DAXING YUANQU
WANGLUO JIANSHE YU GUANLI

大型园区网络建设与管理

魏楚元　等编著

机械工业出版社
CHINA MACHINE PRESS

大型园区网络建设与管理

魏楚元　等编著

机 械 工 业 出 版 社

本书从基础入手，以一个大型网络建设为主线，系统地介绍了一个园区网络规划、设计与实施的原理、方法、技术和管理。本书首先介绍了一个大型园区网络的基本原理、基本概念和关键要素及设计方法。然后分章节、较全面、系统地介绍了网络互连设备、服务器与存储技术、网络安全原理与技术、综合布线系统、网络机房与数据中心和网络管理的设计方法与关键技术。本书涵盖了一个大型网络规划、设计的全过程。作者结合多年从事网络规划设计与管理的实践经验，为读者提供了一个完整的大型园区网络设计方法和当前流行的技术案例，涵盖一个大型园区网络的网络设备、综合布线系统、机房建设、服务器与存储系统、网络管理与安全等主要内容。

本书内容通俗易懂，结构清晰、实例丰富、实用性强。本书适合高等院校计算机科学与技术、网络工程、信息安全、软件工程等专业的学生使用，也适合作为网络工程人员的自学教材和培训教材，特别适合作为网络工程技术人员和网络管理人员的工程实践指导书。

图书在版编目（CIP）数据

大型园区网络建设与管理/魏楚元等编著. —北京：
机械工业出版社，2014.8
ISBN 978-7-111-47722-8

Ⅰ.①大… Ⅱ.①魏… Ⅲ.①计算机网络管理
Ⅳ.①TP393.07

中国版本图书馆 CIP 数据核字（2014）第 191685 号

机械工业出版社（北京市百万庄大街 22 号 邮政编码 100037）
策划编辑：林春泉 责任编辑：翟天睿
版式设计：赵颖喆 责任校对：程俊巧
责任印制：刘 岚
北京京丰印刷厂印刷
2015 年 3 月第 1 版·第 1 次印刷
184mm×260mm·16.5 印张·399 千字
0 001—3 000 册
标准书号：ISBN 978-7-111-47722-8
定价：49.00 元

凡购本书，如有缺页、倒页、脱页，由本社发行部调换

电话服务		网络服务	
社服务中心：	(010)88361066	教材网：	http://www.cmpedu.com
销售一部：	(010)68326294	机工官网：	http://www.cmpbook.com
销售二部：	(010)88379649	机工官博：	http://weibo.com/cmp1952
读者购书热线：	(010)88379203	**封面无防伪标均为盗版**	

前　言

据中国互联网络信息中心（CNNIC）2013 年 7 月 17 日在京发布的第 32 次《中国互联网络发展状况统计报告》显示：截至 2013 年 6 月底，我国网民规模达到 5.91 亿，互联网普及率为 44.1%。在今年上半年的互联网发展中，手机作为上网终端的表现抢眼，不仅成为新增网民的重要来源，在即时通信、电子商务等网络应用中均有良好的表现。进入 21 世纪以来，近 10 年时间，我国网络产业的发展十分迅猛，华为、中兴、锐捷等知名网络厂商推动了网络产业的迅猛发展。中国俨然是一个网络大国，国家层面上推动物联网产业、云计算产业的发展，基础网络设施的建设变得十分重要。行业的发展热潮势必催生了网络基础设施建设的高潮，对网络工程行业的人才需求也变得旺盛。

何为一个大型园区网络，并没有一个严格的定义。人们经常讨论的大型园区网络，通常是指这个网络所服务的用户数、信息点数、网络设备台套数等。如一所大学，拥有人数两三万人，这所大学只有一个网络出口，那么这所大学所建设的园区网络覆盖到全校 100 多栋建筑物，构成了这所大学的局域网，这个局域网通常称为校园网。校园网拥有网络核心与数据中心机房，拥有中心机房至全校各单体建筑的主干光缆，每栋楼宇都有覆盖各单体办公室的双绞线缆，每栋楼宇的弱电间都有网络交换机，数据中心机房拥有多台服务器和存储系统等。这些关键要素就构成了一个大型园区网络。

如何设计一个大型园区网络呢？业界很多企业、厂商、专家、学者都提出了很多解决方案，如知名网络厂商推出的交换、路由方案。实际上，一个大型园区网络的规划、设计与建设是一个系统工程。从系统论的角度，可以把它分解为几大块：第一，一个以网络设备为主的网络解决方案；第二，一个网络与数据中心机房建设方案；第三，一个与网络解决方案相匹配的综合布线系统解决方案；第四，一个完备的网络管理与网络安全解决方案。可以把这四个关键的解决方案及其实践，归结为网络基础设施的建设。本书系统性地以一个大型网络建设为主线，介绍了一个园区网络规划、设计与实施的原理、方法、技术和管理。

本书的作者结合多年从事网络规划设计与管理的实践经验，为读者提供一个完整的大型园区网络设计方法和当前流行的技术案例，涵盖一个大型园区网络的网络设备、综合布线系统、机房建设、服务器与存储系统、网络管理与安全等主要内容。业界不断推出新的产品、新的解决方案，推陈出新，内容繁杂。作者从基础层面着手，抓住主要的要素，由浅入深地介绍一些解决方案。本书最大的特点是实用性强，基本上围绕实践层面，从解决问题入手。这些方案可以供读者理解如何规划一个大型园区网络，如何以最快捷、最实用的方式构建一个大型网络。本书也有部分理论基础，以方便读者理解掌握。

本书共分为 8 章，各章的主要内容如下：

第 1 章　园区网络工程概述。主要介绍了计算机网络的基本组成、功能、局域网的基础知识。对一个大型园区网络规划与设计的要素进行了介绍，并介绍网络逻辑设计、物理设计、网络弱电工程设计的一些基本概念和方法。

第 2 章　网络互连设备。主要介绍了网络互连的基本概念和常用的网络设备，重点介绍

了交换机和路由器的构造、基本原理和性能指标。

第3章　数据中心服务器与存储技术。主要介绍了服务器与存储系统的设备特点、构造、板卡、性能指标，给出了一些存储系统的解决方案。

第4章　网络安全技术。介绍了网络安全的基本概念、基本攻防技术、给出了网络防火墙、入侵检测、入侵防御系统等关键安全设备的解决方案。

第5章　综合布线系统。主要介绍了综合布线系统的规划、设计与施工技术。

第6章　网络核心机房建设。主要以一个网络核心机房与数据中心机房建设案例为主，阐述了网络机房建设的一些关键要素。

第7章　网络管理。主要介绍了网络管理的基本概念、基本原理和常用的网络管理手段。

第8章　大型园区网络规划与设计案例。主要以高校校园网络建设为案例，介绍了园区网络规划与设计的基本方法。

本书内容通俗易懂、结构清晰、实例丰富、实用性强。本书适合高等院校计算机科学与技术、网络工程、信息安全、软件工程、智能建筑弱电工程等专业的学生使用，也适合作为网络工程人员的自学教材和培训教材，特别适合于作为网络工程技术人员和网络管理人员的工程实践指导书。

本书在编写过程中参考了国内外知名企业、厂商提出的一些经典的解决方案和产品资料，也参考了国内同仁编写的专著、教材的新成果、新知识，在此一并表示感谢。

本书的写作得到了张蕾、孙绪华、宋军、李勇振、王东亮、牟综磊等的大力帮助和支持，他们参与编写了部分内容，在此表示感谢。

网络是一个复杂系统。本书内容较为全面，但限于篇幅和章节，很多内容并未深入阐述清楚，再限于作者水平有限，书中难免存在很多错误和不完善的地方，敬请读者批评指正。

编　者

2014年6月

目　录

第 1 章　园区网络工程概述

1.1　计算机网络概述

1.1.1　计算机网络的定义

在计算机网络发展过程的不同阶段中，人们对计算机网络提出了不同的定义，它反映了当时网络技术发展的水平，以及人们对网络的认识程度。计算机和通信的结合对于计算机系统的组织方式产生了深远的影响。把一台大型的计算机放在一个单独的房间中，然后用户带着他们的处理任务去房间里上机，这种“计算机中心”的概念现在已经完全过时了。由一台计算机来处理整个组织中所有的计算需求，这种老式的模式已经被新的模型所取代，在新的模型下，由大量独立的、但相互连接起来的计算机共同完成计算任务。这些系统称为计算机网络（Computer Networks）。

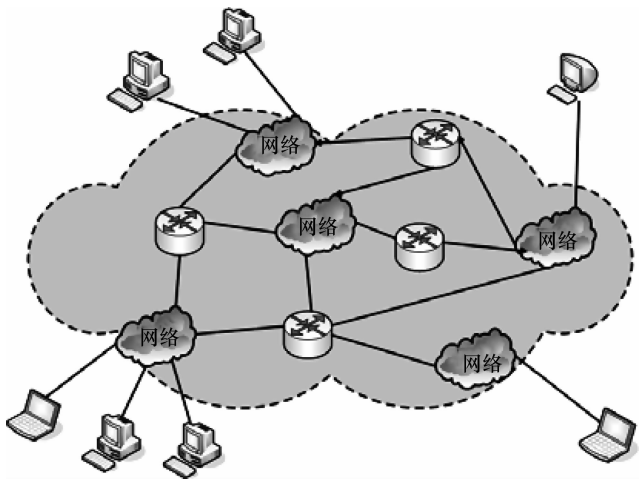


图 1-1　计算机网络示意图

计算机网络是利用通信设备和通信线路将地理位置分散、功能独立的多台计算机和由计算机控制的外部设备连接起来，在网络操作系统的控制下，按照约定的通信协议进行信息交换，实现资源共享的系统，如图 1-1 所示。

1.1.2　计算机网络的功能

计算机网络的功能主要有以下几个方面：

1. 信息交换

信息交换是计算机网络最基本的功能，主要完成网络中各个节点之间的通信。计算机网络为人们提供了快捷地与他人进行信息交换的方式。人们可以在网上收发电子邮件，发布新闻消息，进行电话会议、电子商务、网上求职、娱乐聊天等活动。

2. 资源共享

共享的资源主要是指计算机硬件资源、软件资源和数据资源。通过资源共享，可使网络中各单位的资源互通，有助于分工协作，从而大大提高系统资源的利用率。

（1）硬件共享

在网络范围内能够共享的硬件资源有高速运算器、大容量磁盘、打印机、绘图仪、高性能计算机等。如图 1-2 所示，局域网中的共享打印机就属于硬件共享。通过硬件资源的共享，可以提高设备的利用率，避免重复投资。

（2）软件资源

网络中的某些机器，特别是一些大型机上，装有各种功能完善的软件资源，如大型有限元结构分析程序、专用的绘图程序等。用户可以通过网络登录到远程计算机上去使用这些软件，也可以从网络上下载某些程序在本地机上使用，以实现软件资源的共享。

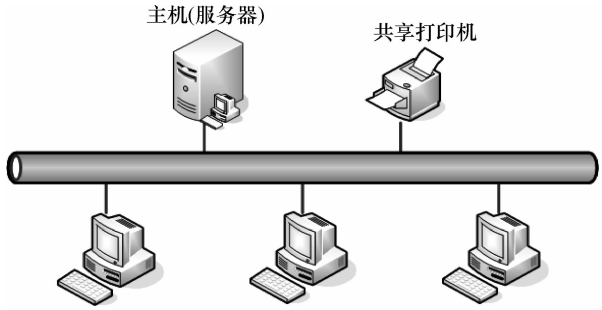


图 1-2　网络打印机共享示意图

（3）信息与数据

网络上的数据库和各种文件中存储有大量的信息资源，内容涉及科学、技术、商业、教育、医学、气象等各个方面。通过计算机网络，这些资源可以供世界各地的人们查询并加以利用。

3. 分布式处理

分布式处理系统将不同地点的或具有不同功能的多台计算机用通信网络连接起来，在控制系统的统一管理控制下，协调地完成信息处理任务。这种协同工作、并行处理要比单独购置高性能的大型计算机便宜得多，而且可以充分利用网络资源，均衡各计算机的负载，从而提高处理问题的实时性。

4. 数据备份

通过计算机网络实现备份技术，可以提高计算机系统的可靠性。当某一台计算机出现故障时，可以立即由计算机网络中的另一台计算机来代替其完成所承担的任务。例如，空中交通管理、工业自动化生产线、军事防御系统、电力供应系统等都可以通过计算机网络设置，以保证实时性管理和不间断运行系统的安全性和可靠性。

1.1.3　计算机网络的分类

计算机网络可以从不同的角度进行分类，根据链路控制技术、覆盖的地理范围、网络拓扑结构等来进行分类，本节重点介绍两种分类方法及相关知识。

1. 根据计算机网络覆盖的地理范围分类

按照计算机网络所覆盖的地理范围的大小进行分类，计算机网络可分为：局域网、城域网和广域网。了解一个计算机网络所覆盖的地理范围的大小，可以使人们能一目了然地了解该网络的规模和主要技术。

局域网（LAN）的覆盖范围一般在方圆几十米到几公里。典型的是一个办公室、一个办公楼、一个企业或一个园区的范围内的网络。如一所大学的校园网络，是典型的一个规模比较大的园区网络。

当网络的覆盖范围达到一个城市的大小时，被称为城域网。网络覆盖到多个城市甚至全国的时候，就属于广域网的范畴了。目前，我国已建成的广域网是 ChinaNet、CERNET 等。

大型企业、院校、政府机关通过租用公共广域网的线路，可以构成自己的广域网。

2. 根据网络拓扑结构分类

网络拓扑结构分为物理拓扑和逻辑拓扑。物理拓扑结构描述网络中由网络终端、网络设备组成的网络节点之间的几何关系，反映出网络设备之间以及网络终端是如何连接的。

网络按照拓扑结构划分有：总线型结构、环形结构、星形结构、树形结构和网状结构，如图 1-3 所示。

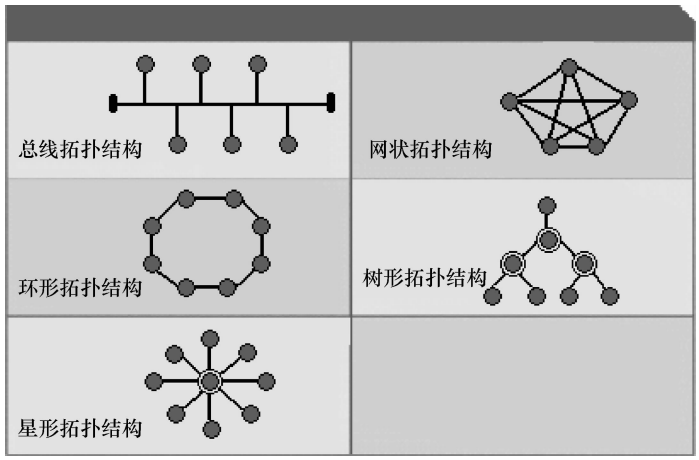


图 1-3　计算机网络的拓扑结构

总线型拓扑结构是早期同轴电缆以太网中网络节点的连接方式，网络中各个节点挂接到一条总线上。这种物理连接方式已经被淘汰。

1）星形拓扑结构是现代以太网的物理连接方式。在这种结构下，以中心网络设备为核心，与其他网络设备以星形方式连接，最外端是网络终端设备。星形拓扑结构的优势是连接路径短，易连接，易管理，传输效率高。这种结构的缺点是中心节点需具有很高的可靠性和冗余度。

2）树形拓扑结构的网络层次清晰，易扩展，是目前多数校园网和企业网使用的结构。这种结构的缺点是根节点的可靠性要求很高。

3）环形拓扑结构的网络中，通信线路沿各个节点连接成一个闭环。数据传输经过中间节点的转发，最终可以到达目的节点。这种通信结构的最大缺点是通信效率低。

4）网状拓扑结构构造的网络可靠性最高。在这种结构下，每个节点都有多条链路与网络相连，高密度的冗余链路，使一条甚至几条链路出现故障，网络仍然能够正常工作。网状拓扑结构的网络的缺点是成本高，结构复杂，管理维护相对困难。

1.2　局域网

1.2.1　局域网的定义及功能

局域网技术是计算机网络研究与应用的热点，也是目前技术发展最快的领域之一。从局

域网应用的角度来看，它的技术特点主要表现在以下方面：

1）局域网覆盖有限的地理范围，通常为0.1～2.5km，适用于公司、机关、校园、工厂等有限范围内的计算机、终端与各类信息处理设备联网的需求。

2）局域网提供高传输速率（100Mbit/s～10Gbit/s）、低误码率（10^{-7}～10^{-12}）的高质量数据传输环境，传输速率高达1000Mbit/s的高速局域网正在发展中。

3）局域网一般属于一个单位，易于建立、维护与扩展。

4）决定局域网特性的主要技术要素为网络拓扑、传输介质与介质访问控制方法。

5）从介质访问控制方法的角度来看，局域网可分为共享介质式局域网与交换式局域网两类。

局域网最主要的功能是提供资源共享和相互通信，它可提供以下几项主要服务：

1）资源共享，包括硬件资源共享、软件资源共享及数据库存共享。在局域网上各用户可以共享昂贵的硬件资源，如大型外部存储器、绘图仪、激光打印机、图文扫描仪等特殊外设。用户可共享网络上系统软件和应用软件，避免重复投资及重复劳动。网络技术可使大量分散的数据能被迅速集中、分析和处理，分散在网内的计算机用户可以共享网内的大型数据库而不必重新设计这些数据库。

2）数据传送和电子邮件。数据和文件的传输是网络的重要功能，现代局域网不仅能传送文件、数据信息，还可以传送声音、图像。局域网站点之间可提供电子邮件服务，某网络用户可以输入信件并传送给另一用户，收信人可打开“邮箱”阅读处理信件并可写回信再发回电子邮件，既节省纸张又快捷方便。

3）提高计算机系统的可靠性。局域网中的计算机可以互为后备，避免了单机系统的无后备时可能出现的故障导致系统瘫痪，大大提高了系统的可靠性，特别在工业过程控制、实时数据处理等应用中尤为重要。

4）易于分布处理。利用网络技术能将多台计算机连成具有高性能的计算机系统，通过一定算法，将较大型的综合性问题分给不同的计算机去完成。在网络上可建立分布式数据库系统，使整个计算机系统的性能大大提高。

1.2.2 局域网的分类

目前，业界应用最广泛的局域网主要是以双绞线、光纤为代表的传输介质以太网，在网络发展历史中，因行业特点，所采用的局域网也不一定都是以太网，局域网主要有以太网（Ethernet）、令牌网（Token Ring）、FDDI网、异步传输模式网（ATM）等几类。但是，目前在业界使用的主要是以太网技术和无线局域网技术，其他组网技术在工业领域多见，其他行业较为少见。本节重点介绍以太网技术和无线局域网技术。

1. 以太网（Ethernet）

1980年，Digital Equipment Corporation、Intel和Xerox（DIX）协会发布了第一个以太网标准。1982年，DIX协会发布了Ethernet Ⅱ标准，是目前LAN中实施的标准。以太网是应用最为广泛的局域网，包括标准以太网（10Mbit/s）、快速以太网（100Mbit/s）、千兆以太网（1000Mbit/s）和10G以太网，它们都符合IEEE802.3系列标准规范。

（1）标准以太网

最开始以太网只有10Mbit/s的吞吐量，它所使用的是CSMA/CD（Carrier Sense Multiple

Access/Collision Detect；带有冲突检测的载波侦听多路访问）的访问控制方法，通常把这种最早期的 10Mbit/s 以太网称为标准以太网。以太网主要有两种传输介质，即双绞线和同轴电缆。所有的以太网都遵循 IEEE 802.3 标准，下面列出的是 IEEE 802.3 的一些以太网标准，在这些标准前面的数字表示传输速度，单位是“Mbit/s”，最后的一个数字表示单段网线长度（基准单位是 100m），Base 表示“基带”，Broad 代表“带宽”。

- 10Base-5：使用粗同轴电缆，最大网段长度为 500m，基带传输方法；
- 10Base-2：使用细同轴电缆，最大网段长度为 185m，基带传输方法；
- 10Base-T：使用双绞线电缆，最大网段长度为 100m；
- 1Base-5：使用双绞线电缆，最大网段长度为 500m，传输速度为 1Mbit/s；
- 10Broad-36：使用同轴电缆（RG-59/U CATV），最大网段长度为 3600m，是一种宽带传输方式；
- 10Base-F：使用光纤传输介质，传输速率为 10Mbit/s。

（2）快速以太网（Fast Ethernet）

随着网络的发展，传统标准的以太网技术已难以满足日益增长的网络数据流量速度的需求。在 1993 年 10 月以前，对于要求 10Mbit/s 以上数据流量的 LAN 应用，只有光纤分布式数据接口（FDDI）可供选择，但它是一种价格非常昂贵的、基于 100Mbit/s 光缆的 LAN。1993 年 10 月，Grand Junction 公司推出了世界上第一台快速以太网集线器 FastSwitch10/100 和网络接口卡 FastNIC100，快速以太网技术正式得以应用。随后 Intel、SynOptics、3COM、BayNetworks 等公司亦相继推出自己的快速以太网装置。与此同时，IEEE802 工程组亦对 100Mbit/s 以太网的各种标准，如 100 Base-TX、100 Base-T4、MII、中继器、全双工等标准进行了研究。1995 年 3 月 IEEE 宣布了 IEEE802.3u 100 Base-T 快速以太网标准（Fast Ethernet），就这样开始了快速以太网的时代。

快速以太网与原来在 100Mbit/s 带宽下工作的 FDDI 相比具有许多的优点，主要体现在快速以太网技术可以有效地保障用户在布线基础实施上的投资，它支持 3、4、5 类双绞线以及光纤的连接，能有效地利用现有的设施。

快速以太网的不足也是以太网技术的不足，即快速以太网仍是基于载波侦听多路访问和冲突检测（CSMA/CD）技术，当网络负载较重时，会造成效率的降低，当然可以使用交换技术来弥补。

100Mbit/s 快速以太网标准又分为：100Base-TX 、100Base-FX、100Base-T4 三个子类。

1）100Base-TX：是一种使用 5 类数据级无屏蔽双绞线或屏蔽双绞线的快速以太网技术。它使用两对双绞线，一对用于发送，一对用于接收数据。在传输中使用 4B/5B 编码方式，信号频率为 125MHz。符合 EIA586 的 5 类布线标准和 IBM 的 SPT 1 类布线标准。使用同 10Base-T 相同的 RJ-45 连接器。它的最大网段长度为 100m。它支持全双工的数据传输。

2）100Base-FX：是一种使用光缆的快速以太网技术，可使用单模和多模光纤（62.5μm 和 125μm），多模光纤连接的最大距离为 550m。单模光纤连接的最大距离为 3000m。在传输中使用 4B/5B 编码方式，信号频率为 125MHz。它使用 MIC/FDDI 连接器、ST 连接器或 SC 连接器。它的最大网段长度为 150m、412m、2000m 或更长至 10km，这与所使用的光纤类型和工作模式有关，它支持全双工的数据传输。100Base-FX 特别适合用于有电气干扰的环境、较大距离连接、或高保密环境等情况。

3）100Base-T4：是一种可使用3、4、5类无屏蔽双绞线或屏蔽双绞线的快速以太网技术。它使用4对双绞线，3对用于传送数据，1对用于检测冲突信号。在传输中使用8B/6T编码方式，信号频率为25MHz，符合EIA586结构化布线标准。它使用与10Base-T相同的RJ-45连接器，最大网段长度为100m。

（3）千兆以太网（GB Ethernet）

随着以太网技术的深入应用和发展，企业用户对网络连接速度的要求越来越高，1995年11月，IEEE802.3工作组委任了一个高速研究组（Higher Speed Study Group），研究将快速以太网速度增至更高。该研究组研究了将快速以太网速度增至1000Mbit/s的可行性和方法。1996年6月，IEEE标准委员会批准了千兆位以太网方案授权申请（Gigabit Ethernet Project Authorization Request）。随后IEEE802.3工作组成立了802.3z工作委员会。IEEE802.3z委员会的目的是建立千兆位以太网标准：包括在1000Mbit/s通信速率的情况下的全双工和半双工操作、802.3以太网帧格式、载波侦听多路访问和冲突检测（CSMA/CD）技术、在一个冲突域中支持一个中继器（Repeater）、10Base-T和100Base-T向下兼容技术千兆位以太网具有以太网的易移植、易管理特性。千兆以太网在处理新应用和新数据类型方面具有灵活性，它是在赢得了巨大成功的10Mbit/s和100Mbit/s IEEE802.3以太网标准的基础上的延伸，提供了1000Mbit/s的数据带宽。这使得千兆位以太网成为高速、宽带网络应用的战略性选择。

1000Mbit/s千兆以太网目前主要有以下三种技术版本：1000Base-SX，-LX和-CX版本。1000Base-SX系列采用低成本短波的CD（Compact Disc，光盘激光器）或者VCSEL（Vertical Cavity Surface Emitting Laser，垂直腔体表面发光激光器）发送器；而1000Base-LX系列则使用相对昂贵的长波激光器；1000Base-CX系列则打算在配线间使用短跳线电缆把高性能服务器和高速外围设备连接起。

（4）10G以太网

现在10Gbit/s的以太网标准已经由IEEE 802.3工作组于2000年正式制定，10G以太网仍使用与以往10Mbit/s和100Mbit/s以太网相同的形式，它允许直接升级到高速网络。同样使用IEEE 802.3标准的帧格式、全双工业务和流量控制方式。在半双工方式下，10G以太网使用基本的CSMA/CD访问方式来解决共享介质的冲突问题。此外，10G以太网使用由IEEE 802.3小组定义的和以太网相同的管理对象。总之，10G以太网仍然是以太网，只不过更快。但由于10G以太网技术的复杂性及原来传输介质的兼容性问题（目前只能在光纤上传输，与原来企业常用的双绞线不兼容），还有这类设备造价太高，因此主要用在大型园区网络的核心交换机等设备上。

2. 无线局域网

无线局域网（Wireless Local Area Network，WLAN）是计算机网络与无线通信技术相结合的产物。通俗地说，WLAN就是在不采用传统电缆的同时，提供传统有限局域网的所有功能，网络所需的基础设施不需要再埋在地下或隐藏在墙里，网络却能够随着用户的需要移动或变化。无线局域网正在日渐普及，越来越多的办公楼、机场和其他的公共场合配备了WLAN。人们越来越深刻地认识到：WLAN不仅能满足移动和特殊应用领域的需求，还能覆盖有线网络难于涉及的范围。WLAN作为传统局域网的补充，目前已成为局域网应用的热点问题之一。

无线局域网的第一个版本发表于 1997 年，其中定义了介质访问接入控制层和物理层。物理层定义了工作在 2.4GHz 的 ISM 频段上的两种无线调频方式和一种红外传输的方式，总数据传输速率设计为 2Mbit/s。两个设备之间的通信可以自由直接（ad hoc）的方式进行，也可以在基站（Base Station）或者访问点（Access Point）的协调下进行。

1999 年，加上了两个补充版本：802.11a 定义了一个在 5GHz ISM 频段上的数据传输速率可达 54Mbit/s 的物理层；802.11b 定义了一个在 2.4GHz 的 ISM 频段上但数据传输速率高达 11Mbit/s 的物理层。2.4GHz 的 ISM 频段为世界上绝大多数国家通用，因此 802.11b 得到了最为广泛的应用。苹果公司把自己开发的 802.11 标准起名叫 AirPort。1999 年工业界成立了 Wi-Fi 联盟，致力解决符合 802.11 标准的产品的生产和设备兼容性问题。802.11 标准和补充如下。

802.11，1997 年，原始标准（2Mbit/s 工作在 2.4GHz）。

802.11a，1999 年，物理层补充（54Mbit/s 工作在 5GHz）。

802.11b，1999 年，物理层补充（11Mbit/s 工作在 2.4GHz）。

802.11c，符合 802.1D 的媒体接入控制层（MAC）桥接（MAC Layer Bridging）。

802.11d，根据各国无线电规定做的调整。

802.11e ，对服务等级（Quality of Service，QoS）的支持。

802.11f，基站的互连性（Interoperability）。

802.11g，物理层补充（54Mbit/s 工作在 2.4GHz）。

802.11h，无线覆盖半径的调整，室内（indoor）和室外（outdoor）信道（5GHz 频段）。

802.11i，安全和鉴权（Authentification）方面的补充。

802.11n，导入多重输入输出（MIMO）和 40Mbit 通道宽度（HT40）技术，基本上是 802.11a/g 的延伸版。

1.3　园区网络规划与设计

1.3.1　园区网络的概念

园区网通常是指大学的校园网及企业的内部网（intranet），其本质就是局域网。可以从几个方面对园区网络进行划分，如根据局域网采用的拓扑结构，可分为总线型局域网、环形局域网、星形局域网和混合型局域网等，这种分类方法比较常用。按局域网使用的协议或媒体访问控制方法，可以将局域网分为以太网、令牌环网等。还可以按数据的传输速度分为 10Mbit/s 局域网、100Mbit/s 局域网、千兆局域网等。按信息的交换方式可分为交换式局域网、共享式局域网等。从园区网组网工程规模大小的角度，我们可以将园区网分为小型园区网、中型园区网以及大型园区网。

小型网络是针对“对等网”或基于服务器、集线器、交换机的初级网络系统。小型网络的需求相对简单，将若干台计算机连接起来，组成对等的网络，计算机之间可以相互之间共享资源，如果其中一台计算机安装了打印机、扫描仪等，其余计算机可以通过网络系统共享打印机和上网服务。中型网络是指那些 PC 和网络设备数量在 50～250 之间的网络，而大型网络可能包括上千台到上万台的终端设备。大型网络大多采用分布式交换网络设计，具有

清晰的分层模型。充分考虑各个主机的流量需求，关键设备实现冗余备份，路由技术和交换技术的有机结合，构建一个高速、稳定、可靠的多业务实施解决方案。

1. 小型园区网

小型园区网主要用来实现网内用户全部信息资源共享。此类局域网往往接入的计算机节点较少，一般在 20 ~ 50 台之间，而且各个节点相对集中，每个节点与集线器或交换机之间的距离不超过 100m，采用双绞线进行结构化布线就足够了。

在选用硬件方面，交换机十分强调端口的交换能力，内置交换模块性能比集线器高出许多，采用交换机可以提高整个网络的性能。另一方面，由于现在低端桌面交换机价格比较便宜，比集线器价格贵不了多少，因此可以采用桌面交换机。

2. 中型园区网

中型园区网的规模较小型园区网略大一些，需要连接的计算机节点一般在 60 台以上，并且各个节点的距离也较远，一般超过 100m 甚至更远，利用双绞线作为传输介质已经远远不够。而且此时对网络性能的要求也比较高，对网络的传输速度也有一定的要求，因此可以使用光纤介质来连接整个网络的主干网络，从而使网络可以有较长的传输距离（2km 以上）。

中型园区网可以采用两层结构，即中心交换机层和供各个节点连入的桌面交换机层。中心交换机可以采用高档的企业级交换机，提供多个千兆网络端口。各个节点的桌面交换机连接到中心交换机上，每一个桌面交换机内部就相当于一个小型园区网。

3. 大型园区网

由于大型的企业园区网的覆盖范围极广，如学校、企业、工厂、政府机构等，因此，必须采用性能优良、功能强大的设备才能保证整个系统稳定、安全、可靠地运行。建立大型园区网时需要考虑的因素很多，需要大型园区网的企业一般都把高性能的网络通信摆在性能需求的第一位。这种大型网络应该使用千兆以太网，中心交换机可选用企业级高密度中型交换机，适宜采用两层结构或者三层结构。三层结构是以中型局域网为基点进行扩展的，多个中型局域网的骨干交换机连接到中心交换机上。这两种方案的选择应根据实际情况来定，如果整个园区网比较分散，部分节点比较集中，则利用三层结构较好；如果各个节点之间都比较分散，桌面交换机到骨干交换机的距离较远，则采用两层结构较为合理。当然也可以采用两层结构和三层结构混合的方法，把相对集中的桌面交换机通过骨干交换机汇集起来连接到中心交换机上，而分散的节点直接接到中心交换机上。

1.3.2 大型园区网络规划与设计

大型园区网络建设工程是一项复杂的系统工程，涉及技术问题、管理问题、组织问题、经费问题。它通常是伴随着现代智能建筑建设的发展而发展，特别是现代建筑中的任何一个楼宇都无法离开网络的建设。大型园区网络规划与设计必须遵守一定的系统分析和设计方法。网络规划设计要处理好整体建设与局部建设、近期建设与远期建设之间的关系，根据用户近期需求、经济实力和中远期发展趋势，结合网络技术的现状和发展进行综合考虑，特别是因网络技术的飞速发展，要具有一定的前瞻性、可扩展性。网络规划设计应解决以下几个主要问题：

1）为什么要建设计算机网络——建设计算机网络的目的。

2）计算机网络可以解决哪些问题——建设计算机网络的目标。

3）建设什么样的计算机网络——计算机网络方案设计。

本节以组建大型校园网为例，讲述大型网络的规划和设计步骤。

1. 需求分析

建设计算机网络，要有明确的目的性，只有充分明确了目标，才能更好地有针对性的进行规划设计。需求分析是网络设计的基础，有助于增强设计者对网络功能的理解，给整个网络设计提供参考。需求分析并不是设计者凭经验或主观上写的文档，它需要与客户进行沟通，并将用户模糊的想法明确化、具体化，然后进行有针对性的分析和设计，使网络能满足用户的需求。同时，搞清楚网络应用的约束，掌握网络分析的技术指标，采用适当的分析网络流量的方法，也是网络需求分析中非常重要的内容。可以说，组建网络、需求分析先行。在需求分析中要充分开展调查，了解关于建设网络单位业主的所有关于建筑、员工、技术等各方面的信息，进行广泛走访、资料收集、分析。

2. 综合布线系统规划设计

根据需求分析的结果，基本上可以判断所需要建设的园区网络的规模。首先需要明确建筑规模的大小，比如是一栋楼内的小型局域网络，还是多栋楼宇之间的中型局域网络或是一个大型园区的局域网络。根据所建设网络规模的大小，对建筑物进行分析，决定单栋建筑物内的综合布线系统和楼宇之间的综合布线系统，可以从这两个层面展开设计和分析——综合布线系统的规划与设计。

综合布线系统以一套单一的配线系统，综合通信网络、信息网络及控制网络，可以使相互间的信号实现互联互通。对于新建、扩建、改建建筑与建筑群综合布线系统工程设计必须做到充分重视需求，既要从整体上考虑，也要细化到每一个房间，每一个桌面端口。综合布线系统设施及管线的建设，应纳入建筑与建筑群相应的规划设计之中。在工程设计时，应根据工程项目的性质、功能、环境条件和近、远期用户需求进行设计，并应考虑施工和维护方便，确保综合布线系统工程的质量和安全，做到技术先进、经济合理。在确定建筑物或建筑群的功能与需求以后，规划能适应智能化发展要求的相应的综合布线系统设施和预埋管线，防止今后增设或改造时造成工程的复杂性增加和费用的浪费。综合布线系统作为建筑物的公用通信配套设施，在工程设计中应满足为多家电信业务经营者提供业务的需求。综合布线系统作为建筑的公共电信配套设施在建设期应考虑一次性投资建设，能适应为多家电信业务经营者提供通信与信息业务服务的需求，保证电信业务在建筑区域内的接入、开通和使用；使得用户可以根据自己的需要，通过对入口设施的管理选择电信业务经营者，避免造成将来建筑物内管线的重复建设而影响到建筑物的安全与环境。因此，在管道与设施安装场地等方面，工程设计中应充分满足电信业务市场竞争机制的要求。

目前，业界主要采用的是超五类和六类综合布线系统，在设计方面主要参照执行国家关于综合布线系统工程设计方面的规范对单体楼宇及建筑群之间的光缆进行设计。在建筑群之间主要采用光缆；同时要考虑设计好每一个建筑物内的弱电间、配线间、弱电竖井的位置、管道和管孔的位置、孔径大小等各方面设计细节，以满足网络传输的需求，也符合国家相关设计和施工规范和标准。

3. 网络核心机房设计

目前，园区网络设计规划，一般都要考虑设立园区网络的核心机房，网络核心机房也是

整个网络的核心位置。从组网的角度来看，它是全网的核心所在；从物理位置上看，也应该尽可能地选择园区的中心位置来设计和建立一个网络核心机房。它的面积大小根据网络规模及应用系统规模的大小来决定。

网络核心机房建设是一项非常复杂的工程，特别是面积较大的网络核心机房，从机房选址、电力供应、水源、防火、防雷等各方面都应考虑。我们一般可以将网络核心机房设计分为 8 个子系统来进行规划和设计：机房装修、机房 UPS 电源及其供配电、照明及防雷接地系统、机房空调通风系统、机房综合布线系统、机房动力环境监控系统、消防及火灾自动报警系统、机房 KVM 集中管理系统等。

4. 网络系统集成方案设计

网络系统集成方案设计的根本任务就是要决定采用什么样的组网技术、如何对整个网络进行规划设计、还有设备选型。从组网技术上看，目前基本上最流行的组网技术仍然是以太网技术，主要是千兆以太网和万兆以太网技术。通俗地说，大型园区网络基本上是“万兆骨干、千兆桌面”，万兆以太网技术也是一种非常成熟的技术方案，而且能较好地进行设备选型，能支持各种应用。

在进行组网方案设计时，要考虑楼宇的分布情况、网络机房的设计、信息点的位置以及综合布线系统的规划、弱电间和设备间的设计，要对整个网络进行一个总体上的规划布局。实际上在设计和规划综合布线系统、网络核心机房之后，我们已经将网络规划为一个以网络核心机房为中心的呈星形敷设状的网络架构，即形成一个从核心机房到各弱电机房辐射的一个网络拓扑结构。

在网络设备选型方面，网络设备选型包括传输介质、交换机、路由器、服务器以及其他硬件产品。在进行设备选型时，要充分考虑到需求。在满足需求的情况下，考虑经济原则与性价比等，综合选择最合适的网络设备。坚持适用性与先进性相结合的原则，对不同品牌的交换机等网络产品价格差异较大，功能也不一样，应该根据应用的实际情况，选择具有高性能、高可靠性、高安全性、高可扩展性、高可维护性的产品。选择网络产品时，既要看产品的品牌也要看生产厂商和销售商品是否有强大的技术支持、良好的售后服务。

1.3.3 大型园区网络工程设计原则

根据目前计算机网络的现状和需求分析以及未来的发展趋势，在网络工程设计时应遵循以下几个原则。

1. 开放性和标准化原则

首先采用国际标准和国家标准，其次采用广为流行的、实用的工业标准，只有这样，网络系统内部才能方便地从外部网络快速获取信息。同时还要求在授权后网络内部的部分信息可以对外开放，保证网络系统具有适度的开放性。在进行网络工程设计时，在有标准可执行的情况下，一定要严格按照相应的标准进行设计，标准可以确保这个网络能做到完美的兼容性。

2. 实用性与先进性兼顾原则

在进行网络工程设计时首先应该以注重实用为原则，紧密结合具体应用的实际需求。在选择具体的网络技术时一定要同时考虑当前及未来一段时间内主流应用的技术；另一方面，最新技术的产品价格非常昂贵，会造成不必要的资金浪费。在选择技术时，一定要选择主流

应用的技术，如像同轴电缆的令牌环以太网和 FDDI 光纤以太网目前已很少使用，就不要选用了。目前的以太网技术基本上都是基于双绞线和光纤作为传输介质，其传输速率最低都应达到 100/1000Mbit/s 甚至 10000Mbit/s；这些技术都比较成熟，可做到充分兼顾实用性和先进性。

3. 无瓶颈原则

网络性能与网络安全一样，最终取决于网络通信链路中性能最低的那部分。进行网络工程设计时一定要综合考虑各部分的性能，而不能只注重局部的性能配置。特别是交换机端口、网卡和服务器组件配置等方面的匹配性。

如某汇聚层交换机连接到了核心交换机的 1000Mbit/s 双绞线以太网端口上，而该汇聚层交换机却只有 100Mbit/s 甚至 10Mbit/s 的端口，很显然这个汇聚层交换机上所连接的节点都只能享有 10Mbit/s 或 100Mbit/s 的性能。如果上联端口具有 1000Mbit/s 性能，而各节点端口支持 100Mbit/s 连接，则性能就完全不一样了。还如服务器的各项硬件配置都非常高档（达到了企业级标准），但所用的网卡却只是普通的 PCI 10/100Mbit/s 网卡，显然这又将成为服务器性能发挥的瓶颈。

4. 可用性原则

网络系统的“可用性”通常是由网络设备（软件系统其实也有“可用性”要求）的“可用性”决定的，主要体现在服务器、交换机、路由器、防火墙等关键设备上，尽量选择国内外知名品牌、应用主流技术和成熟型号的产品。另外，网络系统的电源供应在可用性保障方面也非常重要。通常像服务器、交换机、路由器、防火墙之类的关键设备要接在支持数个小时以上（通常是后备 4h）的 UPS 电源上。

5. 适度安全性原则

网络安全涉及许多方面，最明显、最重要的就是对外界入侵、攻击的检测与防护。在一个安全措施完善的计算机网络中，不仅要部署病毒防护系统、防火墙隔离系统，还可能要部署入侵检测、木马查杀系统和物理隔离系统等。所选用系统的具体等级要根据相应网络规模的大小和安全需求而定。

网络系统的安全性需求还体现在用户对数据的访问权限上，一定要根据对应的工作需求为不同用户、不同数据配置相应的访问权限。对于高权限账户的安全应受到高度重视，要采取相应的账户防护策略（如密码复杂性策略和账户锁定策略等），保护好用户账户，以防被非法用户盗取。

在安全性防护方面，还有一个重要的方面，就是数据备份和容灾。特别是企业数据主要是电子文档的电子商务类企业。在设计网络系统时，一定要充分考虑到用户对数据备份和容灾的需求，部署相应级别的备份和容灾方案。

6. 可扩展性原则

这是为了适应用户业务和网络规模发展的需求，相当重要，特别是对于中小型企业网络来说。这类企业一般成长较快，很可能不到三年时间，网络用户规模就要翻倍，关键应用带宽需求也可能成倍增加。这时如果所设计的网络系统的可扩展性不强，就会给网络用户和性能的扩充带来极大的不便。

网络的可扩展性主要是通过交换机端口、服务器处理器数、内存容量、磁盘架数等来保证。通常要求核心层或骨干层，甚至汇聚层交换机的高速端口（通常为千兆端口）要有两

个以上用于维护和扩展。

1.3.4 组网需求分析

组建网络之前要进行需求分析，主要是了解用户目前的现状，现在和未来需要的功能、性能上有何要求以及建设成本效益等。对可行性研究阶段中所收集的有效数据进行分析，在此基础上依据计算机网络建设的方向、原则和作用，规划计算机网络的建设，为网络设计提供必要的条件。

1. 需求分析的类型

（1）应用背景分析

应用背影分析概括了当前网络应用的技术背景，介绍了行业应用的方向和技术趋势，说明了本企业网络信息化的必然性。应用背景分析要回答一些为什么要实施网络集成的问题。

1）国外同行业的信息化程度以及取得哪些成效。

2）国内同行业的信息化趋势如何。

3）本企业信息化的目的是什么。

4）本企业拟采用的信息化步骤如何。

（2）业务需求分析

目标是明确企业的业务类型、应用系统软件种类以及它们对网络功能指标（如带宽、服务质量 QoS）的要求。业务需求是企业建网中首要的环节，是进行网络规划与设计的基本依据。通过业务需求分析为以下方面提供决策依据。

1）需实现或改进的企业网络功能有哪些。

2）需要集成的企业应用有哪些。

3）需要电子邮件服务吗。

4）需要 Web 服务吗。

5）需要上网的网速或带宽是多少。

6）需要提供网络视频服务吗。

7）需要什么样的数据共享模式。

8）计划投入的资金规模是多少。

9）对网络可靠性的要求是怎么样的。

（3）网络管理需求分析

网络管理是企业建网不可或缺的方面，网络是否按照设计目标提供稳定的服务主要依靠有效的网络管理。高效的管理策略能提高网络的运营效率，建网之初就应该重视这些策略。网络管理的需求分析要回答以下问题。

1）是否需要对网络进行远程管理，远程管理可以帮助网络管理员利用远程控制软件管理网络设备，使网管工作更方便、更有效。

2）谁来负责网络管理。

3）需要哪些管理功能，如需不需要计费，是否要为网络建立域，选择什么样的域模式等？

4）选择哪个供应商的网管软件，是否有详细评估。

5）选择哪个供应商的网络设备，其可管理性如何。

6）需不需要跟踪和分析处理网络运行信息。

7）将网管控制台配置在何处。

8）是否采用了易于管理的设备和布线方式。

（4）网络安全需求分析

网络安全需求分析要明确以下几点。

1）企业的敏感性数据的安全级别及其分布情况。

2）网络用户的安全级别及其权限。

3）可能存在的安全漏洞，这些漏洞对本系统的影响程度如何。

4）网络设备的安全功能要求。

5）网络系统软件的安全评估。

6）应用系统安全要求。

7）采用什么样的杀毒软件。

8）采用什么样的防火墙技术方案。

9）安全软件系统的评估。

10）网络遵循的安全规范和达到的安全级别。

（5）通信量需求分析

通信量需求是从网络应用出发，对当前技术条件下可以提供的网络带宽做出评估。通信量分析通常需要考虑以下几个问题，见表 1-1。

表 1-1　通信量需求分析

应用类型	基本带宽需求	备　　注
PC 连接	56kbit/s ~ 1Mbit/s	远程连接，FTP、HTTP、E-mail
文件服务	100kbit/s ~ 1Mbit/s 以上	局域网内文件共享，C/S 应用，B/S 应用，在线游戏等绝大部分纯文本应用
压缩视频	2100kbit/s ~ 1Mbit/s 以上	MP3、rm 等流媒体传输
非压缩视频	2Mbit/s 以上	Vod 视频点播、视频会议等

1）未来有没有对高带宽服务的要求。

2）需不需要带宽接入方式，本地能够提供的带宽接入方式有哪些。

3）哪些用户经常对网络访问有特殊的要求，如行政人员经常要访问 OA 服务器，销售人员经常要访问 ERP 数据库等。

4）哪些用户需要经常访问 Internet，如客户服务人员经常要收发 E-mail。

5）哪些网络设备能提供合适的带宽，性价比较高。

6）哪些服务器有较大的连接数。

7）需要使用什么样的传输介质。

8）服务器的网络应用是否能够支持负载均衡。

（6）网络扩展性需求分析

网络扩展性有两层含义，其一是指新的部门能够简单地接入现有网络；其二是指新的应用能够无缝地在现有网络上运行。扩展性分析要明确以下指标。

1）企业需求的新增长点有哪些。

2）已有的网络设备和计算机资源有哪些。

3）哪些设备需要淘汰，哪些设备还可以保留。

4）网络节点和布线的预留比率是多少。

5）哪些设备便于网络扩展。

6）主机设备的升级性能。

7）操作系统平台的升级性能。

（7）网络环境需求分析

网络环境需求是指对企业的地理环境和人文布局进行实地勘察以确定网络规模、地理分划，以便在拓扑结构设计和结构化综合布线设计中做出决策。网络环境需求分析需要明确下列指标。

1）园区内的建筑群位置。

2）建筑物内的弱电井位置、配电房位置等。

3）各部分办公区的分布情况。

4）各工作区内的信息点数目和布线规模。

2. 如何获取网络规划与设计需求

获取网络规划与设计需求通常有四种方式。

1）实地考察。实地考察是工程设计人员获得第一手资料采用的最直接的方法，也是必需的步骤。

2）用户访谈。用户访谈要求工程设计人员与工程单位的负责人通过面谈、电话交谈、电子邮件等通信方式以一问一答的形式获得需求信息。

3）问卷调查。问卷调查通常对人数较多的最终用户提出，询问其对将要建设的网络应用的要求。问卷调查的方式可以分为无记名问卷调查和记名问卷调查。

4）向同行咨询。将获得的需求分析中不涉及商业机密的部分发布到专门讨论网络相关技术的论坛或新闻组中，请同行审阅已制定的设计说明书，很多热心的同行，通常会给出许多中肯的建议。

1.3.5 园区网络建设的性能目标

了解客户的建设目标及其约束是网络设计中一个非常关键的方面，只有对客户的建设目标进行透彻分析，才能提出客户认可的网络设计方案。

1. 网络设计目标分析和约束

常见的网络设计目标包括：增加收入和利润、提高市场占有份额、拓展新的市场空间、提高在同一市场内同其他公司竞争的能力、降低费用、提高员工生产力、缩短产品开发周期、使用即时生产方法、制订解决配件短缺的加护、为新客户提供服务、支持移动性、为客户提供更好的支持、为关键要素开发网络、建立达到新水平的良好的信息网和关系网以作为网络组织化模型的基础、避免网络安全问题引发商业中断、避免自然或人为灾害引发商业中断、对过时的技术进行更新改造、降低电信和网络费用并在操作上进行简化等。

进行网络目标分析的步骤包括：首先，从企业高层管理者开始收集业务需求；其次，收集用户群体需求；最后，收集为支持用户应用所需要的网络需求。

在同客户见面之前，最好先调查客户所从事的基本业务信息，如了解客户所属的行业和客户的市场、供应商、产品、服务、竞争优势和财务状况。在同客户见面时，首先要有有关网络工程项目目标的简要叙述。接着，获取有关公司的组织结构图。最后，获取有关安全策略。

在网络设计目标分析和判断用户给出新的网络应用需求时，网络约束对网络设计影响很大。常见的网络约束主要有政策约束、预算约束、时间约束、技术约束、人员约束。

2. 网络技术目标分析

在分析网络设计技术要求时，应当列出用户能够接受的网络性能标准，如延迟、效率、吞吐量、相应时间等。这样技术指标和性能指标就为后期网络升级或更新提供了一种比较依据，这种依据就是性能基线（Baseline）。

（1）可扩展性

可扩展性指的是网络设计应该支持多大程度的网络扩展。网络分层设计易于扩展，平面式网络设计可扩展性差。如下问题属于可扩展性技术目标范畴：在以后的一年里能增加多少站点？在以后的两年里情况如何？每一个新站点的网络范围有多大？在未来的一年中将有多少新的用户访问公司的互联网？未来的两年情况如何？在未来的一年里将会在互联网中增加多少台服务器？

（2）可用性

可用性可以用每年、每月、每天或者每小时内正常工作的时间占该时期总时间的百分率来表示。例如：24/7 运转、在 168h 一周内网络可用 165h、可用性为 98.21% 等。不同的应用程序可能需要不同的可用性级别，关键设备或部门、企业可能需要 99.999%（即“5 个 9”）可用性目标。

衡量可用性通常采用失败的平均时间（MTBF）和修复的平均时间（MTTR）来定义。公式如下：

可用性 = MTBF/（MTBF + MTTR）

例如：网络每 4000h（166 天）失效不能多于一次，并且要在一个小时内修复，则该网络的可用性 = 4000/4001 = 99.98%。

影响可用性的因素主要有可靠性、用户流量的容量、网络冗余、网络弹性（指网络可以承受的压力）等。

（3）网络性能

网络性能也是技术目标的一种，是用户使用网络过程中最关注的一个技术指标。通常性能包括宽带、吞吐量、带宽利用率、提供负载、准确性、效率、延迟和延迟变化、响应时间等。

1）带宽：对于网络链路，带宽（bandwidth）用来衡量单位时间内传输比特的能力，通常用 bit/s 表示，分物理带宽和逻辑带宽。为了能够正常工作，不同类型的应用需要不同的带宽。

2）吞吐量：吞吐量是指单位时间内无差错地传输数据的能力，通常以 bit/s、B/s 或分组/秒（pps）度量。与吞吐量相关的参数通常是通道容量和网络负载。吞吐量和有效吞吐量是两个概念，前者是知道字节/秒，而不管用户数据字节或分组头部字节；后者是指应用层用户字节的吞吐率，有时又称“有效吞吐率”，即每个分组头部浪费掉的带宽不包括在

内。有效吞吐量越高，相应时间越快。影响吞吐量的因素主要包括：分组的大小、分组之间的间隙、转发分组设备的速率（分组/秒）、网络设计、协议、距离、错误率、具体访问时间等。

3）效率：通常指发送一定数量数据需要多少开销。从有效吞吐量角度来看，帧越大，效率越高；帧越小，效率越低。但是，如果出现帧的丢失或者重传，则效率明显降低。

4）响应时间：是指请求和响应之间的时间。通常响应时间不仅与网络相关，同时还与应用程序及其所运行的设备相关。大多数用户期望在 100 ~ 200ms 内在显示器上看到有关内容，即客户默认可以接受的响应时间。影响响应时间的常见因素包括轮询延迟（如令牌网）、连接延迟、CPU 延迟、网卡延迟、物理介质传播延迟。

5）延迟：是指一个帧准备从一个节点传送，并传送到网络里其他节点所花的时间。引起延迟的原因主要包括：传播延迟（信号在电缆或光纤中传播速度仅为真空中传播的 2/3）、发送延迟（又称串行延迟，即将数字数据放到传输线上所需要的时间，例如，在 1.544Mbit/s T1 线上输送 1024 字节需要 5ms）、分组交换延迟、排队延迟和重传延迟。解决延迟的常见方法是增加带宽和选择高级队列算法。

6）抖动：即平均延迟的时间变化量，又称为延迟变化。在网络设计中，语音、视频和音频应用不允许发生抖动。如果客户提不出具体要求，则延迟变化量应该小于延迟的 1% 或 2%。即如果平均延迟为 200ms 分组，则抖动不应该高于 2 ~ 4ms。减少抖动的方法就是为语音、视频和音频提供较大的缓存。

7）丢包率：是指在一定的时段内在两点间传输中丢失分组与总的发送分组的比率。根本原因在于网络对分组的传输是按“尽力而为”方式进行的，直接原因是存储分组队列空间慢和网络链路带宽拥塞。无拥塞时，路径丢包率为 0%，轻度拥塞时丢包率为 1% ~ 4%，严重拥塞时丢包率为 5% ~ 15%。对用户来讲，丢包率高的网络通常使应用不能正常工作。

8）利用率：反映指定设备在使用时所发挥的最大能力。在网络设计中通常考虑两种类型的利用率：CPU 利用率和链路利用率。

（4）安全性

安全目标是指实现安全的费用不超过从安全事故中恢复所需的费用。安全性分析首先要获取需要保护的财产，其次制定详细的安全规划，如确定网络资产，包括价值和期望费用以及因安全丢失后的问题、安全风险分析等。在局域网设计中，需要保护的资产包括硬件、软件、应用、数据、知识产权、商业机密和公司信誉等。

（5）可管理性

通过管理工具，可以帮助组织取得可用性、性能和安全目标，帮助机构测量网络设计是否满足目标，不满足时则可以通过调整网络参数来实现。借助简单网络管理协议（Simple Network Management Protocol，SNMP）可以轻松实现网络的可管理性。

（6）易用性

易用性是指网络用户访问网络和服务的难易程度。主要目的是为了使网络用户的工作更容易进行。通过用户培训，可以改善用户访问网络和服务的难易程度；严格的安全或访问控制则会从负面影响易用性。

（7）适应性

适应性是指适应技术上的变化和更新。灵活的网络设计能适应变化的通信模式和服务质

量（Quality of Service，QoS）需求。同时，尽量排除会使未来新技术的使用变得困难的任何因素。

（8）可付性

可付性是指可以承担得起的网络设计应在给定的财务成本下承载最大的流量。局域网和园区网设计中可付性尤其重要，而企业网则表示在可用性方面。在以流量为计费标准的局域网中，接入网电路每月重复的花费是造成运行大型网络成本很高的一个主要原因，因此可以选用适当的技术加以降低。例如使用静态默认路由、采用支持数据压缩的封装协议提高数据传输效率、动态分配广域网带宽等技术解决。

在实际网络设计中，需要做出折中才能达到目标。为了帮助集成商分析折中，需要客户确定一个最主要的网络设计目标。这些目标可以是商业目标，也可以是技术目标。除此之外，还必须要求客户区分剩余目标的优先顺序，区分优先顺序将有利于完成网络设计折中方案。表 1-2 是一个折中方案，要求客户将他们想花费在可扩展性、可用性、网络性能、安全性、可管理性、易用性、适用性、可付性等方面的成本比例做个选择。

表 1-2　网络技术目标所占比例表

技术指标	所占比例	技术指标	所占比例
可扩展性	20%	可管理性	5%
可用性	25%	易用性	10%
网络性能	15%	适应性	5%
安全性	5%	可付性	15%

折中方案比实际方案描述起来要复杂得多，因为一个技术目标需要其他技术目标的支持或与其他技术目标存在关联。通常来讲，校园网可付性比可用性重要，企业网可用性比可付性重要。

1.3.6　园区网络建设的步骤

设计和实现网络系统遵从一定的网络系统集成模型。模型从系统开始，经历用户需求分析、逻辑网络设计、物理网络设计和测试，并贯彻网络工程监理。即采用自顶向下的网络设计方法，从 OSI 参考模型上层开始，然后向下直到底层的网络设计方法。它在选择较低层的路由器、交换机和媒体之前，主要研究应用层、会话层和传输层功能。该模型是可以循环反复的，并且是进行网络工程设计的第一步。

通常来讲，网络工程系统集成步骤主要包括以下几个方面。

1. 选择系统集成商或设备供应商

建设小型网络，只需选择适当的网络设备和网络设备供应商。如果要建设大中型网络系统，就需要选择系统集成商。用户以招标的方式选择系统集成商，对网络系统的意愿应体现在发布的招标文件上。系统集成商的公司资质、公司业绩、技术实力、公关能力和谈判技巧等综合表现是能否中标的关键。

2. 用户需求分析

用户需求分析是指确定网络系统要支持的业务、要完成的功能、要达到的性能等。通常来讲，网络设计者应从以下三个方面进行用户需求分析：网络的应用目标、网络的应用约束

和网络的通信特征。

3. 逻辑网络设计

在逻辑网络设计中，重点是网络系统如何部署和网络拓扑等细节设计。主要工作包括网络拓扑设计、网络分层设计、IP 地址规划、路由和交换协议选择、网络管理和安全等。

4. 物理网络设计

主要任务包括网络环境设计和网络设备选型，其中网络环境设备主要是指结构化布线系统设计、网络机房设计和供电系统设计等方面；网络设备选型主要是指园区网设备选型和企业网设备选型。

5. 网络安全设计

网络安全是网络集成系统中必须面对的重要问题，涉及资源、设备、数据等资产。设计上，首先界定要保护的资源；其次制定安全策略，采购安全产品；最后，设计适合需要的网络设计方案。

6. 网络设备安装调试和验收

网络设备在正式交付使用之前，必须在仿真环境上经过测试。常见的网络测试包括网络协议测试、布线系统测试、网络设备测试、网络系统应用测试、安全测试等多个方面。

7. 网络系统验收

网络系统验收是指用户方正式认可系统集成商完成的网络工程阶段。这一阶段确认工程项目是否达到设计要求。验收分为现场验收和文档验收。现场验收需要检验环境是否符合要求；文档验收需要检验开发文档、管理文档和用户文档是否完备。

8. 用户培训和系统维护

网络一旦交工，后期维护是非常重要且繁琐的一件事情。系统集成商或设备供应商必须为用户提供必要的培训，培训对象可以是网管人员、一般用户等。培训可分为现场培训和指定地点培训，同时还涉及以合同方式提供产品、设备售后服务和免费技术支持等。

1.4 园区网络逻辑设计

1.4.1 网络拓扑的选择

随着电子集成技术和通信技术的发展，局域网拓扑结构也在不断地变化和更新。在 20 世纪 60 年代推出了环形拓扑结构和星形拓扑结构，随着分布式控制的发展，20 世纪 70 年代推出了总线型和树形拓扑结构。目前，局域网的拓扑结构主要有：星形、环形、总线型、树形、网状型和混合型等几种。其中，前三种是广泛应用的网络拓扑结构单元，实际的企业网络拓扑结构基本上是这三种网络结构单元混合组成的，如后面的树形、混合型结构。网状结构在局域网中目前基本上不单独采用，只是在一个网络中的局部采用，主要用于冗余连接。目前的实际应用中，网络的物理拓扑结构一般都采用星形连接，星形连接在将用户接入网络时具有更大的灵活性，当系统不断发展或当系统发生重大变化时，这种优点将显得更加突出。为网络的平滑升级创造了先天条件。

星形结构是目前应用最广、实用性最好的一种拓扑结构，可在不影响系统其他设备工作的情况下很方便地增加或减少设备。无论在局域网中，还是在广域网中都可以见到它的身

影，但主要应用于双绞线以太局域网中。它采用的传输介质是常见的是双绞线和光纤，担当集中连接的设备是具有双绞线的 RJ-45 以太网端口，或各种光纤端口的集线器或交换机。星形结构的主要优点有网络传输数据快，实现容易，成本低，节点扩展和移动方便，维护容易；主要缺点有核心交换机工作负载重，网络布线比较复杂，广播传输影响网络性能。典型的星形网络扣扑结构如图 1-4 所示。

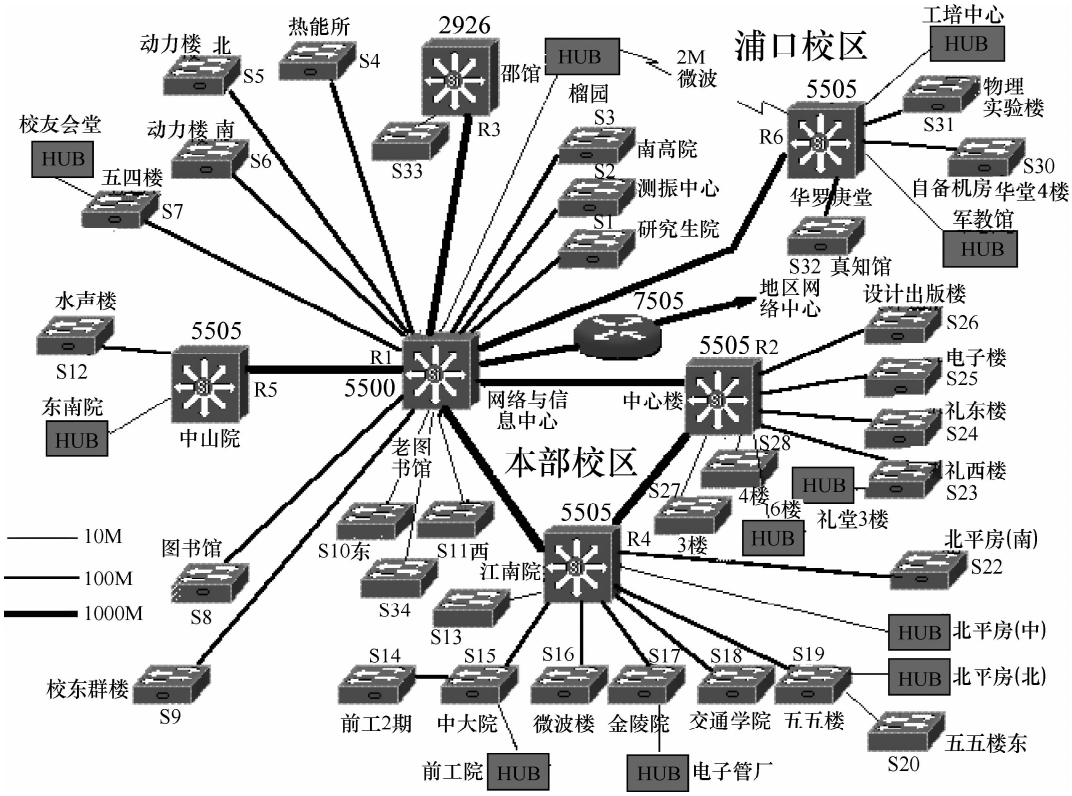


图 1-4　典型的星形网络拓扑结构

1.4.2　网络分层结构设计

1. 层次化网络结构设计

三层网络架构采用层次化模型设计，即将复杂的网络设计分成几个层次，每个层次着重于某些特定的功能，这样就能够使一个复杂的大问题变成许多简单的小问题。如图 1-5 所示，三层网络架构设计的网络有三个层次：核心层（网络的高速交换主干）、汇聚层（提供基于策略的连接）、接入层（将工作站接入网络）。

对于一个中小型园区网络，常见的只有接入层和核心层两层结构。核心层设备充当了接入层的网关功能，既做交换也做路由。这是一种比较简单的方式，但是对于大型园区网络，基本上都是按照三层结构来进行设计和划分的，从二层交换技术的网络架构调整到三层交换技术的网络架构，网络的优化效果明显，配之以网管软件，网络的安全性和可防护性大为提高。通过合理配置核心交换机，充分发挥了核心交换机的硬件性能，调整核心交换机在带宽、网络流量处理能力位置结构，具备良好的扩展性，根据业务需求划分 VLAN，控制广播

范围，抑制广播风暴，提高了局域网的整体性能和安全性。如图 1-6 展示了一个经典的三层网络架构。

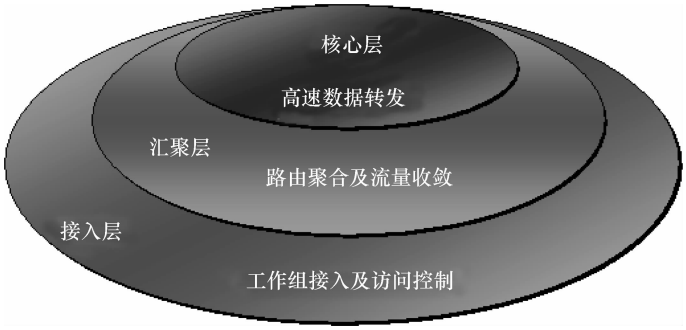


图 1-5　层次化网络及功能划分

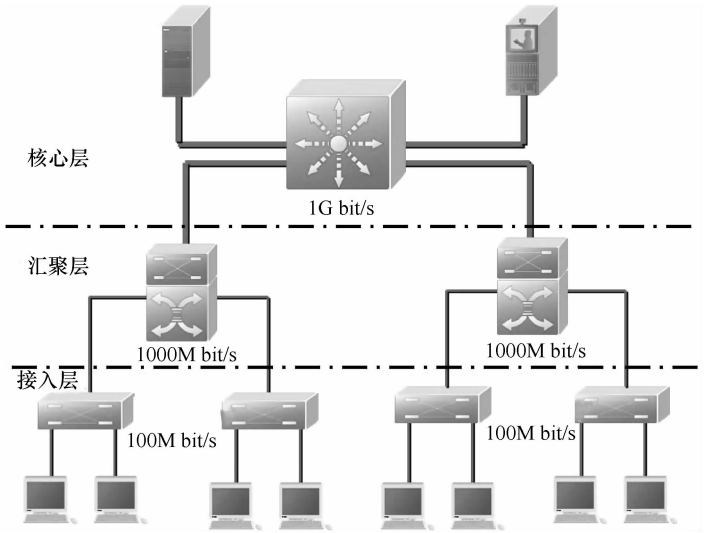


图 1-6　三层网络架构

（1）核心层

核心层的功能主要是实现骨干网络之间的优化传输，负责整个网络的网内数据交换。核心层设计任务的重点通常是在冗余能力、可靠性和高速的传输等方面。

核心层是网络的骨干，必须能够提供高速数据交换和路由快速收敛，要求具有较高的可靠性、稳定性和易扩展性等。对于大型局域网的核心层，必须提供高性能、高可靠的网络结构。核心交换机设备应该在提供大容量、高性能 L2/L3 交换服务的基础上，能够进一步融合硬件 IPv6、网络安全、网络业务分析等智能特性，可为校园园区构建融合业务的基础网络平台，进而帮助用户实现 IT 资源整合的需求。

（2）汇聚层

汇聚层主要负责连接接入层接点和核心层中心，汇集分散的接入点，扩大核心层设备的端口密度和种类，汇聚各区域数据流量，实现骨干网络之间的优化传输。汇聚交换机还负责

本区域内的数据交换，汇聚交换机一般与中心交换机同类型，仍需要较高的性能和比较丰富的功能，但吞吐量较低。

汇聚层来自分布在某个楼宇的接入层交换机的流量，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；对于大型局域网的汇聚层设备，应该能够承载多种融合业务，能够融合 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（Graceful Restart）、环网保护等多种高可靠技术，能够承载大型园区融合业务的需求。

（3）接入层

接入层网络作为二层交换网络，提供工作站等设备的网络接入，设备端口比较密集。接入层在整个网络中接入交换机的数量最多，具有即插即用的特性。对此类交换机的要求，一是价格合理；二是可管理性好，易于使用和维护；三是有足够的吞吐量；四是稳定性好，能够在比较恶劣的环境下稳定地工作。

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。对于大型局域网的接入层设备，现在普遍采用千兆接入的方式，应该具有丰富的 ACL 策略以及高级 QoS 策略等功能。

2. 冗余拓扑网络结构设计

很多行业和企业用户，对网络都有实时性的要求，比如金融、证券、航空、铁路、邮政以及一些企业用户等，其网络一旦出现故障，将会带来巨大的经济损失；但网络涉及环节非常多，比如说线路、电信的设备等，任何一个环节出现问题，都会导致整个网络传输运行的停止。所以应该给用户提供冗余的网络，作为重要的网络设备路由器和核心交换机，就是通过备份来实现网络的冗余，确保网络的畅通。

在具有单点故障隐患的网络连接中，一个核心节点或汇聚节点的故障往往会导致下连所有节点设备的业务中断；或下连节点设备有大流量业务冲击时，上层设备处理能力不够。所以在高可用的网络设计中可采用“网络节点冗余 + 链路冗余”的设计方法。例如，核心级设备的双机热备、双链路接入。如果网络中存在单点故障的隐患，且该隐患处于核心层位置，则网络的可用性受到挑战，进而整个企业的 IT 业务应用也存在隐患。

为了提高整个网络的可靠性，核心交换机采用双机热备份、负载平衡方式，即两台核心交换机正常情况下都参与工作，当其中的任何一台发生故障时，另外一台可以自动、无缝地接管它的工作，这对网络管理员、用户来说都是透明的，无需人工干预故障切换，提高了网络对突发事故的自动容错能力，最小化网络的失效时间。

如图 1-7 所示，核心层采用双机热备的技术，可以防止网络结构中的单点故障，提高企业网络的可用性。在核心层网络中采用双机热备的冗余网络节点的方式，通过冗余协议配置，正常情况下业务应用的数据可通过两台核心设备转发，降低了大业务量对单台核心设备的压力；当一台核心层设备故障的时候，接入层设备的业务可以自动切换到另外一台核心层设备上正常转发，增强了网络对单点设备故障的容错能力。

1.4.3　IP 地址规划与分配

IP 地址的合理规划是网络设计中的重要一环，在设计大型园区网络时，必须考虑对整个园区网络进行 IP 地址的规划和设计。IP 地址规划的好坏，影响到网络路由协议算法的效

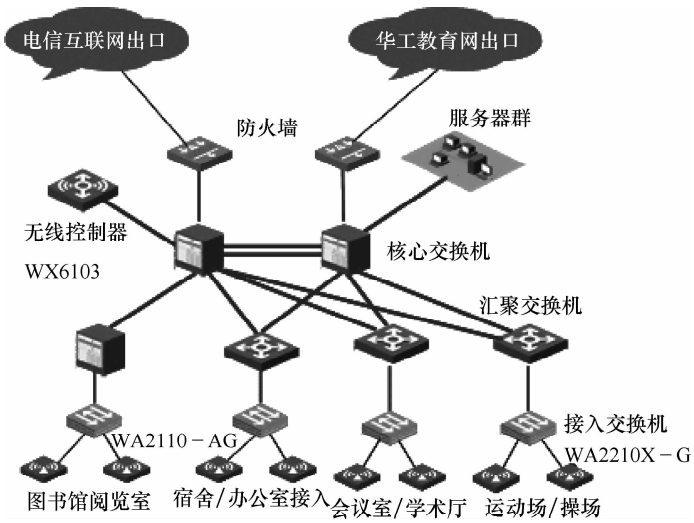


图 1-7　冗余网络设计

率，影响到网络的性能，影响到网络的扩展，影响到网络的管理，也必将直接影响到网络应用的进一步发展。因此，对于一个网络的逻辑设计，IP 地址规划是最重要的，必须针对全局来统一规划。

1. IP 地址分配原则

IP 地址空间分配，要与网络拓扑层次结构相适应，既要有效地利用地址空间，又要体现出网络的可扩展性和灵活性，同时能满足路由协议的要求，以便于网络中的路由聚类，减少路由器中路由表的长度，减少对路由器 CPU、内存的消耗，提高路由算法的效率，加快路由变化的收敛速度，同时还要考虑到网络地址的可管理性。具体分配时要遵循以下原则：

1）唯一性：一个 IP 网络中不能有两个主机采用相同的 IP 地址。

2）简单性：地址分配应简单，易于管理，降低网络扩展的复杂性，简化路由表项。

3）连续性：连续地址在层次结构网络中易于进行路径叠合，大大缩减了路由表，提高了路由算法的效率。

4）可扩展性：地址分配在每一层次上都要留有余量，在网络规模扩展时能保证地址叠合所需的连续性。

5）灵活性：地址分配应具有灵活性，以满足多种路由策略的优化，充分利用地址空间。

主流的 IP 地址规划方案分为纯公网地址、纯私网地址和混合网络地址三种。对于一般的园区网络而言，通常是使用私网地址，然后在出口设备上实现 NAT 功能。

2. IP 地址规划方案

一般需要对园区网络的 IP 地址进行严格编码，每位代表不同的含义。其编码规则如图 1-8 所示。

通过地址标识可以清楚地区分出 IP 地址的来源，便于路由汇聚和访问控制。从上图中我们也可以看出，通过规划，我们能从 IP 地址分析出 IP 地址的来源、用途等，这将为网络的维护带来方便。具体的 IP 地址定义将结合实际情况确定。核心交换机支持静态或动态的

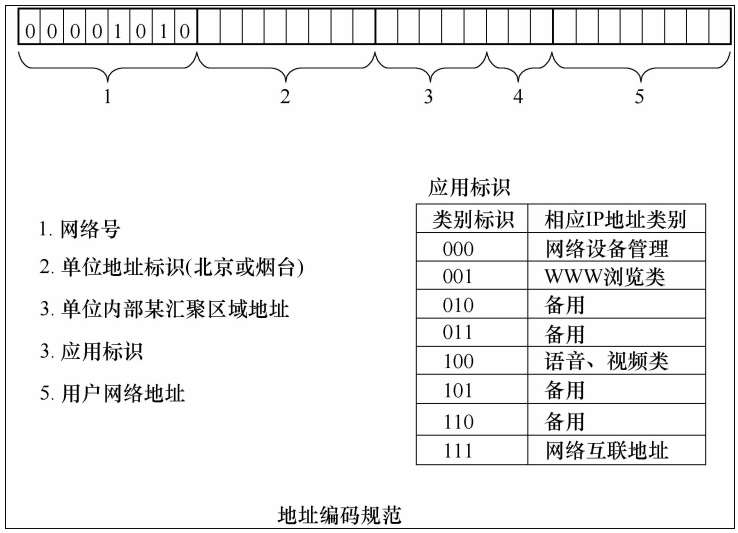


图 1-8　IP 地址编码规则

IP 地址分配，并支持动态 IP 地址分配方式下 DHCP-Relay 功能，DHCP SERVER 可安放在园区内部。对于固定 IP 地址用户，需要针对标识符（MAC 地址）设定保留 IP 地址。对于所有的网络设备，还需要配置管理 IP，以便实现远程管理。

3. IPv4 路由规划

对于大型园区网络，整个骨干网络一般采用 OSPF（Open Shortest Path First，开放式最短路径优先）路由协议，OSPF 协议在整个骨干网中不会引起路由回环，利于园区网骨干网的健壮性。即在汇聚与核心交换机之间采用 OSPF 路由的方式，OSPF 路由的方式可以减少网络中心人员对于校园网的维护量。OSPF 在校园网中只在核心骨干中进行运行，这样大大减少了骨干节点之间 OSPF 协议的收敛周期，在实际的应用过程中可以提高园区网络的高稳定性。

1.4.4　IPv6 地址规划与分配

1. IPv6 地址简介

IP 地址规划主要涉及网络资源利用方便有效的管理网络问题，IPv6 地址有 128 位，其中可供分配为网络前缀的空间有 64bit。按照最新的 IPv6 RFC3513，IPv6 地址分为全球可路由前缀和子网 ID 两部分，协议并没有明确的规定全球可路由前缀和子网 ID 各自占的 bit 数，目前 APNIC（Asia-Pacific Networh Information Center，亚太互联网络信息中心）能够申请到的 IPv6 地址空间为/32 的地址。

IPv6 的地址使用方式有两类：一类是普通网络申请使用的 IP 地址，这类地址完全遵从前缀 + 接口标识符的 IP 地址表示方法；另外一类就是取消接口标识符的方法，只使用前缀来表示 IP 地址。

IP 地址的分配和网络组织、路由策略以及网络管理等都有密切的关系，IPv6 地址规划目前尚没有主流的规则，具体的 IP 地址分配通常在工程实施时统一规划实施，可以遵循一

些分配原则：

1）地址资源应全网统一分配。

2）地址划分应有层次性，便于网络互联，简化路由表。

3）IP 地址的规划与划分应该考虑到网络的发展需求。

4）充分合理地利用已申请的地址空间，提高地址的利用效率。

IP 地址规划应该是网络整体规划的一部分，即 IP 地址规划要和网络层次规划、路由协议规划、流量规划等结合起来考虑。IP 地址的规划应尽可能和网络层次相对应，应该是自顶向下的一种规划。

全球可聚集 IPv6 地址的前缀为 64 位，后 64 位为主机的 interface id，所以各个驻地网用户用于可分配的 IPv6 地址前缀空间的范围为/48 至/64 之间。

IPv6 的地址分配原则同 IPv4 一样遵循 CIDR（Classless Inter-Domain Routing，无类型域间选路）原则。

IPv6 的地址规划时考虑三大类地址：

1）公共服务器地址，如 DNS、EMAIL、FTP 等。

2）网络设备互联地址和网络设备的 LOOPBACK 地址。

根据 IETF IPv6 工作组的建议，IPv6 网络设备互联地址采用/64 的地址。IPv6 网络设备的 LOOPBACK 地址采用/128 的地址。

3）用户终端的业务地址。

此外，由于目前网络设备的 IPv6 MIB 信息的获取和 OSPFv3 中 ROUTER ID 等均要求即使是一个纯 IPv6 网络也必须要求每个网络设备拥有 IPv4 地址。所以一个纯 IPv6 网络也必须规划 IPv4 地址（仅需要网络设备互联地址和网络设备的 LOOPBACK 地址）。

2. IPv6 的优势

IPv6 的发展是从 1992 年开始的，经过了 12 年的发展，IPv6 的标准体系已经基本完善，在这个过程中，IPv6 逐步优化了协议体系结构，为业务发展创造机会。归纳起来 IPv6 的优势有如下几个特点：

1）地址充足：IPv6 产生的初衷主要是针对 IPv4 地址短缺问题，即从 IPv4 的 32bit 地址，扩展到了 IPv6 的 128bit 地址，充分解决地址匮乏问题。同时 IPv6 地址是有范围的，包括链路本地地址、站点本地地址和任意播地址，这也进一步增加了地址应用的扩展性。

2）简单是美：简化固定的基本报头，采用 64bit 边界定位，取消 IP 头的校验和域等措施，以提高网络设备对 IP 报文的处理效率。

3）扩展为先：引入灵活的扩展报头，按照不同协议要求增加扩展头种类，按照处理顺序合理安排扩展头的顺序，其中网络设备需要处理的扩展头在报文头的前部，而需要宿端处理的扩展头在报文头的尾部。

4）层次区划：IPv6 极大的地址空间使层次性的地址规划成为可能，同时国际标准中已经规定了各个类型地址的层次结构，这样既便于路由快速查找地址格式更具层次性，也有利于路由聚合，缩减了 IPv6 路由表大小，降低了网络地址规划的难度。

5）即插即用：IPv6 引入自动配置以及重配置技术，对于 IP 地址等信息实现自动增删更新配置，提高了 IPv6 的易管理性。

6）贴身安全：IPv6 集成了 IPSec，用于网络层的认证与加密，为用户提供端到端安全，

使用起来比 IPv4 简单、方便，可以在迁移到 IPv6 时同步发展 IPSec。

7）QoS 考虑：新增流标记域，为源、宿端快速处理实时业务提供可能，有利于低性能的业务终端支持 IPv6 的语音、视频等应用。

8）移动便捷：Mobile IPv6 增强了移动终端的移动特性、安全特性、路由特性，降低了网络部署的难度和投资，为用户提供了永久在线服务。

3. IPv6 网络整体设计

新建 IPv6 网络相对前一种组网模式简单，选取支持双栈的交换机设备，按照现有的园区网建设模式组建网络即可。核心层和汇聚层可选用双栈交换机，接入层可使用现有的二层接入交换机组网。根据用户带宽的需要，分别选用“百兆到桌面”或“千兆到桌面”的模式。对一些 IPv6 应用特殊场景可以选择 IPv6 双栈交换机进行接入。为提高网络的可靠性，汇聚层与核心层之间、接入层与汇聚层之间采用双归链路上联实现链路冗余；汇聚设备作为用户接入点网关设备，通过运行 HSRP 或 VRRP 协议实现网关冗余；核心节点采用双核心部署保证节点冗余。

4. IPv6 路由规划

路由协议分为域内路由协议和域间路由协议，目前主要的路由协议都增加了对 IPv6 的支持功能。从路由协议的应用范围来看，OSPFv3、RIPng 和 IS-ISv6 适用于自治域内部路由，为内部网关协议；BGP4 + 用来在自治域之间交换网络可达信息，是外部网关协议。

（1）域内路由协议选择

支持 IPv6 的内部网关协议有：RIPng、OSPFv3、IS-ISv6 协议。从路由协议标准化进程看，RIPng 和 OSPFv3 协议已较为成熟，支持 IPv6 的 IS-IS 协议标准草案也已经过多次讨论修改，标准正在形成之中，而且 IS-ISv6 已经在主流厂家的相关设备中得到支持。从协议的应用范围的角度，RIPng 协议适用于小规模的网络，而 OSPF 和 IS-IS 协议可用于较大规模的网络。

对于大规模的 IP 网络，为了保证网络的可靠性和可扩展性，内部路由协议（IGP）必须使用链路状态路由协议，只能在 OSPF 与 IS-IS 之间进行选择，下面对两种路由协议进行简单的对比。

目前，在 IPv4 网络中大量使用的 OSPF 路由协议版本号为 OSPFv2，能够支持 IPv6 路由信息的 OSPF 版本称为 OSPFv3，能够支持 IPv6 路由信息交换的 ISIS 路由协议称为 IS-ISv6。

OSPFv3 与 OSPFv2 相比，虽然在机制和选路算法上并没有本质的改变，但新增了一些 OSPFv2 不具备的功能。OSPFv3 只能用来交换 IPv6 路由信息，ISISv6 可以同时交换 IPv4 路由信息和 IPv6 路由信息。

OSPF 是基于 IP 层的协议，OSPF v3 是为 IPv6 开发的一套链路状态路由协议。大体与支持 IPv4 的 OSPF v2 版本相似。

对比 OSPF v2，在 OSPF v3 中有以下区别：

虽然 OSPFv3 是为 IPv6 设计的，但是 OSPF 的 Router ID、Area ID 和 LSA Link State ID 依然保持 IPv4 的 32 位的格式，而不是指定一个 IPv6 的地址。所以即使运行 OSPF v3 也需要为路由器分配 IPv4 地址。

协议的运行是按照每一条链路（Per-link）进行的，而不是按照每个子网进行的（per-subnet）。

把地址域从 OSPF 包和一些 LSA 数据包中去除掉，使得其成为网络层协议独立的路由协议。

与 OSPFv2 不同，IPv6 的地址不再出现在 OSPF 包中，而是会在链路状态更新数据包中作为 LSA 的负载出现。

Router-LSA 和 Network-LSA 也不再包含网络地址，而只是简单地表示拓扑信息。

邻居路由器的识别将一直使用 Router ID，而不是像 OSPFv2 一样在某些使用端口会将端口地址作为标识。

Link-Local 地址可以作为 OSPF 的转发地址。除了 Virtual link 必须使用 Global unicast 地址或者使用 Site-local 地址。

去掉了认证信息。在 OSPF v3 中不再有认证方面的信息。如果需要加密，可以使用 IPv6 中定义的 IP Authentication Header 来实现。

OSPF 数据包格式发生了一些变化：

OSPF 的版本号由 2 变成了 3；

Hello 包和 Database description 包的选项域增加到 24 位；

去掉了认证域；

Hello 信息中不再包含地址信息；

引入了两个新的选项：R 位和 V6 位；

为实现单链路上多 OSPF 进程，在 OSPF 包头中加入了 Instance ID 域；

类型 LSA 3 名字改为：Inter-Area-Prefix-LSA，类型 LSA 4 名字改为：Inter-Area-Router-LSA。OSPF v2 和 OSPF v3 都使用最短路径优先算法，在 Area 划分、链路类型、LSA 传播等方面基本一致。

总的来说，由于 OSPF 发展成熟，支持厂商广泛，已经成为世界上使用最广泛的 IGP，尤其在企业级网络，也是 IETF 推荐的唯一的 IGP。其他路由协议所能适应的网络，OSPF 都能适应。

（2）域间路由协议选择

域间路由协议采用 BGP4 +，从而实现不同 ISP 核心网络之间的互通，而且目前大多数典型的路由器设备都支持这个协议。BGP4 + 处理各 ISP 间的路由传递，是一种域间路由协议。其特点是有丰富的路由策略，这是 RIPng、OSPFv3 等协议无法做到的，因为它们需要全局的信息计算路由表。BGP4 + 通过在 ISP 边界路由器上增加一定的策略，选择过滤路由，把 RIPng、OSPFv3、BGP4 + 等路由发送到对方。随着 IPv6 网络的大量组建，BGP4 + 将得到越来越多的应用。

（3）IPv6 路由规划建议

以高效接入 IPv6 为例，相比 CERNET2 核心网和城域网，驻地网（校园网）内部的 IPv6 网络的路由规划较为简单。IGP 可以选择 ISISv6 或者 OSPFv3，但是考虑到使用者的习惯，大多数三层交换机不支持 ISISv6 路由，以及必要性，部署 OSPFv3 可能更为实际。OSPFv3 域的设计可以沿用 OSPFv2 的思路。

新建校园网全网部署双协议栈，IPv4 部分和原有校园网平滑对接。三层设备上同时运行 OSPFv2 和 OSPFv3 两套协议，尽管运行在同一个设备上，这两套协议是互相独立的。OSPFv3 的逻辑拓扑图（AREA 规划）和 OSPFv2 可以完全不同。

在校园网 IPv6 出口的路由规划上，按照国际上 IPv6 地址的分配规则，CERNET2 城域网会分配一块或几块 IPv6 PREFIX ::/48 的地址给校园网。对于单出口的情况，可能较为简单。CERNET2 城域网接入路由器将指向驻地网（校园网）的静态路由引入到 IBGP4 + 中去。

1.4.5　子网划分与 VLAN

一个网络实际上可能会有多个物理网段，我们把这些网段称为子网，其使用的 IP 地址是由某个网络号派生而得到的。将一个网络划分成若干个子网，需要使用不同的网络号或子网号。

在划分子网之前，要先分析一下用户需求以及将来的规划。一般情况下我们遵循这样的准则：

1）确定网络中的物理段数量（就是子网个数）。

2）确定每个子网需要的主机数。注意，一个主机至少一个 IP 地址。

3）基于此需求，定义整个网络的子网屏蔽、每个子网唯一的子网号和每个子网的主机号范围。

在定义一个子网屏蔽之前，确定一下将来需要的子网数量及子网的主机数是必不可少的一步。因为当更多的位用于子网屏蔽时，就有更多的可用子网，但每个子网中的主机数将减少（这和定义 IP 地址的概念正好相反）。

VLAN（Virtual Local Area Network）即虚拟局域网，是一种通过将局域网内的设备逻辑地而不是物理地划分成一个个网段从而实现虚拟工作组的新兴技术。IEEE 于 1999 年颁布了用以标准化 VLAN 实现方案的 802.1Q 协议标准草案。VLAN 技术允许网络管理者将一个物理的 LAN 逻辑地划分成不同的广播域（或称虚拟 LAN，即 VLAN），每一个 VLAN 都包含一组有着相同需求的计算机工作站，与物理上形成的 LAN 有着相同的属性。但由于它是逻辑地而不是物理地划分，所以同一个 VLAN 内的各个工作站无须被放置在同一个物理空间里，即这些工作站不一定属于同一个物理 LAN 网段。一个 VLAN 内部的广播和单播流量都不会转发到其他 VLAN 中，从而有助于控制流量、减少设备投资、简化网络管理、提高网络的安全性。VLAN 是为解决以太网的广播问题和安全性而提出的一种协议，它在以太网帧的基础上增加了 VLAN 头，用 VLAN ID 把用户划分为更小的工作组，限制不同工作组间的用户二层互访，每个工作组就是一个虚拟局域网。虚拟局域网的好处是可以限制广播范围，并能够形成虚拟工作组，动态管理网络。

VLAN 在交换机上的实现方法，可以大致划分为 4 类。

1. 基于端口划分的 VLAN

这种划分 VLAN 的方法是根据以太网交换机的端口来划分，比如交换机的 1 ~ 4 端口为 VLAN 10，5 ~ 17 为 VLAN 20，18 ~ 24 为 VLAN 30。当然，这些属于同一 VLAN 的端口可以不连续，如何配置，由管理员决定。如果有多个交换机，例如，可以指定交换机 1 的 1 ~ 6 端口和交换机 2 的 1 ~ 4 端口为同一 VLAN，即同一 VLAN 可以跨越数个以太网交换机，根据端口划分是目前定义 VLAN 的最广泛的方法。IEEE 802.1Q 规定了依据以太网交换机的端口来划分 VLAN 的国际标准。

这种划分方法的优点是定义 VLAN 成员时非常简单，只要将所有的端口都指定一下就可

以了。它的缺点是如果 VLAN A 的用户离开了原来的端口，到了一个新的交换机的某个端口，那么就必须重新定义。

2. 基于 MAC 地址划分 VLAN

这种划分 VLAN 的方法是根据每个主机的 MAC 地址来划分，即对每个 MAC 地址的主机都配置其属于哪个组。这种划分 VLAN 方法的最大优点就是当用户物理位置移动时，即从一个交换机换到其他的交换机时，VLAN 不用重新配置，所以，可以认为这种根据 MAC 地址的划分方法是基于用户的 VLAN。

这种方法的缺点是初始化时，所有的用户都必须进行配置，如果有几百个甚至上千个用户的话，配置是非常累的。而且这种划分的方法也导致了交换机执行效率的降低，因为在每一个交换机的端口都可能存在很多个 VLAN 组的成员，这样就无法限制广播包了。另外，对于使用笔记本电脑的用户来说，他们的网卡可能经常更换，这样 VLAN 就必须不停地配置。

3. 基于网络层划分 VLAN

这种划分 VLAN 的方法是根据每个主机的网络层地址或协议类型（如果支持多协议）划分的，虽然这种划分方法是根据网络地址，比如 IP 地址，但它不是路由，与网络层的路由毫无关系。它虽然查看每个数据包的 IP 地址，但由于不是路由，所以没有 RIP、OSPF 等路由协议，而是根据生成树算法进行桥交换。

这种方法的优点是用户的物理位置改变了，不需要重新配置所属的 VLAN，而且可以根据协议类型来划分 VLAN，这对网络管理者来说很重要。还有这种方法不需要附加的帧标签来识别 VLAN，可以减少网络的通信量。其缺点是效率低，因为检查每一个数据包的网络层地址是需要消耗处理时间的（相对于前面两种方法），一般的交换机芯片都可以自动检查网络上数据包的以太网帧头，但要让芯片能检查 IP 帧头，需要更高的技术，同时也更费时。这也与各个厂商的实现方法有关。

4. 根据 IP 组播划分 VLAN

IP 组播实际上也是一种 VLAN 的定义，即认为一个组播就是一个 VLAN，这种划分的方法将 VLAN 扩大到了广域网，因此这种方法具有更大的灵活性，而且也很容易通过路由器进行扩展。当然这种方法不适合局域网，主要因为是效率不高。

1.4.6 网络 Internet 出口设计

网络出口工作在网络的边缘，是内部网络与 Internet 之间的桥梁。出口设备主要包含三类：路由器类、防火墙类、流量控制类。从出口设备所启用和所关注的功能来看：

功能上，NAT（Network Address Translation，网络地址转换）转发，路由处理是最基本的。针对多出口，策略路由也是必备功能。

性能上，NAT（网络地址转换）和策略路由是大型园区网络现有出口设备的瓶颈所在。其次是安全防护能力，不具备包含出口日志的记录能力。

因此，对于一个大型网络的出口，必须要支持的功能是 NAT、策略路由、安全防护。NAT 可以完成园区内部网络私有 IP 地址向公网 IP 地址的转换；策略路由能实现园区内部网络的路由转发和 Internet 的连接；安全防护主要体现在防火墙 DMZ（Demilitarized zone，隔离区）区的设计，必须要具有防火墙的功能。

国内知名网络厂家锐捷网络在大型园区网络 Internet 出口上提供了非常完备的解决方

案，如图 1-9 所示。在出口设计上采用冗余设计思路。RG-NPE（Network outPut Engine，网络出口引擎）系列产品（简称 NPE），是锐捷网络针对国内网络出口状况研发的专用设备。NPE 基于多核处理器技术进行架构，具备高性能转发、内嵌状态防火墙、日志记录等功能。此外，NPE 针对国内普遍存在的 NAT 进行优化，并发会话和新建会话能力在业内首屈一指。NPE 产品全新融入了智能 DNS 和多链路负载均衡技术，使得用户对内对外访问都能智能选择最优、最快速的路径；集成了 DPI 引擎，让网络管理者轻松应对 P2P 等应用的流量控制；重构了 Web 界面，让 NPE 网络出口引擎在设备管理维护层面变得简化。作为网络出口的专用设备，NPE 系列产品已经广泛应用于政府机关、高校、普教、医疗等各个行业。

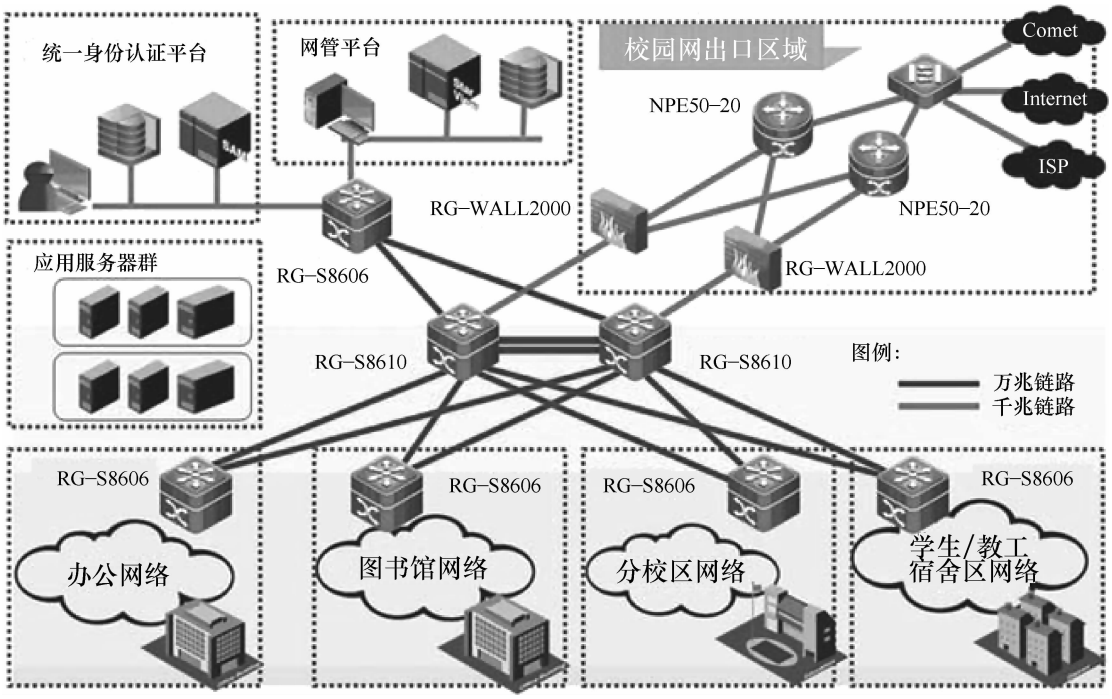


图 1-9　校园网出口解决方案示例

1.5　园区网络物理设计

1.5.1　网络传输介质的选择

组建计算机网络，最关键的是选择采用什么样的传输介质和网络连接设备，这些选择不仅关系到计算机网络的性能，而且关系到组建网络的成本。一般对网络传输介质的选择，要基于综合布线系统设计方案来决定。没有特殊需求的网络，都会采用市场上十分常见而且性价比不错的传输介质产品。常用的传输介质有：双绞线、同轴电缆、光纤、无线传输媒介。

双绞线有 UTP 和 STP 两种，非屏蔽双绞线（UTP）可分为 3 类、4 类、5 类和超 5 类、6 类等多种。屏蔽双绞线（STP）可又分为 3 类、5 类、超 5 类等多种。3 类线用于语音传输及最高传输速率为 10Mbit/s 的数据传输；4 类线和 5 类线用于语音传输和最高传输速率为

16Mbit/s 的数据传输；超5类线和6类线用于语音传输和最高传输速率为1000Mbit/s 的数据传输。

光纤又称为光缆或光导纤维，由光导纤维纤芯、玻璃网层和能吸收光线的外壳组成，是由一组光导纤维组成的用来传播光束的、细小而柔韧的传输介质。应用光学原理，由光发送机产生光束，将电信号变为光信号，再把光信号导入光纤，在另一端由光接收机接收光纤上传来的光信号，并把它变为电信号，经解码后再处理。与其他传输介质比较，光纤的电磁绝缘性能好、信号衰减小、频带宽、传输速度快、传输距离大。主要用于要求传输距离较长、布线条件特殊的主干网连接。具有不受外界电磁场的影响、无限制的带宽等特点，可以实现每秒几十兆位的数据传送，尺寸小、重量轻，数据可传送几百千米，但价格昂贵。单模光纤由激光作光源，仅有一条光通路，传输距离长（2km 以上）。多模光纤由二极管发光，低速短距离（2km 以内）。

无线传输媒介包括：无线电波、微波、红外线等。

在实际局域网组网工程中主要使用的是单模或多模光缆和双绞线作为传输介质。限于成本方面的考虑，一般使用超五类双绞线。不过六类双绞线价格下降了，也得到了大量应用。

1.5.2 结构化布线

建筑物结构化综合布线系统（SCS）又称开放式布线系统，是一种在建筑物和建筑群中综合数据传输的网络系统。它是把建筑物内部的话音交换、智能数据处理设备及其他广义的数据通信设施相互连接起来，并采用必要的设备同建筑物外部数据网络或电话局线路相连接。结构化布线系统是根据各节点的地理分布情况、网络配置情况和通信要求，安装适当的布线介质和连接设备，使整个网络的连接、维护和管理变得简单易行。

综合布线系统由于采用开放式体系结构，符合多种国际上流行的标准，因此它几乎对所有著名厂商的产品都是开放的，如 IBM、HP、DEC、SUN 的计算机设备，AT&T、NT、NEC 等的交换机设备。并对几乎所有通信协议也是开放的，如 EIA-232-D、RS-422、RS-423、ETHERNET、TOKENRING、FDDI、CDDE、ISDN、ATM 等。

综合布线系统应用极富弹性的布线概念，采用光纤与双绞线混布方式，极为合理地构成一套完整的布线系统。所有布线均采用世界上最新通信标准，信息通道均按 B-ISDN 设计标准，按八芯双绞线配置，通过超5类双绞线，数据最大速率可达到 100～1000Mbit/s，对于特殊用户需求可把光纤铺到桌面（Fiber-to the Desk）。干线光缆可设计为 1000Mbit/s 带宽，为将来的发展提供了足够的裕量。通过主干通道可同时传输多路实时多媒体信息，同时物理星形的布线方式为将来发展交换式的网络奠定了坚实基础。

1.5.3 设备选型

在网络设计中，常见网络设备主要是指交换机、路由器、无线访问点和无线网桥。其中主要以交换和路由应用范围最广。依据不同层次，可以选择不同类型的设备，如接入层交换机、核心层交换机等。

1. 网络设备选择标准

通常选择网络设备时可参考如下性能指标项：

- 端口数；

- 处理速度；
- 内存大小；
- 设备中继数据时的延迟；
- 设备中继数据时的吞吐量；
- 支持的 LAN 和 WAN 技术；
- 支持的媒介；
- 易于配置和管理；
- MTBF 和 MTTR；
- 支持热交换组件；
- 支持冗余电源；
- 技术支持质量、文档和培训等。

对于交换机和网桥设备，可增加如下标准：

- 支持的网桥协议；
- 是否支持高级生成树算法；
- 可以学习的 MAC 地址数量；
- 是否支持端口特性（802.1x）；
- 是否支持直通式交换；
- 是否支持可适应的直通式交换；
- 支持的 VLAN 技术；
- 是否支持组播应用。

对于路由器设备（包括带路由选择模块的交换机），可以增加如下标准：

- 支持的网络协议；
- 支持的路由选择协议；
- 是否支持组播应用；
- 是否支持先进的队列、交换技术和其他的优化特性；
- 是否支持压缩；
- 是否支持加密。

2. 不同层次交换机的选择

工作组交换机采用可网管交换机，实现对每台接入计算机的控制，实现 VLAN（虚拟网）的划分，确保最大限度的网络访问安全。骨干交换机采用拥有千兆端口的可网管交换机实现与中心交换机的高速连接，避免可能产生的网络瓶颈。汇聚交换机采用三层交换机，实现 VLAN 间的线速转发，并借助访问列表控制计算机接入和网络服务，搭建高安全性和可用性网络。

因交换机支持端口较多，同时价格较路由器便宜，因此园区网主要是以交换机为主。下面以 Cisco 交换机设备为例，给出接入层、汇聚层、核心层的常用设备。

（1）接入层交换机

接入层交换机负责将终端节点设备连接到网络，因此需要支持端口安全功能、VLAN、快速以太网/千兆以太网、PoE 和链接组合等功能。

1）Catalyst Express 500 适用于端口密度不高的接入层。

2）Catalyst 2960 系列适用于供电不便，空间有限的接入层。

3）Catalyst 3560 适合用做小企业 LAN 接入或分支机构融合网络环境中的接入层。

4）Catalyst 3750 适合用做中型结构和企业分支机构中的接入层。

（2）汇聚层交换机

汇聚层需支持流量安全策略管理、VLAN 路由、ACL、QoS、链路聚合等功能。如 Catalyst 3500、4500、4900 系列设备。

（3）核心层交换机

核心层交换机要求在可用性、链路聚合、高速转发、QoS 方面具有较高的性能，如 Catalyst 4500、6500、7200 系列设备。Cisco 的 Linksys WRT300N 可作为小企业或家庭用户的无线接入设备。

3. 路由器的选择

就企业局域网网络而言，由于大量的数据都发生在局域网内部，对路由器的性能要求不高，因此可以选用中低端路由器。低端路由器主要适用于中小办公网络，考虑的一个主要因素是端口数量，另外还要看包交换能力。中端路由器适用于大中型办公网络，选用的原则也是考虑端口支持能力和包交换能力。

当前路由器的分类方法各异，从能力上分，路由器可分为高端路由器、中端路由器和低端路由器。各厂家划分也不完全一致。通常将背板交换能力大于 40Gbit/s 的路由器称为高端路由器，之下的为中低端路由器。以思科（Cisco）公司为例，Cisco 12800 路由器为高端路由器，7500 以下系列路由器为中低端路由器。

从结构上分，路由器可分为模块化结构与非模块化结构，通常中高端路由器为模块化结构，低端路由器为非模块化结构。

从功能上分，路由器可分为通用路由器与专用路由器，一般所指的路由器都是通用路由器，专用路由器是对硬件和功能有特殊要求的路由器，如宽带接入路由器强调宽带接口数量及种类。

从路由器在网络中的位置划分，路由器可分为核心路由器、企业级路由器和接入路由器等。

4. 防火墙的选择

防火墙有软件防火墙和硬件防火墙两种。软件防火墙是安装在计算机平台的软件产品，它通过在操作系统底层工作来实现网络管理和防御功能的优化。硬件防火墙的硬件和软件都单独进行设计，有专用网络芯片处理数据包。同时，采用专门的操作系统平台，从而避免通用操作系统的安全性漏洞。硬件防火墙分为包过滤防火墙、应用网关防火墙和规则检查防火墙。对于企业网络而言，通常应当选择包过滤防火墙。

防火墙的分类有很多种方法，通常以软、硬件构成来划分。按防火墙软、硬件形式可分为软件防火墙和硬件防火墙以及芯片级防火墙。

（1）软件防火墙

软件防火墙又称个人防火墙，运行于特定的计算机上，它需要客户预先安装好的计算机操作系统的支持，一般来说这台计算机就是整个网络的网关。如美国飞塔公司的 Web 应用防火墙、天网防火墙、瑞星防火墙等。

（2）硬件防火墙

硬件防火墙是区别于专用处理芯片的防火墙。硬件防火墙是把软件防火墙嵌入在硬件

中，一般的软件安全厂商所提供的硬件防火墙便是在硬件服务器厂商定制硬件，然后再把 Linux 系统与自己的软件系统嵌入其中。这些硬件主要运行一些经过裁剪和简化的操作系统，最常用的有老版本的 Unix、Linux 和 FreeBSD 系统。传统硬件防火墙一般至少应具备三个端口，分别接内网、外网和 DMZ 区（非军事化区）。

（3）芯片级防火墙

芯片级防火墙基于专门的硬件平台。专有的 ASIC 芯片促使它们比其他种类的防火墙速度更快，处理能力更强，性能更高。一些代表性的厂商有 FortiNet（飞塔）、Juniper（瞻博）、Cisco（思科）等。这类防火墙由于是专用 OS（操作系统），因此防火墙本身的漏洞比较少。

1.5.4　网络弱电机房设计与施工

网络弱电机房是一个非常复杂的环境，必须满足适宜的温湿度、无尘、无静电等苛刻条件，同时弱电机房安全也很重要，因此在设计时需要特别注意。弱电机房方案设计主要是从以下几个方面来分析：弱电机房供电系统设计、弱电机房空调系统设计、弱电机房防雷接地系统设计、弱电机房监控系统设计、弱电机房消防系统设计。这几个主要的子系统，必须充分设计好。还有要充分考虑机房的装修工程、综合布线工程。

1. 弱电机房方案设计标准

设计弱电机房时必须严格遵循国家出台的相关标准，我国最新出台的标准是：

国家标准《电子信息系统机房设计规范》（GB50174-2008）

国家标准《电子信息系统机房施工及验收规范》（GB50462-2008）

2. 弱电机房供电系统设计

一个弱电机房能够正常工作，不仅需要有良好的主设备和安全舒适的工作环境，还需要有一个设计合理、可靠性高的供配电系统。

一般弱电机房供电系统解决方案分为两部分：一是在前端交流电源引入两路市电，有条件时可加设发电机，成为多路供电，提高供电可靠性；二是在机房里设不间断电源 UPS，附设一定的直流电池组作为后备电源，即可保证供电。前者是传统的提高供电可靠性的方式，后者是近年来随着信息技术飞速发展而越来越广泛应用的方式。

现有两种 UPS 供电方式可供选择：一为在线式，即 UPS 始终在供电状态，时刻都在工作着，UPS 代替了市电为计算机网络设备供电；二为后备式，就是计算机网络设备平时供电依靠市电，只在市电停电时才立即转而由 UPS 供电。后备式供电有个过零问题，即当市电停电时，无论何种合闸方式，都避免不了瞬间无电问题。市电是 50Hz，奔腾Ⅱ PC 是 500MHz 以上，显然，在停电的一瞬间，计算机可能丢失数据。具体办法是分而治之：若是正常停电，事先必有通知，可提前将 UPS 投入；若是故障（短路、接地）停电，因电感上电流不能跃变，电容上电压不能跃变，可将 UPS 的自动接入设定为小于跳闸电流值，即在电路断开前，UPS 就已接入。

UPS 电源正向大功率、低噪声、智能化、网络化方向发展，而这正是中央机房所需要的。大功率的 UPS 电源多具有并机冗余功能，新出现的热插拔、模块化电池阵列进一步提高了供电可靠性。

3. 弱电机房空调系统设计

弱电机房对机房内空气的制冷、制热、加湿、去湿、滤尘有严格的标准要求，设备的寿

命与工作情况与这些标准密切相关。弱电机房空调应选择专用机房精密空调并且设计新风系统。空调送风方式一般采用下送风方式。

4. 弱电机房防雷接地系统设计

弱电机房内大量的电子设备工作电压较低，精密设备较多，对雷击的耐受能力较差，一旦遭受雷击，往往损失巨大。故此处防雷等级较高，对防范各种雷击的措施要求较高。雷击形式多种，弱电机房防雷措施主要针对直击雷和感应雷。

弱电机房接地系统包括防雷接地、交流工作接地、直流接地、PE 保护接地、屏蔽接地及防静电接地等系统，后三者可互连。弱电机房的防雷接地方式一般采用联合接地方式，即防雷接地、保护接地、工作接地等均直接与接地网连接，总的接地电阻应小于 1Ω，即所谓零接地电阻。在条件允许时也可设置专用接地装置。

5. 弱电机房监控系统设计

对于弱电机房，我们考虑采用以大楼闭路监控主机为主的安防系统，机房内可安装少量彩色半球摄像机，用于视频监控。

6. 弱电机房消防系统设计

弱电机房消防系统设计包括烟感报警、气体灭火两部分。烟感报警以吸顶式和缆式烟感器为主要形式。吸顶式烟感器的保护半径一般不大于 5.8m，距墙、风口、大梁不小于 0.5m。缆式烟感器可沿墙敷设。必须通过机房的风管在过墙处设置防火阀（环境温度达到 70℃时自动关闭）。气体灭火系统的作用类似于普通办公室里的喷淋系统，其设计要点有系统类型结构的选择、灭火剂浓度的确定、气体喷射时间、灭火剂用量及浸渍时间等。气体灭火系统主要是二氧化碳灭火系统及卤代烷灭火系统。此外，在室内附设交、直流双电源应急灯、火灾事故广播、119 专线消防电话、火灾报警按钮等消防设施。机房的装修材料应符合有关防火规范的要求。

综上所述，弱电机房需要注意多方面因素，其方案要按规范要求进行设计。

本 章 小 结

本章主要从概述的角度，简单回顾了计算机网络和局域网的基础知识。

1）给出了园区网络的基本概念，并对大型园区网络规划与设计的设计原则、主要内容进行了阐述。

2）建设大型园区网络，首要工作是进行需求分析，对需求分析的主要内容进行了梳理，明确了需求分析的重点工作。

3）对园区网络的建设，重点工作是组网方案。对大型园区网络建设的性能目标、主要建设步骤进行了分析，主要包括综合布线系统设计、网络弱电机房设计以及网络系统集成方案设计等。

4）对大型园区网络组网方案中逻辑设计、IP 地址规划分配、子网划分与 VLAN、Internet 出口方案设计等进行了介绍。

5）对大型园区网络组网方案中物理设计、结构化布线系统、网络设备选型、弱电机房设计等技术要点进行了介绍。

第 2 章　网络互连设备

2.1　网络互连

2.1.1　网络互连的基本概念

网络互连是指将不同的网络连接起来，以构成更大规模的网络系统，实现网络间的数据通信、资源共享和协同工作。Jeffrey S. Beasley 在他的经典著作《网络互连》中给出了网络互连的定义，并对互联互通进行了较好的辨析。

1）互连（Interconnection）：网络在物理上的连接，两个网络之间至少有一条在物理上连接的线路，它为两个网络的数据交换提供了物质基础和可能性，但并不能保证两个网络一定能够进行数据交换，这要取决于两个网络的通信协议是不是相互兼容。

2）互联（Internetworking）：网络在物理和逻辑上，尤其是逻辑上的连接。

3）互通（Intercommunication）：两个网络之间可以交换数据。

4）互操作（Interoperability）：网络中不同计算机系统之间具有透明地访问对方资源的能力。

2.1.2　网络互连的目的及意义

互连网络随着需要而发展，在 20 世纪 50 年代，计算机刚刚开始出现的时候，互连网络根本不存在，计算机是独立的和私有的计算工具。正是因为美国国防部军方对数据包-交换广域网设计感兴趣并且用于军事目的，推动 D A R PA 项目，并建立了第一个真正意义上的互连网络 ARPANet，后来出现了局域网（LAN）、广域网（WAN），直到发展成今天大规模的互联网。可以说，是网络应用需求使得网络互连逐步发展起来。

要实现网络互连，其根本就是要解决互通和互操作性两个问题，否则互连是不可能实现的。我们知道，正是基于互连的原因，OSI 标准参考模型和 TCP/IP 模型逐步被设计并得到了应用，特别是 TCP/IP 的革命性的诞生，主流的网络设备发展到几乎所有设备都支持 TCP/IP，使得网络互连变得简单方便。

因此，网络互连的目的是将不同的网络或相同的网络用互连设备连接在一起形成一个范围更大的网络，为增加网络性能以及从安全和管理方面的考虑，将原来一个很大的网络划分为几个网段或逻辑上的子网，实现异种网之间的服务和资源共享。

异构网络（Heterogeneous Network）是由不同制造商生产的计算机、网络设备和系统组成的，大部分情况下运行在不同的协议上支持不同的功能或应用。近年来，异构网络主要是指无线通信领域不同协议和设备的网络。早期的异构网络，是指并不是基于 TCP/IP 来设计的网络设备和系统，正逐步被淘汰，发展到统一为 IP 的网络。

网络互连的目的是使一个网络上的用户能访问其他网络上的资源，使不同网络上的用户

互相通信和交换信息。这不仅有利于资源共享，也可以从整体上提高网络的可靠性。随着商业需求的推动，特别是 Internet 的深入人心，网络互连技术成为实现如 Internet 这样的在规模网络通信和资源共享的关键技术。

2.1.3 网络互连的基本原理

1. 网络互连的要求

由于不同的网络间可能存在设备或系统使用不同的网络协议等差异，因此对网络互连有如下要求：

1）在网络之间提供一条链路，至少需要一条物理和链路控制的链路。若不存在链路，一个网络的信息就不可能传输到另一个网络中去。

2）提供不同网络节点的路由选择和数据传送。

3）提供网络记账服务，记录网络资源使用情况，提供各用户使用网络的记录及有关状态信息。

4）在提供网络互连时，应尽量避免由于互连而降低网络的通信性能。

5）不修改互连在一起的各网络原有的结构和协议。这就要求网络互连设备应能进行协议转换，协调各个网络的不同性能，这些性能包括：

①不同的编址方式：每个网络有不同的端点名字、编址方法、寻址方式和目录保持方案，需要提供全网编址方法和目录服务。

②不同的最大分组长度：在互连网络中，分组从一个网络送到另一网络时，往往需要分成几部分，称为分段。不同的网络存在着不同的分组大小。

③不同的传输速率：在互连网络中，不同网络的传输速率可能不同。

④不同的时限：对连接的传送服务总要等待回答响应，如超时后仍没有接到响应，则需要重传。但在互连网络中，数据传送有时需要经过多个网络，这需要更长时间，应该设定合适的超时值，以防不必要的重传。

⑤不同的网络访问机制：对不同网络上的多个节点，节点和网络之间的访问机制可以是相同的，也可能是不同的。

⑥差错恢复：各个网络有不同的差错恢复功能。互连网络的服务既不要依赖也不要影响各个网络原来的差错恢复能力。

⑦状态报告：不同的网络有不同的状态报告，对互连网络还应该提供网络互连的活动信息。

⑧路由选择技术：网内的路径选择一般依靠各个网特有的故障检测和拥挤控制技术。而互连网络应提供不同网络之间进行路径选择的能力。

⑨用户访问控制：不同的网络有不同的用户访问控制方法，用于管理用户对网络的访问权限。互连网络需要具有对不同的用户访问权限的控制能力。

⑩连接和无连接服务：不同的网络可能提供面向连接的服务，也可能提供无连接的数据报服务。互连网络的服务不应该依赖于原来各个网络所提供的服务类型。

当源网络发送分组到目的网络要跨越一个或多个外部网络时，这些性能差异会使得数据包在穿过不同网络时产生很多问题。网络互连的目的就在于提供不依赖于原来各个网络特性的互连网络服务。

2. 网络互连的层次

不同目的的网络互连可以在不同的网络分层中实现。由于网络间存在不同的差异，也就需要用不同的网络互连设备将各个网络连接起来。根据网络互连设备工作的层次及其所支持的协议，可以将网间设备分为中继器、网桥、路由器和网关，OSI 七层模型网络互连如图 2-1 所示。

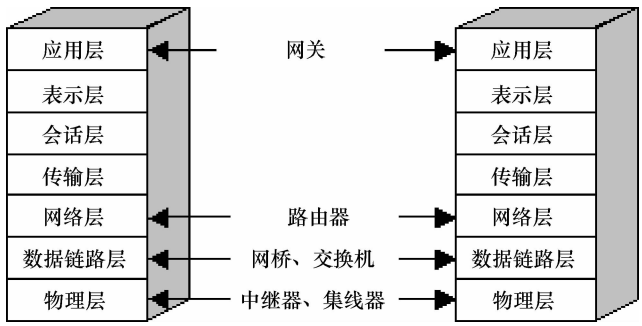


图 2-1　OSI 七层模型网络互连

（1）物理层

用于不同地理范围内的网段的互连。通过互连，在不同的通信介质中传送比特流，要求连接的各网络数据传输率和链路协议必须相同。

工作在物理层的网间设备是中继器、集线器。

用于扩展网络传输的长度，实现两个相同的局域网段间的电气连接。它仅仅是将比特流从一个物理网段复制到另一个物理网段，而与网络所采用的网络协议（如 TCP/IP、IPX/SPX、NETBIOS 等）无关。物理层的互连协议最简单，互连标准主要由 EIA、ITU-T、IEEE 等机构制定。集线器就是多端口的中继器。

（2）数据链路层

用于互连两个或多个同一类型的局域网、传输帧。工作在数据链路层的网间设备是桥接器（或桥）、交换机。桥可以将两个或多个网段互连，如果信息不是发向桥所连接的网段，则桥可以过滤掉，避免了网络的瓶颈。局域网的连接实际上是 MAC 子层的互连，MAC 桥的标准由 IEEE802 的各个分委员会开发。

（3）网络层

主要用于广域网的互连。网络层互连解决路由选择、阻塞控制、差错处理、分段等问题。

工作在网络层的网间设备是路由器、第三层交换机。

路由器提供各种网络间的网络层接口。路由器是主动的、智能的网络节点，它们参与网络管理，提供网间数据的路由选择，并对网络的资源进行动态控制等。路由器是依赖于协议的，它必须对某一种协议提供支持，如 IP、IPX 等。路由器及路由协议种类繁多，其标准主要由 ANSI 任务组 X3S3. 3 和 ISO/IEC 工作组 TC1/SC6/WG2 制定。

（4）网络层以上各层

用于在网络层以上各高层之间进行不同协议的转换，它也最为复杂。工作在第三层以上的网间设备称为网关，它的作用是连接两个或多个不同的网络，使之能相互通信。这种“不同”常常是物理网络和高层协议都不一样，网关必须提供不同网络间协议的相互转换。最常见的是将某一特定种类的局域网或广域网与某个专用的网络体系结构相互连接起来。

3. 网络互连的类型

网络互连可分为局域网-局域网（LAN-LAN）、局域网-广域网（LAN-WAN）、局域网-广域网-局域网（LAN-WAN-LAN）、广域网- 广域网（WAN-WAN）四种类型。

（1）局域网-局域网

LAN-LAN 互连又分为同种 LAN 互连和异种 LAN 互连。同构网络互连是指符合相同协议局域网的互连，主要采用的设备有中继器、集线器、网桥、交换机等。而异构网的互连是指两种不同协议局域网的互连，主要采用的设备为网桥、路由器等。局域网-局域网互连如图 2-2 所示。

（2）局域网-广域网

局域网-广域网是目前常见的方式之一，即局域网接入广域网中，用来连接的设备是路由器或网关，如图 2-3 所示。

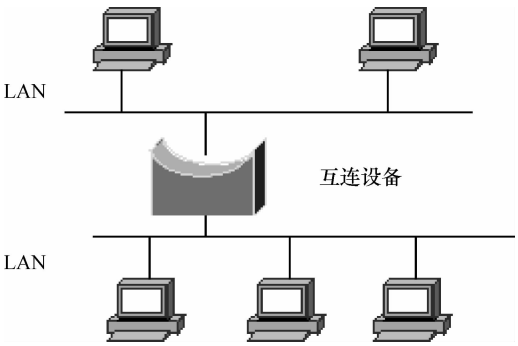


图 2-2　局域网-局域网互连

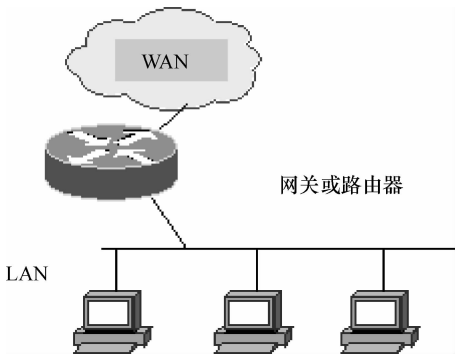


图 2-3　局域网-广域网互连

（3）局域网-广域网-局域网

这是将两个分布在不同地理位置的 LAN 通过 WAN 实现互连，连接设备主要有路由器和网关。

（4）广域网-广域网

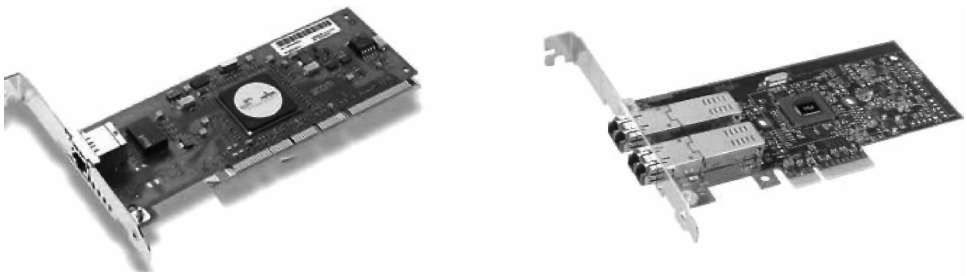
通过路由器和网关将两个或多个广域网互连起来，可以使分别连入各个广域网的主机资源能够实现共享。

2.2　常用的网络设备

2.2.1　网络适配器

1. 网络适配器的工作原理

网络适配器又称网卡，如图 2-4 所示，全称为网络接口卡（Network Interface Card，NIC），它是计算机网络中最基本的元素，也是实现计算机联网的重要设备。平常所说的网卡就是将计算机和局域网连起来的网络适配器，它的主要作用是将计算机数据转换成网络上其他设备能够识别的信号，通过介质传输。一台计算机如果没有网卡就不能上网，像显卡和声卡一样插在计算机主板的扩展槽中，是计算机与局域网相互连接的唯一接口。无论是普通计算机还是高端服务器，只要连接到网络，就都必须拥有至少一块网卡。当然如果有必要，一台计算机也可以同时安装两块或多块网卡。例如，代理服务器就需要安装两块网卡，用于分别连接局域网和 Internet。



PC网卡　　服务器网卡

图 2-4　网络适配器

在 OSI 模型中，网卡属于数据链路层的设备。在上一节网络基本原理介绍中，我们学习了数据的封装与解封的知识，发送时将上一层交下来的数据加上首部和尾部，成为以太网的帧。接收时将以太网的帧剥去首部和尾部，然后送交上一层。网卡的主要功能之一就是完成数据的封装与解封，分为两部分：一是将计算机的数据封装为帧，并通过网络将数据帧打包后发送到网络上去；二是接收网络上传过来的数据包，经过拆包，将其变为计算机可以识别的数据，传送到所在的计算机中。

网卡包括硬件和固件程序（只读存储器中的软件例程）。网卡硬件有处理器、存储器（包括 RAM 和 ROM）等控制芯片，它的主要技术参数为带宽、总线方式、电气接口方式等。网卡和局域网之间通信是通过电缆或双绞线以串行传输方式进行的，而网卡和计算机之间的通信则是通过计算机主板上的 I/O 总线以并行传输方式进行的。网卡在处理数据的时候需要进行串行/并行转换。网卡的固件程序实现逻辑链路控制和媒体访问控制的功能，还记录唯一的硬件地址即 MAC 地址。

MAC 地址即介质访问控制地址，也叫硬件地址，用来定义网络设备的位置。在 OSI 模型中，第三层网络层负责 IP 地址，第二层数据链路层则负责 MAC 地址。因此一个主机会有一个 IP 地址，而每个网络位置会有一个专属于它的 MAC 地址。MAC 地址是烧录进网卡中的，是由 48bit 长、16 进制的数字组成。0 ~ 23 位叫做组织唯一标志符（organizationally unique），是识别 LAN（局域网）节点的标识；24 ~ 47 位是由厂家自己分配。其中第 40 位是组播地址标志位。网卡的物理地址通常是由网卡生产厂家烧入网卡的 EPROM（一种闪存芯片，通常可以通过程序擦写），它存储的是传输数据时真正赖以标识发出数据的计算机和接收数据的主机的地址。

在网络底层的物理传输过程中，是通过物理地址来识别主机的，它一般也是全球唯一的。比如以太网网卡的物理地址是 48bit（比特位）的整数，如：00-23-5A-15-99-42，以机器可读的方式存入主机接口中。以太网地址管理机构 IEEE 将以太网地址，也就是 48bit 的不同组合，分为若干独立的连续地址组，生产以太网网卡的厂家就购买其中一组，具体生产时，逐个将唯一地址赋予以太网卡。MAC 地址具有全球唯一性。在个人计算机上查看 MAC 地址的方法是在命令行输入 ipconfig/all 即可看到 MAC 地址，如图 2-5 所示。

2. 网络适配器的分类

根据网络技术的不同，网卡的分类也有所不同，网卡可按以下的标准进行分类：

1）按网卡所支持带宽的不同可分为 10Mbit/s 网卡、100Mbit/s 网卡、10/100Mbit/s 自

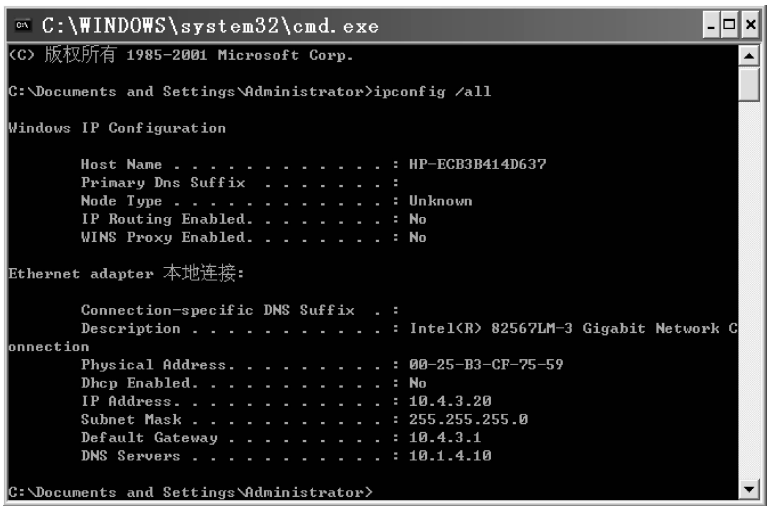


图 2-5　输入 ipconfig/all 查看 IP 地址

适应网卡、1000Mbit/s 网卡四种。现在所使用的网卡基本都是 1000Mbit/s 网卡。

2）按网卡的总线类型一般可分为 ISA 接口网卡、PCI 接口网卡、PCI-X 总线接口网卡（服务器专用）、PCMCIA 接口（笔记本计算机专用）等类型的网卡。现在主流的网卡基本都是 PCI 接口网卡。

3）网卡最终要与网络进行连接，所以必须要有一个接口使网线通过它与其他计算机网络设备连接起来，不同的网络接口适用于不同的网络类型。目前局域网基本采用以太网技术。按网络接口划分，常见的接口主要有以太网的 RJ-45 接口，其他不太常见的有细同轴电缆的 BNC 接口、粗同轴电缆的 AUI 接口、ATM 网卡、令牌环网卡和 FDDI 网卡等。

4）按应用对象的不同来划分，一般分为应用于工作站的网卡和应用于服务器的网卡。服务器通常采用专门的网卡，这种网卡基本都是千兆网卡，能支持高带宽传输的需要。一般服务器配备有两块网卡，能支持冗余备份、热插拔等服务器专用功能。

3. 无线网卡

随着无线网技术的快速发展，无线网卡已非常流行。无线网卡的作用、功能跟普通计算机网卡一样，是用来连接到局域网上的。它只是一个信号收发设备，只有在找到互联网的出口时才能实现与互联网的连接，所有无线网卡只能局限在已布有无线局域网的范围内。无线网卡就是不通过有线连接，采用无线信号进行连接的网卡。无线网卡是终端无线网络的设备，是无线局域网（Wireless LAN）无线覆盖下通过无线连接网络进行上网使用的无线终端设备。常见的无线网卡有适用于台式机使用的 PCI 接口无线网卡、笔记本电脑专用的 PCMCIA 接口无线网卡、USB 接口无线网卡，如图 2-6 所示。

2.2.2　中继器

网络信号在通过电缆进行传输的过程中会不断地衰减，当超越一定的距离时，由于存在损耗，在线路上传输的信号功率会逐渐衰减，衰减到一定程度时将造成信号失真，因此会导致接收错误。中继器（Repeater）就是为解决这一问题而设计的。中继器可以完成物理线路

TP–Link 54M 台式机无线网卡　　笔记本无线网卡　　USB无线网卡

图 2-6　无线网卡

的连接，在传输过程中对衰减的信号进行放大，保持与原数据相同。

中继器工作在物理层，它是连接网络线路的一种装置，常用于两个网络节点之间物理信号的双向转发工作，主要功能是对网线长度和网络覆盖范围进行扩充。中继器是最简单的网络互联设备，主要负责接收、恢复并转发信号，以扩展以太网。其连接拓扑结构如图 2-7 所示。

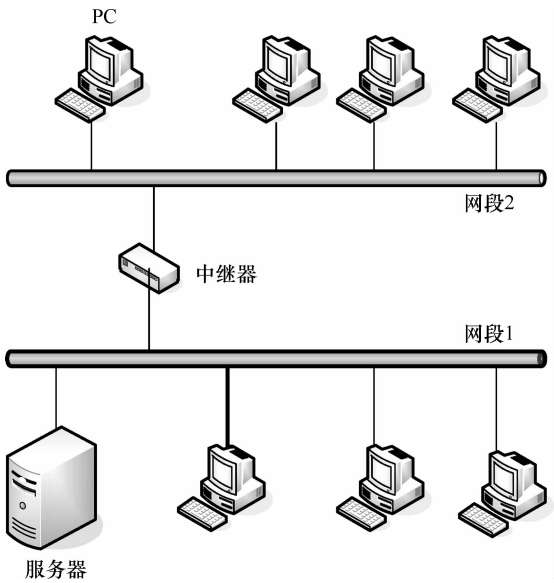


图 2-7　用中继器连接的网络拓扑结构

中继器至少有两个端口，早期同轴电缆中继器多为两个端口，可以连接两个网段。一般情况下，中继器的两端连接的是相同的媒体，但有的中继器也可以完成不同媒体的转接工作。从理论上讲中继器的使用是无限的，网络也因此可以无限延长。事实上这是不可能的，因为网络标准中都对信号的延迟范围做了具体的规定，中继器只能在此规定范围内进行有效的工作，否则会引起网络故障。以太网标准中就约定了一个以太网上只允许出现 5 个网段，最多使用 4 个中继器，而且其中只有 3 个网段可以挂接计算机终端。

多个端口的中继器即多口中继器，可以连接多个网段，形成以中继器为中心的星形结构。多口中继器在双绞线以太网中通常称为中继式集线器，或简称为集线器（HUB），HUB 可以使每个端口只与一个站点相连，形成信号的点对点传输，使以太网形成星形结构。虽然形式上是星形结构，但实际仍然是总线型结构，这种 HUB 被称为共享式集线器。

2. 2. 3　网桥

在计算机网络发展的初期，虽然还没有出现互联网，但具备一定规模的局域网已经出现，如果一个局域网的网段（一个网段下有 255 个 IP 地址）内计算机数量大于 255 台，需要用不同的网段进行连接，而且这些网段要相互连接组成一个完整的网络。但问题是原有的交换机或者集线器虽然可以把整个网络内的计算机连接在一起，但却无法突破不同网段间不能连接的限制，因此并不能够满足需求。这需要一种设备能够完成多个网段间数据包的相互

转发才可以，网桥（Bridge）正是出于这种需求，而被开发出来的。

网桥工作在 OSI 模型的数据链路层，可以用于连接具有不同物理层的网络，如连接使用同轴电缆和双绞线的网络。网桥是一种数据帧存储转发设备，它通过缓存、过滤、学习、转发和扩散等功能来完成操作。利用网桥可以将两个局域网连接起来，网桥根据 MAC 地址来转发帧，可以看作是一个“低层的路由器”。不同的是，路由器工作在网络层，根据 IP 地址进行转发。

网桥比路由器更难以控制，它不同于路由器具有 IP 等协议，并且有路由协议实现大规模的网络互联。网桥只能使用 MAC 地址和物理拓扑进行工作，因此网桥一般适用于小型且简单的网络。

2.2.4 集线器

集线器（HUB）属于数据通信系统中的基础设备，它和双绞线等传输介质一样，是一种不需任何软件支持或只需很少管理软件管理的硬件设备。它是对网络进行集中管理的最小单元，简单易用，被广泛应用到各种场合。集线器工作在局域网（LAN）环境，像网卡一样，应用于 OSI 参考模型第一层，因此又被称为物理层设备。集线器最大的特点是采用共享型模式，它不具备自动寻址能力，也不具备交换作用，所有传到集线器的数据均被广播到与之相连的各个端口。这里所指的“共享”其实就是集线器内部总线。

集线器主要应用于星形拓扑结构的网络环境，可以用集线器建立一个物理上的星形或树形网络结构。在这方面，集线器所起的作用相当于多端口的中继器。而中继器的主要功能是对接收到的信号进行再生放大，以扩大网络的传输距离。因此，集线器可以看作是中继器的一种，其区别仅在于集线器能够提供更多的端口服务，所以集线器又叫多口中继器。

集线器主要用于共享网络的组建，是解决从服务器直接到桌面最经济的方案。在交换式网络中，集线器直接与交换机相连，将交换机端口的数据送到桌面。使用集线器组网灵活，它处于网络的一个星形节点，对节点相连的工作站进行集中管理，不让出问题的工作站影响整个网络的正常运行，并且用户的加入和退出也很自由。8 口集线器如图 2-8 所示。

集线器可分为无源（Passive）集线器、有源（Active）集线器和智能（Intelligent）集线器三种。

图 2-8　8 口集线器

无源集线器：只负责把多段介质连接在一起，对信号只进行传输而不做任何处理，每一种介质段只允许扩展到最大有效距离的一半，比如双绞线只能扩充 50m。

有源集线器：具有对传输信号进行再生和放大从而扩展介质长度的功能，允许扩展到最大有效距离的一倍，如双绞线可扩充 100m。

智能集线器：除了具有有源集线器的功能外，还可以将网络的部分功能集成到集线器中，如网络管理、选择网络传输线路等。

集线器技术发展迅速，已出现网络互联集线器，在集线器上增加了线路交换功能，并且划分网络段。网络互联集线器在背板的多个网段之间实际上提供了一些类型的集成连接。以

后集线器和交换机之间的界限将会变得越来越模糊。

2.2.5　网关

网关（Gateway）有一个非常形象的比喻，从一个房间走到另一个房间，必然要经过一扇门。同样，从一个网络向另一个网络发送信息，也必须经过一道“关口”，这道关口就是网关。

顾名思义，网关就是一个网络连接到另一个网络的“关口”。在 OSI 模型中，网关是传输层及传输层以上的网络的互连设备，连接两个或多个不同的网络，使之能相互通信。网关既可以用于广域网互连，也可以用于局域网互连。网关是一种充当不同网络之间转换的系统或设备。在使用不同的通信协议、数据格式或语言，甚至体系结构完全不同的两种系统之间，网关的作用就像翻译器一样。简言之，网关就是连接两个不同类型网络的连接设备。

网关是一种比较特殊的设备，网关更多表现为一种软件或者软件和硬件的结合体，作为软件时没有一个固定的物质形态，作为硬件时如路由器，实际是一个网关。网关较其他的互联设备更为复杂，它用来连接异构网络并且要将一种协议转换成另一种协议。

在组网中，网关实质上是一个网络通向其他网络的 IP 地址。比如有网络 A 和网络 B，网络 A 的 IP 地址范围为“192. 168. 1. 1 ~ 192. 168. 1. 254”，子网掩码为 255. 255. 255. 0；网络 B 的 IP 地址范围为“192. 168. 2. 1 ~ 192. 168. 2. 254”，子网掩码为 255. 255. 255. 0。在没有路由器的情况下，两个网络之间是不能进行 TCP/IP 通信的，即使是两个网络连接在同一台交换机（或集线器）上，TCP/IP 也会根据子网掩码（255. 255. 255. 0）判定两个网络中的主机处在不同的网络里。而要实现这两个网络之间的通信，则必须通过网关。如果网络 A 中的主机发现数据包的目的主机不在本地网络中，就把数据包转发给它自己的网关，再由网关转发给网络 B 的网关，网络 B 的网关再转发给网络 B 的某个主机，如图 2-9 所示。网络 B 向网络 A 转发数据包的过程也是如此。

因此，只有设置好网关的 IP 地址，TCP/IP 就能实现不同网络之间的相互通信。那么这个 IP 地址是哪台机器的 IP 地址呢？网关的 IP 地址是具有路由功能设备的 IP 地址，具有路由功能的设备有路由器、启用了路由协议的服务器（实质上相当于一台路由器）、代理服务器（也相当于一台路由器）。

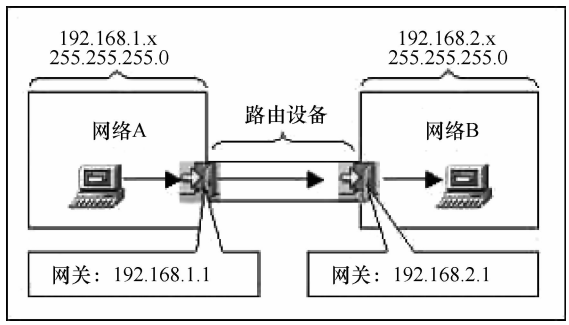


图 2-9　网关工作过程

如果搞清了什么是网关，默认网关也就好理解了。就好像一个房间可以有多扇门一样，一台主机可以有多个网关。默认网关的意思是一台主机如果找不到可用的网关，就把数据包发给默认指定的网关，由这个网关来处理数据包。现在主机使用的网关，一般指的是默认网关。如我们上网手动配置了一个默认网关地址，这个默认网关意味着所有的数据默认就向这个地址转发，这个地址多半是主机上连的局域网络设备（交换机或路由器）的 IP 地址。

2.3 交换机

2.3.1 交换机的基本概念

交换机（Switch，意为“开关”）是一种用于电信号转发的网络设备。它可以为接入交换机的任意两个网络节点提供独享的电信号通路。广义的交换机就是一种在通信系统中完成信息交换功能的设备。最常见的交换机是以太网交换机。其他常见的还有电话语音交换机、光纤交换机等。我们通常所指的交换机就是以太网交换机，是组建局域网中最主要的设备，如图 2-10 所示。

图 2-10 以太网交换机

交换机拥有一条很高带宽的背部总线和内部交换矩阵。交换机的所有端口都挂接在这条背部总线上，控制电路收到数据包以后，处理端口会查找内存中的地址对照表以确定目的 MAC（网卡的硬件地址）的 NIC（网卡）挂接在哪个端口上，通过内部交换矩阵迅速将数据包传送到目的端口，目的 MAC 若不存在广播到所有的端口，接收端口回应后交换机会“学习”新的地址，并把它添加入内部 MAC 地址表中。

使用交换机也可以把网络“分段”，通过对照 MAC 地址表，交换机只允许必要的网络流量通过交换机。通过交换机的过滤和转发，可以有效地减少冲突域，但它不能划分网络层广播，即广播域。

交换机在同一时刻可进行多个端口之间的数据传输。每一端口都可视为独立的网段，连接在其上的网络设备独自享有全部的带宽，无须同其他设备竞争使用。当节点 A 向节点 D 发送数据时，节点 B 可同时向节点 C 发送数据，而且这两个传输都享有网络的全部带宽，都有着自己的虚拟连接。假使这里使用的是 10Mbit/s 的以太网交换机，那么该交换机这时的总流通量就等于 $2 \times 10\text{Mbit/s} = 20\text{Mbit/s}$，而使用 10Mbit/s 的共享式集线器时，一个集线器的总流通量也不会超出 10Mbit/s。

总之，交换机是一种基于 MAC 地址识别，能完成封装转发数据包功能的网络设备。交换机可以“学习” MAC 地址，并把其存放在内部地址表中，通过在数据帧的始发者和目标接收者之间建立临时的交换路径，使数据帧直接由源地址到达目的地址。

2.3.2 交换机的工作原理

在计算机网络基础原理的课程中，我们学习了以太网中的一台主机要传输数据时，一般按如下步骤进行：

1）侦听信道上是否有信号在传输。如果有的话，表明信道处于忙状态，就继续侦听，直到信道空闲为止。

2）若没有侦听到任何信号，说明信道空闲，就开始传输数据。

3）传输的时候继续侦听，如发现冲突则执行退避算法，随机等待一段时间后，重新执行步骤 1）（当发生冲突时，涉及冲突的计算机会发送一个拥塞序列，以警告所有的节点）。

4）若未发现冲突则发送成功，计算机会返回到侦听信道状态。

从这个过程中我们知道早期以太网采用 CSMA/CD（载波侦听多路访问/冲突检测）方法，以广播竞争传输为机制，以处理冲突域。后来以太网发展为快速以太网，引入星形网络结构，仍然遵守 CSMA/CD 广播竞争传输机制，关键在于减少了由于广播带来的冲突。交换式网络正是基于解决这个问题而诞生的，交换式网络会对接收到的所有帧进行检查，读取帧的源 MAC 地址字段后，便做出一个假定：如果监测到一个来自某个端口上的帧，那么发送这个帧的工作站就连接在这个端口上，从而减少了网络冲突，扩展了网络带宽，分割了网络碰撞域，使得网络冲突被限制在最小范围内，目前使用在交换式网络中最为广泛的设备就是交换机。以太网已经发展成快速以太网、千兆以太网、万兆以太网等，成为当今最广泛的标准（IEEE802.3）。

2.3.3　以太网交换机的基本功能

交换机的基本功能包括以下三个方面：

1）地址学习：以太网交换机能够学习到所有连接到其端口的设备的 MAC 地址，地址学习的过程是通过监听所有流入的数据帧，对其源 MAC 地址进行校验，并将 MAC 地址同相应的端口映射起来存放在交换机缓存中的 MAC 地址表中。

2）帧的转发/过滤：当一个数据帧到达交换机后，交换机通过查找 MAC 地址表来决定如何转发数据帧。数据帧的目的地址在 MAC 地址表中有映射时，它被转发到连接目的节点的端口而不是所有端口（如该数据帧为广播/组播帧则转发至所有端口）。

3）消除回路：当交换机包括一个冗余回路时，以太网交换机通过生成树协议避免回路的产生。

目前，交换机还具备了一些新的功能，如对 VLAN（虚拟局域网）的支持、对链路汇聚的支持。交换机除了能够连接同种类型的网络之外，还可以在不同类型的网络（如以太网和快速以太网）之间起到互连作用。如今许多交换机都能够提供支持快速以太网或 FDDI 等的高速连接端口，用于连接网络中的其他交换机或者为带宽占用量大的关键服务器提供附加带宽。

一般来说，交换机的每个端口都用来连接一个独立的网段，但是有时为了提供更快的接入速度，我们可以把一些重要的网络计算机直接连接到交换机的端口上。这样，网络的关键服务器和重要用户就拥有更快的接入速度，支持更大的信息流量。

2.3.4　以太网交换机的分类

交换机功能强大，目前业界推出了各种类型的交换机，主要是为了满足各种不同应用环境需求。交换机的分类标准多种多样，常见的有以下几种：

1）根据传输介质和传输速度划分，分为以太网交换机、快速以太网交换机、千兆以太网交换机、万兆以太网交换机、ATM 交换机、FDDI 交换机和令牌环交换机。

2）根据交换机端口结构划分，分为固定端口交换机和模块化交换机。

3）根据工作协议层划分，分为第二层交换机、第三层交换机和第四层交换机。二层交换机一般做接入交换机使用，三层交换机做核心交换机和汇聚交换机使用。

4）根据网络层次结构划分，分为核心交换机、汇聚交换机和接入交换机。

5）根据是否支持网管功能划分，分为网管型交换机和非网管理型交换机。

6）根据交换机的外观结构划分，分为机架式、固定配置式带扩展槽和固定配置式不带扩展槽交换机。机架式交换机是一种插槽式的交换机，这种交换机扩展性较好，可支持不同的网络类型，如以太网、快速以太网、千兆以太网、ATM、令牌环及 FDDI 等，但价格较贵。固定配置式带扩展槽交换机是一种有固定端口数并带少量扩展槽的交换机，这种交换机在支持固定端口类型网络的基础上，还可以支持其他类型的网络，价格居中。固定配置式不带扩展槽交换机仅支持一种类型的网络，但价格较便宜。

2.3.5 交换机的主要性能指标

以太网交换机的几个主要性能指标决定了交换机的整体性能，主要有：

1）模块化插槽数量：模块化插槽数量是指模块化交换机所能连接的最大模块数，这个参数对固定端口交换机没有实际意义。在模块化交换机中，为用户预留了不同数量的空余插槽，以方便用户扩充各种接口，预留的插槽越多，用户扩充的余地就越大。一般来说，这种结构的交换机的插槽数量不能低于两个。

模块化交换机配备了多个空闲的插槽，用户可任意选择不同数量、不同速率和不同接口类型的模块，以适应千变万化的网络需求，拥有更大的灵活性和可扩充性。像这样模块化交换机的端口数量就取决于模块的数量和插槽的数量。一般来说，企业级交换机应考虑其扩充性、兼容性和排错性，因此应当选用模块化交换机以获取更多的端口。

2）背板带宽：交换机接口处理器或接口卡和数据总线间所能吞吐的最大数据量。背板带宽标志了交换机总的数据交换能力，单位为 Gbit/s，也叫交换带宽，一般的交换机的背板带宽从几 Gbit/s 到上百 Gbit/s 不等。一台交换机的背板带宽越高，所能处理数据的能力就越强，但同时设计成本也会越高。

3）包转发率：标志交换机转发数据包能力的大小。单位一般为 pps（包每秒），一般交换机的包转发率在几十 Kpps 到几百 Mpps 不等。包转发率是指交换机每秒可以转发多少百万个数据包（Mpps），即交换机能同时转发的数据包的数量。包转发率以数据包为单位体现了交换机的交换能力。其实决定包转发率的一个重要指标就是交换机的背板带宽，背板带宽标志了交换机总的数据交换能力。一台交换机的背板带宽越高，所能处理数据的能力就越强，也就是包转发率越高。

4）交换机的传输速度：交换机端口的数据交换速度。目前，常见的有 10Mbit/s、100Mbit/s、1000Mbit/s 等几类。除此之外，还有 10GMbit/s 交换机，但目前很少。

5）交换机设备的端口数量：此参数是针对固定端口交换机而言，常见的标准的固定端口交换机端口数有 8、12、16、24、48 等几种。而非标准的端口数主要有：4 端口，5 端口、10 端口、12 端口、20 端口、22 端口和 32 端口等。

6）网络管理：网络管理员通过网络管理程序对网络上的资源进行集中化管理的操作，包括配置管理等。一台设备所支持的管理程度反映了该设备的可管理性及可操作性。而交换机的管理功能是指交换机如何控制用户访问交换机，以及用户对交换机的可视程度如何。通常，交换机厂商都提供管理软件或满足第三方管理软件的远程管理交换机。一般的交换机满足 SNMP MIB Ⅰ/MIB Ⅱ统计管理功能，而复杂一些的交换机会通过内置 RMON 组（mini-RMON）来支持 RMON 主动监视功能。有的交换机还允许外接 RMON 监视可选端口的网络

状况。

7）交换机堆叠是通过厂家提供的一条专用连接电缆，从一台交换机的“UP”堆叠端口直接连接到另一台交换机的“DOWN”堆叠端口，以实现单台交换机端口数的扩充。一般交换机能够堆叠 4 ~9 台。为了使交换机满足大型网络对端口的数量的要求，一般在较大型网络中都采用交换机的堆叠方式。要注意的是，只有可堆叠交换机才具备这种端口，所谓可堆叠交换机，就是指一个交换机中一般同时具有“UP”和“DOWN”堆叠端口。当多个交换机连接在一起时，其作用就像一个模块化交换机一样，堆叠在一起交换机可以当作是一个单元设备来进行管理。一般情况下，当有多个交换机堆叠时，其中存在一个可管理交换机，利用可管理交换机可对此可堆叠式交换机中的其他“独立型交换机”进行管理。可堆叠式交换机可非常方便地实现对网络的扩充，是新建网络时最为理想的选择。

堆叠中的所有交换机可视为一个整体的交换机来进行管理，也就是说，堆叠中所有的交换机从拓扑结构上可视为一个交换机。堆叠在一起的交换机可以当作一台交换机来统一管理。交换机堆叠技术采用了专门的管理模块和堆栈连接电缆，这样做的好处是：一方面增加了用户端口，能够在交换机之间建立一条较宽的宽带链路，这样每个实际使用的用户带宽就有可能更宽（只有在并不是所有端口都在使用的情况下）；另一方面多个交换机能够作为一个大的交换机，便于统一管理。

8）交换机延时（Latency）：从交换机接收到数据包到开始向目的端口复制数据包之间的时间间隔。有许多因素会影响延时大小，比如转发技术等。采用直通转发技术的交换机有固定的延时，因为直通式交换机不管数据包的整体大小，而只根据目的地址来决定转发方向。所以，它的延时是固定的，取决于交换机解读数据包前 6 个字节中目的地址的解读速率。采用存储转发技术的交换机由于必须要在接收完了完整的数据包后才开始转发数据包，所以它的延时与数据包大小有关。数据包大，则延时大；数据包小，则延时小。采用直通转发技术的千兆交换机有固定的延时，因为直通式交换机不管数据包的整体大小，而只根据目的地址来决定转发方向。所以，它的延时是固定的。

2.4　路由器

2.4.1　路由器的基本概念

首先，我们要明白路由的概念，路由就是从一个地方出发，到达目标地所经过的路线。比如我们从辽宁省沈阳市某街道给广东省广州市某街道邮寄一个包裹，首先填写寄件人（发送方的地址），也需要明确收件人（接收方）的省市、区县、街道等地址；这个包裹开始从发件局发往目标省市，途经北京、郑州、武汉、长沙，抵达广州，然后这个包裹被交给收件人所在街区的邮递员，最终，这个包裹送达收件人。这其中途经的城市和分拣站，形成了一个包裹的“路由”。计算机网络采用类似的过程，发往互联网络的信息首先被送到与目的网络相连的路由器，路由器实际上起着这个网络的分发中心的作用，它把信息送到目的子网，最后此信息被发送到目的主机的目的端口上。

路由器是一种连接多个网络或网段的网络设备，这些网络可能是同构的也可能是异构的，它能将不同网络或网段之间的数据信息进行“翻译”，以使它们能够相互“读”懂对方

的数据，从而构成一个更大的网络。

图 2-11 给出了一个简单的互联网络的系统，用路由器将不同的网络连接起来，网络 1、网络 2、网络 3 通过路由器 A、路由器 B、路由器 C 实现互联，网络 2 中的主机 1 和 2 可以通过路由器 B、路由器 C 与网络 3 上的主机 3 通信。

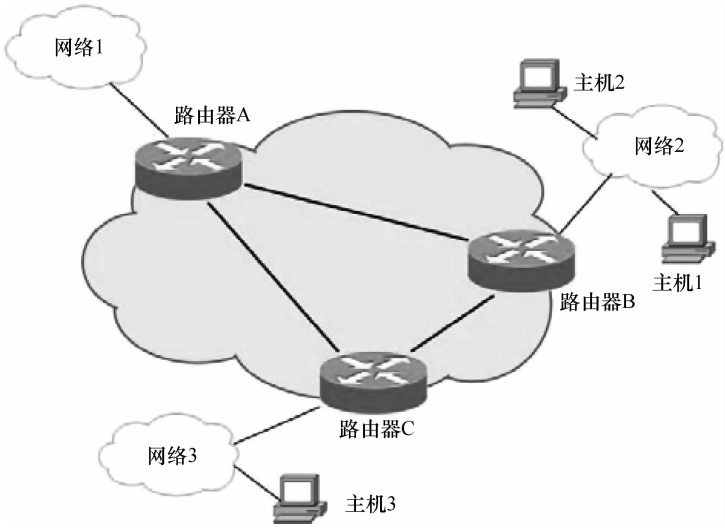


图 2-11　简单的网络连接

从本质上讲，路由器的作用是将一个报文分组从一个网络路由到另一个网络。路由器就是一个中间系统，用来连接两个或者多个网络。一个路由器简单到可以只是一台安装有两块网卡的 PC，从一块网卡接收进来的数据包，经过处理，转发到另一个接口进行发送。路由器是负责在网络层对 IP 数据包进行转发的主要设备，它还负责对 IP 数据包进行灵活的路由选择，把数据逐段向目的地转发。它掩盖了下层网络的细节，使各类网络都在 IP 上达到统一。

2.4.2　路由器的工作原理

路由器工作在 OSI 参考模型的网络层，完成不同网络之间的数据存储、分组和转发，它可以根据报文来传输数据，完成网络层路由和转发任务。路由器的基本用途是连接多个逻辑上分开的网络，必须具有判断网络地址和选择路径的功能，能够在多个网络互联环境中建立灵活的连接，并可用完全不同的数据分组和介质访问方法连接各种子网。路由器可以支持多种协议（例如 TCP/IP、IPX/SPX、AppleTalk），但在以太网中主要运行的是 TCP/IP。

目前，互联网就是 TCP/IP 网络，全球网络通过路由器互连起来，Internet 就是成千上万个 IP 子网通过路由器互连起来的国际性网络。这种网络称为以路由器为基础的网络，形成了以路由器为节点的“网间网”。在“网间网”中，路由器不仅负责对 IP 分组的转发，还要负责与别的路由器进行联络，共同确定“网间网”的路由选择和维护路由表。

路由器主要完成两件事情：寻径和转发。寻径即判定到达目的地的最佳路径，由路由选择算法来实现。路由器利用网络寻址功能使路由器能够在网络中确定一条最佳的路径。由于涉及不同的路由选择协议和路由选择算法，要相对复杂一些。为了判定最佳路径，路由选择

算法必须启动并维护包含路由信息的路由表，其中路由信息依赖于所用的路由选择算法而不尽相同。路由选择算法将收集到的不同信息填入路由表中，根据路由表可将目的网络与下一跳（Next Hop）的关系告诉路由器。路由器间互通信息进行路由更新，更新维护路由表使之正确反映网络的拓扑变化，并由路由器根据量度来决定最佳路径。这就是路由选择协议（Routing Protocol），例如路由信息协议（RIP）、开放式最短路径优先协议（OSPF）和边界网关协议（BGP）等。

转发即沿寻径好的最佳路径传送信息分组。IP 地址的网络部分确定分组的目标网络，并通过 IP 地址的主机部分和设备的 MAC 地址确定到目标节点的连接。路由器的某一个接口接收到一个数据包时，会查看包中的目标网络地址以判断该包的目的地址在当前的路由表中是否存在（即路由器是否知道到达目标网络的路径）。如果发现包的目标地址与本路由器的某个接口所连接的网络地址相同，那么数据马上转发到相应接口；如果发现包的目标地址不是自己的直连网段，路由器会查看自己的路由表，查找包的目的网络所对应的接口，并从相应的接口转发出去；如果路由表中记录的网络地址与包的目标地址不匹配，则根据路由器配置转发到默认接口，在没有配置默认接口的情况下会给用户返回目标地址不可达的 ICMP 信息。

2.4.3　路由器的基本功能

从上一节我们学习到，所有的路由器必须完成两个任务：路由处理和包转发。路由处理主要是收集网络拓扑信息并形成转发表，包转发处理时根据转发表将报文从输入端口转发到适当的输出端口。基本上路由器具有以下功能：

1）实现 TCP、IP、UDP、ICMP 等互联网协议。

2）连接到两个或多个数据包交换的网络，对每个连接到的网络，实现该网络所要求的数据通信的寻址和转发功能。

3）接收及转发数据包，必要时将数据包分段。在收发过程中实现缓冲区管理、拥塞控制以及公平性处理。

4）支持各种网关协议，如内部网关协议（IGP）、外部网关协议（EGP）、边界网关协议（BGP）。动态维护网络路由信息以符合网络当前的拓扑结构，从而能根据路由数据信息为每一个 IP 数据包选路。

5）提供网络管理和系统支持机制，包括配置、诊断、升级、状态报告、异常情况报告及控制等，并实现网络管理功能。

2.4.4　路由器的分类

当前路由器的分类方法各异，从能力上分，路由器可分为高端路由器、中端路由器和低端路由器。各厂家划分也不完全一致。通常将背板交换能力大于 40Gbit/s 的路由器称为高端路由器，之下的为中低端路由器。以思科（Cisco）公司为例，Cisco 12800 路由器为高端路由器，7500 以下系列路由器为中低端路由器。

从结构上分，路由器可分为模块化结构与非模块化结构，通常中高端路由器为模块化结构，低端路由器为非模块化结构。

从功能上分，路由器可分为通用路由器与专用路由器，一般所指的路由器都是通用路由

器，专用路由器对硬件和功能有特殊要求，如宽带接入路由器强调宽带接口数量及种类。

从路由器在网络中的位置划分，路由器可分为核心路由器、企业级路由器和接入路由器等。

2.4.5 路由器的主要性能指标

不同级别的路由器，要求实现的功能以及要达到的性能都不一样。路由器有一些关键性能指标。

1）背板能力：背板是输入与输出端口间的物理通路。背板能力是路由器的内部实现。传统路由器采用共享背板，但高速路由器一般采用可交换式背板设计。背板能力体现在路由器的吞吐量上。

2）吞吐量：吞吐量是路由器的包转发能力，吞吐量与路由器端口数量、端口速率、数据包长度、数据包类型等有关，一般泛指处理器处理数据包的能力。高速路由器的包转发能力至少在20Mbit/s以上。吞吐量包括整机吞吐量和端口吞吐量。整机吞吐量是路由器整机的包转发能力，是整机每秒包转发数量。端口吞吐量是端口的包转发能力。一般整机吞吐量通常小于路由器所有端口吞吐量之和。

3）丢包率：路由器在稳定的持续负载下，由于资源缺少而不能转发的数据包在应该转发的数据包中所占的比例。丢包率通常用来衡量路由器在超负载工作时的性能。

4）全双工线速转发能力：路由器最基本且最重要的功能是数据包转发。在同样端口速率下转发小包是对路由器包转发能力最大的考验。全双工线速转发能力是指以最小包长（以太网64字节、POS口40字节）和最小包间隔（符合协议规定）在路由器端口上双向传输的同时不引起丢包。该指标是路由器性能的重要指标。

5）路由表能力：路由器通常依靠所建立及维护的路由表来决定包的转发。路由表能力是指路由表内所容纳路由表项数量的极限。由于Internet上执行BGP协议的路由器通常拥有数十万条路由表项，所以该项目也是路由器能力的重要体现。一般而言，高速路由器应该能够支持至少25条路由，平均每个目的地址至少提供两条路径，系统必须支持至少25个BGP对等体以及至少50个IGP邻居。

6）网管能力：网管是指网络管理员通过网络管理程序对网络上资源进行集中化管理的操作。包括配置管理、记账管理、性能管理、差错管理和安全管理。设备所支持的网管程度体现设备的可管理性与可维护性。

7）可靠性和可用性：包括路由器部件的冗余，如接口冗余、板卡冗余、电源冗余，以保障设备有足够的可靠性与可用性。路由器还支持热插拔组件的更换等。

2.5 主流网络产品介绍

前面我们学习了关于交换机、路由器的一些基本理论知识，本节我们将结合业界推出的几款主流的网络产品做一些介绍，进一步加深对这些产品的认识。目前，全球知名的网络设备制造商主要有思科系统公司（Cisco Systems，Inc.）、瞻博网络公司（Juniper Networks）等，国内知名的主要有华为、华三通信（简称H3C）、锐捷网络等，这些公司都是互联网解决方案的领先提供者，其设备和软件产品主要用于连接计算机网络系统，相继推出了一系列

业界领先的交换机和路由器等网络互连产品并得到广泛的应用。关于这些产品的详细信息，请访问这些产品制造商的官方网站进行查阅，以了解更多的知识和信息。

2.5.1　交换机简介

思科的交换机产品以“Catalyst”为商标，包含 1900、2900、3500、4500、6500 等多个系列。一类是固定配置交换机，包括 3500 及以下的大部分型号，比如 1924 是 24 口 10M 以太交换机，带两个 100M 上行端口。除了有限的软件升级之外，这些交换机不能扩展。另一类是模块化交换机，主要指 4500 及以上的机型，网络设计者可以根据网络需求，选择不同数目和型号的接口板、电源模块及相应的软件。下面分别介绍几款比较典型的产品。

1. 高端交换机

思科 2008 年推出了 Nexus 7000 系列交换机，主要用于模块化数据中心级产品，适用于高度可扩展的万兆以太网网络，其交换矩阵架构的速度能扩展至 15Tbit/s 以上。它的设计旨在满足大多数关键任务数据中心的要求，提供永续的系统运营和无所不在的虚拟化服务。

我们来认识和了解一下 Nexus 7000 交换机。这是思科推出的业界最先进的一款高端核心路由交换机，Cisco Nexus 7000 系列具有 10 插槽机箱和 18 插槽机箱，也属于模块化交换机，即可以热插拔很多板卡和部件，如图 2-12 所示。

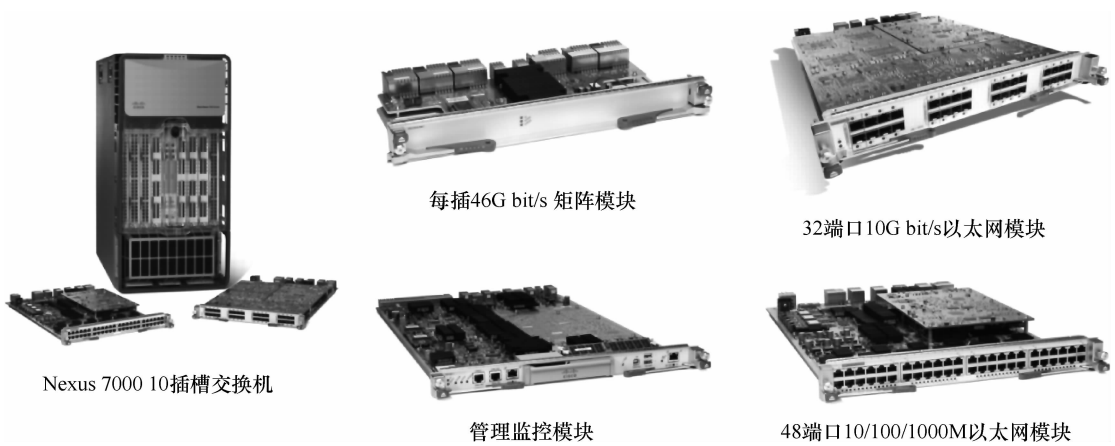


图 2-12　思科 Nexus 7000 系列交换机的常用板卡

拥有最多 8 个 I/O 模块插槽的 Cisco Nexus 7000 系列 10 插槽机箱具有如下特性：

1）最多支持 256 个万兆以太网或 384 个千兆以太网端口，能够满足大型部署的需求。

2）前后通风有助于确保使用 Cisco Nexus 7000 系列 10 插槽机箱能够满足热通道和冷通道部署要求，而不会增加复杂性。

3）分别采用两个系统风扇架和两个交换矩阵风扇架进行冷却。每个风扇架都配备有冗余风扇，独立变速风扇能随着周围温度自动调整，不仅降低了进行出色管理的设施的能耗，而且能实现最佳交换机运行状态。该系统设计提高了冷却效率，并提供冗余功能，使得进行热插拔时不会影响系统；如果一个风扇或整个风扇架发生故障，系统能继续运行，不会对冷却能力造成重大影响。

4）集成电缆管理系统用于完全配置的系统布线，能将所有电缆整齐地放在一边或两

边，以实现最大的灵活性，不妨碍任何重要组件，即使是在系统布线完好的情况下也能轻松地进行维护。

5）系统拥有可选的空气过滤器，有助于确保流过系统的空气清洁。添加空气过滤器能满足 NEBS 要求。

6）机箱顶端的一系列 LED 清晰地提供主要系统组件的状态显示，能提示操作员是否需要执行进一步的调查。这些 LED 负责报告电源、风扇、交换矩阵、控制引擎和 I/O 模块的状态。

7）电缆管理盖和可选的模块前门能使安装在系统中的布线和模块不受意外事件的影响。透明的前门使客户能够查看布线、模块指示灯和状态指示灯情况。

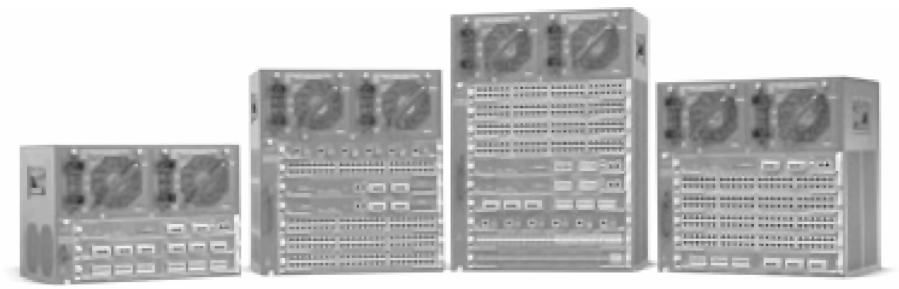
思科推出的 Catalyst 6500 系列交换机，如图 2-13 所示。这一系列交换机属于高端模块化、核心路由交换机，其中以 6509 应用最为广泛。它能够通过多种机箱配置和 LAN/WAN/MAN 接口提供可扩展的性能和端口密度，提供 3 插槽、6 插槽、9 插槽和 13 插槽的机箱，以及多种集成式服务模块，包括数千兆位网络安全性、内容交换、语音和网络分析模块。从 48 端口到 576 端口的 10/100/1000 以太网布线室到能够支持 192 个 1Gbit/s 或 32 个 10Gbit/s 骨干端口，提供每秒数亿个数据包处理能力的网络核心，思科 Catalyst 6500 系列能够借助冗余路由与转发引擎之间的故障切换功能延长网络正常运行时间。

图 2-13　思科 Catalyst 6500 系列交换机

2. 中端交换机

思科 Catalyst 4500 系列交换机属于中端交换机产品，也是模块化交换机，如图 2-14 所示。这个系列包括四种机箱：4510R-E（10 个插槽）、4507R-E（7 个插槽）、4506-E（6 个插槽）和 4503-E（3 个插槽）。思科 Catalyst 4500 系列采用统一的架构，并使用能够扩展到 388 个以太网端口的现有思科 4000 系列线路卡。思科 Catalyst 4500 系列包括“典型”管理引擎和线路卡，以及新开发的“E 系列”管理引擎和线路卡。典型管理引擎和线路卡的每个线路卡插槽提供 6 千兆交换容量，转发性能为 102Mpps。新开发的 E 系列管理引擎和线路卡提供了很多增强特性，包括每个线路卡插槽提供 24 千兆交换容量，以及 250Mpps 的总转发性能。

思科 Catalyst 3500 系列交换机也属于中端产品。其基本特性包括背板带宽高达 10Gbit/s，转发速率为 7.5Mpps，它支持 250 个 VLAN，支持 IEEE 802.1Q 和 ISL Trunking，支



Cisco Catalyst4503-E　Cisco Catalyst4507R-E　Cisco Catalyst4510R-E　Cisco Catalyst4506-E

图 2-14　思科 Catalyst 4500 系列交换机

持 CGMP 网 / 千兆以太网交换机，可选冗余电源等。

3. 低端交换机

思科 Catalyst1900 和 Catalyst 2900 是低端产品的典型代表，这些交换机基本上都是固化交换机。这一类交换机一般具有 24/48 个 10/100Mbit/s 自适应以太网端口和两个千兆以太网端口，24G 背板带宽，带可热插拔的冗余电源，有一系列容错特征和网管特性。

2.5.2　路由器简介

思科提供了业界范围最广、灵活性最高的安全、高性能接入路由器、集成多业务路由器和汇聚路由器，可为最广泛的机构部署种类丰富的服务，其范围从家庭办公机构、小型办公机构直到大型企业的分支机构和总部。

思科路由器产品有三个特点：它的路由器是模块化的、可预制的及可进行混合配置的。另外，思科还与完全的路由器配置一起提供针对个人计算机（PC）设计的路由器平台。将路由器和小型集线器结合在一起，形成一种适于小型办公室安装的设备。在网络环境中，思科路由器成功地实现离不开正确的布局和配置，每台路由器都担负一种特定的职责。

从应用的角度，思科路由器拥有全面的产品组合，思科推出了分支机构路由器、数据中心互联平台路由器、移动互联网路由器、服务提供商核心路由器、服务提供商边缘路由器、精睿系列路由器、广域网汇聚与互联网边缘路由器等多种产品。下面分别介绍几款比较典型的路由器产品。

1. 高端路由器

思科推出的高端路由器主要有 ASR 1000 系列汇聚服务路由器、XR 12000 系列路由器、12400 系列路由器、12000 系列路由器、10000 系列路由器，还有 7600、7500、7200 系列路由器。这一类路由器都是具有强大路由能力的模块化路由器。如图 2-15 所示 7600 系列路由器。

图 2-15　思科 7600 系列路由器

思科推出的 7600 业务路由器可在运营商的网络边缘提供城域网和广域网的连接，主要致力于以干线速提供高起点的 IP 业务。该产品系列可在多种高性能接口上把

直接光纤连接与丰富的智能 IP 业务进行组合，使得电信运营商能使其网络以光速支持业务。思科 7600 业务路由器是 Cisco 端到端电信城域以太网解决方案的重要组件。

思科 7600 系列路由器的核心是思科 7600 路由交换处理器 720（RSP 720），它专门设计用来提供高可扩展性，具有出色性能和快速融合能力，以满足当前和未来要求的语音、视频、数据和移动四网合一服务。思科 7600 RSP 720 采用了与思科 Supervisor Engine 720 相同的高性能 720-Gbit/s 交换矩阵，并结合了全新、基于 ASIC 的转发引擎。这个单一模块提供了每插槽 40Gbit/s 的交换矩阵功能，支持 4 端口万兆以太网和 48 端口 10/100/1000 密度线卡。凭借对于 IPv4、IPv6 单播和组播，以及 MPLS 的硬件转发性能，思科 7600 RSP 720 能够提供高速集中转发和丰富的数据包处理特性，如访问控制列表（ACL）、QoS、MPLS VPN 等。通过将思科 7600 RSP 720 与分布式转发卡（DFC）相结合，整机性能可扩展至 400Mpps。

2. 中端路由器

思科中端路由器主要包括 3600 系列、3700 系列、3800 系列路由器，如图 2-16 所示。思科 3800 系列的集成化服务路由架构构建于强大的思科 3700 系列路由器的基础之上，它内嵌并集成了安全和话音处理以及先进服务，以迅速部署新应用，包括应用层功能、智能网络服务和融合通信。思科 3800 系列支持每插槽多个快速以太网接口、时分多路复用（TDM）互联，以及对于支持 802.3af 以太网电源（PoE）的全面集成配电等的带宽要求。它同时支持现有模块化接口系列。这确保了持续投资保护，可在部署新服务和应用时支持网络扩展或技术变动。通过将多个独立设备的功能集成入单一小巧设备之中，思科 3800 系列大幅降低了管理远程网络的成本和复杂度。

图 2-16　思科 3825 和思科 3845 集成多业务路由器

3. 低端路由器

思科低端路由器有应用于家庭、办公室等无线网络的思科 SOHO 系列、800 系列路由器，也有用于中小型企业与分支结构互联的 1600、1700、1800、2500、2800 等系列路由器，如图 2-17 所示。这一类路由器一般都是集成多业务路由器，均提供嵌入式硬件加密加速、可选防火墙、入侵预防和应用程序服务。此外，这些平台还支持业界最广泛的有线和无线连接选项，如 T1/E1、xDSL、3G 和 GE。

思科890C路由器　　思科1941路由器　　思科2800路由器

图 2-17　思科低端系列路由器

思科 2800 系列路由器能以线速为多条 T1/E1/xDSL 连接提供多种高质量并发服务。这

些路由器提供了内嵌加密加速和主板话音数字信号处理器（DSP）插槽，入侵保护和防火墙功能，集成化呼叫处理和语音留言，用于多种连接需求的高密度接口，以及充足的性能和插槽密度，以用于未来网络扩展和高级应用。思科 2800 系列可满足中小型企业和企业分支机构的 IP 通信需求，同时在单一路由平台中提供业界领先的安全性。

本 章 小 结

网络设备及部件是连接到网络中的物理实体。网络设备的种类繁多，不断推陈出新。基本的网络设备有：计算机（PC、工作站）、服务器、集线器、交换机、网桥、路由器、网关、网络接口卡（NIC）、无线接入点（WAP）、打印机和调制解调器，利用这些基本的网络设备可以组建局域网络或更大规模的互联网络。在这些设备中，专属于网络互连设备的主要包括中继器、网桥、集线器、网关、交换机、路由器等。

本章主要介绍的内容如下：

1）介绍了网络互连的概念和工作原理。

2）分别介绍了交换机、路由器等常用网络设备的工作原理和基本特性；重点介绍以太网交换机和路由器的工作原理和主要性能指标。

3）针对业界主流的思科交换机和路由器产品进行了介绍，通过对这些产品的了解可以增强对网络互连设备原理的理解。

第 3 章　数据中心服务器与存储技术

3.1　服务器技术概述

计算机网络发展的目标之一是给人们带来快捷便利的上网服务和提供信息服务。如人们出门订票、航班、旅游、酒店查询等，这些信息服务都依赖于互联网，而且它们依赖于大量的服务器及信息系统等平台的运行。互联网的高度发达也提供了可以访问的海量信息资源，这些资源都存放在服务器和存储系统上。人们日常访问的网络服务如 WWW、FTP、DNS 等都需要部署在服务器上。因此服务器是组建计算机网络必需的设备之一。服务器作为网络的节点，存储、处理网络上 80% 的数据、信息，因此也被称为网络的灵魂。

服务器（Server）是网络上一种为客户端计算机（简称客户机，Client）提供各种服务的高可用性计算机。从功能上说，它负责侦听网络上其他客户机提交的服务请求，并提供相应的服务；从通信的对象来讲，通常是一对多的通信模式；具体到硬件上，它是网络环境中的高性能计算机，它在网络操作系统的控制下，将与其相连的硬盘、磁带、打印机、调制解调器及各种专用通信设备提供给网络上的客户站点共享，也能为网络用户提供集中计算、信息发布及数据管理等服务。它的高性能主要体现在高速运算能力、长时间的可靠运行、强大的外部数据吞吐能力等方面。服务器也必须具有承担服务并且保障服务的能力。

服务器是一种高性能的计算机，但是服务器区别于 PC，除了在服务器自身的硬件性能上有差别，服务器还必须应用在网络计算环境中，并且要为网络中的客户端提供服务。一台脱离了网络的服务器是没有太大意义的，即使配置再高，也只能被称作是一台高性能计算机，也无法实现为客户端提供网络服务的功能。在网络中，服务器为客户端提供数据存储、查询、数据转发、发布等功能，维系着整个网络环境的正常运行。

服务器从硬件构成上与我们平常所用的 PC 有很多相似之处，服务器和 PC 都有 CPU（中央处理器）、内存、硬盘、各种总线等。对于服务器来说，它能够提供各种共享服务（网络、Web 应用、数据库、文件、打印等）以及其他方面的高性能应用，它的高性能主要体现在高速度的运算能力、长时间的可靠运行、强大的外部数据吞吐能力等方面。一般服务器都是运行比较关键的信息系统等重要软件的平台，是信息化的核心设备之一。服务器从硬件构造和设计上针对网络系统的运行有特别的考虑，在处理能力、稳定性、可靠性、安全性、可扩展性、可管理性等方面比 PC 有更多优势。特别在可靠性上，针对多用户多任务环境下的服务器必备的可靠性，PC 是不具备这种性能的。用 PC 当作服务器的用户一定都曾经历过突然的停机、意外的网络中断、不时的丢失存储数据等，这都是因为 PC 的设计制造从来没有保证过多用户多任务环境下的可靠性，而一旦发生严重故障，其所带来的经济损失将是难以预料的。但一台服务器所面对的是整个网络的用户，需要 7 × 24 小时不间断工作，所以它必须具有极高的稳定性。另一方面，为了实现高速以满足众多用户的需求，服务器通过采用对称多处理器（SMP）安装、插入大量的高速内存来保证工作。它的主板可以同时安

装几个甚至几十、上百个 CPU（服务器一般所用的 CPU 也不是普通的 CPU，是厂商专门为服务器开发生产的）。内存方面当然也不一样，无论在内存容量，还是性能、技术等方面都有根本的不同。

尽管现在服务器技术已经越来越多地被应用于一些高端 PC，如 64 位、多核技术，但是与 PC 的硬件和性能指标上还是有很大的不同。另外，服务器为了保证足够的安全性，还采用了大量普通 PC 没有的技术，如冗余技术、系统备份、在线诊断技术、故障预报警技术、内存纠错技术、热插拔技术和远程诊断技术等，使绝大多数故障能够在不停机的情况下得到及时的修复，具有极强的可管理性。

服务器被大量广泛地应用于数据中心和网络机房中，著名服务器品牌有 SUN、IBM、HP（惠普）、DELL（戴尔）、联想、浪潮、曙光等，这些厂商都提供不同级别的服务器产品，满足不同用户的需求。

3.2　服务器硬件基础

服务器的硬件指标主要包括服务器的运算速度、数据吞吐能力、内外存容量。这些硬件指标取决于服务器的硬件架构、各个部件的芯片处理能力，通常包括服务器 CPU、主板、内存、硬盘等部件。

3.2.1　服务器的 CPU

1. 服务器 CPU 简介

服务器 CPU 是指专门在服务器上使用的 CPU，区别于在 PC 上安装使用的 CPU。CPU 是衡量服务器性能的首要指标。目前，服务器的 CPU 仍按 CPU 的指令系统来区分，通常分为 CISC 型 CPU 和 RISC 型 CPU 两类。随着技术的发展，业界新推出了一种 64 位的超长指令集架构（Very Long Instruction Word，VLIW）指令系统的 CPU，超长指令字体系结构起源于通用处理器，提供了硬件开销相对较低的指令级并行，在嵌入式系统中已经得到了广泛应用。

CISC 型 CPU 是基于复杂指令集的 CPU，复杂的指令系统必然增加微处理器的复杂性，复杂指令集 CPU 内部将较复杂的指令译码分成几个微指令去执行，其优点是指令多、开发程序容易，但是由于指令复杂，执行工作效率较差，处理数据速度较慢。286/386/486/Pentium 的结构都为 CISC 型 CPU。

RISC 是在 CISC 指令系统基础上发展起来的。RISC 型 CPU 是基于精简指令集的 CPU。相对于 CISC 型 CPU，RISC 型 CPU 不仅精简了指令系统，还采用了超标量和超流水线结构，大大增加了并行处理能力。目前在中高档服务器中普遍采用这一指令系统的 CPU，特别是高档服务器全都采用 RISC 指令系统的 CPU。在 RISC 架构的基础上，世界上各大知名服务器厂商纷纷研发了自己的 CPU，如 IBM 公司的 PowerPC、SUN 公司的 SPARC 系列、HP 公司的 RISC 芯片 PA-RISC 等，如图 3-1 所示。

2. Intel 处理器简介

Intel（英特尔）公司是全球最大的半导体芯片制造商，Intel 生产的 x86 系列 CPU（286/386/486/Pentium）推动了 PC 的广泛应用和发展。Intel 生产了一批应用于服务器的 CPU，主要有 Pentimu Ⅱ Xeon、Pentimu Ⅲ Xeon、Pentium Ⅲ Sever、P4 Xeon 和 Xeon MP

图 3-1　RISC 型 CPU

（Multi Processing Platform，多处理器平台）一系列 Xeon 系列 CPU。

2001 年，Intel 创新地推出了 64 位的 Itanium（安腾）处理器，这是业界第一个 64 位的 CPU。2002 年，英特尔公司又将推出 Itanium 家族的第二代产品——Itanium 2 处理器。Itanium 系列 CPU 是与其他 CPU 完全不同的 64 位 CPU，专门用在高端企业级 64 位计算环境。许多在全球业界领先的公司如 IBM、HP、DELL 都选择基于 Intel 推出的 Itanium 2 处理器作为服务器 CPU，主要基于 Itanium 2 微体系结构的特性包括到集成高速缓存的快速访问，处理器与内存之间的出色带宽，以及具有高指令执行速度和吞吐率的大量执行资源。

近年来，多核成为服务器 CPU 的主旋律。Intel 相继研发出 Xeon Clovertown 四核、Xeon MP Tigerton 四核、Dunnington Xeon 六核处理器等和 Corei7 六核等一系列多核服务器 CPU，提供功率更低、更强大的处理能力和计算能力，如图 3-2 所示。

图 3-2　Intel 多核处理器

3. AMD 处理器简介

AMD 是全球范围内知名的、以生产和研发高性能 CPU、高性能独立显卡 GPU、主板芯片组三大组件的半导体公司。自 2001 年起，AMD 相继推出了 Athlon（速龙）MP、K5、K6、K8、AMD Opteron（皓龙）、AMD Phenom（羿龙）等处理器，AMD 也提供全系列 64 位 CPU 产品。为了与 Intel 竞争，AMD 也推出了多核处理器（64 位 AthlonX2 双核、Phenom X3 三核、Phenom Ⅱ四核或 Athlon Ⅱ四核、Phenom Ⅱ X6 六核），如图 3-3 所示。

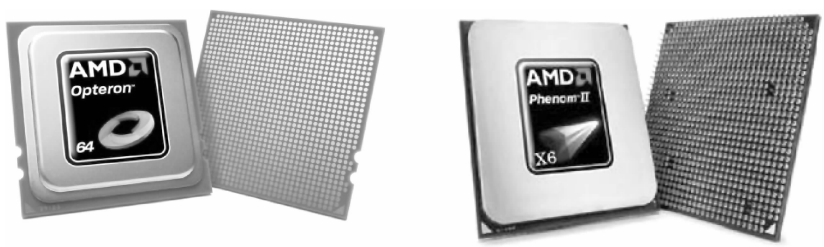


图 3-3　AMD 多核处理器

3.2.2　服务器的关键部件

1. 服务器的主板

服务器要求满足常年 7×24 小时的无故障运行，最核心的板卡就是主板。CPU、内存、硬盘、网络适配器等部件都是与主板连接。因此，主板必须能满足服务器应用的高稳定性、高性能、高兼容性、可持续性的要求。由于服务器的长时间运行、巨大的数据转换量、电源功耗量、I/O 吞吐量，因此对服务器主板的要求与普通 PC 是不同的。

服务器主板对性能方面的要求主要体现在对数据吞吐量的要求上，包括服务器内存及支持内存数量、PCI-X 插槽、板载 SCSI 接口或者 RAID 接口等。服务器主板上面承载一些数据转换量、电源功耗量、I/O 吞吐量，比如高速 SCSI 接口、高速硬盘等，在主板设计时对这些设备与主板连接的要求进行了特别考虑。

芯片组（Chipset）是主板的核心组成部分。主板芯片组几乎决定着主板的全部功能，其中，CPU 的类型、主板的系统总线频率、内存类型、容量和性能、显卡插槽规格、扩展槽的种类与数量、扩展接口的类型和数量决定着服务器的性能。芯片组 PCI Express 总线技术是当前最为先进的一种总线技术。

2. 服务器的内存

服务器内存（RAM）在各种技术上相对兼容机来说要严格得多，不仅内存的速度要求高，特别是内在纠错技术能力和稳定性方面要求更高。因此内存也是制约服务器性能的硬件条件之一。服务器内存有 2G、4G、8G、16G 甚至高达 512G。服务器内存与普通 PC 内存在外观和结构上没有什么明显的实质性区别，主要是在内存上引入了一些新的特有技术，如 ECC（错误检查和纠正）、ChipKill（IBM 推出的一种新的 ECC 内存保护标准）、Register（寄存器）、FB-DIMM（全缓冲内存模组）、热插拔技术等，具有极高的稳定性和纠错性能。如今常用的服务器内存主要有 ECC DDR、ECC DDR2、ECC DDR3，还有一些基于 FB-DIMM 的高端服务器系统的内存体系。

3. 服务器的硬盘

服务器的硬盘主要用来存储和读写非常重要的数据，而且服务器的硬盘要能够适应大数据量读写、超长运行时间的工作环境。硬盘是服务器系统和信息资源的数据仓库，所有的信息、程序、软件、资源等数据都存储在这里，硬盘一旦损坏，将会造成严重后果。因此要求硬盘读写速度快、可靠性高、安全性高。

服务器硬盘的转速通常要求达到 10000r/min（每分钟转速）、15000r/min 以上，数据传输率分别可以达到 320MBs。服务器硬盘一般采用 SMART 技术（自监测、分析和报告技术），同时硬盘厂商都采用了各自独有的先进技术来保证数据的安全。服务器硬盘一般都能承受 300～1000G 的冲击力。热插拔（Hot Swap）是一些服务器支持的硬盘安装方式，可以在服务器不停机的情况下，拔出或插入一块硬盘，操作系统能自动识别硬盘的改动。这种技术对于 24h 不间断运行的服务器来说，是非常必要的。

目前，服务器市场上主要采用三种类型的硬盘：SATA 硬盘、SCSI 硬盘以及 SAS 硬盘，其中 SATA 硬盘主要应用在 PC、低端服务器领域，而 SCSI 和 SAS 硬盘则面向中高端服务器。大多数服务器一般采用数据吞吐量大、CPU 占有率极低、高速、稳定、安全的 SCSI 硬盘。SAS 即串行连接 SCSI，是新一代的 SCSI 技术，继并行 SCSI 接口之后开发出的全新接

口，可进一步改善存储系统的效能、可用性和扩充性，并且提供与 SATA 硬盘的兼容性，如图 3-4 所示。

图 3-4　服务器热插拔 SAS 硬盘

现在业界推出的一些中高端服务器的硬盘类型接口一般为可插拔 SAS、单硬盘容量 146G 或 300G、硬盘数量一般可配置到 16 块甚至更多。

4. 服务器的电源

服务器电源是指使用在服务器上的电源（POWER），它和 PC 电源一样，都是一种开关电源。优质的电源能提供给服务器优质可靠的能量，能防御来自电网的污染或干扰，能承受负载的各种变化。服务器电源的品质优劣直接影响了硬件的安全和系统的稳定。在中高端服务器中为了保证供电需求和可靠性，大多采用冗余电源系统，即冗余热插拔电源，可以进行在线更换，如图 3-5 所示。

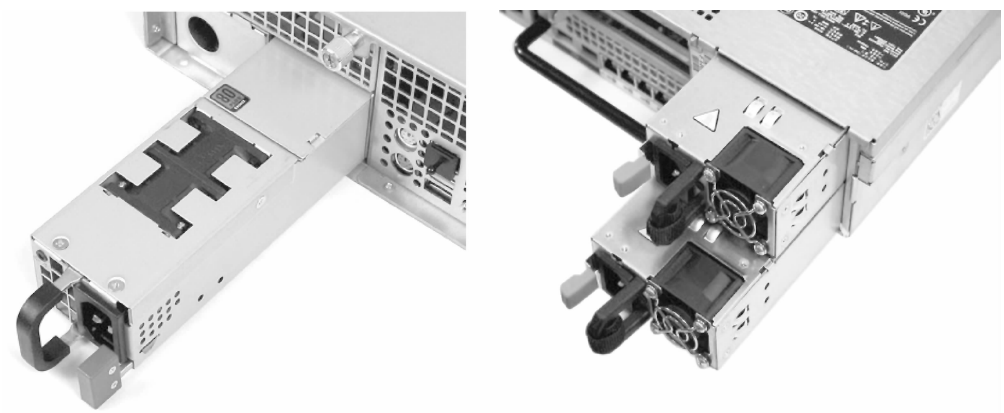


图 3-5　服务器热插拔电源

服务器电源按照标准可以分为 ATX 电源和 SSI 电源两种。ATX 标准使用较为普遍，主要用于台式机、工作站和低端服务器；SSI 标准是随着服务器技术的发展而产生的，适用于各种档次的服务器。

1）ATX 电源是目前 PC 和服务器中普遍使用的标准电源，包括单电源和冗余（Redundant）电源。单电源系统功率一般在 125～350W 之间，主要使用在 PC 和低端服务器上。

2）SSI 电源规范是 Intel 公司联合一些主要的 Intel 架构服务器生产商推出的新型服务器

电源规范。SSI 的推出规范了服务器电源技术、降低了开发成本、延长了服务器的使用寿命。根据使用环境、规模的不同，SSI 电源规范还有更多针对低端服务器、中高端服务器更为详细的规范。随着 SSI 标准的更加规范，服务器电源的发展趋势是：低压化、大功率化、高密度化；电源越做越小、电源的功率密度趋于增大，同时符合国际上电源认证、节能要求。

5. 服务器的风扇

现在随着服务器的集成度越来越高，如刀片服务器属于配件较为密集的服务器，因此散热问题也是影响服务器稳定运行的重要因素之一。风扇在服务器的散热系统中起着很大的作用，对于服务器 CPU、机箱、显卡和电源等所用的风扇是服务器正常稳定工作必不可少的硬件之一。

由于服务器使用的 CPU 的频率通常较高，有的还是双 CPU 或多 CPU，加上高转速的 SCSI 硬盘和大功率电源，这些部件发出的热量通常很大，因此机箱内空气很快变热，温度升高。能否尽快有效地排出这些热空气将是服务器稳定工作的前提条件。为了达到更好的散热效果，服务器机箱设计有多个排风口，而且各个排风口针对系统不同的发热源进行散热。

服务器机箱除了要安装多个风扇外，机箱内的散热系统也是非同寻常的。一般情况下在服务器机箱背面有两个风扇位，可供安装两个风扇，形成一个良好的散热循环系统，将机箱内的热空气迅速抽出，以降低机箱内的温度。中高端服务器还设计了冗余风扇，以避免由于系统风扇损坏而使系统内部温度升高产生工作不稳定或停机现象，如图 3-6 所示。

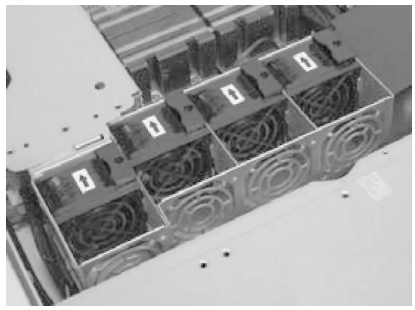
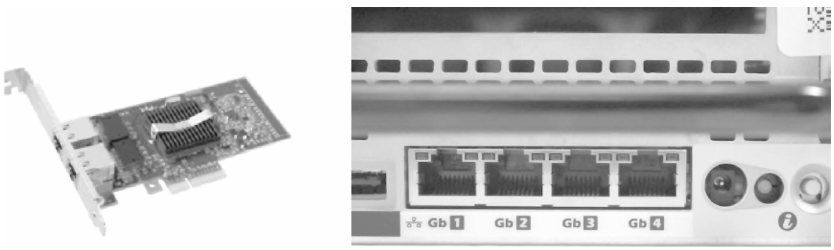


图 3-6　服务器机箱内冗余散热风扇

6. 服务器的网络接口

服务器一般都承担重要的网络应用。服务器网络适配器（网卡），一般是用于服务器与交换机等网络设备之间的连接。服务器不但需要有卓越的服务性能，同样网络接口也非常重要，即确保服务器不能失去网络连接而使得服务发生中断。目前中高档服务器一般都配置有 2 块或 4 块千兆以太网网卡，如图 3-7 所示。



服务器网卡　　服务器网络千兆以太网接口

图 3-7　服务器网络接口

业界一些网络硬件厂商都推出了各自的具有容错功能的服务器网卡。例如 Intel 推出了三种容错服务器网卡，它们分别采用了 Adapter Fault olerance（AFT，网卡出错冗余）、A-

dapter Load Balancing（ALB，网卡负载平衡）、Fast Ether Channel（FEC，快速以太网通道）技术。

（1）AFT 技术

AFT 是在服务器和交换机之间建立冗余连接，即在服务器上安装两块网卡，一块为主网卡，另一块作为备用网卡，然后用两根网线将两块网卡都连到交换机上。在服务器和交换机之间建立主连接和备用连接。一旦主连接因为数据线损坏或网络传输中断连接失败，备用连接会在几秒钟内自动顶替主连接的工作，通常网络用户不会觉察到任何变化。这样一来就避免了因一条线路发生故障而造成整个网络瘫痪，可以极大地提高网络的安全性和可靠性。

（2）ALB 技术

ALB 是让服务器能够更多更快地传输数据的一种简单易行的技术。这项新技术是通过在多块网卡之间平衡数据流量的方法来增加吞吐量，每增加一块网卡，就增宽 100Mbit/s 或 1000Mbit/s 通道。另外，ALB 还具有 AFT 同样的容错功能，一旦其中一条链路失效，其他链路仍可保障网络的连接。当服务器网卡成为网络瓶颈时，ALB 技术无须划分网段，网络管理员只需在服务器上安装两块具有 ALB 功能的网卡，并把它们配置成 ALB 状态，便可迅速、简便地解决瓶颈问题。

（3）FEC 技术

FEC 是思科（Cisco）公司针对 Web 浏览及 Intranet 等对吞吐量要求较大的应用而开发的一种增大带宽的技术。FEC 同时也为进行重要应用的客户/服务器网络提供高可靠性和高速度。

3.2.3 服务器主要性能指标

用户总希望有一种简单、高效的度量标准，来量化评价服务器系统，以便作为选型的依据。但实际上，服务器的系统性能很难用一两种指标来衡量。比如 CPU 是衡量服务器性能最重要的指标之一，但是没有其他硬件的支撑并不能提升服务器的整体性能。服务器从硬件设计到管理软件上是一个非常复杂的过程，应从主板、CPU、芯片组、内存、磁盘系统、网络等各方面硬件进行综合考虑，提升服务器的全面性能。

表 3-1 列举了一些常见的服务器性能参数。在实际的服务器选型中，要结合应用需求，选择性价比较高的服务器，也可以很好地保护投资。

表 3-1 常见服务器性能参数表

指标项	参数	
服务器外形	塔式/机架式/刀片式/机柜式，1U/2U/3U/4U/5U 等高度	
处理器	CPU 类型	Intel \ AMD \ 自主研发 CPU
	CPU 数量	标配数量，最大可装配数量
	CPU 核心	双核/四核/六核/八核等多核运算
	缓存	二级缓存、三级缓存大小
	CPU 标称主频	2GHz/2.13GHz/2.66GHz 等不同主频
主板	主板芯片组	是否支持双路以上的 CPU 架构、支持 DDR3
	扩展槽	可扩展槽的数量

（续）

指标项	参　数	
内存	内存类型	DDR2/DDR3，是否支持 ECC
	内存大小	标配数量，内存插槽数、内存最大数量
内部存储	硬盘大小	标配硬盘数量、大小
	硬盘类型	是否支持热插拔，SATA/SAS
	硬盘阵列	支持 RAID0、1、5 等情况
	存储扩展位	4 个托架或 8 个托架或更多
电源	电源类型	标准电源/大功率冗余电源
	电源数量	单电源/双电源/四电源
	电源功率	瓦数
散热	散热风扇	是否支持热插拔、配置冗余风扇数量
网络接口	千兆位网络接口	千兆位网络接口数量
其他接口	PCI 扩展槽	PCI-E 插槽数量
	I/O 接口	USB 接口、SD 插槽、RJ-45 接口、D-SUB 接口、串行接口等数量
软件系统	是否随机附带相关管理软件	

3.3　服务器分类

服务器分类的标准有很多，比如按照应用级别分类，可以分为工作组级、部门级和企业级服务器；按照处理器个数分类，可以分为单路、双路和多路服务器；按照处理器架构分类，可以分为 RISC 构架和 CISC 架构服务器；按照服务器的外形结构分类，可以分为塔式服务器、机架式服务器和刀片服务器。最常见也最直观的分类方式就是通过服务器的外形结构进行分类和按服务器的用途进行分类。

3.3.1　按服务器的外形结构分类

从服务器外形结构上划分，一般可以分为塔式服务器、机架式服务器、刀片服务器等几种类型，也是日常使用中人们最为直观和形象的一种划分方法。

1. 塔式服务器

塔式服务器是目前应用最为广泛、最为常见的一种服务器。塔式服务器在外观上就像一台体积比较大的 PC，由于服务器的主板扩展性强、板卡插槽也比普通 PC 多、主机机箱也比标准的 ATX 机箱要大，一般都会预留足够的内部空间以便日后进行硬盘和电源的冗余扩展。因此塔式服务器一般比普通 PC 体积大一些。

我们平时常说的通用服务器一般都是塔式服务器，它可以集多种常见的服务应用于一身，不管是速度应用还是存储应用都可以使用塔式服务器。塔式服务器的机箱比较大，服务器的配置也可以很高，可以配置多个处理器、多条内存和多块硬盘，还可以配置多个冗余电

源和散热风扇，支持冗余扩展，所以它的应用范围非常广，应该说目前使用率最高的一种服务器就是塔式服务器，如图 3-8 所示。

图 3-8　IBM 塔式服务器

因为塔式服务器机箱大，一台服务器的扩展升级也会有个限度，而且塔式服务器需要占用很大的空间，不利于服务器的托管，所以在需要服务器密集型部署，实现多机协作的领域，塔式服务器并不占优势。特别是服务器部署较为密集的数据中心，塔式服务器需要占用更多的空间，并且不利于摆放，因此使用并不多。

2. 机架式服务器

机架式服务器指的是可以直接安装在机架上的服务器。机架式服务器在外形上完全不像 PC，它最大的特点是比较“薄”，相比塔式服务器可以节省很大的空间，并且随着技术的不断发展，机架式服务器有着不逊色于塔式服务器的性能。机架式服务器是一种平衡了性能和空间占用的解决方案，如图 3-9 所示。

图 3-9　1U、2U、4U 机架式服务器

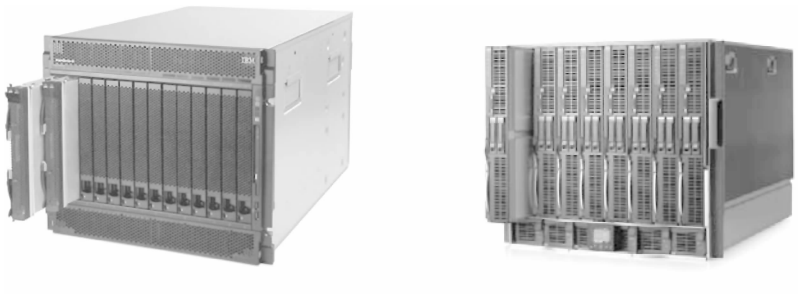
一般来说，不是每一个企业都有建设数据中心机房的条件，而服务器的运行需要有 UPS、精密空调等环境，大部分企业都选择了服务器托管的方式。因此，选择服务器时必须要考虑服务器的体积、功耗、发热量等物理参数，特别是在需要部署很多台服务器时，更是不得不考虑塔式服务器空间占用过大的局限性。

机架式服务器可以统一的安装在按照国际标准设计的机柜中，机柜的宽度为 19in（1in =0.0254m），机柜的高度以 U 为单位，1U 是一个基本高度单元，1U = 1.75in，约 44.5mm 高。机柜的高度有多种规格，如 10U、24U、32U、37U、42U 等，一般服务器标准机柜为 42U 机柜，尺寸为 600mm（宽）×800mm（深）×1990mm（高），根据需求还可以定制。通过机柜安装服务器可以使管理、布线更为方便整洁，也可以方便和其他网络设备的连接。

由于机箱空间有限，机架式服务器也能像塔式服务器那样配置非常均衡，可以集多种应用于一身，所以机架式服务器还是比较适用于一些针对性比较强的应用，如需要密集型部署的服务运营商、群集计算等。

3. 刀片服务器

刀片式结构是一种比机架式更为紧凑整合的服务器结构。它是专门为特殊行业和高密度计算环境设计的。刀片服务器在外形上比机架式服务器更小，只有机架式服务器的 1/3 ~ 1/2，这样就可以使服务器密度更加集中，更大的节省了空间。每个刀片就是一台独立的服务器，具有独立的 CPU、内存、I/O 总线，通过外置磁盘可以独立的安装操作系统，可以提供不同的网络服务，相互之间并不影响。刀片服务器也可以像机架服务器那样，安装到刀片服务器机柜中，形成一个刀片服务器系统，可以实现更为密集的计算部署。多个刀片服务器可以通过刀片架进行连接，通过系统软件，可以组成一个服务器集群，可以提供高速的网络服务，实现资源共享，为特定的用户群服务。如果需要升级，可以在集群中插入新的刀片，刀片可以进行热插拔，升级非常方便。图 3-10 展示了 IBM 公司和 HP 公司推出的刀片服务器。



IBM BladeCenter H 刀片服务器　　HP ProLiant 刀片服务器

图 3-10　刀片服务器

每个刀片服务器不需要单独的电源等部件，可以共享服务器资源，这样可以有效降低功耗，并节省成本。刀片服务器不需要对每个服务器单独进行布线，可以通过机柜统一进行布线和集中管理，这样为连接管理提供了非常大的方便，可以有效节省企业总体拥有成本。刀片服务器在空间节省、集群计算、扩展升级、集中管理、总体成本方面相对于另外两种结构的服务器具有很大优势。

3.3.2　按应用层次分类

按应用层次划分也是常用的划分服务器类别的方法，即根据整个服务器的综合性能，特别是所采用的一些服务器专用技术来衡量和划分。按这种划分方法，服务器可分为：入门级服务器、工作组级服务器、部门级服务器、企业级服务器。

1. 入门级服务器

入门级服务器是指最低档的服务器，硬件配置较低，价格低廉，但也具有服务器的一般特性。入门级服务器类似于高档 PC，经常见到的入门级服务器就是一般的 PC 服务器。入门级服务器通常配置一颗或两颗 CPU，并根据需要配置相应的内存（如 256MB、512MB、1GB

或2GB不等）和大容量IDE或SATA硬盘，如图3-11列举了两款性价比较高的入门级服务器产品。

入门级服务器主要应用于比较简单的应用，如安装Linux/Windows 2003 Server操作系统，提供面向中小型网络用户的文件共享、打印服务、数据处理、Internet接入及简单数据库应用的需求，也可以安装一些简单的网络应用软件。

IBM System x3100 M3

服务器类型：塔式服务器

服务器级别：入门级

CPU类型：Intel Xeon X3450

标称主频：2.66GHz

内存容量：2GB(1×2GB)

标配硬盘容量：500GB

标配硬盘类型：SATA

联想万全T100 G10

服务器类型：塔式

服务器级别：入门级

CPU类型：Intel 奔腾E5500

标称主频：2.8GHz

内存容量：1GB

标配硬盘容量：500GB

标配硬盘类型：SATA

图3-11　入门级服务器

2. 工作组级服务器

工作组（WorkGroup）级服务器是一个比入门级服务器硬件配置稍微高一些的服务器，但仍属于低档服务器。随着服务器硬件技术的发展，入门级服务器和工作组级服务器的性能差别逐渐变小。工作组级服务器一般支持一颗或两颗CPU，可支持大容量的ECC（一种内存技术，多用于服务器内存）内存，采用SCSI（一种总线接口技术）总线的I/O（输入/输出）系统，SMP对称多处理器结构、可选装RAID、热插拔硬盘、热插拔电源等，具备了小型服务器所必备的各种特性。

工作组级服务器一般只能连接规模在50台左右的客户端PC构成的网络。适合于较小网络规模的组网，服务器的性能要求也不高，如作为中小企业Web、Mail等服务器，也能用于中小学构建数字校园网、多媒体教室等。

3. 部门级服务器

部门级的应用对服务器产品在计算效率、存储容量、I/O数据吞吐、散热稳定性等方面有着严格的要求。部门级服务器是指一般中档服务器，一般都是支持双CPU以上的对称处理器结构，具备比较完全的硬件配置，如磁盘阵列、存储托架等，并且集成了大量的监测及

管理电路，具有全面的服务器管理能力，可监测如温度、电压、风扇、机箱等状态参数，在性能、内存、超大存储空间和 I/O 吞吐能力等方面具有较高性价比。此外，结合服务器管理软件，可以使管理人员及时了解服务器的工作状况。同时，大多数部门级服务器具有优良的系统扩展性，能够满足用户在业务量迅速增大时能够及时在线升级系统，充分保护了用户的投资。

部门级服务器主要适合百台或更多客户机的网络环境，为了满足企业对数据和实时性的要求，部门级服务器主要用于一些对应用要求较高配置、数据存储和处理稳定性要求较高的行业用户和服务提供商。如图 3-12 所示，列举了两款部门级服务器。

IBM System X3850 M2

服务器类型：机架式

服务器级别：部门级

CPU类型：Intel Xeon E7420 (四核)

标称主频：2.13GHz

内存容量：4GB(4×1GB)

标配硬盘容量：146GB

标配硬盘类型：SAS

电源类型：热插拔冗余电源

存储扩展位：4×托架

曙光天阔 I620r-G

服务器类型：机架式

服务器级别：部门级

CPU类型：Intel Xeon E5506 (四核)

标称主频：2.13GHz

内存容量：2GB

标配硬盘容量：146GB

标配硬盘类型：SAS

电源类型：单电源

存储扩展位：8×托架

图 3-12　部门级服务器

4. 企业级服务器

企业级服务器属于高档服务器，最显著的特点是企业级服务器普遍可支持 4 ~ 8 个处理器甚至更多。企业级服务器在硬件设计和配置上有更为独特的地方，一般拥有独立的双 PCI 通道和内存扩展板设计，具有高内存带宽、大容量热插拔硬盘和热插拔电源；具有超强的数据处理能力、高度的容错能力、优异的扩展性能、系统性能和群集性能；能满足极长时间的系统连续运行，能在很大程度上保护用户的投资。

企业级服务器的硬件配置最高，系统可靠性也最强。企业级服务器用于联网计算机在数百台甚至千台以上、对处理速度和数据安全要求非常高的大型网络，所采用的操作系统一般也是 Unix（Solaris）或 Linux。

目前，企业级服务器主要适用于需要处理大量数据、高处理速度和对可靠性要求极高的大型企业和重要行业（如金融、证券、交通、邮电、通信等行业）。图 3-13 给出了两款企业级服务器的产品。

惠普 ProLiant DL580 G7

服务器类型：机架式

服务器级别：企业级

CPU类型：Intel Xeon X7560 (八核)

CPU数量：4颗

标称主频：2.266GHz

内存容量：32GB(8×4GB)，64个插座，最高1TB

标配硬盘类型：SAS

电源数量：4个

电源类型：热插拔冗余电源

散热系统：4个热插拔 3+1冗余系统风

存储扩展位：标配8×SFF托架

网络控制器：4×千兆接口

曙光天阔 A950r-F

服务器类型：机架式

服务器级别：企业级

CPU类型：AMD Operton 8350 (四核)

CPU数量：8颗

标称主频：2GHz

内存容量：16GB(8×2GB)，可扩展至256GB

标配硬盘容量：146GB

电源数量：1个

电源类型：大功率冗余电源

散热系统：曙光灵动散热系统

存储扩展位：共有8个热插拔硬盘位

网络控制器：3×千兆接口

图 3-13　企业级服务器

3.3.3　按服务器的处理器类型分类

1. RISC 服务器

RISC 服务器即非 x86 服务器，包括大型机、小型机和 Unix 服务器。RISC 服务器使用 RISC（精简指令集）或 EPIC（并行指令代码）处理器，并且主要采用 Unix 或其他专用操作系统的服务器。精简指令集处理器主要有 IBM 公司的 POWER 和 PowerPC 处理器，SUN 与富士通公司合作研发的 SPARC 处理器。EPIC 处理器主要是 HP 与 Intel 合作研发的安腾处理器等。这种服务器价格昂贵，体系封闭，但是稳定性好，性能强，主要用在金融、电信等大型企业的核心系统中。

在服务器产品中，RISC 服务器主要由几个知名的计算机公司如 SUN、IBM、HP 等的 RISC UNIX 结构的产品所控制，它们的服务器一般采用 Unix、Solaris、AIX 等，被广泛用于数据库服务器、Internet 服务器等各种服务器。这些服务器 CPU 如下：

1）SUN 公司：SUN 公司的处理器为 UltraSPARC，以此处理器形成了品种齐全的服务器产品，包括 SPARCserver 系列、SPARCcenter 系列、SPARCcluster 系列、Netra Internet 系列、New Sun Fire、Sun Enterprise 等。操作系统为 Solaris。

2）IBM 公司：IBM 公司的处理器为 PowerPC，以此处理器形成了品种齐全的服务器产

品，如 RS/6000 系列，操作系统为 AIX。

3）HP 公司：HP 公司的 RISC 处理器为 HP-PA，操作系统为 HP UNIX，以及收购 Compaq 公司后拥有的 RISC 处理器 Alpha，操作系统为 Digital UNIX 和 Windows NT。

2. CISC 服务器

CISC（复杂指令集）服务器，即 x86 服务器，它是基于 PC 体系结构，使用 Intel 或其他兼容 x86 指令集的处理器芯片和 Windows 操作系统的服务器，如 IBM 的 System x 系列服务器、HP 的 Proliant 系列服务器等。相对 RISC 服务器，价格便宜、兼容性好、稳定性和安全性差，主要用在中小企业和非关键业务中，例如中小型局域网的文件或数据库服务器。

3.3.4　按服务器的用途分类

服务器一般都是通用的，这类服务器可以全面提供各种基本服务功能。当前大多数服务器是通用型服务器。因为这类服务器不是专为某一功能而设计，在设计时兼顾多方面的应用需求。但是针对一些特殊的应用需求，市场上出现了一些为了满足各种特定功能而开发、生产的功能型服务器。如果按照这种划分标准，可以分为通用型服务器和专用型服务器。所谓专用型服务器，就是专门为某一种或某几种功能专门设计的服务器。

1. 面向计算类的服务器

这类服务器面向科学计算、数学模型分析等，要求具有很高的 CPU 计算能力。这类服务器一般采用多 CPU 技术，支持对称多处理与非对称多处理技术；对内存容量要求很高；需要较高的高速缓冲技术；具有强大的浮点运算能力。

这类服务器，一般采用大型机（巨型机）或高档工作站。典型应用如气象部门天气预报的计算、大型的统计预测等。

2. 面向数据库的服务器

这类服务器面向数据库服务，作为专门安装数据库管理系统（DBMS）的服务器，如 SQL Server、Oracle、DB2。这类服务器一般要求有较好的并行处理能力；高速的 I/O 吞吐量，具体体现在磁盘（硬盘）的读写速率和高速的网络适配器上；具有较大的磁盘容量，可以配置磁盘阵列；配置数据备份设备，如磁带机，配置备份策略；如果是分布数据库计算模式，要求有较高的网络带宽。

这类服务器，一般采用专用服务器设备，企业或部门级服务器，也可采用高档工作站。典型应用如银行中心数据库服务器、电信计费服务器、企业信息系统数据库服务器或数据仓库服务器。

3. 面向应用系统的服务器

这类服务器是企业使用的应用系统服务器，一般运行着各种企业应用系统，属于客户机/服务器（Client/Server）或浏览器/服务器（Browser/Server）的网络应用。这类服务器一般要求有较好的并行与异步处理能力、较高的网络带宽、高速的 I/O 吞吐量、较高的稳定性。

4. 面向通信与网络系统的服务器

这类服务器面向通信和网络服务，这类服务器一般具有实时性要求，具有处理延时较短、较高的并行与异步处理能力；具有高速的 I/O 吞吐量；具有较大的磁盘容量，可以配置磁盘阵列；配置数据备份设备，如磁带机，配置备份策略；具有较高的安全性和较高的网络带宽。

一般这类服务器采用专用服务器设备，或采用高档工作站。典型应用如 Web 服务器、大型电子邮件服务器。

5. 面向多媒体与视像会议的服务器

这类服务器面向多媒体通信或多媒体网络服务。这类服务器一般具有大容量磁盘存储器，可以配置磁盘阵列；具有较高的视像实时性要求，处理延时短；具有高速的 I/O 吞吐量，具体体现在磁盘（硬盘）的读写速率和高速的网络适配器上。

一般这类服务器采用专用服务器设备，或采用高档工作站。典型应用如视像会议系统、VOD 系统等。

6. 面向可视化与虚拟现实应用的服务器

这类服务器面向多媒体，特别是图像处理业务。这类服务器一般具有高档 CPU 或多 CPU 技术，支持对称多处理与非对称多处理技术，对内存容量要求很高；需要较高的高速缓冲技术；具有强大的浮点运算能力和较高的并行处理能力；具有高级图形处理能力的显示适配器；具有高分辨率的显示器。

一般这类服务器采用专用工作站来实现。典型应用如图像处理系统。

3.4 服务器系统的主要技术

3.4.1 服务器的基本技术

1. 热插拔技术

热插拔（Hot-Plugging 或 Hot Swap）即带电插拔，是指允许用户在不关闭系统停止服务和不切断电源的情况下更换或添加服务器部件，如取出和更换损坏的硬盘、电源或可扩展板卡等部件，从而提高了系统对灾难的及时恢复能力、扩展性和灵活性等。

热插拔技术支持服务器的可靠性，服务器系统主要出现故障的配件不再仅是硬盘，有可能是内存、电源和风扇等；有的甚至支持 CPU 和服务器本身热插拔，特别在高端多路处理器服务器系统和群集服务器系统中。现在，热插拔技术在确保服务器系统可用性方面已显得越来越重要了，已成为服务器的标准技术。尽管不同档次的服务器所支持的热插拔配件并不完全一样，但对于像硬盘、电源和风扇的热插拔技术支持已成为最基本的服务器技术配置。

2. RAID 技术

RAID（Redundant Array of Independent Disk，独立冗余磁盘阵列）技术是应用最广的服务器技术之一。RAID 就是将 N 台硬盘通过 RAID 控制器（分硬件和软件）结合成虚拟单台大容量的硬盘使用。通过把多块独立的硬盘（物理硬盘）按不同的方式组合起来形成一个硬盘组（逻辑硬盘），从而提供比单个硬盘更高的存储性能和提供数据备份技术。组成磁盘阵列的不同方式称为 RAID 级别，RAID 技术主要包含 RAID 0 ~ RAID 7 等数个级别，它们的侧重点各不相同，每个级别都有各自的优缺点。目前应用较多的有 RAID0、RAID1、RAID0 +1 和 RAID5。

（1）RAID 0

RAID 0 连续以位或字节为单位分割数据，并行读/写于多个磁盘上，因此具有很高的数据传输率，但它没有数据冗余，因此并不能算是真正的 RAID 结构。RAID 0 只是单纯地提

高性能，并没有为数据的可靠性提供保证，而且其中的一个磁盘失效将影响到所有数据。因此，RAID 0 不能应用于数据安全性要求高的场合。

（2）RAID 1

它是通过磁盘数据镜像实现数据冗余，在成对的独立磁盘上产生互为备份的数据。当原始数据繁忙时，可直接从镜像复制中读取数据，因此 RAID 1 可以提高读取性能。RAID 1 是磁盘阵列中单位成本最高的，但提供了很高的数据安全性和可用性。当一个磁盘失效时，系统可以自动切换到镜像磁盘上读写，而不需要重组失效的数据。

（3）RAID 0 + 1

也被称为 RAID 10 标准，实际是将 RAID 0 和 RAID 1 标准结合的产物，在连续地以位或字节为单位分割数据并且并行读/写多个磁盘的同时，为每一块磁盘作磁盘镜像进行冗余。它的优点是同时拥有 RAID 0 的超凡速度和 RAID 1 的数据高可靠性，但是 CPU 占用率同样也更高，而且磁盘的利用率比较低。

（4）RAID 2

将数据条块化地分布于不同的硬盘上，条块单位为位或字节，并使用称为“加重平均纠错码（海明码）”的编码技术来提供错误检查及恢复。这种编码技术需要多个磁盘存放检查及恢复信息，使得 RAID 2 技术实施更复杂，因此在商业环境中很少使用。

（5）RAID 3

它同 RAID 2 非常类似，都是将数据条块化分布于不同的硬盘上，区别在于 RAID 3 使用简单的奇偶校验，并用单块磁盘存放奇偶校验信息。如果一块磁盘失效，奇偶盘及其他数据盘可以重新产生数据；如果奇偶盘失效则不影响数据使用。RAID 3 对于大量的连续数据可提供很好的传输率，但对于随机数据来说，奇偶盘会成为写操作的瓶颈。

（6）RAID 4

RAID 4 同样也将数据条块化并分布于不同的磁盘上，但条块单位为块或记录。RAID 4 使用一块磁盘作为奇偶校验盘，每次写操作都需要访问奇偶盘，这时奇偶校验盘会成为写操作的瓶颈，因此 RAID 4 在商业环境中也很少使用。

（7）RAID 5

RAID 5 不单独指定奇偶盘，而是在所有磁盘上交叉地存取数据及奇偶校验信息。在 RAID 5 上，读/写指针可同时对阵列设备进行操作，提供了更高的数据流量。RAID 5 更适合于小数据块和随机读写的数据。RAID 3 与 RAID 5 相比，最主要的区别在于 RAID 3 每进行一次数据传输就需涉及所有的阵列盘；而对于 RAID 5 来说，大部分数据传输只对一块磁盘操作，并可进行并行操作。在 RAID 5 中有“写损失”，即每一次写操作将产生 4 个实际的读/写操作，其中两次读旧的数据及奇偶信息，两次写新的数据及奇偶信息。RAID 4 在商业环境中使用较广。

（8）RAID 6

与 RAID 5 相比，RAID 6 增加了第二个独立的奇偶校验信息块。两个独立的奇偶系统使用不同的算法，数据的可靠性非常高，即使两块磁盘同时失效也不会影响数据的使用。但 RAID 6 需要分配给奇偶校验信息更大的磁盘空间，相对于 RAID 5 有更大的“写损失”，因此“写性能”非常差。较差的性能和复杂的实施方式使得 RAID 6 很少得到实际应用。

（9）RAID 7

这是一种新的 RAID 标准，其自身带有智能化实时操作系统和用于存储管理的软件工具，可完全独立于主机运行，不占用主机 CPU 资源。RAID 7 可以看作是一种存储计算机（Storage Computer），它与其他 RAID 标准有明显区别。

在实际应用中，可以如 RAID 0 + 1 那样结合多种 RAID 规范来构建所需的 RAID 阵列，例如 RAID 5 + 3（RAID 53）就是一种应用较为广泛的阵列形式。用户一般可以通过灵活配置磁盘阵列来获得更加符合其要求的磁盘存储系统。

3. 对称多处理器技术

对称多处理器（Symmetrical Multi-Processing，SMP）技术是指在一个服务器上汇集了一组处理器，即多个 CPU，各 CPU 之间共享内存子系统以及总线结构。它是相对非对称多处理技术而言的一种并行技术，被广泛应用在中、高档服务器上。

在 SMP 架构中，一台服务器不再由单个 CPU 组成，而是同时由多个处理器运行操作系统的单一复本，并共享内存和一台服务器的其他资源。虽然同时使用多个 CPU，但是从管理的角度来看，它们的表现就像一台服务器一样。系统将任务队列对称地分布于多个 CPU 之上，从而极大地提高了整个系统的数据处理能力。所有的处理器都可以平等地访问内存、I/O 和外部中断。在 SMP 系统中，系统资源被系统中所有 CPU 共享，工作负载能够均匀地分配到所有可用处理器上。

3.4.2 服务器的群集与容错技术

1. 群集技术

服务器群集技术是把多个物理服务器通过输入/输出系统互联在一起，这些服务器连接到存储介质中，形成一个整体，分布式地工作，并且由分布资源管理软件进行管理，因而可以更好地利用设备资源的一项新兴技术，近年来得到了广泛的应用。群集技术可以提高特定应用程序或者服务的可用性，也可以提高应用程序的性能，为特定的应用程序或者问题提供强大的处理能力。一旦在服务器上安装并运行了群集服务，该服务器即可加入群集。群集化操作可以减少单点故障数量，并且实现了群集化资源的高可用性。

服务器群集技术最主要的应用即在于网络负载的平衡。网络负载平衡使用两台或更多台一起工作的主机计算机组成的群集，为服务器提供了高可用性和高伸缩性。Internet 客户端使用一个 IP 地址或一组地址访问群集。客户端无法区别群集和单一服务器。服务器应用程序并不表明它们是在群集上运行的。但是，网络负载平衡群集与运行单个服务器应用程序的单个主机有很大的区别，因为即使在某个群集主机发生故障的情况下，它也可以提供不间断服务。群集对客户端请求的响应也比单个主机快。

如图 3-14 所示是由 2 台服务器（Server1，Server2）组成的群集方式，其中每台服务器的地位是平等的，都可以为客户端提供服务并且不用其他服务器的辅助。图中 Server3 是服务器群集虚拟出来的主机，客户端所能看到的群集只是一台 Server3 主机，并不需要知道其他服务器的存在。群集中的主机将均衡处理客户端发来的应用请求，以此来实现负载均衡；如果某一台服务器出现宕机，客户端发来的应用请求将被分配给另外一台服务器，通过这种方式来保障业务应用的高可用性。

常用的服务器操作系统如 Unix/Linux、Windows 2000 Server、Windows Server 2003/2008 都有关于服务器群集的实用工具，用来支持在服务器上安装群集软件或创建新群集。

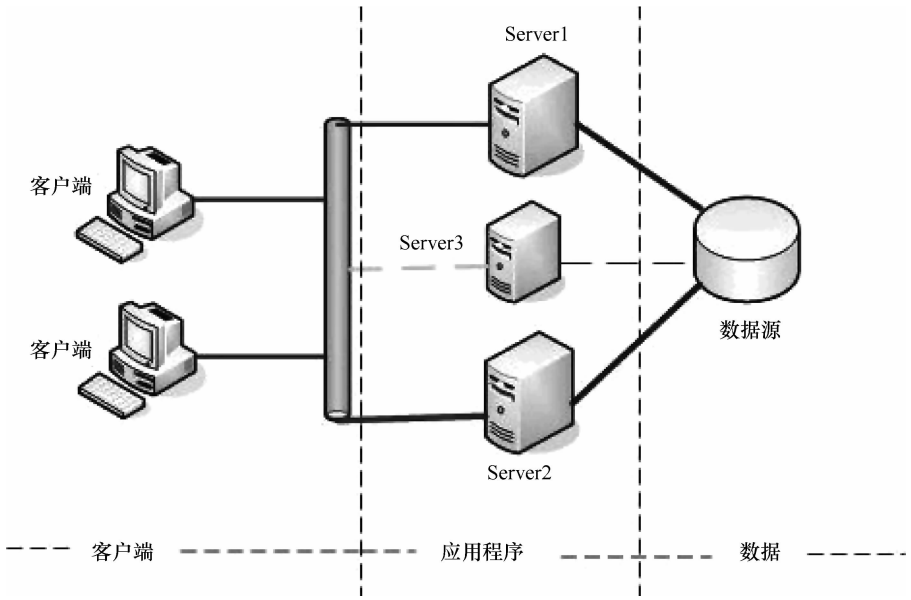


图 3-14　服务器集群

2. 容错技术

尽管服务器的硬件性能越来越高，但是对一些具有特殊应用的行业如证券、银行、电信等需要提供永不间断的服务，发生故障也是难免的。世界上各大服务器厂商都试图通过一种名为容错的技术来解决这种问题，以提供关键服务器和关键应用的高可用性、安全性、稳定性、高管理性及其不间断运行，以便能够很好地满足一些重要行业的应用需求。

容错（Fault Tolerance）是指系统发生错误但能容忍错误而不导致服务中断。对于服务器来说，容错是指服务器对于错误的容纳能力，是应用过程中对于服务器稳定性的一个更高的要求。

当前，服务器容错技术主要有服务器群集技术、双机热备份技术和单机容错技术。实际上，服务器群集和双机热备份技术比较类似，双机热备份可以看作是最简单的集群；也可以把服务器集群技术视为双机冗余的延伸，可以理解为一种多机容错的方案。采用集群技术，通过多台服务器之间的负载均衡，可以解决服务器单点故障所引发的系统不稳定，提高系统的可靠性，因此集群具有更好的容错能力。双机热备份技术也是一种软硬件结合的较高容错应用方案。

单机容错技术是在一台服务器上实现容错能力，这是一种最高级别的容错技术。具有单机容错能力的服务器被称为容错服务器，这种服务器也是各大厂家追逐研究的前沿性产品。单机容错技术以 Stratus 公司的 ftServer、惠普公司的 NonStop 服务器和 NEC 公司的 Express5800/ft 为代表。这种技术具有比双机热备方案更高的容错能力。有研究报告指出，双机热备方案的可靠性可以达到 99.9%，而单机容错技术的可靠性可以达到 99.999% 甚至更高。

3. 双机热备份技术

服务器的故障可能由各种原因引起，如设备故障、操作系统故障、软件系统故障等。对于一些重要系统而言，如果发生服务器故障而造成中断，会造成重大的经济损失。因此，在实际应用中对于一些重要、关键的业务系统需要通过双机热备份来避免可能因发生故障而导致的长时间服务中断，保证系统长期、可靠的运行。

双机热备份技术是一种软硬件结合的较高容错应用方案。一般由两台服务器系统和一个外接共享磁盘阵列柜及相应的双机热备份软件组成，如图 3-15 所示。

在该方案中，将操作系统和应用程序安装部署在两台服务器的本地系统盘上，整个网络系统的数据是通过磁盘阵列集中管理和数据备份的。数据集中管理是通过双机热备份系统，将所有站点的数据直接从中央存储设备读取和存储，并由专业人员进行管理，极大地提高了数据的安全性和保密性。用户的数据存放在外接共享磁盘阵列中，在一台服务器出现故障时，备机主动替代主机工作，保证网络服务不间断。

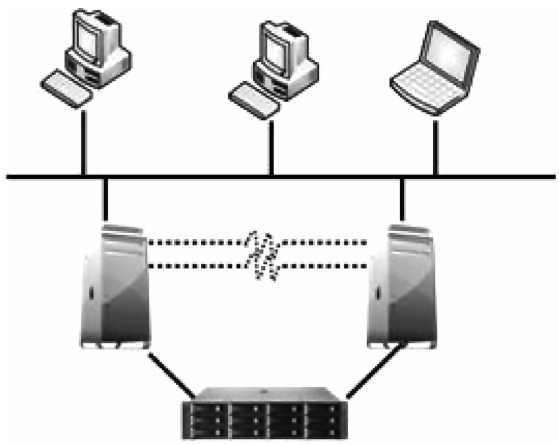


图 3-15　双机热备份方案

双机热备份系统采用“心跳”方法保证主系统与备用系统的联系。所谓“心跳”，指的是主从系统之间相互按照一定的时间间隔发送通信信号，表明各自系统当前的运行状态。一旦“心跳”信号停止表明主机系统发生故障，或者备用系统无法收到主机系统的“心跳”信号，则系统的高可用性管理软件认为主机系统发生故障，主机停止工作，并将系统资源转移到备用系统上，备用系统将替代主机发挥作用，以保证网络服务运行不间断。

双机热备份方案中，最常用的两种热备模式是双机热备模式和双机互备模式。双机互备模式（Active/Standby，激活/停机模式）即一主一备模式，指的是一台服务器处于某种业务的激活状态（即 Active 状态），另一台服务器处于该业务的备用状态（即 Standby 状态）。而双机互备模式（双主机方式）即指两种不同业务分别在两台服务器上互为主备状态（即 Active-Standby 和 Standby-Active 状态）。

3.4.3　服务器的负载均衡技术

由于目前现有网络的各个核心部分随着业务量的提高，特别是面向互联网服务的业务，如在线购物系统、在线订票系统等系统访问量和数据流量的快速增长，其处理能力和计算强度也相应地增大，使得单一的服务器设备根本无法承担。在此情况下，如果扔掉现有设备去做大量的硬件升级，这样将造成现有资源的浪费，而且如果再面临下一次业务量的提升时，这又将导致再一次硬件升级的高额成本投入，甚至性能再卓越的设备也不能满足当前业务量增长的需求。

一台普通服务器的处理能力只能达到每秒几万个到几十万个请求，无法在 1s 内处理上

百万个甚至更多的请求。但若能将多台这样的服务器组成一个系统，并通过软件技术将所有请求平均分配给所有服务器，那么这个系统就完全拥有每秒钟处理几百万个甚至更多请求的能力。这就是负载均衡（Load Balance）最初的基本设计思想。

负载均衡是由多台服务器以对称的方式组成一个服务器集合，每台服务器都具有平等的地位，都可以单独对外提供服务而无须其他服务器的辅助。通过某种负载分担技术，将外部发送来的请求均匀分配到对称结构中的某一台服务器上，而接收到请求的服务器独立地回应客户的请求。均衡负载能够平均分配客户请求到服务器阵列，借此快速获取重要数据，解决大量并发访问服务问题。这种群集技术可以用最少的投资获得接近于大型主机的性能。

负载均衡设备不是基础网络设备，而是一种性能优化设备。对于网络应用而言，并不是一开始就需要负载均衡，当网络应用的访问量不断增长，单个处理单元无法满足负载需求时，网络应用流量将要出现瓶颈时，负载均衡才会起到作用。利用负载均衡技术可以将较大的处理任务进行平衡、分摊到多个操作单元上进行执行，例如 Web 服务器、FTP 服务器、企业关键应用服务器和其他关键任务服务器等，从而共同完成工作任务。负载均衡建立在现有网络结构之上，它提供了一种廉价、有效、透明的方法扩展网络设备和服务器的带宽，增加吞吐量，加强网络数据处理能力，提高网络的灵活性和可用性。

负载均衡有两方面的含义：首先，单个重负载的运算分担到多台节点设备上做并行处理，每个节点设备处理结束后，将结果汇总，返回给用户，系统处理能力得到大幅度提高，这就是我们常说的集群（clustering）技术。第二层含义就是：大量的并发访问或数据流量分担到多台节点设备上分别处理，减少了用户等待响应的时间，这主要针对 Web 服务器、FTP 服务器、企业关键应用服务器等网络应用。

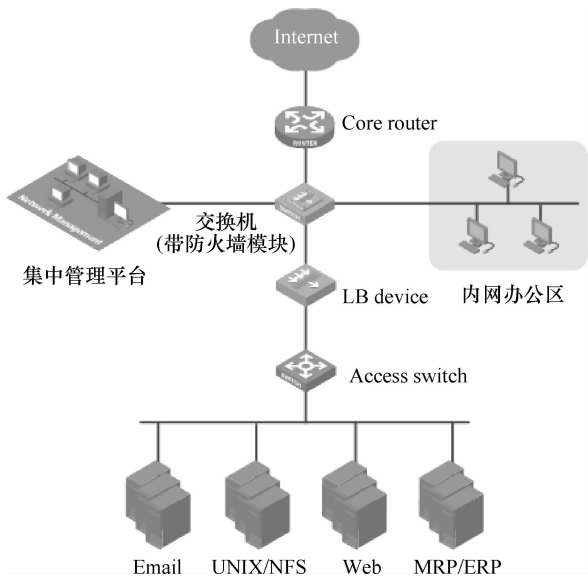


图 3-16　企业园区网的负载均衡应用

服务器负载均衡，顾名思义就是对一组服务器提供负载均衡业务。这一组服务器一般来说都处于同一个局域网络内，并同时对外提供一组（或多组）相同（或相似）的服务。服务器负载均衡是数据中心最常见的组网模型，图 3-16 展示了负载均衡在企业园区网的应用。为了实现对企业资源服务器的快速访问，也需要采用负载均衡设备分担企业数据访问流量。在这种应用环境下，可以将负载均衡设备串接在网络中，服务器通过网络设备连接到负载均衡设备，服务器网关指向负载均衡设备 LB。

3.4.4　服务器虚拟化技术

1. 服务器虚拟化的基本概念

虚拟化技术（Virtual Technology），是指将一台物理的计算机软件环境分割为多个独立

分区，每个分区均可以按照需求模拟出一台完整计算机的技术。模拟出来的计算机称为虚拟机（Virtual Machine，VM）。虚拟化技术的实质是通过中间层次实现计算机资源的管理和再分配，实现资源利用的最大化。虚拟化分区带来的最大好处是使同一物理平台能够同时运行多个同类或不同类型的操作系统，以分别作为不同业务和应用的支撑平台。

服务器虚拟化技术将服务器物理资源抽象成逻辑资源，让一台服务器变成几台甚至上百台相互隔离的虚拟服务器，或者让几台服务器变成一台服务器来用，我们不再受限于物理上的界限，而是让 CPU、内存、磁盘、I/O 等硬件变成可以动态管理的“资源池”，从而提高资源的利用率，简化系统管理，实现服务器整合，让服务器硬件资源对业务的变化更具适应力。简言之，服务器虚拟化就是将一台或几台服务器当作 N 台服务器来使用或把 N 台服务器当作一台服务器来使用，如图 3-17 所示。

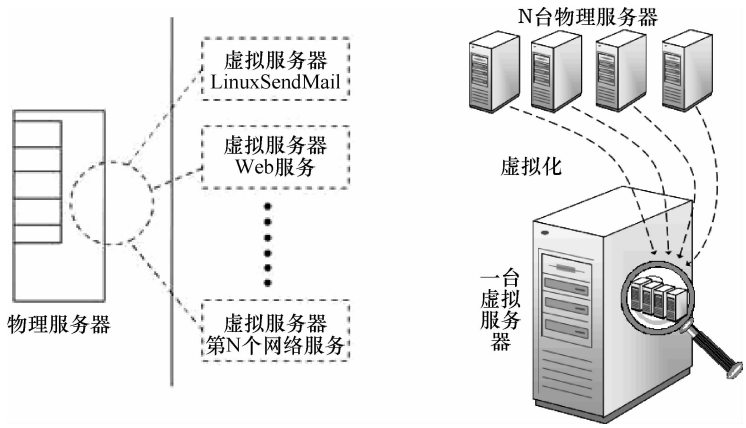


图 3-17　服务器虚拟化

2. 服务器虚拟化的实现技术

实现虚拟化的技术主要有纯软件的虚拟化技术和硬件辅助虚拟化技术两种。前者是当前主流的虚拟化技术，具有成熟的应用，硬件辅助虚拟化技术是今后的发展方向。

（1）软件虚拟化技术

传统的计算机层次结构分为三层，即硬件层（Hardware Layer）、主机操作系统层（Host OS Layer）和应用层（Application Layer）。在这种结构中，主机操作系统统一控制、管理和分配整个计算机的硬件和软件资源，这种结构的缺点主要在于未能充分发挥 CPU 的性能，利用率较低；还有就是一台计算机无法满足同时运行多平台的应用需求，如果对于一种不同的应用程序采用一台独立的物理服务器，解决方案是增加服务器的数量，这无疑将增加投资成本。

服务器虚拟化技术采用纯软件的方法，就是在硬件层之上仍然安装被称为主机操作系统的系统，在其上部署虚拟机软件（Virtual Machine Software，VMS），根据实际应用需求，VMS 可以将物理计算机虚拟出多个分区，每一个分区称为一个虚拟机（Virtual Machine，VM）。虚拟机具有完整的计算机应用环境，包括硬件层（由 VMS 提供）、驱动接口层（由 VMS 提供）、操作系统（Guest OS Layer）及应用层（Applications），都是建立在计算机的应

用环境上，属于用户级软件。这样用户可以“随心所欲”地安装应用程序。实现这种虚拟化技术关键在于虚拟机软件的可靠性。

对于一台独立的物理服务器，在这台服务器上安装操作系统，在操作系统安装相应的应用程序，这种传统架构是一台独立的物理服务器作为一种应用程序服务器使用。服务器虚拟化之后，一台独立物理服务器的资料被虚拟化为若干个独立的主机，这些主机可以单独安装其他的操作系统，在操作系统之上又可以分别安装各种不同的应用程序。其基本原理如图 3-18 所示。

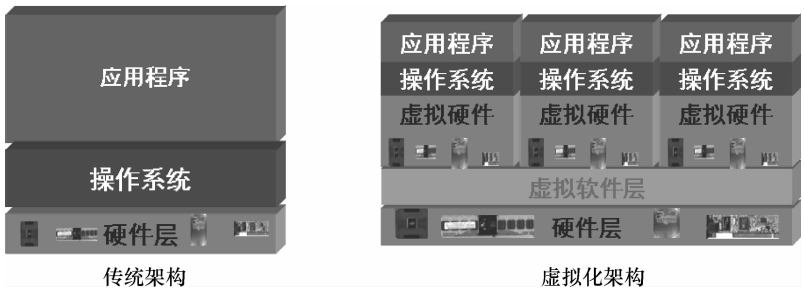


图 3-18　传统架构与虚拟化架构的比较

基于软件虚拟化技术实现的虚拟机软件主要有 VMware 的 Workstation、Microsoft 的 Hyper-V、Parallels 等，这些软件在近年来得到了迅速的推广和应用。

（2）硬件虚拟化技术

硬件辅助虚拟化技术源于 Intel 公布的 Vanderpool 技术，即 VT 技术，该技术对于服务器系统，包括处理器 VT 技术和 IO 虚拟分配技术进行了规范。Intel 和 AMD 公司在最近几年发布的 CPU 产品中都集成了 VT 技术，为进一步推动和发展虚拟化计算环境提供了硬件支持。

3. VMware 虚拟化软件简介

VMware 是一款强大的虚拟机软件。VMware Infrastructure 是一组完整的基础架构虚拟套件，此款集成产品可提供全面的综合虚拟化、管理、资源优化、应用程序可用性和操作自动化功能。VMware Infrastructure 虚拟化并汇总多个系统间的基础物理硬件资源，同时为虚拟环境中的数据中心提供大量虚拟资源。此外，VMware Infrastructure 还提供一组分布式服务，通过该服务，可以实现策略驱动的精细资源分配、高可用性和对整个虚拟数据中心的整合备份。

VMware Infrastructure 3 是 VMware 虚拟机的核心软件，作为虚拟数据中心操作系统，可以将离散的硬件资源统一起来以创建共享动态平台，同时实现应用程序的内置可用性、安全性和可扩展性。为了满足不同组织的需求和预算，VMware Infrastructure 3 将其丰富的功能打包在 3 个版本中：基础版、标准版和企业版。每个版本都包含一个虚拟机管理程序以及一套管理功能。客户可以选择部署 VMware ESX 或 VMware ESXi。VMware ESX Server 是一个在物理服务器上运行的、健壮的、经过生产验证的虚拟化层，它将处理器、内存、存储器和网络资源抽象为多个虚拟机。图 3-19 展示了一个基于 Intel 硬件虚拟化技术与 Vmware 软件虚拟化平台的结合应用案例。

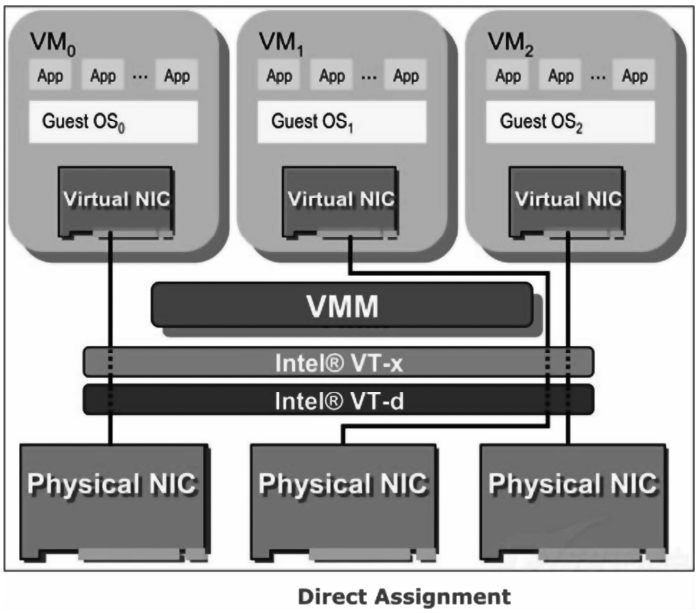


图 3-19　虚拟化应用实例

3.5　网络存储系统

互联网已经走入了寻常百姓家，中国接入互联网的家庭更是数亿计，给人们带来了一个新的信息时代，互联网信息资源呈现出爆炸性增长的态势。大量的信息资源需要存储，单纯依靠服务器的硬盘是远远不够的。另外，如果服务器硬盘坏了，数据丢失了怎么办？那么为保证数据不丢失，这么多数据存储和备份在哪里呢？如学校图书馆的服务器上存放了 20 世纪 80 年代到 2011 年的近 30 年的各种图书资源、视频音像资源、论文资源等，这些数据需要硬盘的空间多达几十 T（1T = 1024G），早先的存储形式是存储设备（通常是磁盘）与应用服务器其他硬件直接安装于同一个机箱之内，并且该存储设备是给本台应用服务器独占使用的。随着服务器数量的增多，磁盘数量也在增加，且分散在不同的服务器上，查看每一个磁盘的运行状况都需要到不同的应用服务器上去查看。更换磁盘也需要拆开服务器，中断应用。于是，一种希望将磁盘从服务器中脱离出来，集中到一起管理的需求出现了。

因此，对大量数据进行有效地存储、管理和使用成为必须解决的问题，对网络信息存储系统的要求也空前提高。网络存储正在得到越来越广泛的应用。目前，存储体系结构的不断发展，使得存储系统在容量、I/O 性能、扩展性、开放性等方面都有了显著的提高和改善。发展一种具有成本效益的和可管理的先进存储方式就成为必然。

3.5.1　网络存储的基本概念

网络存储（Network Storage），就是以局域网或互联网为传输平台，实现数据的传输与存储，数据可以存储在远程的专用存储设备上，也可以存储在本地的存储设备上。

计算机网络技术的发展促进了存储技术的变革，存储技术是全新的存储体系结构，它采

用面向网络的存储体系结构，使数据处理和数据存储分离。网络存储体系结构包括了网络和 I/O 系统的核心技术，将 I/O 的能力扩展到网络上；特别是灵活的网络寻址能力，远距离数据传输能力，I/O 高效的原性能，通过网络连接服务器和存储资源，消除了不同存储设备和服务器之间的连接障碍，提高了数据的共享性、可用性、可扩展性和管理性。

网络存储技术是基于数据存储的一种通用网络术语。网络存储通信中使用到的相关技术和协议包括 SCSI、RAID、iSCSI 以及光纤信道。一直以来，SCSI 支持高速、可靠的数据存储。RAID（独立磁盘冗余阵列）指的是一组标准，提供改进的性能和/或磁盘容错能力。光纤信道是一种提供存储设备相互连接的技术，支持高速通信（将来可以达到 10Gbit/s）。与传统存储技术，如 SCSI 相比，光纤信道也支持较远距离的设备相互连接。iSCSI 技术支持通过 IP 网络实现存储设备间双向的数据传输，其实质是使 SCSI 连接中的数据连续化。通过 iSCSI，网络存储器可以应用于包含 IP 的任何位置。

3.5.2　存储系统相关协议

1. iSCSI

SCSI（Small Computer System Interface，小型计算机系统接口）是一种用于计算机和智能设备之间（硬盘、软驱、光驱、打印机、扫描仪等）系统级接口的独立处理器标准。SCSI 是一种智能的通用接口标准。它是各种计算机与外部设备之间的接口标准，是连接存储设备与服务器的最通用的方法。

iSCSI（Internet Small Computer System Interface，基于因特网的小型计算机系统接口）是一种基于 TCP/IP 的协议，用来建立和管理 IP 存储设备、主机和客户机等之间的相互连接，并创建存储区域网络。存储区域网络使得 SCSI 协议应用于高速数据传输网络成为可能，这种传输以数据块级别在多个数据存储网络间进行。

iSCSI 技术是一种由 IBM 公司研究开发的，是一个供硬件设备使用的可以在 IP 协议的上层运行的 SCSI 指令集。这种指令集可以实现在 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路由选择。iSCSI 技术是一种新储存技术，该技术是将现有 SCSI 接口与以太网络（Ethernet）技术结合，使服务器可与使用 IP 网络的储存设备进行通信。iSCSI 的主要功能是在 TCP/IP 网络上的主机系统（启动器 initiator）和存储设备（目标器 target）之间进行大量数据的封装和可靠传输。此外，iSCSI 提供了在 IP 网络封装 SCSI 命令，且运行在 TCP 上。

支持 iSCSI 技术的服务器和存储设备能够直接连接到现有的 IP 交换机和路由器上，使得存储设备与服务器的连接更加方便，连接距离更长，突破光纤通道存储网络目前 10km 的局限。它利用现有的 TCP/IP 基础设施来构筑存储网络，网络部署成本相对较低；相对其他大多数协议而言：带宽高，功能强（特别是远程复制和灾难恢复），可用性强。

2. FC

FC（Fibre Channel，光纤通道）标准是由美国 T11 标准委员会（美国国家信息技术标准化委员会（NCITS）下属的技术委员会）制定的。定义光纤通道是一种在计算机和海量存储器上广泛应用的高速串行接口。与 SCSI 接口相比，光纤通道兼有 I/O 通道和局域网的特性，光纤通道可以作为 I/O 通道和局域网的传输介质。根据美国国家标准协会（ANSI）的规定，光纤通道支持 IP 协议、SCSI 接口、高性能并行接口（HIPPI）等协议。光纤通道的主要

特性有：热插拔性、高速带宽、远程连接、连接设备数量大等。目前光纤通道用于服务器共享存储设备的连接以及存储控制器和驱动器之间的内部连接，传输率可达到2Gbit/s（将来会达到4Gbit/s）。

3.5.3 存储技术的分类

存储技术主要可以分为直连附加存储、网络附加存储、存储区域网络三类。

1. 直连附加存储

直连附加存储（Direct Attached Storage，DAS）是一种传统的存储技术，也是一种最早被采用的存储技术。它把外部的数据存储设备都直接挂在服务器内部的总线上，数据存储设备是服务器结构的一部分，但由于这种存储技术是把设备直接挂在服务器上（见图3-20），随着需求的不断增大，越来越多的设备添加到网络环境中，导致服务器和存储独立数量较多，资源利用率低下，使得数据共享受到严重的限制。因此DAS适用在一些小型网络应用中。

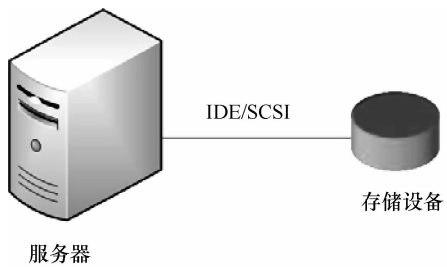


图3-20 直接附加存储体系结构

2. 网络附加存储

网络附加存储（Network Attached Storage，NAS）是传统网络文件服务器技术的发展延续，是一种网络文件服务，它提高了文件系统的处理能力、可靠性、访问连续性和可扩展性。NAS包括存储器件（例如硬盘驱动器阵列、CD或DVD驱动器、磁带驱动器或可移动的存储介质）和专用服务器。这些NAS设备直接连接到TCP/IP网络上，网络服务器通过TCP/IP网络存取管理数据。NAS存储系统都是基于TCP/IP协议的文件访问机制。

传统的网络文件服务器总体可以分为两大类：

1）Unix网络文件服务器，即支持NFS（Network File System，网络文件系统）服务器。

2）NT网络文件服务器，即支持CIFS（Common Internet File System，通用Internet文件系统）服务器。CIFS是一个微软公司提出的协议，它使程序可以访问远程Internet计算机上的文件并要求此计算机的服务。

专用服务器上装有专门的操作系统，通常是简化的Unix/Linux操作系统，或者是一个特殊的Windows 2000内核。它为文件系统管理和访问做了专门的优化。专用服务器利用NFS或CIFS，充当远程文件服务器，对外提供文件级的访问，如图3-21所示。

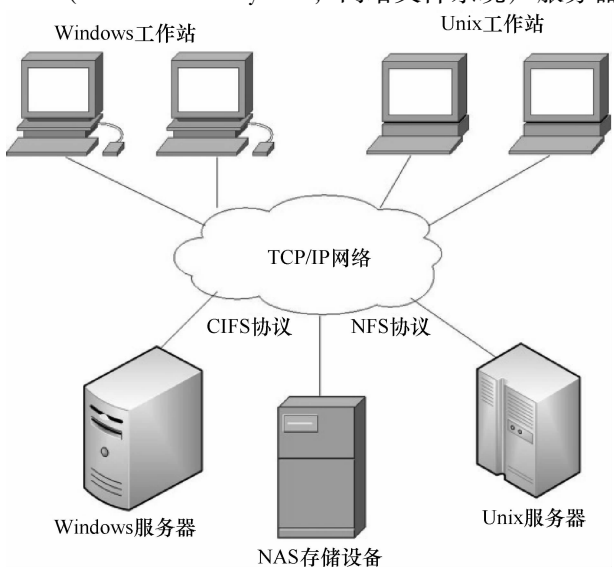


图3-21 NAS结构图

NAS 系统具有很多优点，它支持即插即用、通过 TCP/IP 网络连接到应用服务器，因此可以基于已有的企业网络方便连接；专用的操作系统支持不同的文件系统，提供不同操作系统的文件共享。经过优化的文件系统提高了文件的访问效率，也支持相应的网络协议。即使应用服务器不再工作了，仍然可以读出数据。NAS 技术近年来得到了广泛的应用。

3. 存储区域网络

存储区域网络（Storage Area Network，SAN）是将所有的存储设备连接在一起构成存储网络。它是通过专用高速网将一个或多个网络存储设备和服务器连接起来的专用存储系统。SAN 主要采用数据块的方式进行数据和信息的存储，传统的 SAN 方式采用光纤通道技术，提供给用户高速、高可靠性以及稳定安全的传输。

SAN 由 3 个基本的组件构成：接口（如 SCSI、光纤通道等）、连接设备（交换设备、网关、路由器、集线器等）和通信控制协议（如 IP 和 SCSI 等），这 3 个组件再加上附加的存储设备和独立的 SAN 服务器，就构成一个 SAN 系统。以前的 SAN 多指采用光纤通道（FC）的存储局域网络，到 iSCSI 协议出现以后，为了区分，业界就把 SAN 分为 FC-SAN 和 IP-SAN。但目前较为成熟稳定和应用较广的仍然是 FC-SAN。

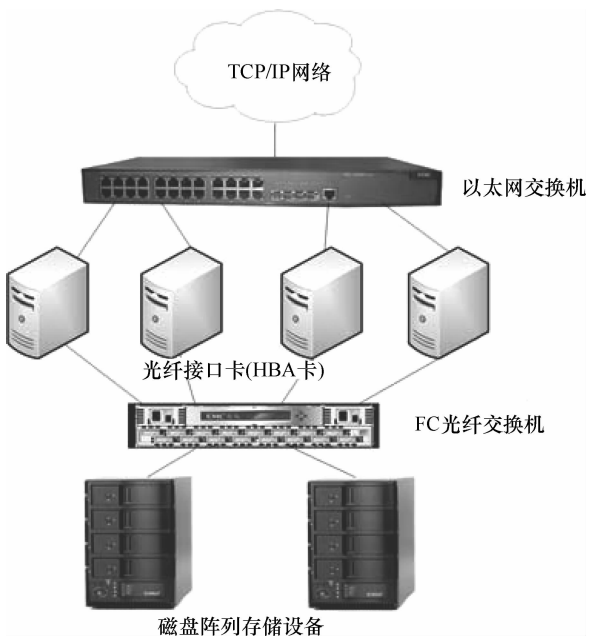


图 3-22　FC-SAN 结构

（1）FC-SAN

FC-SAN 主要由磁盘阵列、FC-Switch 交换机和主机光纤接口卡等组成，如图 3-22 所示。FC-SAN 采用可伸缩的 FC-Switch 网络拓扑结构，它是一种通过光纤通道交换机等连接设备将磁盘阵列、磁带等存储设备与相关服务器连接起来的高速专用子网。光纤通道交换机在逻辑上是 SAN 的核心，它连接着主机和存储设备，光纤交换机规模越大，吞吐率就越高，如：8-port switch 吞吐率为 3.2GB/s，16-port switch 吞吐率为 6.4GB/s。

（2）IP-SAN

FC-SAN 虽然性能优越，可扩展性好，但受限于现有的光纤传输方式，价格昂贵。因此，基于普通 IP 协议和以太网的 SAN 应运而生，这就是 IP-SAN，它将 SCSI 协议映射到 TCP/IP 协议上，使得 SCSI 的命令、数据和状态可以在传统的 IP 网上传输，如图 3-23 所示。

IP-SAN 在整个 IP 网上创建了一个共享存储环境，很好地实现了数据共享和远程访问；由于采用的是 SCSI、以太网、TCP/IP 等现有技术和设施，造价低，便于构建和维护。IP-SAN 存储互操作性好，且克服了 FC-SAN 的距离限制，把共享存储系统扩展到 LAN、WAN 甚至 Internet 上。基于以太网的 IP-SAN 系统可充分利用目前普遍使用的 IP 网络基础设施，节约了大量的成本，加快了实施速度，极大地提高了存储空间的利用率，合理地解决了应用

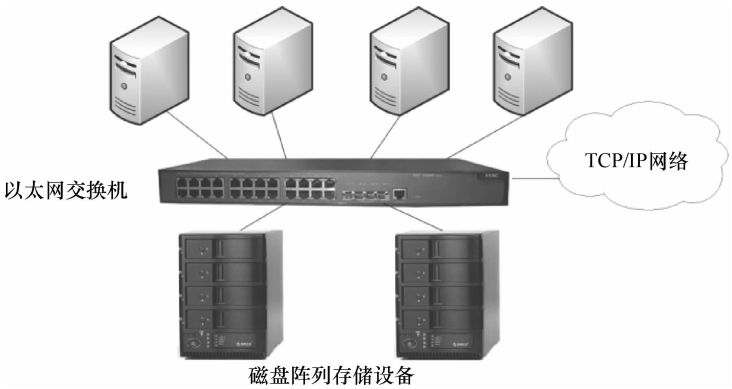


图 3-23　IP-SAN 结构

网络和存储网络异构的问题。

SAN 方式可以在存储设备和服务器之间高效地传输海量数据，减少了用于数据备份和恢复的时间开销以及对局域网网络资源的占用。与服务器之间各自独立，SAN 具有良好的扩展性，可以在不中断与服务器的连接的情况下增加存储而不影响网络性能。通过独立的区域存储，在集中的存储设备上共享数据，SAN 可以对存储设备和数据进行集中的管理和控制，实现无人值守情况下的远程管理。SAN 还可以实现异地存储，提高系统容灾的能力。随着存储技术的发展，SAN 已经得到了越来越广泛的应用。

3.6　云存储技术

3.6.1　云存储技术的基本概念

云存储是在云计算（Cloud Computing）概念上延伸和发展出来的一个新的概念，是指通过集群应用、网格技术或分布式文件系统等功能，将网络中大量不同类型的存储设备通过应用软件集合起来协同工作，共同对外提供数据存储和业务访问功能的一个系统。当云计算系统运算和处理的核心是大量数据的存储和管理时，云计算系统中就需要配置大量的存储设备，那么云计算系统就转变成为一个云存储系统，所以云存储是一个以数据存储和管理为核心的云计算系统。云计算系统可以认为是以数据处理、数据运算为中心的系统。云计算系统不但能对数据进行处理和运算，系统中还有大量的存储阵列设备，以实现对计算数据的保存和管理。在云计算系统中配置相应的存储设备，该计算系统即拥有了云存储系统功能。

云存储一般包含两个含义：

1）云存储是云计算的存储部分，即虚拟化的、易于扩展的存储资源池。用户通过云计算使用存储资源池，但不是所有的云计算的存储部分都是可以分离的。

2）云存储意味着存储可以作为一种服务，通过网络提供给用户。用户可以通过若干种

方式来使用存储，并按使用（时间、空间或两者结合）付费：

①通过互联网开放接口（如 REST），使得第三方网站可以通过云存储提供的服务为用户提供完整的 Web 服务；

②用户直接使用存储相关的在线服务，比如网络硬盘、在线存储、在线备份，或在线归档等服务。

3.6.2　云存储技术的优势

相比传统的存储系统，云存储产品逐步体现出以下几个方面的优势：

1. 成本优势

对于产生大量数据的生产型企业，购买和部署存储系统需要付出的成本非常高，而且存储系统的运行维护费用也不低，致使很多企业想办法去“租用”存储系统，而云存储产品正好可以满足这一市场需求。云存储产品是提供商在互联网上部署一个存储服务器，然后租用给企业，企业可以很方便地像使用自己的存储系统一样来存取数据，可以节省企业的 IT 投入成本。

现在的云存储产品中结合了分级存储的理念，来进一步降低企业的存储成本。分级存储就是根据数据的重要性的不同，将其分别存储在高、中、低端存储系统中。当然不同的存储系统其租用的价格也是不同的。像企业平时的监控数据，其重要性就比较低。而其容量又比较大。如果将其放置在高端存储系统中，需要耗费很大的空间，但是又没有这个必要。此时就可以将其放置在低端存储系统中，以降低空间租用的费用。

2. 管理优势

云存储产品在管理方面也体现出它的优势。云存储产品的运行维护都是由供应商来完成的。也就是说，企业自己并不需要配备专业的存储系统管理员，这一工作是由更专业的云存储服务公司专业人员来承担，在稳定性或者性能上，比自己维护要强得多。

从另一方面看，云存储产品更容易扩展。云存储系统基本上都是根据模块化来设计的。而模块化设计的一个重要的优势就在于其灵活性比较高。在后续可以根据企业的业务来进行扩展，可以根据业务量和数据量的大小灵活地配置和选择，不必担心存储系统容量不够导致的前期投入损失。

3. 访问优势

传统的存储系统部署方式，基本上都是企业自行部署存储系统，存储系统主要局限在企业局域网内部，需要与服务器及应用系统搭建高速的局域网络，带来的弊端是不能更好地在企业之外应用服务。如果采用云存储产品，就可以解决这些问题。用户在外网访问某个文件时，就好像是登录了 163 邮箱一样，不仅速度快，而且不需要经过其他的中间渠道。用户可以随时随地根据自己的需要来访问文件。

云存储产品与自己部署服务器有一个很大的区别，就是服务器的放置位置。自己部署服务器，由于种种原因的限制，服务器往往是放置在企业内部。而云存储产品，其服务器是放置在互联网上。而这个服务器位置的不同，用户访问的途径也就有所不同。云存储产品由于服务器是放置在互联网上，为此无论是内网用户还是外网用户，要访问存储在云存储产品上的信息，都必须通过互联网才可以访问（有些会在企业内部服务器上创建副本）。而由于存储服务器性能优越，会租用比较大的带宽，为此用户访问的速度还是可以接受的。

4. 量身定制的解决方案

云存储产品在提供其存储空间时，其实提供的并不仅仅是空间本身，还会根据企业的需求给出一个量身定制的解决方案。企业有不同的信息化应用，不同的信息化应用对存储设备的要求是不同的。只有分别对待，才能够在节省成本的同时，在性能与安全上得到最大的满足。企业选择使用云存储产品时，对方会根据企业自己的情况以及项目的预算，为企业打造一套合身的存储解决方案。这就是企业购买云存储产品时所享受的附加服务。

3.6.3 云存储的结构模型

与传统的存储设备相比，云存储不仅仅是一个硬件，而且是一个由网络设备、存储设备、服务器、应用软件、公用访问接口、接入网和客户端程序等多个部分组成的复杂系统。各部分以存储设备为核心，通过应用软件来对外提供数据存储和业务访问服务。云存储系统的结构模型如图 3-24 所示。

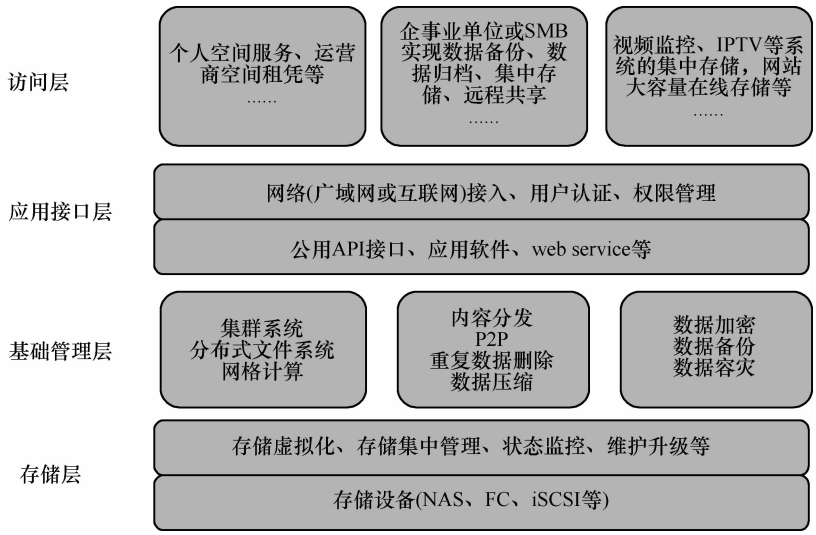


图 3-24 云存储系统的结构模型

云存储系统的结构模型由四层组成。

1. 存储层

存储层是云存储最基础的部分。存储设备可以是 FC 光纤通道存储设备，可以是 NAS 和 iSCSI 等 IP 存储设备，也可以是 SCSI 或 SAS 等 DAS 存储设备。云存储中的存储设备往往数量庞大且分布于不同地域，彼此之间通过广域网、互联网或者 FC 光纤通道网络连接在一起。

存储设备之上是一个统一存储设备管理系统，可以实现存储设备的逻辑虚拟化管理、多链路冗余管理，以及硬件设备的状态监控和故障维护。

2. 基础管理层

基础管理层是云存储最核心的部分，也是云存储中最难以实现的部分。基础管理层通过集群、分布式文件系统和网格计算等技术，实现云存储中多个存储设备之间的协同工作，使多个存储设备可以对外提供同一种服务，并提供更大、更强、更好的数据访问性能。

CDN 内容分发系统、数据加密技术保证云存储中的数据不会被未授权的用户所访问，同时，通过各种数据备份和容灾技术和措施可以保证云存储中的数据不会丢失，从而保证云存储自身的安全和稳定。

3. 应用接口层

应用接口层是云存储最灵活多变的部分。不同的云存储运营单位可以根据实际业务类型，开发不同的应用服务接口，提供不同的应用服务。比如视频监控应用平台、IPTV 和视频点播应用平台、网络硬盘引用平台、远程数据备份应用平台等。

4. 访问层

任何一个授权用户都可以通过标准的公用应用接口来登录云存储系统，享受云存储服务。云存储运营单位不同，云存储提供的访问类型和访问手段也不同。

3.6.4　云存储的特点

云存储系统架构主要以一个高度可扩展和多租户的方式按需交付存储。通用的云存储架构包含一个导出 API（应用程序接口）以访问存储的前端，如图 3-25 所示。在传统的存储系统中，这个 API 是 SCSI 协议。但是在云环境中，这些协议在演化，用户可以找到 Web 服务前端、基于文件的前端，甚至更多传统前端（比如 Internet SCSI 或 iSCSI）。在前端后面是一个中间件层，将它称作存储逻辑。该层通过传统的数据放置算法（考虑地理布局）实现各种功能，比如复制和数据简缩。最后，后端实现对数据的物理存储。这可能是一个实现特定功能的内部协议或物理磁盘的一个传统后端。

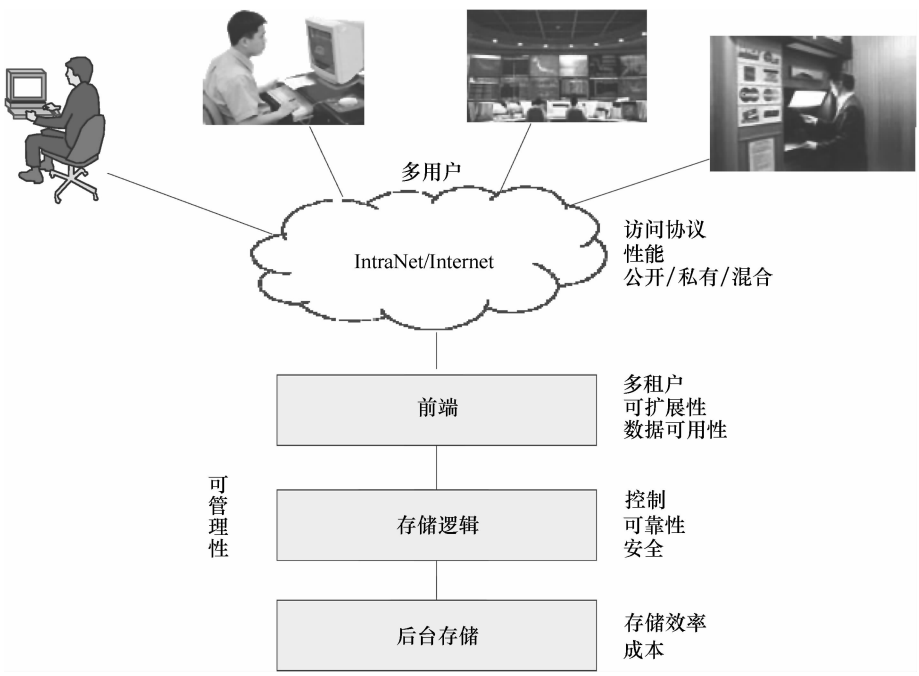


图 3-25　云存储系统通用架构

1. 可管理性

云存储的一个重点是成本。投资成本可划分为两个高级类别：物理存储系统本身的成本和管理运行维护成本。管理运行维护成本是隐式的，但却是总体成本的一个长期组成部分。为此，云存储必须能在很大程度上进行自我管理。引入新存储（其中系统通过自动自我配置来容纳它）的能力和在出现错误时查找和自我修复的能力很重要。在未来，诸如自主计算这样的概念将在云存储架构中起到关键的作用。

2. 访问方法

云存储与传统存储之间最显著的差异之一是其访问方法。大部分提供商实现多个访问方法，但是 Web 服务 APIs 是常见的。Web 服务 APIs 的一个问题是，它们需要与应用程序集成，以利用云存储。因此，对云存储也使用常见的访问方法来提供即时集成。例如，NFS/Common Internet File System（CIFS）或 FTP 等基于文件的协议，iSCSI 等基于块的协议。IBM 还支持从同一存储虚拟化架构同时启用基于文件（NFS 和 CIFS）的协议和基于 SAN 的协议。

3. 性能

性能表现为很多方面，但是在用户与远程云存储提供商之间移动数据的能力是云存储最大的挑战。TCP 基于数据包确认从对等端点控制数据流。数据包丢失或延迟到达情况下将启用阻塞控制，进一步限制性能以避免更多全局网络问题。TCP 适用于通过全局 Internet 启用小量数据，但不适用于会增加往返时间（RTT）的大型数据移动。

通过 Aspera Software，Amazon 解决了这个问题，方法就是从程序中删除 TCP。且开发了一个称为 Fast and Secure Protocol（FASP™）的新协议，以在大型 RTT 和严重数据包丢失的情况下加速批量数据移动。关键是 UDP 的使用，它是 TCP 的缔约方传输协议。UDP 允许主机管理阻塞，将这个方面推进到 FASP（Fast and Secure Protocol，快速安全协议）的应用层协议中。

4. 多租户

云存储架构的一个关键特征称为多租户。这只是表示存储由多个用户（或多个“承租者”）使用。多租户应用于云存储堆栈的多个层，从应用层（其中存储名称空间在用户之间是隔离的）到存储层（其中可以为特定用户或用户类隔离物理存储）。多租户甚至适用于连接用户与存储的网络基础架构，向特定用户保证服务质量和优化带宽。

5. 可扩展性

扩展存储需求（向上和向下）可改善用户成本，提高云存储提供商的复杂性。不仅要为存储本身提供可扩展性（功能扩展），而且必须为存储带宽提供可扩展性（负载扩展）。云存储的另一个关键特性是数据的地理分布（地理可扩展性），支持经由一组云存储数据中心（通过迁移）使数据最接近于用户。对于只读数据，也可以进行复制和分布（使用内容传递网络完成）。在内部，一个云存储架构必须能够扩展。服务器和存储必须能够在不影响用户的情况下重新调整大小。正如在可管理性部分所讨论的，自主计算是云存储架构所必需的。

6. 可用性

如果一个云存储供应商有用户的数据，它必须能够将该数据提供给用户。鉴于网络中断、用户错误和其他情况，这很难以一种可靠而确定的方式予以提供。

7. 控制

一名客户控制和管理其数据存储方式及其相关成本的能力很重要。许多云存储提供商实施控制，使用户对其成本有更大的控制权。

Amazon 实现 Reduced Redundancy Storage（RRS），是为用户提供最小化总存储成本的一种方式。数据是在 Amazon S3 基础架构内复制的，但使用 RRS，数据复制次数较少，且存在丢失数据的可能性。这适用于可重新创建的或在其他地方有副本的数据。Nirvanix 还提供基于策略的复制来对如何以及在何处存储数据提供更细的控制。

8. 效率

存储效率是云存储基础架构的一个重要特征，特别是将重点放在总成本上。下一部分专门介绍成本，但是该特征更多的是关于对可用资源的高效使用，而非成本。

要使一个存储系统更高效，必须存储更多数据。一个常见的解决方案就是数据简缩，即通过减少源数据来降低物理空间需求。实现这一点的两种方法包括：压缩→通过使用不同的表示编码数据来缩减数据→重复数据删除→移除可能存在的相同的数据副本。虽然两种方法都有用，但压缩方法涉及处理（重新编码数据进出基础架构），而重复数据删除方法涉及计算数据签名以搜索副本。

9. 成本

云存储最显著的特征之一是通过使用降低成本。这包括购置存储的成本、驱动存储的成本、修复存储的成本（当驱动器出现故障时）以及管理存储的成本。在从这个角度（包括 SLAs 和增加存储效率）看待云存储时，云存储在某些使用模型中会很有用。

3.6.5　云存储解决方案

当前每个行业的发展都离不开信息系统所提供的智能、快捷、灵活的服务。但信息加速膨胀的压力、纷繁复杂的 IT 网络、难以为继的管理、不断发展的应用类别、快速扩充的客户规模、越来越苛刻的服务水平要求，都让行业用户面临着越来越多的挑战。建立面向服务的“云计算”环境已经从遥不可及的奢望变成一种迫切的现实需求。

“云”分公共云和私有云，尽管对云的建设要求和目标各有不同，但取得成功的关键因素却都离不开能快速交付、灵活、可靠、高可伸缩的云基础设施，以实现云基础设施服务（IaaS）。本节以 IT 巨头 IBM 公司提供的云存储解决方案为例，来说明云存储系统的构建方法。

作为云基础设施的核心，云存储的建设事关项目的成败。IBM 为不同类型业务需求提供一种结合云计算的解决方案和三种云存储解决方案，它们是基础架构云方案 SKC（存储部分使用 SVC）、网格化云存储 XIV、中端虚拟化云存储 Storwize V7000 和文件型云存储 SoNAS。

1. 基础架构云方案 SKC

Starter Kit for Cloud 为虚拟化平台提供关键功能。该产品允许数据中心立即接入云特性，数据中心可根据需要随时动态交付资源并且基于云交付基础设施即是服务，从而获得优势。作为完全集成的软件堆栈，Starter Kit for Cloud 可将虚拟化环境从“云就绪”状态过渡到真正的“云”环境。用户可通过基于 Web 的界面快速请求和调配环境。用户可以启动和停止工作负载、调整工作负载的大小、复制或删除工作负载；可以监控和管理工作负载审批流

程；可以跟踪资源使用情况以便只为所需资源付费；可以创建标准化工作负载或设备。使用 Starter Kit for Cloud 与现有的虚拟化 Power 及 x86 系统环境配合使用，将能够快速启动和运行云基础设施。

数据中心之所以渴望提高投资回报率，是因为用户对异构数据中心当前普遍采用的低效率结构感到不满。当实际情况切实发生变化时，这些组件却无法进行互换。为了帮助创建最佳数据中心，Starter Kit for Cloud 提供的软件堆栈可将 Power 及 x86 服务器硬件从可靠的高性能虚拟化平台转变成易于部署且价格合理的高级私有云，如图 3-26 所示。

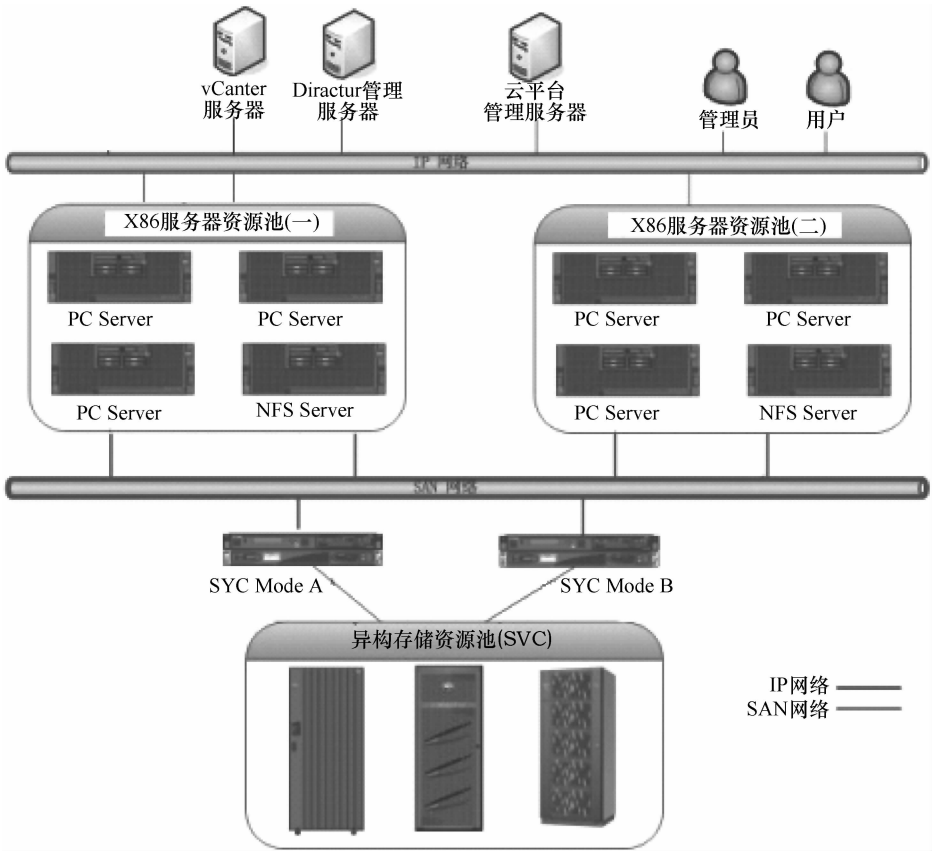


图 3-26　SVC 云存储解决方案

其中，SVC（SAN Volume Controller）存储虚拟化解决方案通过将存储容量整合到一个存储资源池中，简化存储基础架构、对信息进行生命周期管理并维护业务持续性。

通过存储虚拟化，用户可以从单一界面实现统一管理，极大地减少了管理员的配置、管理和服务开销。主机应用程序不再受存储池物理更改的影响。用户可以重新分配和扩展存储容量，而无需中断应用程序的运行，保障了业务的连续性。

SVC 解决方案帮助企业构建一个更加简单、扩展能力更强、成本效益更高的 IT 架构，灵活地与新的业务目标保持一致。

2. 网格化云存储 XIV

XIV 自其诞生之日起就注定是传统磁盘存储产品的颠覆者。它改变了存储设计的游戏规

则，当人们还在纠缠硬盘类型、缓存大小、接口数量等常规技术指标时，XIV 以最直接的方式关心用户体验。传统存储系统通常会面临的难以管理、难以变更、热点盘、长时间重建故障盘等问题在 XIV 上都不存在。

网格化的存储结构让 XIV 的存储性能随磁盘数量的增加自动得到提升。用户无需面对性能优化、配置调整、业务中断等存储管理难题即可快速部署新增业务。一旦磁盘发生故障，XIV 可以最快速地将系统从故障中恢复，并且始终保持性能均衡。XIV 还可挂接其他存储，进行无缝数据迁移。XIV 拥有业界最灵活高效的卷快照功能，快照的数量不影响生产性能，让快照成为备份海量数据最可行的一种方式。

XIV 网络化云存储如图 3-27 所示。

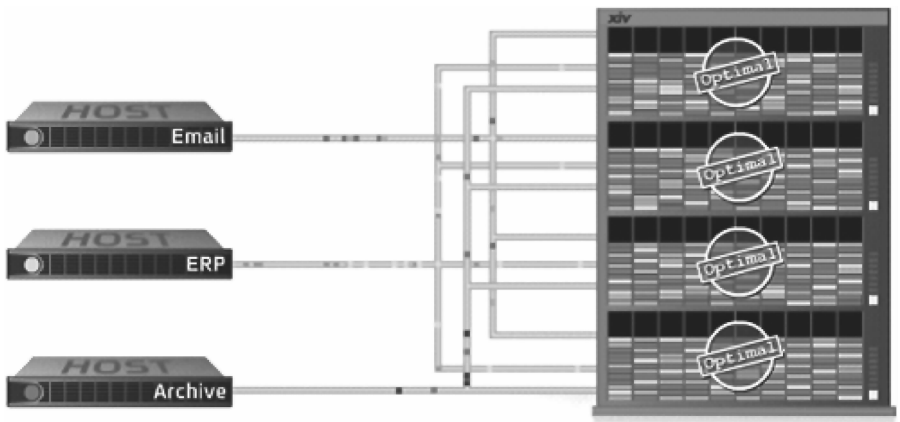


图 3-27　XIV 网络化云存储

3. 中端虚拟化云存储 Storwize V7000

Storwize V7000 的存储虚拟化技术继承自著名的 IBM 存储虚拟化解决方案 SVC。它除了拥有 SVC 所具备的存储虚拟化能力外，还自带磁盘，包括 SSD 固态磁盘和普通磁盘。它通过 EasyTier 技术在 SSD 和普通硬盘间动态迁移数据，将 SSD 的性能优势发挥至极致。Storwize 存储系统如图 3-28 所示。

Storwize V7000 以存储资源池的方式管理自带磁盘和异构的存储设备，通过虚拟化技术屏蔽掉异构存储设备间的差异性，为各类云计算服务提供统一的存储访问界面，从而大幅降低云计算环境的建设难度和成本，并且让云计算基础设施变得更易于管理。

Storwize V7000 提供 Virtual Disk Mirror 功能来提升核心业务的高可用性；提供在线数据迁移功能让物理存储的变更不再影响业务的运营。Storwize 的跨存储快照功能为优化海量信息的备份保护方式提供了可能。这种方案适合中小企业虚拟化云存储部署。

4. 文件型云存储 SoNAS

有些云计算服务需要处理海量的文件信息，如电信行业面向公众的网盘服务、公安部门的高清卡口、媒体业的非线编媒资管理和广泛应用于气象、勘探部门的 HPC 高性能运算业务。此类业务需要处理的文件数量动辄千万计，文件容量有可能超过 1PB。此时，普通的网络文件存储 NAS 会面临性能、容量、信息管理能力瓶颈。

IBM GPFS 并行存储解决方案，从传输性能、海量信息管理、容量在线扩展、信息保护和信息生命周期管理等方面为客户提供优秀的管理能力，从而帮助客户降低风险，提升投资回报，确保业务服务水平。

IBM Scale Out NAS（SoNAS）是以 IBM GPFS 并行文件系统为核心的横向扩展文件型存储解决方案，它将多个 SAN 存储整合到同一命名空间，从而建构一个可高速并行共享访问的存储系统。它具备横向动态扩展存储容量、横向动态扩展 I/O 性能和分层存储管理能力。

IBM SoNAS 提供 CIFS、NFS、SCP、FTP 和 HTTP 等多种网络访问接口，最大可管理 10 亿个文件，提供 14.4PB 磁盘空间，可在数十个物理存储阵列间建立起统一共享的存储命名空间。IBM SoNAS 拥有丰富的信息管理功能，包括快照、复制，与自含 TSM 数据备份接口用于数据备份保护，与 IBM 磁带库系统配合可将历史信息自动迁移到磁带库等。文件型云存储如图 3-29 所示。

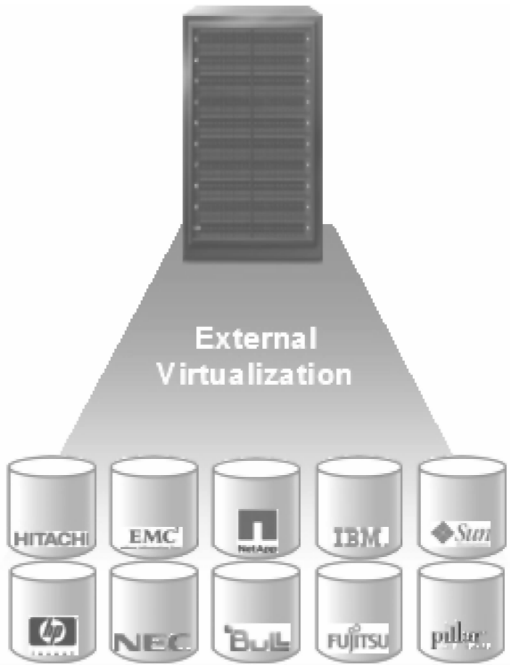


图 3-28　Storwize 存储系统

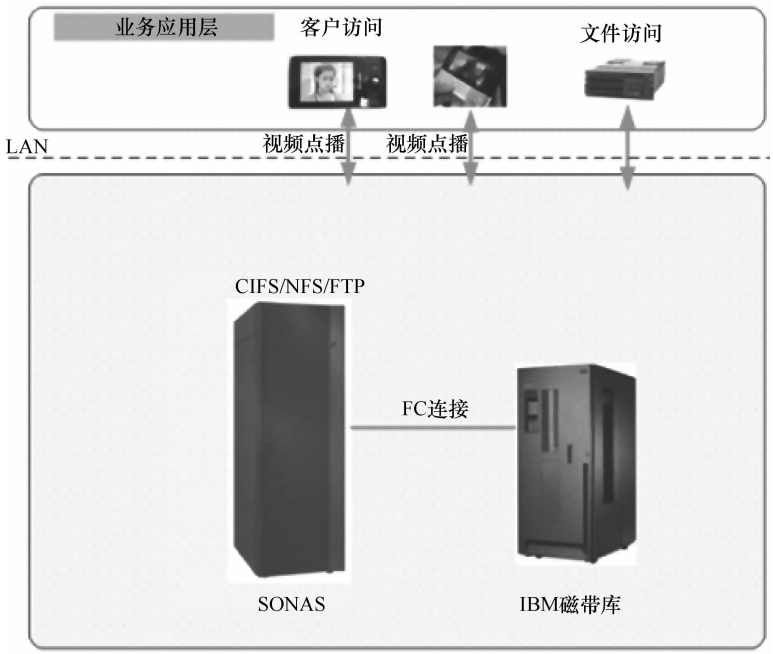


图 3-29　文件型云存储

本 章 小 结

本章主要从服务器和存储技术的角度进行了研究。对于大型园区网络，数据中心的建设是必不可少的。数据中心主要以服务器和存储系统提供信息系统运行的平台，以提供面向本单位的信息服务。

1）服务器是信息系统运行最重要的硬件平台，对服务器硬件基础、服务器的分类和服务器系统的主要技术进行了阐述；特别介绍了刀片服务器技术和虚拟化技术。服务器虚拟化技术是服务器技术发展的方向，使得数据中心建设逐步走向绿色数据中心。

2）存储系统是应对互联网发展大数据时代到来的重要 IT 设备。对存储系统的相关概念、分类和主要技术进行了介绍。特别是针对网络存储系统、最先进的云存储系统进行了介绍，并对云存储解决方案进行了分析。

第 4 章　网络安全技术

4.1　网络安全概述

4.1.1　网络安全的重要性

计算机网络为我们带来了资源共享和数据通信的便利。计算机网络提供了丰富的资源以便用户共享，提高了系统的灵活性和可靠性。计算机网络提供的分布式处理和均衡负载的功能提高了工作效率，这些特点使得计算机网络应用深入到国家的政治、经济、国防、科技、教育等各个领域。一个国家的信息化程度越高，整个国民经济和社会运行对信息资源和信息基础设施的依赖程度也越高。今天计算机网络同人们的生活、工作已经形成了密切的依赖和联系，可以说网络无处不在，它正在改变我们的工作和生活方式。

但是，伴随网络的普及，安全问题逐步成为影响网络效能的重要问题。计算机网络带来便利的同时也增加了遭受威胁和攻击的可能性。例如，电子政务得到了空前的发展，政府推行网上办公，政府的网络代表着国家的形象，1999 年以来，我国的一些政府网站不断遭受到别国黑客组织的攻击；在电子商务领域，经常发生网络欺骗事件，使得人们的资金受到了损失和威胁等。这些问题的产生，告诉我们一个事实：资源共享和网络安全是一对矛盾，随着资源共享的发展，网络安全的问题日益突出。

网络充满了安全隐患，我们必须掌握足够的计算机网络安全技术，才能保证自己的网络和信息系统安全、稳定和可靠的运行。

4.1.2　网络面临的不安全因素

影响网络安全的原因有很多，主要有来自网络系统外部的攻击破坏和网络系统内部的脆弱性。

1. 网络系统的脆弱性

（1）操作系统的脆弱性

当前无论哪一种操作系统在体系结构上都是不安全的，也可以认为是操作系统先天存在缺陷。一方面，操作系统为了达到支持系统集成和可扩充的灵活性而支持动态链接，在为厂商和用户提供方便的同时也为黑客提供了入侵的可能，而且动态链接也是计算机病毒产生的温床。另一方面，操作系统可以创建进程，而且这些进程可以在远程网络节点上被创建与激活，更大的隐患是被创建的进程又可以继续创建其他进程，这一个特性可以让黑客在远程将“间谍”程序以打补丁的方式安装在特权用户上，这样系统的监视程序根本无法探测到“间谍”程序的存在。

（2）计算机系统本身的脆弱性

操作系统的不安全本身会导致计算机系统的不安全。另一方面，计算机系统会因为硬件

故障、软件故障影响到系统的正常运行，导致网络服务的中断。

（3）协议安全的脆弱性

计算机网络通信协议如 TCP/IP 协议及一些应用层协议如 TELNET、FTP、RPC 等存在许多安全漏洞，这些漏洞会被黑客利用来对计算机网络发起攻击。

（4）数据库管理系统的脆弱性

数据库系统的核心数据库管理系统 DBMS 是建立在分级管理的概念上，它本身需要运行在操作系统上，这就导致 DBMS 的安全必须与操作系统的安全配套，这无疑是一个先天的不足之处。

除了以上 4 个方面以外，还存在一些如电磁泄露、网络存储介质的脆弱性及一些人为的因素，这都将成为计算机网络安全的隐患。

2. 各种外部威胁

（1）物理威胁

物理安全是指用于保护计算机硬件和存储介质的装置和工作程序。常见的物理威胁主要包括以下几个方面：偷窃、废物搜寻、间谍行为等。物理安全是计算机安全最重要的方面之一。

（2）系统漏洞威胁

系统漏洞也被称为陷阱，计算机系统本身存在的安全漏洞会造成黑客乘虚而入，还有一些不安全的服务及配置和初始化的错误引起的安全问题。

（3）有害程序威胁

有害的程序包括计算机病毒、代码炸弹和特洛伊木马等。病毒具有较强的威胁性，可以自我复制，感染计算机网络上的计算机系统造成瘫痪；代码炸弹也会像定时炸弹一样触发对计算机系统产生极强破坏性的操作；特洛伊木马被黑客植入到入侵的目标计算机中，能够通过黑客的控制来窃取目标计算机中的数据或做出各种破坏性的操作。

（4）身份鉴别威胁

身份鉴别是计算机判断某个用户是否为合法授权用户的行为。身份鉴别威胁包括口令圈套、口令破解、算法考虑不周等，如口令圈套是黑客采用一种冒名顶替的阴谋诡计来骗取获得进入计算机系统的真实口令。

4.1.3　网络安全的定义及特征

1. 什么是网络安全

我们常常听说网络安全、信息安全、网络信息安全、计算机安全、系统安全等名词，这些不同的说法归根结底就是两层意思：确保计算机网络环境下信息系统的安全运行和信息系统中存储、处理和传输的信息受到保护。这就是通常所说的保证网络系统运行的可靠性、信息的保密性、完整性和可用性。

目前，互联网中存在着各种各样的漏洞和威胁，网络安全涉及的领域极为广泛，从不同的角度可以给出不同的解释。从信息资源的角度来讲，网络安全的本质是保证网络上的信息安全，强调对系统信息的安全保护；从网络系统的角度来讲，要保障计算机网络系统安全、可靠、稳定地运行，网络服务不中断，强调系统安全运行。

网络安全涉及的领域相当广泛，从不同的角度或不同的用户具体有不同的含义。从普通

用户（个人、企业）的角度来说，他们希望涉及个人隐私或商业利益的有价值的信息不被其他人或对手利用窃听、篡改，或以抵赖等手段对他们的利益造成侵害；从网络运行和管理者的角度来看，他们希望对本地网络信息的访问、读写等操作受到保护和控制，避免出现病毒、非法存取、拒绝服务和网络资源的非法占用及非法控制等威胁，制止和防御网络“黑客”的攻击。下面是国际标准化组织（ISO）给出的一个通用的定义。

计算机网络系统的安全定义为：“为数据处理系统建立所采取的技术和管理的安全保护，保护计算机网络系统的硬件、软件和数据不因偶然或恶意的原因而遭到破坏、更改和泄露，系统连续可靠正常地运行，网络服务不中断”。

计算机网络安全的内容包括两个方面：物理安全和逻辑安全。物理安全指系统设备及相关设施受到物理保护，免于破坏、丢失等；逻辑安全包括信息完整性、保密性和可用性。

我们可以通俗的理解为：网络安全是指网络系统的硬件、软件及其系统中的数据受到保护，不因偶然的或者恶意的原因而遭到破坏、更改或泄露，系统连续、可靠、正常的运行，网络服务不中断。从不同的角度出发，对网络安全也有不同的理解：

1）从网络用户（个人、企业）的角度来讲，希望涉及个人隐私或商业利益的信息在网络中传输时，受到几方面的保护（保密性、完整性和真实性等），避免其他人利用窃听、冒充、篡改和抵赖等手段侵犯或损害他们的利益，同时也希望当用户的信息保存在某个计算机系统上时，不受其他非法用户的非授权访问和破坏。

2）从网络运行和管理的角度来讲，希望对本地网络信息的访问、读写等操作受到保护和控制，避免出现病毒、非法存取、拒绝服务的网络资源的非法占用及非法控制等威胁，防范和制止网络黑客的攻击。

3）从安全保密部门的角度来讲，希望对非法的、有害的或涉及国家机密的信息进行过滤和阻截，避免出现机密信息泄露，对社会产生危害，给国家造成巨大的损失，甚至威胁到国家安全。

4）从社会教育和意识形态的角度来讲，希望对网络上不健康的内容加以控制，避免这些信息影响社会的稳定和对人类的发展产生不利的影响。

2. 网络安全的特征

网络安全的特征可以概括为 4 个方面：

1）保密性：利用密码技术对信息进行加密处理，确保信息不泄露给非授权的用户或供其利用。

2）完整性：保护网络系统中的信息不被非法操作，即保证信息在传输或存储的过程中不被非法修改、不被破坏或丢失的特性。

3）可用性：可被授权的用户按需求使用的特性，即保证信息在授权的用户使用的时候可以正常使用，不会在网络环境下拒绝服务或计算机网络系统被破坏导致信息不可用等问题。

4）可靠性：保证网络系统不因各种因素的影响而导致网络服务中断，影响正常的运行。

4.2　网络安全策略及防护体系

4.2.1　网络安全策略

针对各种攻击行为，必须采取相应的对策。一个重要的网络安全任务，就是要制定一个网络安全策略；其次是采取必备的防范措施。

连接到因特网就会面临网络的威胁，针对这些威胁，为了降低网络安全的风险，各计算机网络使用机构、企业或单位，应该建立相应的网络安全管理制度，建立合适的网络安全管理政策，建立安全审计和跟踪机制等，制定具体的网络安全策略，提高整体网络的安全体系。制定网络安全策略的目的是决定一个组织机构怎样来保护自己。网络安全的策略规定了一个组织结构的网络行为，哪些网络行为是允许的，哪些网络行为是禁止的。各个组织机构在制定安全策略的时候，都需要结合本单位的情况，制定本单位的总体安全政策和详细的实施规则，这样可以降低人为的不安全因素带来的威胁；同时可以采取积极主动的方式抵御网络的攻击，可以降低单位的网络安全风险。

一个网络安全策略通常包括两方面的内容：

1）明确人的安全责任。为保证计算机网络系统的安全运行，网络系统的使用单位应该成立计算机安全管理机构，规划网络系统的安全，制定完善的安全策略和措施，建立网络安全管理制度，设立专职安全人员，进行安全管理、安全审计、系统风险分析、软硬件管理等。从事安全管理的人必须严格遵守和执行单位的安全管理规章制度，明确职责。当然计算机网络安全不单是依靠安全管理人员，更多是依靠单位内部所有员工的执行。比如对于普通的计算机用户，必须教会他们正确利用网络资源，规定谁可以使用网络资源，他们可以做什么，不能够做什么，合理地执行网络行为，这些在单位的安全管理制度中应该有明确的规定，可以避免泄露单位敏感的信息，规避人为因素带来的风险。而系统安全管理人员承担更大的责任，必须对计算机网络进行监控，采取专门的安全措施保障网络安全。

2）明确检测到安全问题时的对策。这部分策略要求安全管理人员必须明确遇到安全问题时应采取的应急措施。当安全问题存在时，必须采取什么措施消除安全问题，或者当安全问题发生时，怎样最小程度地降低损失。因此，网络安全策略中必须对网络安全问题的对策提出明确的指导意见。

4.2.2　网络安全防护体系

从系统安全的角度，可以把网络安全的问题分成两大体系：攻击和防御，这就像一对矛和盾。

1. 网络攻击行为

1）网络监听：在计算机上设置一个程序去监听目标计算机与其他计算机通信的数据，从数据中分析出自己感兴趣的内容。

2）漏洞扫描：利用程序去扫描目标主机上开发的端口及服务等，目的是发现目标主机存在的安全漏洞，为入侵目标主机做好准备。

3）网络入侵：通过扫描发现目标主机的漏洞后，利用该漏洞入侵到目标计算机中获取

信息。

4）种植后门：成功入侵目标计算机后，为了实现对目标主机的长期控制，在该主机中种植木马等后门。

5）网络隐身：入侵完毕后退出目标计算机后，将入侵的痕迹清除，以避免被目标主机的管理员发现。

2. 网络防御技术

1）操作系统的安全配置：操作系统的安全是整个网络的关键，尽可能选用更为安全的操作系统，并确保操作系统不存在人为配置上的错误。

2）加密技术：为了保证网络上信息传递的保密性及完整性等，可以使用加密算法及数字签名等技术。

3）防火墙技术：使用防火墙隔离 Web 和内部网络，以保护内部网络的安全，抵御外部网络的入侵行为。

4）入侵检测技术：能够对外部网络的入侵行为进行识别和判断，从而发出报警信号。

4.3 常见的网络黑客攻击方法及防范

4.3.1 网络攻击的步骤

1. 隐藏自己的位置

普通攻击者都会利用别人的计算机隐藏他们真实的 IP 地址。老练的攻击者还会利用 800 电话的无人转接服务联接 ISP，然后再盗用他人的账号上网。

2. 寻找目标主机并分析目标主机

攻击者首先要寻找目标主机并分析目标主机。在 Internet 上能真正标识主机的是 IP 地址，域名是为了便于记忆主机的 IP 地址而另起的名字，只要利用域名和 IP 地址就可以顺利地找到目标主机。当然，知道了要攻击目标的位置还是远远不够的，还必须将主机的操作系统类型及其所提供的服务等资料做个全面的了解。此时，攻击者会使用一些扫描工具，轻松获取目标主机运行的是哪种操作系统的哪个版本，系统有哪些账户，WWW、FTP、Telnet、SMTP 等服务器程序是何种版本等资料，为入侵做好充分的准备。

3. 获取账号和密码，登录主机

攻击者要想入侵一台主机，首先要有该主机的一个账号和密码，否则连登录都无法进行。这样常迫使他们先设法盗窃账户文件，进行破解，从中获取某用户的账户和口令，再寻觅合适时机以此身份进入主机。当然，利用某些工具或系统漏洞登录主机也是攻击者常用的一种技法。

4. 获得控制权

攻击者们用 FTP、Telnet 等工具利用系统漏洞进入目标主机系统获得控制权之后，就会做两件事：清除记录和留下后门。攻击者会更改某些系统设置，在系统中植入特洛伊木马或其他一些远程操纵程序，以便日后可以不被觉察地再次进入系统。大多数后门程序是预先编译好的，只需要想办法修改时间和权限就可以使用了，甚至新文件的大小都和原文件一模一样。攻击者一般会使用 rep 传递这些文件，以便不留下 FTB 记录。用清除日志、删除复制的

文件等手段来隐藏自己的踪迹之后，攻击者就开始下一步的行动。

5. 窃取网络资源和特权

攻击者找到攻击目标后，会继续下一步的攻击。如：下载敏感信息，窃取账号密码，使网络瘫痪。

4.3.2　网络攻击的原理和手段

1. 口令入侵

所谓口令入侵是指使用某些合法用户的账号和口令登录到目的主机，然后再实施攻击活动。这种入侵方法的前提是必须先得到该主机上的某个合法用户的账号，然后再进行合法用户口令的破译。获得普通用户账号的方法很多，如利用目标主机的 Finger 功能：当用 Finger 命令查询时，主机系统会将保存的用户资料（如用户名、登录时间等）显示在终端或计算机上。通常有三种方法：

（1）通过网络监听获得口令

通过网络监听非法得到用户口令，这类方法有一定的局限性，但危害性极大。监听者也往往采用中途截击的方法获取用户账户和密码。当下，很多协议根本就没有采用任何加密或身份认证技术，如在 Telnet、FTP、HTTP、SMTP 等传输协议中，用户账户和密码信息都是以明文格式传输的，此时若攻击者利用数据包截取工具便可很容易收集到用户的账户和密码。还有一种中途截击攻击方法更为厉害，它可以在用户同服务器端完成“三次握手”建立连接之后，在通信过程中扮演“第三者”的角色，假冒服务器身份欺骗用户，再假冒用户向服务器发出恶意请求，其造成的后果不堪设想。另外，攻击者有时还会利用软件和硬件工具时刻监视系统主机的工作，等待记录用户登录信息，从而取得用户密码；或者编制有缓冲区溢出错误的 SUID 程序来获得超级用户权限。

（2）暴力破解

在知道用户的账号后（如电子邮件@ 前面的部分）利用一些专门软件强行破解用户口令，这种方法不受网段限制。如：采用字典穷举法（或称暴力法）来破解用户的密码。攻击者可以通过一些工具程序，自动从计算机字典中取出一个单词，作为用户的口令，再输入给远端的主机，申请进入系统；若口令错误，就按序取出下一个单词，进行下一次尝试，并一直循环下去，直到找到正确的口令或字典的单词试完为止。由于这个破译过程由计算机程序来自动完成，因而几个小时就可以把上十万条记录的字典里的所有单词都尝试一遍。

（3）利用系统管理员的失误

在现代的 Unix 操作系统中，用户的基本信息存放在 passwd 文件中，而所有的口令则经过 DES 加密方法加密后专门存放在一个叫 shadow 的文件中。黑客们获取口令文件后，就会使用专门的破解 DES 加密法的程序来解口令。同时，由于为数不少的操作系统都存在许多安全漏洞、Bug 或一些其他设计缺陷，这些缺陷一旦被找出，黑客就可以长驱直入。例如，让 Windows95/98 系统后门洞开的 BO 就是利用了 Windows 的基本设计缺陷。

2. 放置特洛伊木马程序

特洛伊木马程序可以直接侵入用户的计算机并进行破坏，它常被伪装成工具程序或者游戏等诱使用户打开带有特洛伊木马程序的邮件附件或从网上直接下载，一旦用户打开了这些邮件附件或者执行了这些程序之后，它们就会像古特洛伊人在敌人城外留下的藏满士兵的木

马一样留在用户的计算机中，并在用户的计算机系统中隐藏一个可以在 Windows 启动时悄悄执行的程序。当用户连接到因特网上时，这个程序就会通知攻击者，来报告用户的 IP 地址以及预先设定的端口。攻击者在收到这些信息后，再利用这个潜伏在其中的程序，就可以任意地修改用户计算机的参数设定、复制文件、窥视用户整个硬盘中的内容等，从而达到控制用户的计算机的目的。

3. WWW 的欺骗技术

在网上用户可以利用 IE 等浏览器进行各种各样的 Web 站点的访问，如阅读新闻、咨询产品价格、订阅报纸、电子商务等。然而一般的用户恐怕不会想到有这些问题存在：正在访问的网页已经被黑客篡改过，网页上的信息是虚假的。例如黑客将用户要浏览的网页的 URL 改写为指向黑客自己的服务器，当用户浏览目标网页的时候，实际上是向黑客服务器发出请求，那么黑客就可以达到欺骗的目的了。

一般 Web 欺骗有两种技术手段，即 URL 地址重写技术和相关信息掩盖技术。利用 URL 地址，攻击者可以将自己的 Web 地址加在所有 URL 地址的前面。这样，当用户与站点进行安全链接时，就会毫无防备地进入攻击者的服务器，于是用户的所有信息便处于攻击者的监视之中。但由于浏览器一般均设有地址栏和状态栏，当浏览器与某个站点连接时，可以在地址栏和状态栏中获得连接中的 Web 站点地址及其相关的传输信息，用户由此可以发现问题，所以攻击者往往在 URL 地址重写的同时，利用相关信息掩盖技术，即一般用 JavaScript 程序来重写地址栏和状枋栏，以达到其掩盖欺骗的目的。

4. 电子邮件攻击

电子邮件是互联网上运用得十分广泛的一种通信方式。攻击者可以使用一些邮件炸弹软件或 CGI 程序向目的邮箱发送大量内容重复、无用的垃圾邮件，从而使目标邮箱被撑爆而无法使用。当垃圾邮件的发送流量特别大时，还有可能造成邮件系统对于正常的工作反映缓慢，甚至瘫痪。

电子邮件攻击主要表现为两种方式：

1）电子邮件轰炸和电子邮件“滚雪球”，也就是通常所说的邮件炸弹，指的是用伪造的 IP 地址和电子邮件地址向同一信箱发送数以千计、万计甚至无穷多次的内容相同的垃圾邮件，致使受害人邮箱被“炸”，严重者可能会给电子邮件服务器操作系统带来危害，甚至瘫痪。

2）电子邮件欺骗，攻击者佯称自己为系统管理员（邮件地址和系统管理员完全相同），给用户发送邮件要求用户修改口令（口令可能为指定字符串）或在貌似正常的附件中加载病毒或其他木马程序。

5. 通过一个节点来攻击其他节点

攻击者在突破一台主机后，往往以此主机作为根据地，攻击其他主机（以隐蔽其入侵路径，避免留下蛛丝马迹）。他们通过网络监听方法，尝试攻破同一网络内的其他主机；或通过 IP 欺骗和主机信任关系，攻击其他主机。

这类攻击很狡猾，但由于某些技术很难掌握，如 TCP/IP 欺骗攻击。攻击者通过外部计算机伪装成另一台合法机器。其伪装的目的在于哄骗网络中的其他机器误将其作为合法机器加以接受，诱使其他机器向他发送数据或允许它修改数据。TCP/IP 欺骗可以发生在 TCP/IP 系统的所有层次上，包括数据链路层、网络层、运输层及应用层均容易受到影响。如果底层

受到损害，则应用层的所有协议都将处于危险之中。另外，由于用户本身不直接与底层相互交流，因而对底层的攻击更具有欺骗性。

6. 网络监听

网络监听是主机的一种工作模式，在这种模式下，主机可以接收到本网段在同一条物理通道上传输的所有信息，而不管这些信息的发送方和接收方是谁。因为系统在进行密码校验时，用户输入的密码需要从用户端传送到服务器端，而攻击者就能在两端之间进行数据监听。此时若两台主机进行通信的信息没有加密，只要使用某些网络监听工具（如 NetXRay for Windows95/98/NT/2003、Sniffit for Linux、Solaries 等）就可轻而易举地截取包括口令和账号在内的信息资料。虽然网络监听获得的用户账号和口令具有一定的局限性，但监听者往往能够获得其所在网段的所有用户账号及口令。

7. 利用黑客软件攻击

利用黑客软件攻击是互联网上比较多的一种攻击手法。Back Orifice2000、冰河等都是比较著名的特洛伊木马，它们可以非法地取得用户计算机的超级用户级权利，可以对其进行完全的控制，除了可以进行文件操作外，同时也可以进行对方桌面抓图、取得密码等操作。这些黑客软件分为服务器端和用户端，当黑客进行攻击时，会使用用户端程序登录已安装好服务器端程序的计算机，这些服务器端程序都比较小，一般会附带于某些软件上。有可能当用户下载了一个小游戏并运行时，黑客软件的服务器端就安装完成了，而且大部分黑客软件的重生能力比较强，给用户进行清除造成了一定的麻烦。特别是最近出现了一种 txt 文件欺骗手法，表面看上去是一个 txt 文本文件，但实际上却是一个附带黑客程序的可执行程序。另外，有些程序也会伪装成图片和其他格式的文件。

8. 安全漏洞攻击

许多系统都有这样那样的安全漏洞（Bugs）。其中一些是操作系统或应用软件本身就具有的，如缓冲区溢出攻击。由于很多系统不检查程序与缓冲之间变化的情况，就任意接受任意长度的数据输入，把溢出的数据放在堆栈里，系统还照常执行命令。这样攻击者只要发送超出缓冲区所能处理的长度的指令，系统便进入不稳定状态。若攻击者特别配置一串准备用作攻击的字符，他甚至可以访问根目录，从而拥有对整个网络的绝对控制权。另一些攻击者是利用协议漏洞进行攻击。如攻击者利用 POP3 一定要在根目录下运行的这一漏洞发动攻击，破坏根目录，从而获得超级用户的权限。又如，ICMP 协议也经常被用于发动拒绝服务攻击。它的具体手法就是向目的服务器发送大量的数据包，几乎占取该服务器所有的网络宽带，从而使其无法对正常的服务请求进行处理，导致网站无法进入、网站响应速度大大降低或服务器瘫痪。现在常见的蠕虫病毒或与其同类的病毒都可以对服务器进行拒绝服务攻击。它们的繁殖能力极强，一般通过 Microsoft 的 Outlook 软件向众多邮箱发送带有病毒的邮件，从而使邮件服务器无法承担如此庞大的数据处理量而瘫痪。对于个人上网用户而言，也有可能遭到大量数据包的攻击而无法进行正常的网络操作。

4.3.3　IP 欺骗攻击

1. IP 电子欺骗

所谓 IP 电子欺骗攻击是指利用 TCP/IP 本身的缺陷进行的入侵，即用一台主机设备冒充另外一台主机的 IP 地址，与其他设备通信，从而达到欺骗的目的。被伪造的主机往往具有

某种特权或者被另外的主机所信任。IP 电子欺骗是入侵者攻克 Internet 防火墙系统最常用的方法，也是许多其他攻击方法的基础。对于来自网络外部的 IP 电子欺骗，只要配置一下防火墙就可以了，但对同一网络内的机器实施攻击则不宜防范。实际上，IP 欺骗不是进攻的结果，而是进攻的手段。进攻实际上是破坏信任关系。另外，在互联网络上也出现了大量的可以发送伪造 IP 地址的工具，使用它可以任意指定源 IP 地址，以免留下自己的痕迹。

2. IP 电子欺骗原理

为了清楚地了解 IP 电子欺骗，首先需要回顾一下 TCP/IP 会话的过程。由于 TCP 是面向连接的协议，所以在双方正式传输数据之前，需要用“三次握手”来建立一个稳定的连接。假设 X、Y 两台主机进行通信，Y 首先发送带有 SYN 标志的数据段通知 X 需要建立 TCP 连接，TCP 的可靠性就是由数据包中的多位控制字来提供的，其中最重要的是数据序列 SYN 和数据确认标志 ACK。Y 将 TCP 报头中的 SYN 设为自己本次连接的初始值（ISN）。X 收到 Y 的 SYN 包之后，会发送给 Y 一个带有 SYN + ACK 标志的数据段，告之自己的 ISN，并确认 Y 发送来的第一个数据段，将 ACK 位设置成 X 的 SYN + 1。X 收到 Y 的 ACK 后，连接成功建立，双方可以正式传输数据了。

过程分为三步：

1）Y 发送带有 SYN 标志的数据段通知 X 需要建立 TCP 连接。

2）X 收到 Y 的 SYN 包后，发送给 Y 一个带有 SYN + ACK 标志的数据段，告之自己的 ISN。

3）Y 发送 ACK 给 X，连接成功建立。

从三次握手的过程来看，假如一个攻击者要冒充 Y 对 X 进行攻击，就要先使用 Y 的 IP 地址发送 SYN 标志给 X，但是当 X 收到后，它并不会把 SYN + ACK 发送到冒充者的主机，而是发送到真正的 Y 上去，冒充者的企图将会立即被揭穿，因为 Y 根本没有发过 SYN 请求。因此，要冒充 Y，攻击者首先会让 Y 失去工作能力，比如利用拒绝服务攻击让 Y 瘫痪。

3. IP 电子欺骗攻击的过程解析

IP 电子欺骗是利用主机之间的正常信任关系来发动的。所谓信任关系就是网络上存在两台主机 X 和 Y，Y 可以利用远程登录工具（如 Telnet、Rlogin），无需口令验证就可以登录到 X 主机上，这依靠 X 对 Y 的 IP 地址的验证。如果 X 允许 Y 登录并且提供服务是基于对主机 Y 的 IP 地址的信任。如果一个攻击者冒充 Y，伪造 Y 的 IP 地址，也可以使用远程登录工具访问 X，这样 IP 电子欺骗攻击就发生了。

IP 攻击的全过程如下：

1）选定一个目标主机，比如 X。其次，信任模式已被发现，并找到了一个被目标主机信任的主机，比如 Y。

2）发现被信任的主机 Y，首先使其丧失工作能力，以使其不能接收到任何有效的网络数据，否则会被揭穿。采用的办法是拒绝服务攻击等。

3）攻击者伪装成被信任的主机 Y，同时建立起与目标主机基于 IP 地址验证的应用连接。如果连接成功，攻击者可以使用一种简单的命令设置一个系统后门，以进行非授权操作。

4.3.4　保护口令安全

1. 口令安全概述

口令是访问控制最简单而有效的方法。只要口令保持机密，非授权用户就无法使用该账号。目前，通过口令进行身份认证是实现计算机安全的主要手段之一。一个用户的口令被非法获取，则该非法用户就获得了该用户的全部权限，对于高权限用户来说，主机和网络也失去了安全性。黑客攻击目标系统时，常常把破译普通用户的口令作为攻击的开始，采用字典穷举法进行口令破解。

人们习惯于将口令称为密码。其实，这两者之间还是有所差别的。一般来说，口令比较简单，随便；而密码则不一样，它要正式一些，也要复杂一些。如果针对一台计算机系统上的账号而言，密码是一个变量，而口令则是一个常量。

利用口令作为身份验证是一种常用的基本手段，使用口令也面临着许多安全问题。在 Internet 上，由于系统没有口令或者口令设置的不科学、太简单，从而使得系统被入侵的情况数不胜数。攻击者企图得到系统的口令文件，从口令文件中可以破译出一些口令和用户名，便于以后冒充合法的用户访问这台主机，一旦发现系统的口令文件被非法访问过，一定要更换所有的口令。当在计算机网络上使用口令身份认证的时候，口令很容易被网络监听到，这样就得考虑口令加密的方法。当无法实现加密的时候，就必须保证在网上传输的口令是一次性口令。因为一次性口令即使被人监听了也没有关系。

2. 不安全口令产生的原因分析

安全的口令是那些很难猜测的口令。它们通常不仅由大小写字母组成，还有数字、字符、标点符号、控制字符和空格等，而且毫无规律排列。口令的长度至少是 8 个字符以上，以使破解的难度更大。

不安全的口令通常是名字，包括人名、宠物名、公司名、甚至幻想中的事物的名字，还有一些特殊的号码，如生日、纪念日、身份证号、手机号码等，这些信息是很容易被人获得的，也是极不安全的。产生不安全口令有几个方面的原因：一是人们通常认为好记忆的口令就是好口令，设置复杂的口令不容易记住还觉得麻烦，这些人设置口令的原则就是简单好记好用，所以通常是将自己或家人的生日、有纪念意义的日子作为口令；二是人们对口令安全的重视程度不够，麻痹大意。人人都知道口令很重要，但是要设置一个复杂的口令就觉得麻烦，还是方便记忆为好，这就让黑客有了可乘之机。

3. 安全口令的设置方法

在建立口令时，最好遵循如下的原则：

1）尽量选择长的口令，口令越长，被破解的可能性就越低。通常一般的系统接受 6 个字符的口令，若选择 6 个字符以上甚至更长的口令，可以增加安全性。

2）口令应该由一些大小写字母、数字、标点符号和一些控制字符等组合而成。

3）对用户口令设置情况进行监测，并强制用户定期改变口令。

4. 怎样保护系统的口令

保护口令安全通常有以下一些经验。

1）不要将口令写下来。

2）不要将口令存放在计算机中或带存储功能的电子设备中。

3）不要选择熟悉事物的名字作为口令。
4）不要使用自己名字、家人的名字、宠物的名字作为口令。
5）不要使用熟悉的数字如生日、纪念日等作为口令。
6）不要将口令轻易告诉任何人。
7）不要在不同的系统中使用同一个口令。
8）不要使用英语单词。
9）不要选择不容易记忆的口令。
10）为防止眼明手快的人窃取口令，在输入口令时应确认无人在身边。
11）对口令文件进行隐藏。

4.4 网络安全技术基础理论

4.4.1 密码技术的基本概念

1. 了解密码技术的重要性

密码技术是网络安全的基础。它来源于密码学。密码学是一门古老而深奥的学科，它以认识密码变换为本质，以加密与解密的基本规律为研究对象。一般人对密码学是陌生的，因为长期以来，它只被应用在军事、外交、情报和保密等部门。随着计算机安全问题的日益突出，密码学逐步被应用于计算机网络，利用现代技术手段对计算机系统中的数据进行加密、解密和变换，形成了很多新的密码技术，如数字签名、身份鉴别技术等，密码技术也得到了前所未有的发展和应用。密码学包括密码编码学和密码分析学。密码编码学研究如何对信息进行编码，使得编码后的信息除指定接收这之外的其他人都不能理解；密码分析学研究如何破译一个密码系统，恢复被隐藏信息的本来面目。由此可见，密码编码学是实现对信息加密的，密码分析学是实现对信息解密的，这两个部分相辅相成，互相促进，是一对形成攻防的矛和盾。人们为了使因特网上的有价值的信息不被窃取或者篡改，选择了数据加密技术和基于加密技术的身份认证。加密在网络上的作用就是防止有价值的信息在网络上被拦截后遭到非法阅读，即使攻击者窃取到了在网络上传输的信息，但是如果他无法破解这一信息，无法获取信息的真实内容，就不会使信息造成泄露。要保证信息在网络上传输的安全性以及真实性、防篡改等，只有依靠强大的密码技术才能实现。

2. 加密和解密的基本概念

下面介绍一些密码技术的基本概念。

1）明文（Plaintext），是信息的原文，未做任何处理的原始状态，一般用 P 或 M 表示。

2）密文（Ciphertext），是明文经过特殊变换后的信息，是难以识别的，一般用 C 表示。

3）加密（Encryption），用某种方法把明文的消息伪装或变换成密文、隐藏明文真实内容的过程称为加密，一般用 E 表示。

4）解密（Decryption），把密文还原成明文真实内容的过程称为解密，是加密的反过程，一般用 D 表示。

5）密码算法（Algorithm），是加密和解密变换的一些公式、法则或程序，多数情况下是一些数学函数。加密时使用的算法叫加密算法；解密时使用的算法叫解密算法。

6）密钥（Key），是进行数据加密或解密时所使用的一种专门信息，一般用 K 表示。加密时使用的密钥为加密密钥；解密时使用的密钥为解密密钥。

7）密码系统，是由密码算法、明文、密文和密钥组成的可加密、解密信息的系统。

8）密码算法的安全性，根据被破译密码的难易程度，不同的密码算法可有不同的安全等级，如果破译密码算法的代价大于加密数据的实际价值，或破译密码算法需要的时间比加密数据保密的时间更长，则可以认为密码算法是安全的。举例说，用一个密码算法加密一个价值在 1 万元的机密信息只需要保密 1 个月的时间便失效了，但是攻击者要破译这个密码算法，他需要花费 5 万元购买计算机设备或软件，而且需要花费 1 年甚至更长的时间才可能破译，这就失去了破译的价值。

4.4.2　密码体制

1. 传统密码技术

数据的表示有多种形式，使用最多的是文字，还有图形、声音和图像等，这些信息在计算机系统中都是以某种编码的方式来存储的。传统密码技术的主要对象是文字书信，其内容都是基于某个字母表，如标准英文字母表、汉语拼音表。而现代密码技术主要是应用于所有在计算机系统中运用的数据，具体是以二进制数据为主。

传统密码技术中的文字信息由字母表中的一个个字母组成，字母表可以按照排列顺序进行一定的编码，例如把英文字母表中 26 个大写字母用数字表示，见表 4-1。

表 4-1　英文字母表及其序号

字母	A	B	C	D	E	F	G	H	I	J	K	L	M	N
数字	1	2	3	4	5	6	7	8	9	10	11	12	13	14
字母	O	P	Q	R	S	T	U	V	W	X	Y	Z		
数字	15	16	17	18	19	20	21	22	23	24	25	26		

大多数加密算法具有数学属性，这种表示方法可以对字母进行算术运算，字母的加减法将形成对应的代数码。如果把字母表看成是循环的，那么字符的运算可以用求模运算（mod）来表示：

$$c = x \bmod n$$

在标准英语字母表中，$n = 26$。如 E + 3 = H 或 L − 3 = I，若采用 $c = (x + 5) \bmod n$，对明文 COMPUTER 进行加密，那么对应的密文应该是 HTRUBYJW。

传统密码技术中还有替代密码、移位密码、一次一密钥密码等，它们是基于分组替代和置换等操作、简单的加模运算等，是传统的密码技术。

2. 对称密钥密码体制

对称密钥密码体制的基本思想是“加密密钥和解密密钥相同或者从其中一个很容易推导出另一个”。使用时两个密钥均需要保密，因此该密码体制也成为单密钥密码体制或私钥密码体制，如图 4-1 所示。

对称密钥密码体制的工作流程是：假定 A 和 B 是通信双方的实体，两者之间的通信需要保密。在通信之前，A 和 B 协商通过某种方式获得一个双方可共用的秘密密钥 K，这个密

钥有且仅有 A 和 B 知道。当 A 和 B 之间进行通信时，他们利用密钥 K 对通信的信息进行加密，接收消息的一方利用该密钥解密信息。除 A 和 B 之外的其他任何用户因为无法获得密钥 K 而无法解密通信信息，从而达到了信息传输保密的目的。

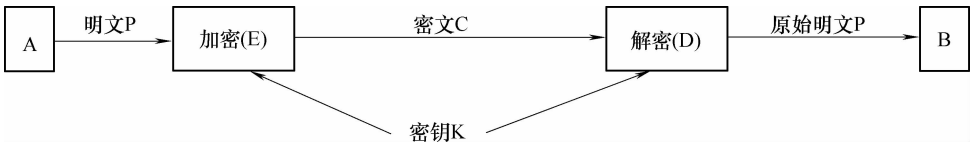


图 4-1　对称密钥密码体制示意图

典型的对称密钥密码算法有 DES、TDEA、IDEA、AES、MD5、RC5 等。

3. 非对称密钥密码体制

非对称密钥密码体制的基本思想是“采用两个不同的密钥来对信息进行加密和解密，并且从其中一个很难推导出另一个”。其中一个密钥是公开的，另一个是保密的。因此，非对称密钥密码体制又称为公开密钥密码体制。通常，在这种密码体制中，加密密钥是公开的，解密密钥是保密的，加密和解密的算法都是公开的，因为密码系统的安全性往往不依赖于对算法的保密而是依赖于对密钥的保密。虽然解密密钥是由公开密钥决定的，而且加密密钥是公开的，但是要从公开密钥中推算出保密的解密密钥是非常困难的，如图 4-2 所示。

图 4-2　公开密钥密码体制示意图

公开密钥密码体制的工作流程是：假定 A 和 B 是通信双方的实体，两者之间的通信需要保密。在通信之前，A 和 B 通过公开密钥算法的计算分别独立拥有一对密钥：A 拥有一个公开密钥和一个私有密钥，B 也拥有一个公开密钥和一个私有密钥，A 和 B 分别将自己的公开密钥公布出去而将自己的私有密钥保密。当 A 和 B 之间进行通信时，他们分别利用对方的公开密钥对通信的信息进行加密，接收消息的一方利用自己的私有密钥解密信息。因为 A 和 B 的私有密钥只有 A 和 B 本人才能拥有，其他任何用户因为无法获得别人的私有密钥，因而无法解密通信信息，从而达到了信息传输保密的目的。

典型的公开密钥密码体制的算法是 RSA。

4. 混合加密方法

对称密钥密码体制的特点是：密码算法简单，加密和解密的速度快。因为对称密钥密码体制在加密和解密时使用同样的密钥，这些密钥需要发送方和接收方分别保存，当通信的实体数增加时，密钥的数量急剧增加。例如网络中有 n 个用户，假设每两用户之间需要进行保密通信，那意味着每两个用户之间需要拥有一个共同的密钥，这样一共需要的密钥总数达到了 $n(n-1)/2$ 个。而且如果每两个用户之间需要进行多次通信，每次通信的密钥需要更新，那么系统中密钥的数量将大量增加，这使得密钥的分配和存储变得十分困难。

与对称密钥密码体制不同，公开密钥密码体制密钥管理方便得多。公开密钥体制要求通

信实体自身只需要拥有一个公开密钥和一个私有密钥组成的密钥对，每一个通信实体将公开密钥发布出去，对于通信实体本身而言，他只需要严格保密自己的私有密钥即可。例如网络中 n 个用户之间的保密通信，系统中只需要保存 $2n$ 个密钥。公开密钥密码体制的缺点是它的运算速度赶不上对称密钥密码体制，因为公开密钥密码体制基于最复杂的数学难题，如大整数的分解、离散对数的难解性等，计算非常复杂。公开密钥密码体制还有一大优点是利用它可以实现数字签名。关于数字签名在下面章节将进一步介绍。

了解了对称密钥密码体制和公开密钥密码体制的优缺点之后，公开密钥密码体制并不能完全取代对称密钥密码体制。在实际应用中，通常采用的方法是混合加密方法，将对称密钥密码体制和公开密钥密码体制的优点结合起来，扬长避短。通常的方法是利用对称密钥密码体制算法的加密/解密速度快的优点可以完成对大批量数据的加密；利用公开密钥密码体制在密钥管理上的优点来分发实现保密通信的秘密密钥。

混合加密方法的基本原理是：首先利用公开密钥密码体制完成两个通信实体之间保密通信需要使用的对称秘密密钥的分发；当两个通信实体得到秘密密钥之后，便可以实现安全的通信。如图 4-3 所示，假定 A 和 B 是通信双方的实体，两者之间的通信需要保密。A 为发送端，B 为接收端。在发送端，A 设计好与 B 实现保密通信的秘密密钥 K，首先用 B 的公开密钥加密密钥 K 发送给 B，然后 A 利用秘密密钥 K 对通信的数据进行加密，加密后发送给 B。在接收端，B 首先将接收到的秘密消息用自己的私有密钥解密，获取到与 A 实现保密通信使用的秘密密钥 K，然后利用密钥 K 解密 A 发送来的大量的通信数据，这样便完成了 A 和 B 之间的保密通信。因为 A 和 B 之间的通信数据量通常很大，用对称密钥算法加密、解密速度快，不会影响通信的效率。而采用公开密钥密码体制完成 A 和 B 之间的保密通信使用的秘密密钥的传输，又保证了通信密钥的安全性，特别是当有多个用户之间需要同时进行保密通信时，采用公开密钥密码体制的优点更明显。

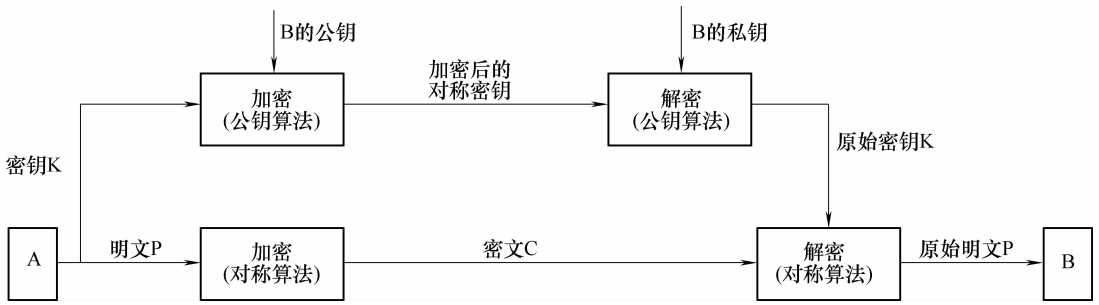


图 4-3　两种密码体制的混合应用

4.4.3　认证技术

认证技术是网络安全中最为重要的技术之一，可以防止他人对系统进行主动攻击，如冒充、伪造、篡改等。认证技术有 3 个目的：

1）验证信息的发送者是真正的，而不是冒充的。

2）验证信息在传送或存储过程中未被篡改、重放或延迟等。

3）验证消息的不可否认性，即防止通信双方事后否认曾经参与过某次活动的行为。

认证技术通常包括两种：消息鉴别和身份认证。消息鉴别是验证消息在传送或存储的过

程中是否被篡改过，判别消息的完整性和真实性；身份认证是核实参与者的真实身份。传统意义下的消息鉴别和身份认证可以通过签章等方式来实现，比如自然人和法人的确立、申报、登记、注册，国家的户籍管理，身份证制度以及西方国家应用个人唯一的社会保险号码来识别人，还可以通过法律对人的行为进行公证、审计和仲裁等。但是进入电子信息社会后，传统的方法已经不适用了。现代的数字认证技术主要是基于前面介绍过的公开密钥密码体制等密码技术来实现的，利用它们设计出的数字签名、身份认证协议等可以解决电子信息世界中的身份认证难题。

1. 消息认证

消息认证主要是确认被传送的内容是否真实，以及消息是否来自真正的发送者，接收者是否准确收到。消息认证的内容包括：消息的来源地是否正确；消息的内容是否真实，是否曾被篡改；消息的序号和时间是否正确。

实现消息认证的方法是采用一种消息摘要或散列函数的密码体制。消息摘要算法是从任意大小的消息中产生固定长度的摘要，这个摘要称为消息摘要，它作为一个附件连同消息一起发送给接收者。接收者在接收到消息后，同样利用消息摘要算法从该消息中产生一个消息摘要，将发送者的摘要与自己产生的消息摘要进行比较，如果两个消息摘要完全吻合，则证明消息在传送过程中没有被篡改；如果不吻合，则说明接收者收到的消息不是发送者发送的真实消息。

消息摘要算法利用的特性是迄今没有一种方法能找到两个摘要相同的消息。虽然摘要是从消息中生成的，它比消息要小得多，但是在很多方面可以看作是与完整消息等同的。最常用的消息摘要算法叫做 MD5，它可以产生一个 128 位长度的摘要。在实际应用中，消息摘要往往需要一定的保护，以免遭到攻击。比如攻击者可能先对消息内容进行篡改，然后从修改过的消息内容中生成一个摘要作为附件连同消息一起发送给接收者，这样接收者很难判断出消息不是原定的发送者发出的。解决这一问题的方法是：发送者在生成消息摘要后，利用接收者的公钥对消息摘要进行加密，这样只有接收者才能用自己的私钥获取消息摘要，防止了攻击者对消息摘要的主动攻击，确保了消息本身的真实性和完整性。

2. 身份认证

身份认证可以定义为：为了使某些授予许可权限的权威机构满意，而提供所要求的用户身份验证的过程。简而言之，身份认证主要是对通信实体的真实身份的核实，一般涉及两个过程：识别和验证。

1）识别是对访问者身份的确认，即要对网络中每个合法用户具有识别能力。要保证识别的有效性，必须保证能代表用户身份的标识符的唯一性。识别信息一般是非秘密的，如用户信用卡号码、用户名、身份证号等。

2）验证就是在确认访问者的身份以后，对其声明的身份进行验证，以防冒充。验证信息一般是秘密的，如用户设置的口令等。

在大多数系统中，用户在他们被允许注册之前必须为其账号指定一个口令，口令的目的就是认证该用户就是他声明的那个人，口令充当了认证用户身份的机制。但是口令很容易被窃取、泄露或者破解，单纯依靠口令的身份认证有时显得单薄无力。于是人们又开始研究了一些更为复杂的认证技术，如生物特征识别技术。计算机安全系统中利用生物特征识别技术已经进行了大量的研究和应用，如指纹识别系统、掌纹识别系统。生物特征识别技术通常是

指某些对人而言是唯一的特征，其中包括指纹手印、声音图像、笔迹甚至人的视网膜血管图像。这些生物识别技术在军事、警方侦察等对控制访问极为严格的场合，用于极为仔细地辨别人员。

4.4.4　PKI 技术

PKI 是“Public Key Infrastructure”的缩写，意为“公钥基础设施”。简单地说，PKI 技术就是一种遵循标准的利用公钥加密技术为电子商务的开展提供一套安全基础平台的技术和规范。PKI 是目前网络安全建设的基础与核心，是电子商务安全实施的基本保障。它是建立在公钥密码体制上的信息安全基础设施，为应用提供身份认证、加密、数字签名、时间戳等安全服务。

随着网络技术和信息技术的发展，电子商务已逐步被人们所接受，并在不断普及。但由于各种原因，国内电子商务的安全性仍不能得到有效的保障。商家和客户通过网上进行电子商务交易时，由于交易双方并不是现场交易，因此，无法确认双方的合法身份，同时交易信息是交易双方的商业秘密，在网上传输时必须保证安全性，防止信息被窃取。双方的交易非现场交易，一旦发生纠纷，必须能够提供仲裁。在电子商务中，必须从技术上保证在交易过程中能够实现身份认证、安全传输、不可否认性、数据完整性。PKI 就是为了解决电子商务安全问题而提出的一种可靠的技术手段。它支持加密传输和数字签名。PKI 已广泛用于保障电子商务的安全，客户可利用 PKI 平台提供的服务进行安全通信。在国内外电子商务中，PKI 得到了广泛的应用。

PKI 的核心部件是数字证书认证中心（Certificate Authority，CA），它的主要任务是数字证书、证书废除列表 CRL 的签发及管理。PKI 采用证书进行公钥管理，通过第三方的可信任机构（认证中心，即 CA），把用户的公钥和用户的其他标识信息捆绑在一起，其中包括用户名和电子邮件地址等信息，以在 Internet 上验证用户的身份。PKI 把公钥密码和对称密码结合起来，在 Internet 上实现密钥的自动管理，保证网上数据的安全传输。

因此，从大的方面来说，所有提供公钥加密和数字签名服务的系统，都可归结为 PKI 系统的一部分，PKI 的主要目的是通过自动管理密钥和证书，为用户建立起一个安全的网络运行环境，使用户可以在多种应用环境下方便地使用加密和数字签名技术，从而保证网上数据的机密性、完整性和有效性。

PKI 作为一组在分布式计算系统中利用公钥技术和 X.509 证书所提供的安全服务，企业或组织可利用相关产品建立安全域，并在其中发布密钥和证书。在安全域内，PKI 管理加密密钥和证书的发布，并提供诸如密钥管理（包括密钥更新、密钥恢复和密钥委托等）、证书管理（包括证书产生和撤销等）和策略管理等功能。PKI 产品也允许一个组织通过证书级别或直接交叉认证等方式来同其他安全域建立信任关系。这些服务和信任关系不能局限于独立的网络之内，而应建立在网络之间和 Internet 之上，为电子商务和网络通信提供安全保障，所以具有互操作性的结构化和标准化技术成为 PKI 的核心。

PKI 在实际应用上是一套软硬件系统和安全策略的集合，它提供了一整套安全机制，使用户在不知道对方身份或分布地很广的情况下，以证书为基础，通过一系列的信任关系进行通信和电子商务交易。

一个典型的 PKI 系统如图 4-4 所示，其中包括 PKI 策略、软硬件系统、证书机构 CA、

注册机构 RA、证书发布系统和 PKI 应用。

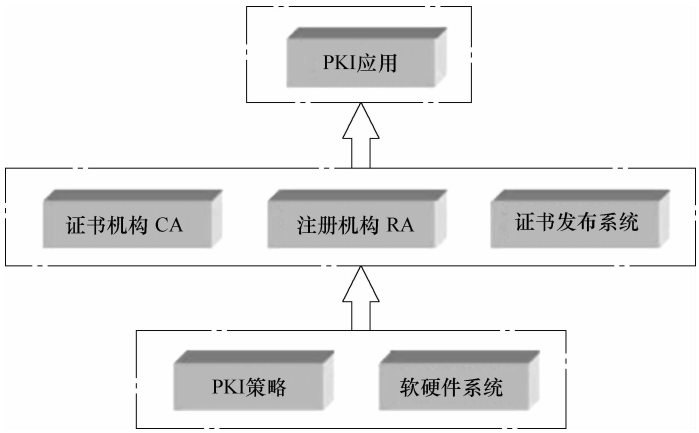


图 4-4　PKI 系统

PKI 安全策略建立和定义了一个组织信息安全方面的指导方针，同时也定义了密码系统使用的处理方法和原则。它包括一个组织怎样处理密钥和有价值的信息，根据风险的级别定义安全控制的级别。一般情况下，在 PKI 中有两种类型的策略：一是证书策略，用于管理证书的使用，比如，可以确认某一 CA 是在 Internet 上的公有 CA，还是某一企业内部的私有 CA；另外一个就是 CPS（Certificate Practice Statement）。一些由商业证书发放机构（CCA）或者可信的第三方操作的 PKI 系统需要 CPS。这是一个包含如何在实践中增强和支持安全策略的一些操作过程的详细文档。它包括 CA 是如何建立和运作的，证书是如何发行、接收和废除的，密钥是如何产生、注册的，以及密钥是如何存储的，用户是如何得到它的，等等。证书机构 CA 是 PKI 的信任基础，它管理公钥的整个生命周期，其作用包括：发放证书、规定证书的有效期和通过发布证书废除列表（CRL）确保必要时可以废除证书。

注册机构 RA 提供用户和 CA 之间的一个接口，它获取并认证用户的身份，向 CA 提出证书请求。它主要完成收集用户信息和确认用户身份的功能。这里指的用户，是将要向认证中心（即 CA）申请数字证书的客户，可以是个人，也可以是集团或团体、某政府机构等。注册管理一般由一个独立的注册机构（即 RA）来承担。它接受用户的注册申请，审查用户的申请资格，并决定是否同意 CA 给其签发数字证书。注册机构并不给用户签发证书，而只是对用户进行资格审查。因此，RA 可以设置在直接面对客户的业务部门，如银行的营业部、机构认证部门等。当然，对于一个规模较小的 PKI 应用系统来说，可将注册管理的职能由认证中心 CA 来完成，而不设立独立运行的 RA。但这并不是取消了 PKI 的注册功能，而只是将其作为 CA 的一项功能而已。PKI 国际标准推荐由一个独立的 RA 来完成注册管理的任务，可以增强应用系统的安全性。

证书发布系统负责证书的发放，如可以通过用户自己，或是通过目录服务器。目录服务器可以是一个组织中现存的，也可以是 PKI 方案中提供的。

PKI 的应用非常广泛，包括在 Web 服务器和浏览器之间的通信、电子邮件、电子数据交换（EDI）、在 Internet 上的信用卡交易和虚拟私有网（VPN）等。

4.5　虚拟专用网络

4.5.1　VPN 的基本概念

虚拟专用网（Virtual Private Network，VPN）是随着 Internet 的发展而迅速发展起来的一种网络应用新技术。在现实世界中，有这样的企业或公司，在全国或全世界都有自己的分公司，除了公司总部有自己的园区网络，每一个分公司分布在各地都有内部的园区网络；还有大量的员工在外地旅行出差或者偶尔在家办公，需要紧急访问公司内部网络进行办公。以往，连接总部 LAN 和分布在各地的分公司 LAN 时，要利用公网 WAN 提供的专线（如 DDN、帧中继、ISDN 等），但是费用较高，而且这种技术不能满足高速率访问内部资源的要求。实际上，公司总部至各个分公司的网络都是相互隔离的，只能通过 Internet 连接在一起，但是它们不能构成一个真正的内部网络。VPN 正是为了解决这样的一个问题而产生的，利用 VPN 能把公司总部和分散在各地的分公司及业务点进行互联。在经济全球化的今天，内部网的网点还将延伸到海外。内部网的广域化成为网络发展的必然趋势。VPN 可使本单位的在外人员像在自己的办公室一样方便地使用内部网。

VPN 被定义为通过一个公共网络（通常是因特网）建立一个临时的、安全的连接，是一条穿过混乱的公共网络的安全、稳定的隧道。VPN 是对企业内部网的扩展。VPN 可以帮助远程用户、公司分支机构、商业伙伴及供应商同公司的内部网络建立可信的安全连接，并保证数据的安全传输。通过将数据流转移到低成本的网络上，一个企业的虚拟专用网解决方案也将大幅度地减少用户花费在城域网和远程网络连接上的费用。同时，这将简化网络的设计和管理，加速连接新的用户和网站。另外，虚拟专用网还可以保护现有的网络投资。随着用户的商业服务不断发展，企业的虚拟专用网解决方案可以使用户将精力集中到自己的生意上，而不是网络上。虚拟专用网可用于不断增长的移动用户的全球因特网接入，以实现安全连接；可用于实现企业网站之间安全通信的虚拟专用线路，用于连接到商业伙伴和用户的安全网络。其应用效果如图 4-5 所示，一个典型的 VPN 可能包括公司总部的局域网、远程分公司或分支机构的其他局域网以及从网络外部连接进来的个人用户。

VPN 可以提供功能认证、加密、隧道化服务。VPN 可以通过特殊加密的通信协议连接到 Internet 上，在位于不同地方的两个或多个企业内部网之间建立一条专有的通信线路，就好比是架设了一条专线一样，但是它并不需要真正地去铺设光缆之类的物理线路。总之，VPN 的核心就是在利用公共网络建立虚拟私有网。

4.5.2　VPN 的工作原理

如何通过 Internet 建立一个虚拟的专用网络？这里面要解决的技术问题主要有加密、认证和隧道技术。最重要的就是隧道技术。隧道技术是 VPN 的基本技术，类似于点对点连接技术，它在公用网建立一条数据通道（隧道），让数据包通过这条隧道传输。隧道是由隧道协议形成的，分为第二、三层隧道协议。第二层隧道协议是先把各种网络协议封装到 PPP 中，再把整个数据包装入隧道协议中。这种双层封装方法形成的数据包靠第二层协议进行传输。第二层隧道协议有 L2F、PPTP、L2TP 等。L2TP 协议是目前 IETF 的标准，由 IETF 融合

PPTP 与 L2F 而形成。VPN 提供了一个隧道，使得在网络上传输的数据包是经过加密处理的，将数据包封装成 IP 包的形式，通过隧道在网上传输，如图 4-6 所示。

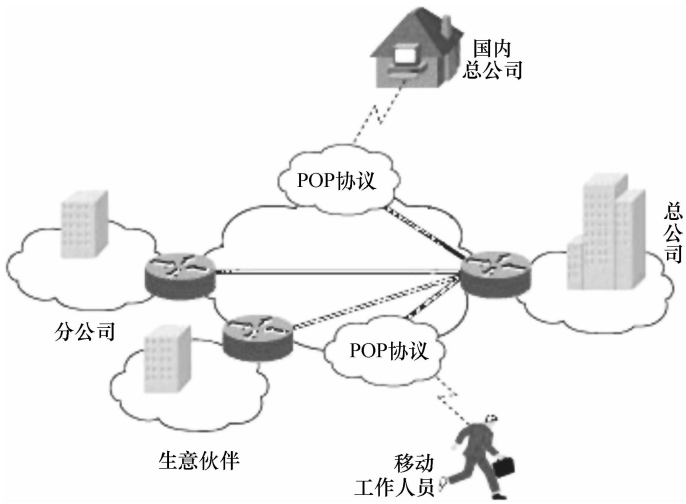


图 4-5　一个典型的 VPN 应用

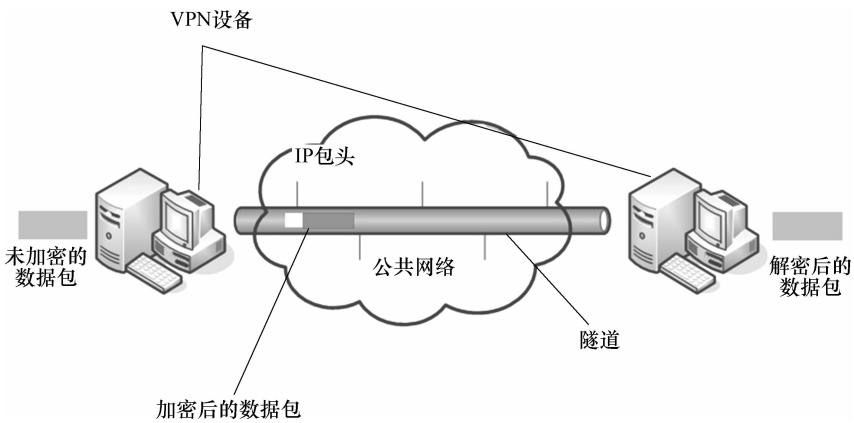


图 4-6　VPN 的工作原理图

4.5.3　VPN 的关键技术和主要协议

1. 实现 VPN 的关键技术

（1）隧道技术

隧道技术（Tunneling）是 VPN 的底层支撑技术，所谓隧道，实际上是一种封装，就是将一种协议（协议 X）封装在另一种协议（协议 Y）中传输，从而实现协议 X 对公用网络的透明性。这里协议 X 被称为被封装协议，协议 Y 被称为封装协议，封装时一般还要加上特定的隧道控制信息，因此隧道协议的一般形式为（（协议 Y）隧道头（协议 X））。在公用网络（一般指因特网）上传输的过程中，只有 VPN 端口或网关的 IP 地址暴露在外边。

隧道解决了专网与公网的兼容问题，其优点是能够隐藏发送者、接收者的 IP 地址以及其他协议信息。VPN 采用隧道技术向用户提供了无缝的、安全的、端到端的连接服务，以

确保信息资源的安全。

隧道是由隧道协议形成的。隧道协议分为第二、第三层隧道协议，第二层隧道协议如 L2TP、PPTP、L2F 等，它们工作在 OSI 体系结构的第二层（即数据链路层）；第三层隧道协议如 IPSec、GRE 等，它们工作在 OSI 体系结构的第三层（即网络层）。第二层隧道和第三层隧道的本质区别在于：用户的 IP 数据包被封装在不同的数据包中在隧道中传输。

第二层隧道协议是建立在点对点协议 PPP 的基础上，充分利用 PPP 协议支持多协议的特点，先把各种网络协议（如 IP、IPX 等）封装到 PPP 帧中，再把整个数据包装入隧道协议。PPTP 和 L2TP 协议主要用于远程访问虚拟专用网。

第三层隧道协议是把各种网络协议直接装入隧道协议中，形成的数据包依靠网络层协议进行传输。无论在可扩充性，还是安全性、可靠性方面，第三层隧道协议均优于第二层隧道协议。IPSec 即 IP 安全协议是目前实现 VPN 功能的最佳选择。

（2）密码技术与认证技术

密码技术是 VPN 的另一核心技术。为了保证数据在传输过程中，不被非法的用户窃取或篡改，一般都在传输之前进行加密，在接收方再对其进行解密。VPN 大都采用单钥的 DES 和 3DES 作为加解密的主要技术，而以公钥和单钥的混合加密体制（即加解密采用单钥密码，而密钥传送采用双钥密码）来进行网络上密钥交换和管理，不但提高了传输速度，还具有良好的保密功能。认证技术可以防止来自第三方的主动攻击。一般用户和设备双方在交换数据之前，先核对证书，如果准确无误，双方才开始交换数据。用户身份认证最常用的技术是用户名和密码方式。而设备认证则需要依赖由 CA 所颁发的电子证书。

目前主要的认证方式有：简单口令如质询握手验证协议 CHAP 和密码身份验证协议 PAP 等；动态口令如动态令牌和 X. 509 数字证书等。简单口令认证方式的优点是实施简单、技术成熟、互操作性好，且支持动态地加载 VPN 设备，可扩展性强。

（3）密钥管理技术

密钥管理的主要任务就是保证在开放的网络环境中安全地传递密钥，而不被窃取。目前密钥管理的协议包括 ISAKMP、SKIP、MKMP 等。Internet 密钥交换协议（Internet Key Exchange，IKE）使用 Internet 安全关联和密钥管理协议（Internet Security Association Key Management Protocol，ISAKMP）来定义密钥的交换，综合了 Oakley 和 SKEME 密钥交换方案，通过协商安全策略，形成各自的验证加密参数。IKE 交换的最终目的是提供一个通过验证的密钥以及建立在双方同意的基础上的安全服务。

IKE 协议是目前首选的密钥管理标准，较 SKIP 而言，其主要优势在于定义更灵活，能适应不同的加密密钥。IKE 协议的缺点是它虽然提供了强大的主机级身份认证，但同时却只能支持有限的用户级身份认证，并且不支持非对称的用户认证。

（4）访问控制技术

虚拟专用网的基本功能就是不同的用户对不同的主机或服务器的访问权限是不一样的。由 VPN 服务的提供者与最终网络信息资源的提供者共同来协商确定特定用户对特定资源的访问权限，以此实现基于用户的细粒度访问控制，以实现对信息资源的最大限度的保护。

访问控制策略可以细分为选择性访问控制和强制性访问控制。选择性访问控制是基于主体或主体所在组的身份，一般被内置于许多操作系统当中。强制性访问控制是基于被访问信息的敏感性。

2. VPN 实现的主要安全协议

VPN 区别于一般网络互联的关键是隧道的建立，数据包经过加密后，按隧道协议进行封装、传送以保证安全性。一般，在数据链路层实现数据封装的协议叫第二层隧道协议，常用的有 PPTP、L2TP 等；在网络层实现数据封装的协议叫第三层隧道协议，如 IPSec。另外，SOCKSv5 协议则在 TCP 层实现数据安全。

（1）PPTP/L2TP

1996 年 Microsoft 和 Ascend 等在 PPP 协议的基础上开发了 PPTP，它集成于 Windows NT Server4. 0 中，Windows NT Workstation 和 Windows 9. X 也提供相应的客户端软件。PPP 支持多种网络协议，可把 IP 、IPX、AppleTalk 或 NetBEUI 的数据包封装在 PPP 包中，再将整个报文封装在 PPTP 隧道协议包中，最后，再嵌入 IP 报文或帧中继或 ATM 中进行传输。PPTP 提供流量控制，减少拥塞的可能性，避免由于包丢弃而引发包重传。PPTP 的加密方法是采用 Microsoft 点对点加密（MPPE：Microsoft Point-to-Point）算法，可以选用较弱的 40 位密钥或强度较大的 128 位密钥。1996 年，Cisco 提出 L2F（Layer 2 Forwarding）隧道协议，它也支持多协议，但其主要用于 Cisco 的路由器和拨号访问服务器。1997 年底，Microsoft 和 Cisco 公司把 PPTP 协议和 L2F 协议的优点结合在一起，形成了 L2TP 协议。L2TP 支持多协议，利用公共网络封装 PPP 帧，可以实现和企业原有非 IP 网的兼容。还继承了 PPTP 的流量控制，支持 MP（Multilink Protocol），把多个物理通道捆绑为单一逻辑信道。L2TP 使用 PPP 可靠性发送（RFC 1663）实现数据包的可靠发送。L2TP 隧道在两端的 VPN 服务器之间采用口令握手协议 CHAP 来验证对方的身份。L2TP 受到了许多大公司的支持。

PPTP/L2TP 协议的优点：PPTP/L2TP 对用微软操作系统的用户来说很方便，因为微软已把它作为路由软件的一部分。PPTP/L2TP 支持其他网络协议。如 NOWELL 的 IPX、NETBEUI 和 APPLETALK 协议，还支持流量控制。它通过减少丢弃包来改善网络性能，这样可减少重传。

PPTP/L2TP 协议的缺点：PM 和 L2TP 将不安全的 IP 包封装在安全的 IP 包内，它们用 IP 帧在两台计算机之间创建和打开数据通道，一旦通道打开，源和目的用户身份就不再需要，这样可能会带来问题，它不对两个节点间的信息传输进行监视或控制。PPTP 和 L2TP 限制同时最多只能连接 255 个用户，端点用户需要在连接前手工建立加密信道，认证和加密受到限制，没有强加密和认证支持。PPTP/L2TP 最适合于远程访问 VPN。

（2）IPSec 协议

IPSec 是 IETF（Internet Engineer Task Force）正在完善的安全标准，它把几种安全技术结合在一起形成一个较为完整的体系，受到了众多厂商的关注和支持。通过对数据加密、认证、完整性检查来保证数据传输的可靠性、私有性和保密性。IPSec 由 IP 认证头 AH（Authentication Header）、IP 安全载荷封载 ESP（Encapsulated Security Payload）和密钥管理协议组成。

IPSec 协议是一个范围广泛、开放的虚拟专用网安全协议。IPSec 适应向 IPv6 迁移，它提供所有在网络层上的数据保护，提供透明的安全通信。IPSec 用密码技术从认证、完整性检查和加密 3 个方面来保证数据的安全。

IPSec 协议可以设置成在两种模式下运行：一种是隧道模式；一种是传输模式。在隧道模式下，IPSec 把 IPv4 数据包封装在安全的 IP 帧中，这样可确保从一个防火墙到另一个防

火墙时的安全性。在隧道模式下，信息封装是为了保护端到端的安全性，即在这种模式下不会隐藏路由信息。隧道模式是最安全的，但会带来较大的系统开销。IPSec 现在还不完全成熟，但它得到了一些路由器厂商和硬件厂商的大力支持。预计它今后将成为虚拟专用网的主要标准。IPSec 有扩展能力以适应未来商业的需要。在 1997 年底，IETF 安全工作组完成了 IPSec 的扩展，在 IPSec 协议中加上 ISAKMP 协议，其中还包括一个密钥分配协议 Oakley。ISAKMP/Oakley 支持自动建立加密信道、密钥的自动安全分发和更新。IPSec 也可用于连接其他层已存在的通信协议，如支持安全电子交易（Secure Electronic Transaction，SET）协议和 SSL（Secure Socket layer）协议。即使不用 SET 或 SSL，IPSec 都能提供认证和加密手段以保证信息的安全传输。

4.5.4　VPN 常见的三种组网类型

1. 基于内部网（Intranet）的 VPN

如果公司有一个或多个远程位置想要加入到一个专用网络中，他们可以建立一个内部网 VPN，以便将局域网（LAN）连接到另一个局域网。内部网是通过公共网络将某一个组织的各个分支机构的局域网联结而成的网络。这种类型的局域网到局域网的联结所带来的风险最小，因为公司通常认为他们的分支机构是可信的，用这种方式联结而成的网络被称为 Intranet，可看作是公司网络的扩展。当一个数据传输通道的两个端点被认为是可信的时候，可以选择内部网 VPN 解决方案。其安全性主要在于加强两个 VPN 服务器之间加密和认证的手段。基于内部网的 VPN 如图 4-7 所示。

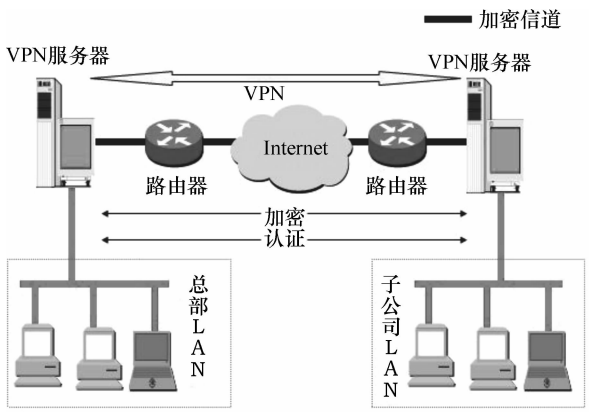


图 4-7　基于内部网的 VPN

2. 基于外联网（Extranet）的 VPN

如果公司同其他公司（例如合作伙伴、供应商或客户）的关系紧密，他们可以建立一个外联网 VPN，以便将局域网连接到另一个局域网，同时让所有公司都能在一个共享环境中工作。外联网 VPN 为公司商业伙伴、客户和在远地的雇员提供安全性保护。外联网 VPN 的主要目标是保证数据在传输过程中不被修改，保护网络资源不受外部威胁，如图 4-8 所示。

外联网 VPN 应是一个由加密、认证和访问控制功能组成的集成系统。通常将公司的 VPN 代理服务器放在一个不能穿透的防火墙之后，防火墙阻止来历不明的信息传输。所有经过过滤的数据通过一个唯一的入口传到 VPN 服务器，VPN 再根据安全策略进一步过滤。

3. 远程访问 VPN

典型的远程访问 VPN 是用户通过本地的信息提供商（ISP）登录到 Internet 上，并在现在的办公室和公司内部网之间建立一条加密通道。有较高安全度的远程访问 VPN 应能截获特定主机的信息流，有加密、身份认证和过滤等功能。这是 VPN 中最为常见的一种应用类型，如图 4-9 所示。

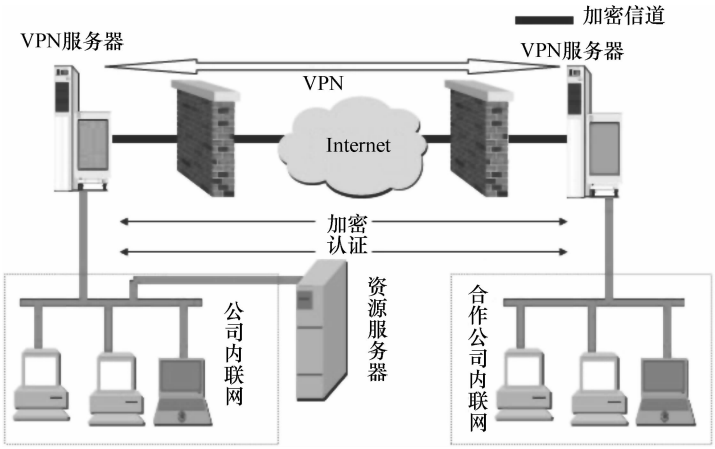


图 4-8　基于外联网的 VPN

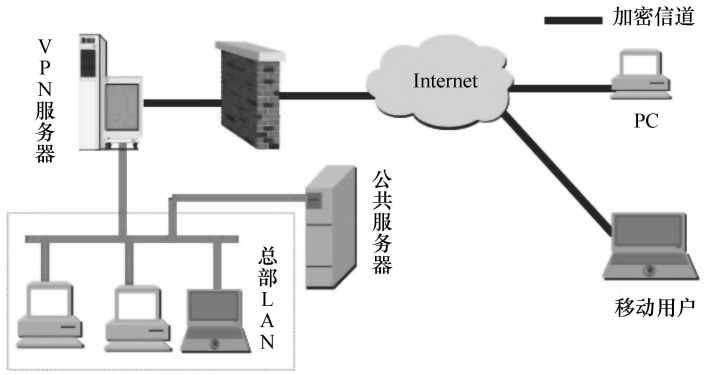


图 4-9　远程访问 VPN

4.5.5　VPN 解决方案

1. IPSec VPN 解决方案

IPSec 基于一组开放的网络安全协议，业务数据流通过 IPSec 加密，IPSec 能够提供服务器及客户端的双向身份认证，并且为 IP 及其上层业务数据提供安全加密保护，能够支持数据加密（包括常见的 DES \ 3DES \ AES 加密算法）、数据完整性验证、数据身份验证以及防重放等功能，充分保证了业务数据的安全性。IPSec VPN 利用 Internet 构建三层隧道 VPN 的方式，可以允许用户以任意方式接入 VPN，并且不受地理因素的限制，无论用户在外地或国外，只需要从当地接入 Internet 即可。IPSec VPN 不仅适用于 SOHO 用户或移动办公用户接入，而且适用于企业分支机构之间的互连互通。正因为 IPSec VPN 具有其他 VPN 不可替代的业务优势，在 VPN 业务较为普及的国外一些国家得到了比较普遍的应用。

本节以杭州华三通信（H3C）公司推出的 IPSec VPN 典型解决方案为例，描述实际使用的 IPSec VPN 的组网方案。H3C 公司提供了一种单链路网关 VPN 组网方案，组网主要是面向部分小型的分支机构，分支用户对于网络的链路要求不高，普通的 ADSL 线路就可以满足基本使用要求；用户也可以通过局域网接入；对于服务器部分，可以只考虑使用单台的设备来进行连接。VPN 客户端设备可以采用静态或动态申请的 IP 地址和总部网关建立 VPN 链

接。根据其业务的需求，对可靠性的要求不高，数据的传输不讲究实时传输。有必要的话，可以在分支节点用设备进行冷备份。其组网方式如图 4-10 所示。

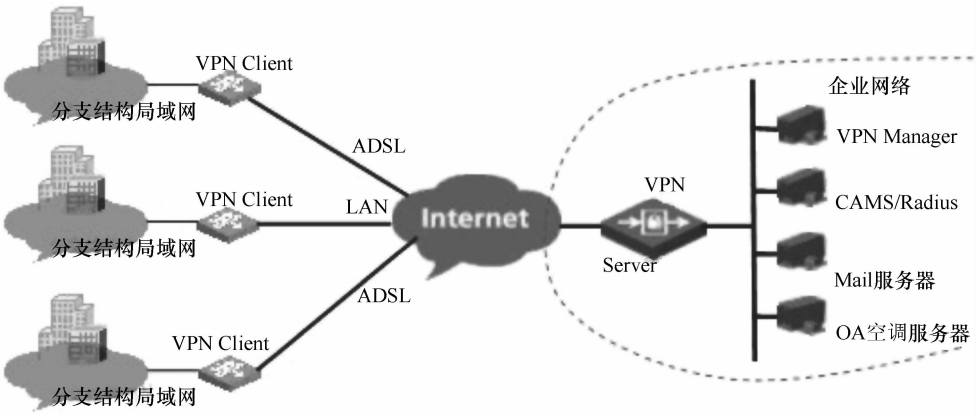


图 4-10　IPSec VPN 组网方式

它的部署方式及特点如下：

1）VPN 接入网关子系统部署：在总部局域网 Internet 边界防火墙后面配置一台专用的高性能的 VPN 网关，在分支机构 Internet 边界防火墙后面配置一台专用 VPN 网关，由此两端的 VPN 网关建立 IPSec VPN 隧道，进行数据封装、加密和传输。

2）VPN 管理子系统部署：在总部局域网数据中心部署 H3C QuidView VPN Manager 组件，实现对 VPN 网关的部署管理和监控；在总部局域网内部或 Internet 边界部署 H3C QuidView BIMS 系统，实现对分支机构 VPN 网关设备的自动配置和策略部署。

3）强大的 VPN 处理性能，高端专用 VPN 网关通过专业的硬件加密处理器可以提供标准加密算法下 350Mbit/s 以上的加密吞吐量，百兆 VPN 网关通过专业的硬件加密处理器可以提供标准加密算法下 60Mbit/s 以上的加密吞吐量。

4）提供图形化界面的 VPN 管理工具 VPN Manager 以及自动部署系统 BIMS 分支智能管理系统，实现 VPN 可视化的 VPN 部署管理以及大规模的自动部署能力。

5）VPN 客户端设备相对来说比较简单。

6）VPN 客户端可以使用动态地址接入服务器，但为了防止客户端 IPSec 配置泄露造成的安全隐患，建议 VPN 客户端口采用静态地址。同时，这样也便于使用 VPN Manager 的配置管理功能。

7）由于 IPSec 不能承载路由协议，需要在分支结构和园区网配置大量的静态路由。

8）单纯的 IPSec 封装，对于带宽资源消耗较小。

2. SSLVPN 解决方案

在 IPSecVPN 之后，又一种 VPN 技术逐渐成为了主流，即基于应用层的 SSLVPN 技术。

近年来，移动办公已成为趋势，移动用户接入公司内部专网的需求不断增加，使得 IPSecVPN 的使用也逐渐增加。但由于 IPSecVPN 存在维护和扩展的困难，造成企业后期 IT 成本过高；另一方面，企业对于内网资源的保护的要求也不断提高，IPSecVPN 由于开放了整网的资源给接入用户，企业内网安全方面的问题逐渐暴露。

鉴于 IPSecVPN 应用中存在的不足，基于应用层的 SSLVPN 开始迅速兴起。SSL 的英文

全称是“Secure Sockets Layer”，中文名为“安全套接层协议”，它是网景（Netscape）公司提出的基于 Web 应用的安全协议。是一种基于应用层的虚拟专网技术，它利用 SSL 技术和代理技术，向终端用户提供安全访问 HTTP 资源、C/S 资源，以及文件共享资源等功能，同时可以实现不同方式的用户认证，以及细粒度的访问控制。通过该技术的应用可真正实现“在任何时候、任何地点、通过任何设备安全地接入公司内部网”的目标。

SSL VPN 技术应用具有以下特点：

1）适合点对网的连接。

2）无需手动安装任何 VPN 客户端软件。

3）兼容性好，支持各种操作系统和终端，不会与终端防火墙、杀毒软件冲突。

4）细致的访问权限控制。

以深信服科技推出的 SSL VPN 典型解决方案为例，描述 SSL VPN 的组网方案。某企业总部需要对各省市分支机构进行业务管理，应用都是基于互联网的 Web 应用软件。企业总部的领导、业务人员需要经常出差，移动办公需求急剧增加。总部员工不仅需要在单位局域网内访问 OA、邮件系统、业务系统等网络资源，在外出差期间他们同样需要安全便捷地接入总部局域网访问相关办公系统。为更进一步提高工作人员的工作效率，有效地解决数据传输中的通道安全、数据安全、接入安全等问题，实现现有邮件系统的安全访问，总部网络管理者考虑通过采用 VPN 接入的方式来实现工作人员对内网邮件系统的安全访问和操作，要求对访问、邮件接收都达到高级别的安全性和稳定性。

深信服 SSL VPN 身份认证的安全性、数据传输的速度、接入操作的易用性较好。企业选择部署两台深信服千兆级 SSL VPN 设备，为远程接入构建了安全高效的接入平台。同时考虑到线路稳定性、设备稳定性等因素，企业总部以双机热备的方式实现系统连接，保障即使一条线路出现故障也能实现远程移动办公接入。并且还引入了深信服独有的多因素身份认证方式，实现了静态认证和动态认证的混合模式身份认证体系，这样保证了所有员工接入总部内网时，可以做到完备的身份安全认证。其组网方式如图 4-11 所示。

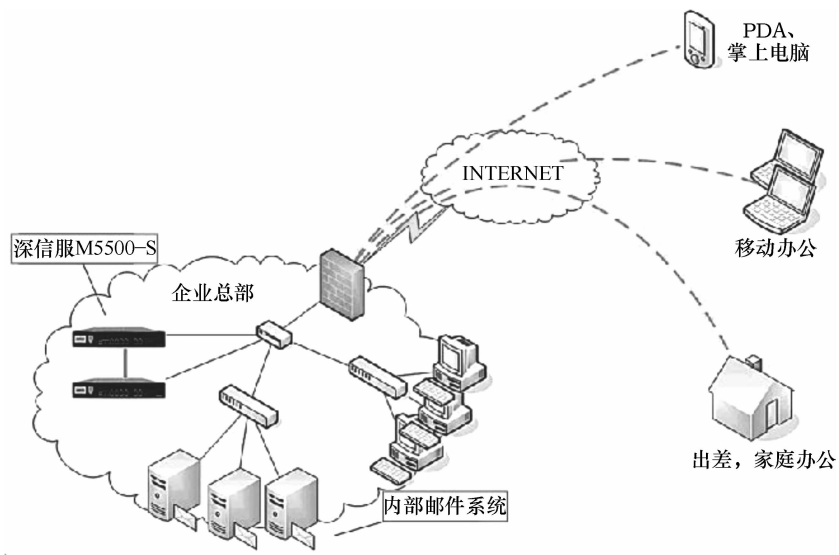


图 4-11　某企业总部部署 SSL VPN 组网方式

该方案具有如下特点：

1）通过 SSL VPN，远程办公和移动用户可以随时访问内部办公平台，获取、提交信息非常便捷。

2）SSL VPN 提供目前最丰富的认证，包括 USB Key、短信口令、软键盘、动态令牌、CA、硬件特征码等，在最大程度上确保接入用户身份的合法性。

3）SSL VPN 能够对内网的访问权限进行细致地设定，对不同的用户分配不同的权限规则，避免内部出现安全隐患。

4）操作简易，支持多种部署模式，不会对现有网络造成任何影响，各种服务及应用均可正常使用，与各种 IT 办公系统结合良好。

4.6　防火墙技术

4.6.1　防火墙的基本概念

防火墙作为网络安全的一种防护手段得到了广泛的应用，并对网络起到了一定的保护作用。

防火墙来源于古代的建筑物防火墙的概念：为了保护建筑物内部财物的安全，建立一座高大的墙体以遮挡、躲避来自于建筑物之外的火灾。古代的护城河也是一种防火墙，保护城内以免遭到外部的攻击。后来这种思想被引入到计算机网络中，主机不断遭到外部网络上的其他主机的攻击，为了抵御这种攻击，防止外部危害入侵到内部网络，创建了计算机网络防火墙，其在网络中的位置如图 4-12 所示。

图 4-12　防火墙在网络中的位置

计算机网络防火墙是设置在内部网络和外部网络之间的一道屏障，它就像内部网络入口的“哨兵”，检查每一个从外部网络进入内部网络的访问者，目的是保护内部网络不受外部网络的侵扰。

防火墙是位于内部网络或 Web 站点与因特网之间的一个路由器或一台计算机，又称为堡垒主机。它是在两个网络之间执行访问控制策略的一个或一组系统，包括硬件和软件，它能够对每一个进入内部网络的访问执行检查，就像是安装在两个网络之间的一道栅栏，能够允许或阻止每一个访问，它提供的是一种过滤机制，提供可控的过滤网络通信，只允许授权的通信。

4.6.2 防火墙的基本功能

一般来说，防火墙可防止来自“外部”未经授权的交互式登录，这将有助于防止破坏者登录到网络用户的计算机上。另一方面，防火墙还充当了外部网络和内部网络连接的一个“阻塞点”，可以在“阻塞点”上设置安全和审计检查，定期系统安全向管理员提供一些情况概要，提供有关通过防火墙的数据流的类型和数量，以及有多少次试图闯入防火墙的信息。

防火墙具有以下基本功能：

1. 防火墙充当内部网络的安全保护屏障

防火墙是信息进出网络的必经之路。可以说，如果切断防火墙，就可以保护内部网络用户免受网络上的任何类型的攻击。防火墙会检查所有经过的数据的细节，它会根据系统预先定义好的安全策略或安全规则允许或禁止这些数据流的通过，这将极大地提高内部网络的安全性。

2. 防火墙能够强化网络安全策略

前面我们学习过网络安全策略的概念，它体现了一个单位的安全政策，为什么要采用防火墙？需要防范哪些威胁？哪些活动是被允许的？哪些活动需要被禁止？解决这些问题需要采用防火墙技术，它是能够帮助一个单位实施网络安全策略的重要技术保障之一。

3. 防火墙能够对网络访问进行监控和审计

所有经过网络进出的信息都必须通过防火墙，因此防火墙能够记录下这些访问的来源、时间等信息，还能够对被保护网络与外部网络之间的事件做出日志记录，同时向系统管理员提供网络使用情况的统计数据。通过对这些数据信息的统计分析，它还能够提供预警功能，对内部网络受到可疑的行为或者攻击企图等信息的统计结果有助于系统管理员做出适当的反应，以保障网络的安全。

4. 防火墙能够限制暴露内部网络的信息

可以利用防火墙对内部网络实现网段的划分，对内部网络中重点网段进行隔离，从而限制局部重点或敏感的网络安全问题对整个网络造成影响。在内部网络中，比如一些重要的服务器，如数据库服务器、Web 服务器等，极易受到来自外部网络的攻击，而防火墙的隔离限制了内部网络的结构等信息的暴露，使得外部网络的攻击者不易发现这些特别重要的服务器资源。

5. 防火墙是一个安全策略的检查站

所有进出网络的信息必须通过防火墙，因此防火墙成为了网络上的一个检查站，对于来自外部的网络进行检测和报警，将发现的可疑访问拒之门外。

4.6.3 防火墙的实现技术

防火墙产品主要采用数据包过滤与代理两种实现技术。这两种技术各有优缺点，有时将这两种技术混合起来使用。在这些基本技术上，又衍生出一些新的技术如状态检测技术、深度检测技术、自适应代理技术等。

1. 数据包过滤技术

数据包过滤是防火墙最基本的过滤技术，在网络层实现。这种类型的防火墙根据定义好

的过滤规则审查每个数据包，以便确定其是否与某一条数据包过滤规则匹配。过滤规则基于数据包的报头信息进行制定，报头信息中包括 IP 源地址、IP 目标地址、传输协议（TCP、UDP、ICMP 等）、TCP/UDP 目标端口、ICMP 消息类型等。数据包过滤类型的防火墙要遵循的一条默认的原则是“未经允许即为拒绝”，即明确允许哪些是可以通过防火墙的数据包，其他未经允许的全部被禁止。

数据包过滤技术是一种简单、有效的安全控制技术，它通过在网络间相互连接的设备上加载允许、禁止来自某些特定的源地址、目的地址、TCP 端口号等规则，对通过设备的数据包进行检查，限制数据包进出内部网络。数据包过滤的最大优点是对用户透明，传输性能高。但由于安全控制层次在网络层、传输层，安全控制的力度也只限于源地址、目的地址和端口号，因而只能进行较为初步的安全控制，对于恶意的拥塞攻击、内存覆盖攻击或病毒等高层次的攻击手段，则无能为力。

状态检测是比数据包过滤更为有效的安全控制方法。对新建的应用连接，状态检测检查预先设置的安全规则，允许符合规则的连接通过，并在内存中记录下该连接的相关信息，生成状态表。对该连接的后续数据包，只要符合状态表，就可以通过。这种方式的好处在于：由于不需要对每个数据包进行规则检查，而是一个连接的后续数据包（通常是大量的数据包）通过散列算法，直接进行状态检查，从而使得性能得到了较大提高；而且，由于状态表是动态的，因而可以有选择地、动态地开通 1024 号以上的端口，使得安全性得到进一步的提高。

2. 代理技术

代理防火墙也叫应用层网关防火墙。这种防火墙通过一种代理（Proxy）技术参与到一个 TCP 连接的全过程。从内部发出的数据包经过这样的防火墙处理后，就好像是源于防火墙外部网卡一样，从而可以起到隐藏内部网结构的作用。

代理服务器，是指代表客户处理服务器连接请求的程序。当代理服务器得到一个客户的连接请求时，它们将核实客户请求，并经过特定的安全化的代理应用程序处理连接请求，将处理后的请求传递到真实的服务器上，然后接收服务器应答，并做进一步处理后，将答复交给发出请求的最终客户。代理服务器在外部网络向内部网络申请服务时发挥了中间转接的作用。

代理类型的防火墙的最突出的优点就是安全。由于每一个内外网络之间的连接都要通过 Proxy 的介入和转换，通过专门为特定的服务如 Http 编写的安全化的应用程序进行处理，然后由防火墙本身提交请求和应答，没有给内外网络的计算机以任何直接会话的机会，从而避免了入侵者使用数据驱动类型的攻击方式入侵内部网。

代理防火墙的最大缺点就是速度相对比较慢，当用户对内外网络网关的吞吐量要求比较高时（比如要求达到 75 ~ 100Mbit/s 时），代理防火墙就会成为内外网络之间的瓶颈。

自适应代理技术是最近在商业应用防火墙中实现的一种革命性的技术。它可以结合代理类型的防火墙的安全性和数据包过滤防火墙的高速度等优点，在毫不损失安全性的基础之上将代理型防火墙的性能提高 10 倍以上。组成这种类型的防火墙的基本要素有两个：自适应代理服务器与动态数据包过滤器。

在自适应代理与动态数据包过滤器之间存在一个控制通道。在对防火墙进行配置时，用户仅仅将所需要的服务类型、安全级别等信息通过相应 Proxy 的管理界面进行设置就可以

了。然后，自适应代理就可以根据用户的配置信息，决定是使用代理服务从应用层代理请求还是从网络层转发包。如果是后者，它将动态地通知数据包过滤器增减过滤规则，满足用户对速度和安全性的双重要求。

4.6.4 防火墙的分类

防火墙的分类有很多种方法，通常以软硬件构成来划分。按防火墙软、硬件形式可分为软件防火墙和硬件防火墙以及芯片级防火墙。

1. 软件防火墙

软件防火墙又称个人防火墙，运行于特定的计算机上，它需要客户预先安装好的计算机操作系统的支持，一般来说这台计算机就是整个网络的网关。如美国飞塔公司的 Web 应用防火墙、天网防火墙、瑞星防火墙等。

2. 硬件防火墙

硬件防火墙是区别于专用处理芯片的防火墙。硬件防火墙是把软件防火墙嵌入在硬件中，一般的软件安全厂商所提供的硬件防火墙便是在硬件服务器厂商定制硬件，然后再把 Linux 系统与自己的软件系统嵌入其中。这些硬件主要运行一些经过裁剪和简化的操作系统，最常用的有老版本的 Unix、Linux 和 FreeBSD 系统。传统硬件防火墙一般至少应具备 3 个端口，分别接内网、外网和 DMZ 区（非军事化区）。

3. 芯片级防火墙

芯片级防火墙基于专门的硬件平台。专有的 ASIC 芯片促使它们比其他种类的防火墙速度更快，处理能力更强，性能更高。一些具有代表性的厂商有 FortiNet（飞塔）、Juniper（瞻博）、Cisco（思科）等。这类防火墙由于是专用 OS（操作系统），因此防火墙本身的漏洞比较少。

4.6.5 防火墙的应用与发展趋势

今天互联网快速发展，信息资源和基础设施形成了现代企业的核心。部署了网络的企业不但能提高业务效率和业绩，还能获得持续竞争优势。但是，网络也会给企业带来风险。目前，不仅网络攻击数量不断攀升，而且攻击的水平也越来越高，致使各机构核心业务面临的风险越来越大。因此，部署防火墙已经成为一个企业必不可少的基础设施。如图4-13，是思科公司设计的一种防火墙在整个企业中的部署架构示意图。

防火墙正在朝着一体化安全网关、多功能方向发展。这类防火墙可以被认为是一种复合型防火墙，不仅在硬件芯片上有很大的提高，在软件算法上也有一些新的突破。当前业界推出的一些包含了状态检测、深度包检测、透明代理的新一代技术的防火墙，进一步基于 ASIC 架构或 X86 架构，把防病毒、内容过滤整合到防火墙里，其中还包括 NAT、路由策略、VPN、入侵检测系统、入侵防御系统、防病毒网关等功能，形成了一体化的安全网关。

业界一些著名的防火墙集成产品主要有思科公司推出的 PIX 防火墙；瞻博公司推出的 ISG、SSG、SRX 等系列产品；阿姆瑞特公司推出的 F500、F1800、F5500 等系列产品；飞塔公司推出的统一安全网关（UTM）系列产品，如图 4-14 所示。

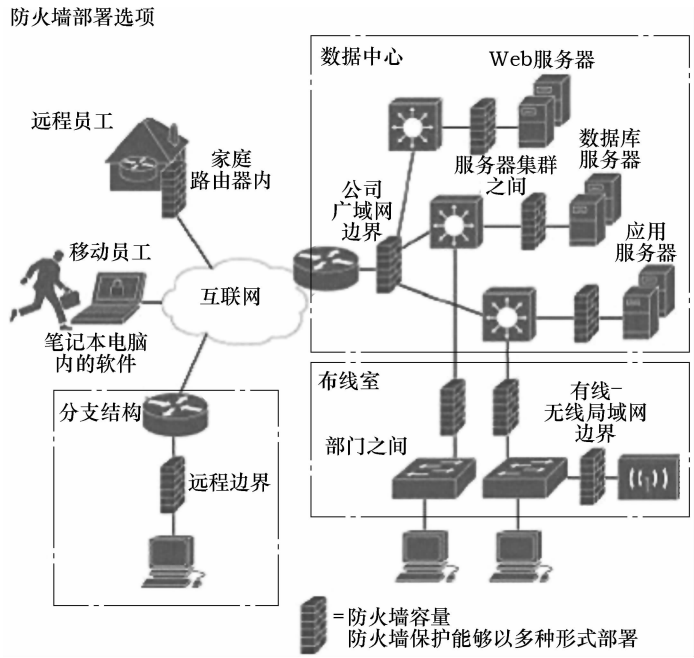


图 4-13　企业防火墙部署应用

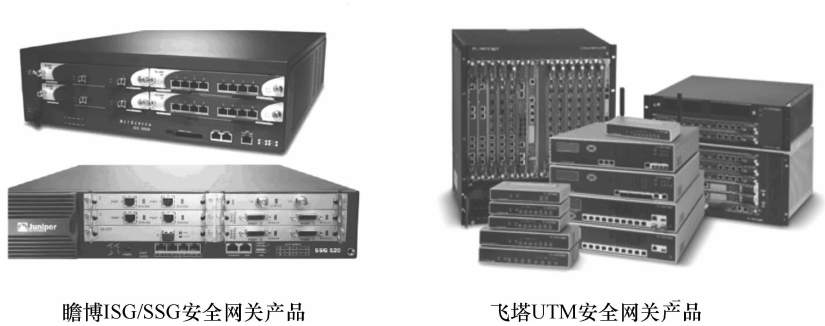


图 4-14　防火墙产品

4.7　入侵检测系统

入侵是指试图破坏信息系统的完整性、机密性、可信性的任何网络活动。防范攻击者入侵最常用的方法就是使用防火墙。防火墙是设置在不同网络（如可信任的企业内部网和不可信任的公共网）或网络安全域之间的一系列部件的组合，其作用是为了保护与互联网相连的企业内部网络或单独节点。它具有简单实用的特点，并且透明度高，可以在不修改原有网络应用系统的情况下达到一定的安全要求。但是，防火墙只是一种被动防御性的网络安全工具，仅仅使用防火墙是不够的。首先，入侵者可以找到防火墙的漏洞，绕过防火墙进行攻击。其次，防火墙对来自内部的攻击无能为力。它所提供的服务方式是要么都拒绝，要么都通过，而这是远远不能满足用户复杂的应用要求的。入侵检测是防火墙的合理补充，帮助系统对付网络攻击，扩展了系统管理员的安全管理能力（包括安全审计、监视、进攻识别和

响应），提高了信息安全基础结构的完整性。入侵检测被认为是防火墙之后的第二道安全闸门，在不影响网络性能的情况下能对网络进行监测，从而提供对内部攻击、外部攻击和误操作的实时保护。相对于防火墙而言，它是一种积极主动的安全防护技术。

4.7.1 入侵检测系统的基本概念及功能

入侵检测（Intrusion Detection），顾名思义，就是对入侵行为的发觉，即识别针对计算机或网络资源的恶意企图和行为，并对此做出反应的过程。它通过对计算机网络或计算机系统中的若干关键点收集信息并对其进行分析，从中发现网络或系统中是否有违反安全策略的行为和被攻击的迹象。

入侵检测系统（Intrusion Detection System，IDS），就是进行入侵检测的软件与硬件组成的独立系统。它能够检测未授权对象（人或程序）针对系统的入侵企图或行为，同时监控授权对象对系统资源的非法操作。与其他安全产品不同的是，入侵检测系统需要更智能，它必须可以将得到的数据进行分析，并得出有用的结果。一个合格的入侵检测系统能大大地简化管理员的工作，保证网络安全的运行。

入侵检测系统具有以下功能：

1）监视、分析用户及系统活动。

2）系统构造和弱点的审计。

3）识别反映已知进攻的活动模式并向相关人士报警。

4）异常行为模式的统计分析。

5）评估重要系统和数据文件的完整性。

6）操作系统的审计跟踪管理，并识别用户违反安全策略的行为。

4.7.2 入侵检测系统的工作原理

1. 工作原理

对一个成功的入侵检测系统来讲，它不但可使系统管理员时刻了解网络系统（包括程序、文件和硬件设备等）的任何变更，还能给网络安全策略的制订提供指南。而且，入侵检测的规模还应根据网络威胁、系统构造和安全需求的改变而改变。入侵检测系统在发现入侵后，会及时做出响应，包括切断网络连接、记录事件和报警等。

2. 入侵检测的步骤

入侵检测系统完成入侵检测功能通常需要两个步骤。

（1）信息收集

入侵检测的第一步是信息收集，内容包括系统、网络、数据及用户活动的状态和行为。而且，需要在计算机网络系统中的若干不同关键点（不同网段和不同主机）收集信息，这除了尽可能扩大检测范围外，还有重要的一点就是从一个源来的信息有可能看不出疑点，但从几个源来的信息的不一致性却是可疑行为或入侵的最好标识。当然，入侵检测很大程度上依赖于收集信息的可靠性和正确性，因此，很有必要只利用所知道的真正的和精确的软件来报告这些信息。因为黑客经常替换软件以搞混和移走这些信息，例如替换被程序调用的子程序、库和其他工具。黑客对系统的修改可能使系统功能失常但看起来跟正常的一样。因此需要保证用来检测网络系统的软件的完整性，特别是入侵检测系统软件本身应具有相当强的坚

固性，防止被篡改而收集到错误的信息。

入侵检测利用的信息一般来自以下 4 个方面：

1）系统和网络日志文件：黑客经常在系统日志文件中留下他们的踪迹，因此，充分利用系统和网络日志文件信息是检测入侵的必要条件。日志中包含发生在系统和网络上的不寻常和不期望的活动的证据，这些证据可以指出有人正在入侵或已成功入侵了系统。通过查看日志文件，能够发现成功的入侵或入侵企图，并很快启动相应的应急响应程序。

2）目录和文件中的不期望的改变：网络环境中的文件系统包含很多软件和数据文件，包含的重要信息的文件和私有数据文件经常是黑客修改或破坏的目标。目录和文件中的不期望的改变（包括修改、创建和删除），特别是那些正常情况下限制访问的，很可能就是一种入侵产生的指示和信号。黑客经常替换、修改和破坏他们获得访问权的系统上的文件，同时为了隐藏系统中他们的表现及活动痕迹，都会尽力去替换系统程序或修改系统日志文件。

3）程序执行中的不期望行为：网络系统上的程序执行一般包括操作系统、网络服务、用户启动的程序和特定目的的应用，例如数据库服务器。每个在系统上执行的程序由一到多个进程来实现。每个进程执行在具有不同权限的环境中，这种环境控制着进程可访问的系统资源、程序和数据文件等。一个进程出现了不期望的行为可能表明黑客正在入侵你的系统。黑客可能会将程序或服务的运行分解，从而导致它失败，或者是以非用户或管理员意图的方式操作。

4）物理形式的入侵信息：这包括两个方面的内容，一是未授权的对网络硬件的连接；二是对物理资源的未授权访问。黑客会想方设法去突破网络的周边防卫，如果他们能够在物理上访问内部网，就能安装他们自己的设备和软件。依此，黑客就可以知道网上的由用户加上去的不安全（未授权）设备，然后利用这些设备访问网络。例如，用户在家里可能安装 Modem 以访问远程办公室，与此同时黑客正在利用自动工具来识别在公共电话线上的 Modem，如果一拨号访问流量经过了这些自动工具，那么这一拨号访问就成为了威胁网络安全的后门。黑客就会利用这个后门来访问内部网，从而越过了内部网络原有的防护措施，然后捕获网络流量，进而攻击其他系统，并偷取敏感的私有信息等。

（2）信息分析

通过收集与入侵有关的系统、网络、数据及用户活动的状态和行为等信息，一般通过模式匹配、统计分析和完整性分析等三种技术手段进行分析。其中，前两种方法用于实时的入侵检测，而完整性分析则用于事后分析。

1）模式匹配：模式匹配就是将收集到的信息与已知的网络入侵和系统误用模式数据库进行比较，从而发现违背安全策略的行为。该方法的一大优点是只需收集相关的数据集合，显著减少了系统负担，且技术已相当成熟。它与病毒防火墙采用的方法一样，检测的准确率和效率都相当高。但是，该方法存在的缺点是需要不断升级以对付不断出现的黑客攻击手法，不能检测到从未出现过的黑客攻击手段。

2）统计分析：统计分析方法首先给系统对象（如用户、文件、目录和设备等）创建一个统计描述，统计正常使用时的一些测量属性（如访问次数、操作失败次数和延时等）。测量属性的平均值将被用来与网络、系统的行为进行比较，任何观察值在正常值范围之外时，就认为有入侵发生。例如，统计分析可能标识一个不正常行为，因为它发现一个在晚八点至早六点不登录的账户却在凌晨两点试图登录。其优点是可检测到未知的入侵和更为复杂的入

侵，其缺点是误报、漏报率高，且不适应用户正常行为的突然改变。这种方法完全取决于统计分析方法，目前采用了很多人工智能的统计分析方法。

3）完整性分析：完整性分析主要关注某个文件或对象是否被更改，这经常包括文件和目录的内容及属性。完整性分析利用强有力的加密机制，称为消息摘要函数（例如 MD5），它能识别哪怕是微小的变化。其优点是不管模式匹配方法和统计分析方法能否发现入侵，只要是成功的攻击导致了文件或其他对象的任何改变，它都能够发现。其缺点是一般以批处理方式实现，不适用于实时响应。

4.7.3 入侵检测系统的分类

现有入侵检测系统的分类，大都基于信息源和分析方法进行分类。

1. 按信息源分类

信息源是入侵检测信息收集的来源，这些来源成为了入侵检测的对象，可以分为基于主机型和基于网络型两大类，也包括基于主机和基于网络的混合模式的入侵检测系统。

（1）基于主机的入侵检测系统（HIDS）

基于主机的 HIDS 通常是被安装在被重点检测的主机上，往往以系统日志、应用程序日志、Windows NT 下的安全记录以及 Unix 环境下的系统记录等作为数据源，也可以通过其他手段（如监督系统调用）从所在的主机收集信息进行分析。当发现系统中文件被修改时，HIDS 将新的记录条目与已知的攻击特征相比较，看它们是否匹配。如果匹配，就会向系统管理员报警或者做出适当的响应。

● 优点：监视所有系统的行为；系统误报率低，检测数据流简单，系统简单；适应交换和加密；不需要额外硬件。对分析“可能的攻击行为”非常有用。举例来说，有时候它除了指出入侵者试图执行一些“危险的命令”之外，还能分辨出入侵者干了什么事：他们运行了什么程序、打开了哪些文件、执行了哪些系统调用。

● 缺点：看不到网络活动状况；运行审计功能需要占用系统资源；对入侵行为的分析的工作量将随着主机数目增加而增加。主机入侵检测系统的缺点是它依赖于服务器固有的日志与监视能力。

（2）基于网络的入侵检测系统（NIDS）

NIDS 通常被设置在比较重要的网段内，以网络包作为分析数据源。NIDS 能够检测那些来自网络的攻击，它能够检测到超过授权的非法访问。它通常利用一个工作在混杂模式下的网卡来实时监视并分析通过网络的数据流。它的分析模块通常使用模式匹配、统计分析等技术来识别攻击行为。一旦检测到了攻击行为，NIDS 的响应模块就做出适当的响应，比如报警、切断相关用户的网络连接等。目前，大部分入侵检测系统的产品是基于网络的。

● 优点：不需要改变服务器等主机的配置。不需要在业务系统的主机中安装额外的软件；不影响系统机器的 CPU、I/O 与磁盘等资源的使用；不影响业务系统的性能。

● 缺点：对加密通信无能为力；对高速网络无能为力；不能预测执行命令的后果。

（3）基于主机和基于网络的入侵检测系统的集成

HIDS 和 NIDS 各有优缺点，单纯使用一种入侵检测系统可能会使防御系统不健全。通常许多机构的网络安全解决方案都同时采用了基于主机和基于网络的两种入侵检测系统。因为这两种系统在很大程度上是互补的。实际上，许多客户在使用 IDS 时都配置了基于网络的

入侵检测。在防火墙之外的检测器检测来自外部 Internet 的攻击。DNS、Email 和 Web 服务器经常是攻击的目标，但是它们又必须与外部网络交互，不可能对其进行全部屏蔽，所以应当在各个服务器上安装基于主机的入侵检测系统，其检测结果也要向分析员控制台报告。因此，即便是小规模的网络结构也常常需要基于主机和基于网络的两种入侵检测能力。

2. 按检测分析方法分类

根据检测所用分析方法的不同，可分为误用检测和异常检测。

（1）误用检测

假定所有的入侵行为和手段都能够表达一种模式或特征。如果将以往发现的网络攻击的行为的特征总结出来，并建立一个入侵特征信息库，当入侵检测系统捕获到网络行为特征，与特征信息库中的特征进行比较，如果匹配，则当前的网络行为就可以被认定为是入侵行为。误用检测方法对已知的入侵行为和手段进行分析，提取检测特征，构建攻击模式，通过系统当前状态与攻击模式的状态进行匹配，判断入侵行为是否发生。

● 优点：通常可以准确地检测出已知的入侵行为，并对每一种入侵提供比较详细的信息，以便入侵检测系统的使用者能够快速准确地做出反应。误用检测方法具有检测准确度高、技术相对成熟、便于进行系统防护等优点。

● 缺点：对入侵的信息收集和更新困难，难以检测本地入侵行为，不能检测未知的入侵行为，特征库的维护存在困难等。

（2）异常检测

异常检测假设网络攻击行为是不常见的或异常的，区别于正常的行为。为实现该类检测，IDS 建立正常活动的“规范集”，当主体的行为违反其统计规律时，认为可能是“入侵”行为。如果能够对用户和系统所有正常行为总结活动规律并建立行为模型，那么入侵检测系统只要将捕获到的网络行为与行为模型进行比较，若该行为偏离了行为模型规定的行为，就可以被认定为入侵。

● 优点：能够检测出新的入侵行为或从未发生过的入侵行为；对操作系统的依赖性较小；可以检测出属于滥用权限的入侵。

● 缺点：系统抽象出正常活动的行为模型比较困难，而且报警率很高。

4.7.4　入侵检测系统产品的选用方法

在互联网高速上网迅速发展的今天，随着安全事件的急剧增加以及入侵检测技术逐步成熟，入侵检测系统将会有很大的应用前景。比如银行的互联网应用系统（支付网关、网上银行等），科研单位的开发系统、军事系统、普通的电子商务系统等，都需要有 IDS 的护卫。

一般在选择入侵检测系统时，要考虑的要点有：

1）系统的价格：性能价格比，以及要保护系统的价值是重要的因素。

2）特征库升级与维护的费用：像反病毒软件一样，入侵检测的特征库需要不断更新才能检测出新出现的攻击方法。

3）最大可处理流量：对于网络入侵检测系统，最大可处理流量是多少？要分析网络入侵检测系统所部署的网络环境，如果在 512K 或 2M 专线上部署网络入侵检测系统，则不需要高速的入侵检测引擎，而在负载较高的环境中，性能是一个非常重要的指标。

4）产品是否存在常见攻击的漏检：有些常用的躲开入侵检测的方法，如：分片、TTL欺骗、异常TCP分段、慢扫描、协同攻击等。

5）产品的可伸缩性：系统支持的传感器数目、最大数据库大小、传感器与控制台之间通信带宽和对审计日志溢出的处理。

6）运行与维护系统的开销：产品报表结构、处理误报的方便程度、事件与日志查询的方便程度以及使用该系统所需的技术人员数量。

7）产品支持的入侵特征数：不同厂商对检测特征库大小的计算方法都不一样，所以不能只听一面之词。

8）是否通过了国家权威机构的评测：主要的权威测评机构有：国家信息安全测评认证中心、公安部计算机信息系统安全产品质量监督检验中心。

4.8 网络安全综合解决方案案例分析

4.8.1 基本思想

在某大学的校园网信息安全保障方案设计中，从技术手段方面入手，对网络系统、主机系统和边界3个层面进行安全考虑。同时大学也要从管理措施上进行安全防护。

根据对大学校园网络建设需求和业务进行仔细分析的结果，在安全方案设计过程中，首先要将信息网络的结构按照深层防御的思想进行划分，即前面所提到的主机、网络和边界的界定；并将主机、网络和边界部分从信息网络中界定出来；然后对这3个网络环节的安全风险进行分析，并提出相应的安全解决方案。因此，在对主机、网络和边界部分进行界定时，可以认为主机和网络设施的界定相对容易和直观，但是系统/网络边界的界定是相对复杂的过程。这是因为边界不仅仅是个地理位置的概念，在一定程度上它还与应用的定义划分密切相关。基于上述思想，对整个网络的安全性设计分为以下几个方面：

1）设备安全性；

2）网络层的安全性；

3）数据资料的安全性；

4）其他安全措施。

4.8.2 安全方案设计

根据大学校园网安全应用需求，通常一个大学园区网络的安全系统应该考虑以下几个子系统：

1）防火墙及入侵防御系统；

2）应用防护系统-Web应用防火墙；

3）安全审计系统；

4）安全日志管理中心；

5）身份认证行为授权系统；

6）流量控制设备；

7）漏洞扫描系统。

某大学校园网安全解决方案示意图如图 4-15 所示。

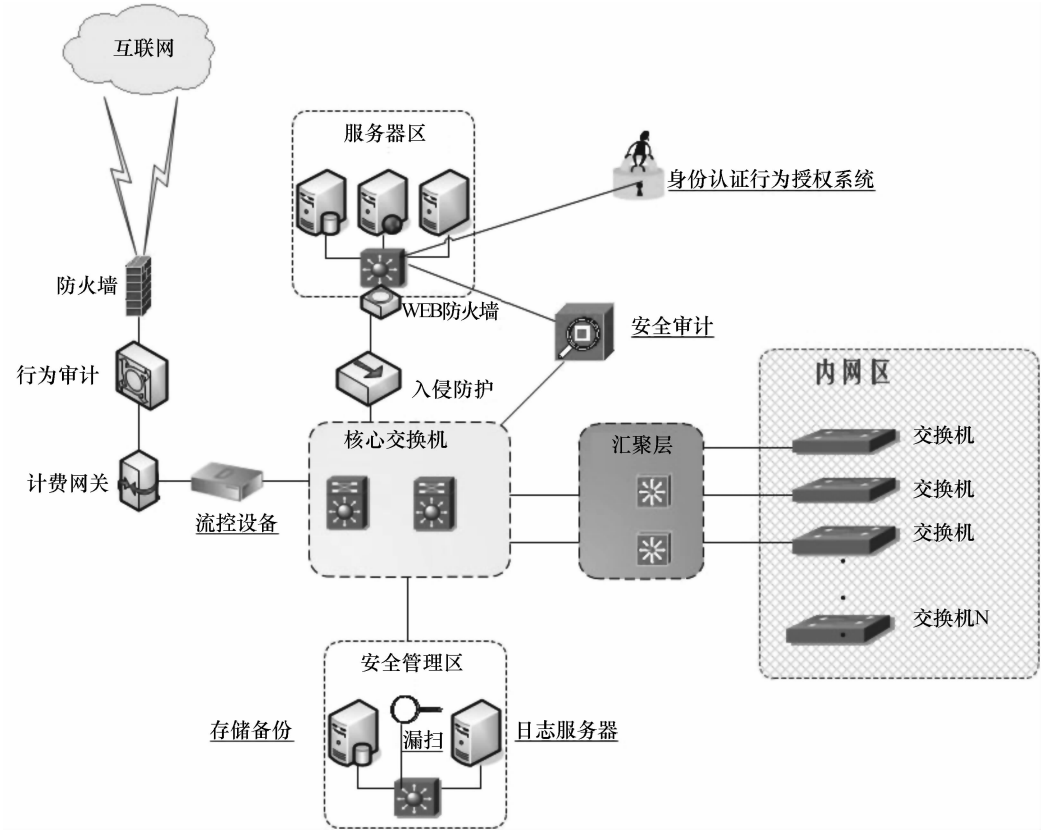


图 4-15　某大学校园网安全解决方案示意图

4.8.3　安全防范措施

通过在校园网中部署一些关键性的网络安全设备，可以极大的保障校园网络的安全，提供安全的网络环境，能够抵御网络病毒、内外部攻击、非法入侵等威胁。采取安全隔离等技术和手段，保证教学用网和学生用网互不影响，可以对学生的上网行为进行记录、识别，并对上网的速率和流量进行策略性控制。提供安全的邮件防护和监控，可防垃圾邮件、防木马、防钓鱼等。

俗话说，网络安全三分技术、七分管理，安全管理贯穿于整个安全防范体系的始终。实践告诉我们，必须具备完善的安全技术防范措施和严格的安全管理制度，否则难以保障网络系统安全。以高校校园网络安全为例，一般大型园区网络需要通过管理人员实施的安全措施主要包括以下几个方面的工作。

1. 网络安全整体策略制定与部署

1）制定符合园区网络实际需求的校园网络安全策略，通过部署防火墙等关键性网络安全设备，有效保障校园网的安全。

2）加强网络安全设备运行的管理、监控、升级和维护等日常管理工作。

3）有效提供校园网对病毒、木马和拒绝服务攻击的安全保护，提高校园网各网段的安全性。

4）开展入侵检测、入侵防御系统技术的研究，运用现有 IDS \ IPS 进一步保障网络安全。

5）运用技术手段，对网络攻击事件进行检测。对发现的攻击事件，及时分析，定位责任人，调整安全措施，做好日志记录工作。

6）运用流控设备，合理分配出口带宽，重点保障关键业务系统的服务。

7）加强对网络及信息安全新技术的研究和培训。

2. 网络设备安全

1）保障网络弱电机房消防、空调、供电等关键系统运行通畅，远离热源、水、暖气等，实行接地或安装防雷设备，保障校园网络设备的防盗和防灾安全。

2）加强对网络设备的运行管理，对物理设备异常故障要及时报告、及时检修。

3）对重要的核心设备实行双机热备，保障网络不中断。

4）及时联系网络设备供应厂商对网络设备 IOS 进行升级更新，防范设备漏洞。

5）加强网络设备运行监控，采取有效的技术措施，定时分析网络设备的日志信息，做好安全预警，防范针对网络设备的攻击。

6）加强对网络设备 ARP、蠕虫等病毒的检测、监控与防范。

3. 服务器系统的安全

1）及时关注服务器新产品、新技术，对服务器的性能、云计算、集群计算、高性能计算、负载均衡、虚拟化、刀片、数据备份、灾难恢复、操作系统、Web 服务等新技术开展研究，为实施有效的网络及信息系统应用提供决策支持。

2）加强服务器操作系统、系统安全技术的研究，根据应用需求有效实施服务器配置，禁止无关服务；设置高强度密码，防止黑客入侵。

3）尽量采用 Unix 作为服务器操作系统，密切关注相关厂商的网站上的补丁列表，及时为系统打上相应的补丁，防范系统漏洞。

4）对于 Windows 操作系统的服务器，采用 Windows 自动更新服务及时升级，及时更新补丁，防范系统漏洞。

5）重要应用服务器、数据服务器必须安装有效的防火墙及防病毒软件，保障系统安全。

6）加强服务器运行监控管理，每周分析一次操作系统日志，采取措施提升服务器安全。

7）对服务器及应用系统的数据进行及时备份。

4. 应用系统的安全

1）研究电子邮件系统、邮件网关新产品、新技术；采取技术措施实施有效的邮件病毒检查和垃圾邮件过滤，做好邮件系统用户数据的备份。

2）研究业务系统应用系统的数据安全、信息安全技术，防范非法程序注入、非法登录，保障数据安全。

5. 用户终端系统安全

1）做好校园网络用户的信息安全培训工作，提高信息安全防范意识。

2）积极倡导校园网络用户使用正版软件，安装防火墙、ARP 防火墙；安装正版防病毒软件，及时升级病毒库。

3）通过在校内实施 Windows 补丁更新服务器，定时从微软网站同步下载补丁程序，并及时下发给广大客户机。

本 章 小 结

本章以网络安全技术为主题，讨论了大型园区网络的安全方案设计和网络安全技术。

1）总结了网络面临的不安全因素，讨论了如何制定网络安全策略及防护体系，对常见的网络黑客攻击的手段和防范方法进行了介绍；这一部分侧重介绍了实用网络安全技术。

2）介绍了网络安全基础理论，对密码算法的原理、PKI、认证等进行了简单的分析。

3）重点介绍了常用的网络安全技术，如防火墙、VPN、入侵检测系统等关键性网络安全设备及其应用。

4）以高校校园网为例，介绍了一个网络安全综合解决方案，并从安全管理的角度剖析了网络管理人员应该完成的日常网络安全管理工作。

第 5 章　综合布线系统

5.1　综合布线系统概述

5.1.1　综合布线系统简介

2009 年 1 月 9 日，由澳信中国传媒集团旗下的 IT168 网站主办的“2009 中国 IT 产品创新与技术趋势大会”隆重召开。IBM 全球副总裁麦特·王博士在大会做了主题为《构建智慧的地球》的演讲，与大家共享一个新的观念，这也是 IBM 在 2008 年年底、2009 年年初所提出的一个观念，即智慧地球，用来控制中国的各种电子系统。自 2009 年 IBM 提出智慧地球的概念以来，云计算、物联网等概念十分火热。我国又提出了发展物联网产业的“感知中国”的概念，标志着我们已经完全步入一个高度信息化发达的时代。

信息社会发展的最终目标是实现万物以互联网相连，并且可互相通信。现代科技的进步使计算机及网络技术飞速发展，提供了越来越强大的计算机处理能力和网络通信能力。计算机及网络通信技术的应用大大提高了现代企业的生产管理效率，降低了运作成本，并使得现代企业能更快速有效地获取市场信息，及时做出决策，提供更快捷、更满意的客户服务，在竞争中保持领先。计算机及网络通信技术的应用已经成为企业成功的一个关键因素。

当今社会，一个现代化的大楼内，除了具有电话、传真、空调、消防、动力电线、照明电线外，计算机网络线路也是不可缺少的。这些布线系统就像一个大楼的神经系统一样，遍布整个楼宇的每一个角落。综合布线系统的对象是建筑物或楼宇内的传输网络，以使话音和数据通信设备、交换设备和其他信息管理系统彼此相连，并使这些设备与外部通信网络连接。它包含着建筑物内部和外部线路（网络线路、电话线路）间的民用电缆及相关的设备连接措施。布线系统是由许多部件组成的，主要有传输介质、线路管理硬件、连接器、插座、插头、适配器、传输电子线路、电气保护设施等，并由这些部件来构造各种子系统。

现代计算机及通信网络均依赖布线系统作为网络连接的物理基础和信息传输的通道。传统的基于特定的单一应用的专用布线技术因缺乏灵活性和发展性，已不能适应现代企业网络应用飞速发展的需要。而新一代的结构化布线系统能同时提供用户所需的数据、话音、传真、视像等各种信息服务的线路连接，它使话音和数据通信设备、交换机设备、信息管理系统及设备控制系统、安全系统彼此相连，也使这些设备与外部通信网络相连接。它包括建筑物到外部网络或电话线路上的连线、与工作区的话音或数据终端之间的所有电缆及相关联的布线部件。布线系统由不同系列的部件组成，其中包括：传输介质、线路管理硬件、连接器、插座、插头、适配器、传输电子线路、电器保护设备和支持硬件。

因此，综合布线系统是专门为现代的建筑物内部及建筑物群之间的计算机、通信设备和自动化设备的布线设计的，可以满足各类不同的计算机、通信设备、建筑物自动化设备传输弱电信号的要求。

5.1.2　综合布线系统的定义

综合布线系统由于各国产品类型不同，其定义是有差异的。我国原邮电部于 1997 年 9 月发布的 YD/T 926.1—1997 通信行业标准《大楼通信综合布线系统第一部分：总规范》中，对综合布线系统的定义为："通信电缆、光缆、各种软电缆及有关连接硬件构成的通用布线系统，它能支持多种应用系统。即使用户尚未确定具体的应用系统，也可进行布线系统的设计和安装。综合布线系统中不包括应用的各种设备。"目前所说的建筑物与建筑群综合布线系统，简称综合布线系统。它是指一幢建筑物内（或综合性建筑物）或建筑群体中的信息传输媒质系统。它将相同或相似的缆线（如对绞线、同轴电缆或光缆）、连接硬件组合在一起，按一定秩序和内部关系集成为整体。

综合布线系统（Premises Distributed System，PDS）又称结构化综合布线系统（Structure Cabling System），是一种用于建筑物内与建筑群之间的建筑智能信息系统的集成化通用传输系统。一般认为，综合布线系统是指由通信电缆、光缆以及各种软电缆及有关连接硬件构成的通用布线系统，在建筑物楼宇内和一定的建筑楼宇构成的园区范围内，通过敷设光缆或双绞线来传输信息，可以连接网络设备、电话、计算机、服务器、监控等多种设备，通过综合布线系统可以搭建一个集语音、数据、图像等信息以及各种应用系统于一身的传输通道。

与传统的布线系统不同，它能同时支持数据传输、语音传输和图像传输，使多种不同的信号在同一条线路中传输，能支持连接多种类型、不同应用系统的电子设备，为实现建设智能化集成系统提供了极大的便利。

5.1.3　综合布线系统的特点

综合布线系统是目前国内外推广使用的比较先进的综合布线方式，它具有兼容性、开放性、灵活性、可靠性、先进性和经济性等特点，在设计、施工和维护方面比传统布线方式更为方便。

1. 兼容性

综合布线的首要特点是它的兼容性。所谓兼容性是指其自身是完全独立的而与应用系统无关，可以用于多种系统的信息传输。综合布线将语音、图像、数据与监控设备的信号线经过统一的规划和设计，采用相同的传输媒体、信息插座、互连设备、适配器等，把这些不同信号综合到一套标准的布线中。综合布线系统具有综合所有系统和互相兼容的特点，采用光缆或高质量的布线部件和连接硬件，能满足不同生产厂家终端设备传输信号的需要。由此可见，这种布线比传统布线更为简化，可节约大量的物资、时间和空间。

2. 开放性

开放性其实也是一种兼容性的表现。传统的布线方式注定了设备需要专用的传输线缆，一旦设备变了，传输线缆也需要重新敷设，这对于现代建筑信息化来说是不可思议的事情。综合布线系统的开放性是指综合布线系统符合多种国际上现行的标准，几乎对所有著名厂商的产品都是开放的，如计算机设备、交换机设备等，并对所有通信协议也是支持的，如 ISO/IEC 8802-3、ISO/IEC 8802-5 等。

3. 灵活性

传统的布线方式结构较为固定，对增加设备或搬迁设备的扩展性考虑不足。综合布线采

用标准的传输线缆和相关连接硬件，模块化设计，因此所有信息通道都是通用的，可以支持电话、传真、计算机、交换机、集线器等多种设备的接入。所有设备的开通及更改均不需改变布线系统，只需增减相应的网络设备以及进行必要的跳线管理即可。

4. 可靠性

由于各个应用系统互不兼容，因而在一个建筑物中往往要有多种布线方式。这些不同的布线往往混杂在一起，互不兼容，容易造成一定程度的信号干扰，同时也不便于管理。

综合布线采用高品质的材料和组合压接的方式构成一套高标准的信息传输通道。所有线缆和相关连接器件均通过 ISO 认证，每条通道都采用专用仪器校核线路衰减、串音、信噪比，以保证其电气性能。在布线的方式上，全部采用物理型拓扑结构，应用系统布线全部采用点到点端接，其结构特点使得任何一条线路故障均不影响其他线路的运行，同时为线路的运行维护及故障检修提供了极大的方便，为各个应用系统的传输提供了可靠的保证。

5. 先进性

综合布线系统采用光纤与双绞线作为传输线缆。业界已经研发出多种技术先进的、高品质的传输光纤；双绞线已经较多地开始使用六类铜缆甚至七类铜缆作为传输线缆，布线产品丰富多样，基本可以满足骨干万兆、千兆到桌面等高带宽应用。

6. 经济性

综合布线与传统的布线方式相比，是一种既具有良好的初期投资特性，又具有很高的性能价格比的布线方式。综合布线系统可以兼容各种应用系统，又考虑了建筑内设备的变更及科学技术的发展，因此可以确保大厦建成后的较长一段时间内，满足用户应用不断增长的需求，节省了重新布线的额外投资。

综合布线系统各个部分都采用高质量材料和标准化部件，并按照标准施工和严格检测，保证系统性能优良可靠，满足目前和今后通信的需要，且在维护管理中减少了维修工作，节省了管理费用。

5.2 综合布线系统的结构

5.2.1 综合布线系统的总体结构

综合布线系统应为开放式网络拓扑结构，应能支持语音、数据、图像、多媒体业务等信息的传递。与网络拓扑结构相似，综合布线系统一般采用分层式星形拓扑结构进行延伸，以一种相对集中的方式进行传输线路的敷设。在综合布线领域被广泛遵循的标准是 EIA/TIA-568A，该标准将综合布线系统划分为 6 个子系统，它们分别是工作区子系统、水平子系统、干线子系统、设备间子系统、管理子系统和建筑群子系统。这 6 个分支子系统都是相对独立的单元，可以单独设计、单独施工，构成了一个有机的整体，其总体结构如图 5-1 所示。

综合布线系统使用标准的双绞线和光纤，支持高速率的数据传输。这种系统使用物理分层星形拓扑结构，积木式、模块化设计，遵循统一标准，使系统的集中管理成为可能，也使每个信息点的故障、改动或增删不影响其他的信息点，使安装、维护、升级和扩展都非常方便，并可节省费用。

综合布线系统的各子系统与应用系统的连接关系，如图 5-2 所示。

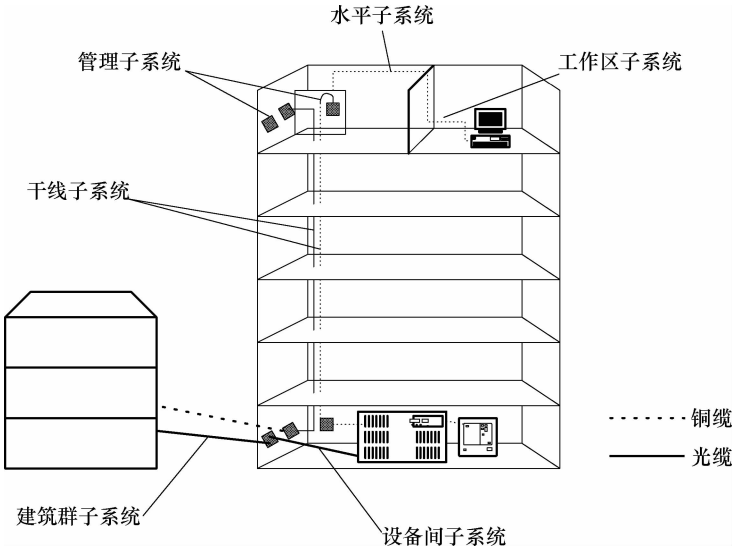


图 5-1　综合布线系统组成结构示意图

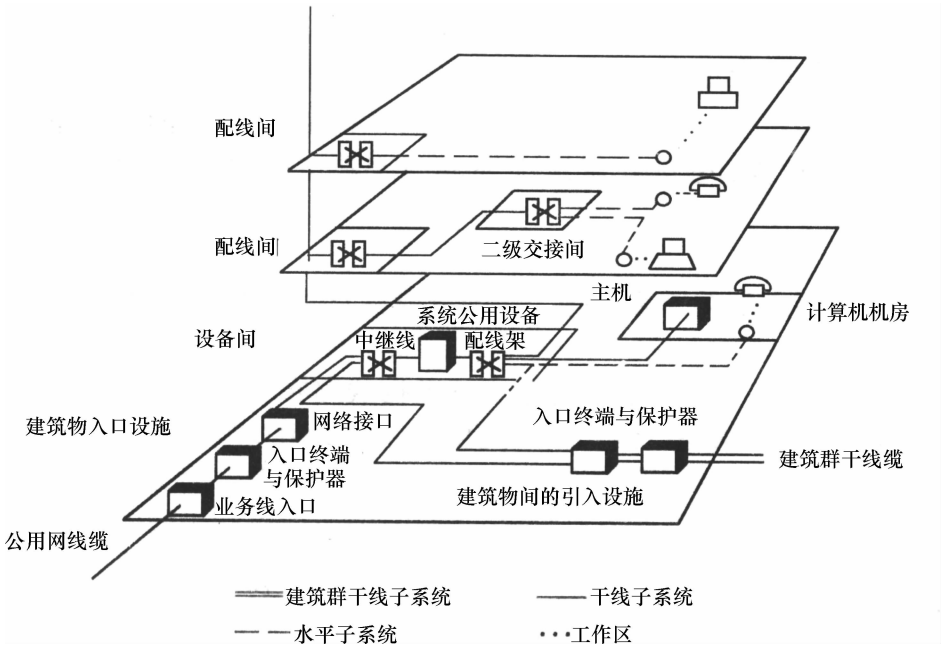


图 5-2　综合布线的各子系统与应用系统的连接关系

5.2.2　综合布线系统的组成

综合布线系统采用模块化结构，按各个模块的功能进行划分，也可以将综合布线系统具体划分为 6 个子系统。

1. 工作区子系统

工作区子系统的目的是实现工作区终端设备与水平子系统之间的连接，由信息插座及终端设备连接到信息插座的连线组成，如图 5-3 所示。工作区常用设备是计算机、网络集线器

（Hub）、电话机、传真机、报警探头、摄像机、监视器、电视机等，工作区也对应配备计算机网络插座、电话语音插座、CATV 电线电视插座等，并配置相应的连接线缆，如 RJ45-RJ45 连接线缆、RJ11-RJ11 电话线、有线电视电缆，信息插座及插座与终端设备连接线缆的选配要根据所连接的终端设备的类型和数量而定。

2. 水平子系统

水平子系统又称配线子系统，主要是工作区的信息插座与楼层管理区的管理器件相连的线缆，如图 5-4 所示。它提供信息插座和管理子系统（配线架）间的连接，将用户工作区引至管理子系统，并为用户提供一个符合国际标准，满足语音及高速数据传输要求的信息点出口。

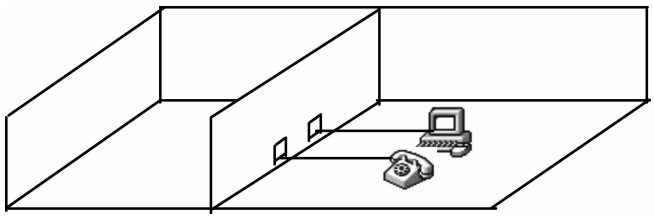


图 5-3　工作区子系统的组成

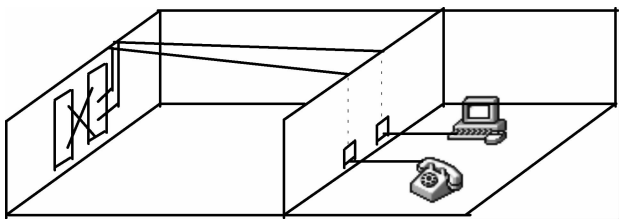


图 5-4　水平子系统

在综合布线系统中，水平子系统要根据建筑物的结构合理选择布线路由，要根据所连接的不同种类的终端设备选择相应的线缆。系统中常用的传输介质是 4 对屏蔽或非屏蔽双绞线，它能支持大多数现代通信设备。如果有磁场干扰或信息保密时可采用屏蔽双绞线。如果需要高宽带应用时，可以采用光缆，构建一个光纤到桌面的传输系统。

3. 干线子系统

干线子系统即垂直干线子系统，是综合布线系统的数据流主干，所有楼层的信息流通过水平子系统汇集到干线子系统。干线子系统是由设备间和楼层配线间之间的连接线缆组成，如图 5-5 所示。

干线子系统一般采用大对数双绞线电缆或光缆，两端分别端接在设备间和楼层配线间的配线架上。干线电缆的规格和数量由每个楼层所连接的终端设备类型及数量决定。干线子系统一般采用垂直路由，干线线缆沿着垂直竖井布放，以提供设备间总配线架与干线接线间楼层配线架之间的干线路由。

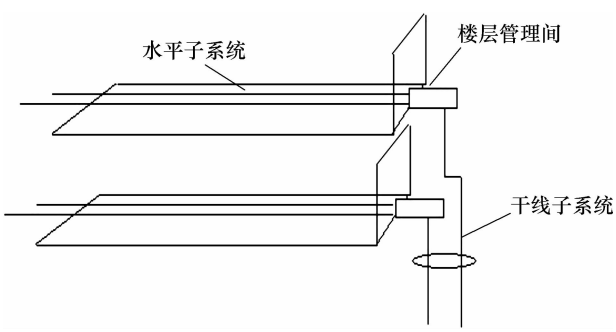


图 5-5　干线子系统

4. 设备间子系统

设备间子系统由设备间内安装的电缆、连接器和有关的支撑硬件组成，作用是将计算机、网络交换机、摄像头、监视器等弱电设备互连起来并连接到主配线架上，如图 5-6 所示。它把公共系统设备的各种不同设备互连起来，如把电信部门的中继线和公共系统设备（如 PBX）互连起来。为便于设备搬运，节省投资，设备间的位置最好选定在建筑物的第二

层或第三层。设备间还包括建筑物的入口区的设备或电气保护装置及其连接到符合要求的建筑物接地点。

5. 管理子系统

管理子系统位于楼层配线间或设备间内，由线路管理器件和跳线组成，如图 5-7 所示。在楼层配线间内水平线缆与干线电缆端接，设备间内干线电缆要与设备连接，这都需要安装相应线缆管理器件对线路进行端接（交连或互连），并通过跳线进行线路的调整、测试等管理工作，以实现综合布线系统的线路管理的灵活性。当工作区内的终端设备需要移动到另一个工作区时，只需简单进行跳线插拔调整即可实现。

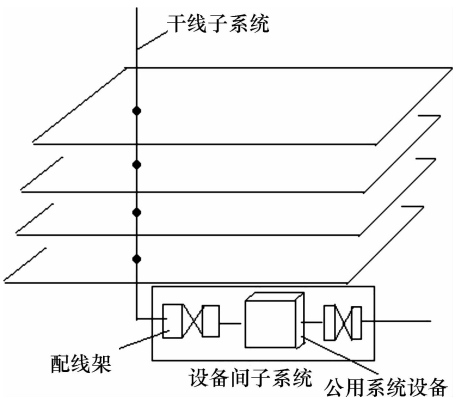


图 5-6　设备间子系统

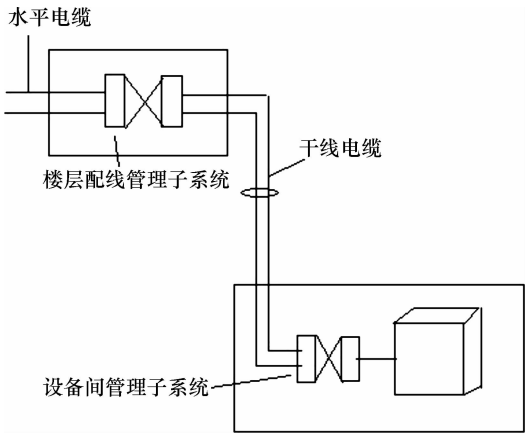


图 5-7　管理子系统

管理子系统常用的管理器件是铜缆配线架和光缆配线架，具体规格及数量由所连接的线缆类型及容量所决定。

6. 建筑群子系统

建筑群子系统是将一个建筑物中的电缆延伸到建筑群的另外一些建筑物中的通信设备和装置，如图 5-8 所示。它提供了楼群之间通信所需的硬件，包括导线电缆、光缆以及防止电缆上的脉冲电压进入建筑物的电气保护装置。

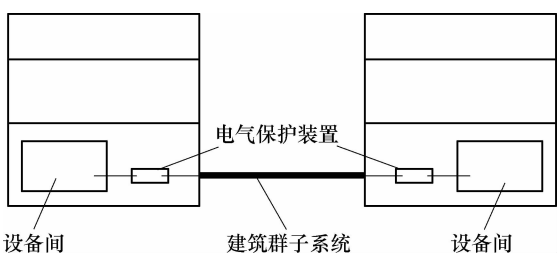


图 5-8　建筑群子系统

建筑群子系统一般采用光缆作为传输介质，它将一个建筑物的电缆延伸到建筑群的另外一些建筑物中的通信设备和装置上，是结构化布线系统的一部分，支持提供楼群之间通信所需的硬件。

5.3　网络传输介质

网络传输介质是指在网络中传输信息的载体。无论是全球性的互联网还是某一个国家的网络，要实现互联互通，基本方法是要用线缆连接各个国家和城市。实现远距离地区网络连接所用的线缆有穿越海底的光缆、也有连接各城市的通信光缆；近距离连接的线缆有小到一

个办公室、一个宿舍连接各台计算机所使用的双绞线，这些都是连接网络所必需的传输介质。常用的传输介质分为有线传输介质和无线传输介质两大类。

1. 有线传输介质

有线传输介质是指在两个通信设备之间实现的物理连接部分，它能将信号从一方传输到另一方。有线传输介质主要有双绞线、同轴电缆和光纤。双绞线和同轴电缆传输电信号，光纤传输光信号。

2. 无线传输介质

无线传输介质指我们周围的自由空间。我们利用无线电波在自由空间的传播可以实现多种无线通信。在自由空间传输的电磁波根据频谱可将其分为无线电波、微波、红外线、激光等，信息被加载在电磁波上进行传输。

5.3.1 双绞线

双绞线是综合布线工程中最常用的一种传输介质，也是一种最廉价的传输媒体，并且易于使用。双绞线也可支持高带宽的传输，因此作为一种最常见的、最主要的网络传输介质被广泛应用于智能建筑的综合布线工程中。

双绞线采用了一对互相绝缘的铜导线互相绞合在一起，形成有规则的螺旋形，来抵御一部分外界电磁波的干扰，更主要的是可降低自身信号的对外干扰。通常是把若干对双绞线集成一束，并且用护套外皮包住，形成了典型的双绞线电缆。把多个线对扭在一块可以使各线对之间或其他电子噪声源的电磁干扰最小。通常所说的双绞线是指由 8 芯（4 对）组成的，如图 5-9 所示。仔细观察可以发现，每一对线在同一长度内绞数不同，且每一对线用不同的颜色区分。

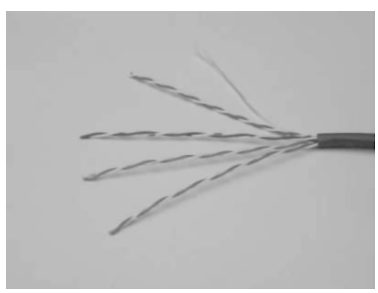


图 5-9　双绞线示意图

1. 非屏蔽双绞线和屏蔽双绞线

双绞线主要分为两大类，即非屏蔽双绞线（Unshielded Twisted-Pair，UTP）和屏蔽双绞线（Shielded Twisted-Pair，STP）。

非屏蔽双绞线是一种数据传输线，由 4 对不同颜色的传输线所组成，就是常用的普通电话线或数据线，广泛用于以太网络和电话线中。当前综合布线系统工程中，非屏蔽双绞线一般可以满足用户的电话业务及数据业务需求，应用非常广泛，也是物美价廉、最易于安装和使用的传输媒体。非屏蔽系统可以在普通的商务楼宇环境下稳定的工作，但不适合在对信息安全有高度要求，或者有电磁干扰的环境中使用，不能满足特殊行业的要求：如政府、军队等行业用户。

屏蔽双绞线在双绞线与外层绝缘封套之间有一个金属屏蔽层。屏蔽层可减少辐射，防止信息被窃听，也可阻止外部电磁干扰的进入，使屏蔽双绞线比同类的非屏蔽双绞线具有更高的传输速率。屏蔽系统在干扰严重的环境下，不仅可以安全地运行各种高速网络，还可以安全地传输监控信号，以避免干扰带来的监控系统假信息、误动作等。对一些对传输有非常特殊要求的网络，包括涉及安全的重要信息，一定要使用屏蔽双绞线。屏蔽系统能防止电磁辐射泄漏，保证机密信息的安全传输。

2. 非屏蔽双绞线的分类

非屏蔽双绞线具有成本低、柔性好、传输性能好等特点，是全世界范围内综合布线工程中应用最广泛的电缆。EIA/TIA（电子工业协会/电信工业协会）按照电气性能的不同，将 UTP 双绞线定义为 8 种类别：

1）一类线：主要用于模拟语音传输（一类标准主要用于 20 世纪 80 年代之前的电话线缆）。

2）二类线：用于语音传输和最高传输速率为 4Mbit/s 的数据传输。

3）三类线：用于语音传输及最高传输速率为 10Mbit/s 的数据传输。

4）四类线：用于语音传输和最高传输速率为 16Mbit/s 的数据传输。

5）五类线：该类电缆增加了绕线密度，外套一种高质量的绝缘材料，传输频率为 100MHz，用于语音传输和最高传输速率为 100Mbit/s 的数据传输，主要用于 100BASE-T 和 1000BASE-T 网络。

6）超五类线：超五类线衰减小，串扰少，并且具有更高的衰减与串扰的比值（ACR）和信噪比（Structural Return Loss）、更小的时延误差，性能得到了很大提高。超五类线主要用于百兆位以太网（100Mbit/s），也可用于千兆位以太网（1000Mbit/s）。这是最常用的以太网电缆。

7）六类线：该类电缆的传输频率为 1 ~ 250MHz，六类布线系统在 200MHz 时综合衰减串扰比（PS-ACR）应该有较大的余量，它提供 2 倍于超五类的带宽。六类布线的传输性能远远高于超五类标准，最适用于传输速率高于 1Gbit/s 的应用。六类与超五类的一个重要的不同点在于：改善了在串扰以及回波损耗方面的性能，对于新一代全双工的高速网络应用而言，优良的回波损耗性能是极重要的。六类标准中取消了基本链路模型，布线标准采用星形的拓扑结构，要求的布线距离为：永久链路的长度不能超过 90m，信道长度不能超过 100m。

8）七类线：带宽为 600MHz，可能用于今后的 10Gbit 以太网。

目前，综合布线系统中主要使用超五类线、六类线作为语音或数据传输系统。六类非屏蔽双绞线可以非常好地支持千兆以太网，并实现 100m 的传输距离。六类双绞线虽然价格较高，但由于与超五类布线系统具有非常好的兼容性，且能够非常好地支持 1000BASE-T，所以正慢慢成为综合布线的主流产品。七类线是一种新的双绞线产品，性能优异，但目前价格较高，施工复杂且可供选择的产品较少，目前很少在综合布线工程中采用。

3. 双绞线的使用

双绞线需要通过 RJ-45 连接器（俗称水晶头）与网卡、集线器或交换机等设备相连。在制作水晶头时，必须符合国际标准。EIA/TIA 制定的双绞线制作标准有 T568A 和 T568B，其规定的线序标准见表 5-1，其中双绞线的这 8 根线的引脚定义见表 5-2：Tx 代表发送端，Rx 代表接收端。

表 5-1　线序标准

引脚号	1	2	3	4	5	6	7	8
T568A 标准	绿白	绿	橙白	蓝	蓝白	橙	棕白	棕
T568B 标准	橙白	橙	绿白	蓝	蓝白	绿	棕白	棕

表 5-2　双绞线引脚定义

线号	1	2	3	4	5	6	7	8
线色	橙白	橙	绿白	蓝	蓝白	绿	棕白	棕
作用	Tx +	Tx –	Rx +			Rx –		

按照双绞线两端线序的不同，我们一般划分两类双绞线：一类两端线序排列一致，称为直通线；另一类是改变线的排列顺序，称为交叉线。其线序见表 5-3、表 5-4。

表 5-3　直通线线序（机器与集线器连）

线序	1	2	3	4	5	6	7	8
A 端	橙白	橙	绿白	蓝	蓝白	绿	棕白	棕
B 端	橙白	橙	绿白	蓝	蓝白	绿	棕白	棕

表 5-4　交叉线线序（机器直连、集线器普通端口级联）

线序	1	2	3	4	5	6	7	8
A 端	橙白	橙	绿白	蓝	蓝白	绿	棕白	棕
B 端	绿白	绿	橙白	蓝	蓝白	橙	棕白	棕

在进行设备连接时，需要正确地选择线缆。设备的 RJ-45 接口分为 MDI 和 MDIX 两类。当同种类型的接口通过双绞线互连时，使用交叉线；当不同类型的接口通过双绞线互连时，使用直连线。通常主机和路由器的接口属于 MDI，交换机和集线器的接口属于 MDIX。例如，路由器和主机相连，采用交叉线；交换机和主机相连则采用直连线，见表 5-5。

表 5-5　直通线与交叉线级联使用表

	主机	路由器	交换机 MDIX	交换机 MDI	集线器
主机	交叉	交叉	直连	N/A	直连
路由器	交叉	交叉	直连	N/A	直连
交换机 MDIX	直连	直连	交叉	直连	交叉
交换机 MDI	N/A	N/A	直连	交叉	直连
集线器	直连	直连	交叉	直连	交叉

RJ-45 水晶头由金属片和塑料构成，特别需要注意的是引脚序号，当金属片面对我们的时候从左至右引脚序号是 1 ~ 8。序号在制作双绞线接头时非常重要，一旦序号出现错误，将无法正常传输数据。

5.3.2　同轴电缆

同轴电缆以硬铜线为芯，外包一层绝缘材料，如图 5-10 所示为同轴电缆结构，其内部的铜芯主要用于实现信号的传输；屏蔽层通常由金属丝编织网构成，以实现与外界电缆干扰的隔离，同时防止外界电磁场对铜芯上传输信号的干扰；内部绝缘层主要隔离铜芯与屏蔽层；外部绝缘层较厚并具有较好的弹性。

同轴电缆可分为粗缆和细缆两种，粗缆用于较大型局域网的布线，具有通信距离长、可靠性较高等优点；细缆主要应用于总线型局域网的布线，成本低、安装方便。

同轴电缆曾经被广泛用于 10Base-5 和 10Base-2 以太网中。当前，在建筑楼宇的综合布线工程中已经被双绞线和光纤取代。

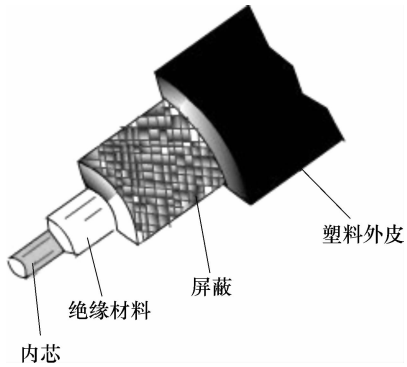


图 5-10　同轴电缆结构

5.3.3　光纤

1. 光纤的基本概念

光纤是光导纤维的简写，是一种利用光在玻璃或塑料制成的纤维中的全反射原理而达成光传导的工具。光纤是一种细小、柔韧并能传输光信号的介质。利用光纤作为传输介质的通信方式叫光通信。光纤是一种传输频带宽、通信容量大、传输损耗低、中继距离长、抗电磁干扰能力强、无串话干扰和保密性好的传输介质。

在局域网或广域网组网工程布线施工中，光缆是一种主要使用的综合布线材料。一根光缆包含有多条光纤，比较常见的有 4 芯、8 芯、12 芯、24 芯、48 芯、96 芯甚至更多芯数的光缆。光缆最核心的部分是它所包含的纤芯，纤芯通常是石英玻璃制成的横截面积很小的双层同心圆柱体，质地脆、易断裂。纤芯外面包围着一层折射率比芯线低的玻璃封套作为包层，以使光纤保持在芯内。在实际组网工程中所用到的光纤都已经加装了保护套层，以形成一个保护外壳，以增强光缆的抗拉强度，有利于在实际布线工程中使用。图 5-11 所示为光缆结构图。

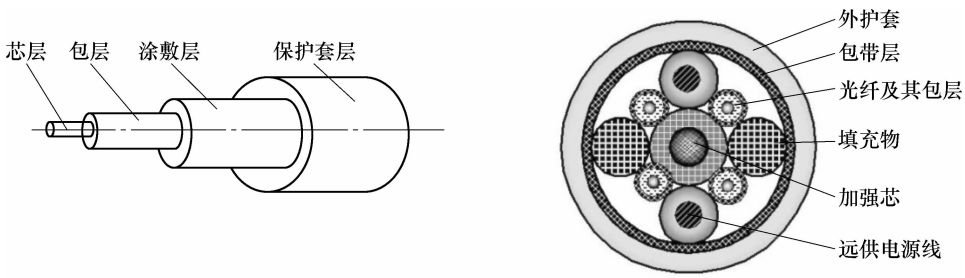


图 5-11　光缆结构图

2. 光纤的分类及其主要性能参数

光纤主要分以下两大类：

（1）按传输点模数分类

按传输点模数分类，光纤可分为单模光纤（Single Mode Fiber）和多模光纤（Multi Mode Fiber）。

单模光纤的纤芯直径很小，在给定的工作波长上只能以单一模式传输，传输频带宽，传输容量大。常用单模光纤的直径一般为 125μm，芯径为 8.3μm 左右。在单模光纤中，因只有一个模式传播，不存在模间色散，因此具有较大的传输带宽，并且在 1310nm 波长区的损耗约为 0.4dB/km，在 1550nm 波长区的损耗约为 0.3dB/km，因损耗较低而被广泛应用于高

速长距离的光纤通信系统中。使用单模光纤时，色度色散是影响信号传输的主要因素，这样单模光纤对光源的谱宽和稳定性都有较高的要求，即谱宽要窄，稳定性要好。单模光纤一般必须使用半导体激光器激励。

多模光纤是在给定的工作波长上，能以多个模式同时传输的光纤。与单模光纤相比，多模光纤的传输性能较差。常用多模光纤的直径也为 125μm，其中芯径一般为 50μm 和 62.5μm 两种。在多模光纤中，可以有数百个光波模在传播。多模光纤一般工作于短波长（0.8μm）区，损耗与色散都比较大，带宽较小，适用于低速短距离光通信系统。多模光纤的优点在于其具有较大的纤芯直径，可以用较高的耦合效率将光功率注入到多模光纤中。多模光纤一般使用发光二极管（LED）激励。

IEEE802.3z 千兆位以太网标准中规定 50/125μm 多模和 62.5/125μm 多模光纤都可以作为千兆位以太网的传输介质使用。50/125μm 渐变折射率多模光纤中传输模的数目大约是 62.5/125μm 多模光纤中传输模的 1/2.5，有效地降低了多模光纤的模色散，使得带宽得到了显著的增加。一般首选 50/125μm 多模光纤。

（2）按折射率分布分类

按折射率分布分类光纤可分为跳变式光纤和渐变式光纤。跳变式光纤纤芯的折射率和保护层的折射率都是一个常数。在纤芯和保护层的交界面，折射率呈阶梯形变化。渐变式光纤纤芯的折射率随着半径的增加按一定规律减小，在纤芯与保护层交界处减小为保护层的折射率。纤芯的折射率的变化近似于抛物线。

目前，国际上单模光纤的标准主要是 ITU-T G.652《单模光纤和光缆特性》；多模光纤的标准主要是 ITU-T G.651《50/125μm 多模渐变折射率光纤和光缆特性》。我国的光纤标准包括国家标准 GB/T 15912 系列和信息产业部颁布的通信行业标准 YD/T 系列。关于光纤详细的性能参数，建议查阅相关国际标准和国内标准，熟悉光纤的技术指标，有利于合理选用单模和多模光纤。

5.3.4 光缆与光纤连接器

1. 光缆的概念与分类

光缆是一种传输光束的细微而柔韧的传输介质。光缆由一捆纤芯组成，是数据传输中最有效的一种传输介质。光缆一般可以分为以下三类：

1）按敷设方式分有：自承重架空光缆、管道光缆、铠装地埋光缆和海底光缆。

2）按光缆结构分有：束管式光缆、层绞式光缆、紧抱式光缆、带式光缆、非金属光缆和可分支光缆。

3）按用途分有：长途通信用光缆、短途室外光缆、混合光缆和建筑物内用光缆。

这些光缆使用不同的光纤作为纤芯，并采用不同的方法制成各种各样的光缆。常见的有 GYTA 光缆、GYTS 光缆、GYXY 光缆、GYTA53 光缆、GYTY53 光缆等多种单模或多模光缆，如 GYTA 是一种松套层绞式非铠装光缆，是室外光缆的一种，可管道、可架空。GYTA 光缆是将 250μm 光纤套入高模量材料制成的松套管中，松套管内填充防水化合物。缆芯的中心是一根金属加强芯，对于某些芯数的光缆来说，金属加强芯外还需挤上一层聚乙烯（PE）。松套管（和填充绳）围绕中心加强芯绞合成紧凑的圆形的缆芯，缆芯内的缝隙充以阻水填充物。涂塑铝带（APL）纵包后挤制聚乙烯护套成缆。

GYTS 光缆是把 9/125μm 单模光纤或 50/125μm、62.5/125μm 多模光纤（二氧化硅）套进用高等阻水材料制成的松套管中，松套管内填充阻水化合材料。缆芯的中心是一根金属加强芯，对于多芯光缆来说加强芯需外加一层 PE 外套。松套管和填充绳围绕中心加强芯互绞紧凑成圆形的缆芯。缆芯内的缝隙充加阻水填充物。双面皱纹钢带（PSP）纵包后挤制聚乙烯护套成缆。

两种常见的光缆如图 5-12 所示。

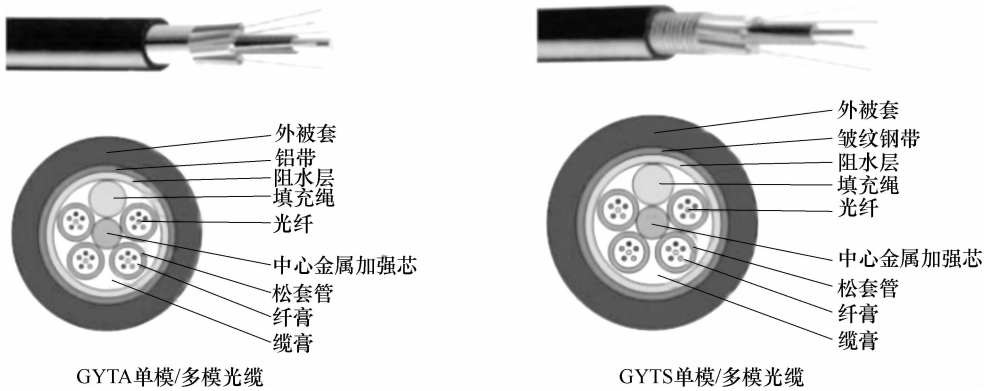


图 5-12　两种常见的光缆

2. 光纤连接器

光纤连接器（又称光纤跳线）是在一段光纤两端安装连接插头，在光纤与光纤之间进行可拆卸（活动）连接的器件。它是把光纤的两个端面精密对接起来，以使发射光纤输出的光能量能最大限度地耦合到接收光纤中去，并使由于其介入光链路而对系统造成的影响减到最小，这是光纤连接器的基本要求。在一定程度上，光纤连接器也影响了光传输系统的各项性能。下面对网络工程中几种常用的光纤连接器进行简单的说明。

1）FC 型光纤连接器：外部加强方式是采用金属套，紧固方式为螺钉扣，金属双重配合螺旋终止型结构。一般在 ODF 配线架上采用。

2）SC 型光纤连接器：连接 GBIC 光模块的连接器，紧固方式是采用插拔销闩式，不须旋转，矩形塑料插拔式结构；特点是容易拆装。多用于多根光纤与空间紧凑的法兰之间的连接。

3）ST 型光纤连接器：常用于光纤配线架，外壳呈圆形，紧固方式为螺钉扣，金属圆形卡口式结构；常用于光纤配线架。

4）LC 型光纤连接器：连接 SFP 模块的连接器，它采用操作方便的模块化插孔（RJ）闩锁机理制成，常用在在路由器接口上。

5）MT-RJ：收发一体的方形光纤连接器。

以上是指接头与光纤桥接器（法兰盘）之间的连接形式，这些结构主要是实现接头与法兰盘之间的坚固连接，并将两端光纤的轴线引导到一条线上。

按光纤端面形状分有 FC、PC（包括 SPC 或 UPC）和 APC，连接器插芯连接的损耗应该是越小越好，因此，对于活动接头的端面的要求比较高。以下是针对端面而制定的一些标准形式：

1）PC 型：端面呈球形，接触面集中在端面的中央，反射损耗为 35dB，多用于测量仪器。

2）APC 型：接触端的中央部分仍保持 PC 型的球面，但端面的其他部分加工成斜面，使端面与光纤轴线的夹角小于 90°，这样可以增加接触面积，使光耦合更加紧密。当端面与光纤轴线夹角为 8°时，插入损耗小于 0.5dB。窄带（155Mbit/s 以下）光传输系统中常采用这种结构的接头。

3）UPC 型：超平面连接，加工精密，连接方便，反射损耗为 50dB，常用于宽带（155Mbit/s 及以上）光纤传输系统中。

光纤接口连接器的种类如图 5-13 所示。

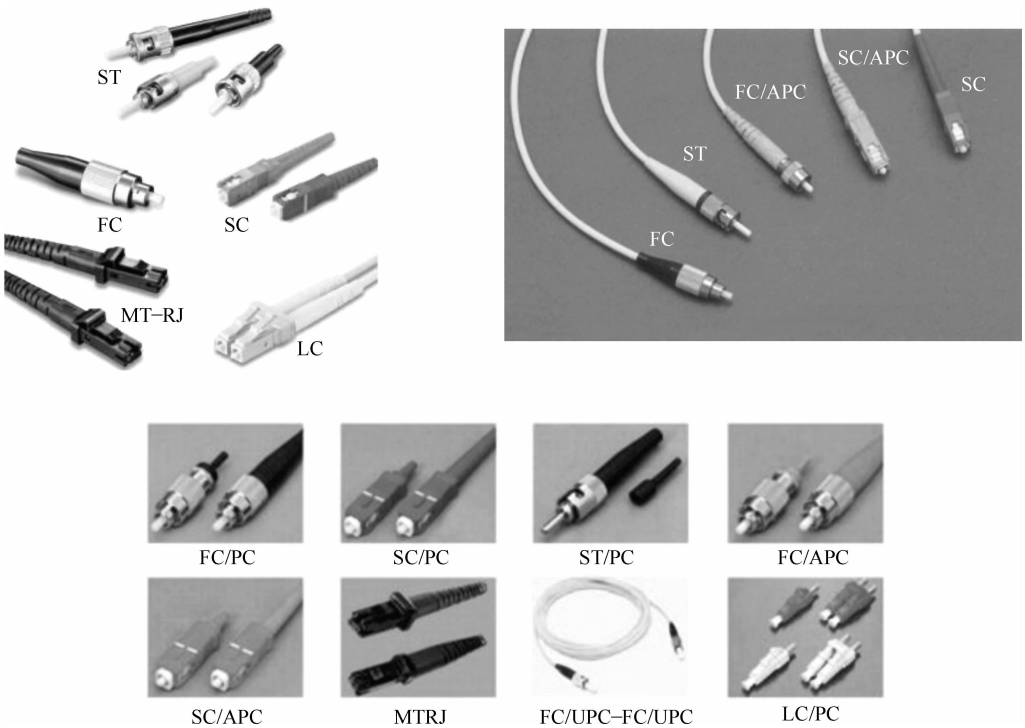


图 5-13　光纤接口连接器的种类

5.4　综合布线系统设计

5.4.1　综合布线系统设计原则

结构化综合布线系统（PDS）的建设是一个综合的、统一的信息系统工程，其中设计是最重要的前期工作。综合布线系统方案的设计一般遵循以下原则：

1）实用性：满足当前及未来的发展需求，满足办公自动化和计算机网络系统对布线系统的需求，同时兼容话音、数据、图像的传输。

2）兼容性：是综合布线系统必备的首要特点。所谓兼容性是指综合布线本身是完全独立、与应用系统相对无关、可适应多种应用的系统。综合布线将语音、数据与监控设备经过

统一规划和设计，采用相同的传输介质、信息插座、交连设备、适配器等，把这些不同信号综合到一套标准的布线中。因此，结构化（模块化）综合布线比传统布线大为简化，节省了大量物资、时间和空间。

3）开放性：结构化综合布线系统采用的是开放式体系结构，符合多种国际上现行的标准，满足几乎所有著名厂商产品的应用需求，支持所有通信协议。

4）灵活性：结构化综合布线系统为开放式结构，能支持话音及多种计算机数据系统，比如支持会议电视、多媒体等系统。即任一信息点能够连接不同类型的设备，如计算机、打印机、终端或电话、传真机，因此充分体现了其灵活性的特点。

5）模块化：在综合布线系统中，除去固定在建筑物内的线缆外，其余所有的接插件都是积木式的标准件，因此便于管理和使用。

6）扩充性：由于综合布线系统是结构化的，因此比较容易实行系统的扩充，在将来有新的需求时，就能比较容易地实现设备的扩展。此外，结构化综合布线通常采用树状星形结构，以支持目前和将来各种网络的应用，并通过跳线和不同网络设备，实现各种不同逻辑拓扑结构的网络，因此当系统需要扩充时仅需在相关节点上增加新的线缆即可。

7）标准性：满足最新、最高的布线系统标准（如中华人民共和国建设部于 2007 年制定的 GB 50311—2007《综合布线系统工程设计规范》，国际标准：ISO/IEC 11801、欧洲标准：EN50173 等）的要求。

8）可靠性：综合布线系统在设计时都会充分考虑系统的长期性和可靠性等，同时在实施时都使用具有高可靠性的机柜型配线系统为核心，提高了系统的可靠性和安全性。

9）经济性：在满足应用要求的基础上，尽可能降低造价，实现最优的性能价格比。

5.4.2　综合布线系统设计标准

做综合布线系统设计时，要依据我们国家的或行业协会制订的相关标准和技术要求，进行综合布线系统工程的规划设计。

《民用建筑电气设计规范》JGJ16—2008

《建筑设计防火规范》GB 50016—2006

《智能建筑设计标准》GB/T 50314—2006

《建筑智能化系统工程设计管理暂行规定》建设部［1997］290 号

《智能建筑弱电工程设计施工图集》中国建筑标准设计研究所、工程建设标准设计分会弱电专业委员会 97X700

《民用闭路监视电视系统工程技术规范》GB 50198—2011

《高层民用建筑设计防火规范》GB 50045—1995

《电子信息系统机房设计规范》GB 50174—2008

《建筑物防雷设计规范》GB 50057—2010

《智能建筑设计标准》GB/T 50314—2006

《信息技术—用户通用布线系统》ISO/IEC11801

《商务楼通信建筑布线标准》EIA/TIA568A

《商务楼通信通道和空间标准》EIA/TIA569

《大楼通信综合布线系统总规范》YD/T926

《计算机场地通用规范》GB/T 2887—2011
《电磁兼容标准》EN5022
《非屏蔽双绞线传输性能标准》EIA/TIA TSB67
《综合布线系统工程设计规范》GB 50311—2007

5.4.3 综合布线系统设计步骤

根据通信工程建设特点，综合布线设计人员在设计施工图时，可根据以下步骤进行设计：

1）获取建筑物平面图：到施工现场与用户沟通并获得建筑施工平面图。
2）进行现场勘查：在获得建设施工平面图后到施工现场进行现场勘查。
3）获取用户需求：了解最终用户的实际需求，进而确定系统需求。
4）设计系统结构：根据建筑结构特点和用户需求设计布线系统结构。
5）设计布线路由：根据建筑施工平面图和用户需求设计布线系统路由。
6）绘制布线施工图：根据建筑施工平面图和用户需求信息设计布线系统施工图。
7）编制布线用料清单：根据布线系统施工图编制布线系统所需的用料清单。

5.4.4 综合布线系统设计时需考虑的问题

由于综合布线系统通常都是覆盖一个建筑物群或几个建筑物群，因此在整个综合布线系统的设计过程中，必须充分考虑建筑物的实际情况，依据建筑物的实际建筑结构进行各个子系统的设计工作。

1. 建筑物综合布线系统设计等级的确定

一般来说，综合布线系统的设计等级是根据客户的需求给客户提供的不同服务等级，系统设计等级通常分为基本型、增强型和综合型三大类，具体等级区分如下。

（1）基本型

基本型设计等级可以满足对语音、数据或高速数据系统的使用需求；满足多种计算机系统数据传输的需求，并且工程造价较低。基本型设计等级通常采用铜制电缆布网，目的是便于日常维护管理，且技术要求不高；其次采用气体放电管式过电压保护和自恢复的过电流保护。因此，基本型设计等级是我国目前普遍采用的布线方案。

（2）增强型

增强型设计等级每个工作区有两个以上的信息插座，不仅灵活机动、功能齐全，还能适应今后发展的要求。任何一个信息插座都可提供话音和数据系统等多种服务。采用以铜芯导线为主的组网方式，利用端子板管理，使用统一色标，简单方便，利于维护。能适应多种产品的要求，具有适应性强、经济有效等特点。

（3）综合型

综合型适用于综合布线系统中配置标准较高的场合，使用光缆和铜芯双绞线组网。综合型综合布线系统应在基本型和增强型综合布线系统的基础上增设光缆系统。综合型布线系统的主要特点是引入光缆，能适用于规模较大的智能大厦，其余与基本型或增强型相同。

2. 建筑物综合布线系统的链路及应用级别

（1）链路指标

综合布线系统中的链路是指两个接口之间所具有的规定性能的传输通道，在链路中不包括终端设备、设备电缆（光缆）和工作区电缆（光缆）。图 5-14 所示的综合布线系统中水平布线模型展示了链路的传输通道。

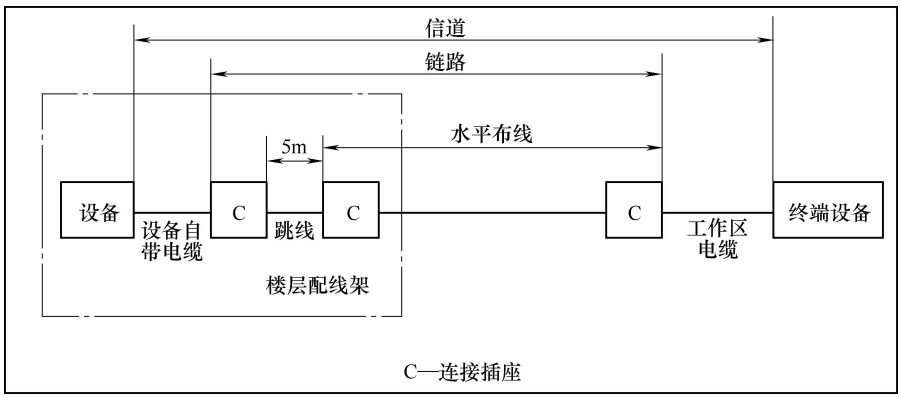


图 5-14　综合布线系统中水平布线模型

（2）链路的应用级别

综合布线系统在设计时，必须根据智能化建筑的客观需要和用户的具体需求来选用综合布线系统的链路，链路的应用级别通常有 5 种，不同的应用级别对应不同的服务范围及技术要求。综合布线系统链路的应用级别见表 5-6。

表 5-6　综合布线系统链路的应用级别

序号	应用级别	布线链路传输媒质	应用场合	支持应用的链路级别	频率
1	A 级	A 级对称电缆布线链路	话音带宽和低频信号	最低速率的级别，支持 A 级	100kHz 以下
2	B 级	B 级对称电缆布线链路	中速（中比特率）数字信号	支持 B 级和 A 级的应用	1MHz 以下
3	C 级	C 级对称电缆布线链路	高速（高比特率）数字信号	支持 C 级、B 级和 A 级的应用	16MHz 以下
4	D 级	D 级对称电缆布线链路	超高速（超高比特率）数字信号	支持 D 级、C 级、B 级和 A 级的应用	10MHz 以下
5	光缆级	光缆布线链路按光纤分为单模光纤和多模光纤，其光纤参数也有相应规定	高速和超高速的数字信号	支持光缆级的应用，支持传输速率 10MHz 及以上的各种应用	10MHz 及其以上

注：1. 单模光纤光缆按通信用单模光纤系列规定的 BI. I 类光纤要求。

2. 多模光纤光缆按通信用多模光纤系列规定的 AIa 和 AIb 型光纤要求。

3. 允许采用的光纤形式为 50μm/125μm 多模光纤和 8. 3μm/125μm 单模光纤，推荐采用的光纤形式为 62. 5μm/125μm 多模光纤。

5. 4. 5　综合布线各子系统设计

1. 工作区子系统设计

工作区子系统是由终端设备以及信息插座的连线（或跳线）组成，我们称它为工作区。

工作区所含的设备主要有：连接器、跳线、信息插座和终端设备等。根据使用位置不同可将信息插座分成墙上型、地上型、桌上型等多种。其结构主要有 RJ-45、RJ-11 及单口、双口、多口等。在工作区子系统中，跳线主要是连接终端设备和输入/输出（I/O）终端设备，主要包括电话、计算机和数据终端，也可以是仪器仪表、传感器的探测器等设备。工作区子系统示意图如图 5-15 所示。

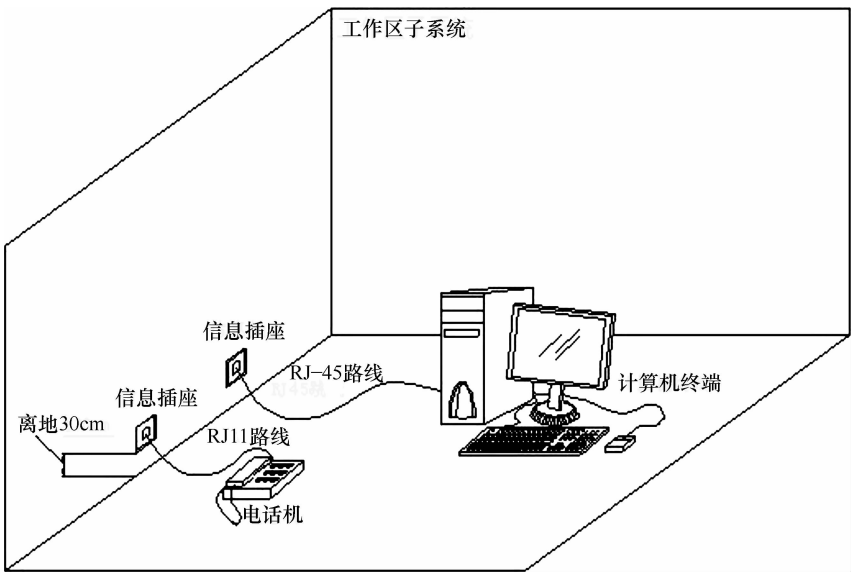


图 5-15　工作区子系统示意图

在设计工作区子系统时，首先需要确定系统的规模，然后根据系统规模确定系统所含内容，具体内容主要包括以下几个方面：

1）综合布线系统工作区内线槽的敷设要整齐、美观。

2）确定系统中所需要的信息插座后，将信息插座设计在距离地面 30cm 以上的位置；同时考虑为将来的扩充留出一定的冗余。

3）信息插座与计算机设备的距离保持在 5m 范围内。

4）选用符合要求的适配器，即网卡接口类型要与线缆接口类型保持一致。

5）所有综合布线系统工作区所需的信息模块、信息插座、面板等必须符合相关标准，同时设计数量必须准确。

6）每个工作区至少应配置一个 220V 交流电源插座。

7）工作区子系统布线的线缆长度必须满足要求。

当确定信息插座的类型后，就可以确定信息插座的安装方式。工作区信息点的信息插座在安装时建议安装在离地 30cm、离电源 20cm 的位置。工作区信息点的信息底盒暗装于墙体中，并和电源插座处在同一平行位置，保证整体的美观协调。信息点的安装位置示意图如图 5-16 所示。

2. 水平干线子系统的设计

水平干线子系统是指从工作区的信息插座开始到管理间子系统配线架间的部分。水平干线子系统的设计涉及介质主要有传输介质和部件，其主要设计内容包括：线路走向，线缆、

线槽、管的数量和类型，电缆的类型和长度，订购电缆和线槽，若打吊杆走线槽时所需的吊杆数量，不用吊杆走线槽时所需的托架数量。

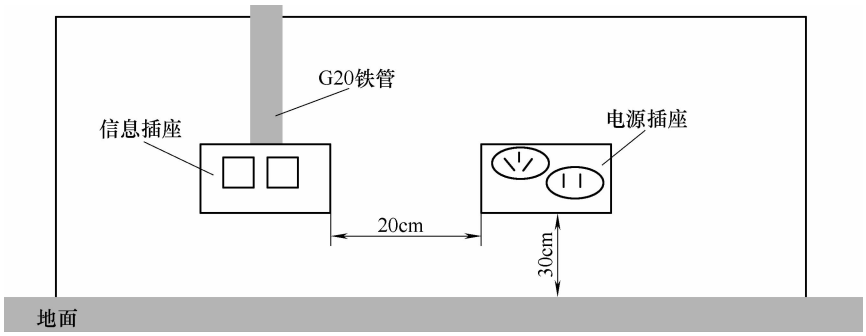


图 5-16　信息点的安装位置示意图

其中，线路走向的确定一般需要由用户、设计人员、施工人员根据现场建筑物的物理位置和施工难易度来确定；而信息插座的数量和类型、电缆的类型和长度一般在总体设计时便已确定，但考虑到产品质量和施工人员的误操作等因素，在配置施工材料时要留出一定量的冗余来。水平干线子系统示意图如图 5-17 所示。

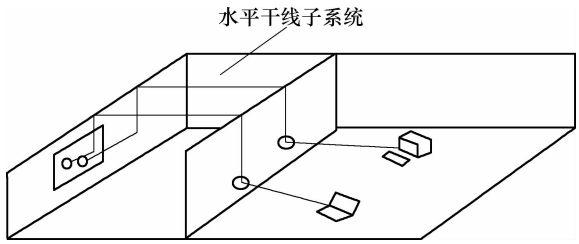


图 5-17　水平干线子系统示意图

水平干线子系统的设计要求主要包括水平干线子系统长度及转接点要求两部分内容。首先，水平干线子系统布线的线路长度不得超过 90m，水平跳线之和（工作区跳线、配线面板跳线）不超过 10m，在具体设计时设计者需根据建筑物的结构特点，从室内美观、路由（线）最短、造价最低、施工方便、布线规范等方面进行综合考虑，从而确定水平干线子系统的最佳布线方案；其次，干线子系统中不允许有转接点，且语音和数据电缆要区分开，干线线缆的交接不应超过 2 次，电缆的限制距离和带宽不能满足需要时应使用光缆。图 5-18 所示为水平干线子系统布线线缆长度示意图。

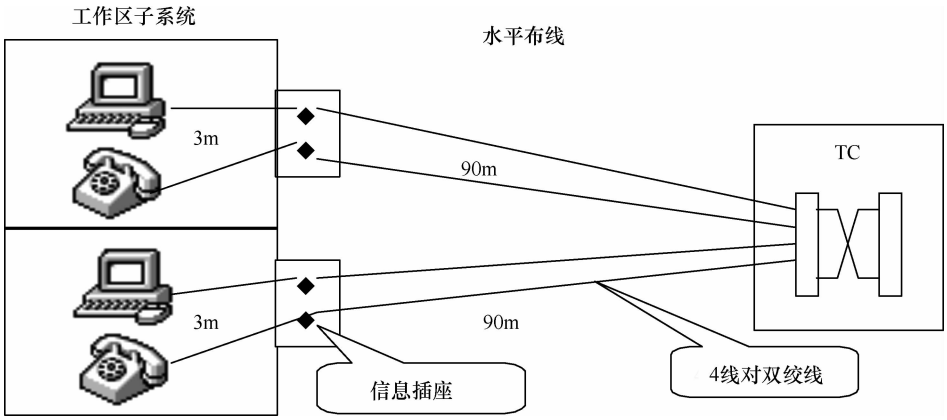


图 5-18　水平干线子系统布线线缆长度示意图

3. 垂直干线子系统的设计

垂直干线子系统由连接主设备间至各楼层配线间之间的线缆构成。其功能是把各分层配线架与主配线架相连；其任务是通过建筑物内部的传输电缆，把各个楼层管理间的信号通过设备间和终端接口送往外部网络；其目的是用主干电缆提供楼层之间通信的通道，使整个布线系统组成一个有机的整体，既满足当前需求，又适应今后的发展需要。垂直干线子系统的布线结构通常采用分层星形拓扑结构，即每个楼层配线间均需采用垂直主干线缆连接到大楼主设备间，而垂直主干线缆和水平系统线缆之间的连接需要通过楼层管理间的跳线来实现。垂直干线子系统示意图如图 5-19 所示。

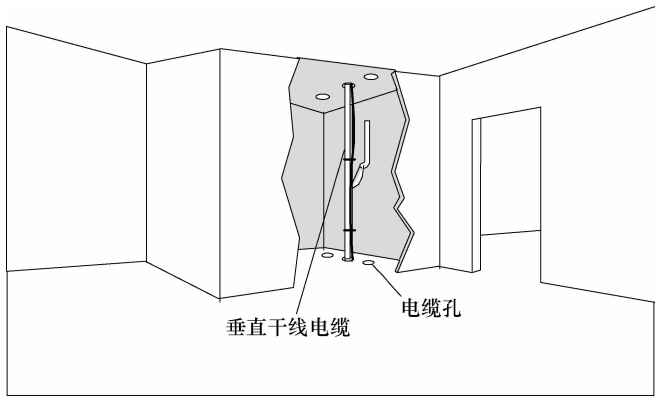


图 5-19　垂直干线子系统示意图

根据垂直干线子系统示意图可看出其设计范围是：各楼层管理间与设备间之间的电缆所使用的竖向或横向通道、主设备间与计算机中心主机房间的电缆、主设备间与建筑物电缆入口之间的电缆等。此外，在设计时应尽量使干线电缆的位置位于建筑物的中心，同时缆线不应布放在电梯、供水、供气、供暖、强电等竖井中。

4. 设备间子系统的设计

设备间通常是设置在每幢大楼的适当位置，并进行网络管理以及管理人员值班的场所。设备间子系统由综合布线系统的建筑物进线设备、电话、数据、计算机等各种主机设备及其保安配线设备等组成。这些设备及其保安配线设备宜设置在一个房间内，必要时，可以分别设置，但程控电话交换机及计算机主机房离设备间的距离不宜太远。

此外，设备间内的所有进线终端设备应该采用色标区别各种不同用途的配线区，从而便于用户对整个系统的管理。设备间子系统示意图如图 5-20 所示。

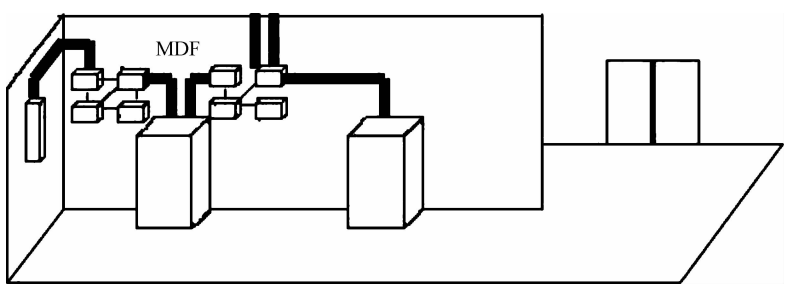


图 5-20　设备间子系统示意图

（1）设备间子系统位置的选择

设备间子系统是一个公用设备存放的场所，也是日常管理设备的地方。在确定设备间的位置时应根据建筑物的结构、综合布线规模、管理方式以及应用系统设备的数量等进行综合考虑，择优选取。在具体确定时可遵循以下原则：

1）应尽量建在建筑物平面及其综合布线干线子系统的中间位置或者在 1、2 层，并尽可能靠近建筑物电缆引入区和网络接口，以方便干线线缆的进出。

2）应尽量靠近服务电梯，以便装运笨重设备。

3）应尽量避免设在建筑物的高层或地下室以及用水设备的下层。

4）应尽量远离强振动源和强噪声源。

5）应尽量避开强电磁场的干扰源。

6）应尽量远离有害气体源以及存放腐蚀、易燃物的地方。

7）设备间应该能为将来可能安装的所有装备提供足够的空间。

8）设备间的位置应选择在环境安全、干燥通风、清洁明亮和便于维护管理的地方。

9）设备间的位置应便于安装接地装置，根据房屋建筑的具体条件和通信网络的技术要求，按照接地标准选用切实有效的接地方式。

（2）设备间的建筑要求

在进行设备间建筑结构的设计时需依据设备大小、设备搬运以及设备重量等因素而设计。设备间的高度一般为 2.5～3.2m。设备间门的大小至少为高 2.1m，宽 1.5m。设备间的楼板承重设计一般分为两级：A 级≥500kg/ m^2；B 级≥300kg/ m^2。

（3）设备间子系统的环境要求

由于设备间子系统内放置着大量精密的电子设备，如计算机、计算机网络设备、电话程控交换机、建筑物自动化控制设备等硬件设备，设备的性能和运行状况容易受到外界环境（主要指温度、湿度、供电、防火和防尘）的影响，因此在设计时必须对设备间环境问题进行认真考虑。设备间内的环境设置可以参照国家标准《电子信息系统机房设计规范》（GB 50174—2008）等相关标准及规范。

1）温度、湿度要求。网络设备间对温度和湿度的要求比较高，一般将温度和湿度分为 A、B、C 级，设备间可按某一级执行，也可以综合执行。在设计设备间温、湿度时可参照 3 个级别进行设计。设备间三级别湿度和温度参数表见表 5-7。

表 5-7　设备间三级别湿度和温度参数表

项目	A 级	B 级	C 级
温度/℃	夏季：22 ±4 冬季：18 ±4	12～30	8～35
相对湿度	40%～65%	35%～70%	20%～80%

设备间的温度、湿度和尘埃对微电子设备的正常运行及使用寿命都有很大的影响，过高的室温会使元件失效率急剧增加，使用寿命下降；过低的室温又会使磁介质变脆，容易断裂。温度的波动会产生“电噪声”，使微电子设备不能正常运行。相对湿度过低，容易产生静电，对微电子设备造成干扰；相对湿度过高，会使微电子设备内部焊点和插座的接触电阻增大。尘埃或纤维性颗粒积聚，以及微生物的作用还会使导线腐蚀断掉。所以在设计设备间时，除了按《计算机场地通用规范》（GB/T 2887—2011）执行外，还应根据具体情况选择安装独立的空调系统。空调系统的主要功能是满足环境温度、湿度以及通风量的要求，即加热或降温，调节空气的温度；加湿或降湿，调节空气的湿度；增强空气的流动速度；增加空气的洁净程度。

2）防尘要求。设备间内的电子设备对尘埃要求较高，尘埃过多会影响设备的正常工作，降低设备的工作寿命。此外，设备间地面一般应先刷防尘绝缘漆进行处理以增强设备间的防尘功能。设备间的尘埃指标一般可分为 A、B 两级，其具体尘埃量度表见表 5-8。

表 5-8　设备间两级别尘埃量度表

项目	A 级	B 级
粒度/μm	>0.5	>0.5
个数/（粒/dm^3）	<10000	<18000

3）电磁场干扰及噪声要求。设备间内无线电干扰场强在频率 0.15～1000MHz 范围内，磁场干扰场强不大于 800A/m，噪声应小于 70dB。如果长时间在 70～80dB 的噪声环境下工作，会严重影响人的身心健康和工作效率。

4）电力供应要求。设备间供电电源应满足频率为 50Hz，电压为 380V/220V，相数为三相五线制、三相四线制或单相三线制的要求。

设备间内供电总容量是将设备间内存放的每台设备用电量的标称值相加后，再乘以系数得到的。从电源室（房）到设备间使用的电缆，除应符合 GBJ232—1982《电气装置安装工程施工及验收规范》中配线工程的规定外，载流量应减少 50%。设备间内的设备所用的配电柜应设置在设备间内，并应采取防触电措施。

此外，设备间应采用 UPS 不间断电源，以防止停电造成网络通信中断。UPS 电源应提供不低于 2h 的后备供电能力。UPS 功率大小应根据网络设备功率进行计算，并具有 20%～30% 的余量；同时设备间电源设备应具有过电压、过电流保护功能，以防止对设备的不良影响和冲击。设备间三级别供电参数表见表 5-9。

表 5-9　设备间三级别供电参数表

项目	A 级	B 级	C 级
电压变动	-5%～5%	-10%～7%	-15%～10%
频率变动	-0.2%～0.2%	-0.5%～0.5%	-1～1
波形失真率	<±5%	<±7%	<±10%

5. 建筑群子系统的设计

建筑群子系统也称楼宇管理子系统。一个企业或某政府机关可能分散在几幢相邻或不相邻的建筑物内，但彼此之间的语音、数据、图像和监控等系统可用传输介质和各种支持设备（硬件）连接在一起。连接各建筑物系统之间的传输介质和支持设备（硬件）组成一个建筑群综合布线系统，连接各建筑物之间的缆线组成建筑群子系统。建筑群子系统结构示意图如图 5-21 所示。

在建筑群子系统中常见的电缆布线方法是地下管道电缆布线，管道系统的设计方法就是把直埋电缆设计原则与管道设计结合在一起。当考虑建筑群管道系统时，还要考虑接合井。在建筑群管道系统中，接合井的平均间距约为 180m，或者在主结合点处设置接合井。接合井可以是预制的，也可以是现场浇筑的。应在结构方案中标明使用哪一种接合井。预制接合井是较佳的选择。现场浇筑的接合井只在下述几种情况下才允许使用：该处的接合井需要重

建；该处需要使用特殊的结构或设计方案；该处的地下或头顶空间有障碍物，因而无法使用预制接合井；作业地点的条件（例如沼泽地或土壤不稳固等）不适于安装预制人孔。地下管道电缆的布线方式如图 5-22 所示。

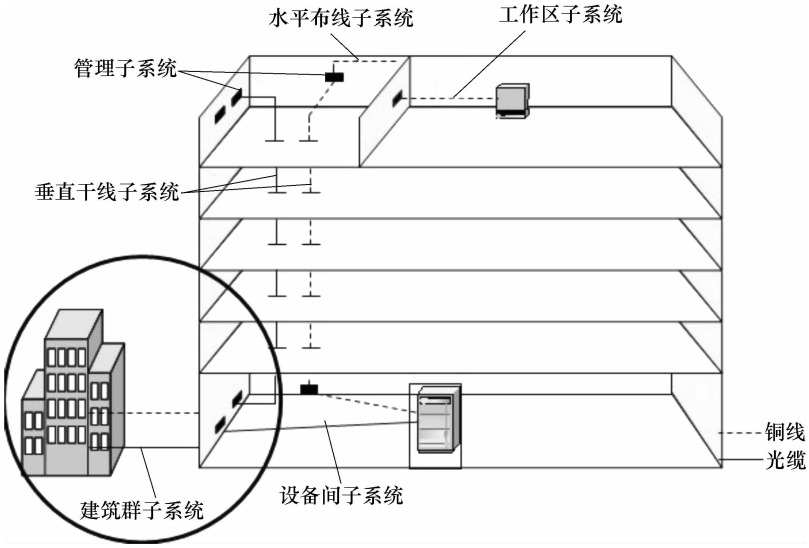


图 5-21　建筑群子系统结构示意图

6. 管理子系统的设计

管理子系统也称管理间子系统，为连接其他子系统提供手段，它是连接垂直干线子系统和水平干线子系统的设备。其主要设备是配线架、HUB、交换机、机柜和电源等。管理子系统示意图如图 5-23 所示。

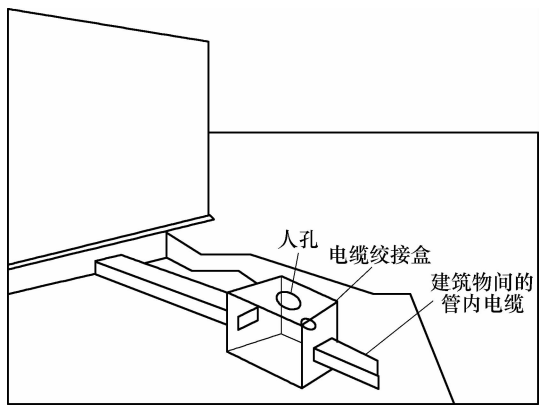


图 5-22　地下管道电缆的布线方式

根据管理间的实际应用需求，需要在管理间内建立一个可调节的、安全的而又能得到保护的环境系统，为此就需要满足：室温保持在 18 ~ 27℃，相对湿度保持在 30% ~ 55%，保持室内无尘、通风良好，安装合适的、符合法规要求的消防系统，安装至少能耐火 1h 的防火墙（从地板到天花板）和阻燃漆，确保至少有一扇窗留作安全出口，确保室内至少有高度为 2. 55m 的无障碍空间，门至少为 90 ~ 210cm，地板的承载能力至少为 500kg/m^2，以及确保凡是需要安装布线硬件的地方，墙壁均覆盖涂有阻燃漆的胶合板或者采用耐火胶合板。

当管理间的面积为 1. 8m^2 时（1. 2m × 1. 5m），可容纳端接 200 个工作区所需的连接硬件和其他设备，若端接的工作区超过 200 个，则在该楼层增加 1 个或多个二级管理间。若管理间同时兼作设备间时，其面积不应小于 10m^2。

在设计综合布线系统时，应该考虑在每一楼层都设立一个管理间用来管理该层的信息

点，摒弃以往几层共享一个管理间子系统的做法，这也是布线的发展趋势。管理间中主要放置集线器、交换机、配线架、语音 S110 集线面板等网络连接及管理设备。管理间子系统提供了与其他子系统连接的手段，使得管理员有可能安排或重新安排路由，通信线路能够延续到建筑物内部的各个信息插座，以实现综合布线系统的管理。

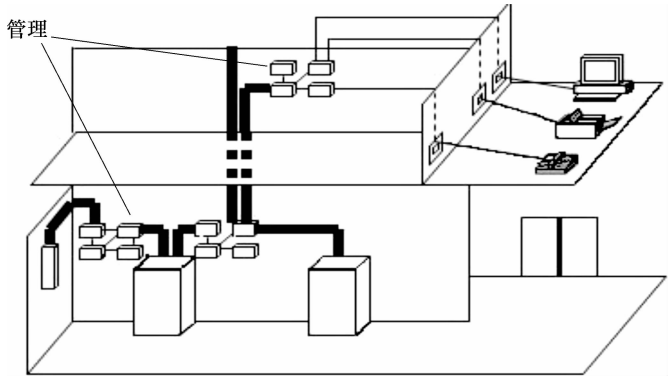


图 5-23　管理子系统示意图

5.5　综合布线系统工程施工技术

5.5.1　综合布线系统工程施工要点

首先，要做好施工准备工作。施工准备工作是保证综合布线工程顺利施工，全面完成各项技术指标的重要前提。施工准备工作一般可分为阶段性施工准备和作业条件的施工准备。阶段性施工准备，是指在工程开工之前针对工程所做的全面准备工作；作业条件的施工准备，是指为某一施工阶段或某一部分工程或某个施工环节所做的准备工作，它是局部性、经常性的施工准备工作。

1. 施工的基本要求

1）综合布线系统工程的安装施工，须按照《建筑与建筑群综合布线系统工程验收规范》中的有关规定进行，也可以根据工程设计要求进行。

2）在智能化小区的综合布线系统工程中，凡与本地电话网络有关，安装施工的基本要求应遵循国家通信行业《本地电话网用户线线路工程设计规范》等标准中的规定。

3）综合布线系统工程中所用的线缆类型和性能指标、布线部件的规格和质量等均应符合我国通信行业标准的规范或设计文件的规定。在工程施工中，不得使用未经鉴定的器材和设备。

4）施工现场要有方案设计的技术人员进行监督、指导，以确保传输线路的工作质量。

5）布线标记要清晰、有序，以确保后续工作的正常进行。

6）要测试检查已敷设完毕的线路，以确保线路的畅通、无误。要检查线路标记是否准确无误，检查线路的敷设是否与施工图样一致等。

7）可敷设一些备用线缆，以便个别线路出问题时，备用线缆可及时、有效地代替这些出问题的线路。

8）高、低压线须分开敷设，以避免电涌干扰。高、低压线平行敷设时，其间隔应按规范中的相关规定执行。

2. 施工技术准备

1）施工人员应熟悉施工图样，了解设计内容及设计意图，清楚工程所采用的设备、材料和图样所提出的施工要求，明确综合布线工程与主体工程和其他安装工程的交叉配合，以便及早采取措施，不与其他工程发生位置冲突。

2）熟悉与工程有关的其他技术资料，如施工及验收规范、技术规程、质量检验评定标准，以及制造厂商提供的资料，即安装使用说明书、产品合格证、试验记录数据等。

3）编制具体施工方案。在全面熟悉施工图样的基础上，依据图样并根据施工现场情况、技术力量及技术装备情况，综合编制出合理的施工方案。

4）编制工程预算。工程预算包括工程材料清单和施工预算。

3. 施工现场环境与器材的准备

（1）施工现场环境的检查

1）对综合布线系统的线缆施工现场和工作区，准备安装的或现有的信息插座、配线架及所有连接器件进行勘察和检查，在符合《建筑与建筑群综合布线系统设计规范》和设计文件相应要求后，方可进行安装。

2）综合布线系统设备的安装包括工作区、交接间、设备间及进线间在内的环境条件，除了要适应配线线缆和连接器件的安装要求外，如果与其他机房合建，还应满足终端设备、计算机网络设备、电话交换机、传输设备及各种接入网设备等的安装要求。不应在温度高、灰尘多、存在有害气体、易爆等场所进行安装，还应避开振动和强噪声、高低压变配电及强电干扰严重的场所。

3）综合布线系统对建筑、结构、采暖通风、供电、照明等工种及预埋管线等配合要求，一般由建筑专业人员承担设计。弱电设计人员应该提出比较详细的布线系统安装环境要求，如室内的净高、地面荷载、线缆出入孔洞位置及大小、室内温湿度条件要求等。

4）如果布线系统设备安装在旧房屋内时，一般可以根据具体情况，在保证综合布线质量的前提下，适当降低对房屋改建的要求。房屋设计还应符合环保、消防、人防等规定。

5）在工业与民用建筑安装工程中，综合布线施工要求与主体建筑有着密切的关系。如配管、配线及配线架或配线柜的安装等，都应在土建实施工程中密切配合，做好预留孔洞的工作。这样，既能加快施工进度，又能提高施工质量：既安全可靠，又整齐美观。

6）要保证照明、供电和接地等条件。如施工中的安全的供电源，以及照明安全灯具等。要注意电源插座应用带保护的电源插座等用电安全问题。根据所连接的设备情况，部分电源插座应考虑采用 UPS 的供电方式。

（2）器材的检查

应在施工之前对综合布线工程所用的各种器材进行检查。若无出厂检验证明或与设计不符，不得在工程中使用。经检验合格的应做好记录，对不合格的器材应单独存放，以备核查与处理。

1）各种钢材和铁件的材质、规格、型号应符合设计文件的规定和质量标准。各种管材的管身和管口不得变形，接续配件齐全有效。各种管材（如钢管、硬质 PVC 管等）内壁应光滑，无节疤，无裂缝；其材质、规格、型号及孔径壁厚应符合设计文件的规定和质量标

准。

2）工程中所用的电缆、光缆的规格、形式和型号应符合设计的规定和合同要求。成盘的电缆（一般以 305m 配盘）、光缆的型号和长度等，应与出厂时的产品质量合格证一致；线缆的外护套应完整无损，电缆所附标志、标签的内容应齐全、清晰。抽查抽测线缆的性能指标；如用户有要求，应附有本批量电缆的技术指标。

（3）接插件及配线设备的检验

配线模块和信息插座及其他接插件的部件应完整，器材质量应满足设计要求；保安单元过电压、过电流保护的各项指标应符合有关规定；光纤插座连接器及其接续设备的形式、规格应符合设计要求。

5.5.2 综合布线工程施工常用工具与使用

综合布线系统的线缆通常是通过暗敷管路或桥架、槽道进行安装敷设。综合布线工程的施工可以分为管槽安装施工、线缆敷设施工、设备安装和调试初验等阶段。施工各阶段都要用到以下常用工具。

1. 双绞线端接工具

（1）剥线钳

使用压线工具上的刀片来剥除双绞线的外套，可能会伤及导线的绝缘层。剥线钳使用高度可调的刀片或利用弹簧张力来控制切割深度，切割时不会伤及导线的绝缘层。图 5-24 所示为一种剥线钳。

（2）压线钳

用来压接 8 位的 RJ-45 连接器和 4 位、6 位的 RJ-11、RJ-12 连接器，可同时提供切线和剥线的功能。常见的压线工具有 RJ-45 或 RJ-11 单用压线钳，也有两用压线钳，如图 5-25 所示。

图 5-24　剥线钳

图 5-25　压线钳

（3）打线刀

用于将双绞线压接到信息模块和配线架上，信息模块和配线架是采用绝缘置换连接器（IDC）与双绞线连接的。IDC 实际上是 V 形豁口的小刀片，当把导线压入豁口时，刀片割开导线的绝缘层，与其中的铜线接触。打线工具由手柄和刀具组成，它是两端式的，一端具有打接和裁线功能，可剪掉多余的线头；另一端不具有裁线功能。在打线工具的一面会有清晰的“CUT”字样，使用户能够识别正确的打线方向。单对打线工具如图 5-26 所示。还有 5 对打线工具，是一种多功能端接工具，如图 5-27 所示。

2. 光纤安装施工工具

光纤安装施工工具分为光缆敷设工具和光缆端接工具。光缆敷设工具主要包括滑车、牵

引机等，与双绞线电缆布线使用的敷设工具相同。下面重点介绍光缆布线中使用的端接工具。

图 5-26　单对打线工具

图 5-27　5 对打线工具

（1）光纤剥离钳

用于剥除光纤涂敷层和外护层。光纤剥离钳的种类很多，图 5-28 所示为双口光纤剥离钳，它具有双开口、多功能的特点，钳刃上的 V 形口用于精确剥离 250μm、500μm 的涂敷层和 900μm 的缓冲层，第二开口用于剥离 3mm 的尾纤外护层。

（2）光纤剪刀

光纤剪刀如图 5-29 所示，主要功能是用来修剪凯弗拉线（Kevlar）。凯弗拉线是一种韧性很高的线，用于光纤加固。光纤剪刀是一种防滑锯齿剪刀，复位弹簧可以提高剪切速度，只能用来修剪光纤的凯弗拉线，不能修剪光纤内芯玻璃层及作为剥皮之用。

图 5-28　双口光纤剥离钳

图 5-29　光纤剪刀

（3）光纤连接器压线钳

用于压接 FC、SC、ST 等连接器，如图 5-30 所示。

（4）光纤接续子

用于尾纤接续、不同类型的光缆转接、室内外永久或临时接续和光缆应急恢复，相当于个接头。光纤接续子有很多类型，图 5-31 所示为不需热熔的光纤接续子，也称光纤冷接子。它是一种简单、易用的光纤接续工具，可以接续多模或单模光纤。光纤接续子使用起来非常简单，没有太多的附件，几乎不需要培训，操作步骤为：剥纤并把光纤切割好，将需要接续的光纤分别插入接续子，直到它们互相接触，然后旋转凸轮锁紧并保护光纤。这个过程中无需使用任何黏结剂或其他专用工具。

图 5-30　光纤连接器压线钳

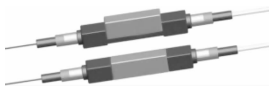


图 5-31　不需热熔的光纤接续子

（5）光纤切割工具

用于光纤的切割，包括光纤切割笔和光纤切割机。光纤切割笔用于光纤的简易切割，如图 5-32 所示。通用光纤切割机用于光纤的精密切割，如图 5-33 所示。

（6）光纤熔接机

主要是靠放出电弧将两头光纤熔化，同时运用准直原理平缓推进，以实现光纤模场的耦合。光纤熔接机是采用芯对芯标准系统进行快速、全自动熔接，能进行光纤接续工作，可以进行自动光纤类型识别，自动校准熔接位置，自动选择最佳熔接程序，自动推算接续损耗，如图 5-34 所示。

图 5-32　光纤切割笔

其他常用光缆施工工具还有光纤固化加热炉、手动光纤研磨工具、光纤头清洗工具、光纤探测器、常用光纤工具包等。

图 5-33　通用光纤切割机

图 5-34　光纤熔接机

5.5.3　配线架的安装与端接

目前常见的双绞线配线架有 110 配线架（见图 5-35）和数据配线架（见图 5-36）等类型。

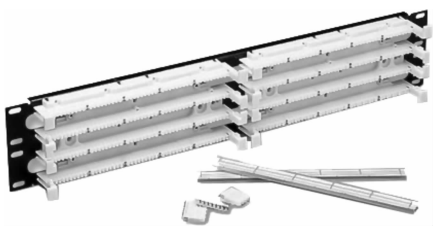


图 5-35　110 配线架

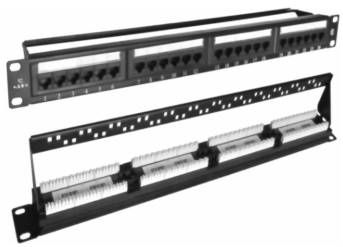


图 5-36　数据配线架

1. 110 配线架的端接

110 配线架是早期综合布线系统的核心产品，起着传输信号的转接、分配以及综合统一管理的作用，利用同一接口和同一种传输介质，通过连接不同信息的配线架之间的跳接来传输各种不同信息。目前常见的双绞线配线架采用 19in RJ-45 口 110 配线架，此种配线架背面进线采用 110 端接方式，正面全部为 RJ-45 口用于跳接配线。各厂家生产的模块式快速配线架的结构和安装方法基本相同。

1）先不要把模块放上去，按照片模上的颜色去打，从左到右，（蓝、橙、绿、棕、灰），再根据大对线上 的“色带”去打，从前打到最后。

2）把线打完之后，再把刚才的模块放上去，用力敲打，使其紧贴在配线架上。

3）最后根据刚才打完的模口，与配线架进行跳线，即可。

大对数的线序是这样的：

- 5 种主色：白色、红色、黑色、黄色、紫色。
- 5 种次色：蓝色、桔色、绿色、棕色、灰色。

25 对及以上的大对数电缆端接要注意其色序，其对数均为 25 的倍数，如 50 对、100 对、300 对。所以每组 25 对里面的着色顺序是完全一样的。区分方法是：在这些大对数电缆中，每个 25 对的线束组用彩色标记按照我们熟悉的色标顺序条进行捆扎，这样无论多少线对电缆都可以不必重复地进行标识了。这些颜色序号排列是从线缆中心向外层进行计数的，各层中计数方向应与单位内线对的计数方向一致。这种色标顺序在 110 配线系统中广泛应用。

2. 数据配线架的端接

数据配线架是管理子系统中最重要的组件，是实现垂直干线和水平布线两个子系统交叉连接的枢纽。配线架通常安装在机柜或墙上。通过安装附件，配线架可以全线满足 UTP、STP、同轴电缆、光纤、音视频的需要。在网络工程中常用的配线架有双绞线配线架和光纤配线架。

双绞线配线架的作用是在管理子系统中将双绞线进行交叉连接，用在主配线间和各分配线间。双绞线配线架的型号有很多，每个厂商都有自己的产品系列，并且对应 3 类、5 类、超 5 类、6 类和 7 类线缆分别有不同的规格和型号，在具体项目中，应参阅产品手册，根据实际情况进行配置。

模块化配线架主要应用于楼层管理间和设备间内的计算机网络电缆的管理。各厂家的模块化配线架结构及安装相类似，因此下面以 IBDN PS5E HD-BIX 配线架为例，介绍模块化配线架的安装步骤。

以 IBDN PS5E HD-BIX 配线架为例，具体安装步骤如下：

1）使用螺钉将 HD-BIX 配线架固定在机架上，如图 5-37 所示。

2）在配线架背面安装理线环，将电缆整理好固定在理线环中并使用绑扎带固定电缆，一般 6 根电缆作为一组进行绑扎，如图 5-38 所示。

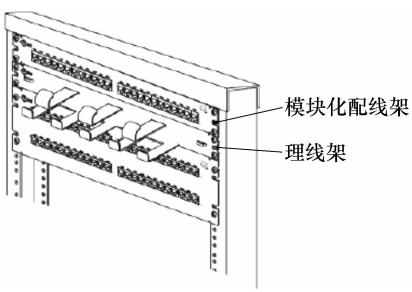


图 5-37　在机架上安装配线架

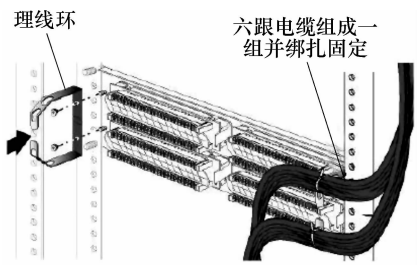


图 5-38　安装理线环并整理固定电缆

3）根据每根电缆连接接口的位置，测量端接电缆应预留的长度，然后使用平口钳截断电缆，如图 5-39 所示。

4）根据系统安装标准选定 T568A 或 T568B 标签，然后将标签压入模块组插槽内，如图 5-40 所示。

5）根据标签色标排列顺序，将对应颜色的线对逐一压入槽内，然后使用 IBDN 打线工具固定线对连接，同时将伸出槽位多余的导线截断，如图 5-41 所示。

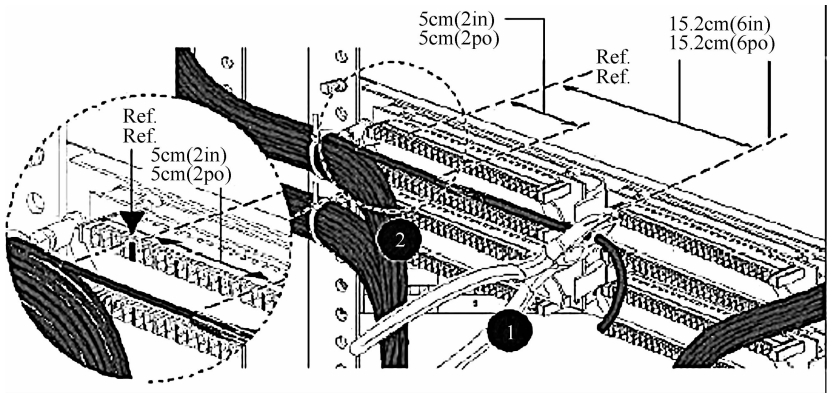


图 5-39　测量预留电缆长度并截断电缆

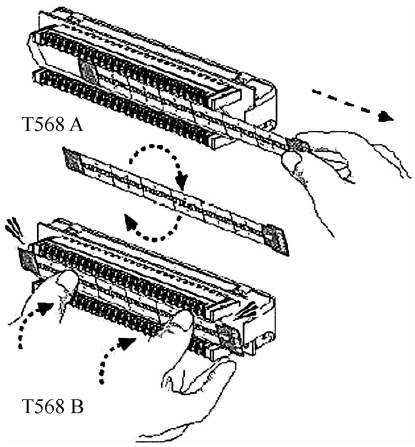


图 5-40　调整合适标签并安装在模块组插槽内

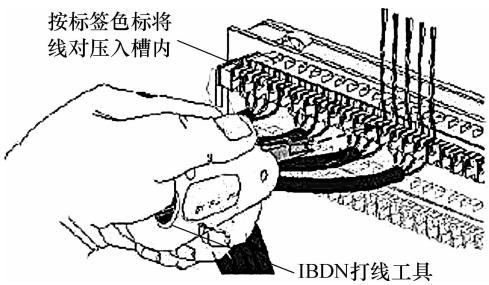


图 5-41　将线对逐次压入槽位并打压固定

6）将每组线缆压入槽位内，然后整理并绑扎固定线缆，如图 5-42 所示。

7）将跳线通过配线架下方的理线架整理固定后，逐一接插到配线架前面板的 RJ-45 接口，最后编好标签并贴在配线架前面板，如图 5-43 所示。

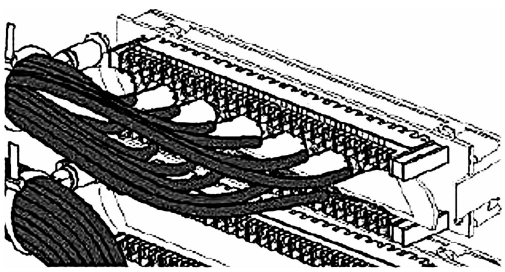


图 5-42　整理并绑扎固定线缆

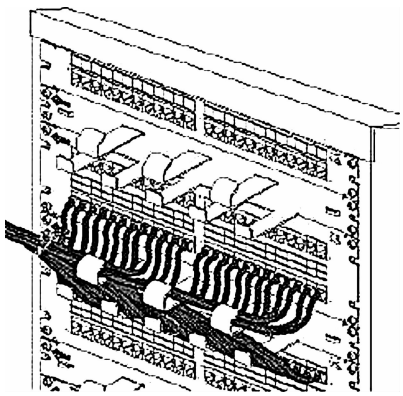


图 5-43　将跳线接插到配线架各接口并贴好标签

5.6　综合布线系统工程测试

5.6.1　综合布线系统测试的必要性

综合布线系统工程质量的好坏直接影响信息通信网络的正常运行。为了保证综合布线工程的质量，防止投入使用后出现网络故障，有必要对其进行严格的工程测试。

对于布线工程的施工方来说，测试的目的有两个：一个是提高施工的速度；另一个是向投资方证明工程的质量保证可靠。综合布线系统工程的测试分为电缆传输通道测试和光缆传输通道测试。

如果对综合布线系统不做测试，不进行合格性验收，工程是不能移交给用户使用的。综合布线系统工程的测试向用户提供质量保证，为工程的顺利验收做好准备。

5.6.2　测试标准与测试模型

1. 测试类型

综合布线的测试，从工程的角度来说可分为两类：验证测试和认证测试。

验证测试是在施工的过程中由施工人员边施工边测试，以保证每个连接的正确性。验证测试又叫随工测试，是边施工边测试，主要检测线缆的质量和安装工艺，以及时发现并纠正问题，避免返工。验证测试不需要使用复杂的测试仪，只需要使用能测试接线通断和线缆长度的测试仪。

认证测试是指对布线系统依照标准例行逐项检测，以确定布线是否能达到设计要求，包括连接性能测试和电气性能测试。认证测试又叫验收测试，是所有测试工作中最重要的环节，是在工程验收时对综合布线系统的安装、电气特性、传输性能、设计、选材和施工质量的全面检验。认证测试通常分为自我认证测试和第三方认证测试。

2. 测试标准

测试标准的两大组织是 TIA/EIA 和 ISO/IEC。主要可供参考的国际测试标准为 EIA/TIA 制定的 TSB-67《现场测试非屏蔽双绞线电缆布线系统传输性能技术规范》、EIA/TIA-568A《商用建筑电信布线标准》和 ISO/IEC 颁布的 ISO/IEC 11801《信息技术-用户房屋综合布线》。其中，TSB-67 包含了验证 EIA/TIA-568 标准定义的 UTP 布线中的电缆与连接硬件的规范。

由于所有的高速网络都定义了支持 5 类双绞线，所以用户要找一个方法来确定他们的电缆系统是否满足 5 类双绞线的规范要求。为了满足用户的需要，EIA 制定了 EIA586 和 TSB-67 标准，它们适用于已安装好的双绞线连接网络，并提供了一个用于认证双绞线电缆是否达到 5 类线要求的标准。由于确定了电缆布线满足新的标准，用户就可以确定他们现在的布线系统能否支持未来的高速网络。

随着超 5 类、6 类系统标准的制定和推广，目前 EIA568 和 TSB-67 标准已提供了超 5 类、6 类系统的测试标准。对于 EIA568-B 标准已经不再认可 4 对 4 类双绞线和 5 类双绞线电缆。TIA/EIA 制定的 EIA/TIA-568-B 和 ISO/IEC 颁布的 ISO/IEC 11801 2002 相比，主要内容大体一致，名词称谓略有差别，个别性能要求不同。

国家标准的制定主要也是以 EIA/TIA-568 和 ISO/IEC 颁布的 ISO/IEC 11801 等作为依

据，并结合国内具体实际情况进行了相应的修改。目前，国家制定的测试标准是 GB/T 50312—2007《建筑与建筑群综合布线系统工程验收规范》，该标准包括了目前使用最广泛的 5 类电缆、5e 类电缆、6 类电缆和光缆的测试方法。

网络电缆及其对应标准见表 5-10。

表 5-10　网络电缆及其对应标准

电缆类型	网络类型	标准
UTP	令牌环 4Mbit/s	IEEE 802. 5 for 4Mbit/s
UTP	令牌环 16Mbit/s	IEEE 802. 5 for 16Mbit/s
UTP	以太网	IEEE 802. 3 for 10Base-T
RG58/RG58 Foam	以太网	IEEE 802. 3 for 10Base2
RG58	以太网	IEEE 802. 3 for 10Base5
UTP	快速以太网	IEEE 802. 12
UTP	快速以太网	IEEE 802. 3 for 10Base-T
UTP	快速以太网	IEEE 802. 3 for 100Base-T4
URP	3、4、5 类电缆现场认证	TIA 568、TSB-67

不同标准所要求的测试参数见表 5-11。

表 5-11　不同标准所要求的测试参数

测试标准	接线图	电阻	长度	特性阻抗	近端串扰	衰减
EIA/TIA568A、TSB-67	*		*		*	
10base-T	*		*	*	*	*
10Base2			*	*	*	
10Base5			*	*	*	
IEEE 802. 5 for 4Mbit/s	*		*	*	*	*
IEEE 802. 5 for 16Mbit/s	*		*	*		*
100Base-T	*		*	*	*	*
IEEE 802. 12 100Base-VG	*		*	*	*	*

电缆级别与应用的标准见表 5-12。

表 5-12　电缆级别与应用的标准

级别	频率	量　程　应　用
3	1 ~ 16MHz	IEEE 802. 5 Mbit/s 令牌环、IEEE 802. 3 for 10Base-T IEEE 802. 12 100Base-VG、IEEE 802. 3 for 10Base-T4 以太网 ATM 51. 84/25. 92/12. 96Mbit/s
4	1 ~ 20MHz	IEEE 802. 5 16Mbit/s
5	1 ~ 100MHz	IEEE 802. 3 100Base-T 快速以太网、ATM 155Mbit/s
6	200MHz	IEEE 802. 3u 1000Base-千兆以太网
7 *	600MHz	

注：* 表示国际标准化组织还没有通过正式标准。

3. 测试内容

综合布线工程测试内容主要包括 3 个方面：工作区到设备间的连通状况测试、主干线连通状况测试、跳线测试。

（1）电缆传输通道的验证测试

对于电缆传输通道的验证测试，主要检查施工中常见的连线故障：电缆标签错、连接开路、双绞电缆接线图错（包括：错对、极性接反、串绕）以及短路。具体说明如下：

1）开路、短路：在施工时由于安装工具或接线技巧问题以及墙内穿线技术问题，会出现这类故障。

2）接反：同一对线在两端针位接反，如一端为 1-2，另一端为 2-1。

3）错对：将一对线接到另一端的另一对线上，比如一端是 1-2，另一端接在 4-5 针上。最典型的错误就是打线时混用 T568A 与 T568B 的色标。

4）串绕：就是将原来的两对线分别拆开而又重新组成新的线对。因为出现这种故障时，端对端的连通性是好的，所以用万用表这类工具检查不出来，只有用专用的电缆测试仪才能检查出来。由于串绕使相关的线对没有扭结，因此在线对间信号通过时会产生很高的近端串绕。

（2）光缆传输通道的测试

对于光缆传输通道的测试主要考察测量参数，具体包含以下几个方面：

1）光纤的连续性

进行连续性测量时，通常是把红色激光、发光二极管或者其他可见光注入光纤，并在光纤的末端监视光的输出。如果在光纤中有断裂或其他的不连续点，在光纤输出端的光功率就会减少或者根本没有光输出。光通过光纤传输后，功率的衰减大小也能表示出光纤的传导性能。如果光纤的衰减太大，则系统也不能正常工作。光功率计和光源是进行光纤传输特性测量的一般设备。

2）光纤的衰减

光纤的衰减主要是由光纤本身的固有吸收和散射造成的。衰减系数应在许多波长上进行测量，因此选择单色仪作为光源，也可以用发光二极管作为多模光纤的测试源。

3）光纤的带宽

带宽是光纤传输系统中的重要参数之一，带宽越宽，信息传输速率就越高。在大多数的多模系统中，都采用发光二极管作为光源，光源本身也会影响带宽。这是因为这些发光二极管光源的频谱分布很宽，其中长波长的光比短波长的光传播速度要快。这种光传播速度的差别就是色散，它会导致光脉冲在传输后被展宽。

5.7　综合布线系统设计方案案例

本节以某高校新校区建设综合布线系统工程为例，介绍大型园区网络综合布线工程的设计方法。

5.7.1　工程概况

某高校新校区规划总建筑面积约 48 万 m^2，其中计划实施面积为 404770m^2，远期实施面

积为 72365m^2。校园规划图如图 5-44 所示，网络机房位于信息中心大楼的首层。

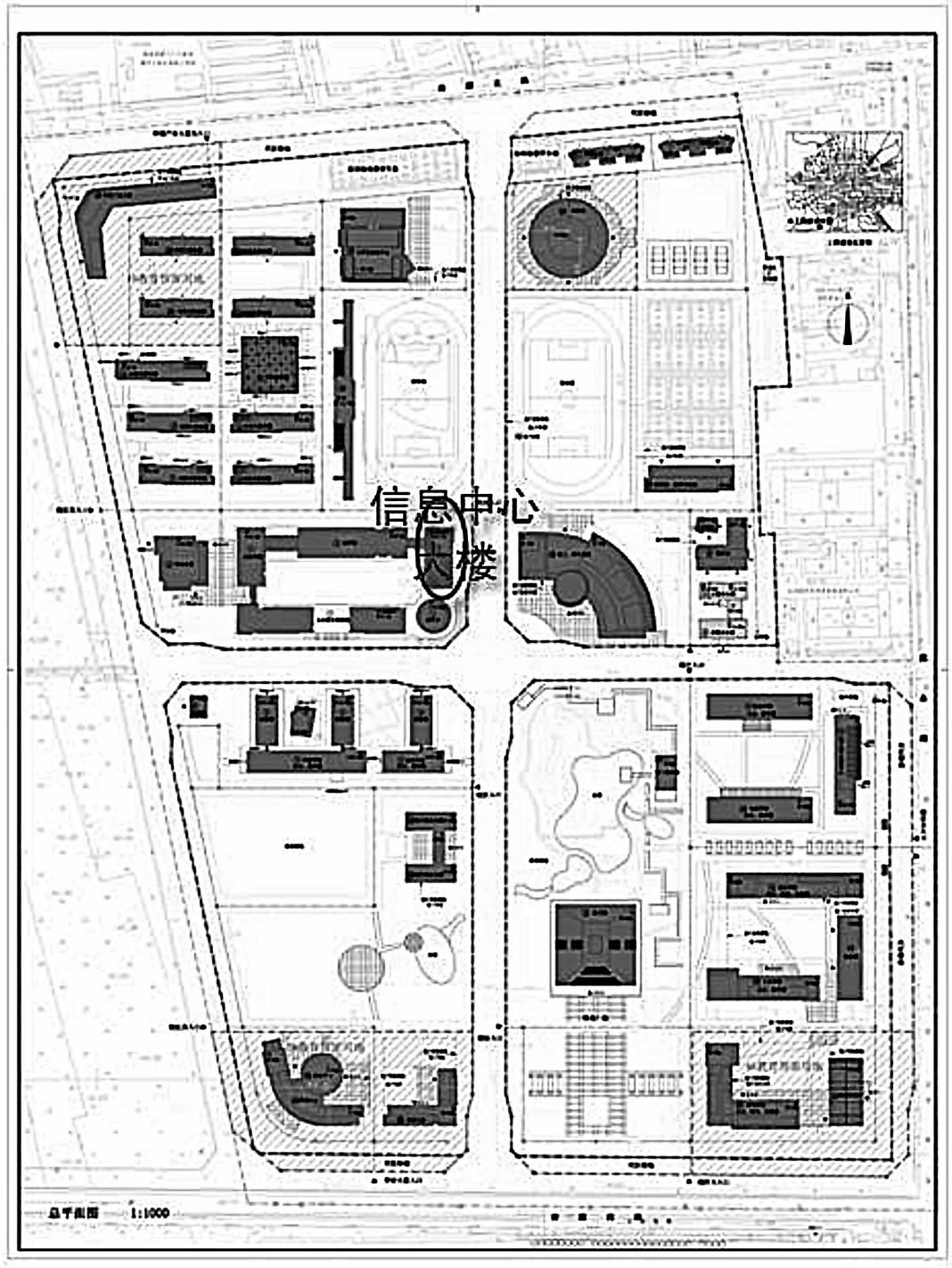


图 5-44　校园规划图

信息中心所在位置基本上为整个园区的中心地带，整个网络采用结构化布线，从信息中心网络核心机房敷设至校园内各楼宇，校园网的综合布线系统采用三级星形结构，可提供满足数据、语音、音频、视频等多媒体应用的服务能力。

5.7.2　功能需求

数据网络系统不仅能提供满足数据、图像、音频、视频等多媒体应用的服务和传输能力，而且能灵活地通过电信运营商提供的接口以多种方式与 Internet 互联。

为了能适应今后 10 年甚至更长时间内网络和通信技术的高速发展，综合布线系统应能满足当今流行的网络技术（如交换式以太网技术），特别是国际上普遍应用的千兆以太网技术的要求。着重强调为今后更先进的如万兆位网络系统应用打好坚实的基础。该综合布线系统应不但能达到目前的国际先进水平，而且应该具有高度的开放性，能为标准的智能型建筑物提供一个高效率、高标准和全开放的基础平台。

建成后的综合布线系统将担负大量的图文信息的传输工作，主要功能如下：

1）数据语音的信号传输。覆盖楼内的高速 1000Mbit/s，满足发展的业务、办公自动化和多媒体会议以及语音电话的需求。

2）灵活、可靠。结构化布线要有前瞻性，具有最大的可靠性、灵活性、兼容性和开放性。

3）广泛的技术和设备适应性。支持目前和正在形成的各种工业和商业标准，支持各种计算机、终端、传真机、电话、不同的局域网/城域网/广域网/、会议电视、多媒体点播。

5.7.3　总体设计思路

依据综合布线系统设计与施工的相关规范和标准，采用结构化综合布线的理念和技术，将园区综合布线系统整体工程分解为 3 个方面的工程进行设计。

1）建筑群之间的布线系统。建筑群之间全部采用单模光缆，从学校信息中心大楼网络核心机房总配线间，通过学校弱电地下管道直埋光缆的方式，敷设至各楼宇的总弱电间。

2）单体建筑楼宇内的布线系统。单体建筑楼宇内的布线系统全部采用六类综合布线系统。

3）单体建筑楼宇内的弱电间的设计。按照弱电间设计规范的要求，在对大楼进行规划设计时，对各单体建筑的弱电管井、弱电间进行基建设计和施工，为综合布线系统提供弱电机房环境。

在进行新校区整个弱电系统的规划设计时，根据各个系统的特点和特殊要求进行充分考虑，校园一卡通系统、多媒体教学系统、安防监控系统等的布线应考虑专网建设，构建单独的网络传输系统，最大程度的共享光缆资源。

整个布线系统由工作区子系统、水平子系统、垂直干线子系统、设备间子系统、建筑群子系统及管理子系统等 6 个子系统构成。综合布线系统工程需按下列 7 个部分进行设计：

1）工作区子系统。一个独立的需要设置终端设备的区域宜划分为一个工作区。工作区应由配线子系统的信息插座模块延伸到终端设备处的连接缆线及适配器组成。

2）水平子系统。由工作区的信息插座模块、信息插座模块至电信间配线设备的配线电

缆和光缆、电信间的配线设备及设备缆线和跳线等组成。根据单体建筑高度和宽度的特点，电信间的分布应设置在不同的楼层并管理相邻楼层的网络信息点。

3）垂直干线子系统。干线子系统应由设备间至电信间的干线电缆和光缆、安装在设备间的建筑物配线设备及设备缆线和跳线组成。

4）设备间子系统。设备间是在每幢建筑物的适当地点进行网络管理和信息交换的场地。对于综合布线系统工程设计，设备间主要安装建筑物配线设备。

5）进线间。进线间是建筑物外部通信和信息管线的入口部位，并可作为入口设施和建筑群配线设备的安装场地，可以与设备间在一起，也可以单独设置。

6）建筑群子系统。建筑群子系统应由连接多个建筑物之间的主干电缆和光缆、建筑群配线设备及设备缆线和跳线组成。

7）管理子系统。管理应对工作区、电信间、设备间、进线间的配线设备、缆线、信息插座模块等设施按一定的模式进行标识和记录。

进行从新校区全校弱电管网的设计到各单体楼宇的建筑规划设计时，需加强与建筑设计院设计人员的沟通。新校区建筑设计人员充分考虑网络综合布线系统设施及管线、线槽和管井的合理设计，并且预留足够面积的设备间、配线间和进线间等，对上述设计均须满足国家最新颁布的综合布线系统工程设计规范（GB 50311—2007）等相关标准和规范。

建筑群子系统是指将一栋建筑的线缆延伸至建筑群内的其他建筑的通信设备和设施，实现楼群之间网络系统的信息连接。从新校区网络核心机房至各汇聚主节点所在的楼宇全部采用室外铠装单模光纤接入，从各汇聚主节点所在楼宇至各个单体建筑，根据实际距离情况采用室外铠装单模或多模光纤接入。

建筑群子系统采用地下管道敷设方式，路由方式充分利用新校区弱电管网。弱电管网的地下通道要预留足够的管槽，支持综合布线系统主干光缆的铺设。设计弱电管网时要充分考虑为二期和三期建设预留足够的管道和管井，以便于今后网络扩展及施工。

建筑群主干布线系统包括从新校区网络核心机房至各区域汇聚主节点所在楼宇设备间、从区域汇聚主节点所在楼宇设备间至各单体建筑设备间的主干光纤铺设工程，包括主干光缆铺设、光纤熔接、跳线、设备间线缆接入等相关布线产品安装和工程实施。综合布线主干光缆分布图如图 5-45 所示。

1）一级主干：从网络核心机房至全校各区域汇聚主节点所在楼宇设备间建设万兆主干链路，采用 4 根 24 芯单模光纤铺设。

2）二级主干：从各区域汇聚主节点所在楼宇设备间至该区域各个单体建筑的设备间建设万兆主干链路，采用 2 根 24 芯单模/多模光纤铺设。

5.7.4 各子系统设计

1. 信息点设置原则

对于新校区各房间单元功能定位的不同，信息点的设置也不尽相同。信息点的设置需要考虑一定的冗余。各个单体建筑在综合布线时均需要预留充足的无线网络接入信息点。对网络布线系统数据部分的设置标准见表 5-13。有特殊需求的布线要求，针对各单位、各部门提出的特殊需求进行信息点分布设计。

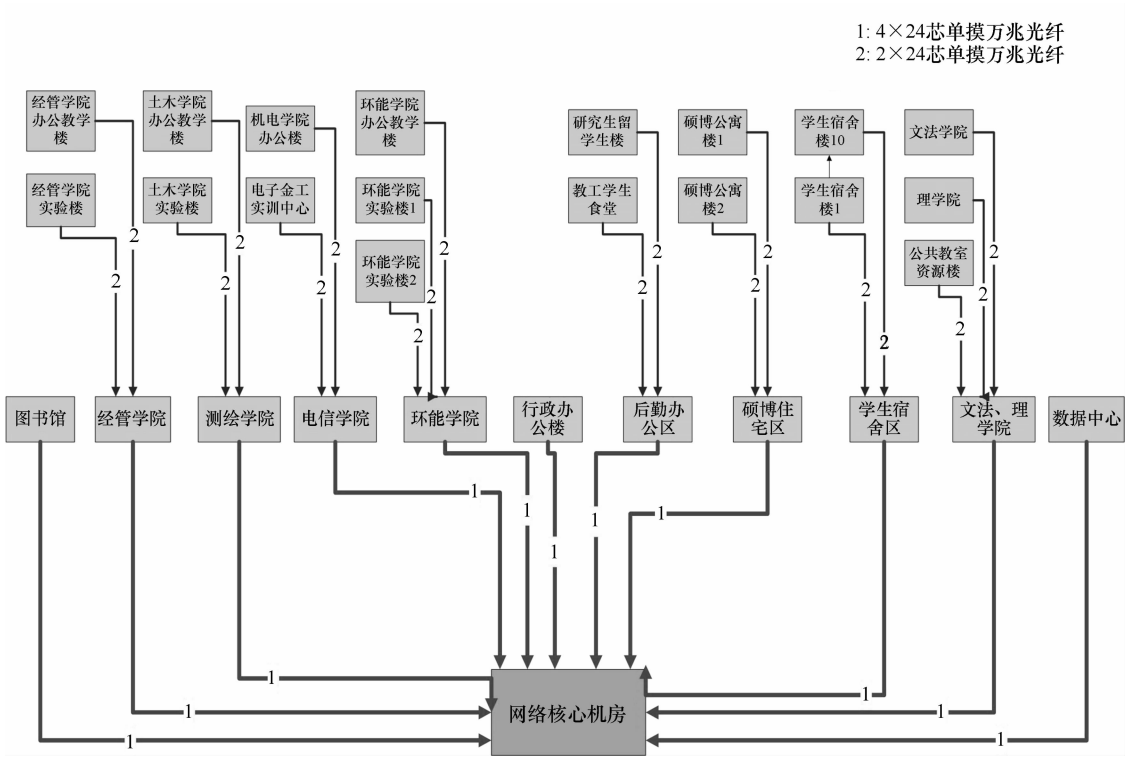


图 5-45　综合布线主干光缆分布图

表 5-13　信息点分配标准

功　能　单　元	信息点个数（数据部分）	备　　注
单班非多媒体教室	2	
多媒体教室	4	
学术报告厅值班室	2	
学术报告厅、阶梯教室	4	2 个数据，2 个无线接入
校领导办公室	4	1 个台式机，1 个笔记本，1 个 IP 电话，1 个视频会议
教职工办公室（每 10m^2）	3	2 个数据，每房间 1 个冗余
普通实验室	4	实验室内部采用交换机自行组建局域网
小型会议室	2	1 个数据，1 个无线接入
大会议室（80m^2 以上）	4	2 个数据，2 个无线接入
各单体建筑门厅	3	2 个数据，1 个无线接入
展示厅及陈列室	2	
学生宿舍（4 人间）	5	每个床位 1 个，每房间 1 个冗余
研究生宿舍（2 人间）	3	每个床位 1 个，每房间 1 个冗余
硕博公寓	3	每间 2 个数据，每房间 1 个冗余
值班室	2	

（续）

功 能 单 元	信息点个数（数据部分）	备 注
监控室	4	
休息室	2	
每层楼道左中右、单体建筑顶层两个外侧	6	预留无线接入
其他辅助用房	2	保证每个房间有网络接入

2. 工作区子系统

工作区子系统是指终端设备到信息插座的连接部分，包括信息插座、用户终端设备连线和终端适配器（特殊情况下使用）。用户终端设备连线是两端均为 6 类 RJ-45 水晶头的一根 6 类接插软线，用于连接各种不同的用户设备。不同型号的话机、计算机终端通过该设备连线可方便地连接到信息插座上。工作区布线示意图如图 5-46 所示。

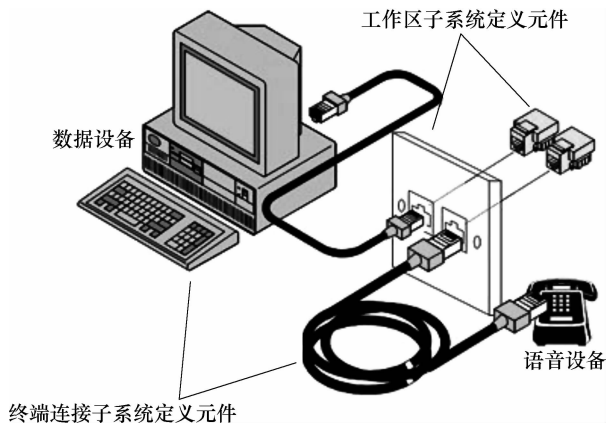


图 5-46 工作区布线示意图

根据相关的规范标准，建筑物工作区面积设计见表 5-14。

表 5-14 建筑物工作区面积设计表

建筑物类型及功能	工作区面积/m^2
信息中心等终端设备较为密集的场地	3 ~ 5
办公区	5 ~ 10
会议、会展	10 ~ 60
商场、生产机房、娱乐场所	20 ~ 60
体育场馆、候机室、公共设施区	20 ~ 100
工业生产区	60 ~ 200

工作区面积划分表见表 5-15。

表 5-15　工作区面积划分表

建筑物名称	层数	幢数	面积/m^2	信息点计算模式	点数
基础部	5	3	33784	办公区	5066
建筑学院	6	1	16481	公共设施区	310
土木学院	6	1	28733	公共设施区	538
测绘学院	6	1		公共设施区	
环能学院	5	2	27991	公共设施区	524
电气学院	6	1	34883	公共设施区	654
机电学院	6	1		公共设施区	
经管学院	5	2	22327	公共设施区	418
文法学院	5	1	6400	公共设施区	120
学生宿舍	8	8	104272	办公区	10000（数据）、2500（语音）
	7	2		办公区	
学生食堂	2	1	20075	公共设施区	376
教工食堂	3			公共设施区	
学生餐厅	2	1		公共设施区	
学生活动中心	1	1	4948	办公区	742
图书馆	7	1	25200	公共设施区	472
科技产业大厦	9	3	30052	办公区	4507
培训中心	11	1	25422	办公区	3813
会议中心	2	1		办公区	
行政办公	5	1	7255	办公区	1088
体育馆			8000	公共设施区	150
后勤办公	4	1	3194	办公区	479
医务室	3	1	4510	办公区	676
市政用房	3			办公区	
教工之家			1200	公共设施区	22
计划实施面积：404770m^2					
行政办公			9888	办公区	1483
科技产业			11769	办公区	1766
博物馆	3	1	9008	公共设施区	168
研究生＼留学生院			41700	公共设施区	781
远期实施合计：72365m^2					
总共（计划＼远期实施）：477135m^2					
合计信息点总数：36653m^2					

根据建设部相关规范，建筑物给出的建设面积不能直接作为使用面积来应用，而国家标准 GB 50311—2007 规定的工作区实际上指的是使用面积，因此，需要将上表中的建筑面积

转换为使用面积，建设部的相关规范给出了换算系数：S = J *（0.6 ~ 0.75），考虑到目前的建筑物使用面积都比较大，因此本工程按照系数 0.75 来取。具体计算方法以基础部为例来说明：基础部建筑物属于办公区，工作区按照国家标准规定，应按照 $10m^2$/个来划分；基础部的建筑面积为 $33784m^2$，则使用面积为 33784 * 0.75 = $25338m^2$，25338/10 = 2533.8 个工作区，即 2533 个工作区。按照国家标准规定，每个工作区宜按照两个信息点计算，则基础部的信息点数量为 5066 个。

对于如学生宿舍，特点是工作区小，通常小于 $5m^2$，而信息量很大，特别是宿舍住宿采用上下铺时，信息密度变得比较高；而另一方面，对于话音系统来讲，则又比较少，往往一间宿舍安装一路电话即可。因此在计算此类建筑物时，学生宿舍区每个宿舍按 4 个学生计算，每个学生配置一个网络端口，则共有 10000 个端口。

对于如建筑学院等教室类建筑，国家标准规定可在 20 ~ $100m^2$ 来取值，考虑到教室只需要在讲台处的多媒体台处安装两个信息点即可，因此，对于如建筑学院类的教室类建筑，工作区按照 $80m^2$ 来取，每个工作区两个信息点。

3. 配线子系统

配线子系统是国家布线标准 GB/T 50311—2007 中的正式称谓，在其他布线标准中，把配线子系统称作“水平布线子系统”。

配线子系统示意图如图 5-47 所示。

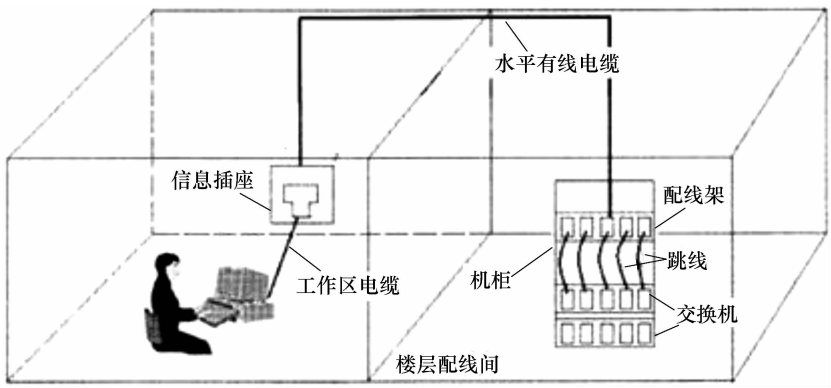


图 5-47　配线子系统示意图

配线子系统是由楼层配线间至各工作区的水平电缆组成，该电缆一端卡接在工作区中的信息插座上，另一端卡接在楼层配线间的配线架上。水平线缆的敷设采用金属线槽与预埋暗管相结合的方式，具体安装依据施工图和施工规范进行。水平电缆的最大布线长度小于 85m，小于标准中的 90m 距离要求，充分保证了系统的性能。

4. 干线子系统（垂直干线子系统）

干线子系统是指设备间子系统与管理子系统之间的连接电缆和光缆，是建筑物中的主干线路。垂直干线均采用 16 芯以上单模光缆。单模光缆通过建筑物的弱电井从大楼主配线间（BD）引至各楼层配线间（FD）。采用点到点端接。对光缆的安装将严格按照施工规范进行。光缆两端打标记以便于管理。其他的楼宇如果楼层较低，从降低成本的角度，应部分采用六类双绞线进行干线级联。干线子系统示意图如图 5-48 所示。

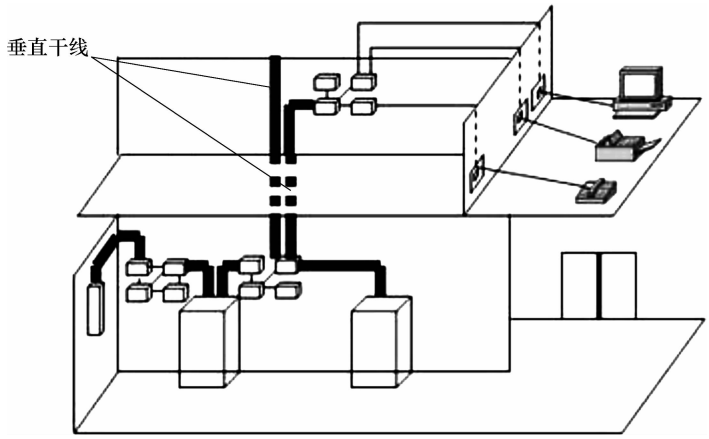


图 5-48　干线子系统示意图

5. 管理子系统

管理子系统是由大楼内的配线架部分组成，包括光纤配线架、快接式 6 类配线架、110 配线架、接插软线。一般来说，综合布线工程中有两种端接铜缆的配线架，一种是快接式配线架，这种配线架适用于综合布线系统数据传输，管理简单，对管理者的要求不高，适用于 6 类线缆的端接；另一种是 110 配线架，它可以支持语音和数据的传输，对管理者的要求较高，它适用于 5 类及 5 类以下线缆的端接，并且它的价格要比快接式配线架便宜。

在本工程中，根据需要在每个配线间放置一个 42U 标准机柜，机柜内安装快接式配线架和光纤配线架。光纤配线架选用 19in 1U 机柜式光纤配线架。

在各个分配线间为保证机柜空间容量，我们设置标准 42U 网络机柜。然后把光纤配线架、24 口 6 类配线架安装在机柜中对语音数据点进行管理。

6. 建筑群子系统

本工程为校园网工程，建筑物数量众多，需要仔细考虑建筑群布线设计。根据以往的经验及当前技术发展状况，采用单模光缆作为校园数据干线，在每栋建筑物的主配线间处设置分支点，与每栋建筑物的综合布线干线相连接。建议单模光缆采用大芯数的光缆，以满足未来发展的需求。校园网干线数据光缆结构示意图如图 5-49 所示。

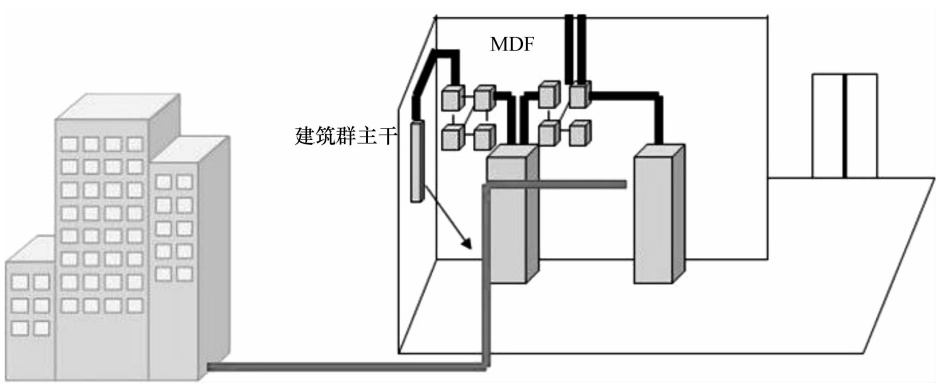


图 5-49　校园网干线数据光缆结构示意图

5.7.5 设备间的环境要求

设备间一般也叫设备间子系统，在实际工程中也是弱电间。设备间是设置进线设备，进行网络管理且有管理人员值班的地方，设备间由综合布线系统的建筑物进户线设备、电话、网络设备、计算机等组成，是放置设备的地方。由于设备间安装设备较多，所以要做好网络产品和电话交换机的空间预留，设备的安放要便于管理人员工作。

设备间统一配置42U标准机柜，用来安放计算机网络设备和光缆。具体光缆和大对数的端接依据施工图来进行。机柜摆放前面净空不宜小于0.8m，后面净空不宜小于0.6m，机柜的具体位置将依据施工图样来摆放。由于综合布线系统本身并不包含有源设备，所以原则上讲，设备间和综合布线的关系不大，但是，综合布线是计算机网络和话音系统的线路基础，为了便于用户管理，综合布线的配线架要求放在设备间里，或者两者距离不能超过30m。

设备间是整个配线系统的中心单元，它的环境条件考虑的是否恰当直接影响到将来信息系统的正常运行及维护使用的灵活性。建议其室内照明不低于300Lx，并应提供UPS电源配电盘以保证网络设备运行及维护的供电。如数据布线采用屏蔽布线系统时，应备有合适的接地线。设备间的环境条件建议如下：

1）室温应保持在18～27℃，相对温度保持在30%～55%。

2）保持室内无尘或少尘，通风良好。

3）安装合适的消防系统。

4）使用防火门，至少能耐火1h的防火墙和阻燃漆。

5）提供合适的门锁，至少要有一扇窗口留作安全出口。

6）分配线间应注意避免电磁干扰和雷击，安装阻值小于1Ω的接地装置；尽量远离存放危险物品的场所、强电和电磁干扰源（如发射机和电动机）。

7）设备间的地板负重能力至少应为500kg/m^2。

8）结构化布线系统中典型的配线间，可以走进人的最小安全尺寸是120cm×150cm，标准的天花板高度为240cm，门的大小至少为高2.1m宽1m，外开。

9）所用材料必须符合IEC对抗拉力、压力和拉力的承受标准。

5.7.6 管道设计

1. 管道的路由选择

室外管道的路由和整个弱电系统的布置有关，凡是综合布线需要敷设的地方都需要室外管道。新建的校园不建议采用架空布线的方式，而是全部采用地下弱电管道。室外管道从网络机房开始延伸到校园的各个角落，以满足校园计算机网等系统敷设线缆的需要。管道的路由一般选择在校园的主要道路上。但由于校园的主干道上的地下管线很多，诸如下水管、供水管、煤气管等，同时道路相对较窄，因此将弱电管道的路由选择在靠近建筑物的绿化带不失为一个好方法。

2. 管道容量、管道材料和孔径的选择

（1）管道容量

大多数的学校都选择将各个中心设置在一个建筑单体内，如计算机网络中心，这样便于

弱电系统的维护和管理。出入中心的管道的容量要根据目前所需要敷设线缆的种类、数量来确定，管孔的含线率为 50% 左右，并且要考虑留有 40% 左右的富余量，以满足今后 20 ~ 30 年的需求。在考虑管道容量时，要结合目前弱电各个系统的组成来决定所需敷设线缆的数量和走向。不同系统的线缆如光缆、通信电缆、广播、有线电视电缆、监控用视频应分别敷设在不同的管孔内。

（2）管道材料

管道的材料一般采用 PVC 管，只有在一些车辆进出口和管道埋深达不到规定的场所才考虑采用钢管。不建议采用混凝土的水泥管作为地下通信管道。

（3）孔径的选择

在校园的主干路由和分支路由上，应采用统一规格的管材，一般为 ϕ98PVC。对于各个弱电系统从管道分支出去的地下管线，由于穿放的线缆种类单一、数量少，可以用 ϕ40 的钢管，例如室外广播点、室外监控点等。由于布点分散，当从主干管道分支至这些布点处时，地下管线可以采用 ϕ40 的钢管，并且可以缩小这些管线的埋深。铺设方式为沿道路绿化带下铺设。

本 章 小 结

本章以大型园区网络综合布线系统设计为主题，讨论了大型园区综合布线系统方案设计和施工技术。

1）介绍了综合布线系统的相关概念、特点、结构和组成。

2）详细介绍了综合布线系统中的网络传输介质。

3）重点介绍综合布线系统设计与施工技术，并对测试技术进行了介绍。

4）以高校校园网为例，介绍了一个网络综合布线系统设计方案。

第 6 章　网络核心机房建设

6.1　网络核心机房基本概念

6.1.1　网络核心机房的概念

网络核心机房是指在一个物理空间内实现信息的集中处理、存储、传输、交换、管理的场所，而计算机设备、服务器设备、网络设备、存储设备等通常认为是网络核心机房的关键设备，关键设备运行所需环境因素，如供配电系统、机柜系统、消防系统、精密空调系统、机房集中监控系统、综合布线系统、机房装修等通常被认为是关键物理基础建设。

对于大型 IT 企业、通信运营商、政府机构、金融行业、机场、保险等信息化程度高、数据量大、业务运行要求高等企事业单位，往往都建设有一流的网络核心机房和数据中心，为信息系统的运行提供符合国家标准规范的机房环境，如图 6-1 所示。


图 6-1　网络核心机房环境

6.1.2　网络核心机房的组成

如果我们把网络核心机房看作是一个系统，那么可以梳理出一个网络核心机房应该包含的一些主要系统：

1）机房装饰子系统。机房环境包含装修装饰工程所达到的符合标准的机房空间布局、简单的机房基建设施，包括墙面、地面、防静电地板、吊顶、防火门、隔断等。

2）机房供电子系统。机房供电包括市电引入、线路、UPS 电源、UPS 电池间、发电机组、电源布线、插座、PDU、照明、防雷接地等。

3）空调通风子系统。机房空调通风子系统包括精密空调机组、室外机、水冷管道、新风系统。

4）机房弱电子系统。机房弱电子系统包括机柜、桥架、配线架、理线架、光缆、跳

线、KVM 系统、机房动力环境监控、网络管理平台等。

5）消防子系统。消防子系统主要包括灭火系统、气体灭火装置、自动报警装置等。

6.1.3　电子机房的类型及特点

电子机房主要有计算机机房、电信机房、控制机房、屏蔽机房等。这些机房既有电子机房的共性，也有各自的特点，其所涵盖的内容不同，功能也各异。

1. 计算机机房

计算机机房内放置有重要的数据处理设备、存储设备、网络传输设备及机房保障设备。计算机机房的建设应考虑以上设备的正常运行，确保信息数据的安全性以及工作人员身心健康的需要。

大型计算机机房一般由无人区机房、有人区机房组成。无人区机房一般包括小型机机房、服务器机房、存储机房、网络机房、介质存储间、空调设备间、UPS 设备间、配电间等；有人区机房一般包括总控中心机房、研发机房、测试机房、设备测试间、设备维修存储间、缓冲间、更衣室、休息室等。

中、小型计算机机房可将小型机机房、服务器机房、存储机房等合并为一个主机房。

2. 电信机房

电信机房是每个电信运营商的宝贵资源，合理、有效、充分地利用电信机房，对于设备的运行维护、快速处理设备故障、降低成本、提高企业的核心竞争力等具有十分重要的意义。电信机房一般是按不同的功能和专业来区分和布局的，通常分为设备机房、配套机房和辅助机房。

设备机房是用于安装某一类通信设备，实现某一种特定通信功能的建筑空间，便于完成相应专业内的操作、维护和生产，一般由传输机房、交换机房、网络机房等组成。配套机房是用于安装保证通信设施正常、安全和稳定运行的设备的建筑空间，一般由计费中心、网管监控室、电力电池室、变配电室和油机室等组成。

辅助机房是除通信设施机房以外，保障生产、办公、生活需要的用房，一般由运维办公室、运维值班室、资料室、备品备件库、消防保安室、新风机房、钢瓶间和卫生间等组成。在一般智能建筑中通信机房经常与计算机网络机房合建。

3. 控制机房

随着智能化建筑的发展，为实现对建筑中智能化楼宇设备的控制，必需设立控制机房。控制机房相对于数据机房、电信机房而言，机房面积较小，功能比较单一，对环境要求较低，但却关系到智能化建筑的安全运行及设备、设施的正常使用。

控制机房包括楼宇智能控制机房、保安监控机房、消防控制室、卫星接收机房、视频会议控制机房等。这些控制机房的共同特点是机房内均有操作人员工作，在保证电子设备运行的同时还要保证操作人员的身心健康。根据设备及操作的要求，这些控制机房也有其相应的特点。

1）楼宇智能控制机房：主要用于安放楼宇智能控制的主机及控制设备，对智能建筑内的公共照明、空调系统、电梯及建筑内的风、水、电等机电设备进行实时监控，以确保智能建筑的安全运行。

2）安保监控机房：内设监控主机及终端显示设备，对建筑各出入口、车库、走道、电

梯轿箱等进行视频监控、防盗报警等。

3）消防控制室：是火灾自动报警和联动系统的控制中心，也是火灾时灭火指挥和信息中心，具有十分重要的地位和作用。《高层民用建筑设计防火规范》GB 50045—1995 和《建筑设计防火规范》GB 50016—2006 对消防监控机房的设置范围、位置、建筑耐火性能都做了明确规定，并对其主要功能提出了原则性要求。

4）卫星接收机房：主要用于安放卫星接收机、调制解调器、混合器、放大器、有线光缆接入设备、各频段接收显示器等。卫星接收机房一般是位于建筑顶层，有利于卫星电视信号的传输。

5）视频会议控制机房：主要用于安放视频会议主控单元（MCU）、调音台、音响扩声系统、信号传输设备、控制台设备、信号源机柜等。但由于一般的视频会议控制机房面积较小，在设备布置时应根据房间的具体情况灵活布置。

4. 屏蔽机房

为了有效地防止电磁干扰式噪声、辐射对电子设备和测量仪器的影响，并严防电子信号泄露从而威胁到机密信息的安全，国家机关、军队、公安、银行、铁路等单位需要建立屏蔽机房。有保密要求的数据机房应建设屏蔽机房，确保数据在处理过程中，其信号不泄露，从而满足数据保密的要求。一些对抗电磁干扰要求较高的环境，如通信设备的测试试验室等场所，需要建设屏蔽机房，以防止外界电磁信号的干扰。有强电磁干扰设备的机房应进行相应的电磁屏蔽处理，以避免干扰临近机房设备的正常运行。

6.2 网络核心机房规划与设计

6.2.1 机房布局规划设计

网络核心机房建设是集建筑、电气、安装、网络等多个专业技术于一体的工程，核心机房的环境必须满足计算机等各种微机电子设备和工作人员对温度、湿度、洁净度、电磁场强度、消防、保安、电源质量、防雷和接地等的要求。网络核心机房规划设计及施工的优劣直接关系到各网络系统能否稳定可靠地运行，保证各类信息通信畅通无阻。校园网核心机房按照功能划分，可设置以下几个分区：

1）网络主干设备区：网络主干设备区通常是整个园区网络的核心部位。为保证设备的安全使用和便于维护，必须在核心机房中设置独立的网络主干设备区。在网络主干设备区中的设备包括网络核心交换机、路由器、防火墙设备、接入设备、通信线缆及接入光电信号转换设备、校园局域网骨干光纤配线架、机房网络布线配线架、VPN 服务接入设备及无线网桥接设备等。

2）服务器区：服务器区是安置提供信息服务的设备的工作区。这些服务器提供的信息服务除了面向校园网用户外，通常还面向外部网络的用户。由于服务器工作间的设备多、噪声大、发热量高，在规划设计时应该注意满足良好的通风、散热和隔绝噪声的要求。为便于维护和管理，在服务器工作区中还应该配置专门的隔架或轨道，按上下双层或多层放置各种服务器，同时配备多计算机控制器 KVM（Keyboard、Video、Mouse）以及机柜专用电源分配单元 PDU（Power Distribution Unit）。

3）系统维护工作区：专门的系统维护工作区是进行系统管理必要的工作条件，各种网络设备和计算机设备的维护，新系统和新软件的试用评估通常都在这里进行。

4）信息技术人员办公区：信息技术人员办公区应该包括网络与系统维护人员办公室、软件开发与应用人员办公室、系统资料和数据备份存档室。

5）机房监控区：机房监控区是对全网设备集中监控和管理的区域。

大型园区网络的核心机房内涉及的设备较多，如何合理布局是一项较重要的工作。应充分考虑机房的面积、设备数量及大小、UPS、空调、电力柜、消防等设备的具体要求，规划设计合理的走廊及维修空间。

目前，一种常见的机房布局为：机柜按列分组摆放，使用 UPS 作为列头柜，分别给每列机柜中的 PDU 供电。该布局结构可以减少 UPS 电池集中摆放所造成的地板负重，同时也可根据每列机柜中的设备不同选用不同的 UPS 负载。

6.2.2　机房工程

根据网络核心机房的功能及其组成，一般大型机房工程可以分为装修工程、弱电工程、电气工程、空调新风系统、消防工程五大部分。机房整体工程分解图，如图 6-2 所示。

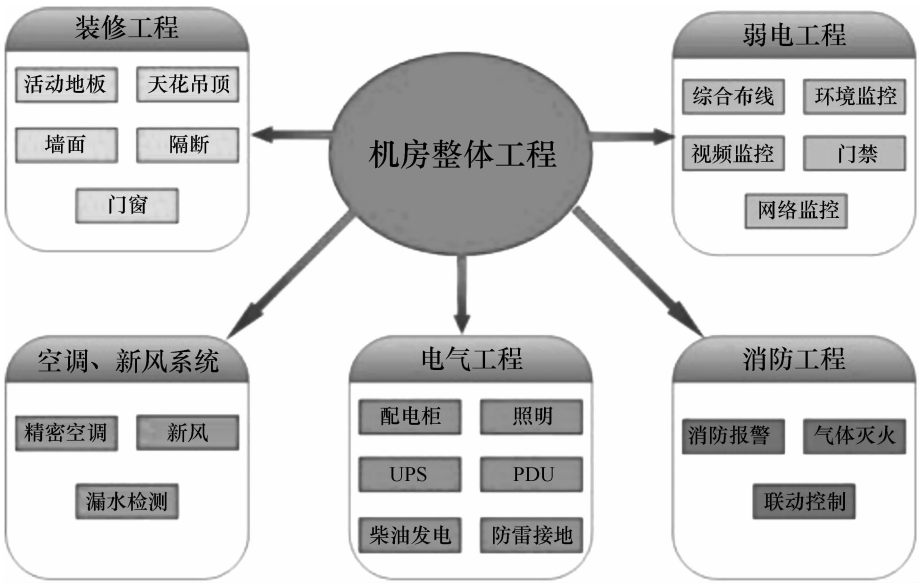


图 6-2　机房整体工程分解图

1. 装修工程

装修工程主要是完成机房建筑环境的设计和施工，重点是防静电地板、天花吊顶等，除了要做到精细化设计，主要是材料选用方面要达到环保节能的要求，并且隔断墙、钢制防火门等都要符合标准。

2. 弱电工程

弱电工程是整个机房工程中非常重要的一块，需要完成机房的综合布线、环境监控、视频监控、门禁、网络监控、KVM 系统、网络管理平台等。特别是综合布线系统要做到精细化设计，并且充分考虑从列头柜到各机柜之间的布线方式、跳线走线方式，发挥桥架的作

用，做到美观整洁、标识有序、便于管理。

3. 空调、新风系统

空调、新风系统的设计与安装是大型网络机房必须解决好的问题。要实现机房恒温恒湿并且符合机房温湿度环境要求，必须要充分考虑空调容量、备份机组等功率设计、室外机位置、新风系统引入等线路设计，机房冷风通道、热风通道的设计。因为机房空调需要冷水管道引入和排水，还要充分考虑漏水自动检测，并且设计报警系统。

4. 电气工程

安全、可靠是供配电系统机房设计和施工的关键出发点。由于机房的供配电系统、照明、设备防雷、机房接地、UPS 不间断电源等与一般的强电设计有所不同，又与弱电专业的十几个子系统密切相关。因此，在设计和施工前必须充分了解并掌握供电对象。充分搜集机房设备和系统的资料才能做好电源布置和系统设计，从而合理地满足机房的用电要求。

5. 消防工程

消防工程包含火灾自动报警系统、消火栓系统、气体灭火系统、防排烟系统、消防应急疏散系统、消防广播通信系统、防火隔断系统（卷帘门、防火门）、泡沫灭火系统、漏电火灾自动报警系统、消防电梯系统。

6.3 网络机房选址及机房装修

6.3.1 机房选址考虑的因素

选择网络核心机房的地理位置很重要。对于一个大型园区，网络核心机房选址有一些细节性因素要充分考虑。

1）要考虑布线的经济合理性，服务相应时间最省。一般应选择园区中心位置附近的楼宇，从网络布线的角度，它到达整个园区任何一个楼宇的距离都是最短的，具有从中心到局部的敷设作用，也符合网络结构化布线和网络拓扑结构的设计要求。

2）要考虑避免一定的干扰。网络核心机房要避开强电磁场干扰，应远离水灾和火灾隐患区域，远离强振源和强噪声源；还应远离产生粉尘、油烟、有害气体以及生产或贮存具有腐蚀性、易燃、易爆物品的场所。

3）机房所在的楼宇电力供应稳定可靠，交通、通信应便捷，自然环境清洁。

4）对于多层或建筑物内的电子信息系统机房，在确定主机房的位置时，应对设备运输、管线敷设、雷电感应和结构荷载等问题进行综合分析和经济比较，选择各方面条件都较好的位置。

5）网络核心机房不宜设置在地下一层或高层。目前从选址上看，网络核心机房设计在一层是比较理想的，对管线敷设、设备搬运、管理等都比较有利。

6）机房外要充分考虑室外空调机的安装条件；同时也要考虑新风管道进入核心机房的有利条件。

6.3.2 机房室内装修

众所周知，网络核心机房的装饰，不同于普通的计算机房、办公室、家庭装饰。核心机

房装饰工程是一项系统工程，是电子科学技术和装饰艺术的综合。机房内放置有复杂的电子设备和机电设备，对装饰的要求，主要是满足 IT 设备对机房提出的技术要求，在机房装饰艺术上以既大方舒适，又满足其技术要求为原则。对装饰材料的选择要达到吸音、防火、防潮、防变形、抗干扰、防静电等要求。装饰后，要使整个机房色调柔和、通透宽敞、不压抑、舒适，以期达到现代化的装饰水平和视觉效果。

电子信息系统机房室内装饰装修包括吊顶、隔断、地面处理、活动地板、内墙和顶棚及柱面处理、门窗制作安装及其他作业的施工及验收。关于机房室内装修，国家在《电子信息系统机房施工及验收规范》GB 50462—2008 中已做了明确细致的规定。室内环境污染的控制及装饰装修材料的选择应按现行国家标准《民用建筑工程室内环境污染控制规范》GB 50325—2010 的有关规定执行。各工种的施工环境条件应符合施工材料说明书的要求。吊顶、隔断墙、内墙和顶棚及柱面、门窗以及窗帘盒、暖气罩、踢脚板等施工的验收内容和方法，应符合现行国家标准《建筑装饰装修工程质量验收规范》GB 50210—2001 的有关规定。地面处理施工的验收内容和方法，应符合现行国家标准《建筑地面工程施工质量验收规范》GB 50209—2010 的有关规定。防静电活动地板的验收内容和方法，应符合国家现行标准《防静电地面施工及验收规范》SJ/T 31469—2002 的有关规定。其他方面的施工规范和细节在本书中不再赘述，可参阅国家标准执行。

6.4　供配电系统

6.4.1　供配电概述

机房电气工程中机房供配电系统是数据中心机房的生命线，因此要建一个好的机房，首先要将供配电问题解决好。在机房电气工程中，安全、稳定、可靠的电力供应是机房供配电系统设计的关键出发点。由于机房的供配电系统、照明、设备防雷、机房接地、UPS 不间断电源等与一般的强电设计有所不同，又与弱电专业的十几个子系统密切相关。因此，它们处于强、弱电专业设计分工的接合部分。

在机房供配电系统的设计中，经常出现的问题有：机房各子系统的设计深度差距较大；主要弱电机房预留的位置不合适，面积过大或偏小；弱电竖井中遗漏接地干线和电源插座；UPS 电源容量、支持时间长短不一；UPS 电源供电方式是采用集中式还是分散式不能确定；各子系统的供电和接地方式不规范等。在一部分设计文件中，还经常发现有文字说明描述不清楚、系统图和平面图五花八门、图形符号不按现行制图标准绘制等问题。

1. 电源布置和系统设计

设计和施工必须充分了解并掌握供电对象。充分搜集机房设备和系统的资料才能做好电源布置和系统设计，从而合理地满足机房用电需要。

机房应设单独电源管理间，用符合防火要求的隔墙与弱电设备隔离，避免电源管理间噪声、蓄电池酸碱液渗漏和电气火灾等传播到计算机设备机房内。通常的做法是设置电源管理间和电池间。将电源管理间和电池间分开独立设置的好处是：蓄电池房间可单独封闭管理，减少了腐蚀性的危害。

网络核心机房与电源管理间中间设单扇朝电源管理间方向开启的连通门，还可考虑设置

玻璃观察视窗。电源管理间应做水泥地面，为防潮、防湿可砌高 0.3 ~ 0.5m 的水泥平台搁置配电柜和 UPS 电源等。专用电池间与 UPS 电源室场景图如图 6-3 所示。


图 6-3　专用电池间与 UPS 电源室场景图

根据国家标准规范，不同类别的机房对电源的要求如下：

1）A 类机房：停电后会产生重大损失和社会影响，要求建立不停电电源系统。

2）B 类机房：停电后会产生一定损失和社会影响，要求建立备用电源系统。

3）C 类机房：停电后不会产生大的损失和社会影响，可按一般用户配置。

从电力应用方面，市电主要提供空调设备、普通照明和给排风、维修插座、一般动力等的电力。不间断电源 UPS 主供：主机设备、网络设备、保安监控设备、多媒体、消防、应急照明等。

2. 市电要求

对于达到一级负载的机房应该具备从不同变电站供给的双路供电，加上柴油发电机，通过应急电源柜切换后供给机房内的 UPS 和精密空调机组。双路供电应装配自动转换开关，实现自动倒闸。

备用发电机系统是至关重要的一个因素。即便其中有一个故障时，也能够直接向计算机和其他设备提供一个理想质量和容量的电力供应。发电机的设计应能够处理 UPS 系统或 IT 设备负载的谐波电流。备用发电机应该提供备用电源给所有的冷却设备，避免负载设备温度上升以及停止运行。如果发电机不支持这些系统，它们所带来的益处就显得很有限。在自动控制发生故障时，发电机应该能够采用手动控制。应该给每一个发电机输出提供瞬时电压浪涌抑制（TVSS）装置。

发电机燃料应该是柴油，这样起动比较快。考虑现场储藏量的要求，通常需要保证有可使用 4 小时到 60 天的储藏量。并且需要给所有燃料储藏系统提供一个远程的燃料监控和警报系统。由于微生物增长是柴油燃料最常见的问题，应设计有便携的或安装固定的清洁系统。在寒冷的季节，需要考虑给燃料系统加热或循环，避免柴油燃料胶凝。当确定好现场燃料储藏系统的容量时，同时需要考虑燃料供货商在紧急情况下的反应时间。

在发电机周围提供 UPS 照明电源或单独的电池，以备在发电机和装置同时发生故障时提供照明。同样，在发电机周围也应该提供 UPS 供电插座。

除组件的分别测试外，备用发电机系统、UPS 系统和自动转换开关应该作为一个系统一起测试。在冗余系统测试单个组件的故障时，冗余系统是为在一个组件发生故障时能够继续

起作用而设计的。此外，一旦网络核心机房开始运行，应该定期测试系统，确保各个组件能够继续正常地发挥作用。

3. 动力供配电系统

由总配电柜输出的动力供配电系统采用 50Hz 交流电，380/220V 三相五线电源，TN-S 接地方式，零线和地线分开设置且零、地线之间的电压小于 1V。动力配电柜、照明配电箱采用放射式配电直接配至各用电设备。机房内所有线缆须设计钢制桥架、线槽或钢管敷设。由于精密空调的供电电流大、负载动态范围宽，为防止干扰，应考虑另选路径单独敷设电缆。

动力配电柜（箱）具有火警联动保护功能，出现火警时可与消防系统联动及时切断电源，关闭防烟防火阀，并且在值班室安装手动电源切断装置。动力柜、照明箱内的开关和主要元器件采用进口产品，并设置有效的防雷措施。有条件时，大型机房最好采用专用电力变压器供电。

4. UPS 供配电系统

UPS 供配电系统的供电范围包括计算机设备（主机和附属设备）、通信设备、网络设备、保安监控设备、消防系统、应急照明等。UPS 输出配电回路（每个配电控制开关为一个回路）需按机房内设备要求设置，小型机/服务器、网络核心交换机及重要路由器要由独立双回路供电，其他计算机设备可用一个回路带 3 ~ 4 个插座，固定于地板下。UPS 电源分别送到主机房配电柜（末端），既可靠，又方便使用。还应该考虑为数据中心中关键的负载设备安装电源分配单元（PDU），这些设施是合并了几个组件功能的一个装置，通常很小，比分开安装几个独立的面板和变压器更有效。如果机房细分为不同的房间或空间，每一个房间或空间是由它们各自独立的紧急电源开关（EPO）所支持，那么这些空间应该拥有自己独立的水平分布区域。

电源分配单元（PDU）集成了独立的变压器、瞬时电压浪涌抑制（TVSS）、输出面板和电源控制功能，并具有更多的优点。一个典型的 PDU 包括以下组件：

1）离线变压器：双输入断路器应被视为允许连接一个临时接驳，允许维护或资源再分布时不用关闭关键的负载。

2）变压器：尽可能靠近负载以减少从地线到零线之间的共模噪声，减少电压源接地和信号源接地之间的差别。当变压器位于 PDU 内时，就达到了最近的位置。

3）瞬时电压浪涌抑制（TVSS）：美国标准 UL1449 是对瞬时电压浪涌抑制器的要求，它不但有结构和机械方面的要求，还有相当多的电气性能方面的测试。当导线长度尽可能的短时，瞬时电压浪涌抑制（TVSS）装置的效率将大大提高。通过在同一个装置中提供瞬时电压浪涌抑制（TVSS）装置，可以提高效率。

4）分配面板：可以将面板与变压器安装在同一个机柜中或在需要更多面板的情况下，可以使用一个远程的电源面板。

5）计量、监测、警报和远程控制：当提供一个传统的面板系统时，通常意味着有大量的空间要求。

6）紧急电源关闭（EPO）控制。

单点接地总线应该用电力分配单元（PDU）将电源分配到关键的负载上。在需要额外分支电路的地方，面板或 PDU“sidecars”可以是次级反馈的。应该提供两个冗余 PDU 给每

个机架供电，每一个 PDU 最好采用不同的 UPS 系统供电。提供给单相或三相计算机设备一个可以安装在机架上的快速转换开关或从每一个 PDU 馈给的静态开关。应该考虑用彩色的表示牌和馈给电缆来区别 A 和 B 的分布，例如，所有的 A 用白色，所有的 B 用蓝色。

一条电路不应该服务多于一个机架，以防止一条电路对多个机架产生电路故障。为了提供冗余，每一个机架和机柜应该用两个专用的、从两个不同的电力分配单元（PDU）或供电面板来的 16A、220V 的电路。对于高密度的机架可能要求更高的安培容量，一些新服务器可能要求一个或多个、单相或三相插座，额定电流要求 50A 或更高。每一个插座应该用服务于它的 PDU 或电路号来标识。

5. 配电设备的安装和线路敷设的问题

在机房设备布局确定的前提下，按照电气设备用途和设计图纸进行设备安装和线路敷设。

（1）设备安装

机房配电柜、UPS 电源柜落地安装。动力配电箱、照明配电箱底边距地 1.4m 墙上暗装。根据机房内设备负载容量和分布情况，机柜（箱）内元器件配置要做到排列有序、安装牢固、理线整齐、接线正确、标志明显、外观良好，内外清洁。分设单相、三相回路，配用小型真空断路器，如 C65N 等线路保护开关。箱内设置辅助等电位接地母排。电源柜及其他电气装置的底座应与建筑楼地面牢靠固定。电气接线盒内无残留物，盖板整齐、严密、紧贴墙面。同类电气设备安装高度应一致。吊顶内电气装置应安装在便于维修的地方。特种电源配电装置应有明显标志，并注明频率、电压。暗装照明箱或开关面板安装在机房出入口附近墙面的方便操作的位置。分体空调插座设置在机房内墙面上距地 1.8m 处。

主机房内应分别设置维修和测试用电源插座，两者应有明显的区别标志。测试用电源插座应由计算机主机电源系统供电。其他房间内应适当设置维修用电源插座。单相检修电源回路要在电源管理间各墙面距地 0.3m 处设置检修电源插座，禁止使用 2kW 以上的大功率电感性电动工具。确需使用这类工具以及三相检修设备时，应使用施工移动式配电盘从机房所在楼层附近的动力或照明配电箱接取电源。

（2）线路敷设

供电距离尽量短，主要是从供电安全考虑，电子计算机电源间应靠近主机房设备。主机房内活动地板下部的低压配电线路应采用铜芯屏蔽导线或铜芯屏蔽电缆。机房内的电源线、信号线和通信线应分别铺设，排列整齐，捆扎固定，长度留有余量。UPS 电源配电箱（柜）引出的配电线路，穿薄皮钢管或阻燃 PVC 管，沿机房活动地板下敷设至各排机柜和配线架的背面，经带穿线孔的活动地板引上，穿管保护进入金属导轨式插座线槽、机柜或配线架。控制台或设备桌后的敷线，用金属导轨式插座线槽并用螺栓固定，安装在设备桌背面距活动地板 0.1 ~ 0.3m 处。

信号线缆在活动地板下从机柜、配线架引至各设备，应采用金属线槽沿设备周围或主机房从设备背面的活动地板穿线孔引入（注意不得与电源线路共用活动地板穿线孔，且间距大于 0.1m），信号线缆避免沿机房墙边敷设以防与强电线管交叉。活动地板下部的电源线应尽可能远离计算机信号线，并避免并排敷设。当不能避免时，应采取相应的屏蔽措施。桌上设备之间的信号连线是短线的（长度小于 3m），应沿设备背部桌面明敷，但不得悬吊在设备桌背侧空中；是长线的（长度大于 3m），应从活动地板穿线孔翻下（上）穿薄皮钢管在

活动地板下敷设。机房照明负载和普通空调负载，由电源管理间分别引出动力和照明回路供电。照明和空调负载线路均沿吊顶内或墙面敷设。

（3）可靠接地

总配电柜、UPS 电源柜、动力配电箱、照明配电箱的金属框架及基础型钢必需接地（PE）或接零（PEN）。门和框架的接地端子间用裸编铜线连接。柜、箱内配线整齐。照明配电箱内的漏电保护器的动作电流不大于30mA，动作时间不大于0.1s。接地（PE）或接零（PEN）支线必须单独与接地（PE）或接零（PEN）干线相连，不得串联连接。UPS 电源柜输出端的中性线（N 极），必须与由接地装置直接引来的接地干线连接，做重复接地，接地电阻小于4Ω。当灯具距地面高度小于 2.4m 时，灯具的可接近裸露导体必须接地（PE）或接零（PEN），并应有专用接地螺栓和标识。外电源进线至机房电源管理间时，应将电缆的金属外皮与接地装置连接；从楼外引入的铠装信号电缆和屏蔽信号线进入弱电机房前也应注意采取防雷击措施，避免沿建筑外墙或防雷引线引雷入室。同轴电缆的屏蔽层必须与机壳一起接地。

上述线缆进入机房后，应设金属接线箱（盒），并将线缆金属（屏蔽）外皮连接避雷器或浪涌电压抑制器（SPD），然后与机房等电位接地母排，用截面积不小于 16mm^2 的铜芯绝缘线连通。这样可以有效地抑制线缆接收到的电磁干扰信号，从而保证信号传输的质量。从机房引出的信号线路应采用金属线槽沿墙并在吊顶内敷设，避免与其他电气管路平行紧贴。尽量避开空调、消防、暖气和给排水等管道，与它们的间距按相关规范执行。金属电缆桥架及其支架和引入或引出的金属电缆导管必须接地（PE）或接零（PEN），且必须符合下列规定：

1）金属电缆桥架及其支架应不少于两处与接地（PE）或接零（PEN）干线相连接。

2）电缆桥架间连接板的两端跨接铜芯接地线，接地线最小允许截面积不小于 6mm^2。

3）接地（PE）或接零（PEN）线在插座间不串联连接。

工程实施中按上述做法可以较好地保证机房供电的可靠和安全，各种不同电压和频率的信号线缆敷设安全、相互隔离度好、整齐、美观并方便维护管理。

（4）消防系统的要求

消防系统的设备动力电缆、控制电缆、电线，按规范要求选用耐火型电缆、电线。其他弱电系统所用电缆、电线均采用阻燃型。在设备选择及线路敷设时，应充分考虑电磁兼容问题。

一般要求主要开关设备应该被设计成适合增容、维护和冗余，并提供双倍的或隔离的冗余配置。设计时应该考虑到开关装置、总线或断路器维护的方便性。瞬时电压浪涌抑制（TVSS）应该被安装在电力分配系统的每一级上，并且采用适当的规格，以便能够抑制可能发生的瞬时能量。

6.4.2　不间断电源

1. 不间断电源的作用

机房常用的供电电源是不间断电源（Uninterruptible Power System，UPS）。UPS 是一种含有储能装置，以逆变器为主要组成部分的恒压恒频的不间断电源。主要用于给单台计算机、计算机网络系统或其他电力电子设备提供不间断的电力供应。当市电输入正常时，UPS 将市电稳压后供应给负载使用，此时的 UPS 就是一台交流市电稳压器，同时它还向机内电池充

电；当市电中断（事故停电）时，UPS 立即将机内电池的电能，通过逆变转换的方法向负载继续供应 220V 交流电，使负载维持正常工作并保护负载软、硬件不受损坏。UPS 设备通常对电压过大和电压过低都提供保护。

由于采用了脉宽调频技术、高效功率器件的成熟、微处理器的发展等因素，UPS 已经成为计算机房供电的主要设备。UPS 最大的特点在于不间断性，而且能最大限度地提供稳定电压，隔离外电网的干扰。外电网一旦停电，UPS 能在设备所允许的极短时间内（微秒至毫秒级）自动将备用能源经逆变器变换成电压、频率和相位都与原供电电源相同的电能继续向计算机供电。或者平时由逆变器供电，只在逆变器发生故障时，才由静态电子开关自动将计算机瞬时切换到外电网供电或切换到另一台与之并联的 UPS 上，实现不间断供电。UPS 提供的电源具有较高的电压和频率稳定性，波形失真也较小，干扰更优于外电网，是计算机系统最理想的供电设备。几乎所有的重要计算机设备都采用 UPS 供电。

2. UPS 的组成

UPS 系统由五部分组成：主路、旁路、电池等电源输入电路，进行 AC/DC 变换的整流器（REC），进行 DC/AC 变换的逆变器（INV），逆变和旁路输出切换电路以及蓄能电池。其系统的稳压功能通常是由整流器完成的，整流器采用晶闸管或高频开关整流器，本身具有可根据外电的变化控制输出幅度的功能，从而当外电发生变化时（该变化应满足系统要求），输出幅度基本不变。净化功能由储能电池来完成，由于整流器不能消除瞬时脉冲干扰，整流后的电压仍存在干扰脉冲。储能电池除具有可存储直流电能的功能外，对整流器来说就像接了一只大容量电容器，其等效电容量的大小，与储能电池容量大小成正比。由于电容器两端的电压是不能突变的，即利用了电容器对脉冲的平滑特性消除了脉冲干扰，起到了净化功能，也称对干扰的屏蔽。频率的稳定则由变换器来完成，频率稳定度取决于变换器的振荡频率的稳定程度。为方便 UPS 系统的日常操作与维护，设计了系统工作开关、不间断电源故障后的自动旁路开关、检修旁路开关等控制开关。

UPS 供电示意图如图 6-4 所示，在电网电压工作正常时，给负载供电如图所示，而且，同时给储能电池充电；当突发停电时，UPS 电源开始工作，由储能电池供给负载所需电源，维持正常的生产（如粗黑→所示）；当由于生产需要，负载严重过载时，由电网电压经整流直接给负载供电（如虚线所示）。

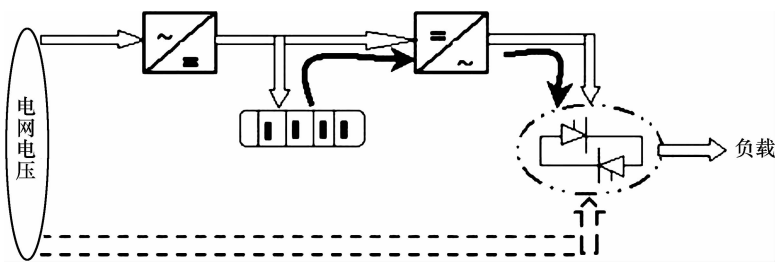


图 6-4　UPS 供电示意图

UPS 系统主要核心组件分为两大块：UPS 主机和储能电池（蓄电池）。额定输出功率的大小取决于主机部分，并与负载驱动性质有关，因为 UPS 对不同性能的负载驱动能力不同，通常负载功率应满足 UPS 70% 的额定功率的要求。储能电池容量的选取，当负载功率确定

后主要取决于其后备时间的长短，这个时间因各企业情况不同而不同，主要由备用电源的接入时间来定，通常在几分钟或几个小时不等。

3. UPS 的工作过程

当市电正常为 AC 380V 时，直流主回路有直流电压，供给 DC-AC 交流逆变器，输出稳定的 220V 或 380V 交流电压，同时市电经整流后对电池充电。当任何时候市电欠电压或突然掉电，则由电池组通过隔离二极管开关向直流回路馈送电能。从电网供电到电池供电没有切换时间。当电池能量即将耗尽时，UPS 发出声光报警，并在电池放电下限点停止逆变器工作，长鸣告警。UPS 还有过载保护功能，当发生超载（150% 负载）时，跳到旁路状态，并在负载正常时自动返回。当发生严重超载（超过 200% 额定负载）时，UPS 立即停止逆变器输出并跳到旁路状态，此时前面输入断路器也可能跳闸。消除故障后，只要合上开关，重新开机即开始恢复工作。其工作原理图如图 6-5 所示。

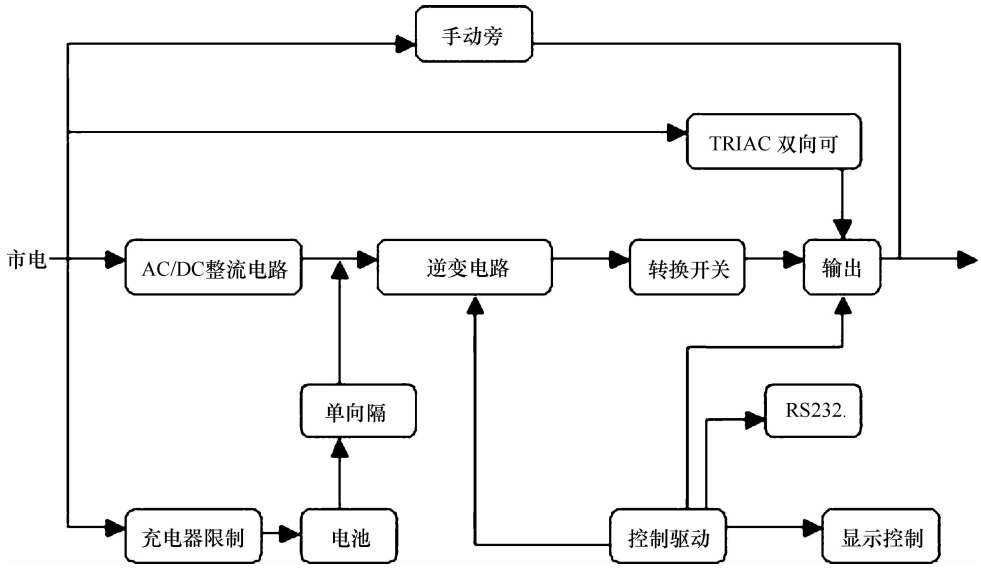


图 6-5　UPS 工作原理图

4. UPS 的种类

UPS 按工作原理分成后备式、在线式与在线互动式三大类。

（1）后备式 UPS

这是最常用的一种 UPS。如四通 HO 系列与 SD 系列，它具备了自动稳压、断电保护等 UPS 最基础也是最重要的功能，虽然一般有 10ms 左右的转换时间，逆变输出的交流电是方波而非正弦波，但由于结构简单而具有价格便宜、可靠性高等优点，因此广泛应用于微机、外设、POS 机等领域。

（2）在线式 UPS

结构较复杂，但性能完善，能解决所有电源问题，如四通 PS 系列，其显著特点是能够持续零中断地输出纯净正弦波交流电，能够解决尖峰、浪涌、频率漂移等全部的电源问题。但由于需要较大的投资，通常应用在关键设备与网络中心等对电力要求苛刻的环境中。

（3）在线互动式 UPS

同后备式相比较，在线互动式具有滤波功能，抗市电干扰能力很强，转换时间小于4ms，逆变输出为模拟正弦波，所以能配备服务器、路由器等网络设备，或者用在电力环境较恶劣的地区。

5. UPS 的选购要点

（1）稳定性

因为 UPS 是起保障作用的，因此它自身的稳定性更为重中之重。当用户选购 UPS 产品的时候，不管是中小型企业用户还是其他用户，首先必须考虑 UPS 产品的质量，产品的质量是用户选用产品的第一要则，我们要选择市场知名度较高的品牌，如艾默生、山特、APC、梅兰日兰等知名厂家的产品。

（2）后备时间

后备时间是很多用户在购买 UPS 产品的时候会比较关注的一个指标。从学术角度讲，UPS 就是停电后继续为用户供电，一般后备时间会从 30min 到 4h 甚至更长时间不等，取决于业务需求。另一功能则是保证用户能够有一个干净的电源，保护用户的设备。

（3）确定 UPS 的类型

根据负载对输出稳定度、切换时间、输出波形的要求来确定是选择在线式、在线互动式、后备式还是正弦波、方波等类型的 UPS。在线式 UPS 的输出稳定度、瞬间响应能力比另外两种强，对非线性负载的适应能力也较强。对一些较精密的设备、较重要的设备要采用在线式 UPS。在一些市电波动范围比较大的地区，应避免使用互动式和后备式 UPS。如果要使用发电机配短延时 UPS，推荐用在线式 UPS。

（4）售后服务能力

每个用户的网络特点、电力环境都不相同，电源保护要求也随之变化。用户在使用 UPS 时可能遇到种种问题，用户希望自己购置的是完全适合实际需求的产品和服务，而且关心设备投资的周期、长期回报率及投资风险。而现实是，绝大多数产品售后缺乏这方面的专业人员，所以，优质的服务体系和主动的服务态度也成为用户选购 UPS 时必须考虑的一个重要因素。

（5）附件功能

为了提高系统的可靠性，建议采用 UPS 热备份系统，系统可以串联热备份或并联热备份。小容量的 UPS（1～2kVA）还可以选用冗余开关。可以选用远程监控面板，实现在远端监视和控制 UPS 工作。可以选用监控软件，实现计算机与 UPS 之间的智能化管理。可以选用网络适配器，实现 UPS 的网络化管理（基于 SNMP）。在某些多雨多雷地区，可以配用防雷器。还要考虑是否能够对网络的使用和对外设进行保护。

6.4.3 机房照明系统

机房照明设计包括平面设计和系统设计。首先要认真进行机房照明的需求分析，如机房照明设计要求光线要柔和，适合人体的生理需要，不能因照明电源产生干扰而影响计算机的工作。主机房内在离地面 0.8m 处，照度不应低于 300Lx；辅助机房内照度不应低于 150Lx；应急照明应大于 30Lx；紧急出口标志灯、疏散指示灯照度应大于 5Lx。

我国机房照明设计标准主要指标为照度。照度是光通量投射到物体表面时，即可把物体表面照亮；就是光通量的表面密度，即射到物体表面的光通量 ϕ 与该物体表面的面积 S 的

比值，即 $E=\phi/S$（其中照度的单位为勒克斯 Lx）。主机房和辅助区一般照明的照度标准值宜符合表 6-1 的规定。

表 6-1　主机房和辅助区一般照明照度标准值

房 间 名 称		照度标准值	统一眩光值 UGR	一般显色指数 Ra
主机房	服务器设备区	500	22	80
	网络设备区	500	22	
	存储设备区	500	22	
辅助区	进线间	300	25	
	监控中心	500	19	
	测试区	500	19	
	打印室	500	19	
	备件库	300	22	

在主机房内基本工作间无眩光，眩光限制等级为 I 级；第一类辅助房间眩光限制等级为 D 级，可以有轻微眩光；第二、第三类辅助房间眩光限制等级为Ⅲ级，允许有眩光感觉。在选择及布置灯具时，除根据机房电气设计规范对照度的要求外，还应充分结合自然采光及墙面反射率等因素来计算确定灯具数量。一般机房照明功率密度（W/m^2）的现行值可按 $18W/m^2$ 计算。各功能房间采用嵌入式格栅荧光灯具。在灯的布置上，根据安装高度（即吊顶高度）决定灯具间隔。在保证照度的前提下，充分考虑照度均匀性和有效抑制眩光等因素。成排安装的灯具，光带应平直、整齐。工作区内一般照明的均匀度（最低照度与平均照度之比）不宜小于 0.7，非工作区的照度不宜低于工作区平均照度的 1/3。

除了各机房按要求布置灯具外，同时要考虑应急照明要求，应设置通道疏散照明及疏散指示标志灯，主机房通道疏散照明的照度值不应低于 5Lx，其他区域通道疏散照明的照度值不应低于 0.5Lx。在市电停电后，为保证工作人员做存盘等紧急处理，机房内应布置一定数量的应急照明灯具。采用高效应急照明灯，当市电停电后自动投入。应急照明由 UPS 供电，灯具布置均匀无死角。保证应急处理后，人员能安全快速地沿通道向出口或应急出口疏散。照明支路管线参照配电箱系统图布线，应急照明采用大楼 EPS 供电。在照明箱供电线路设计中，除了一般性的供电线路外，应考虑有 1/3 左右的 UPS 供电，以保证在应急状态下的人员疏散照明。

主机房和辅助区应设置备用照明，备用照明的照度值不应低于一般照明照度值的 10%；有人值守的房间，备用照明的照度值不应低于一般照明照度值的 50%。备用照明可为一般照明的一部分。电子信息系统机房内的照明线路宜穿钢管暗敷或在吊顶内穿钢管明敷。技术夹层内宜设置照明，并应采用单独支路或专用配电箱（柜）供电。

灯具的控制要求分区、分路、集中控制，尤其是大面积照明场所的灯具，要分区、分段设置开关。一般照明采用电子镇流器，当采用电感镇流器时，应加电容补偿器。

6.4.4　防雷接地系统

电子信息系统机房的防雷和接地设计，应满足人身安全及电子信息系统正常运行的要求，并应符合现行国家标准《建筑物防雷设计规范》GB 50057—2010 和《建筑物电子信息

系统防雷技术规范》GB 50343—2012 的有关规定。保护性接地和功能性接地宜共用一组接地装置，其接地电阻应按其中的最小值确定。对功能性接地有特殊要求需单独设置接地线的电子信息设备，接地线应与其他接地线绝缘；供电线路与接地线宜同路径敷设。

电子信息系统机房内的电子信息设备应进行等电位连接，等电位连接方式应根据电子信息设备易受干扰的频率及电子信息系统机房的等级和规模确定，可采用 S 型、M 型或 SM 混合型。

采用 M 型或 SM 混合型等电位连接方式时，主机房应设置等电位连接网格，网格四周应设置等电位连接带，并应通过等电位连接导体将等电位连接带就近与接地汇流排、各类金属管道、金属线槽、建筑物金属结构等进行连接。每台电子信息设备（机柜）应采用两根不同长度的等电位连接导体就近与等电位连接网格连接。等电位连接网格应采用截面积不小于 25mm^2 的铜带或裸铜线，并应在防静电活动地板下构成边长为 0.6～3m 的矩形网格。等电位连接带、接地线和等电位连接导体的材料和最小截面积，应符合表 6-2 的要求。

表 6-2　等电位连接带、接地线和等电位连接导体的材料和最小截面积

名　　称	材　　料	最小截面积/mm^2
等电位连接带	铜	50
利用建筑内的钢筋做接地线	铁	50
单独设置的接地线	铜	25
等电位连接导体(从等电位连接带至接地汇流排或至其他等电位连接带;各接地汇流排之间)	铜	16
等电位连接导体(从机房内各金属装置至等电位连接带或接地汇流排;从机柜至等电位连接网格)	铜	6

6.4.5　静电防护

因为网络核心机房有大量的电子设备，因此静电防护是一个必须高度重视的问题，主要是通过敷设专业的防静电地板来解决。主机房和辅助区的地板或地面应有静电泄放措施和接地构造，防静电地板、地面的表面电阻或体积电阻值应为（2.5×104～1.0×109）Ω，且应具有防火、环保、耐污耐磨性能。主机房和辅助区中不使用防静电活动地板的房间，可铺设防静电地面，其静电耗散性能应长期稳定，且不应起尘。主机房和辅助区内的工作台面宜采用导静电或静电耗散材料，其静电性能指标应符合“静电地板、地面的表面电阻或体积电阻值为（2.5×104～1.0×109）Ω”的规定。

电子信息系统机房内所有设备的金属外壳、各类金属管道、金属线槽、建筑物金属结构等必须进行等电位连接并接地。

静电接地的连接线应有足够的机械强度和化学稳定性，宜采用焊接或压接。当采用导电胶与接地导体粘接时，其接触面积不宜小于 20cm^2。

6.5　机房空调及新风系统

6.5.1　机房空调系统

网络核心机房必须要安装机房专用空调，主机房和辅助区中的空调系统应根据电子信息

系统机房的等级选择安装。安装机房专用空调，目的是提供一个恒温恒湿的机房环境，以便网络设备散热，保障正常运行。电子信息系统机房的空调设计，应符合现行国家标准《电子信息系统机房设计规范》GB 50174—2008、《采暖通风与空气调节设计规范》GB 50019—2003 和《建筑设计防火规范》GB 50016—2006 的有关规定。

对于大型园区网络，根据信息系统和服务器、存储等网络设备的多少、以及以后网络设备的扩容量等，一般建有从几十平米到几百平米面积不等的专用网络核心机房。网络核心机房一般要求配备恒温恒湿空调机组、新风系统。关于配置空调功率大小，有一个专门的负载计算方法。

电子信息设备和其他设备的散热量应按产品的技术数据进行计算。机房空调系统夏季的冷负载应包括下列内容：

1）机房内设备的散热；

2）建筑围护结构的传热；

3）通过外窗进入的太阳辐射热；

4）人体散热；

5）照明装置散热；

6）新风负载；

7）伴随各种散热过程产生的潜热。

空调系统湿负载应包括下列内容：

1）人体散湿；

2）新风负载。

主机房空调系统的气流组织形式，应根据电子信息设备本身的冷却方式、设备布置方式、布置密度、设备散热量以及室内风速、防尘、噪声等要求，结合建筑条件综合确定。当电子信息设备对气流组织形式未提出要求时，主机房气流组织、风口及送回风温差按表 6-3 选用。

表 6-3　主机房气流组织、风口及送回风温差

气流组织	下送上回	上送上回（或侧回）	侧送侧回
送风口	1）带可调多叶阀的格栅风口 2）条形风口（带有条形风口的活动地板） 3）孔板	1）散流器 2）带扩散板风口 3）孔板 4）百叶风口 5）格栅风口	1）百叶风口 2）格栅风口
回风口	1）格栅风口　2）百叶风口　3）网板风口　4）其他风口		
送风温差	4～6℃，送风温度应高于室内空气露点温度	4～6℃	6～8℃

对机柜高度大于 1.8m，设备热密度大、设备发热量大或热负载大的主机房，宜采用活动地板下送风、上回风方式。大型园区网络核心机房通常采用 42U 标准机柜，设备密度较大，一般都是采用活动地板下送风、上回风的方式，如图 6-6、图 6-7 所示。采用活动地板下送风时，活动地板下的空间应考虑线槽及消防管线等所占用的空间。

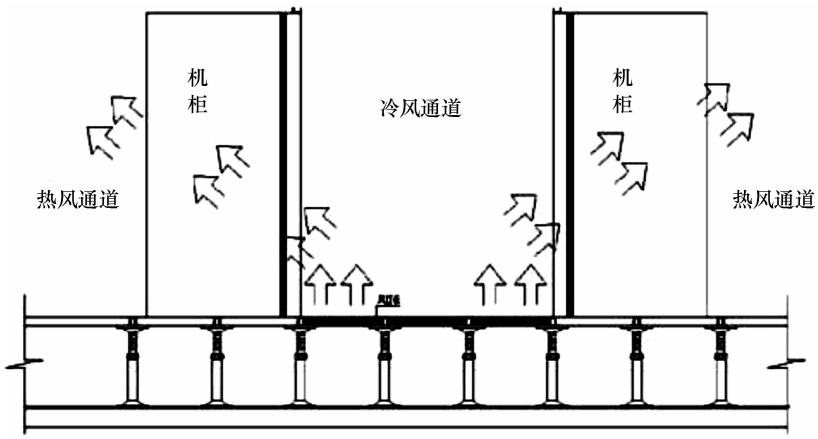


图 6-6　下送风、上回风示意图

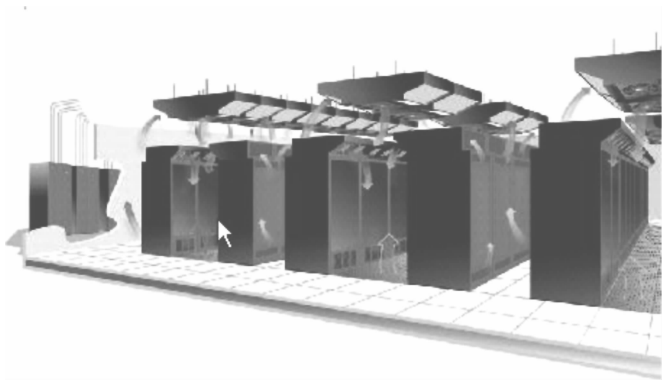


图 6-7　下送风、上回风效果图

6.5.2　精密空调的选择

空调设计应根据当地气候条件，选择采用下列节能措施：

1）大型机房空调系统宜采用冷水机组空调系统。

2）北方地区采用水冷冷水机组的机房，冬季可利用室外冷却塔作为冷源，并应通过热交换器对空调冷冻水进行降温。

3）空调系统可采用电制冷与自然冷却相结合的方式。

在对空调设备进行选择的时候，空调和制冷设备的选用应符合运行可靠、经济适用、节能和环保的要求。空调系统和设备应根据电子信息系统机房的等级、机房的建筑条件、设备的发热量等进行选择。空调系统无备份设备时，单台空调制冷设备的制冷能力应留有 15%～20% 的余量。选用机房专用空调机时，空调机宜带有通信接口，通信协议应满足机房监控系统的要求，显示屏宜为汉字显示。空调设备的空气过滤器和加湿器应便于清洗和更换，设备安装应留有相应的维修空间。

对于大型园区网络的核心机房，一般选择精密空调设备作为机房专用设备。

机房精密空调是针对现代电子设备机房设计的专用空调，它的工作精度和可靠性都要比普通空调高得多。大家都知道，计算机机房中摆放计算机设备及程控交换机产品等，由大量

密集电子元件组成。要提高这些设备使用的稳定性及可靠性，需将环境的温度、湿度严格控制在特定范围。机房精密空调可将机房温度及相对湿度控制于正负 1 摄氏度，从而大大提高了设备的稳定性及可靠性。

在许多重要的工作中信息处理是不可或缺的一个环节，因此，网络核心机房的正常运转离不开恒温恒湿的机房环境。IT 硬件产生不寻常的集中热负载，同时对温度或湿度的变化又非常敏感。温度或湿度的波动可能会产生一些问题，例如，处理时出现乱码，严重时甚至系统彻底停机。这会给企业带来巨大的损失，具体数额取决于系统中断时间以及所损失数据和时间的价值。标准舒适型空调的设计并非为了处理数据机房的热负载集中和热负载组成，也不是为了向这些应用提供所需的精确的温度和湿度设定点。精密空调系统的设计是为了进行精确的温度和湿度控制。精密空调系统具有高可靠性，保证系统终年连续运行，并且具有可维修性、组装灵活性和冗余性，可以保证数据机房四季空调正常运行。

机房精密空调机组主要选择的品牌有艾默生、卡洛斯等。例如，艾默生公司提供了一系列适用于大小机房的机房精密空调系统产品，对于大型机房专用空调，主要有 Liebert. PEX2、Liebert. CRV 高效制冷系统、Liebert. PEX 大型机房专用空调系统、SDC 智能节能双循环空调、机房专用冷冻水机组等产品。如图 6-8 展示了艾默生精密空调的核心组件。

图 6-8　艾默生精密空调核心组件

6.5.3　精密空调机容量的计算方法

为了确定机房精密空调机的容量，以满足机房温度、湿度、洁净度和送风速度的要求（简称四度要求），必须首先计算机房的热负载。机房的热负载主要来自两个方面：

1. 机房内部产生的热量

它包括：室内计算机及外部设备的发热量，机房辅助设施和机房设备的发热量（电热、蒸气水温及其他发热体）。这些发热量显热大、潜热小，包括照明发热（显热）；工作人员的发热（显热小、潜热大）；由于水分蒸发、凝结产生的热量（潜热）。

2. 机房外部产生的热量

它包括：传导热（通过建筑物本体侵入的热量，如从墙壁、屋顶、隔断和地面传入机房的热量（显热）），放射热（也称辐射热）（由于太阳照射从玻璃窗直接进入房间的热量（显热）），对流产生的热量，从门窗等缝隙侵入的高温室外空气（也包含水蒸气）所产生的热量（显热、潜热），为了使室内工作人员减少疲劳和有利于人体健康而引入的新鲜空气所

产生的热量（包括显热和潜热）。

总之，人体放出的热量、缝隙风侵入的热量和换气带进的热量，不仅使室温升高，也会增加室内的含湿量，因此需要除湿。这部分热负载称为潜热负载，而机房内所有设备散发的热量只是室内的温度升高，这种热负载称为显热负载。与一般宾馆、办公室、会议室等潜热占有相当大比例所不同的是，计算机、程控机机房内的热负载是以显热负载为主。因此对于热负载状况不同的场合应选用不同类型的空调机。通常用显热比（SFH）作为空调机的重要指标。

机房热负载的概略计算（也称为估算）方法

在机房初始设计阶段，为了较快地选定空调机的容量，可采用此方法，即以单位面积所需冷量进行估算。

计算机房（包括程控交换机房）：

楼层较高时，250～300kcal/（m^2·h）

楼层较低时，150～250kcal/（m^2·h）（根据设备的密度做适当的增减）；

办公室（值班室）：90kcal/（m^2·h）。

计算机房空调负载，主要来自计算机设备、外部设备及机房设备的发热量，大约占总热量的80%以上，其次是照明热、传导热、辐射热等，这几项计算方法与一般空调房间负载的计算相同。计算机制造商一般能提供设备发热量的具体数值。否则根据计算机的耗电量计算其发热量。

（1）外部设备发热量的计算

$$Q = 860N\text{¢}；(\text{kcal/h})$$

式中，N 是用电量（kW）；¢；是同时使用系数（0.2～0.5）；860 是功的热当量，即1kW 电能全部转化为热能所产生的热量。

（2）主机发热量计算

$$Q = 860 \times P \times h1 \times h2 \times h3$$

式中，P 是总功率（kW）；h1 是同时使用系数；h2 是利用系数；h3 是负载工作均匀系数。

机房内各种设备的总功率，应以机房内设备的最大功耗为准，但这些功耗并未全部转换成热量，因此，必须用以上三种系数来修正，这些系数又与计算机的系统结构、功能、用途、工作状态及所用电子元件有关。总系数一般取0.6～0.8 为好。

（3）照明设备热负载计算

机房照明设备的耗电量，一部分变成光，一部分变成热。变成光的部分最终也因被建筑物和设备等所吸收而变成热。照明设备的热负载计算如下：

$$Q = C \times P$$

式中，P 是照明设备的标称额定输出功率（W）；C 是每输出 1W 的热量（kcal/h·W），通常自炽灯为0.86kcal/h·W，荧光灯为1.0kcal/h·W。

（4）人体发热量

人体内的热是通过皮肤和呼吸器官放出来的，这种热因含有水蒸气，其热负载应是显热和潜热负载之和。

人体发出的热随工作状态而异。机房中工作人员可按轻体力工作处理。当室温为24℃时，其显热负载为56cal，潜热负载为46cal；当室温为21℃时，其显热负载为65cal，潜热

负载为 37cal。在两种情况下，其总热负载均为 102cal。

（5）围护结构的传导热

通过机房屋顶、墙壁、隔断等围护结构进入机房的传导热是一个与季节、时间、地理位置和太阳的照射角度等有关的量。因此，要准确地求出这样的量是很复杂的问题。

当室内外空气温度保持一定的稳定状态时，由平面形状墙壁传入机房的热量可按下式计算：

$$Q = KF(t_1 - t_2)$$

式中，K 是围护结构的导热系数（kcal/m^2h℃）；F 是围护结构面积（m^2）；t_1 是机房内温度（℃）；t_2 是机房外的计算温度（℃）。

当计算不与室外空气直接接触的围护结构如隔断等时，室内外计算温度差应乘以修正系数，其值通常取 0.4 ~ 0.7。常用材料导热系数（kcal/m^2h℃）如下所示：

普通混凝土：1.4 ~ 1.5；石膏板：0.2；

轻型混凝土：0.5 ~ 0.7；石棉水泥板：1；

砂浆：1.3；软质纤维板：0.15；

熟石膏：0.5；玻璃纤维：0.03；

砖：1.1；镀锌钢板：38；

玻璃：0.7；铝板：180；

木材：0.1 ~ 0.25。

（6）从玻璃透入的太阳辐射热

当玻璃受阳光照射时，一部分被反射，一部分被玻璃吸收，剩下的透过玻璃射入机房转化为热。被玻璃吸收的热使玻璃温度升高，其中一部分通过对流进入机房也成为热负载。

透过玻璃进入室内的热量可按下式计算：

$$Q = KFq$$

式中，K 是太阳辐射热的透入系数；F 是玻璃窗的面积（m^2）；q 是透过玻璃窗进入的太阳辐射热强度（kcal/m^2h）。

透入系数 K 取决于窗户的种类，通常取 0.36 ~ 0.4。

太阳辐射热强度 q 随纬度、季节和时间而不同，又随太阳照射角度而变化。具体数值请参考当地气象资料。

（7）换气及室外侵入的热负载

为了给在计算机房内的工作人员不断补充新鲜空气，以及用换气来维持机房的正压，需要通过空调设备的新风口向机房送入室外的新鲜空气，这些新鲜空气也将成为热负载。通过门、窗缝隙和开关而侵入的室外空气量，随机房的密封程度、人的出入次数和室外的风速而改变。这种热负载通常都很小，如需要，可将其折算为房间的换气量来确定热负载。

（8）其他热负载

在机房中，除上述热负载外，在工作中使用示波器、电烙铁、吸尘器等都将成为热负载。由于这些设备的功耗一般都较小，可粗略按其额定输入功率与功的热当量之积来计算。此外，机房内使用大量的传输电缆，也是发热体。其计算如下：

$$Q = 860Pl$$

式中，860 是功的热当量（kcal/h）；P 是每米电缆的功耗（W）；l 是电缆的长度（m）。

总之，机房热负载应由上述（1）~（8）各项热负载之和来确定。

6.5.4 新风系统

新风系统是由风机、进风口、排风口及各种管道和接头组成。安装在吊顶内的风机通过管道与一系列的排风口相连，风机起动，室内受污染的空气经排风口及风机排往室外，使室内形成负压，室外新鲜空气便经安装在窗框上方（窗框与墙体之间）的进风口进入室内，从而使室内人员可呼吸到高品质的新鲜空气。

新风系统是根据在密闭的室内一侧用专用设备向室内送新风，再从另一侧由专用设备向室外排出，在室内形成“新风流动场”的原理，从而满足室内新风换气的需要。实施方案是：采用高压头、大流量小功率直流高速无刷电动机带动离心风机，依靠机械强力由一侧向室内送风，由另一侧用专门设计的排风新风机向室外排出的方式强迫在系统内形成新风流动场。在送风的同时对进入室内的空气进行新风过滤、灭毒、杀菌、增氧、预热（冬天）。排风经过主机时与新风进行热回收交换，回收大部分能量通过新风送回室内。借用大范围形成洁净空间的方案，保证进入室内的空气是洁净的。以此达到室内空气净化环境的目的。

新风系统设备是大型网络核心机房必须要安装的设备，以保障在网络核心机房专用空调空气的新鲜度，保障操作人员的生命安全。

新风系统要考虑风量大小、冷量回风工况、新风工况、热量回风工况等技术指标，满足足量的新风量，安装在空调机房等场合，配合回风箱可调节新风、回风比例。

新风作为机房空调调节设计中的重要组成部分，具有如下重要意义：维持机房内的正压，有利于保持机房内恒定的空气环境，保持机房的洁净；稀释室内不断产生的空气污染物（设备、人员、建筑材料），防止空气品质变坏。

1. 计算机机房内新风处理的要求

机房内对新风处理一般在品质上有以下要求：

洁净度：高于50万级的洁净度（大于0.5μm的粉尘粒子，不多于500000粒/in^3）；室外大气一般含尘量为百万级至千万级之间，因此，相应的过滤器净化效率应在90%以上，新风的净化效率至少在中效以上。

温度：新风处理后引入室内的温度应与室内回风温度相仿，才不至于影响室内温度，造成局部的冷热不均或导致新风管道结露。

湿度：新风是影响室内湿度的主要因素，与风的引进直接相关，新风的湿度最好采用单独处理的方式。

2. 新风设计标准

空调系统的新风量依据机房设计规范应取以下两项中的最大值：

保证工作人员每人40m^3/h；维持室内正压，即主机房相对于室外为9.8Pa，其他房间相对于室外为4.9Pa。

但实际上，根据以上三种条件计算的新风量往往不够准确：由于室内的设备多少、建筑结构、人员多少等在不同的机房各不相同，因此按总送风量计算的新风量不够准确；新风的作用除了保持正压外，往往是保证室内空气的品质；避免发生污染物积聚空气品质霉变，因此人员多少也不能有效反映机房内的新风量。维持室内正压的数值是在工业洁净车间、实验

室的设计规范基础上修改而来的，由于机房的密封无法向洁净车间那样严格，很难准确估算机房内的漏风面积，因此对于维持具体数字的正压要求，其风量是很难计算的，通常需根据经验估算。所以，在机房设计时计算实际的新风需要量，一般是采用经验值的计算方法：按照室内容积的循环次数来计算。根据设计师的经验及不同的机房环境，0.6～1.2 次/h 的新风量系数能较好地满足机房的 9.8Pa 正压需求。

3. 新风处理需要考虑的因素

1）温湿度：新风与室内可能在温度上存在较大的差距，因此大量引进新风会较大地影响室内的温湿度。尤其是湿度，机房专业空调因为风量大，通过表冷器的风速快，因此除湿功能相对较差。新风引进时必须考虑室内其他空调设施的冷量冗余是否足够，否则需要采取对新风的温湿度预处理措施。

2）风速：直接送风时，风速不应超过 3m/s；室内气流速度大致不得超过 1m/s（不准确）；进风口风速不得超过 3m/s。

3）噪声：根据新风设备放置位置、处理风量等确定。

4）气流组织：合理的气流组织才能达到机房内有效通风；气流组织的基本原则是全面通风，不留死角。

5）节能：新风的引进会造成较大的热湿负载，会消耗较大量的空气处理能源，因此在新风引进方案中采取必要的节能措施是值得考虑的。

6）系统的稳定性：新风系统作为机房系统与室外环境的一个窗口，其稳定性影响着机房系统的稳定性，由于新风系统的过滤器等耗材需要经常更换，因此必须考虑更换的方便性、极限情况、系统的耐用性。

6.6　机房消防系统

6.6.1　气体灭火消防系统

电子信息系统机房应根据机房的等级设置相应的灭火系统，并应按现行国家标准《建筑设计防火规范》GB 50016—2006、《高层民用建筑设计防火规范》GB 50045—1995 和《气体灭火系统设计规范》GB 50370—2005，以及国家标准《电子信息系统机房设计规范》GB 50174—2008 的要求执行。

一般大型网络核心机房都应设置洁净气体灭火系统，不宜设置高压细水雾灭火系统或自动喷水灭火系统。而且网络核心机房应设置火灾自动报警系统，并且与消防设施实施联动。

气体灭火系统是指平时灭火剂以液体、液化气体或气体状态存贮于压力容器内，灭火时以气体（包括蒸汽、气雾）状态喷射作为灭火介质的灭火系统。并能在防护区空间内形成各方向均一的气体浓度，而且至少能保持该灭火浓度达到规范规定的浸渍时间，实现扑灭该防护区的空间、立体火灾。

采用管网式洁净气体灭火系统的主机房，应同时设置两种火灾探测器，且火灾报警系统应与灭火系统联动。灭火系统控制器应在灭火设备动作之前，联动控制关闭机房的风门、风阀，并应停止空调机和排风机、切断非消防电源等。机房内应设置警笛，机房门口上方应设置灭火显示灯。灭火系统的控制箱（柜）应设置在机房外便于操作的地方，且应有防止误

操作的保护装置。气体灭火系统的灭火剂及设施应采用经消防检测部门检测合格的产品。

目前，市场上较多使用七氟丙烷（HFC—227ea）灭火系统，自动灭火系统是一种高效能的灭火设备，其灭火剂 HFC—ea 是一种无色、无味、低毒性、绝缘性好、无二次污染的气体，对大气臭氧层的耗损潜能值（ODP）为零，是目前替代卤代烷 1211、1301 最理想的替代品。图 6-9 所示为气体灭火装置示意图。

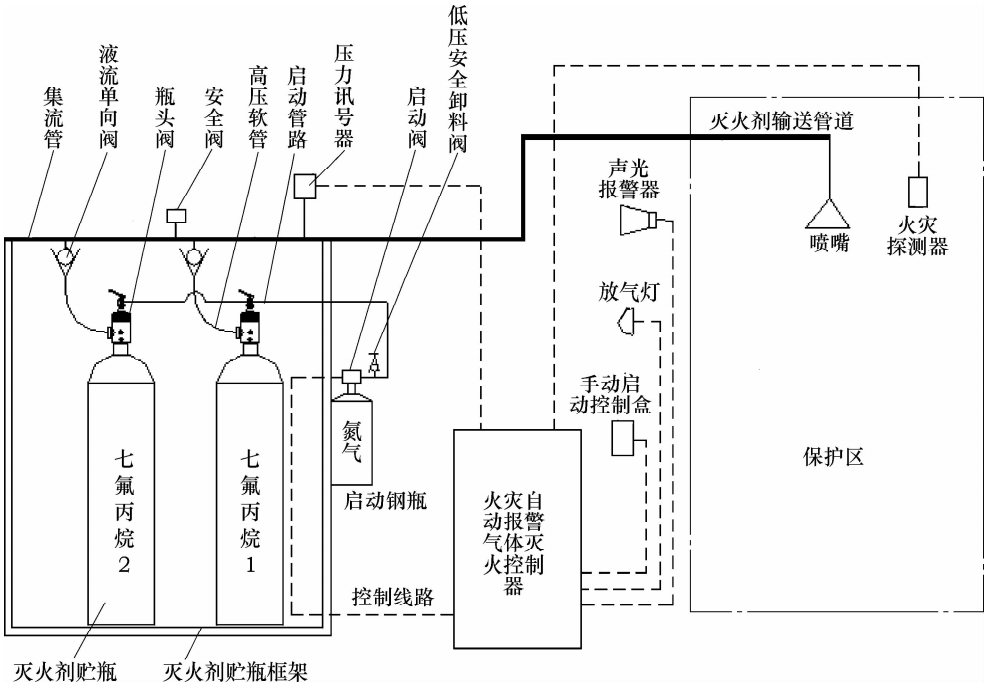


图 6-9　气体灭火装置示意图

6.6.2　消防报警及联动控制系统

消防报警及联动控制系统又称火灾报警系统、消防自动报警系统，由火灾报警主机、火灾特征或火灾早期特征传感器、人工火灾报警设备、输出控制设备组成。传感器完成对火灾特征或火灾早期特征的探测，并将相关信号传送到火灾报警主机。报警主机完成对信号的显示、记录，并完成相应的输出控制。火灾自动报警及联动控制系统，如图 6-10 所示。

火灾探测器通过对火灾发出的燃烧气体、烟雾粒子、温升和火焰的探测，将探测到的火情信号转化为火警电信号。在现场的人员若发现火情，也应立即直接按动手动报警按钮，发出火警电信号。火灾报警控制器接收到火警电信号，经确认后，一方面发出预警、火警声光报警信号，同时显示并记录火警地址和时间，告诉消防控制室（中心）的值班人员；另一方面将火警电信号传送至各楼层（防火分区）所设置的火灾显示盘，火灾显示盘经信号处理，发出预警和火警声光报警信号，并显示火警发生的地址，通知楼层（防火分工程区）值班人员立即察看火情并采取相应的扑灭措施。在消防控制室（中心）还可能通过火灾报警控制器的通信接口，将火警信号在微机彩显系统显示屏上更直观地显示出来。

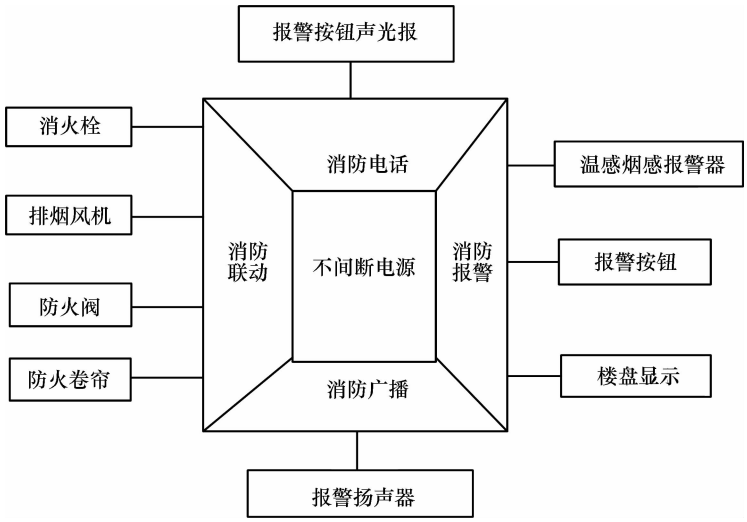


图 6-10　火灾自动报警及联动控制系统

联动控制器则从火灾报警控制器读取火警数据，经预先编程设置好的控制逻辑（“或”、“与”、“片”、“总报”等控制逻辑）处理后。向相应的控制点发出联动控制信号，并发出提示声光信号，经过执行器去控制相应的外控消防设备，如：排烟阀、排烟风机等防烟排烟设备；防火阀、防火卷帘门等防火设备；警铃、警笛和声光报警器等警报设备；关闭空调、电梯迫降和打开人员疏散指示灯等；启动消防泵、喷淋泵等消防灭火设备等。外控消防设备的启停状态应反馈给联动控制器主机并以光信号形式显示出来，使消防控制室（中心）值班人员了解外控设备的实际运行情况，消防内部电话、消防内部广播起到通信联络和对人员疏散、防火灭火的调度指挥作用。

6.7　机房弱电系统

6.7.1　网络核心机房综合布线系统

1. 网络核心机房综合布线系统的特点

网络核心机房主要承载两方面的功能：一是提供整个网络核心设备的运行环境并且与园区类所有楼宇弱电间互连；二是网络核心机房一般还承载数据中心的功能，它需要为所有服务器、存储设备提供标准的机房运行环境。因此，网络核心机房的综合布线系统不同于传统意义的综合布线系统，具有自身的特点如下：

1）单位面积信息点数量大。网络核心机房机柜密集，设备数量多，信息点密度高。

2）扩展性强。网络核心机房机柜多，需要预留大量信息点，可扩展性要求高。

3）以数据传输为主。网络核心机房服务器及存储系统，主要以数据传输业务为主。

4）光纤信息点数量多。牵涉多种设备接口、光纤跳线密度高。

5）以水平子系统模式为主。机房面积固定，主要以水平子系统为主。

6）线路敷设方式特殊，能适应机房的应用特点和设备特点。一般要考虑机房机柜布局，采用上走线架桥方式比较常见。

7）能综合规划一些设备间的非常规布线。非常规布线主要是大量设备及机柜之间不可预测的一些级联。

2. 配线区域的规划

一个大型网络核心机房的综合布线系统是比较复杂的，主要考虑的细节是机房机柜区域的划分，要充分考虑机房的特点、功能布局，进行仔细的规划设计。一般机房机柜内的布线信息点比较密集，既有光纤也有双绞线，并且对配线架、理线架的标示显得非常重要。

网络核心机房一般分为接入区（包括园区其他功能楼宇的光缆接入、电信网络接入等）、核心交换机区（包括校园网核心交换机、路由器、防火墙等）、服务器区（包括应用服务器、Web 服务器、DNS 服务器、邮件服务器、视频服务器等）、存储区等区域。在考虑网络核心机房布线时，应按照不同的区域进行布线并按照不同的功能区域进行线缆的编号。这样即便于管理与维护，也能保证核心机房的整洁与美观。

网络核心机房布线包括核心机房内布线和核心机房外的主进线间（电信间）的布线。对于核心机房内的布线，还要划分为网络核心主配线区、各排列机柜列头配线区和机柜布线区。

（1）主配线区

主配线区主要是网络核心设备的所在地，核心设备主要是指区域网络核心交换机、路由器、防火墙等。这些核心设备既要与互联网等电信级运营商连接，也要与园区内各楼宇的汇聚设备互连，还要与机房内各排列机柜列头柜配线区互连。

（2）各排列机柜列头配线区

采用列头柜结构，本列机柜所有铜缆/光缆都汇聚到列头柜的交换机中，通过有源交换设备把所有铜/光的数据传输转换为多芯的光缆传输（芯数根据性能要求配置）。所有经过列头柜转换出来的多芯光缆汇聚到主配线区的核心交换机中，通过核心有源交换设备传输数据和连接外部电信光缆。两层结构更加灵活和科学，改变和升级简单，电信级别的数据中心采用的结构，线缆数量较少，适合中大型的网络中心或数据中心。列头柜布线机构如图 6-11 所示。

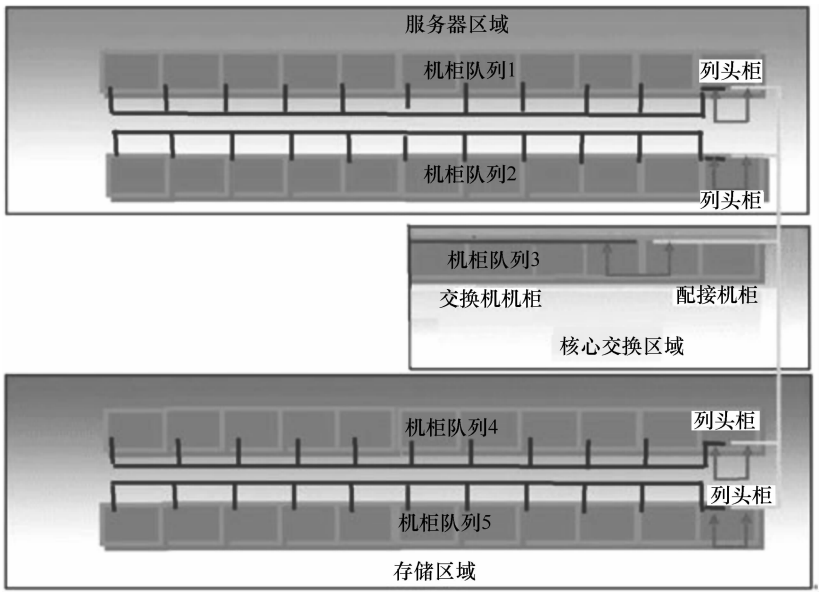


图 6-11　列头柜布线机构

（3）机柜布线区

机柜布线区主要是各机柜内的布线，是分配给终端设备安装的空间，如图 6-12 所示。机柜内可以包括计算机系统和通信设备，服务器和存储设备，刀片服务器和服务器及外围设备。机柜布线区的水平线缆端接在固定于机柜或机架的连接硬件上。需为每个机柜布线区的机柜或机架提供充足数量的电源插座和连接硬件，使设备缆线和电源线的长度减少至最短。

图 6-12　机柜布线区

网络核心机房外支持的布线空间主要包含进线间。进线间是网络核心机房的中心结构化布线系统和外部配线及公用网络之间接口与互通交接的场地，设置用于分界的连接硬件。进线间的设置主要用于电信线缆的接入和通信设备的放置，还有敷设至各楼宇的光缆都汇聚在进线间。这些设施在进线间内经过电信线缆交叉转接，接入网络核心机房内。

3. 新式桥架与上走线

卡博菲是一家法国公司，目前是世界上最大的网格式桥架制造商。卡博菲提供创新的网格式电缆桥架，适用于动力缆、数据缆、光缆、控制缆等各种线缆。另提供各种支架配件，可满足不同的安装方式：吊装、墙装、地板下安装、梁柱安装、环绕机器安装，近年来在各类大型网络机房建设中比较流行，如图 6-13 所示。相比于传统桥架，卡博菲新型的网格式桥架具有以下特点：

1）美观。由于电缆可见，要求施工时电缆顺序摆放。又由于卡博菲桥架做工精细，整个系统在安装完毕后显得很美观。

2）电缆的使用寿命增长。由于是开放式桥架，热量不会在桥架内聚集，即桥架内温度不会升高，使得电缆使用寿命增长。

3）维护维修工作简单。由于经常会增加或变更设备，因此同时就会拆除或增加电缆，而使用卡博菲桥架可以最大限度地观察到电缆，所以很容易辨别需要更换的电缆，使得维护和维修工作变得简单。

4）降低电缆采购成本并降低能耗。由于是开放式桥架，线缆自然通风散热，热量不会聚集，桥架内温度不会升高。因此线缆性能得到了优化，可以使用截面积更小的电缆。从而

降低了电缆采购成本，并在实际运行中降低了能耗。

5）桥架规格可变小，节省空间。由于电缆在封闭式桥架中敷设量最多只能是桥架截面积的40%，造成桥架型号偏大。卡博菲桥架是开放式桥架，电缆在承载力允许的情况下可以满布，从而在使用卡博菲桥架时可以减小规格，节省空间，并有可能降低费用。

6）高耐腐蚀性。卡博菲桥架有多种表面处理工艺可供选择。其中热镀锌的锌层厚度是60～80μm，且镀层均匀，抗腐蚀性强。对于一些特殊的环境，卡博菲还可提供经钝化的304L和316L高品质不锈钢系列桥架和配件，保证了产品的耐用性。

7）灵活性。卡博菲产品不用订制任何弯头、三通、变径等部件。它可按照现场的实际情况采用直段桥架直接加工做成各种形式，从而减少了浪费，降低了成本。

8）安装和拆卸简单、快捷。卡博菲公司众多专利的附件产品和FAS快速安装系统，保证了桥架与墙体之间及桥架与桥架之间连接迅速，拆卸方便。可以大幅度减少施工时间，从而降低成本。

9）重量轻。减轻整个系统的载荷，并降低运输成本。且在施工中可降低劳动力成本。

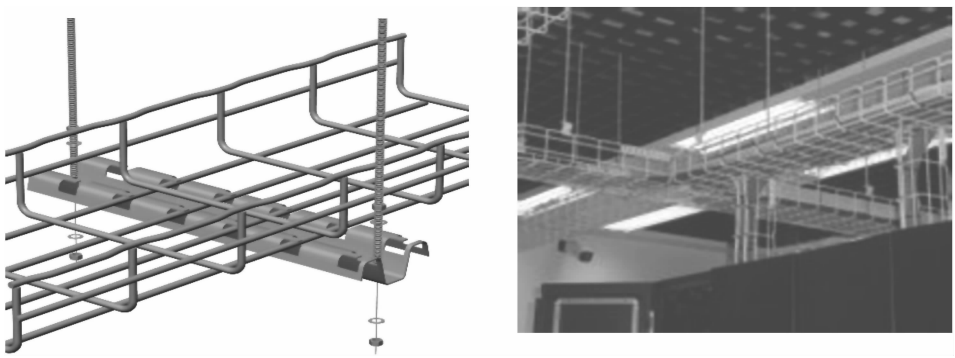


图6-13　卡博菲桥架上走线方式

4. 光纤布线

随着光纤和光纤接入设备价格的持续下降，一些网络核心机房用光纤替代传统双绞线铜缆将光纤延伸至服务器、交换机、存储设备等，以面向高端网络应用的需求。根据TIA/EIA568B和ISO/IEC11801的规定，水平部分敷设的光纤应为OM1、OM2、OM3级别的多模光纤。

1）OM1级别具有200/500MHz·km带宽的62.5/125μm多模光纤，这种光纤在水平90m距离支持千兆应用游刃有余。

2）OM2级别是具有500/500MHz·km带宽的50/125μm多模光纤，由于光纤以太网的快速发展，万兆以太网的不断应用，OM2级别的多模光缆即被OM3所超越，但在千兆以太网的应用中还有一定的空间，特别是千兆光纤到桌面的应用中。

3）OM3是拥有1500/500MHz·km和2000MHz·km两个频带的50/125μm光纤，它的目标是在300m距离上支持万兆以太网应用。

由于光缆及交换机端口的价格不断下降，以及国家对信息的保密要求，光纤布线系统的应用将会是未来发展的趋势。

6.7.2　KVM 系统

KVM 是键盘（Keyboard）、显示器（Video）、鼠标（Mouse）的缩写。KVM 技术的核心思想是：通过适当的键盘、鼠标、显示器的配置，实现系统和网络的集中管理；提高系统的可管理性，提高系统管理员的工作效率；节约机房的面积，降低网络工程和服务器系统的总体拥有成本；避免使用多显示器产生的辐射，营建健康环保的机房。利用 KVM 多主机切换系统，系统管理员可以通过一套键盘、鼠标、显示器在多个不同操作系统的主机或服务器之间进行切换并实施管理。

KVM 系统可以用在网络核心机房、数据中心、信息控制中心 、呼叫中心、证券/金融交易系统、工业控制环境、教学环境、测试中心等所有多服务器或多计算机工作环境。KVM 具有即插即用的功能，操作起来方便简单。可支持 PC、SUN 和 MAC 等各种品牌计算机和服务器。适用于 NETWARE、WIN95/98/2000/ME/XP/NT、UNIX、OS/2 等各种操作系统和应用软件。可适配 VGA、SVGA 和 XGA 等各种分辨率的显示器。有自动扫描、热键切换和 OSD 菜单等强大功能。

近年来流行的数字 KVM 切换器一般有模拟控制台接口，所以又可以称为数模结合产品，从硬件上看与模拟 KVM 不同的是，它有一个以太网接口，通过此接口用户可以远程访问数字 KVM 交换机。从数字 KVM 交换机到用户终端传输的是 IP 数字信号，而服务器到数字 KVM 交换机依然是模拟信号，这样对于数字 KVM 交换机来说，只要它有一个 IP 地址，用户就可以通过网络来控管机房设备了，可以实现强大的远程管理功能。IP-Based KVM 切换器代表着新一代 KVM 切换技术。区别于过去传统 KVM 切换器的使用方法，IP-Based KVM 切换器是一款数字设备，通过现有的网络来连接 KVM 切换器的远程 over-IP，从而实现远程控制连接到 KVM 装置的多台计算机。如果用户不得不管理分布于不同地点的多个服务器机房，IP-Based KVM 切换器提供的远程访问功能将帮助你简化服务器机房的管理。用户只需将 IP-Based KVM 切换器安装在各服务器机房，即可轻松地管理所有服务器。

如图 6-14 展示了某网络核心机房基于 KVM 系统的集中控管方案。通过两台基于 IP 的数字化 KVM 服务器，可以轻松实现远程机房监控管理中心，还可以供远程用户在外对机房的设备进行管控。

6.7.3　机房动力环境监控系统

随着信息时代的来临和迅猛发展，计算机系统的数量和规模与日俱增，网络核心机房已成为各企事业单位的重要组成部分，在日常生产和管理中起着举足轻重的作用。机房环境设备（供配电、UPS、空调、消防、保安等）是大型机房必不可少的重要设备，它为计算机系统的正常运行提供必要的可靠的保障。一旦这些设备出现故障，就会影响计算机系统的运行，甚至影响企事业单位的正常运营，造成严重后果。对于银行、证券、邮局、海关、IDC 等单位，机房管理更为重要，一旦计算机系统出现故障，造成的损失是不可估量的。

机房动力环境监控系统是综合机房整体分布环境的一个机房集中监控系统，是完整的室内集中监控系统。被监控对象按功能分为动力和环境两大类。

1）动力类包括：高压配电、低压配电、UPS、油机、电源、电池组、空调等。

2）环境类包括：门禁、烟感、温度、湿度等。

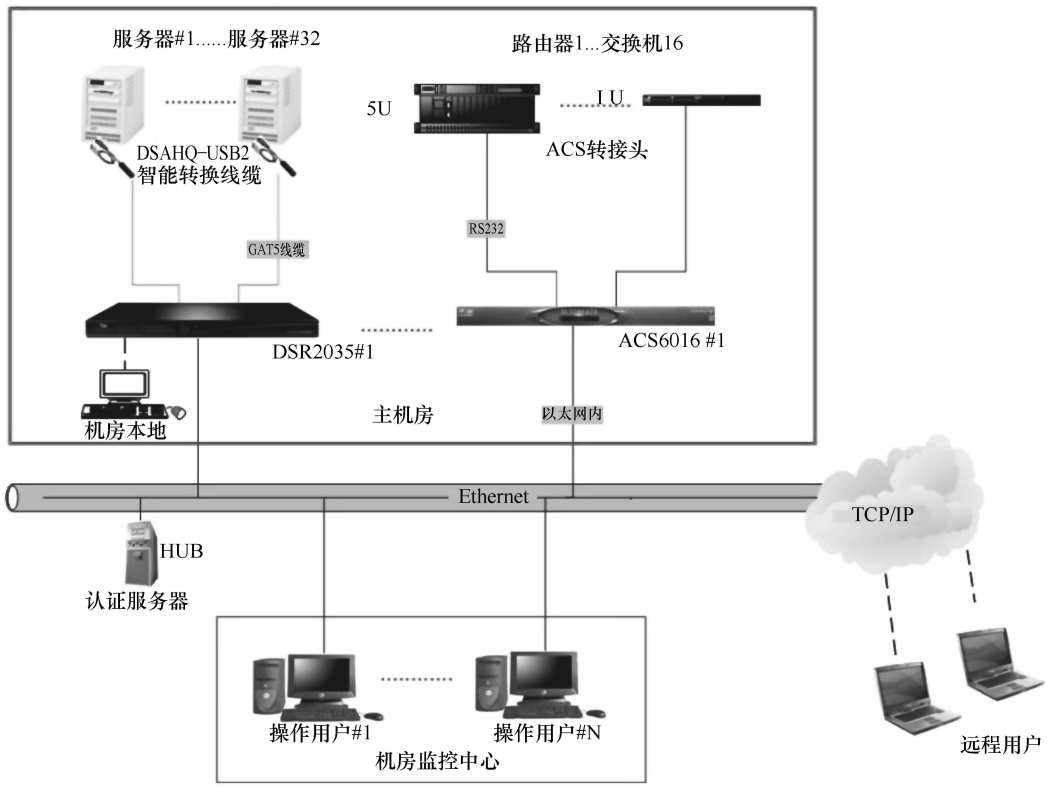


图 6-14　某网络机房基于 KVM 系统的集中管理控制方案

被监控对象按采集方式分为智能设备和非智能设备两大类。

1）智能设备本身具有数据采集和处理能力，并带有智能接口，可以与上位机通信。

2）非智能设备本身不具备数据采集和处理能力，需要增加传感器、变送器和采集器来完成数据采集和上报。

目前，业界一般集成了这两大类监控系统，统称为机房环境综合监控系统或机房动力环境监控系统。

机房动力环境监控系统主要是对机房各类设备的运行信息进行监控数据采集。在采集子系统中，被监控信号的测量至关重要，被监控信号按照特性可以分为模拟量和开关量。

1）模拟量采集技术。模拟量是指随时间连续变化的量，对于这些信号的测量，需采用模-数（A-D，Analogue/Digital）转换设备将模拟量变成数字量后才能适合计算机采集。智能设备的模拟量信号由监控单元完成采集，而非智能设备的模拟量信号需要增加数据采集器、传感器、变送器等来完成采集，将非电量信号转换为适合采集器输入特性的电量信号。

2）开关量采集技术。开关量是指不连续变化的、具有确定的几种状态的量，最典型的是仅有“0”和“1”两种状态的开关量。非智能设备的开关量信号采集也需要增加开关量传感器和采集器。

采集的数据通过有线或无线、短信等方式传送到监控服务器上，在监控服务器上对采集到的数据进行加工分析，形成监控显示、报名和分析、告警功能。图 6-15 展示了一个典型的机房综合监控系统。

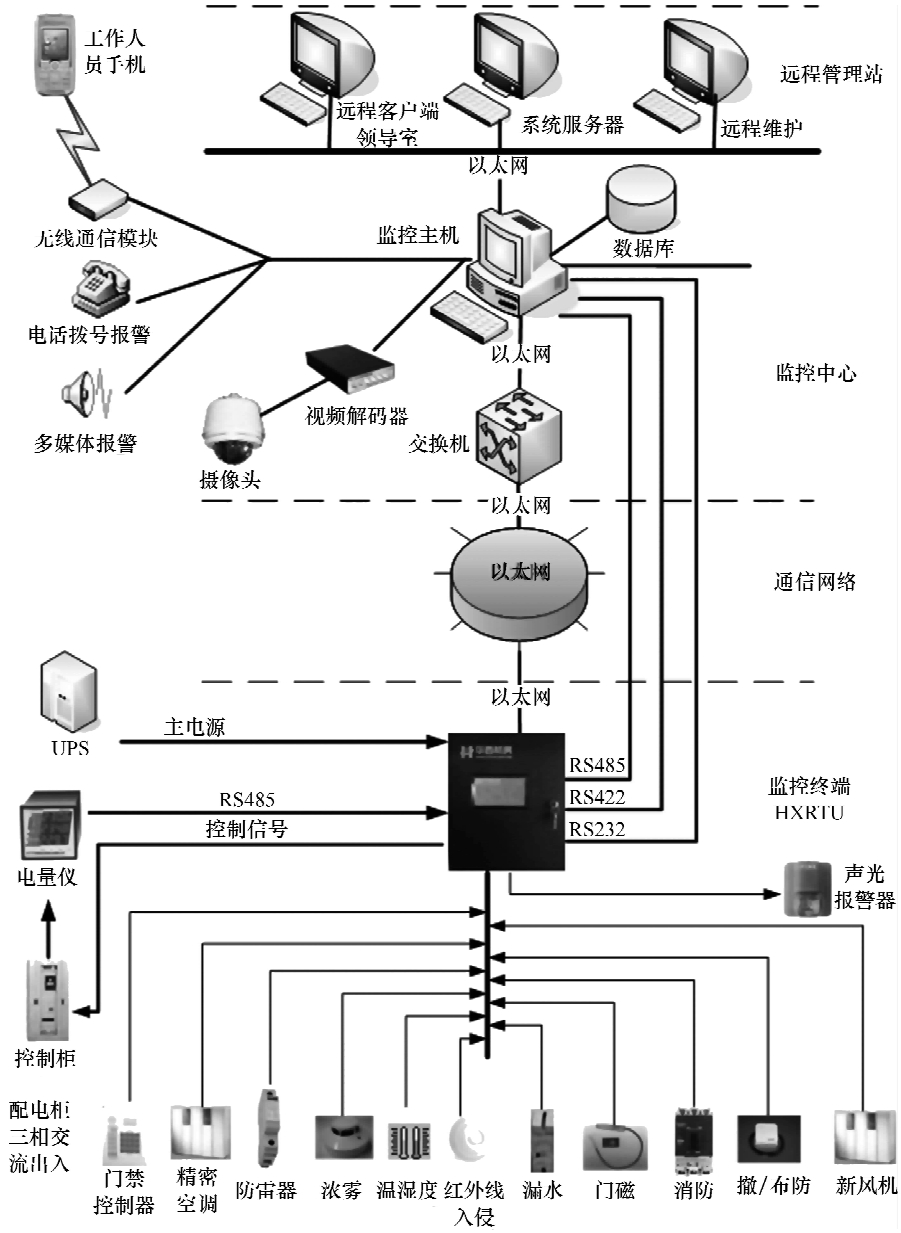


图 6-15　机房综合监控系统

6.8　网络核心机房设计案例

6.8.1　设计案例情况概述

某高校计划设计建设一个校园网核心机房，要求按照最新执行的国家标准 GB 50174—2008《电子信息系统机房设计规范》中 C 级机房建设的标准要求进行设计。一期工程建设范围包含大楼一层面积约 100m^2 的 UPS 配电室、消防钢瓶间以及主机房（200m^2）、视频监

控室、网管监控室、服务中心、用户接待室区域，机房建设面积合计约 400m^2。主机房所在楼层层高约 5.0m，梁下净高 4.0m，主机房内地面下陷 0.5m，架空地板敷设高度为正负 0m，顶棚内墙面、顶棚面作刷漆防尘处理，采用铝合金微孔板吊顶，机房地板面至吊顶面净空高度设计为 2.8m。

市电环境考虑引自大楼地下低压配电室，大楼低压配电室提供来自不同电网的两路市电电源，两个容量为 630A 的断路器，功率为 300kVA，两路市电引至机房 UPS 配电室，互投后给机房内 UPS 和空调等市电电源供电。本工程 UPS 配电系统为便于 2 期的扩容，采用模块化 UPS，一期共安装 15kVA 模块 5 个，组成 15kVA ×4（60kVA）输出 +15kVA ×1 备份模块，可方便地扩容至 120kVA + 备份模块。

现有若干台计算机设备及网络设备，一期建议安装 20 台设备机柜，新机房建成后将它们都装入机柜，由 1 台新增 120kVA 模块化 UPS 供电。本机房工程由以下 7 大子系统组成，主要包括：

1）机房装修工程；
2）机房 UPS 电源及其供配电、照明及防雷接地系统；
3）机房空调通风系统；
4）机房综合布线系统；
5）机房动力环境监控系统；
6）气体消防及火灾自动报警系统；
7）机房 KVM 集中管理系统。

6.8.2 机房装修工程

对机房装修工程设计采用专业设计，提供防静电活动地板敷设和金属石膏复合板饰墙面、柱面、铝合金微孔吊顶顶棚、轻钢龙骨双层双面石膏板隔断墙、亚光不锈钢包封 12mm 防火/钢化玻璃隔断墙和钢制防火门安装，其他各类细节处精装修。

秉承满足先进性、实用性、安全性、可观赏性的原则，核心设备及材料均采用知名品牌。做到专业的设计，一流的设备，精心的施工，以确保本机房质地高雅、精致，线条流畅，具备现代机房风貌的整体品质。装修方案见表 6-4。

表 6-4 装 修 方 案

名称 / 位置	地面	天花	墙面	隔断	门
主机房	德国“林德纳”复合防静电活动地板	荷兰“普菲尔”金属微孔吊顶板	北京“兴铁库”金属石膏复合板	12mm 防火玻璃隔断墙	防火玻璃门
UPS 配电室	德国“林德纳”复合防静电活动地板	荷兰“普菲尔”金属微孔吊顶板	环保乳胶漆	大楼混凝土墙	甲级钢制防火门
网管监控室	德国“林德纳”复合防静电活动地板	荷兰“普菲尔”金属微孔吊顶板	环保乳胶漆	12mm 钢化玻璃隔断墙	钢化玻璃门
视频监控室	德国“林德纳”复合防静电活动地板	荷兰“普菲尔”金属微孔吊顶板	环保乳胶漆	12mm 钢化玻璃隔断墙	钢化玻璃门

（续）

名称 / 位置	地面	天花	墙面	隔断	门
服务中心	石材楼地面	荷兰“普菲尔”金属微孔吊顶板	环保乳胶漆	12mm 钢化玻璃隔断墙	钢化玻璃门
用户接待室	石材楼地面	荷兰“普菲尔”金属微孔吊顶板	环保乳胶漆	12mm 钢化玻璃隔断墙	甲级钢制防火门
钢瓶间	大楼原地面	荷兰“普菲尔”金属微孔吊顶板	环保乳胶漆	大楼混凝土墙	甲级钢制防火门

机房外观如图 6-16 所示。

图 6-16　机房外观图

6.8.3　机房供配电、照明及防雷接地系统

1. 电气设计说明

机房进线电源采用三相五线制；机房内用电设备供电电源均为三相五线制及单相三线制；机房用电设备设过载保护，同时配电系统各级之间有选择性地配合，配电以放射式向用电设备供电；机房配电系统所用线缆均为阻燃聚氯乙烯绝缘导线及电缆，敷设镀锌铁线槽、镀锌电线管及金属软管；机房内配电系统与消防系统联动。

2. 计算机设备配电系统

须由 UPS 提供电力的机房计算机设备包括计算机主机、服务器、存储设备、网络设备、通信设备以及控制终端设备等，由于这些设备进行数据的实时处理与实时传递，关系重大，所以对电源的质量与可靠性的要求最高。在设计中，对计算机主机设备供电选用 A 级标准。

计算机设备的供配电：

本工程机房空调、市电设备输入功率按照 150kVA 考虑，1 台模块化 UPS 输入功率按照 150kVA 考虑，机房内总配电容量为 300kVA。

本工程设计考虑从低压配电室引两路不同母线段的市电电源，功率为 300kVA，开关容量为 630A。采用 4 根 ZRYJV－4×120＋1×70 电缆分成双路分别引至 UPS 配电室内 AT 互投

柜内上口，经过双路切换后，变成一路切换电源，输出至 AP 市电配柜上口。AP 配电柜为精密空调、照明、UPS 系统、新排风等设备供电。UPS 输出至 JAP 输出配电柜，分别为主机房、监控终端等电子信息系统设备供电。考虑采用 UPS 不间断电源，为的是最大限度地满足机房计算机设备对供电电源质量的要求。UPS 电源布线采用放射式配电方式配至各用电设备，采用阻燃聚氯乙烯绝缘电线（ZRBV）沿地板下的金属线槽敷设到位（支路管线可以利用 JDG 管敷设）。

3. 照明配电系统

（1）正常照明配电系统

照明配电系统由市电供电。照明配电电源拟由机房市电配电柜 AP 供电。灯具由配电柜中的断路器、房间区域安装于墙面上的翘板开关控制。根据实际使用情况及 GB 50174—2008《电子信息系统机房设计规范》规定，机房区照度不小于 500Lx，辅助区照度不小 300Lx。本工程机房照度以及其辅助区域照度均严格按照上述规范设计实施，达到机房区照度大于 500Lx，辅助区照度大于 300Lx。

（2）应急照明配电系统

在市电停电后，为保证工作人员做存盘等紧急处理以及工作人员撤离场地，计算机房及消防通道必须具备应急照明系统。设计考虑机房内设应急照明灯，通道及出口设疏散指示灯。机房内应急照明的照度不低于 50Lx，疏散指示灯的照度大于 5Lx。应急照明电源取 UPS 电源。

4. 防雷/接地部分

机房设有四种接地形式，即：计算机专用直流逻辑地、配电系统交流工作地、安全保护地、防雷保护地。本次设计考虑直流逻辑地、交流工作地、安全保护地、防雷保护地均利用大楼联合接地体（接地电阻小于 1Ω，已满足机房要求）。并在机房设置等电位接地箱。用接地母线与大楼联合接地体相连。机房地板支架、机柜外壳等不带电的金属部分均应与此接地网相连。

机房设均压等电位带，即 30mm × 3mm 铜带接地网，敷设在活动地板下，依据计算机设备布局，纵横组成网格状，配有专用接地端子，用软铜线以最短的长度与计算机设备相连。计算机直流地需用接地母线引至等电位带。

容易产生静电的活动地板采用导线布成泄漏网，并用干线引至等电位箱接地端子。活动地板静电泄漏干线采用 ZR-BVR-50mm^2 导线，静电泄漏支线采用 6mm^2 铜箔，支线导体与地板支腿螺栓紧密连接，支线做成网格状，间隔不大于 2.4m × 2.4m；金属吊顶板、金属龙骨、金属壁板、不锈钢玻璃隔墙的金属框架等也用导线连接，接入等电位箱。并且每一连续金属框架的静电泄漏支线连接点不少于两处。

为防止感应雷、侧击雷沿电源线进入机房损坏机房内的重要设备，大楼低压配电屏已设置第一级电源防雷装置，本机房在市电电源配电箱上口加设第二级防雷装置，在 UPS 输出箱上口加设第三级防雷装置。选用德国 OBO 浪涌防雷器。

5. UPS 系统

考虑到机房的建设等级以及便于未来的扩容，设计采用 1 台意大利“先控”（SICON）120kVA 模块化 UPS 系统向主机房内设备提供高质量的电源，一期安装 15kVA 模块 5 台，组成 60kVA + 备份模块输出的 UPS 系统，60kVA UPS 的系统后备电池供电时间为 120min。未

来机房扩建时，可以通过增加功率模块的方式扩展到 120kVA +2（备份模块）。

在本次机房项目中，我们设计使用意大利 SICON CMS 系列供电解决方案来保护整个计算中心内的不同设备。CMS 系列整机采用模块化热插拔技术。模块化结构可以使得系统结构更加清晰，降低系统的复杂度，提高系统的可靠性；模块化热插拔技术可以使得系统的配置随需要任意调整。例如，模块化结构减少了备件的数量，避免购买大量备品备件，浪费资金；模块化结构大大降低了设备维修时间，不需要 UPS 厂商专业工程师就可以及时排除故障，保障系统的连续运行；一个功率模块发生故障，只会影响 15kVA 的功率输出，其他模块仍然可以正常运行，普通 UPS 将会影响到总输出；模块化结构可以实现单机冗余，且冗余度可以随负载量的变化自动调整，其可用性要高于两台普通 UPS 并联；模块化结构在 IT 设备上已被广泛使用（如：小型机、大型机），这种结构是各种设备发展的方向。

6.8.4　机房空调及新风系统

1. 精密空调设计及负载计算

（1）机房设计标准

计算机机房内有严格的温、湿度要求，机房内按国标 GB/T 2887—2011《计算机场地通用规范》的规定配置空调设备：

级　　别	A 级	
	夏季	冬季
	22 ±2℃	20 ±2℃
相对湿度	45% ~65%	
温度变化率	<5℃/h 并不得结露	

同时，主机房区的噪声声压级小于 68dB；主机房内要维持正压，与室外压差大于 9.8Pa；送风速度不小于 3m/s；在表态条件下，主机房内大于 0.5μm 的尘埃不大于 18000 粒/L。为使机房能达到上述要求，应采用精密空调机组才能满足要求。

（2）精确总热负载的计算

本工程主要的热负载来源于设备的发热量及维护结构的热负载。因此，我们要了解主设备的数量及用电情况以确定精密空调的容量及配置。根据以往经验，除主要的设备热负载之外的其他负载，如机房照明负载、建筑维护结构负载、补充的新风负载、人员的散热负载等，如不具备精确计算的条件，也可根据机房的面积按经验进行测算。

根据规范要求并结合本机房的实际特点，在不同的机房区域，我们按 UPS 配电输出功率及空调区围护结构散热等因素，对应实际的机房空调制冷区域进行估算，并根据各区域使用性质，做到不同程度的备份。

2. 空调配置方案

现根据上述因素的计算结果，推荐选用意大利“海洛斯”（HIROSS）牌机房专用精密空调产品。参照计算结果以及考虑到一定余量，查看空调型号，做出以下配置：

主机房选用两台意大利双模块“海洛斯”55.4kW 下送风型精密空调。两台精密空调组成 1 +1 备份运行模式。UPS 配电室采用两台日本“大金”5P 柜式空调系统。其他区域采用

大楼中央空调。

3. 新风系统

本工程机房内新风引自室外新风，主机房采用一台 1500 风量温湿度预处理新风机，将新风送至机房各区域，以维持机房内 9.8Pa 正压。UPS 配电室采用一台 400 风量新风机。

本工程在主机房内设置一台 5000 风量事故排风机，UPS 配电室采用一台 1500 风量事故排风机，以备在消防气体释放后将混合气体排出室外。排风量按照每小时换气 5 次以上计算。

6.8.5 综合布线系统工程

1. 设计范围

本方案在机房内机柜间提供水平布线系统，进户干线由大楼提供端接至网络设备。采用美国“康普”六类非屏蔽布线、室内多模光纤布线系统。

2. 系统实现

主机房一期共设计安装 20 台设备机柜，其中 5 台作为网络设备、配线机柜，另 15 台作为服务器机柜。每台服务器机柜内安装 1 个 24 口六类配线架、一个 12 口光纤配线架。采用“卡博菲”线槽上走线，六类非屏蔽双绞线布线系统。每个六类配线架各布设 24 根六类线，配线架其中的 12 端口为 KVM 系统布线提供。每个光纤配线架敷设 8 芯光纤。各监控室终端布设六类点若干。网络机房至主机房的干线由电信运营商提供安装。

6.8.6 消防系统

本工程采用有管网组合分配式七氟丙烷气体消防、火灾自动报警系统。本工程分为两个消防分区：

气体消防分区 1：主机房，200m^2。

气体消防分区 2：UPS 配电室，80m^2。

采用一套有管网七氟丙烷组合分配式气体自动灭火消防系统以及火灾自动报警系统。

七氟丙烷气体自动灭火消防系统的特点如下：

1）灭火力强，灭火时间短，能灭 A、B、C 型火灾。

2）灭火后无污染、腐蚀作用，不导电，没有残留物，对臭氧层无破坏。

3）低浓度灭火，液态储存，药剂占地面积小。

4）毒性低，可以应用于有人值守的场所。

6.8.7 机房环境及设备集中监控系统

机房环境及设备集中监控系统主要包括：

1）设备监测系统安装——UPS、配电柜、精密空调、温湿度监测。

2）漏水检测系统安装——采用两套绳式空调漏水监测系统。

3）门禁系统安装——采用 12 套磁卡感应式门禁系统。

4）图像监控系统——安装 16 套彩色半球摄像机。

5）防入侵检测系统——安装 5 套微波/红外线双鉴探测器。

6）温湿度监控系统——采用温湿度传感器，地板下、工作区两层检测机房内温湿度。

机房环境与动力设备监控子系统由监控主机、远程管理计算机、计算机网络、智能模块、远程模块、总线协议转换模块、信号处理模块、多设备驱动卡及智能设备等组成。为了增强系统的功能，用户可根据需要选择配置多媒体声卡、智能电话语音卡、短消息发送器等设备，实现系统的扩展功能。

机房 KVM 集中管理系统采用美国“AVOCENT”KVM 集中管理系统，集中管理 128 台服务器设备。

6.9　网络核心机房未来发展趋势

6.9.1　传统数据中心的弊端

传统数据中心的弊端，主要表现在以下几个方面：

1）管理不断增长的能源成本。据国际正常运行时间协会 Uptime Institute 调查，目前服务器三年用电和冷却的费用一般为服务器硬件采购成本的 1.5 倍。随着经济型、功能更加强大的高性能计算机集群需求的增长，电力成本还将不断上升，而且关系到预算能否承受电力和冷却费用的问题。

2）电力不够。由于城市的高速发展，区域电力系统逐渐无法满足日益增长的扩容需求。然而，新的服务器、存储和网络产品在性能提高、价格降低的同时，耗电量却在不断增大。因此，电力不够成为企业面临的棘手问题。

3）冷却能力不够。目前，许多客户的数据中心已用了 10 ~ 15 年，冷却基础设施难以满足当前需求。传统冷却方法可为每机架提供 2 ~ 3kW 制冷量，而目前每机架需要的制冷量却达到了 20 ~ 30kW。单机柜的功率密度比数据中心过去的设计指标提高了许多倍。

4）空间不够。每当新项目或应用上线时，需要配置新的服务器或存储子系统，因此，随着业务需求的增长，设备占地面积的激增，当不能添加服务器和存储时，只好再建一个数据中心，这种扩建的成本非常高。

上述问题的不断出现，表明建立绿色数据中心是企业的必然选择。

6.9.2　数据中心能耗效率计算

在数据业务需求的爆炸式增长及 IT 技术的迅速发展的共同推动下，数据中心在 21 世纪进入迅猛发展时期，而与此同时数据中心的能耗问题也随着其发展变得越来越无法忽视。数据中心的能耗相对于其他的建筑能耗有其自身的特殊性：耗能设备的种类繁多、专业性强，对它的节能研究是一项多专业综合的系统工程。

由于现在仍没有所谓的标准数据中心的概念，数据中心配置变化很大，这使得以往用来评价建筑能耗效率的单位面积能耗量这个参数失去了应有的评判意义，因此需要一个新的指标来评价数据中心的能耗效率。

美国 GreenGrid 提出了 PUE（Power Usage Effectiveness）和 DCE（Datacenter Efficiency）两个参数作为数据中心的能耗效率指标，如下所示：

$$PUE = \frac{TotalFacilityPower}{ITEquipmentPower} \tag{6-1}$$

$$DCE = \frac{TotalFacilityPower}{ITEquipmentPower} \tag{6-2}$$

其中，*TotalFacilityPower* 作为数据中心的总能耗而 *ITEquipmentPower* 则为前面所提到的 IT 设备能耗。PUE 作为目前被广泛接受的数据中心能效指标，在实际使用中也暴露出一些问题：

1）某些数据中心的能耗供应往往不是专用的，这就为 PUE 公式中的 TotalFacilityPower 的获得设置了障碍。

2）最新的制冷技术由于强调所谓的精确制冷，往往是和 IT 设备直接集成，这样制冷能耗和 IT 设备能耗之间的界限变得不再清晰，也为 PUE 的计算带来了困难。

为提高 PUE 的可使用性，GreenGrid 也提出了相应的修正，将 PUE 分解：

$$\text{PUE} = \text{CLF}(\text{Cooling Load Factor}) + \text{PLF}(\text{Power Load Factor}) + 1 \tag{6-3}$$

其中，CLF 为总制冷能耗与 IT 设备能耗的比值，而 PLF 则为电源供应系统与 IT 设备能耗的比值。除了 PUE 及 DCE 之外，GreenGrid 还提出了 DCPE 这一概念性的能效指标，如下所示：

$$\text{DCPE} = \frac{UsefulWork}{Total\ Facility\ Power} \tag{6-4}$$

这个指标的提出实质上将数据中心黑箱处理，只考虑其输入输出量，而如何来确定 UsefuleWork 是阻碍其由概念性定义成为工程使用的指标的障碍。有学者认为，随着 UsefuleWork 量化研究的不断开展，DCPE 参数必将成为未来数据中心能效指标的必然选择。

6.9.3 绿色数据中心

毫无疑问，数据中心能耗巨大，正日益引起人们的高度关注。绿色数据中心（Green Data Center）的呼声日渐高涨。绿色数据中心是指数据机房中的 IT 系统、机械、照明和电气等能取得最大化的能源效率和最小化的环境影响。绿色数据中心是数据中心发展的必然。总的来说，我们可以从建筑节能、运营管理、能源效率等方面来衡量一个数据中心是否为“绿色”。绿色数据中心的“绿色”具体体现在整体的设计规划以及机房空调、UPS、服务器等 IT 设备、管理软件应用上，要具备节能环保、高可靠性、可用性和合理性。

Uptime Institute 白皮书定义了 4 个确定，数据中心相对“绿色”的要素。4 个绿色指标是 IT 系统设计和建筑、IT 硬件资产利用、IT 硬件效率和机房物理基础设施。

IT 设备用电量包括所有 IT 设备以及用于监控或控制数据中心的辅助设备的负载，前者如服务器、存储和网络设备；后者如键盘、视频、鼠标开关、监视器、工作站或移动计算机。基础设施用电总量包括 IT 设备及支持 IT 设备的系统负载，如：

1）供电设备，如不间断电源（UPS）、开关柜、发电机、配电箱（PDU）、电池、IT 设备外部配电损耗。

2）冷却系统，如制冷机组、计算机房空调（CRAC）、直接膨胀空气调节器（DX）、泵及冷却塔等。

3）计算机、网络及存储。

4）低负载条件下工作时，不间断电源（UPS）设备效率下降。

5）其他杂项器件的负载，如数据中心照明。

建设绿色数据中心，必须要考虑 3 个核心要素：

（1）基础设施

机房基础设施方面需要考虑的问题包括：

1）如何以及在何处使用能源。

2）基础设施目前可优化的空间（从 DCiE 或 PUE 来衡量）。

3）本数据中心是以电量和性能为主，还是仅以性能为主。

4）是投资建立新的数据中心，还是投资升级现有数据中心。

5）数据中心现场是否适应变更。

6）数据中心所需要的可靠性水平是否增加了基础设施能耗，现有备份或备用设备存在多少闲置，是否足够，还是过多，能否撤销部分设备。

7）应选择哪些支持设备（不间断电源、飞轮发电机、发电机、配电柜、制冷机组、CRAC 等），今后的发展趋势如何，基础设施能否满足下一代硬件电力和冷却要求，例如，更多的 IT 设备今后采用水冷。

8）基础设施是否存在过热问题，是否存在湿度问题。

9）是否可以采用免费制冷。

10）电力、冷却或空间是否影响当前运营，哪些因素影响今后业务发展，未来能否在现有能源范围内增加计算能力；现场基础设施在以下方面是否达到最佳水平：气流与散热、配电分配、冷却、照明、监控与管理。

11）必要时，是否需要采用水冷。

（2）IT 设备

IT 设备方面的问题如下，其中包括硬件设计以及机架现有冷却、供电和监控方式：

1）设备是否采用节能硬件，是否采用节电功能。

2）目前是按现场、基础设施还是机架选择供电和冷却方法。

3）硬件是否具备电量、热量、资源利用率监控功能，是否可以监控能耗。

4）用电量如何计费。

5）谁可以提供帮助。

（3）利用率

服务器和存储利用率方面的问题如下：

1）基础设施利用率是否达到最佳水平。

2）是否存在不必要的备份设备。

3）可以进行合并与虚拟化吗。

4）如何将离散或孤岛式计算转变为共享模式。

5）是否可以监控资源利用率，当前情况及未来趋势如何。

6）如何对基础设施提供的服务进行计费。

7）谁能提供帮助。

本 章 小 结

网络核心机房建设是集建筑、电气、安装、网络等多个专业技术于一体的工程。对于一

个大型企事业单位，具有多种信息业务系统，往往建有一个大型园区网络的网络核心机房或数据中心机房。本章主要从工程的角度，针对网络核心机房或数据中心建设的技术进行了讨论。

1）简要介绍了网络核心机房的组成。

2）介绍了一个大型核心机房的规划、布局与设计理念。

3）详细分解了一个网络核心机房的各个子系统，并且介绍了各个子系统的设计或建设技术。

4）给出了一个网络核心机房建设案例，并对其进行了分析。

5）探讨了绿色数据中心的未来发展趋势。

第7章　网络管理

随着计算机网络技术的高速发展，网络管理的重要性越来越突出。第一，网络规模逐渐增大，网络的复杂性大大增加；第二，各种网络新技术的不断应用，各种网络新设备不断投入使用，网络设备从生产厂家到型号规格都不相同，而且网络设备的功能有简单的也有极其复杂的；第三，在计算机网络基础上构造的应用系统对计算机网络系统的性能包括可靠性、安全性、稳定性等要求越来越高，这些性能也必须通过网络管理系统解决。从这几点来看，网络管理已经成为网络系统中不可缺少的重要部分，是网络可靠、安全、高效运行的保障和必不可少的手段。

7.1　网络管理的基本概念

7.1.1　什么是网络管理

实际上，网络管理并不是一个新概念。网络管理并不是指对网络进行行政上的管理。狭义上看，网络管理的直观理解类似于物业管理，指网络设备和线路的清单、网络拓扑结构、配置和状态等；广义上看，网络管理的直观理解类似于社会管理，指基础设施管理、网络基础设施之上的数字化社会的管理以及网络和用户行为管理。

目前，关于网络管理的定义很多，一般来说，网络管理主要是规划、监督、设计和控制网络资源的使用和网络的各种活动，以保其尽可能长时间的正常运行，或者当网络出现问题的时候尽可能快地发现和修复故障，使之最大限度地发挥其应有的效益的过程。

国际标准化组织（ISO）在 ISO/IEC7498-4 中定义并描述了开放系统互连（OSI）管理的术语和概念，提出了一个 OSI 管理的结构并描述了 OSI 管理应有的行为。它认为，开放系统互连管理是指这样一些功能，它们控制、协调、监视 OSI 环境下的一些资源，这些资源保证 OSI 环境下的通信。

从网络管理的定义可以看出，网络管理包括：收集网络中各种设备和系统的工作参数、运行状态信息；处理收集到的各种信息，并以各种各样的方式呈现给网络管理员；接收网络管理员的指令或根据对上述信息的处理结果向网络中的设备发出控制指令，即实施网络控制功能，同时监视指令执行的结果。具体来说，网络管理包含两大任务：一是对网络运行状态的监测，二是对网络运行状态进行控制。监测是控制的前提，控制是监测结果的处理方法和实施手段。

网络管理的目的就是使网络中的资源得到更加有效的利用。它应维护网络的正常运行，当网络出现故障时能及时报告和处理，并协调、保持网络系统的高效运行。图 7-1 描述了一个网络管理的一般模型。

该图描绘的网络管理的一般模型是一个 C/S 结构。图中的管理者（Manager）是客户端，管理者驻留在管理工作站上，代理（Agent）是服务端，代理则驻留在被管设备上，通

过网络管理协议进行信息交换。由管理者接收网络管理员的命令，并通过网络管理协议向代理发送，同时接收来自代理进程的响应或通告信息，并向网络管理员显示或报告；代理负责接收来自管理进程的命令并发起响应事件。

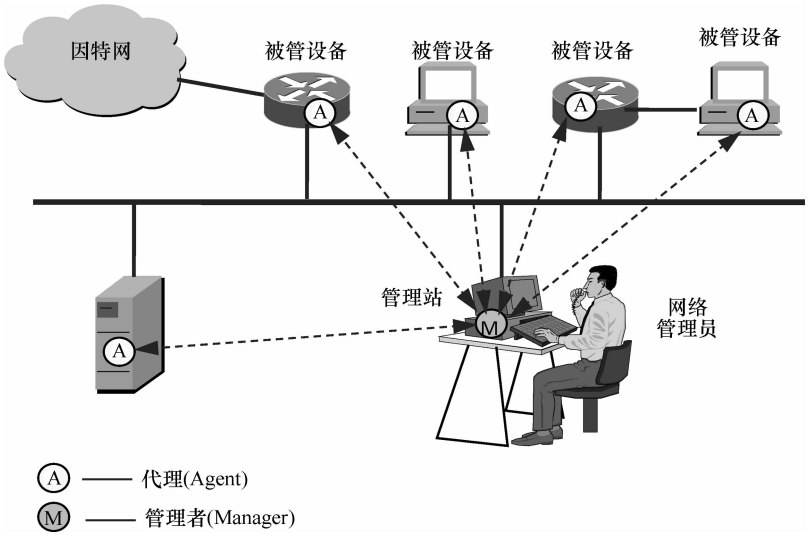


图 7-1　网络管理的一般模型

图中还有一个网络管理工作站，简称管理站，又称为控制台，管理站运行管理应用来监视和控制被管设备。在物理上，管理站通常是具有高速 CPU、大内存、大硬盘等的工作站，管理站作为管理网络的界面，在管理环境中至少需要一台网络管理工作站。管理站一般都是带有监视器的工作站，可以显示所有被管设备的状态，例如，连接是否掉线、各种连接上的流量状况等。

管理站（硬件）或管理程序（软件）都可称为管理者（Manager）。Manager 不是指人而是指机器或软件。网络管理员（Administrator）指的是人。

由此可见，该模型是由计算机网络、管理员及网络管理系统等部分紧密结合而成。目前从技术发展的情况看，实际上现有的网络管理软件已经全部发展为 B/S 结构，基于 Web 的网络管理软件，管理思想基本上一致。

7.1.2　网络管理系统的概念

网络管理系统是在网络运行环境中，实现网络管理方法和网络管理功能的应用系统。它是由硬件设备和软件组成的。网络管理系统的主要任务是收集网络中的各种设备或设施的工作参数、工作状态信息，显示给网络管理人员并接受网络管理人员对它们的控制，对工作参数进行修改等操作。

网络管理系统逻辑模型如图 7-2 所示。

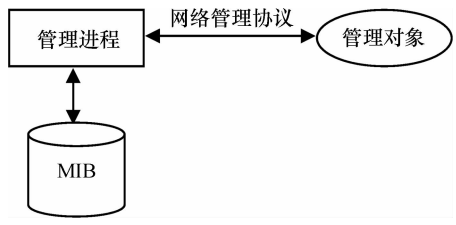


图 7-2　网络管理系统逻辑模型

从图 7-2 可以看到一个最简单的网络管理系统模型。一个网络管理系统从逻辑上可以认为是由管理对象、管理进程、管理信息库和网络管理协议 4

个部分组成的。

1）管理对象。管理对象是经过抽象的网络元素，对应于网络中具体可以操作的数据，如记录设备或工作状态的状态变量、设备内部的工作参数、设备内部用来表示性能的统计参数等。

2）管理进程。又称管理者，是负责对网络中的设备和设施进行全面管理和控制的软件。

3）管理信息库 MIB（Management Information Base）。管理信息库是一个信息存储库，它包含了管理代理中的有关配置和性能的数据，有一个组织体系和公共结构，其中包含分属不同组的许多个数据对象。

4）网络管理协议。网络管理协议有 SNMP 协议等，SNMP 是由一系列协议和规范组成的，它们提供了一种从网络上的设备中收集网络管理信息的方法。

7.2 网络管理的目标和内容

7.2.1 网络管理的基本目标

网络管理的目标就是满足运营者及用户对网络的有效性、可靠性、开放性、综合性、安全性和经济性的要求。这些要求都是网络实际应用过程中网络经营者或者网络使用者提出的基本要求。

1）网络应该是有效的。就是说，网络必须要能够准确及时地传递信息。这里所指的有效性与通信的有效性不同，通信的有效性是指传递信息的效率，而网络的有效性是指网络服务要可用，而且有质量保证。

2）网络应该是可靠的。网络可靠性至关重要，如果网络出现故障导致网络服务中断，那么势必造成巨大的经济损失。网络可靠性要求网络必须保证连续稳定的运转，不能时断时续，并且对各种故障以及自然灾害有较强的抵御能力和一定的自愈能力。

3）现代网络要有开放性。就是网络必须兼容各种厂商生产的网络设备和通信设备。

4）现代网络要有综合性。就是网络业务和服务不能单一化，要有电话网、电报网、数据网等分离的状态向综合业务数字网（ISDN）过渡，以后计算机网络、电话网络、有线电视等网络也走向整合，而且网络图像、视频等各种业务都能在网络上运行。

5）现代网络要有很高的安全性。网络安全的问题日益突出，人们对网络安全的要求越来越高，现代网络必须具备很高的安全性。

6）网络的经济性。网络的经济性有两个方面：一是对网络经营者而言，网络的建设、运营和维护等开支要小于业务收入，否则，其经济性无从谈起；二是对用户而言，网络业务要有合理的价格，如果价格太高，用户承受不起，或虽能承受得起但是感到付出的费用超过了业务的价值，那么用户拒绝应用这些业务，网络的经济性就无从谈起。

从上述六点基本要求来看，网络管理的目的就是最大限度地增加网络可利用的时间，合理地组织、分配和利用网络系统资源，保证网络正常、可靠和安全地运行，提供安全、可靠、经济、有效和优质的网络服务，以满足网络经营者和网络用户的需要。

7.2.2 网络管理的主要内容

从网络管理的定义可以看出，网络管理就是对网络的状态进行监测，对网络的运行状态进行控制。对网络状态的监测主要是检查一下网络是否运行正常；对网络运行状态的控制主要是对网络的状态进行合理调节，保障网络服务的性能。对于一个网络管理员来说，借助于网络管理系统，不仅要完成性能管理、故障管理、计费管理、配置管理和安全管理五大功能，还要完成其他的一些日常管理工作。网络管理员的日常工作虽然很繁杂，但是简要总结一下主要有七项任务：网络基础设施管理、网络操作系统管理、网络应用系统管理、网络用户管理、网络安全保密管理、信息存储备份管理和网络机房管理。这些管理涉及多个领域，每个领域的管理又有各自特定的任务。

1. 网络基础设施管理

在网络正常运行的状况下，网络管理员对网络基础设施的管理主要包括：确保网络通信传输畅通；掌握局域网主干设备的配置情况及配置参数变更情况，备份各个设备的配置文件；对运行关键业务网络的主干设备配备相应的备份设备，并配置为热后备设备；负责网络布线配线架的管理，确保配线的合理有序；掌握用户端设备接入网络的情况，以便发现问题可迅速定位；采取技术措施，对网络内经常出现用户需要变更位置和部门的情况进行管理；掌握与外部网络的连接配置，监督网络通信状况，发现问题后与有关机构及时联系；实时监控整个局域网的运转和网络通信流量情况；制订、发布网络基础设施使用管理办法并监督执行情况。

2. 网络操作系统管理

网络管理员在维护网络运行环境时的核心任务之一是网络操作系统管理。在网络操作系统配置完成并投入正常运行后，为了确保网络操作系统工作正常，网络管理员首先应该能够熟练地利用系统提供的各种管理工具软件，实时监督系统的运转情况，及时发现故障征兆并进行处理。在网络运行过程中，网络管理员应随时掌握网络系统配置情况及配置参数变更情况，对配置参数进行备份。网络管理员还应该做到随着系统环境变化、业务发展需要和用户需求，动态调整系统配置参数，优化系统性能。最后，网络管理员还应该为关键的网络操作系统服务器建立热备份系统，做好防灾准备。因为网络操作系统是网络应用软件和网络用户的工作平台，一旦发生致命故障，这个网络服务将陷入瘫痪状态。

3. 网络应用系统管理

对于普通用户，计算机网络的价值主要是通过各种网络应用系统的服务体现的。网络管理员日常系统维护的另一个重要职责，就是确保这些服务运行的不间断性和工作性能的良好性。任何系统都不可能永远不出现故障，关键是一旦出现故障如何将故障造成的损失和影响控制在最小范围内。对于要求不可中断的关键型网络应用系统，网络管理员除了在软件手段上要掌握、备份系统配置参数和定期备份系统业务数据外，必要时在硬件手段上还需要建立和配置系统的热备份。对于用户访问频率高、系统负载大的网络应用系统服务，必要时网络管理员还应该采取负载分担的技术措施。

4. 网络用户管理

除了通过软件维护进行系统管理外，网络管理员还需要直接为网络用户服务。用户服务与管理在网络管理员的日常工作量中占有很大一部分份额，其内容包括：用户的开户与撤销

管理，用户组的设置与管理，用户使用系统服务和资源的权限管理和配额管理，用户计费管理，以及包括用户桌面联网计算机的技术支持服务和用户技术培训服务的用户端支持服务。建设计算机网络的目的是为用户提供服务，网络管理员必须坚持以人为本、服务至上的原则。

5. 网络安全保密管理

信息存储备份管理和网络机房管理。这些管理涉及多个领域，每个领域的管理又有各自特定的任务。

不设防的网络好比在开门揖盗，网络管理员在提供网络服务的同时必须特别注重网络的安全与保密管理。安全与保密是一个问题的两个方面，安全主要指防止外部对网络的攻击和入侵，保密主要指防止网络内部信息的泄露。根据所维护管理的计算机网络的安全保密要求级别的不同，网络管理员的任务也不同。对于普通级别的网络，网络管理员的任务主要是配置管理好系统防火墙。为了能够及时发现和阻止网络黑客的攻击，可以再配置入侵检测/防御系统对关键服务提供安全保护。对于安全保密级别要求高的网络，网络管理员除了应该采取上述措施外，还应该配备网络安全漏洞扫描系统，对关键的网络服务器采取容灾的技术手段。更严格的涉密计算机网络，还要求在物理上与外部公共计算机网络绝对隔离；对安置涉密网络计算机和网络主干设备房间的要采取安全措施，控制管理人员的进出；对涉密网络用户的工作情况要进行全面的监控管理。

6. 信息存储备份管理

在计算机网络中最贵重的是什么？不是设备，不是计算机软件，而是数据和信息。任何设备都有损坏的可能，任何软件都有过时的时候，设备损坏可以重新购置，软件可以更新，信息和数据一旦丢失，损失将无法弥补。因此网络管理员还有一个重要职责，就是采取一切可能的技术手段和管理措施，保护网络中的信息安全。对于实时工作级别要求不高的系统和数据，最低限度网络管理员也应该进行定期手工操作备份；对于关键业务服务系统和实时级别高的数据和信息，网络管理员应该建立存储备份系统，进行集中式的备份管理；最后，将备份数据随时保存在安全地点更是非常重要的。

7. 网络机房管理

网络机房是安置网络系统关键设备的要地，是网络管理员日常工作的场地。根据网络规模的不同，网络机房的功能复杂程度也不同。一个正规的网络机房通常分为网络主干设备区、网络服务器设备区、系统调试维护维修区、软件开发区和空调电源设备区。对于网络机房的日常管理，网络管理员的任务是：掌管机房数据通信电缆布线情况，在增减设备时确保布线合理，管理维护方便；负责机房设备供电线路的安排，在增减设备时注意负载的合理配置；管理网络机房的温度、湿度和通风状况，提供适合的工作环境；确保网络机房内各种设备的正常运转；确保网络机房符合防火安全要求，火警监测系统工作正常，灭火措施有效；采取措施，在外部供电意外中断和恢复时，实现在无人值守情况下保证网络设备安全运行。另外，保持机房整洁有序，按时记录网络机房运行日志，制订网络机房管理制度并监督执行，也是网络管理员的日常基本职责。

7.2.3 网络管理的基本方式

网络管理的方式是随着网络技术的发展而变化的。早期以人工交换电话网为主的网络管

理是以人工方式进行的，由于网络设备构成和网络业务都非常简单，管理内容主要是电话业务流量的控制以及转接电话路由的选择等工作。自动交换机和计算机网络出现以后，由于交换机和路由器等网络设备本身具有一定的网络管理功能，出现了人工与自动相结合的管理方式。但这时网络设备的管理功能还是很有限的，这时的管理方式主要是以网络管理中心为主的集中方式。随着计算机技术和网络技术的飞速发展，网络设备越来越复杂，网络设备本身就提供了强大的网络管理功能，使得网络管理的方式从集中方式变为以分散方式为主。为了能够综合管理整个网络，在网络之上又专门建立了网络管理网，使网络管理系统在体系结构上更加合理。在传统的常规网络管理方式的基础上，现在还呈现出智能化的网络管理方式，依赖先进的网络管理方式，能更加有效地掌控网络，更好地达到网络管理的目标。

7.2.4 网络管理的对象

一个网络管理系统是在计算机网络环境中，采用一定的网络管理方法，对被管理的计算机网络的运行状态进行监测和控制的软硬件系统。那么，网络管理到底“管理”什么呢？一般来说，凡是与实际所管理的计算机网络相关的硬件设备、软件及其业务系统都是被管理的对象。

1. 网络硬件系统

网络硬件系统主要是指组建计算机网络的一些硬件设备，包括主机、交换机、路由器、服务器、终端、UPS 电源等，也包括一些通信基础设备（如 PDH/SDH 传输设备、DWDM 传输设备等）。这些设备可以看成是构成计算机网络系统的各个节点的业务节点设备，用传输线缆将这些节点设备按照节点之间的关系组建，它们一般都是物理上存在的一些实体，看得见，摸得着，这些硬件设备都属于网络管理的对象。

2. 网络软件系统

网络软件系统是指计算机网络硬件设备正常运行所需要的一些软件，如网络操作系统 Unix、Linux 和 Windows Server 2003 等，还包括一些网络管理的专用软件，用于对计算机网络进行监测和监控，这些软件主要是一些具有较强网络管理功能的系统软件，辅助管理员管理网络使用。

3. 网络业务系统

网络业务系统主要是计算机网络中面向用户提供的各种应用性业务。这些业务在网络设备上运行，从某种意义上说，网络硬件系统和网络软件系统都是为网络业务系统准备的。网络业务系统运行在计算机网络中，网络业务系统也成为网络管理重要的管理对象之一。

7.3 网络管理的基本功能

国际标准化组织 ISO 在网络管理框架（ISO/IEC 7498-4）中为网络管理定义了五大功能并被广泛接受。它们是配置管理、故障管理、性能管理、安全管理和计费管理。实际上，在网络管理过程中，网络管理涉及的工作远远不止这些，包括网络的规划设计和网络操作人员的管理等，都是和网络管理紧密相关的。本节主要围绕这五大功能一一做简单的介绍。

7.3.1 配置管理

配置管理是最基本、最核心的网络管理功能，目的是管理网络的建立、扩充、改造和提

供。主要提供资源清单管理功能、资源开通功能、业务开通功能及网络拓扑服务功能。配置管理负责监控网络的基本配置信息，使网络管理人员可以根据需要随时查询、生成和修改软硬件的运行状态及参数，以保障网络的正常运行。

配置管理是一个中长期的活动，它要管理的是因网络增容、设备更新、新技术的应用、新业务的开通、新用户的加入、业务的撤销、用户的迁移等原因而导致的网络配置的变更。网络规划与配置管理关系密切，在实施网络规划的过程中，配置管理发挥最主要的管理作用。

1. 资源清单管理功能

资源清单管理是配置管理的基本功能。在一个大型网络中，需要管理的设备比较多，如果每个设备的配置信息都完全依靠管理人员人工获取，工作量是相当大的，而且不容易做到。资源清单管理功能可以联机提供网络中的网络设备、器材、电路、服务、客户、设备厂商等资源的信息，即使在网络管理人员不是很熟悉网络结构和配置状况的情况下，也能通过有关的技术手段来完成对网络配置信息的查询。

在网络设备的配置信息中，可以将网络资源清单定义为被管对象，重点描述其属性、连接及状态。根据网络管理协议标准的 MIB 建立资源 MIB，提供对资源清单的提取、增加、删除和修改等功能。

2. 资源开通功能

资源开通功能保证根据客户的业务需求，经济合理地供应、开发和配置所需的资源。资源开通功能所指的资源主要是指提供接入、交换、传输和 MIB 等功能的网络设备。这些网络设备包括硬件和软件，硬件如网络基础设施、公用装置、插接件、跳线等；软件如网络操作系统、数据库等。

3. 业务开通功能

业务的开通从用户要求时开始，到网络实际提供业务时结束。它包含网络装载和管理业务所需要的过程。业务的提供也具有向各个客户或客户组分配物理资源或逻辑资源的能力。

4. 网络拓扑服务功能

网络拓扑服务提供显示网络及各个构成层次的布局的功能。显示的网络布局有 3 种形式，即物理布局、逻辑布局与电气布局。为了支持各个层次各种形式的网络布局显示，需要网络配置数据库的支持，存放当前设备的配置数据，还要存放历史的配置数据，以便能够显示网络布局的变化过程。

7.3.2 故障管理

故障管理是网络管理中最基本的功能之一，它的目的是迅速发现和纠正网络故障，动态维护网络服务水平的一系列活动，这些活动保证了网络有高度的可用性和有效性。故障管理通过检测、记录日志，并通知用户，尽可能地自动修复网络故障，保障网络的正常运行。

用户总是希望网络提供的服务是不间断的、可靠的。事实上，网络对于设备和传输媒体的故障是脆弱的。硬件、软件和数据的问题都可能会引发网络故障。比如断电、程序缺陷、数据库错误、自然灾害等都是引发网络故障的原因。网络发生故障后，必须迅速进行故障诊断和故障定位，以便尽快恢复业务，修复故障。进行故障管理可以采取两种策略，即事后策略和预防策略。事后策略是一旦发现故障迅速进行修复的策略，发生故障首要任务是快速修

复故障，尽快恢复网络提供的业务；然后深入分析故障发生的原因及发生故障的网络组件，这些经验教训对防止类似故障的再次发生相当重要。预防策略是通过随时对网络的性能进行分析，主动探测和收集网络上的各种事件信息，尽可能发现发生故障的苗头，确定好修复措施。或者对网络中非常关键的设备采取冗余备份措施，一旦某些设备发生故障，迅速启用它的备用设备，尽力做到不影响网络的正常运行。一般来说，故障管理可以实现以下功能。

1. 故障检测和报警功能

故障检测是主动检测或被动接收网络上的各种事件信息，分析出其中与网络和系统故障相关的内容，对其关键部分保持跟踪，生成网络故障事件记录。报警功能是接收故障检测模块传来的报警信息，根据报警策略驱动不同的报警程序，以报警窗口/振铃（通知值班网络管理人员）或电子邮件（通知决策管理人员）发出网络严重故障警报。

2. 故障信息管理功能

故障信息管理是一件很有意义的管理，它对于预防故障的再次发生起到了很好的警示作用。有排错经验的管理员会经常检索并分析故障信息，故障信息的管理可以从两个方面入手：第一，网络管理人员应该深入分析故障发生的事件记录，定义网络故障并生成故障卡片，记录故障发生的原因和解决方案，这些故障信息的收集整理都是非常有用的；第二，故障信息很大一部分是网络设备模块自动记录的日志、报警信息等，这些信息对于网络管理人员修复网络故障都是非常有帮助的。

3. 故障定位功能

故障定位功能就是要确定网络设备中故障的位置，找出故障发生的真正原因。故障定位的手段主要有诊断、试运行和软件检查。

1）诊断：检验设备的性能是否正常。需要注意的是，在诊断进行期间，被诊断的设备不能进行正常的业务。

2）试运行：将部分网络设备隔离，利用被试运行设备正常的输入输出端口和测试器，系统地测试被隔离网络设备的所有服务特性。

3）软件检查：利用软件进行的检查有核查、校验和运行测试、程序跟踪等。

4. 电路测试功能

电路测试是对分散在不同位置的网络设备之间的线缆进行测试，看是否发生故障并且确定发生故障的位置。通常的方式是进行端到端的测试以检查故障。

5. 业务恢复功能

业务恢复是指在网络发生故障后，网络必须继续提供业务。通常采用的方法是在网络组建的时候预备一些冗余备用资源，一旦某些设备发生故障，将这些设备先隔离出来，启用备用的设备，以便快速恢复网络的正常运行。

7.3.3 性能管理

性能管理用来评估系统资源的运行状况及通信效率等系统性能。其能力包括监视和分析被管网络及其所提供服务的性能。性能分析的结果可能会触发某个诊断测试过程或重新配置网络以维持网络的性能。性能管理收集分析有关被管网络当前状况的数据信息，并维持和分析性能日志。目前高校的 P2P 流量大量占用着网络带宽，只有有效地对网络带宽进行分析统计并采取相关的措施，才能保证校园网高速地运行。一些高校使用流量控制设备对全网的

流量进行分析、统计，并制定相关的策略限制 P2P 流量，保证带宽的合理使用。校园网性能管理典型的功能包括：

1）收集、分析、统计网络设备的信息。

2）维护并检查系统状态日志。

3）确定自然和人工状况下系统的性能。

4）制定相关的管理措施保证校园网的合理使用。

7.3.4 安全管理

安全管理的任务主要是保证网络资源的安全，包括保护网络设备在内的各种网络资源，防止非法入侵，确保网络中的服务、数据及系统免受侵扰和破坏，包括网络管理系统本身也不会被非法使用，保证整个网络体系的安全。

安全管理的功能可以分为两个层次：一是网络管理系统本身的安全；二是被管网络对象的安全。需要明确的是，安全管理很大程度上依赖于现有的网络与信息安全技术，安全管理不可能做到百分之百保证网络不受到侵扰和破坏，对于安全管理来说，尽可能采用先进的网络安全技术手段抵御网络入侵和破坏，严格履行管理人员的职责，提高网络安全防范意识，最大限度地保障网络的安全。

一般来说，安全管理实现以下的功能。

1. 风险分析功能

网络风险时时刻刻困扰着网络，网络管理人员必须做到对网络系统受到侵扰和破坏的风险进行分析，对系统可能遭受威胁的网络设备做到心中有数，对潜在的各种攻击行为及其产生的严重后果进行分析，尽可能加强安全防范。

2. 安全服务功能

网络安全服务是通过网络安全机制来实现的，一般的网络会采取这些安全机制来提高网络安全性能，保障设备安全可靠地运行。这些安全措施包括加密、数字签名、认证、访问控制、路由控制、业务流分析保护等。

3. 报警、日志和报告功能

网络安全管理提供报警、日志和报告功能，通常可以帮助网络管理人员更好地掌握网络安全状况。一般重要的网络，预先安装有入侵检测系统（IDS），对非法访问网络的行为进行报警；这些报警信息有利于判别网络入侵行为。还有的网络设备提供了日志和报告功能，通过对这些设备运行和被访问的纪录进行分析，也可以判断出当前网络是否存在非法访问等情况。

4. 网络管理系统的保护功能

网络管理系统是网络的中枢机构，有关网络的一切信息和数据都和网络管理系统密切相关，这一部分是网络安全管理中的重点，必须采用高度可靠的安全措施对其保护。一般网络管理系统在设计之初，就格外重视网络安全防范的设计，通常有更为严格的安全身份认证、数据加密机制，并且能提供对网络管理系统自身保护的功能。

7.3.5 计费管理

计费管理主要负责监视和记录网络用户对网络资源的使用情况，并按相关标准核收费

用，其目的是通过收取用户使用网络服务的费用以便进行网络资源利用率的统计分析和网络成本效益的核算。计费管理所涉及的网络资源包括硬件资源和软件资源、网络服务及网络设施的额外开销，如运行、维护费用等。对于以盈利为目的的网络经营者来说，计费管理功能无疑是非常重要的。

计费管理一般有资费管理功能和账单管理功能。

1. 资费管理功能

作为网络的经营者或建设者，计算网络建设和运营成本，并且确定网络提供的资源的利用及收费标准，充分考虑了网络提供的各类服务和供需关系等因素制定出相应的资费政策。

2. 账单管理功能

在资费政策的标准控制下，网络管理系统能捕获用户使用网络资源或服务的事件，并且按相关收费标准，为用户计算出相应的费用账单。

7.4 802.1x 认证管理技术

7.4.1 802.1x 协议介绍

802.1x 协议起源于 802.11 协议（IEEE 的无线局域网协议），制订 802.1x 协议的初衷是为了解决无线局域网用户的接入认证问题。IEEE802LAN 协议定义的局域网并不提供接入认证，只要用户能接入局域网控制设备（如局域网交换机），就可以访问局域网中的设备或资源。这在早期企业网有线局域网应用环境下并不存在明显的安全隐患。

随着移动办公及驻地网运营等应用的大规模发展，服务提供者需要对用户的接入进行控制和配置。尤其是 WLAN 的应用和 LAN 接入在电信网上大规模开展，有必要对端口加以控制以实现用户级的接入控制，802.1x 就是 IEEE 为了解决基于端口的接入控制（Port-Based Network Access Control）而定义的一个标准。IEEE802.1x 协议是标准化的符合 IEEE802 协议集的局域网接入控制协议，其全称为基于端口的访问控制协议（Port Base Network Access Control Protocol），能够在利用 IEEE802 局域网优势的基础上提供一种对连接到局域网用户的认证和授权手段，达到接受合法用户接入、保护网络安全的目的。

7.4.2 802.1x 认证体系

802.1x 是一种基于端口的认证协议，是一种对用户进行认证的方法和策略。端口可以是一个物理端口，也可以是一个逻辑端口（如 VLAN）。对于无线局域网来说，一个端口就是一个信道。802.1x 认证的最终目的就是确定一个端口是否可用。对于一个端口，如果认证成功，那么就“打开”这个端口，允许所有的报文通过；如果认证不成功，就使这个端口保持“关闭”，即只允许 802.1x 的认证协议报文通过。802.1x 的体系为典型的 Client/Server 体系结构，如图 7-3 所示，它的体系结构中包括 3 个部分，即使用 802.1x 的系统包括三个实体：请求者系统、认证系统和认证服务器系统三部分。在实际应用中，三者分别对应：用户终端（Client）、交换机（Network Access Server，NAS）和认证服务器（RADIUS Server）。

1）请求者是位于局域网链路一端的实体，由连接到该链路另一端的认证系统对其进行认证。请求者通常是支持 802.1x 认证的用户终端设备，用户通过启动客户端软件发起

802.1x 认证。请求者即客户端，它是最终用户所扮演的角色，一般是用户 PC，目前最典型的客户端有 Windows XP 操作系统自带的 IEEE802.1x 客户端以及各大公司基于自身产品所推出的客户端，如锐捷公司的 STAR Supplicant 软件。

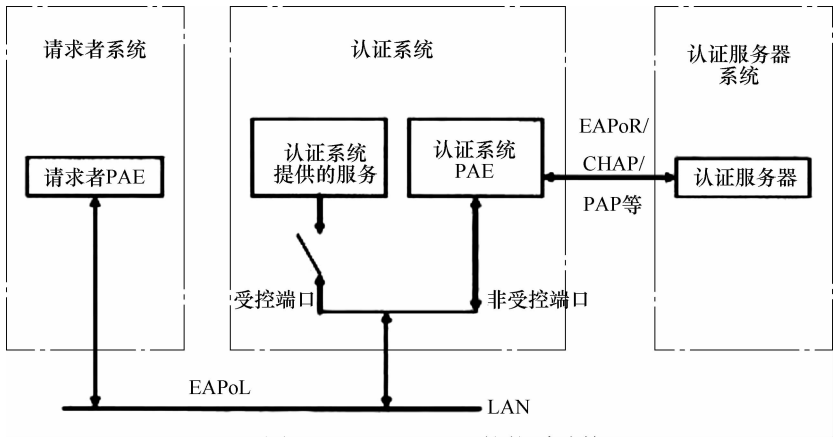


图 7-3 802.1x 认证的体系结构

2）认证系统。认证系统对连接到链路对端的认证请求者进行认证。认证系统通常为支持 802.1x 协议的网络设备，它为请求者提供服务端口，该端口可以是物理端口也可以是逻辑端口，一般在用户接入设备，如局域网交换机（LAN Switch）和无线接入 AP 上实现 802.1x 认证。认证者通常为支持 802.1x 协议的交换机，该设备的职责是根据客户端当前的认证状态控制其与网络的连接状态。在客户端和认证服务器之间，该设备扮演着中介者的角色。从客户端要求用户名核实从服务器端的认证信息并且转发给客户端，交换机要负责把从客户端收到的回应封装到认证服务器格式的报文并转发给认证服务器，同时还要把认证服务器收到的信息解释出来并转发给客户端。

3）认证服务器系统。认证服务器是为认证系统提供认证服务的实体，一般使用 RADIUS 服务器来实现认证和授权功能。请求者和认证系统之间运行 802.1x 定义的 EAPOL（Extensible Authentication Protocol over LAN）协议。当认证系统工作于中继方式时，认证系统与认证服务器之间也运行 EAP 协议，EAP 帧中封装认证数据，将该协议承载在其他高层次协议中（如 RADIUS），以便穿越复杂的网络到达认证服务器；当认证系统工作于终结方式时，认证系统终结 EAPoL 消息，并转换为其他认证协议（如 RADIUS），传递用户认证信息给认证服务器系统。

认证系统每个物理端口内部包含有受控端口和非受控端口。非受控端口始终处于双向连通状态，主要用来传递 EAPoL 协议帧，可随时保证接收认证请求者发出的 EAPoL 认证报文；受控端口只有在认证通过的状态下才打开，用于传递网络资源和服务。

7.4.3 802.1x 认证过程

认证过程可以由用户主动发起，也可以由认证系统发起。一方面，当认证系统探测到有未经过认证的用户使用网络时，就会主动向客户端发送 EAP-Request/Identity 报文，发起认证；另一方面，客户端可以通过客户端软件向认证系统发送 EAPOL-Start 报文，发起认证。

802.1x 系统支持 EAP 中继方式和 EAP 终结方式与 RADIUS 对接，从而利用远端的 RADIUS 服务器完成认证。以下关于两种认证方式的过程描述，都以客户端主动发起认证为例。

1. EAP 中继方式

这种方式是 IEEE 802.1x 标准规定的，将扩展认证协议（EAP）承载在其他高层协议中，如 EAPoR（EAP over RADIUS），以便扩展认证协议报文穿越复杂的网络到达认证服务器。一般来说，EAP 中继方式需要 RADIUS 服务器支持 EAP 属性：EAP-Message 和 Message-Authenticator。基本业务流程如图 7-4 所示，其认证过程如下：

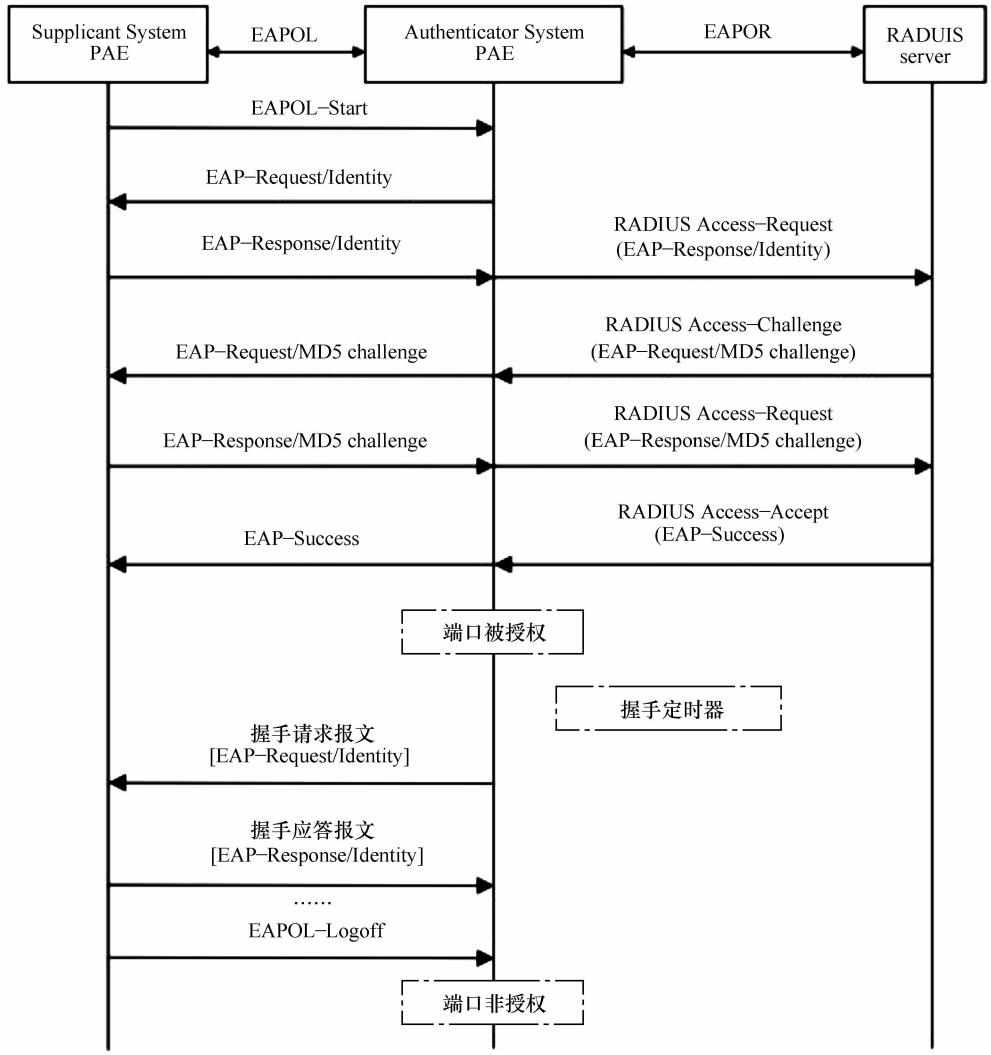


图 7-4　802.1x 认证系统的 EAP 中继方式业务流程

1）当用户有访问网络需求时打开 802.1x 客户端程序，输入已经申请、登记过的用户名和密码，发起连接请求（EAPOL-Start 报文）。此时，客户端程序将发出请求认证的报文给设备端，开始启动一次认证过程。

2）设备端收到请求认证的数据帧后，将发出一个请求帧（EAP-Request/Identity 报文）要求用户的客户端程序将输入的用户名发送过来。

3）客户端程序响应设备端发出的请求，将用户名信息通过数据帧（EAP-Response/Identity 报文）发送给设备端。设备端将客户端发送的数据帧经过封包处理后（RADIUS Access-Request 报文）送给认证服务器进行处理。

4）认证服务器收到设备端发送来的用户名信息后，将该信息与数据库中的用户名表对比，找到该用户名对应的密码信息，用随机生成的一个加密字对它进行加密处理，同时也将此加密字通过 RADIUS Access-Challenge 报文发送给设备端，由设备端转发客户端程序。

5）客户端程序收到由设备端传来的加密字（EAP-Request/MD5 Challenge 报文）后，用该加密字对密码部分进行加密处理（此种加密算法通常是不可逆的，生成 EAP-Response/MD5 Challenge 报文），并通过设备端传给认证服务器。

6）认证服务器将收到的已加密的密码信息（RADIUS Access-Request 报文）和本地经过加密运算后的密码信息进行对比，如果相同，则认为该用户为合法用户，反馈认证通过的消息（RADIUS Access-Accept 报文和 EAP-Success 报文），设备收到认证通过的消息后触发打开端口的动作，允许用户的业务流通过端口访问网络。

7）认证通过后，设备端会定期监测用户的在线情况，方法是设备端向客户端发送握手报文。默认情况下，两次握手请求报文都得不到客户端应答，设备端就会让用户下线，防止用户因为异常原因下线而设备无法感知。

8）客户端也可以发送 EAPOL-Logoff 报文给设备端，主动终止已认证状态，设备端把端口状态从授权状态改变成未授权状态。

2. EAP 终结方式

这种方式将 EAP 报文在设备端终结并映射到 RADIUS 报文中，利用标准 RADIUS 协议完成认证、授权和计费。基本业务流程如图 7-5 所示。

EAP 终结方式与 EAP 中继方式的认证流程相比，用来对用户密码信息进行加密处理的随机加密字由设备端生成，之后设备端会把用户名、随机加密字和客户端加密后的密码信息一起送给认证服务器，进行相关的认证处理。其中，802.1x 认证过程中会启动多个定时器以控制接入用户、设备以及 RADIUS 服务器之间进行合理、有序的交互。

3. 802.1x 在设备中的实现

一般网络交换机设备在 802.1x 的 EAP 中继方式和 EAP 终结方式的实现中，不仅支持协议所规定的端口接入认证方式，还对其进行了扩展、优化，可以支持一个物理端口下挂接多个用户的应用场合；接入控制方式（即对用户的认证方式）可以采用基于 MAC 地址（Mac Based）和基于端口（Port Based）两种方式。当采用 Mac Based 方式时，该端口下的所有接入用户均需要单独认证，当某个用户下线时，也只有该用户无法使用网络。当采用 Port Based 方式时，只要该端口下的第一个用户认证成功后，其他接入用户无须认证就可使用网络资源，但是当第一个用户下线后，其他用户也会被拒绝使用网络。这样可极大地提高系统的安全性和可管理性。

7.4.4 802.1x 认证技术在组网中的应用

按照不同的组网方式，802.1x 认证可以采用集中式组网（汇聚层设备集中认证）、分布

式组网（接入层设备分布认证）和本地认证组网。不同的组网方式下，802.1x 认证系统实现的网络位置有所不同。

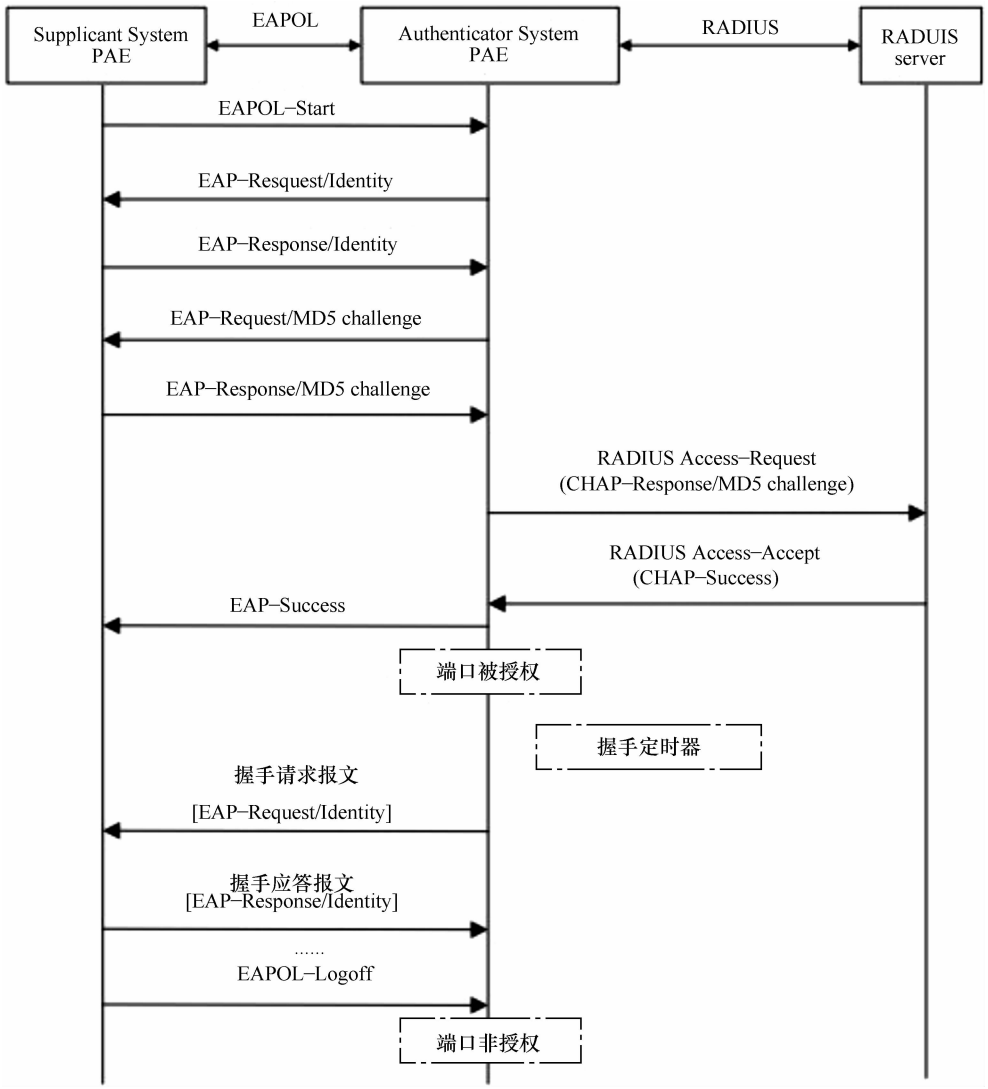


图 7-5　802.1x 认证系统的 EAP 终结方式业务流程

1. 802.1x 集中式组网（汇聚层设备集中认证）

802.1x 集中式组网方式是将 802.1x 认证系统端放到网络位置较高的 LAN Switch 设备上，这些 LAN Switch 为汇聚层设备。其下挂的网络位置较低的 LAN Switch 只将认证报文传给作为 802.lx 认证系统端的网络位置较高的 LAN Switch 设备，集中在该设备上进行 802.1x 认证处理。这种组网方式的优点在于 802.1x 采用集中管理方式，降低了管理和维护成本。汇聚层设备集中认证如图 7-6 所示。

2. 802.1x 分布式组网（接入层设备分布认证）

802.1x 分布式组网是把 802.1x 认证系统端放在网络位置较低的多个 LAN Switch 设备

上，这些 LAN Switch 作为接入层边缘设备。认证报文送给边缘设备，进行 802.1x 认证处理。这种组网方式的优点在于，它采用中/高端设备与低端设备认证相结合的方式，可满足复杂网络环境的认证要求。认证任务分配到众多的设备上，减轻了中心设备的负载。接入层设备分布认证如图 7-7 所示。

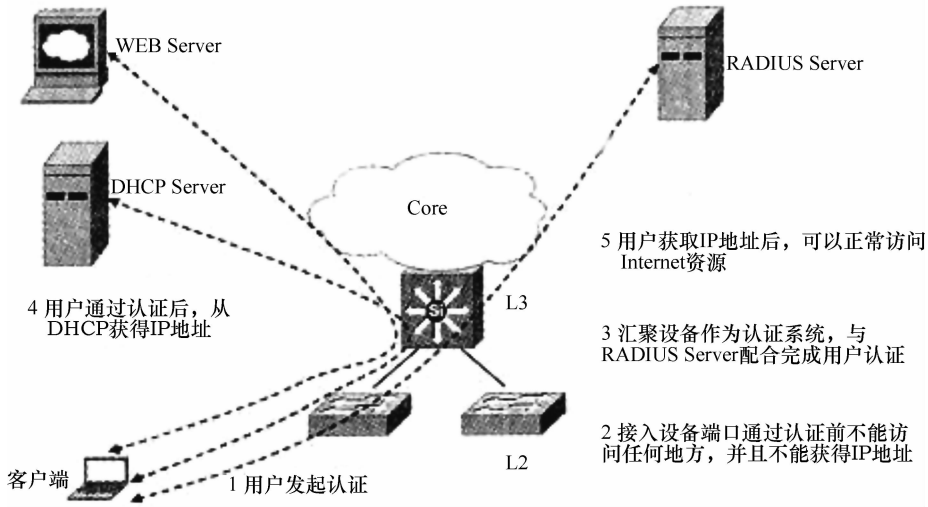


图 7-6　802.1x 集中式组网（汇聚层设备集中认证）

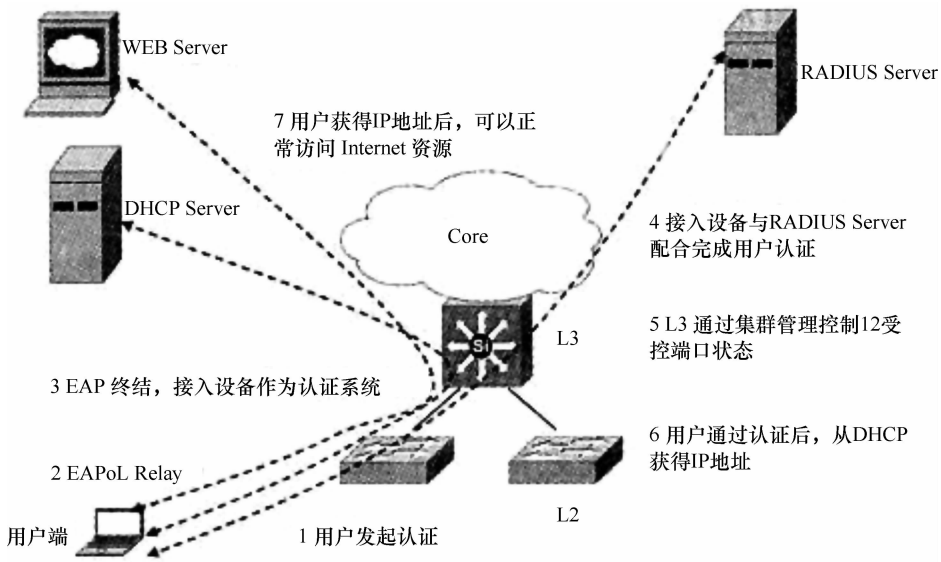


图 7-7　802.1x 分布式组网（接入层设备分布认证）

802.1x 分布式组网方式非常适用于受控组播等特性的应用，建议采用分布式组网对受控组播业务进行认证。如果采用集中式组网将受控组播认证设备端放在汇聚设备上，从组播服务器下行的流在到达汇聚设备之后，由于认证系统还下挂接入层设备，将无法区分最终用户，若打开该受控端口，则汇聚层端口以下的所有用户都能够访问到受控组播消息源。反

之，如果采用分布式组网，则从组播服务器来的组播流到达接入层认证系统，可以实现组播成员的精确粒度控制。

3. 802.1x 本地认证组网

802.1x 的 AAA 认证可以在本地进行，而不用到远端认证服务器上去认证。这种本地认证的组网方式在专线用户或小规模应用环境中非常适用。它的优点在于节约成本，不需要单独购置昂贵的服务器，但随着用户数目的增加，还需要由本地认证向 RADIUS 认证迁移。

7.4.5 802.1x 认证的特点

802.1x 认证系统提供了一种用户接入认证的手段，它仅关注端口的打开与关闭。对于合法用户（根据账号和密码）接入时，该端口打开，而对于非法用户接入或没有用户接入时，则使端口处于关闭状态。认证的结果在于端口状态的改变，而不涉及其他认证技术所考虑的 IP 地址协商和分配问题，是各种认证技术中最为简化的实现方案。

必须注意到 802.1x 认证技术的操作颗粒度为端口，合法用户接入端口之后，端口始终处于打开状态，此时其他用户（合法或非法）通过该端口接入时，不需认证即可访问网络资源。对于无线局域网接入而言，认证之后建立起来的信道（端口）被独占，不存在其他用户非法使用的问题。但如果 802.1x 认证技术应用于宽带 IP 城域网，就存在端口打开之后，其他用户（合法或非法）可自由地接入且难以控制的问题。因此，在提出可运营、可管理要求的宽带 IP 城域网中如何使用该认证技术，还需要谨慎分析所适用的场合，并考虑与其他信息绑定组合认证的可能性。

7.4.6 认证技术应用实例

对于高校园区网络，安全性问题不仅来自外部网络，更主要的威胁还是来自内部网络，很多来自学生出于好奇心或其他心理而采取的网络地址盗用、网络攻击等方式无疑是网络系统中的一个隐患，如何有效地设计安全接入和灵活计费方案是一个很重要的问题。

在校园三层网络架构的基础上，802.1x 与 RADIUS 主要用于校园网用户安全认证与计费系统上。目前一些主流的网络安全产品和计费系统都开发了支持 802.1x 的认证系统，近年来各网络设备厂商生产的主流交换机在物理硬件上都支持 802.1x 协议。

通过对接入层设备后台计费服务器的 RADIUS 认证进行配置，可以简单实现校园网上的 802.1x 认证功能，以下通过锐捷网络的一个认证计费应用实例具体说明如何通过 802.1x 配置及后台 RADIUS 配置来实现安全接入和计费，如图 7-8 所示。采用锐捷安全接入和灵活计费（802.1x）方案具有以下优点：

1）一次同时认证用户名、IP、MAC。

在 802.1x 认证时，客户端同时提交用户名、IP、MAC，一次认证即同时完成用户名、IP、MAC 三者的认证。这样，其他用户盗取用户账号或 IP 或 MAC 或三者中任意两者都无法假冒真正用户。更重要的是，这些都只需简单地在 RADIUS 服务器上设置单一的表格即可实现基于全宿舍网甚至全校的接入控制认证。

2）分布式认证方式，防止出现单一故障点。

各接入交换机（如 S2024 堆叠系列交换机、S1924G +/F + 接入交换机等）直接完成接入认证，不容易出现单点故障；同时，还可提高认证效率。

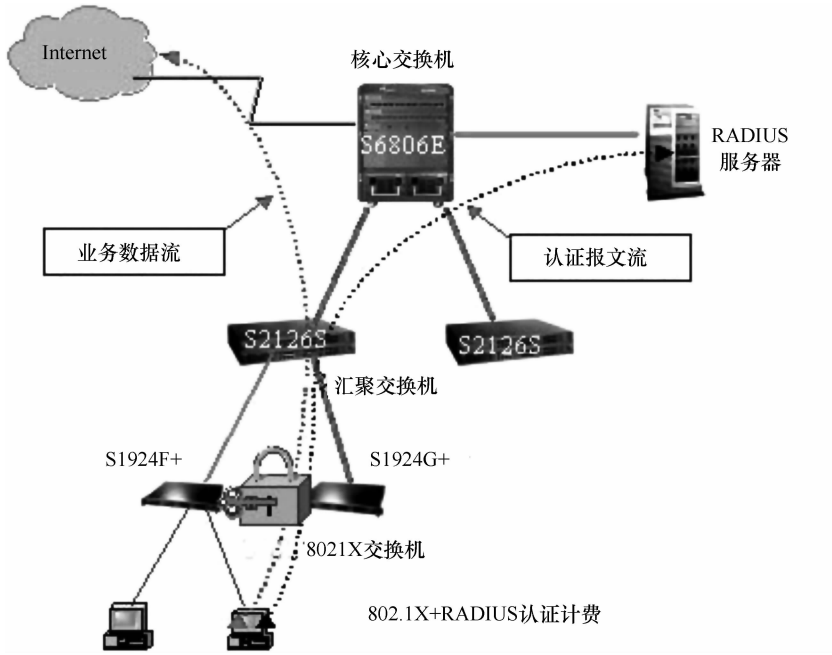


图 7-8 802.1x + RADIUS 认证计费

3）认证流和业务流实现分离，实现高效的认证，防止出现用户无法认证的情况。

802.1x 认证协议的核心设计思想是交换和控制的分离，认证流和业务流的分离。通过端口（可以是交换机的物理端口，用户 PC 的 MAC 地址，也可以是 VLAN ID）的两个逻辑通道（非受控端口和受控端口）来实现对用户的控制。非受控端口始终关闭，只允许认证流上来；受控端口走业务流，始终打开，只有通过认证才能关闭，用户的业务才能上来。

当用户认证流上来后，通过非受控端口进入交换机，由交换机协议体系提取用户名和密码对用户身份进行认证；当用户通过认证后，受控端口关闭，用户的业务流可以上行。这一点类似于窄带交换网的 7 号信令系统，控制信令和语音数据的分离。基于交换与控制分离的设计思路，802.1x 认证协议实现起来简单、高效，认证的容量很大，可以保证用户能及时通过认证，在网络流量大，认证用户数多时不会对设备的性能产生影响，保证整个网络高效、稳定的运行。

4）灵活扩展计费功能。

通过 RADIUS 服务器，802.1x 完全支持计费功能。同时，支持对用户离线信息的检测，对于后续开展基于按时计费的增值服务有利。当用户因计算机死机或异常关闭造成非主动下线，如果没有一种定期检测用户是否在线的机制，则会造成按时计费信息的不准。802.1x 认证设置了对用户离线的检测机制，定期会由认证系统对在线用户进行一次握手，如果用户仍在线，则其客户端会响应认证系统的检测请求；如果用户不在线，则其客户端不会响应认证系统的检测请求，在三次握手不成功后，就会中止计费信息。同时，由于用户名/密码跟特定用户的 IP、MAC 捆绑，用户无需担心用户名/密码泄露引起不必要的麻烦。

7.5 网络管理平台案例介绍

国内外知名的网络设备厂商和一些软件开发商，相继开发了一些网络管理系统，如SiteView、HP OpenView、CiscoWorks 网络管理软件、锐捷 SAM 系统、H3C 一体化智能管理平台等。本节选择 H3C iMC 作为专业网络管理平台软件进行介绍，可以从中学习到如何利用专业的网络管理平台进行网络管理的一些经验。

H3C 有线无线一体化智能管理平台 iMC 介绍

H3C 提供包括网络管理、用户管理、业务管理等全面的管理解决方案：H3C 智能管理中心（H3C Intelligent Management Center，H3C iMC）。

H3C iMC 是 H3C IToIP 解决方案的统一管理中心，基于 SOA 架构，采用灵活的组件化结构，支持与 HP Openview、SNMPc 等通用网管平台的集成，支持集成各厂家设备管理系统，与 H3C 的数据通信设备产品一起为用户提供全网解决方案，帮助客户真正实现网络的按需构建。

H3C iMC 作为 IToIP 解决方案核心管理系统，为用户提供了灵活的组件化结构，包括智能管理平台、智能配置中心（iCC）、ACL 管理、MPLS VPN 管理、用户接入管理、EAD 解决方案、无线管理、EPON 管理等业务组件，用户可以根据自己的管理需要和网络情况灵活选择需要的组件，真正实现“按需建构”。H3C iMC 解决方案架构如图 7-9 所示。

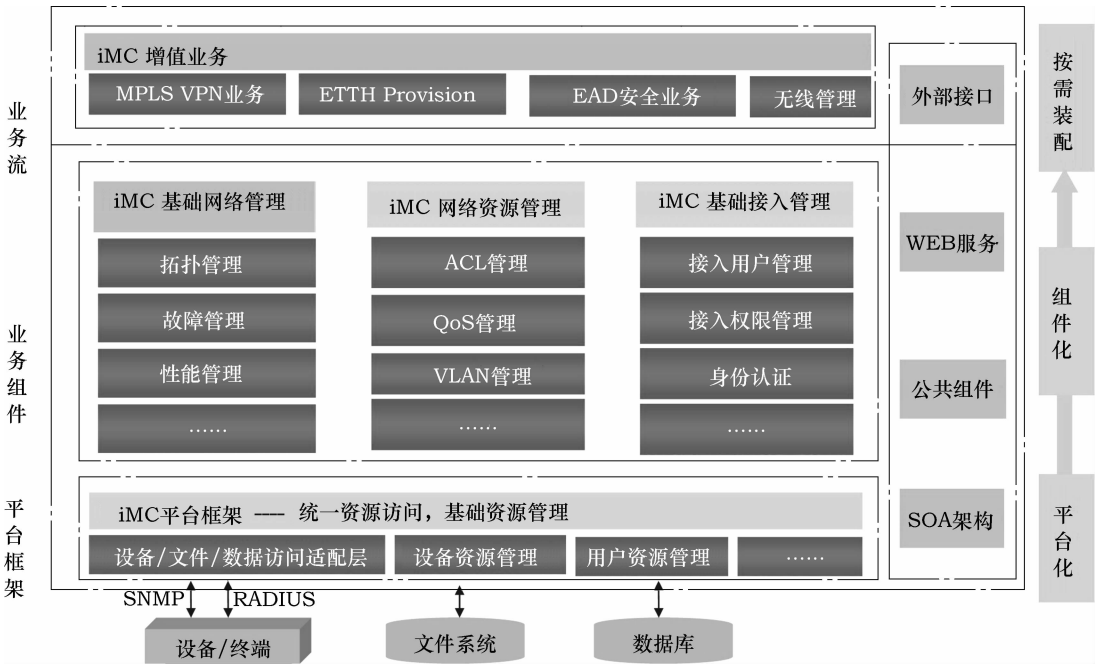


图 7-9 H3C iMC 解决方案架构

由图 7-9 可以看出 H3C iMC 管理系统由智能管理平台以及各个业务组件组成，管理平台提供网络管理的一些基础功能，比如故障管理、性能管理、资源和拓扑管理、用户管理等，

而业务组件提供了相应的业务管理功能；各个业务组件相对独立，并可以无缝的集成在管理平台中，使得整个系统具有很强的可扩展性。

H3C iMC 智能管理平台实现网络资源、用户和业务的融合管理，提供基本的网络资源管理、拓扑管理、故障管理、性能管理、用户管理及系统安全管理，基于 B/S 架构，可以与 H3C iMC 其他业务组件有效集成，形成多种解决方案。H3C iMC 智能管理平台不仅可以实现 H3C 全线数据通信产品的管理，也可通过标准 MIB 实现对 Cisco 等各主流厂商的数据通信设备的管理。

（1）系统安全管理

系统安全管理功能主要包括：操作日志管理、操作员管理、分组分级与权限管理、操作员登录管理等。

（2）资源管理

iMC 资源管理与拓扑管理作为整体共同为用户提供网络资源的管理。通过资源管理：网络自动发现可以通过设置种子的简易方式、路由方式、ARP 方式、IPSec VPN、网段方式五种自动发现方式自学习网络资源及网络拓扑，自动识别包括路由器、交换机、安全网关、存储设备、监控设备、无线设备、语音设备、打印机、UPS、服务器、PC 在内的多种类型的网络设备。支持网络设备手工管理、网络视图管理、设备的管理、分组权限管理、设备及业务管理系统的集成等。

（3）拓扑管理

拓扑管理直观地提供给用户对整个网络及网络设备资源的管理。拓扑管理包括：

1）拓扑自动发现：H3C iMC 可以自动发现网络拓扑结构，支持全网设备的统一拓扑视图，通过视图导航树提供视图间的快速导航。通过自动发现可以发现网络中的所有设备及网络结构（具体参见资源管理），并且可以发现非 SNMP 设备，只要设备可以 ping 通即可。这样就可以将所有网络设备都列入其管理范围（只要设备 IP 可达）。同时支持自动的拓扑图呈现和自定义拓扑。自动拓扑可以自动将网络中的逻辑连接关系显示出来，同时可以保存为自定义拓扑图并可根据具体情况进行修改以便于网管员对整个网络设备的监控。

支持对全网设备的连接定时轮询和状态刷新，实时了解整个网络的运行情况，并且刷新周期可定制（刷新周期：60～7200s），同时也支持对多个设备的刷新周期进行批量配置。

2）支持自定义拓扑：H3C iMC 的拓扑功能支持灵活的自定义功能，管理人员可以根据网络的实际组网情况和设备重要性的不同灵活定制网络拓扑，可对拓扑图进行增、删、改等编辑操作，使网络拓扑能够清晰地呈现整个校园网的网络结构以及 IT 资源分布。

3）自动识别各种网络设备和主机的类型：H3C iMC 可以自动识别 H3C、Cisco 等厂商的设备，Windows、Solaris 的 PC 和工作站，其他 SNMP 设备和 ping 设备，并且以树形方式组织，以不同的图标显示区分。在拓扑图上更可进一步对设备的类型进行区分，如区分路由器、交换机、安全网关、存储设备、监控设备、无线设备、语音设备、打印机、UPS、服务器、PC 等。

4）设备状态、连接状态、告警状态等信息在拓扑图上可以直观地显示出来。H3C iMC 的拓扑功能与故障管理和性能管理紧密融合，使拓扑图能够清晰地看到北建工 IT 资源的状态，包括运行是否正常、网络带宽、接口连通、配置变化都能一目了然。多种颜色区分不同级别的故障，根据节点图标颜色反映设备状态。

H3C iMC 网络拓扑显示图如图 7-10 所示。

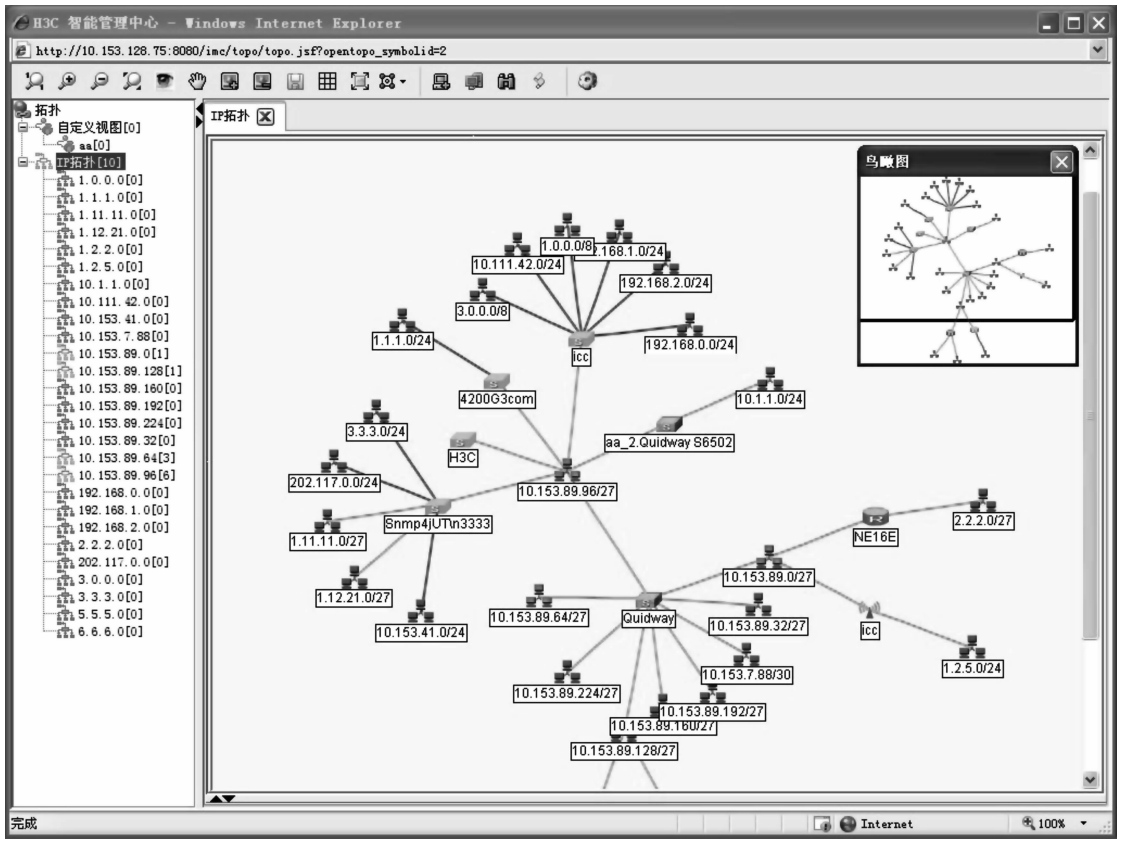


图 7-10　H3C iMC 网络拓扑显示图

5）拓扑能提供设备管理的便捷入口。H3C iMC 拓扑能够提供对设备管理的便捷入口，管理员只需通过右键点击拓扑图中的设备图标即可启动设备管理功能，实现对设备的面板管理等各项功能配置。

（4）故障（告警/事件）管理

故障管理，即告警/事件管理，是 H3C iMC 的核心模块，是 iMC 智能管理平台及其他业务组件统一的告警中心。iMC 告警中心可以接收各种告警源的告警事件，包括设备告警、本级网管站及下级网管站告警、网络性能监视告警、网络配置监视告警、网络流量异常监视告警、终端安全异常告警等；同时通过支持对设备的定时轮询，实现通断告警、响应时间告警等，以告警事件的方式上报给 H3C iMC 告警中心。

iMC 告警中心根据告警脚本中的告警事件定义，接收并解析上报的告警事件。H3C iMC 对接收到的告警事件进行深度关联分析，系统默认支持重复事件阈值告警、闪断事件阈值告警、未知事件阈值告警、未管理设备告警阈值告警，并能在故障恢复时自动确认相关告警。同时用户可以根据自己的需要确定事件的告警规则，以适应网络管理的需要。

H3C iMC 提供告警知识库。告警知识是用户在维护过程中的经验总结，将这些经验输

入系统，下次再出现同样的故障时，可以作为参考。用户选中一条告警记录，系统根据用户选中的告警记录，从告警知识库中查询出该条告警记录的维护经验，供用户进行告警处理时参考。用户将自己的日常处理经验以及业务信息及时写入数据库，更新告警知识库对以后的故障诊断与排除非常有益。

（5）性能管理

H3C iMC 网管系统提供丰富的性能管理功能，同时以直观的方式显示给用户。例如：可以提供折线图、方图、饼图等多种显示方式并能生成相应的报表。通过性能任务的配置，可自动获得网络的各种当前性能数据，并支持设置性能的阈值，当性能超过阈值时，网络以告警的方式通知告警中心：

1）支持 At a Glance、TopN 功能，用户能够对 CPU 利用率、流量等关键指标一目了然。

2）提供各类常用性能指标的默认采集模板；支持实时性能监视，支持二级阈值告警设置，当链路或端口的流量超过阈值，系统将会发送性能告警，使网络管理人员能够及时发现网络中的隐患，及时消除隐患。同时为故障定位提供手段。

3）提供基于历史数据的分析，为用户扩容网络、及早发现网络隐患提供保障。

4）支持饼图、折线图、曲线图等多种图形方式，直观地反映性能指标的变化趋势；提供灵活地组合条件统计和查询；性能报表支持导出 Html、Txt、Excel、Pdf 格式文件。

（6）设备管理组件

H3C iMC 支持对 H3C 全系列 IP 产品进行设备管理，提供丰富的管理功能。通过面板管理，网络管理人员可以直观地看到设备、板卡、端口的工作状态，通过设备信息浏览监视，管理人员可以了解设备的运行情况，实时监视 CPU 利用率、端口利用率等重要信息。同时，H3C iMC 提供图形化的配置方式，使设备功能配置不再复杂。H3C iMC 向用户提供了完善的网元管理功能，通过逼真的面板图片，直观地反映了设备运行情况。

1）通过面板图标直观地反映设备的框、架、槽、卡、风扇、CPU、端口等关键部件的运行状态。

2）能够查看、设置设备端口状态。

3）能够查看路由、VLAN 等配置信息。

4）能够查看端口流量、丢包率、错包率等关键统计数据。

5）支持对 H3C 交换机堆叠能力的管理。

6）通过 Ping、Traceroute 等功能测试当前网络链路的健康状况。

7）支持从设备列表、设备详细信息、拓扑等多个入口打开设备面板。

H3C iMC 网络设备管理面板如图 7-11 所示。

（7）无线管理组件

H3C iMC 无线业务管理组件（以下简称为 WSM 组件）依托 iMC 智能管理平台，实现有线无线一体化的管理。用户可以获得全面的无线业务管理能力，实现 AC、Fat AP、Fit AP、移动终端等无线设备的集中管理，轻松实现设备配置管理功能，并提供无线拓扑、AP 设备物理位置拓扑等多种拓扑功能，对全网无线设备进行直观有效地组织，对网络部署和设备状态一目了然，策略模板等功能实现网络和设备的批量配置，提升了效率，降低了维护成本。基于 Web 的管理系统，为无线业务管理者提供了简便、友好的管理平台。

图 7-11　H3C iMC 网络设备管理面板

7.6　计费管理

7.6.1　校园网计费管理的功能

校园网计费是一个基本的需求，其计费方案是随着管理理念的不断深入而逐渐完善。早期的校园网计费采用计费网关的形式，这对小型网比较合适。但是计费网关最大的问题是处理性能会成为网络应用的瓶颈。同时随着技术的进步，交换机的处理能力越来越强，出现了分布式的网络计费。其中又以基于 802.1x 认证技术的计费方案最为流行。本文将提供完整的校园网计费方案。

丰富的认证、计费、控制策略提高了网络管理效率，实现以网养网。

1. 准确的用户身份确认

校园网计费用户分为两类，一类是不计费，另一类是计费。但是无论是计费还是不计费，我们都需要对其身份进行准确的识别。这是网络安全的需要，同时也是做到准确计费的需要。但是如何进行用户身份确认呢？这就需要通过认证技术来实现。目前认证技术有许多，如 WEB 认证、802.1x 认证、PPPOE 认证。这些认证技术各有千秋，PPPOE 技术被广泛地应用在宽带小区，WEB 认证被应用在一些信息系统内，而 802.1x 认证被应用在广大的校园内。这是因为 802.1x 认证最大的特点是简单，无需特殊的设备支持，同时支持任何网络

应用。

2. 灵活的计费策略

计费策略主要有三种：按时长、按流量和按带宽。从实际情况看，时长计费最普遍，流量计费最科学，带宽计费最简单。同时由于一个校园网的用户有许多类，因此可能这三种计费策略都会被采用。但是，新建和改建的校园网往往采用可操作性强、简单的按时长计费的方式，并且配合预付费的方式进行收费，杜绝了恶意欠费的发生。

3. 精确的费用统计

网络使用一旦收费，那么就需要我们能够精确地计费，这是一个可运营的网络必备的条件。其中最需要关注的是是非否会因 PC 死机等异常情况造成计费不准确。因此我们需要一套保护机制来做到无论采用哪种计费策略，发生什么异常都能保证计费准确。

4. 人性化的网络计费

无论采用什么技术和方法都需要一套计费系统来完成计费。那么什么是好的计费系统呢？除了做到以上三点之外还需提供人性化的解决方案，能够通过优化来降低管理者的工作强度，提供自动化方案，同时对于用户来说又能使其感觉使用方便，收费合理。

7.6.2 校园网计费系统案例介绍

本节我们介绍一款由杭州深澜软件开发的计费认证系统（Srun 3000），该系统在高校等行业得到了广泛的应用，其网络用户部署图如图 7-12 所示。Srun 3000 安全认证网络管理计费系统是一套以实现网络运营为基础，以增强全局安全为中心，以提高管理效率为目的的第三代网络安全运营管理系统。Srun 3000 是一套基于标准的 RADIUS 协议开发的宽带认证计费管理系统。它不仅支持 PPPOE 和网关的认证计费方式，还支持所有的 802.1X 接入控制技术，支持与其他厂商相应标准的产品兼容，支持华为、Juniper、中兴等厂商的 BRAS 设备，也支持 D - Link、思科、H3C、华为、3Com、LINKSYS、中兴、锐捷网络、惠普、神州数码、北电网络、Juniper 等厂商的交换机，并能够提供更加丰富的功能。Srun 3000 在硬件设备有限投入的情况下提供最安全、最稳定的部署解决方案，同时以其基于身份管理为核心的多种计费组合模式为用户提供无限可能的运营管理方案；另外，以好用、易用为原则，通过 B/S 架构访问形式的友好界面，为用户提供贴心的使用形式。

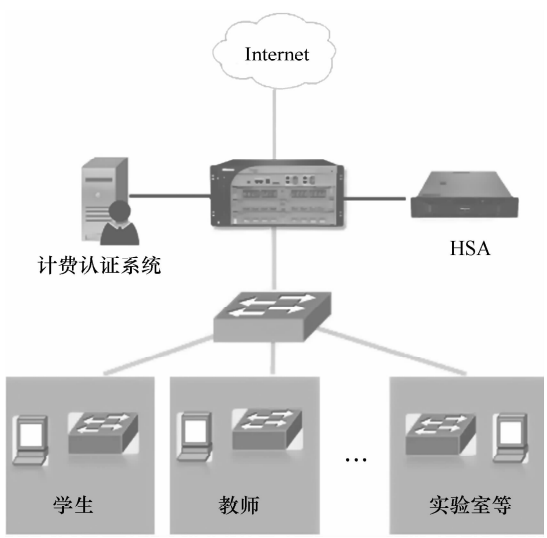


图 7-12 某高校网络用户部署图

作为校园网用户，由于万兆网络、双千兆接入、IPv6 等新技术的应用，并具有用户量大、业务众多、数据流量巨大等特点，往往要求认证计费系统必须具有非常高的性能。Srun 3000 在设计中充分考虑到性能上的要求，使用内存优化技术，采用复杂的多线程、分布式等设计技术；采用优化的数据库结构、算法设计，提高了系统的运算速度，可以达到 1220 次/s 的 RA-

DIUS 认证性能，用户上网认证时间不超过 0.5s。

7.7 校园网安全管理技术

7.7.1 校园网常见的安全风险

校园网是一个开放的网络环境，随着网络的普及，还有庞大、活跃的学生用户群；校园网应用系统较多，部署了大量的服务器，还有大量的个人计算机接入网络；校园网也接入了 CERNET 等因特网。高校校园网安全问题很突出，安全管理问题也非常复杂。

1）校园网规模大，高带宽接入因特网。高校校园网是最早的宽带网络，各学校除接入 CERNET 外，还具有少则几十兆甚至几个 G 的公网出口。目前在校园网中普遍使用了百兆到桌面、千兆甚至万兆实现园区主干互联。校园网的用户群体一般也比较大，少则数千人，多则数万人，一般都建有学生宿舍网，用户群比较密集。正是由于高带宽和大用户量的特点，网络安全问题一般蔓延快、对网络的影响比较严重。

2）活跃的用户群体。大学生通常是最活跃的网络用户，对网络新技术充满好奇，勇于尝试。如果没有意识到后果的严重性，有些学生会尝试使用网上学到的、甚至自己研究的各种攻击技术，可能对网络造成一定的影响和破坏。

3）开放的网络环境。由于教学和科研的特点决定了校园网络环境应该是开放的，管理也是较为宽松的。比如，企业网可以限制允许 Web 浏览和电子邮件的流量，甚至限制外部发起的连接不允许进入防火墙，但是这在校园网环境下通常是行不通的，至少在校园网的主干不能实施过多的限制，否则一些新的应用、新的技术很难在校园网内部实施。

4）有限的投入。校园网的建设和管理通常都轻视了网络安全，特别是管理和维护人员方面的投入明显不足。在中国大多数的校园网中，通常只有网络中心的少数工作人员，他们只能维护网络的正常运行，无暇顾及、也没有条件管理和维护数万台计算机的安全，院、系一级并没有专职的计算机系统管理员。

5）盗版资源泛滥。由于缺乏版权意识，盗版软件、影视资源在校园网中普遍使用，这些软件的传播一方面占用了大量的网络带宽，另一方面也给网络安全带来了一定的隐患。比如，Microsoft 公司对盗版的 XP 操作系统的更新做了限制，安装盗版操作系统的计算机系统今后会留下大量的安全漏洞。另一方面，从网络上随意下载的软件中可能隐藏着木马、后门等恶意代码，许多系统因此被攻击者侵入和利用。

以上各种原因导致校园网既是大量攻击的发源地，也是攻击者最容易攻破的目标。因此，当前校园网常见的风险如下：

1）普遍存在的计算机系统的漏洞，对信息安全、系统的使用、网络的运行构成严重的威胁。

2）计算机蠕虫等病毒泛滥，影响用户的使用、信息安全、网络运行。

3）外来的系统入侵、攻击等恶意破坏行为，有些计算机已经被攻破，用作黑客攻击的工具；拒绝服务攻击目前越来越普遍，不少攻击开始针对重点高校的网站和服务器。

4）内部用户的攻击行为，这些行为给校园网造成了不良的影响，损害了学校的声誉。

5）校园网内部用户对网络资源的滥用，有的校园网用户利用免费的校园网资源提供商

业的或者免费的视频、软件资源下载，占用了大量的网络带宽，影响了校园网的应用。

6）垃圾邮件、不良信息的传播，有的利用校园网内无人管理的服务器作为中转，严重影响了学校的声誉。

7.7.2 校园网安全防范对策

俗话说，网络安全三分技术、七分管理，安全管理贯穿于整个安全防范体系的始终。实践一再告诉我们仅有安全防范技术，而无严格的安全管理体系相配套，是难以保障网络系统的安全的。必须制订一系列安全管理制度，对安全技术和安全设施进行管理。对网络管理人员进行及时的网络安全理论培训、安全技术培训、安全产品培训以及本部业务培训，实现整个网络的安全体系。所以，加强校园网的安全管理工作需要从管理和技术两个方面综合考虑。

1. 加强校园网安全管理政策建设

安全政策（Security Policy）描述校园网安全的目标和需求，是一个组织安全管理的需求说明，它是执行各项管理制度、技术措施的依据，一般规定“做什么”而不是“怎么做”，告诉用户哪些行为是允许的、哪些行为是不允许的，违反了这些约定将会受到怎样的处罚。目前很多学校以安全管理规定、安全条例、安全管理办法等形式发布。一个可行的安全政策应该根据我国的相关法律、法规以及学校的管理制度和具体情况制定，不存在通用的、可实施的安全政策。安全政策应该让所有的校园网用户知道，对校园网用户，无论是院系单位还是学生个人，都可以以签署入网协议的形式让用户知道学校的安全管理政策，一方面起到提高安全意识的作用，同时明确责任和义务，便于对安全事故的处理。

加强网络安全组织建设。目前普遍认为校园网安全管理工作应该由信息网络中心承担，但是事实上，安全管理工作非常复杂，可能涉及各院系、部、处的人员和业务，因此必须由学校具有决策权的机构和领导组织协调各部门的管理工作。学校可以成立信息安全领导小组、信息安全应急处理小组，并由相应的技术人员成立技术小组，安全管理各项措施的实施，单纯依靠网络中心的力量也是不充分的。

由于校园网安全与人的安全意识和技能紧密相关，因此，对校园网不同类型用户进行安全教育，将有利于校园网的安全应用。首先，必须培养一支具有安全管理意识的网络队伍。同时，加强用户安全意识和管理员安全技术的培训工作也非常重要。对于新用户的安全意识的培训，新生入学教育和新员工上岗培训是两个比较好的形式，也可以开展一些职工的在职培训、学生的文化课、选修课等形式的安全意识培训和基本技能的培训。对于系统管理员，一定要重视上岗培训。很多学校院系服务器的管理员都是由助教研究生来担任的，这些学生没有经过必要的培训，容易留下大量的安全问题。对于这些岗位的安全培训是当前校园网安全管理非常重要的环节。

2. 从网络安全管理与技术上防范风险

（1）部署防火墙

防火墙是网络安全的屏障。一个防火墙（作为阻塞点、控制点）能极大地提高一个内部网络的安全性，并通过过滤不安全的服务而降低风险。由于只有经过精心选择的应用协议才能通过防火墙，所以网络环境变得更安全。在防火墙设置上我们按照以下原则来提高网络安全性：

1）根据校园网安全策略和安全目标，规划设置正确的安全过滤规则，规则审核 IP 数据包的内容包括：协议、端口、源地址、目的地址、流向等项目，严格禁止来自公网对校园内部网不必要的、非法的访问。总体上遵从“不被允许的服务就是被禁止”的原则。

2）将防火墙配置成过滤掉以内部网络地址进入路由器的 IP 包，这样可以防范源地址假冒和源路由类型的攻击；过滤掉以非法 IP 地址离开内部网络的 IP 包，防止内部网络发起的对外攻击。

3）在防火墙上建立内网计算机的 IP 地址和 MAC 地址的对应表，防止 IP 地址被盗用。

4）在局域网的入口架设千兆防火墙，并实现 VPN 的功能，在校园网络入口处建立第一层的安全屏障，VPN 保证了管理员在家里或出差时能够安全接入数据中心。

5）定期查看防火墙访问日志，及时发现攻击行为和不良上网记录。

6）允许通过配置网卡对防火墙进行设置，提高防火墙管理的安全性。

（2）架设入侵检测系统和入侵防御系统

架设一个入侵监测系统（IDS）是非常必要的，它处于防火墙之后对网络活动进行实时检测。许多情况下，由于可以记录和禁止网络活动，所以入侵监测系统是防火墙的延续。它们可以和防火墙和路由器配合工作。

IDS 扫描当前网络的活动，监视和记录网络的流量，根据定义好的规则来过滤从主机网卡到网线上的流量，提供实时报警。IDS 是被动的，它监测网络上所有的数据包。其目的就是捕捉危险或有恶意动作的信息包。IDS 是按指定的规则运行的，记录是庞大的，所以我们必须制定合适的规则对它进行正确的配置，如果 IDS 没有正确的配置，其效果如同没有一样。IDS 能够帮助系统对付网络攻击，扩展了系统管理员的安全管理能力（包括安全审计、监视、攻击识别和响应），提高了信息安全基础结构的完整性。

在架设 IDS 的基础上，应该进一步部署入侵防御系统（IPS）。IPS 对那些被明确判断为攻击的行为（会对网络、数据造成危害的恶意行为）进行检测和防御，降低或是减免使用者对异常状况的处理资源开销，是一种侧重于风险控制的安全产品。

（3）加强内网信息系统安全评估

采用先进的漏洞扫描系统定期对工作站、服务器、交换机等进行安全检查，并根据检查结果向系统管理员提供详细可靠的安全性分析报告，为提高网络安全整体水平提供重要依据。

高校校园网是一个由多协议、多系统、多应用、多用户组成的复杂性网络环境，校园网中的网络设备、操作系统、数据库、应用软件都存在难以避免的安全漏洞，为了要保障高校校园网的安全，必须做好校园网漏洞管理。

高校校园网服务器存储大量信息，例如教学系统服务器、科研服务器、人事、学生管理服务器等，对服务器的安全需要进行全面的管理，如：访问要进行安全身份认证，非认证用户无法进行访问；服务器需要提供资源受控制，防止非授权人员复制、修改、发送；服务器支持远程安全管理，校园网管理员能够从远程进行安全登录，为其传输的信息加密；服务器的操作行为有严格审计，能够防止黑客有意删除；服务器的安全状态能够实时显示，各种安全组件的工作状态能够被监测；服务器在受到损害时，能做到数据恢复可用等。

（4）部署网络版防病毒软件

最理想的状况是在整个局域网内杜绝病毒的感染、传播和发作，为了实现这一点，应该

在整个网络内可能感染和传播病毒的地方采取相应的防病毒手段。同时为了有效、快捷地实施和管理整个网络的防病毒体系，应能实现远程安装、智能升级、远程报警、集中管理、分布查杀等多种功能。

统一部署各类公共网络安全的服务：统一的校内杀毒平台，在出口处设立防毒网关；学校重要业务部门的服务器集中管理，关键数据统一容灾备份；对于关键数据实行有控制的访问，防止内、外部数据窃取、数据篡改、非授权访问；统一部署学校内部的网络化的补丁分发服务器（WSUS），满足校内用户经常性打补丁和系统升级的需要；满足信息安全的需求，在核心设备与外网端口部署信息审计设备，实现与相关管理机构的联动报警功能。

采取这种升级方式，一方面确保校园网内的杀毒软件的更新保持同步，使整个校园网都具有最强的防病毒能力；另一方面，由于整个网络的升级、更新都是由程序来自动、智能完成，因此就可以避免由于人为因素造成网络中因为没有及时升级为最新的病毒定义码和扫描引擎而失去最强的防病毒能力。

（5）加强安全监控管理

对校园网络进行安全监控，就如同在教学大楼内安装的闭路电视监控系统，也能增加高校校园网的安全指数。监控管理能对校园网关键区域的信息流动进行动态监测，能够把网络上流过的所有数据包，通过实时检测和分析，及时发现非法或异常行为；还能对校园网紧急事件（网页篡改、试题盗窃）以最快的速度阻止；能够按要求存储校园网访问日志记录，提供关键词查找和离线分析功能；甚至能对校园网特殊安全事件进行回放。

7.8　网络管理员的职责和任务

在网络建成之后投入正常使用之前，必须配备专业的网络管理工作者，才能保证网络的正常使用。计算机网络的运行周期一般是一年 365 天，每天 24 小时不间断地运行和服务，对于很多企业和单位来说，在行政机构中都会设置专门的网络技术部门或者网络管理部门，并且配备专业的技术人员。通常管理和维护网络的这些专业技术人员被称为网络管理员。网络管理员的基本工作是负责网络的运营、管理、维护、故障诊断与排除，维护网络正常平稳地运行。在《中华人民共和国计算机信息网络国际联网管理暂行规定》中规定了网络管理员的管理原则、管理手段、管理职责及应遵守的相关法律法规。在国家职业技能标准中，对网络管理员的要求见表 7-1。

表 7-1　对网络管理员的要求

职业功能	工作内容	技能要求	相关知识
一、维护机房环境	1. 电源设备的操作与管理	1）能够按照操作规程中正确开关机房的小型电源设备 2）能够及时发现电源系统故障	1）电源设备操作规程 2）电源系统常见故障及种类
	2. 空调设备的操作与管理	1）能够按照操作规程正确开关机房内的空调设备 2）能够根据机房要求调整空调设备 3）能够及时发现空调设备故障	1）空调设备操作规程 2）空调设备常见故障的种类

（续）

职业功能	工作内容	技能要求	相关知识
二、维护通信线路	1. 维护对外互连通信线路	1）能够识别对外互连通信线路 2）能够及时发现对外互连通信线路故障	1）常用广域网线缆基本知识 2）常用广域网端口基本知识 3）常用广域网通信线路常见故障知识
	2. 维护局域网的通信线路	1）能够识别局域网通信线路 2）能够及时发现局域网通信线路故障	1）常用局域网线缆基本知识 2）常用局域网端口基本知识 3）常用局域网通信线路常见故障知识
三、维护网络设备	1. 监视网络运行状况	1）能够使用网络实用工具程序和网络管理工具监视网络的运行状况 2）能够判断网络设备是否使用正常	1）网络实用程序知识 2）网络管理工具的使用方法
	2. 网络设备的维护	1）能够识别网络设备 2）能够完成网络设备的日常保养	网络设备常用日常保养知识
四、维护网络服务器和网络终端设备	1. 网络终端设备的安装与配置	1）能够正确安装网络终端设备的软、硬件 2）能够正确配置网络终端设备的软、硬件 3）能够正确使用基本的网络客户软件 4）能够正确配置简单的网络资源共享	1）网络终端设备的软硬件安装配置方法 2）网络客户端软件的安装配置方法
	2. 网络服务器的监视	能够识别服务器硬件故障	服务器保养基本方法
	3. 网络终端设备的日常维护	1）能够使用常用的防病毒软件进行病毒的防治 2）能够进行网络终端设备的日常保养	1）计算机病毒的正确识别和处理方法 2）网络终端设备保养方法
	4. 监视网络基本服务	1）能够正确使用网络工具、网络管理软件和网络应用软件，对网络基本服务进行监视 2）能够判断网络基本服务是否工作正常	利用网络应用软件对网络基本服务进行监视的方法

通常网络管理员的工作包括以下内容。

1. 网络基础设施、硬件设备等的配置、管理与维护

1）确保对外接入网络通信链路、局域网通信链路的通信传输畅通。

2）掌握局域网主干设备的配置情况及配置参数变更情况，备份各个设备的配置文件。

3）对运行关键业务网络的主干设备配备相应的备份设备，并配置为热后备设备。

4）负责网络布线配线架的管理，确保配线的合理有序。

5）掌握用户端设备接入网络的情况，以便发现问题时可迅速定位。

6）采取技术措施，对网络内经常出现的用户需要变更位置和部门的情况进行管理。

7）掌握与外部网络的连接配置，监督网络通信状况，发现问题后与有关机构及时联系。

8）实时监控整个局域网的运转和网络通信流量情况。

9）制定、发布网络基础设施使用管理办法并监督执行情况。

2. 网络操作系统管理

1）在网络操作系统配置完成并投入正常运行后，为了确保网络操作系统工作正常，网络管理员首先应该能够熟练地利用系统提供的各种管理工具软件，实时监督系统的运转情况，及时发现故障征兆并进行处理。

2）在网络运行过程中，网络管理员应随时掌握网络系统配置情况及配置参数变更情况，对配置参数进行备份。网络管理员还应该做到随着系统环境的变化、业务发展需要和用户需求，动态调整系统配置参数，优化系统性能。

3）网络管理员应为关键的网络操作系统服务器建立热备份系统，做好防灾准备。

3. 应用系统与业务系统的管理

1）确保各种网络应用服务运行的不间断性和工作性能的良好性，出现故障时应将故障造成的损失和影响控制在最小范围内。

2）对于要求不可中断的关键型网络应用系统，除了在软件手段上要掌握、备份系统参数和定期备份系统业务数据外，必要时在硬件手段上还要建立和配置系统的热备份。

3）对于用户访问频率高、系统负载大的网络应用服务，必要时网络管理员还应该采取分流的技术措施。

4. 用户服务与管理

1）用户的开户与撤销。

2）用户组的设置与管理。

3）用户可用服务与资源的权限管理和配额管理。

4）用户计费管理。

5）包括用户桌面联网计算机的技术支持服务和用户技术培训服务的用户端支持服务。

5. 安全保密管理

1）安全与保密是一个问题的两个方面，安全主要指防止外部对网络的攻击和入侵，保密主要指防止网络内部信息的泄露。

2）对于普通级别的网络，网络管理员的任务主要是配置管理好系统防火墙。为了能够及时发现和阻止网络黑客的攻击，可以加配入侵检测系统对关键服务提供安全保护。

3）对于安全保密级别要求高的网络，网络管理员除了应该采取上述措施外，还应该配备网络安全漏洞扫描系统，并对关键的网络服务器采取容灾的技术手段。

4）更严格的涉密计算机网络，还要求在物理上与外部公共计算机网络绝对隔离，对安置涉密网络计算机和网络主干设备的房间要采取安全措施，管理和控制人员的进出，对涉密网络用户的工作情况要进行全面的管理和监控。

6. 数据与信息存储备份管理

1）采取一切可能的技术手段和管理措施，保护网络中的信息安全。

2）对于实时工作级别要求不高的系统和数据，网络管理员也应该进行定期手工操作备份。

3）对于关键业务服务系统和实时性要求高的数据和信息，网络管理员应该建立存储备份系统，进行集中式的备份管理。

4）最后将备份数据随时保存在安全地点是非常重要的。

7. 机房管理

1）掌握机房数据通信电缆布线情况，在增减设备时确保布线合理，管理维护方便。

2）掌管机房设备供电线路安排，在增减设备时注意负载的合理配置。

3）管理网络机房的温度、湿度和通风状况，提供适合的工作环境。

4）确保网络机房内各种设备的正常运转。

5）确保网络机房符合防火安全要求，火警监测系统工作正常，灭火措施有效。

6）采取措施，在外部供电意外中断和恢复时，实现在无人值守的情况下保证网络设备安全运行。

7）保持机房整洁有序，按时记录网络机房运行日志，制定网络机房管理制度并监督执行。

本 章 小 结

大型园区网络在建设任务完成后，重点工作就转入日常化的网络运维管理。网络管理是保障网络正常运行的必修课。本章以大型园区网络管理技术为主题，讨论了大型园区管理技术。

1）简要介绍了网络管理的概念、目标和内容、基本功能。

2）详细介绍了 802.1x 认证技术，这是目前最先进的身份认证，对提高网络安全管理水平至关重要。

3）介绍了网络管理平台与案例，进一步阐述网络管理、安全管理等方面的技术和网络管理员的职责。

第 8 章　大型园区网络规划与设计案例

本章我们以某所大学的校园网作为大型园区网络的规划与设计案例进行分析，校园网的用户人数少则几千人，多则几万人，属于典型的大型园区网络。

校园网是为学校师生提供教学、科研和综合信息服务的宽带多媒体网络。它是在学校范围内，在一定的教育思想和理论指导下，为学校教学、科研和管理等教育提供资源共享、信息交流和协同工作的计算机网络，它不仅提供了全校师生访问 Internet 的功能，还是一个具有交互功能和专业性很强的局域网络。学校门户网站、网络教学平台、信息资源、网上图书馆等数字校园平台，都可以通过网络运行工作，校园网应为学校教学、科研提供先进的信息化环境。

8.1　校园网建设与发展历程

高校校园网一直是国内 Internet 发展的领头羊。中国教育和科研计算机网 CERNET 始建于 1994 年，是全国第一个 IPv4 主干网。也就是同一年，清华、北大等顶尖大学建成了自己的校园网，事实上这些网络也是中国 Internet 的开端。高校校园网从 1994 年的启动建立到现在的 19 年间，无论是高校校园网的网络技术，还是高校校园网的关注要点，大致可以分为 3 个阶段：

第一阶段是基础设施建设时期，时间大约从 1994 年到 2000 年。这期间各种网络技术在高校同时都有应用：以太网技术、FDDI、ATM 网络技术。在这个阶段，由于校园网应用的技术比较繁杂，而且业务相对单一，因此，这一阶段主要关注网络的连通性和兼容性，即如何保证校园网的连通，和各种不同网络技术的兼容和融合。

第二阶段是应用平台建设时期，时间大约是从 2000 年到 2005 年。这期间，随着网络技术的发展，各种应用也开始出现并发展迅速，包括 BBS、WWW、FTP、E-mail，以及近两年流行的 BT 下载、视音频业务等，这些应用都对带宽提出了挑战。与此同时，网络技术——特别是以太网技术迅猛发展，1000M 以太网已经步入校园，万兆标准也已经公布。结合实际应用和网络技术来看，这个阶段主要关注：带宽和应用。

第三阶段是信息资源建设时期，时间从 2005 年至今，乃至今后的相当长的一段时期。近几年，万兆以太网已经开始在高校校园网中规模化应用，下一代以太网标准也已经确立为 10 万兆标准。同时，随着中国下一代互联网工程 CERNET2 的启动，IPV6 技术也已经在校园网中实验并逐步应用。当基础设施、应用平台建设之后，信息资源的丰富与否决定了校园网络的真正价值。当信息资源充分丰富后，人们的工作、学习、生活、娱乐完全离不开网络，网络的安全与可信又成为头等重要的问题。纵观这几年的整个网络世界，安全事件频发，如冲击波、震荡波、ARP 攻击等。所以，安全可信成为了高校校园网当前关注的要点。

第一阶段更注重校园网是数字校园的基础平台，校园网升级改造成为了各个高校的热点，从核心设备到终端服务，更多的是强调精细化管理，强调校园网的可靠性和稳定性，更

好地满足数字校园建设的支撑平台的作用。

简单来说，对于校园网，丰富的应用是关键，而稳定可靠的网络是基础，完善的安全和管理手段是保障。

8.2 校园网建设总体方案分析

8.2.1 校园网的设计原则

校园网是一个复杂的系统，校园网建设无疑是一个复杂的系统工程。网络的规划、设计、硬件建设、软件建设以及网络的应用、管理等均以系统的眼光来看待，任何一项工作都从全局、长远的角度出发，体现整体最优性。校园网建设是一项资金和人力投入都较大的工程，一方面各个高校目前对于信息化基础建设投入资金紧张，而网络技术更新发展较快，校园网建设设备更新换代频率较高；广大师生员工对校园网的依赖程度越来越高，对性能要求越来越高，校园网的应用还不够丰富。校园网的建设要做好总体规划设计、分布实施，将校园网各个子系统有规划、有步骤地建设，既要着眼于未来技术的发展变化，具有技术先进性和实用性结合的发展策略，也要注重经济性原则。概括来说，新的校园网建设要尽量遵循以下原则：

1. 开放性

根据开放互连标准的规定，只有开放的、符合国际标准的网络系统才能够实现多厂家产品的互连。目前主流的网络技术标准主要是以太网技术，包括千兆、万兆甚至十万兆网络，选择符合国际标准的网络产品和系统，提供开放的网络接口和数据接口，使不同厂家的产品能够相互兼容，更有利于校园网的数据交换和信息共享。

2. 可扩展性

网络系统要灵活地升级和扩展，可扩展对网络而言有两方面的内容：第一是能够适应网络规模的扩充，第二是能够适应应用提升对系统性能的更高的要求，可以方便地对产品进行升级和更新换代。具有良好扩展性的网络系统能够让学校以较小的代价扩充现有网络设备的功能，这样，就有效地保护了学校的投资。

3. 可靠性

网络系统必须具有一定的容错能力，保障在意外情况下不中断用户的正常工作。可靠性也是通过设备可靠性和技术措施两个层次的方式来解决。首先，要求所选择的网络厂商产品的性能要稳定可靠；其次，要求网络厂商有充足的备件，在设备发生故障后能够得到及时更换；第三，通过技术措施来保证网络的可靠性。比如采取中心双交换机技术，采用部件冗余技术，采用链路通道技术等。通过这些措施使得网络即使出现某些故障仍然能够正常运行。

4. 可管理性

网络系统应该能够支持 SNMP（简单网管协议）和 RMON，应该建设统一的网管系统，能够对整个骨干网内多个厂家设备实现完善的网络拓扑管理、设备管理、性能管理和故障管理，可以实时监控所有设备和线路的运行状况，对全网设备的运行信息进行实时监控，并对故障和性能超限实现实时告警，对设备运行情况进行查询和统计，定期生成运行报告。根据网络运行环境变化提供合适的方式对网络参数进行配置修改，保证网络以最优性能正常运

行。要求能够实现分级管理。网络的可管理性对整个系统具有至关重要的意义。现在网络和应用变得愈来愈复杂，一个不可管理的网络是不可想象的。

5. 先进性和实用性

先进性和实用性是相辅相成的，网络技术和产品的先进性保证了系统的高性能，实用性保证了网络的高效率和真正发挥作用。现在各种新技术和设备层出不穷，不能一味追求新技术，要尽量选择成熟可靠又能具有一定前瞻性的技术方案和产品，充分考虑新技术与现有技术和设备的兼容性。

6. 安全性

网络系统必须具有较高的安全性，网络设备安全可靠运行，网络用户安全接入网络，实现认证、可信和安全，网络系统能够有效防御网络入侵行为和攻击行为，保障数据及信息安全。

8.2.2　校园网总体方案设计思路

相比大型企业网络来说，高校校园网有很多不同之处。高校校园网的设计必须要紧紧围绕学校建设校园网的目标来做好校园网的需求分析。校园网的建设是各个高校信息化建设的重要基础，如同每个大学有高楼大厦一样，那么校园网在每个大学也是必不可少的。校园网的设计要综合学校各方面的情况进行考虑，一般来说，大学校园网整体方案的设计要经过如下几个步骤：

1）全面了解建设背景。全面了解学校的情况，包括学校已有校区校园网现状、新建校区及单体建筑的设计规划、教职工、学生人数规模、教室、实验室等教学资源情况、办公环境、学生宿舍、家属区、后勤产业等各情况，综合这些方面的情况进行分析，确定学校当前规模及今后 3 ~5 年可增长的规模，了解学校建设校园网对教学、办公、科研和后勤等方面业务的需求。

2）做好校园网建设需求分析。学校信息中心技术人员要清楚学校建设校园网的主要目标，梳理学校的业务及需求。首先要对教学、科研、人事、后勤等主要单位的业务类型进行了解，通过设计调查问卷，了解各单位、各部门以及各院系对校园网的应用要求，对这些情况进行梳理，可以更加明确校园网的建设目标。比如学校财务办公网络用专用网络，要求与校园网隔离，并且不得提供因特网接口。设计人员还要会同信息中心人员对网络功能、性能需求、安全需求、管理需求等做进一步充分沟通，以做好详细的需求分析报告。

3）明确校园网建设的主要内容及目标。在了解建设背景和需求分析的基础上，要进一步明确校园网建设的主要内容及总体目标，即建设一个什么样的校园网、校园网整体性能如何、采用什么样的网络技术、建设方案先进性与实用性如何、投资预算规模多大、建设周期多长。对新建校区的园区网络要考虑网络综合布线系统、网络核心机房、数据中心机房、网络方案及系统集成、业务应用系统等各个系统的规划与建设。

4）进行校园网主干网络的设计。校园网主干网络的设计十分重要，它关系到整个校园网的架构及性能。充分参考国内外知名网络设备厂商提供的网络解决技术方案、国内外重点高校成功建设校园网的经验，根据应用需求、建设目标、单体建筑分布及信息点位总数等各个高校的实际情况和特点进行设计。主干网络结构设计的重点是网络拓扑结构的设计，对于较大规模的校园网应采用多核心的拓扑结构，对于小型网络多采用双核心网络拓扑。

5）进一步明确网络技术选型、因特网出口设计、网络拓扑结构设计、系统具体设计等。网络技术选型要考虑一定的先进性及前瞻性，同时又要兼顾实用性。目前千兆以太网技术非常成熟，万兆及十万兆以太网技术逐渐成为主流，在设计时应予以充分考虑。对综合布线系统的设计要考虑充足的光纤芯数、信息点位数，水平布线系统应主要考虑六类铜缆，以达到更高的传输性能。在网络设备选型上，要充分考虑核心设备、接入设备的主要性能参数，选择更稳定可靠的性价比较好的设备。

6）对各个子系统进一步做好详细设计。校园网包括多个子系统，每一块都需要更深入的详细设计，安排合理的投资预算和实施步骤。

8.2.3 校园网的基本功能与建设需求

1. 校园网应提供的应用功能

校园网具有不同于其他网络的特点，不同的是在校园网中服务的对象主要是师生员工，校园网提供了一种促进教学、科研与生活的网络环境。

（1）办公自动化

学校信息网络中心购买或开发基于 Web 的办公自动化系统（Office Automation，OA），基于 Web 的综合管理信息系统，提供行政、人事、学籍、教学、后勤、财务管理、公文收发管理、教师档案管理、学生档案管理、科技档案管理等，使学校日常办公无纸化，减少办公开支，提高办公效率。

（2）网络多媒体教学

将计算机多媒体视听引入课堂教学，使声音、图像、动画的普遍采用可以大大提高教学效果，使在每一节课上都能够发挥有效的作用。

（3）学生自主学习

针对不同的学生，提供不同的教学内容，采取不同的教学手段。主要采用基于 VOD、Web 及 FTP 的课件、光盘软件、Internet 资源，学生可以根据自己的需要自由地选择所需的内容。

（4）电子图书馆

基于 Web 的图书音像资料供学生随时阅读，并与 Internet 连接，使图书馆得到进一步拓展，使学生能够得到近乎无限的网上资源。

（5）电子邮件

电子邮件是 Internet 上的一个最重要的应用，将为每一位教师和学生开设一个电子邮件账号，利用电子邮件学生可以和老师、同学及家长进行交流，同时也可以和国内外等地学校的学生进行交流。

（6）远程教育

实现校内外连通，师生在线、交互式学习、辅导、测验等功能。

（7）校园一卡通工程

利用 IC 卡易于管理的特性，结合校园网络，轻松实现学期注册、考试、教务管理，机房上机管理，食堂餐饮管理，图书借阅管理等，从而为学校开源节流、降低管理费用。

（8）校园移动计算

采用有线和无线网络混合建构，方便学生、老师移动上网学习和办公。

2. 校园网建设的功能需求

在建设校园网的时候，一般应从以下几个方面进行考虑：

（1）网络接入需求

校园网作为基础设施之一，需要师生能够随时随地方便的接入，这也是校园网最基本的功能需求。在校园单体建筑综合布线系统设计和施工时，一般会充分考虑到每一个房间功能单元都要有网络接入，教学楼、办公楼、实验室、图书馆、后勤等各个区域的建筑都有光纤接入。大学的教职员工和学生拥有计算机的普及率相当高，网络接入是最基本的需求。

随着高校办学条件的日趋完善，网络产品的普及，以及计算机硬件设备价格的下降，笔记本电脑、无线网卡、PDA 等无线终端产品价格逐步降低，其在师生中的普及率越来越高，师生对于无线接入的需求越来越高，因此师生要求在校园内实现移动上网的呼声越来越高。目前，各所学校的建筑楼宇、宿舍可以使用有线接入网络。在校园内采用无线局域网技术组建无线校园网，可以作为有线网络的一种补充和延伸，可适应在校师生移动性强、数量大等特点，最大限度地满足师生的上网需求，为师生上网提供极大的便利。这就强调有线网络和无线网络的结合——适合无线网络的地方用无线网络，适合有线网络的地方用有线网络。

（2）骨干网络高性能、高稳定性与可靠性的需求

高校校园网的用户数在不断增加，并且随着网络应用技术的不断丰富，高校校园网应用也越发复杂，例如 FTP、VOD 点播等大数据量的访问，尤其是目前流行的 P2P 应用产生了巨大的网络流量，如何高速进行网络传输，对网络设备的性能提出了很高的要求。网络高性能要求网络核心设备、汇聚级交换机具有较高的背板带宽、端口速率等高性能指标。

随着网络应用的不断丰富，校园网已经成为师生员工工作、学习和生活不可缺少的重要平台，越来越离不开网络，网络的高稳定性、高可靠性就显得越发重要。校园网用户数不断增加、应用的复杂，导致网络流量的飞速提升，需要保证多用户、大流量情况下骨干的高带宽，骨干设备的线速转发；随着师生日常对于网络的依赖性的增强，和网络环境的日趋恶劣，需要保证做到骨干网络具备较高的稳定性、可靠性。

（3）出口区域对性能和功能的需求

当前高校一般都接入中国教育科研与计算机网 CERNET，有条件的高校还接入了电信级运营商提供的宽带接入。这就需要进行多出口的策略部署，并且需要解决多出口部署下的性能问题。校园网出口设备的功能和性能尤为重要，它起着将一个用户数较多的高校园区网络与互联网互联互通的重要桥梁的作用。校园网出口设备需要具备出口路由策略、网络地址转换等功能，这也容易成为校园网访问互联网的一个瓶颈。具体来说，NAT（地址转换）就是上网速度慢的一个重要原因，另外设备启用策略路由时，造成设备性能的下降，也影响整个出口的效能和稳定性。

（4）数字校园网络支撑平台的需求

校园网的建设突出在基础设施建设上，包括校园网络、存储系统、计算机系统及其他硬件设施，整体构成了数字校园的基础支撑平台。校园数据中心是学校信息数据的存储、共享、交换与处理的中心，承担着学校的核心计算、信息系统的运行、信息资源管理、信息资源服务等功能，也是校园网建设时必须重点考虑的要素。校园网中各种信息系统、业务系统、支撑软件系统等都依赖于高性能的校园网络作为基础支撑平台来提供服务。

（5）网络安全的需求

在应用丰富的同时，网络环境也变得异常恶劣。近两年，安全攻击事件呈指数级上升，而所需要的知识却越来越弱化，各种攻击工具在网络上可以随手拈来。这也对网络设备在网络攻击或者病毒泛滥情况下的稳定可靠提出了挑战。

第一，高校面临着严峻的网络安全形势。越来越多的报道表明高校校园网已逐渐成为黑客的聚集地。这一方面是由于网络病毒、黑客工具的泛滥，用户安全意识的淡薄，而另一方面，高校学生——这群精力充沛的年轻一族对新鲜事物有着强烈的好奇心，他们有着探索的高智商和冲劲，却缺乏全面思考的责任感。有关数字显示，目前校园网遭受的恶意攻击，90% 来自高校网络内部，如何保障校园网络的安全成为高校校园网络建设时不得不考虑的问题。

第二，网络安全一定是全方位的安全。首先，网络出口、数据中心、服务器等重点区域要做到安全过滤；其次，不管接入设备，还是骨干设备，设备本身需要具备强大的安全防护能力，并且安全策略部署不能影响到网络的性能，不造成网络单点故障；最后，要充分考虑全局统一的安全部署，需要能够从准入控制，到对网络安全事件进行深度探测，到现有安全设备有机的联动，到对安全事件触发源的准确定位和根据身份进行的隔离、修复措施，从而能对网络形成一个由内至外的整体安全构架。

所以，在对出口等重点区域进行安全部署的同时，要更加全面地考虑安全问题，让整个网络从设备级的安全上升一个台阶，摆脱仅仅局部加强某个单点的安全强度的现状。

（6）方便运营管理的需求

首先，校园网需要进行合理的运营。第一，校园网的投资较大，加上每年的维护成本，对于学校并不是一笔可以忽视的开支；第二，根据各校的情况，进行合理的运营收费，依靠市场化的手段能够推动校园网的运作规范化和提高建设水平。当然，学校不是运营商，运营的模式和业务流程并不清晰。而学校收费和学生缴费又是一对天然的矛盾，当前不少学校采用的运营模式与学校实际的情况差距太大，无法有效杜绝学生逃避收费等问题一直困扰着学校的网管人员。

其次，有效的管理可以从用户管理和设备管理两方面来看。

对于用户管理，最重要的是能够实现事前的身份认证和准确定位，事中的实时处理，事后的完整日志审计。事前的认证和定位是指可严格实现用户身份识别，根据用户账号、密码、MAC 地址、IP 地址、交换机 IP、交换机端口号、用户所在 VLAN 的灵活组合，来识别用户身份。将网络中的虚拟用户和生活中的真实用户相对应。事中的实时处理是指对于正在使用网络的用户，如果出现私自拨号上网、使用代理、更改 IP 地址等行为，认证计费系统会强制用户下线。对于感染病毒，出现安全问题的用户，结合全局安全通过安全联动来进行隔离、阻断和修复，以保证校园网的安全。事后的日志审计是指记录用户上网的详细信息（包括用户名、IP、MAC 等）及完整的用户访问外网的记录（包括源 IP、目的 IP、源端口、目的端口、访问时间），一旦出现安全问题，可以进行快速完整的审计，迅速定位到个人。

对于设备管理，需要的是统一有效的网络管理系统。能够直观全面地监控整个网络和各种设备的运行状态，记录和深入分析网络流量，及时报告各种故障和性能问题，协助管理员找到故障的起源，并且对网络的性能变化和故障发生提前进行预测。

高校用户数和网络节点数众多，因此难以一体化管理众多的设备和用户，出现网络故障无法快速定位、IP 地址盗用、IP 地址冲突等问题日益严重，如何利用有限的人力物力对网

络进行高效管理也成为学校考虑的重点。

8.2.4　校园网设计案例分析

1. 校园网模块化、层次化设计理念

近年来，校园网的建设在国内高校如火如荼地开展，几乎所有的高校都建设有校园网络，而且校园网规模较大，有的重点大学校园网用户数达到 2 ~ 3 万，属于比较大型的网络，一般规模的校园网，用户数也在万人左右。校园网也是一个包罗万象的网络，应用了各种较新的产品和网络技术。从建设校园网的过程来看，校园网也是一个较为复杂的网络。纵观国内大部分高校近 10 年来建设的校园网，主要体现了网络设计模块化、层次化的设计理念，即建设包含出口、核心、汇聚、接入等多层次的网络。根据学校建筑规划，将整个网络进行了功能区的划分：教学区、办公区、学生宿舍区、后勤服务区、家属区、数据中心、网络中心等较大的逻辑区域，对教学楼、办公楼、学生宿舍区、家属区、后勤服务区等园区交换网作为整个网络的承载基础，基本都是基于三层架构进行划分：核心层、汇聚层和接入层。

2. 校园网设计案例分析

本节以一个由星网锐捷网络公司提供的校园网设计方案作为案例进行介绍，从中可以学习到如何设计大型网络的一些理念和经验。该方案体现了主干网络结构按层次化、模块化原则进行设计的理念，由核心层、分布（汇聚）层、接入层三大部分构成校园网络。主干网络采用万兆以太网技术来建设，保证大规模的数据交换快速、稳定和高效。

针对一个高校，校园网按教学区、办公区、学生宿舍区、图书馆等划分为若干个逻辑区域，每个逻辑区域设立一个逻辑区域的汇聚主节点，下联多个汇聚层设备和多个接入层设备。校园网所需要的网络设备主要为路由器、防火墙、核心交换机、汇聚交换机和接入交换机，各单体建筑所需要的接入交换机台数根据该单体建筑所需的信息点位总数确定。根据实际应用情况，对于网络性能要求较高的行政办公楼、计算中心机房、数据中心和上网人数较为密集的区域可采用两台交换机组成汇聚节点，实行双机热备，充分保证网络的稳定性和可靠性。

校园网设备选型要充分考虑满足校园网的主要性能指标，采用国内外技术领先、成熟的网络产品，实现高可靠性、稳定性。对校园网出口策略、路由协议、IP 地址规划、VLAN 划分及校园网计费系统、支持 802.1X 认证、网络管理系统、网络流控系统、负载均衡、网络安全系统等都需要逐步详细分析和规划设计。在综合布线系统设计时，一般要求，校园网从核心节点到各个区域的汇聚主节点、从汇聚主节点到各个楼宇的汇聚节点根据实际布线距离通过单模/多模光纤实现万兆互联。图 8-1 给出了一个比较流行的主干网络结构设计图。

该方案有如下一些设计特点：

（1）负载均衡、冗余备份的出口设计

1）具有较强的网络地址转换（NAT）、出口策略路由（PBR）性能。当前，校园网出口面临的首要问题就是性能问题。性能问题主要体现在出口设备启用 NAT 和 PBR 功能的情况下。锐捷网络为校园网出口开发的一款网络出口引擎 NPE 系列产品，可以支持高速大流量的线速转发，支持高并发数的连接会话，较好地提升了出口性能。

2）出口线路自动负载均衡、出口设备的冗余备份及链路的冗余备份。一方面在流量的策略上，能够实现基于源头的流量区分和基于访问目的的出口控制。具体举例来说，可以将

学生的流量和老师的流量制定不同的路由路径；在对外出口上，根据所访问的资源进行划分，教育网免费资源走 CERNET 出口，免费地址列表之外的都走网通或者电信出口。另一方面，从可用性角度，实现了任何一台设备（任何一台防火墙或者任何一台网络出口引擎）的故障或者任何一条链路的瘫痪，都将使相应的流量自动切换到另外一台设备或者另外一条链路上。充分保证出口的可用性，时刻保持网络的互联互通。

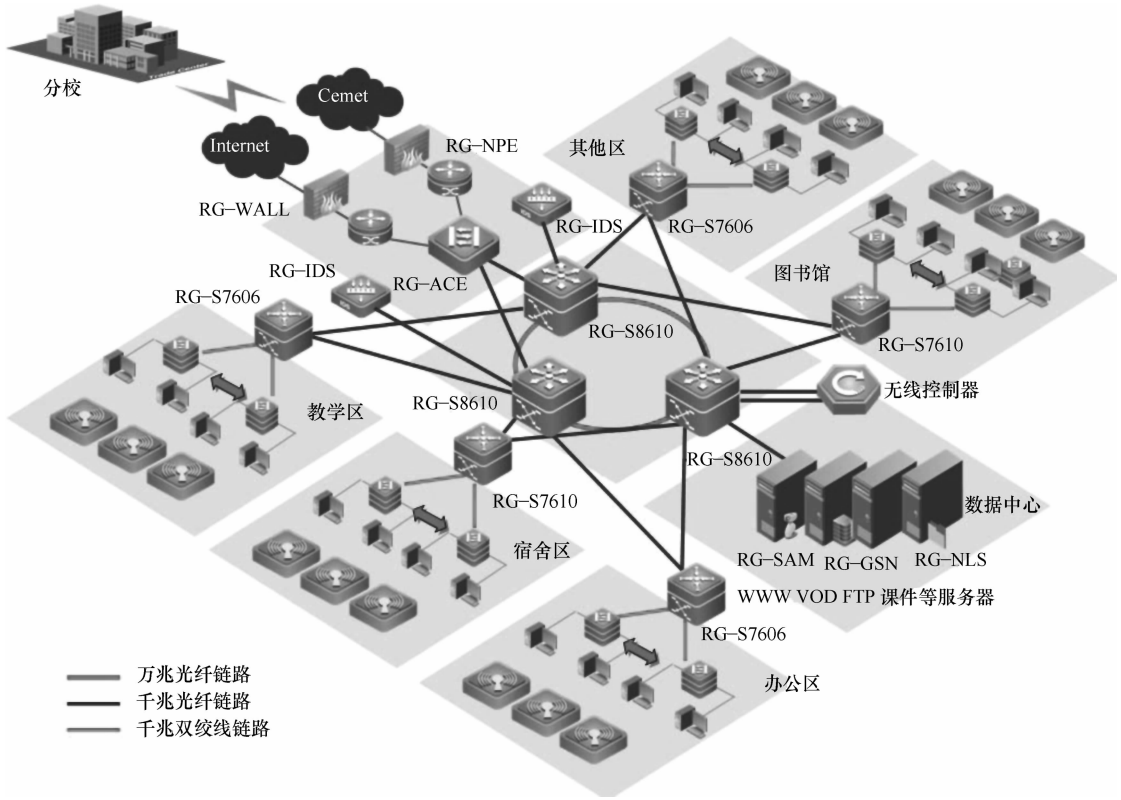


图 8-1　主干网络结构设计图

3）完善的出口日志功能。针对各种网络攻击和安全威胁进行日志记录，采用统一的格式，支持本地查看的同时，还能够通过统一的输出接口将日志发送到日志服务器，为用户事后分析、审计提供重要信息，方案中所能提供的日志包括：设备日志、上网记录日志、攻击日志。

（2）骨干交换网络的高性能、稳定可靠性

整网采用万兆多核心、万兆/千兆骨干、千兆/百兆到桌面的设计理念。骨干网络核心区域采用万兆多核心环网设计，核心交换机分别负责教学、办公、图书馆、数据中心等核心区域的数据交换与转发，每台核心通过千兆光纤和汇聚交换机相连。核心交换机采用高吞吐量，线速转发的核心路由器和三层交换机，所有关键器件的冗余，包括主控板、交换网板、电源等，支持板件的热插拔技术，保证了网络的高效运转。骨干设备双核心双链路，或者核心成环之后，相互之间互为容错备份，并在核心交换机中采用关键模块冗余设计（双电源冗余等）。核心和汇聚之间采用双链路连接，一旦数据传输的活动链路失效以后可以自动切换到另一条链路，保障数据的正常转发。这样，从全网架构上，核心层双链路交换系统不存在单点故障，是一种高级别交换完全冗余的容错方案，这样即使其中一条链路断线或一个主

干交换机发生故障，都能在用户觉察不到的极短的时间内启用备份恢复数据传递，从而保证网络系统可靠、稳定地运行。

（3）有效的安全和管理措施

1）统一的身份准入控制及详细的日志审计。锐捷网络设备能实现安全认证到桌面，对用户 IP 地址、MAC 地址、账号、端口等可实现自动绑定、静态绑定、动态绑定等多种灵活的策略，可以确保用户入网时身份唯一，并且避免了 IP 冲突。在网络管理上，支持管理分级授权，避免了管理的安全隐患。还支持详细的日志审计功能记录用户上网的详细信息（包括用户名、IP、MAC 等）及完整的用户访问外网的记录（包括源 IP、目的 IP、源端口、目的端口、访问时间），一旦出现安全事件，可以进行快速完整的审计，迅速定位到个人。

2）设备本身具有强大的安全防护能力。锐捷网络核心及全线网络产品具有丰富的安全防护功能，包括防 DOS 攻击、防 IP 扫描、防源 IP 地址欺骗 、防 ARP 欺骗、防病毒、带宽控制等。锐捷网络还在继承已有的设备安全防护能力的技术基础上，开发出了集多种强大安全功能于一体的 CSS 安全体系设计，通过硬件安全监控技术、硬件安全防护技术、丰富的设备安全管理保证系统的安全，通过硬件的隧道技术、认证技术、加密技术保护了网络设备传输的数据的安全。此外，还提供了万兆位的安全防护模块同时保护系统和数据。通过提供万兆位安全防护模块，可以对网络中的数据进行 2 ~ 7 层的安全监控防护。

3）GSN（Global Security Network）全局安全解决方案。GSN 全局安全解决方案是锐捷网络提出的一种针对高校校园网安全问题较新的解决理念。GSN 系统对全网的所有安全事件、网络病毒攻击行为、用户行为和用户主机安全信息进行深入分析和全局监控。通过这种实时全网侦测，在第一时间内将网络异常现象通过接入层隔离出网络，使得网络异常现象完全不影响核心网络；在发现安全问题后能自动对用户进行安全事件告警，并迅速根据用户身份选择将用户隔离到安全修复区域或自动阻断异常数据流。通过部署 GSN，还能轻松地进行主机信息获取；实现主机完整性（HI）规则（通过一系列规则的定义，约定了对用户主机的准入标准）；利用先进的“免疫性”ARP 防病毒防攻击技术，彻底解决 ARP 木马等病毒/攻击带来的网络中断事故的影响。

（4）对 WLAN（无线局域网）的支持

锐捷针对无线局域网设计了一种高性能、高稳定性的智能无线组网架构——智能无线交换架构，通过无线交换机 MX 系列产品的控制，无线接入点可具备根据不同用户、不同应用类型、不同 VLAN 等方式来决定数据流量是否需要全部集中流经无线交换机，对于 FTP、视频点播这类大量占用网络资源且安全性要求较低的应用，可以直接通过本地有线网络进行转发，而对于教务系统、考试系统、身份认证系统这类安全性要求高的应用，则可以将流量通过加密隧道送到无线交换机，防止加密数据在有线网络传输过程中被非法用户窃取。同时，这种架构可以确保无线网络承载业务的高稳定性。无线交换机产品通过支持集群和冗余能力，可以实现多台无线交换机对同一个无线接入点提供服务。由于无线交换机之间采用了虚拟化技术，可实时将 AP 与用户的在线信息同步，如果一台无线交换机出现宕机，与其控制的无线接入点失去联系，那么另一台或者多台无线交换机将立即接管这些无线接入点。在这个过程中，用户不会掉线，并且仍然保持正常通信状态。

对于无线网络的管理，锐捷网络“面向无线网络生命周期”的管理系统强调无线网络生命周期的管理，涵盖了无线网络的规划、部署、优化、监测和报表五大方面。在对无线网

络的安全管理上，可以实现合法用户的安全准入、合法设备的安全准入、合法网络的安全准入、合法射频环境的安全准入，并能有效防御无线网络入侵和病毒入侵。

（5）全面支持 IPv4 向 IPv6 的分阶段分步骤平滑过渡

利用支持双栈技术的多业务万兆核心路由交换机（如 RG-S8600 系列）作为骨干校园网 IPv4/v6 过渡设备。实现同时与 IPv6 网和 IPv4 网的互通。此方案同时支持 IPv6/ IPv4 两种业务流，不影响目前学校主要的 IPv4 业务，满足学校在 IPv6 应用时的过渡网络环境。

8.3 校园网建设实际案例

本节我们以一个高校的校园网建设方案作为案例，来讲述大型园区网络的设计步骤和方法。

8.3.1 建设需求调查

某大学新校区总用地面积 1000 亩，新校区建筑面积 38 万平方米，按照整体规划，分三期实施，包括行政中心、理学院、环能学院、建筑学院、土木学院、图书馆、10 栋学生宿舍楼等主要建筑。建筑平面图如图 8-2 所示。

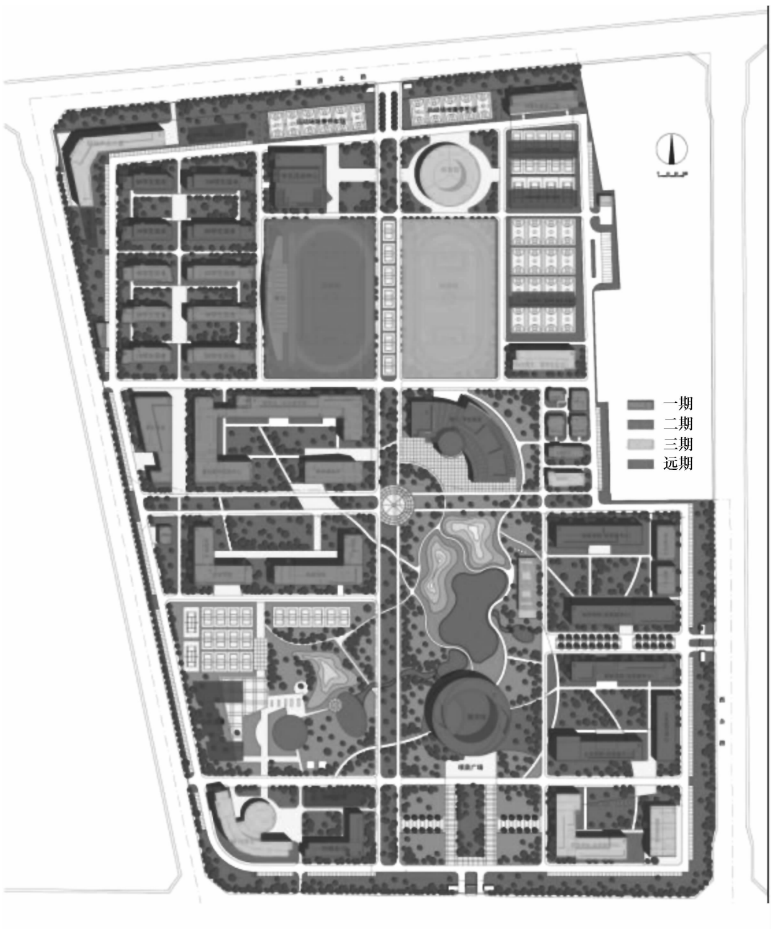


图 8-2 某高校校园建筑平面图

基建项目共分三期：

一期建设项目主要包括：环能学院、经管学院、理学院、基础教学实验室、学术报告厅、金工实习中心、实验中心、运动场、学术报告厅、学生食堂、6 栋学生宿舍、青年教师公寓、后勤办公等。

二期建设项目主要包括：图书馆、行政办公楼、机电学院、电信学院、测绘学院、土木学院、土木实习中心、教工学生食堂等。

三期建设项目主要包括：研究生、留学生宿舍、校医院、建筑学院、建筑展览馆、教工俱乐部。

基本的需求包括以下几点：技术领先满足未来至少 5 年的需求，高可靠性，高性能，千兆桌面，万兆上行，全网支持 IPv6 平滑过渡，无线覆盖，快速收敛，从终端到边界全面的安全解决方案。

8.3.2　逻辑网络设计方案

1. 网络拓扑结构设计

一般，校园园区网络规模比较大，接入节点数目比较多，各院系的数据在网络上的传输也必须保证端到端的安全，各院系、各部门间的业务隔离需求就显得比较迫切，随着各校园业务的快速增长，校园网络的扩展性也应该比较强。该方案包括层次化设计、高可靠性设计。校园 IP 网络平台还包括网络安全性设计、无线网络设计、IPv6 网络设计。

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，并考虑到技术的先进性、成熟性，采用模块化的设计方法。拓扑结构如图 8-3 所示。

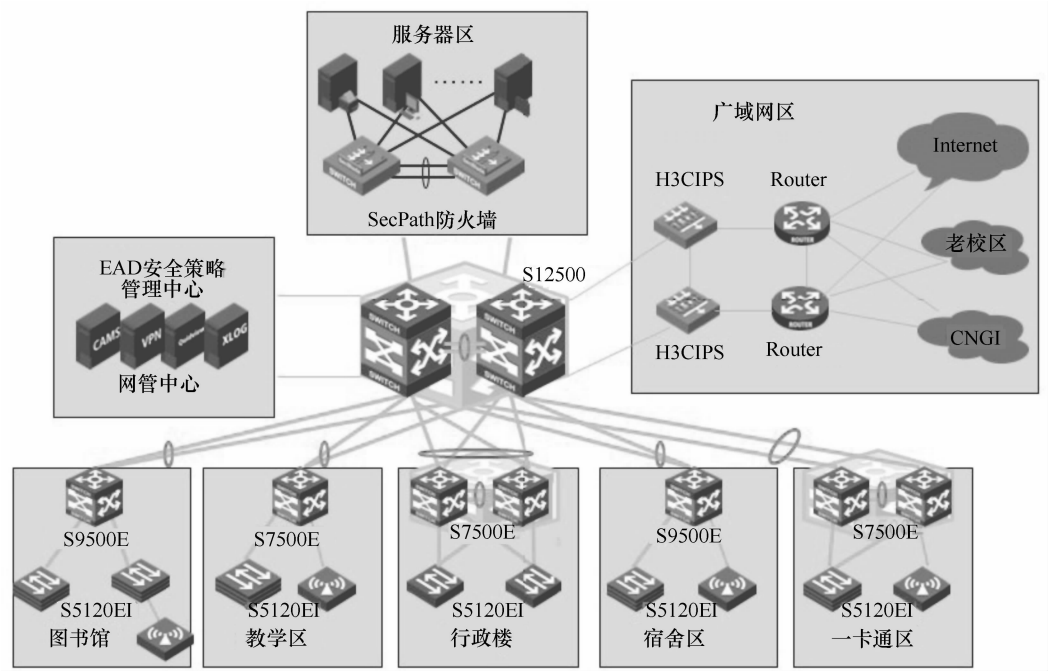


图 8-3　校园网拓扑结构

本方案主要设计要点如下：

（1）模块化设计

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 优化模块等主要逻辑功能部分。根据目前业界主流的根据功能区对网络进行划分的思路将整个网络进行了功能区的划分：园区交换网，数据中心，网管中心，广域网区。

（2）层次化设计

其中园区交换网作为整个网络的承载基础基于三层架构进行划分：核心层、汇聚层和接入层。核心层主要提供无阻塞的高性能交换平台，本次采用 H3C 数据中心级核心产品 S12500 交换机，提供 100G 的高速交换平台；汇聚层为连接本地的逻辑中心，对性能也有较高的要求，推荐采用 H3C S7500E 系列交换机，提供万兆汇聚能力；接入层推荐采用 H3C S5120EI 系列交换机，提供千兆到桌面、万兆汇聚能力，满足高性能接入需求。

（3）高性能

核心交换机 S12500、汇聚交换机 S7500E 在提供大容量、高性能 L2/L3 交换服务基础上，进一步融合了硬件 IPv6、硬件 MPLS、安全、业务分析等智能特性，可为园区网、数据中心构建融合业务的基础网络平台，进而帮助用户实现 IT 资源整合的需求，核心交换机和汇聚交换机提供高密度万兆（10GE）接口。

（4）可靠性设计

核心层采用 S9500E RPR 环路设计，可以实现 10ms 的故障检测时间以及 50ms 的业务倒换时间，可以做到故障切换时完全不影响正在进行的音频业务，完全满足电信级可靠性的要求。汇聚层采用高性能 S7500E 根据实际的建筑分布状况，网络设备主要部署在图书馆、教学区（包括各个学院的教学楼）、行政楼、宿舍区、一卡通区等区域。部分对可靠性要求较高的区域部署两台汇聚交换机，构建 IRF 智能弹性架构。接入层采用 S5120 系列堆叠交换机，简化了管理，利用双链路上行并结合链路聚合 LACP 提高了接入层的可靠性。本项目所采用的设备均可以支持 IPv6，可以平滑过渡到 IPv6，做到最佳的投资保护。

（5）有线无线一体化

本次采用 S9500E 高性能的无线控制器插卡可以充分利用 S9500E 的背板带宽，消除线路瓶颈，减少机架空间，具有电源较少、线缆布防、与有线设备统一管理等优点。通过插卡还可以有效减少侧挂网络形成的性能瓶颈，提高网络性能。

2. 层次化设计

在校园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。典型的校园园区网络结构可以分成三层：接入层、汇聚层、核心层。

（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。对于校园园区网的接入层设备，建议采用千兆接入的方式，应该具有线速交换、丰富的 ACL 策略以及高级 QoS 策略等功能。可以提供 24/48 端口高密度的线速千兆接入端口，同时和汇聚、核心一起部署全网的安全管理方案。在需要控制策略或者设备性能要求更加严格的区域，如服务器接入区推荐采用三层接入交换机，推荐采用 H3C 数据中心级接入

交换机 S5800 系列。

（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；对于校园园区网的汇聚层设备，应该能够承载校园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（Graceful Restart）、环网保护等多种高可靠技术，能够承载校园园区融合业务的需求。

汇聚层设备通过万兆双上行到网络核心；下行 10GE 接口/GE 接口连接接入层交换机。可采用 S7500E 万兆交换机作为汇聚交换机，提供 10GE 上联，10G/GE 高密度下联。对于学生宿舍区和图书馆业务流量较大的区域汇聚节点，推荐采用 H3C 高端核心交换机 S9500 系列产品，对于行政楼等对高可靠性要求比较高的应用场景建议采用双机虚拟化技术提高网络可靠性。

（3）核心层

核心层是网络的骨干，必须能够提供高速数据交换和路由快速收敛，要求具有较高的可靠性、稳定性和易扩展性等。对于校园园区网核心层，必须提供高性能、高可靠的网络结构，推荐采用高可靠的 IRF 技术。对于校园园区网核心层设备，应该在提供大容量、高性能 L2/L3 交换服务的基础上，能够进一步融合硬件 IPv6、网络安全、网络业务分析等智能特性，可为校园园区构建融合业务的基础网络平台，进而帮助用户实现 IT 资源整合的需求。

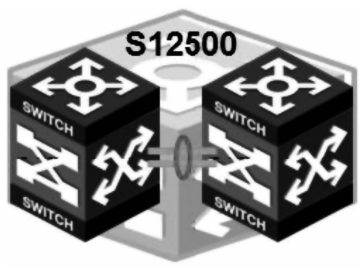


图 8-4　双核心冗余

因为校园网的规模较大，对核心层要求非常高，推荐两台 S12500 核心交换机构建 IRF 虚拟弹性架构，如图 8-4 所示。它的主要优点是将两台设备虚拟为一台更高端的设备，成倍增加性能和设备可靠性；简化了 VRRP、MSTP 和安全等业务部署；同时简化网络架构，提高业务性能和简化网络管理。

8.3.3　IP 地址及路由规划

本方案可以采用 6.3.3 IP 地址的规划与分配的方法进行 IP 分配。主要使用私网 IP 地址分配到每一个设备和终端设备上。对于 IPv4 路由规划，规划如下：

1）整个骨干网络采用 OSPF 路由协议，OSPF 协议在整个骨干网中不会引起路由回环，利于校园网骨干网的健壮性。

2）在汇聚与核心交换机之间采用 OSPF 路由的方式，OSPF 路由的方式可以减少网络中心人员对于校园网的维护量。

3）OSPF 在校园网中只在核心骨干中运行，这样大大减少了骨干节点之间 OSPF 协议的收敛周期，在实际的应用过程中可以提高校园网的稳定性。

4）内置 DHCP Server 实现全网的 DHCP Server 的分散，避免单点故障。

5）核心交换机可以支持防私设 DHCP Server、与 IDS 联动实现全网的安全无阻塞设计。

8.3.4　综合布线系统设计

综合布线系统作为新校区校园网络的骨架和脉络，十分重要。综合布线系统需为开放式

网络拓扑结构，提供满足数据、图像、音频、视频等多媒体应用服务和传输能力，同时还能适应今后 20 年甚至更长时间内网络和通信技术的高速发展，为建设先进的万兆骨干网络系统打好坚实的基础。综合布线系统应具有高度灵活性、可靠性、可扩展性，方便扩容和维护管理，能适应未来的网络通信技术的发展。

新校区综合布线工程要在执行相关国家规范标准和规范的前提下，采用现代信息技术、网络技术、计算机控制技术和系统集成技术，通过周密的设计、择优集成、规范施工、认真安装调试，确保建成高质量的综合布线系统，在布线方面要求具有高度灵活性、可靠性、综合性及适度冗余性，并且要求易扩容、面向未来的发展及方便维护和管理。

新校区校园网布线系统要满足新校区校园网络主干网络结构设计的要求。网络布线系统主要包括建筑群主干布线系统和各单体建筑布线系统。从新校区网络核心机房至各汇聚节点全部采用单模光纤接入至各汇聚节点机房，从各汇聚节点楼宇至汇聚区域各单体建筑，根据实际距离情况采用单模或多模光纤接入，形成一个从核心到各单体的多级星形网络结构。一卡通系统、多媒体教学系统、安防监控等专有网络应构建单独的网络传输系统，在综合布线系统整体设计时根据系统的特殊需求进行充分考虑。

1. 综合布线系统的组成

整个布线系统由工作区子系统、水平干线子系统、管理子系统、主干子系统、设备间子系统及建筑群子系统 6 个子系统构成。综合布线系统工程需按下列 7 个部分进行设计：

1）工作区：一个独立的需要设置终端设备的区域宜划分为一个工作区。工作区应由配线子系统的信息插座模块延伸到终端设备处的连接缆线及适配器组成。

2）配线子系统：配线子系统应由工作区的信息插座模块、信息插座模块至电信间配线设备的配线电缆和光缆、电信间的配线设备及设备缆线和跳线等组成。

3）干线子系统：干线子系统应由设备间至电信间的干线电缆和光缆、安装在设备间的建筑物配线设备及设备缆线和跳线组成。

4）建筑群子系统：建筑群子系统应由连接多个建筑物之间的主干电缆和光缆、建筑群配线设备及设备缆线和跳线组成。

5）设备间：是在每幢建筑物的适当地点进行网络管理和信息交换的场地。对于综合布线系统工程设计，设备间主要安装建筑物配线设备。

6）进线间：是建筑物外部通信和信息管线的入口部位，并可作为入口设施和建筑群配线设备的安装场地。

7）管理：管理应对工作区、电信间、设备间、进线间的配线设备、缆线、信息插座模块等设施按一定的模式进行标识和记录。

在进行新校区从综合布线弱电管网的设计到各单体楼宇的建筑规划设计时，需加强与建筑设计院设计人员的沟通，充分考虑网络综合布线系统设施及管线、线槽和管井的设计，并且预留足够面积的设备间、配线间和进线间等，对上述设计均须满足国家出台的综合布线系统工程设计规范（GB 50311—2007）等相关标准和规范。

2. 建筑群子系统光纤铺设

建筑群子系统将一栋建筑的线缆延伸至建筑群内的其他建筑的通信设备和设施，实现楼群之间网络通信系统的信息连接。主要由室外光纤（其中包括单模光纤和多模光纤）、室外大对数通信电缆组成；建筑群子系统采用地下管道敷设方式，建筑群子系统的路由方式充分

利用全校弱电管网。弱电管网的地下通道要预留足够的管槽，支持综合布线系统主干光缆的铺设。

3. 主干链路

建筑群主干布线系统包括从新校区网络核心机房至各汇聚区域节点所在楼宇设备机房、从汇聚区域节点所在楼宇机房至各单体建筑机房的主干光纤铺设工程，包括主干光缆铺设、光纤熔接、跳线、设备间线缆接入等相关布线产品和工程实施。综合布线光缆示意图如图 8-5 所示。

1）一级主干：从网络核心机房至全校各汇聚级节点单体建筑机房建设万兆主干链路，采用 4 根 24 芯万兆单模光纤铺设。

2）二级主干：从各单体建筑汇聚节点设备间至相关楼层配线间，采用 2 根 24 芯室内万兆单模/多模光纤铺设。

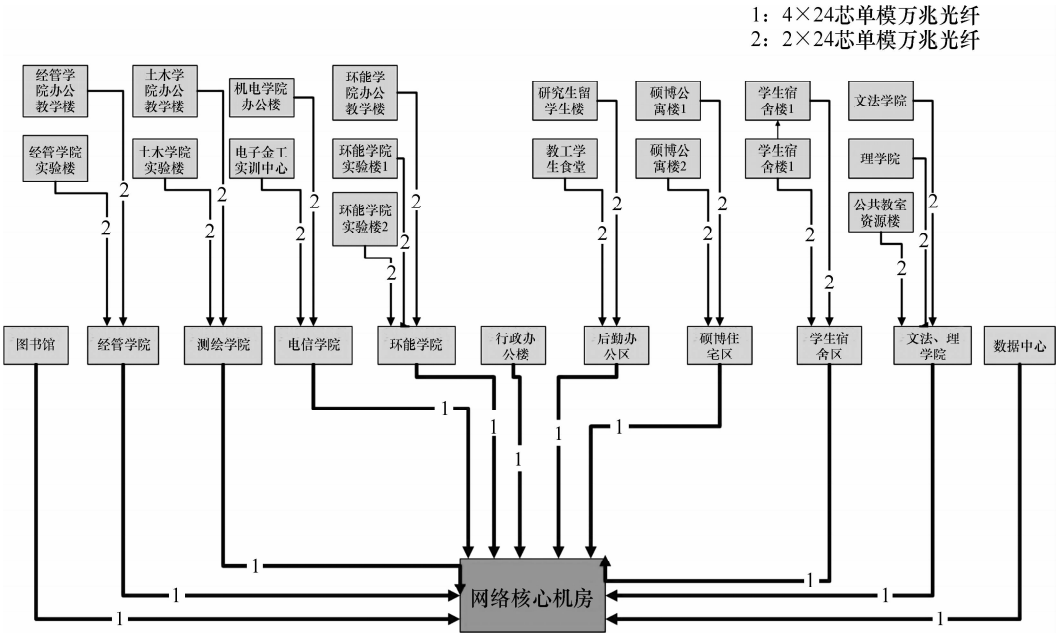


图 8-5　综合布线光缆示意图

4. 水平链路

新校区的水平链路采用六类标准的非屏蔽系统（铜缆）双绞线，对于财务或学校重要涉密系统，根据要求可考虑采用六类标准的屏蔽系统（铜缆）双绞线。

本 章 小 结

本章以校园网作为大型园区网络建设的案例，简要回顾了大学园区网络建设的发展历程，并对大学园区网络的构成、核心技术进行了讨论，最后给出了一个大学园区网络建设的实例。

参 考 文 献

[1] 谢希仁. 计算机网络［M］. 5 版. 北京：电子工业出版社，2008.

[2] 吴功宜. 计算机网络［M］. 3 版. 北京：清华大学出版社，2011.

[3] 思科网络技术学院. 思科网络技术学院教程（第一、二学期）［M］. 3 版. 北京：人民邮电出版社，2004.

[4] 思科网络技术学院. 思科网络技术学院教程（第三、四学期）［M］. 3 版. 北京：人民邮电出版社，2004.

[5] 王云，等. 网络工程设计与系统集成［M］. 2 版. 北京：人民邮电出版社，2010.

[6] 黎连业. 计算机网络与工程实践教程［M］. 北京：科学出版社，2007.

[7] 黎连业. 网络综合布线系统与施工技术［M］. 2 版. 北京：机械工业出版社，2002.

[8] 魏大新，李育龙，强振海. Cisco 网络工程案例精粹［M］. 北京：电子工业出版社，2007.

[9] 胡友彬，陈俊华. 网络工程设计与实验教程［M］. 北京：电子工业出版社，2010.

[10] 苏英如，王俊红，王培军. 局域网技术与组网工程［M］. 北京：清华大学出版社，2010.

[11] 苏英如. 局域网技术与组网工程实训教程［M］. 2 版. 北京：中国水利水电出版社，2007.

[12] 王春海. 非常网管-典型网络实验［M］. 北京：人民邮电出版社，2007.

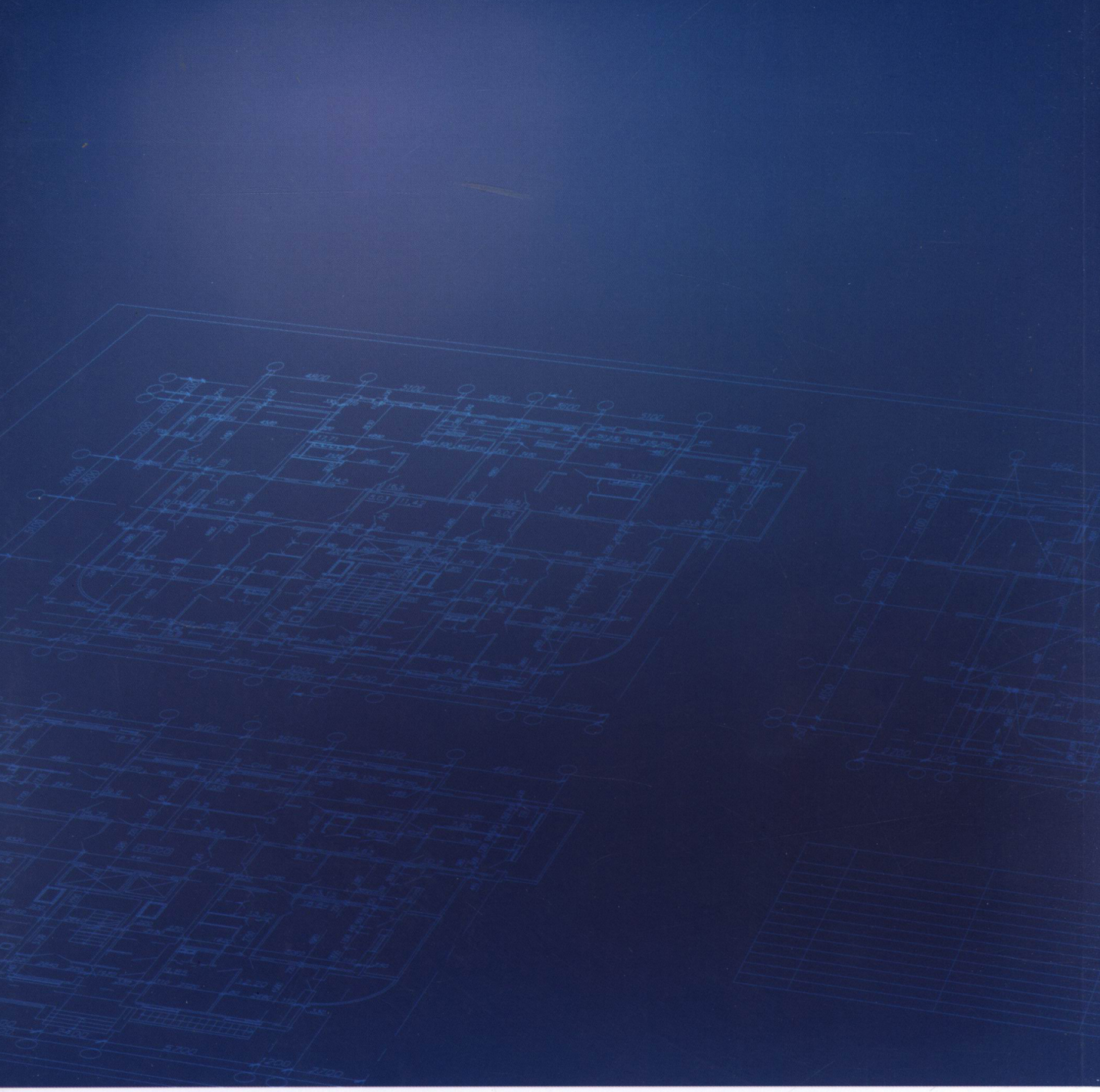
[13] 钟小平，张金石. 网络服务器配置与应用［M］. 3 版. 北京：人民邮电出版社，2007.

[14] 汪双顶，姚羽. 网络互连技术与实践教程［M］. 北京：清华大学出版社，2009.

[15] 石炎生，羊四清，谭敏生. 计算机网络工程实用教程［M］. 北京：电子工业出版社，2007.

[16] 胡胜红，毕娅. 网络工程原理与实践教程［M］. 2 版. 北京：人民邮电出版社，2010.

[17] 张玉兰，张召贤. 组网技术与网络管理［M］. 北京：清华大学出版社，2013.



地址：北京市百万庄大街22号
邮政编码：100037
电话服务
服务咨询热线：010-88361066
读者购书热线：010-68326294
010-88379203
网络服务
机工官网：www.cmpbook.com
机工官博：weibo.com/cmp1952
金书网：www.golden-book.com
教育服务网：www.cmpedu.com
封面无防伪标均为盗版

机械工业出版社微信服务号

ISBN 978-7-111-47722-8

策划编辑◎林春泉

ISBN 978-7-111-47722-8

定价：49.00元