网络安全保密基础

軍事科学出版社

网络安全保密基础

主　编　蔡　红

副主编　杨世松　崔书昆

主　审　曲成义

军事科学出版社

（京）新登字 122 号

图书在版编目（CIP）数据

网络安全保密基础 / 蔡红主编. —北京：军事科学出版社，1999.8

ISBN 7-80137-283-2

Ⅰ. 网… Ⅱ. 蔡… Ⅲ. 计算机网络-安全 Ⅳ. T393

中国版本图书馆 CIP 数据核字（1999）第 25550 号

军事科学出版社出版

（北京市海淀区青龙桥/邮编：100091）

出版人：刘庆忠

印刷：河北省地勘局测绘院印刷厂

开本：850×1168 毫米 1/32	版次：1999 年 6 月北京第 1 版
印张：7.25	印次：1999 年 6 月第 1 次印刷
字数：150 千字	印数：1— 5000 册

书号：ISBN 7-80137-283-2/E・195 定价：16.80 元

本书编著人员名单

主　编　蔡　红

副主编　杨世松　崔书昆

编　委　郝河长　李德洲　刘昱旻　胡　斌
黄世亮　王杰锋　刘波坤　韩忠林
胡娅莉　魏　力　朱宜兵

主　审　曲成义

目　录

第一章　网络概说

网络时代已经到来！

随着因特网的接入和普及，突破了地域与文化的界限，以快速便捷的网络通信进行信息的交换和应用，我们正进入一个没有计算机信息网络就无法工作和生活的信息时代。

网络，作为21世纪十大前沿技术之一，它把金融、市场、商品、技术、劳动力、工业设备、服务、娱乐、生产等联为一体。网络给人类社会带来巨大的进步，也带来了巨大的隐患。本书就是有关网络安全问题的小册子。为了帮助读者了解网络和网络安全问题，先就网络的基本知识作一些介绍。

一、网络的概念和要素

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

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。

因特网（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。因特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有以下部分组成。

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）。它是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）。它是用来联接两个相同网络操作系统的网络。

（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，就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各种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。这是一种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中，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。这是以单根导线为芯，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干道。

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，并对全网资源进行统一管理。网络操作系统必须有相应的安全措施，否则是不能实用的。

二、网络的结构与分类

在公元纪年第三个千年到来之时，人类正进入信息时代。网络作为信息时代的前沿科技从来没有像今天离

我们这样近。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)。在这一环

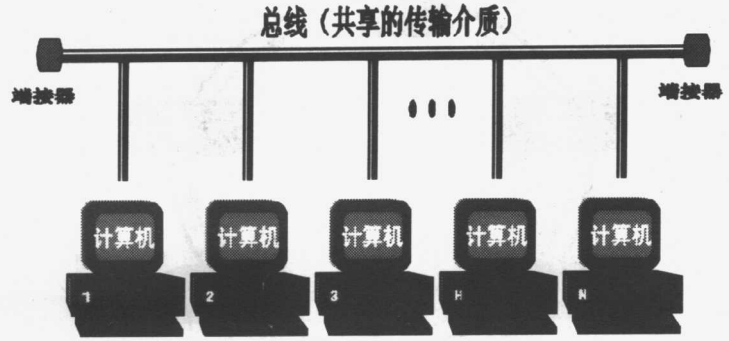

图1-1 总线拓扑

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顺序相连，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）。

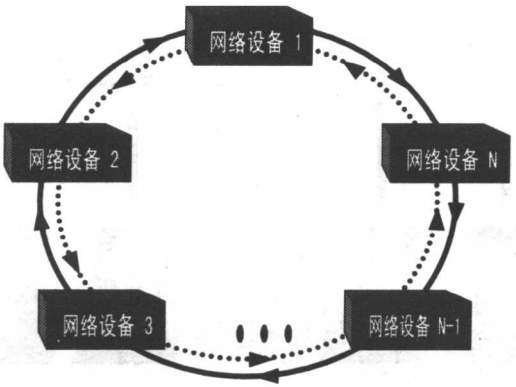

图1-2 具有双环结构的环状拓扑

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）。

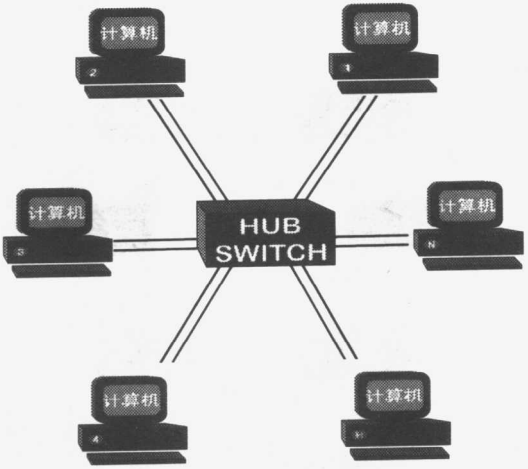

图1-3 星型拓扑

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**。每个网络节点使用二条或二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。

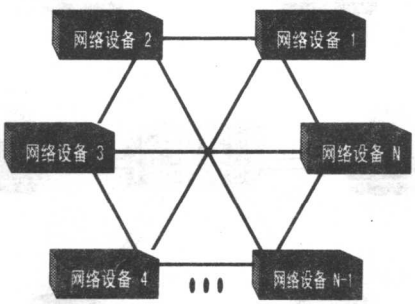

图1-4　网状拓扑

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