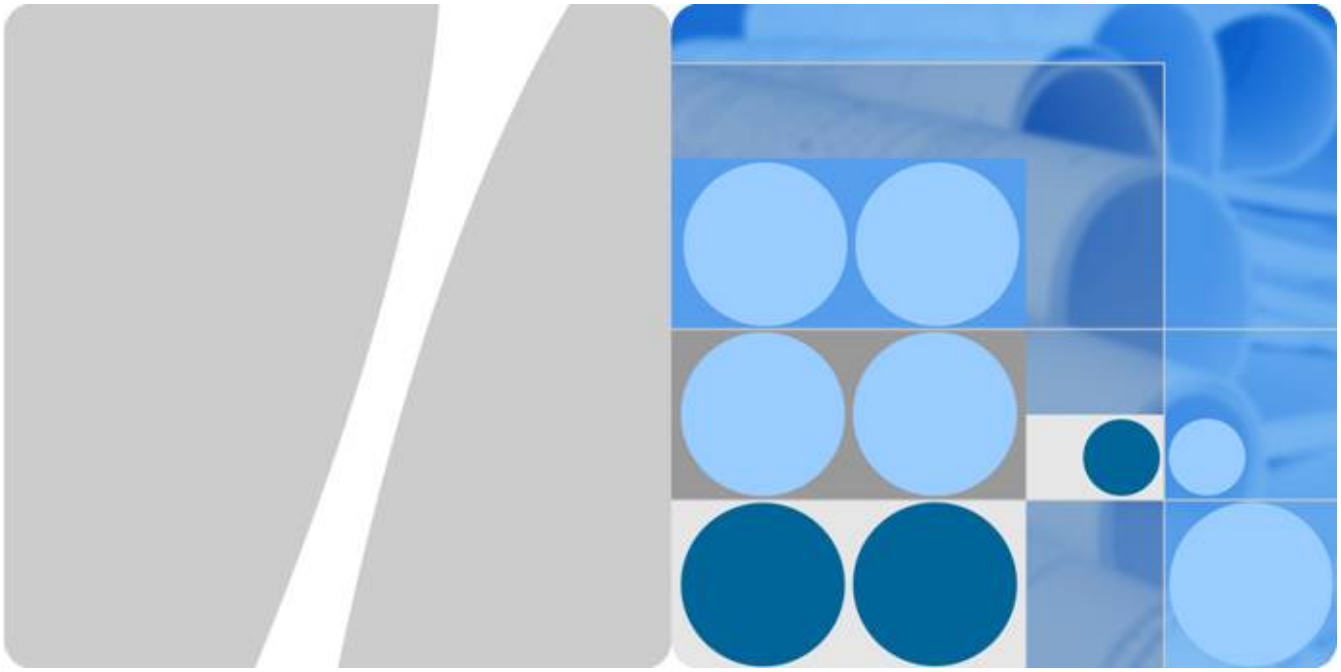


Quidway S9300 T 比特路由交换机
V100R003C00

产品描述

文档版本 02

发布日期 2010-07-15

华为技术有限公司

商标声明


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

注意

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

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

华为技术有限公司

地址： 深圳市龙岗区坂田华为总部办公楼 邮编：518129

网址： http://www.huawei.com

客户服务邮箱： support@huawei.com

客户服务电话： 0755-28560000 4008302118

客户服务传真： 0755-28560111

前 言

读者对象

本文档针对 Quidway S9300 T 比特路由交换机，介绍了产品定位和特点、产品架构、链路特性、业务特性、应用场景、操作和维护、技术指标。

本文档提供 Quidway S9300 T 比特路由交换机 的总体情况，便于读者全面了解产品特征。

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。

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。

符号	说明
说明	以本标志开始的文本是正文的附加信息，是对正文的强调和补充。

修订记录

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

文档版本 02 (2010-07-15)

相对于版本 01(2010-04-30)

增加：

- 增加对 IPSec VPN 的说明：俄罗斯地区发布的版本不提供 IPSec 功能。

修改：

- 更新 IPTV 应用场景 **4.9.1 IPTV 业务的组网**和 **4.9.2 IPTV 业务的保护**

文档版本 01 (2010-04-30)

第一次正式发布。

目 录

插图目录

表格目录

1 产品定位和特点

关于本章

阅读本节可了解 S9300 产品定位、整机接口密度、设备扩展能力、转发能力、支持的业务功能、安全性能、可靠性及可维护性。

1.1 产品定位

面对网络 IP 化和三网（电信网、广播电视网和计算机通信网）合一的趋势，城域以太网上承载的业务越来越丰富，业务传输的质量要求越来越高。为满足多种业务在城域以太网上高质量的传输，华为公司推出 Quidway S9300 T 比特路由交换机 (以下简称 S9300)产品。

S9300 主要应用于城域网中的业务接入、汇聚和传输层，作为城域网的接入和汇聚节点，提供线速的 FE、GE 和 10GE，以及 EPON 接口。也可以应用于行业网、数据中心，提供高密度的端口和丰富的增值业务能力。

S9300 产品为满足不同用户的需求，同时提供 S9303、S9306 和 S9312 三款产品类型，用户可以根据不同的网络需求进行灵活的选择。

- S9303 最大支持 3 块 LPU 线路板
- S9306 最大支持 6 块 LPU 线路板
- S9312 最大支持 12 块 LPU 线路板

S9300 产品基于硬件的转发机制和无阻塞交换技术，采用华为公司自主研发的通用路由平台 VRP（Versatile Routing Platform），具有电信级的可靠性、全线速的转发能力、完善的 QoS（Quality of Service）管理机制、丰富的业务处理能力和良好的扩展性等优点。

同时，S9300 产品具有强大的网络接入、二层交换和 EoMPLS 传输能力，支持丰富的 IP 级服务，能提供宽带上网、三网合一、IP 专用线路、VPN 等多种服务。S9300 还具备丰富的行业网特性，包括防火墙、NAT、网流分析、IPSec VPN、负载均衡等，满足行业网用户多样的业务需求。

说明

俄罗斯地区发布的版本不提供 IPSec 功能。

S9300 也可以与华为公司开发的 S 系列交换机、NE80E、NE40E、ME60 和 MA5200G 等设备组合使用，共同构建一个层次分明的城域以太网络，为客户提供更丰富的业务能力。

1.2 产品特点

S9300 产品提供了高密度的以太网接口能力，本节介绍接口在单板及整机的最高密度、转发能力、主要的业务功能及可靠性等产品特点。

高密度的接口能力

表 1-1 仅给出 S9300 支持的单板密度最高的几类单板的接口类型、单板密度和整机密度。

表 1-1 常用接口整机密度表

接口类型	单板密度	整机密度
10GE	48	S9312：576 S9306：288 S9303：144
GE	48	S9312：576 S9306：288 S9303：144
FE	48	S9312：576 S9306：288 S9303：144

灵活的扩展能力

系统扩展能力主要包括：

- 业务扩展：系统的主控交换板支持灵活业务插卡，满足未来业务的扩展需求。
- 供电能力：目前电源模块的最大供电能力为 1600W，支持 1+1 或者 2+2 备份，未来可支持 4+4 备份。
- CSS（Cluster Switch System）：将 2 台交换机通过专用的堆叠电缆链接起来，对外呈现为一台逻辑交换机。堆叠交换机满足了数据中心大数据量转发和网络高可靠性的需求。

强大的转发能力

S9300 产品实现组播线速转发，硬件完成两级复制：交换网板复制到接口板和转发引擎复制到接口。

表 1-2 S9300 设备的系统配置参数

	S9312	S9306	S9303
交换网容量	1Tbit/s 或 2Tbit/s	1Tbit/s 或 2Tbit/s	720Gbit/s
背板容量	12Tbit/s	6Tbit/s	3Tbit/s
转发能力	1320Mpps	1080Mpps	540Mpps

丰富的业务功能

- 提供丰富的二层业务特性，主要特性包括：
  - VLAN（Virtual Local Area Network）
  - GARP/GVRP（Generic Attribute Registration Protocol / Generic VLAN Registration Protocol）

- 灵活 QinQ
- RRPP（Rapid Ring Protection Protocol）
- SEP (Smart Ethernet Protection)
- SmartLink
- STP（Spanning Tree Protocol）、RSTP（Rapid Spanning Tree Protocol）、MSTP（Multiple Spanning Tree Protocol）
- 端口聚合
- DHCP（Dynamic Host Configuration Protocol） snooping
- IGMP（Internet Group Management Protocol） snooping
- IPV6 ND (Neighbor Discovery) snooping
- MLD（Multicast Listener Discovery)V1/V2 snooping
- Ethernet OAM

- 提供丰富的 IP 业务特性，包括：
  - IPv4 单播路由协议,包括 RIP（Routing Information Protocol）、OSPFv2 （Open Shortest Path First）、ISIS（Intermediate System to Intermediate System）、BGP（Border Gateway Protocol）、MBGP（Multiprotocol Border Gateway Protocol）。
  - IPv6 单播路由协议，包括 RIPng、OSPFv3、ISIS、BGP+。
  - 组播路由协议，包括 IGMP、MLD、MSDP（Multicast Source Discovery Protocol）、组播 VPN、PIM-DM、PIM-SM、PIM-SSM
  - VRRP （Virtual Router Redundancy Protocol）
  - DHCP Relay、DHCP Server、Option82
  - 支持分布式和集中式两种 Netstream
- 全面支持 MPLS 业务
  - MPLS 转发
  - LDP
  - MPLS-TE
  - MPLS-OAM
- 提供完善的 VPN 业务，主要特性包括：
  - VPLS（Virtual Private LAN Service）
  - VLL（Virtual Leased Line）
  - BGP/MPLS IP VPN
- 提供移动承载业务
  - 三级时钟
  - 同步以太
  - 1588v2
- 提供丰富的企业网特性
  - NAC（Network Access Control），S9300 作为 NAC 方案中的 NAD（Network Access Device），支持 Web 认证、802.1x 认证和 MAC 认证。
  - PoE（Power On Ethernet）
  - 支持业务分流功能

- 防火墙/NAT
- 负载均衡
- IPSec VPN

  说明

  俄罗斯地区发布的版本不提供 IPSec 功能。

周密的安全设计

具备分布式设计的 S9300 产品确保了数据平面和控制平面之间的自然分离，提供业界领先的安全性能。

主要安全特性包括：

- 三种用户鉴权模式：本地验证、RADIUS 服务器验证和 HWTACACS 服务器验证，可对用户身份进行验证，并进行合理授权。
- 基于硬件的包过滤和采样，从而实现高性能和高扩展性。
- 对 OSPF、IS-IS、RIP 和 BGP-4 等上层路由协议，提供明文验证和 MD5（Message Digest 5）等多种验证方法。
- 实现转发和控制平面的 ACL（Access Control List）。
- 支持本机防攻击安全特性。可以通过配置黑白名单、CAR 对上送 CPU 的报文进行限制。
- 支持端口安全。
- 支持 URPF（Unicast Reverse Path Forwarding）。
- 支持 DHCP Snooping 和 DHCP Snooping over VPLS。
- 支持 MAC（Medium Access Control）限制和 MFF(MAC Forced Forwarding)。
- 支持 IP source trail、ARP（Address Resolution Protocol）防攻击、ICMP 防攻击、广播流量抑制等功能。
- 支持黑名单和攻击溯源。可以过滤黑名单上的用户流量，对攻击用户可以显示出其物理端口、VLAN 信息。
- 支持白名单。可以为协议报文上送 CPU 提供高优先级的通道。

电信级的可靠性

S9300 产品的整机结构还提供了功能强大的监控系统。通过独立的监控单元实现对整个系统的管理维护。实现对单板、风扇和电源配电模块的管理、监控和维护。

S9300 产品完全满足 EMC（Electro Magnetic Compatibility）要求。系统采用模块级屏蔽，实现了单板间的 EMC 隔离。

S9300 产品满足电信级高端产品的高可靠性要求。在系统的设计与实现上，通过提供如表 1-3 所示的特性来保障产品的高可靠性。

表 1-3 电信级的可靠性

项目	描述
系统保护机制	单板、电源模块和风扇支持热插拔。
	独立的监控单元，与业务系统完全分开。

项目	描述	
	风扇冗余备份，单个风扇失效，系统仍能正常工作 96 小时。	
	主控板采用 1+1 的冗余备份。	
	电源模块采用 1+1 或 2+2 的冗余备份。	
	时钟和管理总线等关键器件实现冗余备份。	
	异常保护	系统出现异常，系统可自动重新启动并恢复。
		单板异常，系统可复位单板并恢复。
		系统具有接口配置自动恢复的功能。
	电源、接口部分具有过流和过压保护。	
	提供单板防误插保护，避免因插错槽位导致故障。	
	电源的告警监视	提供告警提示信息、告警指示、运行状态和告警状态查询。
	电压和环境温度的监视	提供告警提示信息、告警指示、运行状态和告警状态查询。
可靠性设计	采用分布式硬件转发	
	控制通路同业务通路分离，保证控制通路的畅通。	
	具有完善的系统及单板故障检测、指示灯和网管告警功能。	
升级高可靠性	支持在线补丁	
	支持版本回退	
	支持 BOOTROM 在线升级	
	支持 ECC (Error Checking and Correction) RAM	
容错设计	数据备份	主备用单元间实现数据热备份，主用单元出现故障时，可以自动切换到备用单元，不会造成数据或信息的丢失。
	配置同步	各接口板及主控板之间同步操作
	支持自动选择并启动正确应用程序	
	支持 BOOTROM 程序的自动升级和自动恢复	
	支持配置文件备份到远程 FTP（File Transfer Protocol）服务器上	
	支持自动选择并运行正确的配置文件	
	提供系统软件异常监视功能，能够自行恢复异常并保存相应记录。	
操作安全	对系统的操作提供口令保护	
	支持通过配置用户级别和命令级别实现对命令的分级保护	
	支持通过命令锁定当前配置终端，防止非法使用终端	

项目	描述
	提供对不当操作防护和提示，如：对重要的影响系统性能的命令，提示用户是否继续操作，操作的执行需要用户的进一步确认。
操作维护中心	采用华为公司自主开发的通用综合网管平台

良好的可维护性

S9300 提供以下维护特性：

- 支持以太网 OAM，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。S9300 不但支持 IEEE 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，而且还支持 IEEE 802.1ag 中的连通性检测、MAC Trace 和 MAC Ping 功能。
- 支持 MPLS OAM 能力，支持基于 MPLS 的 Ping、Traceroute 等故障检测和定位技术，方便网络的管理和故障定位。
- 支持 802.1ag、802.3ah、BFD 之间的联动，实现端到端的 OAM。
- 支持基于物理端口、VLAN、LSP、ACL（Access Control List）的流量统计。
- 支持 U2000，可以完成对 S9300 的配置，包括设备管理、接口管理、VLAN 管理、组播管理、MPLS 管理、VPN 业务管理、软件升级管理、配置文件管理等。
- 支持端到端的配置、批量配置、向导配置等多种人性化的配置形式，并提供相应管理的缺省配置模板。
- 支持远程设备维护功能。通过 Telnet 等方式远程登录到设备上实现远程维护。
- 支持远程在线升级。设备正常工作中，通过 FTP 或 TFTP 方式实现远程在线平滑升级；结合主备倒换，还可以实现升级过程中业务不中断。
- 支持热补丁功能。可以只针对需要修改的部分特性进行升级。打补丁过程中业务不受影响。热补丁支持确认和删除功能。
- 支持版本回退功能。在线升级和在线补丁过程中如果出现问题，S9300 支持切换回升级或补丁之前的软件版本重新运行。

2 产品架构

关于本章

介绍了 S9300 整机结构、硬件结构和软件结构。

2.1 整机结构
S9300 采用分布式硬件平台。

2.2 硬件结构
介绍了 S9300 硬件结构、背板、SRU、MCU、CMU、LPU、FSU。

2.3 软件结构
S9300 采用华为公司最新的通用路由平台 VRPv5（VRP version 5），提供了丰富的软件特性。VRPv5 由系统服务平面、通用控制平面、数据转发平面、业务控制平面和系统管理平面组成。

2.1 整机结构

S9300 采用分布式硬件平台。

S9300 的硬件系统由机箱、背板、电源模块、风扇框、主控路由板 SRU（Switch Routing Unit）或主控板 MCU（Main Control Unit）、线路板 LPU（Line Processing Unit）和集中监控板 CMU（Central Management Unit）组成。

整机宽度符合业界标准尺寸，可以安装到 IEC297 标准机柜或 ETSI 标准机柜中。

说明

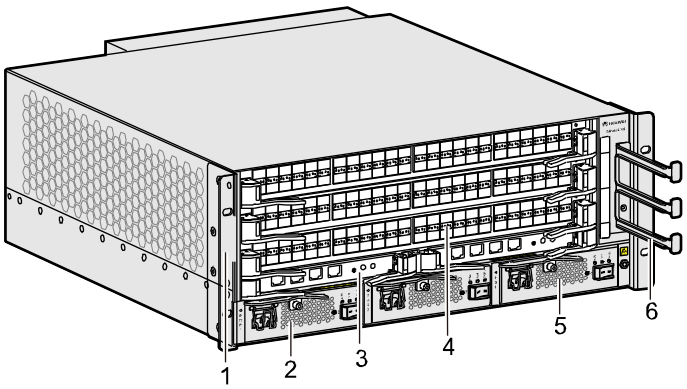
- SRU、CMU 适用于 S9312 和 S9306 设备。
- MCU 只适用于 S9303 设备。

2.1.1 S9303 整机结构

产品外观

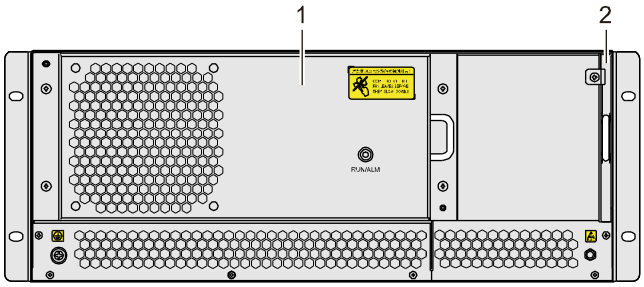
S9303 产品外观如图 2-1 所示。

图 2-1 S9303 产品外观



1. 挂耳
2. 电源模块
3. 主控板 MCU
4. 线路板 LPU
5. PoE 模块
6. 走线架

图 2-2 S9303 产品外观（背面）



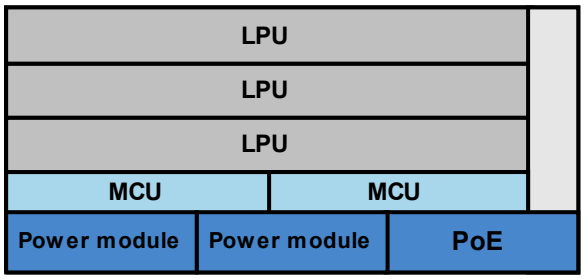
1. 风扇模块 2. 防尘网

S9303 的机箱外型尺寸为 442mm×476mm×175mm（宽×深×高）。

机箱正面从上到下分别为线路板、主控板和电源模块。整个机箱采用后抽风散热。搬运把手位于机箱两侧。

板件布局

图 2-3 S9303 板件布局

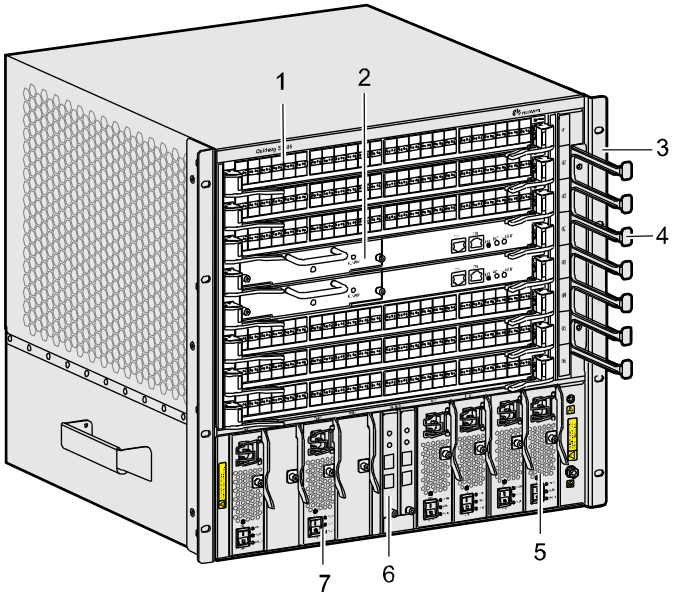


- S9303 采用前维护设计，单板区共有 5 个横插拔的单板槽位。其中，下部两个槽位为半高槽位，固定为主控板 MCU 槽位，MCU 板支持 1+1 备份；其他为线路板 LPU 槽位。
- 风扇区和防尘网位于机箱的后面。
- 电源区位于机箱的底部，电源采用 1+1 冗余备份，支持双电网输入。可选择交流电源（AC）和直流电源（DC）两种供电方式。
- 支持 POE 供电。仅支持交流电源（AC），且不支持备份。

2.1.2 S9306 整机结构

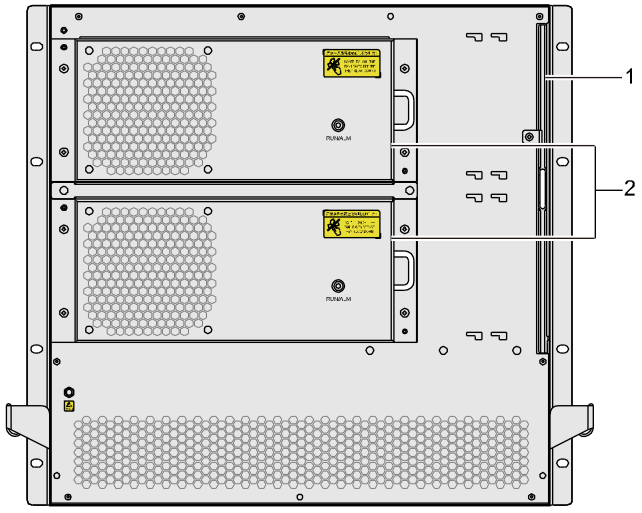
产品外观

图 2-4 S9306 产品外观



1. 线路板 LPU
2. 主控板 SRU
3. 挂耳
4. 走线架
5. PoE 模块
6. 集中监控板 MCU
7. 电源模块

图 2-5 S9306 产品外观（背面）



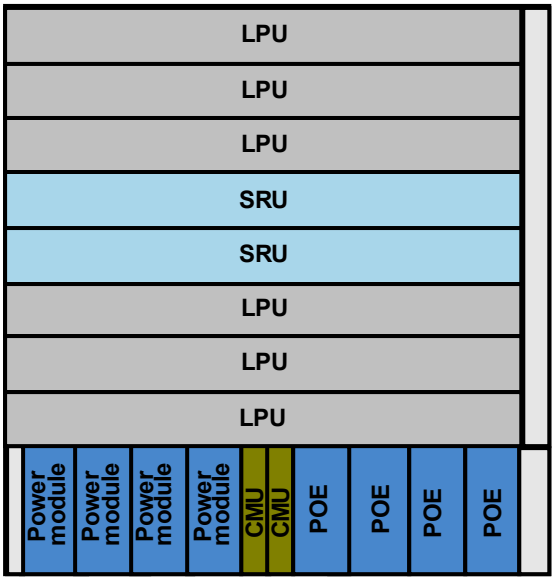
1. 防尘网
2. 风扇模块

S9306 的机箱外型尺寸为 442mm×476mm×441.7mm（宽×深×高）。

机箱正面从上到下分别为线路板、主控板、集中监控板和电源模块。整个机箱采用后抽风散热。搬运把手位于机箱两侧。

板件布局

图 2-6 S9306 板件布局

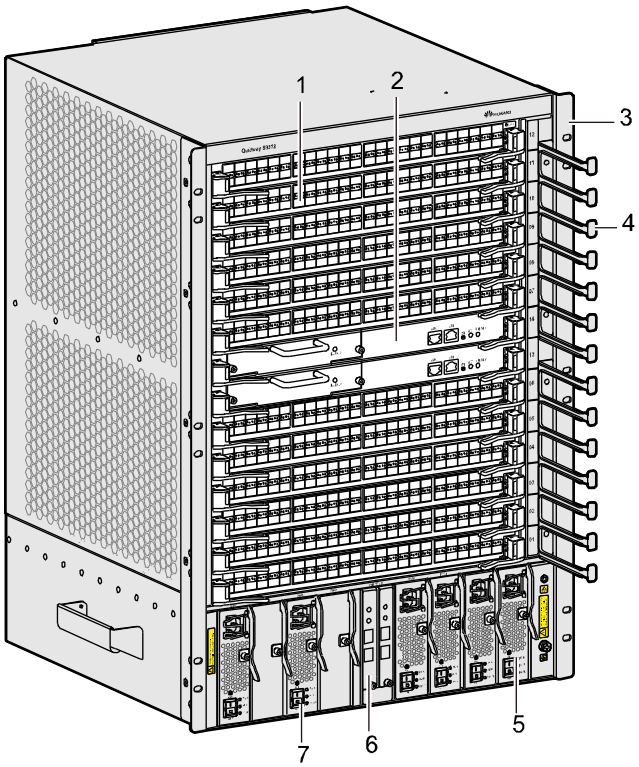


- S9306 的单板区共有 8 个横插拔的单板槽位。其中，中间两个槽位固定为主控板 SRU 槽位，SRU 板支持 1+1 备份；其它为线路板 LPU 槽位
- 风扇区和防尘网位于机箱的后面。
- 电源区位于机箱的底部，支持双电网输入，可选择交流电源（AC）和直流电源（DC）两种供电方式。直流电源支持 1+1 配置，交流电源支持 1+1 或者 2+2 配置。
- 集中监控板（CMU）位于机箱的底部，支持 1:1 备份。
- 支持 POE 供电，仅支持交流电源（AC），支持 4 个 PoE 电源模块，支持 2 ＋ 2 备份、3 ＋ 1 备份或者不备份（4+0）。

2.1.3 S9312 整机结构

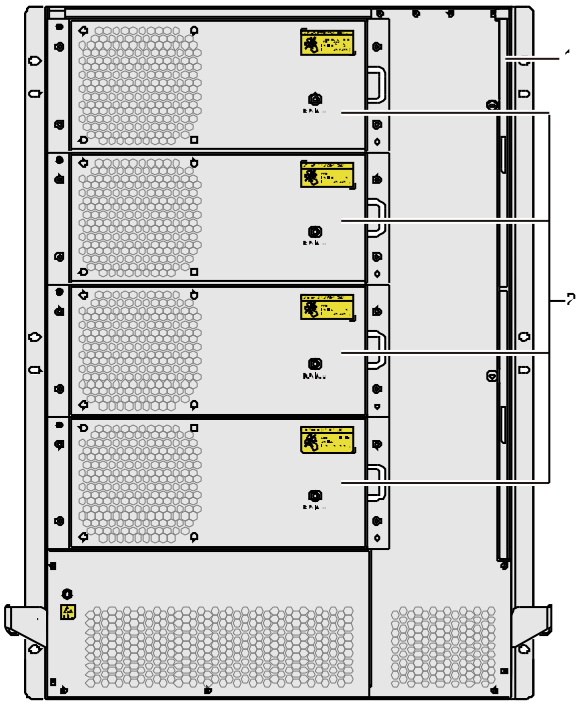
产品外观

图 2-7 S9312 产品外观



1. 线路板 LPU
2. 主控板 SRU
3. 挂耳
4. 走线架
5. PoE 模块
6. 集中监控板 CMU
7. 电源模块

图 2-8 S9312 产品外观（背面）



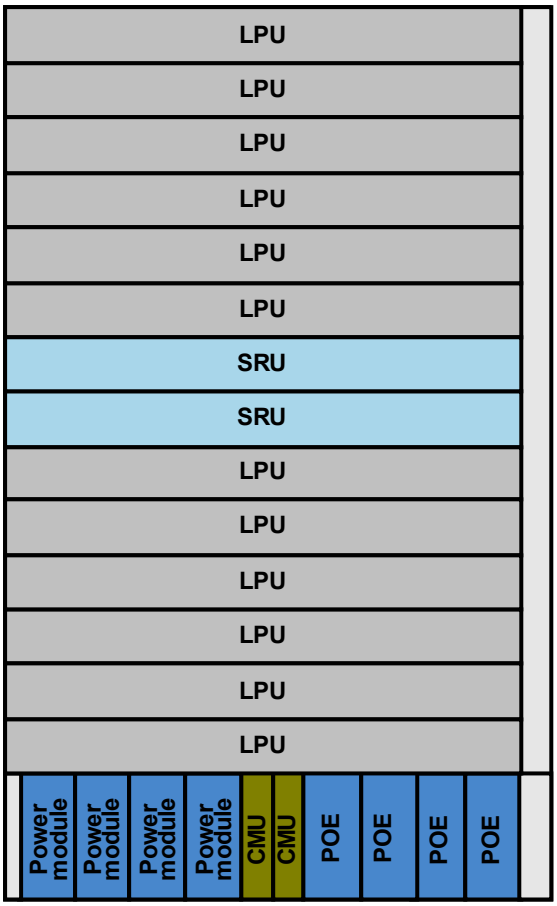
1. 防尘网　　2. 风扇模块

S9312 的机箱外型尺寸为 442mm×476mm×663.95mm（宽×深×高）。

机箱正面从上到下分别为线路板、主控板、集中监控板和电源模块。整个机箱采用后抽风散热。搬运把手位于机箱两侧。

板件布局

图 2-9 S9312 板件布局图



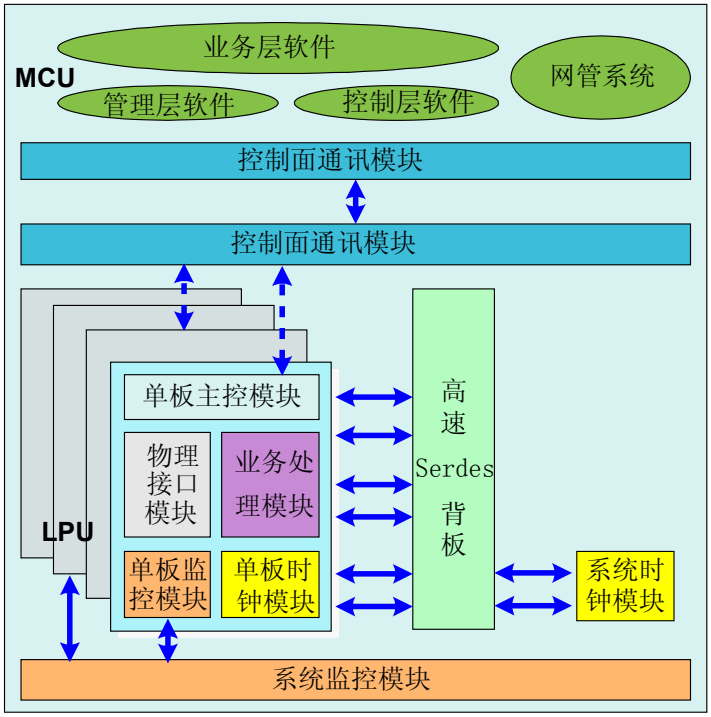
- S9312 的单板区共有 14 个横插拔的单板槽位。其中，中间两个槽位固定为主控板 SRU 槽位，SRU 板支持 1+1 备份；其它为线路板 LPU 槽位
- 风扇区和防尘网位于机箱的后面。
- 电源区位于机箱的底部，支持双电网输入，可选择交流电源（AC）和直流电源（DC）两种供电方式。直流电源支持 1+1 配置，交流电源支持 1+1 或者 2+2 配置。
- 支持 POE 供电。仅支持交流电源（AC），共 4 个 PoE 电源模块，支持 2 ＋ 2 备份、3+1 备份或者不备份（4+0）。
- 集中监控板 CMU 位于机箱的底部，支持 1:1 备份。

2.2 硬件结构

介绍了 S9300 硬件结构、背板、SRU、MCU、CMU、LPU、FSU。

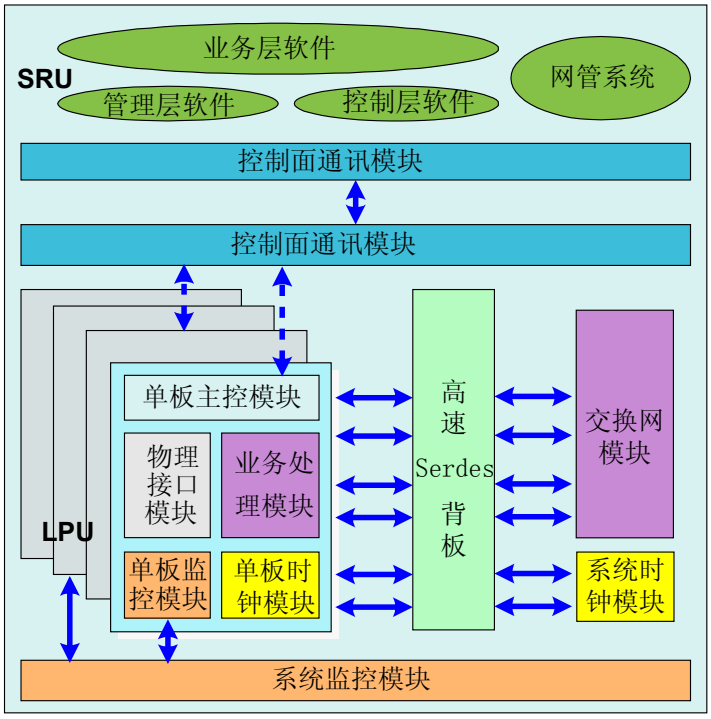
S9303 的硬件结构如图 2-10 所示。

图 2-10 S9303 的硬件结构



S9306 和 S9312 的硬件结构相同，如图 2-11 所示。

图 2-11 S9306 和 S9312 的硬件结构



2.2.1 背板

S9300 采用无源背板，背板提供各槽位的互连，并完成各部件间的各种高速数据信号以及控制信号的互连。

背板提供主控板与其它各部件之间的数据总线、管理总线和时钟总线等，用于主控板与各部件之间的通信。

S9300 背板提供 2 个主控板槽位，根据设备型号的不同分别提供 3 个、6 个和 12 个 LPU 槽位。

2.2.2 SRU

S9300 的 SRU 是主控板，仅用于 S9306 和 S9312 设备。它集成了数据交换模块、主控模块、引擎灵活插卡引擎、CF（Compact Flash）卡模块，和系统监控管理模块，是多个功能模块的集合体。SRU 可以扩展增加时钟模块。SRU 板是系统控制管理和数据交换的核心，负责完成数据交换、系统控制和系统监控功能。

SRU 的主控单元，为 1+1 备份设计；数据交换单元支持 1 ＋ 1 负荷分担和 1:1 备份模式。

S9306 和 S9312 的 SRU 主要完成如下功能：

- 数据平面的数据转发
- 处理各种协议并完成转发控制，例如各种路由协议、网管协议等。
- 监控系统各部件的状态。
- 根据用户的操作指令来管理和维护，并输出设备运行情况。

表 2-1 主控板

单板名称	备注
SRUA	提供 1Tbps 的业务交换能力。
SRUB	提供 2Tbps 的业务交换能力。

2.2.3 MCU

MCU（Main Control Unit）是主控管理单元，仅使用于 S9303 设备。MCU 集成了主控模块、CF（Compact Flash）卡模块，和系统监控管理模块，并可扩展增加时钟模块。

S9300 的 MCU 主要完成如下功能：

- 处理各种协议并完成转发控制，例如各种路由协议、网管协议等。
- 监控系统各部件的状态。定期收集系统各单元运行数据，根据各单元运行状态产生控制信息，如检测各单板在位情况、控制交换网运行状态等。
- 根据用户的操作指令来管理和维护，并输出设备运行情况。

2.2.4 CMU

CMU（Central management Unit）是集中监控板，主要完成以下功能：

- 整机电源的监控、管理
- 风扇的监控、管理
- 外接 PoE 管理

实现设备的监控、管理、节能减排。

2.2.5 LPU

LPU 完成报文的业务处理和提供业务接口。S9300 支持的以太网接口板如表 2-2 所示。

表 2-2 以太网接口板

接口板名称	英文简称	备注
48 端口百兆以太网光接口板（EA，SFP）-32K MAC	F48SA	支持： ● MPLS ● Netstream ● IPv6
48 端口百兆以太网光接口板（EC，SFP）-128K MAC	F48SC	支持： ● MPLS ● Netstream ● IPv6
48 端口百兆以太网电接口板（EA，RJ45）-32K MAC	F48TA	支持： ● MPLS ● Netstream ● IPv6
48 端口百兆以太网电接口板（EC，RJ45）-128K MAC	F48TC	支持： ● MPLS ● Netstream ● IPv6

接口板名称	英文简称	备注
48 端口百兆以太网电接口板 (FA,RJ45)-32K MAC	F48TFA	支持： ● MPLS ● Netstream ● IPv6
48 端口百兆/千兆以太网光接口板（EA,SFP）-32K MAC	G48SA	支持： ● MPLS ● Netstream ● IPv6
48 端口百兆/千兆以太网光接口板（EC,SFP）-128K MAC	G48SC	支持： ● MPLS ● Netstream ● IPv6
48 端口百兆/千兆以太网光接口板（ED,SFP）-512K MAC	G48SD	支持： ● MPLS ● Netstream ● IPv6
48 端口千兆以太网光接口板 (FA,SFP)-32K MAC	G48SFA	支持： ● MPLS ● Netstream ● IPv6
48 端口百兆/千兆以太网电接口板（EA,RJ45）-32K MAC	G48TA	支持： ● MPLS ● Netstream ● IPv6
48 端口百兆/千兆以太网电接口板（EC,RJ45）-128K MAC	G48TC	支持： ● MPLS ● Netstream ● IPv6
48 端口百兆/千兆以太网电接口板（ED,RJ45）-512K MAC	G48TD	支持： ● MPLS ● Netstream ● IPv6

接口板名称	英文简称	备注
48 端口千兆以太网电接口板(FA,RJ45)-32K MAC	G48TFA	支持： ● MPLS ● Netstream ● IPv6
12 端口百兆/千兆光接口和 36 端口百兆/千兆电接口板(EA,RJ45/SFP)－32K MAC	G48CEAT	支持： ● MPLS ● Netstream ● IPv6
48 端口百兆/千兆以太网 POE 电接口板（EA，RJ45，POE）-32K MAC	G48VA	支持： ● MPLS ● Netstream ● IPv6
4 端口万兆以太网光接口板（EA，XFP）-32K MAC	X4UXA	支持： ● MPLS ● Netstream ● IPv6
4 端口万兆以太网光接口板（EC，XFP）-128K MAC	X4UXC	支持： ● MPLS ● Netstream ● IPv6
4 端口万兆以太网光接口板(ED,XFP)-512K MAC	X4UXD	支持： ● MPLS ● Netstream ● IPv6
2 端口万兆以太网光接口板（EA，XFP）-32K MAC	X2UXA	支持： ● MPLS ● Netstream ● IPv6
2 端口万兆以太网光接口板（EC，XFP）-128K MAC	X2UXC	支持： ● MPLS ● Netstream ● IPv6

接口板名称	英文简称	备注
24 端口百兆/千兆以太网光接口和 8 端口百兆/千兆 Combo 电接口板(EA,SFP/RJ45,1588)-32K MAC	G24CEAS	支持： ● MPLS ● Netstream ● IPv6
24 端口百兆/千兆以太网光接口板（SA，SFP）-32K MAC	G24SA	-
24 端口百兆/千兆以太网光接口板（EC，SFP）-128K MAC	G24SC	支持： ● MPLS ● Netstream ● IPv6
24 端口百兆/千兆以太网光接口板（ED，SFP）-512K MAC	G24SD	支持： ● MPLS ● Netstream ● IPv6
24 端口百兆/千兆以太网光接口＋Combo 电接口板（SA，SFP/RJ45）-32K MAC	G24CA	-
12 端口万兆以太网光接口板（SA，SFP+）-32K MAC	X12SA	-
48 端口万兆以太网光接口板(SA,SFP+)-32K MAC	X48SSA	-
24 端口百兆/千兆以太网电接口和 2 端口万兆以太网光接口板（EA，RJ45/XFP）-32K MAC	T24XA	支持： ● MPLS ● Netstream ● IPv6
24 端口百兆/千兆以太网光接口和 2 端口万兆以太网光接口板（EA，SFP/XFP）-32K MAC	S24XA	支持： ● MPLS ● Netstream ● IPv6
12 端口千兆 EPON 光接口和 12 端口百兆/千兆光接口板（SFP）	E12GA	-

说明

SFP、SFP+和 XFP 均为可插拔光模块。

S9300 的 LPU 板分为 S 系列、E 系列、F 系列和 EPON 板，其中：

- S 系列 LPU 包含 SA 板。例如：24 端口百兆/千兆以太网光接口板（**SA**，SFP）-32K MAC
- E 系列 LPU 包括 EA、EC 和 ED 板。例如：48 端口百兆以太网光接口板（**EA**，SFP）-32K MAC
- F 系列 LPU 包括 FA 板。例如：48 端口千兆以太网电接口板(**FA**, RJ45)-32K MAC
- EPON 单板即 12 端口千兆 EPON 光接口和 12 端口百兆/千兆光接口板（SFP）。

2.2.6 FSU

FSU（Flexible Service Unit）是一个灵活插卡业务处理引擎。

S9312 和 S9306 的灵活插卡 FSUA（Flexible Service Unit, A 表示版本）支持的功能包括：

- 基于硬件的以太网 OAM
- 基于硬件的 MPLS OAM
- 基于硬件的 BFD
- 主控 CPU 通道安全保护

说明

基于软件的以太网 OAM、MPLS OAM、BFD 和 NQA 功能在 LPU 板上支持。

FSUA 位于 SRU 主控板上，用户可以根据业务需要选择配置此板卡。

表 2-3 灵活插卡板

单板名称	描述
FSUA	提供 20G 的业务处理能力

2.2.7 VSU

VSU（Virtual Switch Unit）是堆叠插卡，用于支持多台设备的堆叠连接。

S9312 和 S9306 的堆叠插卡板名称为 VSTSA（Virtual Switch，T 表示电口，S 表示标准系列，A 表示版本），位于 SRU 主控板上，用户可以根据业务需要选择配置此板卡。

说明

S9303 不支持设备堆叠。

表 2-4 堆叠插卡

单板名称	描述
VSTSA	提供堆叠连接功能

2.2.8 SPU

SPU（Service Processing Unit）为增值业务处理单元，没有业务接口。

SPU 的单板名称为 VAMPA（Value Added service Multi-core Processor, A 表示版本），支持的功能包括：

- 防火墙
- NAT
- 集中式 NetStream
- 负载均衡
- IPSec VPN

  说明

  俄罗斯地区发布的版本不提供 IPSec 功能。

表 2-5 堆叠插卡

单板名称	描述
VAMPA	增值业务处理单板

2.3 软件结构

S9300 采用华为公司最新的通用路由平台 VRPv5（VRP version 5），提供了丰富的软件特性。VRPv5 由系统服务平面、通用控制平面、数据转发平面、业务控制平面和系统管理平面组成。

- 系统服务平面

  在操作系统的基础上，提供系统的任务管理，内存管理，定时器，软件加载和补丁功能，增强了组件技术，便于系统升级和裁减。

- 通用控制平面

  是 VRP 数据通信平台的核心。提供数据通信的各种链路管理，IP 协议栈，各种路由协议处理功能，是安全和 QoS 功能的基础。通用控制平面的核心功能是控制数据转发平面，完成设备的各项功能。

- 数据转发平面

  在通用控制平面的控制下，完成数据的转发，实现数据通信的功能。VRPv5 支持软件转发和硬件转发。

- 业务控制平面

  提供基于用户、接口的控制和管理功能，主要包括通过 DHCP Option82 携带信息，实现用户的安全认证、授权管理和计费，通过 802.1x 实现接入端口的安全认证。

- 系统管理平面

  提供用户界面和输入输出管理功能，是网络管理、维护的基础。

3 业务特性

关于本章

S9300 提供的主要业务特性包括：IP 特性、MPLS 、MPLS L3VPN、MPLS L2VPN、QoS、以太网、Ethernet OAM、NAC、组播、可靠性、LLDP、安全特性、时钟特性、堆叠、Web 网管、防火墙/NAT、负载均衡、IPSec VPN 和 NetStream 特性。

说明

俄罗斯地区发布的版本不提供 IPSec VPN 功能。

在企业网中，通过 10BASE-T、100BASE-TX、1000BASE-T 以太网网络供电，可以有效的解决 IP 电话、无线 AP、便携设备充电器、刷卡机、摄像头、数据采集等终端的集中式电源供电。

3.10 行业网特性

S9300 为行业网安全提供 NAC、防火墙、NAT 以及负载均衡功能。

3.11 MPLS & VPN 特性

通过 S9300 产品构建 MPLS 网络时，MPLS 网络外部仍旧根据 VLAN 和 MAC 地址进行交换，而 MPLS 网络内各设备依据 MPLS 标签进行交换，从而有效缓解了 VLAN Tag 标签容量瓶颈和 MAC 地址表容量限制的问题。

3.1 以太网特性

S9300 支持的主要以太网特性有：VLAN Mapping、QinQ、灵活 QinQ 和 BPDU Tunnel。

3.1.1 VLAN Mapping

VLAN Mapping 就是指在 S9300 上建立 VLAN 映射表，实现用户 VLAN 到运营商 VLAN 之间的映射。例如将一个或多个用户 VLAN ID 映射到一个运营商 VLAN ID。

说明

用户 VLAN 一般是用户侧端口对应的 VLAN（也称为 C-VLAN），具有局部意义，一般用于标识一个或一类用户。

运营商 VLAN 通常是网络侧由 ISP 指定的 VLAN（也称为 S-VLAN），具有全局意义，一般用于标识一种业务。

对于指定的用户侧端口，S9300 支持以下方式的单 TAG 报文的 VLAN Mapping 功能：

- 1:1 映射

  将一个用户侧 VLAN Tag 标签映射到一个网络侧 VLAN Tag 标签或添加一层 VLAN Tag 标签。
- N:1 映射

  将多个用户侧 VLAN Tag 标签映射到一个网络侧 VLAN Tag 标签或添加一层 VLAN Tag 标签。

S9300 还能够支持增强的双 TAG 报文 VLAN Mapping 功能：

- 2:2 映射

  将用户侧的携带双 VLAN Tag 报文映射到网络侧的双 VLAN Tag 报文，支持报文的内外层 VLAN Tag 的同时切换。
- 2:1 映射

  将用户侧的双 VLAN Tag 报文切换到网络侧的单 VLAN Tag 报文。

S9300 还支持基于 CoS 值的 VLAN Mapping 功能，将多个用户侧 VLAN Tag 标签依据 CoS 值映射到一个网络侧 VLAN Tag 标签或添加一层 VLAN Tag 标签。

3.1.2 灵活 QinQ

S9300 提供的灵活 QinQ 技术，不仅能扩展 Tag 标签空间，还可以根据接收到的 C-VLAN 入标签自由地选择外层 S-VLAN 的 Tag 标签，从而针对不同的私网业务选择不同的传输路径，实现业务分流，让业务部署更加方便。灵活 QinQ 特性可以配置 S9300 的入方向和出方向，使用户的组网配置更加灵活。

S9300 支持以下两种方式的灵活 QinQ 功能：

- 在端口上，根据用户报文中 C-VLAN Tag 的 VLAN ID，增加不同 S-VLAN 外层 Tag 标签。

- 在端口上，根据用户报文中 C-VLAN Tag 的 VLAN ID，先修改内层 Tag。然后增加不同的 S-VLAN 外层 Tag 标签。

灵活 QinQ 配置中，支持基于外层 Tag 进行 MAC 地址学习，上下行转发中支持根据目的 MAC 地址转发。

在 S9300 的强大硬件支持下，可以利用 ACL 识别报文特征进行流分类来实现灵活 QinQ 功能，实现 S-VLAN Tag 的灵活添加和 C-VLAN Tag 的修改。

3.1.3 BPDU Tunnel

BPDU Tunnel 是一种二层隧道技术，可以使不同地域的用户私网，通过运营商网络内指定的 VLAN VPN 进行 BPDU 报文的透明传输，从而使用户私网能够进行统一的生成树计算。并且用户私网和运营商网络拥有各自的生成树，互不干扰，也提高了网络的收敛速度。

使能 BPDU Tunnel 功能后，S9300 将带 Tag 的 BPDU 视为普通二层数据帧在所属 VLAN 内转发，或封装为 MPLS 报文在 MPLS 网络内转发，而不将该数据帧当成 BPDU 来处理。

3.2 IP 特性

S9300 支持 IPv4 和 IPv6 以及 IPv4/IPv6 过渡技术。

说明

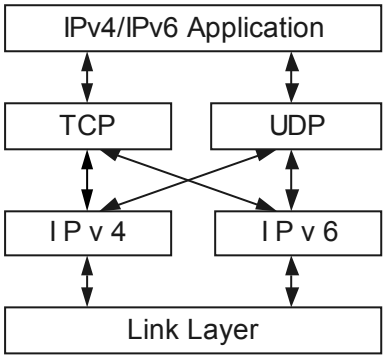
如果需要 IPv6 功能，请联系华为公司购买 License。

介绍了 S9300 持的 IP Session 特性。

3.2.1 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 3-1** 所示。

图 3-1 双协议栈结构



3.2.2 IPv4 特性

S9300 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 DHCP snooping，实现用户 source guard。
- 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。

  说明

  如果需要实现 NQA 功能，请联系华为公司购买 License。
- 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。

3.2.3 IPv6 特性

S9300 支持的 IPv6 特性如下：

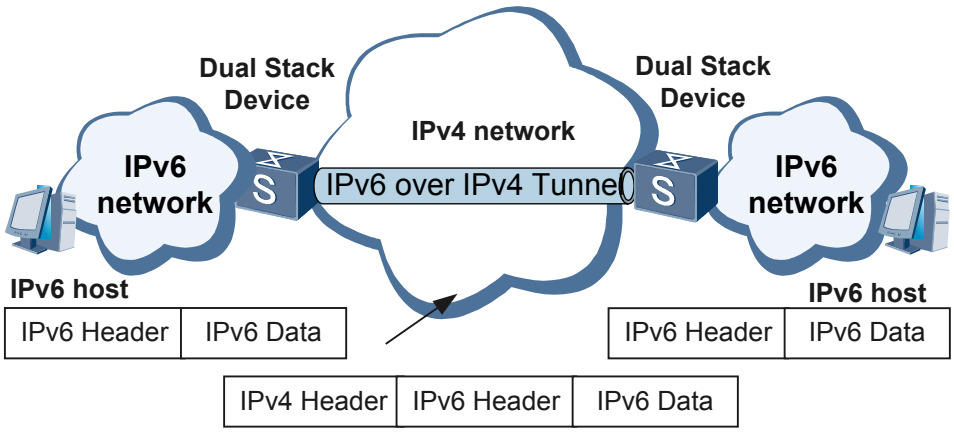
- 支持 IPv6 ND（Neighbor Discovery）。
- 支持 PMTU 发现（Path MTU Discovery）。
- 支持 TCP6、Ping IPv6、Tracert IPv6、Socket IPv6、UDP6、RawIP6。
- 支持 TFTP IPv6 Client。
- 支持 IPv6 策略路由。
- 支持 DHCPv6 snooping 和 MLDv1/v2 snooping。
- 支持 ND（Neighbor Discovery） snooping。

3.2.4 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 3-2 所示。

图 3-2 IPv6 over IPv4 隧道原理图



S9300 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。它相当于通过 IPv4 骨干网连接的两个 IPv6 域的永久链路，是两个边缘路由设备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。

- 6to4 隧道

  6to4 隧道可将多个 IPv6 孤岛网络通过 IPv4 网络连接到 IPv6 网络。

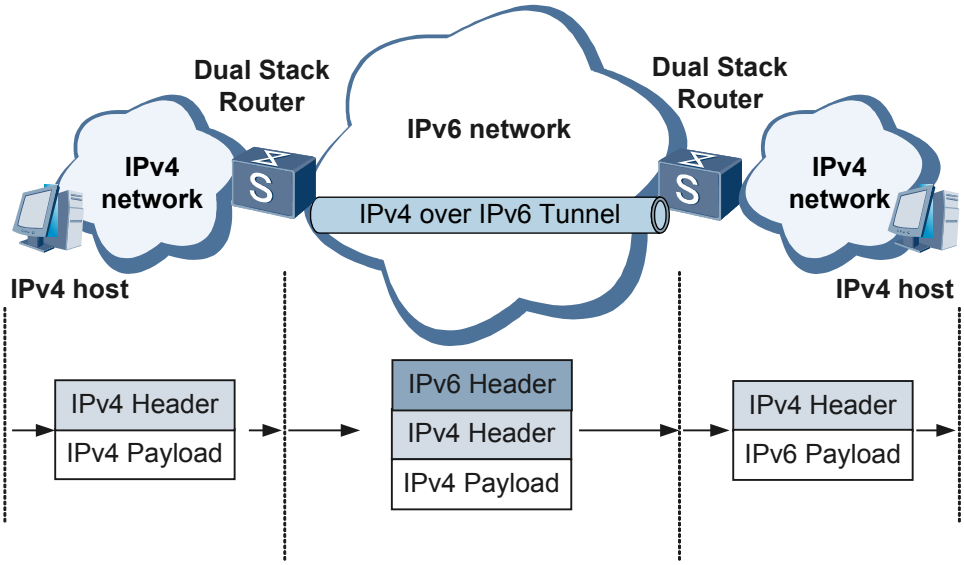
  6to4 隧道与手动配置隧道的主要区别在于，6to4 隧道可以是点到多点的连接，而手动隧道仅仅是点到点的连接。所以 6to4 隧道的路由设备并不是成对配置的。6to4 隧道与自动隧道类似，它可自动查找隧道的另一端点，但它不需要指定兼容 IPv4 的 IPv6 地址。6to4 隧道使用了一种特殊的 IPv6 地址，即 6to4 地址。

IPv4 over IPv6 隧道

在 IPv4 网络向 IPv6 网络过渡的后期，IPv6 网络已被大量部署，此时可能出现 IPv4 孤岛。采用专用的线路将这些孤岛互连显然是不经济的。利用隧道技术可在 IPv6 网络上创建隧道，从而实现 IPv4 孤岛的互连。这类似于在 IP 网络上利用隧道技术部署 VPN。在 IPv6 网络上用于连接 IPv4 孤岛的隧道，称为 IPv4 over IPv6 隧道。

为了实现 IPv4 over IPv6 隧道，需要在 IPv6 网络与 IPv4 网络交界的边界路由设备上启动 IPv4/IPv6 双协议栈（Dual Stack）。

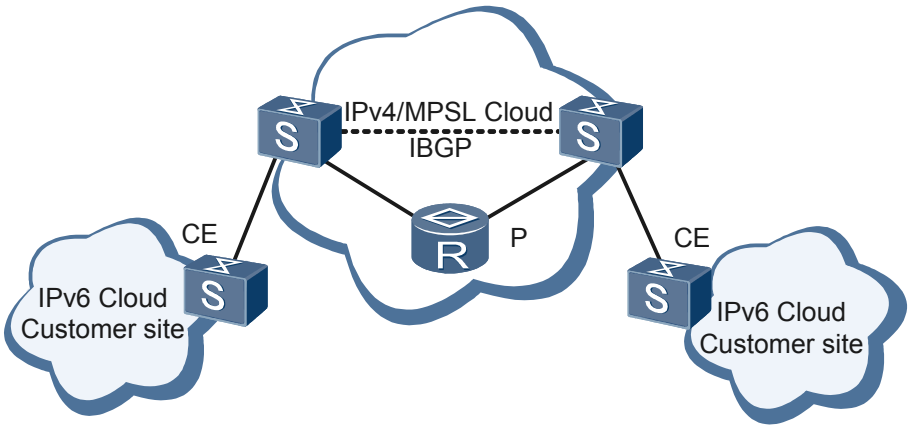
图 3-3 IPv4 over IPv6 隧道组网图



6PE

6PE（IPv6 Provider Edge）路由设备允许 IPv6 孤岛的 CE 路由设备穿过 IPv4 网络进行通信，如图 3-4 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。

图 3-4 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。

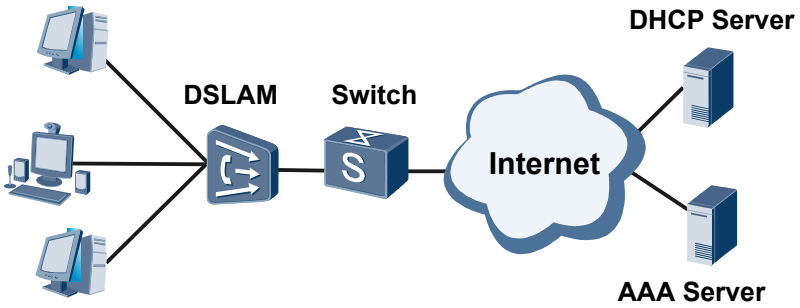
当 ISP 想利用自己原有的 IPv4/MPLS 网络，使其通过 MPLS 具有 IPv6 流量交换能力时，只需要升级 PE 就可以了。所以对于运营商来说，使用 6PE 特性作为 IPv6 过渡机制是一个高效的解决方案。

3.2.5 IP Session

介绍了 S9300 持的 IP Session 特性。

如图 3-5 所示，图中 S9300 以 Switch 表示。

图 3-5 IP Session 组网图



S9300 支持 IP Session 的终结与认证、地址分配。

家庭中的 STB/VOIP 终端发送 DHCP Request 申请地址，S9300 可以直接为终端分配地址，也可以 Relay 到 DHCP SERVER 上分配地址。分配地址前，S9300 组织报文 VLAN (QinQ)或 DHCP Relay Agent 信息发送到 AAA 服务器，对终端的合法性进行认证，认证成功即可分配地址。

S9300 根据不同的业务类型，进行 QoS 调度，也可以将各业务流量封入不同的 VPN，业务之间进行隔离。

3.3 组播特性

S9300 支持组播路由协议、IGMP Snooping、IGMP Proxy、静态组播、组播 VLAN、组播报文复制等丰富的组播特性。同时，S9300 支持组播复制能力。

3.3.1 组播路由协议

S9300 支持以下组播路由协议：

- IGMP、PIM 组播路由协议（包括 PIM-DM、PIM-SM）、组播源发现协议 MSDP（Multicast Source Discovery Protocol）、MBGP 协议。
- 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。一个 RP 失效后，已经在这个 RP 上注册的组播源和接收者，又会选择另一个就近的 RP 注册和加入，实现 RP 的负载分担。
- 支持的 IPv6 组播路由协议包括：PIM-IPv6-DM、PIM-IPv6-SM 和 PIM-IPv6-SSM。
- 支持 MLD（Multicast Listener Discovery），MLD 用来在用户主机和与其直接相邻的组播路由器之间建立、维护组播组成员关系，功能和实现原理都与 IGMP 相同。MLD 有两个版本。
  - MLDv1（由 RFC2710 定义）

    MLDv1 与 IGMPv2 保持一致，直接支持 ASM（Any-Source Multicast）；借助 SSM-Mapping 可以实现 SSM（Source-Specific Multicast）。
  - MLDv2（由 RFC3810 定义）

    MLDv2 与 IGMPv3 保持一致，直接支持 ASM 和 SSM。

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。

3.3.2 IGMP Snooping

S9300 部署在用户主机和组播路由器之间，不仅可以静态配置组播转发表项，还可以通过侦听交互的 IGMP 消息维护组播组、VLAN 和出端口之间的对应关系，动态构建组播报文的二层转发表。

当 S9300 收到组播数据包后，仅向该组播组对应的 VLAN 成员转发。依据二层转发表，组播报文可以在 VLAN 内以组播方式发送，不仅减少了报文数量，节省了带宽，而且提高了信息传送的安全性。

IGMP snooping 功能也可以 VPLS 网络中使用。

端口快速离开

对于只连接一台主机的 S9300 端口，当接收到来自主机的 IGMP 离开消息时，就立即删除该端口对应的组播转发表项。当 S9300 接收到后续 IGMP 查询消息时，不再向该端口转发，不仅节约了带宽和系统资源，还可以实现业务的快速切换。

组播查询器

在没有路由器的二层网络，S9300 可以作为查询器来发送查询报文，终结 IGMP 协议报文，建立二层网络的组播转发表，实现组播功能。查询器可以基于 VLAN 来配置。

当 VLAN 内启动查询器后，S9300 的组播查询器可以实现：

- 终结来自用户的 IGMP 的 Report 报文，根据 Report 报文建立组播转发表项。
- 终结来自路由器的 IGMP 的 Query 报文，组播查询器负责发送查询报文。
- 在 VLAN 内广播 PIM（Protocol Independent Multicast）协议报文。
- 终结来自用户的 IGMP 的 Leave 报文。当用户发送 Leave 报文准备离开时，组播查询器发送特定组查询报文进行确认。

组播协议报文抑制功能

若短时间内 S9300 收到用户 Report 或 Leave 报文，S9300 会通过查看是否在抑制时间内收到相同的 Report 报文或 Leave 报文来决定是否向路由器进行转发。这样可以减少路由器处理 IGMP 协议报文的数量。

可控组播

S9300 可以通过设置 ACL 策略来控制某个组播组只允许哪些 VLAN 或 VPLS VSI 用户加入，达到可控组播的目的。

组播 CAC（Call Admission Control）

组播 CAC 是 IPTV 组播方案的组成部分，主要在二层组播场景下控制 IPTV 的节目数量和带宽，避免出现带宽需求超出接入汇聚网带宽的情况，保证大多数用户的服务质量。

3.3.3 静态组播

用户终端通过 DSLAM 接收组播流，例如 STB（Set Top Box）接收来自 BTV（Broadband TeleVision）的视频节目。在众多 DSLAM 和上游组播路由器之间部署 S9300，S9300 部分 VLAN 上并不启动 IGMP 功能。在这些 VLAN 上，S9300 仅根据各用户定制组播流的实际情况，静态配置组播组成员关系和组播转发表项。

各 DSLAM 提供可控组播功能，可以直接控制用户 STB 的频道添加、删除和切换，避免了 S9300 参与 IGMP 报文的收发，因此极大降低了用户切换频道引起的图像、声音停滞时延。

3.3.4 组播 VLAN 和组播复制

所谓组播 VLAN，是指使用该 VLAN 来汇聚组播流并进行组播流转发。当用户需要某些组播流时，会加入组播 VLAN。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。S9300 同一组播流可以向同一端口最大复制 127 份组播流。

S9300 将去往各用户的组播流通过组播 VLAN 来转发，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，S9300 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。

3.4 QoS 特性

QoS 是 Quality of Service（服务质量）的缩写，QoS 简单地说：就是针对各种不同需求，提供不同服务质量的网络服务功能。

3.4.1 层次化流量监管

S9300 系列交换机支持 2 级的流量监管（基于业务和企业），支持业务和企业带宽统计复用。

流量监管用于在报文的接收端口对匹配流分类规则的业务流进行监管，以使之适应分配给它的那部分带宽等网络资源。流量监管主要体现在对报文“接收端口/业务流”的速率限制上，监督进入某一网络的流量。如果速率过大，流量监管就可以选择丢弃报文或重新设置报文的优先级。

S9300 系列交换机支持双速三色和单速双色标记器，支持更精细的带宽管理。

S9300 系列交换机支持 2 级的流量监管（基于业务和企业），可以提供基于企业的流量监控，以及基于企业内各业务的带宽统计复用。

3.4.2 端口流控

端口流控用于拥塞管理。拥塞是指网络无法满足承诺的或者经过协商的性能指标（如速率等）的情况。

当拥塞发生时，以太网交换机会向相应的连接发出暂停帧，通知对端暂停一个时间间隔后再发送数据，减少注入网络中的流量。端口流控将影响所有的流量。

3.4.3 优先级标记

优先级标记特性用于为匹配访问控制列表的报文重新分配一套服务参数。优先级标记包括以下几种情况：

- 使用交换机自动分配的服务参数。
- 根据报文的 DSCP（Differentiated Services CodePoint Priority）值查找映射表为报文重新分配服务参数。

- 根据用户设定的 DSCP 值查找映射表为报文重新分配服务参数。

3.4.4 队列调度

队列调度用于解决在以太网交换机进行转发报文时解决多个报文同时竞争使用资源的问题。S9300 系列交换机支持以下调度算法：

- SP（Strict-Priority，严格优先级队列）
- WRR（Weighted Round Robin，加权轮询优先级队列）
- SP + WRR
- DRR（Deficit Round Robin）
- SP + DRR

这些算法根据自己的原则处理以太网交换机端口上各个输出队列中的报文转发问题。

3.4.5 拥塞避免

当拥塞发生时，交换机会尽快的丢包释放队列资源，同时尽量不将报文放入高延迟的队列中，以消除拥塞。

S9300 支持 WRED（Weighted Random Early Detection）丢弃算法：WRED 监视各队列中的报文，将队列长度和阈值进行比较，并在拥塞发生时根据如下比较结果来处理队列中的报文。

- 当队列的长度小于低阈值时，不丢弃报文；
- 当队列的长度在低阈值和高阈值之间时，WRED 开始按照丢弃概率随机丢弃报文；
- 当队列的长度大于高阈值时，丢弃所有的报文。

3.4.6 流量整形

流量整形是对输出报文的速率进行控制，使报文以均匀的速率发送出去。

流量整形通常是为了使报文速率与下游设备相匹配，以避免不必要的报文丢弃和拥塞。它和流量监管的主要区别在于流量整形是缓存超过速率限制的报文，使报文以均匀的速率发送出去，而流量监管则是丢弃超过流量速率限制的报文。

但是流量整形会增加延迟，而流量监管不会引入额外的延迟。

S9300 支持分别对端口、COS（Class of Service）、VLAN 进行流量整形，即对端口、COS、VLAN 的所有的流量进行流量整形。可以通过选取不同的参数实现这两种流量整形操作。

3.5 可靠性特性

S9300 支持的可靠性特性有：链路汇聚、BFD、Ethernet OAM、RRPP 多实例、Smart Link 和设备级可靠性。

3.5.1 链路汇聚

S9300 不仅支持手工方式将多个端口捆绑成一个 Eth-Trunk，而且支持静态模式链路汇聚，即由管理员创建聚合组并加入成员链路，并由 LACP 协议负责维护聚合链路。

当聚合链路中一条链路发生故障时，故障链路上的流量会自动分担到其他链路上，从而保证了业务传输不被中断。S9300 支持不同 LPU 上的链路之间形成聚合，从而使业务可靠性进一步增强。

3.5.2 DLDP

S9300 支持 DLDP 协议。DLDP（Device Link Detection Protocol）可以监控光纤或铜质双绞线的链路状态。如果发现单向链路存在，DLDP 会根据用户配置，自动关闭或通知用户手工关闭相关端口，以防止网络问题的发生。

3.5.3 RRPP 及多实例技术

为了缩短收敛时间，消除网络尺寸对收敛速度的影响，华为公司开发了 RRPP（Rapid Ring Protection Protocol）协议，RRPP 是专门应用于以太网环的链路层协议。

它在以太网环完整时能够防止数据环路引起的广播风暴，而当以太网环上一条链路断开时能迅速启用备份链路以恢复环网上各个节点之间的通信通路。

相比其他以太环网技术，RRPP 具有以下优势：

- 拓扑收敛速度快，低于 50ms。
- 收敛时间与环网上节点数无关，可应用于网络直径较大的网络。
- 在以太网环完整时能够防止数据环路引起的广播风暴。
- 当以太网环上一条链路断开时能迅速启用备份链路以恢复环网上各个节点之间的通信通路。

RRPP 在相交环拓扑中，一个环拓扑的变化不会引起其他环的拓扑振荡，数据传输更为稳定。

RRPP 多实例技术，提供在环形以太网组网中，依据不同的用户 VLAN 划分不同的 RRPP 实例，进行独立的拓扑计算和收敛，对于利用全双工的以太网分别实现内环和外环双向流量的负载分担有非常重要的实用价值，同时利用多实例技术，在复杂拓扑，如多相交环、多环多域等逻辑拓扑的应用中，也可以起到优化网络、简化配置的目的。

3.5.4 Smart Link 及多实例技术

双上行组网是目前常用组网之一。一般情况下，通过开启 STP（Spanning Tree Protocol，生成树协议）来实现网络中的链路冗余备份，但 STP 不适用于对收敛时间有很高要求的用户。

Smart Link 功能可以满足用户对链路快速收敛的需求，可以实现主备链路的冗余备份及其快速迁移。在双上行组网环境下，当主用链路出现故障时，设备自动将流量切换到备用链路，这样就起到了冗余阻塞和链路备份的作用。

Smart Link 的主要特点是：专用于双上行组网；收敛速度快（达到亚秒级）；配置简单，便于用户操作。

Smart Link 多实例是指在一个 Smart Link 组中可配置多个实例，不同的实例绑定不同的 VLAN 范围。可以通过命令指定其中一部分实例通过备用链路发送，这样就能实现不同 VLAN 的数据流量的转发路径不同，从而达到负载分担的目的。

3.5.5 以太网 OAM

S9300 上支持的以太网 OAM 功能包括故障管理、性能管理两大部分。

点到点以太网故障管理

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 TraceRoute 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，从而实现业务中断<50ms 的质量目标。

IEEE 802.3 ah 最初是由 EFMA(第一英里以太网联盟)提出的，包括能力发现、链路性能监测、故障侦测和告警、环路测试。同时 802.3ah 还可以检测以太网直连链路上的故障，尤其是运营商接入用户链路上的故障。802.3ah 是一种慢协议，故障定时检测报文发送频率为 1s。

S9300 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，S9300 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。

端到端以太网故障管理

IEEE 802.1ag 用于虚拟桥接局域网中的桥设备（VLAN 感知）提供对网络进行故障检测、确认以及隔离的能力。可以实现小于 50ms 故障检测。故障管理可用于触发保护倒换，从而实现业务的中断小于 50ms 的质量目标。802.1ag 提供的传输故障管理功能包括如下特性：

- 支持故障检测功能(CC)
- 支持故障确认功能(Loopback)
- 支持故障定位和隔离功能(Traceroute route)
- 支持故障通知和告警抑制功能(AIS/RDI) （AIS 功能暂不支持）

S9300 遵循 IEEE 802.1ag 提供端到端以太网故障管理。

- 分级 MD

  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 机制的网络称为 MD（Maintenance Domain），一个 MD 就是由多台 S9300 设备互相连接组成的一个 MST（Multiple Spanning Tree）域。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，连接 CE（Customer Equipment）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 TraceRoute 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 TraceRoute

    基于 LT 报文实现的 MAC TraceRoute 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 TraceRoute 的约束条件和 MAC Ping 功能的要求相同。

以太网性能管理

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。

S9300 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。

3.5.6 BFD

S9300 提供 BFD 机制来实现双向转发检测，从而可以快速检测、监控网络中链路的连通状况。

BFD 通过简单的“Hello”协议，实现转发链路故障的快速检测。在设备之间的通道上周期性的发送检测报文，如果 S9300 在足够长的时间内没有收到对端的检测报文，则认为在这条到相邻设备的双向通道的某个部分发生了故障。这时，BFD 便可以触发相应倒换机制，保证网络的可靠。

S9300 的 BFD 机制提供异步检测模式，能实现毫秒级别的链路缺陷检测。

S9300 支持以下 4 种 BFD 检测：

- 物理链路检测。

- IP 连通性检测。
- LSP、CR-LSP 和 MPLS TE 保护组的连通性检测。
- VPLS 网络中进行 BFD 检测。

  支持基于 VPLS 的 BFD 检测和管理 VPLS 倒换的诊断码报文的处理以及倒换处理。

S9300 的 BFD 还支持与 802.3ad、802.1ag 之间的联动，实现端到端的 OAM。

3.5.7 LSP 保护倒换

S9300 支持 MPLS OAM 技术，可以快速检测 LSP 的故障。通过为主 LSP 指定备用 LSP，形成一对保护组，可以实现 LSP 的 1+1 备份。当主隧道发生故障时，业务能迅速地切换到备用隧道上，从而有效地提高网络的可靠性。

3.5.8 设备级可靠性

部件热备份

S9300 的 SRU/MCU、电源模块、风扇等关键部件都支持冗余备份。

- SRU/MCU

  S9300 可以配置两块 SRU/MCU，支持 1+1 主备配置。
- 两块 SRU/MCU 工作在 1+1 备份方式，支持两种倒换方式：
  - 自动倒换方式

    主用 SRU/MCU 发生严重故障或主用 SRU/MCU 复位时，系统自动触发倒换。
  - 强制倒换方式

    用户通过控制台命令触发倒换。用户也可以通过控制台命令强行禁止 SRU/MCU 的主备倒换。

  发生主备倒换后，备用 SRU/MCU 快速承担原主用 SRU/MCU 的全部工作，保证业务的连续性，提高系统的可用性。
- 电源模块

  S9300 系统电源可以配置 4 个交流电源模块或两个直流电源模块，工作在冗余备份模式。

  当主备电源模块正确插入并上电时，同时提供 S9300 所需要的电力。如果一个电源模块出现故障，另一个电源快速承担全部工作，可以确保业务不中断，提高系统的可用性。

  PoE 电源仅支持交流电源模块，S9303 不支持 PoE 电源备份，S9306、S9312 支持 PoE 电源 M+N 备份。
- 风扇

  S9300 产品每个风扇框使用双层风扇备份方案实现系统冗余备份，满足产品任何一个风扇发生故障的情况下，仍能支持产品单插框应用最高环境温度到 45℃，机柜内应用最高支持到 40℃的环境温度下，短期 96 小时正常工作。

  在风扇出现故障后系统会产生告警信息并告知用户及时更换。

部件热插拔

S9300 的 SRU、MCU、LPU、CMU、电源模块和风扇框都支持热插拔。

警告

FSUA 不支持热插拔。

- 支持 SRU、MCU 的热插拔

  当 S9300 上安装了两块 SRU/MCU，如果工作在 1 ＋ 1 主备模式，则热插拔备用 SRU/MCU 后不影响业务传输，插拔主用 SRU/MCU 后备用 SRU/MCU 将快速倒换，业务平滑过渡。SRU 数据交换单元支持 1:1 负荷分担模式，如果工作在这种模式下，则热插拔 SRU 后，数据交换容量减半。
- 支持 LPU 的热插拔
- 支持电源模块热插拔

  当 S9300 上配置了 4 个电源模块且都正常工作时，插拔其中的 1 或者 2 个电源模块不会中断业务。
- 支持风扇框的热插拔

  风扇框的热插拔不会影响 S9300 的业务。
- 支持防尘网的插拔

  防尘网无需供电，可根据需要随时插拔，不影响 S9300 的运行，方便随时清洁。

以太网端口跨板 Trunk

S9300 支持多个以太网端口捆绑成 Eth-Trunk 接口，这些以太网端口既可以分布在同一块 LPU 上，也可以分布在不同的 LPU 上。

如果 Eth-Trunk 中有多个以太网端口处于正常工作的状态，当某个以太网端口出现故障时，整个 Eth-Trunk 仍能够正常工作。故障端口上的业务将会自动分担到 Eth-Trunk 内其他端口上，业务传输不受影响。

由于被捆绑的以太网端口可以分属于不同的 LPU，因此跨板的 Eth-Trunk 降低了单块 LPU 的故障对整个 Eth-Trunk 接口的影响。

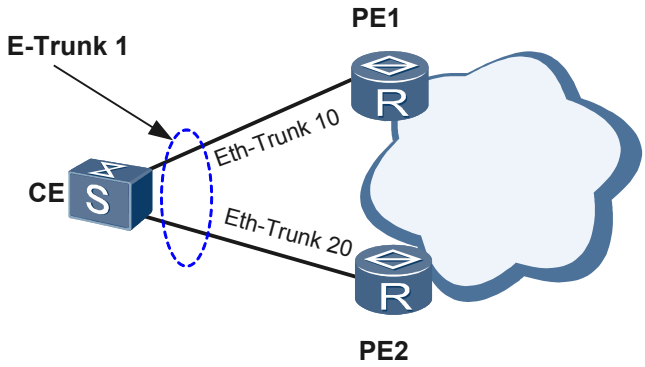
以太网端口跨设备 E-Trunk

E-Trunk（Enhanced Trunk）是一种实现跨设备链路聚合的控制协议，基于 LACP（单台设备链路聚合的标准）进行了扩展，能够实现多台设备间的链路聚合。从而把链路可靠性从单板级提高到了设备级。

E-Trunk 控制协议主要应用于 CE 双归接入 VPLS、VLL、PWE3 网络时，CE 与 PE 间的链路保护以及对 PE 设备节点故障的保护。在没有使用 E-Trunk 前，CE 通过 Eth-Trunk 链路只能单归到一个 PE 设备。

如果 Eth-Trunk 出现故障或者 PE 设备故障，CE 将无法与 PE 设备继续进行通信。使用 E-Trunk 后，CE 可以双归到 PE 上,从而实现设备间保护。

图 3-6 NetStream 组网图



堆叠

随着数据中心数据访问量的逐渐增大以及网络可靠性要求越来越高，单台交换机已经无法满足数据中心大数据量访问的要求；为了满足数据中心大数据量转发的需求和网络高可靠性需求，就提出了交换机堆叠。

S9300 支持 CSS（Cluster Switch System）系统，将几台交换机通过专用的堆叠电缆连接起来，对外呈现为一台逻辑交换机。

堆叠特性给运营商带来了明显的收益：

- 扩容网络时，保护已有投资。
- 扩容的同时，简化配置、管理：将多台物理设备虚拟为一台设备。
- 多台设备间冗余、备份，提高系统的可靠性。

硬件异常保护

S9300 上支持如下硬件异常保护措施：

- 对于内存芯片故障提供纠错功能。
- 电源输入接口具有防止误插和反插的功能。
- 系统每个风扇框有自己独立的供电通道，任意风扇框的故障不相互影响。
- 电源和业务接口提供过流和过压保护。
- 提供单板防误插保护。
- 提供电源、电压和环境温度的监测、告警功能。

操作中的保护

S9300 支持以下保护措施：

- 支持在线升级 BOOTROM、在线安装补丁、版本回退。
- 主备用单元间实现数据热备份。主用单元出现故障时，可以自动切换到备用单元，不会造成数据或信息的丢失。
- 各 LPU 和 SRU/MCU 之间及时同步配置信息。

- 提供 VRP 系统软件异常监视功能，能够自行恢复异常并保存相应记录。
- 提供临终遗言功能，记录系统在异常时的关键故障信息。

此外，S9300 还提供对不当操作的防护和提示。对于重要的、影响系统性能的命令，提示用户是否继续操作，操作的执行需要用户的进一步确认。

3.6 安全特性

S9300 不仅提供设备级安全，而且可以为传输的业务提供安全。

3.6.1 设备的安全

命令行分级保护

用户从以太网端口通过 Telnet 方式登录 S9300 时，出于安全性考虑，S9300 需要对登录用户进行验证。只有通过验证的用户才能成功登录，然后对 S9300 进行配置和维护操作。

S9300 的命令行采用分级保护方式，命令行划分为 4 个级别。登录用户也被划分为 4 个等级，分别与命令级别对应。不同级别的用户登录 S9300 后，只能使用等于或低于自己级别的命令，有效控制了登录用户的权限。

S9300 支持命令级别和用户级别的扩展（即级别映射），将 4 级映射到 16 级，从而实现了对用户级别的精细化管理。

此外，S9300 支持通过命令锁定当前配置终端，防止非法使用终端。

SSH 远程安全登录

S9300 支持 Version1.5 和 Version2 两个版本的 SSH（Secure Shell）。在不安全的网络环境中，SSH 为用户登录 S9300 提供了强大的安全保障和验证功能，可以防范多种攻击。

SNMP 加密认证

S9300 支持 SNMPv3 加密认证功能。当 S9300 在接受网管站 SNMP 管理时，可以通过 IP 地址来验证合法性。

AAA 身份验证

S9300 支持完善的 AAA（Authentication，Authorization and Accounting）机制，根据策略对接入用户进行认证、授权和计费：

- 本地认证
- RADIUS（Remote Authentication Dial-In User Service）认证
- HWTACACS（Huawei Terminal Access Controller Access Control System）认证

S9300 不仅可以配合命令行分级保护机制来对登录用户进行认证、授权，还可以在网络管理中对网管用户的合法性进行验证。基于 AAA 机制，S9300 可以有效防止非法用户登录。

层次化 CPU 通道保护

层次化 CPU 通过保护：2 级的 CPU 通道保护；

- 第一级，接口板保护：

  对于从接口板转发到 CPU 的协议报文和管理报文，S9300 根据协议类型对各类报文进行流量控制，从而避免 CPU 通道受到 DoS（Denial of Service）攻击而阻塞。
- 第二级，主控安全引擎保护：

  对于从接口板转发到 CPU 的协议报文和管理报文，进行详细分类识别、优先级处理，流量控制、白名单报文过滤、CPU 队列 QoS 调度，CPU 端口限速，阻塞防范各种 CPU 攻击，如 DDOS 攻击、IP spoof、 SYN FLOOD 等等。

3.6.2 业务的安全

通过 ACL 过滤报文

包过滤用于过滤那些用户不感兴趣或者不合法的报文。

S9300 对每个报文按照用户所定义的项目进行过滤，例如，比较报文的源地址、目的地址是否符合规则等。包过滤不检查会话的状态，也不分析数据。通过包过滤方法，S9300 可以有效控制通过设备的报文。

DHCP Snooping/Option82

S9300 可以部署在 DHCP 服务器和 DHCP 客户端之间，负责监听双方交互的 DHCP 报文，根据监听记录立 IP+MAC 绑定表，抑制非法报文。同时，S9300 还能为 DHCP 报文插入或剥离 Option82 选项。

- S9300 接收到来自 DHCP 客户端的请求报文后，会在该报文中插入 Option82 选项，DHCP 服务器通过识别 Option82 选项来执行 IP 地址分配策略。
- DHCP 服务器在响应报文中插入 Option82 选项，S9300 分析 Option82 选项并确定转发端口，然后剥离 Option82 选项后转发报文给用户。

由于 Option82 选项记录了用户电路 ID 编号，因此可以有效避免攻击者对 DHCP 报文的非法篡改。

IP Session 与之类似，根据报文的 VLAN 或 Option82 信息，对 IP+MAC+端口+VLAN 进行绑定检查，防止用户仿冒 IP 地址。

端口 MAC 地址学习限制

S9300 支持 MAC 地址学习限制，用于对 MAC 地址学习进行控制。

通过在 S9300 指定端口上配置 MAC 表项学习的最大数目，可以保护设备的 MAC 表项资源不被恶意用户大量占用，避免了恶意用户从该端口发起源 MAC 地址攻击。

S9300 支持三种方式对 MAC 地址数量进行限制：

- 基于端口
- 基于 VLAN
- 基于 VSI

当学习的 MAC 地址数量达到指定阈值时，对于后续新 MAC 地址的报文可以根据配置选择转发或丢弃动作。

黑洞 MAC 表项

S9300 支持黑洞 MAC 功能。S9300 接收到某报文后，会将该报文的目的 MAC 地址和 MAC 表中各项比较，如果和黑洞 MAC 表项相同则丢弃该报文。

当用户察觉到某 MAC 地址的报文具有一定攻击性，则可以在 S9300 上配置黑洞 MAC，从而将具有该 MAC 地址的报文过滤掉，避免遭受攻击。

基于 MAC ＋ VLANs 的端口绑定

为了提高端口安全性，S9300 可以支持网络管理员在 MAC 地址表中加入静态表项，记录特定 MAC 地址 VLAN 和端口的对应关系。这种查表方式可以将设备与端口绑定，防止 MAC 地址仿冒的攻击。

广播流量抑制

对于广播、组播和未知单播报文，S9300 可以基于端口进行速率限制。

S9300 还可以控制端口上的最大广播、组播、未知单播的流量百分比，从而控制广播报文的流量。

3.7 网络管理特性

S9300 提供 LLDP 和 NetStream 网络管理功能。

3.7.1 LLDP
介绍了 LLDP 的基本原理。

3.7.2 NetStream

3.7.1 LLDP

介绍了 LLDP 的基本原理。

S9300 支持遵循 IEEE 802.1ab 标准的 LLDP（Link Layer Discovery Protocol）。LLDP 是一种用来自动发现以太链路层邻接关系的协议，适用于互连设备之间获取对方的连接信息。

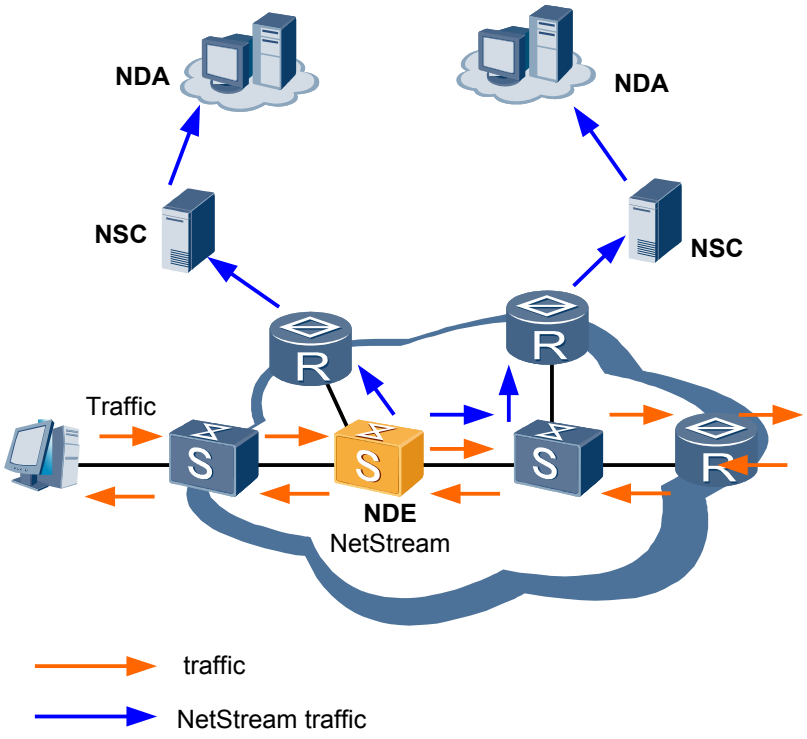
借助 LLDP，本地网管站可以清晰地得知本地网络中所有设备的链路层信息，可以掌握更详细的网络拓扑信息、变化信息，有效地扩大了网管范围。

启动 LLDP 功能的 S9300 上的每个端口定期向周边邻接设备通告本端口状态信息。如果状态发生改变，端口则向与它们直接连接的邻接设备发送状态更新信息。邻接设备会将状态信息存储在标准的 SNMP MIB 中，网管系统从 MIB 处查询出当前网络的链路层连接情况，从而据此计算出整个网络的拓扑。

3.7.2 NetStream

随着网络支持的业务和应用日渐增多，用户对流量统计分析提出了更高的要求。NetStream 给网络管理人员提供了从他们的数据网络访问“详细记录”信息的方法。

图 3-7 NetStream 组网图



NDE: Netstream Data Exporter NSC: Netstream Collector NDA: Netstream Data Analyzer

NetStream 数据可以有多种用途：

- 网络管理和规划
- 企业记帐和分部门的计费
- ISP 编制帐单
- 数据储备
- 用于商业目的的数据采集

在网络中，由于 IP 网络的非面向连接特性，网络中不同类型业务的通信可能是任意一台终端设备向另一台终端设备发送的一组 IP 数据包，这组数据包实际上就构成了网络中某种业务的一个数据流。绝大部分的数据流量都是短暂、阵发的双向数据流。

NetStream 主要根据一个报文的目的 IP 地址、源 IP 地址、目的端口号、源端口号、协议号、ToS（Type of Service）、输入/输出接口组成的 7 元组来区分不同的流。针对这些流做独立的数据统计。

NDE（Netstream Data Exporter）把获得的统计信息定期向 NSC（NetStream Collector）发送，由 NSC 进行进一步的处理，然后交给后续的 NDA（NetStream Data Analyzer）进行数据分析并形成报表，通过报表进行计费、网络规划等。

S9300 支持 NDE 功能，支持对 IPV4/IPV6/MPLS 报文采样，可以支持固定报文个数间隔采样和固定时间间隔采样。支持原始流、Flexible 流、聚合流的建立，支持 V5/V8/V9 统计报文格式。

S9300 既支持分布式 NetStream，又支持集中式 NetStream。

3.8 时钟特性

S9300 支持物理层时钟同步机制、IEEE 1588V2 时钟同步及时间校准机制，为移动通信业务提供高精度的时间信息。

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。S9300 支持从同步以太网链路中提取时钟信息。

IEEE 1588V2 是一种时间同步协议，精度可以达到微秒级，满足 3G 基站的要求。S9300 持 IEEE 1588V2 的以下特性：

- 支持采用 IEEE 1588V2 协议实现时钟定时同步和时间信息同步。
- 支持边界时钟模式、普通时钟模式、透传时钟模式（包括端到端透传时钟模式和点到点透传时钟模式）三种时钟模式，每个端口可以根据需要配置成不同的模式。
- 支持时钟源保护倒换。

3.9 PoE 特性

在企业网中，通过 10BASE-T、100BASE-TX、1000BASE-T 以太网网络供电，可以有效的解决 IP 电话、无线 AP、便携设备充电器、刷卡机、摄像头、数据采集等终端的集中式电源供电。

对于终端而言，不需要考虑其室内电源系统布线的问题，在接入网络的同时就可以实现对设备的供电。

按照 802.3af/802.3at 标准的定义，PoE 供电系统包含两种设备 PSE 和 PD。

对于 PSE 设备的定义如下：PSE（power-sourcing equipment），主要是用来给其他设备进行供电的设备，其又可以分为两种，分别为 Midspan（PoE 功能在交换机外）和 Endpoint（PoE 功能集成到交换机内）。IEEE 标准 802.3af/802.3at 允许 End-point 设备利用 4 对铜线中的 1/2 和 3/6 线对或 4/5 和 7/8 线对提供电源。End-point 模式 PSE 可兼容 10BASE-T、100 BASE-T、1000BASE-T 接口，应用场景较 Mid-Span 模式广泛。

S9300 属于 Endpoint 类型的 PSE 设备，符合 802.3af/802.3at 标准，每端口可提供 30W 供电能力。

S9300 支持每个端口（支持 PoE 的端口）提供 Critical、High、low 三种 PD 设备供电优先级。在 PD 设备消耗的功率大于 PSE 能够提供的总功率时，优先给端口优先级高的 PD 设备供电，如果不同端口的优先级一致，按照端口号进行优先级排序，端口号小的端口优先得到供电保证。

3.10 行业网特性

S9300 为行业网安全提供 NAC、防火墙、NAT 以及负载均衡功能。

3.10.1 NAC

3.10.2 防火墙

3.10.3 NAT

3.10.4 负载均衡

3.10.1 NAC

NAC（Network Admission Control）网络管理控制概念的提出，是为了防止病毒和蠕虫等新兴黑客技术对企业安全造成危害。借助 NAC，客户可以只允许合法的、值得信任的端点设备(例如 PC、服务器、PDA)接入网络，而不允许其它设备接入。

NAC 的主要组件有：

- 终端 Agent 软件
- 网络接入设备
- 策略/AAA 服务器
- 防病毒服务器
- 管理系统

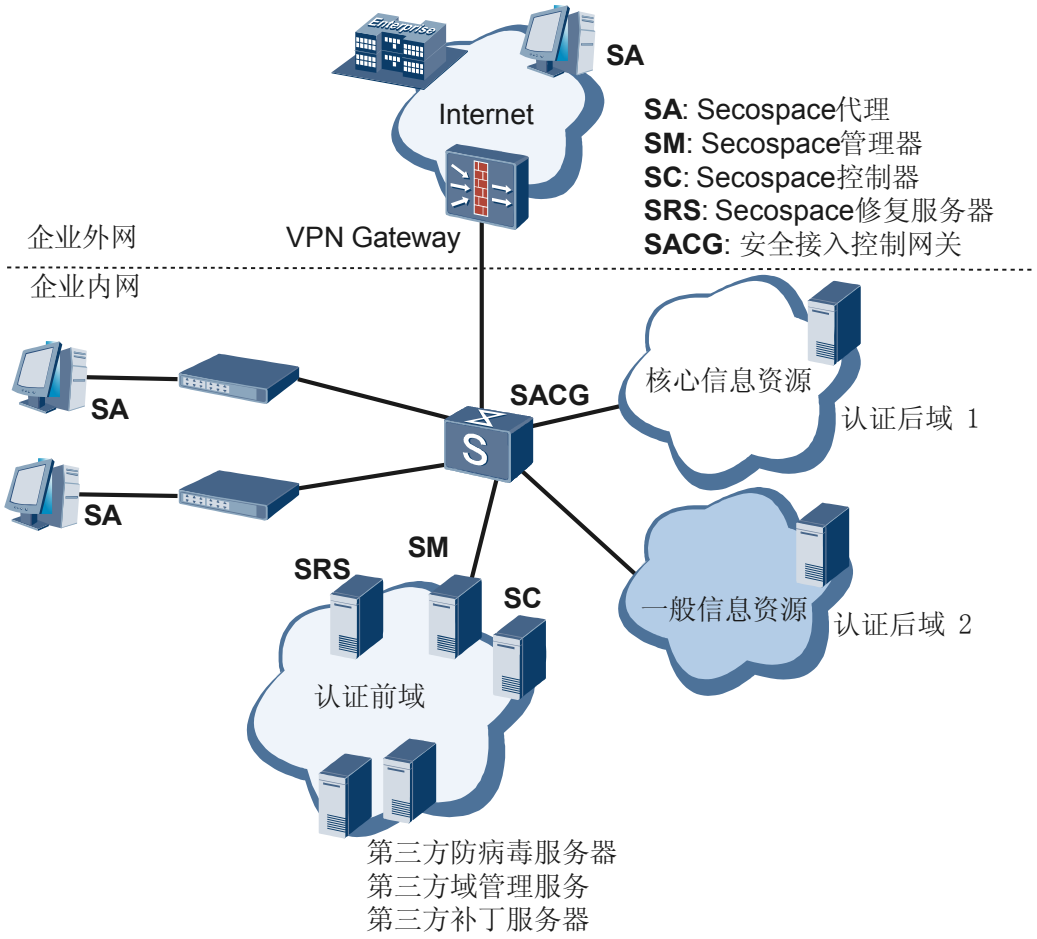
S9300 作为网络接入设备，提供以下功能：

- 基于 802.1X 的接入（端口模式和 MAC 模式）；
- Portal 接入；
- 通过 DHCP Snooping 获取到用户表项的透传认证方式。

此外支持常见的几种特殊的应用场景：

- 逃生功能，RADIUS 服务器 DOWN 的情况下允许用户访问网络）；
- 特权用户以及无 Agent 的设备（打印机/IP 电话机）。

图 3-8 NAC 的主要组件及组网图



3.10.2 防火墙

S9300 提供 10G 处理性能的分布式防火墙，旨在满足大型企业、运营商和数据中心网络高性能的安全防护。支持外部攻击防范、内网安全、流量监控、邮件过滤、网页过滤、应用层过滤等功能，能够有效的保证网络的安全。

S9300 防火墙功能包括以下特性

- 包过滤防火墙
- 状态防火墙
- ASPF（Application Specific Packet Filter）
- 黑名单
- 白名单
- 端口映射
- 攻击防范
- 流量统计及监控
- 防火墙日志

- 虚拟防火墙

S9300 防火墙支持双机热备份，在 Master 和 Backup 防火墙之间进行了实时备份会话表和状态信息。Master 防火墙出现故障时能由 Backup 防火墙平滑地接替工作。

3.10.3 NAT

S9300 为企业提供多对一、多对多、静态网段、双向转换、DNS 映射等 NAT 应用方式。支持多种应用协议正确穿越 NAT，提供各种应用层的 NAT ALG 功能。

S9300 的 NAT 功能包括：

- NAT 地址池
- NAPT（Network Address Port Translation）
- 静态 NAT/NAPT
- Easy IP
- NAT Server
- Twice NAT
- VPN 关联的源 NAT
- VPN 关联的 NAT Server
- NAT ALG

3.10.4 负载均衡

S9300 提供了完全的第 4 ～ 7 层服务器负载均衡功能，可支持多个应用和服务器集群的部署。

S9300 支持如下的负载均衡算法：

- 轮询
- 基于最小连接数
- 基于最小带宽
- 基于负载情况
- 基于响应时间
- 基于报文源 IP 地址
- 基于报文目的 IP 地址
- 基于报文源和目的 IP 地址
- 基于报文四层内容
- 基于 HTTP 报文的 URL
- 基于 HTTP 报文的 Header
- Cookie 和内容

3.11 MPLS & VPN 特性

通过 S9300 产品构建 MPLS 网络时，MPLS 网络外部仍旧根据 VLAN 和 MAC 地址进行交换，而 MPLS 网络内各设备依据 MPLS 标签进行交换，从而有效缓解了 VLAN Tag 标签容量瓶颈和 MAC 地址表容量限制的问题。

说明

如果需要使用 MPLS 功能，请联系华为公司购买 License。

S9300 既可以作为 MPLS 网络中的 PE（Provider Edge）设备，也可以作为 P（Provider）设备。

S9300 支持丰富的 MPLS 特性，包含 MPLS 的基本功能、LDP/RSVP-TE 协议、MPLS TE、MPLS OAM 等。

3.11.1 MPLS 基本功能

S9300 支持的 MPLS 基本功能包含：

- 支持 LDP
- 支持静态 LSP
- 支持两层 MPLS 标签
- 支持 802.1p 优先级到 MPLS 报文 EXP 字段的映射

3.11.2 MPLS TE

S9300 支持丰富的 MPLS TE（Traffic Engineering）功能。S9300 通过 MPLS TE，将流量工程同 MPLS 技术相结合，可以建立指定路径的 LSP 隧道，并且可以进行定时优化。同时，还可以通过备份路径和快速重路由技术，在链路或节点失败的情况下，提供保护。

S9300 支持以下 MPLS TE 特性：

- 支持基于 IGP (Internal Gateway Protocol) 协议（IS-IS、OSPF）的 TE 扩展，实现网络信息的收集。
- 支持 CR-LSP 的抢占，路由锁定和重优化功能。
- 支持采用 RSVP TE 协议建立 CR-LSP，支持 MPLS TE 隧道的 Hotstandby 备份和普通备份。
- 支持使用 CSPF（Constraint Shortest Path First）计算 CR-LSP 的路径，实现基于 CSPF 计算出到达某个节点的最短路径。
- 支持 MPLS TE 隧道的建立，同时支持隧道相关的以下特性：
  - 支持 MPLS TE 隧道的环路检测功能
  - 支持记录路由和标签
  - 支持 MPLS TE 隧道重建

- 隧道优先级配置功能

3.11.3 MPLS OAM

为了在 LSP 链路出现缺陷或故障时迅速进行链路倒换，S9300 支持 MPLS OAM（Operation Administration & Maintenance）机制，提供 50ms 保护倒换，实现端到端的故障检测和保护。MPLS OAM 及保护倒换遵循 ITU-T 的 Y.1710、Y.1711 和 Y.1720 系列标准，支持 LSP 连通性检测和快速连通性检测，连通性检测报文的发送间隔可以根据需要进行调整。

使用这种 MPLS OAM 机制，借助 CV（Connectivity Verification）消息和 FFD（Fast Failure Detection）消息可以有效地检测、确认并定位出 MPLS 网络内部的缺陷；报告缺陷并做出相应的处理；在出现故障的时候，借助 FDI（Forward Defect Indicator）消息和 BDI（Backward Defect Indicator）消息触发保护倒换。

目前，S9300 支持 LSP 的 1:1 和 N:1 保护倒换，主 LSP 隧道和备用 LSP 隧道构成一对保护组。当主隧道发生故障时，业务能迅速地切换到备用隧道上，从而有效地提高网络的可靠性。

3.11.4 VLL

VLL 是对传统租用线业务的仿真，使用 IP 网络模拟租用线，提供非对称、低成本的点到点的虚拟专线业务，主要应用在城域网的接入层和汇聚层。

S9300 支持 4 种方式的 VLL：

- Martini

  Martini 方式使用两层标签，内层标签采用扩展的 LDP 作为信令进行交互。这种方式遵循草案 draft-martini-l2circuit-trans-mpls，在 Martini 草案中对标准的 LDP 进行了扩展，增加了 FEC 类型（VC FEC）用于 VC 标签的交换。

- Kompella

  Kompella 方式使用 MP-BGP 作为交换信令。各个 PE 之间通过建立 BGP (Border Gateway Protocol) 会话自动发现 L2VPN 的各个节点，使用 BGP 作为传递二层信息和 VC 标签的信令协议，在 MPLS 网络上以端到端（CE 到 CE）方式实现 L2VPN。

- SVC

  SVC 的外层标签（公网隧道）建立的方法与 Martini 相同。内层标签在配置 VC 的时候进行手工指定，不需要使用 VC 标签的传递信令。所以 SVC 的网络拓扑模型与报文交互过程与 Martini 完全相同，可以认为 SVC 是 Martini 的简化。

- CCC

  与 SVC 类似，CCC 方式是一种静态配置 VC 连接的方式。与普通 MPLS L2VPN 不同，CCC 采用一层标签传送用户数据，这一层标签在每个 LSR 上进行标签交换。因此 CCC 对 LSP 的使用是独占性的，而且在两个方向都需要配置静态的 LSP。

3.11.5 VPLS

VPLS 技术主要是借助 PSN（Packet Switched Network）网络来连接多个以太网，使它们工作起来时类似于一个局域网。利用 VPLS 技术，ISP（Internet Service Provider）可以在分散用户（例如分散在多个城市办公的企业）间建立多点到多点的 VPN 连接。

S9300 作为 VPLS 网络的 PE 设备，可以通过在所有 PE 之间建立全连接来实现 VPLS 业务。

S9300 支持两种方式的 VPLS：

- Martini
- Kompella

3.11.6 HVPLS

由于 VPLS 要求 PE 之间建立全连接，因此当 VPLS 网络比较大时（节点多或地理范围大），需要建立的连接的数量成 PE 数量的平方级数增加，此时可以采用 HVPLS 来组建大型的 VPLS 网络。

S9300 在 HVPLS 网络中主要作为 UPE（User Provider Edge）设备，接入来自 CE 的业务，并将其汇聚到 NPE（Network Provider Edge）。或 PE-AGG 上 (PE-Aggregation)。

S9300 支持 Martini 方式的 HVPLS。

部署 VPLS（或 HVPLS）网络后，S9300 将不同类型的业务加入不同的 VSI（Virtual Switch Instance），并通过 VPLS 网络透明传输到 NPE 或 PE-AGG 上。

3.11.7 MPLS L3VPN

BGP/MPLS IP VPN 提供基于 MPLS 网络的三层 VPN 服务。通过 MPLS（Multiprotocol Label Switching）技术可以非常容易地实现基于 IP 技术的 VPN 业务，而且可以满足 VPN 可扩展性和管理的需求。

利用 MPLS 构造的 VPN，还提供了实现增值业务的可能；通过配置，可将单一接入点形成多种 VPN，每种 VPN 代表不同的业务，使网络能以灵活方式传送不同类型的业务。

4 应用场景

关于本章

介绍了 S9300 典型组网，以及 S9300 网络中的部署方案。

4.1 概述
介绍了 S9300 城域网的应用位置。

4.2 MPLS L2VPN 应用
介绍了 S9300VLL 和 VPLS 中的应用。

4.3 利用 HVPLS 实现双归属的保护
S9300 可以利用 HVPLS 组网以实现到两个 NPE 的双归属保护，在组建 HVPLS 网络时，S9300 作为 UPE 设备，负责接入 CE 的业务，也可以作为 PE-AGG，进行 UPE 的汇聚。

4.4 利用 RRPP 实现环网的快速保护
介绍了 S9300 用 RRPP 实现环网的快速保护。

4.5 利用 Smart link 实现双归属的保护
介绍了 S9300 用 Smart link 实现双归属的包含。

4.6 Ethernet OAM 应用
介绍了 S9300 城域网内提供以太网 OAM 特性和部署策略。

4.7 QoS 应用
介绍了 S9300 城域网内提供 QoS 的组网和部署策略。

4.8 灵活 QinQ 应用
介绍了 S9300 城域网内提供灵活 QinQ 功能的组网和部署策略。

4.9 IPTV 业务应用
介绍了 S9300 城域网中提供 IPTV 业务的组网和策略。

4.10 NAC 组网应用
介绍了 S9300 在 NAC 组网中的应用。

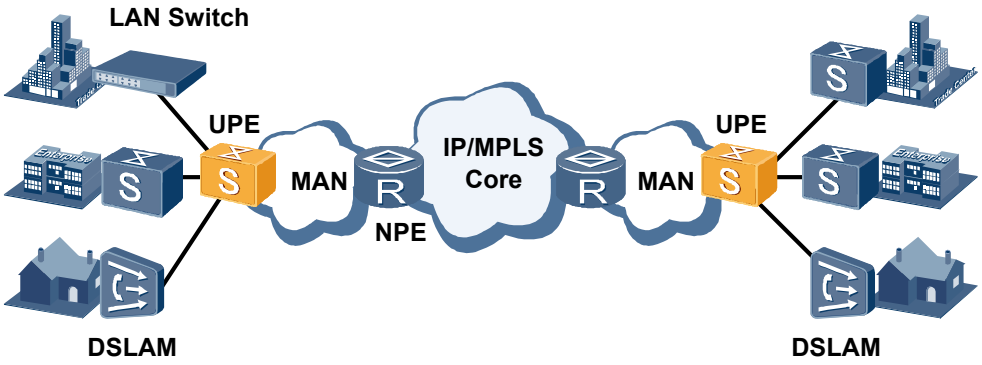
4.11 防火墙组网应用
介绍了 S9300 的防火墙组网和策略。

4.1 概述

介绍了 S9300 城域网的应用位置。

如图 4-1 所示，S9300 定位于城域网的接入层和汇聚层，负责用户业务的接入和汇聚。

图 4-1 S9300 在城域网中的位置



S9300 作为城域网的 UPE，下行可以接入来自 S2300、S3300 等 LAN Switch 和 DSLAM 的 Internet、VPN、IPTV、VoIP 等业务。

S9300 上行可以汇聚到 NPE 设备，例如采用华为公司的 ME60 和 NE40E。如果网络复杂，S9300 可以作为 PE-AGG，实现多级的汇聚。

4.2 MPLS L2VPN 应用

介绍了 S9300VLL 和 VPLS 中的应用。

S9300 具有强大的 MPLS VPN 能力。整机支持 4K 的 VLL PW 和 1K 的 VPLS 实例。

如图 4-2 和图 4-3 所示，S9300 在 L2VPN 网络中作为 UPE，支持 VLL 和 VPLS，提供了点到点的 VPN 应用和多点到多点的 VPN 应用。

图 4-2 点到点的 VPN 应用（VLL）

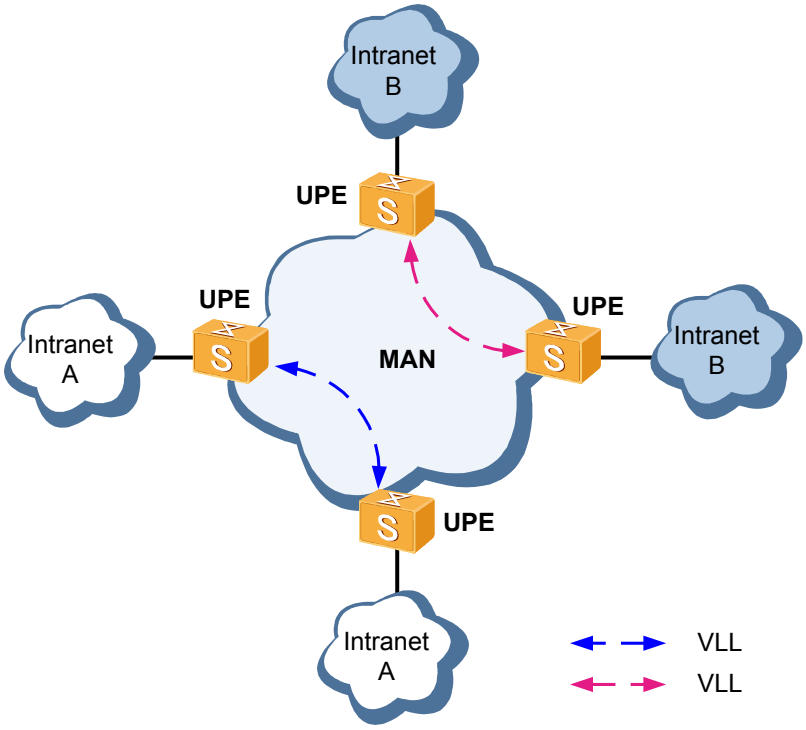
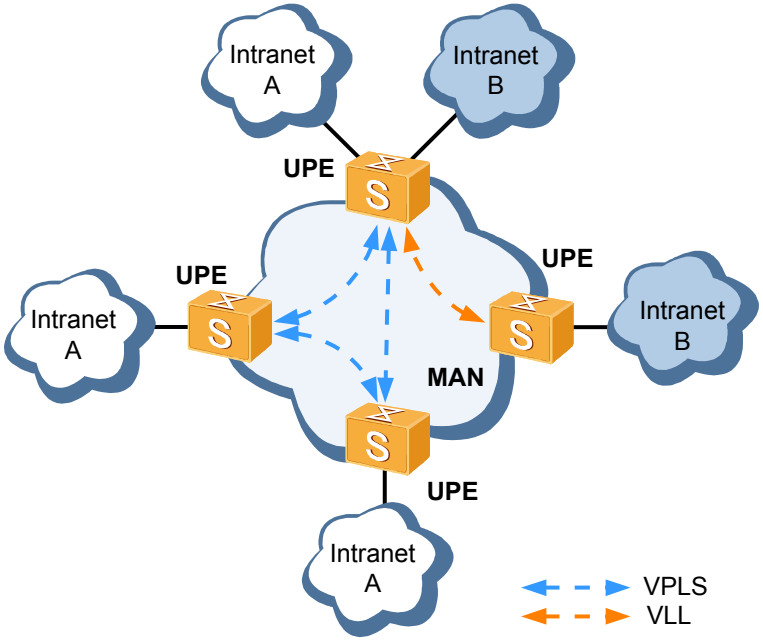


图 4-3 多点到多点的 VPN 应用（VPLS)

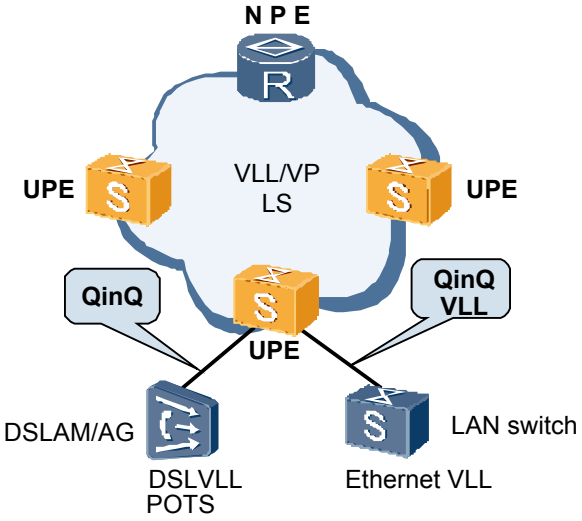


如图 4-4 所示，S9300 作为 UPE 与 DSLAM、AG (Access Gateway)、低端交换机等设备配合，实现了接入业务到 VLL 或者 VPLS 的映射。

- S9300 与 DSLAM/AG 配合，将 QinQ 隧道映射到 VLL 或者 VPLS 业务实例，实现基于 DSL 的专线业务。
- S9300 与低端交换机配合，将 QinQ 隧道和 VLL 隧道映射到 VLL 或者 VPLS 业务实例。

S9300 可以将某一类个人业务，例如宽带上网、VoIP 业务映射到 VLL 或者 VPLS 业务实例，实现接入汇聚层的多业务承载。

图 4-4 S9300 和 CE 设备配合实现 VPN 业务



S9300 低成本的 VLL 或者 VPLS 解决方案，把 MPLS 和 MPLS VPN 推向边缘汇聚层，解决了纯以太网方案存在的扩展性、电信级可靠性和可管理性问题。同时也减轻了更高层次的 NPE 的负担，解决了其负荷过重和单点故障问题。业务起点推向边缘汇聚层实现了业务分布式处理，使得为用户提供个性化业务成为可能。

4.3 利用 HVPLS 实现双归属的保护

S9300 可以利用 HVPLS 组网以实现到两个 NPE 的双归属保护，在组建 HVPLS 网络时，S9300 作为 UPE 设备，负责接入 CE 的业务，也可以作为 PE-AGG，进行 UPE 的汇聚。

S9300 在组建 HVPLS 网络时，支持两种网络结构：

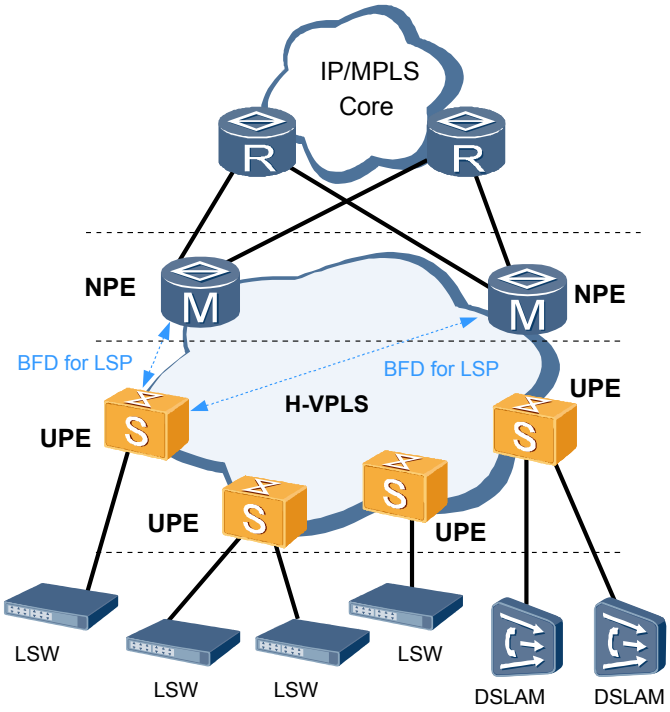
- 网络结构为 UPE+NPE
- 网络结构为 UPE+PE-AGG+NPE

4.3.1 网络结构为 UPE+NPE

4.3.2 网络结构为 UPE+PE-AGG+NPE

4.3.1 网络结构为 UPE+NPE

图 4-5 网络结构为 UPE+NPE 时 S9300 在 HVPLS 网络中的应用



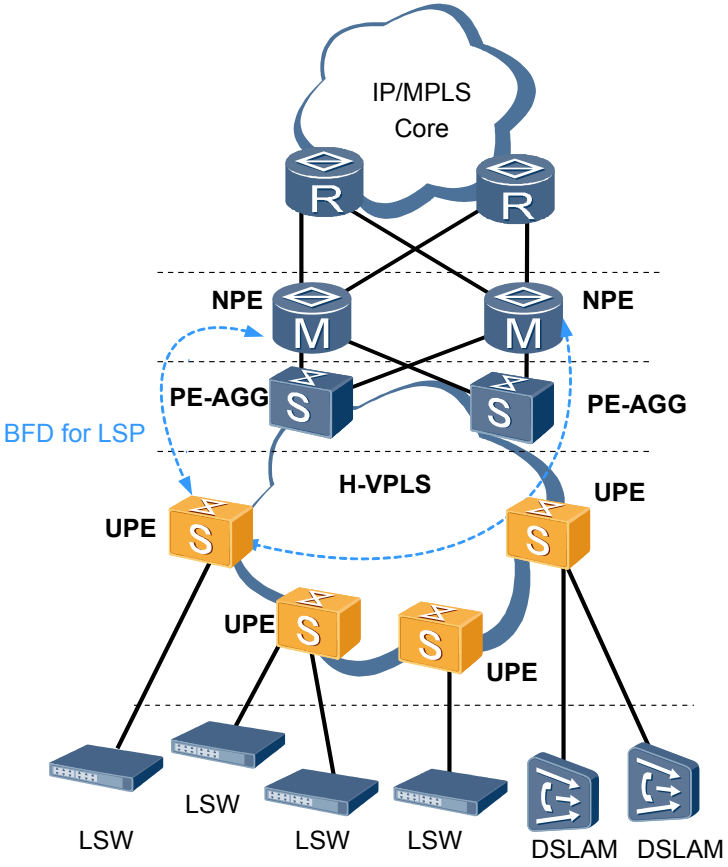
在如图 4-5 所示的 HVPLS 网络中，S9300 作为 UPE 设备，而 NPE 设备可以采用华为公司的 ME60 和 NE40E。

- S9300 作为 UPE 设备，负责用户业务接入，通过灵活 QinQ 对用户业务进行分流，不同类型的业务进入不同的 VSI。然后 S9300 将用户业务通过 HVPLS 透明传输到 NPE（NetWork Provider Edge）设备。
- NPE 设备终结 PW（Pseudo Wire）管道并接入用户业务，根据 VLAN 和 QinQ 信息来处理不同的业务。
- HVPLS 网络中可以通过 MPLS TE 保护组结合 BFD for LSP 来实现链路保护。

4.3.2 网络结构为 UPE+PE-AGG+NPE

如图 4-6 所示，在已有业务网络的情况下，可以考虑在 UPE 和 NPE 之间增加一层 PE-AGG 设备。PE-AGG 用来汇聚 UPE 的业务，终结 VPLS 并将业务透明传输到 NPE。S9300 可以作为 UPE，也可以作为 PE-AGG 使用。

图 4-6 网络结构为 UPE+PE-AGG+NPE 时 S9300 在 HVPLS 网络的应用



在如图 4-6 所示的组网中：

- S9300 作为 UPE 时完成的功能与**网络结构为 UPE+NPE** 中的功能相同。
- UPE 作为 PE-AGG 时，终结 VPLS 管道，将用户业务透明传输到 NPE 设备。
- NPE 负责终结 VLAN 和 QinQ，并处理业务。
- 从作 UPE 的 S9300 到 NPE 设备之间可以通过 BFD for LSP 来实现链路保护。

4.4 利用 RRPP 实现环网的快速保护

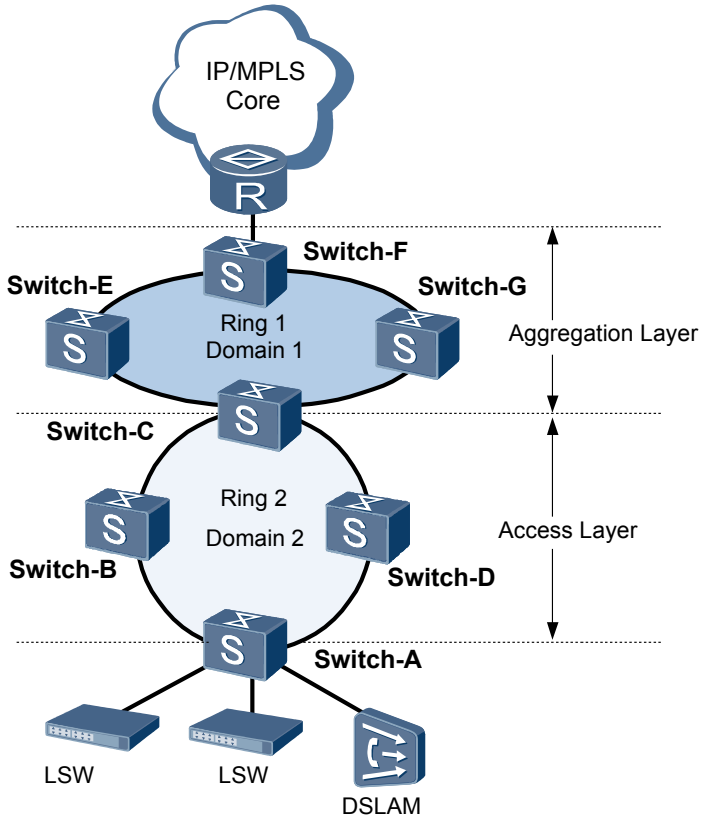
介绍了 S9300 用 RRPP 实现环网的快速保护。

在采用普通的以太环网进行组网的情况下，为了提高网络收敛速度，不部署 MSTP，而是采用 RRPP 来达到网络拓扑变化后的快速收敛。

城域以太网中主要采用两级环网架构：

- 一级为汇聚层，处于 PE-AGG 汇聚设备之间，如图 4-7 中的 RRPP Domain 1。
- 一级为接入层，处于 PE-AGG 与 UPE 之间，如图 4-7 中的 RRPP Domain 2。

图 4-7 RRPP 的应用（相切环）



如图 4-7 所示，Ring1 与 Ring2 分别属于 Domain1 和 Domain2，且相切于 Switch-C。其中：

- 在 Ring1 上，Switch-C 是主节点，Switch-C，Switch-E，Switch-F，Switch-G 是 PE-AGG 设备，
- 在 Ring2 上，Switch-C 是主节点，Switch-A，Switch-B，Switch-D 是 UPE 设备；

在多个相切的 RRPP 环中，当一个环出现故障时不会影响其它的域，本域内的 RRPP 环的状态收敛与单环收敛过程是一样的。

在 RRPP 环上，二层与三层业务都可以实现快速倒换：

- 二层业务快速倒换

  正常情况下，数据流经 Ring2 上的 Switch-A→Switch-B→Switch-C 节点。如果 Switch-A 和 Switch-B 之间的链路故障，数据流将改变在 RRPP 环上的路径。

  Switch-A 和 Switch-B 之间的链路故障，主节点收到链路故障通知，马上放开副端口。

  此时网络的拓扑已经改变，各节点原来的 MAC 表已经不能正确指导转发，二层流量将会中断。主节点在放开副端口后，立即通知环上的所有其他节点重新学习 MAC 表项，二层业务流量在 RRPP 环上的路径切换到 Switch-A→Switch-D→Switch-C。
- 三层业务的快速倒换

  正常情况下，数据流经 Ring1 上的 Switch-C→Switch-E→Switch-F 节点。如果 Switch-C 和 Switch-E 之间的链路故障，数据流将改变在 RRPP 环上的路径。

Switch-C 和 Switch-E 之间的链路故障，主节点收到链路故障通知，马上放开副端口。

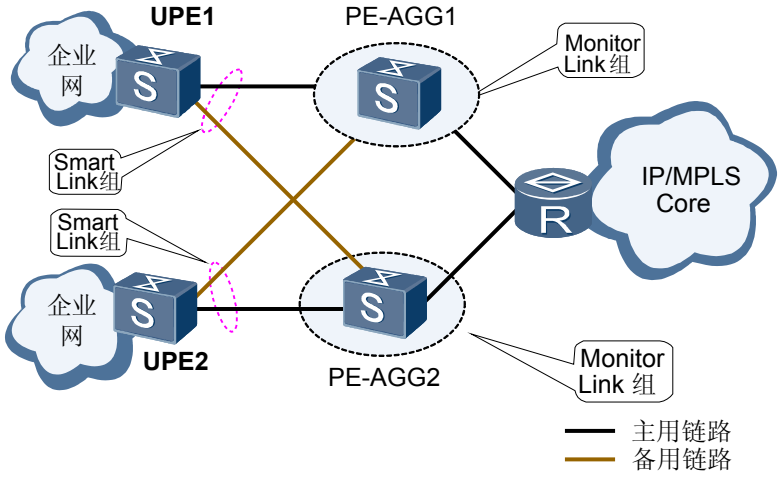
- 此时网络的拓扑已经改变，各节点原来的 ARP 及 FIB，已经不能正确指导三层转发。主节点在放开副端口后，立即通知环上的所有节点重新学习 ARP，实现三层业务流量在 RRPP 环上的路径切换到 Switch-C→Switch-G→Switch-F。

4.5 利用 Smart link 实现双归属的保护

介绍了 S9300 用 Smart link 实现双归属的包含。

在一般的以太双归属组网中，可以使用 Smart link 来进行链路的快速切换。

图 4-8 Smart link 典型组网应用



Smart Link 支持在城域网不同位置提供双归属上行连接。UPE1（或 UPE2）可以借助 Smart Link 双归属到 PE-AGG1 和 PE-AGG2。

例如，在 UPE1 和 UPE2 上配置 Smart Link 组，上游设备上只要能接收和发送 Flush 报文即可。此时，双上行链路中只有一条处于正常转发状态，另一条链路被冗余阻塞。当转发链路出现故障时，Smart Link 迅速感知并切换流量到备用链路。

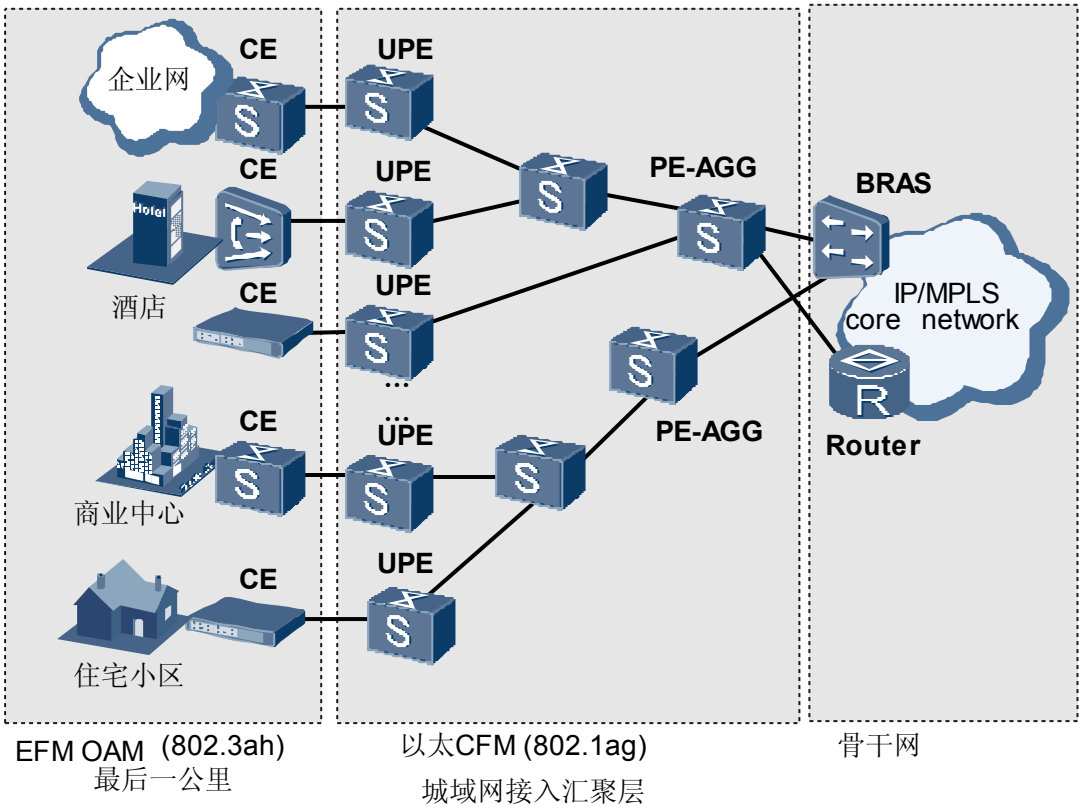
PE-AGG1 和 PE-AGG2 上提供 Monitor Link 组功能，实现了上行接口和下行接口之间的联动机制。

4.6 Ethernet OAM 应用

介绍了 S9300 城域网内提供以太网 OAM 特性和部署策略。

S9300 提供 Ethernet OAM 功能，可以实现小于 50ms 故障检测与保护倒换。

图 4-9 以太网 OAM 在城域网中的典型应用



在接入汇聚层网络中部署以太网 CFM(Connectivity Fault Management)。根据设备所属 ISP 划分 MD(Maintenance Domain)。将相同 ISP 管理的设备划分在同一个 MD 中。根据业务划分 MA(Maintenance Association)。每个 MA 对应一个 VLAN。通过同一 MA 内的 MEP(Maintenance association End Point)定时互发 CCM(Continuity Check Message)来检测 MA 内网络的连通性。当以太网 CFM 检测到连通性故障后，进行报警；并提供 MAC Ping、MAC Trace 进行故障确认和故障定位。

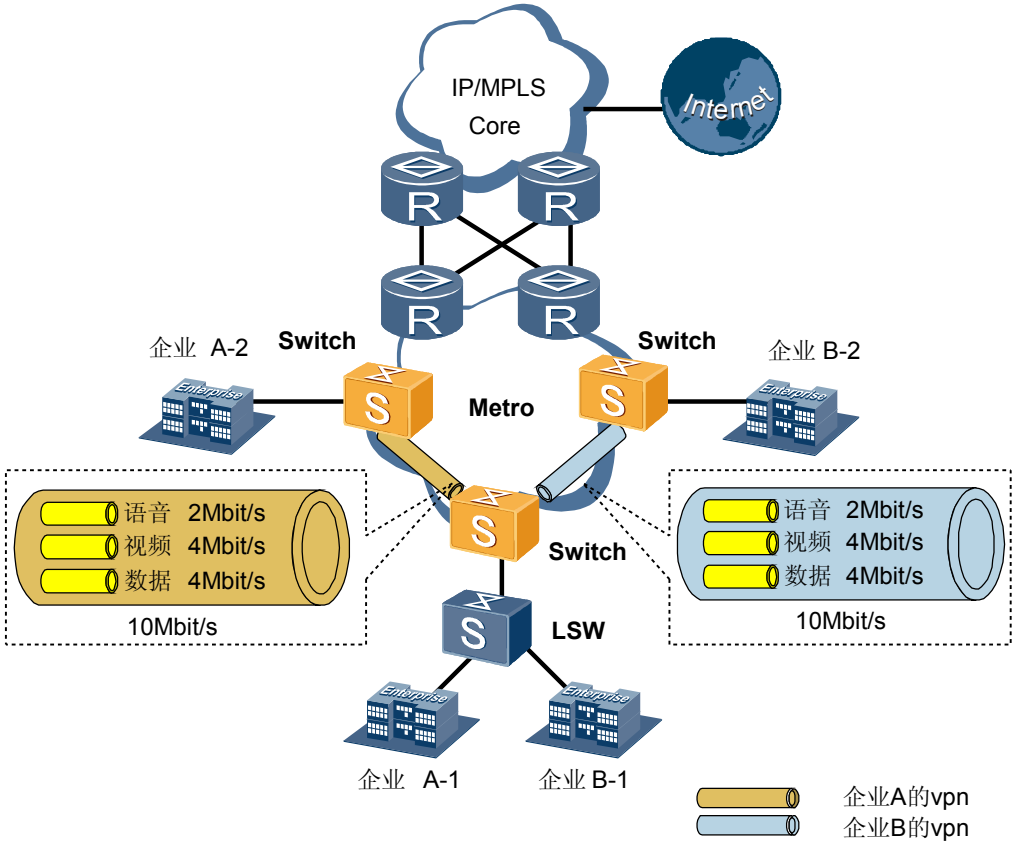
在 CE 设备和 UPE 设备之间的链路部署 EFM(Ethernet in the First Mile) OAM。通过 CE 设备和 UPE 设备之间定时互相发送 OAMPDU (OAM Protocol Data Unit)来检测用户业务接入链路的连通性。通过检测链路的误帧、误码和误帧秒来监测链路的性能，保证为用户提供符合 SLA 要求的传输服务,并提供故障报警功能。

4.7 QoS 应用

介绍了 S9300 城域网内提供 QoS 的组网和部署策略。

在如图 4-10 所示的网络中，企业 A 和企业 B 各有两个分部，称为企业 A-1、企业 A-2、企业 B-1 和企业 B-2。同一企业的各分部之间有专线业务需求，用于承载语音、视频和数据业务。图中 S9300 以 Switch 表示。

图 4-10 S9300 在 QoS 中的应用



企业 A 具体的需求如下。

- 企业 A 两地之间的专线业务需要 10Mbit/s 带宽，对不同的业务提供不同的带宽保证：
  - 语音业务

    保证带宽是 2Mbit/s。
  - 视频业务

    保证带宽是 4Mbit/s。
  - 数据业务

    保证带宽是 4Mbit/s，同时希望专线内空闲的带宽能供数据业务使用，即峰值带宽是 10Mbit/s。

企业 B 的需求与企业 A 相同。

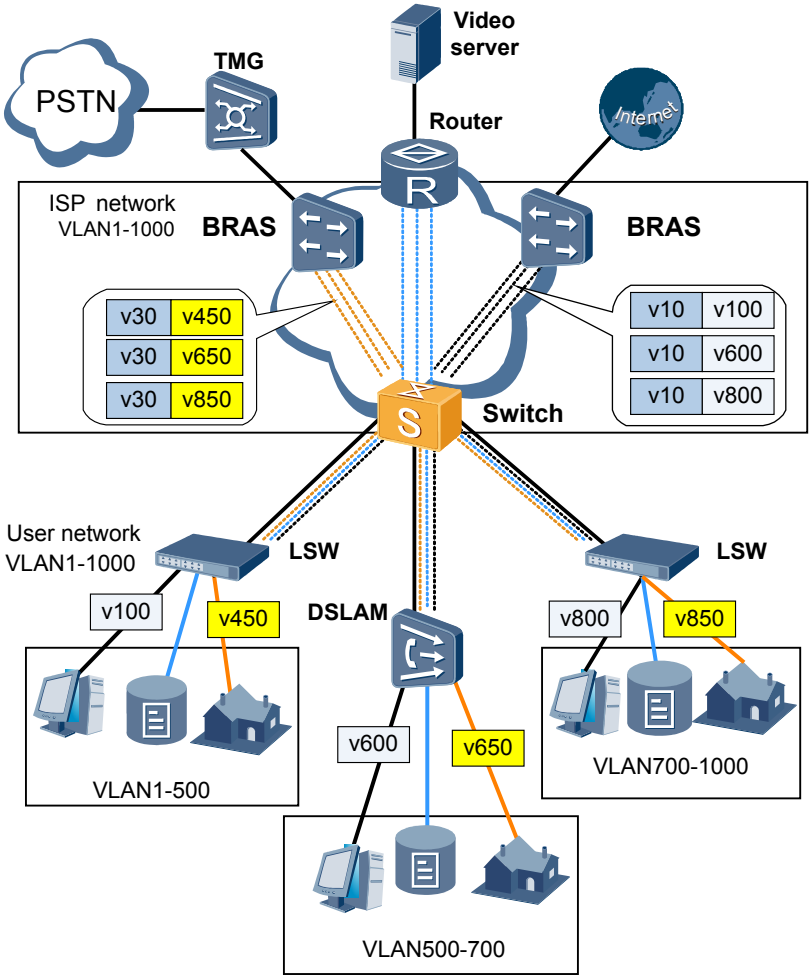
通过在 Switch 上部署 2 级流量管理，可以灵活地实现不同业务、不同用户对于网络资源的不同要求。

4.8 灵活 QinQ 应用

介绍了 S9300 城域网内提供灵活 QinQ 功能的组网和部署策略。

S9300 提供灵活 QinQ 功能的组网如图 4-11 所示。图中 S9300 以 Switch 表示。

图 4-11 S9300 的灵活 QinQ 功能应用



如图 4-11 所示的灵活 QinQ 应用场景中，三个企业/驻地网中都存在数据、语音、视频业务。Switch 根据接入的业务种类不同，分别给报文再封装一层 VLAN Tag 标签。例如：

- 对于来自用户网络的数据业务 VLAN 100、VLAN 600 和 VLAN 800，外侧封装 ISP 网络的 VLAN 10 标签。
- 对于来自用户网络的视频业务 VLAN 450、VLAN 650 和 VLAN 850，外侧封装 ISP 网络的 VLAN 30 标签。

借助灵活 QinQ 功能，S9300 不仅可以实现业务的汇聚，而且可以为不同业务选择不同的传输路径，方便了业务灵活部署。

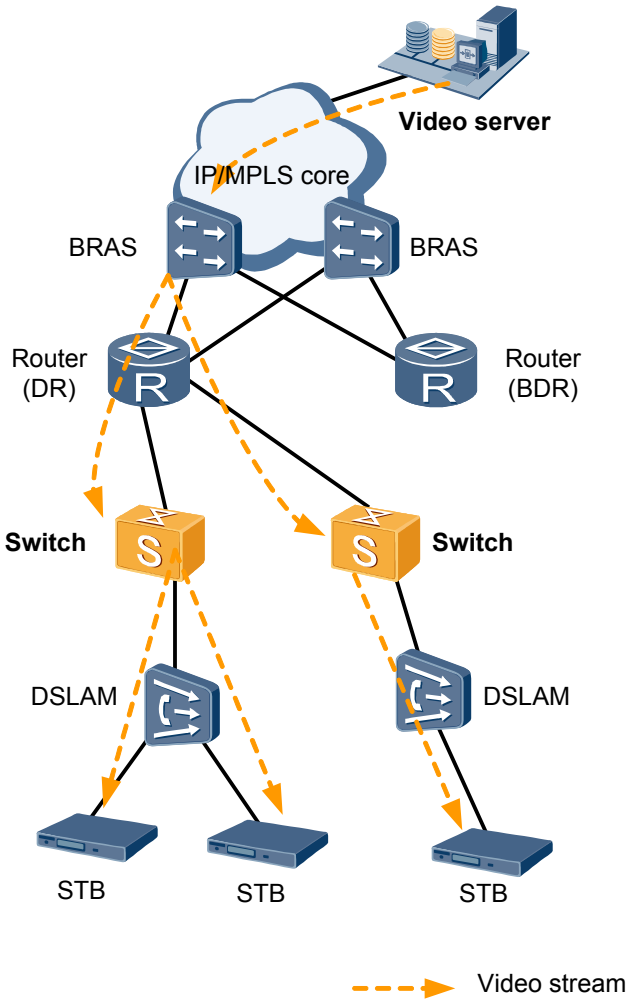
4.9 IPTV 业务应用

介绍了 S9300 城域网中提供 IPTV 业务的组网和策略。

4.9.1 IPTV 业务的组网

S9300 在 IPTV 应用中的组网如图 4-12 所示。

图 4-12 S9300 在 IPTV 中的应用



S9300 提供 IGMP Snooping 功能和组播 VLAN 功能，可以作为城域网接入层的组播复制和控制点，满足大容量的组播业务需求。组播流可以在 VLAN 内或 VLAN 间实现组播复制。

DSLAM 设备提供 IGMP Proxy 功能。

在如图 4-12 所示的组网中：

- Router 运行 PIM 协议，在两台 Router 间竞选 DR/BDR，DR 负责处理 IGMP，并将 IPTV Server 下来的视频流进行组播复制。
- Switch 上运行 IGMP Snooping，监听 IGMP 报文，同一组播组向上只发送一份 IGMP 加入请求，并建立组播转发组，热门频道可以建立静态组播组。
- Switch 根据组播转发表向 DSLAM 复制组播数据。

此外，S9300 支持端口快速加入或离开，可实现 IPTV 业务的快速切换。

4.9.2 IPTV 业务的保护

S9300 与 NPE 配合组网，将提供完善的 IPTV 业务保护机制，如图 4-13 所示。

图 4-13 S9300 对 IPTV 业务的保护

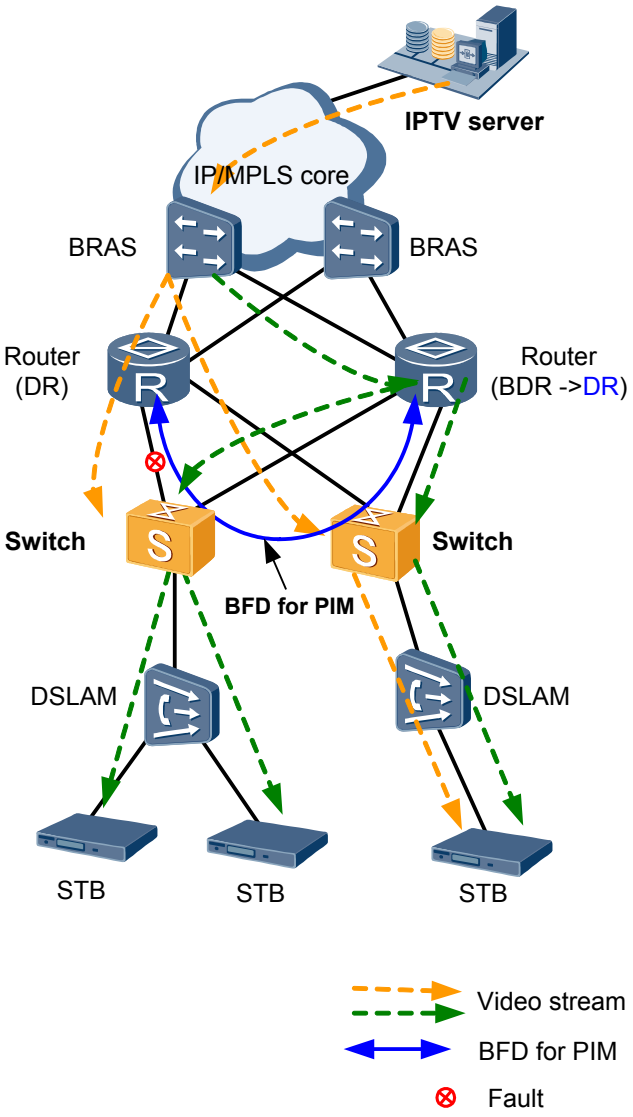


图 4-13 所示的网络通过以下机制来保护 IPTV 业务：

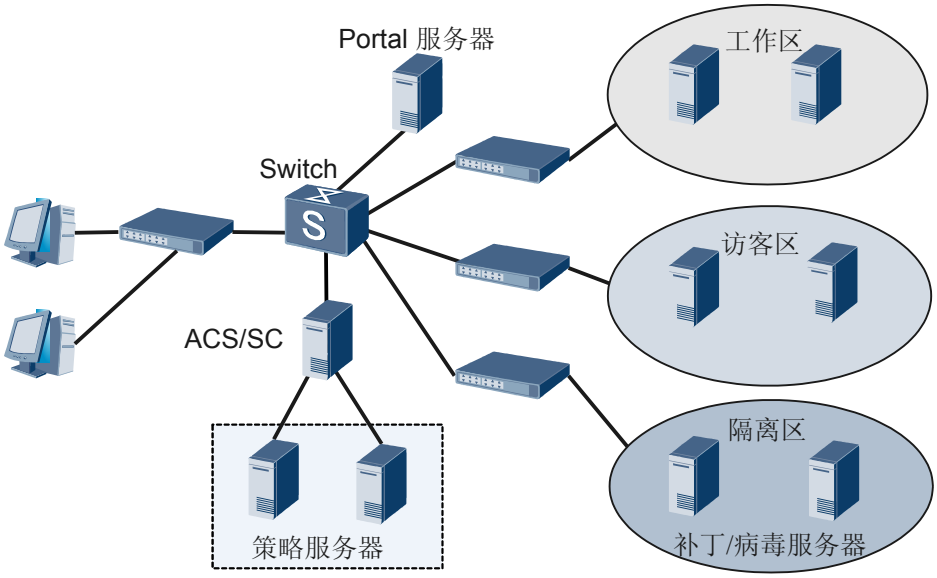
1. 两个 Router 之间运行 BFD for PIM，通过 BFD for PIM 来快速检测组播环路的链路状态。
2. 当链路、Switch 或其中一台 Router 故障时，BFD for PIM 将在 50ms 内发现故障。
3. BDR 快速切换成 DR，这时两个 Router 都成为 DR，同时进行组播转发。
4. 故障消除后，Router 重新竞选 DR/BDR，业务恢复正常。

4.10 NAC 组网应用

介绍了 S9300 在 NAC 组网中的应用。

S9300 在 NAC 应用中的组网如图 4-14 所示。图中 S9300 以 Switch 表示。

图 4-14 S9300 的 NAC 组网应用



企业网中，PC 无需安装终端软件，通过强制 Portal 重定向到登陆页面，输入用户名和密码后由 Switch 将用户名和密码提交 RADIUS 服务器认证。此时用户只能访问隔离区资源。

ACS/SC（相当于 RADIUS 服务器功能）返回认证通过。

PC 和 ACS 之间建立 HTTP 链接，由 ACS 对 PC 机进行安全检查，检查通过后根据用户权限大小可访问一般信息区或者核心信息区。

如果认证服务器不可用（认证超时，RADIUS 服务器无响应），则如果配置了无响应的 Session-Time-Out，则使用户上线，并允许访问网络，但启动 Session-Time-Out 定时器，定时器超时后再次发起认证。

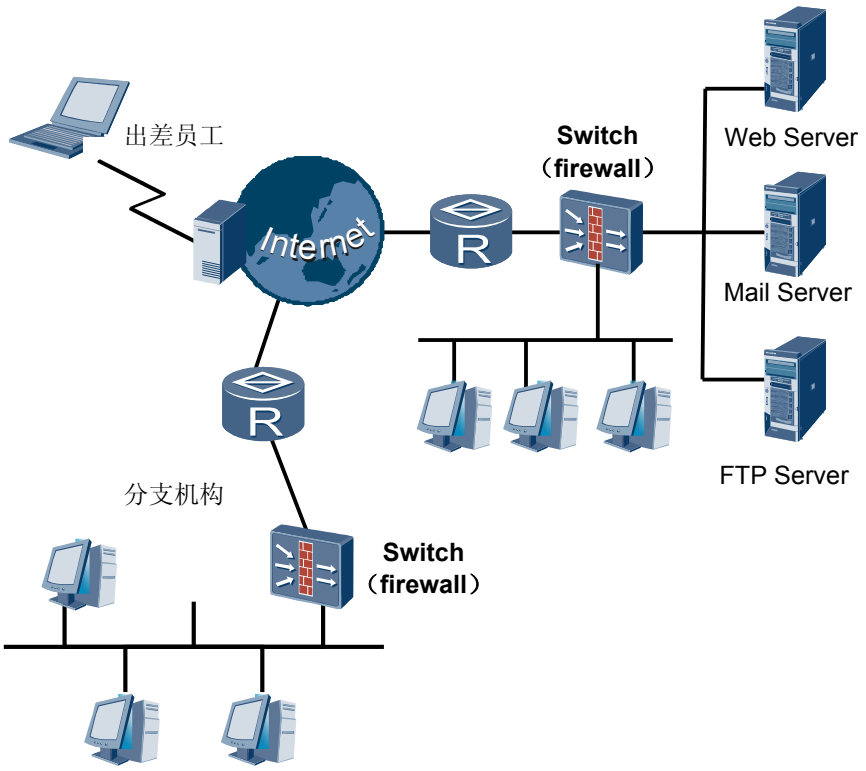
4.11 防火墙组网应用

介绍了 S9300 的防火墙组网和策略。

企业应用

S9300 作为带防火墙功能的交换机部署在公司总部的出口。在对外提供服务（Web、FTP、Mail 等）的同时，保护总部的内部资源免受到来自 Internet 的攻击。为内部员工上 Internet 网提供 NAT 功能，同时作为分支机构的远程 VPN 接入点。防火墙部署的分支机构的出口：保护分支机构的内部资源免受到来自 Internet 的攻击，同时为分支机构的用户提供远程 VPN 接入总部的服务。如图 4-15 所示。

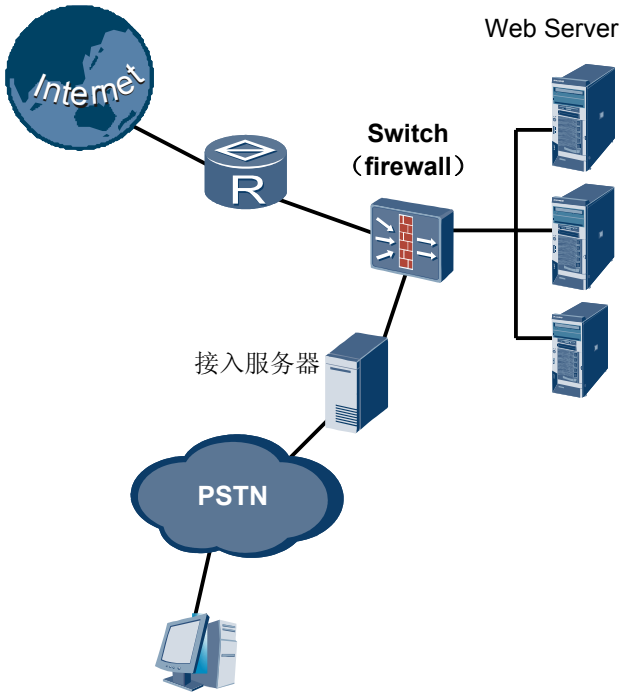
图 4-15 防火墙的企业应用组网图



ISP 应用

S9300 作为带防火墙功能的交换机部署在 ISP 网络的边缘，保护 ISP 的服务器、ISP 的其他用户，免受到来自于 Internet 的攻击，同时作为接入用户访问 Internet 的 NAT 网关。如图 4-16 所示。

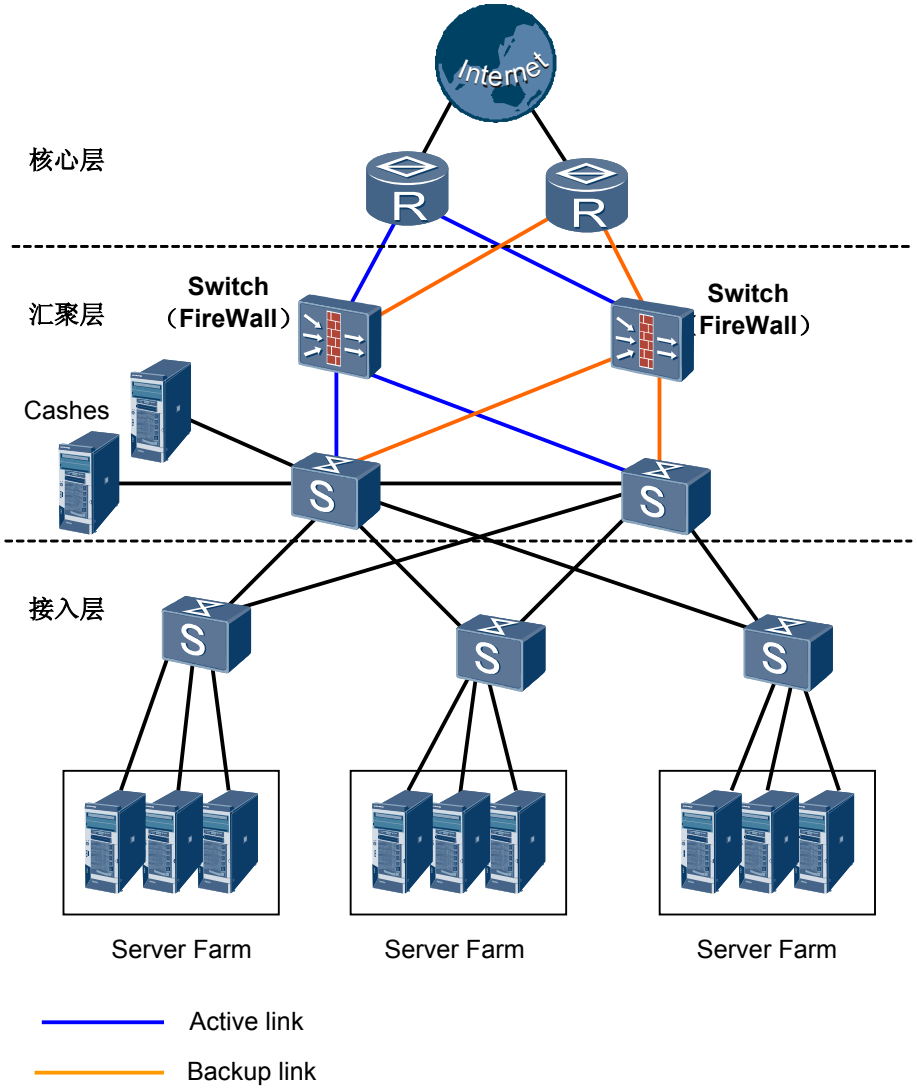
图 4-16 防火墙的 ISP 应用组网图



数据中心应用

S9300 作为带防火墙功能的交换机部署在数据中心的出口处，保护数据中心内的服务器免受到来自 Internet 的攻击，保护数据中心存储的关键数据。防火墙作为数据中心的出口，为了保证数据中心的高可用性，防火墙要冗余备份部署。如图 4-17 所示。

图 4-17 防火墙的 ISP 应用组网图



5 操作和维护

关于本章

S9300 提供的基本维护操作包括在线升级、在线调试、系统调试诊断和状态分析，以及网管系统。

5.1 操作和维护特点
介绍了 S9300 的配置途径和登录方式，设备监控和诊断调测的方法，软件升级和热补丁机制。

5.2 网管系统
网管系统可对 S9300 的资源、拓扑、配置、故障、性能和安全进行管理。

5.1 操作和维护特点

介绍了 S9300 的配置途径和登录方式，设备监控和诊断调测的方法，软件升级和热补丁机制。

5.1.1 配置方式

多种配置途径

S9300 支持多种配置和管理方式：

- 命令行配置

  用户可以通过 S9300 的 Console 接口、ETH 接口(管理网口)登录到 S9300，在命令行界面中进行各种操作。
- 网管配置

  用户通过网管站，基于 SNMP 协议对 S9300 进行管理和配置。
- Web 网管配置

  S9300 内嵌 WebServer。用户通过浏览器，使用 Web 页面对交换机进行配置。

灵活的登录方式

S9300 提供 Console、ETH 配置管理接口，从而实现本地和远程配置。

- PC 通过串口登录到 Console 接口
- PC 通过 Telnet 或 SSH 登录到 ETH 接口

另外，用户还可以通过 Telnet 方式登录到 S9300 的业务接口，然后进行配置和管理。

登录过程中，根据安全性需要可以采用不认证、本地认证和 AAA 认证多种身份验证措施。

5.1.2 监控和维护

设备硬件监控

S9300 提供多种设备硬件的监控功能：

- MCU、SRU、LPU、CMU、电源模块和风扇框的面板上均有指示灯，实时显示部件的运行状态。
- 提供单板在位检测、热插拔检测、Watch Dog、单板复位、风扇监控、电源监控、主备倒换控制等功能，并记录日志便于查阅。
- 自动监测单板温度，并提供温控功能。

- 提供各类异常、错误报文的统计。
- 对转发到 CPU 处理的协议报文分类统计，并可输出报文的详细内容。
- 提供 CPU 和内存占用率的查询功能。

设备管理和维护

S9300 提供多种功能于管理和维护设备：

- 支持多用户操作，支持中文、英文两种操作界面。
- 命令行提供灵活的在线帮助，命令行解释器对关键词进行不完全匹配的搜索方法，加快了命令输入的速度。
- 提供分级的用户权限管理及分级别的命令，未授权用户无法侵入 S9300。
- 提供告警分类和告警过滤等功能。
- 提供类似 DosKey 的功能，可以执行某条历史命令。
- 提供本地、远程两种方式下的软件加载升级、版本回退、备份、保存和清除等功能。
- 支持不同层次的信息收集，例如基于端口、二层、三层等信息进行收集。
- 支持信息中心，提供日志、告警、调试信息的统一管理，并且可以根据需要将信息重定向到多个方向。
- 提供多种信息查询，包括版本、部件状态、环境温度、CPU 和内存占用率。

5.1.3 诊断和调测

Ping 和 Traceroute 探测

S9300 提供如下工具检测三层网络连接是否可达，也可记录报文的传输路径。

- Ping
- Traceroute

S9300 提供如下工具检测 MPLS 网络连接是否可达，也可记录报文的传输路径。

- MPLS Ping
- MPLS Traceroute

S9300 提供如下工具检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。

- MAC Ping
- MAC TraceRoute

Debugging 调试

S9300 针对每个软件特性都提供丰富的 debugging 命令，调试信息丰富、内容详尽，有助于帮助诊断网络故障。每条 Debugging 命令支持多个调试参数，可以通过控制台灵活控制根据指定业务、指定接口打开或关闭某调试开关。

使用调试命令可以详细输出该特性运行过程中的关键事件、进程处理、报文收发和处理、报文解析、状态切换、差错检验等信息。

Trace 功能

S9300 提供系统操作的 Trace 功能，用于更深入地检测和诊断软件运行，在线记录系统的任务切换、中断、队列读写、系统异常等重要事件。

系统发生故障重起后，可以读出 Trace 信息作为故障定位参考。Trace 功能可以通过控制台命令打开或关闭。

镜像功能

S9300 支持基于端口或基于报文流的镜像功能：

- 端口镜像

  被观察端口上输入、输出或双方向上的报文地被复制到观察端口。
- 流镜像

  被观察报文流被复制到观察端口上。

外部监测主机和 S9300 的观察端口相连，网络管理员可以实时、便捷地观察到 S9300 所输入和输出的报文，为流量检测、故障分析定位、数据分析提供了依据，方便让高级维护人员分析网络的运行状况。

虚拟电缆检测

通过虚拟电缆检测特性，用户可以检测设备上以太网接口连接电缆的当前状况，检测内容包括电缆的接收方向、发送方向以及是否存在短路/开路现象，同时可以检测出故障线缆的长度。

5.1.4 软件升级和热补丁

在线升级

S9300 提供多种软件升级方式，支持远程升级。

- 本地菜单升级

  在 S9300 上电启动过程中，通过 BootROM 菜单加载新软件，完成升级。
- 在线升级

  S9300 支持双 MCU，为了确保升级过程中业务不中断，可以先升级备用板，经过主备倒换后再升级另一块新的备用板。

热补丁

S9300 可以通过热补丁来升级或修改部分特性：

- 安装补丁的过程中业务不受影响。
- 热补丁支持确认和删除功能。
- 支持补丁状态提示功能。

版本回退

S9300 支持版本回退功能：

- 升级新版本后发现不可用，重新启动选择另一个版本的软件进行启动。
- 在线升级和安装补丁过程中如果出现问题，切换回升级或安装补丁之前的软件版本重新运行。

5.2 网管系统

网管系统可对 S9300 的资源、拓扑、配置、故障、性能和安全进行管理。

U2000 网管

S9300 采用华为 U2000 作为集中网管系统，支持多语言图形界面，操作直观方便，并可以为第三方网管提供灵活的北向接口，有强大的与运营商的其它网管系统对接集成能力。

U2000 网络管理系统使用简单网络管理协议 SNMP(Simple Network Management Protocol)管理设备，同时也提供通过 CLI(Command Line Interface)进行设备配置管理的方式。U2000 网络管理系统是华为数通网络管理解决方案的基础部分，为管理和维护数据通信网络提供解决方案，实现了网元层管理和部分网络层管理功能。功能如下：

- 资源管理
- 拓扑管理
- 故障管理
- 性能管理
- 测试诊断管理
- 网元配置管理
- VPN 业务管理
- LSP 业务管理
- DC 管理
- Syslog 管理
- 安全管理
- 操作日志管理
- 报表管理

Web 网管

S9300 采用华为 U2000 作为集中网管系统，支持多语言图形界面，操作直观方便，并可以为第三方网管提供灵活的北向接口，有强大的与运营商的其它网管系统对接集成能力。

为了方便用户对 S9300 的维护和使用，推出 Web 网管功能。

Web 网管通过在 S9300 内提供内嵌 WebServer，用户可以通过 WEB 网管终端（PC）登录到 S9300 上，更直观地管理和维护交换机。使用 Web 网管，维护人员只需在 S9300 上配置 IP 地址和 Web 网管账号，在 PC 的浏览器中输入 IP 地址即可管理和维护交换机。操作简单、易学易用，可提高网络管理人员的工作效率。

6 技术指标

关于本章

介绍了 S9300 的外形尺寸和重量，还有 S9300 支持的电流、电压、温度、湿度等指标。

6.1 物理参数
介绍 S9300 的尺寸、功耗、重量、电压、工作环境参数等。

6.2 系统配置
介绍 S9300 的交换容量、备板容量和转发率等。

6.3 性能和容量
介绍了 S9300 品所支持的软件和硬件性能指标。

6.4 软件特性列表
介绍了 S9300 品所支持的主要特性的详细列表。

6.1 物理参数

介绍 S9300 的尺寸、功耗、重量、电压、工作环境参数等。

表 6-1 S9300 产品物理参数

项目		物理参数
外形尺寸（宽×深×高）（不带转接挂耳）		S9303: 442(宽)×476(深)×175(高) S9306: 442(宽)×476(深)×441.7(高) S9312: 442(宽)×476(深)×663.95(高)
整机最大功耗		S9303：≤350W S9306：≤800W S9312：≤1400W
重量（满配置）		S9303: < 22kg S9306: < 42kg S9312: < 70kg
直流（DC）输入电压	额定电压	－48V/-60V
	最大电压范围	－48V：－38.4V ～－57.6V －60V：－48V ～－72V
交流（AC）输入电压	额定电压	S9303、S9306: 110V/220V S9312: 220V
	最大电压范围	90 ～ 290V
PoE	电源输入方式	内置，支持交流电源
	PoE 电源冗余	S9303：不支持备份。 S9306、S9312：不备份或者 3+1、2+2 备份。
	输出功率	S9303：最大 800W。 S9306、S9312：最大 3200W。
温度	长期工作温度	0°C ～ 45°C
	短期工作温度	－5°C ～ 55°C
	存储温度	－40°C ～ 60°C
相对湿度	长期工作湿度	5%RH ～ 85%RH，不结露
	短期工作湿度	0%RH ～ 95%RH，不结露
海拔高度	长期工作海拔	小于 3000 米

项目		物理参数
	储存海拔高度	小于 5000 米

6.2 系统配置

介绍 S9300 的交换容量、备板容量和转发率等。

表 6-2 S9300 产品系统配置

描述	S9312 典型配置	S9306 典型配置	S9303 典型配置	备注
处理器	主频 700MHz	主频 700MHz	主频 500MHz	-
DDR2 SDRAM	1GB	1GB	512MB	-
NVRAM	512KB	512KB	512KB	电池供电
Flash	64MB	64MB	64MB	-
CF 卡	512MB	512MB	512MB	CF 卡作为海量存储设备用来保存数据文件、存储日志等内容。
交换容量	1Tbits/s 或者 2Tbit/s	1Tbits/s 或者 2Tbit/s	720Gbit/s	双向计算
背板容量	12Tbit/s	6Tbit/s	3Tbit/s	双向计算
10GE 端口密度	576	288	144	-
FE/GE 端口密度	576	288	144	-
转发能力	1320Mpps	1080Mpps	540Mpps	-
接口板插槽数目	12	6	3	LPU 线路板（可选）
主控交换板插槽数目	2	2	2	S9306/S9312：SRU 主控交换板 S9303：主控板，Full Mesh 结构
线路板支持的最大端口速率	48GE、48×10GE	48GE、48×10GE	48GE、48×10GE	-

6.3 性能和容量

介绍了 S9300 品所支持的软件和硬件性能指标。

表 6-3 S9300 产品主要性能指标

属性	业务特性	性能指标描述
整机可靠性	可用度	0.99999768
	平均故障间隔时间 MTBF（Mean Time Between Failure）	24.59 年
	平均修复时间 MTTR（Mean Time To Repair）	0.5 小时
	停机时间	1.22 分钟/年
以太业务性能	每 LPU 的 MAC 数	● ED 系列单板：512K ● EC 系列单板：128K ● EA/SA/FA 系列单板：32K
	VLAN	4K
	Trunk 组和每组的最大端口数	128 Trunk 组，每组最大 8 个端口
	MAC 学习速率	大于 3000 个/秒
	整机 ARP 数	最大 16K
	每 LPU 的 ARP 数	● EA/EC/ED 系列单板：16K ● SA/FA 系列单板：8K
QoS 性能	每端口的队列数	8 个
	CAR	● ED/EC/EA/FA 系列单板:8Kbit/s ● SA 系列单板：64Kbit/s

属性	业务特性	性能指标描述
ACL	ACLv4	单板支持的最大 ACLv4 数目： ● ED 系列单板：ingress 70K；egress 1000 ● EC 系列单板：ingress 70K；egress 1000 ● EA 系列单板：ingress 6000；egress 1000 ● SA(24GE)单板：ingress 3000；egress 500 ● SA(X12SA/X48SSA)单板：ingress 1200；egress 500 ● FA(G48SFA/G48TFA/F48TFA)单板：ingress 1200；egress 500 ● FA(G24CFAT)单板：ingress 3000；egress 500
	ACLv6	单板支持的最大 ACLv6 数目： ● ED 系列单板：ingress 67K；egress 250 ● EC 系列单板：ingress 35K；egress 250 ● EA 系列单板：ingress 3000；egress 250 ● SA(24GE)单板：ingress 1500；egress 250 ● SA(X12SA/X48SSA)单板：ingress 250；egress 120 ● FA(G48SFA/G48TFA/F48TFA)单板：ingress 250；egress 120 ● FA(G24CFAT)单板：ingress 250；egress 120
MPLS	LSP 数目	8K
	LDP 邻居数量	大于 256 个
L2VPN	VLL 表项	4K
	VSI 表项	1K
L3VPN	VRF	2K
	VPN 路由	● S9306/S9312：500K ● S9303：140K
IP 单播	路由表项	● S9306/S9312：512K ● S9303：220K

属性	业务特性	性能指标描述
	IPv4 FIB	● ED 系列单板：512K ● EC 系列单板：128K ● EA 系列单板：16K ● SA/FA 系列单板：12K
	IPv6 FIB	● ED 系列单板：256K ● EC 系列单板：64K ● EA 系列单板：8K ● SA/FA 系列单板：6K
组播	组播静态路由项数	256
	二层组播转发表项	1K
	三层组播转发表项	● ED/EC/EA 系列单板：4K ● SA/FA 系列单板：2K
可靠性业务	BFD	● BFD session 数量：2K ● 最小故障发现时间：无灵活插卡时 3s,配置灵活插卡时小于 50ms
	以太 OAM	● 802.1ag 整机可创建 64 个 MD 整机可创建的 MA 数： – S9312、S9306：4K – S9303：2K 检测速率：3.3ms/10ms/100ms/1s/10s/1min/10min ● 802.3ah 检测速率：100ms/1s
	RRPP	● RRPP 最大实例数：48 ● 整机支持环数：64 ● 单板支持环数：5 ● RRPP 支持的域个数：64 ● 链路故障切换时间：小于 50ms
	VRRP	● 整机 VRRP 备份组：255 ● 整机 VRRP 管理组：16 ● 每个 VRRP 备份组内的虚 IP 数：16 ● 倒换时间：无灵活插卡时 3s，有灵活插卡时小于 50ms

属性	业务特性	性能指标描述
	SmartLink	● 整机最大实例数：48 ● 倒换时间小于 50ms
	MSTP	● 整机最大实例数：48 ● 倒换时间小于 100ms
	SEP	● 整机最大 segment 数：256 ● 拓扑收敛时间小于 50ms

6.4 软件特性列表

介绍了 S9300 品所支持的主要特性的详细列表。

表 6-4 S9300 系统特性列表

属性		说明
Ethernet 特性	Ethernet	● 支持全双工、半双工、自动协商工作方式 ● 以太网端口可支持 10Mbit/s、100Mbit/s、1000Mbit/s 和 10Gbit/s 的速率 ● 以太网端口支持自协商速率 ● 支持端口流量控制 ● 支持 Jumbo 帧 ● 支持端口捆绑成 Trunk ● 支持 Trunk 内各链路流量的负载分担 ● 支持 LACP 进行链路聚合 ● 支持 LLDP 进行链路层发现 ● 支持端口隔离、端口转发限制 ● 支持广播风暴抑制
	VLAN	● 支持 Access、Trunk、Hybrid 和 QinQ 接入方式 ● 支持 default VLAN ● 支持 1:1 VLAN Mapping ● 支持 N:1 VLAN Mapping ● 支持基于 802.1p 的 VLAN Mapping ● 支持 QinQ ● 支持灵活 QinQ ● 支持基 VLAN-Switch

属性		说明
	MAC	● 支持 MAC 地址自动学习和老化 ● 支持静态、动态、黑洞 MAC 表项 ● 支持基于端口和 VLAN 的 MAC 地址学习限制
	ARP	● 支持静态、动态 ARP ● 支持 VLAN 上应用 ARP ● 支持 ARP 表项老化
	Smartlink	● 支持 Smartlink ● 支持 Smartlink 多实例 ● 支持 Monitor link
	DLDP	● 支持单向链路检测
	LLDP	● 支持 LLDP
	虚拟电缆检测	● 支持虚拟电缆检测
以太网环路保护	MSTP	● 支持 STP ● 支持 RSTP ● 支持 MSTP ● 支持 BPDU 保护、Root 保护、环路保护 ● 支持 BDPU Tunnel
	RRPP	● 支持 RRPP ● 支持 RRPP 多实例
	Loop Detection	● 支持环路检测功能
IP 单播特性	IPv4 单播	● 网管接口支持接收和发送 IPv4 单播数据报文 ● 网管接口支持 IPv4 单播静态路由 ● 支持 RIP、OSPF、IS-IS、BGP 动态路由协议 ● 支持 DHCP snooping ● 支持 DHCP Server/Relay
	IPv6 单播	● 支持 RIP、OSPFv3、ISISv6、BGP+路由协议 ● 支持 TCP6、Ping IPv6、Tracert IPv6、Socket IPv6 协议栈 ● 支持 DHCPv6 snooping ● 支持 ND Snooping

属性		说明
	过渡技术	● 支持 IPv6 over IPv4 隧道 ● 支持 IPv4 over IPv6 ● 支持 6PE
组播	组播	● 支持 IGMP/MLD/MSDP/PIM-DM/PIM-SM/PIM-SSM 协议 ● 支持 IGMP v1/v2/v3 Snooping 功能 ● 支持 MLDv1 snooping ● 支持用户快速离开机制 ● 支持组播流量控制 ● 支持组播 VLAN ● 支持组播查询器 ● 支持组播协议报文抑制功能 ● 支持组播 ACL ● 支持组播复制功能 ● 支持 IGMP snooping over VPLS ● 组播 VPN
MPLS 特性	MPLS 基本功能	● 支持静态 LSP ● 支持静态 VLAN 到 MPLS SVC 映射，提供虚拟以太网专线 ● 支持 L2VPN，L3VPN ● 支持两层 MPLS 标签 ● 支持在以太网上承载 MPLS 业务
	MPLS OAM	● 提供 LSP ping 和 LSP traceroute 功能 ● 支持 LSP 链路故障自动检测 ● 支持 LSP 链路 1+1 保护倒换
	MPLS-TE	● 支持 MPLS-TE 隧道建立 ● 支持 MPLS-TE 保护组
	VLL/HVPLS	● 支持 SVC/Martini/Kompella/CCC 方式的 VLL ● 支持 Martini/Kompella 方式 VPLS ● 支持 LSP 和 QinQ 方式的 HVPLS ● 支持 VLAN 变换后入 VLL/VPLS
Ethernet OAM	Ethernet OAM	● 支持 IEEE 802.3ah 实现点到点以太网故障管理 ● 支持以太网 OAM IEEE 802.1ag ● 支持 MAC Ping 和 MAC Traceroute

属性		说明
BFD	-	● 支持 BFD 物理链路检测 ● 支持 IP 连通性检测 ● 支持 LSP，CR-LSP 和 MPLS TE 保护组的连通性检测 ● VPLS 网络中进行 BFD 检测。支持基于 VPLS 的 BFD 检测和管理 VPLS 倒换的诊断码报文的处理以及倒换处理
QoS 特性	流分类	● 支持基于 Layer2 协议头、Layer3 协议、Layer4 协议、802.1p 优先级等的组合流分类 ● 支持基于 QinQ 报文的 C-VID 流分类
	流动作	● 支持对分类后报文流的访问控制 ● 支持基于 CAR 的流量监管 ● 支持按照流分类结果重标记报文 ● 支持分类后报文进入指定调度队列中 ● 支持流分类、流行为的组合应用
	队列调度	● 支持 PQ、WRR、DRR、PQ+WRR、PQ+DRR 调度
	拥塞避免	● 支持 WRED ● 支持尾部丢弃
	流量整形	● 支持出方向流量整形
	流量监控	支持 2 级流量监控
时钟特性	-	● 支持同步以太 ● 支持 1588v2
PoE	-	● 支持 802.3af/802.3at 标准 ● 每端口提供 30W 供电能力
行业网特性	NAC	● 支持 802.1X 认证 ● 支持 MAC 认证 ● 支持 Portal 认证 ● 支持旁路认证 ● 支持直接认证
	防火墙	● 支持包过滤 ● 支持 ASPF ● 支持攻击防范 ● 支持透明防火墙 ● 支持防火墙多实例

属性		说明
	NAT	● 支持 NAT 地址池 ● 支持 NAPT ● 支持 NAT Server ● 支持静态 NAT/NAPT ● 支持 Easy IP ● 支持 ALG ● 支持 NAT 多实例
	负载均衡	● 支持服务器探测 ● 支持会话保持国内 ● 支持多种负载均衡算法 ● 提供了完全的第 4 ～ 7 层服务器负载均衡功能
	IPSec VPN **说明** 俄罗斯地区发布的版本不提供 IPSec VPN 功能。	● 支持 IKE V1/V2 协商 ● 支持 AH 和 ESP 两种模式 ● 支持存活检测 ● 支持 NAT 穿越 ● 支持手工静态配置安全联盟 ● 支持多种加密算法
配置与维护	终端服务	● 支持命令行配置 ● 支持英文和中文的提示和帮助信息 ● 支持 Console、Telnet 终端服务 ● 支持 Send 功能，终端用户之间进行信息互通
	文件系统	● 支持文件系统 ● 支持目录和文件管理 ● 支持通过 FTP、TFTP 方式上载、下载文件
	调试和维护	● 支持日志、告警、调试信息统一管理 ● 提供电子标签 ● 支持用户操作日志 ● 支持详尽的调试信息，帮助诊断网络故障 ● 提供黑匣子功能 ● 提供网络测试工具，如 ping、traceroute 命令等 ● 提供端口镜像、流镜像

属性		说明
	可靠性	● 支持电源 1+1 或 2+2 备份、风扇备份 ● 支持主控板、线卡、风扇、电源等关键模块的热插拔 ● 支持主控板的 1+1 热备份 ● 支持主控板的自动和强制倒换 ● 支持以太网端口跨板捆绑
	版本升级	● 支持整机软件加载、在线加载 ● 支持 BootROM 升级和远程在线升级 ● 支持在线补丁 ● 支持版本回退
安全和管理	安全	● 命令行分级保护，未授权用户无法侵入 ● 支持 SSH v1.5 和 v2.0 ● 支持 RADIUS 和 HWTACACS 用户登录认证 ● 支持 ACL 过滤 ● 支持防范 DoS 攻击、TCP 的 SYN Flood 攻击、UDP Flood 攻击、广播风暴攻击、大流量攻击 ● 支持 MAC 地址学习限制 ● 支持黑洞 MAC ● 支持端口隔离 ● 支持包过滤 ● 支持 CPU 通道的保护 ● 支持 ARP 源抑制 ● 支持黑白名单 ● 支持攻击溯源 ● 支持 ALS（Automatic Laser Shutdown）节能
	网络管理	● 支持 ICMP 实现 ping 和 traceroute 功能 ● 支持标准网管协议 SNMPv1/v2c/v3 ● 支持通用特性的标准 MIB ● 支持 RMON