



**S6700 系列以太网交换机**

**V200R002C00**

## **产品描述**

文档版本 02

发布日期 2013-02-08

版权所有 © 华为技术有限公司 2013。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、复制本档内容的部分或全部，并不得以任何形式传播。

## 商标声明



HUAWEI和其他华为商标均为华为技术有限公司的商标。

本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，本档内容会不定期进行更新。除非另有约定，本档仅作为使用指导，本档中的所有陈述、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://enterprise.huawei.com>

客户服务邮箱： [ChinaEnterprise\\_TAC@huawei.com](mailto:ChinaEnterprise_TAC@huawei.com)

客户服务电话： 4008229999

# 前言

## 读者对象

本文档针对S6700设备，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S6700设备的总体情况，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	表示有高度或中度潜在危险，如果不能避免，可能会导致人员死亡或严重伤害。
 警告	表示有低度潜在危险，如果不能避免，可能导致人员轻微或中等伤害。
 注意	表示有潜在风险，如果不能避免，可能会导致设备损坏、数据丢失、设备性能降低或不可预知的结果。
 窍门	能帮助您解决某个问题或节省您的时间。
 说明	正文的附加信息，是对正文的强调和补充。

## 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 02 (2013-02-08)

第二次正式发布。该版本的更新如下：

增加：[7.5 遵循的标准与协议](#)

### 文档版本 01 (2012-12-08)

第一次正式发布。

# 目录

前言.....	ii
<b>1 产品简介.....</b>	<b>1</b>
1.1 产品定位.....	2
1.2 产品特点.....	2
1.2.1 灵活的组网能力.....	2
1.2.2 网络级 QoS 保障.....	2
1.2.3 多层面的扩展能力.....	2
1.2.4 周密的安全措施.....	2
1.2.5 便捷的操作维护.....	3
1.2.6 绿色节能设计.....	3
1.2.7 先进的防雷技术.....	3
<b>2 产品架构.....</b>	<b>4</b>
2.1 概述.....	5
2.2 整机结构.....	5
2.3 硬件模块.....	6
2.3.1 交换主控板.....	7
2.3.2 电源.....	7
2.3.3 风扇.....	7
2.4 软件结构.....	7
<b>3 链路特性.....</b>	<b>9</b>
3.1 以太网特性.....	10
3.1.1 链路聚合.....	10
3.1.2 接口流控.....	10
3.1.3 流量抑制.....	10
3.1.4 VLAN.....	10
3.1.5 QinQ.....	12
3.1.6 GVRP.....	13
3.2 STP/RSTP/MSTP.....	13
3.2.1 STP 和 RSTP.....	13
3.2.2 MSTP.....	13
3.2.3 MSTP 保护功能.....	13
3.2.4 局部 STP 和 BPDU 隧道.....	14

3.3 RRPP.....	14
3.3.1 RRPP 环网组成.....	14
3.3.2 RRPP 工作机制.....	15
3.3.3 多种拓扑结构.....	15
3.4 Smart Link.....	15
3.5 SEP.....	16
3.6 ERPS.....	16
3.7 接口安全保护.....	16
3.8 链路检测.....	17
<b>4 业务特性.....</b>	<b>18</b>
4.1 IPv4 转发.....	19
4.1.1 IPv4 特性.....	19
4.1.2 单播路由特征.....	19
4.1.3 组播路由特性.....	19
4.2 IPv6.....	20
4.3 路由协议.....	20
4.4 组播.....	20
4.4.1 IGMP Snooping/MLD Snooping.....	20
4.4.2 IGMP Snooping Proxy.....	21
4.4.3 组播成员接口快速离开.....	21
4.4.4 组播流量控制.....	21
4.4.5 跨 VLAN 组播复制.....	21
4.4.6 可控组播.....	21
4.5 QoS.....	21
4.5.1 流分类.....	21
4.5.2 访问控制和重标记.....	22
4.5.3 流量监管.....	23
4.5.4 拥塞管理.....	23
4.5.5 拥塞避免.....	23
4.5.6 接口限速.....	23
4.5.7 支持双速三色.....	23
4.5.8 支持聚合 CAR.....	24
4.6 安全.....	24
4.6.1 设备的安全.....	24
4.6.2 业务的安全.....	25
4.6.3 安全认证.....	25
4.7 MAC 强制转发.....	26
4.8 DHCP.....	27
4.9 网络级可靠性.....	27
4.9.1 MSTP 保护倒换.....	28
4.9.2 RRPP 快速保护倒换.....	28
4.9.3 Smart Link 双归属保护.....	28

4.9.4 以太网 OAM.....	28
4.10 LLDP.....	28
4.11 NQA.....	29
4.12 堆叠.....	29
<b>5 特性组网应用.....</b>	<b>30</b>
5.1 数据中心应用.....	31
5.2 企业网络和园区网的汇聚.....	31
5.3 iStack 技术的应用.....	32
<b>6 操作维护和网管系统.....</b>	<b>34</b>
6.1 维护和管理.....	35
6.1.1 多种配置方式.....	35
6.1.2 监控和维护.....	35
6.1.3 诊断和调测.....	36
6.1.4 软件升级和热补丁.....	36
6.1.5 硬件异常处理.....	37
6.2 Web 网管.....	37
6.3 eSight 网管.....	37
<b>7 系统技术指标.....</b>	<b>38</b>
7.1 规格参数.....	39
7.2 光模块属性.....	41
7.3 性能和容量.....	43
7.4 软件特性列表.....	45
7.5 遵循的标准与协议.....	48

# 1 产品简介

---

## 关于本章

1.1 产品定位

1.2 产品特点

## 1.1 产品定位

S6700系列以太网交换机（以下简称S6700），是华为公司自主开发的下一代全万兆盒式交换机，可用于数据中心万兆服务器接入及园区网的核心。

S6700是业内最高性能的盒式交换机之一，同时提供最多24/48个全线速万兆接口，使万兆服务器高密度接入和园区网高密度万兆汇聚成为可能。同时，S6700支持丰富的业务特性、完善的安全控制策略、丰富的QoS等特性以满足数据中心扩展性、可靠性、可管理性、安全性等诸多挑战。

## 1.2 产品特点

### 1.2.1 灵活的组网能力

S6700提供万兆以太网光接口，支持Access、Trunk和Hybrid等多种接口类型。

S6700提供SFP+（Small Form-Factor Pluggable Plus）类型光模块。光纤长度可以根据用户对传输距离的需求灵活选配。SFP+电缆，满足近距离、低成本堆叠和互联要求。

S6700可以组成树状、星型和环状以太网。对于环状以太网，S6700提供STP（Spanning Tree Protocol）、SEP和RRPP，消除环路并提供快速保护倒换。

### 1.2.2 网络级 QoS 保障

S6700具备完善的QoS机制。S6700能够智能感知业务，能够对OSI（Open System Interconnection）模型2~4层信息进行流分类，根据流分类结果提供访问过滤、流量监管、队列调度策略，从而确保不同业务对差别服务的要求。

### 1.2.3 多层面的扩展能力

S6700以华为公司拥有自主知识产权的VRP（Versatile Routing Platform）平台为基础，结合设备和网络管理技术，提供高速的交换能力和丰富的业务特性。

### 1.2.4 周密的安全措施

S6700保障设备和数据传输的安全，有效的防止恶意用户对网络的攻击。

- 提供全面的MAC防攻击保护机制。
- 提供丰富的ACL策略。
- 提供MFF、IPSG、ARP安全、CPU防攻击等大量防攻击保护机制。
- 提供“VLAN+MAC”的查表机制。
- 支持流量抑制。

S6700提供安全的用户登录操作保护。

- 对登录用户提供口令保护，口令可加密功能。
- 通过配置用户级别和命令级别实现对命令的分级保护。
- 通过命令锁定当前配置终端，防止设备被非法使用。

- 对影响系统性能的重要命令，提供确认和提示。

S6700提供ALS（Automatic Laser Shutdown）功能，在光纤连接断开时停止发送激光，有效避免激光对用户的伤害。

## 1.2.5 便捷的操作维护

S6700不仅自身提供基于接口的流量统计功能，支持IP网络中Ping、TraceRoute等故障检测和定位技术。而且还能配合华为公司eSight网络管理系统，提供丰富的性能监视、告警和快速的故障定位能力。

eSight可以完成对S6700的监控配置，包括设备资源管理、拓扑管理、配置文件管理、多设备批量配置工具等。此外，eSight还提供图表化形式对设备重要监控信息进行展示。

## 1.2.6 绿色节能设计

S6700采用多种节能措施，包括：

- 采用静音风扇，风扇转速自动调整，降低系统的噪音，节省风扇功耗
- 当检测不到业务端口对端连接设备，即端口空闲，则芯片进入省电模式，以减小功耗。
- 采用先进工艺、高集成度、低功耗芯片，并配合智能设备管理系统充分利用芯片的低功耗特性，在提升系统性能的同时还降低了整机功耗。

## 1.2.7 先进的防雷技术

S6700采用华为专利内置防雷技术，可降低设备在雷击天气中的损坏概率，大大提高设备可靠性，将安全系数提高30倍。

# 2 产品架构

---

## 关于本章

- 2.1 概述
- 2.2 整机结构
- 2.3 硬件模块
- 2.4 软件结构

## 2.1 概述

S6700系列以太网交换机采用集中式硬件平台，提供前维护结构。硬件系统由机箱、电源板、风扇板、交换主控板SCU（Switch Control Unit）。整机宽度符合业界标准，可以安装到IEC297标准机柜或ETSI标准机柜中。

目前S6700系列以太网交换机包括S6700-24-EI和S6700-48-EI两个型号。

## 2.2 整机结构

### 设备正面外观

S6700系列设备正面外观如表2-1所示。

表 2-1 S6700 系列设备正面外观

设备型号	设备图片
S6700-24-EI	
S6700-48-EI	

1、24个10GE SFP +以太网光接口 <b>说明</b> 支持1000BASE-T光 电转换模块。	2、48个10GE SFP +以太网光接口 <b>说明</b> 支持1000BASE-T光电 转换模块。	3、1个Console接口	4、1个ETH管理接口
5、1个USB接口 <b>说明</b> 配合U盘使用，可用 于开局、传输配置文 件、升级文件等。			

## 设备背面外观

S6700系列设备背面外观如表2-2所示。

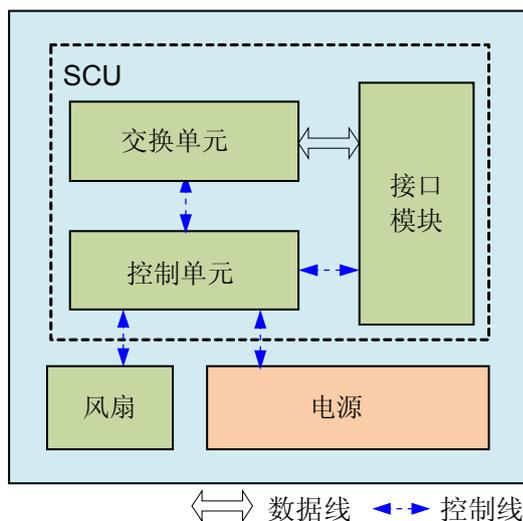
表 2-2 S6700 系列设备背面外观

设备型号	设备图片		
S6700-24-EI S6700-48-EI			
1、接地螺钉 <b>说明</b> 配套使用接地线缆。	2、ESD插孔 <b>说明</b> 在对交换机设备进行安装维护操作时需要佩戴防静电腕带，防静电腕带的一端要插在机箱挂耳上的ESD插孔里。	3、风扇模块插槽 <b>说明</b> 支持的风扇模块： CX7E1FANA风扇模块	4、电源模块插槽 <b>说明</b> 支持的电源模块： ● 500W交流电源模块 ● 500W直流电源模块

## 2.3 硬件模块

S6700硬件模块的逻辑结构如图2-1所示。

图 2-1 S6700 硬件模块的逻辑结构



S6700的硬件模块包括SCU、电源、风扇。

## 2.3.1 交换主控板

SCU是S6700的交换主控板，它固定安装在S6700上。S6700有1块SCU。

SCU提供报文交换和设备管理功能，集成了主控模块、交换模块和接口模块，是多个功能模块的集合体。

### 主控模块

主控模块主要完成如下功能：

- 处理各种协议。
- 作为用户操作的代理，根据用户的操作指令来管理系统、监视性能，并向用户反馈设备运行情况。
- 对SCU上的交换模块、接口模块进行监控和维护。

### 交换模块

交换模块（也称为交换网）负责SCU上接口模块间报文的交换、组播复制、QoS调度、访问控制等功能。

交换模块采用高性能的ASIC芯片，支持全线速转发，并交换模块提供快速、多优先级的数据交换。

### 接口模块

接口模块提供多个以太网接口，负责接入以太网业务。

## 2.3.2 电源

S6700支持直流电源和交流电源输入方式，为整个系统供电。

表 2-3 S6700 支持的电源

设备型号	AC	DC	1+1备份
S6700-24-EI	Y	Y	Y
S6700-48-EI	Y	Y	Y

## 2.3.3 风扇

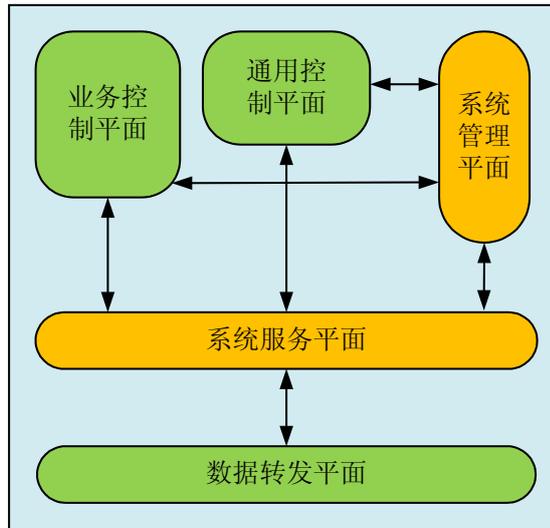
风扇为系统提供强制散热功能。

S6700-24-EI和S6700-48-EI支持可插拔风扇，支持现场更换和在线维护。

## 2.4 软件结构

S6700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。

图 2-2 软件总体架构



- 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 链路特性

---

## 关于本章

- 3.1 以太网特性
- 3.2 STP/RSTP/MSTP
- 3.3 RRPP
- 3.4 Smart Link
- 3.5 SEP
- 3.6 ERPS
- 3.7 接口安全保护
- 3.8 链路检测

## 3.1 以太网特性

### 3.1.1 链路聚合

链路聚合是指将一台设备上多个以太网物理接口或者不同设备上的多个以太网物理接口捆绑成一个逻辑接口（例如Eth-Trunk接口），又称为多接口负载均衡组或链路聚合组。

捆绑接口后，S6700会自动将流经逻辑接口上的流量在参与捆绑的多个物理接口上进行负载分担。当其中一个物理接口发生故障时，故障接口上的流量会自动分担到其他物理接口上，从而保证了业务传输不被中断。当故障恢复后，流量会重新分配，保证流量在汇聚的各接口之间的负载分担。

目前，S6700支持N×10GE和N×GE接口间的捆绑，并且可以根据如下信息进行负载分担：

- 基于源MAC地址
- 基于目的MAC地址
- 基于“源MAC地址+目的MAC地址”
- 基于源IP地址
- 基于目的IP地址
- 基于“源IP地址+目的IP地址”

借助链路聚合技术，不仅可以简单、廉价的扩展两设备之间的传输带宽，无需升级硬件，而且还可以有效的增加链路可靠性。

### 3.1.2 接口流控

接口流控是拥塞管理的一种方式，不区分流量的类别，对所有流量都有效。S6700通过硬件反压机制实现接口流控。接口工作在全双工模式时，S6700支持IEEE 802.3x流控，接口工作在半双工模式时，S6700支持背压式流控。

当发生拥塞时，S6700向数据源方向的上游设备发出连续暂停帧（Pause帧），通知上游设备暂停某时间间隔后再发送数据。上游设备接收到该暂停帧后，减少从出接口注入网络的总流量。这种接口流控机制不区分流量的类别，对所有流量都有效。

### 3.1.3 流量抑制

流量抑制是用来限制网络中传输的未知单播报文、组播报文、广播报文数量，使其在合理的范围内，从而减少对网络运行效率的影响。

S6700支持基于接口来抑制流量。使能该功能的接口监控收到的未知单播报文、组播报文、广播报文，判断流量是否超过阈值。如果超过阈值，则S6700丢弃该接口上超出的流量，使流量降低到合理的范围，从而保证网络业务的正常运行。

S6700还支持控制接口上的最大未知单播报文、组播报文、广播报文的流量百分比，从而控制报文的流量。

### 3.1.4 VLAN

在逻辑上将一个局域网LAN（Local Area Network）划分成多个子集，每个子集形成各自的广播域，即虚拟局域网VLAN（Virtual Local Area Network）。简单地说，VLAN是将

LAN内的设备逻辑地而不是物理地划分为一个个网段，从而实现在一个LAN内隔离广播域的技术。

## VLAN 划分方式

网络管理者不仅可以将同一物理局域网划分成多个VLAN，也可以将不同物理局域网划分到同一个VLAN中。同一VLAN内各设备从属于同一广播域中，彼此之间相互通信；不同VLAN之间相互隔离，即不同VLAN内的设备之间不能互相通信。

S6700支持5种VLAN划分方式：

- 基于接口的VLAN划分  
按照设备接口来定义VLAN成员，将设备上的指定接口加入到不同的VLAN中，则从该接口接收的报文将只能在相应的VLAN内进行传输。
- 基于MAC地址的VLAN划分  
按照报文的源MAC地址来定义VLAN成员。S6700从接口接收到报文后，会根据报文的源MAC地址来确定报文所属的VLAN，然后将报文自动划分到指定VLAN中进行传输。
- 基于协议的VLAN划分  
根据接口接收到的报文所属的协议（族）类型及封装格式来给报文分配不同的VLAN。
- 基于IP子网的VLAN划分  
根据报文的源IP地址及子网掩码来定义VLAN成员。S6700从接口接收到报文后，会根据报文的源IP地址来确定报文所属的VLAN，然后将报文自动划分到指定VLAN中进行传输。
- 基于策略的VLAN划分  
根据报文“MAC地址+IP地址”、“MAC地址+IP地址+接口”策略来定义VLAN成员。S6700从接口接收到报文后，会根据报文的组合策略来确定报文所属的VLAN，然后将报文自动划分到指定VLAN中进行传输。

## VLAN 聚合

为了在S6700上实现VLAN间通信，需要为每个VLANIF接口配置一个IP地址，以实现VLAN间互通，而VLAN过多，将占用IP地址资源。VLAN聚合（VLAN aggregation）可以解决多个VLAN占用多个IP地址的问题。

VLAN聚合，又称为Super VLAN。它是指将多个VLAN集中在一起，形成一个super-VLAN。组成super-VLAN的VLAN被称作sub-VLAN。

## MUX VLAN

MUX VLAN提供了一种在VLAN的端口间进行二层流量隔离的机制。比如在企业网络中，客户端口可以和服务器端口通讯，但客户端口间不能通讯。

MUX VLAN分为主VLAN和从VLAN，从VLAN又分为互通型从VLAN和隔离型从VLAN。主VLAN与从VLAN之间可以相互通信；互通型从VLAN内的端口之间可以互相通信，但是互通型从VLAN间的端口之间不能通讯；隔离型从VLAN内的端口之间不能互相通信。

## DHCP 策略 VLAN

在S6700上配置DHCP策略VLAN后，各接口所连接主机所属的VLAN是通过该主机的IP地址来匹配的。当一个新加入网络的主机连接到某一接口时，由于没有合法的IP地址，

所以它无法加入到对应的VLAN中。引入DHCP策略VLAN功能，是为了使新加入网络的主机能够通过DHCP服务器获得合法的IP地址，然后根据其IP地址划入到对应的VLAN中。

S6700支持的DHCP策略VLAN的配置方法：

- 配置普通DHCP策略VLAN。
- 配置基于MAC地址的DHCP策略VLAN。
- 配置基于接口的DHCP策略VLAN。

## Voice VLAN

Voice VLAN是指为用户的语音数据流划分的VLAN。用户通过创建Voice VLAN并将连接语音设备的接口加入到Voice VLAN中，使语音数据流集中在Voice VLAN中进行传输。

采用Voice VLAN的方式，便于对语音数据流进行有针对性的QoS配置，提高语音数据流的传输优先级，保证通话质量。

## VLAN Mapping

VLAN Mapping即VLAN映射。S6700根据预先建立好的VLAN Tag对应表，通过将数据帧中的外层VLAN Tag替换为其他VLAN Tag，实现用户业务按照运营商的网络规划进行传输。

S6700支持C-VLAN（Customer VLAN）与S-VLAN（Service VLAN）的一对一或多对一的映射关系。

 说明

- C-VLAN是用户侧接口对应的VLAN ID，用于标识一个或一类用户。
- S-VLAN是运营商侧的公网VLAN ID，用于标识一种业务。

### 3.1.5 QinQ

QinQ（802.1Q-in-802.1Q）协议是基于IEEE 802.1Q技术的一种二层隧道协议。由于在公网中传递的帧有两层802.1Q Tag（一个公网Tag，一个私网Tag），所以称之为QinQ协议。

通常，运营商负责规划公网VLAN，用户规划私网内的VLAN，导致不同私网内的VLAN空间可能存在重叠。通过S6700提供的QinQ功能，将私网用户报文进入公网后被添加公网的VLAN Tag，私网的VLAN Tag被隔离在内层，用户报文可以在公网内透明传输，实现私网和公网的有效分离。

目前，S6700支持两种方式实现QinQ功能。

- 基本QinQ功能。  
基于接口的QinQ，将该接口进入公网的所有帧只能加上相同的公网VLAN ID。
- 灵活QinQ功能。  
该功能是对QinQ的功能进行了扩展，使得接口可以根据私网VLAN Tag自由地选择外层VLAN Tag，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。例如，来自不同VLAN的所有语音业务都被标记为相同的外层VLAN Tag，从而得到相同的服务；普通数据业务被标记为不同的VLAN Tag，从而得到不同的服务。

## 3.1.6 GVRP

GVRP是一种VLAN动态注册/注销的协议。GVRP维护交换机中的VLAN动态注册信息，并通过GARP协议，将VLAN信息传播到网络中的其它的交换机中。

GVRP特性使得网络中的VLAN部署可以由协议动态维护和更新，用户无需耗费大量时间进行拓扑分析和配置管理，只需要对少数设备进行配置即可自动应用到整个网络。

S6700支持GARP机制和GVRP协议，支持通过GVRP协议，将本地VLAN向外声明，支持收到VLAN注册消息之后，动态创建VLAN。

## 3.2 STP/RSTP/MSTP

### 3.2.1 STP 和 RSTP

STP（Spanning Tree Protocol）和RSTP（Rapid Spanning Tree Protocol）都属于数据链路层的管理协议，主要应用于存在环路的局域网。STP通过算法有选择性地阻塞网络冗余链路，将网络修剪成树状，达到消除环路的目的。RSTP是STP的扩展，提供了状态快速迁移机制，大大缩短了网络拓扑收敛的时间。

采用STP和RSTP技术，既可以消除由于网络环路而带来的广播风暴，又为数据的转发提供冗余备份链路。

### 3.2.2 MSTP

MSTP（Multiple Spanning Tree Protocol）在STP和RSTP基础上发展起来。MSTP把一个交换网络划分成多个域，每个域内根据VLAN Tag可以形成多个相互独立的生成树，从而将环路网络修剪成为一个无环的树型网络，避免报文在环路网络中的增生和广播风暴。

通过把VLAN和生成树关联起来，MSTP可以让各VLAN沿着不同生成树路径转发报文，既可以快速收敛，又提供了负载分担机制。

与STP和RSTP相比，MSTP提供了数据转发的多个冗余路径，在数据转发过程中实现了按照VLAN的负载均衡。

### 3.2.3 MSTP 保护功能

#### BPDU 保护

S6700上的MSTP提供BPDU保护功能。当S6700上启动BPDU保护功能，如果边缘接口收到BPDU协议报文，S6700会将这些接口关闭，而不是将这些接口设置为非边缘接口，从而避免重新计算生成树，防止网络拓扑震荡。

#### Root 保护

S6700上的MSTP提供Root保护功能。S6700通过维持指定接口的角色来保护根设备的地位。

当使能了Root保护功能的接口收到优先级更高的BPDU协议报文时，接口角色不会变为非指定接口，仅仅进入侦听状态，不再转发报文。待接口长时间不再接收到优先级较高的BPDU协议报文后，该接口重新恢复到正常状态，从而避免网络拓扑震荡。

## 环路保护

在S6700上启动环路保护功能后，如果根接口收不到来自上游的BPDU协议报文时，根接口会被设置进入阻塞状态。原先的阻塞接口如果能接收到BPDU协议报文则变为根接口，并进入转发状态；原先的阻塞接口如果收不到BPDU协议报文，阻塞接口则会一直保持在阻塞状态，不转发报文，从而不会在网络中形成环路。

## 3.2.4 局部 STP 和 BPDU 隧道

### 局部 STP

在企业网中，为了提高链路可靠性，S6700通过双归属方式汇聚到上游以太网。为了消除环路，在整个企业网中运行MSTP。传统方式下不细分MSTP网络，此时整个网络规模过大，MSTP收敛速度慢，网络转发数据能力降低。

S6700逻辑上将每个局部STP网络划分到一个VLAN。通过为BPDU报文添加该VLAN的Tag，BPDU报文只能在它所属的VLAN内转发。这种限制BPDU报文传送范围的方法就称为局部STP功能，不仅消除了环路，而且解决了收敛速度慢的问题。

### BPDU 隧道

所谓BPDU隧道功能，是指实现局部STP时，S6700将带Tag的BPDU报文视为普通二层数据帧并在所属VLAN内转发，而不将该数据帧当成BPDU报文上送本机MSTP模块进行处理。实现BPDU隧道，城域网内的设备不参与局部STP拓扑计算，提高了协议的收敛效率。

在实现BPDU隧道功能时，城域网接入边缘的设备提供MSTP Snooping功能。当局部STP拓扑改变导致转发链路切换时，这些设备可以监听到拓扑变化，并将此变化通知本网络中其它设备，从而根据新拓扑链路进行转发。

## 3.3 RRPP

RRPP（Rapid Ring Protection Protocol）是一个专门应用于以太网环的链路层协议，它在以太网环中能够防止数据环路引起的广播风暴。和STP等协议相比，启动RRPP协议的拓扑收敛速度非常快，因为其协议报文是由硬件转发的。

此外，RRPP环还支持链路捆绑，可广泛应用在大带宽环形网络中。

### 3.3.1 RRPP 环网组成

具有相同ID标识、相同控制VLAN的一组S6700构成一个RRPP域。一个RRPP域主要具有如下组成要素：

- 一个RRPP环物理上对应一个环形连接的以太网拓扑，一个RRPP域由彼此相接的多个RRPP环构成，其中有一个为主环，其它环为子环。
- 每个RRPP域具有两个控制VLAN，分别称为主控制VLAN和子控制VLAN，分别传输主环和子环的协议报文。
- 控制VLAN只用来传递RRPP协议报文；数据VLAN用来传输数据报文。
- 主节点是轮询机制的发起者，也是网络拓扑发生改变后进行操作的决策者。
- 传输节点负责监测和自己连接的RRPP链路状态，并把链路变化通知主节点，然后由主节点来决策如何处理。

## 3.3.2 RRPP 工作机制

主节点在环上的两个接口分为主接口和辅接口。主节点通常周期性从主接口发送环的Hello报文，如果主节点在辅接口上接收到自己发送的Hello报文，主节点认为环网处于完整状态，则立刻阻断辅接口以保证消除环路。

若在一定周期内，主节点未在辅接口上接收到自己发送的Hello报文，主节点认为环网处于故障状态，则会重新开启辅接口使其正常转发业务。

## 3.3.3 多种拓扑结构

### RRPP 单环

网络中只包含一个以太网环，对应一个RRPP域。此时，拓扑改变时反应速度快，不仅可以实现RRPP环状态快速收敛，而且二层和三层业务可以快速倒换。

### RRPP 相切环

网络中有两个或两个以上的以太网环，两级环之间只有一个公共节点，各环分属于不同的RRPP域。

该组网适合网络规模较大，同级网络需要分区域管理。当一个环出现故障或恢复时，不影响其它域，且本域内RRPP环的状态收敛与单环收敛过程是一样的。

### RRPP 相交环

网络中有两个或两个以上的以太网环，两级环之间有两个公共节点，各环同属于一个RRPP域。其中一个作为主环，其它为子环。

子环的协议报文需要通过跨越主环的两个子环边缘接口之间的通道进行传输，可以将整个主环看作是子环上的一个节点。该组网多用于双归属汇聚应用，提供上行链路备份。

### RRPP 与其它网络的混合组网

当RRPP环与STP环邻接时，为了避免RRPP与STP在计算接口阻塞、开启状态时产生资源冲突，目前只支持RRPP环与STP环相切的组网，不支持二者相交的组网。

## 3.4 Smart Link

Smart Link是一种灵活的链路备份机制，为链路双上行（也称为双归属）提供高效可靠的解决方案。相比STP，Smart Link提供更快速的收敛性能。相比RRPP，Smart Link在双归属网络中提供了更简洁的配置方法。

在双上行组网中，Smart Link实现主链路故障后的快速倒换。正常情况下，两条上行链路中一条为主用，一条为备用，即一个接口处于转发状态另一个接口被阻塞。当主用链路故障时，Smart Link组会将流量快速切换到备用链路。

Smart Link支持手动和自动两种模式的链路倒换。链路故障后，Smart Link组发送Flush报文通知周边其他设备刷新MAC表和ARP表。

当多台设备形成逐层汇聚连接时，引入接口联动机制的Monitor Link能够监控上行链路，从而使Smart Link链路备份功能更加完善。在发现上行链路故障时，Monitor Link将触发关闭下行接口；当上行链路恢复正常时将重新开启下行接口，从而实现业务传输路径的整体倒换。

## 3.5 SEP

半环保护协议SEP（Smart Ethernet Protection），是一种专用于以太网链路层的环网协议。SEP协议以SEP段为基本单位。所谓SEP段，就是由一组配置了相同的SEP段ID和控制VLAN且互连的二层交换设备群体构成。

城域网和企业网大多采用环网来构建以提供高可靠性，但环上任意一个节点发生故障都会影响业务。环网采用的技术一般是RPR或以太网环。RPR需要专用硬件，因此成本较高。而随着以太网环的日趋成熟，成本低廉，城域网和企业网采用以太网环的趋势越来越明显。

为了实现开放环、封闭环等组网的保护倒换，支持非固定阻塞点及环网网络拓扑查看，华为公司推出了SEP协议。相比其他以太环网技术，SEP具有以下优势。

- 支持与STP/RSTP/MSTP/RRPP协议混合组网。
- 解决了流量单通问题。
- 流量单通可能产生单向广播风暴，为了避免单向广播风暴产生，可在网络中部署SEP协议。因为SEP协议能够有效地检测出流量单通。
- 支持网络中的拓扑查看，以SEP段为单位显示网络的拓扑结构。
- 在特定应用场景中，SEP可以成功破环且不依赖于其他设备制造商的设备。

## 3.6 ERPS

在二层交换网络中，一旦网络存在环路就会造成报文在环路内不断循环和增生，产生广播风暴。在广播风暴的情况下，所有的有效带宽都被广播风暴占用，网络变得不可用。

ERPS又称G.8032，G.8032作为以太保护协议，通过选择性地阻塞网络冗余链路，阻止环形网络形成逻辑环路，达到消除环路的目的。

G.8032 V1版本仅支持单环拓扑。当环网上没有故障链路时，G.8032能够消除以太网冗余环路。当环网发生链路故障时，G.8032能够迅速恢复环网上各节点间通信通路。与其它环路协议相比，G.8032有以下优势：

- 收敛速度快。
- ITU-T发布的标准，可以满足和其他设备厂商之家的互通。

## 3.7 接口安全保护

接口安全保护是一种对网络接入进行控制的安全机制，主要是检测接口接收到的数据帧的源MAC地址是否是安全MAC地址，发现非法报文并采取相应的保护动作，从而保护接口的安全。

S6700在接口上配置接口安全保护功能后，认为3种MAC地址是合法的：

- 手工配置的静态MAC地址。
- DHCP Snooping绑定表中的动态或静态MAC地址。
- MAC地址学习数量未达到限制前，学习到的动态MAC地址。

接口上收到非法源MAC地址的报文，则S6700的接口安全保护会起作用，进行相应的丢弃或告警操作。

## 3.8 链路检测

链路检测包括端口自环检测和电缆检测VCT（Virtual Cable Test），两者从不同的角度和范围给用户提供了检测局域网链路的手段。

- 端口自环检测主要用来检测局域网中是否存在环路，交换机通过发送特定的报文来发现网络中的环路，它面向的是整个局域网。
- 电缆检测主要实现对网线长度的估计和故障点的定位，模拟雷达的检测方式来检测电缆故障和故障点的位置，它所面向的是单条链路。

# 4 业务特性

---

## 关于本章

- 4.1 IPv4转发
- 4.2 IPv6
- 4.3 路由协议
- 4.4 组播
- 4.5 QoS
- 4.6 安全
- 4.7 MAC强制转发
- 4.8 DHCP
- 4.9 网络级可靠性
- 4.10 LLDP
- 4.11 NQA
- 4.12 堆叠

## 4.1 IPv4 转发

### 4.1.1 IPv4 特性

S6700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等。
- 支持静态DNS和指定DNS服务器。
- 提供FTP Server/Client、TFTP Client、SSH。
- 支持ping、tracert和NQA（Network Quality Analysis）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。
- 支持DHCP Server、DHCP Relay、DHCP Client和DHCP Snooping。
- 支持BFD快速检测功能。支持BFD for OSPF,BFD for ISIS,BFD for BGP,BFD for PIM。

### 4.1.2 单播路由特征

S6700产品支持的单播路由特性如下：

- 支持通过底层ASIC芯片实现IPv4单播线速转发。
- 支持IPv4路由协议：RIP v1/v2、OSPF、IS-IS和BGP4。
- 支持VRF(Virtual Routing Forwarding)。
- 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。
- 通过完善的路由策略功能决定最佳路由。

### 4.1.3 组播路由特性

S6700支持组播，可大大节省网络带宽，减轻网络负荷。并且组播流具有QoS保证，组播流转发性能为线速。

- 支持通过底层ASIC芯片实现IPv4组播流线速转发。
- 支持的组播协议：IGMP、PIM-SM、PIM-DM、MSDP、MBGP等协议。
- 同时支持ASM和SSM模型。
- 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。通过向最近的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。
- 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PIM BFD功能。
- 支持RPF检查。

## 4.2 IPv6

提供IPv6功能，在最大可能性上保护用户的投资，在网络升级的过程中，避免用户对设备的重复投入。

S6700设备支持的IPv6功能包括：

- 支持IPv6协议栈。
- 支持单播路由协议：RIPng/OSPFv3/BGP+/ISISIPv6。
- 支持VRRP6。
- 支持IPv4/IPv6过渡技术。
- 支持DHCPv6 relay、DHCPv6 server。
- 支持PIM-IPv6-DM、PIM-IPv6-SM和PIM-IPv6-SSM。
- 支持MLDv1、MLDv2。

## 4.3 路由协议

S6700支持丰富的单播路由特性：

- 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。
- 支持基于IPv4的动态路由协议。
  - RIP（Routing Information Protocol）
  - OSPFv2（Open Shortest Path First）
  - IS-IS（Intermediate System-Intermediate System）
  - BGP-4（Border Gateway Protocol）
- 支持基于IPv6的动态路由协议。
  - OSPFv3
  - RIPng
  - BGP+
  - ISISIPv6
- 通过完备的路由策略功能决定最佳路由。

## 4.4 组播

IGMP（Internet Group Management Protocol）是负责IP组播成员管理的协议，它用来在IP主机和与其相邻的组播路由器之间建立、维护组播组成员关系。

### 4.4.1 IGMP Snooping/MLD Snooping

S6700部署在用户主机和组播路由器之间，不仅可以静态配置二层组播转发表项，还可以通过侦听交互的IGMP/MLD消息维护组播组、VLAN和出接口之间的对应关系，动态构建组播报文的二层转发表。

当S6700收到组播数据包后，依据二层组播转发表，组播报文只会向VLAN内有组成员的端口转发，不仅减少了相同组播报文数量，节省了带宽，而且提高了信息传送的安全性。

## 4.4.2 IGMP Snooping Proxy

IGMP Snooping Proxy被部署在路由器和主机之间的交换机上，具有代理服务器功能。终结主机发往路由器的IGMP协议报文，代替用户主机响应路由器的查询报文。同时通过处理路由器和用户主机的IGMP协议报文，形成二层组播转发表项，实现二层组播。

## 4.4.3 组播成员接口快速离开

组播成员离开时会触发主机发送IGMP/MLD离开消息。对于只连接一台主机的S6700接口，当S6700接收到IGMP/MLD离开消息时，就立即删除该接口对应的二层组播转发表项。不仅节约了带宽和系统资源，还可以实现业务的快速切换。

## 4.4.4 组播流量控制

对于未知组播报文，即二层组播转发表中不存在对应转发表项的组播报文，S6700可以根据需要进行丢弃或在接口所属VLAN内广播发送两种策略。

同时，S6700还可以在入方向控制以太网接口上的最大组播流量百分比/PPS，从而控制组播业务的流量。

## 4.4.5 跨 VLAN 组播复制

所谓跨VLAN组播复制，是指使用组播VLAN来汇聚组播流，并将组播流复制到多个用户VLAN中。

S6700将去往各用户的组播流通过组播VLAN来下发，然后在分发点根据二层组播转发表进行组播流复制并分发到各用户VLAN中去。跨VLAN组播复制技术将用户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。

## 4.4.6 可控组播

组播协议中没有提供用户认证支持，用户可以随意加入一个组播组，并可以任意离开。组播源无法知道用户何时加入、何时退出，无法统计出某个时间网络上共有多少个用户在接收组播流量，也就无法对用户进行计费。为了解决这些问题，引入可控组播技术，通过对用户的认证，使只有通过认证的用户才能接收组播数据；用户只能接收被授权的组播流。同时允许认证通过的用户，对没被授权的组播流进行预览，在一天之内，可以间隔地多次接收指定时长的组播流。可控组播对静态配置的组播流不作控制。

## 4.5 QoS

S6700提供基于类的QoS机制，支持802.1p优先级，可实现端到端的时延、抖动和带宽保证。

S6700首先按照某种规则对流量进行分类，对于分类后的报文流提供重标记、流量监管、拥塞管理、拥塞避免和接口限速等功能，从而为NGN、IPTV、宽带接入等增值业务提供优质网络服务。

### 4.5.1 流分类

流分类是对封装报文的头部信息和一定规则进行匹配，识别出符合某类特征的报文。例如将OSS（Operating Support System）和NMS网管报文的802.1p优先级被标识为7，将VoIP语音报文的802.1p标识为6，将BTV和VOD视频报文的802.1p标识为5或4，将VPN用户按照重要等级分别表示为3、2或1，将Internet上网业务的802.1p标识为0。从而通过802.1p实现各种业务报文的分类。

S6700采用硬件分类器，保证了各接口线速收发业务数据。

## 简单流分类

在S6700上，用户可以根据DiffServ（Differentiated Services）域中定义的报文优先级与PHB(Per-Hop Behavior)行为之间的映射关系对报文进行简单流分类。对于来自上游设备的报文，在报文的入接口上绑定DiffServ域，在DiffServ域中将报文携带的优先级信息映射到相应的PHB行为、颜色，在设备内部，根据报文的PHB行为进行拥塞管理，根据报文的颜色进行拥塞避免；对于流向下游设备的报文，在报文的出接口上绑定DiffServ域，在DiffServ域中将报文的PHB行为、颜色映射为相应的优先级，下游设备根据报文的优先级提供相应的QoS服务。

简单流分类的分类依据有：

- IP报文中的DSCP优先级
- VLAN报文中的802.1p优先级

## 复杂流分类

用户可以根据报文中携带的二层信息、三层信息或者借助ACL（Access Control List）进行复杂流分类，然后将复杂流分类与某种流行为关联，对符合流分类的报文进行相应处理。

具体采取何种流行为，与报文所处的阶段以及网络当前的负载状况有关。例如，当报文流入S6700时依据承诺速率对它进行流量监管、访问控制；流出S6700之前进行流量整形、重标记等。

复杂流分类的分类依据有：

- VLAN报文中的802.1p优先级
- VLAN报文中的VLAN ID
- VLAN报文中的双层Tag
- 出/入接口
- IP报文中的IP优先级
- IP报文中的DSCP优先级
- TCP报文中的SYN Flag
- 源MAC地址
- 目的MAC地址
- 基于二层封装的协议字段
- 三层协议类型
- IP五元组信息

### 4.5.2 访问控制和重标记

对于流分类后的报文，S6700首先对报文进行访问控制，即允许或禁止该报文转发。然后，S6700对通过报文中的如下信息进行重标记：

- 802.1p优先级（VLAN Tag中的PRI字段）
- DSCP字段
- IP报文的优先级字段

- VLAN ID（QinQ报文中的外层或内层VLAN ID）
- 报文的D-MAC地址

### 4.5.3 流量监管

S6700借助漏桶算法实现CAR（Committed Access Rate）机制，对进入流量进行监管和控制。

通过调节投放令牌的速率来控制流量速率，一个令牌相当于64kbit/s的转发速率。S6700对超出部分的流量进行“惩罚”，使进入的流量被限制在一个合理的范围之内，从而保护网络资源。

### 4.5.4 拥塞管理

S6700借助队列调度技术实现拥塞管理。S6700的每个出接口上都拥有8个队列，流分类后的报文按照优先级自动地被送入各队列。

S6700支持5种队列调度策略：

- PQ（Priority Queuing）
- WRR（Weight Round Robin）
- DRR（Deficit Round Robin）
- PQ+WRR
- PQ+DRR

### 4.5.5 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。

S6700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。

### 4.5.6 接口限速

接口限速是一种主动调整接口上流量接收或发送速率的措施，防止了流量突发，降低了丢包率。S6700结合令牌桶和缓冲区实现了接口限速，具有一定的流量整形能力。通过对超出速率限制的报文进行缓冲，S6700可以在空闲的时候将被缓冲的报文发送出去，从而平滑报文的发送速率。

### 4.5.7 支持双速三色

根据流分类的结果，对该流的流量进行控制，超出流量限制的报文丢弃。S6700支持双速三色算法，可配置四个主要参数：

- 承诺信息速率（Committed Information Rate），即保证能够通过速率。
- 承诺突发尺寸（Committed Burst Size），即瞬间能够通过承诺流量。

- 峰值速率（Peak Information Rate），即最大能够通过速率。
- 超出突发尺寸（Peak Burst Size），即瞬间能够通过峰值流量。

除此以外，还支持根据流量情况对报文着色（红、绿、黄），并配置对不同颜色指定不同的动作（允许通过或者丢弃），以及对报文进行重标记。

## 4.5.8 支持聚合 CAR

聚合CAR是指能够对多个接口上的业务流使用同一个CAR进行流量监管，即如果多个接口应用同一聚合CAR，则这些接口的流量之和必须在此聚合CAR设定的流量监管范围之内。

## 4.6 安全

S6700不仅提供设备级安全，而且可以为传输的业务提供安全。

### 4.6.1 设备的安全

#### 命令行分级保护

用户从以太网口通过Telnet方式登录S6700时，出于安全性考虑，S6700需要对登录用户进行验证。只有验证通过的用户才能登录成功，并进行各种配置和维护操作。

S6700的命令行采用分级保护方式，命令行划分为参观级、监控级、配置级、管理级4个级别，等级逐级升高。登录用户对应的也被划分为4个等级，分别与命令级别对应。不同级别的用户登录S6700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。

S6700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。

#### SSH 远程安全登录

S6700支持SSH（Secure Shell）。在不保证安全的网络环境中，SSH为用户登录S6700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

S6700支持SNMPv3加密认证功能。当S6700在接受网管站SNMP管理时，可以通过基于USM（User-based Security Mode）的加密认证模式来保障S6700的安全。

#### AAA 身份验证

S6700支持完善的AAA（Authentication, Authorization and Accounting）机制，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，S6700可以有效防止非法用户登录。

认证的方式包括：Local、RADIUS、HWTACAS+等。

#### CPU 通道保护

对于上送CPU的协议报文和管理报文，S6700根据协议号、接口及VLAN和接口组合信息对各类报文进行过滤，从而避免CPU通道受到DoS（Denial of Service）攻击而阻塞。

## 接口 MAC 地址学习限制

通过在S6700指定端口上配置MAC表项学习的最大数目，可以避免黑客从该接口发起源MAC地址攻击，从而确保整个S6700设备的MAC表资源不被耗尽。

## 4.6.2 业务的安全

### 划分 VLAN

S6700支持VLAN划分，VLAN间各设备不能互相通信，有效地隔离了广播域，增强了信息的安全性。

### 黑洞 MAC 表项

S6700支持黑洞MAC功能。S6700接收到的某报文后，会将该报文的源MAC地址或者目的MAC地址和MAC表中各项比较，如果和黑洞MAC表项相同则将该报文丢弃。

当用户察觉到某MAC地址的报文具有一定攻击性，则可以在S6700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“VLAN + MAC”的查表方式

为了提高接口安全性，S6700采用“VLAN+MAC”的查表方式。网络管理员在MAC地址表中加入静态表项，记录特定MAC地址和接口的对应关系。这种查表方式可以将设备与接口绑定，防止MAC地址仿冒的攻击。

### 端口隔离

端口隔离是指禁止同一S6700上各端口之间互相收发二层报文，支持单向和双向隔离。采用端口隔离技术，可以防止端口之间的彼此访问，确保了用户网络的安全，有助于低成本构建智能小区网络。同时，隔离技术还可以有效地控制不必要的广播，增加网络吞吐量。

### 包过滤

包过滤用于过滤那些用户不感兴趣或者不合法的数据包。

S6700对每个数据包按照用户所定义的项目进行过滤，如比较数据包的MAC地址、IP地址、端口号、VLAN等信息是否符合规则等。包过滤不检查会话的状态，也不分析数据。通过包过滤方法，S6700可以有效控制通过设备的数据包。

## 4.6.3 安全认证

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

MAC地址认证是一种基于接口和MAC地址对用户访问网络的权限进行控制的认证方法，它不需要用户安装任何客户端认证软件。设备在首次检测到用户的MAC地址以后，即启动对该用户的认证操作。认证过程中，不需要用户手动输入用户名或者密码。

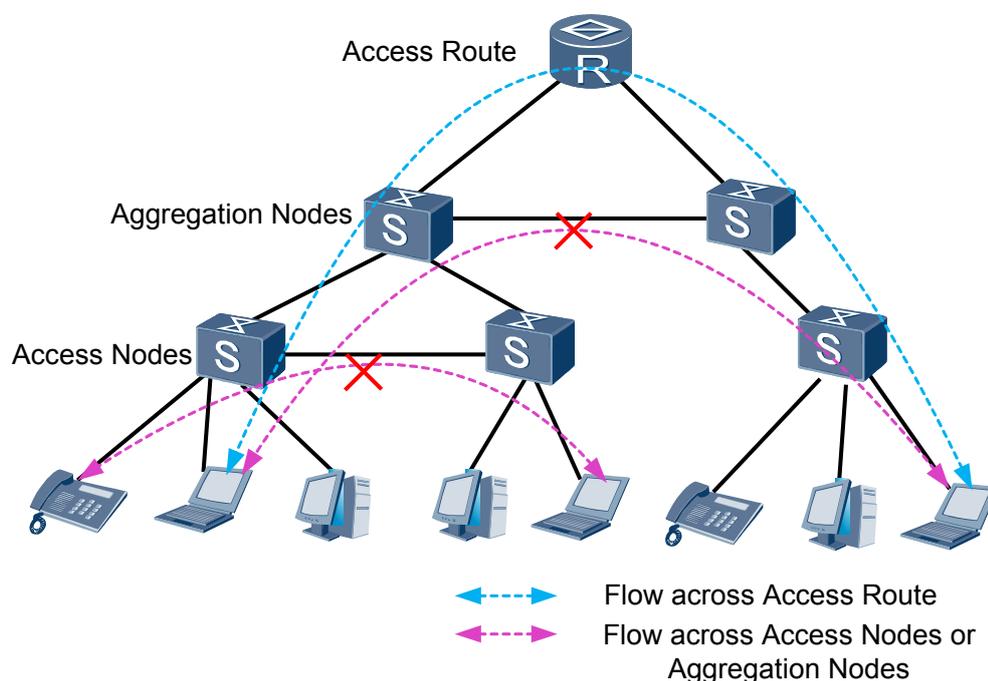
## 4.7 MAC 强制转发

接入层的主要目的是提供用户侧主机和企业网侧接入路由器（AR）之间的网络连接，尤其是提供到互联网和其他IP网络的可靠连接。

接入层可以被划分为用户网络和汇聚网络。用户网络通过用户线与接入结点（AN）连接，用户线是一条物理连接线，即通常所说的“第一公里”。

AN将用户线和汇聚网络连接起来。这样，AN就成为用户线和汇聚网络的边界。汇聚网络实现用户流量的集中和聚合，即经常提到的“第二公里”。请参考图4-1。

图 4-1 接入层连接示意图



对于接入层，企业网有如下两个基本需求：

- 为了使企业网能够借助AR实现对用户流量进行安全过滤，策略调度和计费。需要通过AR对位于不同网络、不同用户主机的流量进行三层转发，而不能通过二层交换。
- 为了减少IPv4地址的过度消耗，有必要提高地址分配的效率。如果是从某个大的地址池中分配主机地址，而不是从相对独立的小网段中分配，那么就需要改善地址分配的有效性。

为了解决接入层用户隔离，实现企业网的上述两个基本需求，产生了MFF（MAC-Forced Forwarding）协议。

MFF协议是一个安全协议，确保共享接入介质的用户主机实现二层隔离。当运行MFF协议时，其安全程序适合任何共享接入介质，不会给这些网络引入任何额外的缺陷。

除了二层隔离，运行MFF协议的AN还会丢弃除了有效的DHCP报文和ARP请求报文以外的任何上行广播报文。特别是会丢弃从用户线接收到的DHCP服务器响应报文。而且，AN会针对DHCP广播报文进行限速。

运行MFF协议的AN必须跟踪了解分配给用户线的IPv4地址，以便充分掌握丢弃带有欺骗IPv4源地址的上行流量信息。

## 4.8 DHCP

### DHCP Client 和 DHCP Server

DHCP协议采用客户端/服务器（Client/Server）的方式工作，DHCP Client向DHCP Server动态请求配置信息。DHCP Server根据地址池策略返回Reply报文。

DHCP服务器通过地址池给用户分配IP地址。当客户端向服务器发出DHCP请求时，DHCP服务器选择合适的地址池，并从中挑选一个空闲的IP地址，与其他相关参数（如网关地址、DNS服务器地址、地址租用期限等）一起传送给客户端。

如果需要动态分配给客户端IP地址，首先需要配置地址池范围。目前，同一地址池中只能配置一个地址段，通过掩码设定地址范围的大小。

### DHCP Snooping

S6700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，根据监听记录建立IP+MAC+PORT+VLAN绑定表，抑制非法报文。

同时，S6700支持Option82选项功能。

- S6700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，S6700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。

在S6700上，Option82有两种实现方法：Option82 insert和Option82 rebuild。

由于Option82选项记录了用户电路ID，用户电路ID中携带了用户设备名称、内外层VLAN ID、端口等信息，因此可以有效避免攻击者非法篡改DHCP报文。

### DHCP 中继

由于DHCP Client和DHCP Server在IP地址动态获取过程中采用广播方式发送报文，因此DHCP协议只适用于DHCP客户端和服务器处于同一个子网内的情况。为进行动态主机配置，需要在各网段上均设置一个DHCP服务器，这显然是很不经济的。

DHCP中继功能的引入解决了这一难题：子网内的客户端可以通过DHCP中继与其他子网的DHCP服务器通信，最终获取到IP地址。这样，多个网络上的DHCP客户端可以使用同一个DHCP服务器，既节省了成本，又便于进行集中管理。

## 4.9 网络级可靠性

## 4.9.1 MSTP 保护倒换

S6700支持MSTP技术，既可以消除网络中的广播风暴，又为数据的转发提供冗余备份链路。

S6700提供Root保护功能。当接口接收到更高优先级的BPDU时，通过长时间维持指定接口的角色来保护根设备的地位，从而避免网络拓扑结构发生错误变动。

S6700提供环路保护功能。当根接口收不到来自上游的BPDU时，根接口会进入阻塞状态，不转发报文。同时，网络内不再选择新的根接口，从而避免在网络中形成环路。

## 4.9.2 RRPP 快速保护倒换

RRPP环可以用于双归属保护的网路中，可以部署在CE和UPE，或UPE和NPE之间，极大地节省了投资。

RRPP环由一个主节点和多个传输节点首尾相连而成。主节点从主接口定时向环路上发送协议报文来检测链路的状态，并且根据链路的实际状态来控制辅接口的打开和关闭，从而实现故障自愈。

当环上出现单点故障时，RRPP环能迅速启用备份链路，快速恢复环网上各个节点之间的通信通路。

## 4.9.3 Smart Link 双归属保护

S6700借助Smart Link技术双归属上行连接，同时该设备的下行链路形成Monitor Link，这种逐层汇聚连接实现了Smart Link和Monitor Link的状态联动。当不存在可用上行链路时，S6700将关闭下行接口，通过接口联动机制实现业务传输路径的整体快速倒换。

## 4.9.4 以太网 OAM

S6700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，S6700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。

S6700提供性能管理功能。性能管理主要是指对网络中的丢包、时延、抖动进行衡量，也包括对网络中各类流量进行统计。性能管理通常在用户接入点实施。有了性能管理工具，运营商可通过网管监测网络运行情况、定位故障，确认网络转发能力是否符合与用户签订的SLA（Service Level Agreement）。

以太网OAM能够有效提高以太网的网络管理能力和维护能力，保障网络的稳定运行。

## 4.10 LLDP

S6700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S6700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。

## 4.11 NQA

随着Internet的高速发展，网络支持的业务和应用日渐增多，传统的网络性能分析方法（如Ping、Tracert等）已经不能满足用户对业务多样性和监测实时性的要求。

S6700提供NQA（Network Quality Analysis）功能。NQA通过发送测试报文，对网络性能或服务质量进行分析，为用户提供网络性能参数，如时延抖动、HTTP的总时延、TCP连接时延、FTP连接时延和文件传输速率等。利用NQA的测试结果，用户可以：

- 及时了解网络的性能状况，针对不同的网络性能，进行相应的处理。
- 对网络故障进行诊断和定位。

## 4.12 堆叠

堆叠是将同一物理位置上的交换机通过堆叠电缆或高速业务口组成一个高可靠的设备组。S6700设备是通过10GE业务口复用为堆叠口实现堆叠的。通过堆叠，可以实现对交换机的集中管理和维护，降低用户的维护成本。堆叠要求参与堆叠的交换机必须是相同的设备形态。

堆叠成员有三种角色：

- 主交换机  
堆叠中只有一台主交换机，负责分配堆叠成员的编号，收集堆叠拓扑信息，并将拓扑信息通告给所有堆叠成员。
- 备交换机  
作为主交换机的备份，在主交换机发生故障的时候，升级为主交换机，并接手主交换机的工作。
- 从交换机  
相当于网络内的纯业务交换机，被动的接受管理。

# 5 特性组网应用

---

## 关于本章

- 5.1 数据中心应用
- 5.2 企业网络和园区网的汇聚
- 5.3 iStack技术的应用

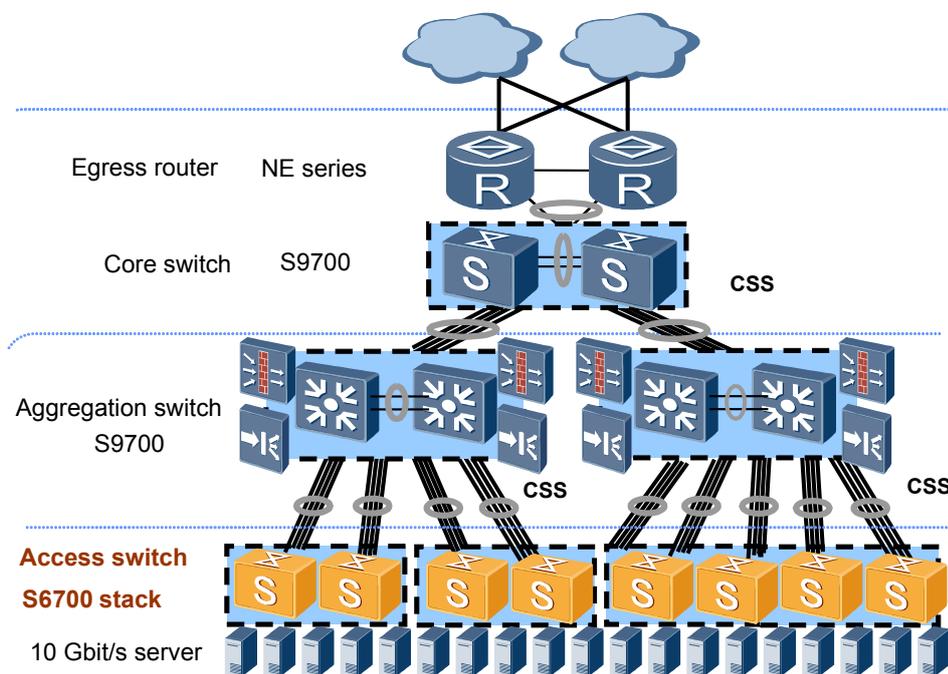
## 5.1 数据中心应用

S9700交换机作为数据中心核心和汇聚层交换机，NE系列路由器作为数据中心出口路由器，通过集成的防火墙、负载均衡等多业务板卡来实现安全保证和流量均衡。S6700作为接入层交换机提供万兆服务器接入方案。如**图5-1**所示。

S9700、S6700采用堆叠技术实现核心、汇聚、接入层交换机的高可靠性，一台设备故障后,另外一台设备自动接管所有的业务。

组网中采用Eth-Trunk实现链路级可靠性。不需要配置任何可靠性的协议，如STP/VRRP等，减化网络，减少故障几率。

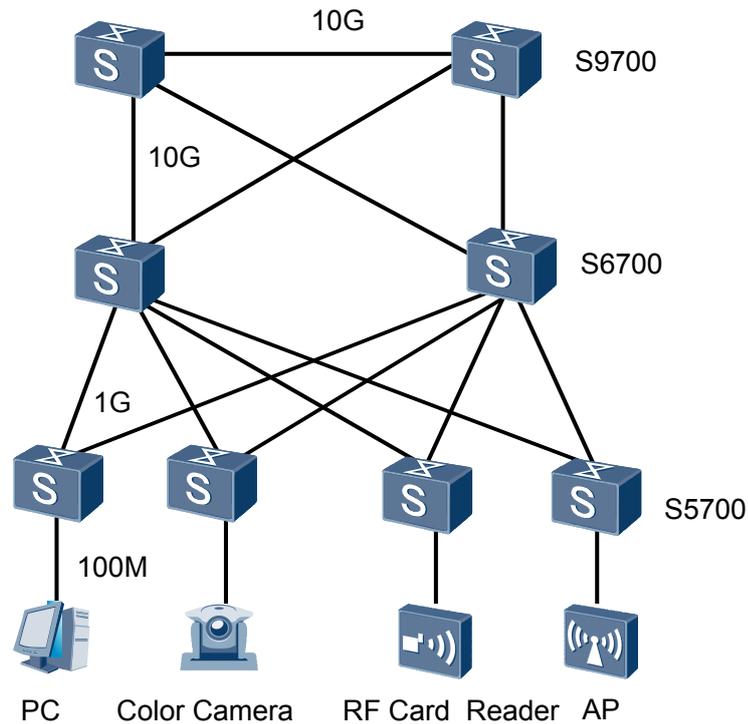
**图 5-1** S6700 在数据中心的应用



## 5.2 企业网络和园区网的汇聚

如**图5-2**所示，在企业网络和园区网中，S6700通过千兆接口接入交换机，上行通过万兆光口接入S9700核心交换机，构成万兆骨干、百兆到桌面的企业网全网解决方案，满足用户高带宽、多业务的需求。

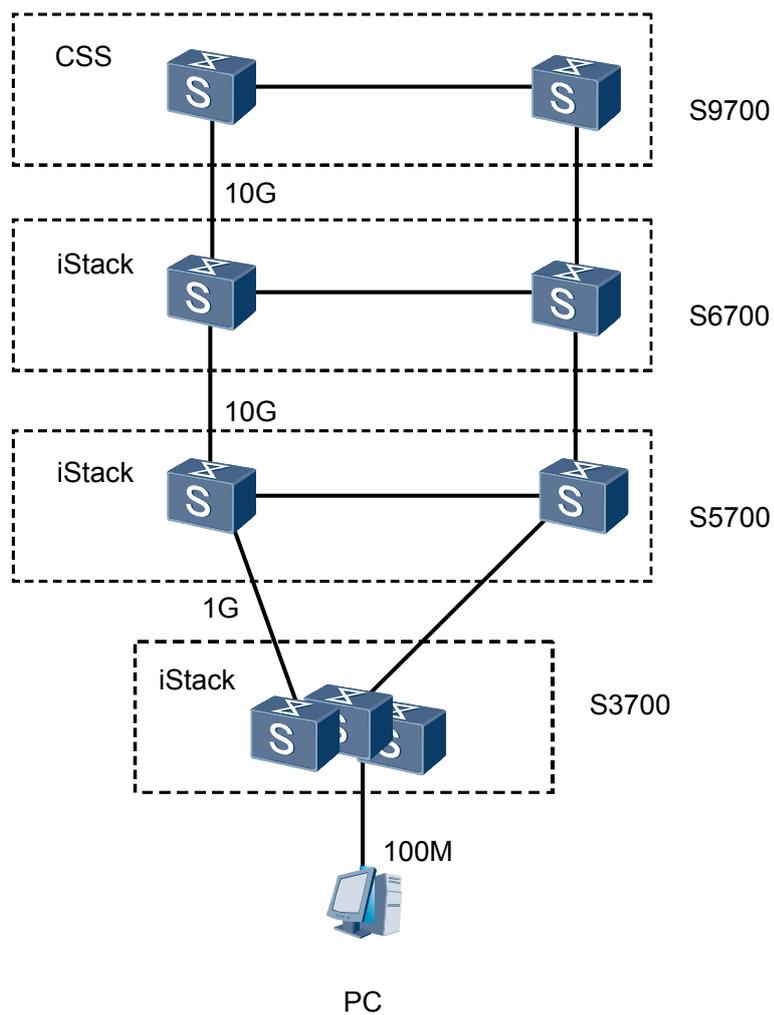
图 5-2 企业网络和园区网的汇聚



### 5.3 iStack 技术的应用

如图5-3所示，利用iStack技术可以实现接入层和汇聚层的高性能和高可靠性。S6700可以通过iStack技术构建堆叠系统，实现分布式转发架构和故障的快速自愈，并且可以在扩展用户端口的同时实现处理性能的同步提升，统一的设备管理，极大简化了网络管理和维护。

图 5-3 iStack 技术的应用



# 6 操作维护和网管系统

---

## 关于本章

[6.1 维护和管理](#)

[6.2 Web网管](#)

[6.3 eSight网管](#)

## 6.1 维护和管理

### 6.1.1 多种配置方式

#### 多种配置途径

S6700支持多种配置和管理方式：

- 命令行配置  
用户从控制台终端登录到S6700的Console接口，或者通过Telnet方式登录到管理网口，在CLI界面中配置各特性和参数。
- 网管配置  
用户通过网管站，基于SNMP协议对S6700进行管理和配置。
- AutoConfig配置  
在设备以空配置启动时，用户可以通过AutoConfig配置自动获取配置文件并执行。

#### 多种登录方式

S6700提供Console配置管理接口，控制台终端可以通过串口登录到Console接口，从而实现本地和远程配置。

另外，用户还可以从其它设备通过Telnet方式登录到S6700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。

### 6.1.2 监控和维护

#### 设备硬件监控

S6700提供多种设备硬件的监控功能：

- 温度出现异常时，系统将上报告警。
- 系统对硬件故障提供再次检测功能，避免瞬间的干扰导致检测结果错误。
- 系统运行中自动检查版本配套性。

#### 设备管理和维护

S6700提供多种设备管理和维护功能：

- 命令行提供灵活的在线帮助，支持中文、英文两种操作界面。
- 提供分级的用户权限管理及分级别的命令。
- 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。
- 提供电子标签功能。通过CLI命令行查询设备各交换主控板、光模块的基本信息，并且可以通过FTP将该信息备份到外部服务器上。

- 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。

## 6.1.3 诊断和调测

### Ping 和 TraceRoute

在传统IP网络中，S6700提供如下连通性测试工具：

- Ping
- TraceRoute

通过检查网络连接是否可达，在线记录数据包的传输路径，作为故障定位的参考。

### Debug 调试

S6700针对每个软件特性都提供丰富的debug调试命令，每条debug命令支持多个调试参数，可以灵活控制。使用调试命令，可以详细输出该特性运行过程中的进程处理、报文收发、差错检验等信息。

### VCT

通过执行VCT测试命令，接口发出测试信号，根据TDR的特性，在一定时间后会收到反射信号。根据反射信号的特征，可以判断Cable的状态。

### 镜像功能

S6700支持单台设备上基于接口或基于报文流的镜像功能，还支持多台设备间基于接口的远程镜像功能：

- 接口镜像  
被观察接口上输入、输出或双方向上的报文原封不动地被复制到观察接口上。
- 流镜像  
被观察报文流原封不动地被复制到观察接口上。
- 远程镜像  
RSPAN（Remote Switched Port Analyzer，远程交换接口分析），即远程接口镜像，突破了被镜像接口和镜像接口必须位于同一台交换机的限制，使被镜像接口和镜像接口可以跨越网络中的多台设备，从而方便网管人员对远端设备进行管理。

外部监测主机和S6700的观察接口相连，网络管理员可以实时、便捷地观察到流经S6700的各类报文信息，为流量检测、故障分析定位、数据分析提供了依据。

## 6.1.4 软件升级和热补丁

### 软件升级

S6700支持在升级前检测系统软件的完整性和正确性，同时还能提供多种软件升级方式。

- 本地菜单升级  
在S6700上电启动过程中，通过BootROM菜单加载新软件，完成升级。
- 远程在线升级

S6700正常工作中，通过FTP或TFTP方式远程在线下载新软件，在重新启动S6700时引导运行新软件，从而实现远程平滑升级。

为了避免升级失败，S6700支持软件版本回退功能。

## 热补丁

S6700支持热补丁功能，打补丁过程中业务不受影响。热补丁支持回退功能，并能记录热补丁操作前后的设备信息。

此外，S6700提供补丁一键式操作，即根据单板槽位号快速得到补丁文件和系统软件的兼容性关系、补丁状态和补丁历史操作等信息。

## 6.1.5 硬件异常处理

S6700支持对硬件异常采取自动或人工干预，让维护人员及时了解设备各种异常状态（如单板的芯片异常），并对各种异常进行紧急处理，从而尽可能减少业务中断。

## 6.2 Web 网管

为了方便用户对S6700的维护和使用，推出Web网管功能。

Web网管通过在S6700内提供内嵌WebServer，用户可以通过WEB网管终端（PC）登录到S6700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S6700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。

## 6.3 eSight 网管

S6700支持eSight网管，作为企业网的统一网管。eSight提供全面的基础网络管理、网元管理、业务管理和系统管理功能。

华为eSight网管具有以下特点：

- 多厂商管理  
具有对多厂商设备的管理能力。
- 精细管理  
提供网流分析功能，聚焦核心业务。
- IT+IP统一管理  
统一管理应用软件系统、IT设备（服务器、打印机等）和网络设备。
- 面向用户的运维系统  
提供桌面安全管理、上网行为监控认证计费等功能。
- 二次开发平台  
提供二次开发平台，可按照客户需求灵活定制管理功能。
- 北向集成  
可与上层OSS系统北向集成。

# 7 系统技术指标

---

## 关于本章

- 7.1 规格参数
- 7.2 光模块属性
- 7.3 性能和容量
- 7.4 软件特性列表
- 7.5 遵循的标准与协议

## 7.1 规格参数

S6700系列设备的规格参数如表7-1所示。

表 7-1 规格参数说明表

规格		参数
处理器		主频1GHz
包转发能力 (按 1Gbps=1.5Mpps计 算)		<ul style="list-style-type: none"> <li>● S6700-24-EI: 360Mpps</li> <li>● S6700-48-EI: 720Mpps</li> </ul>
DDR内存		512MB
Flash Memory		64MB
平均无故障时间 MTBF (年)		<ul style="list-style-type: none"> <li>● S6700-24-EI: 34.54</li> <li>● S6700-48-EI: 33.76</li> </ul>
平均修复时间 MTTR (小时)		2
可用度		大于0.99999
防雷规格	业务口 防护	-
	电源口 防护	<ul style="list-style-type: none"> <li>● AC: 差模±2kV, 共模±4kV。</li> <li>● DC: 差模±1kV, 共模±2kV。</li> </ul>
外形尺寸 (宽×深 ×高)		442.0mm×420.0mm×43.6mm
重量	满配置	≤8.5kg
	空机箱	≤5kg
堆叠口		任意10GE SFP+接口 (最多支持8端口)
RPS		不支持
PoE		不支持
直流输入电压	额定电 压范围	-48V DC~-60V DC
	最大电 压范围	-38.4V DC~-72V DC
交流输入电压	额定电 压范围	100V AC~240V AC; 50/60Hz

规格		参数
	最大电压范围	90V AC~264V AC; 47Hz~63Hz
最大功率（满配置）		<ul style="list-style-type: none"> <li>● S6700-24-EI: 153.6W</li> <li>● S6700-48-EI: 240W</li> </ul>
温度	工作温度	-5° C~+50° C(0~1800米海拔) <b>说明</b> 海拔1800~3000米: 海拔每升高220米, 温度规格降低1℃。
	存储温度	-40° C~+70° C
常温噪声（23° C, 声功率）		小于55dBA
相对湿度		10%RH~90%RH, 无凝露
工作海拔高度		0m~3000m
EMC		<ul style="list-style-type: none"> <li>● CISPR22 Class B</li> <li>● CISPR24</li> <li>● EN55022 Class B</li> <li>● EN50024</li> <li>● ETSI EN 300 386 Class B</li> <li>● CFR 47 FCC Part 15 Class A</li> <li>● ICES 003 Class B</li> <li>● AS/NZS CISPR22 Class B</li> <li>● VCCI Class B</li> <li>● IEC61000-6-2</li> <li>● IEC61000-6-4</li> <li>● IEC61000-4-2</li> <li>● ITU-T K 20</li> <li>● ITU-T K 21</li> <li>● ITU-T K 44</li> </ul>
环境标准		<ul style="list-style-type: none"> <li>● RoHS</li> <li>● REACH</li> </ul>
安全		<ul style="list-style-type: none"> <li>● IEC 60950-1</li> <li>● EN 60950-1/A11/A12</li> <li>● UL 60950-1</li> <li>● CSA C22.2 No 60950-1</li> <li>● AS/NZS 60950.1</li> </ul>

规格	参数
激光安全	<ul style="list-style-type: none"> <li>● IEC60825-1</li> <li>● IEC60825-2</li> <li>● EN60825-1</li> <li>● EN60825-2</li> </ul>

## 7.2 光模块属性

表 7-2 GE 光模块的属性

型号	传输距离 (km)	标准	支持的光纤	支持的设备
eSFP-GE-SX-MM850	≤0.5	1000base-SX	<ul style="list-style-type: none"> <li>● 光纤模式：多模</li> <li>● 模式带宽：400MHz*km</li> <li>● 光纤直径：62.5/125μm</li> <li>● 接头类型：LC</li> </ul>	<ul style="list-style-type: none"> <li>● S6700-24-EI</li> <li>● S6700-48-EI</li> </ul>
SFP-GE-LX-SM1310	≤10	1000base-LX/LH	<ul style="list-style-type: none"> <li>● 光纤模式：单模</li> <li>● 接头类型：LC</li> </ul>	
S-SFP-GE-LH40-SM1310	≤40			
S-SFP-GE-LH40-SM1550				
S-SFP-GE-LH80-SM1550	≤80	1000base-ZX		
eSFP-GE-ZX100-SM1550	≤100			
SFP-GE-LX-SM1310-BIDI (单纤双向)	≤10	1000base-BX		
SFP-GE-LX-SM1490-BIDI (单纤双向)				
LE2MGSC40DE0 (单纤双向)				

型号	传输距离 (km)	标准	支持的光纤	支持的设备
LE2MGSC40ED0 (单纤双向)	≤40			

表 7-3 CWDM 光模块的属性

中心波长 (nm), 型号	1471, eSFP-LH80-SM1471	1491, eSFP-LH80-SM1491	1511, eSFP-LH80-SM1511	1531, eSFP-LH80-SM1531
	1551, eSFP-LH80-SM1551	1571, eSFP-LH80-SM1571	1591, eSFP-LH80-SM1591	1611, eSFP-LH80-SM1611
属性和参数	接口封装: eSFP			
	传输距离: ≤80km			
	支持的光纤: 单模, LC			
	标准: CWDM			
	工作温度: 0° C~70° C			
	<ul style="list-style-type: none"> <li>● 发送光功率: 0dBm~5.0dBm</li> <li>● 接收灵敏度: ≤-28.0dBm</li> <li>● 过载光功率: -9.0dBm</li> <li>● 消光比: 8.5dB</li> </ul>			
支持的设备	<ul style="list-style-type: none"> <li>● S6700-24-EI</li> <li>● S6700-48-EI</li> </ul>			

表 7-4 GE 光电模块的属性

型号	传输距离 (km)	接头类型	标准	工作温度	支持的设备
SFP-1000BaseT	≤0.1	RJ45	1000Base-T	-40° C~85° C	<ul style="list-style-type: none"> <li>● S6700-24-EI</li> <li>● S6700-48-EI</li> </ul>

表 7-5 10GE SFP+光模块的属性

型号	传输距离 (km)	标准	支持的光纤	支持的设备
OSXD22N00	≤0.22	10Gbase-LRM	<ul style="list-style-type: none"> <li>● 光纤模式：多模</li> <li>● 模式带宽：500MHz*km</li> <li>● 光纤直径：62.5μm或50μm</li> <li>● 光纤等级：OM1, OM2, OM3</li> <li>● 接头类型：LC</li> </ul>	<ul style="list-style-type: none"> <li>● S6700-24-EI</li> <li>● S6700-48-EI</li> </ul>
OMXD30000	≤0.3	10Gbase-SR	<ul style="list-style-type: none"> <li>● 光纤模式：多模</li> <li>● 模式带宽：2000MHz*km</li> <li>● 光纤直径：50μm</li> <li>● 接头类型：LC</li> </ul>	
OSX010000	≤10	10Gbase-LR	<ul style="list-style-type: none"> <li>● 光纤模式：单模</li> <li>● 接头类型：LC</li> </ul>	
OSX040N01	≤40	10Gbase-ER		
SFP-10G-BXU1 (单纤双向)	≤10	10GBase-BX		
SFP-10G-BXD1 (单纤双向)				

📖 说明

光模块的详细参数请参见《S6700 系列以太网交换机 硬件描述-光模块》。

## 7.3 性能和容量

表 7-6 S6700 产品主要性能指标

属性	业务特性	性能指标描述
以太业务性能	MAC数	128K
	VLAN	4K
	Trunk组	64
	Trunk组的最大端口数	每组最大8个端口
	整机静态ARP数	8K

属性	业务特性	性能指标描述
	整机动态ARP数	8K
QoS性能	每端口的队列数	8个
	CAR	8Kbps
ACL	ACLv4	支持的最大ACLv4数目：上行1024，下行512
	ACLv6	支持的最大ACLv6数目：上行512，下行256
L3VPN	VRF数量	127
IP单播	IPv4路由表项/IPv4 FIB表项	16K
	IPv6路由表项/IPv6 FIB表项	8K
组播	组播静态路由项数	128
	二层组播转发表项	2K
	三层组播转发表项	2K
可靠性业务	BFD	BFD session数量:128 最小故障发现时间：300ms 300ms
	以太OAM	● 802.3ah 检测速率：1s
	RRPP	● RRPP最大实例数：64 ● 支持环数：16 ● RRPP支持的域个数：8
	VRRP	● VRRP备份组：64 ● 每个VRRP备份组内的虚IP数：16
	SmartLink	● 整机最大实例数：64 ● 整机支持Smart Link组数：16
	MSTP	整机最大实例数：64
	SEP	整机最大segment数：16

## 7.4 软件特性列表

表 7-7 功能特性列表

属性		说明
以太网特性	Ethernet	<ul style="list-style-type: none"> <li>● 支持全双工、半双工、自动协商工作方式</li> <li>● 以太网接口可支持10M、100M、1000M、10G和自协商速率</li> <li>● 支持接口流量控制</li> <li>● 支持Jumbo报文</li> <li>● 支持链路聚合</li> <li>● 支持Trunk内各链路流量的负载分担</li> <li>● 支持接口隔离、接口转发限制</li> <li>● 支持广播风暴抑制</li> </ul>
	VLAN	<ul style="list-style-type: none"> <li>● 支持Access、Trunk、Hybrid和QinQ接入方式</li> <li>● 支持default VLAN</li> <li>● 支持VLAN mapping</li> <li>● 支持灵活QinQ</li> <li>● 支持Voice VLAN</li> <li>● 支持DHCP策略VLAN</li> </ul>
	MAC	<ul style="list-style-type: none"> <li>● 支持MAC地址自动学习和老化</li> <li>● 支持静态、动态、黑洞MAC表项</li> <li>● 支持源MAC地址过滤</li> <li>● 支持接口MAC地址学习限制</li> </ul>
	ARP	<ul style="list-style-type: none"> <li>● 支持静态、动态ARP</li> <li>● 支持VLAN上应用ARP</li> <li>● 支持ARP表项老化</li> </ul>
	Smartlink	<ul style="list-style-type: none"> <li>● 支持Smartlink</li> <li>● 支持Smartlink多实例</li> <li>● 支持Monitorlink</li> </ul>
	LLDP	支持LLDP
	NAC	支持NAC
	VCT	支持VCT

属性		说明
以太网环路保护	MSTP	<ul style="list-style-type: none"> <li>● 支持STP</li> <li>● 支持RSTP</li> <li>● 支持MSTP</li> <li>● 提供BPDU保护、Root保护、环路保护</li> <li>● 提供局部STP、BPDU隧道</li> </ul>
	RRPP	<ul style="list-style-type: none"> <li>● 支持RRPP保护倒换</li> <li>● 支持RRPP单环、RRPP相切环、RRPP相交环</li> <li>● 支持RRPP环和其他环网混合组网</li> </ul>
IPv4/IPv6转发	IPv4特性	<ul style="list-style-type: none"> <li>● ARP/RARP</li> <li>● ARP代理</li> <li>● 支持自动侦测功能</li> </ul>
	单播路由特性	<ul style="list-style-type: none"> <li>● 静态路由</li> <li>● RIP-1/RIP-2</li> <li>● OSPF</li> <li>● BGP</li> <li>● IS-IS</li> <li>● 路由策略、策略路由</li> <li>● uRPF检查</li> <li>● VRF</li> <li>● 支持DHCP Client/Server/Relay</li> <li>● 支持DHCP snooping</li> </ul>
	组播路由特性	<ul style="list-style-type: none"> <li>● IGMPv1/v2/v3</li> <li>● PIM-DM</li> <li>● PIM-SM</li> <li>● PIM-SSM</li> <li>● MBGP</li> <li>● MSDP</li> <li>● 组播路由策略</li> <li>● RPF</li> </ul>
	IPv6特性	<ul style="list-style-type: none"> <li>● 支持IPv6协议栈。</li> <li>● 支持单播路由协议：RIPng/OSPFv3。</li> <li>● 支持VRRP6。</li> <li>● 支持IPv4/IPv6过渡技术。</li> </ul>

属性		说明
设备可靠性	BFD	<ul style="list-style-type: none"> <li>● BFD基本功能</li> <li>● BFD FOR OSPF</li> <li>● BFD FOR IS-IS</li> <li>● BFD FOR BGP</li> <li>● BFD FOR PIM</li> </ul>
	其他	VRRP
二层组播特性	二层组播特性	<ul style="list-style-type: none"> <li>● 支持IGMP Snooping功能</li> <li>● 支持IGMP Proxy功能</li> <li>● 支持用户快速离开机制</li> <li>● 支持组播流量控制</li> <li>● 支持跨VLAN组播复制</li> <li>● 支持可控组播</li> </ul>
以太网OAM	EFM OAM	<ul style="list-style-type: none"> <li>● 支持对端发现</li> <li>● 支持链路监控</li> <li>● 支持故障通告</li> <li>● 支持远端环回</li> </ul>
QoS特性	流分类	<ul style="list-style-type: none"> <li>● 支持基于L2协议头、IP五元组、出接口、802.1p优先级的组合流分类</li> <li>● 支持基于QinQ报文的C-VID和C-PRI的流分类</li> </ul>
	流动作	<ul style="list-style-type: none"> <li>● 支持对分类后报文流的访问控制</li> <li>● 支持基于流分类的流量监管</li> <li>● 支持按照流分类结果重标记报文</li> <li>● 支持分类后报文进入指定调度队列中</li> <li>● 支持流分类、流行为的组合应用</li> </ul>
	队列调度	<ul style="list-style-type: none"> <li>● 支持PQ调度</li> <li>● 支持DRR调度</li> <li>● 支持PQ+DRR调度</li> <li>● 支持WRR调度</li> <li>● 支持PQ+WRR调度</li> </ul>
	拥塞避免	支持WRED
	出接口限速	支持出接口限速
配置与维护	终端服务	<ul style="list-style-type: none"> <li>● 支持命令行配置</li> <li>● 支持英文和中文的提示和帮助信息</li> <li>● 支持Console、Telnet终端服务</li> <li>● 支持Send功能，终端用户之间进行信息互通</li> </ul>

属性		说明
	文件系统	<ul style="list-style-type: none"> <li>● 支持文件系统</li> <li>● 支持目录和文件管理</li> <li>● 支持通过FTP、TFTP方式上载、下载文件</li> </ul>
	调试和维护	<ul style="list-style-type: none"> <li>● 支持日志、告警、调试信息统一管理</li> <li>● 提供电子标签</li> <li>● 支持用户操作日志</li> <li>● 支持详尽的调试信息，帮助诊断网络故障</li> <li>● 提供网络测试工具，如tracert、ping命令等</li> <li>● 提供接口镜像、流镜像</li> </ul>
	版本升级	<ul style="list-style-type: none"> <li>● 支持整机软件加载、在线加载</li> <li>● 支持BootROM在线升级</li> <li>● 支持在线补丁</li> </ul>
安全和管理	系统安全	<ul style="list-style-type: none"> <li>● 命令行分级保护，未授权用户无法侵入S6700</li> <li>● 支持SSH v2.0</li> <li>● 支持RADIUS和HWTACACS用户登录认证</li> <li>● 支持ACL过滤</li> <li>● 支持DHCP报文过滤（插入Option82选项）</li> <li>● 支持预防控制报文攻击</li> <li>● 支持防范Source Address spoofing、LAND、SYN Flood (TCP SYN)、Smurf、Ping Flood (ICMP Echo)、Teardrop、Ping of Death多种攻击</li> </ul>
	网络管理	<ul style="list-style-type: none"> <li>● 支持ICMP实现ping和tracert功能</li> <li>● 支持标准网管协议SNMPv1/v2c/v3</li> <li>● 支持通用特性的标准MIB</li> <li>● 支持RMON</li> </ul>

## 7.5 遵循的标准与协议

表 7-8 IEEE

标准名称		描述
802.1	802.1d	Spanning Tree Protocol
	802.1p	IEEE Standards for Local and Metropolitan Area Networks: Virtual Bridged Local Area Networks
	802.1q	Virtual Bridged Local Area Networks
	802.1s	Multiple Spanning Tree Protocol

标准名称		描述
	802.1w	Rapid Spanning Tree Protocol
	802.1x	Port based network access control protocol
802.3	802.3	Carrier Sense Multiple Access with Collision Detection (CSMA/CD) access method and physical layer specifications
	802.3ad	Aggregation of Multiple Link Segments
	802.3ab	Physical Layer Parameters and Specifications for 1000 Mb/s Operation Over 4 Pair of Category 5 Balanced Copper Cabling, Type 1000BASE-T
	802.3ae	10GE WAN/LAN
	802.3u	100Base-T
	802.3x	Full Duplex and flow control
	802.3z	Gigabit Ethernet Standard, 1000BASE-X

表 7-9 RFC

特性	标准编号	描述
基本协议	RFC 768	User Datagram Protocol(UDP)
	RFC 791	Internet Protocol(IP)
	RFC 792	Internet Control Message Protocol (ICMP)
	RFC 793	Transmission Control Protocol(TCP)
	RFC 826	Address Resolution Protocol(ARP)
	RFC 854	Telnet Protocol Specification
	RFC 894	Standard for the transmission of IP datagrams over Ethernet networks. C. Hornig. Apr-01-1984. (Format: TXT=5697 bytes) (Also STD0041) (Status: STANDARD)
	RFC 951	Bootstrap Protocol
	RFC 1542	Clarifications and Extensions for the Bootstrap Protocol
	RFC 1027	Using ARP to Implement Transparent Subnet Gateways
	RFC 1122	Requirements for Internet Hosts - Communication Layers
	RFC 1256	ICMP Router Discovery Messages
	RFC 1519	Classless Inter-Domain Routing (CIDR): an Address Assignment and Aggregation Strategy
	RFC 1812	Requirements for IP Version 4 Routers

特性	标准编号	描述
	RFC 2131	Dynamic Host Configuration Protocol
	RFC 2338	Virtual Router Redundancy Protocol(VRRP)
BGP	RFC 1269	Definitions of Managed Objects for the Border Gateway Protocol:Version 3
	RFC 1771	A Border Gateway Protocol 4 (BGP-4)
	RFC 1965	Autonomous System Confederations for BGP
	RFC 1966	BGP Route-Reflection
	RFC 1997	BGP Community Attribute
	RFC 2385	TCP MD5
	RFC 2842	Capabilities Advertisement with BGP-4
IP组播	RFC 1112	Host extensions for IP multicasting
	RFC 1122	Requirements for Internet Hosts - Communication Layers.
	RFC 2236	Internet Group Management Protocol, Version 2
	RFC 2283	Multiprotocol Extensions for BGP-4
	RFC 2362	Protocol Independent Multicast-Sparse Mode (PIM-SM):Protocol Specification
	draft-ietf-pim-dm-new-v2-02	Protocol Independent Multicast - Dense Mode (PIM-DM)
IS-IS	RFC 1195	Use of OSI IS-IS for Routing in TCP/IP and Dual Environments
	RFC 2763	Dynamic Hostname Exchange Mechanism for IS-IS
	RFC 2966	Domain-wide Prefix Distribution with Two-Level IS-IS
MPLS	RFC 2547	BGP/MPLS VPNs
OSPF	RFC 1583	OSPF Version 2 (obsoletes RFC 1247/obsoleted by RFC 2178)
	RFC 1587	The OSPF NSSA Option
	RFC 1765	OSPF Database Overflow
	RFC 1850	OSPF Version 2 Management Information Base
	RFC 1997	BGP Community Attribute
	RFC 2328	OSPF Version 2 (obsoletes RFC 2178)
	RFC 2385	TCP MD5
	RFC 2842	Capabilities Advertisement with BGP-4
	RFC 2918	Route Refresh Capability for BGP-4

特性	标准编号	描述
RIP	RFC 1058	Routing Information Protocol
	RFC 2453	RIP Version 2
DoS防范	RFC 2267	Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing (Obsolete)
网络管理	RFC 854	Telnet Protocol Specification
	RFC 951	Bootstrap Protocol
	RFC 1155	Structure and identification of management information for TCP/IP-based internets
	RFC 1157	A Simple Network Management Protocol (SNMP)
	RFC 1212	Concise MIB Definitions
	RFC 1213	Management Information Base for Network Management of TCP/IP-based internets: MIB-II.
	RFC 1215	A Convention for Defining Traps for use with the SNMP
	RFC 1256	ICMP Router Discovery Messages
	RFC 1493	Definitions of Managed Objects for Bridges
	RFC 1573	Evolution of the Interfaces Group of MIB-II
	RFC 1643	Definitions of Managed Objects for the Ethernet-like Interface Types
	RFC 1650	Definitions of Managed Objects for the Ethernet-like Interface Types using SMIV2
	RFC 1657	Basic BGP4 MIB
	RFC 1724	RIP Version 2 MIB Extension
	RFC 1757	Remote Network Monitoring Management Information Base
	RFC 1850	OSPF Version 2 Management Information Base
	RFC 1901	Introduction to Community-based SNMPv2
	RFC 1907	Management Information Base for Version 2 of the Simple Network Management Protocol (SNMPv2)
	RFC 2021	Remote Network Monitoring Management Information Base Version 2 using SMIV2
	RFC 2668	Definitions of Managed Objects for IEEE 802.3 Medium Attachment Units (MAUs)
RFC 2787	Definitions of Managed Objects for the Virtual Router Redundancy Protocol	
安全	RFC 1492	An Access Control Protocol, Sometimes Called TACACS

特性	标准编号	描述
	draft-grant-tacacs-02	TACACS+
	RFC 2138	Remote Authentication Dial In User Service (RADIUS)