1

网络安全系统集成项目概述

项目导引

计算机网络技术是计算机技术和通信技术的融合与交集，涉及多个交叉学科领域。如今，各行各业的大、中、小企事业单位都要组建网络，应当以用户的网络应用需求和投资规模为出发点，综合应用计算机技术和网络通信技术，合理选择各种软硬件产品，通过网络集成商相关技术人员的集成设计、应用开发、安装组建、调试和培训、管理和维护等大量专业性工作和商务工作，使集成后的网络安全系统具有良好的性价比，满足用户的实际需要，成为稳定可靠的计算机网络系统。网络安全系统集成是一项综合性很强的系统工程，本书主要介绍网络安全系统的规划、设计、组建和维护。

通过本项目的学习，读者将达到以下知识和技能目标:

- 了解网络系统集成的基本过程;
- 掌握网络需求分析的内容和方法;
- 掌握网络工程项目规划和实施步骤;
- 具备理论联系实际和团队协作能力。

项目描述

某知名外企 ABC 公司步入中国，在重庆建设了自己的中国总部。为满足公司经营、管理的需要，准备建立公司信息化网络。ABC 公司总部设有市场部、财务部、人力资源部、企划部 4 个部门，并在上海、广州两地各设立一个公司分部。为了业务的开展，需要安全访问公司

内部服务器。根据 ABC 公司的建网需求，在经过竞争激烈的招投标后，从事网络工程及系统集成业务的川海高新技术有限公司承接了 ABC 公司网络组建项目，目前进入了项目的启动阶段。按照 ABC 公司网络的设计要求，为了确保网络部署成功，需要分析用户需求、网络设备选型，并制定项目实施流程。在本项目背景下，川海高新技术有限公司将为 ABC 公司的企业网络进行整体规划和设计，本书正是在针对中小型企业网络安全集成的背景下开展网络设计与实施之旅的。

任务分解

根据项目要求，将本项目的工作内容分解为两个任务：

- 任务 1：分析企业网络的需求；
- 任务 2：绘制网络拓扑结构图。

1.1 预备知识

1.1.1 网络系统集成的基本过程

1．网络系统集成的概念

网络系统集成的概念含有三个层次，即网络、系统、集成。

（1）“网络”的概念。这里提到的网络，针对的是计算机网络，如校园网、园区网、企业网等。从计算机网络的概念来看，它含有系统集成成分，但是不具有更专业的技术和工艺。

（2）“系统”的概念。系统是为实现特定功能以达到某一目标而构成的相互关联的一个集合体。计算机网络中的计算机、交换机、路由器、防火墙、系统软件、应用软件、通信介质等就体现了一个有机的、协调的集合体。

（3）“集成”的概念。集成是将一些孤立的事物和元素通过某种方式集中在一起，产生有机的联系，从而构成一个有机整体的过程和操作方法。因此，集成是一种过程、方法和手段。

到目前为止，关于网络系统集成还没有一个严格的定义。一种较为通用的定义是：以用户的网络应用需求和投资规模为出发点，合理选择各种软件产品、硬件产品和应用系统等，并将其组织为一体，能够满足用户的实际需要，具有性价比优良的计算机网络系统的过程。

从网络系统集成的通用定义可知，网络系统集成包含以下要素：

（1）目标：系统生命周期中与用户利益始终保持一致的服务。

（2）方法：先进的理论+先进的手段+先进的技术+先进的管理。

（3）对象：计算机及通信硬件+计算机软件+计算机使用者+管理。

（4）内容：计算机网络集成+信息和数据集成+应用系统集成。

2．网络系统集成的体系结构

网络系统集成的体系框架用层次结构描述了网络系统集成涉及的内容，目的是给出清晰的系统功能界面，反映复杂网络系统中各组成部分的内在联系，如图 1-1 所示。

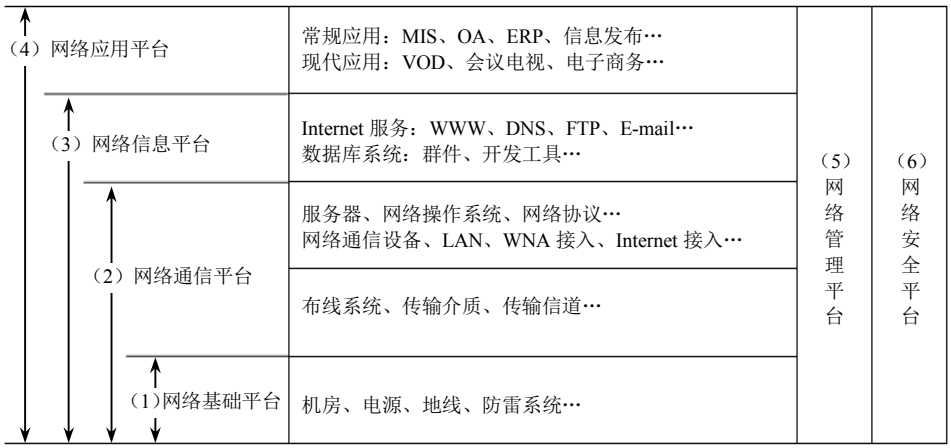

图 1-1　网络系统集成体系架构

（1）网络基础平台。

网络基础平台是指为了保障网络安全、可靠、正常运行所必须采取的环境保障措施。主要考虑计算机网络的结构化布线和机房、电源等环境问题。

（2）网络通信平台。

选择成熟的网络软硬件产品，使用开放的网络通信协议 TCP/IP，依据网络互联规则，进行网络设备的布局和配置，提供数据通信的交换和路由功能。

（3）网络信息平台。

网络信息平台提供支撑网络应用的数据库技术、群件技术和分布式中间件等，以信息沟通、信息发布、数据交换、信息服务为目的，为设计、配置和实现电子邮件（E-mail）、WWW、文件传送（FTP）和域名（DNS）等 Internet 服务。

（4）网络应用平台。

网络应用平台容纳各种应用服务，直接面向网络用户。可以选用成熟的网络应用软件，也可以开发适用的应用软件，例如，用于学校的教学管理系统、企业 OA 系统等。

（5）网络管理平台。

网络管理平台是指网络系统所采用的网络管理措施，涉及网络管理工作站、网管代理、网络管理协议、管理信息库以及有关技术实现。网络管理平台因所采用网络设备的品牌和型号的不同而不同，因此在组建一个网络时，尽量选用同一厂商的网络产品。

（6）网络安全平台。

网络安全贯穿于系统集成体系架构的各个层次。网络的互通性和信息资源的开放性都容

易被不法分子钻空子；不断增长的网络应用，使得安全更让人放心不下。作为系统集成商，在网络安全方案中一定要给用户提供明确的、详实的解决方案，其主要内容是防信息泄露和防黑客入侵。

3. 网络系统集成的基本过程

网络系统集成是一项综合性很强的系统工程，其实施的全过程包括商务、管理和技术三大方面的行为，这些行为交替或混合地执行，需要用户（客户）、系统集成商、产品生产商、供货商、应用软件开发商、施工队以及工程监理等各种人员的相互配合。

通常，从技术层面，按时间推移，将网络系统集成过程粗略分为：用户需求分析、逻辑网络设计、物理网络设计、网络安装与调试、网络验收与维护等，如图 1-2 所示。这一划分方法指出了设计和实现网络系统的阶段划分和各阶段之间的联系，体现了系统化的工程方法，方便了设计和施工，同时强调了技术文档的作用，各部分的反馈联系给出了网络工程实施的灵活性和适应性，同时具有加快网络系统建设速度、分工明确、职责清晰、提供交钥匙解决方案，实现标准化配置所选取的设备，以及建设方法具有开放性等特点。下面对网络系统集成过程的各项任务进行介绍。

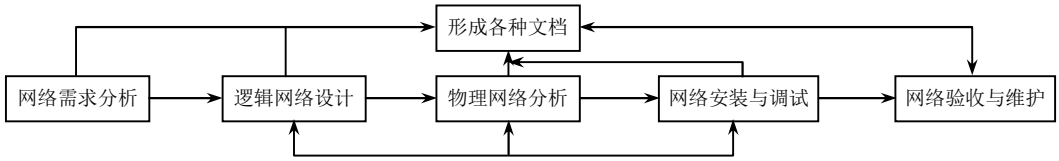

图 1-2　网络系统集成过程模型

（1）网络需求分析。

网络需求分析用来确定该网络系统要支持的业务、要完成的网络功能、要达到的性能等。需求分析的内容涉及到三个方面：网络的应用目标、网络的应用约束、网络的通信特征，这需要全面细致地勘察整个网络环境。网络需求包括：网络应用需求、用户需求、计算机环境需求、网络技术需求。

（2）逻辑网络设计。

什么是逻辑设计？可以用生活中做一双布鞋为例，给出类似的比喻。假设要为某一个人做一双布鞋，则先照他的脚画个“鞋样”，这个形成“鞋样”的过程就是逻辑设计。逻辑设计主要包含四个步骤：确定逻辑设计目标、网络服务评价、技术选项评价、进行技术决策。逻辑网络设计需要确定的内容有：网络拓扑结构是采用平面结构还是采用三层结构、如何规划 IP 地址、采用何种路由协议、采用何种网络管理方案，以及在网络管理和网络安全方面的考虑。

（3）物理网络设计。

什么是物理网络设计？用生活中做布鞋的例子来比喻，就是根据“鞋样”去做鞋子，选择鞋底、鞋面材料，并按工序制作鞋子。物理网络设计涉及网络环境的设计、结构化布线系统设计、网络机房系统设计、供电系统的设计，以及具体采用哪种网络技术，网络设备的选型，

选用哪个厂商生产的哪个型号设备。

（4）网络安装与调试。

网络安装与调试是依据逻辑设计和物理设计的结果，按照设备连接图和施工阶段图进行组网。在组网施工过程中进行阶段测试，整理各种技术文档资料，在施工安装、调试及维护阶段做好记录，尤其要记录下每次出现和发现的问题是什么，问题的原因是什么，问题涉及到哪些方面，解决问题所采用的措施和方法，以后如何避免类似问题的发生，为以后建设计算机网络积累经验。

（5）网络验收与维护。

网络验收与维护的主要工作内容是：给网络节点设备加电，并通过网络连接到服务器运行网络应用程序，对网络是否满足需求进行测试和检查。

1.1.2 网络系统集成实例

1. ABC 公司网络建设概述

ABC 公司是一家从事电子产品研发、销售电子零部件为主的高新技术企业，公司的总部设在重庆，在上海、广州各有一个分部。公司总部设有市场部、财务部、人力资源部、企划部 4 个部门，负责产品的研发、公司的营运管理等；上海分部设有财务部和销售部，负责大陆的产品销售和渠道拓展；广州分部负责港澳地区的产品销售和渠道拓展。

计算机网络在 ABC 公司的业务开展中扮演着非常重要的角色，所有的业务数据全部通过计算机处理，并通过网络在总部和分部之间传递，对网络的可靠性、传递业务数据的安全性有很高的要求。为了使 ABC 公司能适应公司规模的不断扩大和业务的不断拓展，以及员工数量的不断增多和信息应用系统的不断增加，并在未来的几年时间内保持技术的先进性和实用性的需要，公司要求分两期建设网络信息系统。一期工程要求在项目的规划和实施中采用先进的计算机、服务器、网络设备以及系统管理模式，实现公司内部所有资源的合理应用和完善管理，使所有员工都能方便地使用公司内部网络，并能安全、高效地访问公司内部的网络应用服务和 Internet。

2. ABC 公司网络整体需求

ABC 公司决定对当前的总部和分部的办公网络进行建设，以提高公司的办公效率，并降低公司的营运成本。为此召开了信息化建设会议，讨论公司网络建设目标及其他一些细节，得出以下具体需求：

（1）公司网络按照部门进行网段划分，同时保证部门间的广播隔离。

（2）在网络带宽需求方面，确保网络带宽主干千兆位，百兆位到桌面。

（3）在公司的局域网内部，对于网络可靠性要求比较高的部门，其网络必须要有冗余机制，避免单点故障而导致全网瘫痪。而这种冗余机制，对用户要求透明，即不能为了提高网络可用性而增加终端用户的使用难度。

（4）公司网络所有用户能接入 Internet，以保证公司用户通过互联网进行资料查询，将公司内部的公共服务器发布到公网上，以便公网用户随时访问，提高公司的外部形象。

（5）公司总部和分部内网运行动态路由协议，并且要求能实现网络互通。

3．ABC 公司网络功能分析

结合 ABC 公司用户单位的信息及网络需求进行网络功能分析，即可确定网络应具备的功能及涉及到的协议，具体如下：

（1）为了做到总部和分部各部门二层隔离，需要在交换机上划分 VLAN。

（2）为了保障二层链路的冗余和负载均衡，需要在交换机上配置 MSTP 协议。

（3）为了实现网络三层链路的冗余和负载均衡，需在交换机上使用 VRRP 协议。

（4）为了提高网络收敛速度，保障核心网络链路带宽，实现流量的负载均衡，需在核心层交换机上做链路聚合。

（5）因公司网络规模较小，总部和分部的内部网络均采用 RIPv2 协议，用于建立通往内部网络中各个子网的传输路径的路由项。

（6）公司总部和两个分部这三部分通过路由器相连，使用 OSPF 协议用于建立隧道两端经过公共网络的传输路径和内网用户访问 Internet 的传输路径。

（7）为减少广播包对网络的影响，分部网络进行了 VLAN 的划分，使用单臂路由技术实现 VLAN 间的路由。

（8）总部和分部使用 NAT 技术，实现内部用户访问互联网资源，并且为了保障网络资源的合理利用，需要内部用户只能在工作日的上班时间才能访问互联网。

4．ABC 公司网络工程设计

网络工程设计就是要明确采用哪些技术规范，构筑一个满足哪些应用需求的网络系统，从而为用户要建设的网络系统提供一套完整的实施方案。典型的网络工程设计过程包括用户需求分析、逻辑网络设计、物理网络设计、网络部署、网络调试和验收，如图 1-3 所示。

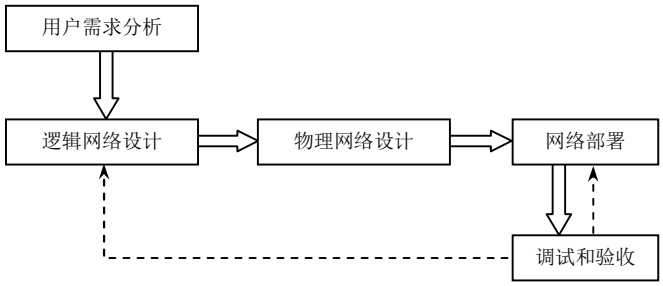

图 1-3　网络设计过程

图中所示的过程中的各个任务往往是迭代循环过程：每个任务为下一任务提供基础，但当前步骤发现问题时，往往需要回溯到上一步，重新改进，直到问题解决。前面已对网络的用户需求进行了详细分析，接下来对网络工程设计过程的后续任务进行介绍。

（1）逻辑网络设计。

1）网络拓扑设计。

目前，绝大多数企业网络采用的是以交换技术为主的经典三层网络架构，由核心层、汇聚

层和接入层三个层面组成，各层分别实现不同的业务功能。考虑网络规模的大小、业务的多样性、功能区的划分等多种因素，尽量简化网络层次，使网络趋近扁平，采用紧缩的二层结构。该架构模式并非必须或一定就是物理连接层次上的减少，而是指网络逻辑层次的简化。它将传统三层架构各个层次模糊的功能区分清晰化，实现了核心业务控制层和网络接入层的分离，实现用户、业务控制的集中化。其中，核心层作为整个网络的控制层，提供集中的管理和业务控制，要求设备性能足够强大；从接入层直接到核心层之间的设备都是使用二层功能。

由于 ABC 业务部门较多，同时还涉及与各分支机构的互联，从网络架构的合理性及易管理性方面考虑，整个 ABC 公司的网络应根据各种应用的功能进行分区域规划设计。在图 1-4 所示的网络拓扑结构中，所采用的分区域规划设计策略划分出了核心交换区域、网络出口区域、办公接入区域、内部服务器区域等。

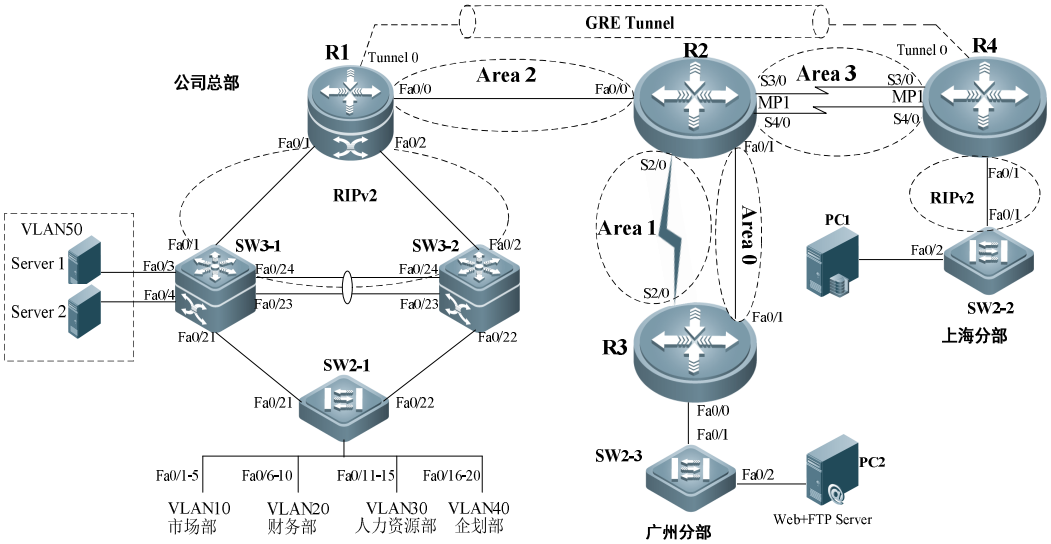

图 1-4　ABC 公司网络结构

这种模块化的区域设计便于后期的运维管理及提高系统的可扩展性，图 1-4 所示的网络拓扑结构具有的独特优势如下：

- 公司总部网络采用了双核心、双链路的设计方案，提供了核心层设备冗余和链路冗余（即存在两台互为冗余的核心交换机，核心交换机与出口路由器之间存在冗余链路，并且每台核心交换机与其他接入层网络设备都存在冗余链路），增强了整个网络平台的高性能、高可靠性和高稳定性。
- 消除了核心层网络的单点故障，提高了网络的可用性，增强了用户对网络造成风险的容忍度。由于两台核心交换机之间使用了虚拟路由器冗余协议（VRRP），对于默认网关设为 VRRP 虚拟 IP 地址的网络终端（如计算机）而言，当任何一台核心交换机失效之后，另外一台核心交换机仍可以处于工作状态，因此任何一台核心设备的失效

都不会导致网络瘫痪。

- 两台核心交换机之间形成了以太网链路聚合通道，可以通过该通道支持负载分担来提高核心层网络的高速转发性能，并且和 VRRP 结合还可以实现负载均衡。
- 从路由层面考虑，路径选择比较灵活，可以有多条备选路径，且易于实现网络流量的负载均衡。由于每台核心交换机与上一级网络的路由器之间都存在两条链路，如果两条链路的带宽相同，就可以采用 RIPv2 等路由协议实现等开销路径上的负载均衡，也可以采用策略路由技术来分摊网络流量。
- 网络出口区域通过路由器连接 ISP 网络，易于实现广域网链路故障自动切换的设计，大大提高了网络出口的可用性。

2）IP 地址规划。

由于要按照部门进行逻辑网段的划分，而且每个部门的员工数量并不相同，因此要求使用 VLSM 技术划分子网。这样做的目的是，一方面确保子网的大小能够符合相应部门或连接对 IP 地址的需求，另一方面又尽量避免 IP 地址的浪费，有关这部分内容的详细设计将在项目 2 中进行介绍。

3）交换策略。

由于要按照部门进行逻辑网段的划分，需在接入层交换机进行 VLAN 的划分，在核心层交换机上进行 VLAN 间的路由设置。对于有较高带宽要求的部门，为确保链路带宽能够满足需求，可以考虑使用 LACP 协议将多条物理链路聚合成一条逻辑链路，以增加链路的带宽。对于网络的可靠性要求比较高的部门，可以在数据链路层引入冗余链路并运行 STP，在主链路正常工作的情况下，逻辑上断开备份链路，而一旦主链路出现故障，备份链路将被启用以保障网络的连通性。有关这方面的内容将在项目 4～5 中进行详细介绍。

4）路由技术。

由于在 IP 地址规划中采用了 VLSM 技术，因此必须要选择无类别的路由选择协议进行不同网段之间的路由。在公司总部和分部的内部网络中运行 RIPv2 协议来实现局域网内部网络各网段之间的路由。对于网络的可靠性要求比较高的部门，可以在网络层引入冗余设备和冗余链路并运行 VRRP 协议，使多台物理网关设备虚拟成一台逻辑网关设备，即使一台物理网关设备出现故障，其他的物理网关设备依然可以保障网络的连通性。有关这方面的详细内容将在项目 6 中进行介绍。

5）广域网技术。

由于在总部和分部之间需要使用到广域网的连接，因此可在广域网连接上配置 PPP 以进行数据链路层的封装，而且在采用 PPP 协议时还可以进行认证的配置以确保对端设备的安全性，这部分内容将在项目 7 中进行介绍。

6）网络设备管理。

为保证网络设备出现故障时能够快速地修复，要求所有网络设备必须能够远程登录进行配置管理，同时必须对所有的网络设备上的操作系统及配置文件进行备份。这部分内容将在项目

3 中进行介绍。

（2）物理网络设计。

物理网络设计是指选择具体的网络技术和设备来实现逻辑设计。这一任务具体包括局域网技术的选择、确定网络设备及选择不同的传输介质（如双绞线、光纤或无线信号等），此时需要确定信息点的数量和具体的物理位置、设计综合布线方案等，这些内容已在“网络综合布线”课程中深入讨论，本书不再涉及，请读者参考其中的内容。

（3）网络部署。

网络部署及具体的施工建设，包括机房装修和综合布线。机房是核心网络设备和服务器的放置场所，对机房的标准化、规范化设计是十分必要的。机房建设主要包括温度和湿度的控制，要防静电、防雷、防晒、防水、防火、防盗，对机房电源和 UPS 电源、机房地板承重等多项内容进行设计。机房建设同样是一门专业技术，本书不做介绍。

网络工程的综合布线施工需要在绘制建筑物平面图，标明建筑群间的距离，确定每个楼宇信息点数量和位置以及通信使用的介质基础上，规划好线缆布线方式，绘制布线施工图，确定具体用料，然后实施，本部分内容已在“网络综合布线”课程中深入讨论，本书不再涉及，请读者参考其中的内容。

（4）调试和验收。

网络工程实施是在网络设计的基础上进行的工作，主要包括软硬件设备的采购、安装、配置、调试和培训等。其中，最为关键的工作是网络互联设备的配置和调试，本书通过具体案例，介绍如何实施网络互联设备的安装、配置、调试过程。网络系统建成后，往往需要 1～3 个月的试运行期，进行总体性能的综合测试。通过系统综合测试，一是为了充分暴露系统是否存在潜在的缺陷及薄弱环节，以便及时修复；二是检验系统的性能是否达到设计标准要求。

1.1.3 网络安全系统集成实例

ABC 公司下属单位多、生产线多，结构复杂。ABC 公司网络将发展为信息承载平台，网上运行的业务将包括 ERP、OA 等。并且，随着接入层网络建设的完善，如何保障网络设备安全、系统安全、各类业务的安全隔离及受控互访等网络安全问题是需要深入探讨的问题。

网络安全系统集成过程一般经历以下过程：在对网络风险分析的基础上，在安全策略的指导下，可以决定所需的安全服务类型，选择相应的安全机制，然后集成先进的安全技术，形成一个全面综合的安全系统，建立相关的规章制度，并对安全系统进行审计评估和维护。

1．ABC 公司网络安全总体要求

ABC 公司在网络安全方面提出 5 个方面的要求：

（1）安全性。全面有效地保护公司网络设备及软件系统的安全，保护数据不因偶然或恶意的破坏遭到更改、泄露和丢失，确保数据的完整性。

（2）可控性和可管理性。可自动和手动分析网络安全状况，实时监测并及时记录潜在的

安全威胁，具有很强的可控性和可管理性。

（3）可用性。在某部分系统出现问题的时候，不影响公司信息系统的正常运行，具有很强的可用性和及时恢复性。

（4）可持续发展。满足公司业务需求和企业可持续发展需求，具有很强的可扩展性和柔韧性。

（5）合法性。所采用的安全设备和技术通过我国安全产品管理部门的合法认证。

2．ABC 公司网络安全工作任务

该公司网络安全项目的工作任务包括以下 4 个方面：

（1）研究该公司的计算机网络系统（包括分支机构、基层生产单位等）的运行情况（包括网络结构、性能、信息点数量和采取的安全措施等），对网络面临的威胁及可能承担的风险进行定性与定量的风险评估。

（2）研究该公司的计算机操作系统（包括服务器操作系统、客户端操作系统等）的运行情况（包括操作系统的版本、提供的用户权限分配策略等），在了解操作系统的最新发展趋势基础上，对操作系统本身的缺陷以及可能承担的风险进行定性与定量的风险评估。

（3）研究该公司的应用系统（包括管理信息系统、办公自动化系统等）的运行情况（包括应用体系结构、开发工具、数据库软件等），在满足各级管理人员、操作人员的业务需求基础上，对应用系统存在的问题、面临的威胁及可能承担的风险进行定性与定量的风险评估。

（4）根据以上的定性与定量的风险评估，结合用户需求和国内外网络安全最新发展趋势，有针对地制定该公司计算机网络系统的安全策略和解决方案，确保该公司计算机网络信息系统安全可靠地运行。

3．ABC 公司信息系统面临的威胁

针对 ABC 公司开展信息化业务的特点，信息系统所面临的主要威胁有以下几点：

（1）ABC 公司信息网络比较开放，终端数量较大，非常容易受到来自 Internet 本身的安全威胁。例如网络蠕虫、网络攻击、垃圾邮件等。此外，企业网络终端没有统一的管理，每台终端上的操作系统安全漏洞补丁不能得到及时更新。这些威胁都会严重影响企业内部网络的正常使用。

（2）对公司自身来说，其科研人员承担了大量的产品研制与开发任务，在开发过程中的数据需要采取严格的保护措施。这部分网络还提供给异地的分支结构的科研人员访问，如果安全性缺失会造成自主知识产权的泄露。

（3）公司网络管理结构相对复杂，没有系统的安全管理和安全事件监控机制。一旦遇到网络蠕虫传播、垃圾邮件拥塞、恶意攻击等紧急情况，没有相应的对策。而且，如果只是通过被动的事件响应，企业必然已经蒙受了损失，从而造成 IT 投资回报无法最大化，总是处在事半功倍的恶性循环中。

4．ABC 公司网络系统安全需求

ABC 公司对网络安全的需求是全方位的、整体的，相应的安全体系也是分层次的，在不同层次反映了不同的安全需求问题。根据网络应用现状和网络结构，ABC 公司的网络安全需

求要从以下几个方面来考虑：

（1）防止网络广播风暴影响系统关键业务的正常运转，甚至导致系统的崩溃。

（2）严格控制各种人员对公司局域网的接入，防止公司内部涉密信息的泄露。

（3）控制公司网络不同部门之间的相互访问。

（4）实现公司局域网与其他网络之间的安全，高效数据访问。

（5）确保广域网数据传输的保密性。

（6）网络系统需要充分考虑到各种网络设备的安全，保障网络系统在受到蠕虫、扫描等攻击时网络设备的稳定性。

5．ABC 公司网络安全风险分析

ABC 公司认为网络系统所要实现网络安全的重点目标为：保障网络中的各种网络设备、系统平台及各类应用业务能够安全可靠地运行。目前，在安全风险分析方面，主要包括如下内容：

（1）整个网络均采用开放的 TCP/IP 协议，面临来自内、外网用户的各类攻击的安全风险。

（2）整个网络建成后将为公司内部的各类业务应用提供服务。由于部门划分细致，所有的企业员工均通过公司的网络平台进行办公，从而可能面临某些少数用户发起的“拒绝服务、病毒传播”等恶意攻击的安全风险。

（3）当网络管理员在利用某些工具（如 Telnet、TFTP 等）对全网进行配置管理时，由于 Telnet 的信息在网络上都是以明文进行传输，从而面临着某些重要信息（如核心交换机等网络设备的配置信息）泄露的安全风险。

（4）由于网络覆盖面大，结构复杂、设备多种多样、应用系统很多，将来在投入运行时可能对公司用户的管理带来较大的困难，同时可能导致整个网络出现安全漏洞隐患。

（5）网络中运行的关键业务，如公司财务往来信息、技术研发资料等，在高质量数据传输的前提下，必须有充分的安全保障。

6．ABC 公司网络安全策略制定

业务需求和风险分析是安全策略制定的主要来源。安全策略规定了用户、管理者和技术人员保护技术和信息资源的义务，也指明了访问机构的技术人员和信息资源人员都必须遵守的规则。安全策略一般包括总体的策略（一般不是某种特定的技术，而是一些与网络运行有关的更加宏观的因素）和具体的规则（组织机构的最佳做法）。ABC 公司建议在网络建设同期制定安全策略来加强对网络安全的限制，各项安全策略应包括以下内容：

（1）授权和陈述范围：规定网络安全策略覆盖的范围。

（2）可接受使用策略：规定对访问网络基础设施所做的限制。

（3）身份识别与认证策略：规定应采用何种技术、设备及其他措施，确保只有授权用户才能访问网络数据。

（4）Internet 访问策略：规定内部在访问 Internet 时需要考虑的安全问题。

（5）内部网络访问策略：规定内部网络用户应如何使用内部网络资源。

（6）远程访问策略：规定远程用户应该如何使用内部网络资源。

7．ABC 公司网络安全机制设计

ABC 公司的网络安全从 3 个层面来进行设计：物理安全、网络系统安全和信息安全。

（1）物理安全机制设计。

首先，要保证网络运行环境的安全，网络机房建设要建立防辐射的屏蔽机柜，把存储重要信息数据的存储设备放在屏蔽机柜中。需要保密的网络采用屏蔽双绞线、屏蔽模块和屏蔽配线架。此外，还需要防雷设备、UPS 的安全配置以及防火系统的配置。

（2）网络系统安全机制设计。

外部网络安全保护机制设计。使用公共子网来隔离内部网络和外部网络，将公共服务器放在公共子网上，在内部网络和外部网络之间使用防火墙，设置一定的访问权限，有效保护网络免受攻击和侵袭。在网络出口处安装专用的入侵检测系统，对网络上的数据信息进行审查和监视。对于特别机密的部门网络，使用 VPN 来创立专用的网络连接，保证网络安全和数据的完整性安全。

内部网络安全保护机制设计。内部网络安全使用 VLAN 来为网络内部提供最大的安全性。通过对网络进行虚拟分段，让本网段的主机在网络内部自由访问，而跨网段访问必须经过核心交换机和路由器，这样保证了网络内部信息安全和防止信息泄露。

（3）信息安全保护设计。

信息安全涉及信息的传输安全、信息存储的安全以及网络传输信息内容的审计等方面。选择加密技术和身份认证技术来保证网络中信息数据的安全。

8．ABC 公司网络安全集成技术

根据前面的详细分析，就本项目而言，ABC 公司采用的网络安全措施主要有以下几种：

（1）身份验证技术。

（2）信息加密技术。

（3）访问控制技术。

（4）虚拟专用网络技术。

（5）网络设备安全加固技术。

（6）网络防病毒技术。

（7）网络安全设备部署。

限于网络防病毒技术、网络安全设备部署内容在“信息安全设备配置与应用”课程中已做深入讨论，本书不再涉及，请读者参考其中的内容。本书内容涉及第（1）～（5），这些内容将在项目 8～11 中进行详细介绍。

1.1.4 网络工程项目实施流程

本项目在网络安全系统集成实训室实施时，将项目实施划分成交换机配置、路由器配置、

网络设备安全配置等 3 大模块，每一模块根据功能的不同，分解成若干不同的工作任务。由于本项目综合性很强且涉及的任务较多，建议该项目在实施过程中，组建一个承担不同任务角色的任务实施小组，并在连续的时间段内完成。

1．项目实施角色任务分配

在项目实施过程中，倡导以工程项目小组的形式组织教学活动，每组大约 4～6 名学生，并选一名学生作为组长承担网络工程项目经理的工作，其余学生充当项目小组网络工程师、服务器工程师、测试工程师等角色，并承担相应工作，如表 1-1 所示。教师充当用户方代表及项目的总规划师和设计师双重角色，负责项目的技术咨询和指导工作，控制课程的组织与开展。

表 1-1　角色任务分配

序号	岗位	工作内容	人数
1	项目经理	负责整个项目的实施质量与实施进度，部署人员分工，掌握施工进度，并组织撰写项目报告	1
2	售前技术工程师	依据网络架构工程师和系统架构工程师提供的解决方案，撰写网络技术方案并提供具体的构建网络的成本预算	1
3	网络架构工程师	依据企业的业务，设计网络基础设施构架和服务器结构，保障企业网络高效、可靠、可扩展	1
4	网络工程师	根据网络设计方案，对项目中的基础设备（路由器、交换机）等进行配置	1
5	服务器工程师	根据网络设计方案，对项目中的所有的应用服务器进行配置	1
6	网络安全工程师	根据网络设计方案，对项目中的网络设备安全进行配置	1
7	网络测试工程师	根据网络设计方案，对整个网络运行状态进行评测，并撰写测试报告	1

2．项目实施设备

本项目实施所需要的接入层设备和计算机终端数量较多，路由器和核心层的设备相对少很多。考虑到本项目实施的重点是路由器和核心交换机这两类设备，因此主要的实训设备如表 1-2 所示。另外，项目实施需要相关软件，并需要安装在不同的服务器和终端上。

表 1-2　项目实训设备清单

设备类型	设备型号	设备数量（台）
路由器	RG-RSR20-18	4
二层交换机	RG-S2328G	3
三层交换机	RG-S3760-24（核心交换机）	2
计算机	联想启天 M330E	4

1.2 项目实施

1.2.1 任务 1：分析企业网络的需求

1．任务描述

根据项目 1 中“项目描述”和实地考察得到的相关数据，对拟新建的 ABC 公司网络安全系统集成项目进行需求分析。在需求调查时考虑了许多方面，本任务主要从网络的一般状况需求、性能需求、管理需求、应用需求和安全需求等五大方面阐述了收集需求分析的过程。ABC 公司网络建设具体需求如下：

（1）按照层次网络拓扑结构进行网络设计和网络实施。

（2）根据公司部门业务的不同进行区划。

（3）总部与分部的业务流量通过专用链路传输，当专用链路损坏后，保证业务流量能够正常安全传输。

（4）允许用户使用合法的全局地址访问互联网，并且内部用户只能在上班时间才能访问互联网。

（5）采用安全技术对接入层用户进行安全限制，并对用户登录进行审计。

（6）构建公司应用服务平台，并把公司相关资源发布到互联网上，实现信息共享。

（7）公司网络采用合适的路由协议，确保全网互联互通。

2．任务要求

（1）教师或非本项目组的学生扮演所选择的调查目标关键人物（网络中心主任、网管、普通员工、客户等），学生扮演项目组的需求调查人员，双方进行沟通。通过面谈、问卷、研究等各种调查手法，对业务、管理、应用、安全、规模、扩展性等各方面进行需求调查。收集、统计调查结果，得出目标网络需求。

（2）对目标网络需求进行分析，按任务实施步骤的要求，填写相关术语于空白处。

3．任务实施步骤

请参考图 1-4，完成如下工作任务。

（1）ABC 公司总部内网在网络结构上分为两层：（　　）和（　　），（　　）全部冗余上行链路，分别级联到 2 台（　　），采用（　　）实现 VLAN 间的路由；同时 2 台（　　）之间使用（　　）进行冗余备份，为了增加两台（　　）的传输速率，需要使用（　　）技术增加带宽，并需要基于（　　）进行负载均衡，保证网络的健壮性和可靠性。同时，内网部分会启用（　　），实现 VLAN 的统一管理和（　　）。

（2）此次网络建设，ABC 公司会增加大量服务器提供各种网络应用服务，所以在公司总部的 LAN 中将所有服务器都分配在（　　）上并单独划分一个（　　）作为服务器的区域，放置网络系统中的 Web、FTP 和 OA 等服务器。

（3）在 ABC 公司内网设计中，由于规模不大，采用（　　）协议，以支持子网间路由功能。将 ABC 公司的总部和分部互联起来的公网，使用（　　）协议的子区域概念，可以减少路由选择协议对路由器的（　　）和（　　）占用，还能降低路由选择协议的通信量，这使得构建一个层次化的互联网络拓扑成为可能。

（4）ABC 公司总部和分部使用（　　）技术，并使用出口路由器外部接口的 IP 地址作为全局地址，实现内部用户可以访问互联网资源。将总部服务器群的多台 Web 服务器发布到互联网，为了提高服务器的高可靠性，要求使用（　　）负载分担功能来实现。

（5）由于 ABC 公司总部与分部之间需要传输服务器群中的业务数据，为了保障业务数据在互联网传输的安全性，使用（　　）技术对数据进行加密，总部与分部的内部网络运行（　　）协议，并且（　　）路由也需要通过互联网进行传输，所以需要使用（　　）隧道传递（　　）路由协议更新。为了保障公司总部与分部骨干网链路安全，需要在公司总部与分部连接的链路上配置（　　），并采用（　　）的验证方式。

（6）为保障网络路由协议更新数据的安全，需要在（　　）或（　　）动态路由协议中配置（　　）或（　　）方式的安全验证。

（7）为保障网络资源的合理利用，需要内网用户只能在工作日的上班时间（周一至周五，9:00～18:00）才能访问互联网，需在出口路由器上使用（　　）进行数据包的过滤，出入互联网的通信量都必须通过公司出口路由器的过滤。为了网络安全的需要，禁止财务部的用户与其他部门的用户进行互相访问。

（8）在服务器群中，部署了 DHCP 服务器，为内网用户动态分配 IP 地址，网络中会存在无赖设备攻击和 DOS 攻击，为了保障 DHCP 服务器的正常工作，需要配置（　　）功能和（　　）功能。为了防止网络中存在（　　）欺骗或（　　）攻击，网络中采用动态（　　）检查技术。

（9）在 ABC 公司网络接入层安全方面，采用（　　）技术，对所有的接入端口配置（　　），如果有违例者，则（　　）或（　　）或（　　），并要求接口配置为（　　），对闲置不用的端口，则（　　）端口。

1.2.2　任务 2：绘制网络拓扑结构图

1．任务描述

按照企业网络的规划要求，绘制 ABC 公司网络拓扑结构图。

2．任务要求

（1）选择合适的网络拓扑图绘制工具。

（2）确定网络拓扑结构设计内容。

（3）根据需求分析的结果和确定的拓扑结构设计内容，按如下规范和参考图 1-4 绘制 ABC 公司网络拓扑结构图：

1）准确呈现网络逻辑结构。

2）网络层次分明易读，设备使用情况及互联情况清晰。

3）网络关键节点信息完善、准确。

4）重点突出，可适当取舍。

5）图例注释完善，拓扑格式统一。

6）符合工业规范（如果是工程制图）。

（4）描述绘制的网络拓扑图的结构特点。

3．任务实施步骤

（1）选择合适的网络拓扑图绘制工具。

小型、简单的网络拓扑结构中涉及的网络设备较少，图元外观也不要求完全符合相应产品的型号，此时，可以通过简单的画图软件（如 Windows 系统中的“画图”软件、HyperSnap 等）进行绘制。而对于一些大型、复杂网络拓扑结构图的绘制则通常采用一些非常专业的绘图软件，如 Visio、亿图图示专家、LAN MapShot 等。在这些专业的绘图软件中，不仅会有许多外观漂亮、型号多样的产品外观图，而且还提供了圆滑的曲线、斜向文字标注，以及各种特殊的箭头和线条绘制工具。

（2）确定网络拓扑结构设计内容。

1）确定网络设备总数。确定网络设备总数是整个网络拓扑结构设计的基础，因为一个网络设备至少需要连接一个端口，设备数一旦确定，所需交换机的端口总数也就确定了。

2）确定交换机端口类型和端口数。一般来说，在网络中的服务器、边界路由器、下级交换机、网络打印机、特殊用户工作站等所需的网络带宽较高，所以通常连接在交换机的高带宽端口。其他设备的带宽需求不是很明显，只需连接在普通的 10/100Mbit/s 快速自适应端口即可。

3）保留一定的网络扩展所需端口。交换机的网络扩展主要体现在两个方面，一个是用于与下级交换机连接的端口，另一个是用于连接后续添加的工作站用户。与下级交换机连接的端口一般是提供高带宽的端口，如果交换机提供了 Uplink（级联）端口，也可直接使用级联端口。

4）确定可连接的工作站总数。交换机端口总数不等于可连接的工作站数，因为交换机中的一些端口还要用来连接那些不是工作站的网络设备，如服务器、下级交换机、网络打印机、路由器、网关、网桥等。

5）确定关键设备连接。把需要连接在高带宽端口的设备连接在交换机可用的高带宽端口上。

6）确定工作站用户计算机和其他设备的连接。

7）与其他网络连接。如果要通过路由器与其他网络连接，如通过 Internet 等。

（3）Visio 绘制网络拓扑图的一般步骤。

1）打开模板开始创建图形元素。

2）将形状拖到绘图页上，然后重新排列这些形状、调整它们的大小和旋转它们。

3）使用连接线工具连接图形元素中的形状。

4）为图形元素中的形状添加文本并为标题添加独立文本。
5）使用格式菜单和工具栏按钮设置图形元素中形状的格式。
6）在绘图文件中添加和处理绘图页。
7）保存和打印图表。
（4）使用 Visio 绘制网络拓扑图时的注意要点。
1）选择合适的图形元素来表示设备。
2）线对不能交叉、串接，非线对尽量避免交叉。
3）线接处及芯线避免断线、短路。
4）对主要设备名称和商家名称加以标注。
5）不同连接介质使用不同的线型和颜色加以注明。
6）标明绘制日期和制图人。

1.3 项目小结

本项目首先介绍了网络系统集成的基本概念、体系结构、集成模型，详细分析了网络工程设计过程，包括用户需求分析、逻辑网络设计、物理网络设计、网络部署、网络调试和验收。每一阶段都需要完成特定目标，在工程进展过程中有可能需要回溯到前一个乃至第一个阶段，最终保证达到用户目标。

本项目还特别介绍了网络层次设计模型，在网络逻辑设计阶段，需要选取相应的设计模型来设计网络拓扑结构。本项目是网络系统集成的方法论，从下一项目开始将介绍具体的实现技术和方法。

1.4 过关练习

1.4.1 知识储备检验

1．填空题
（1）网络系统集成的概念含有三个层次，即（　　）、（　　）、（　　）。
（2）层次化网络设计模型，可以把网络分成 3 个功能层次，分别是（　　）、（　　）和（　　）。
（3）典型的网络工程设计过程包括（　　）、（　　）、（　　）、（　　）和（　　）。
2．选择题
（1）按照拓扑结构可以对网络进行分类，下列选项中（　　）不是网络拓扑结构类型。
A．星型网络　　B．总线型网络
C．以太网　　D．网状型网络
（2）网络系统在试运行期间不间断连续运行的时间不应少于（　　）。

A．1 个月　　B．2 个月

C．3 个月　　D．6 个月

（3）（　）是连接终端设备的网络边缘，用于控制用户对网络资源的访问，其服务和设备位于网络覆盖范围的每栋大楼、每个远程站点和服务器群。

A．核心层　　B．汇聚层

C．接入层　　D．分布层

3．简答题

（1）简述网络系统集成的概念。

（2）简述网络系统集成模型各部分的功能。

（3）简述网络层次化设计模型各部分的主要作用。

1.4.2　实践操作检验

使用 Cisco 系统公司的网络图标工具（可在互联网上搜索下载），重新绘制任务 2 的网络拓扑图，比较使用网络图标工具和 Visio 绘图软件绘制网络拓扑图的优缺点。

1.4.3　挑战性问题

某职业学院人员包括教师、学生、行政人员，由南北校区构成，希望构建一个教师、学生、行政人员能相互通信但相互隔离的网络，需求如下：

（1）在接入层采用二层交换机，并且要采取一定的方式隔离广播域。

（2）核心交换机采用高效能的三层交换机，且采用双核心交换机互为备份方式。接入交换机分别通过 2 条上行链路连接到 2 台核心交换机，由核心交换机实现 VLAN 间的路由。

（3）2 台核心层交换机之间也采用双链路连接，并提高核心交换机之间的链路带宽。

（4）在接入交换机上实现对允许连接终端数量的控制，以提高网络的安全性。

（5）为了提高网络的可靠性，整个网络中存在大量环路，要避免环路可能造成的广播风暴等。

（6）三层交换机上配置路由端口，与路由器之间实现全网互通。

（7）两地办公的路由器之间通过广域网链路连接，并提供一定的安全性。

（8）在路由器上利用少量的公网 IP 地址实现校园网内网到互联网的访问。

（9）在路由器上对内网到外网的访问进行一定的控制，要求行政人员不能访问互联网，学生只能访问 WWW 和 FTP 服务，其余不受限制。

请对该项目进行需求分析、安全策略设计。并据此画出该职业学院的基本网络拓扑图，最终为该校园网设计一个完整的安全解决方案。