第 1 章　网络系统规划和设计

大纲要求：

- 应用需求分析，包括应用需求的调研、网络应用的分析。
- 现有网络系统分析，包括现有网络系统结构调研、现有网络体系结构分析。
- 需求分析，包括功能需求、通信需求、性能需求、可靠性需求、安全需求、维护和运行需求、管理需求。
- 技术和产品的调研及评估，包括收集信息、采用的技术和产品的比较研究、采用的技术和设备的比较要点。
- 网络系统的设计，包括确定协议、确定拓扑结构、确定连接(链路的通信性能)、确定节点(节点的处理能力)、确定网络的性能、确定可靠性措施、确定安全性措施、网络设备的选择、制定选择标准、通信子网的设计、资源子网的设计。
- 新网络业务运营计划。
- 设计评审。
- 安装工作。
- 测试和评估。
- 转换到新网络的工作计划。
- 用户措施，包括用户管理、用户培训、用户协商。
- 制订维护和升级的策略和计划，包括确定策略、设备的编址、审查的时间、升级的时间。
- 维护和升级的实施，包括外部合同要点、内部执行要点。
- 备份与数据恢复，包括数据的存储与处置、备份、数据恢复。
- 网络系统的配置管理，包括设备管理、软件管理、网络配置图。
- 网络系统的监视，包括网络管理协议(SNMP、MIB-2、RMON)、利用工具监视网络性能、利用工具监视网络故障、利用工具监视网络安全(入侵检测系统)、性能监视的检查点、安全监视的检查点。
- 故障恢复分析，包括故障分析要点(LAN 监控程序)、排除故障要点、故障报告的撰写要点。
- 系统性能分析，包括性能要点。
- 危害安全的对策，包括危害安全的情况分析、入侵检测要点、对付计算机病毒的要点。
- 系统评价，包括系统能力的限制、潜在的问题分析、系统评价要点。
- 改进系统的建议，包括系统生命周期、系统经济效益、系统的可扩充性。

1.1 网络系统的需求分析

1.1.1 考点辅导

1.1.1.1 应用需求分析

1. 应用需求的调研

需求分析是构建网络的第一个阶段，通过需求分析，可以帮助网络设计者更好地理解网络功能，更好地评价现有网络，更客观地做出决策；有助于为网络设计者提供更加完善的交互功能和移植功能，使其更合理地使用用户资源等。

应用需求的调研内容包括应用系统性能、信息产生和接收点、数据量和频度、数据类型和数据流向等。

1) 应用系统性能

用户系统中的应用有许多类型，其中一些应用在整个系统中占有相当重要的地位。应用系统的性能往往是用户最为关注的，常见的性能指标包括可靠性/可用率、响应时间、安全性、可实现性和实时性等。

2) 信息产生和接收点

网络上的信息流都有其产生和接收的位置，产生信息的称为源，接收信息的则称为宿(即目的)。在进行需求分析时，分清信息的源和宿是非常必要的。

3) 数据量和频度

网络中的通信类型包括数据、视频信号和音频信号等，不同类型的流量使用不同的量度。数据的流量一般用平均或高峰时每秒传送的位数(比特每秒，简写为 bps)来表示；视频信号的流量用电视通道数来表示，每个通道占 6 MHz 带宽；音频信号的流量则用欧拉数来表示。

频度是指数据在单位时间内传送的次数，不同类型的数据，传送的频度不同。

流量估计应该先分析用户的网络应用，分别估计每种应用产生的分流量，然后再把各种分流量乘以频度，累计得出系统的总流量。

准确的流量估计可以避免网络系统因带宽过窄而形成瓶颈，导致网络吞吐量和性能的下降，因此，对网络通信业务量的估计必须留有足够的余量。

4) 数据类型和数据流向

网络服务一般分为 3 种：共享数据服务、综合语音服务和多媒体应用服务。其中共享数据服务是最常见的业务，综合语音服务主要是电话类业务，而多媒体应用服务则包括语音、图形、图像等多种服务。不同的服务有不同的数据类型。

数据流向是指数据流传输的方向，在客户机/服务器工作模式中，数据的流向既可以是客户机到服务器的，也可以是服务器到客户机的。

因此，网络设计人员必须根据用户具体的应用情况，详细分析网络承载的数据类型和数据流向，合理地分配网络容量。

2. 网络应用的分析

网络的主要功能是通过数据传输实现数据共享，目前应用在科研、教育、金融证券、企业管理、制造、办公自动化、电子商务、家庭娱乐等许多领域。

网络应用按照响应时间可以分为两种：实时应用和非实时应用。不同的应用有着不同的网络响应性能需求，对网络延迟和带宽有不同的影响。

实时应用要求将节点机产生的数据立即传送出去，一般不需要用户干预。实时应用要求信息传输的速率稳定，具有可预测性。令牌传递网络(令牌环网或 FDDI)和面向连接的服务(如 ATM)可以为这些应用提供支持，但在网络分析与设计中通常不考虑实时应用。

通常所说的应用指的是非实时应用，此类应用对网络带宽和数据传输能力的要求比较高，当暂时争用不到网络介质时，只要介质可以承受任何突发性的数据收发任务，非实时应用就不会出现问题。所以，这种应用适合于类似以太网的共享介质网络。

另外，按照应用是否共享，又可以把应用分为独立应用和共享应用两种类型。

不同的应用对网络功能和性能方面的需求不同，网络设计人员应对网络应用需求加以分析，以便确定网络的应用目标及其他相关指标。

1.1.1.2　现有网络系统分析

1. 现有网络系统结构调研

如果需要在已有网络上构建新系统，那么就应该全面了解现有网络情况，尽可能考虑旧系统的利用，这样既可以保护用户原有投资，又能让用户在使用新系统时有一个平滑的过渡，从而大大节省培训的时间和费用。

网络系统的建设一般需要分成几个阶段来实施，每个阶段都是在前期网络的基础之上进行的，不可能完全抛弃现有网络。因此，必须对现有网络进行仔细调研，以考查在原有网络中哪些部分是可以利用的，哪些部分是需要升级的，哪些部分是无用而必须舍弃的。重点考查的内容有以下几个方面。

1)　服务器的数量和位置

服务器是网络中提供专门服务的设备，是网络中的稀缺资源，新网络应该尽量将它们包括进去。在建设新网络之前，需要了解清楚服务器的台数、位置、型号、使用的软件、提供的服务类型以及其他各项性能指标。

2)　客户机的数量和位置

客户机是用户使用网络服务的窗口，有的客户机只供单个用户使用，而有的则供多人使用(如图书馆的查询机)；另外，在客户机上运行的应用系统有差别，对网络服务的需求也不一样。网络中包含的客户机的数量及承担的任务决定了网络的负载，因而有关客户机的信息对网络系统的设计也非常重要，新建网络时必须仔细考虑它们。

3)　使用情况

网络的使用情况包括客户机的数量、访问类型、每天的用户数、每次使用的时间、每次数据传输的数据量、网络拥塞的时间段等，这些数据都可以通过查询网络管理系统的日志文件获得。如果没有完整的日志数据，也可以通过与用户交谈获得有用信息。这些数据虽然不需要十分准确，但其准确性将影响今后网络的设计方案。

4) 采用的协议

协议是网络通信的基础，原有网络可能包含有多种协议，协议间存在着一定的差异。这就需要进行详细的调查，以便新建网络时能够很好地照顾到多种协议间的差异，以方便不同协议数据之间的转换。

5) 通信模式

通信模式就是用户接入网络的方式。网络设计要兼顾各种通信模式。

2. 现有网络体系结构分析

网络体系结构是定义和描述一组用于计算机及其通信设备之间互联的标准和规范的集合，遵循这组规范就可以实现计算机设备之间的通信。目前有两大主流体系结构标准：一个是国际标准 OSI(开放系统互联)参考模型，另一个是工业标准 TCP/IP 模型。

OSI 参考模型通过分层和抽象，将网络划分为七个功能各异的层次，同一端系统中的低层为高层提供服务，不同端系统中的对等层之间进行通信并交换协议数据单元。它是一个开放系统模型，概念清晰，但偏重于理论研究，复杂而不实用，目前实现的范例还较少。

TCP/IP 简化了 OSI 参考模型的分层结构，层次明显减少，实现简单，功能强大，目前为大多数厂商支持，已成为网络通信协议事实上的标准，并已得到普遍的推广。其他还有 IBM 的系统网络体系结构(SNA)和 DEC 的数字网络体系结构(DNA)等。

通过对现有网络体系结构进行分析，可以为建设新网络提供参考依据。同时在设计新网络时也应该照顾到原有网络的体系结构，尽量发挥其优势，而不应该完全抛弃。

1.1.1.3 需求定义

网络系统的需求包括功能需求、通信需求、性能需求、可靠性需求、安全需求、维护和运行需求以及管理需求等，下面逐一介绍。

1. 功能需求

功能需求即网络在用户单位业务中应该提供的功能，可以通过了解用户单位所从事的行业、该单位在行业内的地位以及和其他单位的关系等来确定其功能需求。另外，还可以通过了解项目背景来明确用户单位建网的目的，从而有助于描述详细的功能需求。

2. 通信需求

在网络中，网络通信是个人通信模式和流量的组合。通信模式以发生在节点(客户机)之间的通信方式为基础。通常有以下几种通信方式。

- 对等通信方式。
- 客户机/服务器通信方式。
- 服务器/客户机通信方式。

独立节点之间可以在一种或多种方式下通信，如何选择通信方式取决于网络的资源、节点和应用程序的性能。例如，在对等通信方式下，各工作站之间可共享资源；在客户机/服务器通信方式下，可以访问中央文件服务器上的核心数据库。

1) 对等通信方式

对等通信方式是在一种结构和功能相似的节点之间的通信，通信节点具有相似的应用和通信能力。在该种网络中，每个节点与网络中的其他节点相连接，没有明显的源通信模

式和目的通信模式。

2)　客户机/服务器通信方式

客户机/服务器通信方式是网络中的客户机和服务器之间的通信。客户机可以是任何类型的节点，这些节点可以访问一些共享的资源。服务器在大小和功能上有所不同，既可以是基于 PC 的服务器，也可以是中型计算机和大型计算机。

3)　服务器/客户机通信方式

数据库服务器应用程序使数据从服务器流向客户机。通常情况下，客户机请求比服务器响应所传送的通信量要少。例如，在典型的 Web 方案中，服务器根据客户机浏览器的请求向客户机发送大量的 Web 页面，这就是所说的服务器/客户机分布。

4)　相关指标

为了确定用户的通信需求，需要了解用户单位的建筑物布局、入网站点的分布情况，并记录下述信息。

- 网络中心(或计算中心)及各级设备间的位置。
- 用户数量及其位置。
- 任何两个用户之间的最大距离。
- 用户群组织(即在同一楼里或同一楼层里的用户，尤其注意那些地理上分散，却属于同一部门的用户)。
- 特殊的需求或限制(例如，网络覆盖的地理范围内是否有道路、山丘；建筑物之间是否有阻挡物；电缆等介质布线是否有禁区；是否存在可以利用的介质系统等)。

3. 性能需求

在需求分析中要分析网络的多种性能特性，包括响应时间、延迟、等待时间、利用率、带宽、容量、吞吐量、可用性、可靠性、可恢复性、冗余度、适应性、可伸缩性、效率和费用等。有些需求用户不是很关心，但对于设计者却是必须考虑的。随着计算机网络数量的增长、规模的扩大，如何提高网络性能成为十分重要的问题。与衡量单机系统的性能不同，网络性能是衡量多台计算机系统的性能。了解网络用户的需要，设定恰当的性能目标，合理选择网络结构和组成，便能得到满足用户需求且性能比较好的网络。

网络用户关心的网络性能是能否获得最快的响应，网络管理员关心的网络性能是能否获得最高的资源利用率，两者需要很好地平衡。这种平衡包括两个方面：一方面是性能和价格的折中，另一方面是吞吐量和响应时间的平衡。

4. 可靠性需求

可靠性需求就是用户需要什么样的可靠性。一个系统的可靠性定义为在指定的条件和时间内，系统能够实现指定功能的概率。而整个系统的可靠性又取决于组成系统的各个部件的可靠性。

可靠性指标一般包括平均无故障时间(MTBF)和平均修复时间(MTTR)、可用性和故障率等。

5. 安全需求

1)　安全需求概述

网络安全性包括对物理产品的布局和对过程的操作，合理的物理产品布局与安全设置

可以保护网络和系统的完整性、可行性及可靠性。现代的网络安全性是把基本的网络安全性概念运用在分布式网络环境中。网络安全性的目的是对资源的保护，目前还没有彻底的解决方法。

安全设计包括安全服务和实施两方面。原则上讲，每一个网络系统都具有独立和通用的安全协议，而基于安全服务的安全信息则是存放在管理信息库(MIB)中的，只有授权人员或系统才可访问、修改或删除这些机密信息。通过对网络易损点的识别，可使这些易损点得到保护和监控，要确保安全，应采取一种分层管理策略。

安全性策略的 3 个属性定义为保密性、完整性和可信性。信息损失通常由以下原因引起：更改、破坏和泄露。对网络安全构成威胁的形式有很多，而且它们经常导致网络失常和重要信息的毁坏。

采取何种安全措施需要视用户需要而定，不同单位或一个单位的不同部门要求的安全等级往往是有差异的，并不是安全等级越高越好，较高的安全等级意味着额外的系统开销和高昂的费用。

2) 安全性标准

网络系统是否达到一定的安全性主要依照相关的安全性标准来判断，最早的信息系统安全性标准由美国国防部颁布的黄皮书(TC-SEC-NCSC，可信计算机系统)规定。该手册将 IT 系统划分为 A(A1)、B(B1、B2、B3)、C(C1、C2)、D(D1)4 类，共 7 个安全等级。

(1) D 类安全等级。D 类安全等级只包括 D1 一个级别，D1 的安全等级最低，它只为文件和用户提供安全保护。D1 系统最常见的形式是本地操作系统，或者是一个完全没有保护的网络。

(2) C 类安全等级。C 类安全等级能够提供审慎的保护，并为用户的行动和责任提供审计能力。C 类安全等级可划分为 C1 和 C2 两类。

(3) B 类安全等级。B 类安全等级可划分为 B1、B2 和 B3 三类。B 类系统具有强制性保护功能，这就意味着如果用户没有与安全等级相连，系统就不会让用户存取对象。

(4) A 类安全等级。A 类系统的安全级别最高。目前，A 类安全等级只包含 A1 一个安全类别。A1 类与 B3 类相似，对系统的结构和策略不作特别要求。A1 系统的显著特征是：系统的设计者必须按照一个正式的设计规范来分析系统。对系统进行分析后，设计者必须运用核对技术来确保系统符合设计规范。A1 系统必须满足下列要求：系统管理员必须从开发者那里接收一个安全策略的正式模型；所有的安装操作都必须由系统管理员进行；系统管理员进行的每一步安装操作都必须有正式文档。

欧洲等价的分类手册是 ITSEC(信息技术安全评估标准)。与美国的黄皮书类似，ITSEC 标准目录将 IT 系统划分为 7 个安全等级(E0～E6)，这些等级与黄皮书中的各个等级大致对应。

6. 维护和运行需求

维护和运行是网络系统投入正常运行后的日常管理工作，这项工作主要由网络管理人员承担。网络管理人员通过网络管理系统可以完成系统的配置、监控和统计等事务的处理，有时还要对网络设备进行检修。网络设计人员需要根据用户需求，提供必要的网络管理工具和策略，以方便网络管理人员对整个网络进行管理和维护，提高网络的运行效率，保证

网络的可靠性。

7. 管理需求

从用户的角度来讲，一个网络管理系统应该满足以下要求。

- 同时支持网络监视和控制两方面的能力。
- 能够管理所有的网络协议。
- 尽可能大的管理范围。
- 尽可能小的系统开销。
- 可以管理不同厂家的联网设备。
- 容纳不同的网络管理系统。
- 网络管理的标准化。

在 OSI 网络管理框架模型中，基本的网络管理功能被分为 5 个功能域：配置管理(Configuration Management)、性能管理(Performance Management)、故障管理(Fault Management)、安全管理(Security Management)和计费管理(Accounting Management)。

网络管理的标准化产品包括 ISO 的 CMIS/CMIP(Common Management Information Service/Common Management Information Protocol)、Internet 体系结构委员会(Internet Architecture Board，IAB)的 SNMP 和管理信息库(MIB)，这些内容将在第 5 章详细介绍。

1.1.2　典型例题分析

例 1　【说明】(2017 年上半年下午试题一)

某企业网络拓扑如图 1-1 所示，中国电信和中国移动双链路接入，采用硬件设备实现链路负载均衡：主磁盘阵列的数据通过备份服务器到备份磁盘阵列。请结合下图，回答相关问题。

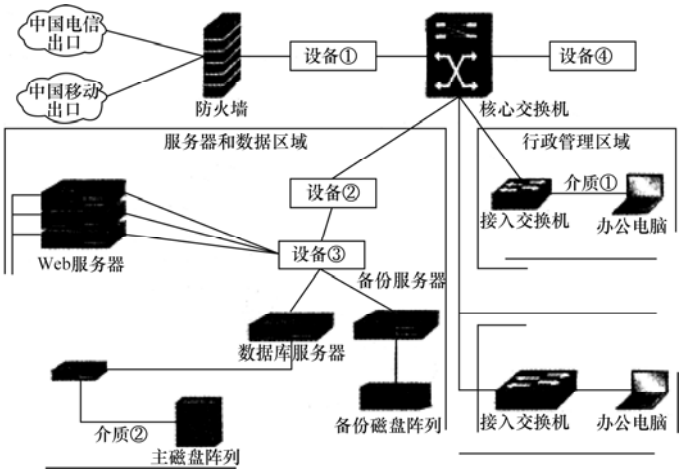

图 1-1　某企业网络拓扑

【问题 1】(共 6 分)

图 1-1 中，设备①处部署 (1) ，设备②处部署 (2) ，设备③处部署 (3) 。(1)～

(3)备选答案(每个选项限选一次):

A. 入侵防御系统(IPS)　　B. 交换机　　C. 负载均衡

【问题 2】(共 4 分)

图 1-1 中，介质①处应采用 (4) ，介质②处应采用 (5) 。

(4)～(5)备选答案(每个选项限选一次):

A. 双绞线　　B. 同轴电缆　　C. 光纤

【问题 3】(共 4 分)

图 1-1 中，为提升员工的互联网访问速度，通过电信出口访问电信网络，移动出口访问移动网络，则需要配置基于 (6) 地址的策略路由；运行一段时间后，网络管理员发现电信出口的用户超过 90%，网络访问速度缓慢，为实现负载均衡，网络管理员配置基于 (7) 地址的策略路由，服务器和数据区域访问互联网使用电信出口，行政管理区域员工访问互联网使用移动出口，生产业务区域员工使用电信出口。

【问题 4】(共 6 分)

1.图 1-1 中，设备④处应为 (8) ，该设备可对指定计算机系统进行安全脆弱性扫描和检测，发现其安全漏洞，客观评估网络风险等级。

2.图 1-1 中， (9) 设备可对恶意网络行为进行安全检测和分析。

3.图 1-1 中， (10) 设备可实现内部网络和外部网络之间的边界防护，依据访问规则，允许或者限制数据传输。

答案:

【问题 1】(1) C　(2) A　(3) B

【问题 2】(4) A　(5) C

【问题 3】(6) 目的　(7) 源

【问题 4】(8) 漏洞扫描设备　(9) IPS　(10) 防火墙

解析:

【问题 1】综合分析可知设备 3 是交换机，那么设备 2 为 IPS，设备 1 为负载均衡。

【问题 2】介质 1 连接接入交换机和用户，故为双绞线。介质 2 连接 FC 交换机和磁盘阵列，应为光纤。

【问题 3】访问电信网络通过电信出口，移动网络通过移动出口，这是通过访问目的来区分的，故是基于目的地址的策略路由。而后根据访问人群的划分更改为基于源地址的策略路由。

【问题 4】漏洞扫描通常是指基于漏洞数据库，通过扫描等手段，对指定的远程或者本地计算机系统的安全脆弱性进行检查，发现可利用的漏洞的一种安全性检测行为。在图 1-1 中 IPS 设备对恶意网络行为进行分析。防火墙设备则为内外网之间的安全保护屏障。

例 2　【说明】(2016 年下半年下午试题二)

图 1-2 是某互联网企业网络拓扑，该网络采用二层结构，网络安全设备有防火墙、入侵检测系统，楼层接入交换机 32 台，全网划分 17 个 VLAN，对外提供 Web 和邮件服务。数据库服务器和邮件服务器均安装 CentOS 操作系统(Linux 平台)，Web 服务器安装 Windows 2008 操作系统。

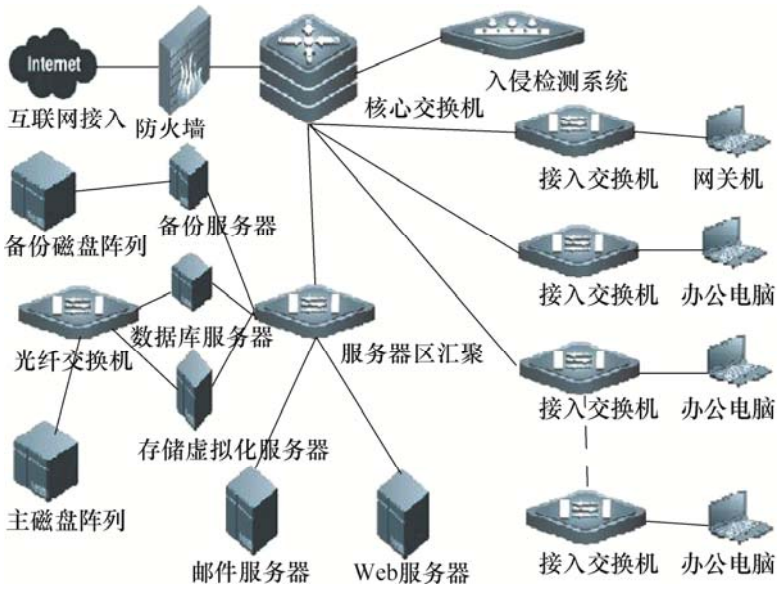

图 1-2　某互联网企业网络拓扑

【问题 1】(6 分)

SAN 常见方式有 FC-SAN 和 IP-SAN，在图 1-2 中，数据库服务器和存储设备连接方式为 (1) ，邮件服务器和存储设备连接方式为 (2) 。虚拟化存储常用文件系统格式有 CIFS、NFS，为邮件服务器分配存储空间时应采用的文件系统格式是 (3) ，为 Web 服务器分配存储空间时应采用的文件系统格式是 (4) 。

【问题 2】(3 分)

该企业采用 RAID5 方式进行数据冗余备份，请从存储效率和存储速率两个方面比较 RAID1 和 RAID5 两种存储方式，并简要说明采用 RAID5 存储方式的原因。

【问题 3】 (8 分)

网络管理员接到用户反映，邮件登录非常缓慢，按以下步骤进行故障诊断：

1. 通过网管机，利用 (5) 登录到邮件服务器，发现邮件服务正常，但是连接时断时续。

2. 使用 (6) 命令诊断邮件服务器的网络连接情况，发现网络丢包严重，登录服务器区汇聚交换机 SI，发现连接邮件服务器的端口数据流量异常，收发包量很大。

3. 根据以上情况，邮件服务器的可能故障为 (7) ，应采用 (8) 的办法处理上述故障。

(5)～(8)备选答案：

(5) A. ping　　B. ssh　　C. tracert　　D. mstsc

(6) A. ping　　B. telnet　　C. tracet　　D. netstat

(7) A. 磁盘故障　　B. 感染病毒　　C. 网卡故障　　D. 负荷过大

(8) A. 更换磁盘　　B. 安装防病毒软件，并查杀病毒

C. 更换网卡　　D. 提升服务器处理能力

【问题 4】 (3 分)

上述企业网络拓扑存在的网络安全隐患有：__(9)__、__(10)__、__(11)__。

(9)～(11)备选答案：

A. 缺少针对来自局域网内部的安全防护措施

B. 缺少应用负载均衡

C. 缺少流量控制措施

D. 缺少防病毒措施

E. 缺少 Web 安全防护措施

F. 核心交换机到服务器区汇聚交换缺少链路冗余措施

G. VLAN 划分太多

答案：

【问题 1】(1) FC-SAN (2) IP-SAN (3) NFS (4) CIFS

【问题 2】

(1) 存储效率上，RAID5 的存储利用率为$(n-1)/n$，RAID1 的存储利用率为 50%，RAID5 的存储效率高。

(2) 存储速率上，RAID5 的速率快于 RAID1。

原因：RAID5 具有数据安全，读写速度快，空间利用率高、成本低的特点。

【问题 3】(5) B (6) A (7) B (8) B

【问题 4】(9) A (10) D (11) E

解析：

【问题 1】

1. SAN 主要包含 FC-SAN 和 IP-SAN 两种。

1) 存储区域网络(Storage Area Network，SAN)：存储设备组成单独的网络，大多利用光纤连接，采用光纤通道协议(Fiber Channel，FC)。服务器和存储设备间可以任意连接，I/O 请求也是直接发送到存储设备。光纤通道协议实际上解决了底层的传输协议，高层的协议仍然采用 SCSI 协议，所以光纤通道协议实际上可以看成是 SCSI over FC。

2) IP-SAN：由于 FC-SAN 的高成本使得很多中小规模存储网络不能接受，一些人开始考虑构建基于以太网技术的存储网络。但是在 SAN 中，传输的指令是 SCSI 的读写指令，不是 IP 数据包。iSCSI(互联网小型计算机系统接口)是一种在 TCP/IP 上进行数据块传输的标准。它是由 Cisco 和 IBM 两家公司发起的，并且得到了各大存储厂商的大力支持。iSCSI 可以实现在 IP 网络上运行 SCSI 协议，使其能够在诸如高速千兆以太网上进行快速的数据存取备份操作。为了与之前基于光纤技术的 FC-SAN 区分开来，这种技术被称为 IP-SAN。iSCSI 继承了两大最传统技术：SCSI 和 TCP/IP 协议。这为 iSCSI 的发展奠定了坚实的基础。

2. CIFS 和 NFS。

1) CIFS(Common Internet File System)是由 Microsoft 在 SMB 协议的基础上发展并扩展到 Internet 上的协议。它和具体的 OS 无关，在 UNIX 上安装 Samba 后可使用 CIFS。

2) NFS(Network File System)即网络文件系统，由 Sun 公司开发，主要用于 UNIX 和类 UNIX 系统，在 Windows 上使用则需要安装客户端软件进行认证时的指令映射。

将 NFS 置于 Windows 上，有两种选择：Microsoft Services for UNIX (SFU)和 DiskShare。CIFS 采用 C/S 模式，基本网络协议：TCP/IP 和 IPX/SPX。

【问题 2】

RAID1 阵列由磁盘对组成，因为需要用作备份，在数据的安全性方面是最好的，但是只能利用磁盘总容量的一半，存储效率只有 50%，存储性能不高。RAID5 是一种存储性能、数据安全和存储成本兼顾的存储解决方案，以 n 块硬盘构建的 RAID5 阵列可以有 $n-1$ 块硬盘的容量，磁盘空间利用率能达到$(n-1)/n$。在 RAID5 上，读/写指针可同时对阵列设备进行操作，提供了更高的存储性能。

【问题 3】

1. 远程登录到服务器做诊断或配置可以通过 Telnet、SSH、远程桌面等方式。

Telnet 是 C/S 构架的服务，登录后是命令行界面，客户端和服务器间的传输无私密性保护，一般用于管理网络设备(如路由器交换机)、Linux 或 UNIX 服务器主机。

SSH 和 Telnet 类似，但是提供私密性保护。

远程桌面管理，是登录上服务器的图形化界面配置，一般用于登录 Windows 服务器主机，也可以用于登录 Linux 的图形化界面配置，但是需要 Linux 安装桌面组件。

2. 使用命令诊断邮件服务器的网络连接情况，发现网络丢包严重，根据“丢包”的文字描述，应该是 ping 命令。

3. 交换机上某个端口数据流量异常，收发包量很大，可能的原因很多，比如病毒、端口或网卡物理故障(不是彻底损坏)、环路导致广播风暴等，但是只有木马类病毒才会故意隐藏自己而让服务正常，只是可能木马窃取数据占用了大量带宽导致一些异常。而其他故障都会导致服务不正常，所以依据本题文字描述，登录服务器成功，服务正常，综合考虑，病毒的可能性最大。

【问题 4】

本题说的是“网络安全隐患”，关于网络的安全隐患和性能以及可用性一定要区别清楚，负载均衡、流量控制、划分 VLAN 都是性能方面的问题，链路冗余是可用性方面的问题，而防病毒、针对 Web 的安全防护措施才是安全方面的问题，故 B、C、F、G 体现的是关于网络可靠性、可用性的特征。

1.1.3　同步练习

1. 网络开发设计的整个过程分为哪几个阶段？每个阶段各有什么任务？请用流程图的方式说明。

2. 网络工程是一项复杂的系统工程，一般可分为网络规划、网络设计、工程实施、系统测试验收和运行维护等几个阶段。网络规划是在需求分析的基础上，进行系统可行性分析和论证，以确定网络总体方案。网络规划阶段任务完成之后转入下一阶段，即网络设计阶段。

【问题】

(1)　简述网络规划阶段需求分析的方法和解决的问题(控制在 100 字以内)。

(2)　在需求分析过程中应对已有网络的现状及运行情况作调研，如果要在已有的网络上作新的网络建设规划，如何保护用户已有投资(控制在 100 字以内)?

1.1.4　同步练习参考答案

1. **答案：**

网络开发的过程一般分为 5 个阶段，具体流程图如图 1-3 所示。

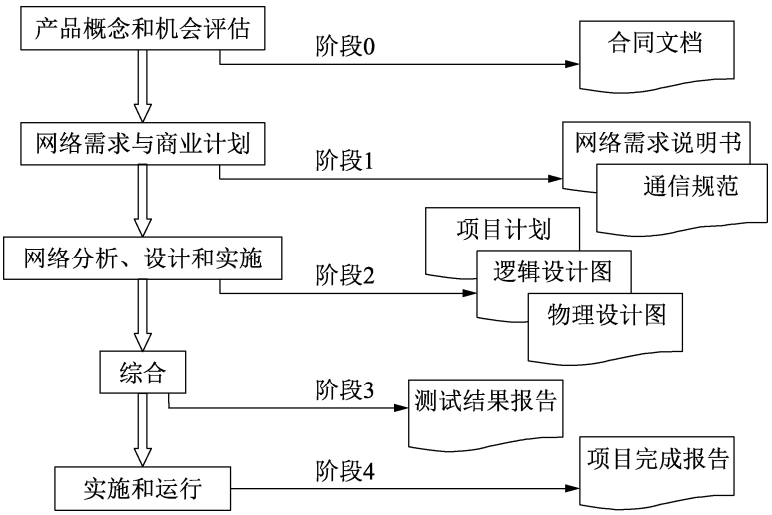

图 1-3　网络开发流程图

2. 答案：

(1) 先采用自顶向下的分析方法，调查用户单位建网的背景、必要性、上网的人数、信息量等，从而确定建网目标。接着进行纵向的、深入的需求分析和调研，为网络设计提供依据。

(2) 在设计新系统时要充分考虑利用已有系统的资源，让原有系统纳入到新系统中运行，不要“推倒重来”，也可以把已有系统的设备降档次使用。

1.2　网络系统的设计

1.2.1　考点辅导

1.2.1.1　网络设计的基本原则

网络系统性能要求高、技术复杂、涉及面广，在其规划和设计过程中，为使整个网络系统更合理、更经济、性能更好，需要遵守以下设计原则：性价比高；统一建网模式；统一网络协议；保证可靠性和稳定性；保证先进性和实用性；具有良好的开放性和扩充性；在一定程度上保证安全性和保密性；具有良好的可维护性等。

由于不同单位的网络发展水平和应用需求差异很大，而且网络的组网方法和备选设备种类繁多，因此设计时必须根据具体情况进行规划。

1.2.1.2　收集信息

在网络开发过程中，一旦设计者了解网络需求之后，便可进入逻辑网络设计阶段。进入这一阶段的前提是设计者必须有详尽的需求报告和通信规范。

在网络设计的初始阶段，网络设计人员首先需要对用户的需求了如指掌，然后着手进行网络设计前的准备工作。准备工作首先从收集信息(这些信息包括技术层面的和产品层面的)开始，收集信息一定要以满足用户需求为目标，为网络设计和实施服务。

收集信息的途径有很多种，主要有以下几个。

- 通过参观访问其他单位获得。
- 通过厂商资料和宣传品获得。
- 通过 Internet 获得。
- 通过投标公司获得。
- 通过其他渠道获得。

对于收集到的信息需要分类整理，参照需求分析说明书找到可靠的且满足需要的技术、产品和设备，然后进一步分析研究。

1.2.1.3　采用的技术和产品设备的比较研究

任何设计都需要权衡，其中最常见的是成本与性能的权衡。如果要增强性能，成本就会明显上升。在考虑成本时，设计者不仅要考虑运行的成本，还要考虑实施网络的成本。图 1-4 说明了技术选择与成本之间的关系。

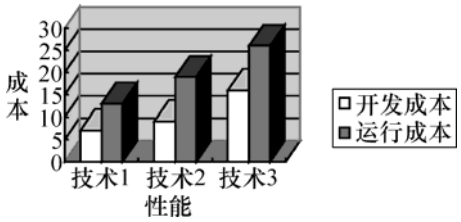

图 1-4　成本/性能示意图

根据需求收集阶段初期收集到的基本需求，可以预测项目的成本，同时也可确定开发成本和运行成本的阈值。在选择技术时，设计者通常也会提供备选的技术及相关的成本，选择的结果一般会超出所确定的水平。给定一个设计目标时，设计者必须考虑以下方面。

- 最低的运行成本。
- 最少的安装费用。
- 最高的性能。
- 最大的适应性。
- 最大的安全性。
- 最高的可靠性。
- 最短的故障时间。

以上目标不可能同时达到，需要仔细权衡。其中技术上的考虑处于核心地位，技术上的考虑包括后台通信、连接类型和可伸缩性等方面。

1. 后台通信

后台通信通常是指广播通信，与应用间的通信不同，它是发生在网络上的通信。考虑后台通信是因为它可能会大大增加网络的容量要求。在典型的情况下，后台通信占全部通信的 5%～20%。

通常遇到的后台通信都是基于路由广告协议(Routing Advertisements Protocol，RAP)和服务广告协议(Service Advertisements Protocol，SAP)。在网络上向其他设备做服务广告的服

务器、路由器和打印机将产生这种类型的通信。如果网络协调不当，后台通信就会在整个网络通信中占很大一部分。

2. 连接类型

连接类型是逻辑设计时必须考虑的另一个问题。在无连接和面向连接的协议间需要一个权衡。有些协议，如 IP 协议是无连接的，在这类协议中，不用花时间来建立虚拟电路，只需简单地通过网络来发送分组。用无连接协议传送信息比起面向连接的协议来说，每个分组的系统花费都要多一些。

面向连接的协议(如 ATM)需要花费较长时间来建立连接。一旦建立起了连接，通信的效率就会高许多。面向连接的协议通常同时提供多层次的服务，当应用需要以相同的速率发送大量的信息时最适合使用面向连接的协议。如果应用是突发的而且不需要多层次服务，则用无连接协议最合适。

3. 可伸缩性

设计者同样需要考虑网络的可伸缩性，即考虑现在以及将来网络所需的容量。容量设计必须易于调整以适应单位、应用以及网络的适当增长。例如，当设计者实施以太网接口卡(NIC)和非屏蔽双绞线(UTP)连接时，即使只实现 10 Mbps 的以太网，也可能选择购买 10/100 Mbps 的网卡和 5 类线。这样做，不更换接口卡和线缆平台就能升级到百兆。

要想作出具体的技术选择，需要设计者详细考虑每种方法的优缺点。考虑的不同技术类型和重点内容如下。

- 物理层。
- 网络互联。
- 逻辑网络图。
- 虚拟网策略。
- 现代广域网技术。
- 网络管理。
- TCP/IP 地址设计。
- 网络安全。
- 防火墙。
- 备选设计。

1.2.1.4 确定连接

除了考虑各种类型的网络的传输特性及优缺点外，还需要考虑在实际网络环境中如何评估各类介质。以下列举了必须要考虑的主要环境因素，并对不同的条件推荐了适当的传输介质。

1) 高 EMI 或 RFI 区域

如果环境内拥有许多电能源，应尽可能使用抗噪性最好的介质。Thick Ethernet(粗缆以太网)和光缆在目前是抗噪性最好的介质。

2) 拐角和狭窄空间

如果环境要求电缆在拐角处弯曲或穿过狭窄空间，应该尽可能使用最灵活的传输介质，如 STP 和 UTP。

3)　距离

如果环境要求远距离传输，应考虑光缆或无线介质，也可以使用双绞线或同轴电缆，但它们更易受衰减和干扰的影响，同时需要中继器。

4)　安全性

如果某个机构对传输安全性要求较高，应选择具有最高安全性的传输介质，光缆和红外介质对这种环境都是很好的选择。

5)　既有体系结构

如果为一个已有的电缆设备增加电缆，应考虑它将如何与已有电缆设备相互作用以及两者之间所需的连接性硬件。选择的介质应与机构以前安装的设备相适应。

6)　发展

应弄清本单位准备如何扩展网络，以及在设计布线时是如何考虑将来的应用、通信业务和地理扩展等问题的，所选的介质应该能适应机构的需求。

1.2.1.5　确定节点

节点是网络中功能相对独立的部分，它可以发送、接收或转发、处理并存储数据，它可能是一台用户终端或服务器，也可能是一个集线器、交换机或路由器等。对于网络设计和规划中需要多少个节点、它们应该如何分布在不同的地理位置、每个节点的处理能力是多少等问题都必须有明确的答案。这就需要网络设计人员综合考虑多种因素，如用户需求、3～5 年后的发展情况、现有网络资源的利用、保证可靠性而采取的冗余措施等。

1.2.1.6　确定网络的性能

网络作为一个系统来看，其性能取决于多种因素，主要包括构成网络的各个部件的性能。网络的性能包括以下 6 个方面。

- 响应时间、延迟和等待时间。
- 利用率。
- 带宽、容量和吞吐量。
- 可用性、可靠性和可恢复性。
- 冗余度、适应性和可伸缩性。
- 效率与费用。

确定网络的性能就是要针对每一种性能选取适当的指标，以保证在网络工程施工后期测试时有据可依，为此，需要评判建成的网络是否满足性能设计要求。

总的来说，网络的性能与网络的投入成正比，即选用的组网设备和部件越好，整个网络的性能就越好。但不同的单位有不同的需求，需要在性能和投入两者之间找到一个平衡点，力争做到投入少、性能好。

1.2.1.7　确定可靠性措施

对于一个网络系统来说，可靠性就是对应用程序和数据的有效支持。在实际应用中，提高网络可靠性的可行方法是消除故障孤点，特别是单点故障。

1. 可靠性设计的内容

可靠性设计包含以下 3 方面的内容。

(1) 物理可靠，指系统对关键硬件设备(如 CPU、存储介质等)损坏，不可预见性灾难(如地震、飓风、陨石、强磁场等)，硬件、数据库及服务资源等破坏的耐受能力。

(2) 逻辑可靠，包含操作系统可靠、数据库管理系统可靠和应用程序可靠等。

(3) 健壮性，指系统在故障情况下恢复正常的难易程度。

对关键硬件设备的损坏，通常采取一定程度的容错措施来应对。根据经验，系统最可能出现的故障原因依次为电源故障、雷击、线路连接和火灾失效等。

2. 广域网的可靠性设计

广域网的可靠性包括冗余的广域网线路及其所带来的额外开销。一种主要的方法是连接备份线路，这样可以避免重复路由的保持和再计算。例如，路由器通过 DDN/Frame Relay(数字数据网/帧中继)连接主干的通信线路，当主干线路出现故障时，路由器可以自动通过 PSTN(公共交换电话网络)或 ISDN(综合业务数字网络)拨入中心路由器。

广域网的可靠性设计包括线路的备份和中心路由器的备份。系统中两个以上部件出现故障时，系统能够自动地在数秒内切换到备份部件上，而无须人工干预。

3. 通信设备的可靠性设计

随着租用线路服务可靠性的增强及其 ISDN/PSTN 后备技术的成熟，系统的可靠性已经在很大程度上转移到了通信设备连接的可靠性上。

防止通信设备损坏对网络造成不良后果的较好解决方案就是使用双电源和双路供电。例如，中心路由器可以采用 Cisco 公司的高性能大型路由器 7204(Cisco 7204 路由器具有双电源容错系统，并且具有端口容错等安全措施来保证系统的稳定运行)。

4. 局域网的可靠性设计

随着通信线路和通信设备的可靠性提高，系统的可靠性已经在很大程度上转移到了局域网连接的可靠性上。一个很好的解决方案就是使用双局域网服务。主机与两个局域网适配器相连，每个适配器连接到一个单独的集线器或交换机上，这样主机与主干交换设备之间的关键连接就具有较高的可靠性。

网络设计人员应根据组网需求，选择符合要求的可靠性结构和策略。

1.2.1.8 网络设备的选择

网络设备质量的高低直接影响着网络系统的性能。选择设备时，首先必须制定选择标准，即根据用户单位实际需要制订成本、性能、容量、处理量、延迟等指标和浮动范围，在能够满足需求的情况下，没有必要一味地求高求贵，而要参照产品的性能价格比来决定。

在设备到达现场时，需要检验其标称性能参数与既定标准的一致性，看是否有性能不达标的产品存在，以免设备投入运行后影响整个系统的性能。

设备安装到位且初步调试通过后，还需要采取专门的测试手段对关键设备进行高级测试，只有当设备在实际环境中的性能表现和与其他设备的兼容性和互联性完全符合标准后才能通过验收。

在选择产品时，除了要求产品支持应用需求之外，还建议考虑如下因素：选用符合工业标准的流行产品(保证产品的兼容性、可靠性和可扩充性)，具有较多的工具软件和应用软件支持，具有进一步开发的接口，具有完整的资料说明等。

作为网络工程，被选择的产品主要包括传输介质、网络接口、互联部件、网络服务器以及通信协议和应用软件等。

1. 传输介质

传输介质是网络的最基本部分，用于在用户设备之间传输信号。选择传输介质时，应当考虑如下因素。

- 安装特性：包括单段介质的最大长度、网络的覆盖范围、铺设时允许的最小弯角和最大直径等。
- 连接性：包括网络拓扑、可支持的连接数据等。
- 容量及性能：包括可使用的带宽、支持的逻辑信道数、每个信道可以支持的最大传输速率等。
- 防护性能：包括电气干扰与噪声、物理损害、安全性等。
- 价格：介质的价格。

目前可以选择的介质类型包括以下几类。

- 无屏蔽双绞线：支持点到点连接(包括环形)，价格较低，用于计算机联网的双绞线应为 3 类线以上。
- 屏蔽双绞线：支持点到点连接(包括环形)，仅用于电磁干扰较严重的环境，价格适中。
- 基带同轴电缆：支持总线连接(包括环形)，价格适中。
- 宽带同轴电缆：支持总线连接(包括环形)，价格略高。
- 光纤：支持点到点连接(包括环形)，价格偏高。

随着结构化布线技术的推广以及多介质应用的增多，双绞线和光纤成为组网的主要传输介质。

需要指出的是，传输介质的选择应当具有足够的超前意识，因为传输介质的布放一般会对建筑物的本身造成影响，因此应当尽可能避免因设备的更新换代和升级而改变传输介质。

2. 网络接口

网络接口的用途是将用户设备接入网络，网络接口通常以网络适配卡的形式出现。使用不同的传输介质和采用不同的访问介质控制方法时，要求使用不同类型的网络适配卡。

目前，常用的网络适配卡包括以下几种。

- 以太网卡：支持总线方式，具有不同的速率和工作方式的接口，可以连接双绞线、同轴电缆和光纤。
- ARCnet 网卡：支持总线方式，具有不同的接口，可以连接双绞线、同轴电缆，常用于生产控制环境。
- 令牌环卡：支持环形结构，连接双绞线。
- X.25 卡：支持用户终端接入 X.25 网络，连接双绞线。

- ATM 适配卡：支持用户设备接入 ATM 网络，连接光纤。
- FDDI 适配卡：支持用户设备接入 FDDI 网络，连接光纤或者铜芯电缆。

3. 互联部件

互联部件主要用于网络的扩展或者网络的互联。为了结构化布线的需要、减少设备之间的干扰和方便系统升级，局域网组建建议采用集线器方式。常用的互联部件包括以下几个。

- 集线器：有一般集线器和智能集线器之分，主要用于连接节点，所有端口共享链路带宽。
- 交换器(交换式集线器)：一种采用线路交换技术的集线器，具有端口链路分隔的特征，常用于连接网段或者相同类型的局域网。
- ATM 交换机：可以直接连接节点或者和其他 ATM 交换机连接，形成 ATM 网络。
- FDDI 集中器：可以直接连接节点或者和其他 FDDI 集中器等连接，形成 FDDI 网络。
- 路由器：常用的路由器包括远程访问路由器(支持远程用户通过拨号/专线方式访问内部网)、局域网/广域网路由器(支持用户通过各种公共网络进行互相访问)。

目前较高档的互联部件均采用了模块化结构，允许用户根据具体的应用需求选择和插入不同的模块。

选用交换器或者交换机时，应当注意其内部的交换结构；选用路由器时，应当考虑采用的路由算法，以及支持分组过滤的安全策略。

4. 网络服务器

网络服务器通常是小型机或者高档微机，它通过网络适配卡接入网络，向用户提供各种共享服务，如文件共享、打印共享、通信共享、电子邮件和 WWW 服务等。网络服务器可根据服务的类型，扩充不同的设施，例如，文件服务器要求较大容量的硬盘和高速缓冲区支持，打印服务器应当配置打印机。原理上，一台服务器可以提供多种应用服务，但在实际应用中，尤其是从安全和可扩展的角度出发，仍然建议在经费许可的前提下，根据应用服务划分和配置多台服务器。

5. 通信协议和应用软件

通信协议和应用软件的选择除了要满足具体的应用需求之外，还应考虑开放性，不仅要保证和不同厂家的不同产品之间的相互操作，还应兼顾和其他相关部门之间的关系(例如，对于数据库管理系统的选择应当兼顾与上级部门选择的一致性)。设计时应当允许三个阶段的并存，即原有的网络协议软件可能是“封闭”的，仅适合于连接同一厂家的产品(大多数生产控制系统具有这样的特性)；现行的网络协议软件要求是“开放”的，此时的整个网络系统为“混合型”的；将来的系统是完全“开放”的。

需要指出的是，任何一个系统(包括网络系统)都具有一定的生命周期，因此，应当从系统的功能、技术和效益等方面，对所设计的系统作出正确的系统生命周期估计。就现阶段而言，TCP/IP 协议应是通信协议选择的主流。

产品选择阶段的工作应由专业技术人员完成，或者直接委托供应商和公司完成。采用委托方式时，应在企业代表的全面控制下进行。

在选择供应商时，建议考虑如下因素：资金相对雄厚且具有良好的业绩，可以提供可

靠的产品，能够提供可靠的服务质量，尤其是售后服务质量好的公司。组建网络的最终目的是应用，因此，具有相关拳头产品或者应用软件开发能力较强也可成为选择供应商的指标之一。

1.2.1.9　设计管理

网络设计方案管理的任务包括设计复查、设计验证、设计确认和设计变更。

(1)　设计复查：项目计划中规定，对设计结果必须复查且对复查应留有备案。

(2)　设计验证：在项目计划中，经过设计复查和测试后，设计验证才能完成。需要按照复查结果验证设计输出是否符合设计输入的需求，如果任一部分的设计未通过验证，必须进行设计修复。

(3)　设计确认：设计确认就是要确保产品遵照产品需求说明书进行设计。产品的质量保证依赖于用来进行验证、确认和控制的测试工具，以及在确认及验证阶段使用的程序。

(4)　设计变更：设计变更需要修改相关设计文档并备案。

1.2.1.10　新网络业务运营计划

新网络运营过程一般是公司业务由旧的网络向新的网络迁移的过程。旧有业务应用适合于原有网络，而新系统由于在功能、性能、技术等方面都与旧的网络系统存在较大差异，因而对业务系统的支持也不同，直接将旧的业务系统迁移到新系统上是不太现实的，新系统的使用往往与新的业务系统配套。

在向新系统升迁前，应该周密计划，需要仔细考察新、旧系统的差异，分析升迁对用户造成的影响并及时通知他们。考虑到用户不能很快接受并适应新系统，升迁前还需要对他们进行系统的业务操作培训。如果一个单位的业务应用分为若干部分，也可以按照先易后难的顺序，一个部分一个部分地迁移到新系统，逐步积累新系统的使用经验，为后续部分的升迁作准备。

在整个升迁过程中，要及时做好系统备份，包括旧系统的备份，以便在新系统不可用时能够及时恢复到旧系统，保证业务正常开展。迁移完毕后，还需要对新业务系统进行测试，检查其对于设计目标的可满足性。新系统迁移成功后，对旧系统应采取措施妥善处理。

所有这些工作都将在网络系统实施阶段完成，因而在设计阶段应该针对每一个环节制订详细的计划，以便以后按计划实施。

1.2.1.11　设计方案测试

测试一个网络、预测和衡量网络性能是一门科学。没有两个完全相同的系统，因此对测试方法和测试工具的正确选择需要具有一定的创造性，还需要对所测试的系统有透彻的理解。

1. 测试原型网络系统的方法和工具

根据所要测试项目的应用目的正确选择测试方法和测试工具，通常包括以下内容。

- 验证该设计是否满足商业技术目标。
- 验证所选择的局域网技术、广域网技术和设备是否合适。
- 验证服务提供者是否能够提供要求的服务。
- 找出系统瓶颈或连通性问题。

- 测试网络冗余。
- 分析网络链路故障对性能的影响。
- 确定必要的优化技术，需满足的性能和其他技术目标。
- 分析网络链路和设备升级对性能的影响。
- 证明该设计优于其他竞争方案。
- 通过一个“验收测试”以获得进行下一步的网络实现。
- 发现可能妨碍执行的风险，并拟定相应的补救措施。
- 决定还需要多少其他测试。

如果网络设计方案中选用的设备不是全新的设备，也即该设备或相应的组网方案已经得到应用，上述测试内容就可以大大简化。一个比较简单的方法是，考查采用类似方案的现有网络系统，如果可能，可以考虑在不影响该网络业务正常运行的前提下，支付必要的费用，对该网络进行所需要的测试。这种方法的优点是：可以节省大量的资金和时间，与实际结合比较紧密。

如果采用的是全新的设备和网络设计方案，也应该要求设备厂商进行必要的测试或提供尽可能全面的测试资料，特别是第三方的权威测试结果报告，以降低测试费用。

2. 建立和测试原型网络系统

原型网络系统是新系统的一个初始实现，为最终完成系统提供了一个样板，可以帮助网络设计者验证所设计的新系统的功能和性能。

建立和测试原型网络系统能否顺利实施取决于所能得到的资源支持，包括人工、设备、资金和时间等。完成有效的测试需要有足够的资源，但是如果资源消耗过多会导致项目预算超支、时间过长或对用户产生不利影响。

以下就是建立和测试原型系统常用的 3 种方法。

- 在实验室中建立和测试网络。
- 与正在运行的网络集成，利用空闲时间进行测试。
- 与正在运行的网络集成，在正常工作时间内进行测试。

一旦网络设计方案得到认可，剩下的关键问题就是对原型网络系统进行测试，以考查可能出现的设计瓶颈。这种测试可以在空闲的时间进行，但最终的测试必须放在正常的工作时间内进行，从而能够在正常负载的情况下对系统进行评估。

在确定了原型系统的测试范围后，应该制订测试计划，说明如何测试该原型系统。

测试计划涉及的内容应当包括以下方面。

- 测试目标和验收标准。
- 测试的种类。
- 网络设备和所需的其他资源。
- 测试脚本。
- 测试项目的时间划分和阶段划分。

测试计划执行的过程主要是按测试脚本执行并将工作归档。由于在编写测试脚本时不可能把所有突发情况和可能出现的各种问题都考虑到，因而无法按部就班地执行测试计划。所以，在测试计划执行的过程中对日志记录进行维护就显得非常重要。

日志记录应当包括测试数据、测试结果以及每日活动记录。每日活动记录用来记载测试记录，包括对测试脚本或设备配置所做的改变、遇到的问题和对引起这些问题原因的推测。这些推测记录在分析测试结果时往往能够发挥重要的作用。

3. 网络测试工具

网络设计的测试工具一般包括以下几个。

- 网络管理和监控工具。
- 建模和仿真工具。
- 服务质量和服务级别管理工具。

1.2.1.12　设计评审

对于按照以上规范提出的网络逻辑设计方案，必须得到批准后才能够实施。

先交由单位组建的网络评审委员会讨论，审查该方案是否满足本单位对新网络的各种类型的需求，网络规划是否合理，使用的技术是否先进，选择的设备厂商是否信誉良好，网络的实施成本是否在单位的预算之内等，不同的单位可能有不同的审查准则。在所有条件均满足之后，网络设计方案才能得到批准。

批准时，需要由单位的管理部门、MIS(管理信息系统)职员和咨询公司代表签字。

1.2.2　典型例题分析

例 1　阅读以下说明，回答问题。(2015 年上半年下午试题一)

【说明】

某企业网络拓扑图如图 1-5 所示。

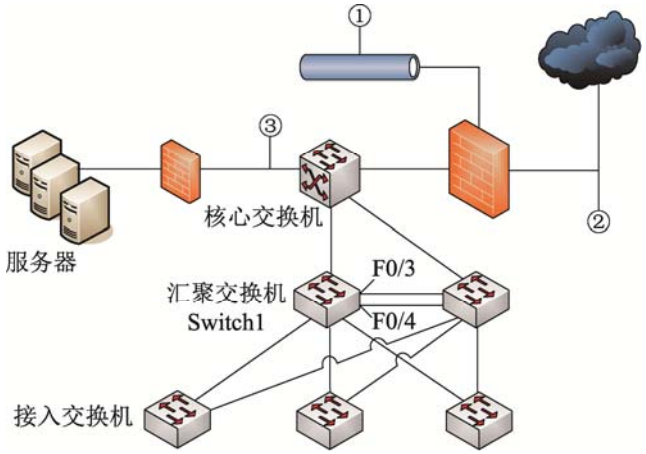

图 1-5　某企业网络拓扑图

工程师给出了该网络的需求：

1. 用防火墙实现内外网地址转换和访问控制策略；
2. 核心交换机承担数据转发，并且与汇聚层两台交换机实现 OSPF 功能；
3. 接入层到汇聚层采用双链路方式组网；

4. 接入层交换机对地址进行 VLAN 划分；

5. 对企业的核心资源加强安全防护。

【问题 1】(4 分)

该企业计划在①、②或③的位置部署基于网络的入侵检测系统(NIDS)，将 NIDS 部署在①的优势是 (1) ；将 NIDS 部署在②的优势是 (2) 、 (3) ；将 NIDS 部署在③的优势是 (4) 。

(1)～(4)备选答案：

A. 检测外部网络攻击的数量和类型

B. 监视针对 DMZ 中系统的攻击

C. 监视针对关键系统、服务和资源的攻击

D. 能减轻拒绝服务攻击的影响

【问题 2】(4 分)

OSPF 主要用于大型、异构的 IP 网络中，是对 (5) 路由的一种实现。若网络规模较小，可以考虑配置静态路由或 (6) 协议实现路由选择。

(5) 备选答案：A. 链路状态　　B. 距离矢量　　C. 路径矢量

(6) 备选答案：A. EGP　　B. RIP　　C. BGP

【问题 3】(4 分)

对汇聚层两台交换机的 F0/3、F0/4 端口进行端口聚合，F0/3、F0/4 端口默认模式是 (7) ，进行端口聚合时应配置为 (8) 模式。

(7)、(8)备选答案：

A. multi　　B. trunk　　C. access

【问题 4】(6 分)

为了在汇聚层交换机上实现虚拟路由冗余功能，需配置 (9) 协议，可以采用竞争的方式选择主路由设备，比较设备优先级大小，优先级大的为主路由设备。若备份路由设备长时间没有收到主路由设备发送的组播报文，则将自己的状态转为 (10) 。

为了避免二层广播风暴，需要在接入与汇聚设备上配置 (11) 。

(10)、(11)备选答案：

A. Master　　B. Backup　　C. VTP Server　　D. MSTP

【问题 5】(2 分)

阅读汇聚交换机 Switch 1 的部分配置命令，回答下面的问题。

```
Switch 1(config)#interface vlan 20
Switch 1 (config-if)#ip address 192.168.20.253 255.255.255.0
Switch 1(config-if)#standby 2 ip 192.168.20.250
Switch 1(config-if)#standby 2 preempt
Switch 1(config-if)#exit
```

VLAN20standby 默认优先级的值是 (12) 。

VLAN20 设置 preempt 的含义是 (13) 。

答案：

【问题 1】

(1) B　　(2) A　　(3) D　　(4) C

【问题 2】

(5) A　　(6) B

【问题 3】

(7) C　　(8) B

【问题 4】

(9) HSRP　　(10) A　　(11) D

【问题 5】

(12) 100　　(13) 设置抢占模式

解析：

【问题 1】由图 1-5 可知，①位于 DMZ 区，所以可以监视针对 DMZ 中系统的攻击。②连接外网，所以可以检测外部网络攻击的数量和类型、减轻拒绝服务攻击的影响。③位于内网服务器区域，所以可以监视针对关键系统、服务和资源的攻击。

【问题 2】OSPF 属于链路状态路由协议。网络规模小，可采用 RIP 路由协议，而 EGP 和 BGP 属于外部网关路由协议。

【问题 3】交换机默认端口的模式为接入模式 access，对汇聚层交换机进行端口聚合时，一般配置为 trunk 模式。

【问题 4】汇聚交换机采用虚拟路由冗余，目的是当一台汇聚交换机出现故障时，启用备份线路。根据设备情况可以采用虚拟路由器冗余协议(VRRP)或热备份路由器协议(HSRP)。

生成树协议是一种二层管理协议，它通过有选择性地阻塞网络冗余链路来达到消除网络二层环路的目的，同时具备链路的备份功能。

【问题 5】

```
Switch1(config)#interface vlan 20   //进入 VLAN20 虚接口
Switch1(config-if)#ip address 192.168.20.253 255.255.255.0 //配置 IP 地址
Switch1(config-if)#standby 2 ip 192.168.20.250   //配置备份组 2 的虚拟 IP
Switch1(config-if)#standby 2 preempt     //配置抢占功能
Switch1(config-if)#exit
```

默认优先级为 100，取值范围为 0～255，值越大，优先级越高。

例 2　【说明】(2014 年下半年下午试题一)

某企业的网络结构如图 1-6 所示。

【问题 1】(6 分)

1. 图 1-6 中的网络设备①应为__(1)__，网络设备②应为__(2)__，从网络安全的角度出发，Switch9 所组成的网络一般称为__(3)__区。

2. 图 1-6 中③处的网络设备的作用是检测流经内网的信息，提供对网络系统的安全保护。该设备提供主动防护，能预先对入侵活动和攻击性网络流量进行拦截，避免造成损失，而不是简单地在恶意流量传送时或传送后才发出警报。网络设备③应为__(4)__，其连接的 Switch1 的 G1/1 端口称为__(5)__端口，这种连接方式一般称为__(6)__。

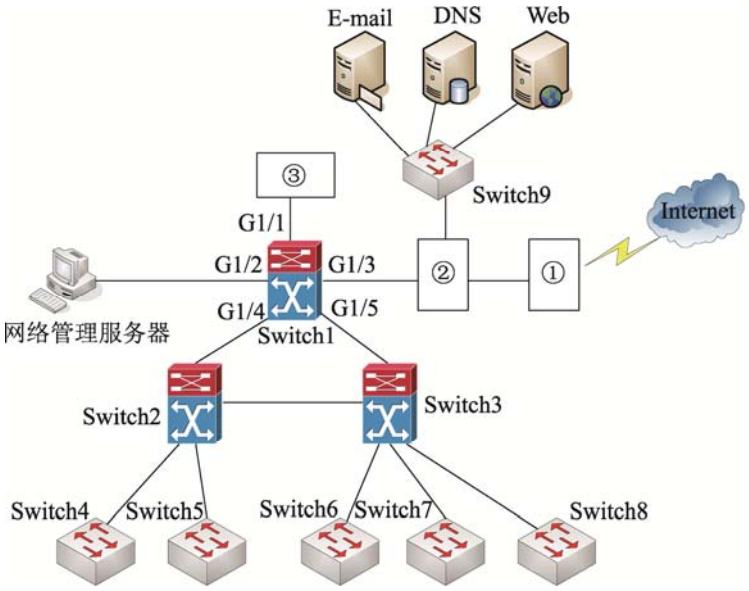

图 1-6　某企业的网络结构

【问题 2】(5 分)

1. 随着企业用户的增加，要求部署上网行为管理设备，对用户的上网行为进行安全分析、流量管理、网络访问控制等，以保证正常的上网需求。部署上网行为管理设备的位置应该在图 1-6 中的 (7) 和 (8) 之间比较合理。

2. 网卡的工作模式有直接、广播、多播和混杂四种模式，缺省的工作模式为 (9) 和 (10)，即它只接收广播帧和发给自己的帧。网络管理机在抓包时，需要把网卡置于 (11) 模式，这时网卡将接受同一子网内所有站点所发送的数据包，这样就可以达到对网络信息监视的目的。

【问题 3】(5 分)

针对图 1-6 中的网络结构，各台交换机需要运行 (12) 协议，以建立一个无环路的树状网络结构。按照该协议，交换机的默认优先级值为 (13)，根交换机是根据 (14) 来选择的，值小的交换机为根交换机；如果交换机的优先级相同，再比较 (15)。当图 1-6 中的 Switch1—Switch3 之间的某条链路出现故障时，为了使阻塞端口直接进入转发状态，从而切换到备份链路上，需要在 Switch1—Switch3 上使用 (16) 功能。

【问题 4】(4 分)

根据层次化网络的设计原则，从图 1-6 中可以看出该企业网络采用了由 (17) 层和 (18) 层组成的两层架构，其中，MAC 地址过滤和 IP 地址绑定等功能是由 (19) 完成的，分组的高速转发是由 (20) 完成的。

答案：

【问题 1】

(1) 路由器　(2) 防火墙　(3) DMZ　(4) IPS　(5) 镜像　(6) 旁路模式

【问题 2】

(7) 防火墙　(8) SW1　(9) 直接　(10) 广播　(11) 混杂

【问题 3】

(12) STP　(13) 32768　(14) 交换机 ID　(15) MAC 地址　(16) 上行速链路

【问题 4】

(17) 核心层　(18) 接入层　(19) 接入层　(20) 核心层

解析：

【问题 1】网络设备①接入 Internet 应为路由器，那么设备②即为防火墙，Switch9 所接区域应为 DMZ 区。

根据该设备提供主动防护，能预先对入侵活动和攻击性网络流量进行拦截，避免造成损失，而不是简单地在恶意流量传送时或传送后才发出警报，可判断设备③为 IPS，则其连接的 G1/1 端口称为镜像端口，这样的连接方式为旁路模式。一般 IPS 以串接的方式接入网络，但是此题的部署方式并不常规，根据题意预先对入侵活动和攻击性网络流量进行拦截，避免造成损失来判断应为 IPS。

【问题 2】上网行为管理是指帮助互联网用户控制和管理对互联网的使用，包括对网页访问过滤、网络应用控制、带宽流量管理、信息收发审计、用户行为分析，上网行为管理设备的位置应该在防火墙和 SW1 之间。

网卡具有如下几种工作模式。

(1) 广播模式(Broad Cast Model)：它的物理地址(MAC)是 0Xffffff 的帧为广播帧，工作在广播模式的网卡接收广播帧。

(2) 多播传送(MultiCast Model)：多播传送地址作为目的物理地址的帧可以被组内的其他主机同时接收，而组外主机却接收不到。但是，如果将网卡设置为多播传送模式，它可以接收所有的多播传送帧，而不论它是不是组内成员。

(3) 直接模式(Direct Model)：工作在直接模式下的网卡只接收目地址是自己 MAC 地址的帧。

(4) 混杂模式(Promiscuous Model)：工作在混杂模式下的网卡接收所有的流过网卡的帧，信包捕获程序就是在这种模式下运行的。

网卡的缺省工作模式包含广播模式和直接模式，即它只接收广播帧和发给自己的帧。如果采用混杂模式，一个站点的网卡将接受同一网络内所有站点所发送的数据包，这样就可以达到对于网络信息监视捕获的目的。

【问题 3】生成树算法的网桥协议 STP(Spanning Tree Protocol)，通过生成树来保证一个已知的网桥在网络拓扑中沿一个环动态工作。

STP 的算法分为 3 个步骤：

(1) 选择根网桥(Root Bridge)，依据：网桥 ID(BID)= 网桥优先级+网卡的 MAC 地址，其中网桥 ID 是唯一的，以及选择交换网络中网桥 ID 最小的交换机成为根网桥。注意：优先级取值范围为 0～65535，缺省值为 32768。

(2) 选择根端口(Root Ports)，依据：到根网桥最低的根路径成本，直连的网桥 ID 最小，直连的端口 ID 最小。注意：端口 ID=端口优先级+端口编号，端口优先级范围为 0～255，缺省值为 128。其中根路径成本为：网桥到根网桥的路径上所有链路的成本之和。

(3) 选择指定端口(Designated Ports)。

配置上行速链路，当接入层或汇聚层的交换机主用的上行链路断开的时候，被阻塞的

端口迅速转换到转发的状态，不需要经历侦听和学习状态。

【问题 4】层次化网络模型包括：

(1) 由经过可用性和性能优化的高端路由器和交换机组成的核心层。

(2) 由用于实现策略的路由器和交换机构成的汇聚层。

(3) 通过用以连接用户的低端交换机等构成的接入层。

核心层是网络高速交换的主干，接入层为用户提供了在本地网段访问应用系统的能力，具有过滤 MAC 地址、绑定 IP 地址等功能。

1.2.3 同步练习

【说明】(2014 年上半年下午试题一)

某单位计划部署园区网络，该单位总部设在 A 区，另有两个分支机构分别设在 B 区和 C 区，各个地区之间距离分布如图 1-7 所示。

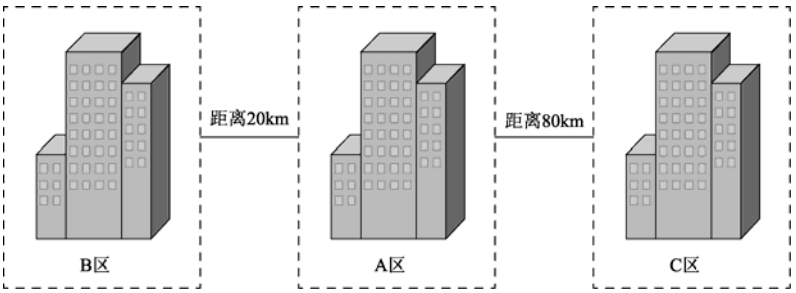

图 1-7 各地区之间距离分布

该单位的主要网络业务需求在 A 区，该网络中心及服务器机房亦部署在 A 区；B 区的网络业务流量需求远大于 C 区；C 区虽然业务流量小，但是网络可靠性要求高。根据业务需要，要求三个区的网络能够互通并且都能够访问互联网，同时基于安全考虑，单位要求采用一套认证设备进行身份认证和上网行为管理。

【问题 1】(6 分)

为了保障业务需求，该单位采用两家运营商接入 Internet。根据题目需求，回答下列问题：

1. 两家运营商的 Internet 接入线路应部署在哪个区？为什么？

2. 网络运营商提供的 MPLS-VPN 和千兆裸光纤两种互联方式，哪一种可靠性高？为什么？

3. 综合考虑网络需求及运营成本，在 AB 区之间与 AC 区之间分别采用上述哪种方式进行互联？

【问题 2】(8 分)

该单位网络部署接入点情况如表 1-1 所示。

根据网路部署需求，该单位采购了相应的网络设备，请根据题目说明及表 1-1，确定表 1-2 所示的设备数量及合理的部署位置(注：不考虑双绞线的距离限制)。