

The page features decorative geometric shapes in the top-left and bottom-right corners. These shapes are composed of overlapping triangles in various colors: light green, light purple, light yellow, and light pink. The background is a solid light gray.

厂区网络设计方案

网络及电话设计方案



目 录

| | |
|-----------------------|----|
| 第 1 章 网络需求分析 | 4 |
| 1.1 需求分析 | 4 |
| 1.2 建设目标 | 4 |
| 第 2 章 组网方案规划设计 | 6 |
| 2.1 建设原则 | 6 |
| 2.2 层次化设计 | 8 |
| 2.3 高可靠性 | 9 |
| 2.4 网络总体规划 | 12 |
| 第 3 章 安全管理安全渗透网络设计 | 12 |
| 3.1 网络完全实际办法 | 15 |
| 3.2 核心交换机强大内置安全特性 | 16 |
| 3.3 基层网络安全 | 16 |
| 1、端口+IP+MAC 地址的绑定: | 15 |
| 2、MAC 地址盗用的防止 | 16 |
| 3、防止对DHCP 服务器的攻击 | 16 |
| 4、防止ARP 的攻击 | 16 |
| 5、组合丰富的VLAN 功能进行业务隔离 | 18 |
| 6、配置防火墙和IPS 进行网络区域的隔离 | 18 |
| 3.4 配置全面的网络防病毒系统 | 19 |
| 集中控管能力: | 19 |
| 采取用户端点准入防御解决方案 | 20 |
| 第 4 章 设备选型 | 21 |
| 网络设备 | 21 |
| 4.1 核心交换机 | 21 |
| 产品概述 | 21 |
| 4.2 接入交换机 | 21 |
| 4.3 外网接入路由器 | 21 |
| 第 5 章 组网优势 | 25 |

第1章 网络需求分析

1.1 需求分析

总厂办公楼共3层，核心机房在1楼。整个办公楼大约150-170个信息点，车间及办公室大约50个信息点（包括预留）信息点位分布如下表：

| 楼层 | 1F | 2F | 3F | 厂区 |
|--------|----|----|----|----|
| 电话信息点位 | 5 | 20 | 20 | 70 |
| 网络信息点位 | 30 | 30 | 30 | 30 |

本次组网设计为企业内网和互联网两部分，出于安全考虑，设计为内外网物理隔离方式。

网络设计为接入多功能路由器，核心交换机，接入交换机等，核心线路使用光纤连接，以达到千兆主干千兆桌面的方案，启动vlan和限速功能来合理利用互联网资源。并在多能路由器上做多种防范攻击措施，保证网络稳定。

本次网络建设总结起来，需要满足以下几个方面的要求：

- 1: 建设一个高可靠、高性能的大楼办公网；
- 2: 由于需要接入Internet，需要考虑上网的高安全性；
- 3: 在网络边界，需要考虑网络病毒及攻击的防范。

1.2 建设目标

通过对大楼办公网络需求进行分析，在以下几个方面需要特别关注：

- 1、可靠性。

办公网络是一个承载日常业务的重要平台，随着各种业务办公的自动化程度越来越高，对网络平台的依赖性也越来越强，因此，首先需要构建一个具有高度可靠性的网络，可靠性主要体现在业务系统、服务器存储系统和网络系统的稳定性上，针对网络系统的稳定性有堆叠技术做支撑；

2、高性能

目前，随着全球信息时代的到来，越来越多的业务都可以承载到 IP 网络平台之上，网络平台的容量也在急剧上升，而所有容量的 80%来自于局域网，因此，局域网的高性能，成为提高工作效率的关键。此次，西安泵阀总厂的网络建设需要充分考虑的网络的高性能目标。

3、安全性。

现在病毒、黑客和终端用户是造成整网安全的隐患，尤其是终端用户的安全管理长期以来没有一个很好的解决方案，这次设计专业网络行为管理设备来对用户的网络接入安全进行细致安全合理的优化。

4、高带宽。

网络是一个庞大而且复杂的网络，为了保障全网的高速转发，网全网的组网设计的无瓶颈性，要求方案设计的阶段就要充分考虑到，同时要求核心交换机具有高性能、高带宽的特，整网的核心交换要求能够提供无瓶颈的数据交换。

5、可增值性。

网络的建设、使用和维护需要投入大量的人力、物力，因此网络的增值性是网络持续发展基础。所以在建设时要充分考虑业务的扩展能力，能针对不同的用户需求提供丰富的宽带增值业务，使网络具有自我造血机制，实现以网养网。

6、可扩充性。

考虑到用户数量和业务种类发展的不确定性，要求对于核心交换机与汇聚交换机具有强大的扩展功能，网络要建设成完整统一、组网灵活、易扩充的弹性网络平台，能够随着需求变化，充分留有扩充余地。

7、可开放性。

技术选择必须符合相关国际标准及国内标准，避免个别厂家的私有标准或内部协议，确保网络的开放性和互连互通，满足信息准确、安全、可靠、优良交换传送的需要；开放的接口，支持良好的维护、测量和管理手段，提供网络统一实时监控的遥测、遥控的信息处理功能，实现网络设备的统一管理。

8、安全可靠性的。

设计应充分考虑整个网络的稳定性，支持网络节点的备份和线路保护，提供网络安全防范措施。

第2章 组网方案规划设计

2.1 建设原则

总的建设原则是设备先进、功能齐全、适应发展、突出重点、量力而行。

1、实用性原则：

以现行需求为基础，充分考虑发展的需要来确定规模。

2、冗余性原则：

特别注重网络硬件系统自身在突发事件时的可用性，以冗余备份的设计方式加以保障。

3、安全性原则：

系统应能提供较高的安全手段，防止系统外部成员的非法侵入以及操作人员的越级操作。安全性是信息化建设的基础保障。出于安全及保密因素，现在信息化建设工程对安全性有很高的要求。设计的过程中必须依据国家各种有关

安全法规政策，对硬件支撑平台的访问控制、在线监视、信息加密等方面进行完善考虑，在网络建构上根据功能划分相应的区域，使用如防火墙、入侵检测、加密设备对信息过滤、隔离、数据加密等手段，同时采用虚拟网划分及目前较流行的 VPN 及安全认证等技术，防止非法用户、非法信息及病毒的入侵和泄密事件的发生。同时还要在企业内部建立健全各种相关安全管理制度，确保全网的安全。

4、先进性原则：

系统要采用国际上先进的前沿技术，满足今后一段时期的需要。

5、易维护原则：

系统要易于管理、易于维护。网络需要很高的可管理性，特别是在数据、视频等多业务的网络系统里，要使用可管理的网络设备，可以识别关键资源，根据流量状况以及网络性能配置阈值并为不同的应用提供不同的带宽，使所有的服务能够顺利完成。

随着系统的投入运行和系统资源的不断增加，网络系统应具有很好的易维护性，使管理人员易于维护，减少不必要的额外劳动，提高工作效率。

6、易扩展原则：

提供开放性好、标准化程度高的技术和设备，便于功能扩展。考虑到业务日益增长的长远需求，提供网络的可扩充性。用户的数量、需求和应用在不断变化，技术也不断发展，随着网络技术的不断发展，网络应用规模在不断扩大。因此，在网络结构上要实现真正开放，基于国际开放式标准，设计过程中应当保证在用户业务量和业务类型的变化增长的情况下，硬件支撑平台能够方便的升级并扩展，网络可以自如地扩充容量，支持更多的用户及应用。网络平

台设计时必须按照各种国际通用标准进行，以保证各种设备、网络的兼容通用。开放的网络使用户可以自由地选择不同厂家的产品，将来网络在实现扩容、升级时不会受到某些厂家专有标准的限制。网络结构与网络技术的选择，要具有相当的前瞻性，以确保随着网络技术的不断发展，网络能够平滑地过渡到更先进的技术和设备，充分保障用户现有的投资和利益。

网络的扩展能力包括设备交换容量的扩展能力、端口密度的扩展能力、主干带宽的扩展，以及网络规模的扩展能力。

2.2 层次化设计

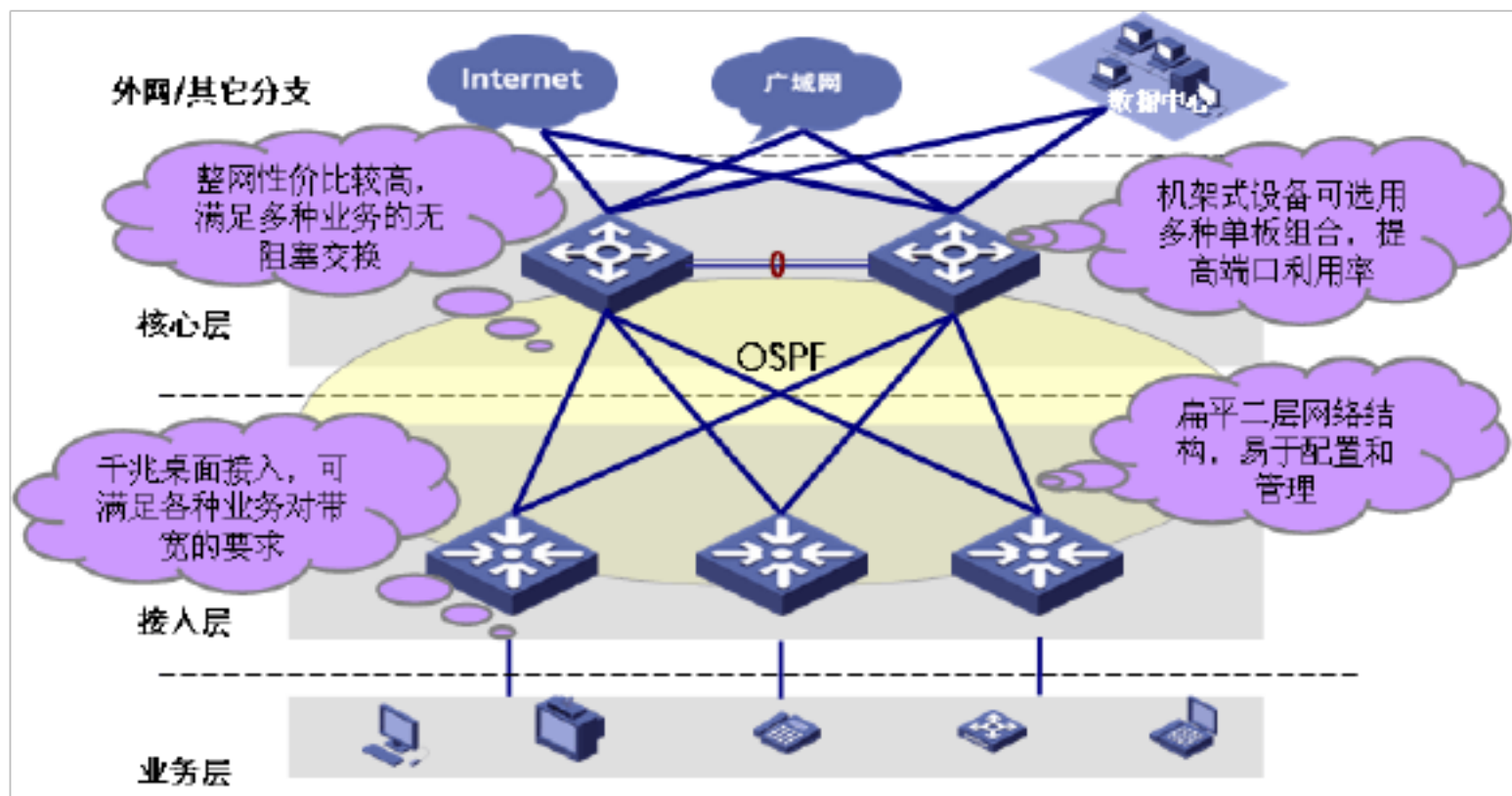
在园区网络整体设计中，采用层次化、模块化的网络设计结构，并严格定义各层功能模型，不同层次关注不同的特性配置。典型的园区网络结构可以分成二层：接入层、汇聚层。

1) 接入层：提供网络的第一级接入功能，完成简单的二、三层交换，安全、QoS 和 POE 功能都位于这一层。对于园区网的接入层设备，建议采用千兆三层接入的方式，应该具有线速三层交换、IRF 智能弹性堆叠技术以及高级 QoS 策略等功能。

2) 汇聚层：汇聚来自配线间的流量和执行策略，当路由协议应用于这一层时，具有负载均衡、快速收敛和易于扩展等特点，这一层还可作为接入设备的第一跳网关；对于园区网的汇聚层设备，应该能够承载园区的多种融合业务，能够融合了 MPLS、IPv6、网络安全、无线、无源光网络等多种业务，提供不间断转发、优雅重启、环网保护等多种高可靠技术，能够承载园区融合业务的需求。

2.3 高可靠性

厂区外网高可靠网络设计方案



对于厂区外网网络，接入端口数量不多、但可靠性要求较高；对交换容量、带宽要求较高。我们推荐高速、无阻塞交换千兆两层扁平组网模型。为用户提供千兆接入、支持语音和POE、网络可以运行 OSPF 协议，两层扁平网络结构，易于配置和管理，并能适应用户未来几年网络应用的需要，提供预留容量。

两层简化扁平网络结构，汇聚、核心合为一层，减少了网络设备数量，易于配置和管理，为用户提供千兆桌面接入、支持语音和POE 功能。接入、核心层设备都为机架式，可用多种不同端口类型的单板组合，使用灵活、可扩充性强，节省网络投资。整网带宽较高、稳定可靠、可满足多种业务的无阻塞交换。

2.4 网络总体规划

网络解决方案总体设计以高性能、高可靠性、高安全性、良好的可扩展性、可管理性和统一的网管系统及可靠组播为原则，以及考虑到技术的先进性、成熟性，并采用模块化的设计方法。

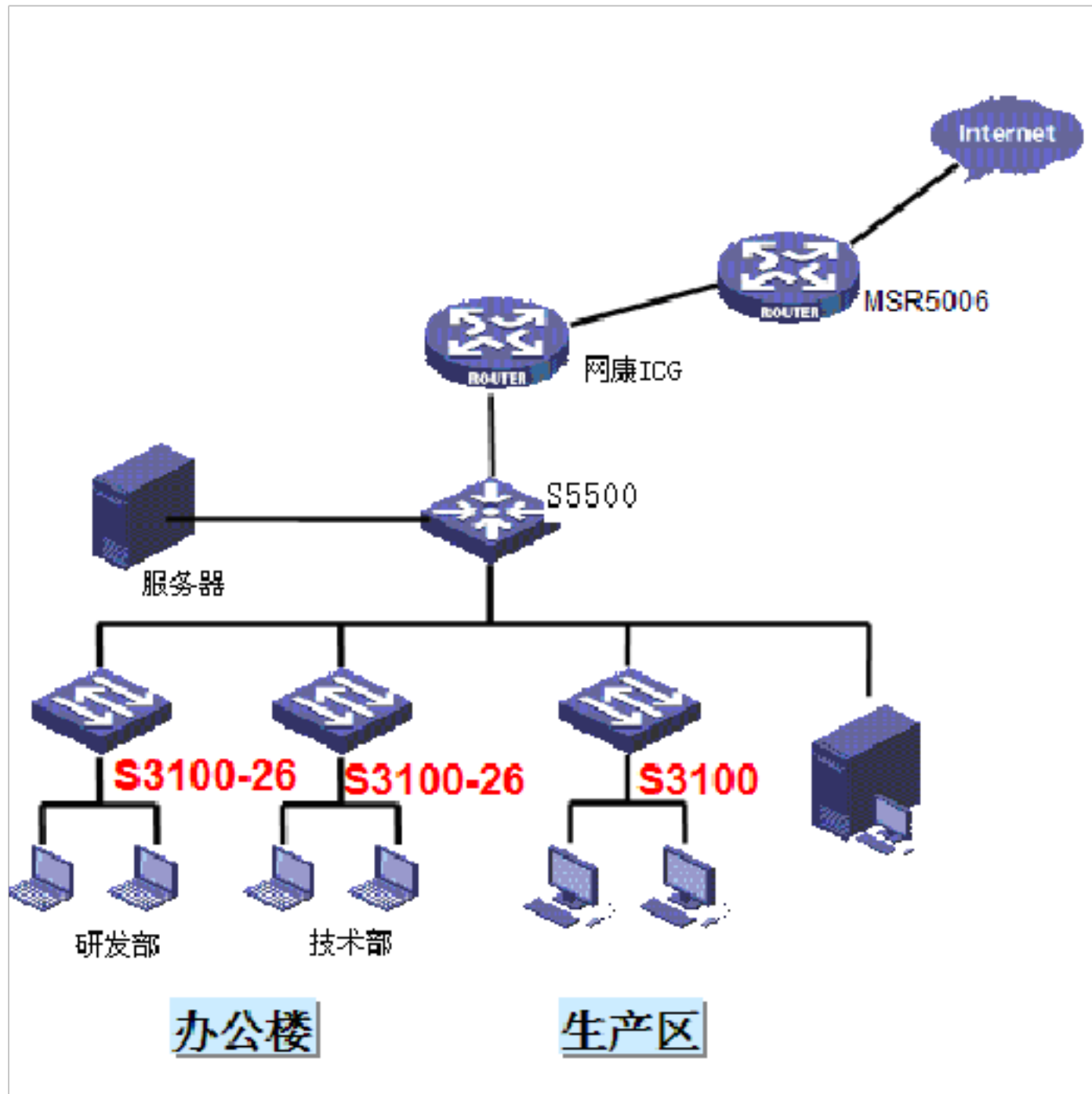
网络主要目的是将网络的性能、带宽、主要网络业务进行全网的建设。网络设计主要包含高品质 IP 核心网模块、智能弹性接入网模块、安全渗透网络模块、网络系统综合管理、自适应无线网、IPv4/v6 地址与路由模块、组播与 QoS 优化模块等主要部分。

新厂区网络均以网线为媒介由办公楼 1 楼机房向厂区各个车间铺设，办公楼主要以网线铺设，在会议室等场所配备无线 AP 设备，所有网线均从各个机房内铺设。

本建网方案为扁平化结构设计，分为核心和接入两层架构设计。

- 1、核心采用 1 台核心三层千兆路由交换机。保证有足够的转发能力
- 2、接入采用千兆二层可智能网管交换机，以千兆双归属到核心。

外网结构如下图所示：



本次方案设计采用二层扁平化方式组网，进一步提高核心网络的可靠性、以及高性能。星形化结构的优势有以下几点：

层次结构清晰，能够将网络进行充分的规划。

星形化组网使网络复杂度降低，网络稳定性提升，网络维护难度降低。

采用星形化结构还具有高扩展性的特点，在今后网络规模扩大时只需要增加相应的接入设备，原有的网络配置可以最大限度得到保留，实现平滑网络扩容。

较高的网络带宽可以满足多种业务无阻塞交换

网络管理者不必再为每种业务配置不同的服务质量策略，简化了设备的配置与维护工作。

第3章 安全管理安全渗透网络设计

在规划网络安全系统时，我们将遵循以下原则，以这些原则为基础，提供完善的体系化的整体网络安全解决方案：

体系化设计原则

通过分析信息网络的网络层次关系、安全需求要素以及动态的实施过程，提出科学的安全体系和安全模型，并根据安全体系和安全模型分析网络中可能存在的各种安全风险，针对这些风险以动态实施过程为基础，提出整体网络安全解决方案，从而最大限度地解决可能存在的安全问题。

全局性、均衡性原则

安全解决方案的设计从全局出发，综合考虑信息资产的价值、所面临的安全风险，平衡两者之间的关系，根据信息资产价值的大小和面临风险的大小，采取不同强度的安全措施，提供具有最优的性能价格比的安全解决方案。

可行性、可靠性原则

在采用全面的网络安全措施之后，应该不会对XX大学原有的网络，以及运行在此网络上的应用系统有大的影响，实现在保证网络和应用系统正常运转的前提下，有效的提高网络及应用的安全强度，保证整个信息资产的安全。

可动态演进的原则

方案应该针对泵阀厂制定统一技术和管理方案，采取相同的技术路线，实现统一安全策略的制定，并能实现整个网络从基本防御的网络，向深度防御的网络以及智能防御的网络演进，形成一个闭环的动态演进网络安全系统。

3.1 网络完全实际办法

网络安全问题的解决，三分靠技术，七分靠管理，严格管理是企业、机构及用户免受网络安全问题威胁的重要措施。事实上，多数企业、机构都缺乏有效的制度和手段管理网络安全。网络用户不及时升级系统补丁、升级病毒库的现象普遍存在；随意接入网络、私设代理服务器、私自访问保密资源、非法拷贝机密文件、利用非法软件获取利益等行为在企业网中也比比皆是。管理的欠缺不仅会直接影响用户网络的正常运行，还可能使企业蒙受巨大的商业损失。

为了解决现有网络安全管理中存在的不足，应对网络安全威胁，北京网康公司的 ICG 上网行为管理设备可以简单易用的完成各种网络审计，应用控制，流量限速等策略。并可以做到以下几点

1、检查：

检查网络接入用户的身份；

检查网络接入用户的访问权限；

检查网络接入用户终端的安全状态；

2、隔离

隔离非法用户终端和越权访问；

隔离存在重大安全问题或安全隐患的用户终端；

3、修复

帮助存在安全问题或安全隐患的用户终端进行安全修复，以便能够正常使用网络；

4、监控

实时监控在线用户的终端安全状态，及时获取终端安全信息；

以上内容仅为本文档的试下载部分，为可阅读页数的一半内容。如要下载或阅读全文，请访问：<https://d.book118.com/878031142031007004>