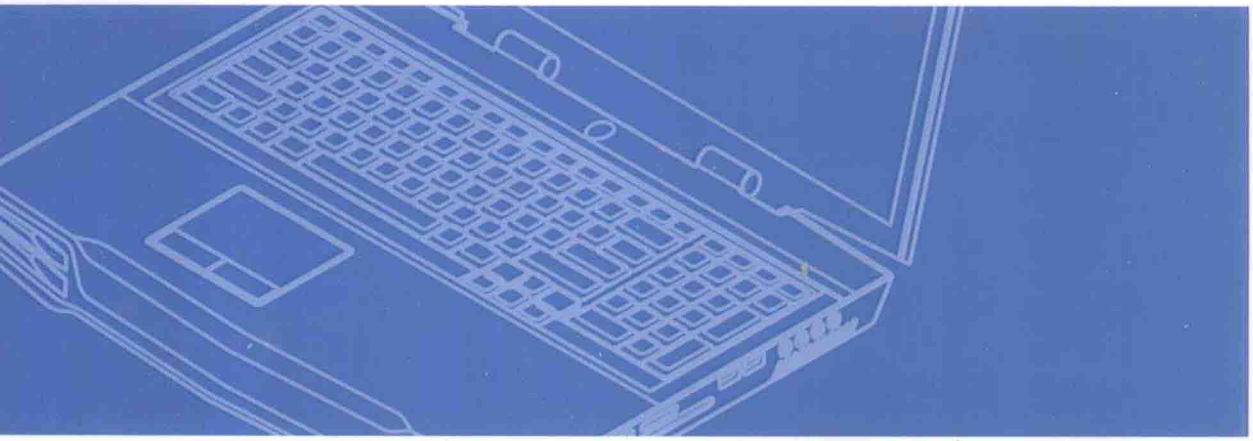
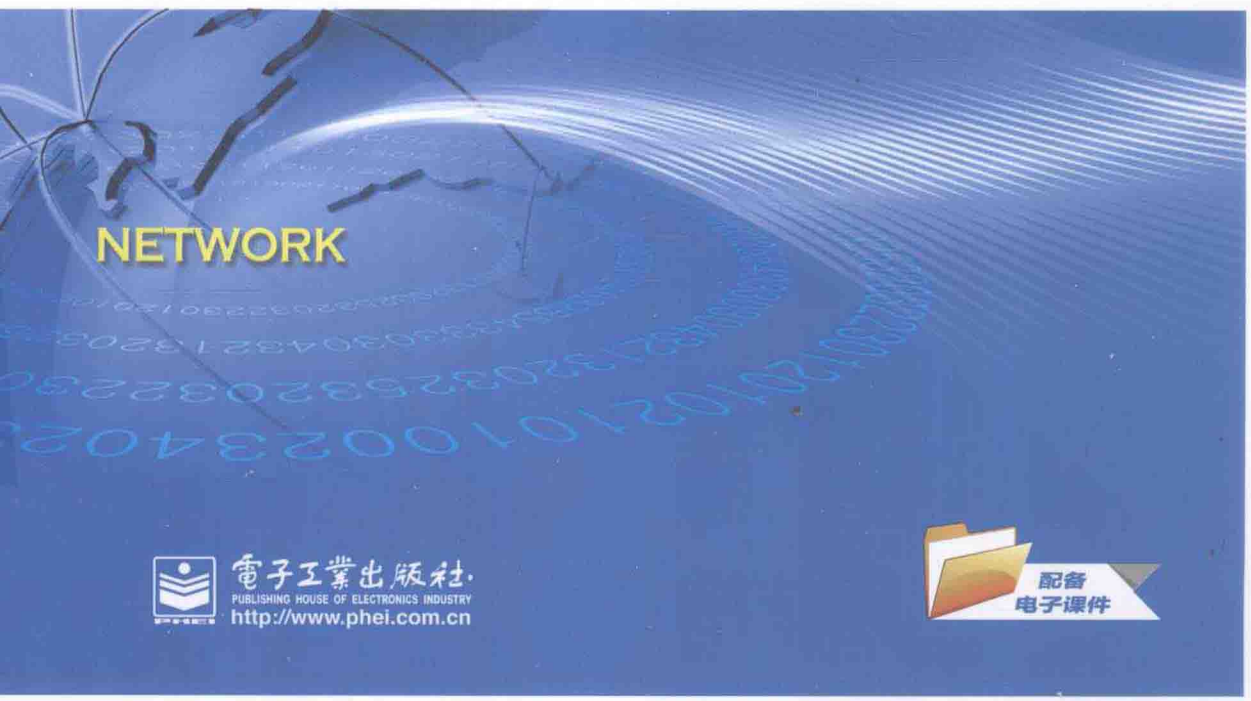


21世纪高等职业教育 计算机系列规划教材

网络设备配置与管理

◆ 邱　洋　计大威　主编

◆ 胡国胜　张迎春　蔡军英　副主编



電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

配备电子课件

21世纪高等职业教育计算机系列规划教材

网络设备配置与管理

邱　洋　计大威　主　编

胡国胜　张迎春　蔡军英　副主编

電子工業出版社

Publishing House of Electronics Industry

北京 · BEIJING

内 容 简 介

交换机和路由器是计算机网络的核心设备，对于希望今后从事网络系统集成、网络管理与维护等工作的学生，掌握交换机和路由器的基本应用技术十分重要。

本书主要针对高等职业院校计算机及网络相关专业，以组建某学校的校园网网络项目为主线，从项目任务需求描述开始，按照基本知识、配置技能、项目实施等过程来介绍学习内容。本书内容主要涉及组建网络所需的最基本的技术和技能，包含交换式局域网组建、交换网络优化、提高网络可靠性、实现网络互联等 9 个项目场景，对应学生今后工作岗位的相应技能。

本书可作为大专院校计算机相关专业的教材或参考书，以及各类网络设备培训班的网络培训教材或辅助教材，并适合所有从事网络管理和系统管理的专业人员及网络爱好者阅读。

图书在版编目（CIP）数据

网络设备配置与管理/邱洋，计大威主编. —北京：电子工业出版社，2014.9
（21 世纪高等职业教育计算机系列规划教材）
ISBN 978-7-121-24125-3

Ⅰ. ①网… Ⅱ. ①邱… ②计… Ⅲ. ①网络设备－配置－高等职业教育－教材②网络设备－设备管理－高等职业教育－教材 Ⅳ. ①TP393

中国版本图书馆 CIP 数据核字（2014）第 191897 号

策划编辑：徐建军（xujj@phei.com.cn）
责任编辑：郝黎明
印　　刷：三河市鑫金马印装有限公司
装　　订：三河市鑫金马印装有限公司
出版发行：电子工业出版社
　　北京市海淀区万寿路 173 信箱　邮编 100036
开　　本：787×1 092　1/16　印张：12.5　字数：320 千字
版　　次：2014 年 9 月第 1 版
印　　次：2014 年 9 月第 1 次印刷
印　　数：3 000 册　　定价：28.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

服务热线：（010）88258888。

前言
Preface

随着物联网、云计算等应用的不断发展，计算机网络技术作为这些应用的基础平台显得尤为重要，社会对高技能的网络应用型人才需求也与日俱增。在计算机网络平台中，交换机、路由器是最常见、也是最常用的网络设备，这两种设备的配置与管理技术成为计算机网络的核心技术，掌握这两种设备的应用能力对网络专业学生的就业有很大的帮助。

本书以作者多年网络设备配置的工作经历与教学经验为基础，以 Cisco 设备为平台，以校园网网络平台管理项目为中心，详细讲解了网络设备在网络系统集成中的规划、实施、管理和维护，如网络设备的管理、交换网络的优化、网络间互联和广域网连接等内容。本书内容全面，讲解精练，图文并茂，结构清晰，突出了实用性和可操作性。本书在编写风格上尽量避免枯燥、空洞的理论堆砌，使读者容易上手，在不知不觉之中掌握网络设备的管理与网络应用的方法和技巧，是一本不可多得的网络技术参考书。

本书采用“任务驱动”的案例教学方式，根据校园网项目实施过程进行介绍。每章都先给出需要完成的任务目标，然后介绍为实现该目标而所需的基本技能，最后通过详细步骤完成本章的学习任务。通过这种安排，教师可通过任务引导学生进行实际操作，力求减少实用性不强、晦涩枯燥的理论讲解，能够让学生体验形象直观、生动有趣的知识学习和技能训练的过程。

针对初学者的特点，本书在编排上注意由简到繁、由浅入深和循序渐进，力求通俗易懂、简捷实用。本书概念清晰、逻辑性强、层次分明、实例丰富，非常适合教师教学和学生学习。全书图文并茂，所有操作都依据实际效果显示一步一步讲述，读者可以边看书边上机操作，通过范例和具体操作，理解基本概念和学会操作方法。

为了保证全书内容的实用性和可操作性，本书所有例子和项目实施都使用 Cisco Packet Tracer 模拟器搭建实验环境，方便了学生的课后学习。为了能够让学生更方便地对书上的实验进行验证，本书所有实验内容都可以在思科的 Cisco Packet Tracer 模拟器上进行操作。

本书由上海电子信息职业技术学院的邱洋、计大威担任主编，胡国胜、张迎春、蔡军英担任副主编，全书由邱洋统稿。另外，参与本书编写的还有胡敬华、周巧婷、张月红、范晓燕等。

为了方便教师教学，本书配有电子教学课件及相关资源，请有此需要的教师登录华信教育资源网（www.hxedu.com.cn）注册后免费进行下载，如有问题可在网站留言板留言或与电子工业出版社联系（E-mail:hxedu@phei.com.cn）。

教材建设是一项系统工程，需要在实践中不断加以完善及改进，由于编者水平有限，书中难免存在疏漏和不足之处，恳请同行专家和读者能给予批评和指正。

编　者

目录
Contents

第1章 认识网络

计算机网络是指将地理位置不同的具有独立功能的多台计算机及其外部设备，通过通信线路连接起来，在网络操作系统、网络管理软件及网络通信协议的管理和协调下，实现资源共享和信息传递的计算机系统。

随着信息化社会的不断推进，目前的社会处在一个信息爆炸的时代，网络已成为我们身边必不可少的工具。计算机网络技术的发展深刻地影响了人类的生活，为信息的传播带来了新的动力。信息传递从原始的口传到后来训练信鸽进行飞鸽传书，再开始利用简单的信号原理使用烽火台、孔明灯经历了一代又一代的变革，到今天终于进入了网络信息时代。生活在今天的人们已经充分认识到信息的重要性，因此各种信息传播和信息共享技术就成了热门的技术。

在学习了计算机网络的相关基础知识以后，如何设计、规划和组建各种实用的计算机网络，通过网络间的互联为用户提供高效的网络服务和信息共享就成为一种重要的职业追求，这一类职业有哪些技术素质，怎样开展这一类工作呢？本书将以一个校园网项目为载体，带领大家学习网络设备的配置与管理知识。

1.1 网络体系结构

计算机网络是一个复杂的具有综合性技术的系统，为了允许不同的系统实体互联，在通信时都必须遵从相互均能接受的规则，这些规则的集合称为协议（Protocol）。计算机网络体系结构为不同的计算机之间互联提供相应的规范和标准。

1.1.1 OSI/RM 模型

在 20 世纪 80 年代末和 90 年代初，网络的规模和数量都得到了迅猛的增长，但是许多网络都是基于不同的硬件和软件而实现的，这使得它们之间互不兼容，而且很难在使用不同标准的网络之间进行通信。

为了解决这个问题，国际标准化组织 ISO（International Organization for Standardization）

提出了网络模型方案以标准方式帮助规范厂商生产相互操作的网络产品，于 1984 年发表了 OSI/RM 参考模型，它是 ISO 在网络通信方面所定义的开放系统互连模型。有了这个开放的模型，各网络设备厂商就可以遵照共同的标准来开发网络产品，最终实现彼此兼容。

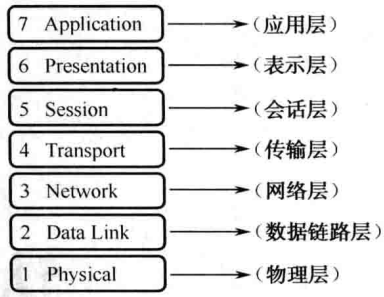


图 1-1　OSI/RM 模型

整个 OSI/RM 模型共分 7 层，从下往上分别是：物理层、数据链路层、网络层、传输层、会话层、表示层和应用层。

1.1.2　OSI/RM 模型各层的功能

当接收数据时，数据是自下而上传输；当发送数据时，数据是自上而下传输，下面简要介绍这几个层次。

（1）物理层

OSI 参考模型的最低层，它的任务就是提供网络的物理连接，所以物理层是建立在物理介质上（而不是逻辑上的协议和会话）。它提供的是机械和电气接口，主要包括电缆、物理端口和附属设备，如双绞线、同轴电缆、接线设备（如网卡等）、RJ-45 接口、串口和并口等在网络中都是工作在这个层次的。

物理层提供的服务包括：物理连接、物理服务数据单元顺序化（接收物理实体收到的比特顺序，与发送物理实体所发送的比特顺序相同）和数据电路标识。

（2）数据链路层

数据链路层是建立在物理传输能力的基础上，以帧为单位传输数据，它的主要任务就是进行数据封装和数据链接的建立。封装的数据信息中，地址段含有发送节点和接收节点的地址，控制段用来表示数格连接帧的类型，数据段包含实际要传输的数据，差错控制段用来检测传输中帧出现的错误。

数据链路层的功能包括：数据链路连接的建立与释放、构成数据链路数据单元、数据链路连接的分裂、定界与同步、顺序和流量控制，以及差错的检测和恢复等方面。

（3）网络层

网络层属于 OSI 中的较高层次了，它解决的是网络与网络之间，即网际的通信问题。网络层的主要功能即是提供路由，即选择到达目标主机的最佳路径，并沿该路径传送数据包。除此之外，网络层还要能够消除网络拥挤，具有流量控制和拥挤控制的能力。

网络层的功能包括：建立和拆除网络连接、路径选择和中继、网络连接多路复用、分段和组块、服务选择和传输，以及流量控制。

（4）传输层

传输层解决的是数据在网络之间的传输质量问题，它属于较高层次。传输层用于提高网络层服务质量，提供可靠的端到端的数据传输，如常说的 QoS 就是这一层的主要服务。这一层主要涉及的是网络传输协议，它提供的是一套网络数据传输标准，如 TCP 协议。

传输层的功能包括：映像传输地址到网络地址、多路复用与分割、传输连接的建立与释放、分段与重新组装、组块与分块。

（5）会话层

会话层利用传输层来提供会话服务，会话可能是一个用户通过网络登录到一个主机，或一个正在建立的用于传输文件的会话。

会话层的功能主要有：会话连接到传输连接的映射、数据传送、会话连接的恢复和释放、会话管理、令牌管理和活动管理。

（6）表示层

表示层用于数据管理的表示方式，如用于文本文件的 ASCII 和 EBCDIC，用于表示数字的 1S 或 2S 补码表示形式。如果通信双方用不同的数据表示方法，他们就不能互相理解。表示层就是用于屏蔽这种不同之处。

表示层的功能主要有：数据语法转换、语法表示、表示连接管理、数据加密和数据压缩。

（7）应用层

这是 OSI 参考模型的最高层，它解决的也是最高层次，即程序应用过程中的问题，它直接面对用户的具体应用。应用层包含用户应用程序执行通信任务所需要的协议和功能，如电子邮件和文件传输等，在这一层中 TCP/IP 协议中的 FTP、SMTP、POP 等协议得到了充分应用。

1.1.3 数据的封装和解封装过程

数据在网络上传输的过程中，为了使数据能够被顺利、正确地传送到目的地，需要对数据进行包装，称为数据的封装（Encapsulation），即将协议数据单元（PDU）封装在一组协议头和尾中的过程。在 OSI 7 层参考模型中，每层主要负责与其他机器上的对等层进行通信。该过程是在“协议数据单元（PDU）”中实现的，其中每层的 PDU 一般由本层的协议头、协议尾和数据封装构成。

在发送端，数据的封装是按照 OSI 参考模型自上而下层层封装的，每层都会添加一些特定的控制数据传输的信息，称为包头，如图 1-2 所示。

从应用层来的数据流到达传输层时，被分割成一个个便于传输的数据段，传输层对每个数据段单独进行封装，然后再传给网络层。网络层把上层传递下来的整个内容——包含数据和包头，看做自己的数据再次对其封装。数据链路层把来自网络层的数据包再次封装，这次不但增加了帧头，还在尾部增加了帧的附加部分（Trailer），这部分携带的是数据的校验值。

经过层层封装的数据在物理层以比特流的方式传送出去。

因为每一层所完成的任务不同，所以每层加入的信息也不相同，这也正是为什么要进行多层封装的原因。

在接收端，主机要想知道对方传输来的真实信息，需要自下而上一层一层地把包头和尾去掉，最终复原数据，这个过程叫解封装。

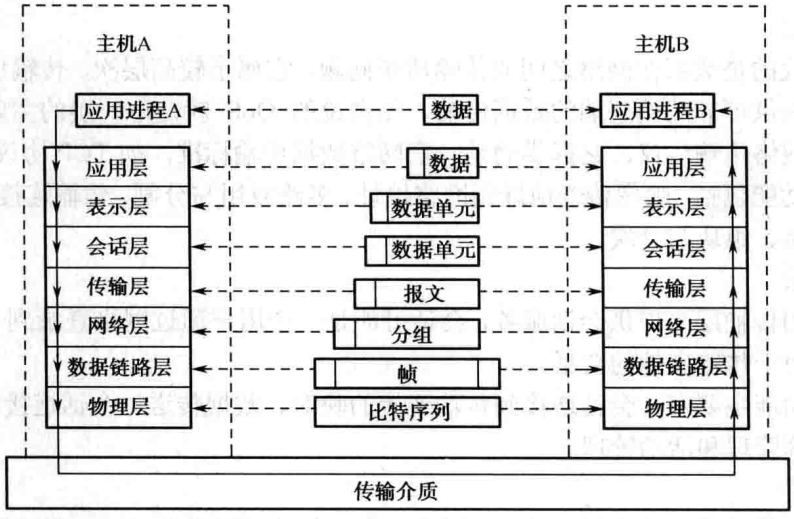


图 1-2　数据的封装与解封装

在特定层次上的包含数据和包头的数据单元称为协议数据单元(Protocol Data Unit, PDU),并给它们命名:

- 传输层以上的 PDU 称为数据;
- 由于在传输层对数据进行了分段,所以第 4 层的 PDU 称为“段”(Segment);
- 网络层的 PDU 称为数据包(Packet);
- 数据链路层的 PDU 称为帧(Frame);
- 物理层的 PDU 称为比特(Bit)。

1.1.4　网络设备在层次模型中所处的位置

- 中继器(Repeater):工作在物理层,在电缆之间逐个复制二进制位(bit);
- 交换机(Bridge):工作在链路层,在 LAN 之间存储和转发帧(frame);
- 路由器(Router):工作在网络层,在不同的网络之间存储和转发分组(packet)。
- 协议转换器(Gateway):工作在三层以上,实现不同协议的转换。Internet 中通常把路由器也叫网关(Gateway)。

本书的主要内容就是介绍交换机和路由器这两种设备的配置和管理。

工作在各层的网络设备如图 1-3 所示。

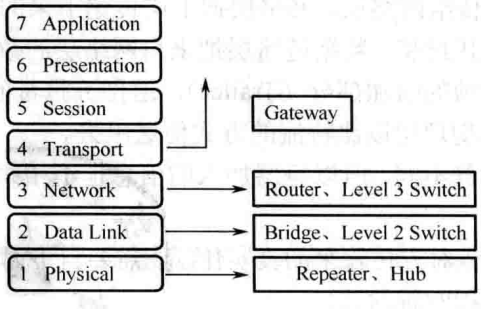


图 1-3　工作在各层的网络设备

1.1.5 TCP/IP 协议

TCP/IP 协议是互联网中实际使用的协议，也就是说，没有一个操作系统是按照 OSI 协议的规定编写自己的网络系统软件，而都是按照 TCP/IP 协议要求编写的。OSI 模型和 TCP/IP 模型的比较如图 1-4 所示。

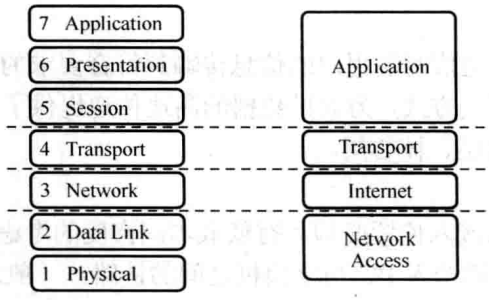


图 1-4 OSI 模型和 TCP/IP 模型的比较

TCP/IP 协议的层次并不是按 OSI 参考模型来划分的，只跟它有一种大致的对应关系。TCP/IP 协议是一个协议集，它由十几个协议组成，其中的两个重要协议：TCP 协议和 IP 协议。图 1-5 是 TCP/IP 协议集中各个协议之间的关系。

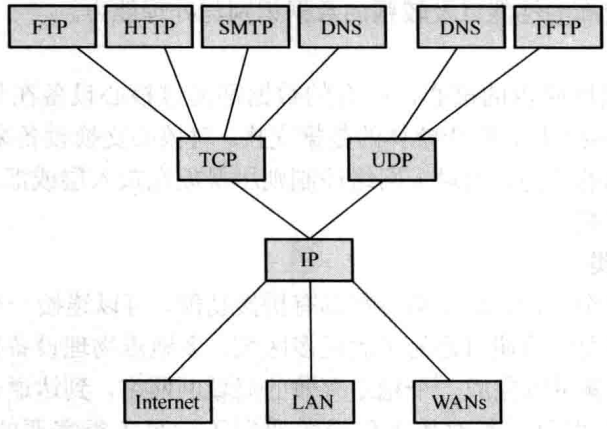


图 1-5 TCP/IP 协议集中的协议

TCP/IP 协议集给出了实现网络通讯第三层以上的协议，主要的 TCP/IP 协议如下。

① 应用层：FTP、TFTP、Http、SMTP、POP3、SNMP、DNS、Telnet。

② 传输层：TCP、UDP。

③ 网络层：IP、ARP（地址解析协议）、RARP（逆向地址解析协议）、（DHCP 动态 IP 地址分配）、ICMP（Internet Control Message Protocol）、RIP、IGRP、OSPF（属于路由协议）。

POP3、DHCP、IGRP、OSPF 虽然不是 TCP/IP 协议集的成员，但是都是非常知名的网络协议，因此仍然把它们放到 TCP/IP 协议的层次中来，可以更清晰地了解网络协议的全貌。

1.2 认识常用设备

1.2.1 交换设备

1. 交换设备的作用

交换（Switching）是将通信两端用户的信息传输到符合要求的相应位置的技术统称，这是种快速、高效与低成本的解决方式，为大量数据的高速传递提供了可行性，通常将网络分为三个层次称为：接入层、汇聚层、核心层。

（1）接入层

接入层通常指最底层的接入位置必须具有低成本高密度的考虑，就是用户使用个人 PC 将网线插入 PC 的网卡从而连通个人 PC 与交换机之间的链路。一般这个位置的交换机就称为接入层交换机，只需要满足即插即用的网络设备能力，这样易于网络工程师对于整体网络的维护与保障。

（2）汇聚层

汇聚层指的是，大量相同行为的用户，发出的数据通过接入层交换进入内网网络，转交给核心网络设备，并对核心网络进行保护与协助，完成这项任务的交换机称为汇聚层交换机。在这一层中接入层交换较高的性能以及较强的数据识别与处理能力。

（3）核心层

核心层交换通常是网络内的核心，所有的数据都通过核心设备在骨干网络中进行高速交换，之后再从汇聚层到接入层，完成整体的数据交换。对核心交换设备来说冗余能力、可靠性、转发效率都是重点考虑的能力，而对于网络控制则尽量放在接入层或汇聚层，以便降低网络控制对核心设备能力的影响。

2. 交换设备的种类

接入层交换采用多个端口，每个端口都具有桥接功能，可以连接一个局域网或一台高性能服务器或工作站。采用大量的端口是为了满足多区域、多地点物理设备接入的需要，只需要将预设的网线接入设备，就可以完成一个稳定有效的局域网网络，到达通信的目的。目前主流的设备厂商分别是华为与思科，都对接入层设备研发了满足各类需要的接入层交换设备。如图 1-6 所示。

图 1-6　接入层交换机

汇聚层通常是网络内，楼宇之间的网络连接。通常会采用携带路由功能的三层交换进行连接沟通。其目的是为了在保证数据交换快速的前提下。可以使用路由技术进行数据转发，使用户可以进行远端目的地的访问请求。汇聚层在接入层与核心层之间形成桥梁。可以处理一些局域网连通选路，而无需使用核心交换的转发能力。并为核心网络提供有限的网络保障能力。

图 1-7 为常见的汇聚层交换设备。

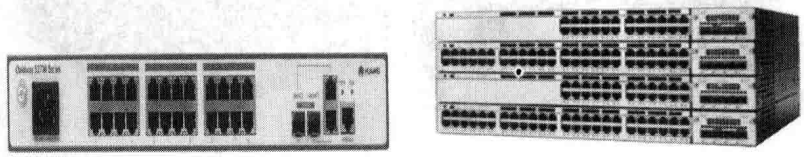


图 1-7 汇聚层交换机

核心层主要考量的就是对核心网络冗余性，以及安全可靠的网络数据传输保障。并在此基础上对网络的高速传输，进行最大程度上的提高，可以说核心网络传输不存在网络安全方面的考虑，只是对于物理设备进行保护，所有安全问题都将在接入层与汇聚层之间展开，但核心层无疑是占整个网络投资的重中之重，如图 1-8 所示。

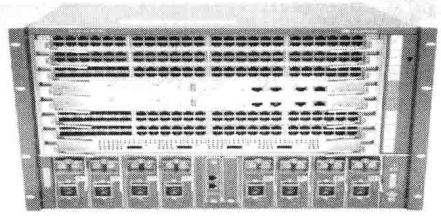


图 1-8 核心交换机

1.2.2 路由设备

1. 路由设备的作用

路由从字面解释就是，在道路上行走，而如何走上正确的道路，就是路由器需要做的任务。路由器做的最基本的两个动作就是，首先通过不同协议确定最短且正确的道路，其次就是如同交换一样进行转发，并带上正确的数据转发信息。

路由器一般位于网络出口，作为整体网络的网关，对公司外围网络进行数据传输，并在一定程度上防止外围网络对内进行的各种攻击，其在数据传输能力上无法与交换机相提并论，当路由能力毋庸置疑使其可以完全胜任网关的能力。

2. 路由设备的种类

目前一般公司内部采用两种路由设备，一种为网关路由器，另一种更趋向于接入层的无线路由器。两者侧重点不同，网关路由器通常只对整体网络与外网沟通负责，并对网络进行简单的防护与控制，而无线路由器面向的是在物理线路无法覆盖到的地方进行网络部署，方便网络管理人员对于网络进行控制。

路由器与交换机相同，也采用多个接口相互通信，但每个接口之间都是通过使用 IP 地址进行数据的交互，就如同邮局按照邮编以及地址等数据，进行收发邮件，图 1-9 为基本功能的网关型路由器。

无线路由器就是增加了无线功能的路由器，使用户可以安全快捷地接入已经配置完成的网络中，而无需再次进行物理布线等繁琐操作，从而大大减少了在接入层范围内，由于设计等原因导致的物理网络线缆无法完全覆盖而导致的一系列问题，节约了大量的物理线路成本，也更符合当今社会的移动办公的模式，图 1-10 为无线路由器。

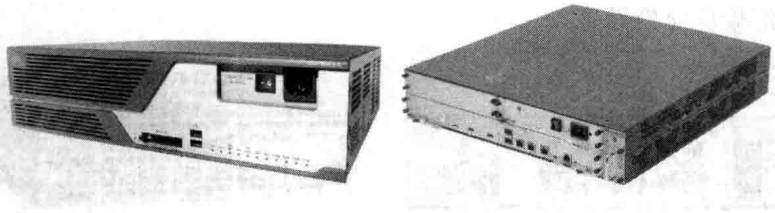


图 1-9　路由器

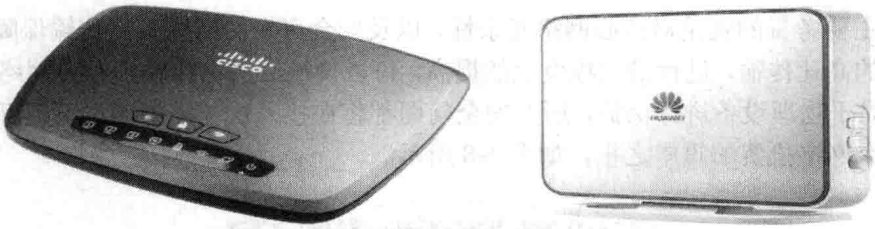


图 1-10　无线路由器

1.2.3　安全设备

防火墙在内部与外部网络之间、专用与公用网络之间的一层屏障。这是一种是通过软件硬件叠加的方式，进行安全防护的设备。并能扩展与衍生出例如：VPN、流量统计、日志记录、流量监控等各类特殊应用。所有进出网络的数据都必须要经过防火墙的审查、修改、记录等行为。才能被认定为此数据是安全可靠可以使用的。根据安全定义，防火墙适用于网络边界等，相当于路由网关的位置。其自身的安全抗打击能力是非常强的。

使用此种设备，当外部非法用户攻击内部网络时进行内网安全保障的设备，这是企业内网安全的第一面盾牌，通过对于数据流的分析，网络管理人员可以对于目前公司内部所使用的地址与端口进行了解，关闭不使用的端口从而在最大限度上的保护整体网络的通信安全，图 1-11 为防火墙设备。

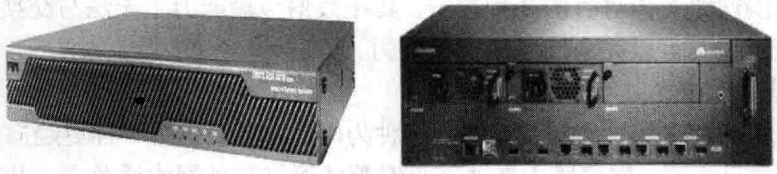


图 1-11　防火墙

虽然防火墙设备可以集成各类特殊应用进行数据处理，但由于大量的数据再经过防火墙处理时，其本身就承担了巨大的数据压力，这将导致整体网络数据处理速度缓慢，这是绝对不会允许的，所以就出现了专门的网络安全设备，例如：入侵检测系统 IDS（Intrusion Detection Systems）、入侵防御系统 IPS（ Intrusion Prevention System）。而防火墙只是将所有数据进行拷贝传输到类似于模拟拓扑中的监控区域进行数据检查和处理，这样在不影响数据处理的前提下，仍然做到了安全可控的行为，图 1-12 为入侵防御和入侵检测设备。