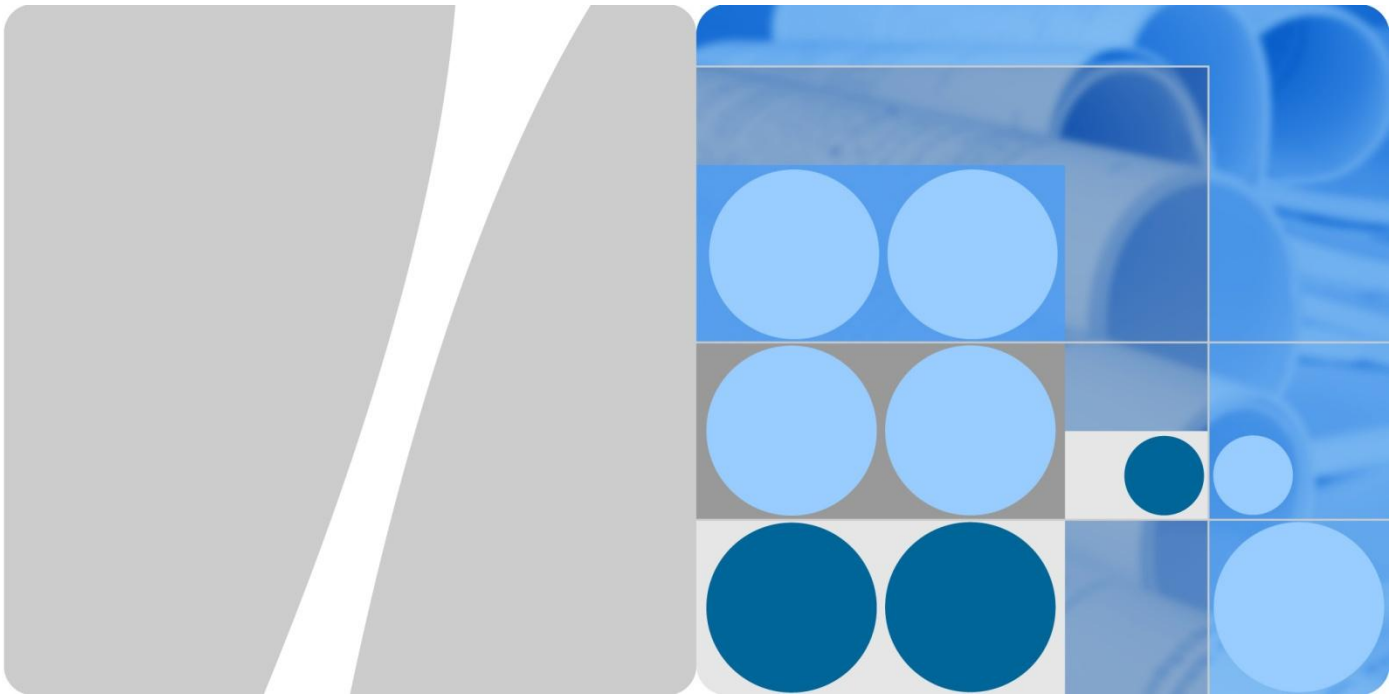


华为安全高效的酒店一体化基础网络解决方案技术建议书

文档版本 01

发布日期 2012-08-31

华为技术有限公司

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：　0755-285600004008302118

客户服务传真：　0755-28560111

目录

1 概述

1.1 目的

本文从技术角度，对酒店信息化项目提出规划设计和建议，本文的目的如下：

1. 对酒店基础网络子系统进行设计，明确子系统功能、组网方案、关键指标、部署建议和设备选型。

2 高速稳健的酒店基础网络系统

2.1 设计原则

酒店基础网络作为整个酒店业务运营的基础，不但承载着酒店的核心管理业务，同时也为客户提供方便的网络服务，对酒店至关重要。设计上要充分考虑承载业务的带宽容量，保证业务稳定，安全的运行，并且满足酒店日益发展的需求。酒店基础网络设计需要满足如下几个要求：

1. 网络结构层次化设计，同时满足酒店数据、语音、视频各业务容量需求，并提供一定的扩展容量，千兆骨干网络，千兆或者百兆到桌面，支持 POE 功能，方便无线部署。
2. 网络设计高可靠，确保酒店业务(上网，办公，监控)运行稳定，满足酒店平均无故障时间要求。
3. 办公网络与客房网络逻辑隔离，客房间网络相互隔离，不同业务配置不同 QOS 策略。
4. 提供安全的远程访问通道，确保远程数据传输安全。
5. 确保酒店网络防外部攻击如 DDos，服务器区保护，局域网的安全保证，防止非法客户端接入酒店网络。
6. 网络部署、运维简单，易于管理，平均故障修复时间满足酒店要求。
7. 整个网络设计满足低能耗，满足酒店绿色节能要求。

2.2 标准和规范

IEEE 802.3u：100Base 规范

IEEE 802.3z：1000Base-X(GBIC)规范

IEEE 802.3ae：10G 规范

IEEE 802.1Q/1P：Virtual Bridged Local Area Networks

IEEE 802.3ad：Link Aggregation

RFC2401：Security Architechure for the Internet Protocol

RFC2139：RADIUS Accounting

RFC2138：Remote Authentication Dial In User Service (RADIUS)

RFC 2475 DiffServ

RFC 3270 Pipe tunneling over DiffServ

2.3 华为酒店基础网络解决方案

2.3.1 层次化的酒店网络架构

对于酒店的基础网络架构，华为推荐层次化的网络架构设计，每层功能清晰，架构稳定，易于扩展和维护；在关键部位采用冗余配置，提供高效的故障恢复机制，保证酒店整体网络运行的可靠性；在关键节点部署安全特性，保障网络安全。华为酒店基础网路组网推荐采用如下架构：

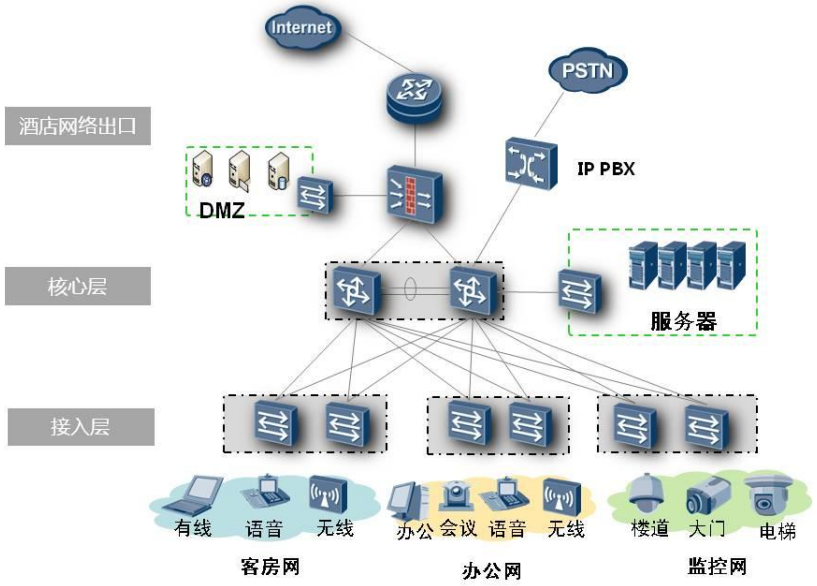


图 1 基础网络组网图

1. 酒店网络出口

酒店网络出口是酒店网络到外部网络的接口，酒店网络的内部用户通过网络出口接入到外部网络，外部用户（包括客户、合作伙伴、分支机构、远程用户等）通过网络出口接入到酒店网络。酒店可以根据实际要求部署 DMZ 区域，放置对外提供的服务器，如 WEB 服务器等。

在酒店网络出口部署路由器以提供高性能的 Internet 接入服务；并部署防火墙，实现安全防护的同时也作为 VPN 网关，实现酒店和集团总部的互联，以及单点用户与酒店内部的互访；酒店网络出口设备可部署在酒店中心机房。

当酒店考虑即插即用(PnP)及上网计费功能时，可以在酒店网络出口同时部署 PnP 和计费认证网关，用于为客户提供更人性化的服务和计费管理功能。同时，建议酒店客房网络出口和酒店办公网络出口分开部署。

2. 核心层

酒店各个系统间通过核心层互联。核心层用作网络骨干，建议部署在酒店中心机房，负责酒店网络的高速互联，并同时承担连接 L2/L3 边缘设备的角色，提供用户管理、安全管理、QoS 调度等各项跟用户和业务相关的处理。

核心层汇聚内部服务器、Internet 接入流量、办公网络、客房网络、监控网络、语音网络等业务。核心设备故障会影响到整个酒店的网络使用，因此必须具备足够高的可靠性和稳定性，华为主流的核心交换拥有数十项可靠性技术保障，并且在国内网上有大量的应用，成熟稳定性经历了充分考验。

3. 接入层

接入层设备需要面对各种各样的终端设备，一般部署在楼道弱电井，通过光纤或千兆电口汇聚到酒店核心交换机。接入设备通常由以太网交换机组成，对于某些终端，可能还要增加特定的接入设备，例如无线接入设备 AP、IP 监控摄像头、IPTV 终端、POTS 话机接入的 IAD 等。

2.3.2 高可靠性技术保证酒店网络的稳定运行

为了满足酒店对网络高可靠性要求，华为提供了多种可靠性技术，来确保酒店网络的稳定运行，这些可靠性技术包括：设备组网的可靠性、二层链路的可靠性，以及三层链路的可靠性。华为推荐按如下方式来保障网络的可靠性：

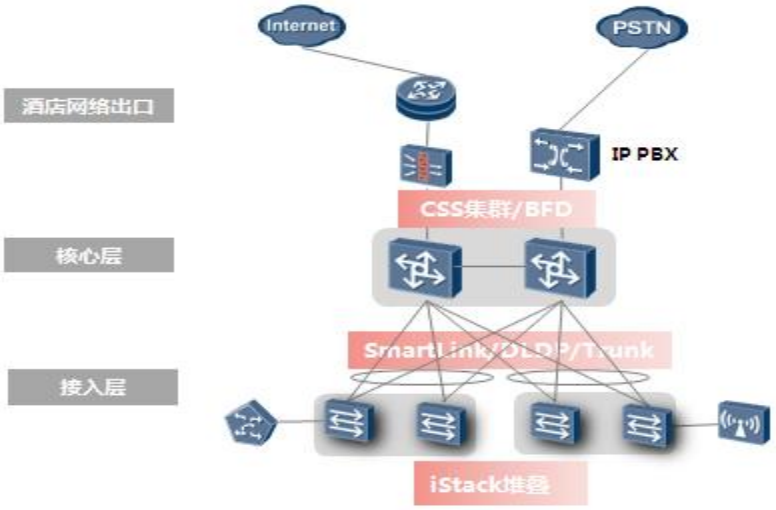


图 2 酒店网络可靠性的技术保证

1. 设备组网的可靠性

为保证基础网络的可靠性，需要部署双上行链路，这样不可避免链路冗余，需要部署破环协议。随着网络规模的不断扩大，xSTP 协议收敛时间慢，可用性差，而 CSS/iStack 技术可以提高基础网络组网的可靠性。

在接入层推荐采用 iStack（堆叠）技术，即多台交换机堆叠在一起，选举出一台交换机做为主交换机，另一台交换机为备交换机，剩下的交换机称为从交换机。主交换机是整个堆叠系统中的控制中心。堆叠中每一台交换机都同时具备成为主交换机或者备交换机的能力。iStack 中多台交换机作为一个整体对外体现为一台逻辑设备，共用一个管理 IP 地址和一个 MAC 地址，且组网方便。堆叠的运维费用低，空间占用小，绿色节能。核心层采用 CSS（集群）技术，即将两台交换机通过专用的堆叠电缆连接起来，选出一台为主交换机，一台为备交换机，对外呈现为一台逻辑交换机。

CSS/iStack 技术在网络扩容时，可以保持已有网络规划不变，扩容方便简单。CSS 技术将两台物理设备虚拟为一台设备，简化了设备的配置和管理。多台设备互为冗余备份，提高系统的可靠性。

Eth-trunk 是将一组物理接口捆绑在一起作为一个逻辑接口来增加带宽的方法。在不同网络层级之间建立 Eth-Trunk，支持跨成员端口聚合，消除了在单台交换机上的单点故障，具有很高的可用性。Eth-trunk 通过在两台设备之间建立链路聚合组，可以提供更高的通讯带宽和更高的可靠性。

CSS/iStack 技术代替传统的 MSTP+VRRP 组网，克服了网络复杂时 MSTP 收敛时间过长、网络拓扑不稳定的弊端。

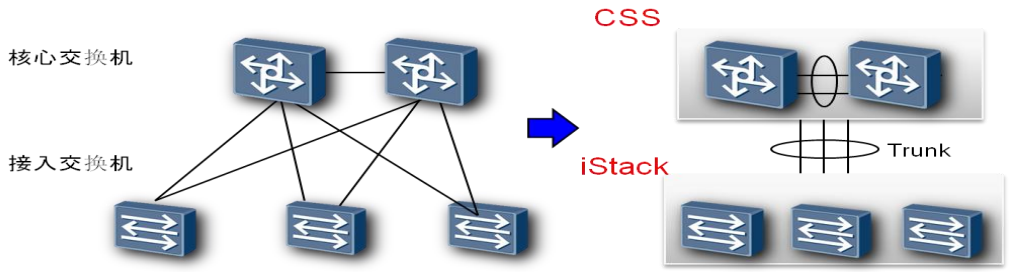


图 3 设备组网可靠性

2. 二层网络的可靠性

在二层链路，DLDP 部署在设备之间用于检测光纤是否存在单通的情况，发现单通后进行链路阻塞，触发上层进行倒换，避免出现流量黑洞，建议光纤连接的设备间都部署 DLDP。

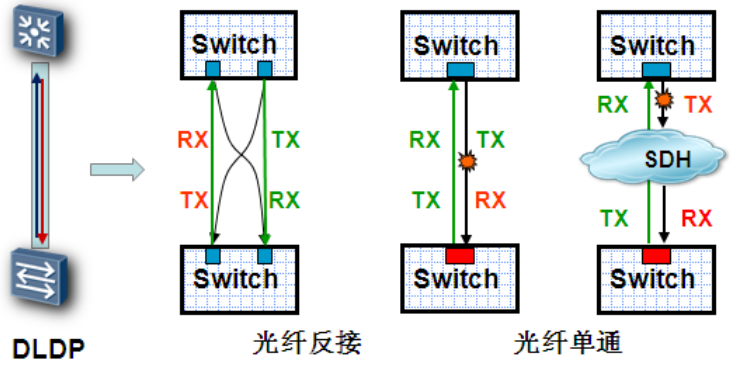
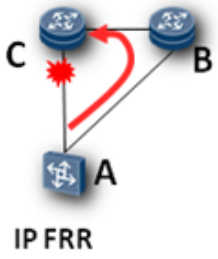


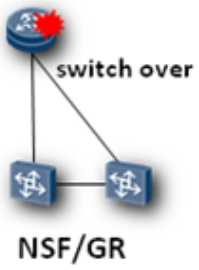
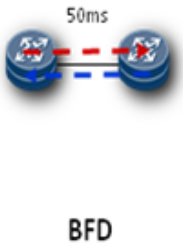
图 4 二层链路的 DLDP 部署

3. 三层网络的可靠性

三层网络的可靠性主要关注路由层面的可靠。酒店网络部署相对简单，这里只对几个概念做必要的解释，客户可以根据实际情况选择部署。

表 1 三层可靠性的部署建议

三层可靠性保护方式	组网	部署建议
IP FRR		在核心层部署 IP FRR。对主用路径和备用路径可以灵活指定。

NSF/GR		在核心层和出口路由器上部署 GR 功能，当设备主用主控失效，备用主控接管控制平面，转发平面不受影响。
BFD		在核心层、出口路由器上部署 BFD For OSPF。

4. 硬件级故障检测能力

硬件级的 Ethernet OAM 链路故障检测机制(3.3ms)，实现 ms 级故障检测和联动倒换(应用于集群分裂、TRUNK 链路选路、路由重选路)；

2.3.3 根据 VLAN 划分业务网络，合理布局酒店业务

华为酒店信息化解决方案通过基础网络承载各种酒店业务，如：酒店管理、IPTV、视频监控、视频会议、电话等。根据业务数据的最终流向，我们把酒店业务分为两个大类：Internet 业务和酒店内部服务业务。

通过 VLAN 的划分，可以有效隔离各个业务间的二层互访，并通过 VLAN ID 提供最简单便捷的业务识别和用户组区分，为后续用户权限管理、业务访问控制等提供方案。

为了给酒店住客提供即插即用的上网服务（PnP），需要客房网的上网业务 VLAN 终结于出口网关，以确保 PNP 功能正常运行，并由该网关来分配 DHCP 地址。同时为减少不必要的其它业务流量冲击该出口网关，华为建议其它业务的 VLAN 终结于核心交换机，并由核心交换机分配 DHCP 地址。

详细的 VLAN 推荐规划如下：

1. Internet 业务分析

1) 客户（住户、访客）Internet 业务流，二层 VLAN 终结于客房网认证计费网关，并由该网关负责接入认证及 DHCP 地址分配

2) 酒店人员 Internet 业务流，二层 VLAN 终结于核心交换机，由核心交换机负责分配 DHCP，并路由至办公网出口网关

3) 视频会议业务，二层 VLAN 终结于核心交换机，与酒店其它会场的数据由核心交换机路由至办公网出口网关

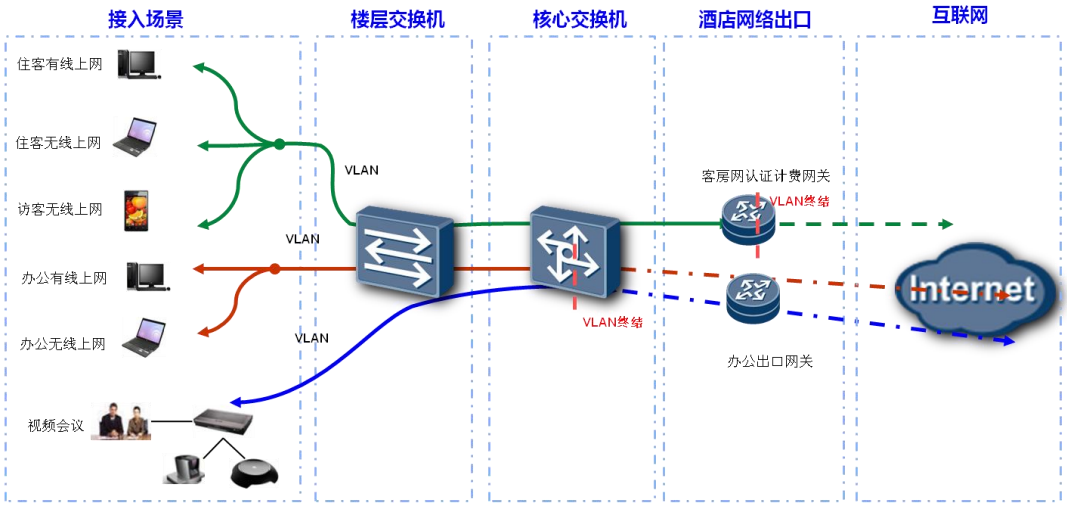


图 5 Internet 业务 VLAN 分析

2. 酒店内部业务分析

1) 酒店对内业务服务，VLAN 终结于核心交换机，并由核心交换机负责 DCHP 分配

2) 不同业务之间的互访需求，由核心交换机进行三层路由

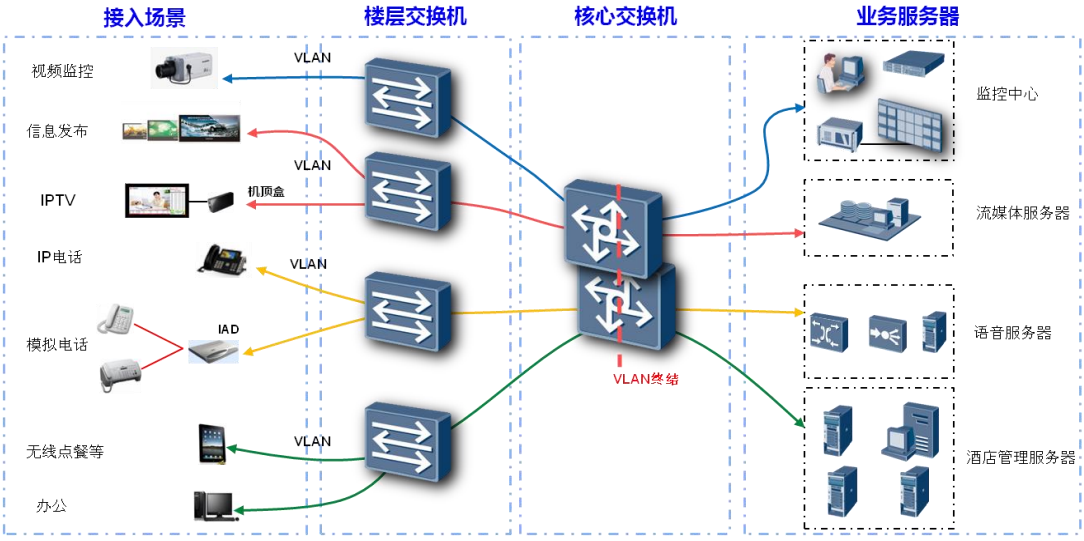


图 6 酒店内部业务 VLAN 分析

3. 酒店基础网络 VLAN 规划

根据上述业务分析，建议酒店 VLAN 按如下原则进行划分：

1) 酒店内部的业务服务，VLAN 终结于核心交换机，并由核心交换机负责 DCHP 分配

2) 不同业务之间的互访需求，由核心交换机进行三层路由

3) 网管及 AC 无线控制报文，可分配在办公 VLAN 上，也可以独立划分一个 VLAN

酒店内 VLAN 规划建议，见如下表：

业务	VLAN ID	VLAN 终结	说明
客房有线上网	楼层+两位数房间号 VLAN1022	PnP、认证计费网关	PnP 服务需要工作与二层网络。 每个客房网络通过 VLAN 隔离，保障隐私。
住户无线上网	VLAN88	PnP、认证计费网关	酒店无线网络通过不同的 SSID 对应不同的 VLAN ID。 Guest:VLAN88(无需认证，覆盖有限区域) Consumer:VLAN80（需认证，全覆盖） Office:VLAN9（SSID 隐藏，需认证，全覆盖）
访客无线上网	VLAN80	PnP、认证计费网关	
办公无线上网	VLAN9	核心交换机	
办公有线上网	VLAN9	核心交换机	办公网络和网关等可以划分在一个 VLAN
商务上网	VLAN6	核心交换机	视频会议等商务网络需求，独立划分 VLAN，并使用酒店办公网络出口，保障网络带宽
信息发布	VLAN5	核心交换机	当信息发布系统有和第三方系统连接需要时（如：IPTV 等），可以通过核心交换机路由实现
视频监控业务	VLAN3	核心交换机	视频监控属于安防，通过 VLAN/ACL 实现二三层隔离，保证其独立性
语音业务	VLAN2	核心交换机	语音独立划分一个 VLAN,用于承载话音和信令业务。对于计费、客户管理等与酒店管理系统联动的业务，可以通过核心交换机三层路由实现
IPTV 业务	VLAN1	核心交换机	视频点播和直播相应的单播和组播视频数据包都统一

			承载在 VLAN1 上，在二层网络上传输。

按上述规划后的酒店 VLAN 划分总图如下：

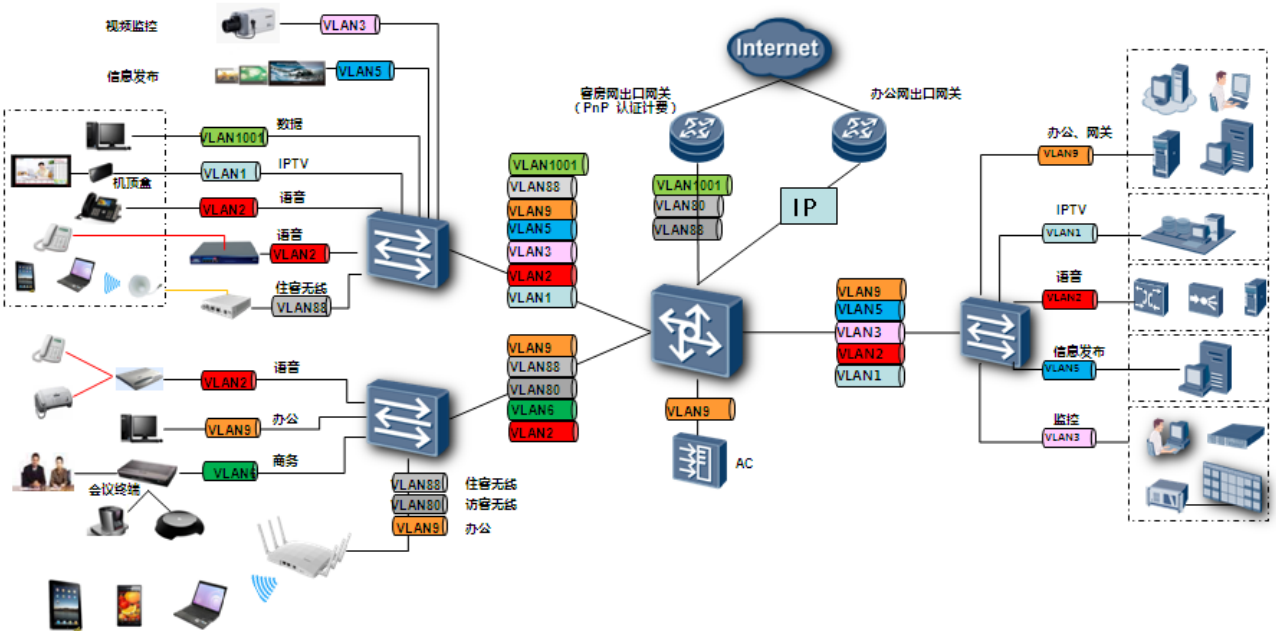


图 7 酒店 VLAN 划分总图

2.3.4 基于业务的分层 QoS，合理规划酒店网络流量

酒店基础网络除了承载传统的客户 Internet 上网需求（WWW、E-Mail、FTP 等数据业务），还承载着视频监控、电视会议、语音等业务。IP 网络需要提供端到端的 QoS 服务，才能保证实时业务如语音数据的传输。QoS 部署模型规定了多种 QoS 技术如何组合满足用户网络服务需求。

Diff-Serv（Differentiated Service）模型是一种多服务模型，它通过携带在报文头部的优先级参数（802.1P、DSCP、EXP）来告知网络节点的 QoS 需求，这样，Diff-Serv 在提供服务时，可以为属于同一需求类别的分组提供同样的服务策略，而无需通过信令协议再去申请资源。

正是由于拥有“带内”信令和基于流进行服务的特点，在网络部署中，Diff-Serv 具有良好的可扩展性，因此华为选择其作为主要的网络 QoS 部署方式。

对于 Diff Serv 部署，RFC4594 把业务划分为 12 种类型，并规划了报文优先级参数和 PHB 动作：

表 2 酒店业务 QOS 映射规则表

业务分类	RFC 名称	说明	流量比例	PHB	DSCP	802.1P	EXP
网络控制	Network Control	网络控制平面业务，如 OSPF/BGP/VRRP/EIGRP 等。	2%	CS6	48	6	6
语音业务	VoIP Telephony	VoIP 业务，包括 G.711、G.729 等语音流	10%	EF	46	5	5
广播视频	Broadcast Video	广播电视和视频监控业务，特点是丢包敏感，不具备重新发送和流控能力。	10%	CS5	40	5	5
桌面会议	Multimedia Conferencing	桌面多媒体协同应用软件，包括语音和视频的应用，如华为 eSpace。	10%	AF41、AF42、AF43	32、36、38	4	4
交互视频	Real-time Interactive	室内部署的交互视频应用，具有语音和视频能力。如视频会议、高清视频等	13%	CS4	32	4	4
视频点播	Multimedia Streaming	VoD 视频点播业务。这类业务允许一定的时延，丢包能够重传，比广播和实时媒体业务更具弹性	10%	AF31、AF32、AF33	26、28、30	3	3
呼叫信令	Signaling	IP 语音和视频业务信令流。如 SIP、H323、MGCP、VMP 等	2%	CS3	24	3	3

业务分类	RFC 名称	说明	流量比例	PHB	DSCP	802.1P	EXP
事务处理	Low-Latency Data	交互式的重要数据业务，如即时消息、ERP、数据库查询	10%	AF21、AF22、AF23	18、20、22	2	2
网络管理	OAM	网络维护和管理业务。SNMP、SSH、Sys Log	2%	CS2	16	2	2
Bulk 数据	High-Throughput Data	指非交互式“背景”业务，其特点是不需要等待业务响应，不会影响工作效率。如 Email、FTP、文件共享等业务	5%	AF1	10、12、14	1	1
背景流量	Low-Priority Data	与公司业务无关，多是娱乐性的业务。如 BT、eMule、YouTube 等非组织性的内容	1%	CS1	8	0	0
尽力服务	Standard	采用默认优先级 0，大多数业务不进行优先级标记	25%	DF(CS0)	0	0	0

酒店网络部署 QoS 主要是防止 BT 等非正常业务流量对酒店关键业务以及关键客户流量形成冲击，酒店内 QoS 需要端到端的部署，每一层承担不同的角色，主要分为接入层业务识别、核心层 DiffServ 部署、出口路由器带宽控制三个方面。其部署如下图所示：

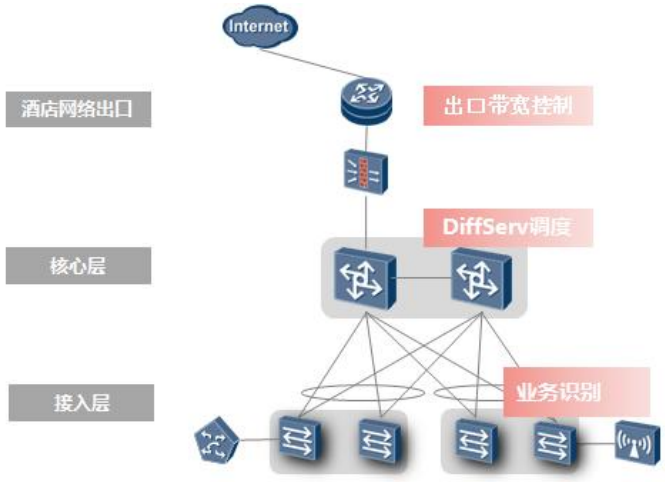


图 8 三层 QOS 部署

1. 接入层业务识别

接入交换机作为边界交换机，在 UNI（User Network Interface）侧需要担负数据流的识别、分类以及流标记的工作，而在 NNI（Network Node Interface）侧需要担负不同应用数据流的拥塞管理、拥塞避免、流量整形等工作。

在实际部署的时候，接入交换机上不同的端口接入了不同的终端。在接入交换机上可以给这些不同的业务分配不同的优先级，根据 802.1Q 和 802.1p 对流量进行标识或重新标识。之后，在网络中按这样的优先级进行调度就可以了。对于 IP 电话等语言设备可同时启用 Voice VLAN，使得语音流可以优先转发。

2. 核心层 Diffserv 调度

汇聚层和核心层设备端口信任 DSCP（或者 802.1p），基于接入层标识的 QoS 参数，通过队列调度、流量整形、拥塞避免等方式实施 QoS 策略，保证高优先级业务优先获得调度。

3. 出口路由器带宽控制

对于出口路由器，同样作为 DiffServ 域，根据设备标识的 DSCP/802.1P 参数，实施 QoS 策略。需要说明的是，在路由器的 WAN 口上，由于受限于出口带宽，相关 WAN 口带宽参数设置需要考虑差异性。

2.3.5 四重酒店网络安全防护

当前酒店网络面临着多方面的安全威胁，如客人 PC 携带病毒进入客房网络、外部网络攻击、内部网络攻击、机密数据安全保障、以及分店与酒店总部间的安全通信等。酒店网络的安全稳定直接影响到酒店运营管理和客户的住店体验。华为的多重网络安全防护解决方案能很好解决酒店面临的安全问题，从网络监管、边界防御、接入安全等方面入手，保护酒店网络的安全。

1) 网络监管通过防火墙部署，实现病毒分析、流量监控、上网行为管理等功能，支撑酒店网络审计功能，防止病毒泛滥。

2) 边界防御通过 IPS/IDS 防火墙对酒店网络出口与酒店内网的关键网元进行有效防护和隔离。

3) 酒店内网安全主要通过交换机的安全特性来保证网络的安全。包括 DHCP Snooping、ARP 防攻击、MAC 防攻击、IP 源防攻击等。

4) 接入安全主要指酒店内的安全接入，包括终端安全接入控制，例如：用户隔离，端口隔离等；远程接入涉及分支机构、出差人员对酒店内部的安全访问。

酒店安全性推荐按下图部署：

图 9 酒店安全性部署

1. 客房网络的安全接入认证

接入认证对于酒店客房网络的管理、计费、审计等工作具有重要的意义。目前主流的接入认证技术包括 802.1x、Web 认证和 MAC 认证。根据酒店客房网络的使用特点，不需要安装任何客户端软件、基于标准 Web 浏览器进行认证无疑是最合适的一种认证方式，因此在酒店网络中得到了广泛的应用。

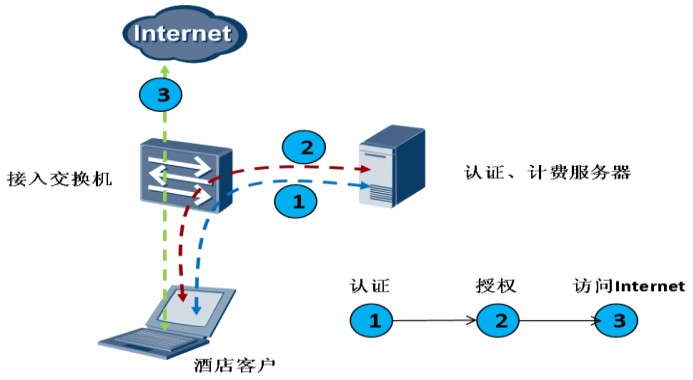


图 10 酒店 Web 认证

1. 酒店客户 PC 连接到网络，当打开浏览器输入网址后，交换机会自动将请求重定向到酒店的认证策略中心，并且由策略中心来推送定制化的认证界面；

2. 客人在认证界面执行一定的操作，例如输入用户名密码，或者点击页面相应按钮接受酒店的网络使用协议等，之后交换机会附加例如交换机 ID，端口，VLAN，IP 地址等送向策略中心进行认证，策略中心会判断该客人的帐号，或者根据附加信息定位到相应的酒店房间，并判断是否开通 Internet 服务业务，如果已经开通且附加信息符合原有的设定，则会通过 Radius 消息告知交换机该用户已通过认证，如果未开通则不会执行该操作；

3. 交换机接到通过认证的消息后，会开启当前用户的访问权限，用户则可以正常访问网络。

2. 客房网络的隐私保护

如何保护客人个人电脑上的隐私信息不被窃取，是酒店客房网络安全的另一关注重点。为保障数据隐私，在技术上对每个客房的数据流进行隔离是一个根本的解决办法。传统的方法是为每一个客房用户分配一个 VLAN 和一个 IP 子网，并且用一台三层交换机或路由器来连接这些子网。这种方法要求网络设备支持大量的 VLAN 和三层接口，并且随着 VLAN 数量的增加会大大增加生成树和访问控制列表（ACLs）的维护复杂程度。

针对以上问题，采用华为公司的 Super VLAN 技术能够很好的解决，Super VLAN 通常用来防止连接到某些接口或者接口组的组网设备之间的相互通信，但却允许与默认网关进行通信。这种特性很好的满足了酒店客房之间的隔离，保护客户隐私，同时降低了网络管理成本。

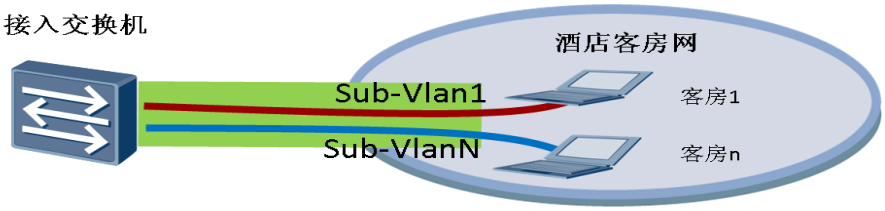


图 11 客房端口隔离

3. 客房网络的流量管理

酒店客户上网期间，使用 P2P 在线视频，迅雷下载等占用大量酒店出口带宽，影响酒店业务办理效率和其它客户的上网体验，因此需要对客户的上网带宽做好控制。

华为的安全解决方案中提供了丰富的流量控制手段，能够帮助酒店真正实现带宽的精细化管理，目前支持以下三种的流量控制手段：

1) 基于 IP 地址（地址段）的流量控制

2) 基于 DPI 应用的流量控制

DPI(Deep Packet Inspection)作为一种较新的包检测技术，除了能够检测 P2P、IM，还可以识别包括 VOIP（skype、H.323、SIP、RTP），Game，web_Video（PPlive、QQlive），Stock，Attack 等 20 多种大类，上千种应用协议，该 DPI 库支持在线升级，保证 DPI 库的实时更新。

基于 DPI 应用的流量控制可采用的控制策略包括：允许通过、禁止通过、流量限速、连接数限制。

3) 基于用户（用户组）的流量控制

在流量识别对应用户身份的基础上，只需要针对用户（组）信息配置限流策略，而不再需要根据复杂多变的 IP 网段来进行限流配置，这样不同的用户（组）身份可配置不同的流量控制策略，简化了策略配置与网络管理。

4. 酒店内部网络安全保障

内部局域网承载着酒店的核心业务，如 PMS 等系统，局域网的安全稳定至关重要。目前局域网潜在的威胁有 MAC 地址泛滥攻击，ARP 欺骗，DHCP 欺骗等。

华为交换机提供了丰富的安全手段来确保局域网的安全，减少安全攻击和病毒危害，将威胁第一时间阻止在网络入口处。华为交换机支持如下安全特性：DHCP Snooping 技术、中间人攻击与 IP/MAC Spoofing 攻击防护、IP Source Guard、DAI 技术。

对酒店服务器数据的非法访问，入侵篡改，及信息泄漏等都严重威胁着酒店安全和客户隐私，如何保护服务器安全运行和数据安全对酒店的运营至关重要。

华为公司的防火墙提供了可管理的安全区域管理功能，访问控制规则定制简单。华为防火墙默认提供四个安全区域：Trust、Untrust、DMZ、local，在提供三个最常用的安全逻辑区域的基础上还新增加了本地逻辑安全区域，本地安全区域可以定义到防火墙本身的报文，保证了防火墙本身的安全防护。

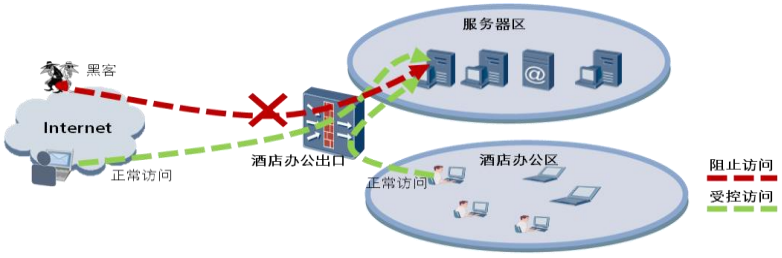


图 12 服务器访问控制

除了安全区域的划分，防火墙还提供强大的 IPS 功能，全面防范各种漏洞攻击：如针对操作系统的漏洞攻击，针对数据库服务器的溢出等攻击。

5. 员工的上网行为管理

华为为酒店提供了强大的上网行为管控功能，有效控制酒店员工访问非法网站以及非工作性质的网络聊天、游戏等。华为可支持如下形式的行为管理功能：

1) 支持 URL 分类技术

URL 过滤业务通过识别并屏蔽对恶意网站的访问，能够在一定程度上减少木马，以及各种各样的恶意网页的传播，为用户提供一个更安全的网络环境。对于钓鱼网站，URL 过滤功能更是其克星。

2) 深度的协议分析、解码，多层次、细粒度的行为控制

通过对 HTTP、FTP、SMTP、POP3、webmail 的分析，区分上传、下载、收邮件、发送邮件等行为，以及发送文件的名称、类型、大小等信息，酒店可以根据自身的需要设定上网行为：完全禁止网络访问、允许浏览、下载，不允许外发信息等。

图 13 酒店员工上网行为管理

6. 互联网出口安全

酒店网络出口容易受到外部网络的攻击，华为的 USG 系列高度集成了防火墙，IPS，AV 等强大的安全功能：

1) 丰富的 DoS 防御手段

根据数据报文的特征，以及 DoS 攻击的不同手段，可以针对 ICMP Flood、SYN Flood、UDP Flood 等各种 DoS 攻击手段进行 DoS 攻击的防御。

2) 强大的防病毒能力

扫描 HTTP，SMTP， POP3 协议上传，下载的文件，可检测感染型病毒，木马，间谍软件等，支持病毒文件的摘除，页面推送告警，邮件打标签等

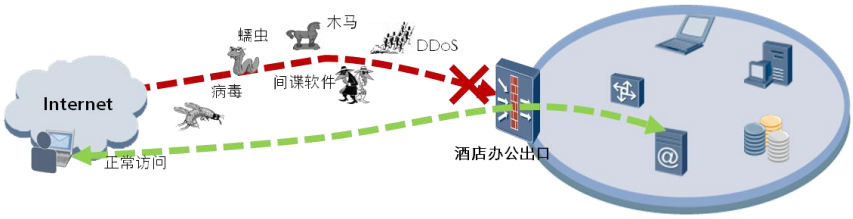


图 14 酒店办公出口防护

7. 安全的远程酒店业务应用

酒店出差员工的远程办公以及访问通道的安全，是目前酒店网络建设中需要考虑的一环。通过 VPN 方式，可以利用现有的网络资源实现远程用户对酒店内部网络的访问，不但节省了大量的资金，而且具有很高的安全性。华为的防火墙集成了多种 VPN 应用：

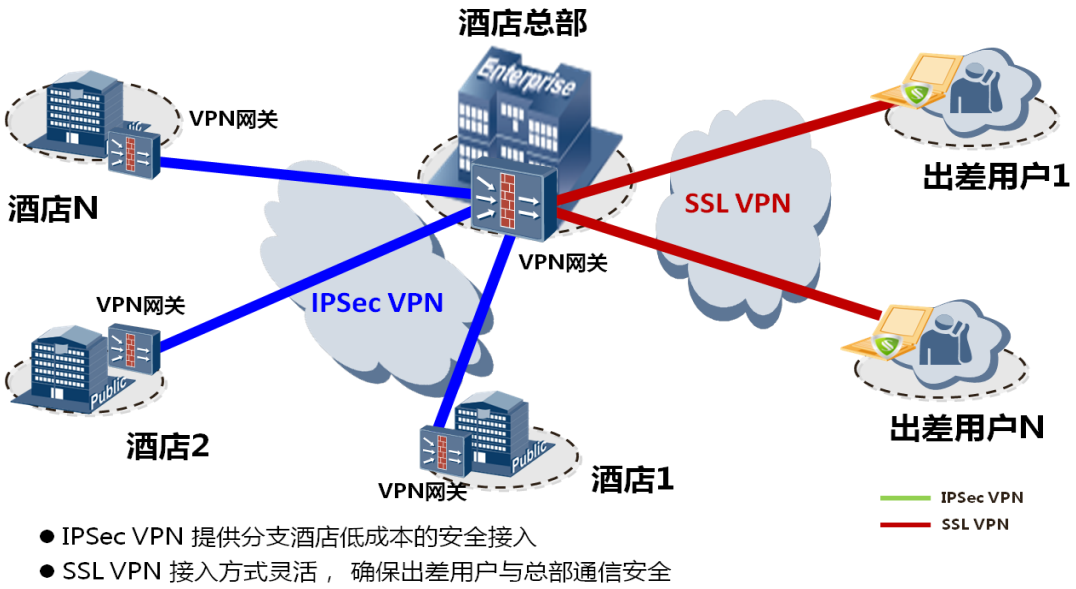


图 15 远程办公接入

2.3.6 创新的节能技术

能耗管理作为酒店最关心的项目之一，如何降低整体能耗，需要各子系统的配合，基础网络作为酒店系统中的重要环节，同样承担着降能耗的责任，同时又能确保网络的正常运营。华为交换机系列产品提供了丰富节能技术，整体能效提升 30％以上，帮助酒店实现绿色稳定网络:

1. SSS-Energy 精细化节能技术

华为创新的节能技术，拥有两项创新专利，实现交换机的整机休眠，空闲端口直接进入端口休眠，端口无流量同样进入休眠，当所有唤醒端口无流量，整机进入休眠模式，使用华为的 SSS-Energy 技术，耗电量仅为业务同等产品的 52%。

2. 能效以太网 IEEE 802.3az

Energy Efficient Ethernet（能效以太网）依据链路利用的情况按需供电，链路无数据发送的端口关闭。

3. 超静音设计“芯”静自然凉

盒式交换机无风扇超静音设计。高集成“变流”芯片，实现按流量动态调整功率，降低整机功耗 8%。

4. 智能 POE 闲暇更省电

智能 POE 供电基于 PD 设备角色启动不同的能源管理方案，保持能源管理弹性。

5. 模糊风扇调速精细温度控制

智能风扇调速策略，监测关键器件温度，模糊控温技术有效降低转速，延长风扇使用寿命。

2.3.7 网络的高效运维

酒店整体网络搭配功能强健的华为 eSight 统一网管系统，无论是系统开局部署，还是运维等方面都可以为客户带来简单便捷的体验。华为 eSight 统一网管系统是轻量级的 IP+IT 综合一体化运维管理平台，采用标准协议和接口，支持多厂家设备，提供有线和无线一体化管理，其简单易用的操作界面让酒店整网设备的配置、升级、维护轻松搞定。

1. 快速开局部署能力

1) 设备快速识别

eSight 统一网管可以对 SNMP 网络设备进行添加，通过手动输入 IP 地址、IP 地址网段，以及通过文件方式导入设备列表的方式完成设备快速添加；同时，eSight 系统提供对多厂商多设备的支

持，除了华为网络设备外，还预集成了 H3C、思科等第三方设备适配包，可以轻松识别第三方网络设备，如果是非标准设备，还可以通过下载设备适配包的方式自行添加。

2) 设备智能化部署

eSight 系统提供了智能配置工具采用两种手段进行快速配置，一是预置了常用的业务配置模板，用户可以方便的选择模板，进行设备批量配置；二是通过规划表单的方式，进行设备差异化批量配置。此外，配置下发之前会通过命令行方式进行校验，降低配置出错的风险。

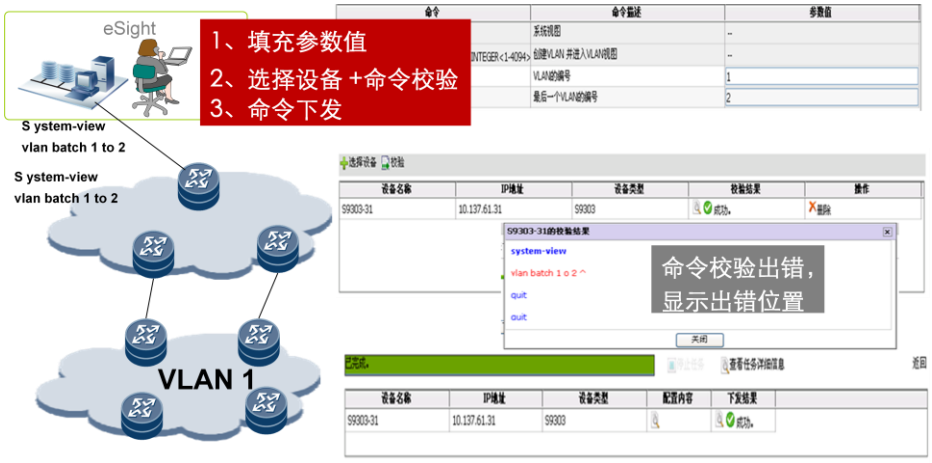


图 16 基于模板配置

图 17 基于规划表单配置

2. 维护管理简单

eSight 统一网管系统提供了强大的管理功能，采用可以定制化的 Portal 管理页面，实现一站式设备信息浏览和监控，图形化显示设备基本信息、设备可用率、设备告警、设备性能图表等信息，满足不同角色差异

化的维护需求，全面提升维护管理效率，降低维护工作强度，而且采用图形化人机界面，操作简单。只需一台安装有 eSight 软件的高性能笔记本电脑，即可轻松玩转酒店整网维护。

1) 网络拓扑管理

通过物理拓扑或 IP 拓扑两种拓扑图呈现网络结构，实现网络设备的图形化、层次化展示，同时显示子图、网元、链路，以及网元状态的显示。

物理拓扑图可以对全网设备的层次结构和运行状态一目了然。

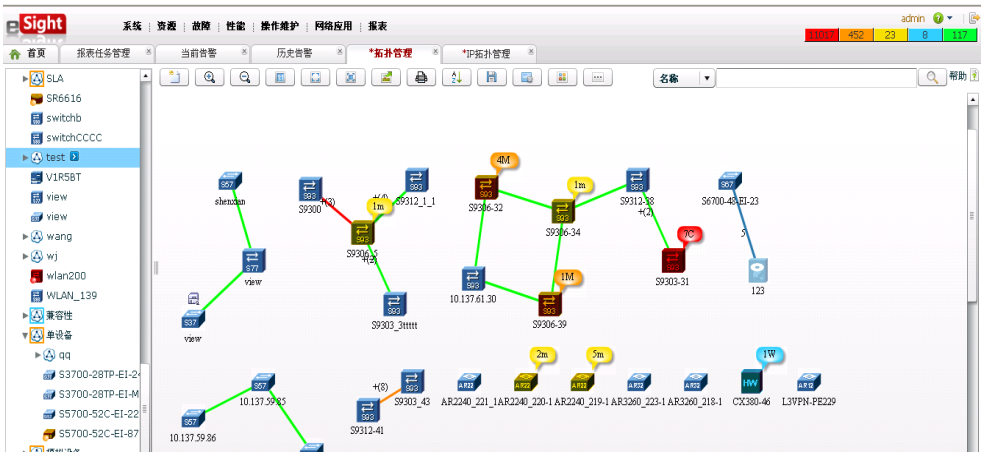


图 18 网络物理拓扑图

IP 拓扑图可以直观显示子网划分情况，以及设备间链路、设备和子网间链路等等信息，让用户实施掌控二层、三层网络状态。

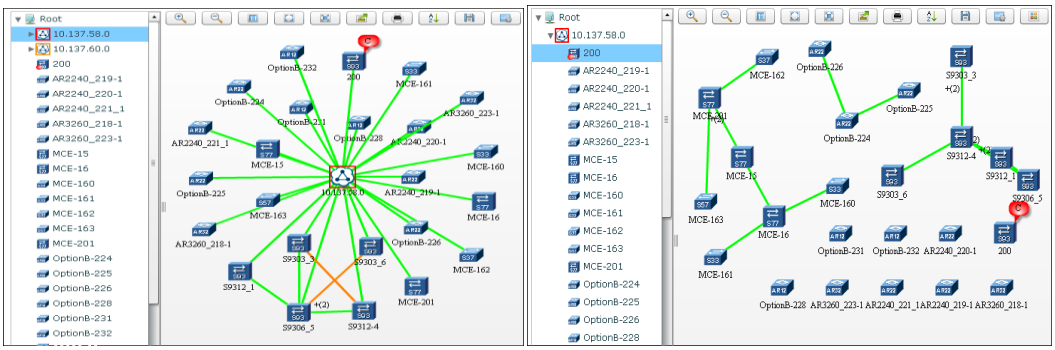


图 19 网络 IP 拓扑图

2) 故障采集和告警

eSight 支持设备故障的实时采集，即时接收设备上报的告警，并进行界面展示。告警界面中包含当前告警管理、历史告警管理、告警转储、告警通知等功能，通过这些告警信息，可以帮助用户及时找到故障原因，快速排除故障。

图 20 故障告警页面

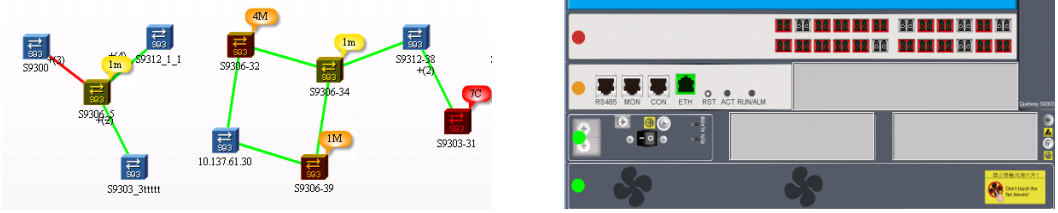


图 21 故障快速定位

3) 性能管理

eSight 可以通过采集数据的阈值、指标模板、对比历史性能数据的方式进行网元性能的管理。主要呈现方式有：

- 多种性能监视指标，多维度掌握网络状况；
- 不同图表展现不同性能监视指标；
- 性能监视图动态持续刷新；
- 历史数据比较分析。

4) 报表管理

eSight 系统内置了丰富的预定义报表，同时提供强大易用的报表设计功能，用户可根据酒店行业特点和自身运维要求进行客户报表定制。

图 22 报表管理和设计

此外生成的报表可以导出报表类型为 word 、excel、PDF 等格式，报表数据字段可以自定义；同时支持日、周、月、季度等周期性报表，并提供 Email 分发方式进行自动分发。

5) 日志管理

系统提供对系统运行状态、用户历史操作的日志信息管理功能。用户可根据日志信息，了解系统的运行状况和用户操作记录。

2.4 推荐部署及选型

2.4.1 选型依据

首先统计××酒店各房间的类型及数量，统计出各种信息点的数量，从而在总结端口类型及数量的基础上，计算出各种交换机的配置。

××酒店的房间类型及数量统计如下：

表 3 房间数量统计表

楼层	豪华标间	豪华套房	娱乐会所	多功能厅	餐厅	办公室	库房	楼层总计（间）
19 楼			5					5

18 楼	12	2						14
17 楼	14	2						16
4-16 楼	16＊13	1 ＊ 13						17 ＊ 13
3 楼						2	5	7
2 楼					1			1
1 楼				1	1			2
总结	234	17	5	1	2	2	5	266

根据上述的酒店的类型及数量，统计的信息点按下表部署：

表 4 客房区域信息点部署统计表

客房楼层	客房 IP 信息点				其它			楼层总计	
	桌面网络端口	IPTV	桌面 IP 电话	床头 IP 电话	无线 AP	IAD(模拟电话汇聚转 IP)	IP 摄像头	实际	预留
18 楼	14	14	14(POE)	14(POE)	3(POE)	2	5(POE)	30+36(POE)	4+2（POE）
17 楼	16	16	16(POE)	16(POE)	3(POE)	2	5(POE)	34+40(POE)	4+2（POE）
4-16 楼	17	17	0	0	3(POE)	2	4(POE)	36+7(POE)	4+2（POE）
总计	251	251	30(POE)	30(POE)	45(POE)	40	62(POE)	532+167(POE)	60+30（POE）

表 5 公共区域信息点部署统计表

公共区域楼层	公共区域楼层 IP 信息点统计						楼层总计	
	网络端口	IPTV	无线 AP	IAD	IP 摄像	信息发布	实际	预留
19 楼 娱乐会所	10	5	5(POE)	1	5(POE)	5	21 + 10(POE)	2
3 楼 办公室、库房	20		2(POE)	1	7(POE)		21 + 9(POE)	6
2 楼 餐厅	4		1(POE)	1	3(POE)	1	6 + 4(POE)	0
1 楼 多功能厅	6		3(POE)	1	9(POE)	1	8 + 12(POE)	0
地下停车场			2（POE）		7(POE)		7(POE)	
总计	40	5	13(POE)	4	31(POE)	7	56 + 44(POE)	8

2.4.2 选型及部署

1. 楼层交换机推荐部署及选型

表 6 楼层交换机部署及选型表

产品编号	产品描述	部署建议		数量
		楼层	接入设备	
S5710-28C-PWR-LI POE 供电	24 个 10/100/1000BASE-T，4 个 1000Base-X 支持业务口堆叠，最大可支持双向 10G 堆叠带宽 交换容量 208G 转发速率 42Mpps	17、18、19 楼	15 个 IP 监控摄像头 9 个 AP 无线	1
		5-16 楼	每 3 层部署一个(每层 3 个 AP 点、4 个 IP 摄像头)	4
		2、3、4 楼	14 个 IP 监控摄像头	1

			5 个 AP 点	
		-1、1 楼	15 个 IP 监控摄像头 5 个 AP 点	1
		预留	预留	1
S2700-26TP-PWR-EI POE 供电	24 个 10/100Base-TX，2 个千兆 Combo 口 (10/100/1000Base-T 或 100/1000Base-X) 交流供电，支持 POE+ 转发性能：6.6Mpps 交换容量：32Gbps	17、18 楼	60 路 IP 电话接入	
S2700-26TP-SI 无需 POE 供电	24 个 10/100Base-TX，2 个千兆 Combo 口 (10/100/1000Base-T 或 100/1000Base-X) EI 版本提供交流供电和直流供电两种机型，SI 版本提供交流机型 转发性能：6.6Mpps 交换容量：32Gbps	19 楼	21 个信息点（IPTV、网络端口、IAD 等）	1
		4-18 楼	平均每三层总计 120 信息点（IPTV、网络端口、IAD、预留），需部署 5 台	25
		1-3 楼	35 个信息点	2

2. 中心机房推荐部署及选型

酒店的核心层设备负责全网的数据交换，是整个酒店网络互联的关键。因此，核心交换机的性能好坏、可靠性如何直接影响到整个网络。核心网络设备应是能够提供高带宽、大容量的核心路由交换设备。核心交换机应具备极高的可靠性，能够保证 7*24 小时全天候不间断运行；同时还应拥有非常好的扩展能力，以便随着网络的发展而发展。楼层配线间的接入交换机通过千兆网线或光纤接入到中心机房，核心交换机采用华为 S7703 型交换机，配置 2 台，可进行 CSS 集群部署。支持 10G、40G 交换端口，有效保障酒店内部视频点播、视频监控等大流量等大流量的应用部署。

目前××酒店的中，网络上承载的业务主要有以下几类

1、 宽带上网流量

2、 视频监控流量

3、 视频会议流量

4、 IPTV 流量

5、 IP 语音流量

6、 信息发布流量

宽带上网主要取决于酒店申请的出口带宽，一般酒店申请出口带宽在 100Mbps 以下，因此宽带上网流量不会成为 S7700 核心交换机的瓶颈，语音流量根据××酒店的配置，大约 60 门 IP 电话，740 门模拟电话，模拟电话由 IAD 接入 IP 网络，以 G.711 编码为例，每路占用带宽 64Kbps，交换性能完全满足。考虑占用较大带宽的视频监控与视频会议、IPTV，每路占用带宽约为 5~8Mbps，目前××酒店配置监控点 110 个，IPTV 点 256 个，视频会议点 5 个，总流量约为 3Gbps，对于 S7700 来说同样不会成为交换瓶颈，况且信息点不会同时占用网络带宽。信息发布系统目前布置 27 个点，每路带宽约 5Mbps。综上所示，部署的 S7700 完全能够满足目前酒店的带宽需求，同时具备可扩展性。

表 7 中心机房设备部署及选型表

产品编号	产品描述	部署建议	数量
S7703	背板容量 3Tbps 交换容量 720Gbps/1.92Tbps 包转发率 576Mpps/1440Mpps 业务槽位 3	S7700 作为酒店核心交换机，可部署 AC 模块、防火墙模块等扩充网络应用	2
S5700-28C-EI	24 个 10/100/1000Base-T，上行支持 4×1000Base-X SFP、 2×10GE XFP、2×10GE SFP+、4×10GE SFP+插卡 可插拔双电源， 分交流供电和直流供电	汇聚服务器应用，可根据服务器数量配置	1

	两种机型 包转发率：96Mpps 交换容量：256Gbps		
AR2220	转发性能：1Mpps 固定接口：3*GE（1* Combo） 插槽：4*SIC + 2*WSIC 外形尺寸（H x W x D）：44.5mm x 442mm x 420mm	作为酒店网络出口网关	1
USG2220	支持 IPS 入侵检测 支持 AV 防病毒 支持 AS 反垃圾邮件 URL 过滤 VPN：IPSec/SSL VPN	作为酒店出口防火墙	1
eSight 标准版	自定义设备管理、报表管理、安全管理、智能配置工具以及 WLAN、IPSec、SNMP 告警北向接口等业务组件。提供数据库备份工具、故障采集工具。支持多用户管理。 CPU：1*双核 2G 以上 内存：4G 硬盘空间：40G	0-200 节点	1

2.5 方案亮点

1. 层次化的可靠性设计，高速稳健的酒店网络

接入层采用 iStack 堆叠设计，核心层 CSS 集群，硬件实现 3.3ms 高精度链路故障检测，保障酒店业务不中断、电话不断线、视频无马赛克

2. 基于业务的分层QoS，灵活的带宽分配及保障机制

深度业务识别，防止 BT 等非正常业务流量对酒店关键业务以及关键客户流量形成冲击，并可以对 VIP 客户进行流量定制化，提供更高的网络带宽保障。对于语音等高优先级数据，可以提供 VoiceVLAN 等技术保障优先转发。

3. 四重安全防护，阻断病毒对网络的威胁，酒店网络安全无忧

华为从网络监管、边界防御、接入安全及远程接入等方面入手，为酒店提供四重网络安全防护：

1) 客房间 VLAN 隔离

2) 办公终端部署 NAC

3) 客房网与办公网隔离、服务器区 ACL 访问控制

4) 出口部署 UTM

4. 创新的节能技术，营造绿色酒店

1) 支持 IEEE802.3az 标准，端口能耗降低 30%

2) 独家整机休眠智能唤醒专利节能技术，助力客户构建绿色网络。业界领先节能技术，节能 40%

3) 接入交换机采用无风扇设计，自然散热、减少污染

4) 智能 POE 供电：基于 PD 设备角色启动不同的能源管理方案，保持能源管理弹性

5. eSight统一网管，简单运维

华为eSight统一网管系统是轻量级的一体化运维管理平台，采用标准协议和接口，支持多厂家设备，提供有线和无线一体化管理，其简单易用的操作界面让酒店整网设备的配置、升级、维护轻松搞定