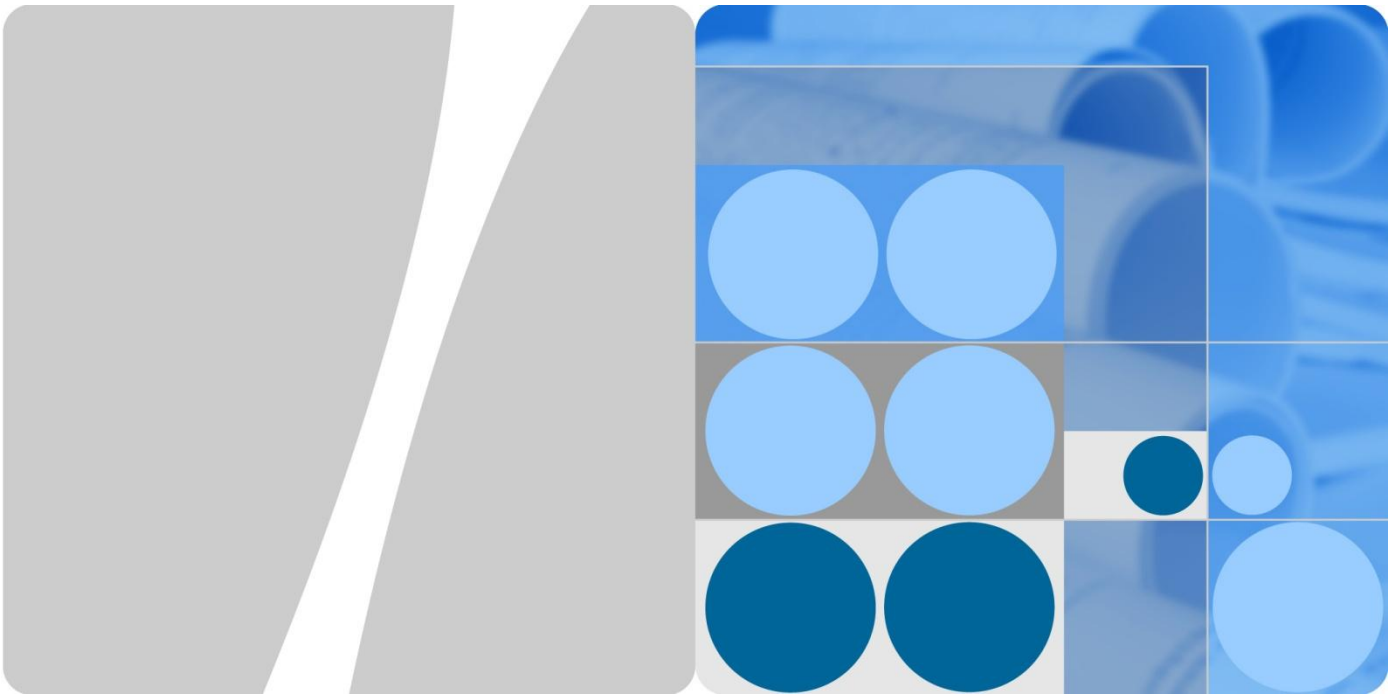
资料编码



One Net Campus 机场基础网络通信解决方案 V100R001C03

部署指南

文档版本 01

发布日期 2012-08-30

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暗示的声明或保证。

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://enterprise.huawei.com

客户服务邮箱： ChinaEnterprise_TAC@huawei.com

客户服务电话： 400-822-9999

目 录

1 方案概述

1.1 机场园区基础网络通信解决方案简介

本技术方案建议书在基于对实际项目的实施基础上，分析现有数据中心网络、灾难备份网络的网络架构和网络管理等方面的现状，并结合国内外相关行业发展经验，对机场园区基础网络通信解决方案进行深化设计和实施。

机场园区的网络系统从机场信息业务处理及总体规划上可分为航站楼网络（面向旅客的航班服务）、物流区网络（面向货物的航班运输服务）和办公区网络（面向企业 OA 和管理服务）。这三个网络中，航站楼网络为机场园区网络的核心，本技术方案主要针对航站楼网络的部署给出技术建议。

航站楼网络根据机场不同业务应用的特殊要求，分为几个物理上相对独立的网络系统。分别是信息网、离港网、安防网、安检网、安检信息网、商业 POS 网、综合业务网和设备专网，这些网络连接到航站楼骨干网，实现网间信息交换及不同区域信息交换。

1.2 网络总体需求及设计原则

1.2.1 先进性要求

机场航站楼网络系统是机场整个业务的基础，在网络建设中首先要考虑网络系统的先进性。先进性首先体现在网络设计和建设需具备开放性、安全性和扩充性。整个网络结构设计应具有长远、统一的规划并预留开放、标准的接口，为今后的进一步扩展打下基础。在技术上、系统能力上充分参考国内外成功案例及先进的技术，使网络架构可以保持五年以上的先进性，从而有效保护了用户的利益。同时先进性还体现在设备选型、二层河三层网络参数规划、安全、管理及业务扩展等各个方面。

1.2.2 适用性要求

机场航站楼网络系统服务于全机场的各业务系统和机场用户。设计需要在充分理解机场应用系统、业务数据流以及用户访问模式的前提下，综合考虑业务永续性、安全控制策略、网络层负载均衡等应用需求，进行细致的网络设计与规划。

1.2.3 标准化要求

标准化要求是指遵循业界公认的标准制定一个高兼容性网络架构，确保设备和技术的互通性、互操作性，支持网络、节点的扩展，方便快速部署新的产品和技术，以适应业务的快速增长。标准化要求是网络规划及设备采购的一个最基本的要求，可以提升网络的扩展能力，同时保护用户投资。

1.2.4 可用性要求

网络的稳定可靠是业务系统健康运行的重要条件之一，所以对网络整体架构的高可用性和高可靠性设计必须全面考虑。网络架构必须能够达到业务系统对服务级别的要求，并且能够通过多层次的冗余，使得整个架构能够满足业务系统不间断稳定运行的需求，同时实现网络层面的灾难恢复。

1.2.5 可管理性要求

机场航站楼网络的架构、规划和管理都建立在“一个整体”的基础之上。整体设计过程中需充分考虑网络架构的易于管理性。网络设计的简单化直接关系到网络的运行和维护成本，也是网络稳定运行的保障。

1.3 关键需求及目标网络架构

1.3.1 网络总体架构要求

航站楼网络包括如下 8 个物理独立的功能网络。

- 信息网

  信息网是机场地面信息系统的核心部分，主要支持地面信息系统、航班显示系统、广播系统等。

- 离港网

  离港网主要为离港系统（自助值机、离港控制系统 DCS、行李再确认系统）提供网络服务。

- 综合业务网

  综合业务网是综合网络支撑平台，目前承载的业务系统主要有 OA、EGIS 等，以后可能还会有新的业务系统运行在综合业务网上。另外，综合业务网为用户提供 Internet 接入。

- POS 网

  POS 网主要为机场各种商业销售系统提供网络平台。

- 安检网

  安检网主要为机场安检系统提供网络支撑服务。安检系统分为集中安检和手提行李安检 2 个部分。

- 安检信息网

  安检信息网主要为安检信息管理系统提供网络服务。

- 安防网

安防网主要为视频监控系统和门禁系统提供网络支撑服务。

- 设备专网

  设备专网为楼宇控制、电动扶梯、登机桥、照明系统等提供网络平台，本方案中设备专网考虑到设备工作环境等因素，接入层交换机采用工业以太网交换机，而核心、汇聚设备采用商业交换机。

1.3.2 网络路由要求

为提高网络稳定性及可扩展性，机场网络需要采用支持分区域的路由规划，并且需要综合考虑路由协议的开放性、可扩展性、灵活性和可管理性等方面进行比较和选择。可以选择成熟的、稳定的路由协议作为航站楼网络的路由协议，同时要求路由协议可以很好地支持航站楼的网络规模。

1.3.3 网络数据链路层控制要求

实施广播控制是要将广播带来的副作用（CPU 资源占用、网络带宽占用等）尽量限制在一个小的范围内。对于使用广播传输的应用应将广播转换为单播的方式进行转发。对广播主要采取以下两个方面进行限制。

- 对本地接入用户进行分类，并进行 VLAN 划分。
- 限制跨交换机的 VLAN 划分。

1.3.4 网络性能要求

在需求分析过程中，需要充分了解各个子网的性能需求特性。将其映射到网络对于系统架构和技术的要求，以保障业务系统可以正常地在网络平台上运行。

1.3.5 网络安全控制要求

网络安全实现的内容包括防火墙系统、入侵检测系统（IDS）、防病毒系统、远程访问安全、无线局域网络（WLAN）安全和安全管理系统（网络安全设备综合管理系统和终端安全管理系统）等方面。

防火墙系统

防火墙系统是整个安全体系中的第一道防护设备，为外网与内网之间、内网用户之间建立起安全防护系统。从而保护内网或服务器区免受非法用户的侵入。防火墙系统对流经它的网络通信进行扫描，过滤掉一些 L2-L4 的简单攻击。

防火墙布置于内网与外网的连接处，以防止来自外网的非法用户的侵入。

- 部署双防火墙能够实现冗余备份、负载均衡及高可靠性。
- 防火墙系统支持日志服务器。
- 防火墙系统包括内部防火墙和外部防火墙。
  - 内部防火墙用于航站楼网络的各业务网之间的安全隔离和访问控制。
  - 外部防火墙用于综合业务网外部互联、离港网异地值机与空管等外部网络的互连，采用独立防火墙设备。

入侵检测系统（IDS）

IDS 在网络系统中的若干关键点收集信息并分析，从中发现网络系统中是否有违反安全策略的行为和被攻击的迹象，识别出已知的攻击行为并报警。

IDS 系统部署在核心或者汇聚交换机出口。

远程访问安全

远程访问的用户是指通过互联网或直连网络访问机场业务网络的外部用户（信息网的 ATC、航空公司以及 DCS 广域网中民航实时外联用户除外）。远程访问的用户需要进行相应的远程访问安全认证，可以通过 SSL VPN 网关设备建立加密的 VPN 的隧道，达到访问相应业务系统的目的。

防病毒系统

随着计算机数字病毒的种类与传播手段日益增加，数字病毒更迅速地通过网络共享文件、电子邮件及 Internet/Intranet 在网络中传播。由于数字病毒的破坏力难以预料，计算机病毒防护已经成为现代的网络系统安全策略中的重要内容。

部署防病毒系统主要防止来自内部的病毒（U 盘等）对主机的破坏，进而防止对整个网络的破坏。设备部署上，在骨干节点区（航站区路由交换机）部署一级防病毒服务器，在不同的业务网设置二级防病毒服务器，对客户端和服务器系统进行集中安全防护管理。

无线局域网络（WLAN）安全

WLAN 安全包括 WLAN 移动终端同 AP 之间加密、认证授权等安全措施，也包括移动终端接入 WLAN 后，访问内部网络及 Internet 的安全措施。

对于移动终端同 AP 之间加密、认证和授权，可以采用业界标准 EAP、WEP 等加密方式和标准的 RADIUS 系统。

1.3.6 网络管理要求

部署需求

网络管理系统是对整个网络性能、网络运行状况和故障进行统一管理的平台。该平台能够提供自动发现、可视化展现、网络故障分析、配置管理、安全管理和性能管理等全面细致的网络管理功能。

在设备部署上，在骨干节点区部署网络资源管理服务器，在不同的业务网络均可考虑设置网络管理工作站，构成集中 / 分布式的网络管理解决方案。在分布式管理模式时，可以按照所管辖的网络范围进行划分，实现分层次的管理方式。

总体要求

- 采用国际标准的 SNMP 协议实现对网络设备和网络安全设备的管理。
- 具有管理大型、多节点网络的能力。
- 自动发现网络的拓扑结构图，全面管理网络中的各种设备，并通过不同的色彩描述网络设备的运行状态。

- 能自动对网络进行监测，自动轮询网络状态，搜集网络中的故障和报警等信息。
- 实现全面、统一、深入的网络设备管理模式，提供故障管理、配置管理和性能管理等功能。
- 采用易于操作的图形界面。

具体要求

- 网络管理系统能针对设备提供网元级管理，其功能如下。
  - 提供配制管理；
  - 提供 RMON 管理；
  - 可以监控网络设备的物理状态，实时提供详细的管理信息，查看端口状态；
  - 提供网络流量统计等。
- 能自动发现网络拓扑结构，构造和维护网络系统的配置。能完成网络关键设备配置的语法检查，自动生成配置文件和自动配置备份系统，对于配置的一致性进行严格的检验。
- 可提供链路及端口可用性、利用率、吞吐量等性能指标。采集和分析网络对象的性能数据，统计网络运行状态信息，对网络的使用发展做出评测、估计，为网络统一规划与调整提供依据。
- 能过滤网络事件。能有效地发现、定位网络故障，给出处理建议，形成整套的故障发现、告警与处理机制。
- 能提供各 VLAN 的逻辑视图和相关目录信息。
- 可通过目录服务，提供分支式资源管理。
- 能通过保存配置文件，快速恢复设备内所有的配置。

1.3.7 网络 QoS 要求

针对网络承载应用的特点，对应用进行分类，以保证各自数据传输不受影响。对于敏感性的应用能提供带宽保证，如语音通讯、视频通讯等。数据可以根据重要级别进行重要、尽力而为和不必尽力的分类，并根据需要将重要的流量进一步划分成若干子类。

服务质量保证要符合 DiffServ QoS，在网络拥塞情况下，针对关键业务提供高优先级保证。

1.3.8 网络可靠性要求

在网络设计中，需要考虑网络的可靠性，关键节点设备需要双备份，充分考虑技术实现的冗余。可以利用网络 L2、L3 不同层面的技术，充分保障航站楼网络运行的稳定性。

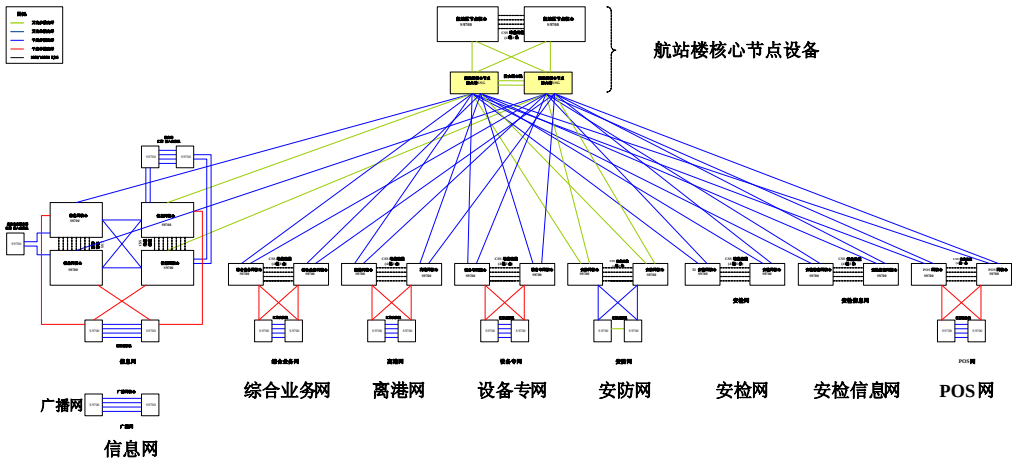
2 骨干网网络需求

2.1 骨干网络架构需求

航站楼网络总体架构如图 2-1 所示。设备可用的选型如下。

- 航站楼核心设备选用 S9700 系列交换机
- 各个二级网络核心设备选用 S9700 系列交换机
- 核心防火墙设备选用 USG 系列防火墙
- 汇聚层设备选用 S9700/7700 系列交换机
- 接入层设备选用 S5700 系列交换机

图2-1 航站楼网络总体架构示意图



信息网、离港网、综合业务网、POS 网、安检网、安检信息网、安防网和设备专网各网络都由各自独立的网络核心、汇聚、接入设备（安检网和安检信息网只有核心设备和接入二层设备）。所有这些网络都通过各自网络核心设备连接到航站楼核心节点的防火墙，从而形成全网的互连互通。在核心节点防火墙上，可以部署网间的访问控制。

其中信息网和安防网以万兆链路连接到核心节点设备，其它网络则以千兆链路连接到核心节点设备。

核心节点设备由一对核心节点交换机和核心节点防火墙组成。核心节点交换机实现高速的数据交换。核心节点防火墙则将航站楼不同的子网定义为对应的安全域，通过访问安全策略来实现不同子网间的互连互通，以提高网络安全性。

在机场完成了物流园区和办公区网络建设后，航站楼节点核心交换机将提供航站楼网络与其它网络的互连互通。

2.2 骨干网络路由需求

路由规划是网络规划的重要内容之一，需要考察路由协议的成熟性、开放性、可扩展性、灵活性和可管理性等方面，进行比较和选择。

表2-1 路由协议对比

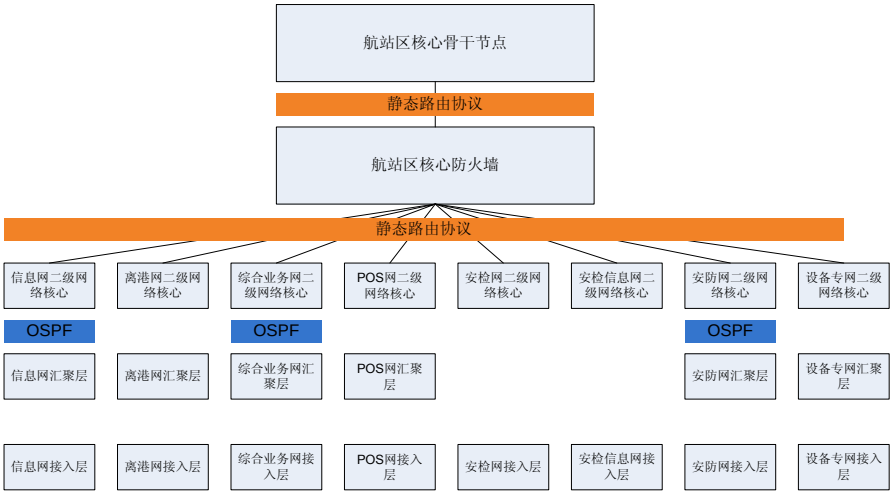
路由协议	优点	注意事项
OSPF	开放的路由协议。 路由收敛快。 有区域划分的概念，支持中等规模网络。	路由负载均衡控制能力弱。 配置相对复杂。
BGP	开放的路由协议。 对数据路径的控制手段很强。 通过自治域内、域间的定义，支持大规模网络。	配置相对复杂。 需要较高的维护技能。
静态路由	配置简单。	只适合小规模网络。 容易形成路由环路。

如表 2-1 所示，不同的网络路由协议有不同的特性以及所适应的应用场合，考虑到航站楼各个网络的架构设计，建议按照如下思路部署路由协议。

- 信息网、综合业务网、安防网采用 OSPF 动态路由协议，提高网络灵活性，并且易于管理和维护；
- 安检网、安检信息网由于是核心-接入两层网络架构，建议核心-接入之间部署纯 L2 结构；
- 离港网、设备专网、POS 网由于考虑到业务需求，部署纯 L2 结构网络，因此采用静态路由协议；
- 考虑防火墙对静态路由的支持更加稳定，航站区核心节点设备与各个网络二级核心之间选用静态路由。

部署路由协议后的网络如图 2-2 所示。

图2-2 部署路由协议后的航站网络示意图



2.3 骨干网络性能需求

航站楼各子网汇接到航站楼节点防火墙，实现全网的互连互通，各子网根据业务流量不同可以使用不同的带宽。另外建议各子网节点采用双链路链接，保证网络的可靠性。

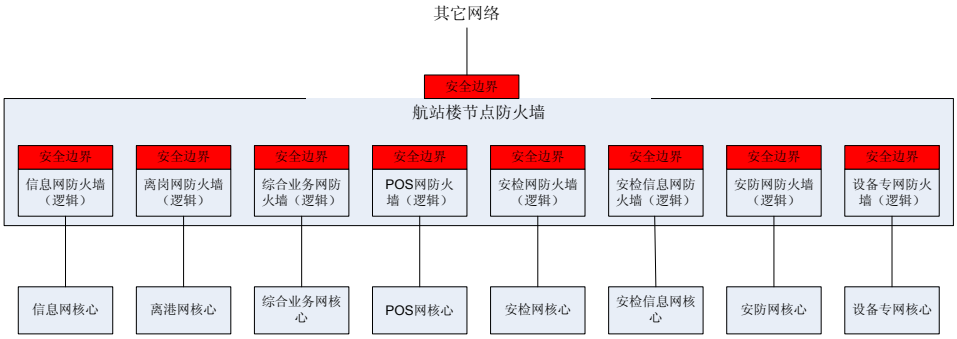
2.4 骨干网络安全性需求

骨干网核心节点防火墙承担了航站楼各子网的链路汇聚。在防火墙上，需要对各个子网划分不同的安全域（等效于多个虚拟防火墙），并通过访问策略的部署，实现各个子网间、有访问控制的互连互通。

另外，核心节点防火墙也承担整个航站楼网络与其它网络间的互联互通的访问安全控制，例如与办公区网络的访问安全控制等。

骨干网络安全架构如图 2-3 所示。

图2-3 航站骨干网络安全架构示意图

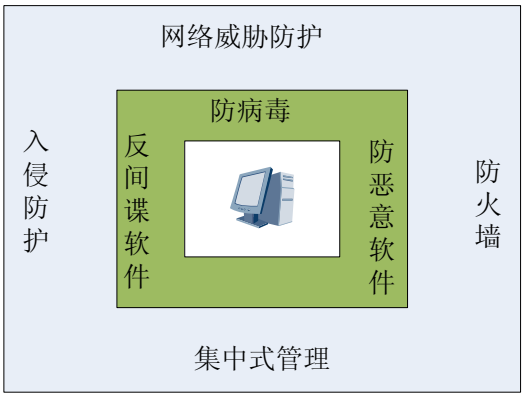


2.5 骨干网络其它需求

2.5.1 防病毒系统

航站楼网络部署了防病毒系统。航站楼将拥有各类型功能不同且为数众多的工作台，基于保护终端操作系统安全以及网络异常流量与攻击行为多由工作台所引起等原因，必需为各工作台建制相关的安全防护机制以确保工作台的网络操作安全。

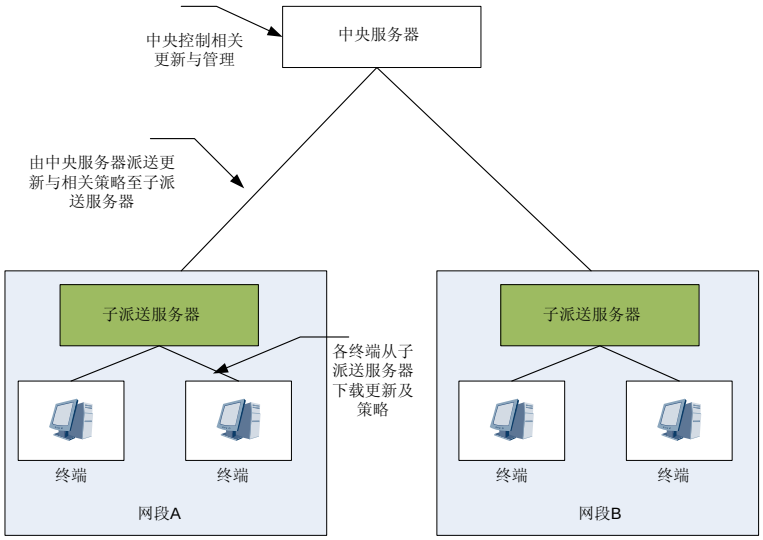
图2-4 防病毒系统



防病毒系统在航站楼为笔记本、台式机和服务器提供抵御恶意软件的防护能力。可以防御复杂的攻击，如 rootkit、零日攻击和间谍软件。

系统架构如图 2-5 所示，采用“统一控制，二级管理”架构，中央防病毒服务器部署在核心节点，在其它网络单元部署防病毒分发系统。

图2-5 防病毒系统架构



2.5.2 集中网管系统

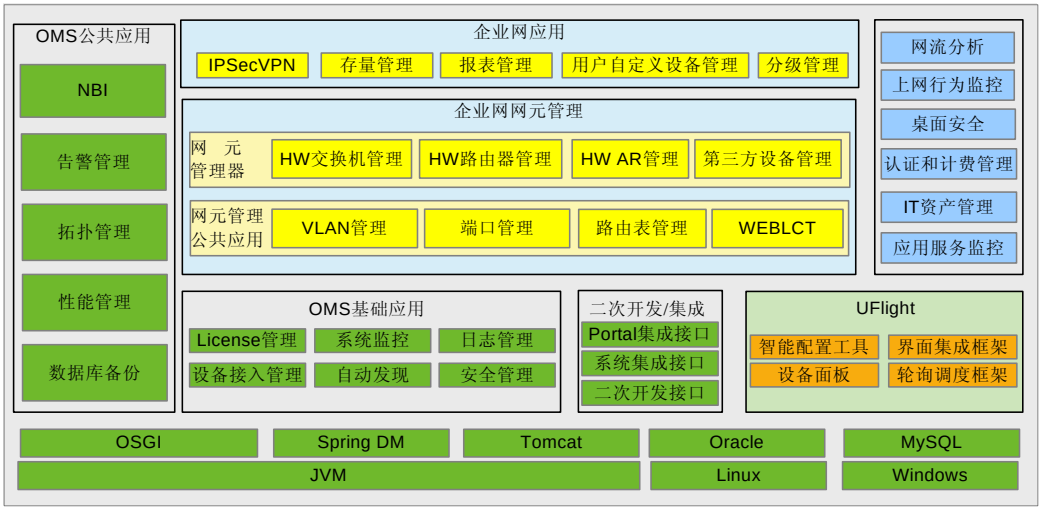
eSight 网管平台简介

eSight 网管平台是华为面向企业网管理推出的新一代面向企业园区和分支网络管理系统，可以实现对企业资源、业务、用户的统一管理以及智能联动。eSight 应用平台支持对 IT&IP，以及第三方设备的统一管理，同时可以对网络流量、接入认证角色等进行智能分析，自动调整网络控制策略，全方位保证企业网络安全。同时，eSight 应用平台提供灵活的开放平台，为企业量身打造自己的智能管理系统提供基础。

eSight 具备灵活的第三方设备管理能力，支持多种操作系统，可以根据管理需要提供差异化的版本。同时 eSight 是多业务管理承载平台，eSight 应用平台不仅在网络资源管理的基础上实现了拓扑、故障、性能、配置、安全等管理功能，而且还可以作为其他业务管理组件的承载平台，共同实现管理的深入融合联动。软件通过流程向导的方式告诉用户如何使用功能，为用户提供了精细化的管理。

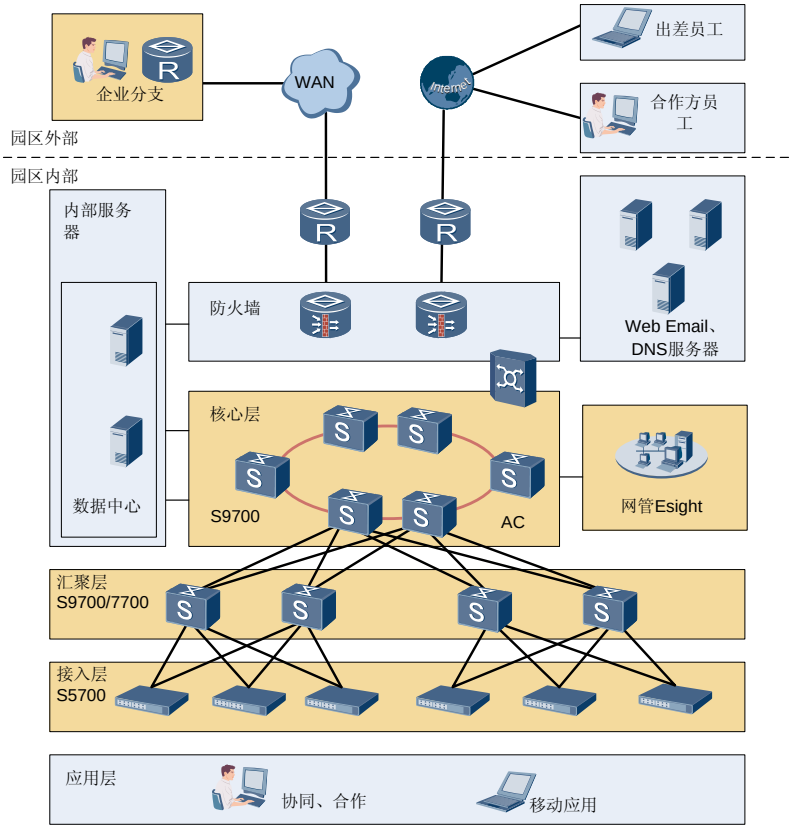
eSight 应用平台作为 B/S 架构，拥有 B/S 架构的先天优势。它运行在客户端的浏览器之上，系统升级或维护时只需更新服务器端软件即可，这样就大大减轻了客户端电脑载荷，简化了系统维护与升级的成本和工作量。

图2-6 eSight 应用平台组件图



eSight 应用平台部署模式是 B/S 模式，支持多浏览器同时接入。eSight 能实现多系统集成管理和 IT 与 IP 的统一管理。eSight 与网元配合的解决方案场景如图 2-7 所示。

图2-7 eSight 配合解决方案场景



eSight 网络管理功能

eSight 应用平台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。

- 安全管理

  安全管理实现对网管系统本身的安全控制，通过对用户、角色、权限和操作集等管理，保证网管系统的安全。

- 日志管理

  日志信息记录了用户进行的一些重要操作。用户可以查看、过滤日志列表，还可以详细查看某条系统日志的内容。支持管理操作日志、安全日志和系统日志，提供提示、一般和危险三种级别的信息。

- 网元管理

  网管对设备的管理，包括设备添加和删除。提供子网的管理方式，用户可以根据实际设备的物理位置，划分不同的子网对设备进行区域管理。

- 拓扑管理

  拓扑管理是指以拓扑图的方式显示被管网元及其之间连接的状态。用户可通过浏览拓扑视图来实时了解整个网络的运行情况。

- 告警管理

  告警管理是对网络中的异常运行情况进行实时监视，通过告警实时浏览、告警操作、告警规则设定（屏蔽规则、声音设定）、告警远程通知等手段，便于网络管理员及时采取措施，恢复网络正常运行。

- 性能管理

  eSight 可以对网络的关键性指标进行监控，并对采集到性能数据进行统计。通过可视化的操作界面，方便用户对网络性能进行管理。

- 物理资源

  eSight 可以针对企业提供用户对设备的配置功能，提供用户对设备机框、单板、子卡及端口的查询功能。

- 报表管理

  eSight 通过任务执行生成报表，支持周期报表任务、即时报表任务。支持报表导出为 PDF、Excel、Word、PowerPoint 等常见文件格式。eSight 预集成了丰富的报表模板，可以满足常见的网络运维报表需求。同时，提供了灵活的报表设计工具，支持用户自定制报表模板，以实现个性化的报表需求。

- 自定义设备管理

  针对企业网用户需要管理多种厂商的设备类型，eSight 提供了自定义管理功能。用户通过自定义管理模块，完成对设备类型、性能指标、告警参数、配置文件管理、设备面板的定制，增强对设备基本能力的管理。

- 配置文件管理

  配置文件管理指对设备的配置信息进行管理，提供对设备配置文件的备份、恢复、比较和基线化管理。当网络出现问题时，可以根据之前备份的网络可运行时的配置文件与当前设备正在运行的配置进行比较，帮助您快速定位并恢复当前出现的故障。

- 智能配置工具

  智能配置工具用于对华为设备进行单网元业务配置，或者多网元批量配置。

- WLAN 业务管理

  WLAN（Wireless Local Area Network）无线局域网是指应用无线通信技术将计算机设备互联起来，构成可以互相通信和实现资源共享的网络体系。它是一种利用无线技术实现快速接入以太网的技术。

- 分级网管管理

  eSight 支持用户建立分级分层的网络管理方案。用户可以将网络按照需求，将网络进行分级分层。eSight 支持在上级网管维护下级网管列表，通过链接可以直接打开下级网管的界面。从而实现查看下级网管告警、拓扑、性能和报表等功能。

- 系统 Portal 首页

  Portal 首页以图形化形式提供重要监控信息一览，并支持用户自定义显示监控信息和格式。

- 数据转储与备份

  eSight 应用平台提供独立于网络应用平台的 WEB 服务实现数据库备份、恢复管理。供用户进行数据库数据的备份和恢复功能。

3 信息网网络需求

3.1 业务概述

信息网是机场的核心业务网络，主要承载的业务系统包括：地面信息系统（GOIS）、航显系统（FIDS）和广播系统（广播网在设备层面看是物理独立的网络。但从业务上来讲属于信息网范畴）。

3.2 信息网络架构需求

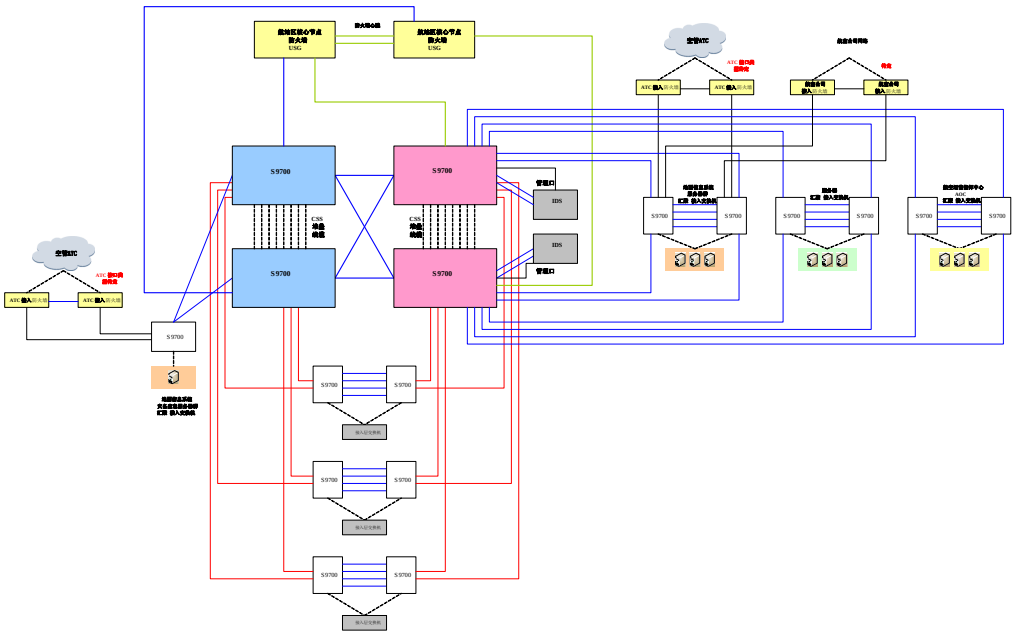
信息网将采用万兆以太网技术。整个信息网分为核心、汇聚、接入三层星型网络架构，其中核心--汇聚速率为千兆，汇聚--接入为千兆，终端--接入为 100M。信息网核心以万兆连接至航站楼核心节点。

在信息系统主机房内和航站楼主机房内分别设置核心交换机 S9700/7700 系列，建议通过 CSS 堆叠线缆连接，构成 1 台逻辑的交换机。该虚拟化的技术，将处于同一物理位置的两台核心设备虚拟成逻辑上一台更大容量的核心设备，可以提高信息网核心设备的可靠性，冗余性更好，并可以实现流量分担。

主机房核心交换机通过万兆以太链路与航站区核心节点防火墙相连，实现信息网与其他网络间的数据交换。

设置服务器区汇聚/接入层交换机（S9700/7700 系列）用于 GOIS 等服务器接入。在航站楼分别设置一组汇聚层交换机（S9700/7700 系列）用于用户终端汇聚。用户汇聚交换机分别连接到信息网核心交换机上，信息网网络拓扑如所示。

图3-1 信息网网络拓扑



另外，从业务定义上来看，信息网框架内还包括广播网。广播网是信息网内的广播系统的网络支撑平台，从网络设备角度来看，广播网为完全物理独立的网络，不直接与信息网互连，与信息网之间的信息交互通过广播网服务器双网卡实现。

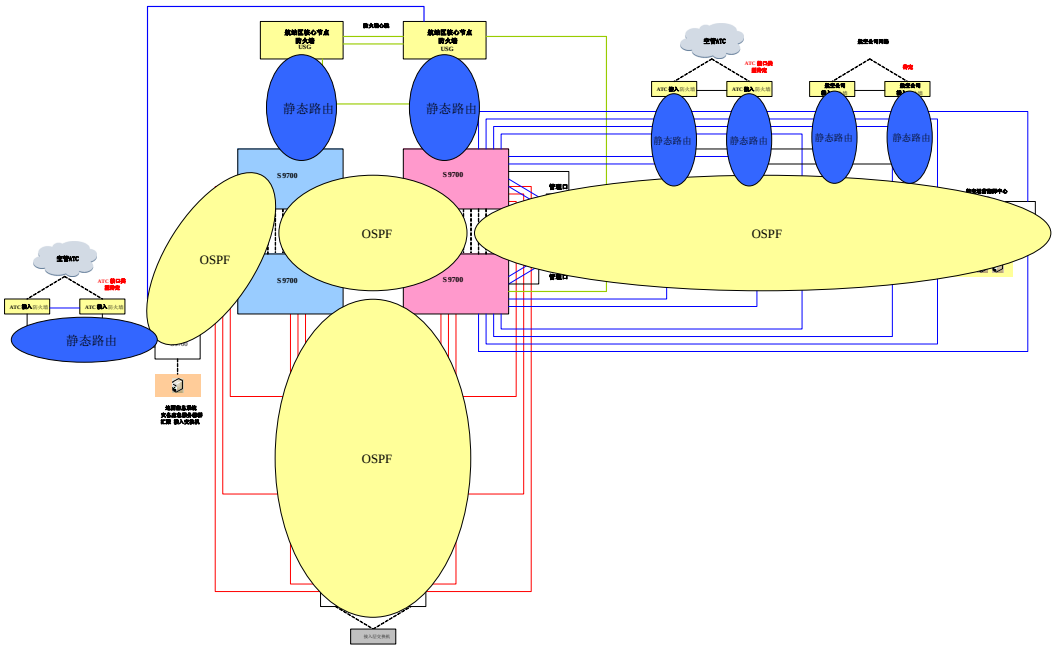
3.3 信息网络路由需求

从网络规模来看，信息网属于中型网络。从网络建设最佳实践来看，标准化、开放的路由协议是首先需要考虑的。同时在信息网内部路由协议的选择方面，内部路由协议需具备快速收敛、能够区域划分、支持中等规模网络等技术特性。从这个意义上来讲，OSPF路由协议是适合于信息网网内的路由协议。

信息网与航站楼其它网络之间，以及信息网与 ATC 之间，由于有防火墙隔离，考虑到路由配置管理的便利性和路由的稳定性，建议采用静态路由，因此，建议信息网采用如图 3-2 所示的路由设计。

- 信息网网内利用 OSPF 动态路由协议
- 信息网与核心节点防火墙之间运行静态路由协议
- 信息网与 ATC 之间运行静态路由协议

图3-2 信息网的路由设计示意图



3.4 信息网络承载业务需求

3.4.1 地面信息系统

地面信息系统是机场的核心生产业务系统，其主要业务功能包括：

- 机场运行数据库（AODB）作为存储中心，完成季度航班计划、短期航班计划、日航班计划、营运航班计划、航班业务基础参数、航班运行相关数据和历史数据等的存储；
- 智能集成业务交换平台（IMF）作为 AODB 与各子系统和外部接口之间通讯的集成业务平台，它将基于中间件平台，支持跨平台系统连接，实现地面信息系统与各子系统、子系统与子系统之间数据的交互和通信；
- 集成信息网关（IMG）负责接收航班计划和动态信息，并根据优先级处理所有的航班动态信息和计划信息。作为航班信息源的有 AFTN 报文、SITA 报文、基地航空公司、空管；
- 航班信息管理系统（FIMS）负责管理机场航班及其资源的季度计划、短期计划、日计划、营运计划、历史计划、资源动态变化情况和历史情况；
- 机场营运资源管理系统（ORMS）负责对机场营运资源进行分配和管理；
- 运行监控管理系统（OMMS）用于监控和管理外场和航站楼内的各种保障服务和生产活动，对外场和航站楼内的各种航班运营保障服务提供实时监控管理的综合系统；
- 重要旅客服务系统（VIPSS）根据机场重要旅客服务工作的需要，为行政贵宾旅客（VIP）和商务贵宾旅客（CIP）提供全方位的乘机服务，包括 VIP（含 CIP）服务计划的记录、查询等；

- 航班信息查询系统（FQS）（含 FQDB），FQS 是机场内部各单位进行信息发布与沟通的重要工具；
- AMDB 及航空业务分析系统，机场管理数据库 AMDB（Airport Management DataBase）存储机场用于管理、统计、业务分析用途的各种数据。对于地面信息系统，航班历史记录需要存储到 AMDB 中；
- 应急预案管理系统（EPMS）是一个基于用户配置的流程维护管理系统，用以辨别相关事故，维护事故处理流程预案；
- 运行管理平台（OMMP）的功能主要包括：
  - 地面信息系统的操作系统安全、数据库安全、用户安全策略以及防病毒等方面的内容；
  - 网络的运行管理和安全管理；
  - 为地面信息系统范围内（包括：AODB、IMF、IMG、FIMS、ORMS、OMMS、FQDB、FQS、VIPSS、EPMS、DBS、外部接口等）的应用进行监控，数据库、主机、操作系统、集群系统等的性能监控，用户统一管理，地面信息系统报修管理，地面信息系统维护流程等。

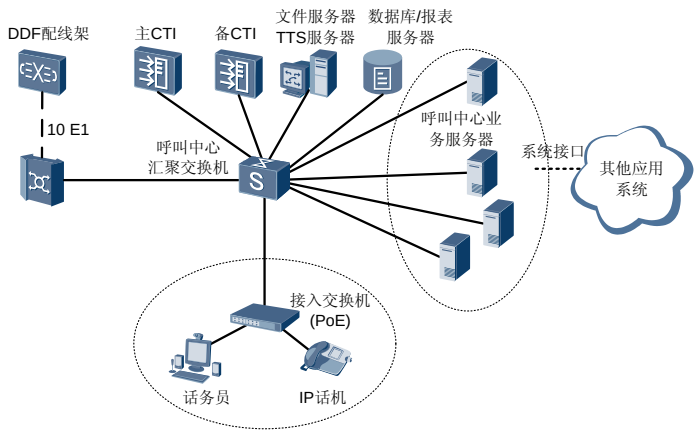
3.4.2 呼叫中心

呼叫中心系统业务描述

航站楼信息网内部署有呼叫中心。呼叫中心作为综合信息服务平台，是一个集计算机技术、Internet 技术、CTI 技术、IVR 技术、数据库技术、CRM 技术、PBX 技术和网络技术等为一体的集成系统。它将机场内分属各职能部门为客户提供的服务，集中在一个统一的对外联系“窗口”，通过采用统一的标准服务界面，为用户提供系统化、智能化、个性化、人性化的服务。

呼叫中心系统架构示意如图 3-3 所示，呼叫中心平台系统采用华为呼叫中心平台，系统设备包括 CTI/IVR、平台数据库、文件服务器、TTS 服务器，以及话务员坐席等。

图3-3 呼叫中心系统技术架构示意图



呼叫中心系统数据流向分析

- 呼叫中心坐席以浏览器访问呼叫中心应用服务器

- 呼叫中心服务器之间互相访问
- 呼叫中心接口服务器实现与其它业务系统的接口

呼叫中心系统应用服务端口表

在详细设计阶段，将需要系统供应商提供应用服务访问端口表，以在网络实施时部署准确的应用服务访问控制，提高应用服务的安全性。

呼叫中心系统外联接口需求列表

呼叫中心系统与集中安检、安检信息系统、行李分拣、地面信息系统有系统接口。

呼叫中心系统内服务器节点部署需求列表

示例如表 3-1 所示。

表3-1 呼叫中心系统内服务器节点部署需求列表

服务器名称	用途	数量	部署位置	接口需求
文件服务器				
报表服务器				
呼叫中心业务服务器				

3.5 信息网络安全性需求

信息网安全边界如图 3-4 所示，边界包括外部安全边界和内部安全边界。

红色部分为外部安全边界，包括以下几部分。

- 信息网与航站楼其它网络，以及与航站楼节点外的其它节点网络（例如物流园区网络、办公区网络等）的边界；
- 信息网与 ATC 网络之间的安全边界；
- 信息网与航空公司网络之间的安全边界。

针对上述安全边界，需要部署防火墙实施严格的网络隔离和控制，利用 ACL，控制网络间、系统间的系统访问，提高网络安全性。

橙色部分为内部安全边界，包括：

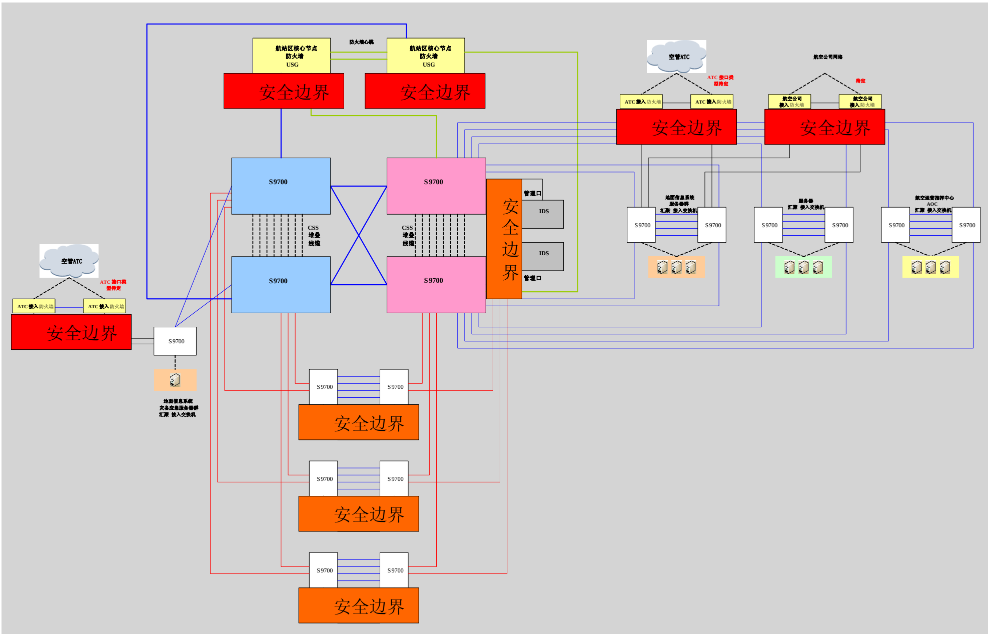
- 信息网内服务器接入网络的安全边界；
- 信息网内客户端接入网络的安全边界。

针对内部安全边界，需要部署适当的网络安全技术，提供访问安全保护，包括：

- 在核心交换机部署 IDS，检测网络访问安全事件；

– 在客户端，通过防病毒系统，提供客户端自身的防病毒能力，以提高客户端的系统安全性。

图3-4 信息网安全边界



3.6 信息网网络 QoS 需求

首先，从技术应用角度来看，只有在网络出现拥塞的情况下，才需要部署 QoS，以对业务应用进行分类，并保障关键业务优先使用网络资源。信息网承载的业务应用都是基于 TCP/IP 的数据类应用，各业务系统的数据流量都不大，S9700/7700/5700 系列交换机可以很好地支持业务应用，因此，信息网不需要部署 QoS。

3.7 信息网网络管理需求

在航站楼网络节点核心集中部署网络管理系统，用于网络拓扑、网络设备等的集中管理，因此，需要信息网网络设备具备以下能力。

- 支持 SNMP 功能；
- 支持设定网管系统定义的 SNMP read community 和 SNMP write community；
- 支持将系统时钟（NTP）服务器指定为网络统一的 NTP 时钟源。

说明

考虑到配置的小型机服务器以及数据库等的管理需求，需要配置带外管理交换机，在详细设计阶段需要考虑。

4 离港网网络需求

4.1 离港网架构需求

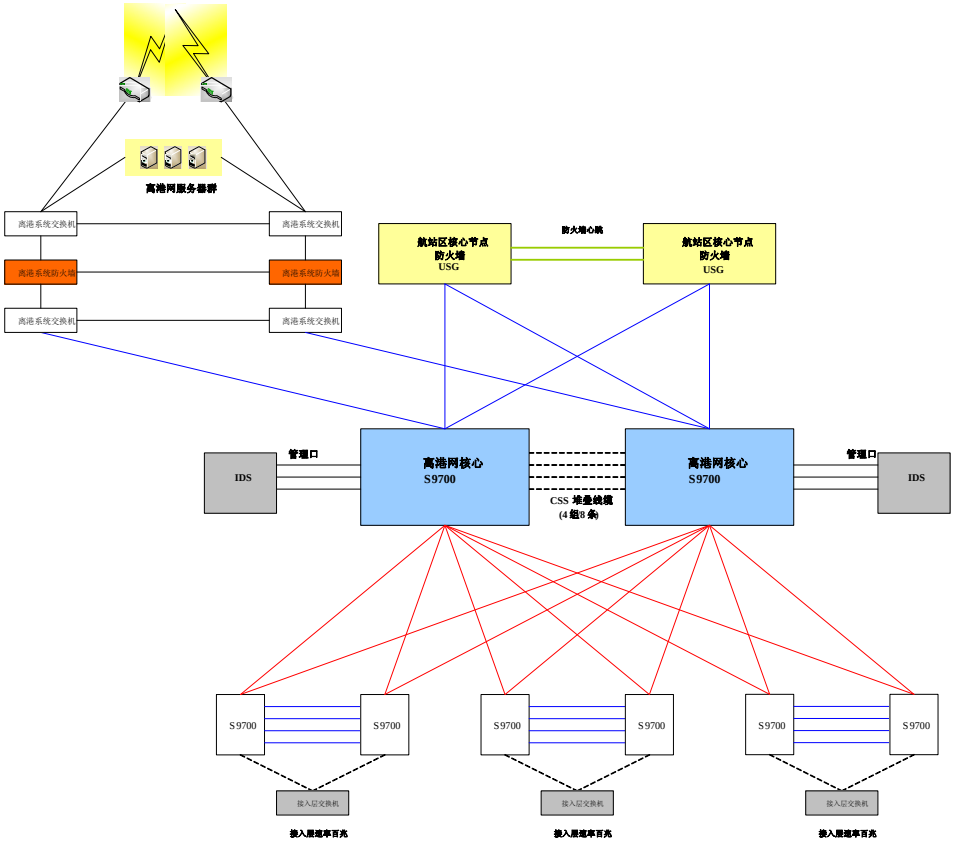
离港网主要是为离港系统（自助值机、DCS、行李再确认系统）提供网络接入服务的网络。

离港网采用千兆以太网技术，网络拓扑采用核心、汇聚、接入三层网络设计。进行端口聚合的端口要求跨板或者跨框部署，并预留千兆备用链路。

离港网核心层采用 S9700 系列交换机，通过 CSS 堆叠线缆连接，可以将两台交换机构成一台逻辑的交换机。该虚拟化的技术，将处于同一物理位置的两台核心设备虚拟成逻辑上一台更大容量的核心设备，提高信息网核心设备的可靠性，冗余性更好，并可以实现流量分担。

汇聚设备采用 S9700/7700 系列交换机。

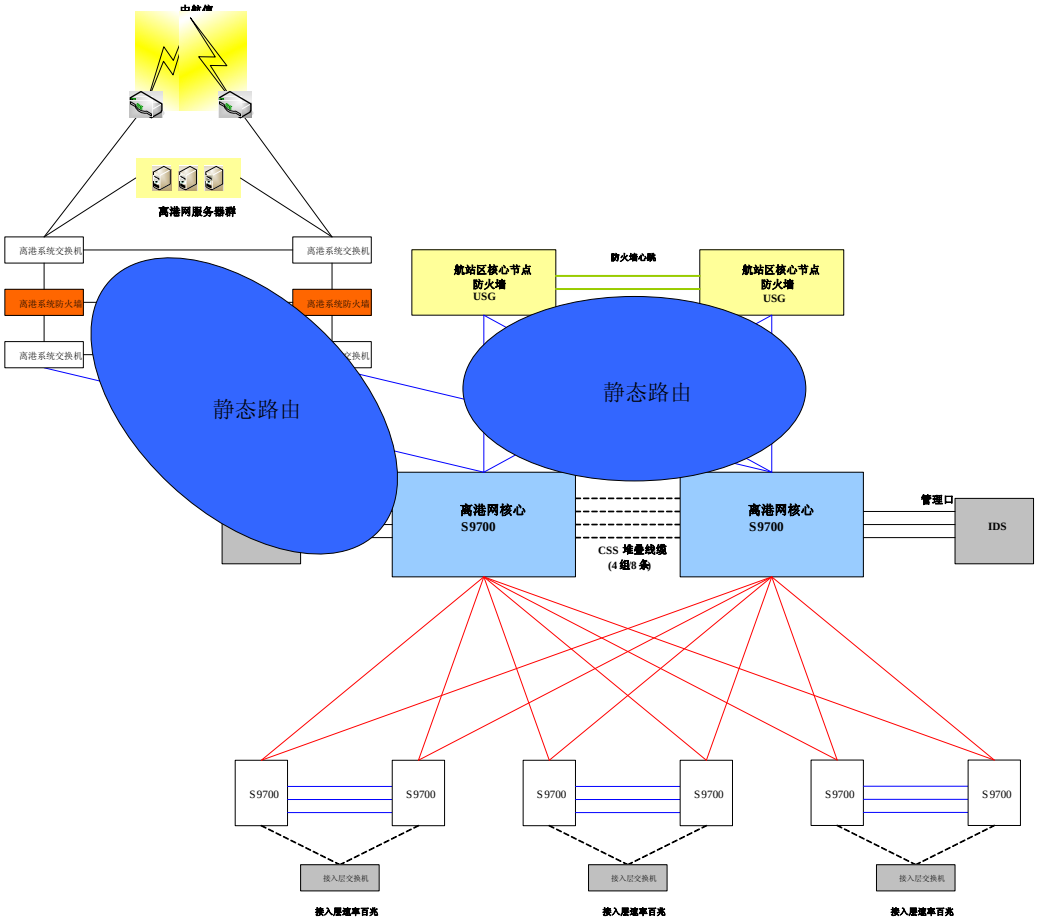
图4-1 离港网网络拓扑示意图



4.2 离港网路由需求

离港系统与离港网核心之间，离港网与航站楼其它网络之间，由于有防火墙隔离，离港系统前端需要将网关部署在离港网核心交换机上，因此，离港网将全部采用静态路由。离港网的路由设计如图 4-2 所示。

图4-2 离港网的路由设计



4.3 离港系统架构需求

DCS 系统业务描述

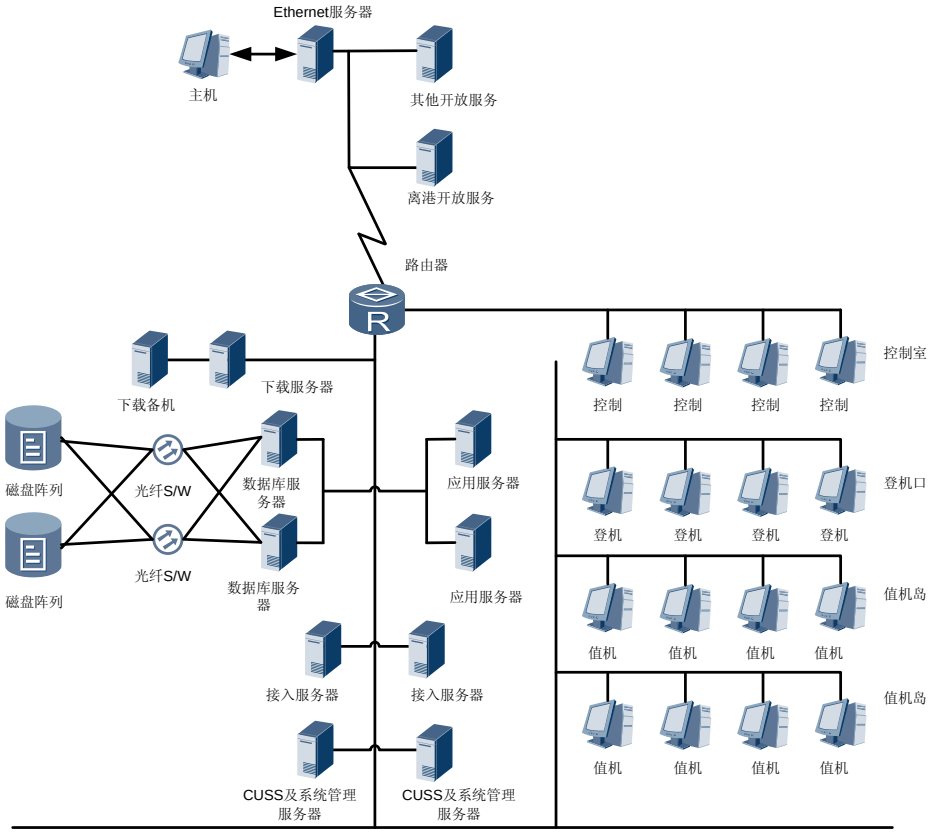
离港控制系统（Departure Control System）是面向旅客服务的实时交易系统，是航空公司及其代理、机场地面服务人员在处理旅客乘机过程中，为旅客办理值保证航班正点安

全起飞的一个面向用户的实时的计算机事务处理系统。离港系统主要包括值机、控制、配载等业务功能。

离港网主要为离港系统（自助值机、DCS、行李再确认系统）提供网络服务。其中 DCS 为离岗系统的核心，离港网系统建好后，建议机场网络通过统一的互联接口接入。

DCS 系统技术架构示意图

图4-3 DCS 系统架构示意图



DCS 系统由自助值机服务器、报文下载服务器、集成接口服务器、离港应用服务器等和离港值机、登机、配载、控制工作站等组成。

- 数据库服务器用于业务数据的存储、管理；
- 报文下载服务器用于与中航信服务器之间报文收发、格式转换等工作；
- 离港应用服务器用于为本地值机、登机等终端提供应用服务。

DCS 系统数据流向分析

- 离港前端访问离港应用服务器；
- 自助值机设备访问自助值机服务器；
- 离港前端访问离港应用服务器；

- 自助值机设备访问自助值机服务器；
- 集成接口（AMB）服务器与其它业务系统互访；

DCS 系统数据流量分析

每终端 100M 接入，并发数以 20%计算，根据终端数量确定离港核心与离港系统防火墙（中航信提供的防火墙）之间连接带宽。

DCS 系统应用服务端口表

在详细设计阶段，将需要系统供应商提供应用服务访问端口表，以在网络实施时部署准确的应用服务访问控制，提高应用服务的安全性。

DCS 系统外联接口需求列表

DCS 系统与集中安检、安检信息系统、行李分拣、地面信息系统有系统接口。

DCS 系统内服务器节点部署需求列表

示例如表 4-1 所示。

表4-1 DCS 系统内服务器节点部署需求列表

服务器名称	用途	数量	部署位置	接口需求
数据库服务器				
报文下载服务器				
离港应用服务器				
自助值机服务器				
集成接口（AMB）服务器				
其它服务器				

4.4 DCS 网网络吞吐量需求

根据实际需求确定。

4.5 DCS 网网络性能需求

每终端 100M 接入，并发数以 20%计算，来确定离港核心与离港系统防火墙（中航信提供的防火墙）之间连接带宽。

4.6 DCS 网网络广播控制需求

离港网将是一张二层网络，离港前端设备网关集中部署在离港网核心交换机上。

4.7 DCS 网网络安全需求

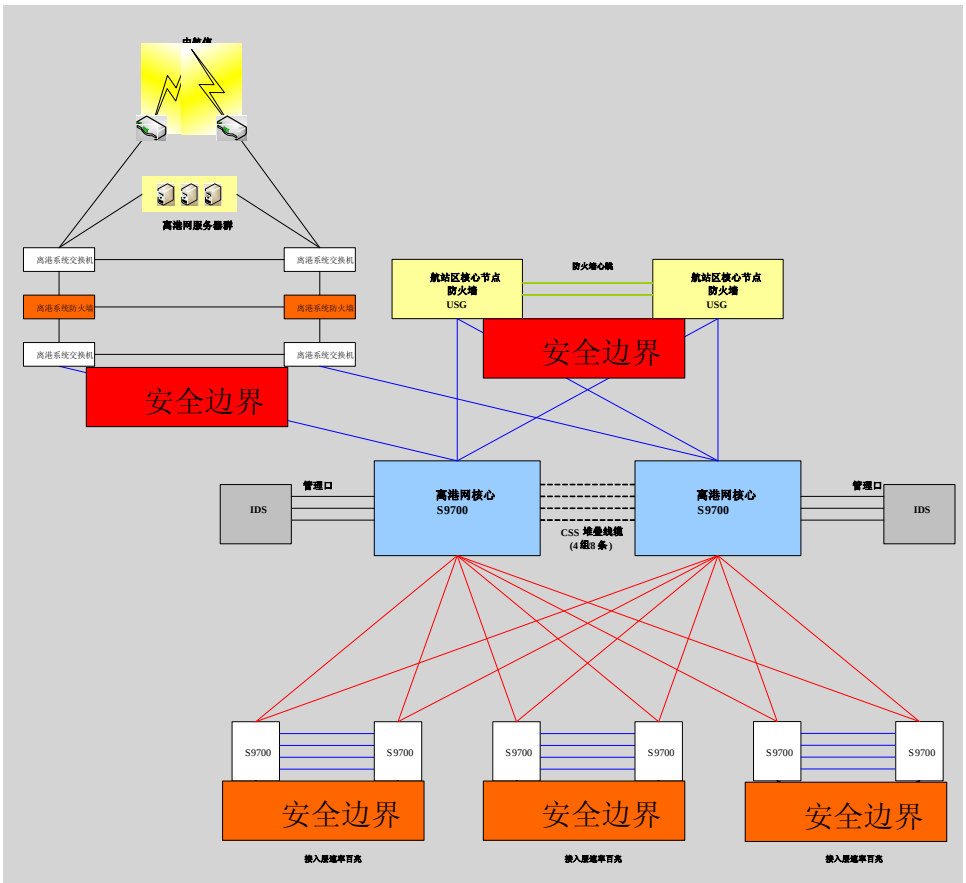
离港网安全边界如图 4-4 所示，包括外部边界安全和内部边界安全。

- 红色部分为外部安全边界（以航站楼网络为基准，DCS 系统作为外部系统），包括：
  - 航站楼 DCS 网络与 DCS 系统之间的安全边界；
  - 航站楼 DCS 网络与航站楼其它网络之间的安全边界；

  针对上述安全边界，需要部署防火墙实施严格的网络隔离和控制，利用 ACL，控制网络间、系统间的系统访问，提高网络安全性。DCS 系统服务器前端需要部署防火墙。
- 橙色部分为内部安全边界，包括 DCS 网网络边缘，客户端接入的安全边界；

  在客户端，通过防病毒系统 SEP，提供客户端自身的防病毒能力，提高客户端的系统安全性。

图4-4 DCS 网网络安全边界



4.8 DCS 网网络 QOS 需求

从技术应用角度来看，只有在网络出现拥塞的情况下，才需要部署 QoS，以对业务应用进行分类，并保障关键业务优先使用网络资源。而 DCS 网络承载的业务应用，都是基于 TCP/IP 的数据类应用，各业务系统的数据流量都不大，S9700/7700/5700 系列交换机可以很好地支持业务应用，因此，DCS 网络不需要部署 QoS。

4.9 DCS 网网络管理需求

在航站楼网络节点核心集中部署网络管理系统，用于网络拓扑、网络设备等的集中管理，因此，需要 DCS 网络设备具备以下能力。

- 支持 SNMP 功能；
- 支持设定网管系统定义的 SNMP read community 和 SNMP write community；
- 支持将系统时钟（NTP）服务器指定为网络统一的 NTP 时钟源。

说明

考虑到配置的小型机服务器以及数据库等的管理需求，需要配置带外管理交换机，在详细设计阶段需要考虑。

4.10 DCS 网其它需求

离港网中需要考虑无线网络。考虑在值机大厅与行李分拣大厅，为行李再确认终端等应用提供 WLAN 接入，按照实际规划给出相关数量，布放方式。建议接入交换机需要配置 PoE 功能，为无线 AP 提供网络供电功能。

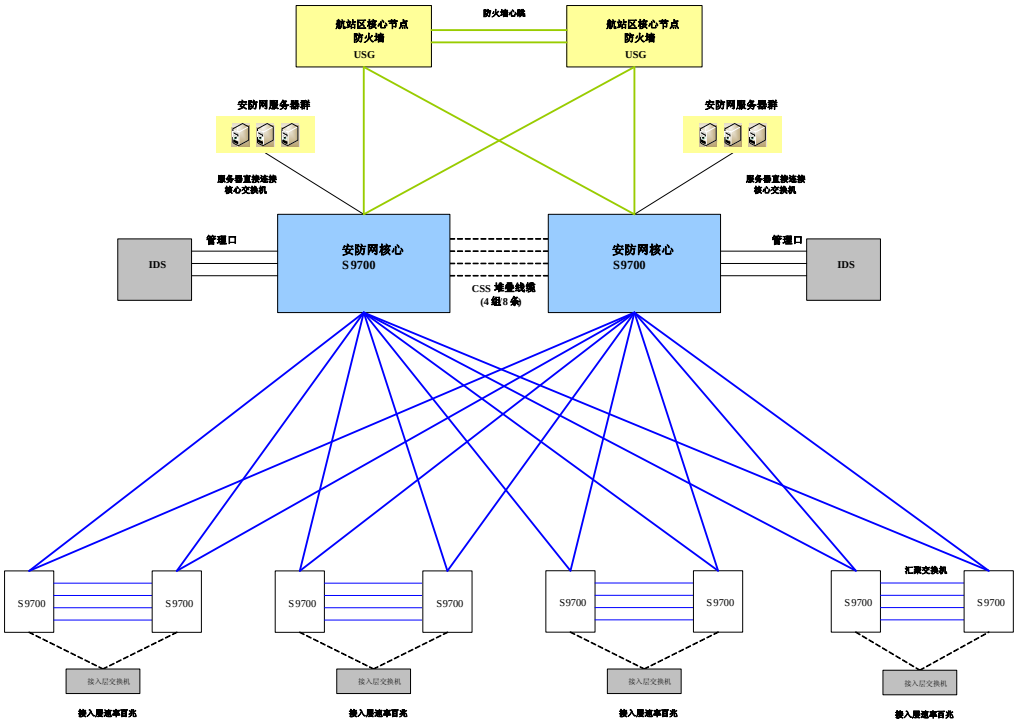
5 安防网网络需求

5.1 安防网架构需求

安防网主要是为视频监控系统、门禁系统和道路系统提供网络接入服务。安防网采用万兆以太网技术。网络结构为核心、汇聚、接入三层网络设计，核心层采用高性能交换机S9700/7700 组成，核心交换机之间通过虚拟化技术，构成一个整合的逻辑实体，简化网络 L2 的设计。

在安全边界部份，安防网需要部署 IDS 设备以作为服务器的安全保护边界，安防网拓扑如图 5-1 所示。

图5-1 安防网拓扑



安防网内主要数据流为视频数据流，网络中需考虑组播的设计。考虑到集中监控中心以及移动监控终端访问各个视频采集设备（摄像头）的需求，在安防网的 IP 组播设计中，将考虑针对每一路的摄像机数据流作为一个独立的视频组播组传输。

视频数据流主要由视频采集前端设备（数字化摄像头/视频编码器），以组播方式向视频存储服务器/LCD 监视器传送。另外，在安防网内以及安检信息网，可能有远程视频调度终端，访问现场视频数据的需求。

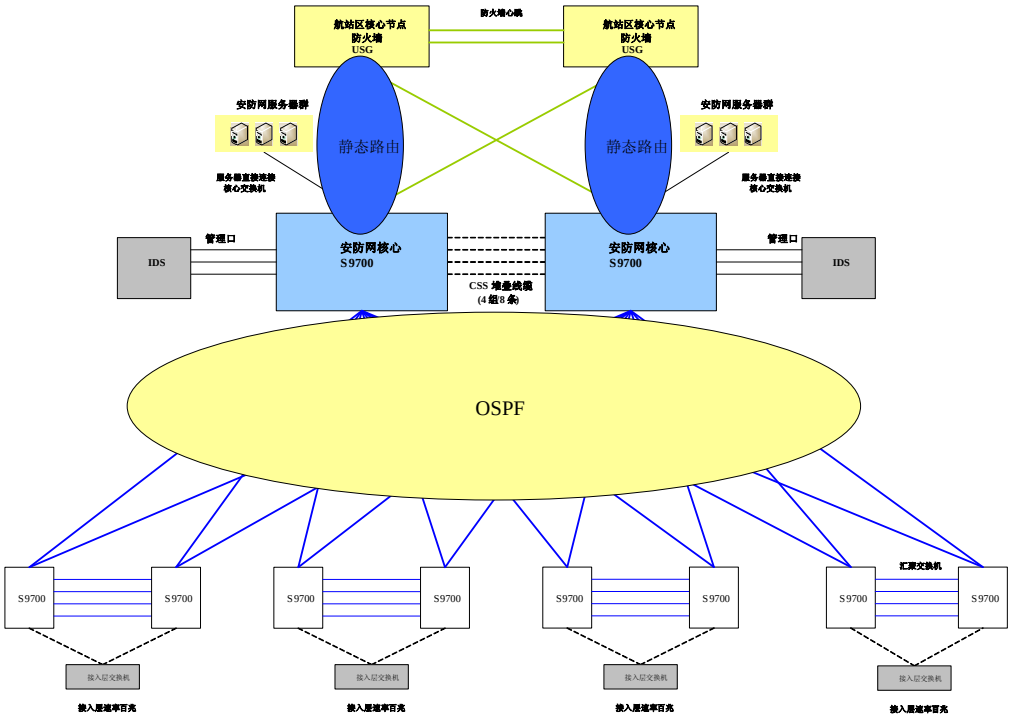
安防网内还有门禁管理系统，门禁系统除了后台服务器与区域控制器间的通信使用的是IP网络协议与一般的RJ45通信接口外。区域控制器与读卡器模块间通讯使用的是RS485串列口与RS485专用缆线。读卡器模块与读卡器间使用专用线路连接（非网络线连接）。

安防网内还有外接道路监控系统。道路监控系统使用EPON汇聚交换机连接外点的监控设像头，EPON汇聚交换机在上连到安防网核心交换机。

5.2 安防网路由需求

从网络规模来看，安防网内虽有为数众多的监控摄像头数量及门禁系统读卡器，但应用内容架构单一，无特殊性能要求，与信息网一样属于中型网络，推荐使用OSPF路由协议作为安防网路由协议。安防网与航站楼节点防火墙之间采用静态路由。安防网的路由设计如图 5-2 所示。

图5-2 安防网的路由设计



5.3 安防网承载的各业务系统（或子网）需求描述

5.3.1 安防视频监控系统需求

安防视频监控系统业务描述

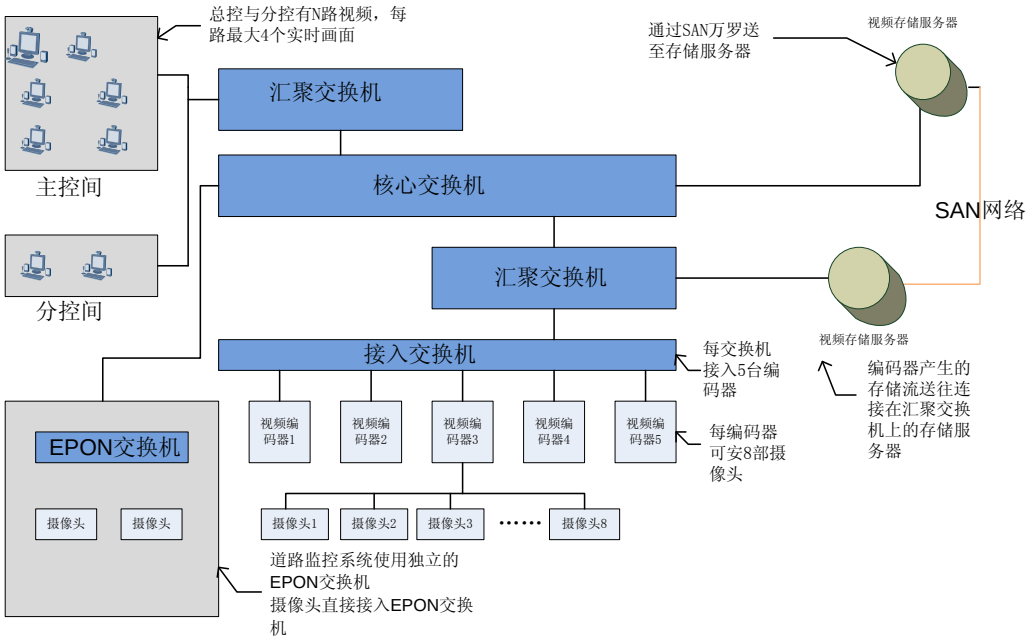
安防视频系统主要是视频监控类业务应用，实现安防视频流的采集、存储和管理。

安防视频监控系统技术架构示意图

安防视频系统由摄像头、视频编码器、视频存储服务器、安防系统服务器、管理服务器和监控屏幕及天网道路监控系统所组成。安防视频监控系统技术架构如图 5-3 所示。

道路监控系统采用独立 EPON 交换机连接航站楼周边摄像机，EPON 汇聚交换机连接到安防网核心交换机。

图5-3 安防视频监控系统技术架构示意图



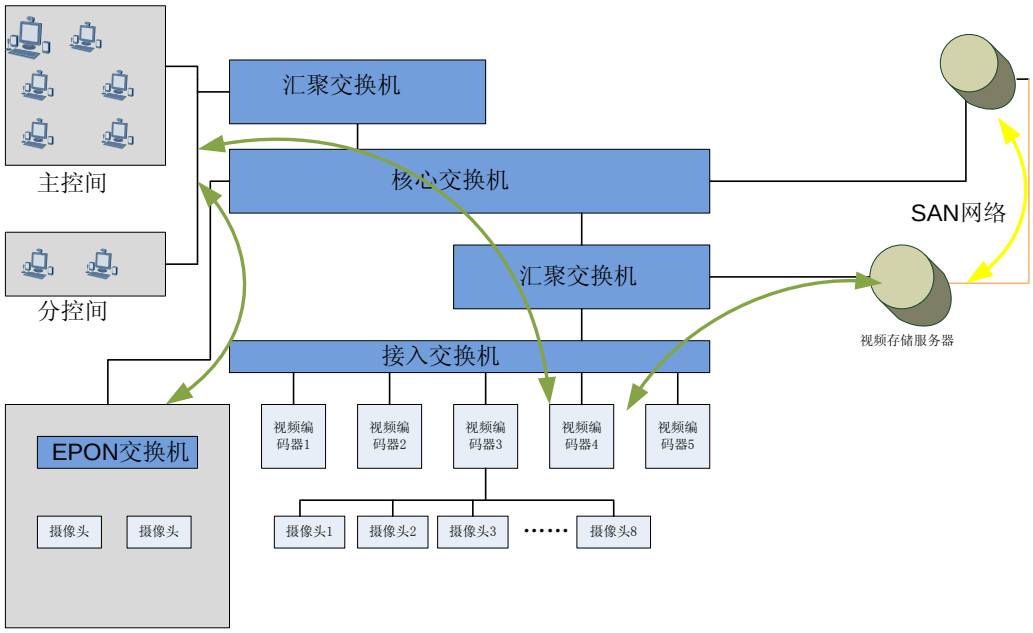
安防视频监控系统数据流向分析

安防视频监控存在以下 3 类视频数据流向。

- 各个视频前端采集设备产生的，以组播（Multicast）方式送往视频存储服务器的数据流；
- 各个视频前端采集设备产生的，也是以组播方式送往监控大屏以及远程调度终端的实时数据流；
- 视频存储服务器通过 SAN 存储网将视频历史数据传送至存储媒介的数据流。SAN 数据流由独立的 SAN 网络承载。

以上三个数据流与安防视频监控系统架构对应关系如图所示。

图5-4 视频系统数据流与安防视频监控系统对应关系图



安防视频监控系统数据流量分析

安防视频监控系统主要有以下两类视频流。

- 各个视频前端采集设备产生的，送往视频存储服务器的数据流。存储流采用 4CIF 格式，峰值流量约 3.7Mbit/s，中间值约 2Mbit/s；

  视频存储数据里是稳定存在于网络中的，视频存储服务器部署在各个汇聚设备层。
- 各个视频前端采集设备产生的，送往监控大屏幕以及远程调度终端的实时数据流，实时数据流采用 4CIF 格式，峰值流量约 3.7Mbit/s，中间值约 2Mbit/s。

  安防网设置有安全监控中心、航站楼管理中心、指挥中心和 IT 操作中心。在汇聚层设置有登机桥分控中心、消防控制中心、安检分控中心和总控中心。各中心分别有不等数量的显示大屏。

示例如下：

假设某一区域连接末端摄像头最多的汇聚层下连 500 路摄像头，每台交换机下连不超过 5 台视频编码器、每编码器连接 8 路摄像头，则：

- 每台视频编码器加载 8 台摄像头，这样每台视频编码器总峰值流量即为 8 * 3.7Mbit/s = 29.6Mbit/s；
- 每台接入交换机连接不超过 5 台视频编码器，则每台接入交换机最大峰值流量为 5 * 29.6Mbit/s ≈ 150Mbit/s;
- 500 台摄像头，则总存储视频流峰值为：500 * 3.7Mbit/s ≈ 1850Mbit/s；

因此安防网汇聚-接入带宽需要大于 1.85Gbps。

实时视频流流量分析

安防网设置有安全监控中心、航站楼管理中心、指挥中心和 IT 操作中心。在汇聚层设置有登机桥分控中心、消防控制中心、安检分控中心和总控中心。各中心分别有不等数量的显示大屏。

示例如下：

每块屏幕最大可以同时显示 4 路实时视频流。另外有一定数量 N（根据实际情况定）的远程调度终端，需要远程调用摄像头实时视频流，但是远程调度终端的接入位置不确定，我们假定都是来自安防网核心。

- 分控中心：各分控中心部署在不同的汇聚层假定为 Y 块大屏，实时视频流峰值流量=Y * 4 * 3.7Mbit/s；
- 总控中心：假定有 X 块大屏，则实时视频流峰值流量=X * 4 * 3.7Mbit/s；
- 远程调度终端实时视频流峰值流量=N * 3.7Mbit/s；

综述综合目前的网络设计，以及上述计算结果。

- 网络核心层交换机最大需要处理的流量主要就是总控中心、分控中心的实时视频流和远程调度终端的实时视频流≈X*4*3.7Mbps+N*3.7Mbps；
- 汇聚层交换机最大需要处理的流量主要包括该汇聚区域视频存储流和分控中心实时视频流≈Y*4*3.7Mbps+1850Mbps；

在带宽设计方面，安防网核心层和汇聚层需要满足上述核心层、汇聚层峰值流量需求。

安防视频监控系统应用服务端口表

在详细设计阶段，将需要系统供应商提供应用服务访问端口表，以在网络实施时部署准确的应用服务访问控制，提高应用服务的安全性。以下表格为示例样表。

服务端口描述	地址	协议（TCP/UDP）	端口范围	访问控制需求
XX 系统接口	n.n.n.n	TCP	1521	允许 x.x.x.x 和 y.y.y.y

安防视频监控系统外联接口需求列表

安检信息网远程调度终端需要访问安防网，安检信息网终端来直接远程调用安防网的视频数据。因此安防视频系统无系统外联接口需求。

安防视频监控系统内服务器节点部署需求列表

示例如表 5-1 所示。

表5-1 安防视频监控系统内服务器节点部署需求列表

服务器名称	用途	数量	部署位置	接口需求
安防系统服务器				100M 以上
天网系统服务器				100M 以上

服务器名称	用途	数量	部署位置	接口需求
集成管理服务器				100M 以上
视频存储服务器				1000M

安防视频监控系统内部终端/工作站节点布置需求列表

示例如表 5-2 所示。

表5-2 安防视频监控系统内部终端/工作站节点布置需求列表

终端/工作站	接入交换机	数量	部署位置	接口需求
视频编码器				100M 以上

5.3.2 门禁系统需求

门禁系统业务描述

门禁系统用于航站楼内门禁系统的管理。

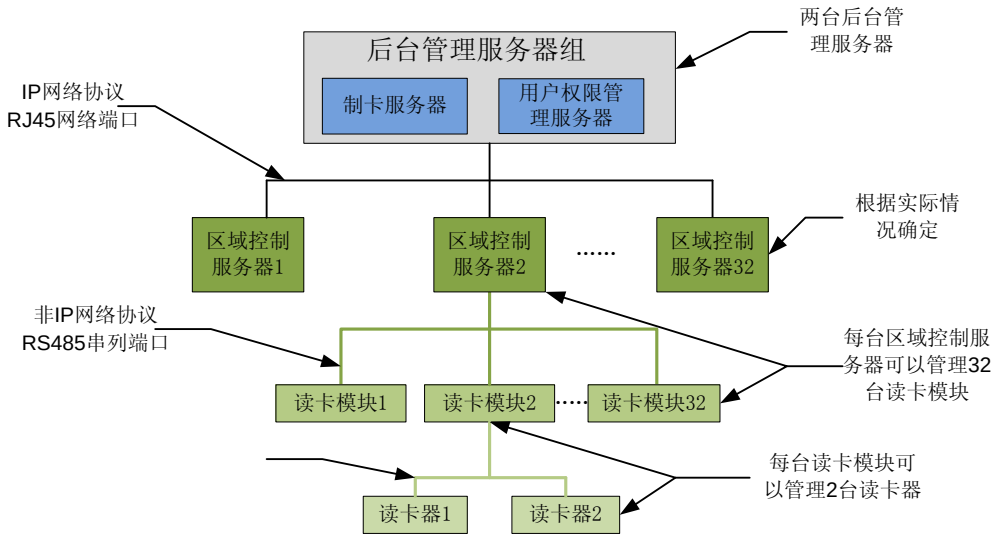
门禁系统技术架构示意图

门禁系统是由后台管理服务器、区域控制器、读卡器模块与读卡器等几部分组件所构成。其中，后台服务器与区域控制器间使用的是 IP 网络协议与一般的 RJ45 通信接口，区域控制器与读卡器模块间使用的是 RS485 串列口与 RS485 专用缆线，读卡器模块与读卡器间使用专用线连接。

以图 5-5 的部署为例说明门禁系统的架构。门禁系统后台部署有二台服务器。一台是系统管理服务器，用于用户权限管理，另一台为制卡服务器。每台区域控制器控制 32 个读卡器模块，每个读卡器模块带 2 个读卡器。

门禁系统配置有实时管理终端用于系统管理。区域控制数量根据实际情况确定。

图5-5 门禁系统架构示意图



门禁系统数据流向分析

- 当读卡器读取 IC 卡的用户信息后，通过专用连接线由读卡模块将信息传送至区域控制服务器。从门禁系统的区域控制服务器的记录中查找用户相应的权限，并根据查询结果执行对应的开关操作；
- 区域控制器通过网络线路，从后台服务器更新及获取用户数据库；
- 区域控制器内缓存的用户数据不会因为掉电丢失。因此，通常区域控制器的工作不依赖于后台服务器，可以独立工作。

门禁系统数据流量分析

门禁应用为 CS 架构且应用架构单纯，此外授权相关数据非实时传送，只在当有人员读卡以及人员授权内容更动时才有网络流量产生，因此门禁应用流量很小。

门禁系统应用服务端口表

在详细设计阶段，将需要系统供应商提供应用服务访问端口表，以在网络实施时部署准确的应用服务访问控制，提高应用服务的安全性。以下表格为示例样表。

服务端口描述	地址	协议（TCP/UDP）	端口范围	访问控制需求
XX 系统接口	n.n.n.n	TCP	1521	允许 x.x.x.x 和 y.y.y.y

门禁系统外联接口需求列表

根据目前系统调研分析暂无要求，若有其它要求提出会进一步补充。

门禁系统内服务器节点部署需求列表

示例如表 5-3 所示。

表5-3 门禁系统内服务器节点部署需求列表

服务器名称	用途	数量	部署位置	接口需求
制卡服务器				100M 以上
系统管理服务器				100M 以上

门禁系统内部终端/工作站节点布置需求列表

示例如表 5-4 所示。

表5-4 门禁系统内部终端/工作站节点布置需求列表

终端/工作站	接入交换机	数量	部署位置	接口需求
区域控制器				100M 以上
管理终端				

5.4 安防网网络吞吐量需求

根据实际情况确定。

5.5 安防网网络性能需求

考虑安防网络中的安防视频监控系统与门禁系统的性能要求，对网络架构有以下需求。

- 安防视频系统

  服务器 1000M 接入，终端视频编码器 100M 接入，接入交换机使用 1000M 上行接至汇聚交换机。汇聚交换机可以使用 CSS 技术捆绑多条 10G（根据实际情况确定链路数量）上行至核心交换机。

- 门禁系统

  门禁系统因应用流量小，使用与安防视频系统同样的网络架构，在流量方面也可以满足业务需求。

5.6 安防网网络广播控制需求

安防视频监控系统广播控制需求

安防网网络内安防视频监控系统由于摄像头分布范围广、数量较大，且无在同一 VLAN 的特别需求。从广播域来看，根据不同接入区域，适当地划分摄像头接入 VLAN，可以将广播域控制在合理范围内。

门禁系统广播控制需求

为了便于管理，门禁系统后台服务器与区域服务控制器需要在同一网段（VLAN）。

5.7 安防网网络安全需求

安防网安全边界如图 5-6 所示，包括外部安全边界和内部安全边界。

红色部分为外部安全边界，包括安防网与航站楼其它网络，以及与航站楼节点外的其它节点网络（例如物流园区网络、办公区网络等）的边界。

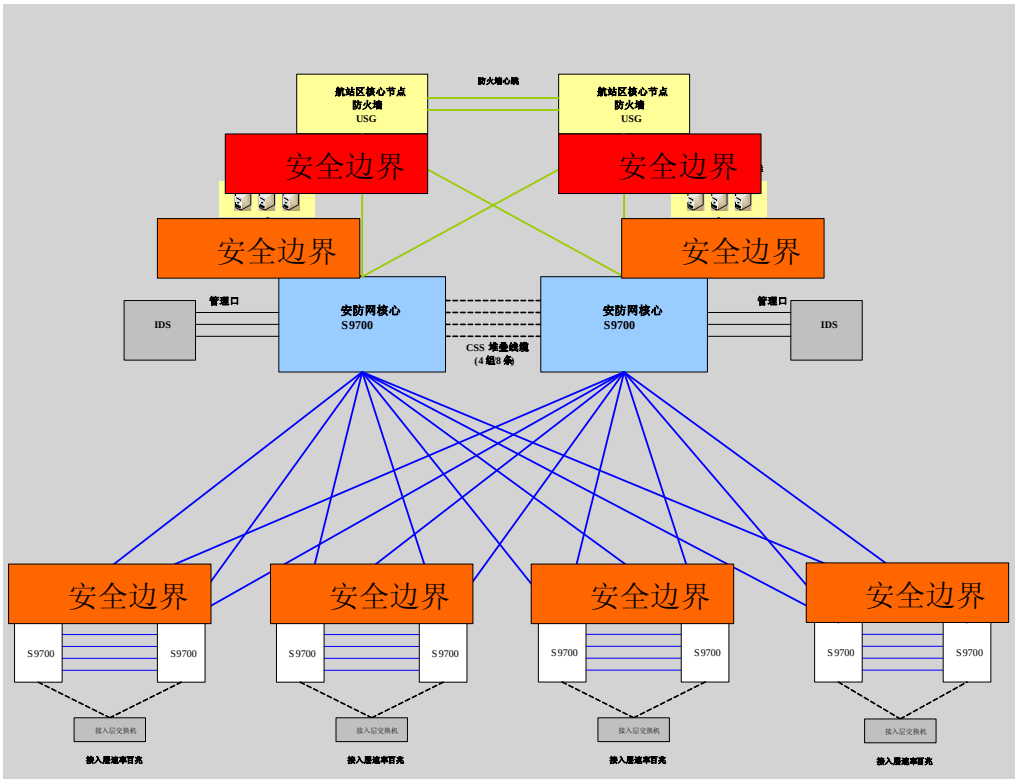
橙色部分为内部安全边界，包括以下几方面。

- 安防网内服务器接入网络的安全边界；
- 安防网内客户端接入网络的安全边界。

针对内部安全边界，需要部署适当的网络安全技术，提供访问安全保护，包括：

- 在核心交换机部署 IDS 设备，检测网络访问安全事件；
- 在客户端，通过防病毒系统（SEP），提供客户端自身的防病毒能力，以提高客户端的系统安全性。

图5-6 安防网安全边界



5.8 安防网网络 QOS 需求

首先，从技术应用角度来看，只有在网络出现拥塞的情况下，才需要部署 QoS，以对业务应用进行分类，并保障关键业务优先使用网络资源。而信息网承载的业务应用，都是基于 TCP/IP 的数据类应用，各业务系统的数据流量都不大，使用本方案推荐 S9700/7700/5700 系列交换机可以满足需求。

另外，安防网内主要以安防视频监控信息流为主要的网络应用与流量，视频监控信息数据使用的是组播（Multicast）协议传送相关视频数据。局域网环境内，将连接组播来源与目地的交换机端口启用 IGMP 协议以优化组播包传递效率。

综上所述，安防网不需要部署 QoS。

5.9 安防网网络管理需求

在航站楼网络节点核心集中部署网络管理系统，用于网络拓扑、网络设备等的集中管理，因此，需要安防网网络设备具备以下能力。

- 支持 SNMP 功能；
- 支持设定网管系统定义的 SNMP read community 和 SNMP write community；
- 支持将系统时钟（NTP）服务器指定为网络统一的 NTP 时钟源。

说明

考虑到配置的小型机服务器以及数据库等的管理需求，需要配置带外管理交换机，在详细设计阶段需要考虑。

6 安检网网络需求

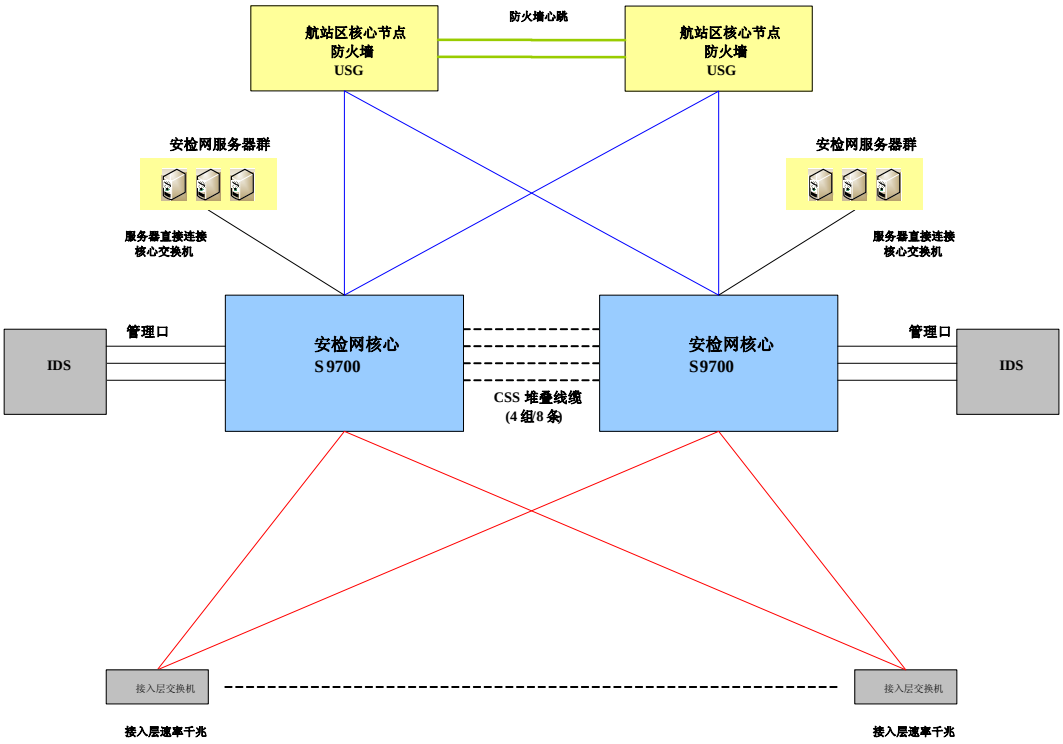
6.1 安检网架构需求

安检网是为安检系统提供网络接入的平台。安检网承载的业务系统有集中安检系统和手提行李安检系统。

安检网采用千兆以太网技术，网络结构采用核心、接入二层网络设计。核心层采用 S9700/7700 系列交换机组成，部署在信息系统主机房，主要负责系统后台服务器接入。接入层交换机通过两路千兆以太链路与核心交换机连接。其中核心层设备采用虚拟化技术，构成一个整合的逻辑实体，简化网络 L2 的设计。

除此之外，手提行李终端和服务器要求在一个网段内，集中安检系统终端和服务器要求在一个网段内，安检网需要部署 IDS 设备。

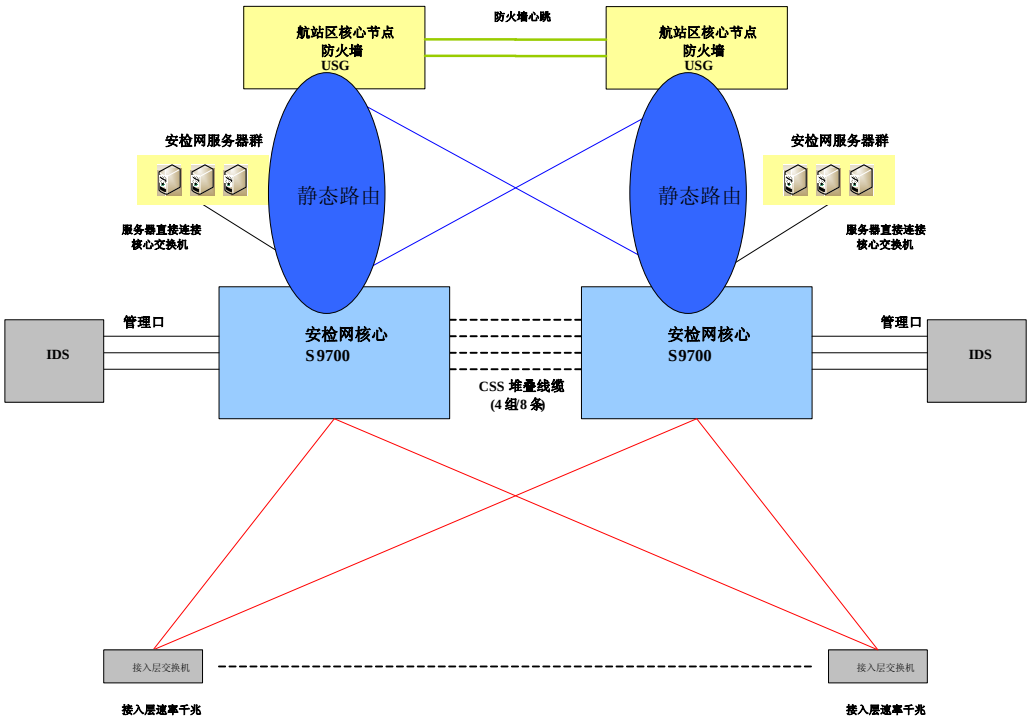
图6-1 安检网拓扑示意图：



6.2 安检网路由需求

安检网由于只有核心--接入两层架构，建议安检网为纯 L2 架构网络。由静态路由完成安检网与航站楼节点间的互连互通。安检网路由设计如图 6-2 所示。

图6-2 安检网的路由设计



6.3 安检网承载的各业务系统（或子网）需求描述

6.3.1 集中安检系统需求

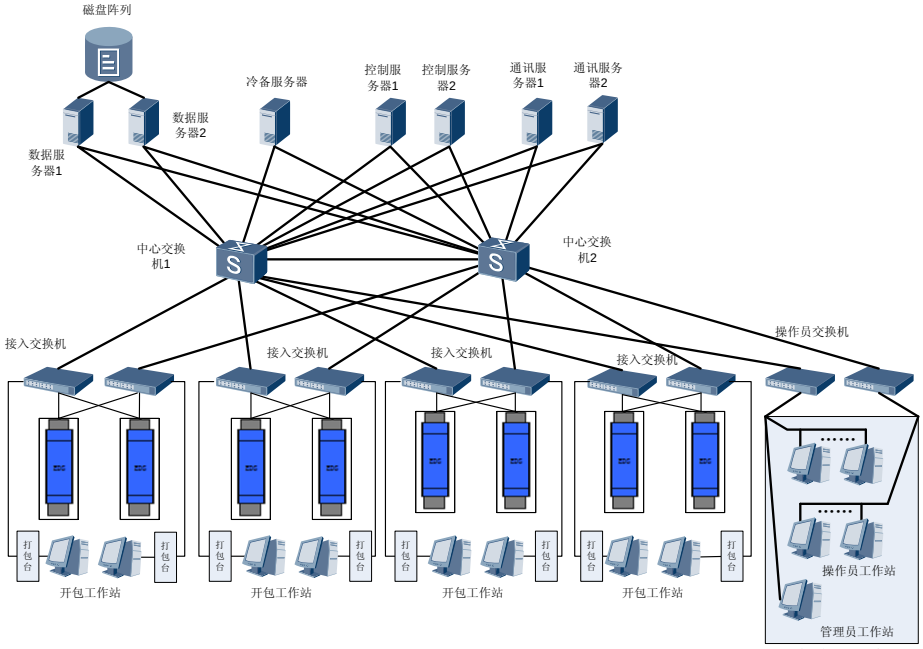
集中安检系统业务描述

集中安检系统用于旅客托运行李的安全检查。

集中安检系统技术架构示意图

航站楼的集中安检系统将 X 射线机、安检操作员工作站、开包工作站、管理员工作站、数据库服务器等服务器、终端、网络设备组成一个完整、独立的系统，为旅客托运行李提供集中安检服务。集中安检的系统架构如图 6-3 所示。

图6-3 集中安检系统的系统架构



集中安检系统中的服务器包括数据服务器、域控制服务器和通讯服务器。

- 数据服务器通过光纤通道共享存储磁盘柜，用于保存旅客、设备信息及相关管理信息，并提供数据库服务。数据服务器还用来存储出发值机柜台所采集的旅客交运行李图像文件，也用来保存系统中所有工作站的工作状态、X 射线机设备状态、网络设备初始化数据等内容。另外，数据库服务器同时还保存着工作人员记录表，授予不同操作人员对系统的访问权限，以实现对工作人员的工作状态查询和安检人员的权限管理。
- 域控制服务器用来管理整个网络的用户和计算机权限分配，同时用来作为系统的冷备服务器。
- 通讯服务器用来实现与离港系统、安检信息管理系统、行李处理系统、地面信息系统和时钟系统之间的接口。

集中安检系统还包括 X 射线检查设备，放置于值机岛，每岛需要两台，用于托运行李的集中安检。每台 X 射线检查设备需布线系统提供 4 个信息点（其中 1 个点作为备份）。X 射线检查设备还需要 3 个网络设备端口，其中 2 个端口用于数据接入（分别连接到 2 台不同的接入交换机），另一个端口用于 PLC 远程开关机。

集中安检系统需要在集中控制室部署安检操作员工作站和管理员工作站。在值机岛岛头部署开包台工作站。

在系统安全方面，系统内部是一个逻辑独立局域网，系统内部工作站和服务器的光驱和 USB 端口都被封锁，防止外部介质进入系统。系统内的工作站和服务器对人员的访问权限进行管理，防止非授权人员对信息资源的非法访问。系统内的网络设备需进行安全设置，网络设备的每个端口都需要管理员开通后才能接入使用，限制外系统点引入。与系统外部通过通讯服务器与外部系统通讯。通讯服务器设置了严格的用户访问权限，以保证系统内的数据不被损坏、丢失。

集中安检系统数据流向分析

系统中工作站之间、工作站和数据库服务器之间都会有图像及数据传送。

集中安检系统数据流量分析

集中安检系统在终端与服务器之间的主要流量为 X 光机与服务器之间的图像传输，以及开包工作站与服务器之间的图像传输，以下分别对这 2 类数据流流量进行理论计算分析。

- X 光机上传流量

  X 光机在集中安检系统业务过程中，需要传送静态图像。

流量计算示例如下，在图像传送过程中，假设同时并发 12 台 EDS-MV10080 设备同时采集图像，每 2 秒钟采集一件行李图像，EDS-MV10080 每件行李存储 3 个视角图像，每幅图像平均 800KB，则核心层和汇聚层网络最大流量分别如下。

  - 核心层网络最大流量

    （12*3）*8000KByte/2s = 14400KByte/s = 14400*8Kbit/s = 115200kbit/s = 115200/1024Mbit/s = 112.5Mbit/s = 112.5/8MByte/s = 14.06MByte/s

  - 汇聚层网络最大流量

    6*3*800KByte/2s = 7200KByte/s = 7200*8kbit/s = 57600kbit/s = 57600/1024Mbit/s = 56.25Mbit/s = 56.25/8MByte/s = 7.03MByte/s

- 开包工作站上传流量：

  旅客行李开包检查时，需要将开检图像由操作员工作站回送到开包员工作站.

  流量计算示例如下，依据每幅图像 800KB 计算，回送开包员工作站图像流量与上传图像数据量相等。计算公式如下。

  6*3*800KByte/2s = 7200KByte/s = 7200*8kbit/s = 57600kbit/s = 57600/1024Mbit/s = 56.25Mbit/s = 56.25/8MByte/s = 7.03MByte/s

  总流量应为 56.25Mbit/s*2＝112.5Mbit/s

  安检系统的带宽设计满足 X 光机的接入流量和开包工作站的上行汇聚流量。

集中安检系统应用服务端口表

在详细设计阶段，将需要系统供应商提供如上述格式内容的应用服务访问端口表，以在网络实施时部署准确的应用服务访问控制，提高应用服务的安全性。

服务端口描述	地址	协议（TCP/UDP）	端口范围	访问控制需求
XX 系统接口	n.n.n.n	TCP	1521	允许 x.x.x.x 和 y.y.y.y

集中安检系统外联接口需求列表

集中安检与离港系统、安检信息管理系统、行李处理系统、地面信息系统和时钟系统之间有系统接口。

集中安检系统内服务器节点部署需求列表

示例如表 6-1 所示。

表6-1 集中安检系统内服务器节点布置需求列表

服务器名称	用途	数量	部署位置	接口需求
数据库服务器				1000M 以上
域控制器				
冷备服务器				
通讯服务器				

集中安检系统内部终端/工作站节点布置需求列表（示例样表）

示例如表 6-2 所示。

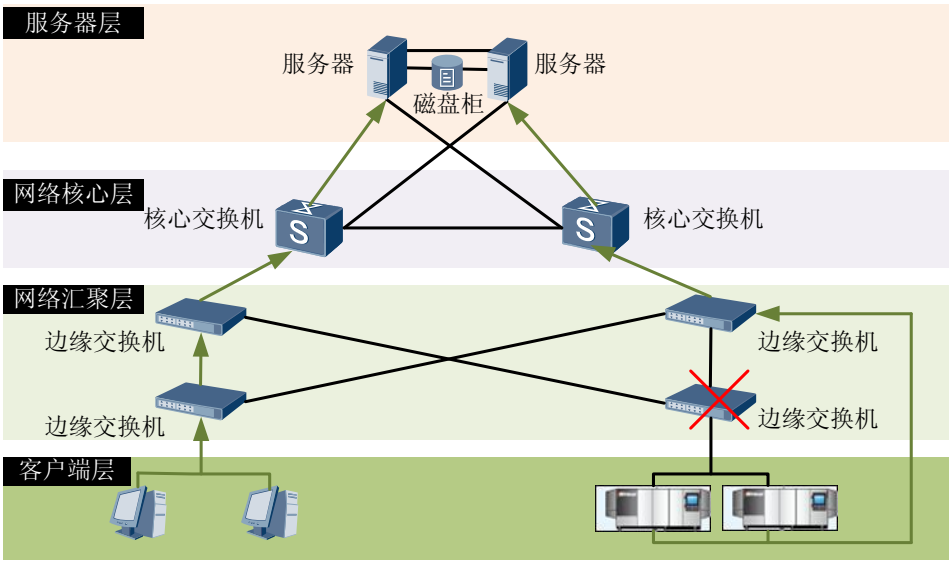
表6-2 集中安检系统内部终端/工作站节点布置需求列表

终端/工作站	接入交换机	数量	部署位置	接口需求
区域控制器				100M 以上
管理终端				

其它

根据用户需求，考虑到系统的稳定运行，集中安检 X 光机需要冗余的网络接入，即 X 光机的 2 个数据端口需要连接到 1 对冗余的堆叠交换机上，这样，在主用的接入交换机出现故障时，另外一台接入交换机可以继续为 X 光机提供网络接入。

图6-4 X 光机冗余接入组网示意图



6.3.2 手提行李安检系统需求

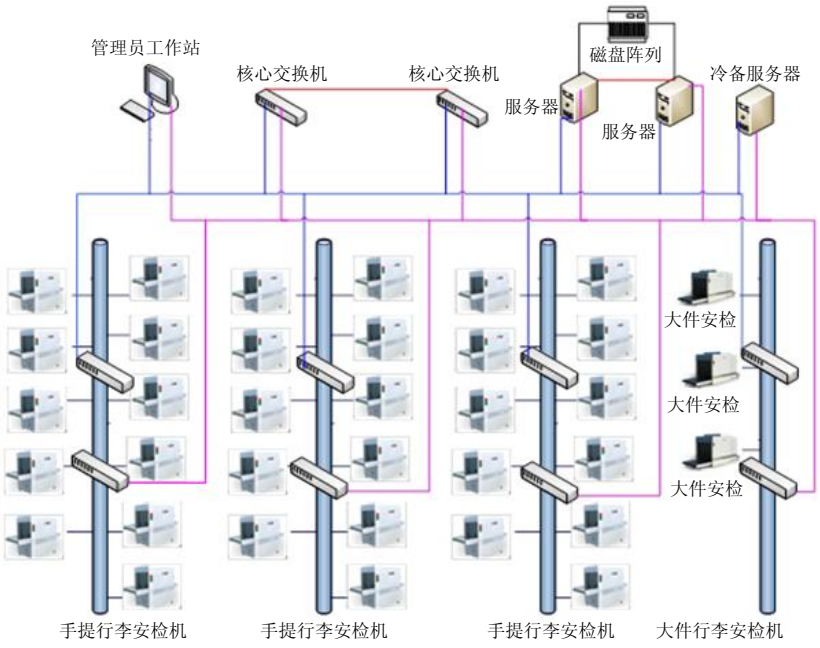
手提行李安检系统业务描述

手提行李安检系统是用于对旅客随身携带行李和超限行李进行安全检查的系统。

手提行李安检系统技术架构示意图

手提行李安检系统的架构如图 6-5 所示。

图6-5 手提行李安检系统的架构示意图



手提行李安检系统中，为确保所有手提行李和大件行李安检 X 光机能够与服务器建立可靠的、有冗余备份的网络连接，需要为每台 X 光机配备 2 个网络连接点，一个平时使用，另外一个作为备份，一旦网络出现故障，可将网线插入到备份网络连接点，以便快速恢复 X 光机与服务器之间的网络连接。

为满足机场平时安检需要、并能应对高峰时客流量的要求，需要确保上述网络带宽为千兆。

系统需部署双机热备的服务器组，用于业务应用访问。有一台冷备服务器作为备机，一台管理员工作站用于日常的系统管理维护。

X 光机设备配备有专用的终端，用于配合 X 光机工作，检查行李中是否有违反民航安全条例规定的、不允许携带的物品，该专用终端不连接网络，而是直接连 X 光机。

手提行李安检系统只允许与安检信息系统之间的应用系统接口互相访问，并与时钟系统通信，其它任何访问，都需要禁止。

手提行李安检系统数据流向分析

系统只允许与安检信息系统之间的应用系统接口互相访问，并与时钟系统通信，其它任何访问，都需要禁止。X 光机需要向服务器上传静态图像数据，并接收服务器下传的指令和信息。

手提行李安检系统数据流量分析

为满足机场平时安检需要、并能应对高峰时客流量的要求，需要确保上述网络带宽。根据经验，，终端 1000M 可以满足业务需求。

手提行李安检系统应用服务端口表

在详细设计阶段，将需要系统供应商提供如上述格式内容的应用服务访问端口表，以在网络实施时部署准确的应用服务访问控制，提高应用服务的安全性。

服务端口描述	地址	协议（TCP/UDP）	端口范围	访问控制需求
XX 系统接口	n.n.n.n	TCP	1521	允许 x.x.x.x 和 y.y.y.y

手提行李安检系统外联接口需求列表

手提行李安检系统与安检信息管理系统、时钟系统有系统接口。

手提行李安检系统内服务器节点部署需求列表

示例如表 6-3 所示。

表6-3 手提行李安检系统内服务器节点布置需求列表

服务器名称	用途	数量	部署位置	接口需求
服务器（热备）				1000M
冷备服务器				1000M

手提行李安检系统内部终端/工作站节点布置需求列表

示例如表 6-4 所示。

表6-4 门禁系统内部终端/工作站节点布置需求列表

终端/工作站	接入交换机	数量	部署位置	接口需求
手提行李 X 光机				1000M
大件行李 X 光机				1000M
管理终端				100M

6.4 安检网网络吞吐量需求

根据实际需求确定。

6.5 安检网网络性能需求

为满足机场平时安检需要、并能应对高峰时客流量的要求，需要确保上述网络带宽满足需求。根据经验，终端 1000M 可以满足业务需求。

6.6 安检网网络广播控制需求

由于手提行李安检和集中安检都要求其终端和服务器要求在一个网段内，因此安检网将是纯 L2 层架构网络。集中安检系统与手提行李安检系统分别配置不同的 VLAN，从系统终端数量来看，广播域处于较小的范围。

6.7 安检网网络安全需求

安检网的安全边界如图 6-6 所示，包括外部安全边界和内部安全边界两部分。

红色部分为外部安全边界，包括安检网与航站楼其它网络，安检网与航站楼节点外的其它网络（例如物流园区网络、办公区网络等）的边界。

针对上述安全边界，需要部署防火墙实施严格的网络隔离和控制，利用 ACL，控制网络间、系统间的系统访问，提高网络安全性。

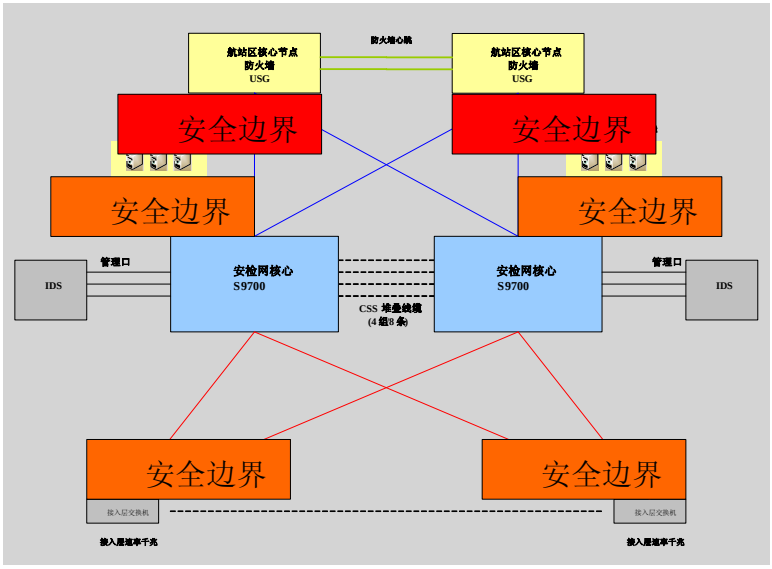
橙色部分为内部安全边界，包括以下两部分。

- 安检网内服务器接入网络的安全边界；
- 安检网内客户端接入网络的安全边界。

针对内部安全边界，需要部署适当的网络安全技术，提供访问安全保护，包括：

- 在核心交换机部署 IDS 设备，检测网络访问安全事件；
- 在客户端，通过防病毒系统（SEP），提供客户端自身的防病毒能力，以提高客户端的系统安全性。

图6-6 安检网安全边界



6.8 安检网网络 QOS 需求

从技术应用角度来看，只有在网络出现拥塞的情况下，才需要部署 QoS，以对业务应用进行分类，并保障关键业务优先使用网络资源。安检网承载的业务都是基于 TCP/IP 的数据类应用，各业务系统的数据流量都不大，采用本方案推荐配置的 S9700/7700/5700 系列交换机，安检网不需要部署 QoS。

6.9 安检网网络管理需求

在航站楼网络节点核心集中部署网络管理系统，用于网络拓扑、网络设备等的集中管理，因此，需要安检网网络设备具备以下能力。

- 支持 SNMP 功能；
- 支持设定网管系统定义的 SNMP read community 和 SNMP write community；
- 支持将系统时钟（NTP）服务器指定为网络统一的 NTP 时钟源。

说明

考虑到配置的小型机服务器以及数据库等的管理需求，需要配置带外管理交换机，在详细设计阶段需要考虑。

7 安检信息网网络需求

7.1 安检信息网架构需求

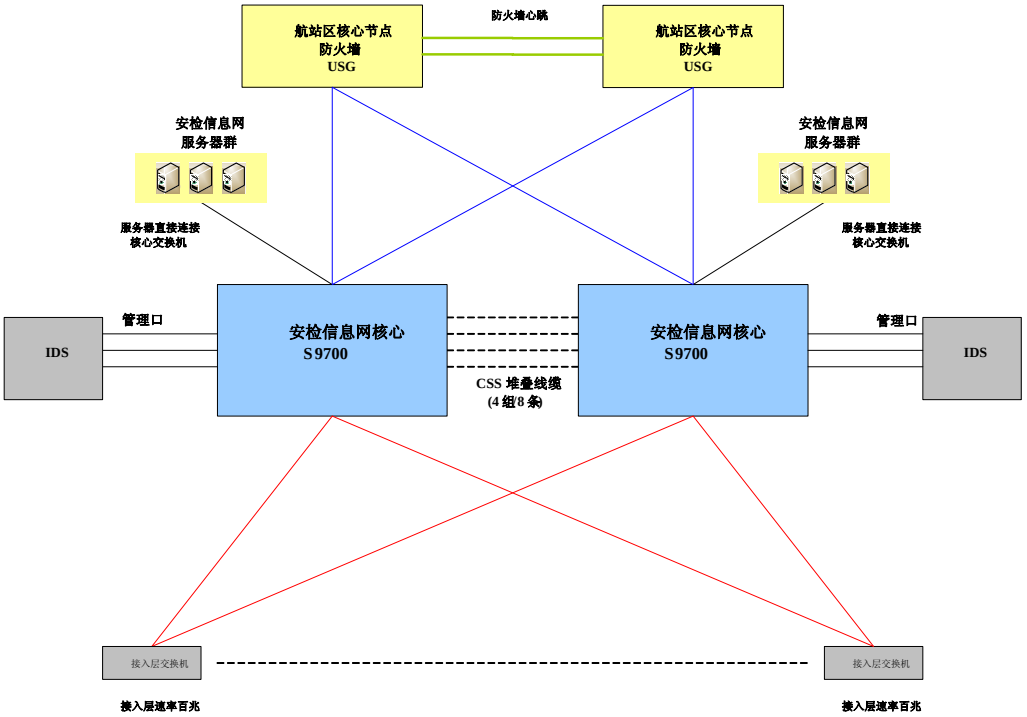
安检信息管理系统是集旅客身份验证、肖像采集、安检过程录像、行李 X 光照片采集、行李开包录像、安检人员管理和布控信息管理于一体的综合性安检信息管理系统。系统功能主要包括旅客值机信息获取、交运行李图像采集、旅客照片采集、布控、航空意外险检查和行李状态提示等。

安检信息管理系统由主服务器、接口服务器、管理工作站、阅读器和摄像头等设备组成。系统为 Client-Server 架构，因此需确保 Client 到 Server 间的网络传输性能可以满足应用执行要求。

安检信息网是为安检信息系统提供网络接入的平台。安检信息网采用千兆以太网技术，网络结构为核心、接入二层网络设计。核心层采用冗余交换机组成，主要负责系统后台服务器接入。接入层交换机通过以太链路与核心交换机连接，其中核心层设备采用虚拟化技术，构成一个整合的逻辑实体，简化网络 L2 的设计。

安检信息网中的服务器直接连接到核心交换机 S9700 上，此外，安检信息网需要部署 IDS 设备。安检信息网拓扑如图 7-1 所示。

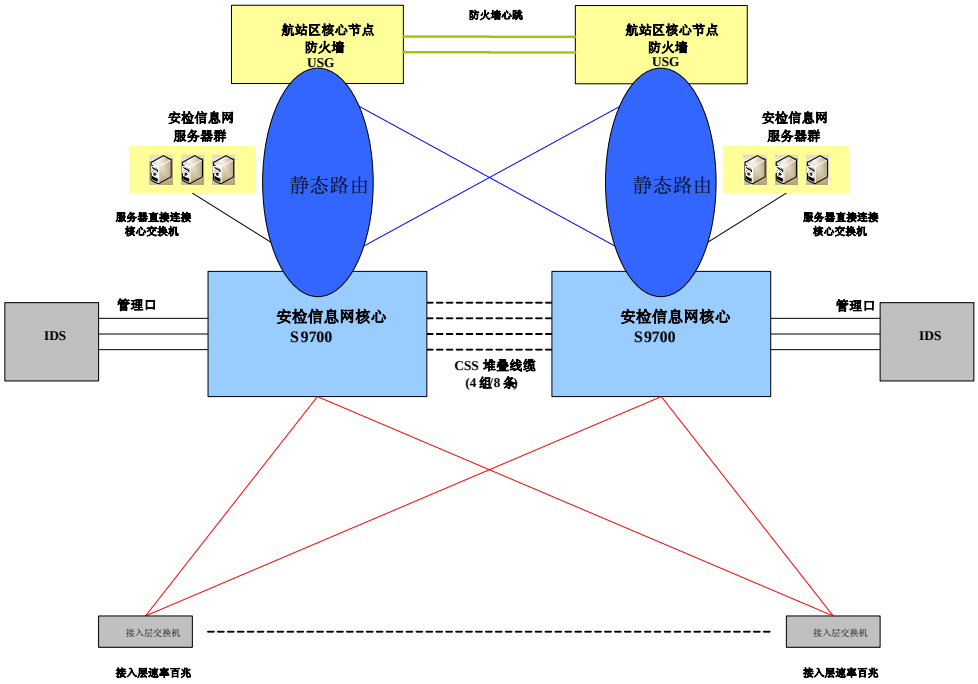
图7-1 安检信息网拓扑示意图



7.2 安检信息网路由需求

安检信息网由于只有核心--接入两层架构，建议安检信息网为纯 L2 架构网络，由静态路由完成安检信息网与航站楼节点间的互连互通。安检信息网路由架构如图 7-2 所示。

图7-2 安检信息网的路由设计



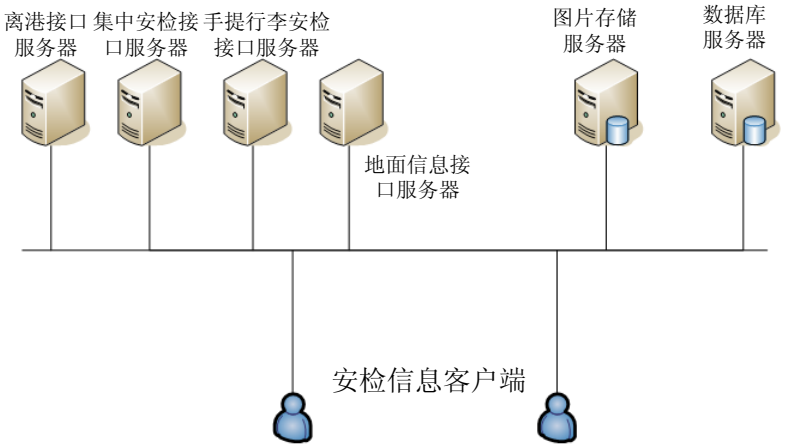
7.3 安检信息系统架构需求

安检信息系统业务描述

安检信息管理系统是集旅客身份验证、肖像采集、安检过程录像、行李 X 光照片采集、行李开包录像、安检人员管理和布控信息管理于一体的综合性安检信息管理系统。系统通过计算机网络，综合利用机场现有安全检查设施和信息资源，提高安检质量，规范安检管理，最大限度的确保民航空防安全。

安检信息系统的技术架构如图 7-3 所示。

图7-3 安检信息系统的技术架构



安检信息系统为 C/S 架构（服务器、客户端），系统包括 X 台系统服务器和 Y 台接口服务器。

- 数据库服务器用于存储、管理安检信息业务数据；
- 图片存储服务器用于存储、管理存储业务图像数据；
- 接口服务器包括以下几种。
  - 离港接口服务器
  - 集中安检接口服务器
  - 手提行李安检接口服务器
  - 地面信息系统接口服务器

安检信息系统数据流向分析

安检信息网终端之间需要进行点对点的消息传递。某些情况下，可能也需要在终端之间以广播形式发布消息通告。

开包台、安检通道、值班室终端在执行业务时，需要分别访问数据库服务器和图片存储服务器。

集中安检系统与安检信息系统之间的应用系统接口，通过网络实现。

安检信息网的某些用户终端需要访问安防网，进行安防视频录像的下载、回放等操作。

安检信息系统与安检网的手提行李系统的应用系统接口实现，可以采用如下的方案：

在手提行李安检服务器配置双网卡，分别配置不同的 IP 地址。其中一块网卡为安检信息网访问手提行李安检系统的网络访问接口，而另一块网卡则为安检网内手提行李系统内部终端访问系统服务器的网络接口。

安检信息系统数据流量分析

安检信息系统的数据流量需要参考机场服务器和终端的数量，同时综合机场的业务量来确定。

安检信息系统应用服务端口表

在详细设计阶段，将需要系统供应商提供如上述格式内容的应用服务访问端口表，以在网络实施时部署准确的应用服务访问控制，提高应用服务的安全性。

服务端口描述	地址	协议（TCP/UDP）	端口范围	访问控制需求
XX 系统接口	n.n.n.n	TCP	1521	允许 x.x.x.x 和 y.y.y.y

安检信息系统外联接口需求列表

安检信息系统与离港系统、地面信息系统和安检系统有应用系统接口。安检信息网的用户终端需要访问安防网，进行安防视频录像的下载、回放等操作。

安检信息系统内服务器节点部署需求列表

示例如表 7-1 所示。

表7-1 安检信息系统内服务器节点布置需求列表

服务器名称	用途	数量	部署位置	接口需求
数据库服务器				100M
接口服务器				100M

安检信息系统内部终端/工作站节点布置需求列表

示例如表 7-2 所示。

表7-2 安检信息系统内部终端/工作站节点布置需求列表

终端/工作站	接入交换机	数量	部署位置	接口需求
安检信息系统终端				100M

安检信息网网络吞吐量需求

根据具体需求确定。

7.4 安检信息网网络性能需求

安检信息系统无特殊具体流量需求，需要参考机场服务器和终端数量，同时综合机场的业务量来确定服务器接入和终端接入流量。

7.5 安检信息网网络广播控制需求

由于安检信息网架构为核心--接入两层架构，同时考虑服务器及各类终端总数量，建议考虑构建纯 L2 架构网络，一方面方便管理，另外广播范围适中，可以满足业务要求。

7.6 安检信息网网络安全需求

安检信息网的安全边界如图 7-4 所示，包括外部安全边界和内部安全边界两部分。

红色部分为外部安全边界，包括安检信息网与航站楼其它网络，以及与航站楼节点外的其它节点网络（例如物流园区网络、办公区网络等）的边界。

针对上述安全边界，需要部署防火墙实施严格的网络隔离和控制，利用 ACL，控制网络间、系统间的系统访问，提高网络安全性。

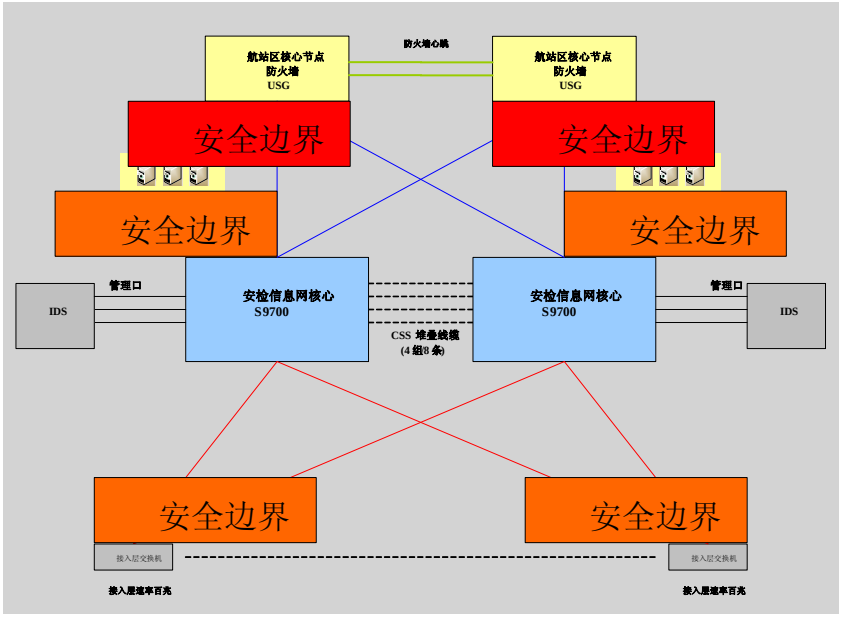
橙色部分为内部安全边界，包括以下两个部分。

- 安检信息网内服务器接入网络的安全边界。
- 安检信息网内客户端接入网络的安全边界。

针对内部安全边界，需要部署适当的网络安全技术，提供访问安全保护，包括：

- 在核心交换机部署 IDS 设备，检测网络访问安全事件；
- 在客户端通过防病毒系统，提供客户端的防病毒能力，以提高客户端的系统安全性。

图7-4 安检信息网的安全边界示意图



7.7 安检信息网网络 QOS 需求

从技术应用角度来看，只有在网络出现拥塞的情况下，才需要部署 QoS，以对业务应用进行分类，并保障关键业务优先使用网络资源。安检信息网承载的业务都是基于 TCP/IP 的数据类应用，各业务系统的数据流量都不大，采用本方案推荐的 S9700/7700/5700 系列交换机配置，安检信息网不需要部署 QoS。

7.8 安检信息网网络管理需求

在航站楼网络节点核心集中部署网络管理系统，用于网络拓扑、网络设备等的集中管理，因此，需要安检信息网网络设备具备以下能力。

- 支持 SNMP 功能；
- 支持设定网管系统定义的 SNMP read community 和 SNMP write community；
- 支持将系统时钟（NTP）服务器指定为网络统一的 NTP 时钟源。

说明

考虑到配置的小型机服务器以及数据库等的管理需求，需要配置带外管理交换机，在详细设计阶段需要考虑。

8 POS 网网络需求

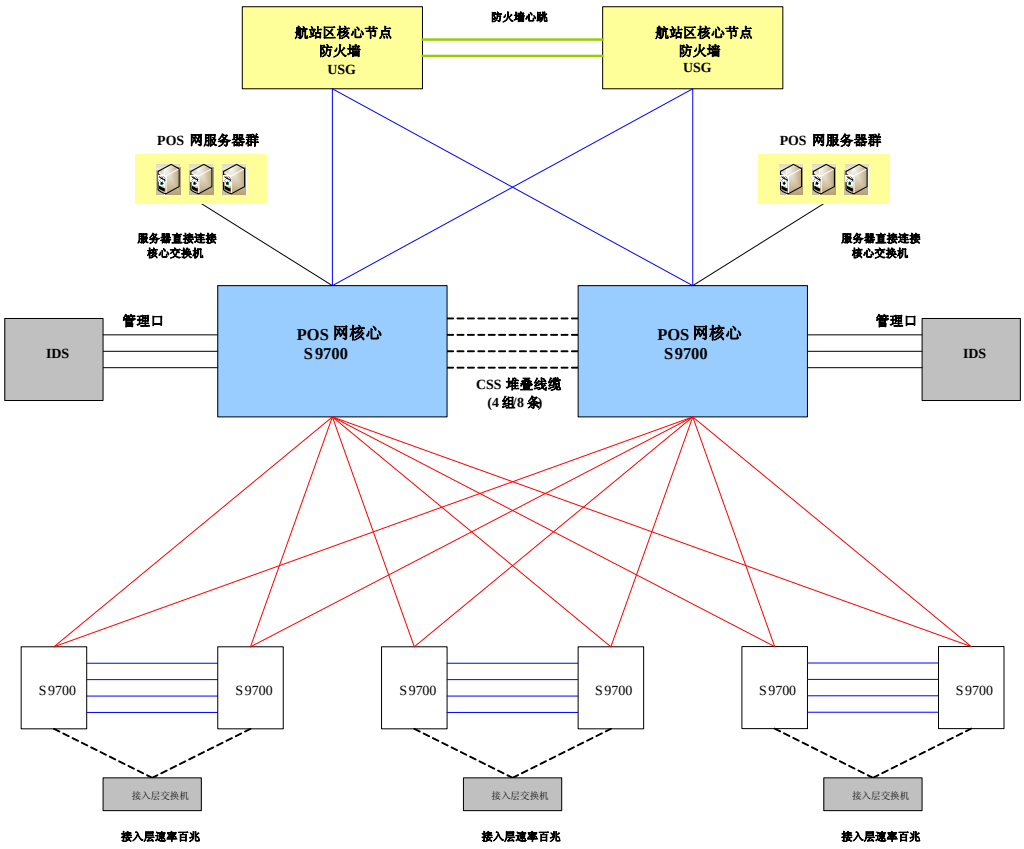
8.1 POS 网架构需求

航站楼 POS 网主要是为航站楼内各种业态的商业销售系统，提供 POS 系统接入的网络平台。

POS 网络结构为核心、汇聚、接入三层网络设计，其中核心层设备采用虚拟化技术，构成一个整合的逻辑实体，简化网络 L2 的设计。汇聚交换机只作为网络 L2 层使用，终端设备的网关全部放置在核心交换机上。

POS 网需要部署 IDS 设备。POS 网的网络拓扑如图 8-1 所示。

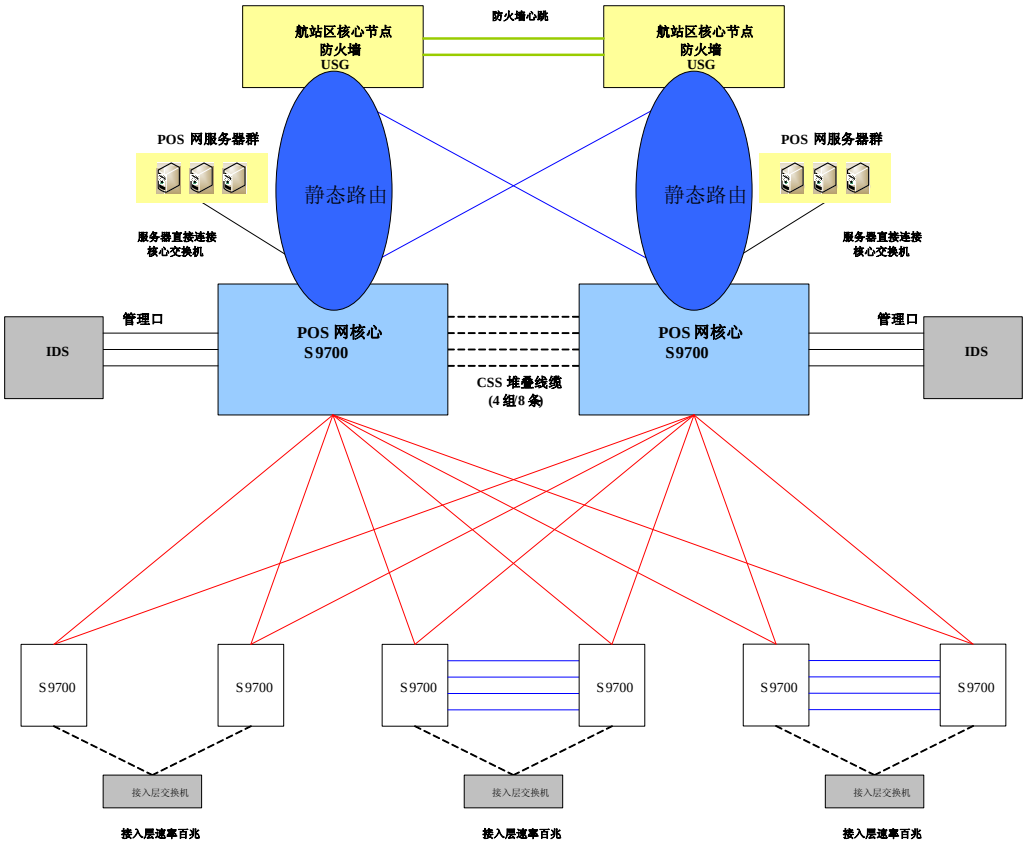
图8-1 POS 网的网络拓扑示意图



8.2 POS 网路由需求

POS 网推荐使用 L2 架构网络，在核心交换机部署静态路由，实现 POS 网与航站楼节点的互连互通。POS 网的路由设计如图 8-2 所示。

图8-2 POS 网路由设计



8.3 POS 网系统需求

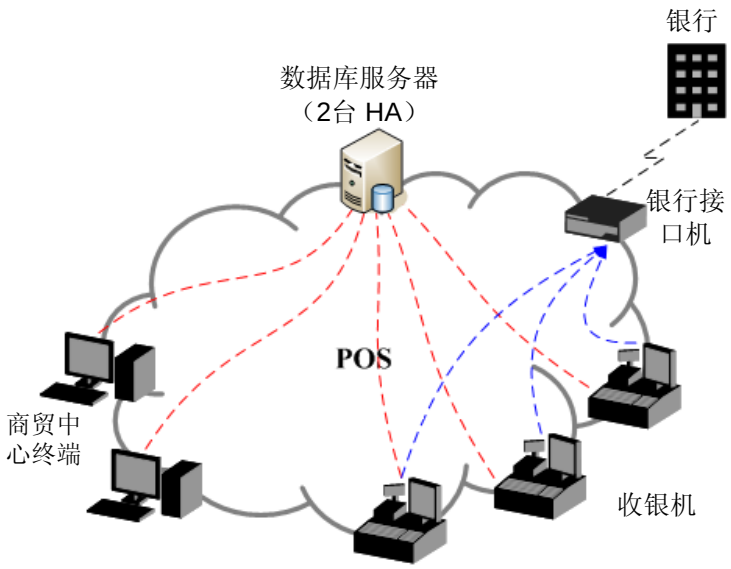
POS 系统业务描述

POS 系统部署了其他厂商的系统软件，主要包括“销售终端”、“系统管理”、“合同管理”、“物价管理”、“进货管理”、“库存管理”、“销售管理”、“结算管理”等多个子系统。系统涉及了商场的进、销、调、存等多项业务环节，监控、管理商场的商务活动。

POS 系统技术架构示意图

POS 系统后台部署数据库服务器用于数据的存储和管理，部署 FTP 服务器用于软件更新。前台收银机部署 POS 软件，用于收银业务处理。机场商贸中心有多台管理终端部署 ERP 软件，用于销售分析、供应商结算等功能。在 POS 网部署有银行接口机（设备由银行提供和管理），用于与有银行的系统接口。POS 系统的架构如图 8-3 所示。

图8-3 POS 系统架构示意图



POS 系统数据流向分析

业务流程上看，主要的业务交易数据流有 3 类，从系统商的经验来看，数据流可能有以下几种。

- 现金交易

  前端交易结算方式为付现。收银员收取现金后，通过收银机的软件界面完成商品销售的交易记录，并交付到后台数据库。

- 刷卡交易（无银行联动）

  前端交易结算方式为刷卡，但是由收银员手工分别完成银行刷卡交易和收银机的业务处理交易。

- 刷卡交易（银行联动）

  前端交易结算方式为刷卡，收银员在业务处理过程中，部署在收银机上的 POS 软件会自动调用银行收银系统接口，在刷卡交易完成后，再完成系统的业务处理交易。

POS 系统数据流量分析

从建设经验来看，终端 100M 接入，可以满足业务需求。

POS 系统应用服务端口表

TCP 1521 和 TCP 21（FTP）端口需求已经明确，但是 IP 地址尚未确定, 在详细设计阶段将参照如下表格制定明确的应用服务端口表。

服务端口描述	地址	协议（TCP/UDP）	端口范围	访问控制需求
XX 系统接口	n.n.n.n	TCP	1521	允许 x.x.x.x 和 y.y.y.y

POS 系统外联接口需求列表

软件系统需要与航站楼内部分商户（例如 KFC）的系统有系统接口。

POS 系统内服务器节点部署需求列表

示例如表 8-1 所示。

表8-1 POS 系统内服务器节点布置需求列表

服务器名称	用途	数量	部署位置	接口需求
数据库服务器				100M
FTP 服务器				100M

POS 系统内部终端/工作站节点布置需求列表

示例如表 8-2 所示。

表8-2 POS 系统内部终端/工作站节点布置需求列表

终端/工作站	接入交换机	数量	部署位置	接口需求
POS 机				100M
商贸中心用户终端				100M

8.4 POS 网网络吞吐量需求

根据具体需求确定。

8.5 POS 网网络性能需求

根据具体需求确定。

8.6 POS 网网络广播控制需求

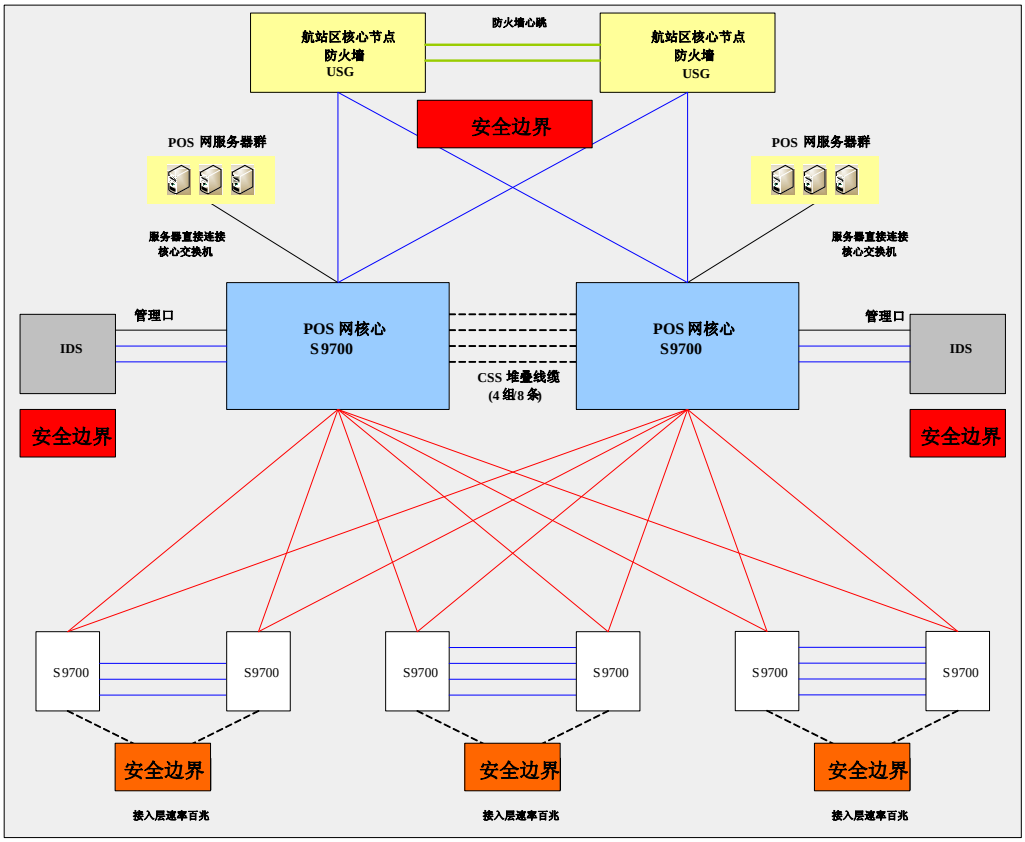
POS 网由于业务单一，终端类型和数量都不多，可能只有收银机和刷卡机 2 类。可以将服务器和前端设备划分到同一个 VLAN，既能简化维护管理，也可以使 VLAN 广播域处于适当的程度。

8.7 POS 网网络安全需求

POS 网安全边界如图 8-4 所示，包括外部边界安全和内部边界安全。

- 红色部分为外部安全边界（以航站楼网络为基准），包括航站楼 POS 网络与航站楼其它网络之间的安全边界。针对外部安全边界，需要部署防火墙实施严格的网络隔离和控制，利用 ACL，控制网络间、系统间的系统访问，提高网络安全性。
- 橙色部分为内部安全边界，包括服务器接入的安全边界和客户端接入的安全边界。
  - POS 网服务器接入的安全边界，该边界部署 IDS 设备，检测网络访问安全事件。
  - POS 网网络边缘，客户端接入的安全边界。在客户端，通过防病毒系统（SEP），提供客户端自身的防病毒能力，以提高客户端的系统安全性。

图8-4 POS 网的安全边界



8.8 POS 网网络 QOS 需求

从技术应用角度来看，只有在网络出现拥塞的情况下，才需要部署 QoS，以对业务应用进行分类，并保障关键业务优先使用网络资源。而 POS 网承载的业务应用只有 POS 系统应用，并且是基于 TCP/IP 的数据类应用，系统的数据流量不大，采用本方案推荐的 Sx7 系列交换机配置，POS 网不需要部署 QoS。

8.9 POS 网网络管理需求

在航站楼网络节点核心集中部署网络管理系统，用于网络拓扑、网络设备等的集中管理，因此，需要 POS 网网络设备具备以下能力。

- 支持 SNMP 功能；
- 支持设定网管系统定义的 SNMP read community 和 SNMP write community；
- 支持将系统时钟（NTP）服务器指定为网络统一的 NTP 时钟源。

说明

考虑到配置的小型机服务器以及数据库等的管理需求，需要配置带外管理交换机，在详细设计阶段需要考虑。

9 综合业务网网络需求

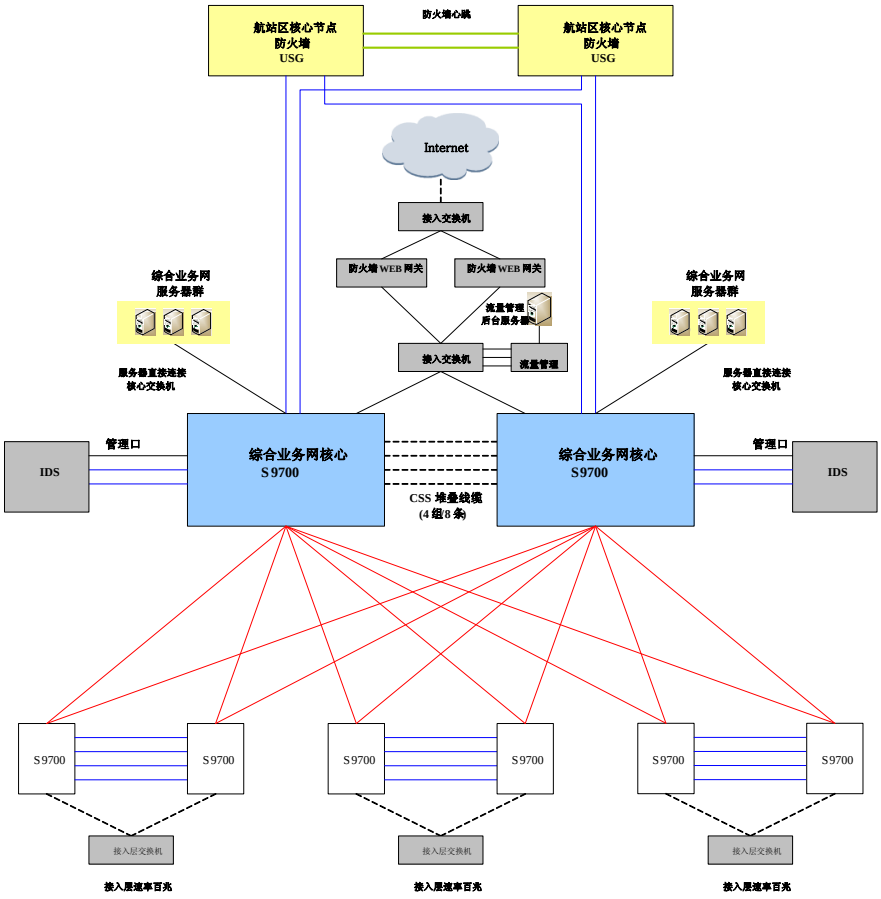
9.1 综合业务网架构需求

综合业务网是一个综合性的网络接入平台，为各种专业业务系统之外的应用系统提供接入。目前的综合业务网承载的应用系统包括 OA 系统、机房环境监控系统和 EGIS 等系统，同时综合业务网提供 Internet 接入。

综合业务网络结构为核心、汇聚、接入三层网络设计。进行端口聚合的端口要求跨模块部署，并预留备用链路，核心层设备采用虚拟化技术，构成一个整合的逻辑实体，简化网络 L2 的设计。接入层分散于各 SCR（含 DCR/SCR）间。同时，综合业务网需要部署 IDS 设备。

核心交换机可以使用 S9700 系列交换机，汇聚可以使用 S9700/7700 系列交换机，接入可以使用 S5700 系列交换机。

图9-1 综合业务网网络拓扑示意图



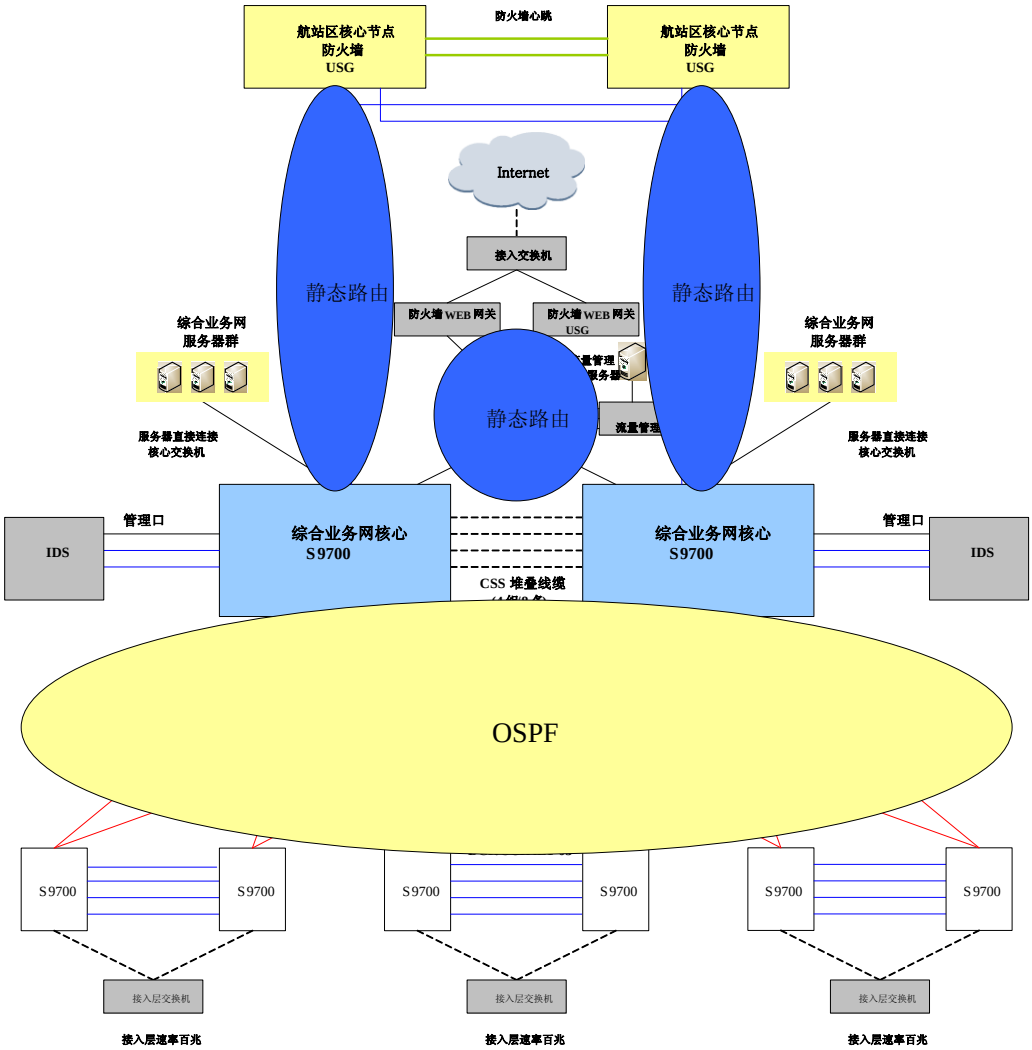
9.2 综合业务网路由需求

从网络规模来看，综合业务网属于中型网络。从网络建设最佳实践来看，标准化、开放的路由协议是首先需要考虑的。同时在信息网内部路由协议的选择和考虑方面，需要内部路由协议具备协议的成熟性、快速收敛、区域划分、支持中等规模网络等技术特性。从以上角度来看，OSPF 路由协议是适合于综合业务网网内的路由协议。

综合业务网与航站楼其它网络之间，以及综合业务网与 Internet 之间，由于有防火墙隔离，考虑到路由配置管理的便利性，同时考虑到路由的稳定性，建议采用静态路由，综合业务网可采用如下的路由设计。

- 综合业务网网内利用 OSPF 动态路由协议。
- 综合业务网与核心节点防火墙之间运行静态路由协议。
- 综合业务网与 Internet 之间运行静态路由协议。

图9-2 综合业务网路由设计



9.3 综合业务网承载的各业务系统（或子网）需求描述

9.3.1 工程地理信息系统（以下简称 EGIS）系统需求

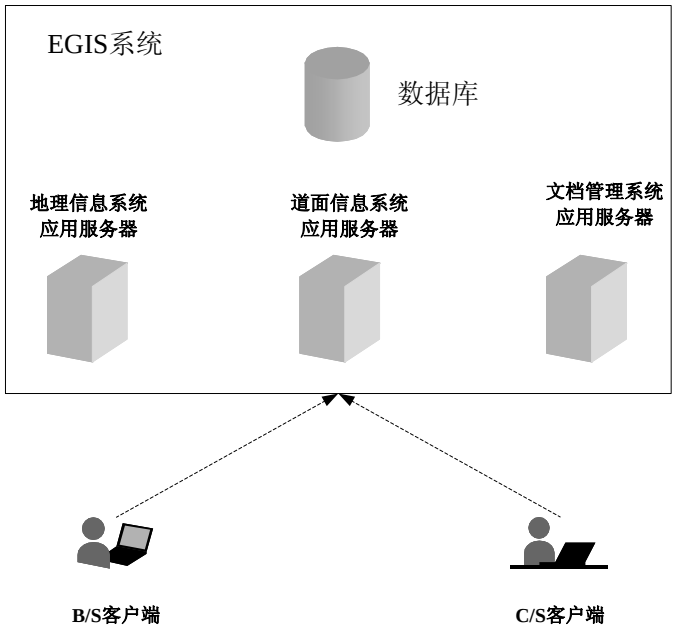
EGIS 系统业务描述

EGIS 系统建立和维护机场工程原始数据数据库，即所谓的 AGDB（机场地理信息数据库），是机场地理信息管理与服务的平台。

EGIS 系统技术架构示意图

EGIS 系统架构如图 9-3 所示。

图9-3 EGIS 系统架构图



EGIS 系统服务器包括数据服务器、应用服务器。数据库服务器用于地理信息数据、文档的存储和管理。应用服务器包括地理信息系统应用服务器、路面信息系统应用服务器和文档管理系统应用服务器。

EGIS 的应用分 B/S 和 C/S 两种架构，B/S 架构客户端通过浏览器访问应用系统，C/S 架构通过安装客户端软件访问系统。

EGIS 的主要用户是相关的机场管理人员。

EGIS 系统数据流向分析

B/S 架构的应用客户端通过浏览器访问系统；C/S 架构应用通过安装客户端软件访问系统。

EGIS 系统数据流量分析

为确保本系统的正常访问，需要保证 100M 或者以上的带宽。

EGIS 系统应用服务端口表

在详细设计阶段，将需要系统供应商提供如上述格式内容的应用服务访问端口表，以在网络实施时部署准确的应用服务访问控制，提高应用服务的安全性。

服务端口描述	地址	协议（TCP/UDP）	端口范围	访问控制需求
XX 系统接口	n.n.n.n	TCP	1521	允许 x.x.x.x 和 y.y.y.y

EGIS 系统外联接口需求列表

- 与 GOIS 系统 AODB 的接口，获取航班动态信息、旅客人数和飞行器出入位状态信息等。
- 与机场空管雷达系统接口加载或者获取飞行器进场运动轨迹。
- 与车辆定位系统接口加载或者显示应急车辆或其它移动目标运动轨迹。

EGIS 系统内服务器节点部署需求列表

示例如表 9-1 所示。

表9-1 EGIS 系统内服务器节点布置需求列表

服务器名称	用途	数量	部署位置	接口需求
EGIS 数据库服务器				100M
EGIS 应用服务器				100M

EGIS 系统内部终端/工作站节点布置需求列表

根据具体需求确定。

9.3.2 办公自动化系统（以下简称 OA）系统需求

OA 系统业务描述

目前 OA 系统的主要功能是实现公文流转、审批等办公自动化功能。另外，OA 系统还承担集团内部的邮件服务。航站楼综合业务网内部署 OA 系统的客户端。

OA 系统技术架构示意图

OA 系统架构为 B/S 架构，客户端通过 WEB 浏览器访问 OA 系统。

OA 系统数据流向分析

- OA 客户端利用浏览器加插件的方式，访问 OA 系统服务器；
- 机场管理办公人员通过局域网方式访问 OA 系统；
- 航站楼内用户，通过内网直接访问 OA 系统；
- 分支机构或合作伙伴的 OA 用户，通过 VPN 方式访问 OA 系统。

OA 系统数据流量分析

从系统建设、维护经验来看，终端采用 100M 接入可以满足业务需求。

OA 系统应用服务端口表

在详细设计阶段，将需要系统供应商提供如上述格式内容的应用服务访问端口表，以在网络实施时部署准确的应用服务访问控制，提高应用服务的安全性。

服务端口描述	地址	协议（TCP/UDP）	端口范围	访问控制需求
XX 系统接口	n.n.n.n	TCP	1521	允许 x.x.x.x 和 y.y.y.y

OA 系统外联接口需求列表

根据目前系统调研分析暂无要求，若有其它要求提出会进一步补充。

OA 系统内服务器节点部署需求列表

示例如表 9-2 所示。

表9-2 OA 系统内服务器节点布置需求列表

服务器名称	用途	数量	部署位置	接口需求
OA 服务器				100M

9.3.3 机房环境监控（含 KVM）系统需求

机房环境监控（含 KVM）系统业务描述

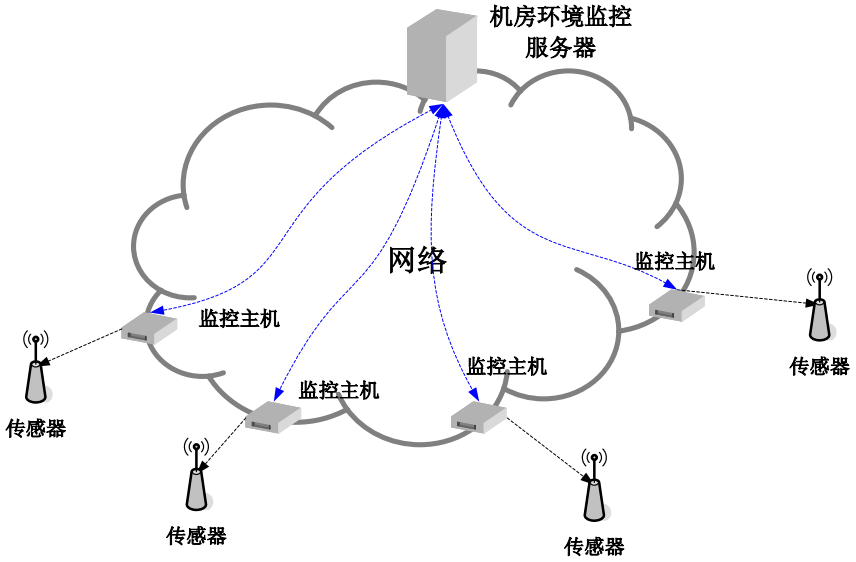
机房环境监控系统是用于监控机房温度、湿度、灰尘颗粒度、机房空调/UPS 运行状态以及配电回路状态的系统。

KVM 系统部署在机房用于服务器的维护管理使用，KVM 用于服务器的日常维护管理，不需要网络支持。

机房环境监控（含 KVM）系统技术架构示意图

机房环境监控系统架构如图 9-4 所示。

图9-4 机房环境监控系统架构图



机房环境监控系统中各设备间部署有嵌入式监控主机，监控主机通过 RS485 线路连接各个传感器，监控主机采集传感器信息，并转换为 IP 数据后，通过网络上传至后台环境监控服务器。

嵌入式监控主机具体数量根据实际情况确定。

由于机房环境系统的嵌入式监控主机部署在各个设备间，需要通过网络连接到环境监控服务器。机房环境监控系统是否需要接入到航站楼设备专网，可以根据实际情况确认。

机房环境监控（含 KVM）系统数据流向分析

在各设备间部署有嵌入式监控主机，监控主机通过 RS485 线路连接各个传感器，监控主机定时采集传感器信息，并转换为 IP 数据后，通过网络上传至后台环境监控服务器。

机房环境监控（含 KVM）系统数据流量分析

数据流类型均为环境状态信息等数据量较小。

机房环境监控（含 KVM）系统应用服务端口表

在详细设计阶段，将需要系统供应商提供应用服务访问端口表，以在网络实施时部署准确的应用服务访问控制，提高应用服务的安全性。

服务端口描述	地址	协议（TCP/UDP）	端口范围	访问控制需求
XX 系统接口	n.n.n.n	TCP	1521	允许 x.x.x.x 和 y.y.y.y

机房环境监控（含 KVM）系统内服务器节点部署需求列表

示例如表 9-3 所示。

表9-3 机房环境监控（含 KVM）系统内服务器节点布置需求列表

服务器名称	用途	数量	部署位置	接口需求
XXX 连廊机房环境监控服务器	环境监控	1		100M
XXX 机房环境监控服务器	环境监控	1		

机房环境监控（含 KVM）系统内部终端/工作站节点布置需求列表

示例如表 9-4 所示。

表9-4 机房环境监控（含 KVM）系统内部终端/工作站节点布置需求列表

终端/工作站	接入交换机	数量	部署位置	接口需求
监控主机			各弱电设备间	100M

9.4 综合业务网网络性能需求

综合上述各个业务系统，关于性能方面的需求有以下几点。

- OA 系统：根据系统管理人员的维护经验来看，终端 100M 接入可以满足业务需求。
- EGIS 系统：为确保本系统的正常访问，需要保证 100M 或者以上的带宽。
- 机房环境监控：数据量很小。
- Internet 访问的流量：假定 Internet 接入带宽 100M，那么极限的出口峰值应该在 100M 左右。

9.5 综合业务网网络广播控制需求

由于综合业务网只有 OA 系统的客户端设备，而 EGIS 系统的用户是相关的机场管理人员，另外还有访问 Internet 的终端，从经验上来看，这几类用户可能是重叠的，因此，综合业务网内部根据汇聚/接入区域划分不同 VLAN，以控制广播域。

9.6 综合业务网网络安全需求

综合业务网安全边界如图 9-5 所示，包括外部安全边界和内部安全边界。

- 红色部分为外部安全边界，包括两个部分。

- 综合业务网与航站楼其它网络，以及与航站楼节点外的其它节点网络（例如物流园区网络、办公区网络等）的边界。
- 综合业务网与 Internet 之间的安全边界。

针对上述安全边界，需要部署防火墙实施严格的网络隔离和控制，利用 ACL 控制网络间、系统间的系统访问，提高网络安全性。

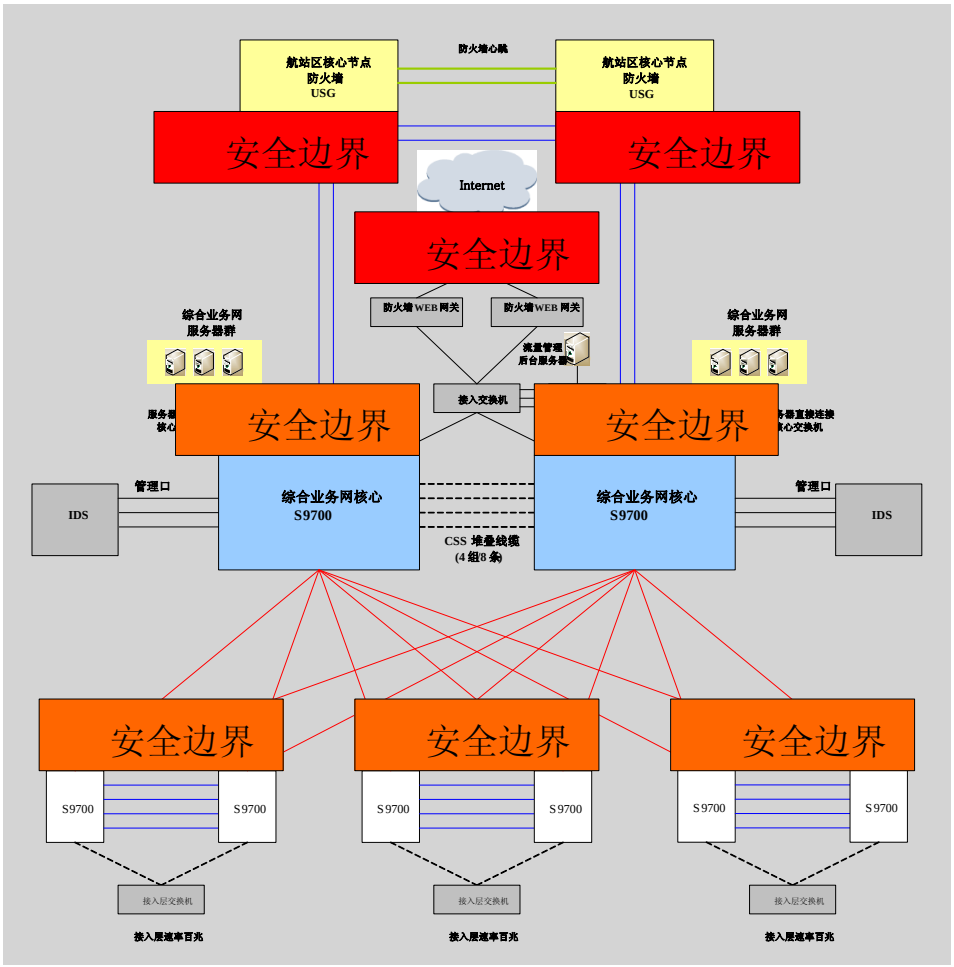
对于 Internet 边界，除了需要防火墙进行网络隔离外，还需要部署流量管理设备，来针对互联网上下行流量进行基于内容的管理，以提高互联网接入的安全性。

- 橙色部分为内部安全边界，指的是综合业务网内服务器与客户端之间的安全边界。

针对内部安全边界，需要部署适当的网络安全技术，提供访问安全保护。包括：

- 在核心交换机部署 IDS 设备，检测网络访问安全事件。
- 在客户端，通过防病毒系统，提供客户端自身的防病毒能力，以提高客户端的系统安全性。

图9-5 综合业务网安全边界示意图



9.7 综合业务网网络 QOS 需求

从技术应用角度来看，只有在网络出现拥塞的情况下，才需要部署 QoS，以对业务应用进行分类，并保障关键业务优先使用网络资源。而综合业务网承载的业务应用，都是基于 TCP/IP 的数据类应用，各业务系统的数据流量都不大，采用本方案推荐的 S9700/7700/5700 等系列交换机配置，综合业务网不需要部署 QoS。

9.8 综合业务网网络管理需求

在航站楼网络节点核心集中部署网络管理系统，用于网络拓扑、网络设备等的集中管理，因此，需要综合业务网网络设备具备以下能力。

- 支持 SNMP 功能；
- 支持设定网管系统定义的 SNMP read community 和 SNMP write community；
- 支持将系统时钟（NTP）服务器指定为网络统一的 NTP 时钟源。

说明

考虑到配置的小型机服务器以及数据库等的管理需求，需要配置带外管理交换机，在详细设计阶段需要考虑。

10 设备专网网络需求

10.1 设备专网架构需求

设备专网主要是为智能照明、电梯、扶梯、自动步行道、登机桥监控、楼宇等环境与设施控制系统系统提供承载服务的网络平台。设备专网业务系统对于网络高可靠性方面有较高要求。

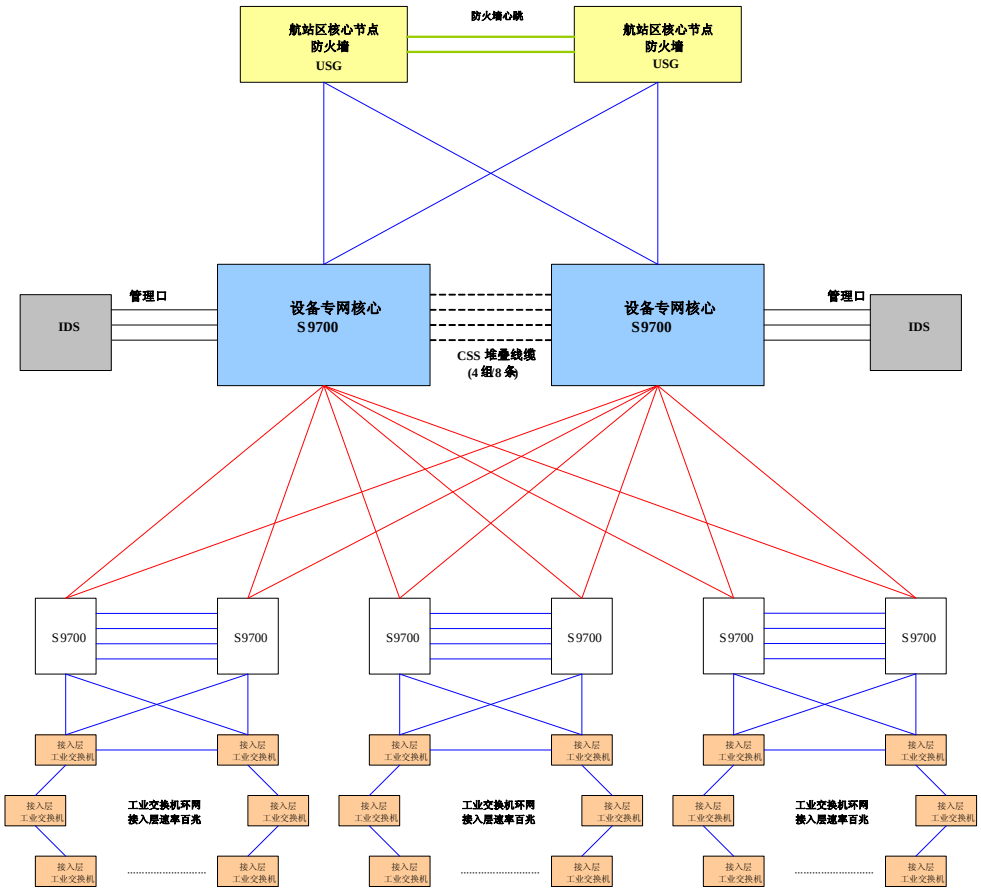
设备专网为多层星型、环型混合网络架构。设备选择采用商用交换机、工业交换机混合组网架构，商用交换机可以使用 S9700 系列交换机。核心交换机采用虚拟化技术，构成一个整合的逻辑实体，简化网络 L2 的设计。

考虑到设备专网中设施对于粉尘、电磁、电力、温度、湿度等环境条件的要求，在设备专网接入层，需要由工业交换机为其提供网络接入。

每台汇聚交换机通过以太链路分别连接两台核心交换机。接入层工业交换机通过采用光纤组成环网，环内连接速率为 100M。在环内部署 2 台汇聚工业交换机，配置两路以太链路与汇聚层交换机连接，作为整个环网与汇聚设备的连接点，连接速率为 1000M。登机桥部分采用前端放置工业交换机，采用星型方式接入环交换网络。

设备专网网络拓扑架构如图 10-1 所示。

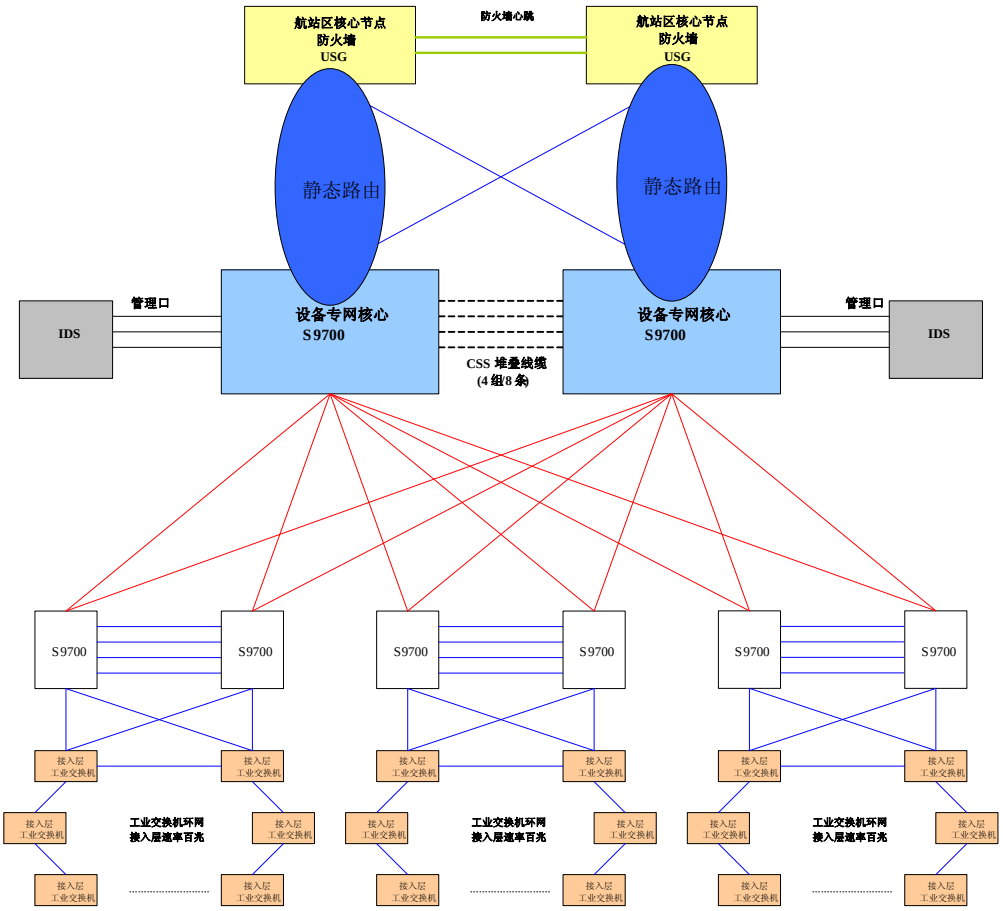
图10-1 设备专网拓扑架构示意图



10.2 设备专网路由需求

设备专网内，承载有多个专业化监控系统，从管理角度和网络安全考虑，需要在这些专业监控系统间（包括监控服务器和前端信息采集设备）通过 VLAN 实施隔离，因此，设备专网将是 L2 架构的网络。在设备专网核心设备上，通过静态路由，实现设备专网与航站楼其它网络的互连互通。

图10-2 设备专网路由架构示意图



10.3 设备专网承载的各业务系统（或子网）需求描述

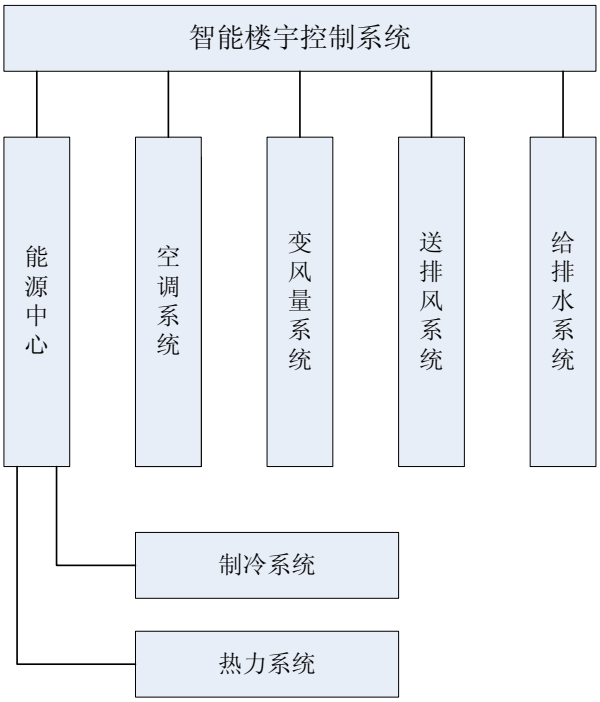
10.3.1 楼宇自动控制系统（以下简称楼控）需求

楼控系统业务描述

航站楼的楼控系统中分控工作站与航站楼中央管理系统通过以太网进行通讯，将分控数据备份于航站楼中央管理系统中。

楼宇自控系统（BAS）架构如图 10-3 所示。

图10-3 楼宇自控系统架构



楼控系统的主要控制设备包括：空调、新风机、排风机、空调三次泵、排污泵、排烟天窗等。

楼控系统的控制服务器包括：BA 总控服务器、能源中心分控服务器、分控服务器。

在办公坐席规划有管理终端，具体位置根据实际情况定。

直接数字控制系统 DDC 通过专用线缆连接受控设备，采集设备运行状态信息后，上传至对应的监控服务器，每台 DDC 需要 1 个网络设备端口，数量根据实际情况定。

楼控系统数据流向分析

DDC 采集受控设备的状态信息，并上传至管理站。

楼控系统数据流量分析

数据流类型均为状态信息、控制信息等，数据量较小。

楼控系统应用服务端口表

在详细设计阶段，将需要系统供应商提供应用服务访问端口表，以在网络实施时部署准确的应用服务访问控制，提高应用服务的安全性。

服务端口描述	地址	协议（TCP/UDP）	端口范围	访问控制需求
XX 系统接口	n.n.n.n	TCP	1521	允许 x.x.x.x 和 y.y.y.y

楼控系统外联接口需求列表

- 通过 IBMS 以 OPC 接口方式实现与地面信息系统之间的系统接口。
- 楼控系统除了监控空调、新风机等系统内的受控设备，还通过 IBMS 采集电梯、电扶梯（步道）、登机桥、供配电、智能照明、行李转盘等系统受控设备的状态信息。

楼控系统内服务器节点部署需求列表

示例如表 10-1 所示。

表10-1 楼控系统内服务器节点布置需求列表

服务器名称	用途	数量	部署位置	接口需求
XXX 机房楼控服务器		1		100M
XXX 机房楼控服务器(备机)		1		100M
XXX 分控服务器		1		100M
XXX 分控服务器		1		100M
XXX 分控服务器		1		100M

楼控系统内部终端/工作站节点布置需求列表

示例如表 10-2 所示。

表10-2 楼控系统内部终端/工作站节点布置需求列表

终端/工作站	接入交换机	数量	部署位置	接口需求
办公坐席管理终端			各弱电设备间	100M
DDC				

10.3.2 智能照明系统需求

智能照明系统业务描述

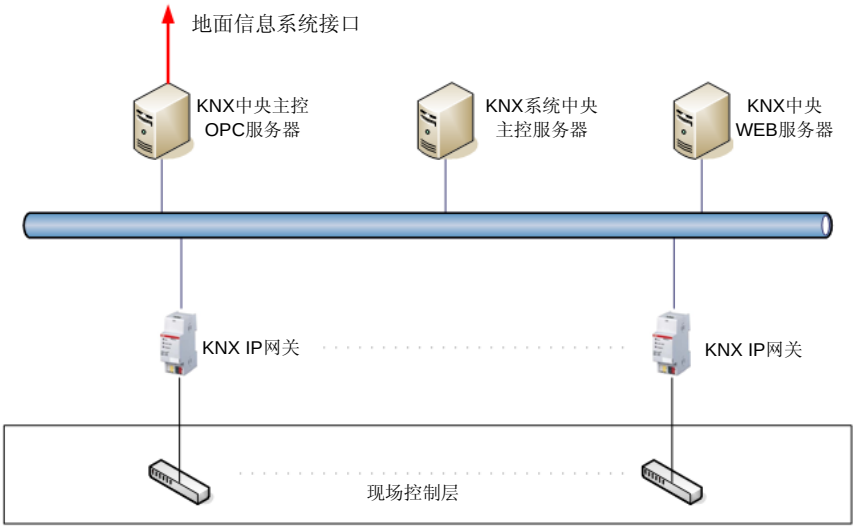
智能照明系统是为了满足机场照明需求而建设的智能灯光管理系统。智能照明系统承担的控制功能包括以下几部分。

- 航站楼单体内智能照明控制
- 支线航站楼内智能照明控制
- 近机位及站坪远机位高杆灯智能照明控制

- 站坪道路照明
- 高架桥智能照明控制
- 站坪景观智能照明控制

智能照明系统技术架构如图 10-4 所示。

图10-4 智能照明系统架构示意图



说明

KNX 总线是独立于制造商和应用领域的系统。所有的总线设备连接到 KNX 介质上（这些介质包括双绞线、射频、电力线或 IP/Ethernet）,它们可以进行信息交换。

智能照明系统采用 ABB i-bus 智能建筑控制系统。系统设置一个主控制中心，位于监控机房内。系统结构为线性、星型或树型的总线型分布式结构，通过在总线上传输通信数据包，可对每一个智能照明设备进行独立控制。

智能照明系统分为三层结构：中央管理层、数据网络层、现场控制层。

根据管理需要，有关灯具使用时间以及运行状态和故障的信息均可被中央监控工作站以及楼宇管理系统读取。

智能照明系统数据流向分析

智能照明系统的主要数据流向包括：

- 系统主控采集各个控制点的状态信息的轮询流
- 故障节点触发的故障信息上传流
- 中央自动控制的控制流

智能照明系统数据流量分析

智能照明系统的前端控制点约 X 千个，每个控制点采集的信息类型包括：电流值状态、系统总线状态、故障状态、受控点运行状态。系统主控对于控制点的轮询时间间隔一般

为几分钟，如果控制点设备故障，会主动触发从 IP 路由器网关设备（IPR/S2.1）到中央主控的故障信息数据流。

综上所述，智能照明系统的数据量，相对于网络带宽而言比较小。

智能照明系统应用服务端口表

在详细设计阶段，将需要系统供应商提供应用服务访问端口表，以在网络实施时部署准确的应用服务访问控制，提高应用服务的安全性。

服务端口描述	地址	协议（TCP/UDP）	端口范围	访问控制需求
XX 系统接口	n.n.n.n	TCP	1521	允许 x.x.x.x 和 y.y.y.y

智能照明系统内服务器节点部署需求列表

示例如表 10-3 所示。

表10-3 智能照明系统内服务器节点布置需求列表

服务器名称	用途	数量	部署位置	接口需求
系统中央监控主机		1		100M
WEB SERVER 服务器		1		100M
KNX OPC SERVER 服务器		1		100M
景观控制分站分控机		1		100M

智能照明系统内部终端/工作站节点布置需求列表

示例如表 10-4 所示。

表10-4 智能照明系统内部终端/工作站节点布置需求列表

终端/工作站	接入交换机	数量	部署位置	接口需求
IP 路由器网关设备（IPR/S2.1）				100M

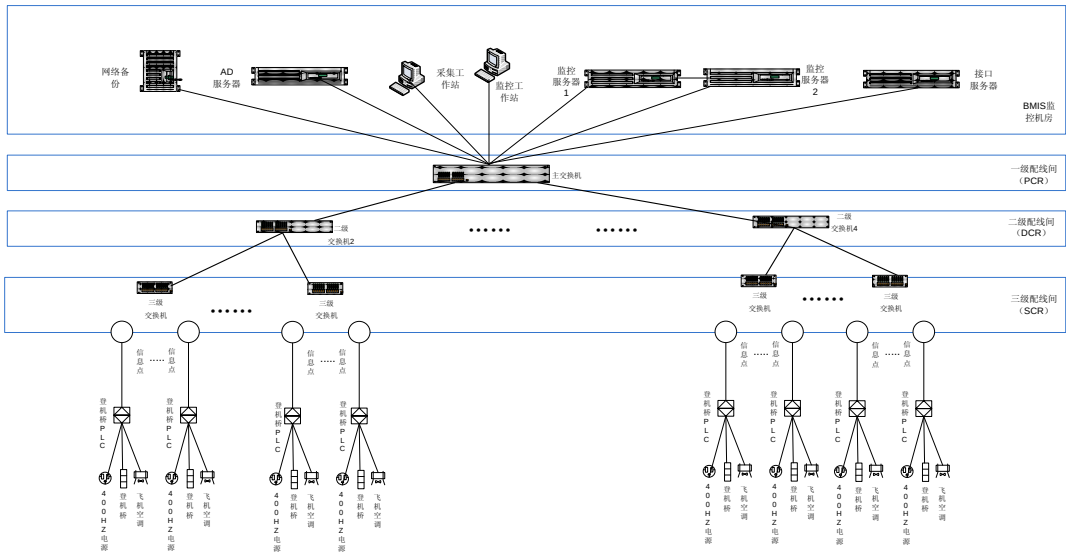
10.3.3 登机桥监控系统需求

登机桥监控系统业务描述

航站楼登机桥监控系统的基本功能为状态监视和信息采集，对登机桥、400Hz 电源、飞机专用空调的工作数据进行采集，并对这些设备的工作状态进行监控。

登机桥监控系统技术架构如图 10-5 所示。

图10-5 登机桥监控系统架构示意图



登机桥监控系统主要是由数据采集工作站和数据库服务器以及监控工作站构成。

- 登机桥主数据采集 PLC 本身的网络接口为 RJ45 电口。
- 数据采集工作站网络和登机桥 PLC 通讯，将采集到的登机桥的相应数据，送入数据库服务器，服务器将对送入的数据进行处理。
- 400HZ 电源通过干节点信号与登机桥 PLC 相连接，其开关状态信息由登机桥 PLC 转换后送入登机桥监控系统的数据库服务器，服务器将对送入的数据进行处理。
- 飞机专用空调通过干节点信号与登机桥 PLC 相连接，其开关状态信息由登机桥 PLC 转换后送入登机桥监控系统的数据库服务器，服务器将对送入的数据进行处理。
- 监控工作站随时可调取服务器处理过的数据，并通过报表和查询的方式进行显示和存储，可在监控中心内的监控工作站对登机桥的运行状态进行全面、实时的监控。
- 数据库服务器主要作用是将采集电脑采集的数据进行集中和处理，同时将处理过的数据进行保存，并提供相应的数据通道供监控计算机读取数据，或通过接口服务器向其它信息系统提供数据或是从其它信息系统获得数据并保存。数据库服务器由两台服务器组成，为双机热备的工作方式。
- AD 服务器可以为本系统所有设备提供统一的时钟信息和帐号管理。
- 监控工作站计算机用于显示和查询登机桥的各种运行状态，直观的显示各种图形和数据以及报表等。

- 登机桥主数据采集工作站主要利用 OPC Server 采集各登机桥、400Hz 电源、飞机专用空调的现场数据，并对各登机桥、400Hz 电源、飞机专用空调的数据进行简单的归类与处理，并向数据库服务器实时发送登机桥、400Hz 电源、飞机专用空调的实时数据。

登机桥监控系统数据流向分析

桥头 PLC 设备采集登机桥、400Hz 电源、飞机专用空调的运行状态信息，并上传数据库服务器。

登机桥监控系统数据流量分析

从系统建设经验来看，桥头终端 100M 接入，可以满足业务需求。

登机桥监控系统应用服务端口表

在详细设计阶段，将需要系统供应商提供应用服务访问端口表，以在网络实施时部署准确的应用服务访问控制，提高应用服务的安全性。

服务端口描述	地址	协议（TCP/UDP）	端口范围	访问控制需求
XX 系统接口	n.n.n.n	TCP	1521	允许 x.x.x.x 和 y.y.y.y

登机桥监控系统外联接口需求列表

登机桥监控系统与如下系统有系统接口。

- 地面信息系统（获取航班信息）
- 楼控系统（楼控系统从登机桥系统获取状态信息）
- 时钟系统（时钟校准）

登机桥监控系统内服务器节点部署需求列表

示例如表 10-5 所示。

表10-5 登机桥监控系统内服务器节点布置需求列表

服务器名称	用途	数量	部署位置	接口需求
数据库服务器				100M
接口服务器				100M
AD 服务器				100M
网络备份服务器				100M

登机桥监控系统内部终端/工作站节点布置需求列表

示例如表 10-6 所示。

表10-6 登机桥监控系统内部终端/工作站节点布置需求列表

终端/工作站	接入交换机	数量	部署位置	接口需求
登机桥 PLC 设备				100M
采集工作站				100M
监控工作站				100M

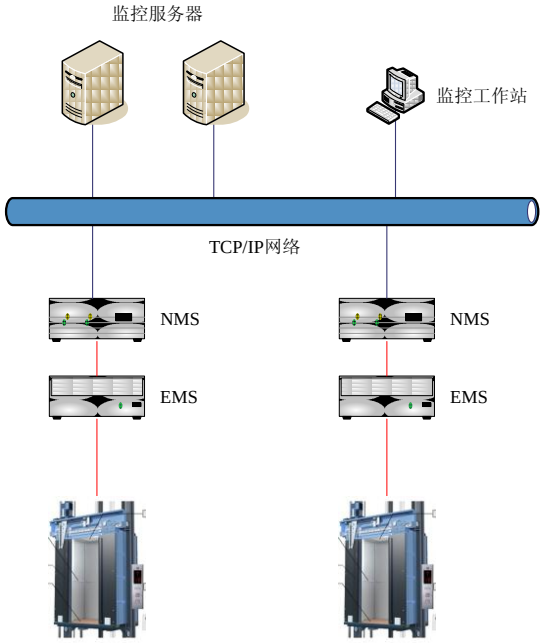
10.3.4 升降电梯监控系统需求

升降电梯监控系统业务描述

升降电梯监控系统用于对电梯运行状态的监控，电梯的运行状态信息包括设备的运行、停止、故障和报警状态。

升降电梯监控系统技术架构如图 10-6 所示。

图10-6 升降电梯监控系统架构示意图



升降电梯监控系统数据流向分析

升降电梯监控系统的主要功能包括：设备的运行状态和楼层显示、故障显示。

升降电梯监控系统包括如下组件。

- 监控服务器：用于升降电梯设备的监控。

  每 1 台监控服务器可以管理多台升降电梯，根据实际需要配置监控服务器数目。
- NMS 网络监控系统：用于将设备状态信息数据转换为 TCP/IP 报文，通过网络，将状态信息上传至监控服务器。
- EMS 升降电梯监控系统：用于从设备采集运行状态信息，并将状态信息，通过与 NMS 送至 NMS。

  每台 NMS 可以管理多台电梯设备，根据实际情况，可能由于布线等原因，采用 1:1 配置 EMS，NMS。NMS 具有网络接口，需要接入 TCP/IP 网络。
- 监控工作站用于对监控设备的维护管理。

升降电梯监控系统数据流量分析

- EMS 采集设备运行状态信息，并经过专用连接，送至 NMS。
- NMS 将状态信息数据转换为 TCP/IP 报文，上传至监控服务器。

升降电梯监控系统应用服务端口表

在详细设计阶段，将需要系统供应商提供应用服务访问端口表，以在网络实施时部署准确的应用服务访问控制，提高应用服务的安全性。

服务端口描述	地址	协议（TCP/UDP）	端口范围	访问控制需求
XX 系统接口	n.n.n.n	TCP	1521	允许 x.x.x.x 和 y.y.y.y

升降电梯监控系统外联接口需求列表

升降电梯与楼控系统有系统接口。

升降电梯监控系统内服务器节点部署需求列表

示例如表 10-7 所示。

表10-7 升降电梯监控系统内服务器节点布置需求列表

服务器名称	用途	数量	部署位置	接口需求
监控服务器				100M

升降电梯监控系统内部终端/工作站节点布置需求列表

示例如表 10-8 所示。

表10-8 升降电梯监控系统内部终端/工作站节点布置需求列表

终端/工作站	接入交换机	数量	部署位置	接口需求
NMS				100M

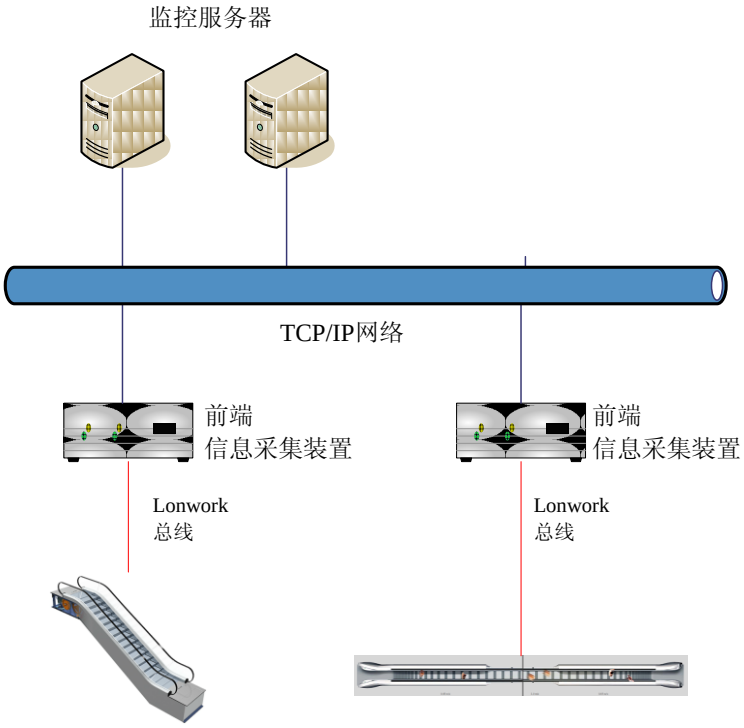
10.3.5 电扶梯、步道（以下简称电扶梯）监控系统需求

电扶梯监控系统业务描述

电梯、步道监控系统用于对电梯、步道的运行状态监控，状态信息包括设备的运行、停止、故障和报警状态。

电扶梯监控系统技术如图 10-7 所示。

图10-7 电扶梯监控系统架构示意图



电梯监控系统的主要监控状态信息包括上行、下行、停止等几个状态；

自动扶梯监控系统包括如下组件。

- 监控服务器：用于电扶梯设备的监控
- 前端信息采集装置：用于将设备状态信息数据转换为 TCP/IP 报文。通过网络将状态信息上传至监控服务器。信息采集装置与受控设备（电扶梯、步道）之间通过 Lonwork 总线连接，信息采集装置有 1 个网络接口，需要接入 TCP/IP 网络。

  信息采集可以根据实际情况采用 1：N 或者 1:1 灵活配置；

  每 1 台监控服务器可以管理多台自动扶梯，需要根据实际情况确定服务器数量；

监控工作站是否使用，及如果使用具体数量是多少待定。

电扶梯监控系统数据流向分析

- 前端采集装置通过 Lonwork 专用连接采集设备运行状态信息。
- 前端信息采集装置将从 Lonwork 总线采集的状态信息数据转换为 TCP/IP 报文，上传至监控服务器。

电扶梯监控系统数据流量分析

数据流类型均为状态信息、控制信息等，数据量较小。

电扶梯监控系统应用服务端口表

在详细设计阶段，将需要系统供应商提供应用服务访问端口表，以在网络实施时部署准确的应用服务访问控制，提高应用服务的安全性。

服务端口描述	地址	协议（TCP/UDP）	端口范围	访问控制需求
XX 系统接口	n.n.n.n	TCP	1521	允许 x.x.x.x 和 y.y.y.y

电扶梯监控系统内服务器节点部署需求列表（示例样表）

示例如表 10-9 所示。

表10-9 电扶梯监控系统内服务器节点布置需求列表

服务器名称	用途	数量	部署位置	接口需求
监控服务器				100M

电扶梯监控系统内部终端/工作站节点布置需求列表

示例如表 10-10 所示。

表10-10 电扶梯监控系统内部终端/工作站节点布置需求列表

终端/工作站	接入交换机	数量	部署位置	接口需求
前端信息采集装置				100M

10.4 设备专网网络吞吐量需求

根据具体需求确定。

10.5 设备专网网络性能需求

设备专网内登机桥监控、电梯监控、智能照明等系统均为设备监控类应用，其业务数据均为小数据量的状态信息、控制信令等。从经验来看，当前的设备专网设计应该可以很好地支持设备专网的业务应用。

10.6 设备专网网络广播控制需求

设备专网内承载有楼控、登机桥监控、电梯监控、智能照明等多个业务系统，这些业务系统虽然数据流量较小，但是在系统安全性方面，需要更多考虑。

从管理角度和网络安全考虑，需要在这些专业监控系统间（包括监控服务器和前端信息采集设备）通过 VLAN 实施隔离，因此，设备专网将是 L2 架构的网络。各个监控服务器与其对应的受控设备处于同一 VLAN，不同监控系统之间将需要通过实施隔离。当不同监控系统间需要通信时（例如楼控系统的 BMS 服务器需要从其他监控系统收取状态信息），需部署访问控制，以提高安全性，同时也可以有效控制广播域。

10.7 设备专网网络安全需求

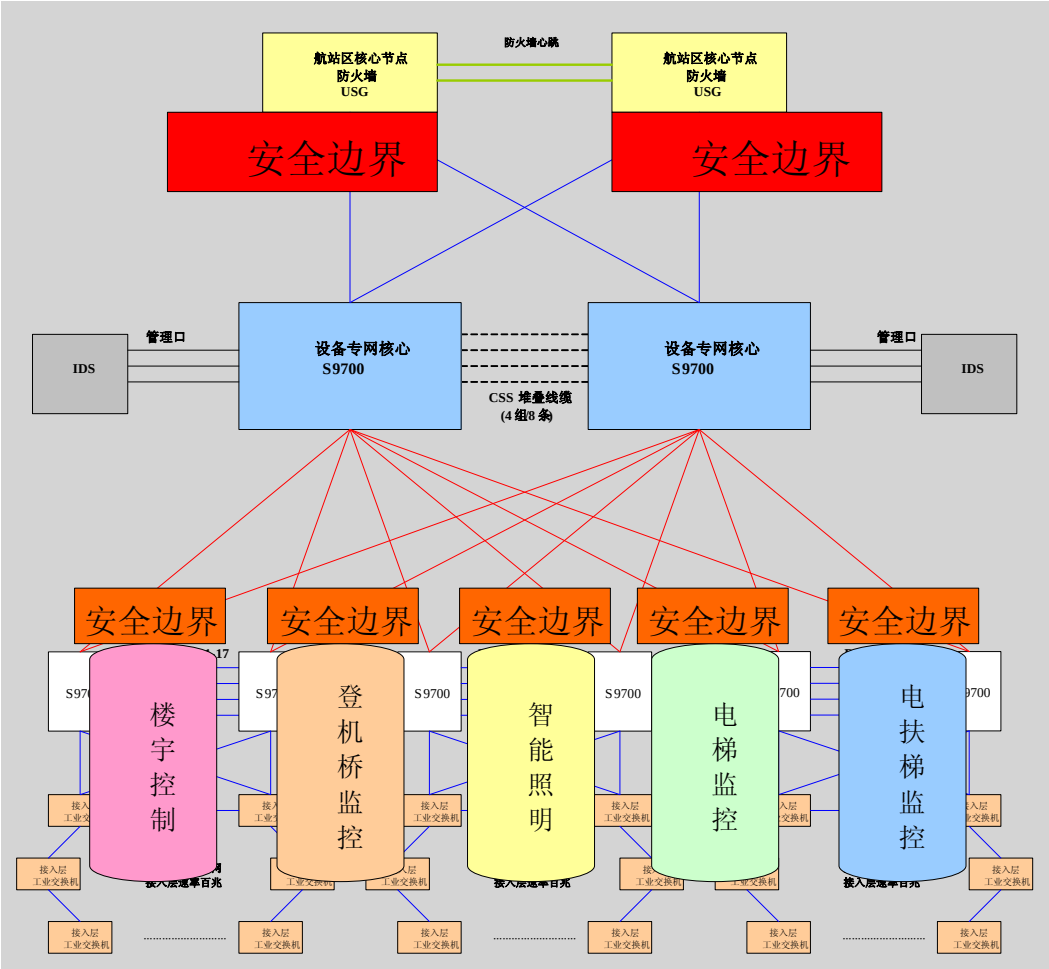
设备专网安全边界如图 10-8 所示，包括外部安全边界和内部安全边界两部分。

红色部分为外部安全边界，包括设备专网与航站楼内其它网络，以及与航站楼外的其它节点网络（例如物流园区网络、办公区网络等）的边界。针对该类安全边界，需要部署防火墙实施严格的网络隔离和控制，利用 ACL，控制网络间、系统间的系统访问，提高网络安全性。

橙色部分为内部安全边界。设备专网内部设备网内的终端，都是各类工业化信息采集专用设备，且各监控系统监控服务器与终端都在同一 VLAN。不同系统（VLAN）间的访问，会在网络层（L3）进行严格的访问控制，从这个意义上来讲，IDS 部署的必要性不大。

针对内部安全边界，可以在核心交换机上部署 ACL 来提供访问安全控制，以提高网络安全性。

图10-8 设备专网安全边界示意图



10.8 设备专网网络 QOS 需求

从技术应用角度来看，只有在网络出现拥塞的情况下，才需要部署 QoS，以对业务应用进行分类，并保障关键业务优先使用网络资源。而综合业务网承载的业务应用，都是基于 TCP/IP 的数据类应用，各业务系统的数据流量都不大，采用本方案推荐的 Sx7 系列交换机配置，设备专网不需要部署 QoS。

10.9 设备专网网络管理需求

在航站楼网络节点核心集中部署网络管理系统，用于网络拓扑、网络设备等的集中管理，因此，需要设备专网网络设备具备以下能力。

- 支持 SNMP 功能；
- 支持设定网管系统定义的 SNMP read community 和 SNMP write community；

- 支持将系统时钟（NTP）服务器指定为网络统一的 NTP 时钟源。

说明

考虑到配置的小型机服务器以及数据库等的管理需求，需要配置带外管理交换机，在详细设计阶段需要考虑。

A 缩略语

Numeric

A

AODB	Airport Operation DataBase	机场运行数据库

B

BAS	Building Automation System	楼宇自动化系统

C

CSS	Cluster Switch System	集群交换机系统

K

KVM	Keyboard、Video、Mouse	多计算机切换器

Q

QOS	Quality of Service	服务质量