DF89DD 29A24AD8 51E55CCA 8DB1F130 7CE0798F
    83
  0203
    010001
 public-key-code end
 peer-public-key end
#
ip dcn vpn-instance __dcn_vpn__
 ipv4-family
#
bfd
#
dcn
#
isis 65534
 description auto-generated for virtual-access
 is-level level-2
 cost-style wide
 virtual-access enable
 network-entity 00.38ba.1a42.1f01.00
 binding interface GigabitEthernet1/1/0/1 down-weight 10
 binding interface GigabitEthernet1/1/0/2 down-weight 10
#
interface GigabitEthernet1/1/0/1
```

```
 undo shutdown
 isis enable 65534
 isis circuit-type p2p
 dcn
 virtual-access enable
#
interface GigabitEthernet1/1/0/2
 undo shutdown
 isis enable 65534
 isis circuit-type p2p
 dcn
 virtual-access enable
#
interface LoopBack2147483646
 description virtual-access loopback interface
 ip binding vpn-instance __dcn_vpn__
 ip address 1.1.1.1 255.255.255.255
#
interface LoopBack2147483647
 description DCN loopback interface
 ip binding vpn-instance __dcn_vpn__
 ip address 10.1.1.1 255.255.0.0
#
ap-id 2000
 sysname ap2000
 esn 391092333866236
 admin 2.2.2.2
 login-user sys-admin login-password %^%#(p@y@~'n3/4m<"=;YyWDZIyvCQuK5D1JbuYk^ODQ%^%#
 login-user sys-admin sftp-directory cfcard:/
 authentication-mode local
 #
 ap-user
  local-user sys-admin password cipher %^%#otll=pnt1#I_[1TE|k'F9-RT!@>rGAa%<&J@q9H&%^%#
 inner-connect GigabitEthernet1/0/1 binding GigabitEthernet1/1/0/1
 remote-interface GigabitEthernet1/0/2 binding GigabitEthernet1/1/0/1
 remote-interface GigabitEthernet1/0/3 binding GigabitEthernet1/1/0/1
#
ap-id 2001
 sysname ap2001
 esn 391092333000298
 admin 3.3.3.3
 login-user sys-admin login-password %^%#/md1*$flA+)0\t.0B"43,q{>+2*)f-k&PWLDzjcL%^%#
 login-user sys-admin sftp-directory cfcard:/
 authentication-mode local
 #
 ap-user
  local-user sys-admin password cipher %^%#(1F!FQJ[FP&+-H@%pe)G5h9r:g$)DF&19m@N\T(9%^%#
 inner-connect GigabitEthernet1/0/1 binding GigabitEthernet1/1/0/2
 remote-interface GigabitEthernet1/0/2 binding GigabitEthernet1/1/0/2
 remote-interface GigabitEthernet1/0/3 binding GigabitEthernet1/1/0/2
#
interface NULL0
#
ospf 65534 vpn-instance __dcn_vpn__
 description DCN ospf create by default
 opaque-capability enable
 hostname
 vpn-instance-capability simple
 area 0.0.0.0
  network 0.0.0.0 255.255.255.255
#
!The DCN function implements the capability of plug-and-play for this device.
!A NE IP address based on the unique NE ID is automatically generated in VPN
!of DCN. It is recommended that the NE IP address be changed to the planned
!one by running the ne-ip X.X.X.X <MASK> command after the device being online.
dcn
 bandwidth ethernet 1024
#
ssh authorization-type default aaa
```



```
#
ssh client publickey dsa ecc rsa rsa_sha2_256 rsa_sha2_512
#
ssh client cipher aes256_gcm aes128_gcm aes256_ctr aes192_ctr aes128_ctr
ssh client hmac sha2_512 sha2_256
ssh client key-exchange dh_group_exchange_sha256
#
ssh client first-time enable
ssh client 172.16.1.1 assign rsa-key 172.16.1.1
ssh client 172.16.1.2 assign rsa-key 172.16.1.2
ssh client 2.2.2.2 assign rsa-key 2.2.2.2
ssh client 3.3.3.3 assign rsa-key 3.3.3.3
#
user-interface con 0
#
local-aaa-server
#
return
```

