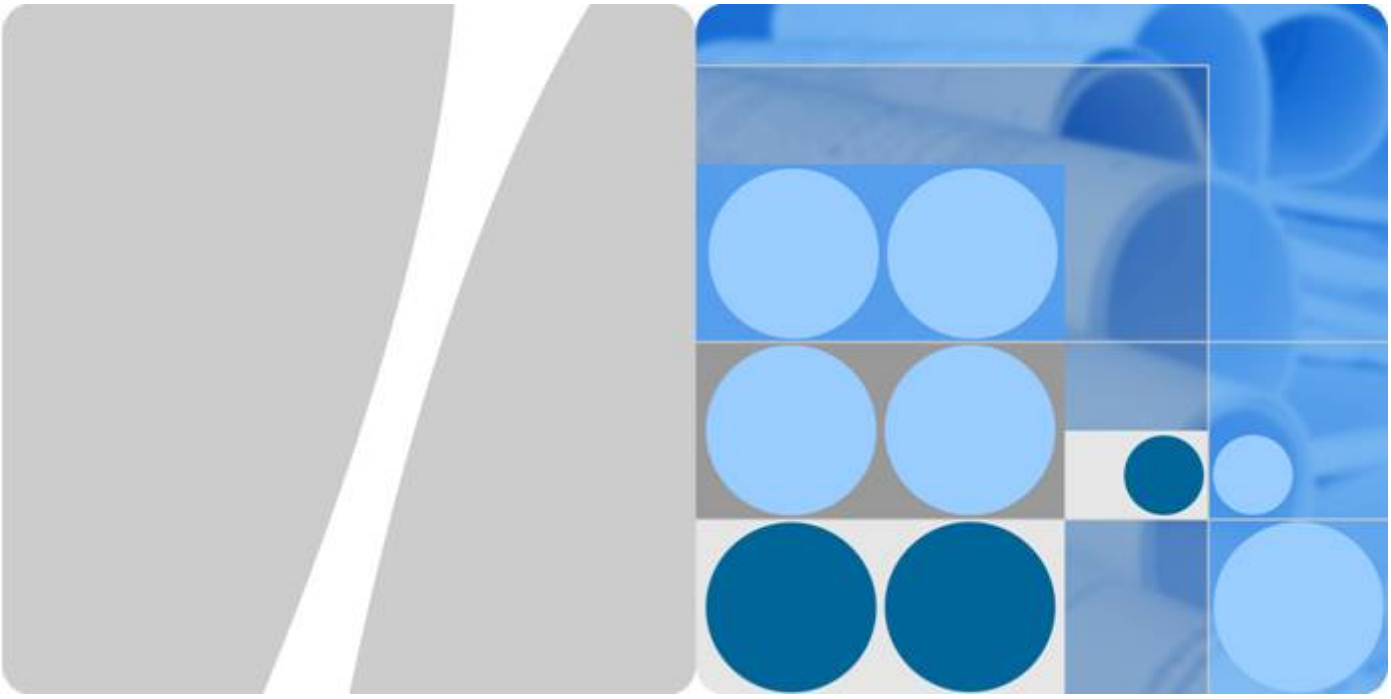


HUAWEI PTN 6900-16 分组传送平台

V600R006C00

产品描述

文档版本　01

发布日期　2012-11-10

华为技术有限公司

版权所有 © 华为技术有限公司 2012。 保留一切权利。

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

商标声明


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

注意

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

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

华为技术有限公司

地址： 深圳市龙岗区坂田华为总部办公楼 邮编：518129

网址： http://www.huawei.com

客户服务邮箱： support@huawei.com

客户服务电话： 4008302118

前 言

概述

本文档针对 PTN 6900 设备的产品特性，从网络应用、功能、结构、特性等几方面进行描述。

本文档介绍设备的网络应用、功能、结构、特性等内容。

产品版本

本文档适用于 PTN 6900-16。

与本文档相对应的产品版本如下所示。

产品名称	产品版本
PTN 6900	V600R006C00
Huawei iManager U2000	V100R008C00

读者对象

本文档主要适用于以下工程师：

- 网络规划工程师
- 硬件安装工程师
- 调测工程师
- 数据配置工程师
- 现场维护工程师
- 网络监控工程师
- 系统维护工程师

符号约定

在本文中可能出现下列标志，它们所代表的含义如下。

版权所有 © 华为技术有限公司

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

图形界面元素引用约定

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

修订记录

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

文档版本 01(2012-11-10)

第一次正式发布。

版权所有 © 华为技术有限公司

目 录

版权所有 © 华为技术有限公司

版权所有 © 华为技术有限公司

版权所有 © 华为技术有限公司

1 产品定位和特点

关于本章

本章介绍 PTN 6900 分组传送平台在网络中的定位和 PTN 6900 分组传送平台的特点。

版权所有 © 华为技术有限公司

1.1 产品定位

PTN 6900 分组传送平台是华为公司面向分组传送的新一代城域光传送设备，主要定位于城域传送网中的核心层和汇聚层，组建移动业务和大客户专线业务的承载网络。

设备简介

各种新兴的数据业务应用对带宽的需求不断增长，同时对带宽调度的灵活性提出了越来越高的要求。作为一种电路交换网络，传统的基于 SDH 的多业务传送网难以适应数据业务的突发性和灵活性。而传统的面向非连接的 IP 网络，由于其难以严格保证重要业务的质量和性能，因此不适宜作为电信级承载网络。

PTN 6900 利用 PWE3（Pseudo Wire Emulation Edge-to-Edge）技术实现面向连接的业务承载，采用针对电信承载网优化的 MPLS（Multiprotocol Label Switching）转发技术，配以完善的 OAM（Operation, Administration and Maintenance）和保护倒换机制，集中了分组传送网和 SDH 传送网的优点，实现了电信级别的业务。

PTN 6900-16 外观如下所示。

PTN 6900-16

PTN 6900-8 外观如下所示。

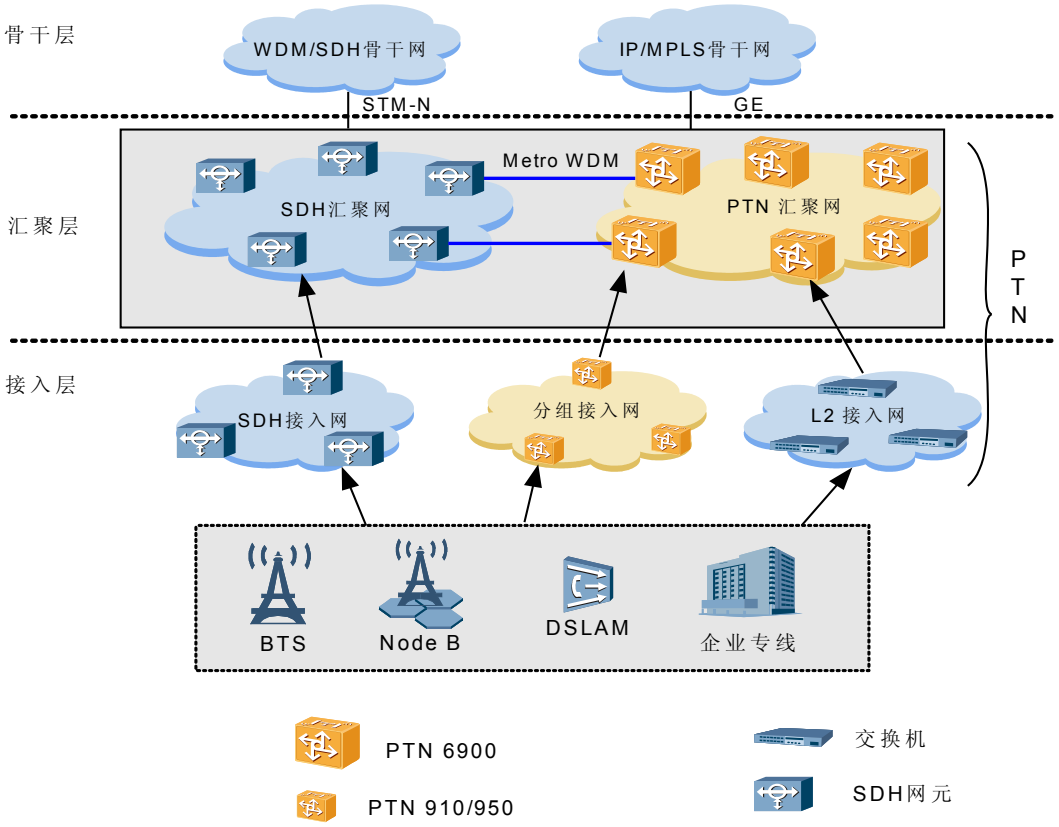
PTN 6900-8

版权所有 © 华为技术有限公司

网络应用

PTN 6900 分组传送平台在网络中的应用如图 1-1 所示。

图 1-1 PTN 6900 分组传送平台的网络应用



1.2 产品特点

PTN 6900 分组传送平台支持多种业务类型，并提供丰富的功能特性，以保证业务传输质量与效率。

1.2.1 丰富的业务类型

PTN 6900 分组传送平台支持 CES 业务、以太网业务、L3VPN 业务和组播业务。

PTN 6900 分组传送平台支持的业务如表 1-1 所示。

表 1-1 PTN 6900 分组传送平台支持的业务类型

业务类型	描述
CES 业务	支持 E1 电接口接入和通道化 STM-1 光接口接入。

版权所有 © 华为技术有限公司

业务类型		描述
以太网业务	以太专线业务（E-Line）	点对点的以太网仿真业务，即 VPWS（Virtual Private Wire Service）业务。
	以太专网业务（E-LAN）	多点对多点的以太网仿真业务，即 VPLS（Virtual Private LAN Service）业务。
L3VPN 业务		采用 BGP/MPLS 技术实现 L3VPN 业务。 支持静态 L3VPN 业务。
多播业务		采用 IGMP Snooping 实现多播业务。

1.2.2 强大的处理能力

PTN 6900 分组传送平台的业务处理能力包括交换能力和业务接入能力。

交换能力

PTN 6900 分组传送平台支持的交换能力如表 1-2 所示。

表 1-2 PTN 6900 分组传送平台交换能力

产品	交换容量	线速 I/O 能力
PTN 6900-16	3200G（单向）	1600G
说明 PTN 6900-16 交换容量的出方向和入方向均为 3200G，即双向为 6400G。当前版本的端口容量为 1600G。		

最大接入能力

PTN 6900 分组传送平台各种接口的接入能力如表 1-3 所示。

表 1-3 PTN 6900 分组传送平台最大接入能力

接口类型	整机最大接口数量
E1/T1	PTN 6900-16：1536
通道化 STM-1	PTN 6900-16：512
FE 电接口	PTN 6900-16：768
FE 光接口	PTN 6900-16：768
GE	PTN 6900-16：768
10GE	PTN 6900-16：160
40GE	PTN 6900-16：32

版权所有 © 华为技术有限公司

1.2.3 丰富的接口类型

PTN 6900 分组传送平台的对外接口包括业务接口和管理及辅助接口。

业务接口

PTN 6900 分组传送平台支持的业务接口如表 1-4 所示。

表 1-4 PTN 6900 分组传送平台业务接口

接口类型	描述	备注
GE 接口	电接口：10/100/1000Base-RJ45 光接口：100/1000Base-X-SFP	可用于客户侧和网络侧
10GE 接口	10GBASE-XFP	可用于客户侧和网络侧
40GE 接口	40GBASE-CFP	可用于客户侧和网络侧
E1 接口	75 欧姆/120 欧姆 E1 电接口：DB100 连接器	可用于客户侧和网络侧
通道化 STM-1 接口	通道化 STM-1 光接口	可用于客户侧和网络侧

管理及辅助接口

PTN 6900-16 提供的管理及辅助接口如表 1-5 所示。

表 1-5 管理及辅助接口

名称	连接器类型	描述
MGMT-ETH 以太网接口（10M/100M/1000M Base-TX 自适应）	RJ45	用于连接系统网管工作站。自带 LINK 和 ACT 指示灯。
Console 接口	RJ45	用于连接控制台，实现对系统的现场配置功能。
AUX 接口	RJ45	用于连接 Modem，通过拨号实现远程维护。
CLK/TOD0	RJ45	用于输入或输出 2Mbps 时钟信号/2MHz 时钟信号/1pps+ASCII 组合的时间信号/2 路 DCLS 时间信号。
CLK/TOD1		

版权所有 © 华为技术有限公司

名称	连接器类型	描述
CLK/1PPS	SMB	用于输入或输出 2Mbps 时钟信号/2MHz 时钟信号/1pps 信号。
CLK/Serial	SMB	用于输入或输出 2Mbps 时钟信号/2MHz 时钟信号/RS232 信号。

1.2.4 分层的 OAM

PTN 6900 分组传送平台具有分层的 OAM 功能，实现各个层面的快速故障检测和定位。

PTN 6900 分组传送平台支持的 OAM 功能如表 1-6 所示。

表 1-6 PTN 6900 分组传送平台支持的 OAM 功能

OAM 类型	实现的 OAM 功能
MPLS Tunnel OAM	CV/FFD
	Ping
	Traceroute
MPLS TP OAM	MPLS-TP OAM 故障管理功能： ● CC（Continuity Check）连通性持续检测 ● CV（Connectivity Verification）转发故障持续检测 ● LB（Loopback Function）环回检测 ● RDI（Remote Defect Indication）远端缺陷通告 ● AIS（Alarm Indication Signal）服务层告警指示 MPLS-TP OAM 性能管理功能： ● LM（Loss Measurement）丢包率统计： – 单端丢包统计 – 双端丢包统计 ● DM（Delay Measurement）时延和时延抖动统计： – 单向时延和时延抖动统计 – 双向时延和时延抖动统计
PW OAM	CV/FFD
	VCCV
	Traceroute

版权所有 © 华为技术有限公司

OAM 类型	实现的 OAM 功能
	性能监测
以太业务 OAM	CC
	LB
	LT
	性能监测
以太端口 OAM	以太网物理链路的连通性及性能检测
BFD	故障检测
业务镜像	本地业务镜像
	远程业务镜像

1.2.5 完善的保护

PTN 6900 分组传送平台提供电信级的设备级保护和网络级保护。

设备级保护

PTN 6900 分组传送平台提供丰富的设备级保护，如表 1-7 所示。

表 1-7 PTN 6900 分组传送平台提供的设备级保护

保护对象	保护方式
交叉和交换网板	PTN 6900-16：3+1 热备份
主控板	1:1 备份
电源	PTN 6900-16：4+4 热备份

网络级保护

PTN 6900 分组传送平台提供丰富的网络级保护，如表 1-8 所示。

表 1-8 PTN 6900 分组传送平台提供的网络级保护

保护对象	保护方式
MPLS Tunnel	1:1 保护
PW	1:1 保护
Ethernet 链路	LAG（Link Aggregation Group）保护、板间 LAG 保护、MC-LAG（Multi-Class）保护

版权所有 © 华为技术有限公司

保护对象	保护方式
	MSTP（Multiple Spanning Tree Protocol）保护
通道化 STM-1	1+1 线性复用段保护
	1:1 线性复用段保护
	MC-线性复用段保护
ATM over E1	IMA 保护

1.2.6 完善的 QoS 机制

PTN 6900 分组传送平台提供层次化的端到端的 QoS（Quality of Service）管理，能够提供高质量的按业务区分的差异化传送服务。

PTN 6900 分组传送平台具备完善的 QoS 调度机制：

- 支持基于流分类的 DiffServ 模式，完整实现了标准中定义的 PHB（Per-hop Behavior），使网络运营商可为用户提供具有不同服务质量等级的服务保证，实现同时承载数据、语音和视频业务的综合网络。
- 提供端到端业务的 QoS
  - 设备在接入侧支持 HQoS（Hierarchical QoS）机制，可以分别控制单个业务类型、单个业务接入点、多个业务接入点、单个业务或多个业务的总带宽。
  - 设备在网络侧支持 TE（Traffic Engineering）机制，平衡网络流量，保证业务质量。

完善的 QoS 机制，可以充分保证不同业务对延迟、抖动、带宽的要求，保证电信级业务的开展。

1.2.7 精确的同步

PTN 6900 分组传送平台支持物理层时钟同步机制，提供外部时钟输入输出接口和设备内部系统时钟，并支持 IEEE 1588 V2 时钟 / 时间同步和 1588 ACR 时钟同步。

物理层时钟

物理层时钟同步机制是从传输链路物理通道的信号中提取时钟信息，从而完成频率同步的技术。

PTN 6900 分组传送平台从以下传输链路中提取时钟信息：

- 支持从通道化 STM-1 接口提取时钟。
- 支持从同步以太网接口提取时钟。
- 支持从 E1 接口提取时钟。
- 支持从 2Mbit/s 或者 2MHz 外时钟接口获取时钟。

同步以太网是一种以太网物理层时钟同步技术，类似于 SDH 时钟。直接从以太线路上的串行码流里提取时钟，并利用该时钟来发送数据，实现时钟的传递。

版权所有 © 华为技术有限公司

IEEE 1588 V2

IEEE 1588 V2 是一种时间同步协议，精度可以达到纳秒级，满足 3G 基站的要求。PTN 6900 分组传送平台支持 IEEE 1588 V2 的以下特性：

- 支持采用 IEEE 1588 V2 协议实现时钟同步和时间同步。
- 支持 BC（Boundary Clock）模式、OC（Ordinary Clock）模式、TC (Transparent Clock)/TC+OC 时钟模式。TC 时钟又可分为 E2E（End-to-End)模式和 P2P(Peer-to-Peer)模式。
- 支持 BMC 时钟选源算法。

1588 ACR

1588 ACR(Adaptive Clock Recover)，是指支持 IEEE 1588 V2 的 Master 设备将本地系统时钟信息封装到 1588 V2（又称 PTP）报文中发送，经第三方网络透传到对端 Slave 设备，Slave 设备从 1588 V2 报文中获取时戳并恢复时钟，实现 PSN 网络两端设备的频率同步。在这种方案里，中间的第三方网络不需要支持 IEEE 1588 V2 协议。

PTN 6900 设备支持的 1588 V2 时钟报文是多播的以太报文。RNC 侧 PTN 6900 设备将携带系统信息的时戳增加到 1588 V2 时钟报文中，通过第三方网络将时钟信息多播到 NodeB 侧的 PTN 6900 设备。PTN 6900 设备接收到 1588 V2 时钟报文后获取时戳，通过计算恢复出时钟并用作系统时钟，同时将时钟传递给 NodeB，从而达到网络两端设备频率同步。

1.2.8 DHCP Relay

PTN 6900 分组传送平台支持 DHCP Relay 功能，实现基站对 IP 地址的自动获取。

基站通电之后，需要通过 DHCP 自动获取 IP 地址。PTN 6900 分组传送平台位于基站与控制器之间的传输线路上，对基站与控制器之间的 DHCP 报文进行中继。从而使基站获取 IP 地址。

版权所有 © 华为技术有限公司

2 产品架构

关于本章

从功能模块、硬件结构、软件结构等方面对 PTN 6900 分组传送平台的产品架构进行介绍。

版权所有 © 华为技术有限公司

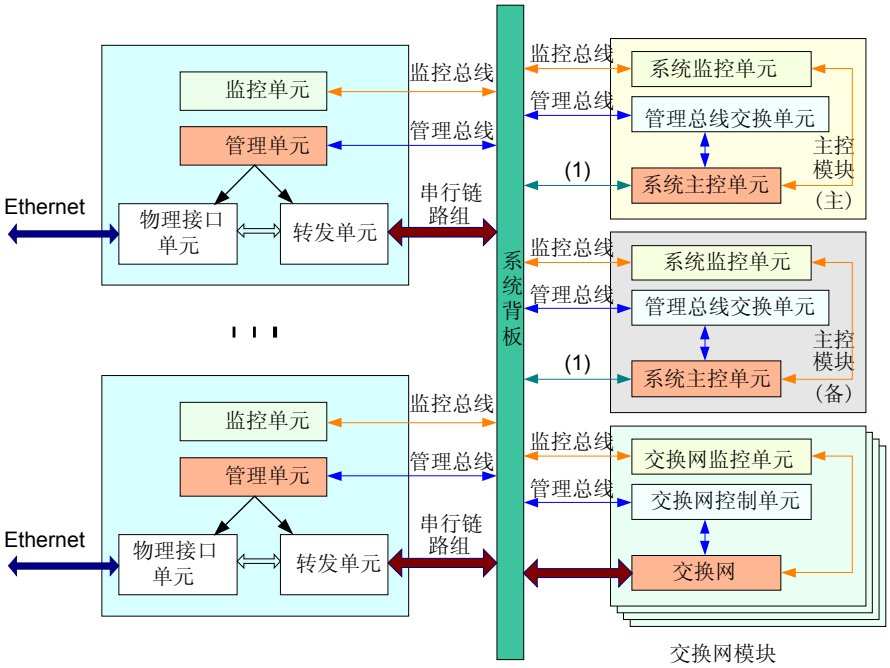
2.1 物理架构

PTN 6900 的物理架构包括以下子系统：

- 电源配电子系统
- 功能主机子系统
- 风扇散热子系统
- 网管子系统

功能主机子系统由系统背板和主控板、业务处理板及交叉和交换板组成。主要完成数据处理功能，此外还完成对整个系统设备的监控和管理。包括控制管理电源配电子系统、风扇散热子系统，并通过网管接口连接到网管系统。功能主机框图如图 2-1 所示。

图 2-1 功能主机框图



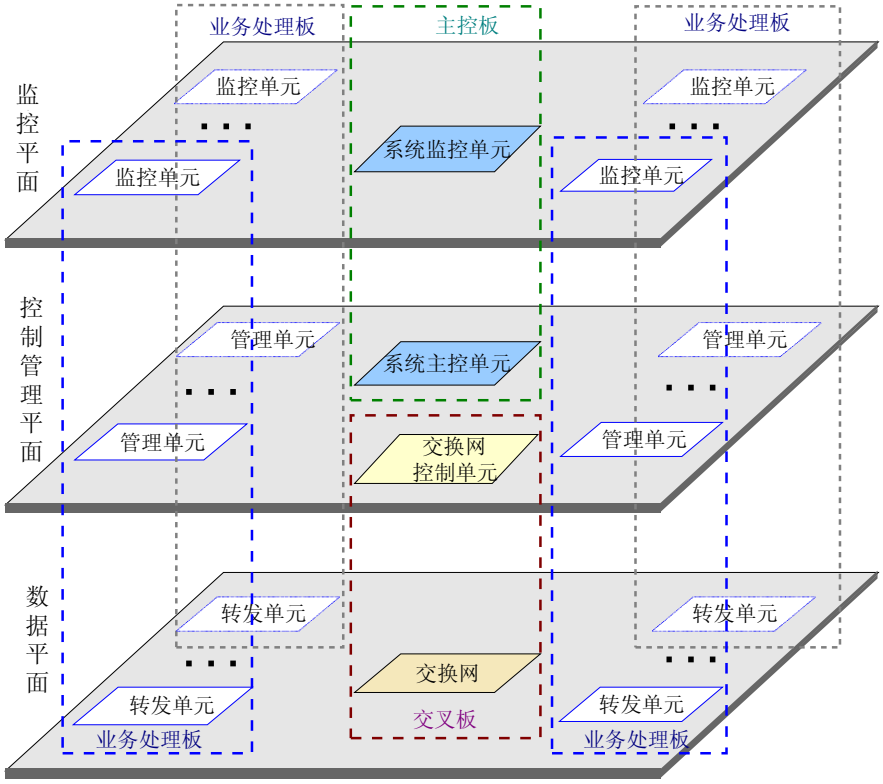
(1)：该链路连接到另一个主控模块的管理总线交换单元

2.2 逻辑架构

PTN 6900 的逻辑架构分为三个平面：数据平面、控制管理平面和监控平面。如图 2-2 所示。

版权所有 © 华为技术有限公司

图 2-2 逻辑框图



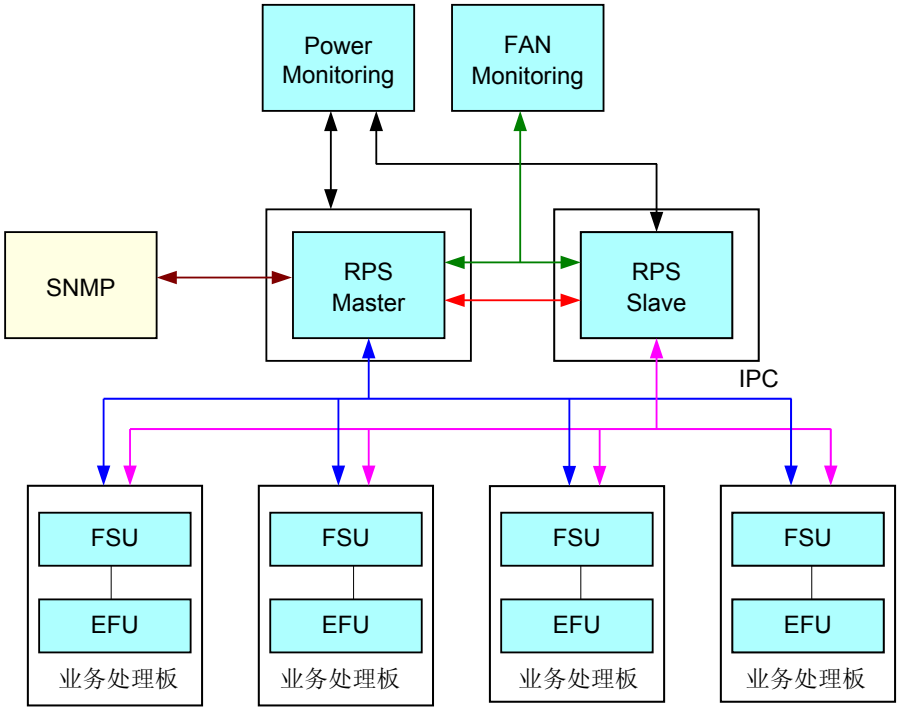
- 数据平面完成数据报文的高速处理和内部无阻塞交换。包括报文的封装与解封装、IPv4/IPv6/MPLS 转发处理、QoS 与调度处理、内部高速交换以及各种统计。
- 控制管理平面完成系统的控制管理功能，是整个系统的中枢神经系统。控制管理单元完成的功能包括协议和信令的处理、系统状态的配置与维护管理、系统状态报告与控制等。
- 监控平面独立完成系统的环境监控，包括电压检测、系统上下电控制、温度监测与风扇控制等，以保证系统的安全稳定运行，在出现单元故障的情况下及时隔离故障，保障系统其它部分的正常运行。

2.3 软件总体架构

PTN 6900 软件总体架构如图 2-3 所示。

版权所有 © 华为技术有限公司

图 2-3 软件总体架构



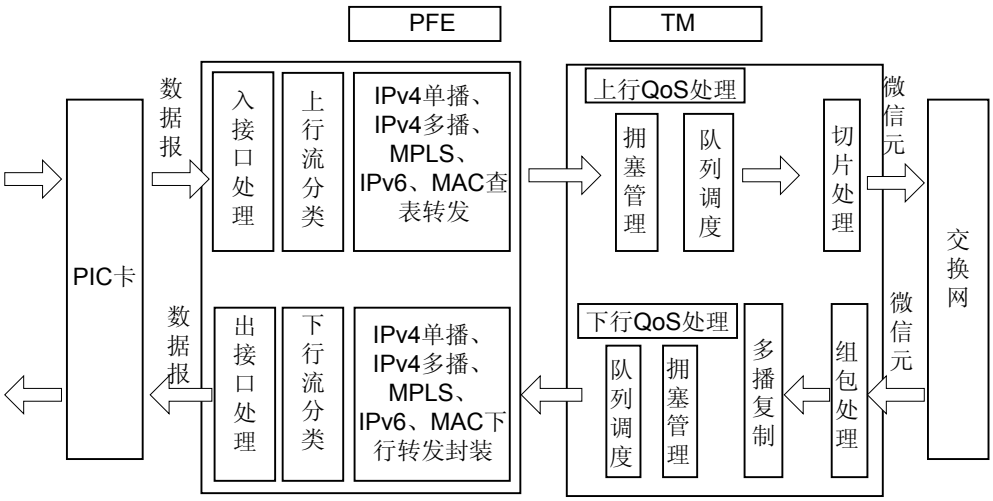
PTN 6900 的软件由 RPS（Routing Process System）、电源监控、风扇监控、FSU（Forwarding Support Unit）和 EFU（Express Forwarding Unit）几部分组成：

- RPS 是系统的控制管理模块，运行于主控板，主用主控板和备用主控板的 RPS 模块互为备份，主要完成 IPv4/IPv6、MPLS、LDP 和路由协议的运行，进行路由计算、LSP 生成、组播树的建立，生成单播、组播和 MPLS 转发表，并将其下发至业务处理板。RPS 包括 IPOS 软件、VRP 软件及产品适配软件。
- FSU 主要完成接口链路层和部分 IP 协议栈的功能。
- EFU 主要完成基于硬件的 IPv4/IPv6 转发、组播转发、MPLS 转发和统计等功能。

版权所有 © 华为技术有限公司

2.4 转发流程介绍

图 2-4 数据转发流程



如图 2-4 所示，包处理引擎（PFE, Packet Forwarding Engines）采用网络处理器（NP, Network Processor）或者专用集成电路（ASIC, Application Specific Integrated Circuit）完成报文高速查表转发功能。外接存储器主要有静态随机存储器（SRAM, Static Random Access Memory）、动态随机存储器（DRAM, Dynamic Random Access Memory）、查找引擎（NSE, Net Search Engine），其中 SRAM 主要存储转发表项，DRAM 存储报文，查找引擎用做非线性查找。

根据数据流方向，可以分为上行、下行两个流程。

- 上行处理流程：报文经 PIC 卡（Physical Interface Card，物理接口卡）打包成帧后，送给 PFE。在入接口处理模块对链路层协议进行解析、识别报文类型，之后在上行流分类模块根据入接口的配置进行流分类，将调度优先级信息携带给 TM（Traffic Manager，流量管理器）供调度使用。随后查转发表项进行转发，例如对于 IPv4 单播报文，根据报文目的 IP 地址查找 FIB（Forwarding Information base，转发信息表）表，获得报文出口和下一跳。最后将查表获得的必要信息和报文一起送给 TM。
- 下行处理流程：在上行已经解析出报文类型，在下行根据报文类型和出接口类型进行链路层封装，存入内部接口。如对于出接口为 Ether 类型的 IPv4 报文，需要根据下一跳获得对应 MAC 地址。之后根据出接口配置情况，可以针对出接口做流分类。最后在出接口处理模块，将新的二层头封装好，发给 PIC。

2.5 硬件结构

本节介绍安装 PTN 6900 所需的机柜、组成部分以及单板类型及安装槽位说明。

2.5.1 概述

PTN 6900 为一体化机箱设计，可以安装在 ETSI（European Telecommunications Standards Institute）标准的 19 英寸标准机柜和 N68E 机柜中。

版权所有 © 华为技术有限公司

PTN 6900 采用集中式路由引擎、分布式转发架构进行设计，在实现大容量转发的同时还可以提供丰富灵活的业务。

PTN 6900 为一体化机箱设计，其主要组成部件都支持热插拔。

PTN 6900 可以安装在 ETSI（European Telecommunications Standards Institute）标准的 19 英寸标准机柜和 N68E 机柜中。

PTN 6900 使用的机柜如图 2-5 所示。

图 2-5 N68E 机柜外形

2.5.2 组成部件及槽位说明

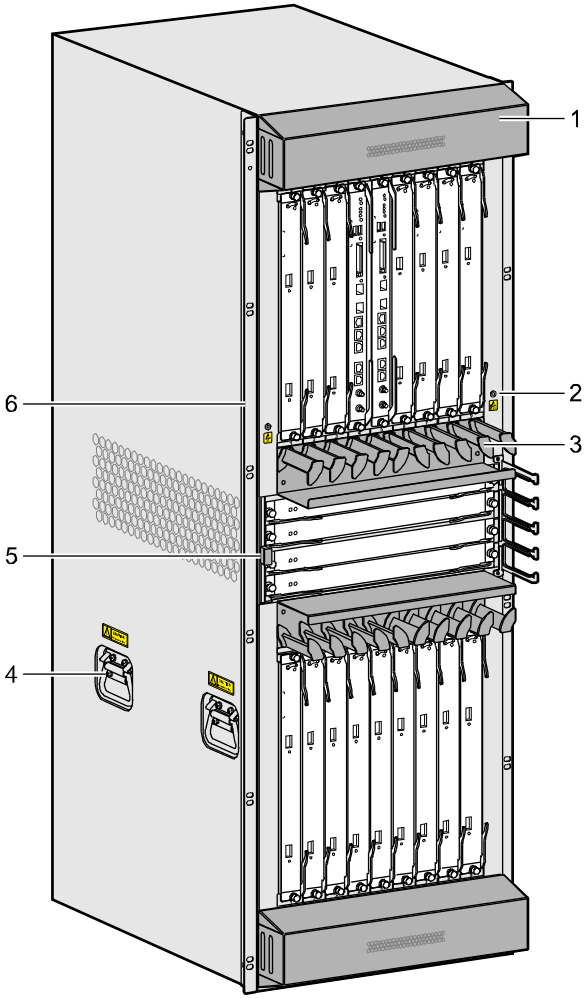
PTN 6900 分为业务处理板区、主控板区、电源板区、风扇区和走线槽。

PTN 6900-16

PTN 6900-16 的组成部件如图 2-6 和图 2-7 所示。

版权所有 © 华为技术有限公司

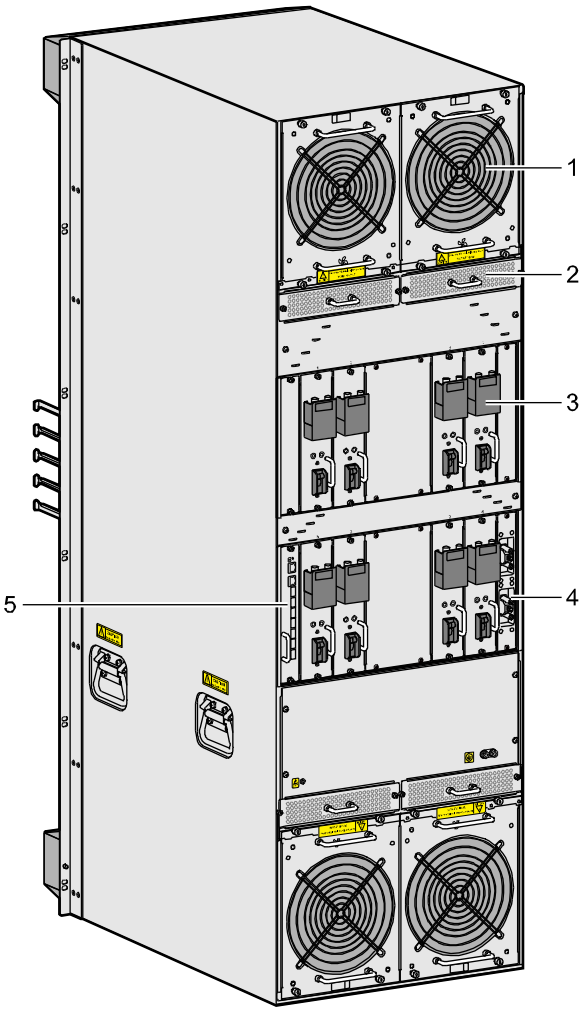
图 2-6 PTN 6900-16 组成部件（正面）



1.进风口　2.ESD 插孔　3.走线槽
4.把手　5.交叉和交换板区防尘网　6.挂耳

华为专有和保密信息
版权所有 © 华为技术有限公司

图 2-7 PTN 6900-16 组成部件（背面）

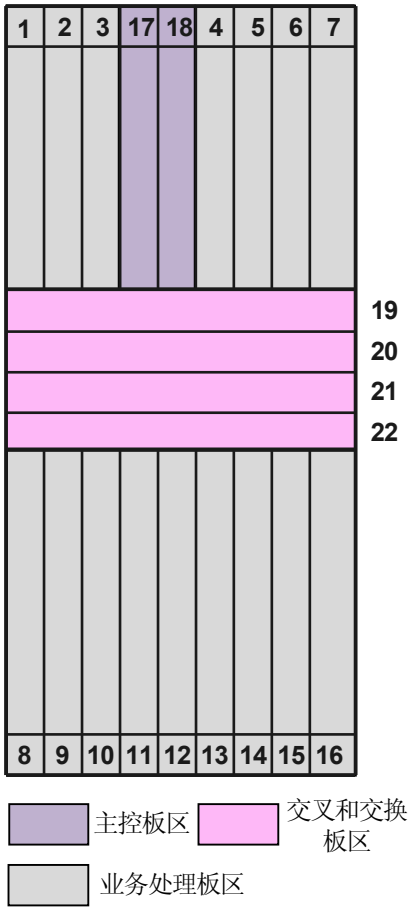


1.风扇模块　2.滤波盒　3.直流电源模块
4.交流电源管理接口　5.环境监控板

PTN 6900-16 的槽位分布如图 2-8 所示。

版权所有 © 华为技术有限公司

图 2-8 PTN 6900-16 槽位分布图



PTN 6900-16 单板槽位分布说明如表 2-1 所示。

表 2-1 PTN 6900-16 单板槽位分布

板槽位	数量	槽位宽度	备注
1 ～ 16	16	41mm（1.6 英寸)	安装业务处理板
17 ～ 18	2	41mm（1.6 英寸）	安装主控板，1:1 备份。
19 ～ 22	4	41mm（1.6 英寸）	安装交叉和交换板，3+1 备份。

2.5.3 单板及其子卡

PTN 6900 支持多种业务处理板，且这些单板可以在 PTN 6900-16 和 PTN 6900-8 共用。

PTN 6900 支持的业务处理板如表 2-2 所示。

版权所有 © 华为技术有限公司

表 2-2 PTN 6900 分组传送平台支持的业务处理板列表

分类	单板名称	重量	功耗
PTN 6900-16	主控及通信处理单元 B(含 1 块 2G 内存和 2 块 1G CF 卡)	4.2 kg	63 W
	40G 交叉和交换处理单元 B	3.5 kg	38 W
	200G 交叉和交换处理单元 B	4.26 kg	90 W
多协议以太网处理灵活插卡板-10及其子卡	多协议以太网处理灵活插卡板-10	5.0 kg	198 W
	8 路 FE/GE 光以太网处理灵活插卡(支持 1588V2)	0.46 kg	22 W
	2 路通道化 OC-3C/STM-1 灵活插卡	0.5 kg	34 W
	24 路通道化 E1/T1-DB100 灵活插卡	0.5 kg	29 W
多协议以太网处理灵活插卡板-40及其子卡	多协议以太网处理灵活插卡板-40	6.6 kg	280 W
	2 路 10GE 以太网处理灵活插卡(支持 1588V2)	0.15 kg	27 W
	20 路 FE/GE 光以太网处理灵活插卡(支持 1588V2)	0.5 kg	39 W
	20 路 FE/GE 电以太网处理灵活插卡	0.61 kg	27 W
多协议以太网处理灵活插卡板-50及其子卡	多协议以太网处理灵活插卡板-50	6.7 kg	184 W
	2 路 10GE 以太网处理灵活插卡(支持 1588V2)	0.5 kg	18.5 W
	8 路通道化 OC-3C/STM-1 灵活插卡	0.5 kg	32 W

版权所有 © 华为技术有限公司

分类	单板名称	重量	功耗
	8 路 FE/GE 光以太网处理灵活插卡(支持 1588V2)	0.46 kg	22 W
	2 路通道化 OC-3C/STM-1 灵活插卡	0.5 kg	34 W
	24 路通道化 E1/T1-DB100 灵活插卡	0.5 kg	29 W
多协议以太网处理灵活插卡板-100及其子卡	多协议以太网处理灵活插卡板-100	6.65 kg	274 W
	5 路 10GE 以太网处理灵活插卡(支持 1588V2)	0.9 kg	29.3 W
	1 路 40GE 以太网处理灵活插卡(支持 1588V2)	1.2 kg	28.8 W
多协议以太网处理灵活插卡板-06及其子卡	多协议以太网处理灵活插卡板-06	8.2 kg	144.4 W
	8 路 FE 光以太网处理灵活插卡(支持 1588V2)	0.46 kg	22 W
	2 路通道化 OC-3C/STM-1 灵活插卡	0.5 kg	34 W
	8 路通道化 OC-3C/STM-1 灵活插卡	0.5 kg	32 W
	24 路通道化 E1/T1-DB100 灵活插卡	0.5 kg	29 W
以太网处理板	10 路 10GE 以太网处理板(支持 1588v2)	8.85 kg	328.6 W
	8 路 10GE 以太网处理板(支持 1588v2)	8.83 kg	318.4 W
	5 路 10GE 以太网处理板(支持 1588v2)	5.55 kg	157 W

版权所有 © 华为技术有限公司

分类	单板名称	重量	功耗
	2 路 40GBase-CFP 以太网处理板(支持 1588V2)	9.65 kg	327.6 W
	12 路 FE/GE 光以太网处理板(支持 1588v2)	5.5 kg	138 W
	16 路 FE/GE 光以太网处理板(支持 1588v2)	5.5 kg	142 W
	24 路 FE/GE 光以太网处理板(支持 1588v2)	5.65 kg	150.6 W
	32 路 FE/GE 光以太网处理板(支持 1588v2)	5.7 kg	159.4 W
	48 路 FE/GE 光以太网处理板(支持 1588v2)	5.75 kg	177 W
	2 路 100GBase-CFP 以太网处理板(支持 1588v2)	327.6W	9.65kg
	6 路 40GBase-CFP 以太网处理板(支持 1588v2)	327.6W	9.65kg
	4 路 40GBase-CFP 以太网处理板(支持 1588v2)	327.6W	9.65kg
	2 路 40GBase-CFP 以太网处理板(支持 1588v2)	327.6W	9.65kg
	24 路 10GE 以太网处理板(支持 1588v2)	157 W	5.55kg

版权所有 © 华为技术有限公司

3 业务简介

关于本章

以下介绍设备的主要业务。

3.1 业务模型
根据对接设备的不同，PTN 6900 设备的业务在 UNI（User-Network Interface）侧和 NNI（Network-Network Interface）侧具有不同的层次模型。

3.2 CES 业务
CES 电路仿真技术在分组传送网络上实现 TDM 电路交换数据的业务透传。PTN 6900 分组传送平台支持对 TDM E1 业务和通道化 STM-1（CES E1）业务的仿真透传。

3.3 IGMP Snooping
IGMP Snooping（Internet Group Management Protocol）功能实现了组播分发。

3.4 以太网业务

3.5 BGP/MPLS L3VPN

3.6 静态 L3VPN
静态 L3VPN 主要应用于 LTE 网络的核心层，它通过在节点之间部署静态路由来实现路由互通，可以提高网络的可靠性。

3.7 IP 特性

3.8 路由协议

3.9 MPLS 特性

3.10 VPN 特性

版权所有 © 华为技术有限公司

3.1 业务模型

根据对接设备的不同，PTN 6900 设备的业务在 UNI（User-Network Interface）侧和 NNI（Network-Network Interface）侧具有不同的层次模型。

PTN 6900 分组传送平台采用基于 MPLS 的 PWE3 模型处理以太网业务和 CES 业务。

PTN 6900 分组传送平台采用 BGP/MPLS 模型处理 L3VPN 业务。

基本概念

相关的基本概念包括：CE、PE、P 和 Site。

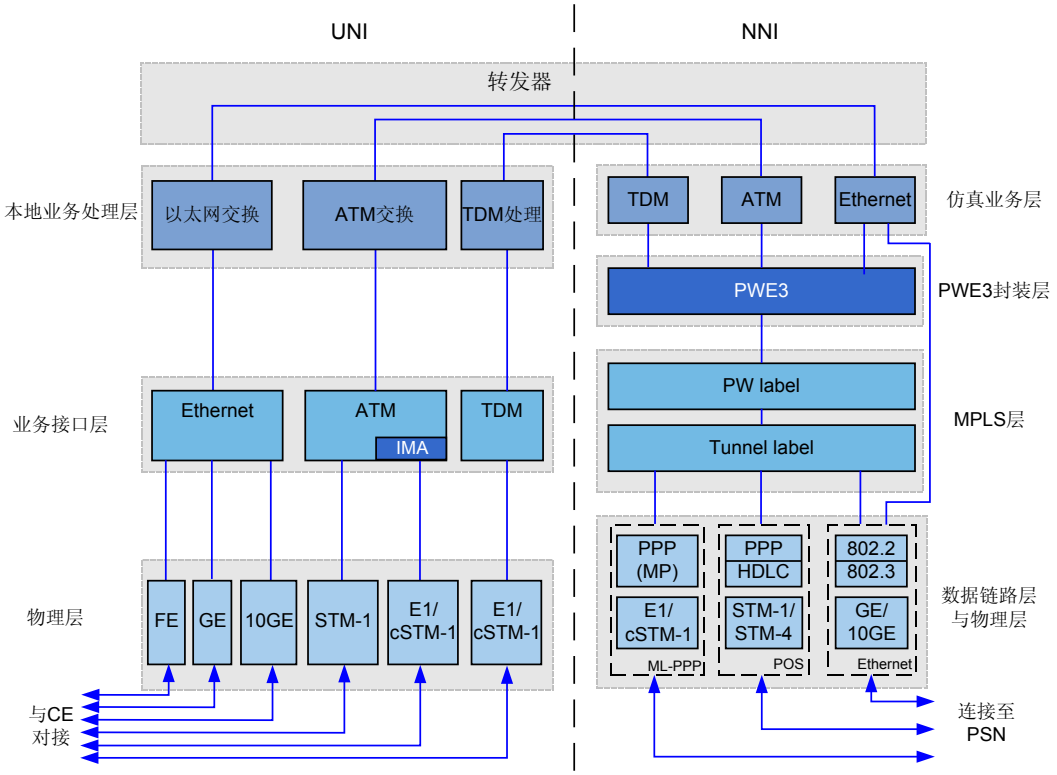
- CE（Customer Edge）：用户网络边缘设备，有接口直接与服务提供商 SP（Service Provider）网络相连。CE 可以是路由器或交换机，也可以是一台主机。通常情况下，CE 不需要支持 MPLS。
- PE（Provider Edge）：服务提供商边缘路由器，是服务提供商网络的边缘设备，与 CE 直接相连。
- P（Provider）：服务提供商网络中的骨干路由器，不与 CE 直接相连。P 设备只需要具备基本 MPLS 转发能力。
- Site：指相互之间具备 IP 连通性的一组 IP 系统，并且，这组 IP 系统的 IP 连通性不需通过服务提供商网络实现。site 通过 CE 连接到服务提供商网络，一个 site 可以包含多个 CE，但一个 CE 只属于一个 site。

基于 MPLS 的 PWE3 模型

PTN 6900 分组传送平台作为 PE 设备时，其基于 MPLS 的 PWE3 业务模型如**图 3-1** 所示。

版权所有 © 华为技术有限公司

图 3-1 基于 MPLS 的 PWE3 模型



UNI 侧与用户设备（CE）对接，负责将用户业务接入 PSN 网络。业务模型 UNI 侧各层次的功能如下：

- 物理层

  物理层提供 PTN 6900 设备与传输媒介（如电缆、光纤）之间的接口。

  - 在 CE->PE 方向，物理层处理由用户设备送来的物理信号（电信号或光信号），从中提取信息，送往业务接口层。
  - 在 PE->CE 方向，物理层接收由业务接口层送来的信息，转换成适合在传输媒介上传输的信号，通过物理通道发往用户设备。

- 业务接口层

  - 在 CE->PE 方向，业务接口层接收物理层上送的信息，区分业务类型，并发往相应的本地业务处理层进行处理。
  - 在 PE->CE 方向，业务接口层接收由本地业务处理层送来的业务信号，选择合适的物理通道类型将数据送往物理层。

- 本地业务处理层

  本地业务处理层按照用户的要求，对不同业务进行相应处理。

NNI 侧与 PSN 设备对接，完成用户业务在 PSN 网络中的传输。业务模型 NNI 侧各层次的功能如下：

- 仿真业务层

  仿真业务层对应于将要被封装入 PW 的净荷。一条仿真业务对应于一条 PW。这是一个抽象的逻辑层次，PTN 6900 设备在此层次不进行具体操作。

华为专有和保密信息
版权所有 © 华为技术有限公司

- PWE3 封装层

  PWE3 封装层针对不同的仿真业务采用各自的封装方式，统一封装成 PWE3 报文，或者从 PWE3 报文中解封装出不同的仿真业务。

- MPLS 层

  MPLS 层包括两层 MPLS 标签：

  - 外层 MPLS 标签为 Tunnel（隧道）标签，用于在业务两端的 PE 站点之间建立和维护一条穿越 MPLS 网络的 Tunnel，以便承载 PW。
  - 内层 MPLS 标签为 PW 标签，用于在同一 Tunnel 中区分不同的 PW。

- 数据链路层与物理层

  数据链路层与物理层作为 MPLS 的承载层，为 MPLS 层提供传输数据的链路。PTN 6900 分组传送平台支持以下网络侧链路类型：

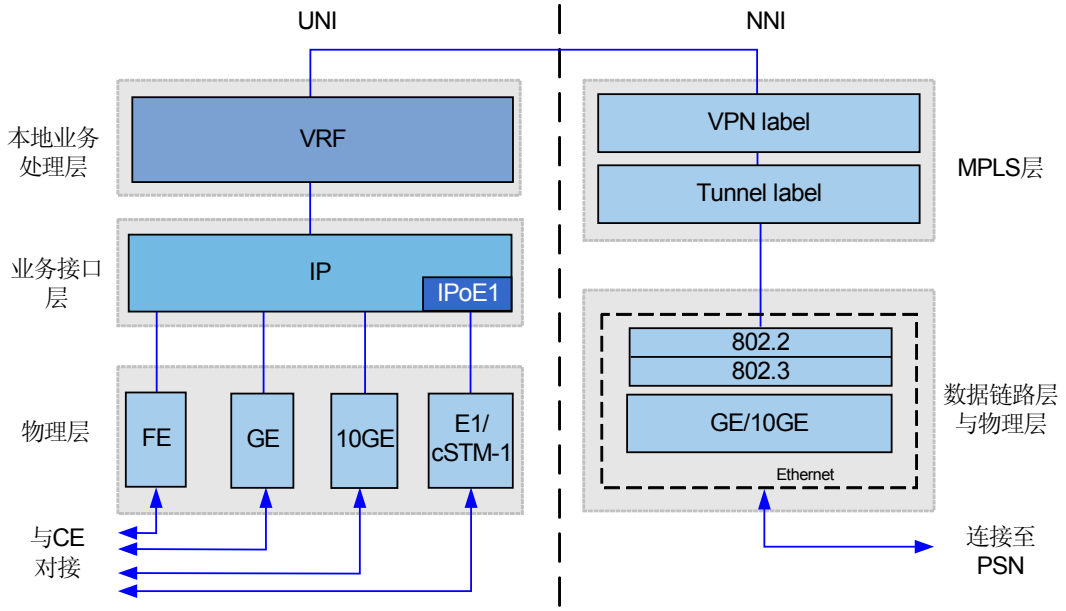
  - 以太网链路（GE/10GE）
  - ML-PPP 链路（E1 接口或通道化 STM-1 接口）

UNI 与 NNI 之间的转发器将 UNI 侧经过本地处理后的业务和 NNI 侧的仿真业务进行相互转发。

BGP/MPLS 模型

PTN 6900 分组传送平台作为 PE 设备时，其 BGP/MPLS 业务模型如图 3-2 所示。

图 3-2 BGP/MPLS 模型



UNI 侧与用户设备（CE）对接，负责将用户的 L3VPN 业务接入公共 PSN 网络。BGP/MPLS 模型 UNI 侧各层次的功能如下：

- 物理层

  物理层提供 PTN 6900 设备与传输媒介（如电缆、光纤）之间的接口。

版权所有 © 华为技术有限公司

- 在 CE->PE 方向，物理层处理由用户设备送来的物理信号（电信号或光信号），从中提取信息，送往业务接口层。
- 在 PE->CE 方向，物理层接收由业务接口层送来的信息，转换成适合在传输媒介上传输的信号，通过物理通道发往用户设备。

- 业务接口层
  - 在 CE->PE 方向，业务接口层接收物理层上送的信息，提取 IP 报文，并发往相应的 VRF（VPN Routing and Forwarding table）进行处理。
  - 在 PE->CE 方向，业务接口层接收由 VRF 送来的业务信号，选择合适的物理通道类型将数据送往物理层。
- 本地业务处理层

  在设备的本地业务处理层，每一个 L3VPN 的业务都由各自独立的 VRF 进行处理。VRF 完成以下功能：
  - 根据本 VPN 的路由表对本 VPN 各业务端口（包括 UNI 端口和 NNI 端口）的 IP 报文进行转发。
  - 通过运行与 CE 相同的路由协议，完成与 CE 设备之间的路由同步更新。
  - 通过 MP-BGP（Multi-protocol Extensions for Border Gateway Protocol）协议，完成 VPN 的私网路由在同一 VPN 内所有 PE 设备上的同步更新。

NNI 侧与 PSN 设备对接，完成 L3VPN 业务在公共 PSN 网络中的传输。BGP/MPLS 模型 NNI 侧各层次的功能如下：

- MPLS 层

  MPLS 层包括两层 MPLS 标签：
  - 内层 MPLS 标签为 VPN 标签，用于在 PE 设备上区分该业务所属的不同 VPN。
  - 外层 MPLS 标签为 Tunnel（隧道）标签，用于在业务两端的 PE 站点之间建立和维护一条穿越 MPLS 网络的 Tunnel，以便承载 L3VPN 业务。
- 数据链路层与物理层

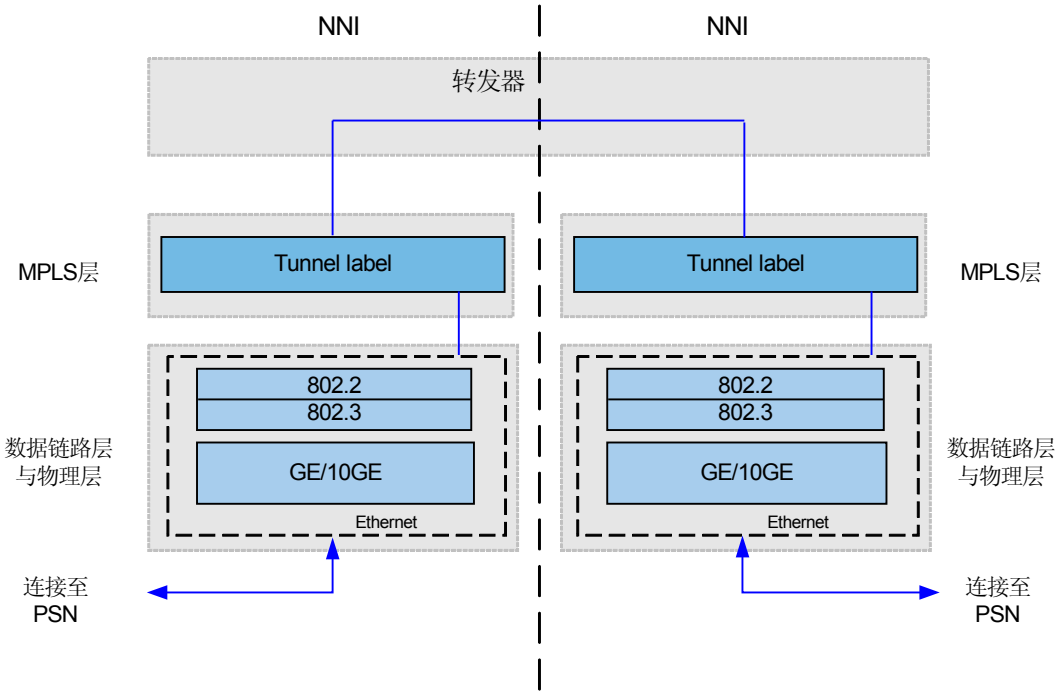
  数据链路层与物理层作为 MPLS 的承载层，为 MPLS 层提供传输数据的链路。PTN 6900 分组传送平台支持以下网络侧链路类型：
  - 以太网链路（FE 接口或 GE 接口）

P 设备的业务模型

PTN 6900 分组传送平台作为 P 设备时，其业务模型如图 3-3 所示。

版权所有 © 华为技术有限公司

图 3-3 PTN 6900 分组传送平台业务模型



NNI 侧与 PSN 设备对接，完成业务在公共 PSN 网络中的传输。

只具有 MPLS 转发功能，PTN 6900 分组传送平台对于进入的 Tunnel label 根据 MPLS 标签转发表进行 MPLS 转发。

3.2 CES 业务

CES 电路仿真技术在分组传送网络上实现 TDM 电路交换数据的业务透传。PTN 6900 分组传送平台支持对 TDM E1 业务和通道化 STM-1（CES E1）业务的仿真透传。

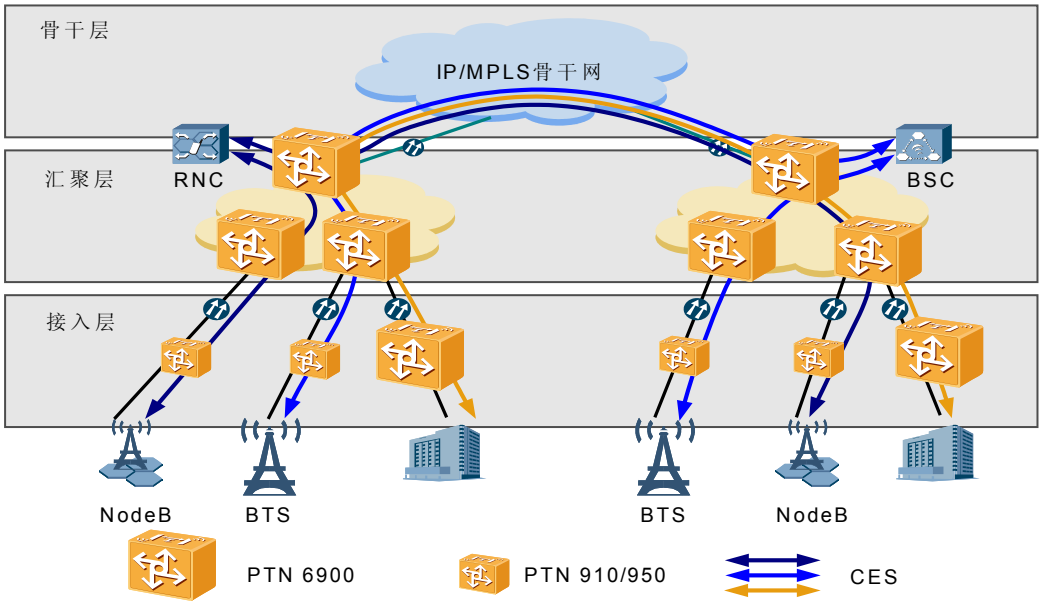
应用模型

PTN 6900 分组传送平台使用 PWE3 技术实现 CES 业务。

CES 业务主要应用在无线业务和企业专线业务中。2G/3G 站点或企业专线通过 E1/通道化 STM-1 线路接入 PTN 6900 设备，设备再将 E1 信号切片封装到数据包中，通过 PW 在城域传送网中传送到对端，如图 3-4 所示。

版权所有 © 华为技术有限公司

图 3-4 CES 业务应用模型



仿真模式

PTN 6900 支持结构化仿真模式和非结构化仿真模式的 CES 业务。

1、结构化仿真

结构化仿真模式即 CESoPSN（Structure-aware TDM Circuit Emulation Service over Packet Switched Network），在此模式下：

- 设备感知 TDM 电路中的帧结构、定帧方式、时隙信息。
- 设备会处理 TDM 帧中的开销，并将净荷提取出来，然后将各路时隙按一定顺序放到分组报文的净荷中，因此在报文中每路业务是固定可见的。
- 提供 TDM 信号中的空闲时隙压缩功能，节省传输带宽。
- 每个承载 CES 业务的数据包装载固定个数的 TDM 帧，报文装载时间可灵活配置。
- 抖动缓冲时间可灵活配置。

2、非结构化仿真

非结构化仿真模式即 SAToP（Structure-Agnostic TDM over Packet），在此模式下：

- 设备不感知 TDM 信号中的任何结构，而将 TDM 信号看成恒定速率的比特流，对整个 TDM 信号进行仿真。
- TDM 信号中的开销和净荷都被透明传输。
- 报文装载时间可灵活配置。
- 抖动缓冲时间可灵活配置。

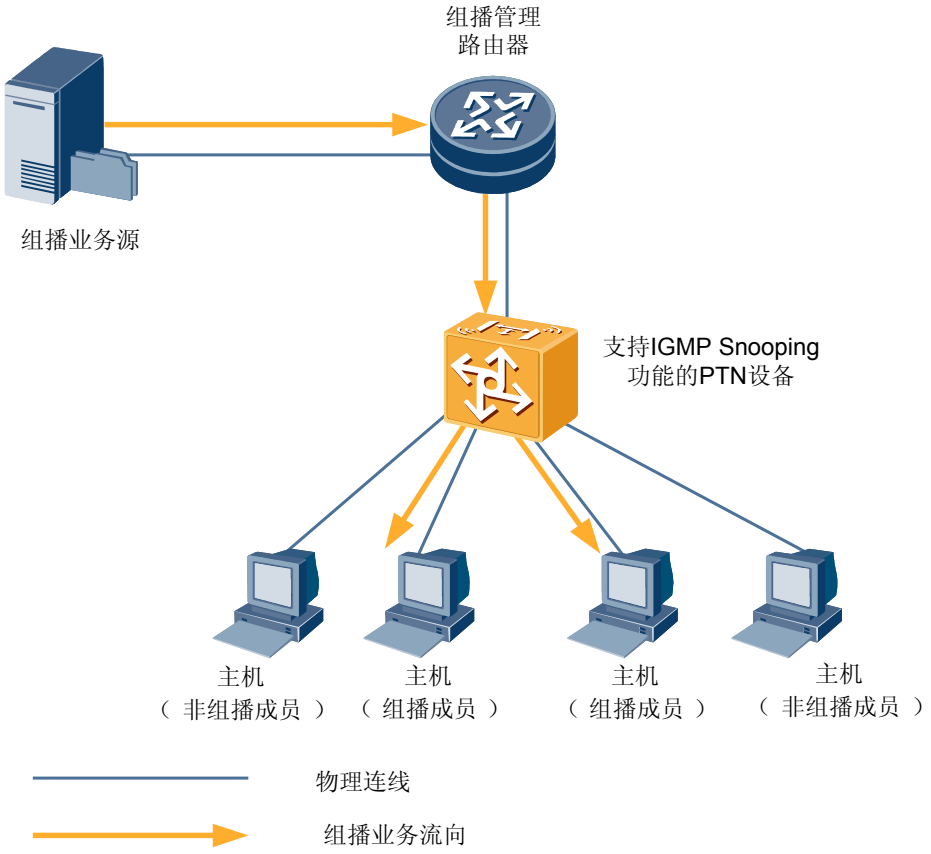
3.3 IGMP Snooping

IGMP Snooping（Internet Group Management Protocol）功能实现了组播分发。

版权所有 © 华为技术有限公司

使能 IGMP Snooping 功能的 PTN 6900 设备通过侦听组播管理路由器与主机之间的 IGMP 协议报文，对路由器端口、组播组以及组播成员进行动态学习，从而避免组播报文在二层交换机中进行广播。由于 IGMP Snooping 具有较强的组播业务感知能力(动态响应客户 IGMP Join/Leave 请求)，所以较适合应用于边缘接入和汇聚层设备，如图 3-5 所示。

图 3-5 支持 IGMP Snooping 功能的设备在网络中的应用



在设备上应用 IGMP Snooping，主要有益于以下三个方面：

- 节约网络带宽。
- 各个 VLAN 独立转发，提高信息安全性。
- 快速响应链路故障，增强可靠性。

3.4 以太网业务

PTN 6900 支持多种形态的以太网业务，提供了完善的 L2VPN 解决方案。

VPN（Virtual Private Network）即指利用公共网络构建的私人专用网络。L2VPN 就是基于链路层技术实现的 VPN。在公共网络上组建的 VPN 可以跟企业现有的私有网络一样提供安全性、可靠性和可管理性。

对于服务提供商而言，向企业提供 VPN 这种增值服务，可以充分利用现有网络资源，提高业务量，同时也加强了与企业的长期合作关系。 对于 VPN 用户而言，使用 VPN 可以缩减网络租赁费用，降低运维负担。VPN 组网的灵活性，也给企业的网络管理带来便

版权所有 © 华为技术有限公司

利。同时随着网络安全和加密技术的发展，也使得通过公用网络传输私有数据的安全性得到保证。

业务形态

PTN 6900 提供的以太网业务主要有两种形态：

- 点对点的业务，即 E-Line 业务
- 多点对多点的业务，即 E-LAN 业务

以太网业务支持进行流分类、带宽控制等 QoS 处理。

ITU-T、IETF 和 MEF 等标准化组织从各自的角度出发对 L2 以太网业务定义了各自的模型框架，如表 1 所示。本文采用 MEF 的定义。

表 3-1 各标准关于 L2 以太网业务定义的对比

业务类型		业务复用（接入侧）	传送隧道（网络侧）	IETF 模型	ITU-T 模型	MEF 模型
点对点业务	Line	物理隔离	物理隔离	-	EPL	E-Line
	Virtual Line	物理隔离	VLAN	-	EPL	
			MPLS	VPWS		
		VLAN	物理隔离	-		
			VLAN	-		
			MPLS	VPWS		
多点对多点业务	LAN	物理隔离	物理隔离	-	EPLAN	E-LAN
	Virtual LAN	VLAN	物理隔离	-	EVPLAN	
			S-VLAN	-		
			MPLS	VPLS		
		S-VLAN	B-MAC B-VLAN	-		

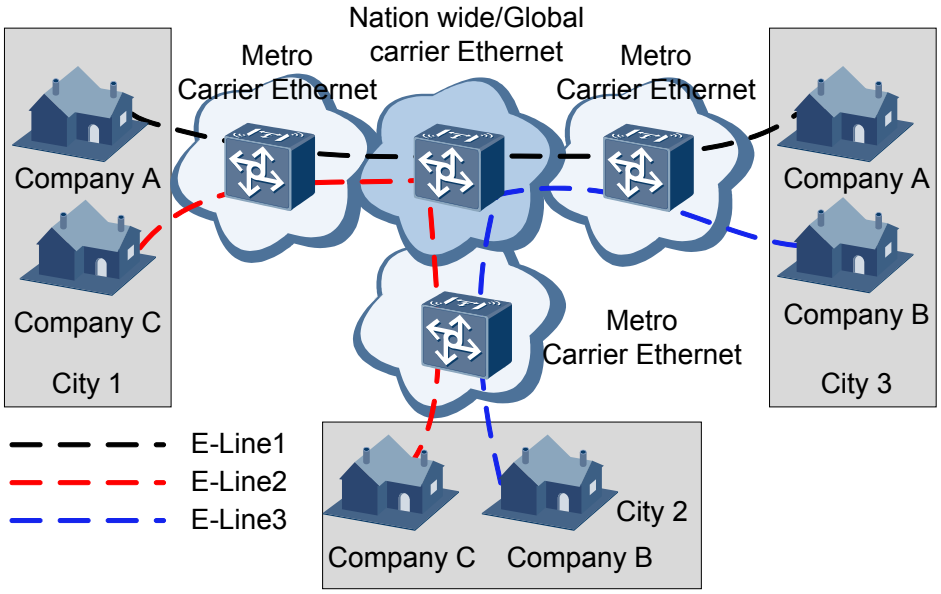
E-Line 业务示例

图 3-6 所示为 PTN 产品提供的 E-Line 业务示例。

A 公司在 City1 和 City3 两地有分部，B 公司在 City2 和 City3 两地有分部，C 公司在 City1 和 City2 两地有分部。A、B、C 公司的异地分部间分别有数据通信的需求。PTN 产品可以分别为 A、B、C 公司提供专线业务，满足其通信需求，同时保证其业务数据完全隔离。

版权所有 © 华为技术有限公司

图 3-6 E-Line 业务示例



E-LAN 业务示例

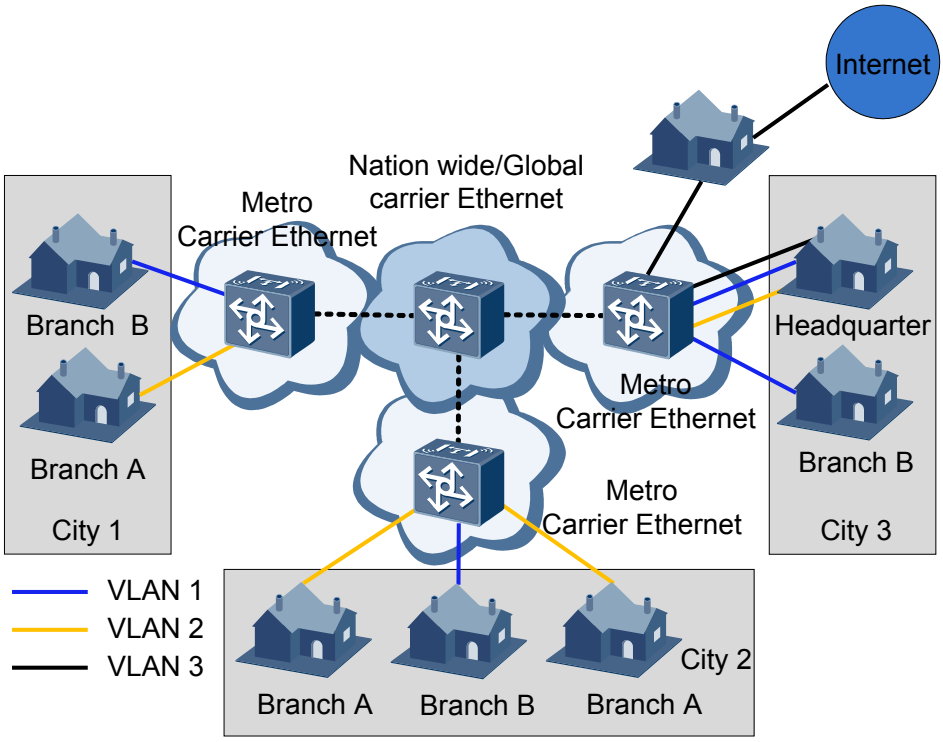
图 3-7 所示为 PTN 产品提供的 E-LAN 业务示例。

Z 公司的总部在 City3。Z 公司在 City1，City2 建有部门 A，在 City1，City2，City3 建有部门 B。部门 A，B 之间无业务往来，需要进行数据隔离；总部与各部门之间有通信需求，同时总部还有接入 Internet 网络的需求。

通过 PTN 产品为 Z 公司提供 E-LAN 服务，用不同的 VLAN 标识不同部门的业务数据，以达到部门内的数据互通和部门间的数据隔离。总部的上网数据也通过 VLAN 与内部的业务数据隔离。

版权所有 © 华为技术有限公司

图 3-7 E-LAN 业务示例



3.5 BGP/MPLS L3VPN

BGP/MPLS VPN 业务介绍

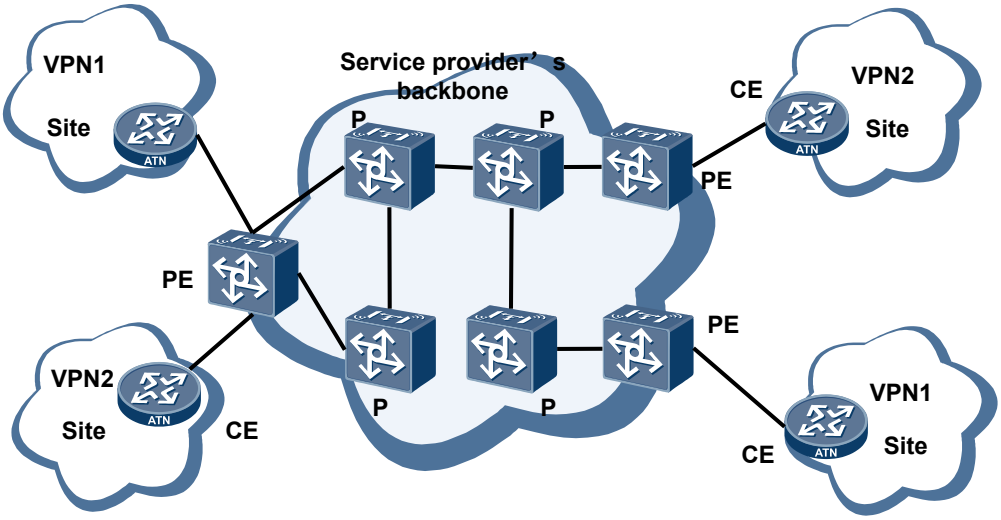
虚拟专用网 VPN 是依靠 ISP（Internet Service Provider）和 NSP（Network Service Provider），在公共网络中建立的虚拟专用通信网络。PTN 设备通过 BGP/MPLS 等协议实现 BGP/MPLS VPN 功能。

1. BGP/MPLS VPN

   BGP/MPLS VPN 使用 BGP（Border Gateway Protocol）在服务提供商骨干网上发布 VPN 路由，使用 MPLS（Multiprotocol Label Switch）在服务提供商骨干网上转发 VPN 报文。BGP/MPLS VPN 的基本模型如图 3-8 所示。

版权所有 © 华为技术有限公司

图 3-8 BGP/MPLS VPN 的模型



BGP/MPLS VPN 的基本模型由以下部分组成：

- CE（Customer Edge）：用户网络边缘设备，有接口直接与服务提供商 SP（Service Provider）网络相连。CE 可以是路由器或交换机，也可以是一台主机。通常情况下，CE“感知”不到 VPN 的存在，也不需要支持 MPLS。
- PE（Provider Edge）：服务提供商边缘设备，是服务提供商网络的边缘设备，与 CE 直接相连。在 MPLS 网络中，对 VPN 的所有处理都发生在 PE 上，对 PE 性能要求较高。
- P（Provider）：服务提供商网络中的骨干设备，不与 CE 直接相连。P 设备只需要具备基本 MPLS 转发能力，不维护 VPN 信息。

PE 和 P 设备仅由 SP 管理；CE 设备仅由用户管理，除非用户把管理权委托给 SP。

一台 PE 设备可以接入多台 CE 设备。一台 CE 设备也可以连接属于相同或不同服务提供商的多台 PE 设备。

2. BGP

BGP 与 IGP 不同，其着眼点不在于发现和计算路由，而在于控制路由的传播和选择最佳路由。VPN 本身就是利用公共网络传递 VPN 数据，而公共网络通常已经应用 IGP 发现和计算自身的路由。构建 VPN 的关键在于控制 VPN 路由的传播，及如何在两个 PE 之间选择最佳的路由。

BGP 使用 TCP 作为其传输层协议，提高了协议的可靠性。可以利用这一点来进行跨设备的两个 PE 设备之间交换 VPN 路由。

BGP 可以承载附加在路由后的任何信息，作为可选的 BGP 属性，任何不了解这些属性的 BGP 设备都将透明的转发它们。这为在 PE 间传播 VPN 路由提供了便利。

路由更新时，BGP 只发送更新的路由，减少了传播路由所占用的带宽，提供了在公共网络上传播大量的 VPN 路由的可能。

BGP/MPLS VPN 业务应用场景

BGP/MPLS VPN 主要包括 Intranet VPN、Extranet VPN 和 Hub and Spoke 三种应用场景。

1. Intranet VPN

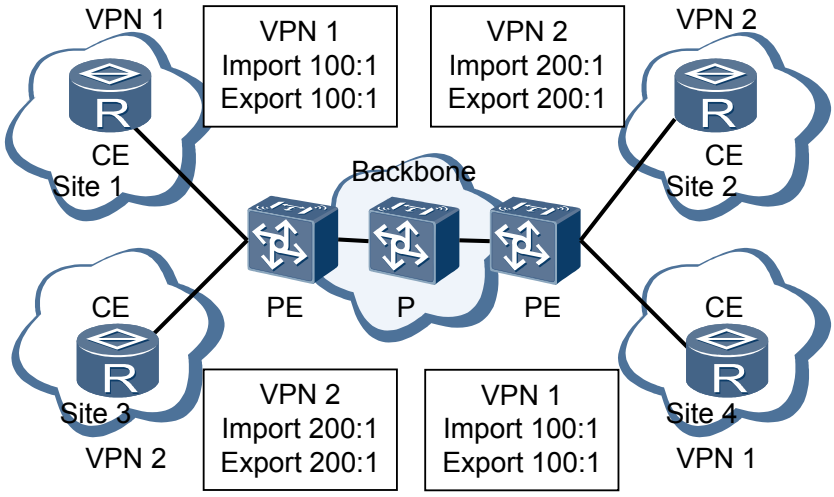
版权所有 © 华为技术有限公司

最简单的情况下，一个 VPN 中的所有用户形成闭合用户群，相互之间能够进行流量转发，VPN 中的用户不能与任何本 VPN 以外的用户通信。这种组网方式的 VPN 叫做 Intranet VPN，其站点通常是属于同一个组织。

对于这种组网，需要为每个 VPN 分配一个 VPN Target，作为该 VPN 的 Export Target 和 Import Target，并且，此 VPN Target 不能被其他 VPN 使用。

在图 3-9 中，PE 上为 VPN1 分配的 VPN Target 值为 100:1，为 VPN2 分配的 VPN Target 值为 200:1。VPN1 的两个 site 之间可以互访，VPN2 的两个 site 之间也可以互访，但 VPN1 和 VPN2 的 site 之间不能互访。

图 3-9 Intranet VPN 组网方案

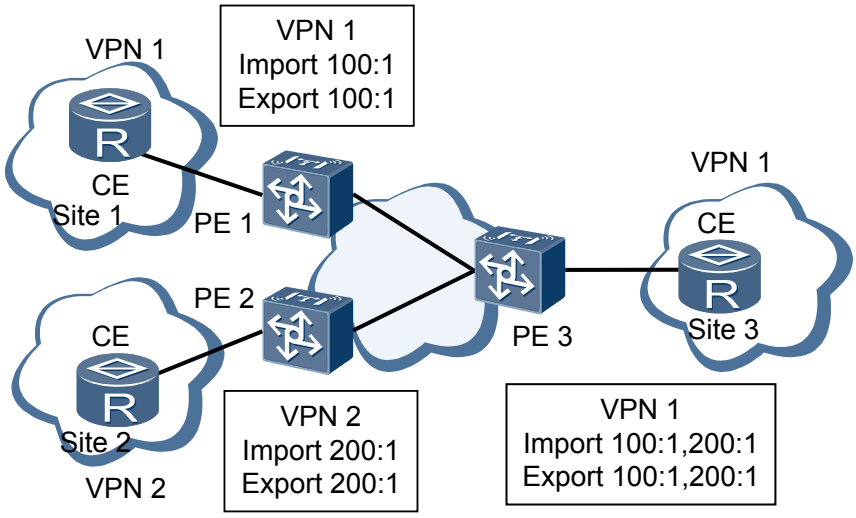


2. Extranet VPN

如果一个 VPN 用户希望提供部分本 VPN 的站点资源给其他 VPN 的用户访问，可以使用 Extranet 组网方案。

对于这种组网，如果某个 VPN 需要访问共享站点，则该 VPN 的 Export Target 必须包含在共享站点的 VPN 实例的 Import Target 中，而其 Import Target 必须包含在共享站点 VPN 实例的 Export Target 中。

图 3-10 Extranet 组网方案



版权所有 © 华为技术有限公司

在图 3-10 中，VPN1 的 site3 能够被 VPN1 和 VPN2 访问：

- PE3 能够接收 PE1 和 PE2 发布的 VPN-IPv4 路由；
- PE3 发布的 VPN-IPv4 路由能够被 PE1 和 PE2 接收；
- 基于以上两点，VPN1 的 site1 和 site3 之间能够互访，VPN2 的 site2 和 VPN1 的 site3 之间能够互访；
- PE3 不把从 PE1 接收的 VPN-IPv4 路由发布给 PE2，也不把从 PE2 接收的 VPN-IPv4 路由发布给 PE1，因此，VPN1 的 site1 和 VPN2 的 site2 之间不能互访。

3. Hub and Spoke

如果希望在 VPN 中设置中心访问控制设备，其它用户的互访都通过中心访问控制设备进行，可以使用 Hub&Spoke 组网方案。其中，中心访问控制设备所在站点称为 Hub 站点，其他用户站点称为 Spoke 站点。Hub 站点侧接入 VPN 骨干网的设备叫 Hub-CE；Spoke 站点侧接入 VPN 骨干网的设备叫 Spoke-CE。VPN 骨干网侧接入 Hub 站点的设备叫 Hub-PE，接入 Spoke 站点的设备叫 Spoke-PE。

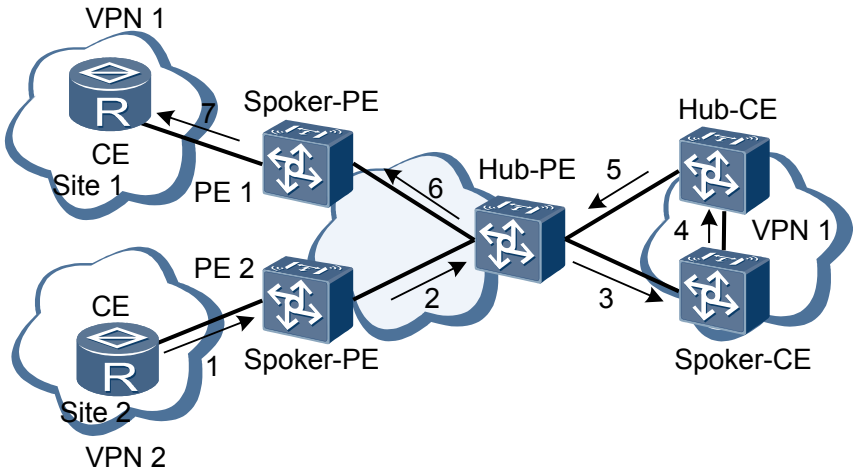
Spoke 站点需要把路由发布给 Hub 站点，再通过 Hub 站点发布给其他 Spoke 站点。Spoke 站点之间不直接发布路由。Hub 站点对 Spoke 站点之间的通讯进行集中控制。

对于这种组网情况，需要设置两个 VPN Target，一个表示“Hub”，另一个表示“Spoke”。

各 site 在 PE 上的 VPN 实例的 VPN Target 设置规则为：

- 连接 Spoke 站点的 PE（Spoke-PE）：Export Target 为“Spoke”，Import Target 为“Hub”；
- 连接 Hub 站点的 PE（Hub-PE）：Hub-PE 上需要使用两个接口或子接口，一个用于接收 Spoke-PE 发来的路由，其 VPN 实例的 Import Target 为“Spoke”；另一个用于向 Spoke-PE 发布路由，其 VPN 实例的 Export Target 为“Hub”。

图 3-11 Hub&Spoke 组网到 Site2 到 Site1 的路由发布途径



在图 3-11 中，Spoke 站点之间的通信通过 Hub 站点进行（图中箭头所示为 site2 的路由向 site1 的发布过程）：

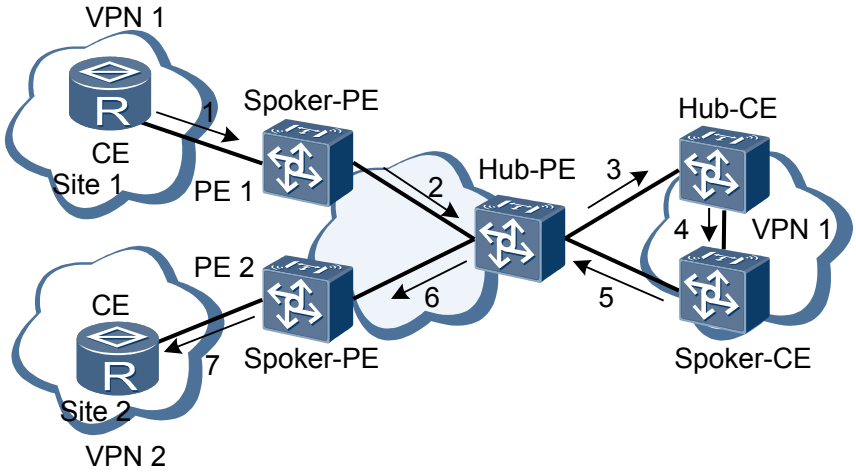
- Hub-PE 能够接收所有 Spoke-PE 发布的 VPN-IPv4 路由；
- Hub-PE 发布的 VPN-IPv4 路由能够为所有 Spoke-PE 接收；

版权所有 © 华为技术有限公司

- Hub-PE 将从 Spoke-PE 学到的路由发布给 Hub-CE，并将从 Hub-CE 学到的路由发布给所有 Spoke-PE。因此，Spoke 站点之间可以通过 Hub 站点互访。
- 任意 Spoke-PE 的 Import Target 属性不与其它 Spoke-PE 的 Export Target 属性相同。因此，任意两个 Spoke-PE 之间不直接发布 VPN-IPv4 路由，Spoke 站点之间不能直接互访。

图 3-11 中的 site1 和 site2 之间通讯数据的传输路径请参见图 3-12（图中箭头所示为数据传输方向）。

图 3-12 Site1 到 Site2 的数据传输途径



3.6 静态 L3VPN

静态 L3VPN 主要应用于 LTE 网络的核心层，它通过在节点之间部署静态路由来实现路由互通，可以提高网络的可靠性。

目的和收益

在 LTE 解决方案中，整个核心层需要部署 L3VPN 业务作为业务交换层。为了避免在核心层部署动态协议给网络所带来的不确定性，在整个核心层部署静态 L3VPN。

与 BGP/MPLS VPN 相比，一方面静态 L3VPN 没有部署动态协议，网络可靠性更高；另一方面，静态 L3VPN 的静态路由都可在网管上进行配置，可操作性和可维护性更好。

组网应用

如图 3-13 和图 3-14 所示，静态 L3VPN 应用于 LTE 网络的核心层，作为 eNodeB 和 MME/SGW 之间的业务交换平面。在接入/汇聚层部署 L2VPN，用来承载从各个基站接入的流量。PTN2 和 PTN5 上分别配置绕接线，实现 L2VPN 和 L3VPN 之间的互通。另外，整个 LTE 网络还综合部署 PW FPS、VRRP、MPLS Tunnel APS、PW APS、VPN FRR 和 BFD 等特性，对业务进行有效保护。

场景一和场景二的区别在于：根据 MME/SGW 对 VRRP 和 Link BFD 的支持情况，PTN 设备和 MME/SGW 对接时采用的方案不同。场景 1 中，PTN 设备和 MME/SGW 上配置 VRRP，并配置 PTN 设备指向 MME/SGW 的静态路由跟踪 VRRP 状态；场景 2 中，PTN

版权所有 © 华为技术有限公司

设备和 MME/SGW 上配置 Link BFD，并配置 PTN 设备指向 MME/SGW 的静态路由跟踪 BFD 状态。

图 3-13 静态 L3VPN 的应用（场景一）

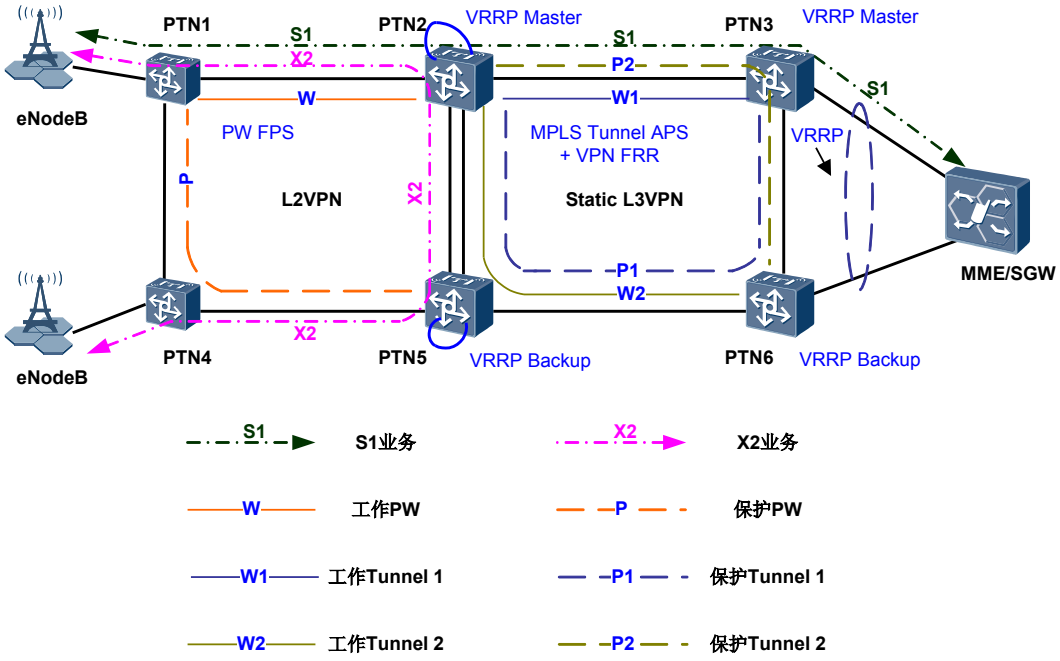
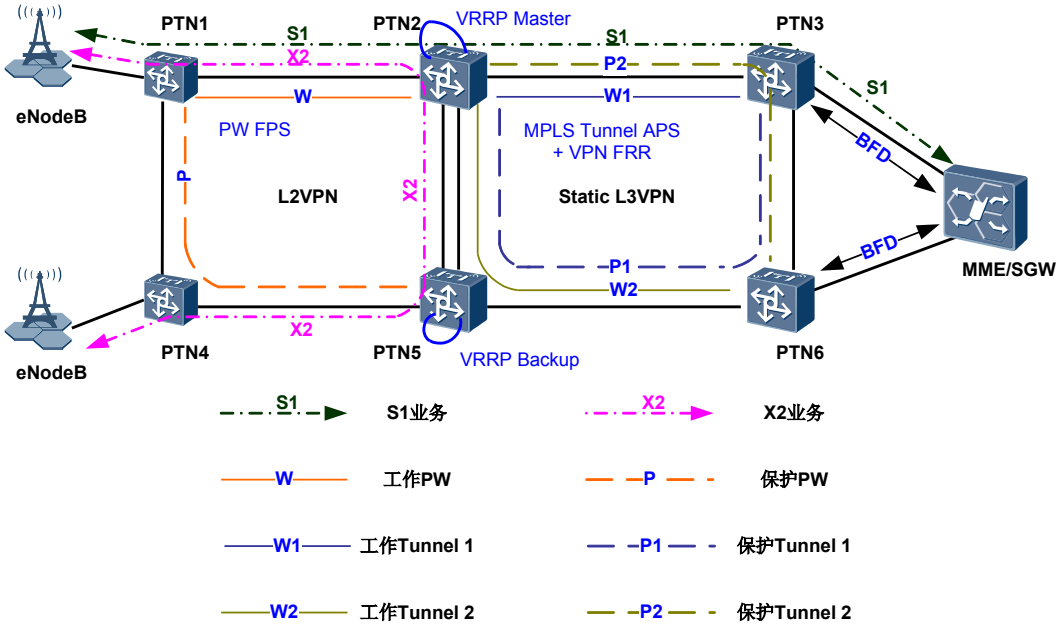


图 3-14 静态 L3VPN 的应用（场景二）



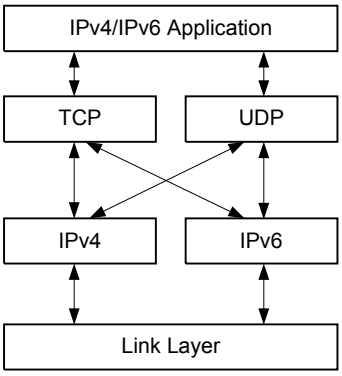
版权所有 © 华为技术有限公司

3.7 IP 特性

3.7.1 支持 IPv4 和 IPv6 双协议栈

IPv4/IPv6 双协议栈具有互通性好和实现简单的优点。它的结构如图 3-15 所示。

图 3-15 双协议栈结构



3.7.2 IPv4 特性

PTN 6900 支持的 IPv4 特性如下：

- 支持基本的 TCP/IP 协议栈，包括 ICMP、IP、TCP、UDP、Socket（TCP/UDP/Raw IP）、ARP。
- 支持静态 DNS 和指定 DNS 服务器。
- 支持 FTP Server/Client、TFTP Client。
- 支持 DHCP Relay Agent、DHCP Server。
- 支持 Ping、tracert 和 NQA 操作。

  NQA 可以探测 ICMP、TCP、UDP、DHCP、FTP、HTTP、SNMP 服务是否打开以及测试各种服务的响应时间。并且在 UDP Jitter 及 ICMP Jitter 测试中，支持基于接口板收发报文的 NQA 特性；支持发包的最小频率为 10ms，每块接口板最大支持并行 100 个 Jitter，整个系统最大支持并行 1000 个 Jitter。
- 支持 IP 策略路由，可根据报文的属性直接指定下一跳，不必查找路由。

3.7.3 IPv6 特性

PTN 6900 支持的 IPv6 特性如下：

- 支持 IPv6 ND（Neighbor Discovery）。
- 支持 PMTU 发现（Path MTU Discovery）。
- 支持 TCP6、Ping IPv6、Tracert IPv6、Socket IPv6。
- 支持静态 IPv6 DNS 和指定 IPv6 DNS 服务器。
- 支持 TFTP IPv6 Client。

版权所有 © 华为技术有限公司

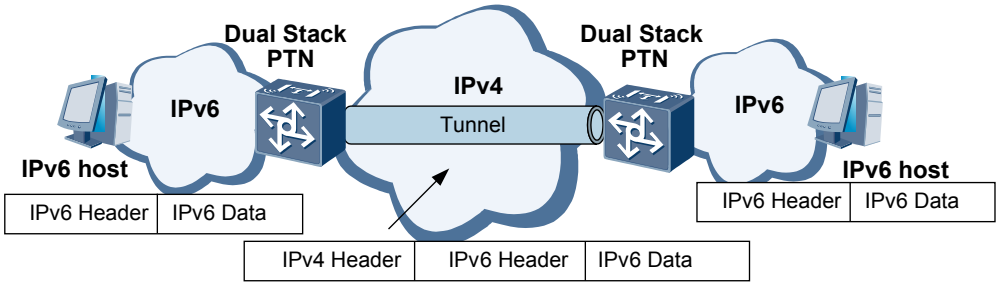
- 支持 IPv6 策略路由。
- 支持 DHCPv6 Relay。

3.7.4 IPv4/IPv6 过渡技术

IPv6 over IPv4 隧道

IPv6 over IPv4 隧道是 IPv4 网络向 IPv6 网络过渡的一种技术，其原理如图 3-16 所示。

图 3-16 IPv6 over IPv4 隧道原理图



PTN 6900 支持采用如下的 IPv6 over IPv4 隧道模式：

- IPv6 手动隧道

  手动隧道是在隧道两端的边界 PTN 6900 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。它相当于通过 IPv4 骨干网连接的两个 IPv6 域的永久链路，是两个边缘 PTN 6900 之间进行定期安全通信的固定通道，可用于 IPv6 孤岛之间的通信。

- IPv4 兼容 IPv6 自动隧道（简称自动隧道）

  创建 IPv6 over IPv4 自动隧道时，需要使用一类特殊的 IPv6 地址，即兼容 IPv4 的 IPv6 地址。这个地址中的低阶 32 位就是 IPv4 地址，根据它来自动识别隧道的目的地址。

  在配置自动隧道时，只需要在边界 PTN 6900 或主机上指定隧道源地址，不需要指定隧道的目的地址。隧道的目的地址是根据 IPv6 报文的下一跳地址（即兼容 IPv4 的 IPv6 地址）自动识别的。

- 6 to 4 隧道

  6 to 4 隧道可将多个 IPv6 孤岛网络通过 IPv4 网络连接到 IPv6 网络。

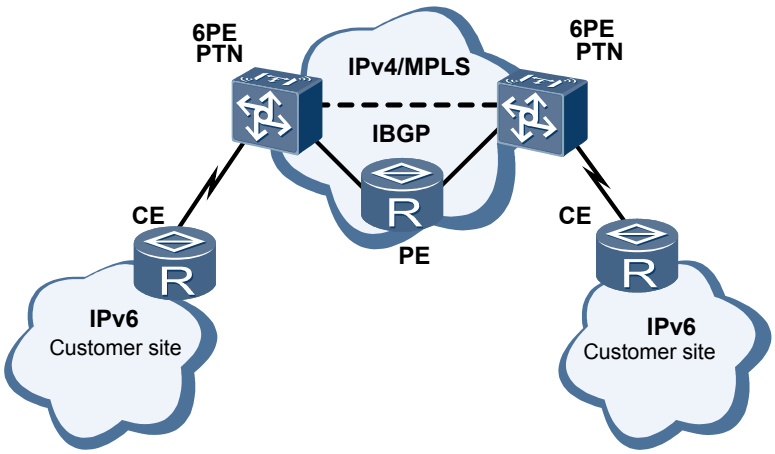
  6 to 4 隧道与手动配置隧道的主要区别在于，6 to 4 隧道可以是点到多点的连接，而手动隧道仅仅是点到点的连接。所以 6 to 4 隧道的 PTN 6900 并不是成对配置的。6 to 4 隧道与自动隧道类似，它可自动查找隧道的另一端点，但它不需要指定兼容 IPv4 的 IPv6 地址。6 to 4 隧道使用了一种特殊的 IPv6 地址，即 6 to 4 地址。

6PE

6PE（IPv6 Provider Edge）PTN 6900 允许 IPv6 孤岛的 CE 路由器穿过 IPv4 网络进行通信，如图 3-17 所示。ISP 可以利用已有的 IPv4 骨干网为分散用户的 IPv6 网络提供接入服务。

版权所有 © 华为技术有限公司

图 3-17 6PE 拓扑图



6PE 的主要思想是：用户的 IPv6 路由信息转换为带有标签的 IPv6 路由信息，并且通过 IBGP（Internal Border Gateway Protocol）会话扩散到 ISP 的 IPv4 骨干网中。在转发 IPv6 报文时，当流量在进入骨干网的隧道时，首先会被打上标签。隧道可以是 MPLS LSP 等。

运营商网络的 IGP 协议可以是 OSPF 或 IS-IS，CE 和 6PE 之间可以是静态路由、IGP 协议或者 EBGP。

当 ISP 想利用自己原有的 IPv4/MPLS 网络，使其通过 MPLS 具有 IPv6 流量交换能力时，只需要升级 PE 就可以了。所以对于运营商来说，使用 6PE 特性作为 IPv6 过渡机制是一个高效的解决方案。

3.8 路由协议

PTN 6900 支持丰富的单播路由协议和组播路由协议，可以满足不同的组网需求。

3.8.1 单播路由特性

PTN 6900 支持的单播路由特性如下：

- 支持 IPv4 路由协议：RIP、OSPF、IS-IS 和 BGP4。
- 支持 IPv6 路由协议：RIPng、OSPFv3、IS-ISv6 和 BGP4+。
- 支持静态路由，由管理员手工配置，以简化网络配置，提高网络性能。
- 具有大容量的路由表项，有效支撑城域网的运营。
- 通过完备的路由策略功能决定最佳路由。
- 支持 BGP 下一跳分离和按组打包。

3.8.2 组播路由特性

PTN 6900 支持组播，可大大节省网络带宽，减轻网络负荷。

基本组播特性

PTN 6900 提供如下基本组播特性：

版权所有 © 华为技术有限公司

- 支持的组播协议包括：IGMP、PIM（包括 PIM-DM、PIM-SM）组播路由协议、MSDP（Multicast Source Discovery Protocol）组播源发现协议、MBGP 协议。
- 支持 RPF 检查：PTN 6900 创建并维护组播路由表项时，需要执行 RPF（Reverse Path Forwarding）检查，从而确保组播数据能够沿正确的路径传输。
- 支持 PIM-SSM：在组播源确定的情况下，直接向组播源加入，而不必向 RP（Rendezvous Point）注册。
- 支持 Anycast RP：在一个域内，支持多个 RP，RP 之间建立 MSDP 对等体关系。组播源可以选择最近的 RP 注册，接收者也可以选择最近的 RP 加入其共享树。通过向就近的 RP 发起注册和共享树加入，实现 RP 的负载分担。一个 RP 失效后，其原来注册的源和加入者，又会选择另一个就近的 RP 注册和加入，实现了 RP 的冗余备份。
- 支持组播静态路由。
- 支持在以太网等物理接口和 Eth-Trunk 接口上配置组播协议。
- 组播路由模块在接收、引入、发布组播路由时，支持使用路由策略对路由进行过滤。在 IP 转发组播报文时，也支持按策略对组播报文进行过滤和转发。
- 支持组播 VPN，采用 MD（Multicast Domains）方案，实现集中式处理。
- 支持 Dummy 项添加和删除。

IGMP Snooping

PTN 6900 支持在二层接口、三层接口、QinQ 接口、STP、RRPP 和 VPLS PW 上的 IGMP Snooping 特性。

IGMP Snooping 通过侦听 PTN 6900 和主机之间发送的 IGMP 消息来建立组播数据报文的二层转发表，从而管理和控制组播数据报文的转发，实现二层组播。

IGMP Snooping 的目的是控制组播流的泛洪，实现“按需”转发，节约网络资源。对于没有使用 IGMP Report 申请加入某个组播组的端口，设备不会把组播流发送到该端口。

组播流量控制

对于未知组播报文，即组播转发表中不存在对应转发表项的组播报文，PTN 6900 支持根据需要进行丢弃或在端口所属 VLAN 内广播发送两种策略。

同时，PTN 6900 还可以控制以太网端口上的最大组播流量百分比，从而控制组播业务的流量。

组播 VLAN

组播 VLAN 是指使用 VLAN 来汇聚组播流。当用户需要某些组播流时，会向组播 VLAN 提出需求，组播 VLAN 将组播流复制到各用户 VLAN 中，从而实现跨 VLAN 组播复制功能。

PTN 6900 将去往各用户的组播流通过组播 VLAN 来下发，然后在分发点根据组播表项进行组播流复制并分发到各用户 VLAN 中去。借助组播 VLAN 技术，PTN 6900 可以将所有用户 VLAN 内的组播流汇聚到一个或几个指定的 VLAN 中进行传送。

组播 VLAN 技术将用户单播数据和组播数据限定在不同 VLAN 内传送，不仅方便了对组播流的管理和控制，而且可以减少带宽浪费，更提高了网络安全性。

版权所有 © 华为技术有限公司

组播 VLAN 1+1 保护

所谓组播 VLAN 1+1 保护，是指借助跨 VLAN 组播实现组播流 1+1 保护。

组播流被 ICP（Internet Context Provider）复制到两个组播 VLAN 中，组播流报文和检测链路状态的 CCM 报文在两个组播 VLAN 中都会被转发到用户侧 PTN 6900。PTN 6900 根据收到 CCM 报文的情况判断链路状态，选择一条状态好的链路接收组播流。

目前，PTN 6900 仅支持基于 VLAN 的组播流 1+1 保护。

组播 VPN

随着 VPN（Virtual Private Network）技术的广泛应用，用户对在 VPN 中运营组播业务的需求日益迫切。PTN 6900 采用 MD（Multicast Domains）方案实现跨越 VPN 网络的组播传输。

关于组播 VPN 的详细描述请参见“**3.10 VPN 特性**”中的具体描述。

组播 CAC 功能

PTN 6900 支持组播 CAC（Call Admission Control）特性，通过配置组播 CAC 规则，在接口、全局进行 IGMP Snooping 的组播组数量、带宽限制。

组播 CAC 是 IPTV 组播方案的组成部分，随着 IPTV 的发展，节目频道数量快速增加，用户带宽需求已经超出了接入汇聚网的带宽。因此，原来的静态管理的方式已经不能适应需要，必须在汇聚网络进行控制，在每条链路上设置允许接入的用户数量。

组播 CAC 控制组播转发表项的生成，在超出设置的限制时，就不允许生成组播转发表项，从而保证了设备处理能力，实现了链路带宽的控制。

3.9 MPLS 特性

3.9.1 基本特性

PTN 6900 支持 MPLS 特性，支持静态 LSP 和动态 LSP。静态 LSP 需要管理员对沿途的 LSR 进行相应配置，手工建立 LSP 隧道；动态 LSP 由 LDP 协议或 RSVP-TE 根据路由信息动态建立 LSP 隧道。

PTN 6900 支持多协议标签交换 MPLS，特性包括：

- 支持 MPLS 的基本功能和转发业务，实现了 LDP 信令协议。MPLS 信令协议负责分发标签、建立 LSP 并传递 LSP 建立过程中需要的参数。
- LDP 支持：
  - DU 和 DoD 两种标签发布方式。
  - 独立标签分配控制和有序标签控制方式两种标签分配控制方式。
  - 自由标签保持方式和保守标签保持方式两种标签保持方式。
  - 最大跳数和路径向量两种环路检测机制。
- 支持 MPLS Ping/Tracert，使用 MPLS echo request 和 MPLS echo reply 检测 LSP 的可用性。
- 支持基于 LSP 的流量统计。

版权所有 © 华为技术有限公司

- 支持 LSP 环路检测机制等管理功能。
- 支持 MPLS QoS，支持 IP 报文从 ToS 域到 MPLS 报文 EXP 域的映射，并且支持 MPLS Uniform、Pipe 和 Short Pipe 三种模式。
- 支持基于流分类静态配置 LSP，基于流分类进行标签转发。
- 支持 MPLS 的 TRAP 功能。

PTN 6900 可以作为标签边缘路由器 LER（Label Edge Router）、标签交换路由器 LSR（Label Switch Router）。

- LER 是指 MPLS 网络同其它网络的边缘设备，它具有业务分类、分发标签、封装或者剥去多层标签等多种功能。
- LSR 是 MPLS 网络的核心路由器，它提供标签交换、标签分发的功能。

3.9.2 MPLS TE

网络拥塞是影响骨干网络性能的主要问题。拥塞的原因可能是网络资源不足，也可能网络资源负载不均衡，导致局部拥塞。流量工程 TE（Traffic Engineering）解决的是由于负载不均衡导致的拥塞。

MPLS TE 结合了 MPLS 技术与流量工程，通过建立到达指定路径的 LSP 隧道进行资源预留，使网络流量绕开拥塞节点，达到平衡网络流量的目的。

在资源紧张的情况下，MPLS TE 能够抢占低优先级 LSP 隧道带宽资源，满足大带宽 LSP 或重要用户的需求。同时，当 LSP 隧道故障或网络的某一节点发生拥塞时，MPLS TE 可以通过备份路径和快速重路由 FRR（Fast Reroute）提供保护。

MPLS TE 主要实现两类功能：

- 静态 LSP 的处理：创建和删除静态 LSP。这些 LSP 有带宽需求，但都是通过手工配置。
- CR-LSP（Constrained Route-Label Switched Path）处理：包括对不同类型 CR-LSP 的处理。

静态 LSP 的处理比较简单。对于 CR-LSP，MPLS TE 在实现上主要包括如下几个部分。

RSVP-TE

资源预留协议 RSVP（Resource Reservation Protocol）是为 IntServ（Integrated Service）模型而设计的，用于在一条路径的各节点上进行资源预留。

简单来说，RSVP 具有以下几个主要特点：

- 单向
- 面向接收者，由接收者发起对资源预留的请求，并维护资源预留信息
- 使用“软状态”（Soft State）机制维护资源预留信息

RSVP 经扩展后可以支持 MPLS 标签的分发，并在传送标签绑定消息的同时携带资源预留信息，这种扩展后的 RSVP 称为 RSVP-TE，作为一种信令协议用于在 MPLS TE 中建立 LSP 隧道。

自动路由

自动路由（Auto Route）是指将 LSP 看作逻辑链路参与 IGP 路由计算，使用隧道接口作为出接口。这里，LSP 被看做点到点链路。自动路由方式有两种：

版权所有 © 华为技术有限公司

- 转发捷径（IGP Shortcut）：不将这条 LSP 链路发布给邻居 PTN 6900，因此，其他 PTN 6900 不能使用此 LSP。
- 转发邻接（Forwarding Adjacency）：将这条 LSP 发布给邻居 PTN 6900，因此，其他 PTN 6900 能够使用此 LSP。

快速重路由

快速重路由 FRR（Fast ReRoute）是 MPLS TE 中实现网络局部保护的技术。FRR 的切换速度可以达到 50 毫秒，能够最大程度减少网络故障时数据的丢失。

但 FRR 只是一种临时性保护措施，一旦被保护的 LSP 恢复正常或建立了新的 LSP，流量就会切换回原 LSP 或新建立的 LSP。

对 LSP 配置 FRR 功能后，当 LSP 上的某条链路或某个节点失效时，流量会被切换到保护链路上，同时 LSP 入节点尝试建立新的 LSP。

自动快速重路由

快速重路由要求在配置被保护隧道的时候，需要再手工配置一条旁路隧道与之绑定，当出现链路或节点失效时，可以自动将数据切换到旁路隧道。

这种 FRR 保护需要手工配置旁路隧道，如果没有配置，或者忘记配置旁路隧道，将无法对被保护隧道进行保护。Auto FRR 在这样的情形下应运而生。

Auto FRR 是对 MPLS TE FRR 功能的扩展，通过在主隧道下配置旁路隧道的属性、全局 Auto-FRR 属性和接口 Auto-FRR 属性，可以在 LSP 上自动创建符合要求的旁路隧道。并且随着主隧道路径的变化，旧的旁路隧道会自动的删除，然后建立新的符合要求的旁路隧道。

CR-LSP 备份

同一条隧道下对主 LSP 进行路径备份的 LSP 称为备份路径。当入节点感知到主 LSP 不可用时，将流量切换到备份路径上，当主 LSP 路径恢复后再将流量切换回来，以实现对主 LSP 路径的备份保护。

PTN 6900 支持两种备份方法：

- 热备份：创建主 CR-LSP 后随即创建备份 CR-LSP。主 CR-LSP 失效时，通过 MPLS TE 直接将业务切换至备份 CR-LSP。
- 普通备份：指主 CR-LSP 失效后创建备份 CR-LSP。

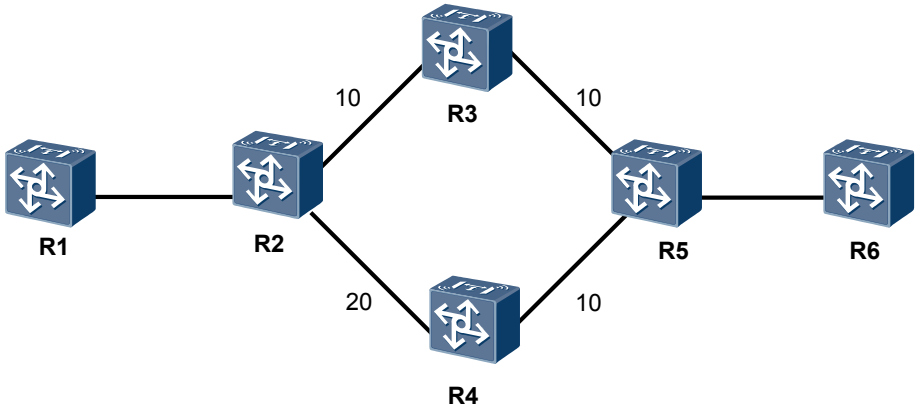
LDP over TE

在现有网络中，并不是所有设备都支持 MPLS TE。可能仅有网络的核心部分支持 TE，而在边缘使用 LDP。由此产生了 LDP over TE 的应用。即 TE Tunnel 作为整个 LDP LSP 的“一跳”。

目前，LDP 被广泛应用在 MPLS VPN 中。为防止 VPN 流量在某些节点发生拥塞，可以配置 LDP over TE 特性。

版权所有 © 华为技术有限公司

图 3-18 LDP over TE



上图是一个 MPLS VPN 网络，采用 LDP 作为信令协议。

R1 和 R6 作为 PE，在接入大量用户后，发现 R2 到 R3 的链路非常拥塞，因为 R1 和 R6 之间的流量都要经过此链路。而 R2 与 R4 间的链路空闲，但由于 IGP 的 Cost 值影响，LSP 不会使用 R2 和 R4 之间的链路。

可以在 R2 和 R5 之间建立一条穿过 R4 的 TE 隧道，然后调整 IGP Shortcut 或转发邻接的 Metric 值，使 R2 上有以下两条路由可以进行负载分担：

- R2 与 R3 之间物理接口
- R2 到 R5 的 TE 隧道接口

这样，LDP 就可以建立负载分担的 LSP，使一部分流量流经空闲的链路。

3.10 VPN 特性

版权所有 © 华为技术有限公司

4 QoS 特性

关于本章

PTN 6900 实现了承载包括实时业务在内的综合业务的 QoS 特性。对 Diff-Serv 提供了完善支持，包括流分类、流量监管（Policing）、流量整形（Shaping）、拥塞管理、队列调度（Scheduling）等。PTN 6900 完整实现了标准中定义的 EF、AF1 ～ AF4、BE、CS6、CS7 等八组 PHB 及业务，使网络运营商可为用户提供具有不同服务质量等级的服务保证，使 Internet 真正成为同时承载数据、语音和视频业务的综合网络。

下面对 PTN 6900 中主要的 QoS 特性进行介绍。

版权所有 © 华为技术有限公司

4.1 基础 QoS

Diff-serv 模型

业务在进入网络时进行分类和调整，并被分配给不同的行为集合，该行为集合由 DSCP 编码来标识。在网络核心，报文根据 DSCP 编码所标识的 PHB（per-hop behavior）属性来转发的。

DiffServ 的优点：多个业务流可以汇聚成一个行为集合(Behavior Aggregate)，在 PTN 6900 上使用相同的 PHB 进行转发处理，由此简化了业务的处理和存储过程。

在 Diffserv 核心网络，由于 QoS 保证是基于每个报文的，因此省略了信令处理。

流分类

流分类是指通过对流量按照某种规则进行分类，并对同种类型的流量实施某种动作，将流分类与动作关联起来从而形成某种策略。将该策略应用后实现基于类的流量监管、流量整形、拥塞避免等功能。

在不需要 QoS 保证或不进行流分类的情况下，或者报文通过流分类没有相匹配的规则时，对报文作尽力转发 BE（Best-Effort）处理。

PTN 6900 支持简单流分类和复杂流分类。

通常是在相对边界的 PTN 6900 上配置复杂流分类，在相对核心的设备上配置简单流分类。

- 简单流分类

  简单流分类是指根据 IP 报文的 IP 优先级或 DSCP 值、MPLS 报文的 EXP 域值、VLAN 报文的 802.1p 值，将报文划分为多个优先级或多个服务等级。配置基于简单流分类的流量策略可以将一种网络流量中的优先级映射到另外一种网络流量中，使流量在另外一种网络中按照原来的优先级传送。

  目前，PTN 6900 不仅支持在物理接口及其子接口实现简单流分类，而且支持在 VLANIF、Trunk 等逻辑接口实现简单流分类。

- 复杂流分类

  复杂流分类是指根据五元组（源/目的地址、源/目的端口号、协议类型）等信息对报文进行分类，通常应用在网络的边缘位置。流分类必须与某种流量控制或资源分配动作关联起来，从而实现对不同的业务提供差分服务。

  目前，PTN 6900 支持根据以太报文头中的源 MAC 地址、目的 MAC 地址、报文链路层承载的协议号、带 TAG 报文的优先级进行分类；支持根据 IPv4 报文的 IP 优先级/DSCP/ToS 域值、源 IP 地址前缀、目的 IP 地址前缀、IP 报文承载的协议号、分片标志、TCP SYN 标志、TCP/UDP 源端口号或端口范围、TCP/UDP 目的端口号或端口范围进行分类。

  并且，除了物理接口，PTN 6900 还支持在多种逻辑接口上实现复杂流分类，包括子接口、Trunk 接口。

流量监管

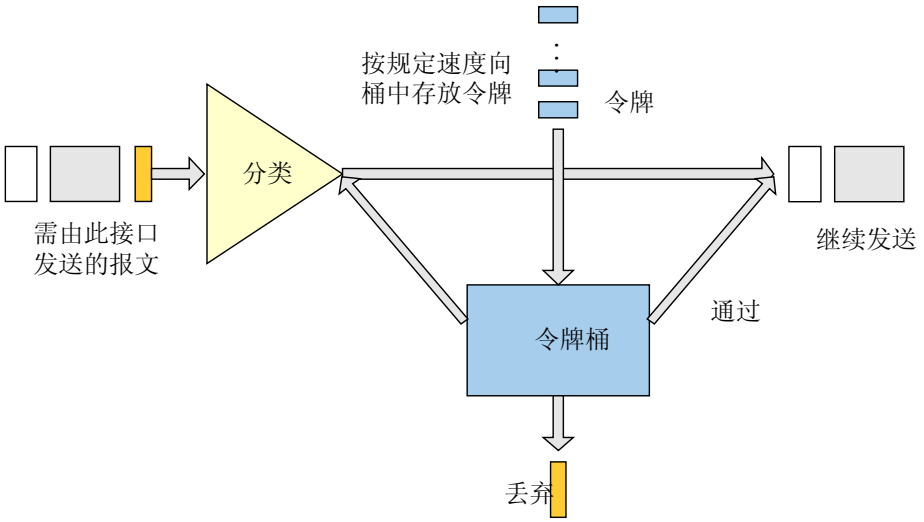
流量监管采用承诺访问速率 CAR（Committed Access Rate）来对流量进行控制。首先，根据预先设置的匹配规则来对报文进行分类，如果是符合流量规定的报文，则报文通过

版权所有 © 华为技术有限公司

继续发送；如果是超出流量规定的报文，可以选择丢弃报文或重新设置报文的优先级再发送。

CAR 技术对流量进行控制采用令牌桶 TB（Token Bucket）实现。具体处理流程如图 4-1 所示。

图 4-1 CAR 处理过程示意图



- 令牌桶按用户设定的速度向桶中放置令牌，并且令牌桶有用户设定的容量，当桶中令牌的数量超出桶的容量的时候，令牌的数量不再增加。
- 当报文到来时，首先根据报文的 IP precedence/源/目的地址等信息对报文进行分类。满足某类特征的报文进入令牌桶中进行处理。
- 如果令牌桶中有足够的令牌可以用来发送报文，则报文直接通过并继续发送，同时令牌桶中的令牌量按报文的长度做相应的减少；如果令牌桶中的令牌数量不足或为空，则无法得到足够转发令牌的报文将被丢弃或进入标记器进行 IP Precedence、DSCP 或 EXP 值的重标记然后再发送，此时令牌桶中的令牌数量不发生变化。

从上述可以看出，CAR 技术不仅可以做到流量控制，还可以进行报文的标记（mark）或重新标记（remark）。

速率限制功能是 CAR 的主要功能。主要是通过使用令牌桶对流经端口的数据流进行度量，使得在特定时间内只有得到令牌的流量通过，从而实现限速功能。也就是说它可以限制接口入和出两个方向的流量的最大速率。同时我们还可以根据特定的数据特征来对特定的数据流进行速率控制，如针对数据的 IP 地址，端口号，优先级等。不符合条件的数据流设备将不进行限速处理，以端口原速率转发。

CAR 技术主要应用于网络边缘，从而保证核心设备的正常数据处理。PTN 6900 支持在上下行两个方向上做 CAR。

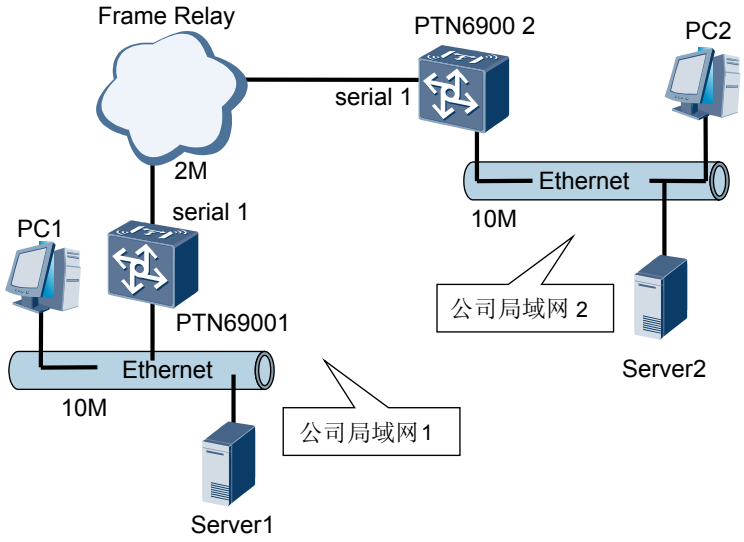
队列调度

在计算机数据通信中，通信信道是被多个计算机共享的。并且，广域网的带宽通常要比局域网的带宽小。这样，当一个局域网的计算机向另一个局域网的计算机发送数据时，由于广域网的带宽小于局域网的带宽，数据将不可能按局域网发送的速度在广域网上传输。此时，处在局域网和广域网之间的 PTN 6900 将不能发送一些报文，即网络发生了拥塞。

版权所有 © 华为技术有限公司

如图 4-2 所示，当公司局域网 1 向公司局域网 2 以 10M 的速度发送数据时，将会使 PTN 6900 1 的 Serial 1 接口发生拥塞。

图 4-2 网络拥塞示意图



拥塞管理是指网络在发生拥塞时，如何进行管理和控制。处理的方法是使用队列调度技术。将所有要从一个接口发出的报文进入多个队列，按照各个队列的优先级进行处理。通过适当的队列调度机制，可以优先保证某种类型的报文的 QoS 参数，例如带宽、时延、抖动等。我们这里所说的队列是指出队列，其作用是在接口有能力发送报文之前先将报文在队列中保留下来。所以队列调度机制都是在出端口发生拥塞情况下产生作用，另外一个主要作用就是将报文重新排序（先进先出队列除外）。

常用的队列调度算法有先进先出队列 FIFO（First In, First Out Queuing）、PQ（Priority Queuing）优先队列、CQ（Custom Queuing）定制队列、WFQ（Weighted Fair Queuing）加权公平队列、CBWFQ（Class-Based WFQ）队列, LPQ(Low Priority Queue)队列列等。

PTN 6900 支持 FIFO、PQ 和 WFQ 队列技术，实现端口的队列调度。

拥塞管理

PTN 6900 采用的拥塞控制算法为加权随机早期检测 WRED（Weighted Random Early Detection）。

PTN 6900 针对端口上的每个优先级队列，可单独配置拥塞控制算法。系统以微秒级的定时器一阶加权迭代跟踪共享内存的占用程度，不仅能及时“感知”网络的拥塞状况，同时可避免网络的振荡。由此对各种业务流以及同一业务流内部不同的丢弃级别报文进行不同统计概率的丢弃，可及时有效的避免和控制网络拥塞。

流量整形

当网络发生拥塞的时候，利用流量监管（采用 CAR 技术）可以控制报文的流量特性，对流量加以限制，将不符合流量特性的报文进行丢弃。有时，为了减少报文的丢弃，可以先将超出规格的报文进行缓冲，然后在令牌桶的控制下再均匀地发送，这就是流量整形。流量整形既可以减少报文的丢弃，同时又能满足报文的流量特性。

版权所有 © 华为技术有限公司

流量整形的典型作用是限制流出某一网络的某一连接的突发流量，使这类报文以比较均匀的速度向外发送。流量整形采用的技术叫做 Generic Traffic Shaping（通用流量整形，简称GTS），可以对不规则或不符合预定流量特性的流量进行整形，以利于网络上下游之间的带宽匹配。

4.2 HQoS

HQoS(Hierarchical QoS)是一种既能控制用户的流量，又能同时对用户业务的优先级进行调度的 QoS 技术。

PTN 6900 实现了如下的 HQoS 特性：

- 五级调度机制实现了丰富的业务能力。
- 可配置流队列的最大队列长度、WRED、低时延、SP/WRR 权重、带宽突发度 CBS、PBS 和统计使能等参数。
- 可配置每个用户的 CIR、PIR、流队列数目、流队列之间的调度算法等参数。
- 完善的流量统计功能，使用户可以看到各种业务的带宽使用情况，并通过分析流量，合理的划分各业务的带宽分配。
- 在 VPLS、L3VPN、VLL、TE 场景下支持 HQoS。

4.3 流量负载分担

在实际网络中，如果有多条等价路径可以到达同一目的地，PTN 6900 支持在这些路径上对流量进行负载分担。根据网络及客户的要求不同，既支持等值（均衡）负载分担，也支持非等值（按接口带宽比例）负载分担。

4.3.1 等值负载分担

PTN 6900 支持在 Eth-Trunk 的成员链路间对流量进行均衡负载分担；当有多条等价路由可以到达同一目的时，PTN 6900 也支持在这些等价路由间对流量进行均衡负载分担。

流量的负载分担方式分为逐流和逐包负载分担两种方式。缺省情况下，使用逐流负载分担。

4.3.2 非等值负载分担

PTN 6900 支持如下方式的非等值负载分担：

- 通过路由分担：如果直连路由的 Cost 值相同，可以配置负载分担权重。
- 通过接口分担：在 Eth-Trunk 中，可以配置成员链路间的负载分担权重。
- IGP 基于链路带宽的非均衡负载分担：支持在负载分担路径出接口上按照链路带宽实现非等值逐流负载分担，在各个路径上的流量分担比例接近或等于各条链路的带宽比例。这种方式充分考虑了链路带宽的因素。有效地解决了低带宽链路过分拥塞而带宽链路空闲的问题。

PTN 6900 不仅支持流量在物理接口之间进行负载分担，同时也支持流量在物理接口和逻辑接口之间进行负载分担。并且，系统能够感知逻辑接口由于人工配置或成员链路 Up/Down 状态变化引起的带宽动态变化。当逻辑接口带宽变化后，流量会自动按照接口变化后的带宽比例重新进行负载分担。

版权所有 © 华为技术有限公司

4.4 流量统计

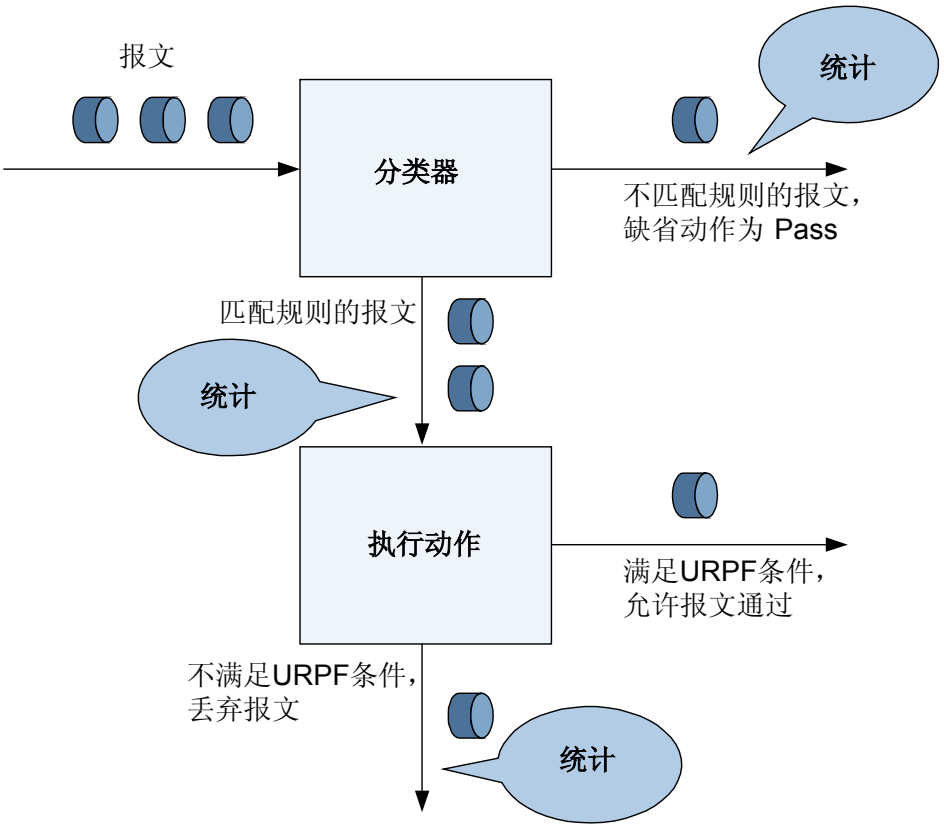
PTN 6900 提供多种的流量统计功能，可以对不同用户接入网络的流量进行统计。

流量统计功能有助于运营商分析网络的流量模型、为部署及维护 Diffserv TE 提供参考数据、并可以支持按流量对非包月用户进行计费。

4.4.1 URPF 流量统计

PTN 6900 支持对符合 URPF 规则的总流量进行统计，同时也支持对不符合 URPF 规则被丢弃的流量进行统计。

图 4-3 URPF 中的流量统计



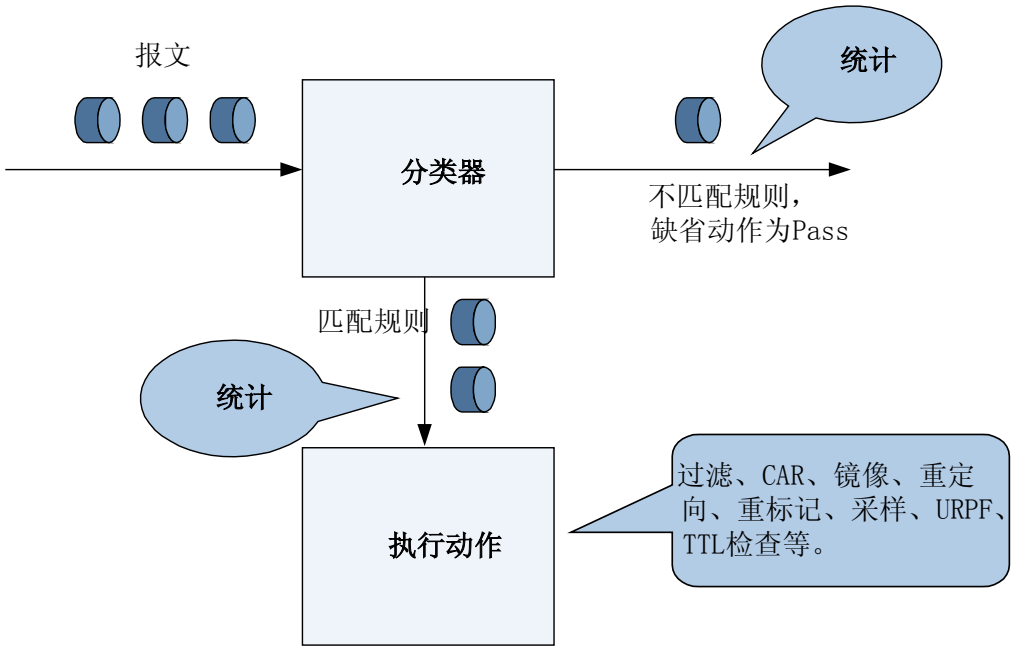
4.4.2 CAR 流量统计

PTN 6900 支持流分类、流量监管（CAR）、队列调度等多种 QoS 特性。针对这些 QoS 特性，PTN 6900 提供了相应的 QoS 流量统计功能。

- 在流分类中，支持分别对命中规则和没有命中规则的流量进行统计。

版权所有 © 华为技术有限公司

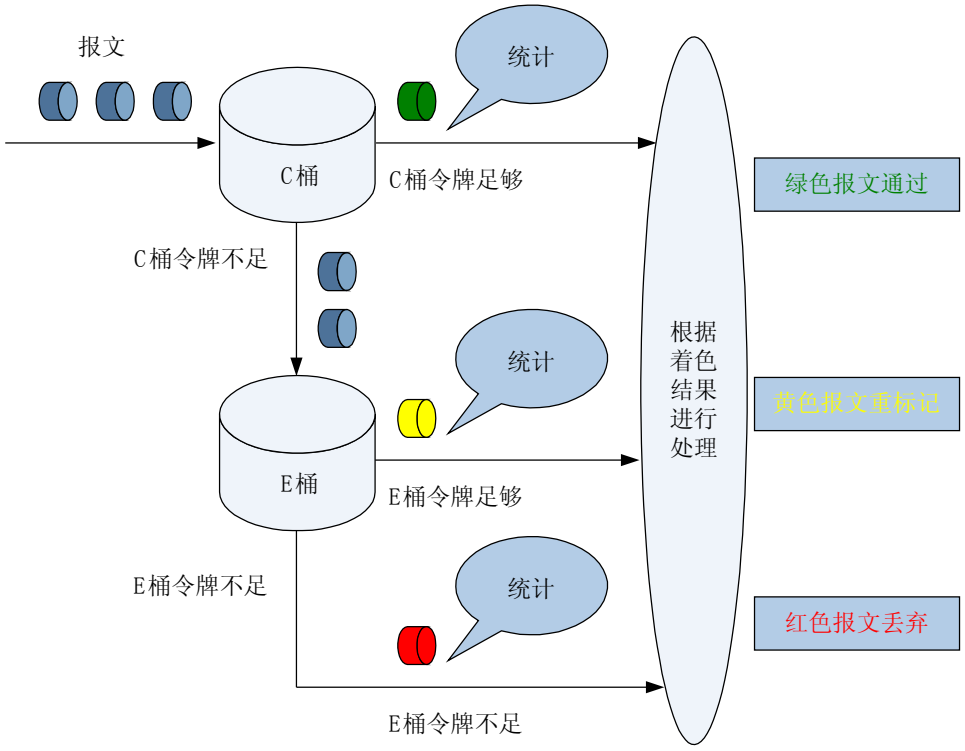
图 4-4 流分类中的流量统计



在流量监管中支持的流量统计形式如下：

- 支持对符合 CAR 规则的总流量进行统计。
- 支持分别对 CAR 动作是通过（或丢弃）的流量进行统计。

图 4-5 CAR 中的流量统计



版权所有 © 华为技术有限公司

- 支持基于接口的流量策略统计功能。
- 相同的流量策略应用到不同的接口时，流量策略中的 CAR 统计是基于接口的。

4.4.3 HQoS 流量统计

支持用户流队列的统计，包括 8 个优先级的转发报文数、字节数和丢弃报文数。

支持用户组的转发报文数、字节数和丢弃报文数。

支持端口队列 8 个优先级的转发报文数、字节数和丢弃报文数。

4.4.4 接口流量统计

支持接口、子接口的流量统计。

4.4.5 VPN 流量统计

在 VPLS 网络中，PTN 6900 做为 PE 设备时可以对接入的 L2VPN 用户的出入流量进行统计。

在 L3VPN 网络中，PTN 6900 做为 PE 设备可以对多种接入用户的出入流量进行统计，这些用户包括：

- 通过接口（包括逻辑接口）接入网络的用户。
- 多角色主机。
- 通过 VPLS/VLL 接入网络的用户。
- 在配置 MPLS HQoS 业务时，作为入口 PE 设备可以提供网络侧发送流量的统计。

4.4.6 TE 隧道流量统计

PTN 6900 做为 MPLS TE 网络中的 PE 设备时，支持对出入 Tunnel 隧道的流量进行统计。对于 VPN 静态绑定 TE 的情况，可以统计 TE 上承载的每一个资源隔离 VPN 的流量，以及 TE 的总流量。

DS-TE 支持隧道内每个 CT 的流量统计。

版权所有 © 华为技术有限公司

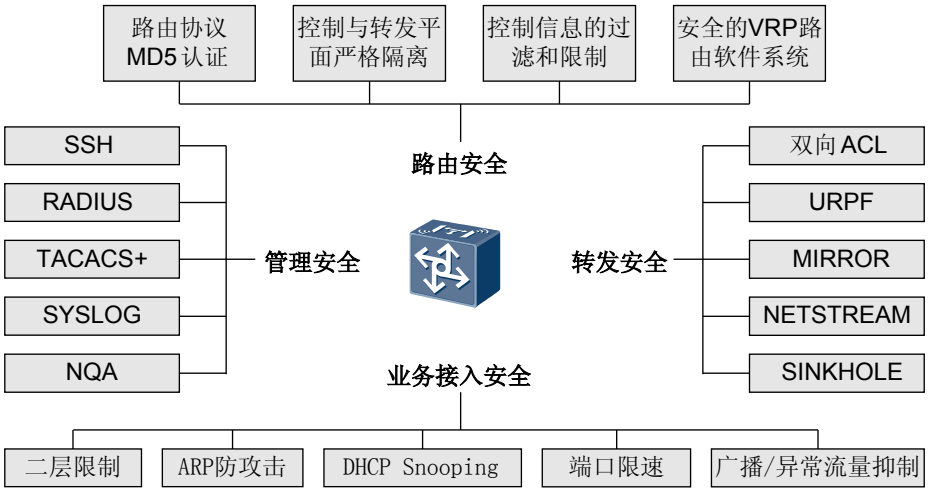
5 安全特性

关于本章

PTN 6900 做为网络中大客户接入和业务系统接入的安全网关，可以提供：

- 先进的安全体系结构
- 丰富的安全协议
- 严格的业务接入控制功能

图 5-1 安全特性



下面对 PTN 6900 支持的主要安全特性进行介绍。

5.1 安全验证

5.2 RPF/URPF 检测

5.3 MAC 限制

5.4 未知流量限制

版权所有 © 华为技术有限公司

版权所有 © 华为技术有限公司

5.1 安全验证

PPP 支持 PAP 和 CHAP 验证方式。

路由协议（RIPv2、OSPF、IS-IS、BGP）支持报文明文认证和 MD5 密文认证。

LDP 和 RSVP 支持 MD5 密文认证。

SNMP 支持 SNMPv3 的加密和认证。

5.2 RPF/URPF 检测

单播反向路径查找 URPF（Unicast Reverse Path Forwarding），防止基于源地址欺骗的网络攻击行为。

一般情况下，PTN 6900 接收到报文，获取报文的目的地址，针对目的地址查找路由。如果找到了就转发报文，否则丢弃该报文。URPF 通过获取报文的源地址和入接口，以源地址为目的地址，在转发表中查找源地址对应的接口是否与入接口匹配，如果不匹配，认为源地址是伪装的，丢弃该报文。通过这种方式，URPF 就能有效地防范网络中通过修改源地址而进行的恶意攻击行为的发生。

5.3 MAC 限制

PTN 6900 支持丰富的 MAC 限制功能，可以为大型的二层网络和 VPLS 网络提供多种安全解决方案。

MAC 地址限制

随着城域以太网（Metro Ethernet）市场的高速增长，安全在城域网络的入口位置扮演着愈发重要的角色。城域以太网中，大量的个人用户通过以太链路接入 Internet，网络上的黑客和病毒进行 MAC 攻击比较普遍。PTN 6900 提供的 MAC 地址限制能够有效防范这些攻击，保证运营商网络的安全。

强大的 MAC 表项限制功能，一方面能够限制一个用户接入的 MAC 数目，防止挤占其它用户的 MAC 地址空间；另一方面又能将攻击报文在入口处丢弃，禁止非法报文消耗带宽资源。

MAC 地址学习是二层转发的基本特性，完全自动进行，使用简单，但必须谨慎规划，以防招致攻击。

PTN 6900 支持对 MAC 地址的学习限制功能，包括：

- 限制最多允许学习的 MAC 数量
- 限制 MAC 学习的速度
- 基于端口的 MAC 地址限制
- 基于 PW 的 MAC 地址限制
- 基于 VLAN+端口的 MAC 地址限制
- 基于端口+VSI 的 MAC 地址限制
- 基于双层 VLAN（QinQ）的 MAC 地址限制

版权所有 © 华为技术有限公司

MAC 地址学习限制可以应用于接入用户固定，但又不够安全的网络环境，如小区接入或缺乏安全管理的企业内部网。当接入的用户数量达到限制值后，新接入的用户 MAC 将不被学习，该用户的流量将全部采用广播方式，速度有限。

MAC 地址删除

在 VPLS 和二层组网中，MAC 地址表是转发的关键，同时也是一种易受攻击的稀缺资源，尽管 MAC 地址表项有定时老化机制，但仍然需要为 MAC 地址表提供丰富的表项删除功能，以保证在尽可能少的影响其它正常业务的条件下，快速删除失效的表项，释放 MAC 资源。

PTN 6900 提供如下的 MAC 地址表项删除功能：

- 基于端口+VSI 删除 MAC 地址
- 基于端口+VLAN 删除 MAC 地址
- 基于 Trunk 接口删除 MAC 地址
- 基于 QinQ 出接口删除 MAC 地址

5.4 未知流量限制

PTN 6900 提供的未知流量限制功能，可以在 VPLS 和二层组网中完成如下的功能：

- 对用户的流量进行管理。
- 对用户的带宽进行分配。

从而达到合理的利用网络的带宽和保证网络安全的目的。

5.5 DHCP Snooping

DHCP Snooping 是一种 DHCP 安全特性，可以过滤不信任的 DHCP 消息并建立和维护一个 DHCP Snooping 绑定表。该绑定表包括 MAC 地址、IP 地址、租约时间、绑定类型、VLAN ID、接口信息。DHCP Snooping 的作用就如同在 Client 和 DHCP Server 之间的建立一道防火墙。

DHCP Snooping 主要是解决设备应用 DHCP 时遇到 DHCP DoS 攻击、DHCP Server 仿冒攻击、ARP 中间人攻击及 IP/MAC Spoofing 攻击的问题。

根据不同的攻击类型，DHCP Snooping 提供不同的工作模式，见表 5-1。

表 5-1 攻击类型与 DHCP Snooping 工作模式对应表

攻击类型	DHCP Snooping 工作模式
DHCP 饿死攻击	MAC 地址限制
DHCP Server 仿冒者攻击	信任（Trusted）/不信任（Untrusted）
中间人攻击/IP/MAC Spoofing 攻击	DHCP Snooping 绑定表
改变 CHADDR 值的 DoS 攻击	检查 DHCP 报文的 CHADDR 字段

版权所有 © 华为技术有限公司

5.6 本机防攻击特性

PTN 6900 提供统一的本机防攻击功能模块完成整个设备防攻击策略的管理和维护，可以为用户提供一套可操作和可维护的全方面防攻击解决方案。

白名单

白名单指合法用户或者是高优先级用户的集合。通过设定白名单信息可主动保护现有业务、保护高优先级用户业务。通过 ACL 可以设置自定义的白名单，后续匹配白名单特征的报文会被采用高速率高优先级上送。

可将确定为正常使用设备的合法用户或者是高优先用户业务设置到白名单中。

黑名单

黑名单指非法用户的集合。通过 ACL 可以设置自定义黑名单，后续匹配黑名单特征的报文会被丢弃或者低优先级上送。

可将确定为攻击的非法用户设置到黑名单中。

用户自定义流

用户自定义流指用户自定义防攻击 ACL 规则。主要应用于当后续网络中出现不明攻击时，用户可灵活指明攻击流数据特征，将符合此特征的数据流进行上送限制。

动态链路保护特性

PTN 6900 支持通过白名单特性保护所有基于 TCP 的应用层协议的 Session 数据。当 Session 建立时，系统会将 Session 信息同步加入到白名单中，保证当前系统的所有 Session 都受到白名单的保护，以高优先级上送。该特性统称为动态链路保护特性 ALP (Active Link Protection)。通过动态链路保护特性可保护设备已有业务在攻击发生时的正常运行。

当设备检测到 Session 删除时，会将此 Session 信息从白名单中删除。

统一的 CAR 参数配置

CAR 用来设置上送 CPU 的报文的分类限速上送规则，针对每类报文可设置均值速率、峰值速率、优先级信息等。通过对不同的报文设置不同的 CAR 规则，可以降低报文的相互影响，达到保护 CPU 的目的。

PTN 6900 提供更加方便的 CAR 参数配置方法：

- 可以对不同接口板提供统一的 CAR 参数配置。
- 对用户提供统一的配置界面。
- 并且提供常用协议的协议级粒度的 CAR 参数配置，使用户配置界面更加友好。

最小包补偿

PTN 6900 通过最小包补偿功能有效解决小报文攻击问题。PTN 6900 收到上送 CPU 的报文后，进行报文长度检测：

版权所有 © 华为技术有限公司

- 如报文实际长度小于预设的最小包长，便使用设定长度计算报文上送速率.
- 如报文实际长度大于预设的最小包长，便使用报文实际长度计算报文上送速率。

应用层联动

PTN 6900 支持应用层联动功能。PTN 6900 可以动态检测开启的上层应用协议业务信息。如果检测到上层业务开启，PTN 6900 接收该类业务应用报文并上送 CPU；如果检测到上层业务关闭，PTN 6900 直接丢弃此类报文或者以指定带宽限制上送该类报文。

本机 URPF

URPF 功能是在网络入接口同时对转发报文和本机报文进行检测。在大型网络中，为了避免对转发性能造成较大的影响，可以部署本机 URPF。即只对本机报文进行源地址合法性检查，不合法的报文进行丢弃处理，起到防源地址欺骗攻击的效果。

管理和业务平面保护

PTN 6900 接口可以分成两类，一类是管理口（管理报文可以通过该接口访问 PTN 6900），一类是非管理口。比如城域网的部署，一般来说，下行接用户的接口是非管理口。

为了防止黑客从非管理口控制设备，或者进行管理报文的 Flood 攻击，PTN 6900 支持管理平面保护功能，指定只有管理接口可接收管理流量，使管理流量进一步可控。

TCP/IP 类网络报文防攻击

当前网络中，基于 TCP/IP 网络的攻击日益增多，造成的影响越来越大。PTN 6900 支持对如下 TCP/IP 类网络攻击的防范功能。

- 畸形报文攻击：通过向目标系统发送有缺陷的 IP 报文，使得目标系统在处理这样的 IP 包时会出现崩溃，给目标系统带来损失。系统支持对如下畸形报文的转发引擎和软件识别，并丢弃。
- 载荷为空的 IP 报文
- 空 IGMP 报文
- LAND 攻击：源 IP 地址和目的 IP 地址一致的 TCPSYN 报文
- Smurf 攻击：目的地址为广播地址或子网广播地址的 ICMP echo request 报文
- TCP 标志位非法攻击： 6 个标志位（URG、ACK、PSH、RST、SYN、FIN）全为 1；6 个标志位全为 0；SYN 和 FIN 位同时为 1。
- 分片报文攻击：分片报文攻击造成 PTN 6900 的 CPU 繁忙，使得系统无法接受正常用户的请求，或者系统崩溃不能正常的工作。系统支持对如下分片报文攻击由转发引擎或软件识别，并通过 CPCAR 保证重复分片上送的速率，软件保证重组正确，或丢弃重组有错误的报文。
- 分片数量巨大的攻击和巨大 offset 报文的攻击
- 重复分片报文攻击
- Tear Drop 攻击、syndrop 攻击、nesta 攻击、fawx 攻击、bonk 攻击、NewTear 攻击、Rose 攻击、死亡之 ping 攻击、Jolt 攻击
- TCP SYN：系统支持对 TCP SYN 泛洪攻击的识别，并在接口板上进行限速 CAR 处理。

版权所有 © 华为技术有限公司

- UDP FLOOD：系统支持对 Fraggle 攻击和 UDP 诊断端口攻击报文的识别，并丢弃或进行基于接口板的过滤。

攻击溯源特性

PTN 6900 支持在设备自身受到恶意攻击时，提取、存储可疑报文，并能格式化显示（包括设备命令行和离线工具显示两种手段），为安全攻击定位攻击源头提供一种简单、易用的辅助手段。

在攻击发生时，系统自动将攻击报文裁剪掉传输层后面的数据，缓存在内存中。当内存中缓存的报文数目到达一定数量（如 20000 条/板）时，覆盖最先缓存的数据。

5.7 GTSM

目前网络上的一些攻击者模拟一些“有效报文”对 PTN 6900 进行攻击，导致设备有限资源（如主控板 CPU）的过载和消耗。例如，攻击者模拟真实的 BGP 协议报文，对一台 PTN 6900 不断地发送报文，PTN 6900 接口板收到这些报文后，发现是发送给本机的报文，则直接上送给主控板的 BGP 协议处理模块进行处理，而不辨别其合法性，这样导致主控板因为处理这些“合法”报文，系统异常繁忙，CPU 占用率高。

为了防止以上的攻击方式，PTN 6900 提供 GTSM（Generalized TTL Security Mechanism），即通用 TTL 安全保护机制。GTSM 通过检查 IP 报文头中的 TTL 值是否在一个预定的范围内，对 IP 层以上业务进行保护。在实际应用中，GTSM 主要用于保护建立在 TCP/IP 基础上的控制层面（路由协议等）免受 CPU 利用（CPU-utilization）类型的攻击，如 CPU 过载（CPU overload）。

PTN 6900 支持 BGP GTSM、OSPF GTSM 和 LDP GTSM。

5.8 ARP 防攻击

在现今的运营商网络中，Ethernet 是最常用的接入手段，而 ARP 作为 Ethernet 网络上的开放协议，为恶意用户的攻击提供了可能。恶意用户的攻击主要从空间与时间两方面进行。

- 空间方面的攻击主要利用 PTN 6900 的 ARP 缓存的有限性，通过发送大量伪造的 ARP 请求、应答报文，造成设备的 ARP 缓存溢出，从而无法缓存正常的 ARP 表项，进而阻碍正常转发。
- 时间方面的攻击主要利用 PTN 6900 计算能力的有限性，通过发送大量伪造的 ARP 请求、应答报文或其他能够触发 PTN 6900 ARP 处理的报文，造成 PTN 6900 的计算资源长期忙于 ARP 处理，影响其他业务的处理，进而阻碍正常转发。

基于接口的 ARP 表项限制

基于接口的 ARP 表项限制能够在 ARP 表项溢出攻击发生的情况下有效的限制攻击影响的范围，使攻击范围局限在接口之内，从而保证整板或整机的其他端口不受影响。

基于时间戳的防扫描

基于时间戳的防扫描特性能够在扫描（无论是 ARP 扫描还是 IP 报文扫描）攻击发生时，及时识别并抑制对扫描产生的请求的处理，从而保护 CPU 免受攻击。

版权所有 © 华为技术有限公司

ARP 双向分离

由于 ARP 请求报文来自设备外部，并且可以在任意时间由外部设备主动发起，因此，对于 ARP 请求报文，只要它的 IP 地址合法，一般无法区分是正常报文还是攻击报文。

通过对一些在运营网上实际发生的 ARP 攻击案例分析知道，在 ARP 攻击流量中，ARP 请求报文和 ARP 响应报文几乎各占 50%。因此，要想有效解决大流量 ARP 攻击问题，必须从 ARP 请求报文和 ARP 响应报文两方面同时入手。

ARP 双向分离处理是将 ARP 请求和 ARP 响应分开处理。

- 对 ARP 请求进行“无状态应答”，即在进行 ARP 应答之后不产生 ARP 表项及相关的状态，不上送 CPU 进行处理，而防止了使用 ARP 请求报文对网关设备 ARP 表进行地址欺骗的可能；
- 设备只上送 CPU 请求过的 ARP 响应报文，非 CPU 发出的 ARP 请求的 ARP 响应报文将被丢弃，有效地保证了来自正常主机的 ARP 请求报文被及时响应处理。

过滤非法 ARP 报文

目前 PTN 6900 支持对三种 ARP 报文进行过滤，这三种 ARP 报文为：

- 非法 ARP 报文。包括：目的 MAC 地址为单播的 ARP 请求报文、源 MAC 地址为非单播的 ARP 请求报文、目的 MAC 地址是非单播的 ARP 响应报文。
- 免费 ARP 报文。
- 请求 MAC 地址为非空的 ARP 请求报文。

可以通过命令行配置同时对上述一种或几种非法报文进行过滤。

ARP VLAN CAR

ARP VLAN CAR 主要应用在接口+VLAN 中，保证攻击发生时 VLAN 间的隔离，只影响到攻击所在的 VLAN，这样对设备和业务的影响就会大大降低。

PTN 6900 支持对于上送 CPU 的 ARP 报文，进行两级 CAR 限制。ARP VLAN CAR 为第二级 CAR 限制，可由用户进行设置。

在 ARP 报文上送 CPU 之前首先应用第一级 CAR 进行限制，当 ARP 报文上送值超出第一级 CAR 值时，超出报文将被丢弃。同时允许通过的上送流量将和第二级的 CAR 值进行比较，如果超出用户配置的阈值，第二级 CAR 值将对上送流量进行限制。 如果 ARP 报文上送值没有超过第一级 CAR 值，则所有的 ARP 报文将直接上送。

版权所有 © 华为技术有限公司

6 OAM

关于本章

6.1 MPLS Tunnel OAM

6.2 MPLS TP OAM
MPLS-TP OAM 用于 MPLS-TP 网络的运维管理，可以有效检测、识别和定位 MPLS-TP 网络的故障，在链路出现缺陷或故障时迅速进行保护倒换，从而有效降低网络维护的成本。

6.3 PW OAM
PW OAM 在 PW 层面提供了完善的故障检测与定位机制和网络性能监控功能。

6.4 以太业务 OAM

6.5 以太端口 OAM

6.6 BFD

6.7 业务镜像

版权所有 © 华为技术有限公司

6.1 MPLS Tunnel OAM

MPLS Tunnel OAM 为 MPLS 网络在 Tunnel 层面提供了完善的故障检测与定位机制和网络性能监控功能。故障检测与定位机制包括 Tunnel 的单双向连通性检测与故障点定位机制，并能在 Tunnel 出现缺陷或故障时迅速触发保护倒换；网络性能监控功能包括 MPLS Tunnel 的丢包率、时延和抖动等性能事件的检测和上报，在包交换网络中保证电信级的服务质量。

定义

MPLS OAM 机制可以有效地检测、确认并定位出源于 MPLS 层网络内部的缺陷并对网络性能进行监控。设备可以利用 OAM 的检测状态来触发保护倒换，实现快速故障检测和业务保护。 PTN 系列设备支持以下 MPLS OAM 功能：

- 采用硬件支持对 CV（Connectivity Verification）/FFD（Fast Failure Detection）/FDI（Forward Defect Indicator）/BDI（Backward Defect Indicator）消息的发送、接收和超时判断，实现快速连通性检测与失效指示。
- 支持 MPLS Tunnel 的 Ping、Traceroute 命令，便于故障检测与定位。
- 支持对 MPLS Tunnel 的性能监测，通过硬件实现对于丢包率、时延和抖动的监测。

目的和收益

MPLS 作为可扩展的下一代网络的关键承载技术，提供具有 QoS 保障的多业务能力。由于 MPLS 引入了一个独特网络层次，会存在由这个新的网络层引起的故障，因此 MPLS 网络需要具备 OAM 能力。

MPLS 支持多种三层和二层协议，如 IP、ATM、Ethernet 等。它提供一个完全不依赖于任何上层或下层的 OAM 机制，在 MPLS OAM 可以实现以下特性：

- 提供按需查询和连续的检测，随时了解被监控的 LSP 是否存在缺陷。
- 能够检测到网络的缺陷，并分析、定位缺陷，同时上报网管。
- 在链路出现缺陷或故障时迅速触发保护倒换。
- 能够实时监控丢包率、时延和抖动等性能事件，同时上报网管。

通过 MPLS OAM，运营商可以随时监控网络状态，及时判断网络故障产生的具体位置并采取措施，确保网络的顺畅。

6.2 MPLS TP OAM

MPLS-TP OAM 用于 MPLS-TP 网络的运维管理，可以有效检测、识别和定位 MPLS-TP 网络的故障，在链路出现缺陷或故障时迅速进行保护倒换，从而有效降低网络维护的成本。

目的和收益

随着网络和业务的转型和融合，各种新兴的网络和业务，例如三重播放、NGN、电信级以太网（Carrier Ethernet）、FTTx 等，都对单纯的分组传送网的投资成本、运维成本、QoS 保证、全业务接入、网络扩展性、网络可靠性和网络可管理性等提出了更高的要求。与缺乏控制平面、不能适应这些新需求的传统传送网技术相比，具有传送网特性、支持分组业务处理能力的 MPLS-TP 可以满足这些需求。

版权所有 © 华为技术有限公司

MPLS-TP 提供了完善的 OAM 能力，主要包括三个方面：

- 故障管理（Fault Management）
- 性能监控（Performance Monitoring）
- 保护倒换（Protection Switching）

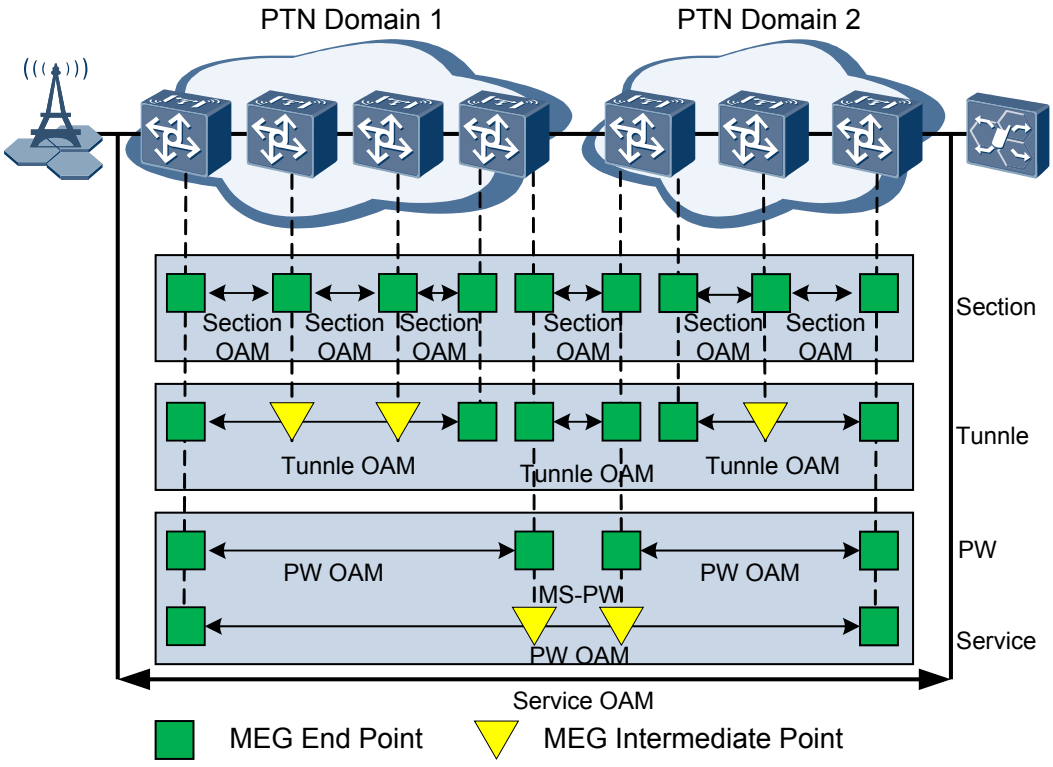
PTN 6900 支持 DM（Delay Measurement）时延和时延抖动统计：

- 单向时延和时延抖动统计
- 双向时延和时延抖动统计

应用

MPLS-TP 网络可以分为三层，包括 Section 层、LSP 层和 PW 层。Section 层是 LSP 层的服务层，LSP 层是 PW 层的服务层，PW 层是业务层的服务层；反过来说，LSP 层是 Section 层的客户层，PW 层是 LSP 层的客户层，业务层是 PW 层的客户层。MPLS-TP OAM 就应用于 MPLS-TP 网络的 Section 层、LSP 层和 PW 层，对出现的故障进行检测、识别和定位，如图 6-1 所示。

图 6-1 MPLS-TP OAM 的应用场景示意图



MPLS-TP OAM 提供了多种检测和定位故障的功能，Section 层、LSP 层和 PW 层各自支持的 MPLS-TP OAM 功能如表 6-1 所示。

版权所有 © 华为技术有限公司

表 6-1 Section 层、LSP 层和 PW 层各自支持的 MPLS-TP OAM 功能

MPLS-TP 层	MPLS-TP OAM 功能									
	CC	LB	LT	AIS	RDI	LCK	TST	LM	DM	CSF
Section	支持	支持	-	-	支持	支持	支持	支持	支持	-
LSP	支持	支持	支持	支持	支持	支持	支持	支持	支持	-
PW	支持	支持	支持	支持	支持	支持	支持	支持	支持	支持

说明

OptiX PTN 设备对 AIS 的支持情况如下:

- 端口故障向 Tunnel 下插 AIS
- Section 故障向 Tunnel 下插 AIS
- Tunnel 故障向 PW 下插 AIS

说明

OptiX PTN 设备目前只支持单端 LM。

说明

OptiX PTN 设备不支持在 ML-PPP 链路上配置 MPLS-TP Section OAM。

6.3 PW OAM

PW OAM 在 PW 层面提供了完善的故障检测与定位机制和网络性能监控功能。

支持的功能

PW OAM 机制可以有效地检测、确认并定位出源于 PW 层网络内部的缺陷和网络性能的监控。设备可以利用 OAM 的检测状态来触发保护倒换，实现快速故障检测和业务保护。

PTN 6900 系列设备支持以下 PW OAM 功能：

- 采用硬件支持对 CV（Connectivity Verification）/FFD（Fast Failure Detection）/FDI（Forward Defect Indicator）/BDI（Backward Defect Indicator）消息的发送、接收和超时判断，实现快速连通性检测与失效指示。在 PW 出现缺陷或故障时迅速触发保护倒换。
- 支持 PW 的 VCCV（Virtual Circuit Connectivity Verification）、Traceroute 命令，便于故障检测与定位。

应用场景

PW OAM 的应用场景如表 6-2 所示。

版权所有 © 华为技术有限公司

表 6-2 PW OAM 的应用场景

OAM 类型	作用	应用场景
CV/FFD	连通性检测	PW 状态实时检测
VCCV	连通性检测	单端定位或单端检测
Traceroute	故障点定位	PW 路由检测

6.4 以太业务 OAM

端到端以太网故障管理

下面从分级 MD 和端到端的故障检测和定位两方面介绍端到端以太网故障管理。

- 分级 MD

  PTN 6900 支持两种方式来提供端到端的以太网故障管理，即遵循 IEEE 802.1ag 实现和脱离 802.1ag 来实现。

  802.1ag 用于以太网端到端的连通性检测和故障定位，提供了基于不同级别（Level）的管理域配置，低 Level 的 OAM 报文不会被转发到高 Level 的管理域内，从而保证了网络的安全性和可维护性。

  在 802.1ag 中，将部署以太网 OAM 机制的网络划分为 MD（Maintenance Domain），一个 MD 就是由同一管理者维护的一个互相连接的以太网络。MD 中可以支持多个服务实例 SI（Service Instance），每个 SI 对应一个 VLAN。一个 SI 可以由多台设备组成，SI 边界的端口称为 MEP（Maintenance association End Point），其它端口负责实现 MEP 间的连接，称为 MIP（Maintenance association Internal Point），MEP、MIP 统称为 MP。一个 SI 中的所有 MEP 组成一个 MA（Maintenance Association），故障检测就是在 MA 中所有 MEP 之间进行的。

  MD 内的部分网络可能由另一个管理者维护，即 MD 可能嵌套。在一个 MA 内部可以运行不同层次的 OAM，MD Level 用于区分不同层次的 OAM。MD Level 在 OAM 报文中携带，低 Level 的 OAM 报文在高 Level 的 MP 上被丢弃。

- 端到端的故障检测和定位

  故障检测已逐渐成为 ISP（Internet Service Provider）或 ICP（Internet Context Provider）确保服务质量、降低维护成本的一个重要手段，主要通过定时发送和检测 CC（Continuity Check）报文来实现。

  故障定位通过 802.1ag 提供的 LB（LoopBack）和 LT（Link Trace）报文来实现 MAC Ping 和 MAC Trace 功能。

- MAC Ping

  基于 LB 报文实现的 MAC Ping 功能主要用于探测网络中某设备是否链路层可达，并获取网络状态和时延参数。

  网络中任意位置的两设备间进行 MAC Ping 功能，需要满足：发起点为 MEP，两点属于同一个 MA 且都是 MP 节点，两点间的以太网业务报文可通达。

- MAC Trace

  基于 LT 报文实现的 MAC Trace 功能主要用于探测网络中两设备间的实际业务路径，以及两设备之间的链路断路点。

  进行 MAC Trace 的约束条件和 MAC Ping 功能的要求相同。

版权所有 © 华为技术有限公司

以太网性能管理

PTN 6900 遵循 ITU-T Y.1731 标准提供以太网性能管理功能，通过在 802.1ag 的 LB 报文中插入时间戳可以测量传输过程中的时延、抖动、丢包率等指标，从而对指定时间段、指定网段进行性能检测，来获取某业务流端到端的性能参数。性能参数的测量可以配置为定时任务，并和网管信息结合共同输出报表。

有了性能管理工具，ISP 可以通过网管站实时监测网络运行情况，确认网络的转发能力是否符合与用户签订的 SLA（Service Level Agreement），并快速定位网络故障。由于不需要在用户侧执行这些检测操作，所以极大降低了网络维护费用。

6.5 以太端口 OAM

PTN 6900 上支持的以太网 OAM 功能包括故障管理和性能管理两大部分。

故障管理是通过定时或手动触发的方式发送检测报文来探测网络的连通性，其实现机制类似于 BFD（Bidirectional Forwarding Detection），同时也提供类似于 IP 网络中 Ping 和 Tracert 的手段对以太网进行故障定位。故障管理可用于触发保护倒换，从而实现小于 50ms 的保护倒换。

性能管理主要指对网络传输中的丢包率、时延、抖动等参数的衡量，也包括对网络中各类流量（如接收发送字节数、错误报文数等）进行统计。

点到点以太网故障管理

IEEE 802.3 ah 最初是由 EFMA 提出的，包括能力发现、链路性能监测、故障侦测和告警、环路检测。802.3ah 是一种慢协议，故障定时检测报文发送频率为 1s。

PTN 6900 遵循 IEEE 802.3ah 提供点到点以太网故障管理功能，可以用于检测用户侧最后一公里以太网直连链路上的故障。目前，PTN 6900 支持 802.3ah 中的邻居自动发现、链路故障监控、远端故障通知、远端环回设置功能。

6.6 BFD

BFD（Bidirectional Forwarding Detection）是一套全网统一的检测机制，用于快速检测、监控网络中链路或者 IP 路由的转发连通状况。

BFD 在双向链路两端同时发送检测报文，检测两个方向上的链路状态，实现毫秒级别的链路缺陷检测。支持 BFD 单跳检测和多跳检测。

PTN 6900 的 BFD 特性支持以下的应用。

BFD for VRRP

使用 BFD 检测、监控网络中链路或者 IP 路由的转发连通状况，触发 VRRP 快速切换。

BFD 触发快速重路由

- BFD for LDP FRR
- 可以通过 BFD 检测被保护的接口，触发 LDP FRR 切换。
- BFD for IP FRR 以及 BFD for VPN FRR
- 在 PTN 6900 中，通过 BFD 检测故障的上报，可以触发 IP FRR 以及 VPN FRR。

版权所有 © 华为技术有限公司

BFD for 静态路由

静态路由自身没有检测机制，当网络发生故障时需要管理员介入。

使用 BFD for 静态路由特性，可以利用 BFD 会话检测公网 IPv4 静态路由的状态。路由管理系统根据 BFD 会话的状态决定静态路由是否可用。

BFD for IS-IS

PTN 6900 支持使用静态配置的 BFD 会话对 IS-IS 邻居关系进行检测。

通过 BFD 检测 IS-IS 邻居节点间的链路故障，快速报告给 IS-IS 协议，从而触发 IS-IS 路由快速收敛。

BFD for IPv6 IS-IS

PTN 6900 支持 IPv6 IS-IS 协议动态创建和删除 BFD 会话。

- 当路由协议邻居建立成功时，路由协议通过路由管理模块通知 BFD 建立会话，对路由协议的邻居关系进行快速检测。BFD 会话的检测参数由路由协议设置。
- 当 BFD 会话检测到故障时，状态变为 Down，BFD 通过路由管理模块触发路由收敛。

  说明

  路由协议一般基于 Hello 报文的 KeepAlive 机制，只能实现秒级检测。而 BFD 检测是毫秒级。当配置 10ms 检测周期和 3 倍检测间隔时，BFD 可以在 50ms 内通报协议故障，因此能够提高路由的收敛速度。
- 当邻居状态不可达时，路由协议通过路由管理模块通知 BFD 删除相应会话。

BFD for OSPF/BGP

支持 OSPF 和 BGP 协议动态创建和删除 BFD 会话。

- 当路由协议邻居建立成功时，路由协议通过路由管理模块通知 BFD 建立会话，对路由协议的邻居关系进行快速检测。BFD 会话的检测参数由路由协议设置。
- 当 BFD 会话检测到故障时，状态变为 Down，BFD 通过路由管理模块触发路由收敛。

说明

路由协议一般基于 Hello 报文的 KeepAlive 机制，只能实现秒级检测。而 BFD 检测是毫秒级。当配置 10ms 检测周期和 3 倍检测间隔时，BFD 可以在 50ms 内通报协议故障，因此能够提高路由的收敛速度。

- 当邻居状态不可达时，路由协议通过路由管理模块通知 BFD 删除相应会话。

BFD for OSPFv3/BGP4+

PTN 6900 支持 OSPFv3 和 BGP4+协议动态创建和删除 BFD 会话。

- 当路由协议邻居建立成功时，路由协议通过路由管理模块通知 BFD 建立会话，对路由协议的邻居关系进行快速检测。BFD 会话的检测参数由路由协议设置。
- 当 BFD 会话检测到故障时，状态变为 Down，BFD 通过路由管理模块触发路由收敛。

版权所有 © 华为技术有限公司

说明

路由协议一般基于 Hello 报文的 KeepAlive 机制，只能实现秒级检测。而 BFD 检测是毫秒级。当配置 10ms 检测周期和 3 倍检测间隔时，BFD 可以在 50ms 内通报协议故障，因此能够提高路由的收敛速度。

- 当邻居状态不可达时，路由协议通过路由管理模块通知 BFD 删除相应会话。

BFD for PIM

PIM BFD 适用于多个 PIM 设备共享网段，快速检测 DR 或 Assert Winner 接口故障。

PIM BFD 使用规范的 BFD 消息，在 PIM 邻居接口之间自动建立 BFD session，监测 PIM 邻居状态，在邻居失效时能够快速响应。

BFD 对 Eth-Trunk 的检测

Eth-Trunk 都由多条成员链路组成，用于提供大带宽或增强可靠性。

只有处于 Up 状态的成员链路条数达到一定数目时，相应的 Trunk 才能保持 Up 状态。

PTN 6900 的 BFD 实现对 Trunk 和 Trunk 成员链路的分别检测，既可以检测整个 Trunk 的连通情况，也可以检测 Trunk 中某条重要成员链路的连通情况。

BFD for LSP

BFD for LSP 是指在静态 LSP、动态 LDP LSP、RSVP-TE 隧道和 PW 上发送 BFD 报文，通过 BFD 报文的快速收发，完成对这些隧道链路故障的快速检测，从而引导上面承载业务的快速切换，达到业务保护的目的。

BFD for LSP 通过对 LSP、TE 隧道和 PW 三种逻辑链路故障的快速检测和传递，可以实现 VPN FRR、TE FRR、VLL FRR 等各种 MPLS 业务的快速倒换。

6.7 业务镜像

镜像是在不影响原有转发的情况下，将网络中通过当前节点的报文复制一份到指定的观测端口。用户可以根据需要定义被镜像的端口号，然后将报文分析设备与观测端口相连，进行流量观测。如果观测端口与镜像端口在同一设备，称为本地镜像；如果观测端口与镜像端口在不同的设备，称为远端镜像。PTN 6900 既支持本地镜像，也支持远程镜像功能。

根据复制报文满足的条件，镜像分为端口镜像和流镜像两种：

- 端口镜像：指将镜像端口接收或发送的报文完整地复制输出到指定的观测端口。
- 流镜像：指将镜像与流分类相结合，只复制满足特定条件的报文，过滤报文分析设备不关心的报文，为报文分析提供更精细的控制，提高报文分析设备的工作效率。

根据复制报文的方向，镜像又可分为上行镜像和下行镜像两种：

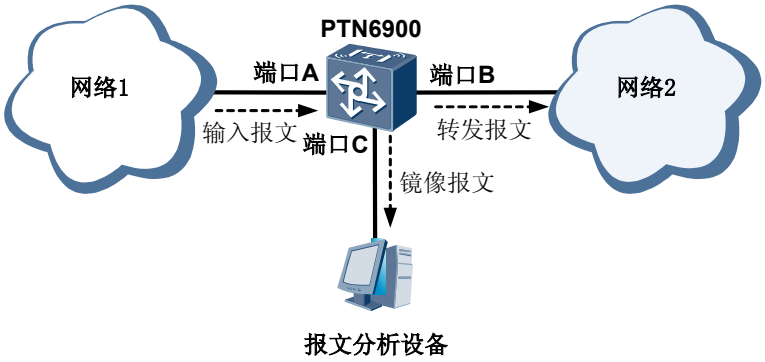
- 上行镜像：指将镜像端口接收到的全部报文或满足特定流分类条件的报文完整地复制输出到指定的观测端口。
- 下行镜像：指将镜像端口即将发送出的全部报文或满足特定流分类条件的报文完整地复制输出到指定的观测端口。

版权所有 © 华为技术有限公司

本地镜像

本地镜像的典型组网环境如图 6-2 所示。

图 6-2 本地镜像典型组网示意图



网络 1 和网络 2 通过 PTN 6900 连通，要监控端口 A 上网络 1 的输入流量，可以将端口 A 的上行流量复制一份镜像报文，流量正常转发的同时，镜像报文可以从端口 C 转发到报文分析设备处理。某些情况下，需要对网络 1 的输入输出流量同时进行监控，PTN 6900 需要将端口 A 的上下行流量同时镜像一份到观测端口。

对于本地镜像，系统一个接口板允许配置一个物理观测端口以及多个逻辑观测端口；一个接口板允许配置多个镜像端口。

在进行本地镜像时，系统支持跨板镜像，即观测端口和镜像端口可以配置在不同的单板上。

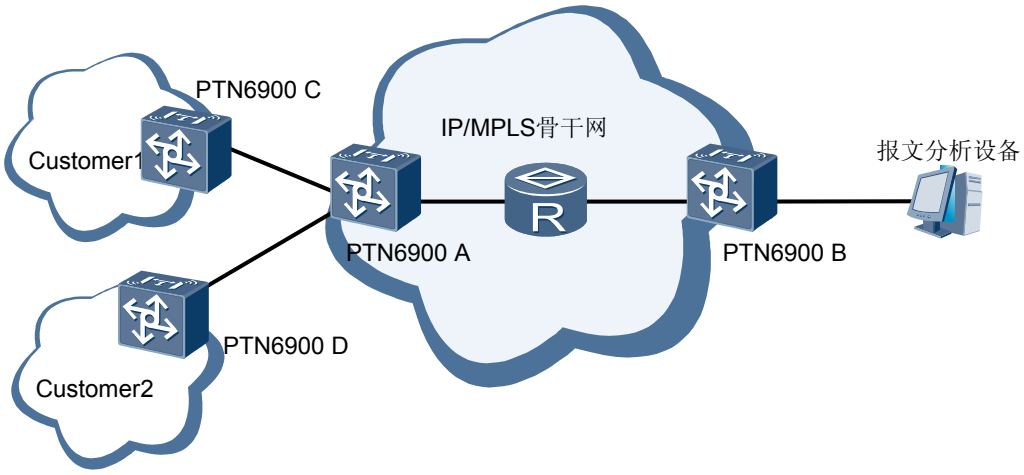
远端镜像

相对于本地镜像，远端镜像有如下好处：

- 网络维护人员不需要赶到现场，能够远程分析镜像报文。
- 一个网络维护人员同时可以处理不同站点设备的镜像操作，节省了维护人力。

远端镜像的典型组网环境如图 6-3 所示。

图 6-3 远端镜像典型组网图



版权所有 © 华为技术有限公司

PTN 6900 A 和 PTN 6900 B 是 IP/MPLS 骨干网络的边界设备，客户端网络 customer 通过 PTN 6900 C 和 PTN 6900 D 接入骨干网络，出于维护、分析攻击或定位问题的需要，可能需要查看 PTN 6900 A 发出或接收的协议报文是否正确，或者查看 PTN 6900 C 的一个绑定客户 VPN 的子接口是否受到攻击，这时就需要将 PTN 6900 A 收到的某一类协议报文，或者 PTN 6900 A 发出到 PTN 6900 C 的协议报文，或者 PTN 6900 A 的子接口收到的报文镜像到远端 PTN 6900 B 的报文分析设备进行分析。

在远端镜像中，远端镜像源的镜像接口的数据会被复制一份从指定的隧道发出，到达远端的一个目的设备（即远端镜像观测口所在的设备），然后由该远端镜像观测口输出至报文分析设备。并且每一个远端镜像源和一个远端镜像观测口组成一条流；如果有 2 个远端镜像源的数据都从一个远端镜像观测口输出，那么就是 2 条流。

PTN 6900 支持做为远端镜像的隧道类型有 MPLS LSP 和 MPLS TE。

对于远端镜像，系统一个接口板支持配置多个观测端口和多个镜像端口。

远端镜像同时提供对镜像报文的截取功能。

版权所有 © 华为技术有限公司

7 保护

关于本章

PTN 6900 分组传送平台在各个层面提供完善的电信级保护，包括 GR、NSR、设备级保护和网络级保护。

7.1 GR

7.2 NSR

7.3 设备级保护
设备级保护包括了关键部件冗余备份、业务处理板的高可靠性、传输告警的定制和抑制。

7.4 网络级保护
网络级保护包括 VRRP、MPLS Tunnel 的 1:1 保护、PW APS 保护、快速重路由保护、线性复用段保护、以太网 LAG 保护、生成树保护、分组 E1 ML-PPP 保护。

版权所有 © 华为技术有限公司

7.1 GR

GR（Graceful Restart）是提供 HA 的一个关键技术。管理员或故障都可触发 GR 倒换和后续重启。GR 在发生故障倒换时既不删除路由表/转发表中的路由信息也不复位接口板，因此整个系统可以不中断业务。

GR 具有如下优势：

- 简单易实现，无须对现有软件做大的改动，只须修改一些协议即可；
- 无须备份协议的状态信息；
- 仅少量信息需要从 AMB 备份到 SMB，这些信息包括配置修改或更新的信息和事件、接口状态变化信息，及重启后可从邻居获得拓扑或路由信息；
- 发生主板切换时中断转发业务的概率很低；
- 正常情况下网络聚合迅速。

PTN 6900 支持系统级 GR 和协议级 GR。协议级 GR 包括：

- OSPFv3
- BGP 协议级 GR
- OSPF 协议级 GR
- ISIS 协议级 GR
- MPLS LDP 协议级 GR
- VLL GR（matini）
- VPLS GR（matini）
- RSVP GR
- L3VPN GR
- RSVP GR
- PIM GR

7.2 NSR

不间断路由 NSR（Non-Stop Routing）是系统控制平面发生故障，且存在备用控制平面的场景下邻居控制平面不感知的一种技术，不仅仅局限于路由信令的邻居关系不中断，也包括 MPLS 信令协议，以及其他为满足业务需求而提供支撑的协议。

NSR 作为可靠性的解决方案，其根本目的都是为了保证用户业务在设备故障的时候不受影响或者影响最小。

目前，支持 NSR 功能的协议有：

- OSPF 和 OSPFv3
- LDP
- RSVP-TE
- PIM、MSDP 和 IGMP
- ARP
- L3VPN

版权所有 © 华为技术有限公司

- ISIS 和 ISIS6
- BGP 和 BGP4+
- VRRP 和 VRRP6

7.3 设备级保护

设备级保护包括了关键部件冗余备份、业务处理板的高可靠性、传输告警的定制和抑制。

7.3.1 关键部件冗余备份

PTN 6900 支持主控板单配置和双配置（冗余方式）两种工作方式。且主控板支持热备份功能。当主控板双配置时，主用板正常工作，备用板处于 Standby 状态。备用板的管理网口不允许用户访问，Console 口和 AUX 口也不接受用户的配置命令。备用主控板只和主用主控板交互信息（包括心跳信息和备份数据），和其他单板（或设备）没有信息交互。

系统支持两种倒换方式：自动倒换和强制倒换两种方式。自动倒换的触发条件包括：主用板发生严重故障、主用板复位。强制倒换通过控制台命令触发。另外，用户可以通过控制台命令强行禁止主控板的主备倒换。

PTN 6900 系统内部支持管理总线的备份，系统供电电源的 1+1 备份，另外系统各单板及电源、风扇模块均具有热插拔功能。

这些设计使得设备或网络出现严重异常时，系统能够快速地恢复和作出反应，从而提高系统的平均无故障运行时间，尽可能地降低不可靠因素对正常业务的影响。

7.3.2 业务处理板的高可靠性

PTN 6900 实现了主要业务接口上同类业务接口的协议备份功能，包括：

- 在以太网口上提供 VRRP 功能。PTN 6900 可以通过扩展的 VRRP 协议，对处于同一 PTN 6900 或者不同 PTN 6900 上的两个接口进行相互备份，保证 PTN 6900 在以太网侧接口上的高可靠性。
- 在 Eth-Trunk 上支持成员端口采用组内备份和组外备份。
- 在进行 Trunk 捆绑时，支持跨板捆绑：
  - 用户可以通过双链路接入不同业务处理板，进行跨板捆绑，确保业务高可靠性。
  - 跨板捆绑功能是通过高性能硬件引擎实现，从而可以在多条链路上实现报文的负载分担转发。
  - 基于源＋目的 IP 地址 HASH 算法，实现各链路流量均衡转发。
  - 链路故障情况下无缝切换，不影响业务转发。

PTN 6900 通过协议扩展，在主要的业务接口类型上实现了接口备份，从而保证了 PTN 6900 在承载局域、城域和广域业务时，都可以实现接口运行状态的监控与备份，达到了需要备份的接口状态发生变化不影响路由表的变化、提高业务恢复速度的目的。

7.3.3 传输告警定制抑制

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，因为告警信息上报速度加快，引起接

版权所有 © 华为技术有限公司

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：

- 实现对告警的定制，可以指定哪些告警能够引起接口状态变化等。
- 实现对告警的抑制，可以达到过滤毛刺、抑制网络反复振荡的目的。

7.4 网络级保护

网络级保护包括 VRRP、MPLS Tunnel 的 1:1 保护、PW APS 保护、快速重路由保护、线性复用段保护、以太网 LAG 保护、生成树保护、分组 E1 ML-PPP 保护。

7.4.1 MPLS Tunnel 1:1 保护

MPLS Tunnel 的 1:1 保护，通过保护通道来保护工作通道上传送的业务。当工作通道故障的时候，业务倒换到保护通道。1:1 保护的业务单发单收。

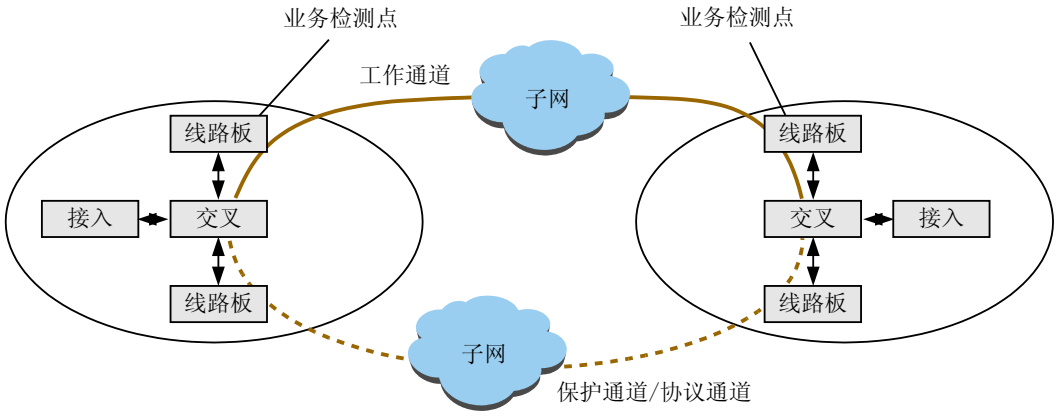
MPLS Tunnel 保护的扩展 APS 协议通过保护通道传送，相互传递协议状态和倒换状态。两端设备根据协议状态和倒换状态，进行业务倒换。

保护符合 ITU-T G.8131 协议。

MPLS Tunnel 的 1:1 保护

设备支持的 MPLS Tunnel 的 1:1 保护如图 7-1 所示。

图 7-1 MPLS Tunnel 的 1:1 保护



MPLS Tunnel 的 1:1 保护，业务从工作通道传送。当工作通道故障的时候，倒换到保护通道，业务单发单收。扩展 APS 协议通过保护通道传送，相互传递协议状态和倒换状态。两端设备根据协议状态和倒换状态，进行业务倒换。

- 检测方法：

版权所有 © 华为技术有限公司

- 物理层检测：检测信号丢失，检测时间微秒级。
- 链路层检测：通过 MPLS OAM 进行检测。如果要保证 MPLS 自动保护倒换时间在 50ms 内，MPLS OAM 的检测时间为 3.3ms。

- 倒换过程：通过扩展 APS 协议相互协商，发送端倒换业务到保护通道，接收端从保护通道接收业务。

保护参数

MPLS Tunnel 的 1:1 保护的参数如表 7-1 所示。

表 7-1 MPLS Tunnel 的 1:1 保护的参数

倒换类型	恢复类型	倒换协议	倒换时间	倒换拖延时间	默认恢复时间
1:1 双端倒换	非恢复式	扩展 APS 协议	≤50ms	0 ～ 10s，缺省为 0	-
1:1 双端倒换	可恢复式	扩展 APS 协议	≤50ms	0 ～ 10s，缺省为 0	300s
倒换条件（满足任一条件即可）： ● 工作通道故障 ● 单板故障 ● 单板硬复位 ● 人工下发倒换命令 ● 物理链路失效 ● MPLS OAM 检测到 LSP 失效					

7.4.2 VRRP

VRRP（Virtual Router Redundancy Protocol）是一种容错协议，通过物理设备和逻辑设备分离，实现在多个出口网关之间选路。

VRRP 适用于支持组播或广播的局域网（如以太网等），提供逻辑网关确保高可用度的传输链路，不仅能够解决因某网关设备故障带来的业务中断，而且无需修改路由协议的配置。

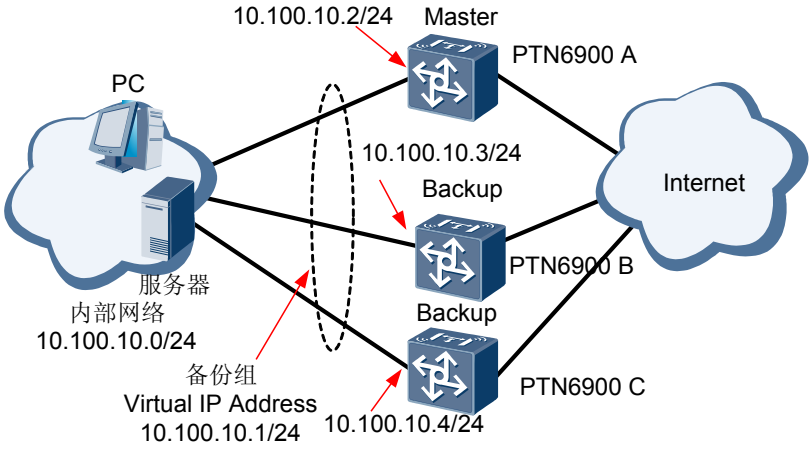
VRRP 将局域网的一组 PTN 6900 构成一个备份组，相当于一台虚拟 PTN 6900。局域网内的主机仅知道这个虚拟 PTN 6900 的 IP 地址，并不知道备份组内具体某台设备的 IP 地址，它们将自己的缺省路由下一跳地址设置为该虚拟 PTN 6900 的 IP 地址。于是，网络内的主机就通过这个虚拟 PTN 6900 与其它网络进行通信。

备份组中，仅有一台设备处于活动状态，称为主用设备（Master）；其余设备都处于备份状态，并随时按照优先级高低做好接替任务的准备，称为备份设备（Backup）。

图 7-2 所示为三台 PTN 6900 组成的备份组。

版权所有 © 华为技术有限公司

图 7-2 采用 VRRP 的虚拟 PTN 6900 组网



VRRP 机制将该虚拟 PTN 6900 动态关联到承担传输业务的物理 PTN 6900 上，当该物理 PTN 6900 出现故障时，再次选择新 PTN 6900 来接替业务传输工作，整个过程对用户完全透明，实现了内部网络和外部网络不间断通信。

mVRRP

mVRRP（Management Virtual Router Redundancy Protocol）是指管理 VRRP。管理 VRRP 备份组从本质上讲就是普通的 VRRP 备份组，它与普通 VRRP 备份组的唯一区别在于：管理 VRRP 备份组可以绑定其他的业务备份组，并根据绑定关系，决定相关业务备份组的状态。

一个管理 VRRP 备份组可以绑定多个业务备份组，但它不能作为业务备份组与其他管理备份组进行绑定。

管理 VRRP 备份组也可以作为一般成员加入 VGMP 组中。在将管理 VRRP 备份组加入 VGMP 组后，可以配置管理 VRRP 监视 Peer BFD 和 Link BFD 会话状态，但管理 VRRP 备份组状态机将会丧失自己的独立性，除了 Initialize 状态之外，Backup 和 Master 状态需要根据所加入 VGMP 组的状态来决定。

VGMP

在一些严格要求会话的来回路径一致（即同一个会话来回的报文要通过同一台设备）的应用中，VRRP 提供的路由备份功能存在局限性，即如果发生了主备状态切换，将不能保证同一个会话来回路径一致。

华为公司为防止 VRRP 状态不一致现象的发生，在 VRRP 的基础上自主开发了扩展协议 VGMP（VRRP Group Management Protocol），基于 VGMP 协议建立的 VRRP 管理组负责统一管理加入其中的各 VRRP 备份组的状态，保证一台 PTN 6900 上的接口同时处于主用或备用状态，实现 PTN 6900 VRRP 状态的一致性。

在以下的应用场景中，需要配置 VGMP 特性：

- 系统配置大量 VRRP 备份组
- VRRP 协议报文在主控板处理，配置大量 VRRP 备份组会产生大量 VRRP 协议报文，这些协议报文和其它协议报文竞争 CPU 资源和板间通信的通道和带宽，将对系统造成沉重的负担。

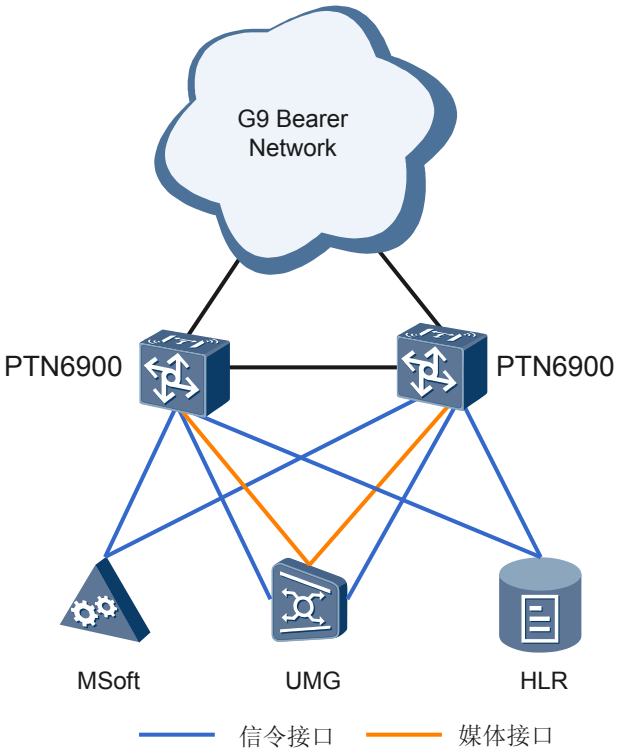
版权所有 © 华为技术有限公司

- 配置一个 VRRP 管理组来统一管理这些 VRRP 备份组，被管理的 VRRP 备份组不再各自发送协议报文，可以减少系统资源占用率。
- PTN 6900 具有防火墙、Proxy 服务器功能
- 这些功能都要求同一会话来回路径一致，配置一个 VRRP 管理组对 VRRP 备份组进行统一协调，保证管理组内 VRRP 备份组状态一致。

E-VRRP

E-VRRP 主要解决 NGN 接入中非 SCTP 多归属/非负载分担方式组网的可靠性。

图 7-3 E-VRRP 组网



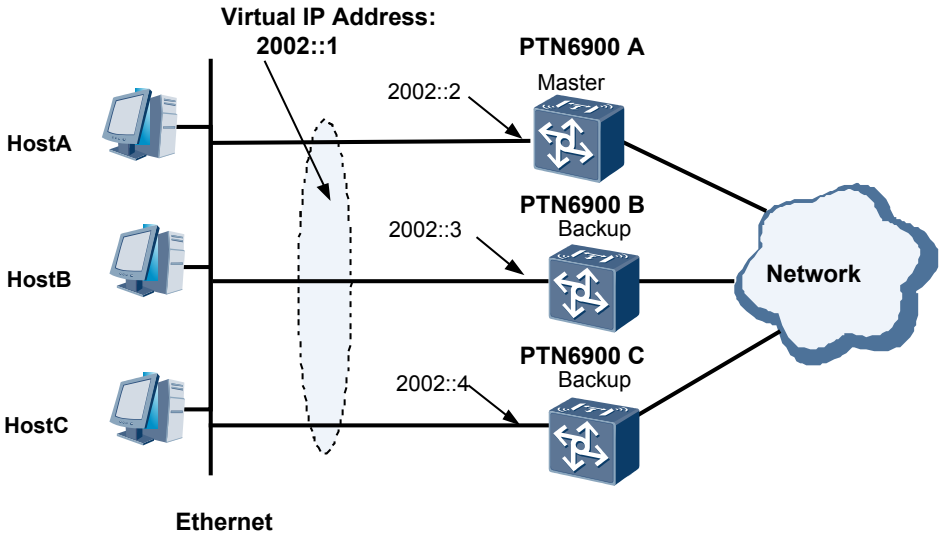
如图 7-3 所示，MsoftX、UMG 和 HLR 设备双归接入到 VRRP 主备网关。媒体面可靠性通过 VRRP 接入 UMG 可以解决；信令面可靠性可以通过使用 SCTP 多归属保证，但是如果不支持 SCTP，则可通过 E-VRRP 来实现可靠性。

VRRP For IPv6

VRRP For IPv6 是指在 IPv6 网络中应用 VRRP 功能，VRRP 的基本原理没有发生变化。

版权所有 © 华为技术有限公司

图 7-4 VRRP For IPV6 基本组网



如图 7-4 所示，在 IPv6 组网中，各个主机和 PTN 6900 运行 IPv6 协议。VRRP 将局域网的一组 PTN 6900 构成一个备份组，相当于一台虚拟 PTN 6900。局域网内的主机只需要知道这个虚拟 PTN 6900 的 IPv6 地址，并不需知道具体某台设备的 IPv6 地址，将网络内主机的缺省网关设置为该虚拟 PTN 6900 的 IPv6 地址，主机就可以利用该虚拟网关与外部网络进行通信。为了在确保可靠性的同时充分利益 PTN 6900 资源，可以创建多个备份组，形成多个虚拟 PTN 6900 来均衡网络流量。

7.4.3 FRR

PTN 6900 提供多种快速重路由特性，可以根据网络的需求在不同的组网环境中进行部署，从而提高网络的可靠性。

IP FRR

快速重路由功能，也称为 FRR（Fast ReRoute），它的切换速度可以达到 50ms，能够最大程度减少网络故障时数据的丢失。

PTN 6900 提供的快速重路由功能，可以使系统实时监视并保存接口线路板和端口的状态，并在转发过程中检查端口的状态。在端口发生异常时 PTN 6900 可以迅速地切换到另外一条路由（预先建立），从而提高了无故障运行时间，减少了丢包数量。

LDP FRR

传统的 IP FRR（Fast ReRoute）无法有效保护 MPLS 网络中的流量，PTN 6900 提供 LDP FRR 功能，为 MPLS 网络提供端口级的保护方案。

LDP 工作在下游自主标签分发、有序标签控制以及自由标签保持方式时，LSR 会保存所有收到的标签映射，但只有从 FEC 对应路由的下一跳发送来的标签映射会生成标签转发表。利用这一特点，如果为 liberal 标签映射也生成标签转发表，就相当于建立了备份 LSP。

网络运行正常时，使用正常的 LSP 转发，如果正常 LSP 的出接口 Down，使用备份 LSP 转发，这样可以在网络收敛之前的短时间内保证流量不中断。

版权所有 © 华为技术有限公司

TE FRR

TE FRR 是 MPLS TE 中实现网络局部保护的技术，只有速率在 100Mbps 以上的接口才支持 TE FRR。TE FRR 的切换速度可以达到 50ms，能够最大程度减少网络故障时数据的丢失。

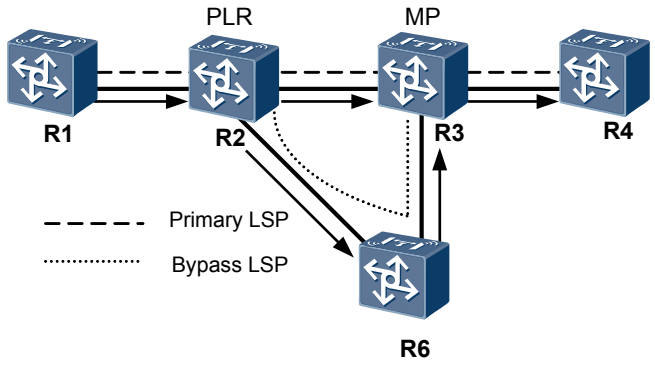
但 TE FRR 只是一种临时性保护措施，一旦被保护的 LSP 恢复正常或建立了新的 LSP，流量就会切换回原 LSP 或新建立的 LSP。

对 LSP 配置 TE FRR 功能后，当 LSP 上的某条链路或某个节点失效时，流量会被切换到保护链路上，同时 LSP 入节点尝试建立新的 LSP。

根据保护的对象不同，TE FRR 分为两类：

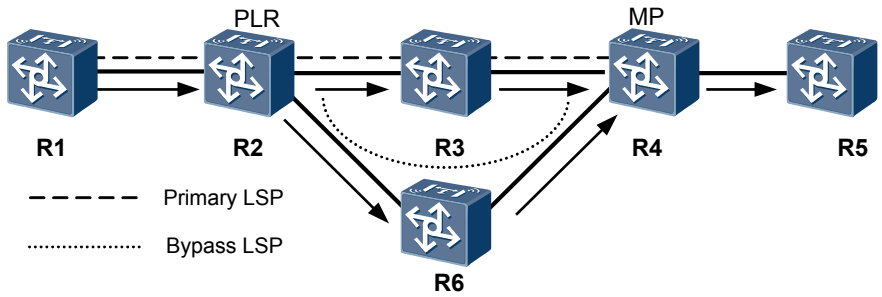
- 链路保护：PLR 和 MP 之间有直接链路连接，主 LSP 经过这条链路。当这条链路失效时，流量可以切换到 Bypass LSP 上。如图 7-5 所示，主 LSP 是 R1→R2→R3→R4，Bypass LSP 是 R2→R6→R3。

图 7-5 TE FRR 链路保护示意图



- 节点保护：如图 7-6 所示，PLR 和 MP 之间通过 R3 连接，主 LSP 经过 R3。当 R3 失效时，流量可以切换到 Bypass LSP 上。图中，主 LSP 是 R1→R2→R3→R4→R5，Bypass LSP 是 R2→R6→R4，R3 是被保护的 PTN 6900。

图 7-6 TE FRR 节点保护示意图



版权所有 © 华为技术有限公司

VLL FRR

VLL FRR 是 L2VPN 网络中实现网络保护的技术，它可以在网络发生故障后快速将用户流量切换到备份链路上，从而到达提高 L2VPN 网络高可靠性的目的。VLL FRR 又称 VLL 冗余备份（VLL Redundancy）。

L2VPN 网络中的 VLL FRR 主要包括故障的检测、故障的传递和主备链路的切换三部分。

PTN 6900 可以提供多种特性，将这些特性结合起来最终完成 VLL FRR 的功能。

- 故障的检测
- BFD for PW 功能可以快速的检测到 L2VPN 网络中网络测的 PW 的故障。
- 以太网 OAM、PPP 可以快速检测 L2VPN 网络中 AC 侧的故障。
- 故障的传递
- 通过 LDP、BGP 或 RSVP 向远端 PE 通告 LSP/PW 或 AC 的故障。
- 通过 BFD for LSP/PW 向远端 PE 通告 LSP/PW 或 AC 的故障。
- 通过以太网 OAM、PPP 向本端 CE 通告故障。
- 主备链路的切换
- 在对称的网络中，由 CE 设备完成切换。
- 在非对称的网络中，由 PE 设备和 CE 设备共同完成切换。

VPN FRR

传统 L3VPN 网络中本端 PE 对于远端 PE 的故障，需要通过 BGP hello 报文的超时感知。这个感知时间典型配置是 90s，也就是说远端 PE 故障 90s 后，本端 PE 上的 VPN 路由才能重新收敛。

PTN 6900 支持的 VPN FRR 可以解决以上的问题。在 CE 双归属情况下，当发生 CE 与 PE 之间的链路断掉或 PE 重启时，VPN FRR 可以实现 VPN 业务能够快速的倒换到备用隧道和备用 PE，从而保证流量在很短的时间内可以恢复。

- 本端 PE 的转发平面同时保留远端主用 PE 的外层标签和其分配给 VPN 路由的内层标签，以及对应的远端备用 PE 的外层标签和其分配给 VPN 路由的内层标签。
- 使用 BFD 等端到端故障检测方法，在 200ms 内感知远端主用 PE 故障，然后进行主备内外层标签的同时切换。
- VPN FRR 解决的是内层标签的切换问题，其倒换优先级低于 LDP/MPLS TE FRR，因此故障感知时间要长于 LDP/TE FRR 的保护倒换时间。

7.4.4 PW APS 保护

PW APS(Automatic Protection Switching)是一种网络保护机制，当工作 PW 发生故障时，业务倒换到保护 PW 上，从而保护工作 PW 上承载的业务。

特性简介

PW APS 通过 PW OAM 检测机制检测工作 PW、保护 PW 的状态，当 PE 设备检测到工作 PW 故障时，两端 PE 设备交互 APS 协议，执行 PW APS 倒换，业务倒换到保护 PW 上，实现业务保护。APS 保护协议运行在保护 PW 上。

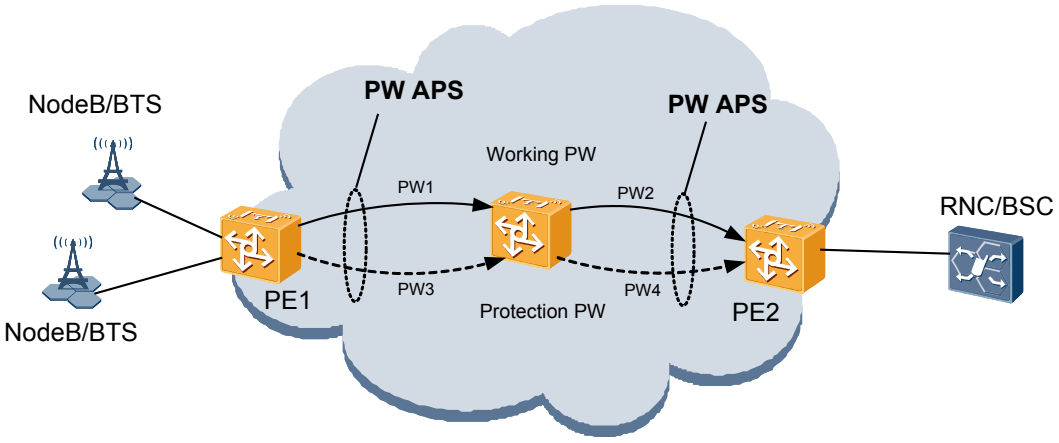
版权所有 © 华为技术有限公司

组网应用

PW APS 支持两种组网应用：设备内保护组、跨设备（MC-PW APS）保护组。PTN 6900 分组传送平台支持作为双归点创建跨设备保护组。

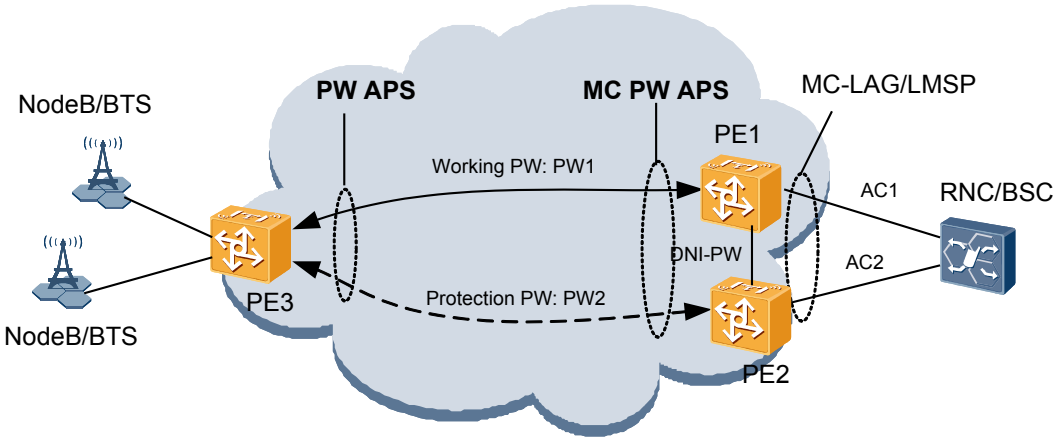
设备内保护组如图 7-7 所示，PE1 与 PE2 之间创建工作 PW、保护 PW，PW APS 保护组。正常情况下，业务在工作 PW 上传送；当工作 PW 故障时，发生 APS 保护倒换，业务在保护 PW 上传送。

图 7-7 设备内 PW APS 组网



跨设备保护组如图 7-8 所示，PE3 与 PE1 之间创建工作 PW1，PE3 与 PE2 之间创建保护 PW2，PE1 与 PE2 之间创建 DNI-PW。PE3 上配置设备内保护组，PE1 与 PE2 之间创建跨设备保护组。跨设备的 PW APS 保护组用于双归保护场景。

图 7-8 MC-PW APS 组网



支持情况

PTN 6900 设备当前仅支持 1:1 恢复式、双端倒换的 PW APS 保护。

PW APS 支持对 CES、以太网专线业务及以太网专网业务中的 PW 进行保护。

版权所有 © 华为技术有限公司

PW APS 保护组的工作 PW、保护 PW 所在的 Tunnel，不能创建 Tunnel APS 保护组。即，同一条 Tunnel 上不能同时配置 Tunnel APS 和 PW APS。

对于同一条 PW 只能配置一种保护。即，同一条 PW 上不能同时存在设备内 PW APS 保护和 MC-PW APS 保护。

7.4.5 环网保护

环网保护主要用于二纤双向环的单环组网和多环相交组网场景中，当多节点故障时，能够对业务进行完善保护。

目的和收益

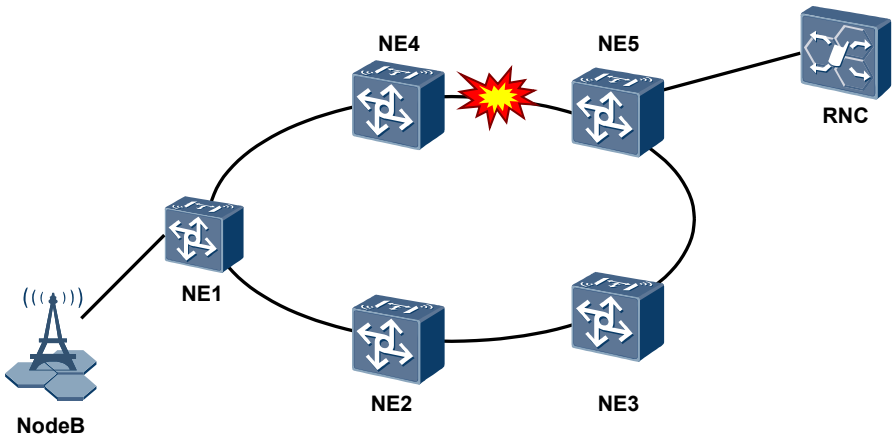
在传输网络中，环网保护方案具有很多线性保护方案无法比拟的优势。

- 减轻了配置工作量，并节约了隧道资源。传统的线性保护要求用户为每个工作隧道配置相应的保护隧道，而环网保护不需要配置保护隧道。
- 降低了对设备和链路带宽资源的消耗。传统的线性保护要求为每个隧道配置相应的 OAM 实例，而且每个保护组还需要配置一个 APS 实例。而环网保护仅要求每个设备使用两个 OAM 实例和两个环网 APS 实例，OAM 实例与 APS 实例数量与业务数无关。
- 减轻了维护工作量。传统的线性保护在调整保护链路路径时，需要更改每条业务相应的保护链路的配置，维护工作量非常大。而部署环网保护后，在保护链路上进行破环加点操作时，仅需在增加的节点上进行环网配置，即可完成整个任务。
- 提高了保护的可靠性。线性保护方案中，若工作和保护链路上分别有一个故障点，则业务中断。而环网保护方案则可以实现部分多点故障场景的保护。

组网应用

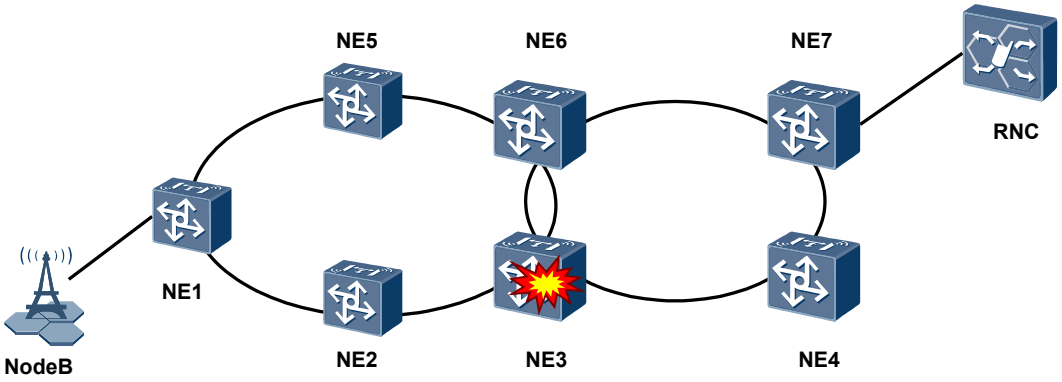
环网保护主要应用在二纤双向环的单环组网和多环相交组网场景中，如图 7-9 和图 7-10 所示。当业务正常传输路径出现故障时，通过环网保护可以实现业务的继续传输。

图 7-9 环网保护典型应用场景一



版权所有 © 华为技术有限公司

图 7-10 环网保护典型应用场景二



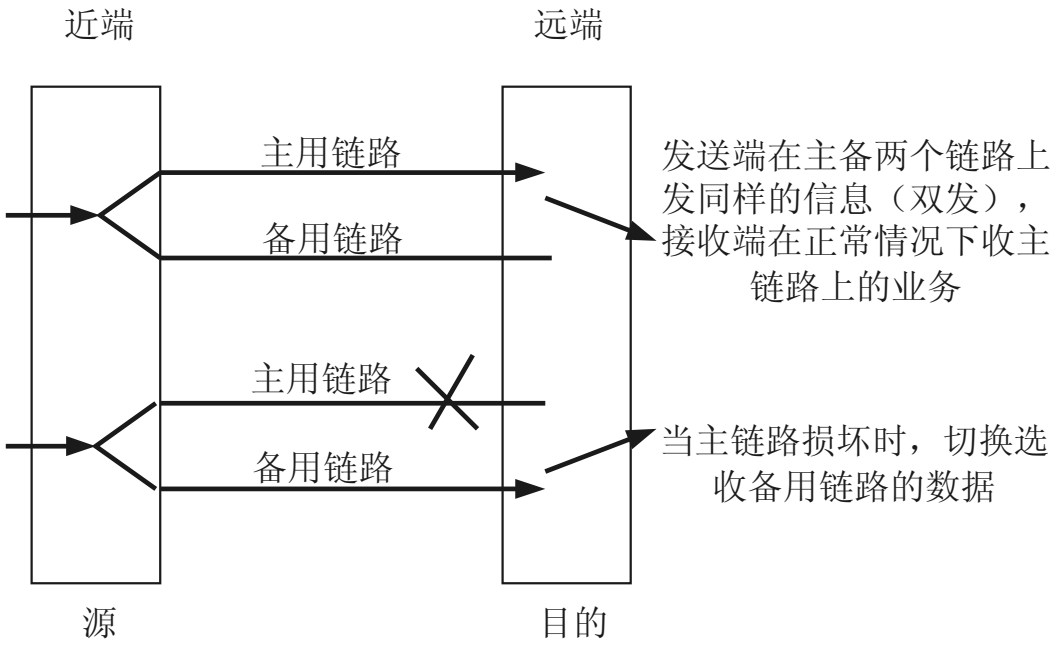
7.4.6 LMSP 保护

1+1 保护

1+1 保护是指每一条工作链路都有一条专有的保护链路为其提供备份。发送端在工作链路和保护链路上同时传输数据(此过程称为桥接：Bridge)，在正常情况下，接收端从工作链路上接收数据，当工作链路出现故障被接收端检测出来时，接收端将切换到保护接口上接收数据。一般情况下切换过程只在接收端进行动作，配合单端保护进行实现，不需要通过 K1K2 字节进行 APS 协商。

它具有切换时间短，可靠性高等优点，但是缺点的是信道利用率低(50%)。具体过程如图 7-11 所示：

图 7-11 1+1 保护

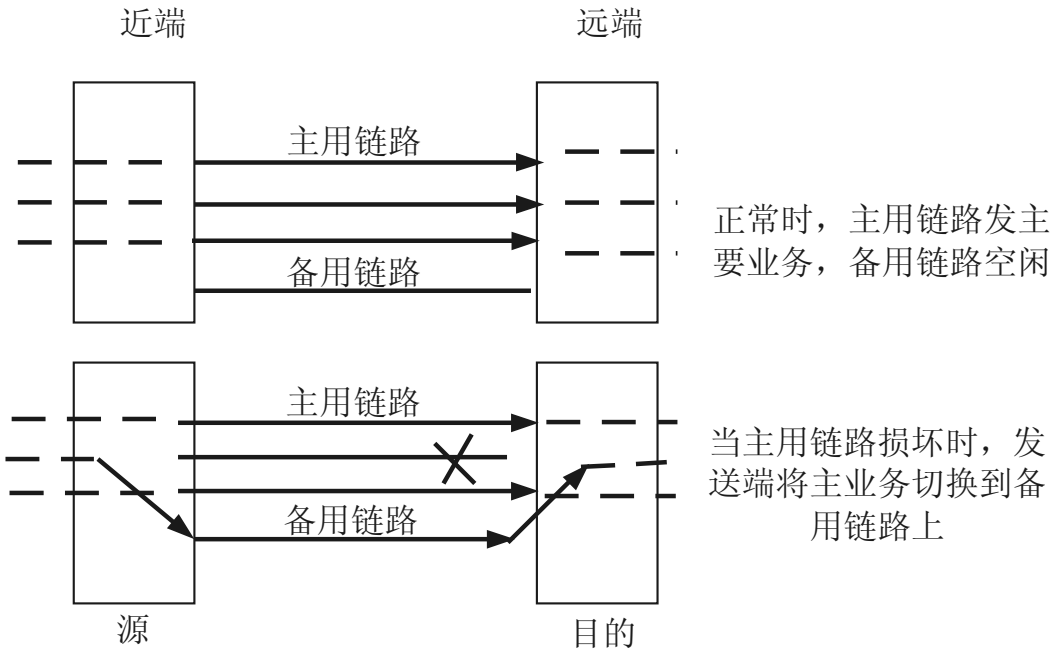


版权所有 © 华为技术有限公司

1:1 和 1:N 保护

1:N 保护是指一条保护链路同时为 N 条工作链路提供保护(1<=N<=14)。 在正常情况下，发送端只在相应的工作链路上传输数据，保护链路上此时可以传输一些低优先级的数据(当然，也可以不进行数据的传输)。当工作链路出现故障时，发送端将要传输的数据桥接(Bridge)到保护链路上，接收端此时从保护链路上接收数据。如果保护链路上原本有低优先级数据在进行传输，此时，低优先级的数据要让位于高优先级的被保护数据，也就不能进行传输了。实现过程如图 2 所示。 **图 7-12** 所示。

图 7-12 1:1 和 1:N 保护



当同时有几条工作链路出现故障时，则根据工作链路的优先级，只有最高优先级链路上的数据可以倒换到保护链路上。其它出现故障的保护链路上的数据只能丢失。

当 N=1 时，就为我们所熟悉的 1:1 模式。

1:N 保护在保护过程中需要发送端和接收端同时进行切换，因此，这种保护需要通过 K1K2 字节进行协商。1:N 保护的优点是信道利用率高，但是可靠性不如 1+1 保护。

按照倒回模式分，可以分为倒回模式和非倒回模式。倒回模式是指工作链路恢复正常以后，过一段时间(这一段时间一般为几分钟到十几分钟)，待工作链路稳定后，在保护链路上的数据是否可以倒换回工作链路上。如果可以倒回，则称为这种保护为倒回模式；否则，则为非倒回模式。1+1 和 1:1 保护即可以配置为倒回模式，也可以被配置为非倒回模式。

按照发生链路故障时，两端是否同时切换，可以分为单端倒换和双端倒换。

- 单端倒换是指发生链路故障时，接收端检测故障发生切换，发送端未检测到故障不进行切换，只进行接收端的倒换桥接，切换的结果是 APS 连接的两端可能选择不同的链路接收流量。

版权所有 © 华为技术有限公司

- 双端倒换是指发生链路故障时，接收端检测故障发生切换，发送端未检测到故障也需要通过 SDH 的 K 字节协商进行切换，切换的结果是 APS 连接的两端需要选择同一条链路进行发送接收。

单端切换一般配合 1 ＋ 1 进行保护，双端切换一般配合 1:1 进行保护。

按照配置 APS 的设备数目不同，可分为单机 APS 和双机 APS（即 E-APS）

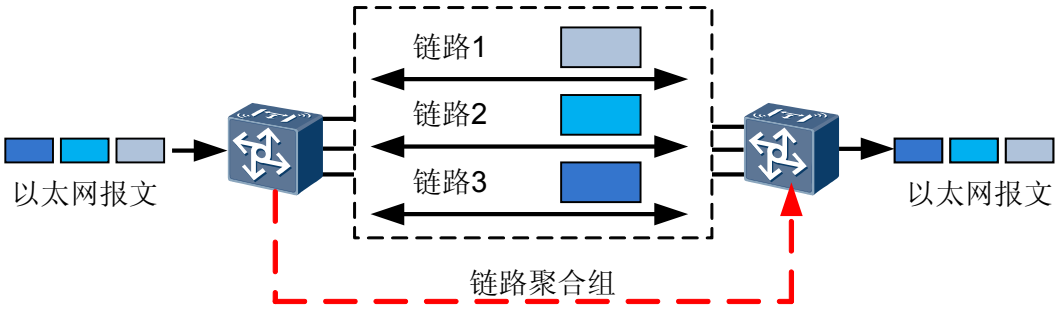
7.4.7 LAG

LAG（Link Aggregation Group）是指将一组物理以太链路捆绑在一起的一条逻辑链路（链路聚合组），它能够提供更高的带宽和链路可靠性。PTN 设备支持以太链路的 LAG 保护，支持的聚合方式有手工聚合与静态聚合。

定义

链路聚合（Link Aggregation）是指将一组物理以太网接口捆绑在一起作为一个逻辑接口（链路聚合组）来增加带宽并提供链路保护的一种方法。如图 7-13 所示，链路聚合的作用域在相邻设备之间，和整个网络结构不相关。在以太网中，链路实际是和端口一一对应的，因此链路聚合也叫做端口聚合。

图 7-13 链路聚合组



设备支持的聚合方式有手工聚合和静态聚合。每一种聚合方式的业务分担方式有负载分担和非负载分担两种方式。

手工聚合：手工聚合方式需要用户创建 LAG，手工添加聚合组的成员链路。手工聚合方式的 LAG 不需要使用 LACP（Link Aggregation Control Protocol）协议。这种聚合方式能够与不支持 LACP 协议的设备互连时仍然可以用链路聚合。某成员链路单向故障（例如以太网光口某一方向断纤）时，断纤的发端不能检测到这一故障，业务会受影响。

静态聚合：静态聚合方式需要用户手工创建 LAG，手工添加聚合组的成员链路。静态聚合需要使用 LACP 协议，LACP 不会改变用户的配置信息。链路两端的系统通过交互 LACP 协议报文对聚合进行协商，而不是完全依靠单端的配置，因此对聚合的控制更加准确和有效。

负载分担聚合：在负载分担的 LAG 中，聚合组的各成员链路上同时都有业务流量存在，它们共同承担业务的传送。为了保证聚合链路上的报文在接收端不会错序并且业务流量在各聚合链路上分布均匀，在接收端采用 LAG 算法对报文进行乱序重组，在发送端采用分担算法根据报文的某个特征值（例如源 MAC、目的 MAC 等）将报文分发到聚合组的各链路上。当聚合组成员发生改变，或者部分链路失效时，系统会自动进行流量的重新分配。这可以获得链路聚合所带来的好处，例如更高的、线性增长的带宽等。

版权所有 © 华为技术有限公司

非负载分担：聚合组内最多能够同时存在两个成员，一个处于 active 状态，作为活动链路承载业务流量，另外一条处于 standby 状态，当聚合组中的活动链路失效时，系统将处于 STANDBY 状态的链路激活，用于承载业务流量。

目的和收益

LAG 工作在 MAC 子层和 LLC 子层之间，属于数据链路层。

LAG 可以实现以下功能：

- 提高链路可靠性：链路聚合组中，成员互相动态备份。当某一链路中断时，其它成员能够迅速接替其工作。链路聚合启用备份的过程只与聚合组内的链路相关，与聚合组外的链路无关。
- 增加链路容量：链路聚合组可以为用户提供一种经济的提高链路传输率的方法。通过捆绑多条物理链路，用户不必升级现有设备就能获得更大带宽的数据链路，其容量等于各物理链路容量之和。聚合模块按照其负载分担算法将业务流量分配给不同的成员，实现链路级的负载分担功能。
- 使用 LAG 无需更改高层协议或应用程序：聚合组工作在数据链路层，与高层协议和应用程序无关。

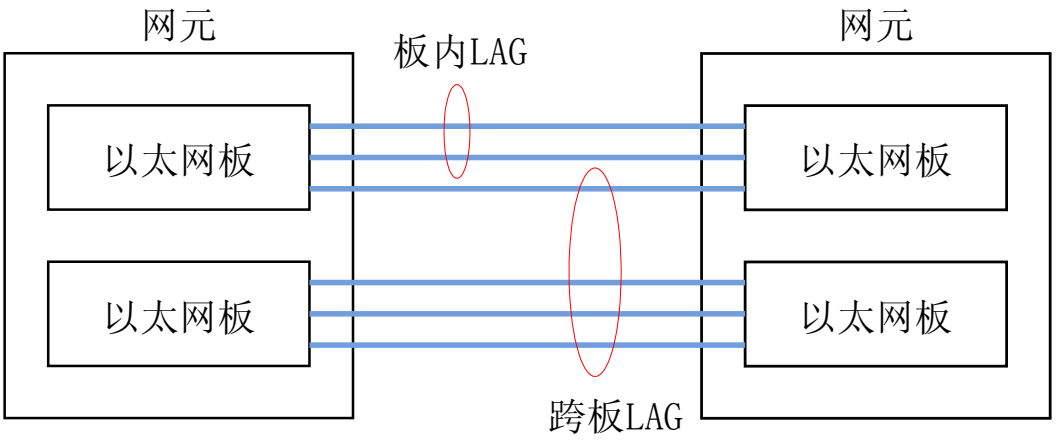
组网应用

设备支持的 LAG。如图 7-14 所示，创建 LAG，支持板内 LAG 和跨板 LAG。线性增加相邻设备间的以太网业务带宽，提高链路的可靠性。

LAG 可以实现以下功能：

- 提高链路可靠性：链路聚合组中，成员互相动态备份。当某一链路中断时，其它成员能够迅速接替其工作。链路聚合启用备份的过程只与聚合组内的链路相关，与聚合组外的链路无关。
- 增加链路容量：链路聚合组可以为用户提供一种经济的提高链路传输率的方法。通过捆绑多条物理链路，用户不必升级现有设备就能获得更大带宽的数据链路，其容量等于各物理链路容量之和。聚合模块按照其负载分担算法将业务流量分配给不同的成员，实现链路级的负载分担功能。
- 使用 LAG 无需更改高层协议或应用程序：聚合组工作在数据链路层，与高层协议和应用程序无关。

图 7-14 LAG 的应用



版权所有 © 华为技术有限公司

7.4.8 以太网生成树保护

多生成树协议 MSTP（Multiple Spanning Tree Protocol）可用于消除网络环路。MSTP 通过一定的算法阻断某些冗余路径，将环路网络修剪成无环路的树型网络，从而避免报文在环路网络中增生和无限循环产生广播风暴。MSTP 与 STP、RSTP 的区别在于 MSTP 能够按照 VLAN 报文进行转发，实现 VLAN 数据的负载均衡。

设备支持的 MSTP，符合标准 IEEE 802.1s，兼容 STP 和 RSTP。

MSTP 使用域(region)和实例(instance)的概念。MSTP 把一个交换网络按照不同的需求划分成不同的域。每个域内形成多棵彼此独立的生成树。每棵生成树称为多生成树实例 MSTI（Multiple Spanning Tree Instance），每个域叫做一个 MST 域。MSTP 通过设置 VLAN 映射表（即 VLAN 和 MSTI 的对应关系表），将 VLAN 和 MSTI 进行映射。每个实例对应一个或一组 VLAN。

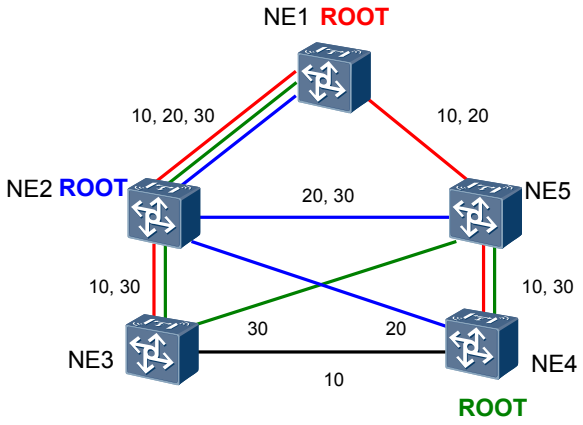
说明

- 实例：运行 MSTP 的设备可以同时具有多个生成树，为了区分这些生成树，每一个生成树叫做一个多生成树实例。
- 域：一组划分了相同 VLAN 和实例对应关系的相互连接的交换设备的集合。

设备之间传输带有域和实例信息的桥接协议数据单元 BPDU（Bridge Protocol Data Unit），设备通过 BPDU 信息判断自己是否属于某个域，域内可以运行多个实例生成树，域间只运行一个生成树。

图 7-15 是一个具有多个 VLAN 的交换网络。

图 7-15 多个 VLAN 的交换网络

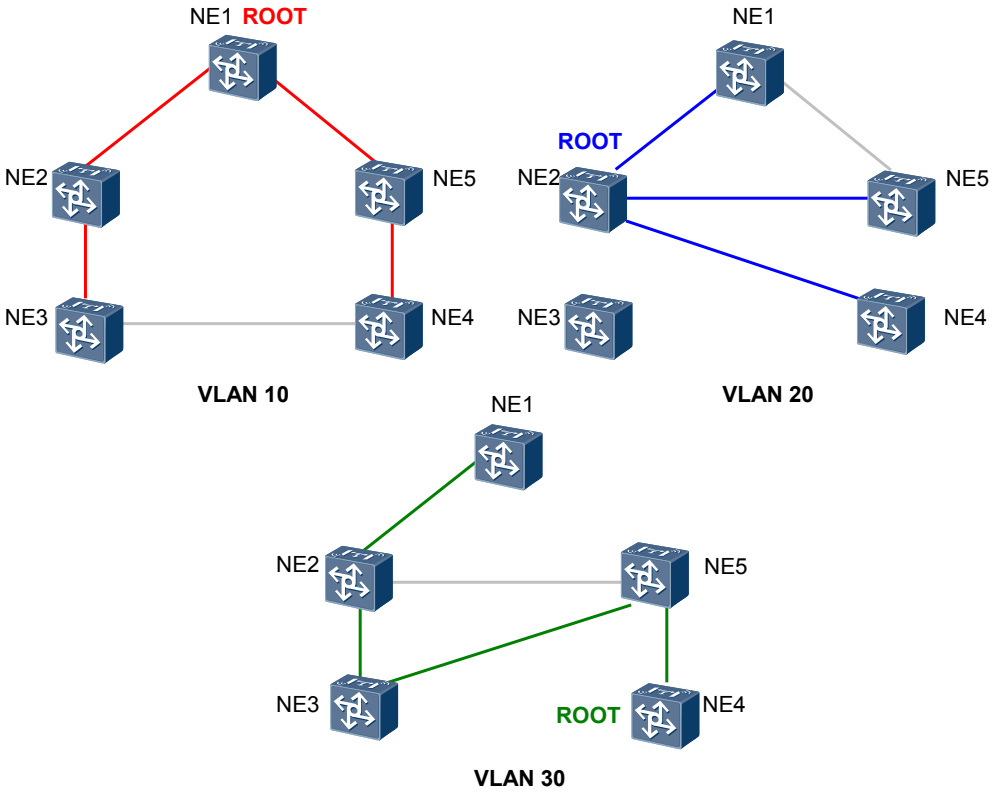


由于 RSTP 的 VLAN 无关性，有可能右下角的设备上的所有端口都处于 Discarding 状态。直接连接到该设备的终端都会通信中断。

运行 MSTP 之后，每个 VLAN 会有一个独立的 MST，如图 7-16 所示：

版权所有 © 华为技术有限公司

图 7-16 运行 MSTP 之后的网络拓扑



由于每个实例对应一个或一组 VLAN，因此 MSTP 可以按照 VLAN 报文进行数据转发，实现 VLAN 数据的负载均衡。从而实现了 RSTP 和 VLAN 的完美结合。

版权所有 © 华为技术有限公司

8 同步

关于本章

8.1 物理层同步
介绍 PTN 6900 设备物理层同步的功能和应用场景。

8.2 IEEE 1588 V2
PTN 6900 设备支持 IEEE 1588 V2 同步，实现时钟和时间的同步。

8.3 1588 ACR 介绍
1588 ACR(Adaptive Clock Recover)，是指支持 IEEE 1588 V2 的 Master 设备将本地系统时钟信息封装到 1588 V2（又称 PTP）报文中发送，经第三方网络透传到对端 Slave 设备，Slave 设备从 1588 V2 报文中获取时戳并恢复时钟，实现 PSN 网络两端设备的频率同步。在这种方案里，中间的第三方网络不需要支持 IEEE 1588 V2 协议。

版权所有 © 华为技术有限公司

8.1 物理层同步

介绍 PTN 6900 设备物理层同步的功能和应用场景。

功能

物理层同步是指设备直接从物理光信号中恢复出时钟频率，从而使得上下游的设备频率同步，保证业务的正常传送。物理层同步是保证网络正常工作的基础。

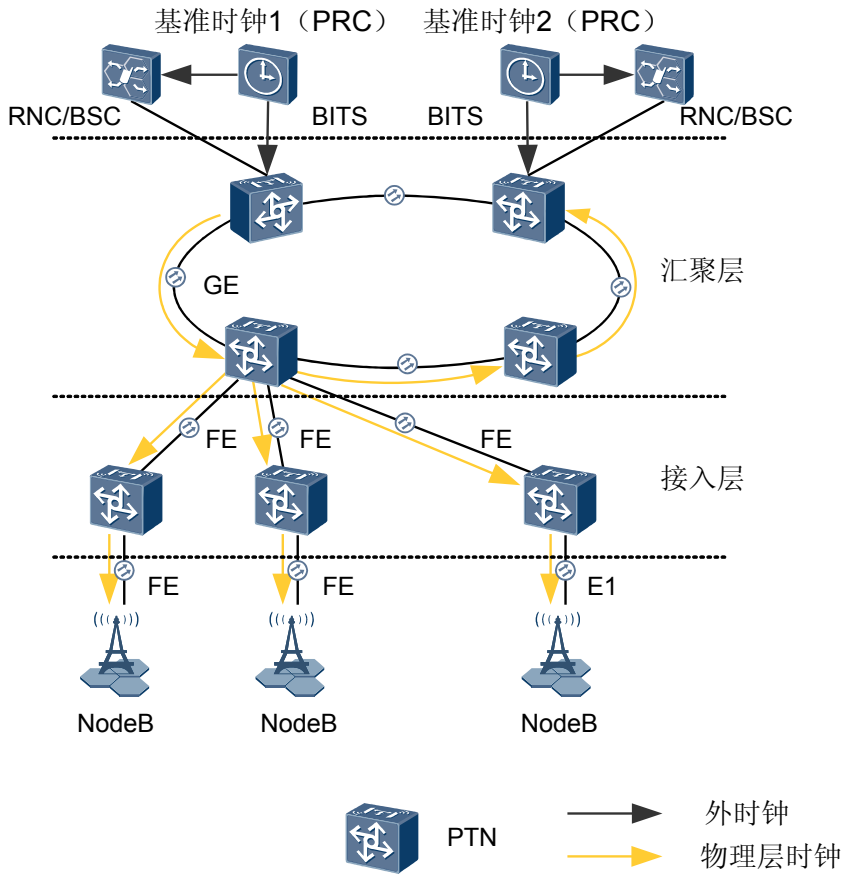
移动承载产品时钟同步的目的如下：

PTN 6900 设备支持从同步以太信号、SDH 光信号以及内部晶振提取物理层时钟。

应用场景

如图 8-1 所示，BITS 将基准时钟源的时钟信息提供给 PTN 6900 设备和 RNC/BSC。PTN 6900 设备通过物理层同步将时钟信息传递到下游基站。中间的物理路径可以是支持物理层时钟的以太链路、SDH 链路。

图 8-1 物理层时钟同步组网图



华为专有和保密信息
版权所有 © 华为技术有限公司

主从同步方式

PTN 6900 设备支持的物理层同步方式为主从同步方式。主从同步方式使用一系列分级的时钟，每一级时钟都同步于其上一级时钟。在网络中最高一级的时钟称为基准主时钟或基准时钟（PRC）。

主从同步方式的主要优点是网络稳定性较好，组网灵活，适于树形结构和星形结构，控制简单，网络的抗滑动性较好。主要缺点是对基准主时钟和传输链路的故障较敏感，一旦基准主时钟发生故障会造成全网的问题。为此，基准主时钟应采用多重备份以提高可靠性。

如**图 8-1** 所示，时钟子网中有两个基准时钟，其中基准时钟 1 作为主用基准时钟，当时基准时钟 1 故障时，全网时钟切换，跟踪基准时钟 2。

主从同步方式需要通过人工设置时钟源优先级，以此保证时钟的逐级跟踪和倒换。同时可以通过 **SSM 协议**避免时钟互跟，通过**扩展 SSM 协议**避免时钟成环。

从时钟的工作模式

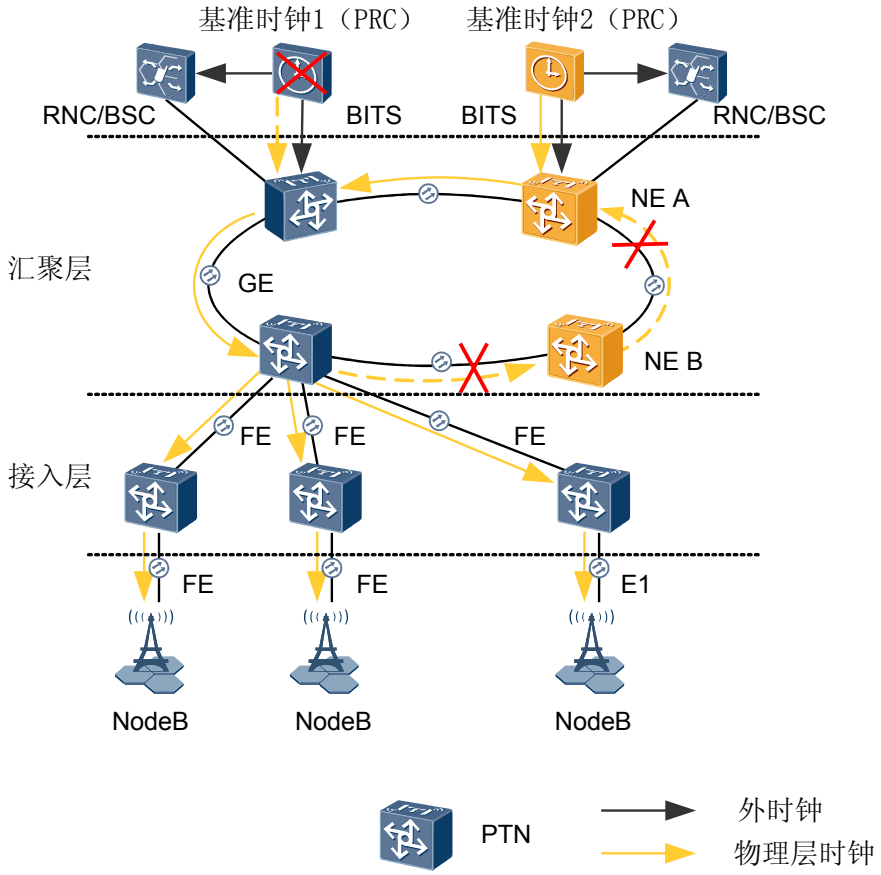
通信网络一般采用主从同步方式，即拥有高精度、高稳定度的主时钟由支持物理层同步的设备传送给下游各设备，下游设备同步于来自上一级的时钟信号，从而达到全网同步。从时钟有三种模式。

- 跟踪模式：正常工作模式，指本地时钟同步于基准时钟。
- 保持模式：当所有外部定时基准都丢失后，从时钟进入保持模式。从时钟利用定时基准信号丢失之前所存储的频率信息作为其定时基准。
- 自由振荡模式：当从时钟丢失所有的外部定时基准，同时也失去了定时基准记忆或根本没有保持模式时，从时钟内部振荡器工作于自由振荡方式。

如**图 8-2** 所示，汇聚层中的两处线路和基准时钟 1 同时故障。此时 NE B 没有时钟源可以跟踪，变为保持模式。经过一段时间，NE B 存储的时钟信息劣化，转而跟踪 NE B 设备内部的时钟，变为自由震荡模式。而 NE A 变为跟踪基准时钟 2，工作模式仍然为跟踪模式。虚线表示故障之前的时钟跟踪路径，实线为切换之后的时钟跟踪路径。

版权所有 © 华为技术有限公司

图 8-2 时钟的工作模式



SSM 协议和扩展 SSM 协议

标准 SSM 协议是网络进行同步管理的一种机制。它利用同步状态信息第 5 ～ 8 比特在节点之间交换时钟源的质量信息，以确保设备自动选择质量最高且优先级最高的时钟源。同时 SSM 协议可以防止时钟互锁，可改进同步网性能，方便实现不同网络结构的同步。标准 SSM 协议可用于不同厂商的设备对接。

扩展 SSM 协议是华为公司在标准 SSM 的基础上加入了时钟 ID 的概念，对原有的 SSM 协议进行了扩展。它利用同步状态信息的第 1 ～ 4 比特为时钟源定义唯一的 ID，并随 SSM 一起传送。节点接收到 SSM 之后，通过检验位于第 1 ～ 4 比特的时钟 ID 来判断该时钟是否是由本站发出的。若是，则认为该源不可用，避免了时钟环路的产生。扩展 SSM 协议主要用于华为公司的传输设备间的互连。

性能指标

设备的定时和同步性能符合 ITU-T G.813 标准要求。

8.2 IEEE 1588 V2

PTN 6900 设备支持 IEEE 1588 V2 同步，实现时钟和时间的同步。

版权所有 © 华为技术有限公司

功能

随着以太网数据传输速度的提升到千兆，出现了以太网同步能力不足的问题。为解决同步问题，提出了 NTP（Network Time Protocol），通过该协议，时钟的同步精度已经达到 200 微秒，但仍然不能满足测量仪器和工业控制所需要的精度。为了同步精度的进一步提升，2002 年 IEEE 标准委员会推出了 IEEE 1588 时钟协议，随着该协议的不断完善，目前通过该协议，时钟的同步精度已经达到纳秒级。

时间同步分为两种：频率同步和时间（相位）同步。时间（相位）同步主要应用在对于全网绝对时间有精度要求的网络，例如电力网络、3G 网络。虽然通过在网络中各节点放置 GPS 也可以满足要求，但高成本导致这种方案不能广泛应用。

传统的时钟协议只能实现频率的同步。IEEE 1588 V2 时钟协议是能够实现频率和相位同步的协议标准。

IEEE 1588 V2 协议用于精确同步分布式网络通讯中各个节点的时间同步。通过硬件和软件将网络设备（客户机）的系统时钟与网络的主时钟同步，精度可达纳秒级，与未启用 1588 V2 协议的以太网延迟时 1000us 相比，整个网络的定时同步指标有显著改善。

通过 IEEE 1588 V2 协议提供时钟和时间的同步是电信级 IP 网络为转型所做的技术变革和创新之一。

通过 IEEE 1588 V2 协议，满足了 3G 网络中 Node B 和 RNC 对于时钟和时间的要求。

说明

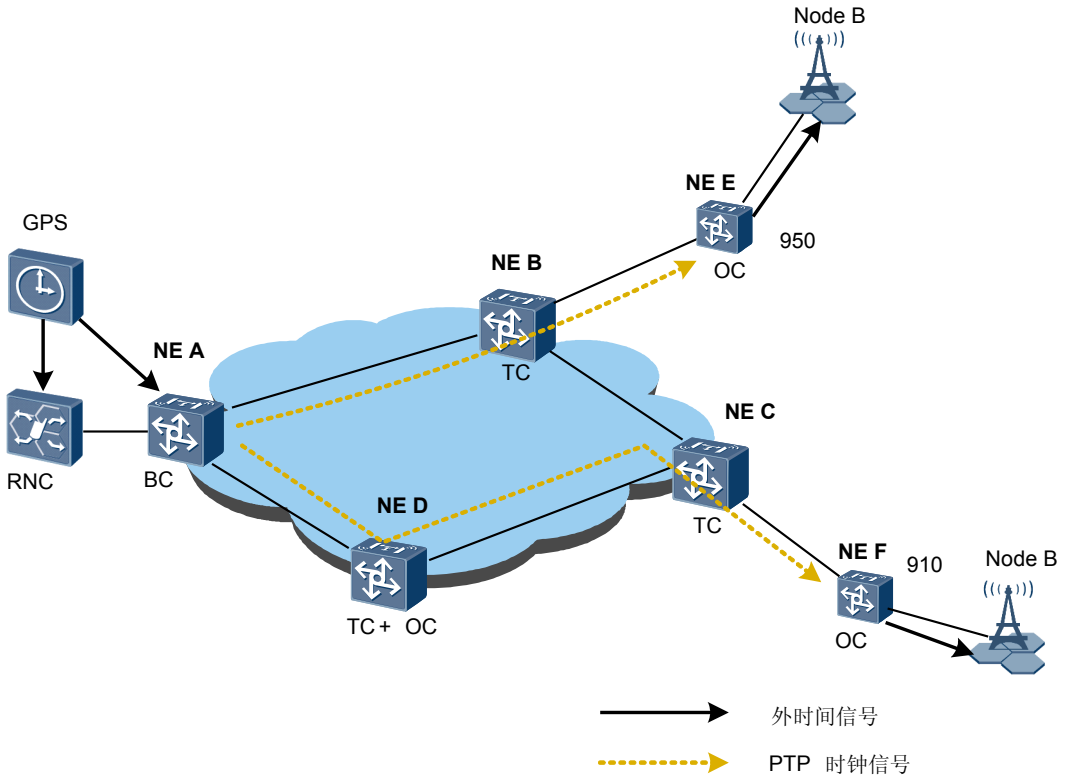
- 时钟同步就是频率同步。
- 时间同步就是相位同步，要求时间与频率同时同步。

应用

设备支持的 PTP 时钟的应用场景如图 8-3 所示。

版权所有 © 华为技术有限公司

图 8-3 PTP 时钟同步典型组网



在图 8-3 中，BITS 向 NE A 和 RNC 传递时钟信号。NE A 作为 BC 向两个端口发送 PTP 报文，下游设备作为 BC 对 PTP 报文进行透传。与 Node B 对接的 NE E 和 NE F 作为 OC 设备恢复 PTP 时钟并通过外时间接口将时钟传递给 Node B。

性能指标

- 背靠背时间同步精度优于±30ns（测试时间 120000s）。
- 途经 30 个网元后时间同步精度优于±1us（测试时间 120000s）。

8.3 1588 ACR 介绍

1588 ACR(Adaptive Clock Recover)，是指支持 IEEE 1588 V2 的 Master 设备将本地系统时钟信息封装到 1588 V2（又称 PTP）报文中发送，经第三方网络透传到对端 Slave 设备，Slave 设备从 1588 V2 报文中获取时戳并恢复时钟，实现 PSN 网络两端设备的频率同步。在这种方案里，中间的第三方网络不需要支持 IEEE 1588 V2 协议。

简介

当运营商网络中间穿越第三方网络，而第三方网络不支持物理层时钟但支持多播业务时，可以将 1588 V2 时钟报文作为业务透传，通过静态 1588 ACR 方案实现两端设备频率同步。

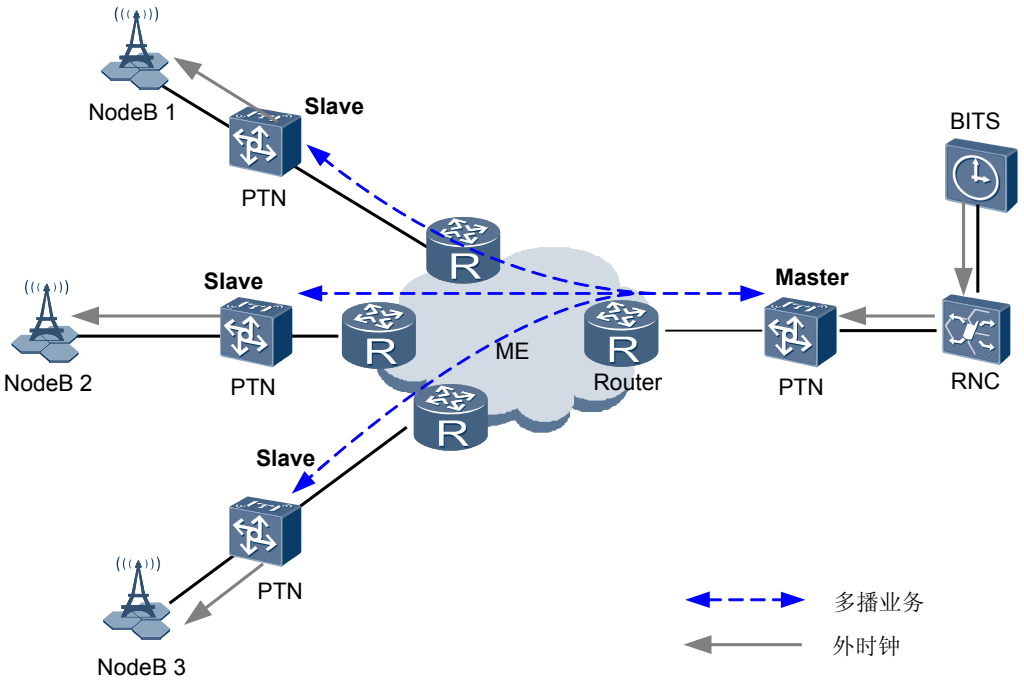
当 PTN 6900 设备穿越第三方网络时，如果全网设备均支持 IEEE 1588 V2 协议，则可以通过 1588 V2（PTP）时钟将 RNC 侧的时钟传递到 NodeB 以实现全网时钟同步。但由于要求全网所有设备都支持 IEEE 1588 V2 协议，对于第三方网络而言成本很高。如果

版权所有 © 华为技术有限公司

第三方网络可以将 1588 V2 时钟报文透传，就可以采用静态 1588 ACR 方案实现两端设备频率同步。

PTN 6900 设备静态 1588 ACR 方案支持的 1588 V2 时钟报文是多播的以太报文和 IP 报文，如图 8-4 所示，PTN 6900 设备将携带系统信息的时戳增加到 1588 V2 时钟报文中，通过第三方网络将时钟信息多播到 NodeB 侧的 PTN 6900 设备。PTN 6900 设备接收到 1588 V2 时钟报文后获取时戳，通过计算恢复出时钟并用作系统时钟，同时将时钟传递给 NodeB，从而达到网络两端设备频率同步。

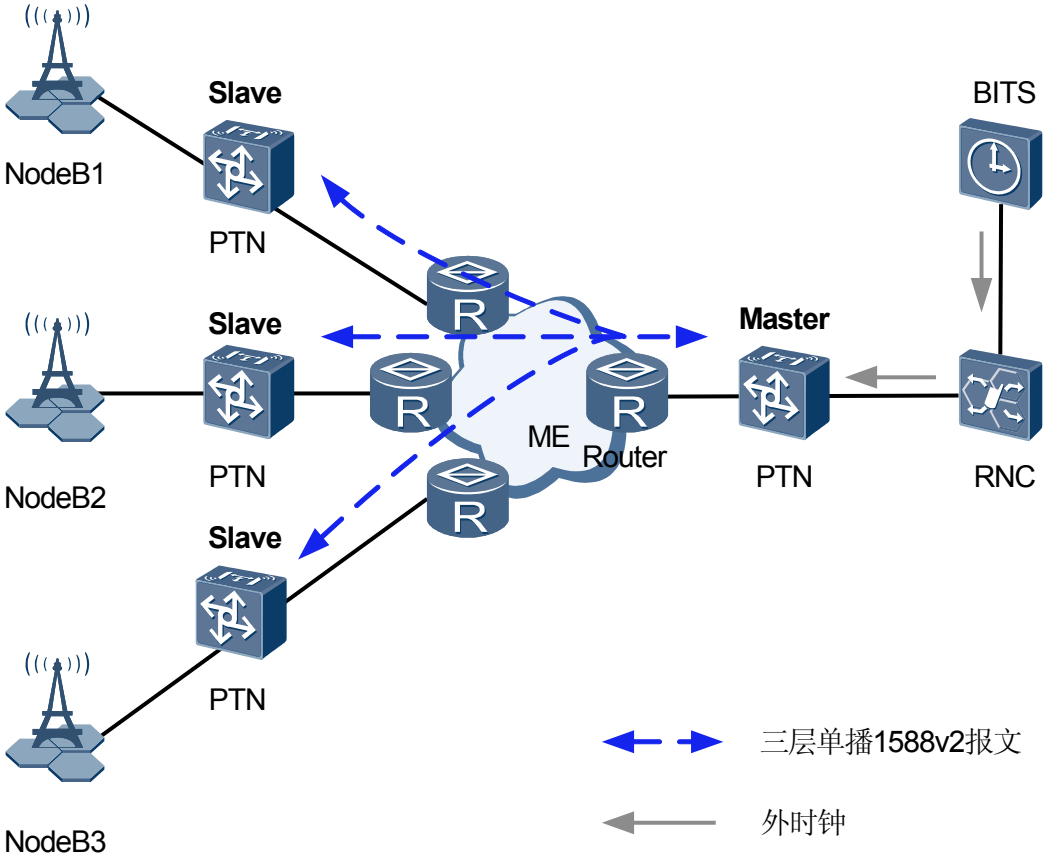
图 8-4 1588 ACR 时钟应用场景图



PTN 6900 设备同时支持带有三层单播协商机制的 1588 ACR 方案。如图 8-5 所示，master、slave 端 PTN 6900 设备均支持带有三层单播协商机制的 1588 ACR 功能，slave 端 PTN 6900 设备作为客户端主动向 master 端 PTN 6900 设备发起三层单播连接请求，master 端 PTN 6900 设备收到连接请求并授权通过 后，开始向 slave 端 PTN 6900 设备发送三层单播 1588 V2 时钟报文，如果第三方网络可以将三层单播 1588 V2 时钟报文透传，就可以采用带有三层单播协商机制的 1588 ACR 方案实现两端设备频率同步。

版权所有 © 华为技术有限公司

图 8-5 1588 ACR 时钟应用场景图



性能指标

PTN 6900 设备 1588 ACR 满足以下性能指标：

- 参照 ITU-T G.8261 组网测试建议，时钟恢复指标满足 ITU-T G.823 Traffic。
- ACR 恢复时钟的保持性能满足优于±50ppb 的要求。
- 中间网络 PDV 小于 16ms，丢包率小于 0.05%时，恢复时钟性能指标满足 ITU-T G.823 Traffic。

版权所有 © 华为技术有限公司

9 操作、维护与管理

关于本章

PTN 6900 分组传送平台提供和支持强大的操作、维护与管理功能。

9.1 系统配置方式

9.2 U2000 网管系统
PTN 6900 分组传送平台采用 U2000 统一管理。

9.3 监控及维护
PTN 6900 分组传送平台支持多种监控和维护功能。

9.4 诊断及调测
PTN 6900 分组传送平台提供对系统软硬件故障的诊断与调测功能。

9.5 升级
PTN 6900 分组传送平台支持多种升级方式。

版权所有 © 华为技术有限公司

9.1 系统配置方式

PTN 6900 分组传送平台提供两种配置方式：命令行配置和网管配置。

命令行配置方式支持：

- 用户可以通过 Console 口本地配置
- AUX（Auxiliary）口 Modem 远程配置
- Telnet 远程登录

Console 接口作为 CLI 输入接口可以向控制平面发送命令行。

Console 接口作为调试接口，可以从控制平面和数据平面接收各种 debug 信息，也可以下发调试命令和控制命令。

网管配置支持基于 SNMP 协议的网管系统对 PTN 6900 分组传送平台进行配置。

9.2 U2000 网管系统

PTN 6900 分组传送平台采用 U2000 统一管理。

网管系统符合 ITU-T 建议，采用标准的管理信息模型和面向对象管理技术。通过通信模块与网元主机软件交换 信息，实现对网络上设备的监控和管理。

网管软件运行于工作站或 PC 机上，主要功能是实现对设备及网络的管理。网管软件具备对传输设备的操作维护功能和对传输网络进行管理的能力。网管软件的管理功能包括以下几点：

告警性能管理

可实现告警的实时收集、提示、过滤、浏览、确认、核对、清除、统 计，以及告警插入、告警相关性分析、故障诊断等，如：

- 实现自动上报告警和执行告警一致性检查
- 核对告警和删除告警
- 清除和过滤网元当前或历史告警，过滤异常事件列表
- 告警数据的保存

配置管理

可实现网元的接口、时钟、业务、隧道、保护、时间等的配置和管理，如：

- 创建或删除网络实体
- 创建/修改光纤
- 设置或修改网元属性及下发配置
- 配置接口属性
- 配置隧道和保护
- 配置 OAM
- 配置业务

版权所有 © 华为技术有限公司

- 配置时钟源
- 上载配置数据或检查数据一致性
- 查看网元信息

维护管理

可提供多种方式帮助维护人员定位、消除设备故障，如：

- 设置环回
- 设置网元时间同步方式
- 复位单板或主控软件
- 设置激光器自动关断
- 启动业务性能检测
- 备份网元数据库

安全管理

可通过多种方式对网元进行安全管理，如：

- 网元用户管理
- 网元登录管理
- 网元登录锁定
- 网元设置锁定
- 网元用户组管理
- 网元安全参数
- 网元安全日志

9.3 监控及维护

PTN 6900 分组传送平台支持多种监控和维护功能。

PTN 6900 分组传送平台支持的监控和维护功能如下：

- 支持对业务、PW 和 Tunnel 进行性能统计。
- 支持光纤自动搜索功能。
- 提供告警管理和性能管理的 SNMP 接口，SNMP 版本支持 V1、V2 和 V3。
- 各单板均有运行、告警状态指示灯，协助网络管理员及时定位、处理故障。
- 提供告警级别管理、告警过滤等功能。
- 支持激光器自动关断功能。
- 支持软件版本平滑升级。
- 支持数据库在线备份和加载。
- 支持通过数据库方式和 CF 卡方式恢复系统配置。
- 支持通过网管对设备进行配置初始化。
- 通过网管能动态地监视网上各站的设备运行、告警及性能状况。
- 支持单板及主机软件的包加载和远程加载，并提供防误加载和断点续传功能。

版权所有 © 华为技术有限公司

- 支持业务镜像功能。

9.4 诊断及调测

PTN 6900 分组传送平台提供对系统软硬件故障的诊断与调测功能。

PTN 6900 分组传送平台通提供 NQA（Network Quality Analysis）功能。NQA 可以测量网络上运行的各种协议的性能，使运营商能够实时采集到各种网络运行指标，例如：HTTP 的总时延、TCP 连接时延、DNS 解析时延、文件传输速率、FTP 连接时延、DNS 解析错误率等。通过对这些指标进行控制，运营商可以为用户提供不同等级的网络服务，收取不同的费用。同时，NQA 也是网络故障诊断和定位的有效工具。

NQA 支持以下功能：

- 支持 PWE3 TraceRoute
- 支持 Multicast Ping
- 支持 Multicast Tracert
- 支持通过 DISMAN-TRACEROUTE-MIB 进行 traceroute 操作
- 支持通过 DISMAN-PING-MIB 进行 ping、udp、tcp、snmp 业务测试
- 支持 ce-ping(在 VPLS PE 上 ping 主机)
- 支持 VPLS MAC ping 和 VPLS MAC trace
- 支持 VPLS MAC purge 和 VPLS MAC populate
- 支持 LSP ping、LSP traceroute 和 MPLS jitter
- 通过 NQA-MIB 支持全部 NQA 功能通过 NMS 管理
- 一次测试支持连续发送 3000 报文模拟语音
- 最短 10ms 的发包频率

9.5 升级

PTN 6900 分组传送平台支持多种升级方式。

- 在线升级

  PTN 6900 分组传送平台支持软件在线升级的功能。同时，还提供软件在线补丁的功能，可以只针对需要修改的特性进行升级。

- 整机升级

  PTN 6900 分组传送平台对升级过程进行了优化。整个升级过程由一条命令自动完成升级全过程，为客户节省了宝贵的时间。升级过程给出进度提示，并在升级结束后可以查看升级结果。

- 回退功能

  在升级系统过程中，新的系统软件无法启动时，系统可以使用上一次成功启动的系统软件进行启动。

  PTN 6900 分组传送平台提供的回退功能可以避免系统升级失败对业务的影响。

版权所有 © 华为技术有限公司

10 安全管理

关于本章

网管通过多种方式实现对 PTN 6900 分组传送平台的安全管理。网元安全管理包括认证管理，授权管理，网络安全管理，系统安全管理，网元安全日志管理。合理的规划才能保证网元安全管理的有效性。

10.1 网络安全管理
网管和网元之间，以及网络中的数据的安全传送，是网管有效管理网元的前提。

10.2 Syslog 日志管理
系统日志服务 (Syslog service) 用户网元的安全管理。各种不同类别的信息会按照符合系统日志（Syslog）协议的格式传送到日志服务器，便于维护人员统一监控。

版权所有 © 华为技术有限公司

10.1 网络安全管理

网管和网元之间，以及网络中的数据的安全传送，是网管有效管理网元的前提。

- 设置 ACL（Access Control List）规则，对接收的 IP 报文进行过滤，控制网络数据流量，同时可防范恶意攻击。根据系统安全程度可分为：基本 ACL 规则和高级 ACL 规则。
  - 对于安全级别要求较低的网元，可以设置基本 ACL 规则，只对 IP 报文的源地址进行校验。
  - 对于安全级别要求很高的网元，可以设置高级 ACL 规则，网元会对接收的 IP 报文的进行源宿地址、源宿端口以及协议类型进行详细的校验。
  - 在高级 ACL 规则和基本 ACL 规则同时存在的情况下，系统优先按照高级 ACL 规则进行校验。
  - 查询 ACL 规则。
  - 修改 ACL 规则。
  - 删除 ACL 规则。
- 网元可通过以下方式接入到网管：
  - 以太网接入（网管网口 ETH 和扩展网口 EXT）。缺省情况下，网元是允许网管通过以太网接入。
  - 串口接入。
- 在网管和网元通信时，对于敏感信息，比如用户名，密码等进行加密。
- 支持 AAA。

10.2 Syslog 日志管理

系统日志服务 (Syslog service) 用户网元的安全管理。各种不同类别的信息会按照符合系统日志（Syslog）协议的格式传送到日志服务器，便于维护人员统一监控。

PTN 6900 分组传送平台通过信息中心提供完备的设备运行状态监控功能。 Syslog 是信息中心（info-center）的一个子功能。Syslog 使用 UDP 进行传输，使用端口号 514 将日志信息输出到日志主机中。

信息中心可以接收和处理 3 类信息：

- log 类：即日志信息
- debug 类：即调试信息
- trap 类：即告警信息

根据信息的严重等级或紧急程度，信息分为 8 个等级，信息越严重，其严重等级值越小。详细信息见下表。

显示值	严重等级	描述
0	Emergency	设备致命的异常，系统已经无法恢复正常，必须重启设备。如程序异常导致设备重启，内存的使用被检测出错误等。

版权所有 © 华为技术有限公司

显示值	严重等级	描述
1	Alert	设备重大的异常，需要立即采取措施。如设备内存占用率达到极限等。
2	Critical	设备重大的异常，需要采取措施进行处理或原因分析。如设备内存占用率超过告警线，温度超过告警线，BFD 探测出设备不可达，检测出错误的消息（消息是由本设备内部生成）等。
3	Error	错误的操作或设备的异常流程，不会影响后续业务，但是需要关注和原因分析。如用户的错误指令，用户密码错误，检测出错误协议报文（报文是由其他设备获得）。
4	Warning	设备的异常运转的异常点，可能引起业务故障的流程，需要引起注意。如用户关闭路由进程，BFD 探测的一次报文丢失，检测出错误协议报文等。
5	Notice	用于设备正常运转的关键操作信息。如用户执行 shutdown 命令，邻居发现，协议状态机的正常跳转等。
6	Informational	用于设备正常运转的一般性操作信息。如用户使用 display 命令等。
7	Debugging	设备正常运转的一般性信息，用户无需关注。

信息中心支持 10 个通道，其中，通道 0 ～ 5 有缺省通道名。并且，这 6 个信息通道缺省与 6 个输出方向分别关联。设备上的 CF 卡缺省情况下，日志信息输出到日志文件使用通道 9，即，共支持 7 个缺省输出方向。

在配置多日志主机的情况下，用户可以配置日志信息通过一个通道或多个通道输出到不同的日志主机中。例如配置部分日志信息通过通道 2（loghost）输出到日志主机，部分日志信息从通道 6 输出到日志主机，还可以更改通道 6 的名称，便于对信息通道的管理。

PTN 6900 分组传送平台所有的告警信息都存储到日志文件中，日志文件存储在 CF 卡中。告警信息存储的时间是由告警数量决定的，一般情况下可以存储数月的告警信息。

版权所有 © 华为技术有限公司

11 技术指标

关于本章

介绍了 PTN 6900 的相关技术指标。

11.1 物理参数和容量
PTN 6900-16 的整机技术指标包括机柜技术指标和子架技术指标。

11.2 可靠性指标
PTN 6900 分组传送平台可靠性指标主要包括系统可用度，系统平均年返修率，MTTR 系统平均修复时间，MTBF 系统平均故障间隔时间等。

11.3 EMC 性能指标
PTN 6900 分组传送平台 EMC 指标满足 ETSI EN 300 386 V1.3.3 的要求。

11.4 安全认证
PTN 6900 分组传送平台设备通过了多项安全认证。

11.5 存储环境
PTN 6900 设备对其存储环境有各方面的要求。

版权所有 © 华为技术有限公司

11.1 物理参数和容量

PTN 6900-16 的整机技术指标包括机柜技术指标和子架技术指标。

表 11-1 PTN 6900-16 技术指标

项目	PTN 6900-16
外形尺寸（宽×深×高）	442mm×770mm×1420mm
机柜	可安装在 N68E 和 19 英寸标准机柜中
重量（满配置）	248kg
最大功率	5360W (40G) 5400W (100G) 5460W (200G)
散热值	17390 BTU/hour (40G) 17520 BTU/hour (100G) 17714 BTU/hour (200G)
总槽位数量	22
业务槽位数量	16
转发能力	3200Mpps
交换能力	3.2T（双向）
背板带宽	30T
端口容量（双向）	3200Gbps（双向）
SDRAM	2 GB(可扩展到 4 GB)
Flash	32M
CF Card	每块主控板有 2 块 CF 卡，每块 1GB
直流（DC）输入电压	额定电压：-48V 最大电压范围：-38V ～-72V
交流（AC）输入电压	额定电压：220V 最大电压范围：175 V to 275 V

11.2 可靠性指标

PTN 6900 分组传送平台可靠性指标主要包括系统可用度，系统平均年返修率，MTTR 系统平均修复时间，MTBF 系统平均故障间隔时间等。

PTN 6900 分组传送平台可靠性指标如表 11-2 所示。

版权所有 © 华为技术有限公司

表 11-2 可靠性指标

项目	指标要求
系统可用度	PTN 6900-16：0.9999984，设备年停机时间不大于 0.83 分钟
MTTR 系统平均修复时间	PTN 6900-16：0.5 小时
MTBF 系统平均故障间隔时间	PTN 6900-16：36.29 年

11.3 EMC 性能指标

PTN 6900 分组传送平台 EMC 指标满足 ETSI EN 300 386 V1.3.3 的要求。

PTN 6900 分组传送平台遵循的 EMC 标准有：

- ETSI EN 300 386 1.3.3（2005-04）
- ETSI EN 300 132-2（2003-09）
- CISPR22（2003-04）
- IEC 61000-4-2（2001-04）
- IEC 61000-4-3（2002-09）
- IEC 61000-4-4 (1995+A1:2000.11+A2:2001.07)
- IEC 61000-4-5（2001-04）
- IEC 61000-4-6（2003-05）
- IEC 61000-4-29（2000-08）

11.4 安全认证

PTN 6900 分组传送平台设备通过了多项安全认证。

PTN 6900 分组传送平台通过的安全认证如**表 11-3** 所示。

版权所有 © 华为技术有限公司

表 11-3 PTN 6900 分组传送平台通过的安全认证

认证项目	认证标准
Electromagnetic compatibility (EMC)	CISPR22 Class A CISPR24 EN55022 Class A EN50024 ETSI EN 300 386 Class A ETSI ES 201 468 CFR 47 FCC Part 15 Class A ICES 003 Class A AS/NZS CISPR22 Class A GB9254 Class A VCCI Class A
Safety	IEC 60950-1 IEC/EN41003 EN 60950-1 UL 60950-1 CSA C22.2 No 60950-1 AS/NZS 60950-1 BS EN 60950-1 IS 13252 GB4943
Laser safety	FDA rules 21 CFR 1040.10 and 1040.11 IEC60825-1 IEC60825-2 EN60825-1 EN60825-2 GB7247
Health	ICNIRP Guideline 1999-519-EC EN 50385 OET Bulletin 65 IEEE Std C95.1
Environment protection	RoHS

版权所有 © 华为技术有限公司

11.5 存储环境

PTN 6900 设备对其存储环境有各方面的要求。

气候环境

PTN 6900 对存储时的气候环境如**表 11-4** 所示。

表 11-4 PTN 6900 在存储时对气候环境的要求

项目	要求
工作环境温度	长期：0°C～45°C 短期：-5°C～55°C 备注：温度变化速率限制：30°C/小时
存储温度	-40°C～70°C
工作环境相对湿度	长期：5%RH～85%RH，无凝结 短期：5%RH～95%RH，无凝结
存储相对湿度	0%RH～95%RH，无凝结
长期工作海拔高度	小于 3000 米
存储海拔高度	小于 5000 米

版权所有 © 华为技术有限公司