

第 2 章 网络体系结构

知识目标

- 网络通信的概念及要素
- 网络传输介质
- 网络通信协议及标准
- 网络体系结构

教学重点和难点

- 通信三要素
- 分层结构与层次模型
- OSI 参考模型与 TCP/IP 参考模型

2.1 网络通信

2.1.1 通信的概念

人类进行通信的历史已很悠久。千百年来,人们一直使用语言、纸张等来通信,传递信息最基本的方式就是听觉和视觉,人们通过听别人说话,看代表某种意义的字母和符号来得到信息。

1837 年, Samuel Morse 发明了电报, 这个发明使通过一根铜线上的电脉冲来传递信息成为可能。报文的每一字符被转换为一串或长或短的电脉冲。这种传递信息的能力不需明显的听觉或视觉作为媒体, 它带来了一系列的技术革新, 并且永远改变了人们的通信方式。

1876 年, Alexander Graham Bell 进一步发展了电报技术。他发现, 不仅消息能被转换为电信号, 声音也能直接被转换为电信号, 然后由一条电压连续变化的导线传输出去。在导线的另一端, 电信号被重新转换为声音。这样, 任意的两点, 只要它们之间存在着物理连接, 连线两端的人们就能互相通话。在接下来的 70 年里, 电话系统不断发展, 到如今成了一种家庭常用设备。我们只要键入一个号码, 就能和世界各地的人进行交流。

1945 年,世界上第一台电子计算机 ENIAC(电子数字计算机)(图 2.1-1)问世了。尽管 ENIAC 与数据或计算机通信似乎没有直接关系,但是它表现出的快速计算能力在当时的通信系统中至关重要。

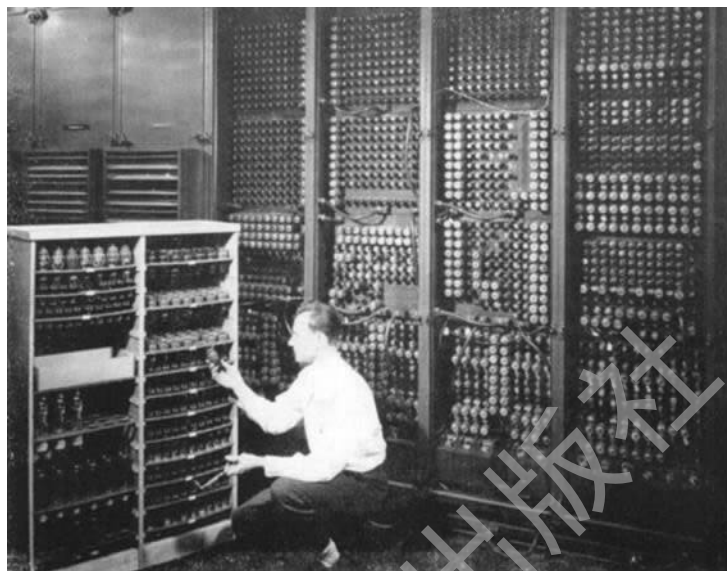


图 2.1-1 ENIAC 的一角

最早的计算机间的通信系统简单而可靠。它基本上是这样实现的:首先,把信息写到一张磁盘上,然后通过人工将磁盘送到另一台计算机。这样,另一台计算机就能从磁盘上读出信息了。

随着 20 世纪 80 年代 PC 机的发展,几乎每一个企业、公司、学校和组织机构都拥有计算机。随着计算机的增加,则要求计算机之间能够更简便地交换信息。90 年代诞生了 Internet,这一应用使世界各地的信息都能够在个人的计算机上轻易得到。计算机和通信发展如此迅猛,以至于一旦失去它们,大多数的企业和学校将无法正常运转。

计算机之间互传数据只是通信的一个方面。很多家庭选用有线电视服务,通过光纤和同轴电缆将电视信号带进家里。通信技术的其他应用还有局域网和广域网,分别允许近距离(LAN)或远距离(WAN)的不同计算机进行通信。一旦连接完毕,用户就可以收发数据文件,进行远程登录了。数据通信与传统的电话通信相比,它们之间在技术和原理上都有很大的不同。

2.1.2 数据信息和数据通信

1. 数据信息

数据是信息的载体,它是客观事实、概念或图像等用于通信的一种形式化的表现。信号是数据的电或电磁的编码。在通信中,我们把数据变成可在传输介质上传送的信号来发送,它可以有两种形式:模拟信号和数字信号(图 2.1-2)。数字信号具有对称的方波波形,而且能发送 1 或 0 的值。我们把具有一定编码、格式和位长要求的数字信号称为数据信息。

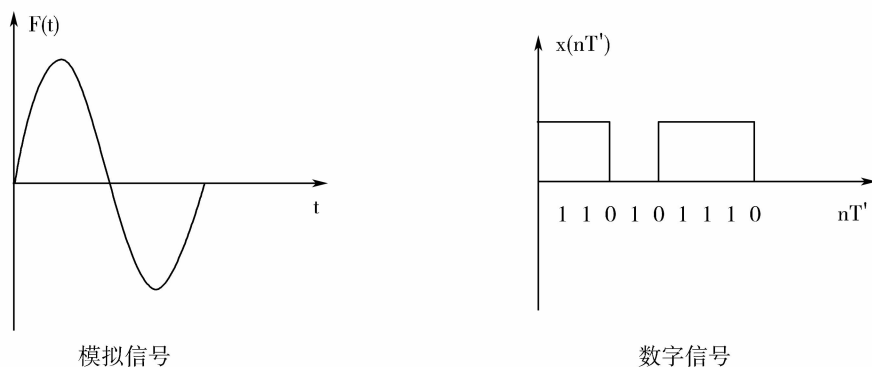


图 2.1-2 模拟信号与数字信号

2. 数据通信

简单地说,数据通信就是将数据信息通过适当的传输线路从一台机器传送到另一台机器。这里的机器可以是计算机、终端设备以及其他任何通信设备。数据通信实质上包含处理和数据传输两层含义。在计算机网络中,数据处理的工作主要由计算机系统来完成,数据传输是靠数据通信系统来实现的。

3. 数据通信的特点

与传统的电报和电话通信相比,数据通信的特点如下:

(1)数据通信可实现人与机器或机器与机器之间的通信,而电话仅仅能完成人与人之间的通信。由于计算机不具备人脑的思维能力,因此要实现计算机与人或计算机之间的交流就一定要靠预先编制的程序来完成,这远比电话系统要复杂。

(2)数据传输的准确性和可靠性要求高。在数据通信中,通常是用二进制的1和0来表示信息的,任何错误都可能造成严重的后果,因此需要较低的误码率,并且传递系统应有自动纠正错误的能力。

(3)传输速率高,响应时间快。数据信号的传输速率依照所使用的带宽不同而不同,通常比电话线传输要迅速快捷。

(4)通信的持续时间差异较大。数据通信的平均信息长度和平均时延随着应用的不同而不同。

(5)数据通信具有灵活的接口,能满足各种设备之间的相互通信。

4. 数据通信的质量指标

数据通信的目的就是及时有效地传递信息。衡量数据传输的质量标准是从有效性和可靠性两方面来考虑的。

(1) 有效性

有效性是指在给定的信道内所能传输的信息量大小。有效性越高的系统性能越好。通常衡量有效性的指标是信息传输速率,在计算机数据通信中,用比特每秒(bit/s)来表示传输速率。

(2) 可靠性

可靠性是指在给定的信道内接收信息的可靠程度。通常衡量可靠性的指标是误码率。在计算机二进制系统中,误码率的定义为:出现错误的比特数/传输的总比特数。

通常误码率越低,通信系统的可靠性也就越高。可靠性和有效性是相互矛盾的。在实际应用中,随着有效性的提高,可靠性往往会降低。因此,应在满足可靠性的前提下,尽可能提高系统的有效性,或在一定的有效性指标下,使信号传输的可靠性尽量提高。

2.1.3 数据传输方式

数据的传输方式分为三大类:基带传输、频带传输和宽带传输。

1. 基带传输

所谓基带就是电信号所固有的基本频率。例如,电视信号的基本频带为 $0\sim 6\text{MHz}$,数字信号的基本频带为零至若干千兆赫兹,由传输速率而定。当利用数据传输系统直接传输基带信号时,则称之为基带传输。

2. 频带传输

所谓频带传输,就是利用调制器把二进制信号调制成能在公共电话线上传输的音频信号(模拟信号),将音频信号在传输介质中传送到接收端后,再经过解调器的解调,把音频信号还原成二进制的电信号。这种把数字信号经过调制后再传输,传输到接收端后再解调还原成数字信号的传输,称为频带传输。频带传输克服了电话线不能直接传送基带信号的缺点,而且能够实现多路复用的目的,从而提高通信线路的利用率。

3. 宽带传输

宽带是指比音频带宽更宽的频带,它包括大部分电磁波频谱。使用这种宽频带进行传输的系统,称为宽带传输系统。它可以容纳全部广播,并可进行高速数据传输。宽带传输系统允许在同一信道上进行数字信息和模拟信息服务。计算机局域网的数据传输系统使用基带传输和宽带传输两种方式,它们的主要区别在于数据传输速率不同。基带数据传输速率为 $0\sim 10\text{Mb/s}$,更典型的是 $1\sim 2.5\text{Mb/s}$;而宽带数据传输速率为 $0\sim 400\text{Mb/s}$,常用的是 $5\sim 10\text{Mb/s}$ 。而且一个宽带信道能被划分为多个逻辑信道,这样就能把声音、图像和数据信息的传输综合在一个物理信道中进行。

依据传输线数目的多寡,可以将数据传送分为两种方式:并行通信和串行通信。通常情况下,并行通信用于短距离、高速率的通信,串行通信用于长距离、低速率的通信。

(1) 并行通信

在并行通信中,数据由多条数据线同时传送与接收,每个比特使用单独的一条线路。如图2.1-3所示,计算机将8个数据位通过8条数据线同时传送给接收端。计算机内部的数据传送,以及计算机与接口之间的数据传送通常都是以并行方式进行的。并行的数据传送线也叫总线,如并行传送8位数据就叫8位总线,并行传送16位数据就叫16位总线。并行通信传输速率快,但是线路成本高,维修不易,且易受干扰。

(2) 串行通信

串行通信就是以比特为单位,按照字符所包含的比特位的顺序,一位接一位地传送,到达对方后,再由通信接收装置将串行比特流还原成字符,如图2.1-4所示。串行通信虽然速度较低,但在接收端与发送端之间只需要一根传输线即可,因而造价低,在计算机网络中普遍采用这种串行通信方式。

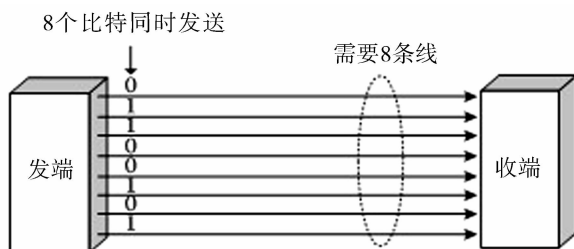


图 2.1-3 并行通信

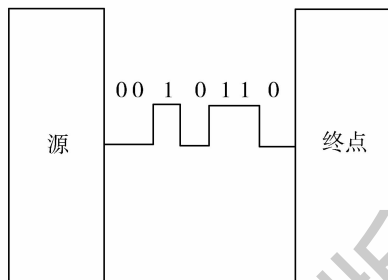


图 2.1-4 串行通信

2.1.4 网络通信要素

通信的目的是传送消息(message),如语音、文字、图像等都是消息。数据(data)是运送消息的实体。信号(signal)则是数据的电气的或电磁的表现。

通信的第一步是将消息或信息从一个人或设备发送给另一个人或设备。人们使用许多不同的通信方式来交流观点。所有这些方式都有三个共同的要素:第一个要素是消息来源,即发送方。消息来源是需要向其他人或设备发送消息的人或电子设备。第二个要素是消息的目的地址,即接收方。目的地址接收并解释消息。第三个要素称为通道,包括提供消息传送途径的介质。

现在我们以使用文字、图片和声音进行通信为例,比如打电话。这些消息都可以通过数据或信息网络来发送。首先将其转换为二进制数字,即比特(亦称位)。然后,将这些比特编码成可以通过适当介质传输的信号。在计算机网络中,介质通常是一种电缆或者无线传输。

所以,在上面的例子中,可以把拨号的一方看成消息来源,接听电话的一方看成是接收方。而电话信号传输依靠的通道,即电话线,就是介质了。

理论上来说,可以将一次通信的内容(如音乐视频或电子邮件消息)作为一大块连续的高容量比特流,通过网络从源发送到目的地。但如果真以这种方式传输消息,那就意味着在传输此数据期间,同一个网络中的其他设备都不能发送或接收消息。这种大型数据流会导致严重的延迟。而且,一旦互联网络基础架构中有一条链路在传输期间出现故障,那么整个消息都会丢失,必须全部重传。

所以,更好的办法是先将数据划分为更小、更易于管理的片段,然后再通过网络发送。将数据流划分为较小的片段称为分段。消息分段主要有两个优点:

首先,通过从源设备向目的设备发送一个个小片段,就可以在网络上交替发送许多不同

的会话。在网络上将交替发送的多个不同会话片段组合起来的过程称为多路复用。

其次,分段可以增强网络通信的可靠性。每个消息的独立片段无须经过网络中的同一条路径从源设备传送到目的设备。因此,如果某条路径因数据流量过大或故障而堵塞,仍可以使用备用路径将各个消息片段转发到目的设备。如果有部分消息未能传送到目的地,则只需重新传输丢失的部分。

由于计算机网络中传输系统的设备费用常常要占整个计算机网络费用的一半左右,因此当通信用户较多而传输的距离较远时,通常不采用两两固定连接的专用线,而采用交换技术,使通信传输线路为各个用户公用,以求提高传输设备的利用率,降低系统费用。

目前实现交换的方法很多,概括起来主要有线路交换和存储交换两大类。

1. 线路交换

线路交换(图 2.1-5)方式就是当计算机与终端或计算机之间需要通信时,由交换机负责在其间建立一条信道,而不改变数据形式。在完成线路接通后,双方通信内容不受交换机干预,即传输的符号、编码、格式及通信控制规程均随用户需要而定,通信速度在信道传输的范围内一般也是任意的,线路的任务仅仅是提供信道和建立连接。

在线路交换方式中,信道为收、发双方独占,数据传送速度快,延迟小,适用于远程成批处理和发送大量数据的场合。但是信道容量完全被用于整个连接过程,即使没有数据传送也是如此,因而线路的利用率相对较低。线路交换又分为空分线路交换和时分线路交换两种类型。

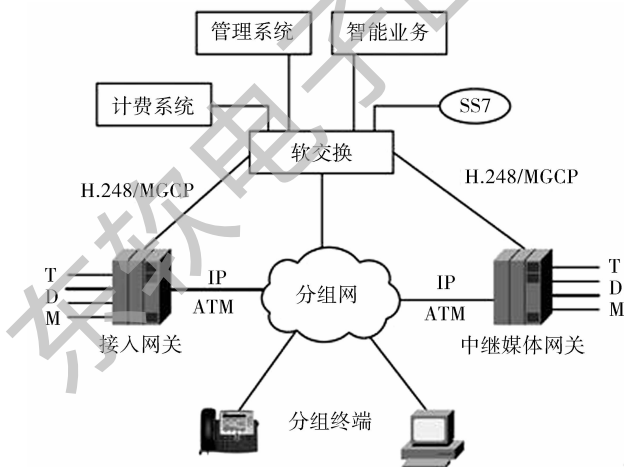


图 2.1-5 线路交换

2. 存储交换

存储交换方式就是在通信处理机中,对所传信息进行存储转发的一种工作方式。当节点收到要求转发的信息后,不管是否接通了目的节点,都让发送节点发送信息,中间节点只起到传递信息的作用,不要求把发送节点和接收节点连接之后才允许发送信息。这种交换方式要求信息有一定格式。根据信息的大小,存储交换又可分为报文交换、分组交换、帧中继交换和信元交换。

(1) 报文交换

报文交换方式就是用户把需要传输的数据,分割成一定大小的报文,每个报文要包含一

个目的地址,以报文为单位在网络中传输。当某一个节点收到一个不是传送给自己的报文后,并且该报文所去终点地址的路径非空闲时,则将报文存储到本节点的外存储器,并且登入输出待发报文登记表中,等到该节点至报文终点地址的路径空闲时,再将该报文向终点地址的方向发送。

报文交换方式的主要优点是:信道可由许多报文同时共享,线路效率比较高;在网络的通信量较大时,报文不会被拒收,而且当原始报文不能通过网络时,报文可以复制、编写和存档;两个数据传输率不同的站可以通过网络中的其他节点连接起来。其缺点是不适合实时或交互通信,网络传输延迟较长。报文交换的主要应用领域是电子邮件、电报、非紧急的业务查询和应答。

(2) 分组交换

分组交换方式也称包交换方式,它是将用户发送的一个报文,分割成若干规定长度的信息组,即分组信息,接着这些分组信息逐一地在网络上通过多个地点(分组交换)发送出去,当这些分组信息到达终点后,再将它们重新装配成完整的报文。在主机中产生的信息是以报文形式出现的,送到主机去的信息也是报文形式,也就是说主机与主机间是以报文形式通信的,报文是面向用户的,根据用户需要而定,格式和长度都是与用户使用要求紧密相连的。而分组是面向网络的,是为传输方便而采用的措施,无论是什么用户,在同一个计算机网络中,其分组的格式都是一样的。分组交换方式具有线路交换方式和报文交换方式的共同优点,并将它们的缺点降至最少。分组交换的主要应用领域是快速查询和应答的任何场合,例如信用核实、储备、电子转账及股票牌价等。

(3) 帧中继交换

由于信道质量差、误码率较高,分组交换技术采用帧校验、接收确认和流量控制等措施来提高传输的可靠性。但同时也严重限制了帧的传输速率。帧中继是在分组交换(x.25)基础上,简化了差错控制(包括检测、重发和确认)、流量控制和路由选择功能而形成的一种新型的交换技术。帧中继以帧为单位进行交换,传输速率可达 2.048 Mb/s。

帧中继的通信子网只有物理层和数据链路层,没有网络层。差错控制仅在源和目的两端进行,并在数据链路层通过永久虚电路的映射来进行路由选择。

(4) 信元交换

信元是比帧更小的信息单元,由信头和信息段组成,传输系统通过信头识别通路。在异步传输模式(ATM)中,信元规定为 53 字节,前 5 个字节为信头,其余 48 个字节为信息段。这样,每一个信元都花费同样的传输时间,从而可以把信道的时间划分为一个时间片序列,每个时间片用来传输一个信元。当交换器有信元发送时,便逐个时间片地把信元投入信道;接收时,若信道不空闲,也将逐个时间片地取得信元,时间片和信元一一对应。这种对应关系可大大简化对信元的传输控制,便于采用高速硬件对信头进行识别和交换处理。

在 ATM 中,只要信道空闲,便将信元投入信道,有利于提高信道的利用率。由于发送无固定周期,因而又被称为异步传输模式。

2.1.5 网络传输介质

1. 网络传输介质分类

网络传输介质是指在网络中传输信息的载体,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

指在两个通信设备之间实现物理连接的部分,它可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

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。

不同的传输介质其特性也各不相同,它们不同的特性对网络中数据通信质量和通信速度有较大影响。

任何信息传输和共享都需要有传输介质,计算机网络也不例外。对于一般计算机网络用户来说,可能没有必要了解过多的细节,例如计算机之间依靠何种介质、以怎样的编码来传输信息等。但是,对于网络设计人员或网络开发者来说,了解网络底层的结构和工作原理是必要的,因为他们必须掌握信息在不同介质中传输时的衰减速度和发生传输错误时如何去纠正这些错误。

2. 网络传输介质的特性

当需要决定使用哪一种传输介质时,必须将连网需求与介质特性进行匹配。通常说来,选择数据传输介质时必须考虑 5 种特性:吞吐量和带宽、成本、尺寸和可扩展性、中间设备以及抗噪性。

(1) 吞吐量和带宽

在选择一个传输介质时所要考虑的最重要的因素可能是吞吐量。吞吐量是在一给定时间段内介质能传输的数据量,它通常用每秒兆位(1 000 000 位)或 Mbps 进行度量。吞吐量也被称为容量,每种传输介质的物理性质决定了它的潜在吞吐量。例如,物理规律限制了电沿着铜线传输的速度,也正如它们限制了能通过一根直径为 1 英寸的胶皮管传输的水量一样,假如试图引导超过它处理能力的水量,最后只能是溅你一身水;同样,如果试图将超过它处理能力的的数据量沿着一根铜线传输,结果将是数据丢失或出错。

与传输介质相关的噪声和设备能进一步限制吞吐量,充满噪声的电路将花费更多的时间补偿噪声,因而只有更少的资源可用于传输数据。带宽这个术语常常与吞吐量交换使用。严格地说,带宽是对一个介质能传输的最高频率和最低频率之间的差异进行度量;频率通常用 Hz 表示,它的范围直接与吞吐量相关。例如,若 FCC(美国联邦通讯委员会)通知你能够在 870~880 MHz 之间传输无线信号,那么分配给你的带宽将是 10 MHz。通常情况下,带宽越高,吞吐量就越高。

(2) 成本

不同种类的传输介质涉及的成本是难以准确描述的。它们不仅与环境中现存的硬件有关,而且还与你所处的场所有关。下面的变量都可能影响采用某种类型介质的最后成本。

安装成本:你能自己安装介质吗?或你必须雇佣承包商做这件事吗?你是否需要拆墙或修建新的管道或机柜?你是否需要从一个服务提供商处租借线路?

新的基础结构相对于复用已有基础结构的成本:你是否能使用已有的电线或在某些情

况下安装所有新的 5 类 UTP? 如果你能使用已有的 3 类 UTP, 电线将可以不用付费。假如仅仅替换基础结构的一部分, 它是否能轻易地与已有介质集成?

维护和支持成本: 假如复用已有的介质基础结构常常需要修理或改进, 复用并不省任何钱。同时, 假如使用了一种不熟悉的介质类型, 可能需要花费更多成本去雇佣一个技师维护它。你是否能自己维护介质, 或你是否必须雇佣承包商维护它?

因低传输速率而影响生产效率所付出的代价: 如果你通过复用已有的低速的线路来省钱, 你是否可能因为降低了生产率而遭受损失? 换言之, 你是否使你的员工在进行保存和打印报告或发送邮件时等待更长的时间?

更换过时介质的成本: 你是否选择了要被逐渐淘汰或需迅速替换的介质? 你是否能发现某种价格合理的连接硬件与你几年前选择的介质相兼容?

(3) 尺寸和可扩展性

三种规格决定了网络介质的尺寸和可扩展性: 每段的最大节点数、最大段长度以及最大网络长度。在进行布线时, 这些规格中的每一个都是基于介质的物理特性的。每段最大节点数与衰减有关, 即通过一给定距离信号损失的量有关。对于一个网络段来说每增加一个设备都将略微增加信号的衰减。为了保证一个清晰的强信号, 必须限制一个网络段中的节点数。

网络段的长度也应因衰减而受到限制。在传输一定的距离之后, 一个信号可能因损失得太多以至于无法被正确解释。在这种损失发生之前, 网络上的中继器必须重发和放大信号。一个信号能够传输并仍能被正确解释的最大距离即为最大段长度。若超过这个长度, 更易于发生数据损失。类似于每段最大节点数, 最大段长度也因介质类型不同而不同。在一种理想的环境中, 网络可以在发送方和接收方之间实时传输数据, 不论两者之间相隔多远。不幸的是我们没有生活在一个理想的环境中, 一个信号从它的发送到它的最后接收之间存在一个延迟, 每个网络都受这个延迟的支配。

例如, 当你在计算机上敲一个键将一个文件保存到网络上时, 文件的数据在它到达服务器的硬盘时必须通过网络接口卡、网络中的一个集线器或也可能是一个交换机或路由器、更多的电缆以及服务器的网络接口卡。虽然电子传输迅速, 它们仍然不得经过传输这一过程。这个过程在你敲键的那一刻和服务器接收数据的那一刻之间必然存在一个短暂的延迟, 这种延迟被称为时延。如同存在一个连通设备, 如一路由器, 接入设备的转换时间将影响时延, 所使用的电缆的长度也将影响时延。但是, 仅仅当一个接收节点正期望接收某种类型的数据时, 如它已开始接收的数据流的剩余部分, 时延的影响将可能成为问题。假如该接收节点未能接收数据流的剩余部分, 它将认为没有更多的数据输入, 这将导致网络上的传输错误。同时, 当连接多个网络段时, 也将增加网络上的时延。为了限制时延并避免相关的错误, 每种类型的介质都标定一个最大连接段数。

(4) 中间设备

中间设备是连接电缆与网络设备的硬件。网络设备可以是一个文件服务器、工作站、交换机或打印机。每种网络介质都对应一种特定类型的连接器。所使用的连接器的种类将影响网络安装和维护的成本、网络增加段和节点的难易度, 以及维护网络所需的专业技术知识。用于 UTP 电缆的连接器在接入和替换时比用于同轴电缆的连接器的接入和替换要简

单得多,UTP 电缆连接器同时也更廉价并可用于许多不同的介质设计。

(5)抗噪性

在网络传输中,噪声能使数据信号变形。噪声影响一个信号的程度与传输介质有一定关系。某些类型的介质比其他介质更易于受噪声影响。无论是何种介质,都有两种类型的噪声会影响它们的数据传输:电磁干扰(EMI)和射频干扰(RFI)。EMI 和 RFI 都是从电子设备或传输电缆发出的波。发动机、电源、电视机、复制机、荧光灯以及其他的电源都能产生 EMI 和 RFI。RFI 也可由来自广播电台或电视塔的强大广播信号产生。

任何一种噪声,其实都能够采取措施限制它对网络的干扰。例如,可以远离强大的电磁源进行布线。如果环境仍然使网络易受影响,应选择一种能限制影响信号噪声量的传输。电缆可以通过屏蔽、加厚或抗噪声算法获得抗噪性。假如屏蔽的介质仍然不能避免干扰,可以使用金属管道或管线以抑制噪声并进一步保护电缆。但这些措施都会进一步加大成本,所以如何在成本和质量间找到平衡点,是选用网络介质时需要考虑的问题。

3. 主要使用的三种介质

现代网络主要使用三种介质来连接设备并提供传输数据的途径。

(1)双绞线

双绞线(图 2.1-6)简称 TP,将一对以上的双绞线封装在一个绝缘外套中。为了降低信号的干扰程度,电缆中的每一对双绞线一般是由两根绝缘铜导线相互扭绕而成的,也因此把它称为双绞线。双绞线分为非屏蔽双绞线(UTP)和屏蔽双绞线(STP)。

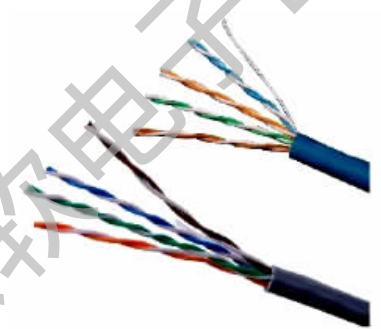


图 2.1-6 双绞线

(2)光纤

光纤(图 2.1-7)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。它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。



图 2.1-7 光纤

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。光纤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。

(3)无线传输

无线电波是指在自由空间(包括空气和真空)传播的射频频段的电磁波。无线电技术是通过无线电波传播声音或其他信号的技术,如图 2.1-8 所示。

无线电技术的原理在于,导体中电流强弱的改变会产生无线电波。利用这一现象,通过调制可将信息加载于无线电波之上。当电波通过空间传播到达收信端,电波引起的电磁场变化又会在导体中产生电流。通过解调将信息从电流变化中提取出来,就达到了信息传递的目的。



图 2.1-8 无线技术

2.2 网络协议与体系结构

2.2.1 网络协议概述

无论是面对面还是通过网络进行的所有通信都要遵守预先确定的规则,即协议。这些协议由会话的特性决定。在日常的个人通信中,通过一种介质(如电话)通信时采用的规则不一定与使用另一种介质(如邮寄信件)时的协议相同。

网络中不同主机之间的成功通信需要在许多不同协议之间进行交互。执行某种通信功能所需的一组内在相关协议称为协议族。这些协议通过加载到各台主机和网络设备的软件和硬件中执行。

通常将网络协议定义成为在计算机网络中进行数据交换而建立的规则、标准或约定的

集合。例如,网络中一个微机用户和一个大型主机的操作员进行通信,由于这两个数据终端所用字符集不同,因此操作员所输入的命令彼此不认识。为了能进行通信,规定每个终端都要将各自字符集中的字符先变换为标准字符集的字符后,才进入网络传送,到达目的终端之后,再变换为该终端字符集的字符。当然,对于不相容终端,除了需变换字符集字符外,其他特性,如显示格式、行长、行数、屏幕滚动方式等也需作相应的变换。

要直观地了解所有协议在特定主机上的交互方式,最好的办法之一是将其视为协议栈。协议栈显示了在主机上实现协议族中每个协议的方式。协议被显示为分层的架构,每种上层服务都依赖于其余下层协议所定义的功能。协议栈的下层负责通过网络传输数据和向上层提供服务,而上层则负责处理发送的报文内容和用户界面,如图 2.2-1 所示。

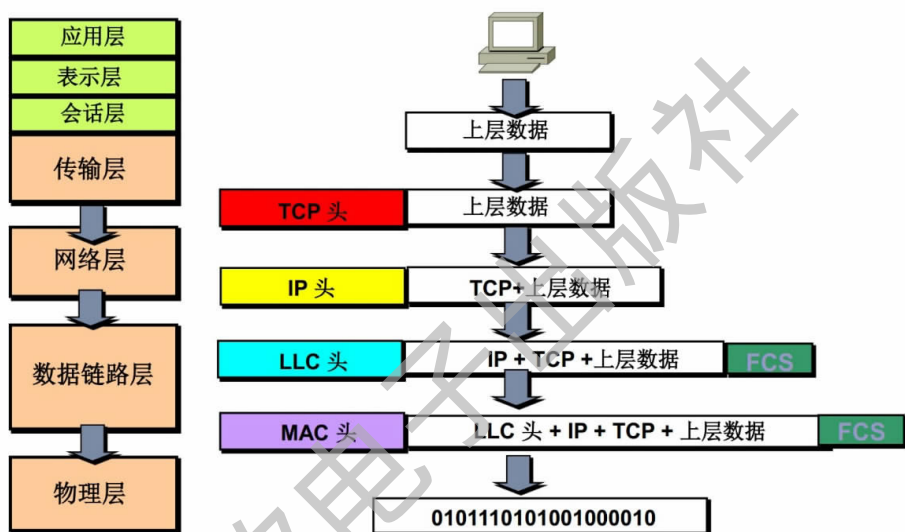


图 2.2-1 数据交互

以两人面对面通信为例,我们可以使用三个层来描述此活动。底层是物理层,两人都可以通过声音说出词语。第二层是规则层,两人同意用通用语言交谈。顶层是内容层,两人实际说出来的词语,即通信的内容。

总的说来,协议是用来描述进程之间信息交换数据时的规则术语。在计算机网络中,两个相互通信的实体处在不同的地理位置,其上的两个进程相互通信,需要通过交换信息来协调它们的动作达到同步,而信息的交换必须按照预先共同约定好的规则进行。

网络协议由三个要素组成:

(1)语义。语义是解释控制信息每个部分的意义。它规定了需要发出何种控制信息,以及完成的动作与做出什么样的响应。

(2)语法。语法是用户数据与控制信息的结构与格式,以及数据出现的顺序。

(3)时序。时序是对事件发生顺序的详细说明(也可称为“同步”)。

人们形象地把这三个要素描述为:语义表示要做什么;语法表示要怎么做;时序表示做的顺序。

网络上的计算机之间又是如何交换信息的呢?就像我们说话用某种语言一样,在网络上的各台计算机之间也有一种语言,这就是网络协议,不同的计算机之间必须使用相同的网

络协议才能进行通信。

网络协议是网络上所有设备(网络服务器、计算机及交换机、路由器、防火墙等)之间通信规则的集合,它规定了通信时信息必须采用的格式和这些格式的意义。大多数网络都采用分层的体系结构,每一层都建立在下层之上,向它的上一层提供一定的服务,而把如何实现这一服务的细节对上一层加以屏蔽。一台设备上的第 n 层与另一台设备上的第 n 层进行通信的规则就是第 n 层协议。在网络的各层中存在着许多协议,接收方和发送方同层的协议必须一致,否则一方将无法识别另一方发出的信息。网络协议使网络上各种设备能够相互交换信息。常见的协议有 TCP/IP 协议、IPX/SPX 协议、NetBEUI 协议等。

当然,网络协议也有很多种,具体选择哪一种协议则要看情况而定。Internet 上的计算机使用的是 TCP/IP 协议。

ARPAnet 成功的主要原因是因为它使用了 TCP/IP 标准网络协议,TCP/IP (Transmission Control Protocol/Internet Protocol)——传输控制协议/互联网协议是 Internet 采用的一种标准网络协议。它是由 ARPA 于 1977~1979 年推出的一种网络体系结构和协议规范。随着 Internet 的发展,TCP/IP 也得到进一步的研究开发和推广应用,成为 Internet 上的“通用语言”。

2.2.2 分层与协议

在计算机网络中,要使数据从源传递到目的地,网络上所有设备需要“讲”相同的语言,比如交流什么、怎样交流,及何时交流等,都必须事先约定好互相都能接受的规则,这就是协议。协议是使网络通信更加有效的一组规则的集合。这就好比我们在现实生活中需要通过遵守相应的规则使生活和社会变得更加有序一样。例如开车的时候,在转弯时必须打出转弯灯来通知周围的车辆,否则将会造成交通的混乱和阻塞。

我们把计算机网络中用于规定信息的格式以及如何发送和接收信息的一套规则称为网络协议。

网络通信的过程是复杂的。数据以电子信号的形式,穿越介质到达正确的目的计算机,然后被转换成它最初的形式,以便接收者能够阅读。这一过程由多个步骤构成,网络设计者在为这个过程设计协议时,为了减少网络协议设计的复杂性,并不是设计一个单一、巨大的协议来为所有形式的通信规定完整的细节,而是采用把通信问题划分为许多个小问题,然后为每个小问题设计一个单独的协议的方法,亦即协议分层的方法。这样做使每个协议的设计、分析、编码和测试都比较容易。分层模型是一种用于开发网络协议的设计方法。本质上,分层模型描述了把通信问题分为几个小问题(称为层次)的方法,每个小问题对应于一层。

我们以邮政系统为例来说明协议分层。人们平常写信时,都有个约定,这就是信件的格式和内容。首先,我们写信时必须采用双方都懂的语言文字和文体,开头是对方称谓,最后是落款等。这样,对方收到信后,才可以看懂信中的内容,知道是谁写的,什么时候写的等。信写好之后,必须将信装在信封里交由邮局寄发,寄信人和邮局之间也要有约定,这就是规定信封写法并贴邮票。在中国寄信必须先写收信人地址、姓名,然后才写寄信人的地址和姓名。邮局收到信后,首先进行信件的分拣和分类,然后交付有关运输部门进行运输,如航空

信交民航,平信交铁路或公路运输部门等。这时,邮局和运输部门也有约定,如到站地点、时间、包裹形式等。信件运送到目的地后进行相反的过程,最终将信件送到收信人手中,收信人依照约定的格式才能读懂信件。

在整个过程中,主要涉及用户、邮局和运输3个方面。为了将信件准确地送达收信人,用户和用户、邮局和邮局、运输部门和运输部门,以及用户和邮局、邮局和运输部门之间都就具体的事情有一些约定。信件在传递时,并不是由写信人直接送到了收信人,而是经由写信人、邮局一级级送到运输部门,再由运输部门将信送出去,到达收信人所在地运输部门,再经邮局送到收信人手中。在这个过程中,写信人和收信人都是最终用户,处于最高层,邮局处于用户的下一层,是为用户服务的,对于用户来说,他只需知道如何按邮局的约定把信写好寄出去就行了,而无须知道邮局是如何为他服务的,这个过程对用户是透明的。运输部门是为邮局服务的,并且负责实际的邮件的运送,处于整个邮政系统的最底层,

网络中的通信与此类似,大多数网络都是按层的方式来组织的,每一层都建立在它的下层之上。不同的网络,其层的数量以及各层的名字、内容和功能都不尽相同。然而,在所有的网络中,每一层的目的都是向它的上一层提供一定的服务,而把如何实现这一层的细节对上一层加以屏蔽。网络中的数据也并不是从一台机器的第 n 层直接传送到另一台机器的第 n 层,而是每一层都把数据和控制信息交给它的下一层,直到最下层,将数据传送到对方的最下层,再一层一层地往上送至第 n 层。

分层的基本原则是:

(1)网络中的每一节点都具有相同的分层结构,在每一相邻层间有一个定义清晰的接口,该接口定义下层向上层提供的原语操作和服务。

(2)每一层完成一组特定的有明确含义的协议功能,并尽可能地减少在相邻层间传递信息的数量。

(3)同一节点中的每一层能够同相邻层通信,但是不能跨层通信。两个节点间的通信,除物理层(最低层)为水平通信外,其他各层都是垂直通信,也就是说网络中各个节点之间的直接接口,只能是物理层。

协议分层带来以下几个好处:

(1)使复杂的通信控制结构便于管理,因为每一个控制层的功能,都是在它的下一层提供的服务上增加一部分新的相对来说较少的功能,整个系统的正确性建立在每一控制层的正确性的基础上。

(2)使复杂的通信控制结构的实现更为可靠,避免在一个功能部件或接口上出现的故障扩散成为危及整个系统的大故障。

(3)由于每一层的功能都是独立的,因此对其修改和增加不会影响其他的控制层。

在分层结构中,各层有各层的协议。一台机器上的第 n 层与另一台机器上的第 n 层进行通话,通话的规则就是第 n 层协议。不同机器(节点)内包含相应协议层的实体叫做对等进程。换句话说,正是这些对等进程利用这些协议进行通信。

层和协议的集合叫做网络体系结构。体系结构的描述必须包含足够的信息,使实现者可以用来为每一层编写程序和进行硬件设计,并使之符合有关协议。协议的具体实现(含软件和硬件)叫做规程,它们对外部来说是不可见的。只要机器能够正确地使用全部协议,其

实现的细节和接口完全不必相同。例如,用卫星信道来代替所有的电话信道,只要这种新的技术能向上层提供旧的技术所提供的同样一组服务就行了。

OSI 参考模型用物理层、数据链路层、网络层、传输层、会话层、表示层和应用层七个层次描述网络的结构,它的规范对所有的厂商是开放的,具有指导国际网络结构和开放系统走向的作用。它直接影响总线、接口和网络的性能。常见的网络体系结构有 FDDI、以太网、令牌环网和快速以太网等。从网络互联的角度看,网络体系结构的关键要素是协议和拓扑。

网络体系结构定义计算机设备和其他设备如何连接在一起以形成一个允许用户共享信息和资源的通信系统。存在专用网络体系结构,如 IBM 的系统网络体系结构(SNA)和 DEC 的数字网络体系结构(DNA);也存在开放体系结构,如国际标准化组织(ISO)定义的开放式系统互联(OSI)模型。网络体系结构在层中定义。如果这个标准是开放的,它就向厂商们提供了设计与其他厂商产品具有协作能力的软件和硬件的途径。然而,OSI 模型还保持在模型阶段,它并不是一个已经被完全接受的国际标准。考虑到大量的现存事实上的标准,许多厂商支持在工业界使用的不同协议,而不是仅仅接受一个标准。

通信是任何网络体系结构的基本目标。在过去,一个厂商需要非常关心他自己的产品可以相互之间进行通信,并且如果他公开这种体系结构,那么其他厂商就也可以生产和此竞争的产品了,这样就使这些产品之间的兼容通常是很困难的。在任何情况下,协议都是定义通信如何在不同操作的级别发生的一组规则和过程。一些层定义物理连接,例如电缆类型、访问方式、网络拓扑,以及数据是如何在网络之上进行传输的。向上是一些关于在系统之间建立连接和进行通信的协议,再向上就是定义应用如何访问低层的网络通信功能,以及如何连接到这个网络的其他应用

如上所述,OSI 模型已经成为所有其他网络体系结构和协议进行比较的一个模型。这种 OSI 模型的目的就是协调不同厂商之间的通信标准。虽然一些厂商还在继续追求他们自己的标准,但是像 DEC 和 IBM 这样的一些公司已经将 OSI 和像 TCP/IP 这样的 Internet 标准一起集成到他们的联网策略中了。

当许多 LAN 被连接成企业网时,互操作性是很重要的,可以使用许多不同的技术来达到这一目的,其中包括在单一系统中使用多种协议或使用可以隐藏协议的“中间件”的技术。中间件还可以提供一个接口来允许在不同平台上的应用交换信息。使用这些技术,用户就可以从他们的台式应用来访问不同的多厂商产品了。

2.2.3 计算机网络体系结构的形成

网络体系结构是指通信系统的整体设计,它为网络硬件、软件、协议、存取控制和拓扑提供标准。它广泛采用的是国际标准化组织(ISO)在 1979 年提出的开放系统互联(OSI-Open System Interconnection)的参考模型。

要研究计算机网络体系结构的诞生,不得不提到一个词:ARPA。所谓“阿帕”(ARPA),是美国高级研究计划署(Advanced Research Project Agency)的简称。它的核心机构之一是信息处理处(Information Processing Techniques Office, IPTO),一直在关注电脑图形、网络通信、超级计算机等研究课题。

阿帕网为美国国防部高级研究计划署开发的世界上第一个运营的封包交换网络,它是全球互联网的始祖。

从某种意义上说,Internet 可以说是美苏冷战的产物。在美国,20 世纪 60 年代是一个很特殊的时代。60 年代初,古巴核导弹危机发生,美国和苏联之间的冷战状态随之升温,核毁灭的威胁成了人们日常生活的话题。在美国对古巴封锁的同时,越南战争爆发,许多第三世界国家发生政治危机。由于美国联邦经费的刺激和公众恐惧心理的影响,“实验室冷战”也开始了。人们认为,能否保持科学技术上的领先地位,将决定战争的胜负。而科学技术的进步依赖于电脑领域的发展。到了 60 年代末,每一个主要的联邦基金研究中心,包括纯商业性组织、大学,都有了由美国新兴电脑工业提供的最新技术装备的电脑设备。电脑中心互联以共享数据的思想得到了迅速发展。

美国国防部认为,如果仅有一个集中的军事指挥中心,万一这个中心被苏联的核武器摧毁,全国的军事指挥将处于瘫痪状态,其后果将不堪设想,因此有必要设计这样一个分散的指挥系统——它由一个个分散的指挥点组成,当部分指挥点被摧毁后其他点仍能正常工作,而这些分散的点又能通过某种形式的通信网取得联系。

1969 年 11 月,ARPA 开始建立一个命名为 ARPAnet 的网络,但是只有 4 个节点:分布在洛杉矶的加利福尼亚州大学洛杉矶分校、加州大学圣巴巴拉分校、斯坦福大学、犹他州大学四所大学的 4 台大型计算机。选择这 4 个节点的一个因素是考虑到不同类型主机联网的兼容性。对 ARPAnet 发展具有重要意义的是它利用了无限分组交换网与卫星通信网。通过专门的接口信号处理机(IMP)和专门的通信线路,把美国的几个军事及研究中心用电脑主机连接起来。起初是为了便于这些学校之间互相共享资源而开发的。ARPAnet 采用了包交换机制。当初,ARPAnet 只连接 4 台主机,从军事要求上是置于美国国防部高级机密的保护之下,从技术上它还不具备向外推广的条件。ARPAnet 主要是用于军事研究目的,它主要是基于这样的指导思想:网络必须经受得住故障的考验而维持正常的工作,一旦发生战争,当网络的某一部分因遭受攻击而失去工作能力时,网络的其他部分应能维持正常的通信工作。ARPAnet 在技术上的另一个重大贡献是 TCP/IP 协议族的开发和利用。作为 Internet 的早期骨干网,ARPAnet 的试验奠定了 Internet 存在和发展的基础,较好地解决了异种机网络互联的一系列理论和技术问题。

到了 1975 年,ARPAnet 已经连入了 100 多台主机,并结束了网络试验阶段,移交美国国防部国防通信局正式运行。在总结第一阶段建网实践经验的基础上,研究人员开始了第二代网络协议的设计工作。这个阶段的重点是网络互联问题,网络互联技术研究的深入促进了 TCP/IP 协议的出现与发展。到 1979 年,越来越多的研究人员投入到了 TCP/IP 协议的研究与开发之中。在 1980 年前后,ARPAnet 所有的主机都转向 TCP/IP 协议。到 1983 年 1 月,ARPAnet 向 TCP/IP 的转换全部结束。同时,美国国防部国防通信局将 ARPAnet 分为两个独立的部分,一部分仍叫 ARPAnet,用于进一步的研究工作;另一部分稍大一些,成为著名的 Milnet,用于军方的非机密通信。

1983 年,ARPA 和美国国防部通信局研制成功了用于异构网络的 TCP/IP 协议,美国加利福尼亚伯克利分校把该协议作为其 BSDUNIX(是加州大学伯克利分校软件组设计的操作系统)的一部分,使该协议得以在社会上流行起来,从而诞生了真正的 Internet(互联网)。同时,

局域网和广域网的产生和蓬勃发展对 Internet 的进一步发展起了重要的作用。其中最引人注目的是美国国家科学基金会 NSF(National Science Foundation)建立的 NSFnet。NSF 在全美国建立了按地区划分的计算机广域网并将这些地区的网络和超级计算机中心互联起来。

1986 年,NSF 利用 ARPAnet 发展出来的 IP 通讯,在 5 个科研教育服务超级电脑中心的基础上建立了 NSFnet 广域网。由于 NSF 的鼓励和资助,很多大学、政府资助的研究机构甚至私营的研究机构纷纷把自己的局域网并入 NSFnet 中。那时,ARPAnet 的军用部分已脱离母网,建立自己的网络——Milnet。网络之父 ARPAnet 逐步被 NSFnet 所替代。到 1990 年,ARPAnet 已退出了历史舞台。如今,NSFnet 已成为 Internet 的重要骨干网之一。

ARPA 于 1971 年更名为 DARPA,因此有时用 DARPAnet 来表示 ARPAnet,这两个词表示同一个意思。

以现在的水平论,这个最早的网络显得非常原始,传输速度也慢得让人难以接受。但是,阿帕网的四个节点及其链接,已经具备网络的基本形态和功能,所以阿帕网的诞生通常被认为是网络传播的“创世纪”。

不过,阿帕网问世之际,大部分电脑还互不兼容。于是,如何使硬件和软件都不同的电脑实现真正的互联,就是人们力图解决的难题。这个过程中,文顿·瑟夫为此做出首屈一指的贡献,从而被称为“互联网之父”。

计算机网络是一个非常复杂的系统,需要解决的问题很多并且性质各不相同。所以,在 ARPAnet 设计时,就提出了“分层”的思想,即将庞大而复杂的问题分为若干较小的易于处理的局部问题。

1974 年美国 IBM 公司按照分层的方法制定了系统网络体系结构 SNA(System Network Architecture)。SNA 已成为世界上较广泛使用的一种网络体系结构。

一开始,各个公司都有自己的网络体系结构,使各公司自己生产的各种设备容易互联成网,有助于该公司垄断自己的产品。但是,随着社会的发展,不同网络体系结构的用户迫切要求能互相交换信息。为了使不同体系结构的计算机网络都能互联,国际标准化组织 ISO 于 1977 年成立专门机构研究这个问题。1978 年 ISO 提出了“异种机连网标准”的框架结构,这就是著名的开放系统互联基本参考模型 OSI/RM(Open Systems Interconnection Reference Model),简称 OSI。

OSI 得到了国际上的承认,成为其他各种计算机网络体系结构依照的标准,大大地推动了计算机网络的发展。20 世纪 70 年代末到 80 年代初,出现了利用人造通信卫星进行中继的国际通信网络。网络互联技术不断成熟和完善,局域网和网络互联开始商品化。

2.3 OSI 参考模型

2.3.1 OSI 参考模型概述

OSI(Open System Interconnect)开放式系统互联,一般都叫 OSI 参考模型,是 ISO(国

际标准化组织)组织在 1985 年研究的网络互联模型。国际标准化组织 ISO 发布的最著名的标准是 ISO/iIEC 7498,又称为 X.200 协议。该体系结构标准定义了网络互联的七层框架,即 ISO 开放系统互联参考模型。在这一框架下进一步详细规定了每一层的功能,以实现开放系统环境中的互联性、互操作性和应用的可移植性。

开放系统 OSI 标准定制过程中所采用的方法是将整个庞大而复杂的问题划分为若干个容易处理的小问题,这就是分层的体系结构方法。在 OSI 中,采用了三级抽象,即体系结构、服务定义和协议规定说明。

OSI 参考模型定义了开放系统的层次结构、层次之间的相互关系及各层所包含的可能的服务。它作为一个框架来协调和组织各层协议的制定,也是对网络内部结构最精练的概括与描述进行整体修改。

OSI 的服务定义详细说明了各层所提供的服务。某一层的服务就是该层及其下各层的一种能力,它通过接口提供给更高一层。各层所提供的服务与这些服务是怎么实现的无关。同时,各种服务定义还定义了层与层之间的接口和各层所使用的原语,但是不涉及接口是怎么实现的。

OSI 标准中的各种协议精确定义了应当发送什么样的控制信息,以及应当用什么样的过程来解释这个控制信息。协议的规程说明具有最严格的约束。

ISO/OSI 参考模型并没有提供一个可以实现的方法,只是描述了一些概念,用来协调进程间通信标准的制定。在 OSI 范围内,只有各种协议是可以被实现的而各种产品只有和 OSI 的协议相一致才能互联。这也就是说,OSI 参考模型并不是一个标准,而只是一个在制定标准时所使用的概念性的框架。

从历史来看,在制定计算机网络标准方面起着很大作用的两大国际组织是 CCITT 和 ISO。CCITT 与 ISO TC97 的工作领域是不同的,CCITT 主要是从通信角度考虑一些标准的制定,而 ISO 的 TC97 则关心信息的处理与网络体系结构。但是随着科学技术的发展,通信与信息处理的界限变得比较模糊了。于是,通信与信息处理就成了 CCITT 与 TC97 共同关心的领域。CCITT 的建议书 X.200 就是开放系统互联的基本参考模型,它和 ISO 7498 基本是相同的。

网络刚刚出现的时候,很多大型的公司都拥有了网络技术,公司内部计算机可以相互连接,可是却不能与其他公司连接,因为没有有一个统一的规范。计算机之间相互传输的信息对方不能理解,所以不能互联。

ISO 为了更好地使网络应用更为普及,就推出了 OSI 参考模型,其含义就是推荐所有公司使用这个规范来控制网络,这样所有公司都有相同的规范,就能互联了。提供各种网络服务功能的计算机网络系统是非常复杂的。根据分而治之的原则,ISO 将整个通信功能划分为七个层次,划分原则是:

- (1) 网路中各节点都有相同的层次;
- (2) 不同节点的同等层具有相同的功能;
- (3) 同一节点内相邻层之间通过接口通信;
- (4) 每一层使用下层提供的服务,并向其上层提供服务;
- (5) 不同节点的同等层按照协议实现对等层之间的通信。

2.3.2 OSI 参考模型的内容

为了使不同计算机厂家生产的计算机能够相互通信,以便在更大的范围内建立计算机网络,ISO 在 1978 年提出了“开放系统互联参考模型”,即著名的 OSI/RM 模型(Open System Interconnection/Reference Model),如图 2.3-1 所示。它将计算机网络体系结构的通信协议划分为七层,自下而上依次为:物理层(Physical Layer)、数据链路层(Data Link Layer)、网络层(Network Layer)、传输层(Transport Layer)、会话层(Session Layer)、表示层(Presentation Layer)、应用层(Application Layer)。

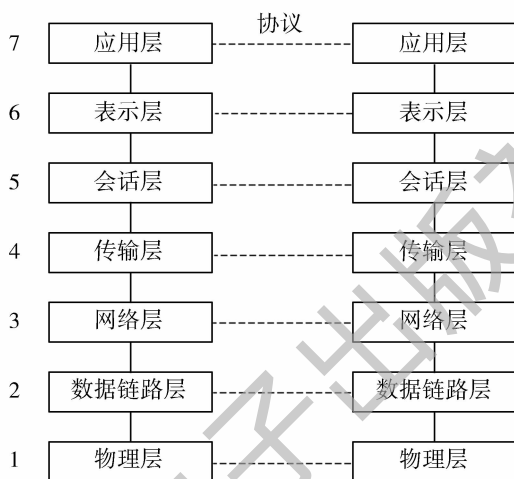


图 2.3-1 网络体系结构

其中第四层完成数据传送服务,上面三层面向用户。对于每一层,至少制定两项标准:服务定义和协议规范。前者给出了该层所提供的服务的准确定义,后者详细描述了该协议的动作和各种有关规程,以保证服务的提供。

1. 物理层

物理层是 OSI 分层体系结构中的最底层,它是建立在通信介质的基础上,实现系统和通信介质的物理接口。利用机械的、电气的功能和规程特性,在数据终端设备(DTE)和数据通信设备(DCE)之间,实现对物理链路的建立、保持和拆除功能;在两个或多个节点互联的链路上,进行发送端到接收端位流的传送。而物理的连接可以是专线连接或交换连接,也可以是全双工传输或半双工传输、同步传输或异步传输等。

物理层考虑的是怎样才能能在连接各种计算机的传输媒体上传输数据的比特流,而不是指连接计算机的具体的物理设备或具体的传输媒体。现有的计算机网络中的物理设备和传输媒体的种类非常多,而通信手段也有许多不同的方式。物理层的作用正是要尽可能地屏蔽掉这些差异,使其上面的数据链路层感觉不到这些差异,这样就可以使数据链路层只需要考虑如何完成本层的协议和服务,而不必考虑网络具体的传输媒体是什么。用于物理层的协议也常称为物理层规程(procedure)。

可以将物理层的主要任务描述为确定与传输媒体的接口的一些特性,即:

(1)机械特性:规定了物理连接时采用的连接器的规格、尺寸、引脚数量和排列方式等。

一般来说, DTE 的连接器常用插针形式, 其几何尺寸与 DCE 连接器相配合, 插针芯数和排列方式与 DCE 连接器成镜像对称。

(2) 电气特性: 规定了二进制位流传输时, 线路上信号电压高低、阻抗匹配、传输速率和距离限制。它定义了发送器和接收器的电气特性, 同时还规定了互连电缆的内容。物理层接口的电气特性主要分为三类: 非平衡型、非平衡输出/平衡输入型和平衡输出/非平衡输入型。

(3) 功能特性: 说明某条线上出现的某一电平的电压表示何种意义。

(4) 规程特性: 定义了信号线传输二进制位流的一组操作过程, 即信号线的工作过程及次序。

在物理连接上的传输方式一般都是串行传输, 即一个一个比特按照时间顺序传输。但是, 有时也可以采用多个比特的并行传输方式。出于经济上的考虑, 远距离的传输通常都是串行传输。

2. 数据链路层

数据链路层在物理层提供比特流服务的基础上, 建立相邻节点之间的数据链路, 通过差错控制提供数据帧(frame)在信道上无差错的传输, 并进行各电路上的动作系列。

数据链路层在不可靠的物理介质上提供可靠的传输。该层的作用包括物理地址寻址、数据的成帧、流量控制及数据的检错、重发等。

所谓链路是指一条中间没有任何交换节点的点到点的物理线路。计算机之间进行数据通信的通路, 由许多链路串接而成, 链路也称为物理链路。要在一条链路上传输数据, 除物理线路外, 还必须有控制数据传输的规程。链路加上实现这些规程的软、硬件构成数据链路。当采用复用技术时, 一条物理链路上可以有 multiple 数据链路, 因而将数据链路叫做逻辑链路。

由于物理链路不可能绝对可靠, 数据链路层的作用就是通过一些数据链路层协议(即链路控制规程), 在不太可靠的物理链路上实现可靠的数据传输。因此, 数据链路必须具备以下主要功能:

(1) 链路管理: 当网络中的两个节点要进行通信时, 数据的发送方必须确认接收方是否已经准备就绪, 为此, 通信的双方必须先要交换一些必要的信息, 即必须先建立一条数据链路; 同样地, 在传输数据时要维持数据链路, 而在通信完毕时要释放数据链路。数据链路的建立、维持和释放就叫链路管理。

(2) 帧同步: 在数据链路层, 数据的传送单位是帧。数据一帧一帧地传送, 就可以在出现差错时, 将有差错的帧再重传一次, 从而避免了将全部数据都进行重传。帧同步是指接收方应当能从收到的比特流中准确地分出一帧的开始和结束在什么地方。

(3) 流量控制: 发送方发送数据的速率必须使接收方来得及接收, 当接收方来不及接收时, 就必须及时控制发送方发送数据的速率。

(4) 差错控制: 在计算机通信中, 一般都要求极低的误码率, 为此, 必须采用差错控制技术, 它分前向纠错和检错重发两类。

(5) 透明传输: 由于数据和控制信息都是在同一信道中传送, 而在许多情况下, 数据和控制信息处于同一帧中, 因此一定要有相应的措施使接收方能够将它们区分开来。这样才能

保证数据链路层的传输是透明的。

(6)寻址:在多点连接的情况下,必须保证每一帧都能送到正确的目的站,接收方也应当知道发送方是哪一个站。

在数据传送时,数据帧会由于噪声等的干扰出错,或根本无法到达接收方,这时如果发送方只是不断地发送帧而并不考虑它们是否正确到达对方,将不能保证所有的帧最终都能按照正确的顺序交付给目标机器的网络层。

为了保证可靠传输,常采用的方法是由接收方向数据发送方提供有关接收情况的反馈信息。典型的做法是,协议要求接收方在收到数据帧后,发回一个特殊的控制帧,确认接收正确或错误。如果发送方收到了关于某个帧的肯定确认,则表示此帧已正确到达;如果收到的是否定确认,则表示发生了某种差错,该数据帧必须被重传。

还有一种情况,数据帧在传送中被完全丢失,比如消失在突发性噪声之中。此时,接收方由于没有收到任何数据而不会发送任何的确认信息。如果协议规定发送方必须在收到接收方的确认帧后才能发送下一帧,则发送方将会永远等下去。这个问题可以通过引入计时器来解决。当发送方发出一帧时,启动计时器,发送方收到接收方的确认信息后,将计时器清零。如果帧在传送过程中丢失,则计时器会超时,此时发送方重传此帧。

这种方法虽然解决了帧的丢失问题,却可能会引起一个新的差错——帧重复。假设数据帧正确到达了接收方,接收方也发出了确认帧,但是该确认帧却在中途完全丢失,这种情况同样会引起计时器超时,而导致发送方重传数据帧,这样接收方就接收到了两个相同的帧。为了防止这种情况发生,通常对发出的各帧编号,这样接收方就能够辨别是重复帧还是新帧。采用定时器和序号的主要目的是保证每帧都能最终正确地传送给目的地——网络层,这也是数据链路层责任的重要部分。

如果发送方发送能力比接收方接收能力强时,也就是说某一时刻接收方没有能力接收下全部发来的帧,即使传输过程中毫无差错,也会发生帧丢失的现象,因此需要有某种信息来查获接收方当前尚有多少缓存空间可利用。通常,流量控制是与差错处理控制一起完成的。特别是在双工通信时,应用捎带(piggybacking)技术能巧妙地解决流量控制的问题。

(1) 停等协议

停等协议(Stop and Wait)是数据链路层中最基本、最简单的协议。数据链路层从网络层接收一个分组后,加上数据链路层帧头和帧尾,再把它发送出去,同时启动一定时计数器,等待接收方发出的确认帧的到来。接收方链路层收到数据帧后,它必须首先发出一个确认帧 ACK(认为所接收的数据正确无误)或否定性确认帧 NAK(认为接收的数据有误)给发送方链路层,再处理接收到的帧。正确接收的帧提交给网络层,错误接收的帧丢弃。发送方如果在计时时间范围内得到的是 ACK,则发下一帧;如果收到的是 NAK 或者计时时间已到而没有收到 ACK 或 NAK,则重发刚才发送出去的帧。因此,需要有某种机制解决帧的被重传问题,通常的做法是给帧添上一个序号。

(2) 滑动窗口的协议

在假想的不正常状况下也能非常可靠地工作。它们是滑动窗口协议、退后 N 帧协议和选择性重传协议。三者的区别仅仅在于效率、复杂性和对缓冲区的需求不同。滑动窗口协议的关键是,每个要发出的帧包含一个序号,从 0 到某个最大值(通常是 $2N-1$)。在任意时

刻,发方都保持一个连续序号表,对应于允许发送的帧,这些帧称作发送窗口。同样收方也保持一个接收窗口,对应于允许接收的帧。实际上,发方和收方完全不必具有同样大小的窗口上、下限以及窗口尺寸。

滑动窗口协议的工作过程如下:

在发方窗口内的序号代表已发而尚未确认的帧。当一个新的分组从网络层到达链路层时被赋予当前最大的序号,而窗口上限加1;当一个确认到达时,窗口下限加1。以这种方式,窗口继续保持一个未确认帧的序号表。

因为在发方的窗口内的帧最终有可能在传输中丢失或损坏,所以发方必须在内存中保存所有这些帧以备重发。

收方数据链路层的窗口对应于允许接收的帧。任何落在窗口外的帧都无条件地废弃。当收到序号等于窗口下限的帧时,将其交给网络层并产生一个确认,窗口整个向前移动一个位置。不像发方的窗口,收方的窗口总是保持初始值大小。注意,大小为1的窗口(即窗口尺寸为1)意味着数据链路层只能顺序接收帧,大于1的窗口却不是这样。与此相比,无论数据链路层窗口大小如何,它交给网络层分组的顺序总是正确的。

3. 网络层

在计算机网络中进行通信的两个计算机之间可能会经过很多个数据链路,也可能还要经过很多通信子网。网络层的任务就是选择合适的网间路由和交换节点,确保数据及时传送。网络层将数据链路层提供的帧组成数据包,包中封装有网络层包头,其中含有逻辑地址信息——源站点和目的站点地址的网络地址。

网络层主要功能是寻址,实现路由选择。数据链路层仅是在相邻节点间建立连接并将数据成帧后从链路的一端传送至另一端。而网络层是在数据链路连接的基础上,将源端发出的分组信息经各种路径(路由选择)送到目的端,由于源端到目的端途径多个中间节点,即使源端与目的端同属一个网络,仍存在路径选择问题。所以网络层是处理端数据传送的最低层。如果源端处于一个网络,目的端处于另一个网络中,除存在路由选择外,还有协议转换的问题。

网络层还必须向传输层提供服务。但有的网络如 ARPA 和 X.25 网络,其网络层是在通信子网(IMP)中运行,而传输层是在主机(HOST)中运行。因此,网络层和传输层之间的界面成了通信子网与主机之间的界面。这意味着,网络层提供的服务就是通信子网提供的服务。如果通信子网由某一大的机构主管,如邮电部或通信公司,而主机由用户管理,网络层的服务就成了邮电部或通信公司与用户之间的接口。

(1)网络层服务必须遵循的原则

- ①服务与通信子网的技术无关。
- ②通信子网的数量、类型与拓扑结构对传输层是透明的。
- ③传输层所获得的网络地址采用统一编号。

(2)为传输层提供的服务

网络层为传输层提供服务,它是按下列目标进行设计的:

- ①服务应与通信子网的技术无关。
- ②通信子网的数量、类型和拓扑结构对于传输层来说是隐蔽的。

③传输层所能获得的网络地址应该采用统一的编码模式,即使通过局域网和广域网也是如此。

在遵循上述目标的情况下,网络层的设计者有很大的自由度书写提供给传输层的服务规范。根据实现服务功能的位置不同,服务可分成面向连接和无连接两种方式。前者的实现被置于网络层(通信子网)中,它所追求的是可靠的、简单的服务,并且这些服务最好由连接来提供;而后的实现被置于传输层(主机)中,它的目的是充分利用主机的性能和价格优势,确保通信子网的功能和投资的相对稳定。国际标准化组织 ISO 最终把支持两种类型服务的协议综合进了 OSI 体系结构中。

(3)路由选择、拥塞控制和网际互联

①路由选择

在绝大多数通信子网中,分组的整个旅途需经过若干个站点,即使在无线网中,如果源端和目的端不在同一个网络中,仍然有路径选择问题。所以,选择路径的算法和它们使用的数据结构是网络层设计的一个主要对象。

路由选择算法负责确定所收到的分组应传送的外出线路。无论是为每个分组单独地选择路径(数据报情况),还是仅当建立新连接时选择路径(虚电路情况),我们都希望路径选择算法具有正确性、简单性、强大性、稳定性、公平性和最优性等特征。

路由选择算法可以分成两大类:非自适应型和自适应型。非自适应算法是一种静态策略,它不根据实测或估测网络的当前传输量和拓扑结构来作路径选择,常见的有最短路径选径法和多路径选径法。相反,自适应算法试图改变其路径选择决策来反映网络当前流量和拓扑结构的变化,常见的有集中式、孤立式和分布式选径法。

②拥塞控制

当一部分通信子网中有太多的分组时,其性能降低,这种情况就叫拥塞。造成拥塞有若干因素。如 IMP 的处理速度太慢以致不能执行要求它们做的日常工作(排队缓冲区、更新表格等),即使有多余的线路容量,也可能使队列饱和。另一方面,就算 IMP 的 CPU 的处理速度是无限快,每当输入的通信速率超过输出线路的容量时,也将造成队列饱和。不论哪一种情况,问题都归结于没有足够的 IMP 缓冲区。此外,拥塞还可能导致恶性循环,即拥塞—丢弃分组—重传分组—拥塞加重。

拥塞控制与流量控制是不同的两个概念。拥塞控制是全局性问题,涉及所有主机、所有 IMP 和 IMP 中存储、转发处理的行为,以及所有将导致削弱通信子网吞吐能力的其他因素。而流量控制只与某发送者和某接收者之间的点到点线路的通信量有关。

对于拥塞问题,可以采用预先分配缓冲区、丢弃分组或限制子网中分组数量的办法来解决。限制分组数量也有多种手段,如固定令牌法,或当过载时让 IMP 发送遏制分组来减慢输入速率。

③网际互联

网际互联涉及把两个网络连接在一起的问题。实际上,并非所有的网络均采用同一种协议,这意味着不同的分组格式、分组头、流控制过程和确认规则等。即使是相同协议的网络,当源端机器和目的端机器不在同一个网络中时,仍然存在跨网络的选径问题。所以网络互联是至关重要的。

网络互联可以在数据链路层通过桥接器,或在网络层通过网关来实现。在网络层进行互联具有更大的灵活性,实现的复杂性和代价也相对要大些。

4. 传输层

第四层的数据单元也称作处理信息的传输层。但是,当你谈论 TCP 等具体的协议时又有特殊的叫法,TCP 的数据单元称为段(segments),而 UDP 协议的数据单元称为“数据报(datagrams)”。这个层负责获取全部信息,因此,它必须跟踪数据单元碎片、乱序到达的数据包和其他在传输过程中可能发生的危险。第4层为上层提供端到端(最终用户到最终用户)的透明的、可靠的数据传输服务。所谓透明的传输是指在通信过程中传输层对上层的屏蔽了通信传输系统的具体细节。

OSI 参考模型中传输层处于网络层之上、会话层之下,是 OSI 的核心层。如果将 OSI 分为两部分,低层(即 1~3 层)作为数据传输服务的提供者,而高层(即 5~7 层)可看作是数据传输服务的用户。用户通过传输层得到网络服务。这样,传输层就成为数据传输服务提供者和数据传输服务用户之间的接口。

(1) 传输层的功能

- ① 提供建立、维护和拆除运输层连接。
- ② 选择网络层提供合适的服务。
- ③ 提供端到端的错误恢复和流量控制。
- ④ 向会话层提供独立于网络层的传送服务和可靠的透明数据传送。

(2) 传输层服务

传输层提供两类服务:面向连接的传送服务和无连接的传送服务。面向连接服务经过三个阶段:连接建立、数据传输和连接释放,包括管理跨网连接的建立和释放。除此而外,传输层还必须完成:传输层地址到网络层地址的映射;多个传送连接复用到一个网络连接上,即几个报文流多路复用一条通道;端到端的顺序控制和流量控制以及端到端的差错控制和差错恢复等。

5. 会话层

这一层也可以称为会晤层或对话层,在会话层及以上的高层次中,数据传送的单位不再另外命名,统称为报文。会话层不参与具体的传输,它提供包括访问验证和会话管理在内的建立和维护应用之间通信的机制,如服务器验证用户登录便是由会话层完成的。

6. 表示层

这一层主要解决用户信息的语法表示问题。它将欲交换的数据从适合于某一用户的抽象语法,转换为适合于 OSI 系统内部使用的传送语法,即提供格式化的表示和转换数据服务。数据的压缩和解压缩、加密和解密等工作都由表示层负责,例如图像格式的显示,就是由位于表示层的协议来支持。

7. 应用层

应用层为操作系统或网络应用程序提供访问网络服务的接口。

OSI 模型最初由国际标准化组织(图 2.3-2)设计,旨在提供一套开放式系统协议的构建框架。其初衷是希望使用这套协议开发一个独立于私有系统的国际网络。

不过,由于基于 TCP/IP 协议的 Internet 迅速得到广泛采用并且扩展速度极快,致使

OSI 协议族的制定和认可相对滞后。但即使目前只有少数使用 OSI 规范制定的协议得到了广泛使用,七层 OSI 模型对适用于所有新兴网络类型的其他协议的制定和产品的开发作出的贡献也不容忽视。

作为一种参考模型,OSI 模型详细罗列了每一层可以实现的功能和服务。它还描述了各层与其上、下层之间的交互。

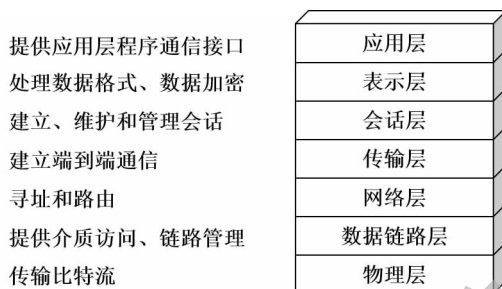


图 2.3-2 OSI 参考模型

OSI 模型各层的真正功能是向它的上一层提供服务。下层能够向上层提供的服务有两种形式:面向连接服务(connection-oriented)和无连接服务(connectionless)。

面向连接服务,又称为虚电路服务,以电话系统最为典型。要和某人通话,先拿起电话,拨号码,通话,挂断。网络中的面向连接服务类似打电话过程,某一方欲传送数据时,首先给出对方全称地址,并请求建立连接,对方同意后,双方之间的链路便建立起来;第二步是传送数据,通常以帧为单位,按序传送,不再标示地址,只标示所建立的链路号,并由接收方对收到的帧予以确认,此为可靠传送方式,也有用不着确认的场合,为不可靠方式;第三步为数据传送结束后,拆除链路。

无连接服务没有建立和拆除链路的过程,一般也不采用可靠方式传送。像普通的电子邮件,其用户并不希望为发一条信息而去经历建立和拆除链路的麻烦,也不要求百分之百可靠。

无连接服务有以下 3 种类型:

(1)数据报(datagram):它的特点是不需要接收端做任何响应,因而是一种不可靠的服务。数据报常被描述为“尽最大努力交付”(best effort delivery)。

(2)证实交付(confirmed delivery):又称为可靠的数据报。这种服务对每一个报文产生一个证实给发送方用户,不过这个证实不是来自接收方的用户而是来自提供服务的层。这种证实只能保证报文已经发给远端的目的站了,但不能保证目的站用户已收到这个报文。

(3)请求回答(request reply):这种类型的数据报是接收方用户每收到一个报文,就向发送方用户发送一个应答报文。事务(即 transaction,又可译为事务处理或交易)中的“一问一答”方式的短报文,以及数据库的查询,都很适合使用这种类型的服务。

OSI 参考模型中,服务原语分为四类:请求、指示、响应、证实。

(1)请求(request)

服务用户要求服务提供者做某项工作,即服务用户用它促成某项工作,如请求与谁建立连接或请求发送数据等。

(2)指示(indication)

服务用户被告知某事件发生。如服务提供者在服务用户请求下执行“连接请求”(connect

request——OSI 表示法)原语之后,则用“指示”(indication)原语通知收方用户实体,收方用户实体就是“连接请求”(connect request)原语中地址段内所指定的对等层实体。该实体收到的一个“连接指示”(connect indication)原语,通知有人(服务用户)想与它建立连接。

(3) 响应(response)

服务用户表示对某事件的响应。如收到“连接指示”原语的实体使用“连接响应”(connect response)原语回答,表明自己是否愿意接受建立连接的请求。

(4) 证实(confirm)

服务用户收到关于它的请求的答复。无论请求建立连接的服务用户收到什么样的连接响应,是愿意还是不愿意建立连接,它都可以通过收到的“连接证实”(connect confirm)原语得到对方态度的证实。

下面举一个打电话的例子,以帮助理解原语是如何应用的。请考虑打电话邀请朋友到家里来喝茶的步骤:

- (1) 连接请求:拨朋友家的电话号码(请求建立连接);
- (2) 连接指示:他家的电话铃响了(指示有人请求建立连接);
- (3) 连接响应:他拿起电话(被呼方用来表示接收/拒绝建立连接的请求);
- (4) 连接证实:你听到了电话铃停止(通知呼叫方建立连接的请求是否被接收);
- (5) 数据请求:你邀请他来喝茶(发送数据);
- (6) 数据指示:他听到了你的邀请(表示数据的到达);
- (7) 数据响应:他说他很高兴来(发送数据);
- (8) 数据指示:你听到他接受了邀请(表示数据的到达);
- (9) 断连请求:你挂断了电话(请求释放连接);
- (10) 断连指示:他听到了挂断声,也挂断了电话(通知对等实体释放连接的完成情况)。

2.4 实训一 双绞线的制作

一、实训目的

学会使用双绞线制作直通线、交叉线。

二、实训任务

1. 制作符合 T-568A 和 T-568B 标准的双绞线
2. 测试双绞线的连通性

三、实训步骤

1. 剪线

利用压线钳的切线刀剪下所需要双绞线的长度,最多不超过 100 m。

2. 剥线

使用压线钳上的剥线刀片轻压双绞线并旋转,剥去双绞线两端外保护皮 2 cm~5 cm。

剥去外保护皮时,注意压线钳力度不宜过大,否则容易伤害到导线,如图 2.4-1 所示。



图 2.4-1 剥线

3. 排序

把每对都是相互缠绕在一起的线缆逐一解开,解开后根据需要按规则把几组线缆依次排列好并理顺,如图 2.4-1 所示,排列时应该注意尽量避免线路的缠绕和重叠。把线缆依次排列并理顺之后,由于线缆之前是相互缠绕着的,线缆会有一些的弯曲,此时我们应该把线缆尽量扯直并尽量保持线缆平扁。

制作双绞线最常用的标准是:TIA/EAI 568A 和 TIA/EAI 568B,如表 2.4-1、图 2.4-2 所示。

表 2.4-1 双绞线排列顺序

标准	1	2	3	4	5	6	7	8
T568A	绿白	绿	橙白	蓝	蓝白	橙	棕白	棕
T568B	橙白	橙	绿白	蓝	蓝白	绿	棕白	棕

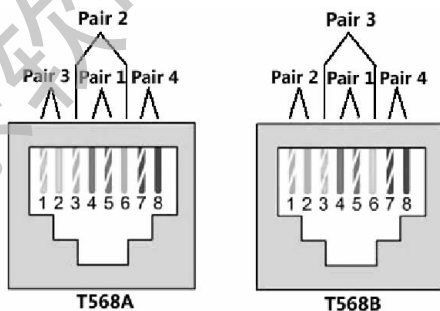


图 2.4-2 T568A/T568B 线序

针对以上两个标准,我们将网线分为直通线与交叉线。

直通线就是两端采用同一个标准,例如两头都是采用 T568B 标准,如图 2.4-3 所示。这种情况下线是连接不同类型的网络设备时使用的,比如:计算机与交换机、交换机与路由器的连接等。

交叉线就是一端采用 T568A 标准,另一端采用 T568B 标准,如图 2.4-4 所示。这种网线用在连接同一类型的网络设备,比如:计算机与计算机、交换机与交换机等。



图 2.4-3 直通线

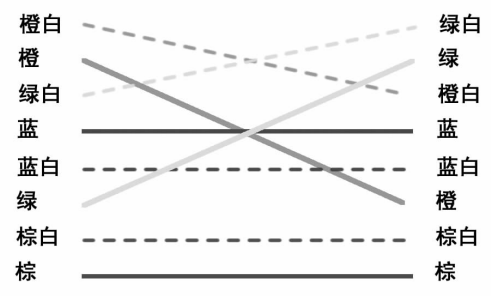


图 2.4-4 交叉线

4. 切平

将芯线按标准的顺序排列好并理顺压直之后，用压线钳的切线刀口将线头剪平齐。如图 2.4-5 所示。

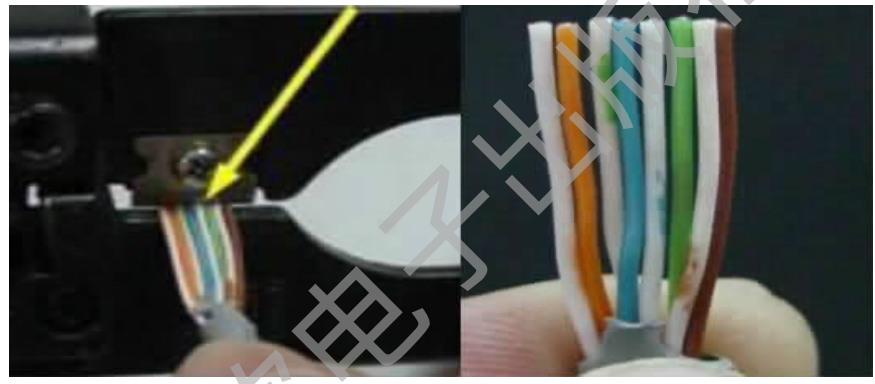


图 2.4-5 切平线缆

5. 插线

把整理好的线缆插入水晶头内，并检查线序是否正确，双绞线是否越过了金属片，如图 2.4-6 所示。

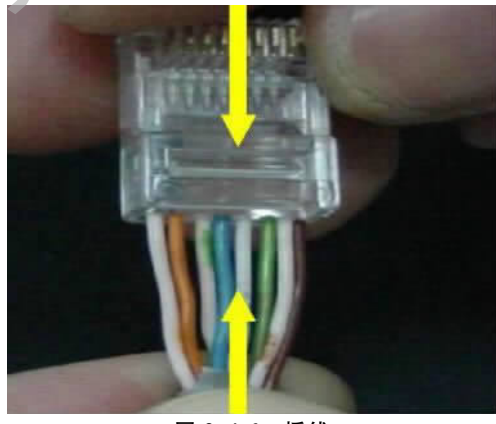


图 2.4-6 插线

6. 压线

确定双绞线的每根线已经放置到位且线序正确之后,就可以用压线钳将水晶接头压紧。把水晶头插入后,用力握紧线钳,若力气不够的话,可以双手一起压,这样压的过程使水晶头凸在外面的针脚全部压入水晶头内,受力后听到轻微的“啪”一声即可,如图 2.4-7 所示。

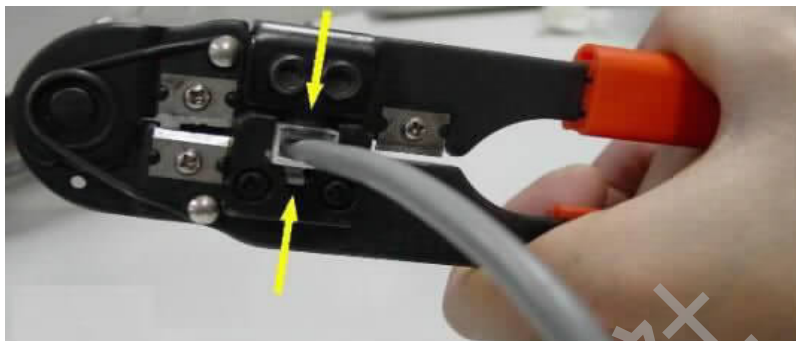


图 2.4-7 压线

7. 测试

最后使用测线仪测试你的网络线是否接通,也可以直接用到网络上测试数据能否接通,如图 2.4-8 所示。



图 2.4-8 使用测线仪测线

测线仪一般由两部分组成:主机和子机。一般两部分上面都有 8 盏指示灯,除了 RJ-45 接口之外,可能还有 BNC 接口或者 RJ-11 接口。将网线两端分别插入主机和子机的 RJ-45 接口内,打开主机的电源开关,观察指示灯。

如果制作的是直通线,子机 8 盏指示灯按 1—2—3—4—5—6—7—8 顺序依次闪亮,说明网线制作成功,否则网线制作失败,需要重新制作。

如果制作的是交叉线,主机 8 盏指示灯按 1—2—3—4—5—6—7—8 顺序依次闪亮,但子机 8 盏指示灯的闪亮顺序为 3—6—1—4—5—2—7—8,则说明网线制作成功,如果不亮或者顺序不对,则网线制作失败,需要重新制作。