**xx酒店网络解决方案**

目录

[需求分析 3](#_Toc12371)

[1.1行业特点 3](#_Toc29983)

[1.2场景分析 3](#_Toc6661)

[1.3用户需求框架 4](#_Toc2341)

[1.4用户需求分析 4](#_Toc15169)

[1.5设计原则 5](#_Toc7081)

[基础网络设计方案 8](#_Toc30377)

[2.1网络总体设计 8](#_Toc4017)

[2.2网络结构设计 9](#_Toc10864)

[2.2.1网络系统拓扑图 9](#_Toc15581)

[2.2.2核心层设计 10](#_Toc24840)

[2.2.3接入层设计 10](#_Toc6115)

[2.2.4无线设计 10](#_Toc10289)

[2.2.5安全模块设计 12](#_Toc15320)

[2.3关键技术点 13](#_Toc18845)

[2.3.1VSU虚拟化技术 13](#_Toc17111)

[2.3.2 智能出口 14](#_Toc14716)

[2.3.3 网络运维 16](#_Toc4293)

[解决方案价值 17](#_Toc29362)

[3.1“易组合”的网络设计 17](#_Toc2366)

[3.2“易部署”的网络架构 17](#_Toc30094)

[3.3“易安全”的网络体系 17](#_Toc12789)

[3.4“易使用”的网络管理 17](#_Toc1319)

# 需求分析

## 1.1行业特点

酒店作为服务性行业，酒店未来的竞争将主要在智能化、信息化方面展开，店内装璜、客房数量、房间设施等质量竞争和价格竞争将退居二线。网络基础设施的建设是最基本的服务，如何为顾客提供高速、稳定、易访问的优质网络体验已经成为酒店竞争的方向，同时由于酒店内部存储大量酒店房客和会员信息以及公安部82号令对安全的要求，酒店PSM专网和办公、客房网络的安全性也是酒店网络建设的重要部分，伴随着移动终端的普及和移动办公的发展，酒店无线网络建设也将成为新的热点。

## 1.2场景分析

对于智能化建筑为酒店的工程，其智能化功能主要集中的通信系统、多媒体系统、视频通话系统等，其对于建筑内部语音、数据、图像传输要求较高，往往同时存两张独立的网络，并且对网络性能要求各也不相同。

为更快更好的理解，采用化繁为简的设计思想，提炼出以下几种常见的应用场景：

1.办公网络、客房网络：以OA、MAIL、业务系统为主的办公网络和客房网络，网内用户数量大，数据流量大，对网络带宽，数据转发性能要求非常高。客房网络对于网关管理有着较高的需求，通常涉及：高速路由、链路选择策略和均衡负载、网关安全、出口带宽管理、上网行为管理、内容加速等技术。

2.酒店PMS专网：承载酒店客户资料管理、预订管理、账户管理和客房管理等核心业务，安全保密是首要要求，从接入层到核心层，要求具有防止非法接入、联网认证、访问控制等安全机制，各层网络与安全保密产品无缝融合，构建总体安全保密体系。

## 1.3用户需求框架

根据场景分析，结合网络和业务模型，用户对于基础网络要求主要包含有以下方面：

* 物理链路网络：以有线和无线构建全覆盖的基础网络链路，并要求易扩展易维护；
* 计算机网络：网络架构清晰，易于快速部署和搭建，并具有高转发性能和系统安全；
* 安全体系：从接入控制、访问控制、网关安全到内容安全的安全体系架构；
* 业务系统：分析用户的业务和应用对于网络的要求；
* 管理套件：系统设备管理和运维管理；
* 原网络核心的平滑接入或迁移。

**用户需求框架图**

## 1.4用户需求分析

1. 管理

带宽管理P2P技术的普及使得在线看电影、下载东西占用大量带宽，如果没有合理的带宽管理机制的话，将会造成网络带宽分配不均匀，客户感觉上网速度慢。

办公、客房区管理酒店的信息点的布置一般分为办公以及客房两大模块，办公的网络一般建议采取设置固定IP地址，这样方便根据实际的网络使用需求，配置相应的防火墙规则，如屏蔽某些网站、软件、上网时间管制等，而客房内的网络，一般建议采取DHCP自动获取，这样可以大大方便客人使用网络。

1. 安全

客户信息保密机制客房内的信息点应该禁止局域网互访，防止客人的电脑接入局域网后被局域网内其他的电脑入侵或者访问到其共享资源。

局域网安全防范机制由于客房内的信息点终端流动性比较大，带来通过局域网传播的病毒的可能性也大大增加，因此应该建立一个完善的局域网安全机制，能够有效地防止DOS蠕虫攻击、ARP病毒攻击等常见的局域网网络攻击。

响应公安部的82号令实现实时监控酒店客房上网情况。

1. 网络维护

网络维护成为酒店IT网络管理员头疼的事情机房网线排序不规则、通常都不清楚那根线接哪个房间。 

1. 良好的售后服务

酒店身为一个服务业企业，服务是立身之本，希望能为客人提供迅速有效的反馈。但由于酒店网管一般对路由器了解不深因此希望能很快得到咨询，并解决问题。本地化技术服务以及远程技术支持就显得非常重要了。

## 1.5设计原则

基础网络及安全是一个多系统的集成工作，它与网络规模、结构、通信协议、应用业务程序的功能和实现方式密切相关，一个好的网络设计应该结合现有网络和业务特点并充分考虑发展需求。一般应遵循以下原则：

* 方案实用

网络设计不仅要求能够满足目前酒店使用的要求，而且还应适应未来若干年以后的网络发展需要。网络的扩展可以在现有网络的基础上通过简单的增加设备和提高电路带宽的方法来解决，以适应不断增长的业务需求，保护本次网络建设的投资。

网络系统在设计时应采用国际标准协议，如网络传输协议TCP/IP、IPX/SPX等，支持SNMP、RMON等网络管理协议、支持VLAN 802.1Q标准，支持基于策略的服务RSVP、802.1P等。网络平台应具备多网络协议的支持能力，支持和兼容所有主流产品，以避免原有网络设备投资的浪费。

* 性能卓越

随着业务的增加和计算机技术的发展，接入局域网的用户将越来越多，终端和工作站的处理能力越来越强，以及图形图像和多媒体的应用越来越广泛，要求每个用户实际可用带宽很高才能使网络通信流畅，网络将成为提供多种业务的统一网络平台，并应该为不同的业务提供服务质量保证（QoS）。因此，设计时应充分考虑到将来业务量的增大，保证当前及今后一定时期内网络的高效与通畅。

* 稳定可靠

网络的可靠性是网络设计中需要考虑的一个主要原则。作为信息系统应用的依赖和基础，要求系统必须具备连续安全可靠地运行的能力，所以在系统结构设计中选用高可靠性网络产品，合理设计网络架构，尽可能利用成熟技术，网络关键部分要制定可靠的网络备份策略，对于重要的网络节点应采用先进可靠的容错技术，以保证网络系统具有故障自愈的能力，最大限度地支持专网内各业务系统的正常运行。

* 易于管理

随着网络规模的扩大和系统复杂程度的增加，网络管理和故障排除变得越来越困难。采用先进的网络管理工具，通过图形界面对网络设备进行集中化统一管理，对网络实行集中监测、分权管理，统一分配带宽资源，进行流量统计分析和故障自动报警，大大简化网络管理难度。

* 整体安全

从一个完整的安全体系结构出发，综合考虑安全保密的各种用户身份认证和各个环节，采用多种安全手段，包括防止非法接入、访问控制、入侵检测、网关安全、边界防护、身份认证、内容安全等等。即保证网络的安全可靠，又尽量符合界面友好人性化的特点。

* 行业特点

行业业务特征决定了网络设备的需求，也决定了网络设备的技术选型要求，因此必须以用户的实际需求出发，合理的选择使用网络技术和产品。

# 基础网络设计方案

## 2.1网络总体设计

计算机网络系统以目前国际流行的TCP/IP为基础，采用OSI体系结构，遵循国际标准，整个计算机网络系统采用星型拓扑结构。

* 规范化的网络基础架构

采用扁平化(二层物理架构)的基于万兆IP以太网络，将传统酒店的PMS网络、酒店OA网络、客房网络(无线网络)进行分类有效整合，满足酒店PMS专网高安全、高稳定的需求，实现酒店OA及客房网络对网络应用行为、人员身份的智能化控制，减少网络硬件设备数量，降低因为网络设备硬件故障造成网络中断的概率，同时为未来网络扩展做好充分预留保护投资。

* IT运行维护—智能化

XX网络凭借强大的自主研发能力，在满足所有硬件设备及软件协议符合业界标准的同时，开发出VSU交换机虚拟化技术、CPP路由交换机设备CPU保护、TPP网络拓扑保护等功能，使网络设备的维护工作量尽可能的降为最低，同时使网络故障处理最大程度的智能化，实现大部分网络故障无人工干预智能完成。

* 网络应用—特色化

在酒店传统客房有线网络的基础上，XX网络增加基于802.11N技术的无线网络、WEB重定向、ANY IP等全新的酒店网络应用，使酒店客房网络应用更丰富，更具有特色，从而提升住店客人体验，增强酒店竞争力，为酒店创造更多收入。

在本方案中，网络系统按系统结构规划为：局域网和广域网两个部分。

广域网主要由各种功能的路由器、应用服务器、网络安全设备等组成。

局域网按网络层次分为：核心层、汇聚层、接入层。

无线系统作为局域网的重要组成部分不仅能覆盖有线难以敷设区域，同时满足无线需求，由各型终端AP和控制器组成。

## 2.2网络结构设计

网络设计通常要遵循层次化设计模型。网络可分为核心层、接入层。以无线网络作为酒店服务的亮点。

核心层主要承担高速数据交换的任务，同时要为各汇聚节点提供最佳传输通道。

接入层的主要任务是完成用户的接入，它直接和用户连接，可能遭受ARP风暴、MAC扫描、ICMP风暴、带宽攻击等等攻击方式，对安全性的要求很高，另一方面必须提供灵活的用户管理手段。

通过层次化的网络设计，网络的不同层次设备承担不同的任务，使整个网络结构清晰，便于维护和管理，便于以后的网络扩展。

### 2.2.1网络系统拓扑图

酒店网络系统由两张网组成，一张是酒店PMS专网，一张是酒店OA和客房网络，如下图：

酒店网络系统拓扑图

### 2.2.2核心层设计

核心层：由高性能的设备和高速冗余的链路构成，实现数据的高速转发、负载均衡、流量控制、网络管理等功能。

在网络的中心节点，核心层的设备传统上会使用高性能的交换机和高速路由器来进行第二层交换和第三层路由。在网络核心层，网络核心设备不仅要能保证第二层的交换和第三层的路由，还要提供完善的虚拟网划分，多协议路由，QoS处理，以及多媒体的通信支持。

### 2.2.3接入层设计

接入层负责所有信息节点的接入，由高性能设备和高速冗余的链路构成，实现数据的高速转发、路由快速汇聚、负载均衡、流量控制、网络管理等功能。

接入层往往信息点数量较多，所以接入层设备需要高性能的交换能力，考虑到对未来应用的集成及现有的安全部署能够很好支持，接入交换机

至少应满足如下条件：

1.全线速智能可网管百兆交换机；

2.对于需要POE供电的AP需要接入交换机支持POE供电

3.二至四层线速转发，二至七层智能识别；

4.支持802.1X认证、端口隔离和端口、MAC、IP绑定功能；

5.强大的流控和广播风暴抑制功能；

6.先进的服务质量(QoS)、精确速率限制、ACL和组播服务，实现了网络控制和带宽优化；

7.支持多种验证方法、数据加密技术和基于用户、端口和MAC地址的NAC。

### 2.2.4无线设计

将WLAN技术应用于桌面系统可以为一个组织提供传统LAN所不能提供的灵活性。桌面客户机系统可以被放置在不可能进行或不适于进行布线的地方。桌面PC可以根据需要在设施内的任何地方进行重新部署，这一特性使无线方案成为临时工作组或快速成长组织的理想选择。

无线网络已经得到越来越多的应用，成为有线网络覆盖的有力补充和替代方案，XX网络对酒店的无线网络的设计具体表现在以下几个方面。

* **无线信号覆盖最优**

对于酒店客房，由于厚实的墙壁以及内部洗手间对无线信号的阻碍，传统放装式的无线部署方式无法实现客房信号的完全覆盖，甚至由于无线AP的密集部署造成严重的信号干扰，客户体验很差，传统的室分AP由于需要穿墙并使用功分器、耦合器等配件导致无线实施复杂，且增加故障点。深圳市艺通能科技有限公司对于酒店这种类型的部署环境推出GNT-AP520/GNT-AP535，采用了墙面安装设计，整个安装过程只需要两步就能快速实现无线网络覆盖。第一步、拆去房间内原有的有线网络的接口面板，第二步、将原有网线插在GNT-520/GNT-535上并直接安装就能即插即用。它打破了以往无线网络建设的老旧方式，无需再拉新的网线，而是有效利用了既有的网络，将网络新建对酒店等环境的影响时间降到最低。

对于酒店会议大厅，传统的放装AP信号覆盖范围有限，XXX发出GNT-AP260、GNT-AP270、GNT-AP280彻底解决传统天线存在覆盖盲区的弱点。无论在任何角落，真正实现全面覆盖，绝无死角。

* **无线性能最优**

桢田无线AP全部采用支持802.11n协议的无线AP，最高带宽可达300M，满足高密度用户的接入，并且桢田推出支持802.11ac协议的千兆无线AP，满足高带宽的需求。

* **无线集中管理**

无线AP全部为胖瘦一体化结构，当工作在FIT模式时，由无线控制器统一进行配置和管理，并且能够实现无线的快速故障定位，减轻无线管理的工作量

### 2.2.5安全模块设计

安全模块设计

如图所示，安全保障体系可以划分为身份鉴别、访问控制、安全防护和存储备份几部分，其中，访问控制层包括安全网关、访问控制系统，身份鉴别层包括用户身份认证系统、证书注册管理系统、用户鉴权访问系统和实体鉴别器，安全防护层包括等。

1. 防火墙

防火墙可以作为不同网络之间信息的出入口，进行网络边界防御，控制不同网段之间的信息通道，对进出相应网段的网络访问行为进行严格控制，监控进出网络的全部信息，避免各业务系统被非法访问和使用，以及网络资源和重要数据被泄露或遭到破坏。

1. 访问控制

安全保障体系的访问控制层包括安全网关、访问控制系统和VPN密码系统，分别加以描述。安全网关是用户进入政务业务网的接入和访问控制设备，它具有用户身份认证代理的功能，能够和认证服务器交互，完成用户身份认证，根据认证结果和对该用户的可信网络访问授权，完成网络接入的鉴权控制。

1. 网关管理

出口采用综合性网关支持URL自动过滤、用户日志审计、行为审计等安全功能

具有强大的防火墙功能，支持快速包过滤、报文过滤、状态检测，根据安全策略对数据流进行检查，让合法的流量通过，将非法的流量阻止，从而达到访问控制的目的。支持防攻击、防扫描，同时可记录攻击主机的地址信息，定位攻击源。RG-EG系列可防御目前几乎所有类型的攻击。硬件过滤攻击报文，不占用CPU资源。

## 2.3关键技术点

### 2.3.1VSU虚拟化技术

VSU（Virtual Switch Unit）是一种虚拟化技术，将两台或更多台设备组合为单一的虚拟交换机，解决了MSTP+VRRP上述提到的问题，从而，简化网络拓扑，降低网络的复杂性，缩短恢复的时间和业务中断时间，提高网络设备与链路的利用率。

1. 更高效的、更合理的链路与设备的利用率

在VSU环境中，连使用AP口连接下联设备，达到三层网关备份和无环路的链路冗余备份作用。在VSU系统中，通过VSL(Virtual Switch Link)链路把VSU成员设备组成一台虚拟逻辑设备，接入层设备通过AP口上联到VSU系统，对外表现是一条逻辑链路，不存在网络环路，并可以根据AP的复杂均衡机制，提高链路带宽利用率。而且，每台VSU成员设备所保存的配置文件相同，当VSU断裂后，能保持业务的连续性。

2. 更高的可靠性

VSU设备间采用毫秒级的心跳探测机制，IP BFD和MADP（多活动主机检测协议），故障切换能达到毫秒级，接入设备通过AP口上联到VSU系统，AP链路本身除了负载均衡外，链路切换也是在毫秒级别的。

3. 更简化的网络拓扑、更简便的设备管理

VSU系统对外表现是一台逻辑的设备，各种控制协议作为一台设备运行，减少设备间大量协议报文的交互，缩短了路由收敛时间；在管理上，有统一的管理界面、一致的转发表项，简化了网络拓扑，设备管理与维护更简单。

2.3.2WALL-AP

GNT-AP520/GNT-AP535是桢田专门为酒店、办公室和小区楼房无线网络推出的新一代基于802.11n协议的迷你型无线接入点（AP）。GNT-AP520/GNT-AP535的尺寸符合标准的86开关面板盒规格，而且还集成了以太网口和IP电话接口，整机设计简洁美观、部署便捷，是酒店等环境无线网络建设的最佳选择。

 WallAP

* 只需两步，轻松部署无线

GNT-AP520/GNT-AP535采用了墙面安装设计，整个安装过程只需要两步就能快速实现无线网络覆盖。第一步、拆去房间内原有的有线网络的接口面板，第二步、将原有网线插在GNT-AP520/GNT-AP535上并直接安装就能即插即用。它打破了以往无线网络建设的老旧方式，无需再拉新的网线，而是有效利用了既有的网络，将网络新建对酒店等环境的影响时间降到最低。无线部署，就是这么简单、快捷！

* 最优信号，畅享快捷无线

GNT-AP520/GNT-AP535因实际部署在房间内部墙面上直接进行无线网络覆盖，避免了普通AP直接安装在楼道中必须要穿透厚重墙壁甚至是入室厕所等带来的室内信号差、网络不可用的问题。用户在房间内任意位置都能获得满格无线信号，语音、视频或者浏览网页等任何业务使用都能尽享优质快捷无线！

* AP再多，都能集中快速管理

AP都支持胖（Fat）和瘦（Fit）两种工作模式，客户可根据自身网络规模灵活选择，有利于将客户的WLAN网络由小型平滑升级到大型网络，很好地保护了用户投资。而且在酒店等场景下，客房数量多，所用到的AP也多，只需配合我司无线控制器（AC）就能进行集中批量管理，甚至是快速故障定位等。相较于普通soho级AP(家用)，极大的方便了网络运维人员管理整个无线网络！

### 2.3.2 智能出口

桢田的RG-EG出口网关作为一款ALL IN ONE设备在为酒店提供流控、行为管理、防火墙、高性能NAT、智能DNS、日志审计、用户管理等综合业务的同时，将原来的多台网络设备简化为单台网络设备，大大减轻了酒店网络运维的压力。

通过DPI技术实现业内第四代基于应用的弹性带宽控制技术，良好的解决了酒店出口带宽紧张的问题。

1. 智能出口

首先将酒店客房网与OA出口进行按应用的流量控制，当客房网流量空闲时，OA网络可以抢占客房网络带宽；当OA网空闲时，客房网可以抢占OA网带宽(如夜间酒店大部分员工都已下班，OA网络带宽使用率低，而白天客房网带宽利用率又相对较低)；同时保留核心业务的关键带宽不可以被抢占，以保证核心关键业务的正常运行；然后分别对客房网与OA网的应用流量进行分类弹性限速，当带宽有剩余时，可抢占，当网络带宽紧张时，每类应用只使用预分配的固定带宽，从而始终保持酒店OA与客房网出口带宽处于最大利用率，同时又不会因为P2P之类的应用导致酒店OA与客房网络出口带宽紧张进而影响酒店其它网络应用正常工作。

1. 权限控制

酒店OA网络主要是为酒店正常的日常办公使用，若上网行为无管理控制、记录审计，就会出现员工利用酒店OA网络做与工作无关的事情，如打网游、看电影、炒股等，导致工作效率下降，酒店重要数据丢失或被篡改，酒店经营受到损失。

1. 上网审计

桢田RG-EG出口网关设备，具有强大的网络上网WEB实名认证、行为管理、上网应用审计并记录的功能。在同一台RG-EG出口网关设备下，可以方便灵活地控制酒店OA网员工的上网行为，比如必须实名认证，工作时间不得在网上聊天、炒股、看电影等行为，并对酒店内部员工在网络中通过邮件、FTP、IM等方式的数据转发进行关键字过滤审核，并进行实名记录。这样一来，既提高了酒店员工的工作效率，又保护酒店核心机密数据的安全。而对于酒店住店客人，则根据需要灵活控制上网是否认证；当然，针对酒店员工的上网应用控制，对住店客户可完全放开，只对不良关键字及URL进行过滤，最大程度的满足住店客人的上网灵活性与多样性，同时不侵犯住店客人的隐私。

RG-EG，以WEB重定向功能主动推送酒店信息，提升酒店品牌，扩大销售机会。对于酒店来说，品牌的提升意味着更高的品牌认知度和客户忠诚度，便于形成酒店稳定的客户群体，从而稳定酒店的营业收入。通过RG-EG的WEB重定向功能，酒店客人第一次在酒店访问internet时，页面将直接推送酒店官方页面或可展示酒店广告、 宣传信息的相关链接，刺激住客需求，增加酒店经济效益。

### 2.3.3 网络运维

桢田AC控制器专注于拓扑展现、网络变更、设备故障监控、配置管理，采用纯B/S友好的全中文Web浏览器界面，可以远程协同维护和管理，采用非代理模式，避免了传统的“Agent”模式的繁琐和重复性劳动，而且便于实施和后期维护，极大地节省了工作时间和工作繁杂度；主动式的网管，可定义管理任务，主动收集网络状况并及时备份，做到状态变更的及时响应，出现故障可及时恢复；提供直观绚丽的网络拓扑图，俯瞰整个网络现状，出现异常时，在拓扑图上及时呈现。通过热点图了解当前网络故障点等信息。产品可跨异构网络进行发现和管理，支持大部分厂家的众多设备，提供图形化的配置界面，实现对设备配置修改,从而大大降低管理员的维护强度和难度。

# 解决方案价值

## 3.1“易组合”的网络设计

根据用户行业特点和网络细分要求进行设计网络方案

根据用户数的规模快速定位和设计网络方案

根据用户对网络性能的要求合理的选择网络技术和产品选型

根据用户智能建筑子系统类别提供不同特性网络产品支持

## 3.2“易部署”的网络架构

三层网络架构分层分级部署，配置灵活

无线系统终端、控制器与交换机无缝结合，方便部署

网络设备管理集中，无线配置管理集中，实施快速，维护简易

## 3.3“易安全”的网络体系

从接入认证、防止非法接入、防止私自串联到边界防护的总体网络安全防护技术

高速易用的SSL VPN技术，方便子网和分支结构的安全快速接入

802.1x技术，极大的提高了无线网络访问控制安全

出口管理按需分配链路资源，结合内容缓存提高宽带利用率；实现实名制认证，便于管理

信息发布内容保护、防攻击防窃取，立体防御安全联动机制

## 3.4“易使用”的网络管理

统一的网管平台

统一的无线管理平台

统一的身份认证中心

统一的运营管理平台

统一的服务保障体系

统一的健康监控管理