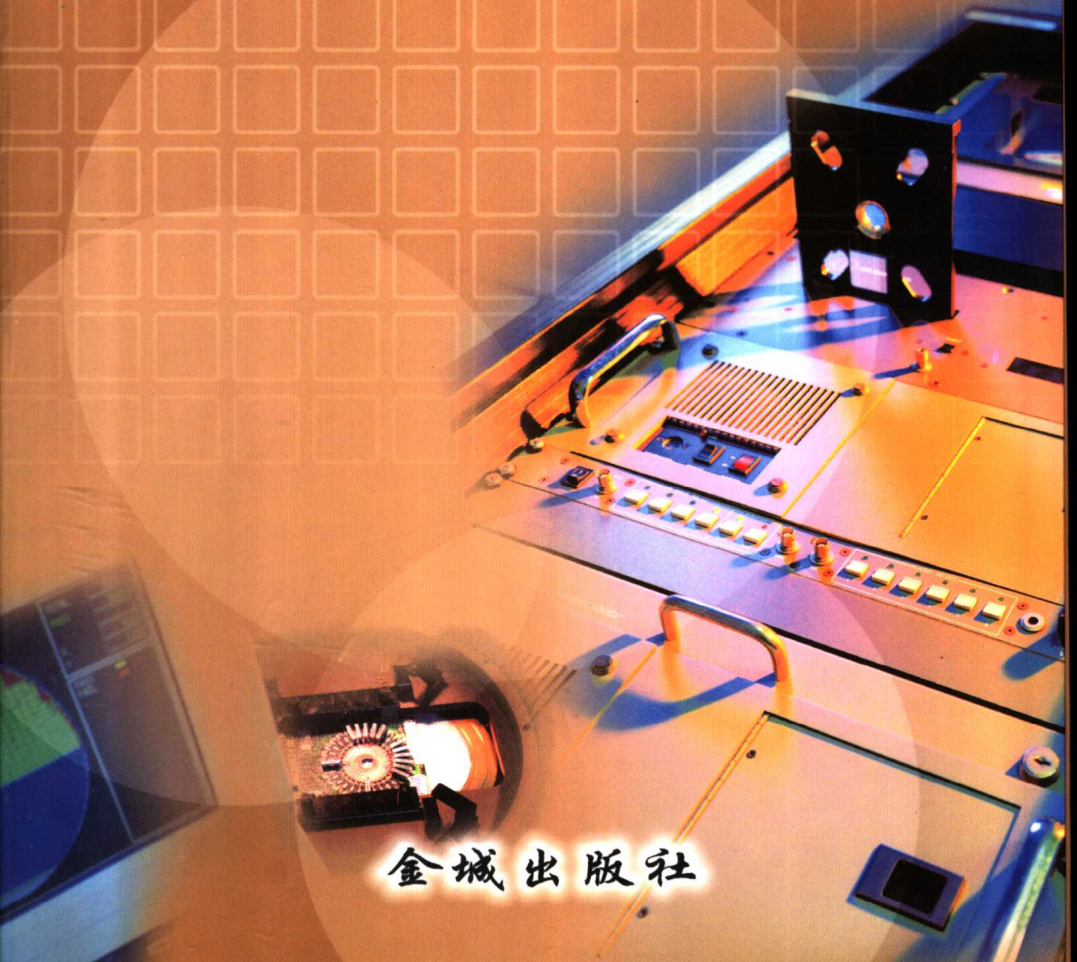
涉密信息系统建设实务

● 杨世松　主编



金城出版社

涉密信息系统建设实务

主　编：杨世松

副主编：王大会　王连海　韩忠林　陈南轩

编　委：（以姓氏笔划为序）

王　涛　白　桦　刘亚光　孙德军

张　林　张劲松　陈　晨　邵广纪

赵　征　侯风华　贾保平　贾耀刚

高志成　董红勋　潘冬存

金城出版社

图书在版编目（CIP）数据

涉密信息系统建设实务/杨世松等编著．－北京：金城出版社，2002.10

ISBN 7－80084－437－4

Ⅰ.涉… Ⅱ.杨… Ⅲ.①电子计算机－信息系统－系统开发 ②电子计算机－信息系统－系统管理 Ⅳ.TP3

中国版本图书馆 CIP 数据核字（2002）第 070323 号

金城出版社出版发行

（北京市朝阳区和平街 11 区 37 号楼 100013）

中国农业出版社印刷厂印刷

850×1168 毫米 1/32 8.375 印张 190 千字

2002 年 10 月第 1 版 2002 年 10 月第 1 次印刷

印数：1－5000 册

ISBN 7－80084－437－4/TP·15

定价：15.00 元

出版说明

保密技术防范是保密工作的一项重点工作，涉密计算机信息系统的建设与管理更是重中之重。为加强涉密计算机信息系统的建设与管理，国家保密局制定了一系列法规、标准，明确了要求和程序。但由于此项工作刚刚起步，特别是各地、各部门情况各异、问题不一，在实际工作中暴露出来的问题，还需要在实践中解决，在理论上完善。目前，有关涉密计算机信息系统的建设、审批工作的综合性业务用书还比较缺乏，无法满足工作的需要。为此，我们不揣鄙陋，策划编辑了《涉密信息系统建设实务》一书，以期对涉密计算机信息系统的建设与管理提供一定的借鉴和参考。本书观点不代表国家保密局，只是作为一家之言与读者作一交流。由于缺乏较为成功的经验，加之编著者水平有限，书中的某些表述和观点可能存在疏漏不当之处，敬请方家指正，更愿意就此与有识之士作进一步的探讨，以期再版时能将一部更为完善的作品呈现给广大读者。

目　录

第一章　网络安全保密概说 …… (1)

第一节　网络的结构与功能 …… (2)
第二节　网络安全保密面临的威胁 …… (25)
第三节　国外网络安全保密工作的发展状况 …… (42)
第四节　保密工作部门在涉密信息系统安全保密工作中的职责 …… (49)

第二章　涉密网络的规划与建设 …… (54)

第一节　涉密网络的设计原则 …… (54)
第二节　信息安全保密体系结构 …… (65)
第三节　涉密网络的物理安全 …… (75)
第四节　涉密网络的运行安全 …… (80)

第三章　涉密网络的安全保密技术 …… (94)

第一节　安全操作系统 …… (94)
第二节　身份鉴别与验证 …… (98)
第三节　访问控制 …… (108)

第四节　信息加密技术……（113）
第五节　防火墙技术……（122）
第六节　审计跟踪……（126）
第七节　电磁辐射防护……（130）
第八节　数据库安全保密技术……（135）
第九节　网络安全检测技术……（141）

第四章　涉密信息系统的集成资质……（148）

第一节　涉密系统集成单位的资质审批……（148）
第二节　资质等级介绍……（152）

第五章　涉密计算机信息系统的保密管理……（161）

第一节　强化安全管理机构……（161）
第二节　落实安全管理制度……（164）
第三节　健全网络安全保密管理措施……（173）
第四节　加强对涉密网络工作人员的管理……（182）

第六章　涉密计算机信息系统的审批……（185）

第一节　审批概述……（185）
第二节　审批程序……（189）
第三节　审批内容……（195）
第四节　其他有关内容的审查……（199）

第七章　电子政务与安全保密……（209）

第一节　电子政务建设中的安全保密问题……（210）
第二节　电子政务的安全保密管理……（218）

第八章　运用法律手段，保障和促进信息网络发展
…… (224)

第一节　网络安全保密的方针、原则 …… (224)
第二节　依法管理涉密计算机信息系统 …… (230)
第三节　依法防范、查处网上泄密行为 …… (244)

后　记 …… (257)

第一章　网络安全保密概说

我们的世界正在演变为一个电子化的世界（E—WORLD），所有的信息正在全面数字化，电子世界中四通八达的网络把全球连在一起。与此同时，信息安全保密问题，显得越来越重要。计算机网络作为国家的关键基础设施和战略命脉，其安全保密状况直接关系着国家的安全与发展。信息安全保密将是21世纪最重要的课题之一。自网络出现以来，计算机网络系统曾遭到几十万次入侵与攻击，其中不仅有政府系统网络，也有私人公司网络系统。计算机及其网络因自身的脆弱性、技术的垄断性以及人为破坏等，给人类带来许多安全问题。

据国家信息安全课题组的《国家信息安全报告》介绍，20世纪90年代以来，我国的信息产业和技术及互联网络等虽然获得了突飞猛进的发展，但在信息安全领域还存在许多问题和缺陷。如以9分为满分计算，我国信息安全综合得分只有5.5分，介于相对安全和轻度不安全之间。我国未来发展目标是国民经济信息化和社会信息化，而国家信息安全体系的建设是我国信息化目标实现的重要保障。

第一节　网络的结构与功能

信息网络化的迅速发展，对政治、经济、军事、科技、文化、社会各领域产生了深刻的影响。我们要抓住信息网络化发展带来的机遇，加快发展我国的信息技术和网络技术，并在经济、社会、科技、国防、教育、文化、法律等方面积极加快运用。同时，我们也要高度重视信息网络化带来的严峻挑战。国家之间的经济实力、国防实力和政治实力越来越集中在信息技术及信息产业的竞争上。政治、经济、文化、科技领域中的情报战愈演愈烈，而且手段越来越先进，形式越来越隐蔽，小到商业情报的窃取，大到国家秘密的侦获，无不危及到国家安全。在论及网络安全保密时，我们先介绍一下网络的基础知识。

互联网最早产生于20世纪60年代。当时，美国国防部高级研究计划局负责寻找一种最佳方法来互连许多电脑网点。其实际目的是对付苏联的核威胁，将一些与国防中心有关的网络链接起来，并能经得住一次核打击的破坏。该计划局向BBN公司提供一笔研究资金，来探索研究计算中心之间的通信方法，以期在受到一次性核打击后，军用设备能够尽快恢复工作。1969年，BBN公司提出了被称为网络控制协议的分组交换网络协议，并设计了控制电脑的网络。同年，第一台信息报文处理器安装成功。1970年，美国第一个分组交换电脑网阿帕网投入运行。该网络将位于美国不同地区的四所大学连接起来，这就是互联网的开端。70年代，以阿帕网为基础的以太网开始应用于大学校园。现在，互联网已把全球联成一个巨大的网络。据预测，到2005年，使用互联网的人数将高达10亿。

一、网络的含义

网络是通过网络介质彼此进行通信的计算机和其他设备的集合。“网络”一般有三层含义：一是指信息网络；二是指计算机网络；三是指互联网。

信息网络是一个国家乃至全球的信息基础设施，它综合了一国或全球现有的通信网络、计算机网络以及广播电视网络等。信息网络是一种分层的结构，可对其进行横向和纵向的描述。从横向上可划分为骨干网、接入网和用户住地网。从纵向上可划分为应用网、业务网和传送网三个层次。

计算机网络是指在协议规约的控制下，将分布在不同地点的若干计算机、终端设备、数据传输设备和通信控制处理设备等通过通信线路互相连接起来，实现资源共享和信息交换的网络。它是计算机与通信相结合而形成的网络，其目的是在计算机之间、计算机与终端设备之间实现信息的交换。

互联网（INTERNET）是一个特定的世界性的网络，它是连接全球各种局域网及广域网所形成的国际最大的计算机通信网络集合体。互联网是一个包含丰富资源的联机服务网络，能提供包括电子公告牌、新闻组、电子邮件和最新消息在内的各种信息。

这里重点介绍计算机网络的构成要素。一般说来，一个计算机网络通常由以下部分组成。

1. 物理设备：包括主计算机、客户机等服务器，终端、通信处理机、通信线路等。

2. 软件：包括网络应用软件、操作系统等。

3. 共享资源：计算机硬件资源、网络型打印机、软件资源、数据资源等。

计算机网络互联是为了将不同的网络或相同的网络用互联设

备联接在一起，形成一个更大的网络；或为了增加网络的性能和便于管理而将一个很大的网络划成几个子网或网段。常用的网络互联和组网的要素有：

1. 设备。网络互联的设备主要有：

（1）网络适配器（Network Adapter，简称网卡）。它插在计算机主板槽中，一方面通过总线接口与计算机设备相连；一方面又通过电缆接口与网络传输媒介相连。

（2）中继器（Repeater）。这是用来延伸网络距离的实用设备。

（3）集线器（HUB）。这是一种特殊的中继器。它作为网络传输介质间的中央节点，是一个信号再生转发的设备。

（4）网桥（Network Bridge）。用来联接两个相同网络操作系统。

（5）路由器（Router）。当两个以上的同类网络互联时，必须选用路由器。路由器不仅具有网桥的全部功能，还可以根据传输费用、网络拥塞情况以及信息源与目的地的距离等不同情况自动选择最佳路径来传送数据包。

（6）网关（Gateway）。在不同网络操作系统的计算机网络互联时，要用网关来完成不同协议之间的转换。

（7）交换机（Switch）。是网络中用于交换信息的核心设备。它为每个终端站提供独占的点对点链路，同时支持通信设备间的多条链路，可分为帧交换机和信元交换机等。

（8）服务器（Server）。可分为文件服务器、打印服务器和通信服务器。文件服务器能将大容量磁盘空间提供给网上客户，接收客户机提出的数据处理和文件请求，向用户提供各种服务。打印服务器接收来自客户机的打印任务。通信服务器主要用于网与网之间的通信和提供调制解调器等多种接口。

（9）客户机（Client）。又称工作站，是网络的前端窗口。用户通过它来访问网络的共享资源。它与终端的主要区别是具有对数据进行处理的能力。每一个客户机都运行在它自己的、并为服务器所认可的操作系统环境中。

2. 传输介质。即用于计算机网络传输数据的物质，例如光缆、电缆、大气等。按传输介质性质划分，计算机网络数据通信有：有线通信、光纤通信、无线通信和卫星通信四种。常用传输介质有：

（1）双绞线。两根铜线按一定的密度互相绞在一起，可以减少串扰及信号放射影响的程度，每一根导线在导电传输中发出的电波会被另一根线上发出的电波所抵消。这是一种价格低廉、易于联接的传输介质。虽然传输距离一般只有数百米，但它非常适合于局域网的联接，尤其适合于在机关或学校的一座办公楼范围内使用。

（2）同轴电缆。这种电缆以单根导线为芯，周围是绝缘材料层，再向外是一层直径较大的管状导体，一般为铜的辫状编织线，最外边是一层绝缘材料。其传输速度与双绞线差不多，但它的抗干扰性较强，同时它的联接也不太复杂。

（3）光缆。这是用硅石构成的很多细丝，其外面用一种折射率低的物质材料包起来而组成的特殊“电缆”。它一般不受外界电场和磁场的干扰，不受带宽限制，可以实现高达数千兆/秒（1000Mbps 以上）的传输速率，而且尺寸小、重量轻，传送距离远，是一种较为理想的通信介质，其应用也较广，是敷设信息高速公路的主要材料。

3. 软件。软件包括网络应用软件、操作系统。网络应用软件即协议。网络互联需要有一个规划或一组规则和标准。协议就是规则，它帮助实体之间、网络之间相互理解和正确进行通信。

语法、语义和同步是协议的关键因素。

操作系统是一个大型的系统软件。它直接运行在裸机之上，是硬件的第一级扩充。任何软件的运行都必须依靠操作系统的支持。其主要的目的是控制与管理计算机的硬件和软件资源，合理地组织计算机工作流程，方便用户使用计算机。

网络操作系统是运行在计算机上的网络高层软件，它执行网络协议，负责计算机间的信息交换，并对网络资源进行统一管理。网络操作系统必须有相应的安全措施，否则是不能使用的。

二、网络的结构与分类

网络的结构主要有：

（一）常用的网络拓扑结构

1. 总线拓扑。由多台计算机共享单一传输介质的网络结构，称之为总线拓扑结构（见图 1－1）。

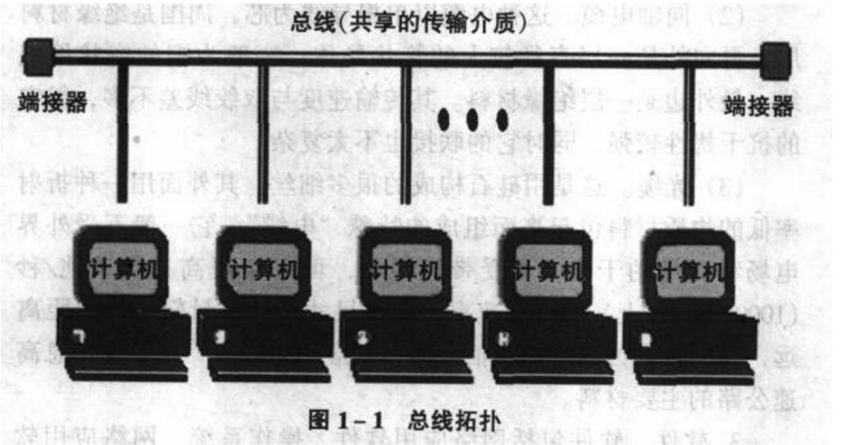


图 1－1　总线拓扑

在这一环境下，当一台计算机向另一台计算机传送数据时，总线上的其他计算机必须等待。当数据呈广播方式沿着总线传送

时，其他计算机均可监听、查看这个数据的地址，按照网络协议的规定，它们只取走属于自己的信息。采用细缆（同轴电缆）连接的以太网结构就是一种典型的总线拓扑结构。总线型结构简单、费用低，但可靠性差，网络上的每个部件均可影响整个网络的正常工作。信息安全性较差。

2. 环状拓扑。由多台计算机通过共享的传输介质依次相连，首尾相接，形成一个封闭的圆环，这种网络结构称为环状拓扑结构（见图 1－2）。

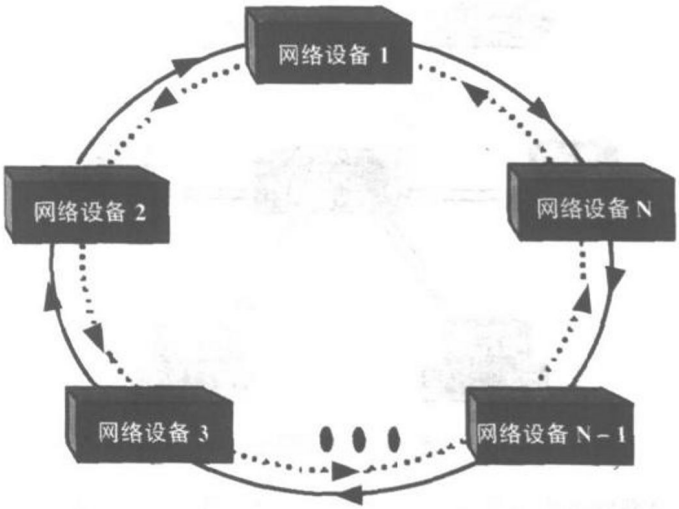


图 1－2　具有双环结构的环状拓扑

环状网络使用一种令牌传送的存取机制，环上只有一个令牌，令牌和数据都是绕环上逐个节点传递的。为了发送数据，计算机必须先持有令牌，然后发送一个基本单位（帧）的数据。当这一数据发送过程结束后，令牌向下一台计算机传递，开始新的数据传输过程。FDDI 环状网络就是环状拓扑的一个应用实例。

环状网络具有可靠性高、负载能力强的特点，适用于覆盖范围大的网络，如：园区之间、城市的区之间、城市之间。但是环状网络设备价格高，没有适合网络管理的中心点，同时信息的安全性较差。

3. 星型拓扑。由多台计算机通过各自独占的传输介质连接在一个中心节点上，这种像车轮轮辐的网络结构，称为星型拓扑结构（见图 1－3）。

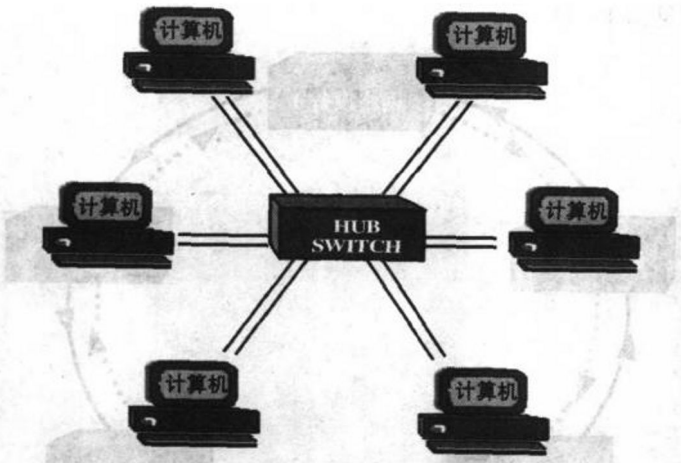


图 1－3　星型拓扑

星型网络中心节点上的设备是一台交换机（Switch）或集线器（HUB）。星型结构具有结构合理、可靠性高、适应能力强、信息安全性好、便于扩充的优点，同时，还具有便于对网络进行管理的优点。星型拓扑已成为主要流行的网络结构。

4. 网状拓扑。每个网络节点使用两条或两条以上传输介质与其他网络节点相连而构成的网络，称为网状拓扑结构（见图 1－4）。这种网络结构造价昂贵，可靠性高，具有很强的容错能

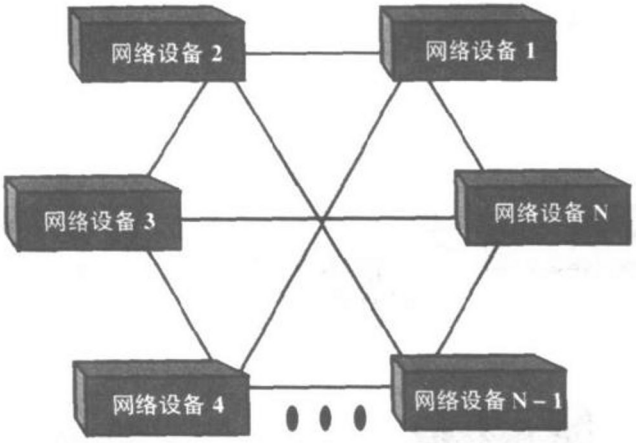


图 1－4　网装拓扑

力，但信息的安全性较差。主要用于跨地区的大型网络结构或某些可靠性要求很高的场合。

5. 拓扑结构形态的变化。每种单一的拓扑结构都有各自的优缺点，事实上，每一个实际应用的拓扑结构都是根据实际的需求和经费的多少等因素进行综合设计的。因此，网络的结构形态也会在应用中发生一些变化。需要说明的是，拓扑结构一般分为物理和逻辑两种意义上的拓扑结构。前面所描述的各种拓扑结构主要是指逻辑意义上的拓扑结构。图 1－5 所示的网络结构，在物理上是星型结构，而在逻辑上是环状结构，这种结构是在采用环状网络设备的基础上考虑到今后向 ATM 或千兆以太网升级而采用的拓扑结构。结构与设备是确定网络性能的两个主要方面。

（二）基本的广域网网络拓扑结构

广域网一般是通过路由器和 X.25、DDN、FR、卫星等访问介质将各局域网连接起来，并通过 OSPF、RIP 等协议实现整个网络的路由选择等功能（见图 1－6）。

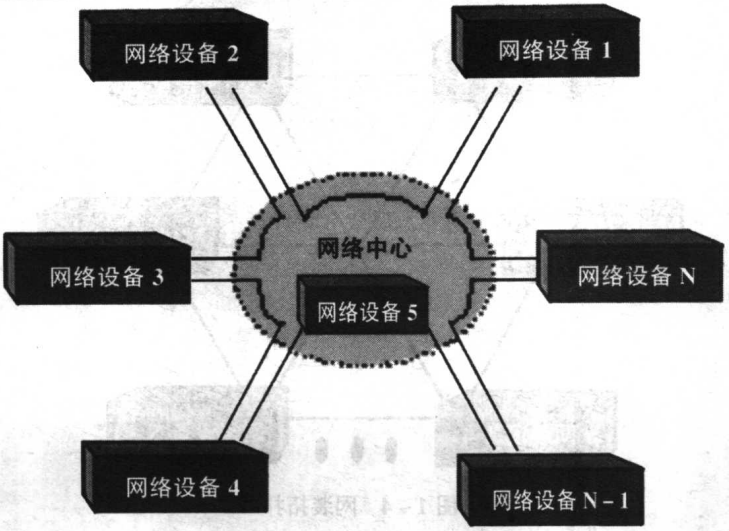


图 1－5　一种实际应用的网络拓扑结构

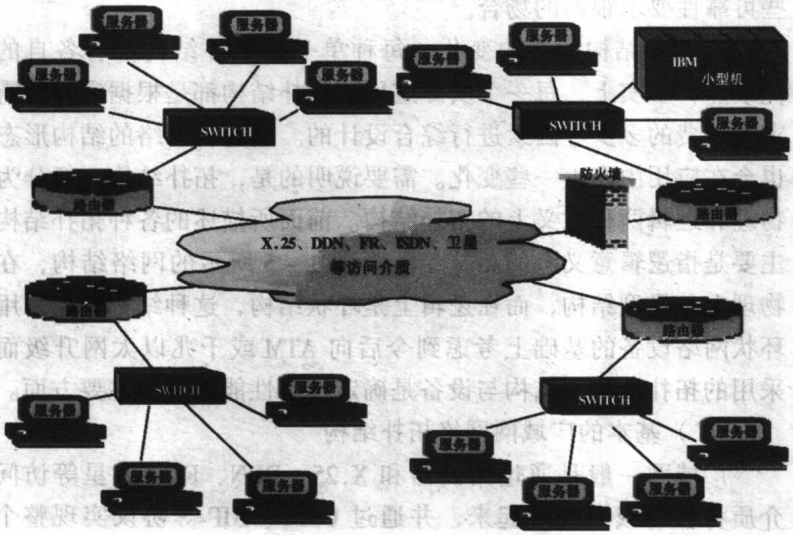


图 1－6　基本的广域网网络拓扑结构