# 第3章 网络基础知识

网络是信息传输、接收、共享的虚拟平台，通过它把各个点、面、体的信息联系到一起，从而实现这些资源的共享。

人们现在所说的网络通常是指计算机网络。计算机网络就是用物理链路将各个孤立的工作站或主机相连在一起，组成数据链路，从而达到资源共享和通信的目的。凡将地理位置不同，并具有独立功能的多个计算机系统通过通信设备和线路而连接起来，且以功能完善的网络软件（网络协议、信息交换方式及网络操作系统等）实现网络资源共享的系统，可称为计算机网络。

从以上定义中，可以看出组成一个网络需要硬件支持和软件支持，还要按照一定的结构将各个终端连接起来。网络中的硬件主要有集线器（Hub）、交换机、路由器、传输介质、中继器等。软件支持主要是各个协议，所谓协议，就是在信息传输的工程中都要遵守的规范。例如，TCP、UDP、IPSec、SMTP、HTTP 以及 IP 地址分配等。不同的协议工作在 TCP/IP 体系结构的不同层，下面将分别具体介绍。

## 3.1 网络硬件设备介绍

### 3.1.1 传输介质

目前常见的传输介质有双绞线、同轴电缆、光纤、光缆。

#### 1. 双绞线

由两根有绝缘保护层的铜导线逆时针缠绕而成的是双绞线（每根导线加绝缘层并标有颜色来标记），由多对双绞线构成的电缆称为双绞线电缆。双绞线分为非屏蔽双绞线（Unshielded Twisted Pairwire，UTP）和屏蔽双绞线（Shielded Twisted Pairwire，STP）两种。非屏蔽双绞线由双绞线和塑料外壳组成。屏蔽双绞线在非屏蔽双绞线的基础上增加了一层屏蔽防护层，起到屏蔽防护的作用。

非屏蔽双绞线是计算机中使用最为普遍的传输介质，它分为一类至五类。目前常用的就是五类双绞线，由 4 对双绞线构成，最高传输速率为 100Mb/s。

一般来说，双绞线的最大传输距离为 100m，也就是说，网络中任意一台和交换机相连的计算机的双绞线距离不应大于 100m。如果网络的距离过长，可以使用中继器设备，中继器将在下面介绍。中继器的作用是把接收到的信号按照原样放大，并继续向下传输。使用中继器可以使网络距离有较大延长，但也不能使用太多，否则会导致网络质量严重下

降，甚至无法使用。

在使用双绞线的时候需要安装一个水晶插头，方便与计算机连接，这种插头称为水晶头（也叫作 RJ-45 接头）。使用时，将双绞线电缆（多对双绞线构成）的 4 对 8 芯铜线按一定规则插入水晶头即可。

### 2. 同轴电缆

随着以双绞线和光纤为基础的标准化布线的推广，同轴电缆已逐渐退出市场。下面对同轴电缆只做简单的介绍。

同轴电缆以硬铜线为芯，外包一层绝缘材料，绝缘材料外有一层密织的网状导体环绕，最外层覆盖一层保护性材料。根据传输频带的不同，同轴电缆可以分为基带同轴电缆和宽带同轴电缆；按直径的不同，可以分为粗缆和细缆两种类型。粗缆适用于比较大型的局部网络，它传输距离长、可靠性高。由于安装时不需要切断电源，因此可以根据需要灵活地调整计算机的入网位置。但粗缆网络必须安装收发器和收发器电缆，安装难度大，所以总体造价高。细缆安装则比较简单，造价低，但由于安装过程要切断电源，两头必须装上基本网络连接头（BNC），然后接在 T 型连接器两端，当接头多时容易产生接触不良的现象。为了保持同轴电缆的正确电气特性，电缆屏蔽层必须接地，同时两头要有终端器来削弱信号反射作用。

同轴电缆抗干扰能力好，能支持的网段距离比较长，但是价格比双绞线昂贵。由于同轴电缆的网络传输速率为 10Mb/s，现在已经很少使用了。

### 3. 光纤和光缆

光纤和光缆是目前为止传输速度最快的介质。

光纤即为光导纤维的简称。光纤通信是以光波为载频，以光导纤维为传输媒介的一种通信方式。光纤由单根玻璃光纤、紧靠纤芯的包层以及塑料保护涂层组成。

为了使用光纤传输信号，光纤两端必须配有光发射机和接收机，光发射机执行从光信号到电信号的转换。实现电光转换的通常是发光二极管（LED）或注入式激光二极管（ILD）；实现光电转换的是光电二极管或光电三极管。

根据光在光纤中的传播方式，光纤可以分为多模光纤和单模光纤两种类型。单模光纤只能携带一种（某种频率）光波，这种模式的光纤的数据传输速度较快，有效传输距离也远，但是利用率低、成本高，普通网络很少使用。多模光纤可以在单根光纤上传输多种不同的光波，这样光波的带宽大大增加，提高了利用率、降低了成本，这种光纤在网络中被真正地应用。

光纤具有传输速率高、功能损失小、带宽大、抗电磁干扰能力强以及能够在长距离内保持很高的传输效率等特点，但其价格昂贵，并且连接技术比较复杂，一般用于组建大型局域网的骨干网、城域网以及广域网。

光缆可以包含一根光纤（有时称单纤）或两根光纤（有时称双纤），或者更多光纤（48 纤、1000 纤）。在普通计算机网络中安装光缆是从用户设备开始的，因为光缆只能单向传输，为了实现双向通信，光缆必须成对出现，一个用于输入，一个用于输出，光缆两端接光学接口器。

### 3.1.2　集线器

集线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，但它不具备自动寻址能力，即不具备交换作用，所有数据广播到与集线器相连的各个端口，这样容易造成数据堵塞，以致整个网络速度均变慢。总之，集线器是对网络进行集中管理的最小单元。

按照端口数量来分类，集线器一般情况下分为 8 口、16 口或 24 口集线器；按照总线带宽分类，可分为 10Mb/s、100Mb/s 和 10/100Mb/s 自适应三种；按照配置形式，集线器可分为独立型集线器、模块化集线器和可堆叠式集线器。独立型集线器是最早使用的设备，它具有低价格、容易查找故障、网络管理方便等优点，在小型的局域网中广泛使用。模块化集线器一般带有机架和多个卡槽，每个卡槽中可以安装一块卡，每块卡的功能相当于一个独立型的集线器，多块卡通过安装在机架上的通信底板进行互连并进行相互间的通信，它在大型网络中得到了广泛的应用。可堆叠式集线器是利用高速总线将单个独立型集线器“堆叠”或短距离连接设备，其功能相当于一个模块化集线器。可堆叠式集线器可以非常方便地实现对网络的扩充。

### 3.1.3　交换机

交换机对传递过来的信息进行重新生成，并经过内部处理后转发至指定端口，具备自动寻址能力和交换作用。由于交换机能够根据所传递信息包的目的地址，将每一信息包独立地从源端口送至目的端口，真实地实现了点对点的数据传送，这样就摒弃了原来 Hub 的那种广播式的工作方式，从而避免了和其他端口发生冲突，互不影响地传送信息包，提高了网络的实际吞吐量。

按采用技术的不同来分类，交换机可以分为直通式交换机、存储转发交换机和无碎片转发交换机。直通式交换机一旦收到数据帧中的目标地址，就立即开始转发。由于不需要存储，延迟非常小，交换非常快，这是它的优点。由于数据包内容并没有被以太网交换机保存下来，所以无法检查所传送的数据包是否有误，而且由于没有缓存，容易造成丢包，这是它的缺点。当存储转发交换机收到完整的帧时，先将其存储起来，然后进行 CRC（循环冗余码校验），经过坏帧处理后再转发。正因如此，存储转发方式在数据处理时延时大，但是它可以对进入交换机的帧进行错误检测，有效地改善网络性能。无碎片转发交换机介于直通式交换机和存储转发机之间，比存储转发交换机快，比直通式交换机慢，但它能够避免残帧的转发，因此被广泛地用于低档交换机中。

按传输速率分，可以分为 10Mb/s 交换机、100Mb/s 交换机、10/100Mb/s 自适应交换机和 1000Mb/s 交换机。其中，10Mb/s 交换机已经被淘汰了，现在常见的是 10/100Mb/s 交换机。按照端口数量分类可以分为 4 口、8 口以及 16 口等。按传输介质可以分为有线交换机和无线交换机。

交换机与集线器的区别：

（1）集线器属于物理层设备，交换机属于数据链路层设备。即集线器只是对数据的传输起到同步、放大和整形的作用，对数据传输中的短帧、碎片等无法进行有效的处理，不

能保证数据传输的完整性和正确性；交换机不但可以对数据的传输做到同步、放大和整形，而且可以过滤短帧、碎片等。

（2）集线器是一种广播模式，当集线器的某个端口工作的时候，其他所有端口都能够收到信息，容易产生广播风暴，当网络流量较大时，网络性能就会受到很大的影响；交换机工作的时候，只有发出请求的端口和目的端口之间相互响应而不影响其他端口，因此交换机能够隔离冲突域，有效地抑制广播风暴的产生。

（3）集线器的所有端口共享一条带宽，工作在半双工模式下，即在同一时刻只能有两个端口传送数据，其他端口只能等待；交换机每个端口都有一条独占的带宽，各端口互不影响。交换机有半双工和全双工两种模式。

### 3.1.4 路由器

路由器工作在网络层，它的作用主要有两个：一是连通不同的网络，它支持采用不同的网络协议、不同子网之间的通信；另一个作用是选择信息传送的路径，它就好比一个路口，有好多条岔路，路由器负责为数据包选择最适合它的那条路。

按处理能力来分，路由器可以分为高端路由器和中低端路由器。通常将背板交换能力大于 40Gb/s 的路由器称为高端路由器，低于 40Gb/s 的称为中低端路由器。

按结构来分，路由器可以分为模块化结构路由器和非模块化路由器。通常，中高端路由器为模块化结构路由器，低端路由器为非模块化结构路由器。

按所处网络位置来分，路由器可以分为核心路由器和接入路由器。核心路由器位于网络中心，通常使用的是高端路由器；接入路由器位于网络边缘，通常使用的是中低端路由器。

按功能来分，路由器可以分为通用路由器和专用路由器。通常所说的路由器是指通用路由器，专用路由器通常为实现某种特定功能对路由器接口、硬件等作专门优化。另外，还有一种常见的分类就是有线路由器和无线路由器。

### 3.1.5 中继器

中继器（repeater）是局域网环境下用来延长网络距离的最简单最廉价的互连设备，操作在 OSI 的物理层。中继器对在线路上的信号具有放大再生的功能，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。

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。中继器就是为解决这一问题而设计的。它完成物理线路的连接，对衰减的信号进行放大，保持与原数据相同。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作了具体的规定，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。

### 3.1.6　网卡

网卡(NIC)是局域网中最基本的部件之一,有时也称为网络卡、网络接口卡或者网络适配器。

网卡主要有两大作用:一是负责接收网络上传送过来的数据包,解包后,将数据通过主板上的总线传输给本地计算机;二是将本地计算机上的数据包打包后送入网络。每块网卡有其世界唯一的地址,MAC 地址,以后会讲到。

按接口类型分类,有 ISA 网卡、PCI 网卡、PCI-E 网卡和 USB 网卡 4 种。目前,ISA 网卡在市场上已很少见到,PCI(Peripheral Component Interconnect,外部设备扩展接口)网卡是目前市场上最常见、使用最广的网卡。PCI 网卡采用并行传输模式,传输速率快,并且不占用 CPU 资源。PCI-E(Peripheral Component Interconnect Express,外部设备高速接口)是第三代互连技术产品,它采用串行传输数据的模式,相比于 PCI 网卡,它的最大优势就是传输速率快。目前的 USB 网卡多为 USB 2.0 标准的,USB 2.0 标准的传输速率可以高达 480Mb/s。

根据工作对象的不同,网卡可以分为普通工作站网卡、服务器专用网卡和笔记本专用网卡 PCMCIA。现在市场上最常见的普通网卡就是个人计算机网卡,其传输速率一般为 10～100Mb/s。这类网卡具有价格低廉、工作稳定、安装方便等优点。服务器网卡是专门为服务器设计的,由于这类网卡采用了专用的控制芯片,因此它能独立完成网络中的大量数据处理工作,并具有高传输率、低占用率等优点,非常适合网络服务器的工作要求。笔记本专用网卡具有体积小、功耗低、安装方便等优点。

按传输介质的不同可以分为有线网卡和无线网卡。有线网卡是通过连接有线传输介质来进行数据传输的。无线网卡近几年使用的越来越广泛,基本每个笔记本都会配备无线网卡,可方便笔记本移动。

按传输速率分可将网卡分为 10Mb/s 网卡、10/100Mb/s 网卡和 1000Mb/s 网卡。

### 3.1.7　终端设备

终端设备很好理解,就是指连接在网络中的计算机、服务器、输入设备、输出设备。具体又分为专用终端和通用终端,远程批处理终端和交互式终端等。

### 3.1.8　主流设备介绍

目前市场上比较有影响力的网络硬件设备生产厂家有华为、思科、中兴等。

华为 Quidway®S5300 系列全千兆交换机是华为为满足大带宽接入和以太网多业务汇聚而推出的新一代全千兆高性能以太网交换机,可为客户提供强大的以太网功能。产品特性:

S5300 基于新一代高性能硬件和华为统一的 VRP®(Versatile Routing Platform)软件,具备大容量、高密度千兆端口,可提供万兆上行,充分满足客户对高密度千兆和万兆上行设备的需求。S5300 可满足运营商园区网汇聚、企业网汇聚、IDC 千兆接入以及企业千兆到桌面等多种场合的需求。

华为赛门铁克 Oceanspace S6800E 路由器。高速缓存 32GB。系统支持 Windows、Linux、Solaris、HP-UX、AIX、FreeBSD。外接主机通道 12 个 4Gb FC 或 4 个 4Gb FC+4 个 GE iSCSI 16 个 4Gb FC 或 8 个 4Gb FC+4 个 GE iSCSI。RAID 支持 0、1、5、6、10、50 等。单机磁盘数量 24 个。内置硬盘接口 4 个 4Gb FC、8 个 4Gb FC。64 位多核处理器。硬盘保护功能有全局热备、预拷贝、硬盘坏道修复；掉电保护功能有数据保险箱、一体化 UPS 技术；Web GUI、CLI 等管理界面。

思科 Cisco Catalyst 2918 系列交换机是面向中国市场中小规模网络部署的入门级固定配置交换机。Catalyst 2918 采用简体中文的设备面板和图形化界面，以特优的性价比，为入门级配线间和小型分支机构提供桌面快速以太网和千兆上行网络连接。Cisco Catalyst 2918 系列通过提供完备的入门级安全策略、服务质量(QoS)和可用性功能，降低了企业网络总体拥有成本。该系列交换机还为中国企业用户提供了从非智能集线器和不可管理的交换机向便于扩展的可管理网络迁移的简便的途径。

思科 Cisco 1900 系列集成多业务路由器集思科 25 年创新和产品领先的精髓。新平台的构建旨在继续推动分支机构的发展，为分支机构提供富媒体协作和虚拟化，同时最大程度地节省运营成本。第 2 代集成多业务路由器平台支持未来的多核 CPU，具有增强 POE 的千兆位以太网交换产品以及新能源监控和控制功能，同时提高整体系统性能。此外，全新 Cisco IOS 软件通用映像和服务就绪引擎模块，可将硬件和软件部署分离，从而奠定坚实的技术基础以及时满足不断发展的网络需求。总而言之，通过智能集成市场领先的安全、统一通信、无线和应用程序服务。

中兴 ZXR10 5900E 易维系列 MPLS 路由交换机采用高速 ASIC 交换芯片实现 L2～L7 数据线速转发，提供完备的以太网协议族支撑和高效的 QOS 优先级机制，具备灵活多样的管理手段。支持完整的三层路由协议。ZXR10 5900E 提供高密度的千兆以太网端口，为 IP 城域网或者园区网提供千兆以太网接口的汇聚功能，是组建园区网、IP 城域网、智能楼宇汇聚层的理想产品。

中兴 ZXR10 GER 通用高性能路由器是针对城域网、企业网、校园网等市场需求而推出的一款中高端路由器产品，可为用户提供安全、可控、可管理的高性能宽带网络解决方案。GER 采用模块化设计思想、高性能网络处理器和 Crossbar 交换结构，根据提供的用户槽位数不同，可细分为 GER08、GER04、GER02 三款，分别可提供 8、4、2 个用户槽位，满足用户不同场合的需求。中兴 ZXR10 GER 不仅能提供高端路由器的优异性能，更能提供丰富的基于硬件或软件的业务功能。

## 3.2 网络协议

网络中仅有硬件设备是不可以工作的，就像计算机只有硬件不能工作一样，计算机中要有操作系统，网络中要有网络协议，各个部件按照规定统一的网络协议有条不紊地工作。

### 3.2.1　TCP/IP 基础

#### 1. OSI 开放系统互连参考模型

为使不同计算机厂家生产的计算机能相互通信，以便在更大范围内建立计算机网络，国际标准化组织（ISO）在 1978 年提出“开放系统互连参考模型”（Open System Interconnection/Reference Model，OSI/RM）。开放系统互连参考模型将整个网络的通信功能分为 7 个层次，每个层次完成不同的功能。这 7 个层次由低到高分别是物理层、数据链路层、网络层、传输层、会话层、表示层和应用层。

（1）物理层（physical layer）。物理层传输数据的单位是比特。该层包括物理联网媒介，如电缆连线、连接器。在桌面 PC 上插入网络接口卡，就建立了计算机联网的基础。换言之，即提供了一个物理层。物理层的协议产生并检测电压以便发送和接收携带数据的信号。尽管物理层不提供纠错服务，但它能够设定数据传输速率并监测数据出错率。物理层的作用是尽可能屏蔽由于物理设备不同或传输媒介不同引起的差异，对它的高层即数据链路层提供统一的服务。

（2）数据链路层（data link layer）。数据链路层传输数据的单位是帧。帧是用来移动数据的结构包，它不仅包括原始数据，还包括发送方和接收方的网络地址以及纠错和控制信息，数据链路层有纠错功能，其中的地址确定了帧将发送到何处，而纠错和控制信息则确保帧无差错到达。它控制网络层与物理层之间的通信，在不可靠的物理线路上进行数据的可靠传递，为它的上层即网络层屏蔽错误。有一些连接设备，如交换机，由于它们要对帧解码并使用帧信息将数据发送到正确的接收方，所以它们是工作在数据链路层的。

（3）网络层（network layer）。网络层的传输单位是报文分组或包。其主要功能是将网络地址翻译成对应的物理地址，并选择最佳的路由，使发送端传输层的报文能够正确无误地按照目的地址找到接收端，并交付给接收端的传输层。网络层处理路由，路由选择的好坏在很大程度上决定了网络的性能，如网络吞吐量（在一个特定的时间内成功发送数据包的数量）、平均延迟时间、拥塞控制、资源的有效利用率等。路由器连接网络各段，并智能指导数据传送，属于网络层。

（4）传输层（transport layer）。传输层传输的数据单位是报文。传输层正好是 7 层的中间一层，是通信子网（下面三层）和资源子网（上面三层）的分界线，它屏蔽通信子网的不同，使高层用户感觉不到通信子网的存在。传输协议进行流量控制，即基于接收方可接收数据的快慢程度规定适当的发送速率。除此之外，传输层按照网络能处理的最大尺寸将较长的数据包进行强制分割。例如，以太网无法接收大于 1500B 的数据包，发送方节点的传输层将数据分割成较小的数据片，同时对每一数据片安排一序列号，以便数据到达接收方节点的传输层时，能以正确的顺序重组，该过程即被称为排序。传输层完成资源子网中两节点的直接逻辑通信，实现通信子网中端到端的透明传输。TCP（传输控制协议）和 UDP（用户数据报协议）是传输层中最常用的协议。

（5）会话层（session layer）。负责在网络中的两节点之间建立和维持通信。会话层的功能包括：建立通信链接，保持会话过程通信链接的畅通，同步两个节点之间的对话，决定通信是否被中断以及通信中断时决定从何处重新发送。

(6) 表示层(presentation layer)。在计算机与计算机用户之间进行数据交换时,不同的计算机可能采取不同的编码方法来表示数据的类型和结构,为了使计算机间能够进行交互通信,能相互理解所交换数据的值,采用抽象的标准法来定义数据结构,并采用标准的编码形式。表示层管理这些抽象数据结构,并且在计算机内部表示和网络的标准表示法之间进行转换。表示层也管理数据的解密与加密,如系统口令的处理。例如,在Internet 上查询银行账户,使用的即是一种安全连接。账户数据在发送前被加密,在网络的另一端,表示层将对接收到的数据解密。除此之外,表示层协议还对图片和文件格式信息进行解码和编码。

(7) 应用层(application layer)。应用层是 OSI 网络协议体系的最高层,是用户与计算机沟通的窗口,负责对软件提供接口以使程序能使用网络服务,为网络用户之间的通信提供专用的程序。应用层提供的服务包括文件传输、文件管理以及电子邮件的信息处理。DNS(域名系统)、HTTP(超文本传输协议)、SMTP(简单邮件传输协议)等工作在应用层。

### 2. TCP/IP 体系结构

互联网是个复杂的系统,需要一个更加完善的网络模型,这个模型要更加适应网络的发展,TCP/IP 体系结构应运而生。在 TCP/IP 体系结构中,将网络模型分为 4 层:应用层、传输层、网络层和网络接口层。表 3-1 给出了 TCP/IP 结构和 OSI 结构的对应关系。

**表 3-1 TCP/IP 与 OSI 结构的对应关系**

| TCP/IP | | OSI |
|---|---|---|
| 应用层 | FTP、HTTP、Telnet、SMTP、POP3、SNMP、DNS | 应用层 |
| | | 会话层 |
| | | 表示层 |
| 传输层 | TCP UDP | 传输层 |
| 网络层 | IP ICMP ARP IGMP | 网络层 |
| 网络接口层 | Ethernet、FDDI、ATM、X.25 | 数据链路层 |
| | | 物理层 |

(1) 网络接口层:这是 TCP/IP 网络模型的最底层,负责数据帧的发送和接收。这一层从网络层接收 IP 数据报并通过网络发送它,或者从网络上接收物理帧,抽出 IP 数据报,交给网络层。这一层涉及网络的物理组件,包括电缆、路由器、交换机和网络接口卡(NIC),也包含各种不同的硬件层协议,以太网就是其中一种广泛使用的协议。

(2) 网络层:网络层将传输层的数据报封装成 IP 分组,注入网络中,使用路由算法将数据报送到指定目的地。这一层对用户来说是透明的,用户不需要关心网络层具体是怎么转发数据报的。本层的中心工作就是 IP 分组的路由选择,这是通过路由协议和路由器进行的。本层还进行流量控制。

(3) 传输层：传输层在计算机之间提供端到端的通信。传输层负责打包数据以便数据能在主机之间发送。这一层将应用层的数据封装，形成称为“数据报”(packets)的逻辑单元。每一个数据包包含一个包头，其中包括说明使用的传输协议特点的各种域，数据包还可能有一个载荷，其中含有应用层数据。

(4) 应用层：这是 TCP/IP 的最高层，应用程序通过该层访问网络。该层与 OSI 模型中的上三层相对应，这一层使得应用程序可以在服务器和客户端之间传输数据。

### 3.2.2　应用在 TCP/IP 各层的协议

(1) 应用在网络接口层的协议：以太网协议(Ethernet)、光纤分布式数据接口(FDDI)、异步传输模式(ATM)、X.25 协议。

以太网协议建立在 MAC 地址的基础上。MAC 地址是被封装在网卡上的全球唯一的，由 6 字节十六进制数组成，例如，00-1B-38-9E-3A-99。MAC 地址也叫硬件地址，这个地址是永远不会改变的。

光纤分布式数据接口(FDDI)是由美国国家标准化组织(ANSI)制定的在光缆上发送数字信号的一组协议。FDDI 使用双环令牌，传输速率可以达到 100Mb/s。由于支持高宽带和远距离通信网络，FDDI 通常用作骨干网。

ATM(Asynchronous Transfer Mode)顾名思义就是异步传输模式，就是国际电信联盟 ITU-T 制定的标准，ATM 是一种传输模式。在这一模式中，信息被组织成信元，因包含来自某用户信息的各个信元不需要周期性出现，这种传输模式是异步的。ATM 信元是固定长度的分组，共有 53 个字节，分为两个部分。前面 5 个字节为信头，主要完成寻址的功能；后面的 48 个字节为信息段，用来装载来自不同用户、不同业务的信息。话音、数据、图像等所有的数字信息都要经过切割，封装成统一格式的信元在网中传递，并在接收端恢复成所需格式。由于 ATM 技术简化了交换过程，去除了不必要的数据校验，采用易于处理的固定信元格式，所以 ATM 交换速率大大高于传统的数据网，如 X.25 等。

X.25 协议是 CCITT(国际电报电话咨询委员会)建议的一种协议，它定义终端和计算机到分组交换网络的连接。分组交换网络在一个网络上为数据分组选择到达目的地的路由。X.25 是一种很好实现的分组交换服务，传统上它是用于将远程终端连接到主机系统的。这种服务为同时使用的用户提供任意点对任意点的连接。来自一个网络的多个用户的信号，可以通过多路选择通过 X.25 接口而进入分组交换网络，并且被分发到不同的远程地点。一种称为虚电路的通信信道在一条预定义的路径上连接端点站点通过网络。

(2) 应用在网络层的协议：网络互联协议(IP 协议)、国际控制报文协议(ICMP)、地址解析协议(ARP)、互联网组管理协议(IGMP)、Internet 安全协议(IPSec)。

IP 协议是一个面向无连接的协议，主要负责在主机和网络间寻址并为 IP 分组设定路由。IP 协议不保证数据分组是否正确传递，在交换数据前它并不建立会话，数据在收到时，IP 不需要收到确认，因此 IP 协议是不可靠的传输。IP 地址经常被间接使用，当用户需要访问网络上某个资源时，通常会输入服务器的名字而不是 IP 地址。这个名字就是域名，并且通过 DNS 应用层协议被映射到 IP 地址，因为域名比 IP 地址更好记忆，而且域名一般不会变化，而 IP 地址则不一样(这个以后会讲到)，通过域名引用到主机，不管当前

使用的是什么 IP 地址，用户总能访问到这台主机。

国际控制报文协议(ICMP)用于报告错误，传递控制信息。报告差错是指，当中间网关发现传输错误时，立即向信源主机发送 ICMP 报文，报告出错情况，以使信源主机采取相应的纠正措施；传递控制信息是指，用 ICMP 来传递控制报文，常用的 ping、traceroute 等工具就是利用 ICMP 报文工作的。

地址解析协议(ARP)用于获得同一物理网络中主机的硬件地址。主机在网络层用 IP 地址来标识。但在网络上通信时，主机就必须知道对方主机的硬件地址。ARP 实现将主机 IP 地址映射为硬件地址的过程。

互联网组管理协议(IGMP)使 IP 主机能够向本地多播路由器报告多播组成员，以实现多播。

Internet 安全协议(IPSec)是 Internet 工作组 IETF 提出的保护 IP 报文安全通信的一系列规范，它提供私有信息通过公用网的安全保障。因为传统的 IPv4 没有提供安全服务，缺乏对通信双方身份真实性的鉴别能力，而且没有提供传输数据的完整性和机密性保护，Internet 的网络层面面临业务流监听、IP 地址欺骗、信息泄漏和数据项篡改等多种安全威胁。IPSec 是一族协议，用于在 IP 层提供机密性、数据源鉴别和完整性保护。

(3) 应用在传输层的协议：传输控制协议(TCP)、用户数据报协议(UDP)。

TCP 是一种可靠的面向连接的传输服务。TCP 在主机之间建立连接，并尽最大努力确保数据在此连接上可靠传递。TCP 在通信双方建立连接后，将数据分成数据报，为其指定顺序号。在接收端收到数据报之后进行错误检查，对正确发送的数据发送确认数据报，对于发生错误的数据报发送重传请求。TCP 可以根据 IP 协议提供的服务传送大小不等的数据，IP 协议负责对数据进行分段、重组，并在多种网络中传送。

UDP 提供的是非连接的、不可靠的数据传输。UDP 在数据传输之前不建立连接，而是由每个中间节点对数据报文独立进行路由。因此，当丢失一些数据对应用程序来说没有多大影响时，可以使用 UDP。因为 UDP 是无连接的，它的开销和延迟比 TCP 小。一些应用层的协议，如 DNS(域名系统)、DHCP(动态主机配置协议)、SNMP(简单网络管理协议)等都是使用 UDP 的。

(4) 应用在应用层的协议：文件传送协议(FTP)、超文本传输协议(HTTP)、远程登录协议(Telnet)、简单邮件传输协议(SMTP)、邮局协议第三版(POP3)、互联网邮件访问协议第 4 版(IMAP4)、简单网络管理协议(SNMP)、域名系统(DNS)。

文件传送协议(FTP)是计算机网络中最常见的应用之一，用于完成不同计算机之间的文件传输的任务，同时 FTP 还有交互式访问、格式规定和认证管理等功能，允许用户查看远程服务器上的文件清单，允许用户规定所存储数据的类型和格式，并采用“用户名/密码”的形式对用户进行认证和管理。FTP 的工作是基于 TCP 来完成的，其端口号为 21。

超文本传输协议(HTTP)是互联网中使用最为广泛的应用层协议。浏览网页就是通过 HTTP 进行的。HTTP 不仅支持 WWW 服务，它同时支持采用不同协议访问不同的服务，如 FTP、NNTP、Archie、SMTP 等。

远程登录协议(Telnet)允许一个地点的用户与另一个地点的计算机上运行的应用程序进行交互对话，提供一个相对通用的、双向的、面向字节的通信方法。该协议建立的基

础是网络虚拟终端的概念、对话选项的方法和终端与处理的协调。

简单邮件传输协议(SMTP)是一组用于由源地址到目的地址的地址传送邮件的规则,用来控制邮件的中转传递方式。SMTP 能够提供通过一个或多个中继 SMTP 服务器传送邮件的机制。中继服务器将接收原始邮件,然后尝试将其传递至目标服务器,或重定向至另一中继服务器,最终把邮件寄到收件人的服务器上。

邮局协议第三版(POP3)是规定邮件接收节点如何连接邮件服务器进行邮件接收和管理的协议,能够远程从服务器上收取邮件到本地,同时根据客户端操作删除或保留服务器上的邮件。

互联网邮件访问协议第 4 版(IMAP4)是一种邮件获取协议,能够从远程邮件服务器上获取邮件信息,并能交互式地操作服务器上的邮件。与 POP3 相比,IMAP4 除了支持 POP3 协议的脱机操作模式外,还支持联机操作和断连接操作,无须像 POP3 那样把邮件下载到本地,可在客户端直接对服务器上的邮件进行远程操作,例如移动、删除、改名等。

简单网络管理协议(SNMP)是由互联网工程任务组(IETF)定义的一套网络管理协议。利用该协议,一个管理工作站可以远程管理所有支持这种协议的网络设备,包括监视网络状态、修改网络设备配置、接收网络事件警告等。

域名系统(DNS)是计算机网络中把 IP 地址和域名相互转化的系统。域名解析就是把域名转化为 IP 地址,反向域名解析就是把 IP 地址转化为域名。之所以要使用域名代替 IP 地址,是因为域名比 IP 地址要更好记忆,IPv4 使用 32 位 IP 地址,而新一代 IPv6 使用 128 位 IP 地址,记一个名字总比记一长串数字要容易得多。

### 3.2.3　IP 地址及其相关知识

IP 地址就是指 IP 层,即网络层使用的标识符,它被用来唯一地标识互联网上的每一个设备以确保所有设备的全球通信。IP 地址的编址方法共经历了三个历史阶段——IP 分类编址、子网划分和超网构成。IPv4 是使用 32 位的二进制地址来表示的。32 位的二进制太难记忆,故将 IP 地址按照 8 位二进制数为一组,用“.”号隔开的×××.×××.×××.×××来表示,其中×××是 0～255 之间的一个十进制数,如 192.134.0.34,其二进制表示为 11000000 10000110 00000000 00100010。由于 IPv4 的地址空间已快被分配完,故提出了 IPv6 编址方法,IPv6 使用 128 位二进制表示,每 16 位二进制数为一组,用 4 位十六进制表示,中间用“:”隔开,例如,2002:00D3:0000:0043:FA28:3E33:00DD:323A。

#### 1. IP 分类编址

在 IP 分类编址中,IP 地址由网络 ID(net-id)和主机 ID(host-id)组成。网络 ID 就好比电话区号,主机 ID 就相当于 7 位或 8 位电话号码。网络中的计算机进行通信的时候,先按照网络 ID 查找目标主机所在的网络,将数据传到该网络,之后再按照目标主机 ID 找到该主机,将数据传到该目标计算机。网络 ID 是由互联网域名与地址管理机构(ICANN)分配的,主机 ID 是由各个网络的管理员分配的,这样就保证了 IP 地址的全球唯一性。由于连入 Internet 的各种网络的差异很大,有的网络中的主机数很多,有的则很少,为了便于管理,人们将 IP 地址按网络 ID 分为 5 类:A 类、B 类、C 类、D 类、E 类。在

IP 地址的二进制表示法中，左起数值 0、10、110、1110、11110 分别对应着 A 类、B 类、C 类、D 类和 E 类地址。

如图 3-1 所示，A 类、B 类、C 类地址的 net-id 的长度分别为 1 字节、2 字节和3 字节，host-id 的长度分别为 3 字节、2 字节和 1 字节。D 类和 E 类地址不划分 net-id 和 host-id。

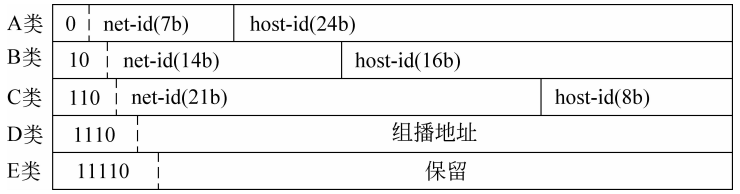


图 3-1　IP 地址分类

(1) A 类地址。A 类地址占整个地址空间的 1/2，按网络号可分为 128 个块，每一块包含 16 777 216 个地址。第一块覆盖的地址范围为 0.0.0.0～0.255.255.255(net-id 为 0)，最后一块覆盖的地址范围为 127.0.0.0～127.255.255.255(net-id 为 127)。除了三块地址(第一块、最后一块和 net-id 为 10 的块)为保留地址作为专用外，其余 125 个块可被分配。

(2) B 类地址。B 类地址占整个地址空间的 1/4，按网络号可分为 16 384 个块，每一块包含 65 536 个地址。第一块覆盖的地址范围为 128.0.0.0～128.0.255.255(net-id 为 128.0)，最后一块覆盖的地址范围为 191.255.0.0～191.255.255.255(net-id 为 191.255)。除了其中 16 个块保留为专用地址之外，其余 16 368 个块可被分配。

(3) C 类地址。C 类地址占整个地址空间的 1/8，按网络号可分为 2 097 152 个块，每一块包含 256 个地址。第一块覆盖的地址范围为 192.0.0.0～192.0.0.255(net-id 为 192.0.0)，最后一块覆盖的地址范围为 223.255.255.0～223.255.255.255(net-id 为 223.255.255)。除了其中 256 个块保留为专用地址之外，其余 2 096 896 个块可被分配。

(4) D 类地址。D 类地址是组播地址，主要留给互联网体系结构委员会(IAB)使用。D 类地址只有一个块，占整个地址空间的 1/16。

(5) E 类地址。E 类地址是保留块，只有一个块，占整个地址空间的 1/16。

上述 5 类地址总结如表 3-2 所示。

**表 3-2　IP 地址总结**

| 类型 | 划分依据 | 网络号比特数 | 主机号比特数 | 范围 | | 网络数量 | 主机数量 | 功能 |
|---|---|---|---|---|---|---|---|---|
| | | | | 开始 | 结束 | | | |
| A | 0 | 7 | 24 | 0.0.0.0 | 127.255.255.255 | 128 | 16 777 216 | 巨型网络 |
| B | 10 | 14 | 16 | 128.0.0.0 | 191.255.255.255 | 16 384 | 65 536 | 中到大型网络 |
| C | 110 | 21 | 8 | 192.0.0.0 | 223.255.255.255 | 2 097 152 | 256 | 小型网络 |
| D | 1110 | 28 | | 244.0.0.0 | 239.255.255.255 | | | 组播地址 |
| E | 11110 | 27 | | 240.0.0.0 | 247.255.255.255 | | | 保留地址 |

在这些 IP 地址中，有一些是特殊的 IP 地址，如表 3-3 所示。

表 3-3　特殊 IP 地址

| IP 地 址 | 功　　能 |
| --- | --- |
| 127.×.×.× | 回送地址 |
| 0.0.0.0 | 默认路由 |
| 网络位全 0 | 本网络上的特定主机 |
| 主机位全 0 | 本网络的网络地址 |
| 主机位全 1 | 广播地址 |
| 10.0.0.0～10.255.255.255 | 预留 A 类地址 |
| 172.16.0.0～172.31.255.255 | 预留 B 类地址 |
| 192.168.0.0～192.168.255.255 | 预留 C 类地址 |
| 网络位全 1，主机位全 1 | 受限广播地址 |

回送地址：这个地址用来测试软件。这种地址只能用作目的地址，当使用时，分组永远都不会离开主机，而是简单地返回协议软件。这种地址是 A 类地址。

默认路由：这个全 0 的地址表示这个网络上的这个主机。当某个主机不知道自己的 IP 时，为了要发现自己的 IP 地址，以全 0 地址作为自己的源地址，向引导服务器发送 IP 分组。这种地址也是 A 类地址。

本网络上的特定主机：当某一台主机想向本网络中的其他主机发送分组时，将以这种 IP 地址为分组的目的地址，路由器可以阻拦这样的分组，分组将被严格限制在本网络上。这种地址是 A 类地址，不管网络是什么类。

本网络的网络地址：这种地址的主机号全为 0。表示本网络的地址，主要用在路由选择上，在路由算法中，常用这种地址作为判断条件，选择该往哪条线路上转发。

广播地址：主机号全为 1 的是直接广播地址。路由器使用这种地址将一个分组发送到一个特定网络（由 net-id 决定）上的所有主机，所有主机都会收到以这种目的地址的分组。

受限广播地址：这个地址全由 1 组成，用于定义在当前网络上的广播地址。路由器可以阻拦目的地址为这种地址的分组从而使广播仅局限在本地网络。这种地址属于 E 类地址。

### 2. 子网划分

从上述可以看出 A 类地址和 B 类地址都可容纳非常多的主机，但实际是，这样的大型网络很少，如果一个网络分配一个网络 ID 是非常浪费的，为了解决这个问题，从 1985 年起在 IP 地址中又增加了一个“子网号域”，使二级 IP 地址变为三级 IP 地址，即 IP 地址由三部分组成：网络 ID、子网 ID（subnet-id）、主机 ID，如图 3-2 所示。

可见，子网划分只是将 IP 地址的本地主机地址进行了划分，不改变 IP 地址的网络部分。划分子网后，整个网络对外还是表现为一个网络。当采用三级 IP 地址时，IP 数据报的路由选择包含三个步骤，先找到网络 ID 所标识的网络，然后交付到子网，最后交付到主

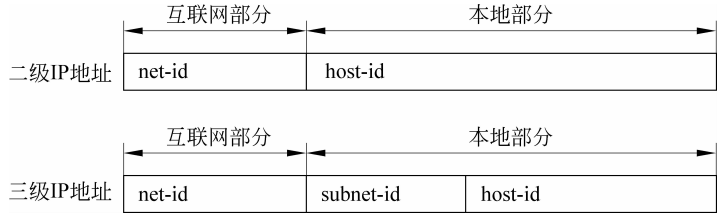


图 3-2　子网 IP 划分

机。从图 3-2 看到，子网号和主机号都是本地部分，如何区分呢？答案就是使用子网掩码。

子网掩码使用 32 位二进制数表示，表示的形式与 IP 地址相同。在子网掩码中用于标识网络地址位置的位为 1，主机地址位置的位为 0。A 类地址默认的子网掩码是 255.0.0.0，B 类地址默认的子网掩码是 255.255.0.0，C 类地址默认的子网掩码是 255.255.255.0。

例如，有一个 C 类地址 192.168.134.0，如果使用默认的 C 类子网掩码 255.255.255.0，则此 C 类地址包括的 IP 地址 192.168.134.1～192.168.134.254 属于同一个网段；如果子网掩码是 255.255.255.192，则此 C 类地址包括 4 个子网。具体区分方法是用 IP 地址与子网掩码逐位相与。现有一 IP 为 192.168.134.123，二进制表示为 11000000 10101000 10000110 01111011，子网掩码 255.255.255.192 的二进制表示为 11111111 11111111 11111111 11000000。如图 3-3 所示，前 24 位为 C 类网址的默认掩码，接下来的两位 1 代表该网络的子网，可见该网络被划分为 4 个子网 00、01、10、11。令子网掩码与 IP 地址逐位相与得到 11000000 10101000 10000110 01000000，十进制表示为 192.168.134.64。这说明该 IP 属于子网号为 01 的网络，其网络地址是 192.168.134.64。

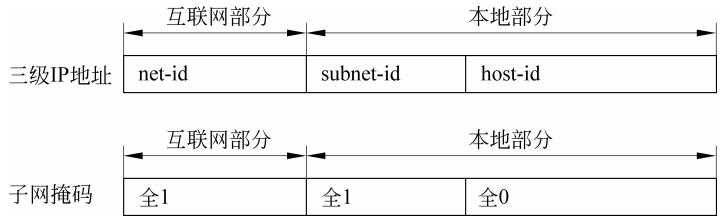


图 3-3　子网掩码

注意：子网能够容纳的主机个数等于 $2n-2$（$n$ 是正整数），因为每个子网都有两个 IP 地址不能给主机用：子网的网络地址（主机号为 0）和广播地址（主机号为 1）。

现在互联网的标准规定，所有网络都必须有一个子网掩码，同时在路由器的路由表中也必须有子网掩码这一栏。如果一个网络不进行子网划分，那么该网络的子网掩码就使用默认掩码。另外，互联网允许一个网点使用变长子网划分。当某一个网点准备拥有几个子网，但各个子网所连接的主机数差异较大，使用定长的子网掩码不能很好地利用网络资源，使用变长的子网掩码可以解决上述问题，此时，路由器使用两个不同的子网掩码，在使用过一个之后再使用另一个。

### 3. 超网构造

A 类和 B 类地址已经快被用完，但 C 类地址还可以申请到。但 C 类地址只能容纳 256 台主机，显然，在很多情况下 C 类地址是无法满足的。解决上述问题的方法就是进行超网构造。将若干个 C 类地址块合并为一个更大的地址范围。

能够合并的地址块是有具体要求的，不是随便几个地址块都能合并。要求 1：地址块数必须是 2 的整数次方；要求 2：这些地址块在地址空间中必须是连续的，即块和块之间没有空隙；要求 3：超块的第一个地址的第 3 个字节必须能够被块数均匀地分割开，即如果块数为 $N$，则第 3 个字节必须能够被 $N$ 整除。例如，下列 4 组 C 类地址：

第一组：198.47.32.0　198.47.33.0　198.47.34.0

第二组：198.47.32.0　198.47.42.0　198.47.52.0　198.47.62.0

第三组：198.47.31.0　198.47.32.0　198.47.33.0　198.47.34.0

第四组：198.47.32.0　198.47.33.0　198.47.34.0　198.47.35.0

第一组地址块数不是 2 的整数次方，不满足构造条件要求 1；第二组地址块不连续，不满足构造条件要求 2；第三组地址块的第一个地址的第三个字节，即 31，不能被块数 4 整除，不满足构造条件 3；第四组地址块满足所有构造要求，可以构造成超网。

当一个机构把分配到的几个地址块组合成一个超块时，必须知道这个超块的第一个地址和超网掩码。超网掩码中 1 的个数比默认 C 类地址掩码中 1 的个数少，令超网掩码和 C 类地址默认掩码相比较，它们相差的 1 的个数 $N$ 是 2 的幂指数，即该超网被划分为 $2^N$ 个子网。例如一个超网：

默认掩码为：11111111　11111111　11111111　00000000

超网掩码为：11111111　11111111　11111000　00000000

超网掩码中 1 的个数比默认掩码中 1 的个数少了 3 位，则该超网被划分为 $2^3$ 个，即 8 个子网。

## 3.3　网络架构

Internet 是个复杂的网络，由很多种网络构成。按照计算机网络的覆盖范围，计算机网络可以分为局域网、城域网和广域网三种类型；按照传输媒介可分为有线网络和无线网络。还有一种特殊的网络，虚拟网。

### 3.3.1　局域网、城域网和广域网

局域网(LAN)一般限制在较小的区域内，小于 10km 的范围。城域网(MAN)一般限定在一座城市的范围内，10～100km 的区域。广域网(WAN)一般跨越国界、州界甚至全球的范围，广域网典型的代表是 Internet。局域网是组成城域网和广域网的基础，通过局域网可以将计算机和各种网络设备连在一起，实现数据传输的资源共享。

局域网的拓扑结构是指局域网传输介质与节点(计算机网络或网络连接设备)的物理布局。常见的拓扑结构有：总线型结构、星状结构和环状结构。

### 1. 总线型拓扑结构

在总线型拓扑结构中，文件服务器和工作站都连在一条公共的电缆线上。总线型结构使用的电缆一般为细同轴电缆。这种结构使用电缆较少，且容易安装，各工作站和文件服务器只需将网卡上的 BNC 接头与总线上的 BNC T 型连接器相连即可，但是在总线主干两端必须安装终端电阻器。总线拓扑结构的优点是结构简单、安装方便，节点的添加和删除都比较方便；缺点是总线故障诊断和隔离困难，总线上的任何一点出现故障都会导致网络瘫痪。

### 2. 星状拓扑结构

星状拓扑的网络有一个中央节点，网络的其他节点如工作站、服务器等与中央节点直接相连。中央节点可以是文件服务器，也可以是无源或有源的连接器（如共享式 Hub 或交换机等）。一般使用共享式 Hub 或交换机作为中心节点。星状拓扑结构的优点是网络组建容易，容易检测和隔离故障；缺点是整个网络对中心节点的依赖性强，如果中心节点发生了故障，将导致整个网络的瘫痪。

### 3. 环状拓扑结构

环状局域网中全部的计算机连接成一个逻辑环，数据沿着环传输。环状拓扑结构内始终存在一个“令牌传送”信号，它沿着整个逻辑环路传输，需要发送信息的源主机首先需要捕捉到这个“令牌传送”信号，然后将其状态标示变为“令牌忙”，宣布占用网络的传输数据，然后将“令牌”原有的数据替换成想要传输的数据，再加上目标主机收到的网卡 MAC 地址发送出去，此数据包通过网络上的一台台主机传送到目的主机。目的主机收到数据后将“令牌”数据修改，表明其已经成功收到数据，当此“令牌”沿环状网络回到源主机时，源主机将“令牌”状态恢复为“令牌空闲”，清除数据，并将“令牌”交给逻辑环路中的下一台主机。环状网的优点在于网络数据传输不会出现冲突和堵塞情况，可以构成实时性较高的网络；缺点是环中某一点故障将导致整个网络的瘫痪，而且网络节点的添加、退出以及环路的维护和管理都比较复杂。

## 3.3.2 有线网络和无线网络

### 1. 有线网络

计算机有线网络的种类繁多，从连接不同大陆的海底光纤网络，到两台相邻计算机之间直接用交叉线序的网线相连，都属于有线网络的范畴。这里介绍三种常见的以太网、xDSL 接入网、EPON（以太无源光网络）有线网络以及主机接入互联网的方式。

以太网是一种流行的分组交换局域网（LAN），包括铜介质以太网、光纤以太网、无线以太网等。通常所说的以太网是指铜介质的，采用载波监听多路访问/冲突检测（CSMA/CD）机制来共享通信线路。目前的以太网多数采用交换机连接。交换机不是简单的广播信息，而是根据发送数据的目标主机，只发送给相应的端口。因此交换机网络的带宽不是共享的，而是主机收、发双发独占带宽，只有相同端口的数据才会共享带宽。

xDSL 是各种类型 DSL（数字用户线路）的总称，包括 ADSL（非对称 DSL）、RADSL

(速率自适应 DSL)、VDSL(甚高速 DSL)等。xDSL 的数字传输技术是使用专门的调制解调器(Modem),在现有的铜质电话线路上采用较高的频率及相应调制技术,即利用在模拟线路中加入或获取更多的数字数据的信号处理技术来获得高传输速率。各种 DSL 技术的区别体现在信号传输速率和距离的不同,以及上下行信道的对称性不同。电信公司利用 xDSL 技术,把原有铜质话音线路的电话接入网升级为计算机接入网。用户端和电信公司交换机房端各自部署 xDSL Modem,用户主机可接入到电信公司的数据网络中。该数据网络可以是专网,也可以与互联网相连。常用的是 ADSL 网络。

EPON(以太无源光网络)是一种光纤接入网技术,采用点对多点结构、无源光纤传输,在以太网上提供多种业务。它在物理层采用 PON(被动光网络)技术,在链路层使用以太网协议,利用 PON 的拓扑结构实现以太网的接入,从而综合了光网络和以太网的优点:成本低、高带宽、扩展性强、兼容性好、方便管理等。

每一台接入网络的计算机都会有一个 IP 地址,人们平时用自己的计算机上网时,IP 地址是临时分配的,这样可以有效利用 IP 地址,没有上网时,可以把 IP 让出来。这种动态的 IP 地址分配有一种常见的协议,就是动态主机设置协议(DHCP)。DHCP 基于 UDP,由 DHCP 服务器向接入网络的主机(客户端)提供无重复的 IP 地址。简单而言,一台未设置固定 IP 的主机接入到网络中,会以广播方式寻找 DHCP 服务器,正常情况是 DHCP 服务器分配给该主机一个未被占用的 IP 地址,从而主机能够在网络中进行通信。当主机退出网络后,DHCP 服务器就会收回 IP,以便分配给其他主机。所以,每次上网的时候 IP 地址都不一样。有些主机的 IP 地址则是固定的,比如实验室中的主机,IP 地址一般都是固定的。

### 2. 无线网络

计算机无线网络的种类有很多,而计算机的概念范围相当广,笔记本、手机智能终端、传感器、智能卡等都可称为计算机。

无线网络可以分为无线广域网、无线城域网、无线局域网和无线个人网络。

(1) 无线广域网(WWAN):主要是指通过移动通信卫星进行的数据通信,其覆盖范围最大。代表技术有 3G,以及未来的 4G 等。

(2) 无线城域网(WMAN):主要是通过移动电话或车载装置进行的移动数据通信,可以覆盖城市中的大部分区域。

(3) 无线局域网(WLAN):一般用于区域间的无线通信,其覆盖范围较小。

(4) 无线个人网(WPAN):无线传输距离一般在 10m 左右。

现在比较常见的 Wi-Fi 是一种可以将个人计算机、手机等终端以无线方式互相连接的技术,一般采用 CSMA/CA(载波侦听/冲突避免)协议。常见的 Wi-Fi 网络设备是无线网卡和无线访问节点(AP),有了 AP 如同有线局域网(LAN)有了集线器(Hub),可以进一步与有线网络相连。常见的简单组网方法是用无线路由器作为 AP,接入到有线网络中,则 AP 附近的计算机如果配有无线网卡,就能组成无线局域网(WLAN),并有机会通过 AP 与有线网络连接。

### 3.3.3 虚拟专用网

RFC 2764 对虚拟专用网(VPN)的定义是：利用公用网络将异地的站点或用户互连而形成的一个具有私有(专用)性的网络。这种私有性是指 VPN 可以保证其上通信的私有数据不被未授权访问，这可以通过认证、加密或路由隔离等机制实现。

VPN 使用的是公共网络基础设施传输私有数据，而不使用专用的私有线路。也就是说，VPN 没有自己的专用链路和网络基础设施，但通过 VPN 协议它可以提供与专用网络相同的安全服务，因此称为虚拟专用网。

实现 VPN 的典型技术有两种：隧道技术和虚拟路由技术。采用隧道技术实现 VPN 的基础框架如图 3-4 所示。在 VPN 设备之间建立 VPN 隧道，VPN 设备是实现 VPN 协议的对等实体，可以使用路由器、防火墙实现。VPN 隧道实际上是采用某种协议(即隧道协议)对网络数据包进行封装，从而提供安全特性。隧道技术将用户数据包采用隧道协议进行重新封装，并在公用网络中传输私有 VPN 数据。封装后的数据仍采用公共网络使用的协议(如 IP 协议)进行传输，传输过程对公共网络节点(如路由器)透明，即公用网络中的路由节点不会知道所传输的数据是否是用于专用网络。VPN 客户端使用 VPN 客户端软件接入 VPN 服务器，接入后即产生 VPN 隧道。

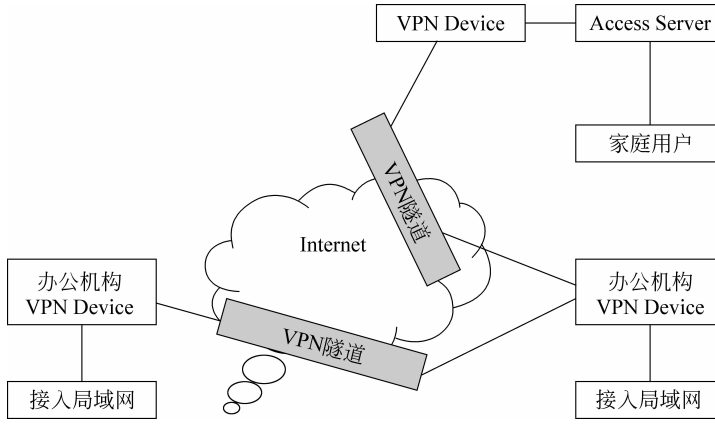


图 3-4　隧道技术的 VPN 基础构架

另一种实现 VPN 的技术是虚拟路由(VR)或虚拟路由器技术。虚拟路由器在软件层面上效仿物理路由器。虚拟路由器有其各自的 IP 地址和转发表，并且它们的路由是相互独立和隔离的。从用户的角度出发，虚拟路由器的功能和物理路由器是相同的。虚拟路由器正是利用路由信息隔离的特性为 VPN 用户提供数据私有性服务的。

如图 3-5 所示，VPN-1 连接在虚拟路由器 VR-1 中，而 VPN-2 连接在虚拟路由器 VR-2 上，VR-1 和 VR-2 的路由表是各自独立和相互隔离的。因此，VPN-1 和 VPN-2 之间相当于处在两个不同子网中。而 VR-1 的本地和远程网络之间可以通过因特网交换路由信息，相当于处在同一个子网中，可以互相访问。而无论是本地还是远程的 VR-2 连接的网络用户都不能访问 VR-1 网络的数据，因为它们没有该网络的路由信息。

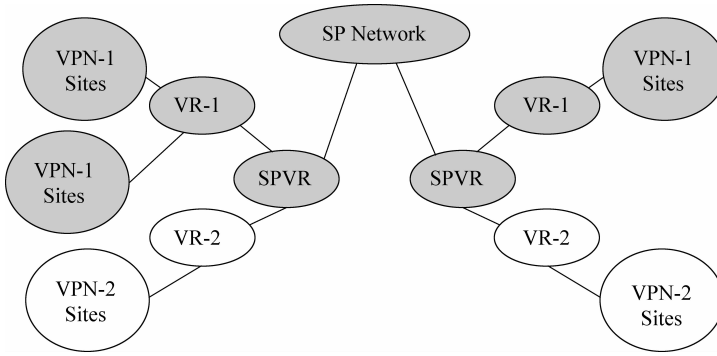


图 3-5　基于虚拟路由器的 VPN

## 3.4　基于网络的应用

### 3.4.1　计算机病毒

计算机病毒是一种小程序，能够自我复制，会将自己的病毒代码依附在其他程序上，通过其他程序的执行，伺机传播病毒程序，有一定潜伏期，一旦条件成熟，就会进行各种破坏活动，影响计算机使用。

计算机病毒的产生过程可分为：程序设计—传播—潜伏—触发、运行—实行攻击。

（1）程序设计期。计算机病毒是程序代码，这些代码中通常都加入一些具有破坏性的内容来达到设计者的目的。

（2）孕育期。在一个病毒制造出来后，病毒的编写者将其复制并传播出去。通常的办法是感染一个流行的程序，再将其放入 BBS 站点上、校园网或其他大型网络中。

（3）潜伏期。病毒是自动复制的。一个设计良好的病毒可以在它发作前长时期里被复制。这使得它有了充裕的传播时间。这时病毒的危害在于暗中占据存储空间。潜伏期的病毒，它们会不断地复制与继续传染，一个比较完美的病毒会有很长的潜伏期。

（4）病毒发作期。带有破坏机制的病毒会在遇至某一特定条件时发作，一旦遇上某种条件，比如某个日期或出现了用户采取的某特定行为，病毒就被激活了。没有感染程序的病毒属于没有激活，这时病毒的危害在于暗中占据存储空间。

### 3.4.2　木马

木马的全称是特洛伊木马，是一种秘密潜伏的能通过远程网络进行控制的恶意程序。攻击者可以控制被秘密植入木马的计算机，是攻击者进行窃取、破坏信息等行为的工具。

木马也同样是人为编写的程序，关键特征是秘密植入系统，能够接受远程控制。因此木马代码中必然带有指令部署（植入）和通信、系统控制的功能片段。为了隐藏自身，木马还可能使用各种技术来清除或伪装自身的各种存在痕迹。木马程序的原理是通过某种方式让其进程获得系统控制权，然后开启远程监控的服务端功能，随时准备接收攻击者的控

制指令。而攻击者有远程监控的客户端程序，能够与木马的服务端通信。

木马根据其功能进行分类，有密码窃取、文件破坏、自动拨号、寄生 Telnet/FTP/HTTP 服务、蠕虫型、邮件炸弹、ICQ 黑客、IRC 后门、C/S 等类型。典型的木马有 BACK Orifice(简称 BO)、网络公牛、冰河、广外女生、网络神偷、灰鸽子、PC-share 等。这些木马功能强大，包括远程文件管理、远程进程控制、远程键盘鼠标控制、密码窃取等功能，并且变得越来越隐蔽，技术手段日渐完善，对网络安全造成了很大的隐患。

木马程序与其他恶意程序相比有其特殊性。

(1) 隐蔽性：木马可能会通过某种技术隐藏自身在文件系统中的文件、隐藏在内存中的进程、隐藏在对外进行网络通信的网络连接和网络端口，从而实现看不见的功能。

(2) 自启动特性：木马为了长久控制目标主机，希望随系统的启动而启动。因此，木马必须把自己添加在相关自启动项中。

(3) 具备自我保护特性：木马为了防删除，采用多线程保护技术、多启动机制、多文件备份技术，从而实现删不掉、删不尽的功能。

(4) 具有非法的功能：如键盘记录、口令获取等。

完整的木马程序一般由服务器程序和控制端程序组成。“中了木马”就是指安装了木马的服务端程序。若计算机被安装了服务端程序，则拥有控制端程序的人就可以通过网络控制计算机，为所欲为，这时目标主机上的任何文件、程序，以及使用的账号、密码就无安全可言。木马程序本质上不是计算机病毒，但杀毒软件可以查杀已知的木马。

作为服务端的主机一般会打开一个默认的端口并进行监听，如果控制端向服务器端发送连接请求，服务端上的相应程序就会自动运行，来应答控制端的请求。反过来，服务端也可以主动连接控制端，并响应控制端的请求。

### 3.4.3 防火墙

防火墙是一种保护计算机网络安全的技术型措施，它可以是软件，也可以是硬件，或两者的结合。它在两个网络之间执行访问控制策略系统，目的是保护网络不被他人侵扰。通常，防火墙位于内部网或不安全的网络(Internet)之间，它就像一道门槛，通过对内部网和外部网之间的数据流量进行分析、检测、筛选和过滤，控制进出两个方向的通信，以达到保护网络的目的。

防火墙基本上是一个独立的进程或一组紧密结合的进程，它有效地监控了内部网和 Internet 之间的任何活动，保证了内部网络的安全，本质上它遵循的是一种允许或阻止业务来往的网络通信安全。一个防火墙应具备如下特性。

(1) 防火墙通常位于内部网和外部网之间的连接处，它是一个网关型的设备，所有进出的流量都必须经过防火墙。

(2) 只有被允许或授权的合法数据，即符合防火墙安全策略的数据，才可以通过防火墙。

(3) 从理论上讲，防火墙本身不受任何攻击的影响。

防火墙的基本功能有以下几个。

(1) 强化安全策略，通过对数据包进行检查，保护内部网络上脆弱的服务。防火墙在