CHAPTER 1

第 1 章　网络基础知识博文精选

网络技术的范围非常广泛，本章将精选出几篇通向网络世界大门的博客网志，每篇网志都非常有代表性地包含了很多网络入门的知识点。本章从一家公司办公室发生的一系列的故事开始，介绍了计算机网络的定义，并对网络连接的基本条件进行分析。接下来的事情更加让人发笑，由于网管员跳槽，公司安排财务人员填写一份网络设备调查表，这可难坏了他们，基建科的胖科长都来帮忙，谁也没有想到胖科长却是一位“资深专家”。

接下来的故事有点让人心酸，估计你也曾有过差 2 分就能及格的经历吧，我们将解决网管考试中可能遇到数学问题，把这 2 分补上。最后一个故事是办公室里面的“带宽大战”，你可以参与他们的争论，激励得很。故事讲完之后，我们认真地分析了一位网友的发言，解释了各种网络的特性及区分它们的方法。在本章最后，重点讲解 OSI 参考模型和 TCP/IP 的重点知识，并且将介绍一个网络故障从发现到解决的完整过程。

本章学习要点

- 掌握计算机网络的定义，理解通信子网与资源子网的概念。
- 了解通信系统及网络连接的基本条件，初步掌握交换机、路由器等网络基础设备的定义。
- 掌握不同数制之间的换算，理解网络带宽的表达方法。
- 了解 LAN、WAN、MAN、VPN 和 SAN 网络的特点。
- 了解 OSI 参考模型的概念，掌握 OSI 各层的功能，以及层间通信的原理。
- 了解 TCP/IP 分层与 OSI 分层之间的对应关系。
- 理解 ARP、IP、ICMP、IGMP 数据包结构和特性。
- 掌握 TCP 工作原理和通信机制，了解 UPD 协议的基本内容。

知识点索引

关　键　词	描　　述
NIC	网络接口卡（NIC）：提供计算机和网络之间通信连接的一种设备
Hub	集线器：一种特殊的中继器，可作为多个网段的转接设备
Switch	交换机：在通信系统中完成信息交换功能的设备
Router	路由器：网络互连设备，为网络上的数据分组选择最佳传递路径
Firewall	防火墙：在不同网络之间设置安全访问的控制设备
Gateway	网关：又称网间连接器、协议转换器
Bandwidth	带宽：在指定时间内通过某个网络连接的信息量
OSI	开放系统互连参考模型
MAC	Media Access Control：每一台网络设备接口的唯一标识
PDU	Protocol Data Unit：协议数据单元，负责层间通信
Encapsulation	数据沿着堆栈向下传输并加入头和尾的方法称为“封装”
TCP/IP	传输控制协议/网际协议：因特网的成功正是因为 TCP/IP 的应用和普及
ARP	地址解析协议：负责将 IP 地址解析成 LAN 硬件使用的媒体访问控制地址
IP	网际协议：它主要负责在主机之间为数据包进行寻址和路由
ICMP	Internet 控制消息协议：为数据通信中的源主机报告错误
TCP	传输控制协议：它可以提供可靠的、面向连接的网络数据传递服务
UDP	用户数据报协议：提供无连接的网络服务

1.1　办公室连网的故事

计算机网络是计算机技术和网络技术相结合的产物，在当今社会，无论是处理日常事务，还是进行信息传输，以及科研领域，人们都离不开计算机网络。本节内容是发生在某公司办公室的小插曲，网络从无到有，杨经理的心里面也是有苦有甜。

1.1.1　秘书的苦恼

某建筑公司杨经理像往常一样拿着 U 盘走到小王（秘书）身边说：“帮我把里面的文件送到楼上的孟总那里，他要看里面的销售合同。”小王转身跑着上了楼，过了十分钟她又跑了回来说：“经理，孟总说里面的合同是上个月的。”杨经理重新复制了最新的销售合同，就这样，小王每天都在楼上楼下运动着，这样有一个好处，就是保持了很好的身材。

每天，楼下的餐厅都和打仗差不多，排队的时候都能在这里听见很多人发牢骚，突然听到小王气愤地说：“我就纳闷了，公司干吗还不连网呀？”

网络是不是可以解决小王的苦恼呢？答案当然是肯定的，那么什么是计算机网络呢？

计算机通信网络是计算机技术和通信技术相结合而形成的一种通信方式，主要是满足数据通信的需要。它将不同地理位置、具有独立功能的多台计算机、终端及附属设备用通信链路连接起来，并配备相应的网络软件，以实现通信过程中资源共享而形成的通信系统。

因此，计算机网络需要两个或两个以上的单机系统共享某些事物（数据），单机系统必须通过传输线路（传输介质）相连才能形成网络，如图 1-1 所示。在通信的时候，为了使发送方和接收方都能理解彼此的数据，双方（包括网络上所有的单机系统）必须遵循一套公共的通信规则（协议），否则会陷入迷惑状态，就好像你在给英国人读一本法语书。

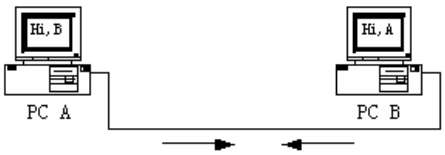


图 1-1　两台相互连接的计算机

1.1.2　经理的电脑坏了

在小王、小李、小张等一群“小”字辈的要求下，公司终于建成了网络。杨经理只要每次将文件放在“共享文件夹”里，其他人都可以从“网上邻居”访问到这些文件了。随着公司的网络发展，公司临时招聘了一位网管员，在他的努力下，公司的网络应用也逐渐开始完善，并且增加了服务器和很多连网设备。

突然有一天，杨经理的电脑坏了，是不是所有人都无法访问到这些文件了呢？

这次你猜错了，杨经理早已经成为公司里的“网络高手”了，他将所有文件都放在公司的文件服务器上了（事情的真相：网管员要求每个人必须使用服务器存储重要文件）。

服务器是专门为用户提供网络服务的网络设备，为什么将它也称为网络设备呢？这就需要进一步了解网络的组成部分。计算机网络可以划分成通信子网和资源子网两部分。各计算机之间通过通信媒体、通信设备进行数据通信，在此基础上各计算机又可以通过网络软件共享其他计算机上的硬件资源、软件资源和数据资源。

从计算机网络各组成部件的功能来看，各部件主要完成两种功能，即网络通信和资源共

享。我们常把计算机网络中实现网络通信功能的设备及其软件的集合称为网络的通信子网，而把网络中实现资源共享功能的设备及其软件的集合称为资源子网。

由图 1-2 可以看出，计算机网络系统以通信子网为中心。通信子网处于网络的内层，是由网络中的各种通信设备及其用做信息交换的物理介质构成，通信子网的重要任务是负责全网的信息传递。从通信子网向外发散的是服务器和终端设备，它们都处于网络的外围，构成了资源子网。

具体而言，通信子网由网卡、线缆、集线器、中继器、网桥、路由器、交换机及一些专用远程通信设备和相关软件组成。资源子网由连网的服务器、工作站、共享的打印机和其他设备及相关软件所组成。

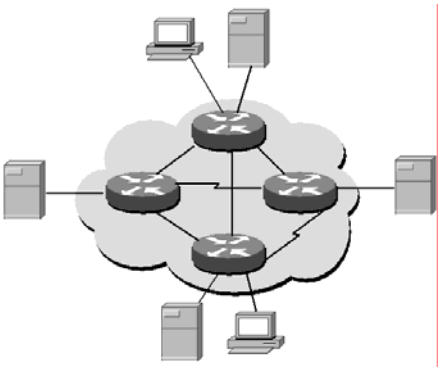


图 1-2　通信子网和资源子网

本书中的内容将围绕通信子网的规划设计和管理展开。

1.1.3　网管员的维修记录

就在办公室所有人都在庆祝上网成为现实的同时，公司网络管理员的维修记录却是记录得满满的，图 1-3 是公司 2007 年 9 月的维修登记表。

	A	B	C	D	E
1	主机编号	故障	时间	原因	处理结果
2	A19	无法上网	9:12	网线脱落	插拔
3	C24	无法上网	9:45	网卡损坏	更换
4	C22	无法上网	13:04	人为操作，删除TCP/IP协议	重新安装
5	A08	游戏中黑屏	15:56	内存问题	未处理
6	C01	无法上网	19:40	病毒，IE被篡改	未处理

图 1-3　网管员的维修记录

由于办公室的网络建设比较仓促，网络布线环境比较混乱，管理机制也不完善，网络经常会出现各种各样的问题，可真让杨总头疼，尤其是网络建设的负责人已经不在公司了，这群人消失在中关村茫茫的人海中了。

杨经理公司的网络故障归纳起来和网络连接的 3 个条件有关：物理连接（Physical Connection）、逻辑连接（Logical Connection）、应用程序（Application），只有这 3 个方面的条件都满足的时候，网络的功能才能发挥出来。下面我们分析一下这些故障出现的原因：

1）物理连接故障

计算机是 Internet 的根基，没有计算机也就没有了信息的制造者和收发者。而计算机要连接网络必须先具有一个专门的扩展卡（调制解调器或者网络接口卡“Network Interface Card, NIC”），其次是连接线路，如电话线路、网络连接线、光纤和无线等。图 1-3 中的前两个故障都是属于物理故障：网卡损坏和线路脱落。

2）逻辑连接故障

由于公司没有严格的计算机使用规定，使用人员的操作水平也比较低，随意性较大，因此，删除操作系统文件的事情常有发生。如果删除了一些网络硬件的驱动程序或者网络协议文件计算机肯定是无法正常通信了。那么，什么是网络协议呢？

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过程进行。计算机网络的协议主要由语义、语法和交换规则 3 部分组成，即协议三要素。

- 语义：规定通信双方彼此“讲什么”，即确定协议元素的类型，如规定通信双方要发出什么控制信息，执行的动作和返回的应答。
- 语法：规定通信双方彼此“如何讲”，即确定协议元素的格式，如数据和控制信息的格式。
- 交换规则：规定了信息交流的次序。

3）应用程序故障

公司既没有进行上网限制，也没有安装统一的防毒系统，所以饱受网络病毒困扰；尤其针对 IE（Internet Explorer）浏览器的病毒，一旦 IE 被病毒侵蚀，那么上网浏览信息必定不会正常。

这说明了一个问题，要访问网络，还必须在计算机中安装必要的应用程序，并保证应用程序正常运行。程序：简单来讲就是系统中一套有序动作的系列指令，它完成网络之间数据的解释和转换功能，这些功能是使计算机正常接收或发送通信数据。如 Web 浏览器和网络下载工具等都是应用程序。

1.2　填写网络设备调查表引发的趣事

直接连接到网络的器件也称为设备（Device），这些设备分为两类：终端设备和网络设备。终端用户设备包括计算机、打印机、扫描仪和其他直接为用户提供服务的设备，也称主机（Host）或工作站；而网络设备是指把终端用户连接起来使他们能够通信的所有设备，如网卡、中继器、网桥、交换机、路由器和防火墙等。

这些网络中的专用术语，对于一个有经验的网管员来说没有什么，但对于一些刚学习网络的人来说却是一头雾水，这次倒霉的人轮到了公司的财务部。

1.2.1　财务人员的困惑

杨经理的公司是事业单位，有在事业单位或政府机关工作经历的人都知道，一般年初和年底有个习惯，每次都要填无数的表格。这些表格主要调查各单位的网络建设情况，网络使用情况等，比如：局域网建设、因特网接入、网站建设、办公自动化，以及网络设备的数量等情况，表格的最后一般是问题与建议。图 1-4 显示了这种网络调查表中网络设备部分的摘要信息。

设备名称	品牌与型号	购置年度	数量（台）
中心交换机			
路由器			
防火墙			
集线器			
通过拨号或宽带上网的机器数量（台）			

图 1-4　网络调查表

杨经理公司的网络建立没有多久，就接到了这样的通知：要求填报单位的真实情况。通知中一段话引起了所有领导们的重视：“本调查表将作为全区科技基础条件平台建设和网络科技环境工程建设的重要依据，请各单位按调查表所列内容认真选择、填报，此表将作为今后设备下拨的主要依据。”

重视是重视了，可填这个表格的难度确实不小，最主要的一个问题是：由于网管员在混乱的网络故障压力下不堪重负，跳槽走人了。公司开了个会，大家觉得除了网管员之外，熟悉这些名称就是当初和网管一起采购的财务部门，因此决定由财务部负责完成此项工作。

1.2.2　解读表格填写内容

这次网络调查表填写的事情，落到财务部门不是意外，而是财务部门的人逞强所造成的，在没见到表格内容就在会议上说“网卡”什么的，这肯定成为领导关注的对象了。当真的看到表格之后，可难坏了他们，什么“交换机、路由器、防火墙”等一堆专业术语后面应该填什么呀？如果财务部门的同事和你一起看完下面的内容，估计也能正确填入这些信息了。

1．不用填表的设备

1）网络接口卡

财务部对网卡很熟悉，因为他们的计算机网卡就曾经坏过，而且也见过网管员拆过网卡。当然，另外一个熟悉的词是“网线”。但对于一般的调查表来说，“网卡”可能是各种调查表中唯一不用填写的网络设备了。

网卡的全称是：网络接口卡（NIC），如图 1-5 所示，它是提供计算机和网络之间通信连接的一种设备。

图 1-5　网络接口卡

NIC 在物理层（第一层）和数据链路层（第二层）规范的支持下执行其功能。NIC 中基本定义了电缆物理连接方法和利用比特流传输网络数据帧的方法。此外还定义了提供网络数据传输定时的控制信号。最常见的数据链路层协议有以太网 CSMA/CD 和令牌环（Token Ring）等。

2）中继器

中继器（Repeater）在现在的调查表中几乎是看不到了，不过翻阅很早以前的调查表，还真的能够发现它的身影。中继器工作于 OSI 的物理层，是局域网上所有节点的中心，它的作用是：放大信号，补偿信号衰减，支持远距离的通信。

中继器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。中继器是最简单的网络互连设备，主要完成物理层的功能，负责在两个节点的物理层上按位传递信息，完成信号的复制、调整和放大功能，以此来延长网络的长度。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。中继器就是为了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。但在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做了具体的规定，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。如以太网常常利用中继器扩展总线的电缆长度，标准细缆以太网的每段长度最长 185m，最多可有 5 段，但是增加中继器后，最长网络电缆长度可提高到 925m。

2．有可能填表的设备

1）集线器

集线器（Hub）是一种特殊的中继器，可作为多个网段的转接设备，因为几个集线器可以级联起来。智能集线器，还可将网络管理、路径选择等网络功能集成于其中，不过在最新的调查表中，Hub 应该被“交换机”这个词替代了。

“集线器”一词来自英文 Hub，本意是中枢或多路交汇点。它对工作站进行集中管理，不让出问题的区段影响整个网络的正常运行。Hub 是局域网中应用最广的连接设备，目前若按配置形式可分为独立型集线器、模块化集线器和堆叠式集线器 3 种。市场上常见到的是 10Mbps、100Mbps 或用于千兆以太网的 1000Mbps 速率集线器。集线器的连接应考虑所使用的网络传输介质，一般集线器应具有：BNC 和 RJ-45 两个接口，或 BNC、RJ-45 和 AUI 3 个接口。集线器接口数通常有：8 口、12 口、16 口或者具有更多的端口，如图 1-6 所示。

图 1-6　有多个端口的集线器

2）网桥

网桥工作在数据链路层，将两个局域网（LAN）连接起来，根据 MAC 地址（网桥维护 MAC 地址表，称为网桥表）来转发帧，可以看做一个“低层的路由器”（路由器工作在网络层，根据网络地址，如 IP 地址进行转发），如图 1-7 所示。

网桥的实际外观产品也很像集线器，如图 1-8 所示的低成本的交换式以太网桥。这是一种高性能、自学习式远程以太网桥。它体积小、成本低，很适宜对成本敏感的桥接应用，或作为比特流基础结构上的局域网延伸器或分段器。设备能不间断地学习与其相连的局域网上的 MAC 地址，并根据数据帧的目的 MAC 地址来决定是否能发还是过滤。

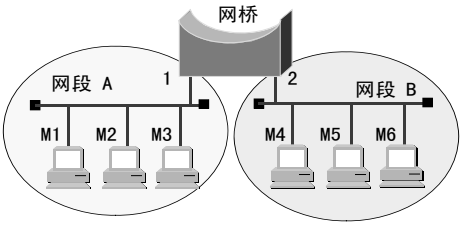


图 1-7　网桥

图 1-8　HN-10 交换式以太网桥

3．必填设备

1）交换机

交换机（Switch）是集线器的升级换代产品。如图 1-9 可以看出来，从外观上对比，它与集线器基本上没有多大区别，都是带有多个端口的长方形盒状体。交换机是按照通信两端传输信息的需要，用人工或设备自动完成的方法，把要传输的信息送到符合要求的相应路由上的技术统称。广义的交换机就是一种在通信系统中完成信息交换功能的设备。交换机完全克服了集线器的上述种种不足之处，所以在短时间内得到业界广泛的认可和应用。目前最快的以太网交换机端口带宽可达到 10Gbps，千兆（G 位）级的交换机在各企业骨干网络中早已得到广泛应用。

交换机提供了桥接能力，以及在现存网络上增加带宽的功能。用于 LAN 上的交换机与网桥相似，因为它们都运作在数据链路层的 MAC 子层上，检验着所有进入的网络流量的设备地址。与网桥还有一点相似，交换机保持一张有关地址的信息表，并利用该信息来决定如何过滤并转发 LAN 流量。而与网桥不同，交换机则采用交换技术来增加数据的输入/输出总和安装介质的带宽。

新的使用存储转发交换技术的交换机（有时称为路由交换机），由于组合了路由和交换技术，因此可以在网络层（第三层）上操作，以建立到达目标的最快的路径。组合了路由功能的交换机的优点之一是在网络流量分段方面具有更大的灵活性，从而可以避免在以太网应用中的广播风暴。

可管理的交换机大多数可以实施虚拟局域网（Virtual LAN，VLAN）技术。VLAN 是一种基于软件将网络逻辑地划分为子网的方法，这些逻辑的子网相当独立于真实的物理网络拓扑结构。

关于路由交换机是否真如公认的那样是严格的第二层设备，在网络互连专家中还存在一些争议。根据 20 世纪 80 年代发展的交换机的定义，第三层的交换机实际上是路由器，这个路由器采用交换技术来发送包，速度要高于传统的路由器。

2）路由器

路由器（Router）是网络互连设备，属于第三层设备，如图 1-10 所示。

图 1-9　交换机

图 1-10　路由器

路由器能做出决定为网络上的数据分组选择最佳传递路径。简单地讲，路由器主要有以下几种功能。

- 网络互连：路由器支持各种局域网和广域网接口，主要用于局域网互连和广域网，实现不同网络互相通信。
- 数据处理：提供包括分组过滤、分组转发、优先级、复用、加密、压缩和防火墙等功能。
- 网络管理：路由器提供包括配置管理、性能管理、容错管理和流量控制等功能。

路由器利用网络层定义的“逻辑”上的网络地址（即 IP 地址）来区别不同的网络，实现网络的互连和隔离，保持各个网络的独立性。路由器不转发广播消息，而把广播消息抑制在各自的网络内部。发送到其他网络的数据先被送到路由器，再由路由器转发出去。在后续章节中会更详细地介绍路由器和第三层协议的功能。

3）网关

网关（Gateway）又称为网间连接器，或者说协议转换器。网关在传输层上以实现网络互连，是最复杂的网络互连设备，仅用于两个高层协议不同的网络互连。网关的结构也和路由器类似，不同的是网关主要用于广域网互连。

在早期的因特网中，网关即指路由器，是网络中超越本地网络的标记。公共的基于 IP

的广域网的出现和成熟促进了路由器的成长，现在路由器变成了多功能的网络设备，失去了原有的网关概念，然而作为网关仍然沿用了下来，它不断地应用到多种不同的服务功能中。目前主要有 3 种类型的网关：协议网关、应用网关和安全网关。

4）防火墙

财务部的所有人正在聚精会神地研究调查表的各个陌生的名词，这时候基建科的胖科长凑来，一眼就看见了“防火墙”这个词，自豪地说：“这个我可熟悉的很。”为什么基建科科长会熟悉防火墙呢？

“防火墙”一词来自建筑结构里的安全技术。在楼宇里用来起分隔作用的墙，用来隔离不同的公司或房间，尽可能地起防火作用。一旦某个单元起火，这种方法会保护其他的居住者。然而，多数防火墙里都有一个重要的门，允许人们进入或离开大楼。因此，防火墙保护了人们的安全，也在提供增强安全性的同时允许必要的访问。

网络中的防火墙（Firewall）是指设置在不同网络（如可信任的企业内部网和不可信的公共网）或网络安全域之间的一系列部件的组合。它是不同网络或网络安全域之间信息的唯一出入口，能根据企业的安全政策控制（允许、拒绝、监测）出入网络的信息流，且本身具有较强的抗攻击能力。它是提供信息安全服务，实现网络和信息安全的基础设施。

防火墙技术可根据防范的方式和侧重点的不同而分为很多种类型，但总体来讲可分为两大类：包过滤（分组过滤）和应用代理。网络安全中系统安全产品使用最广泛的技术就是防火墙技术，即在 Internet 和内部网络之间设一个防火墙。目前在全球连入 Internet 的计算机中约有三分之一是处于防火墙保护之下。

1.3　网络工程师考试中的数学题

纯粹的数学也叫基础数学，专门研究数学本身的内部规律。学校课本里介绍的代数、几何、微积分、概率论知识，都属于纯粹数学。纯粹数学的一个显著特点就是暂时撇开具体内容，以纯粹形式研究事物的数量关系和空间形式。网络中遇到的数学却是实实在在解决具体问题的算法。

1.3.1　糟糕的考试

我国的网络工程师考试一年考两次，5 月份和 11 月份各一次，我们单位的小李（网管员）在上半年的考试中没有顺利通过。这位老兄只差 2 分就通过考试了，我能理解他收到成绩单时郁闷的心情。在聊天时，他回忆“计算机科学基础”部分中的很多数制计算题都拿不准，好像其中一道题就是让写出 168 的二进制数是多少？没有想到这么基础的知识他却没有通过，看来需要补补课了。

其实数制计算题并不难，我找出很早以前的复习笔记交给了他，希望能对他在下半年的考试复习中有所帮助。

1.3.2　考试复习笔记

数据制式就是数据的进位计数原则，也是人们利用符号来计数的科学方法，又称为进位计数制，简称“数制”或“进制”。简单地说，数制就是用一组固定的数码和一套统一的规

则来表示数值的方法。我们最熟悉的应该是十进制数进行计数，其实在现实生活中也使用其他进制，如用六十进制计时，用十二进制作为月到年的进制等。

在计算机通信中，最常用到的就是二进制数，有时需要在不同制式中相互转换，如在配置注册表、计算机 IP 地址、子网掩码、IPv6、路由器寄存器地址等，所以数据制式的转换就成为了网络管理员所必须掌握的一项基本功。

第 1 课：数制的表示

复习笔记中的第 1 课数制表示，常用的数制包括如下几个：

1）二进制

计算机利用电子开关（On 或 Off）来对数据进行操作和存储。在计算机系统中采用的是二进制数，只有“0”和“1”两个数，其主要原因是便于进行电路设计，使数据运算更简单，可靠性更强。

二进制的数即基数为 2。二进制的特点为：逢二进一，借一当二。一个二进制数各位的权是以 2 为底的幂。例如：二进制数 1101 表示十进制数 13

$(1101)_2 = 1\times2^3+1\times2^2+0\times2^1+1\times2^0=8+4+0+1=13$

2）十进制

十进制数是人们最熟悉的一种进位计数制，它由 0、1、2…、8、9 共 10 个数码组成，即基数为 10。十进制的特点为：逢十进一，借一当十。一个十进制数各位的权是以 10 为底的幂。

3）八进制

由 0、1、2、3、4、5、6、7 共 8 个数码组成，即基数为 8。八进制的特点为：逢八进一，借一当八。

4）十六进制

由 0、1、2、3、4、5、6、7、8、9、A、B、C、D、E、F 16 个数码组成，即基数为 16。十六进制的特点为：逢十六进一，借一当十六。

表 1-1 中是四位二进制数与其他数制的对应关系。

表 1-1　二进制与其他数制的对应

二　进　制	十　进　制	八　进　制	十 六 进 制
0000	0	0	0
0001	1	1	1
0010	2	2	2
0011	3	3	3
0100	4	4	4

续表

二　进　制	十　进　制	八　进　制	十 六 进 制
0101	5	5	5
0110	6	6	6
0111	7	7	7
1000	8	10	8
1001	9	11	9
1010	10	12	A

1011	11	13	B
1100	12	14	C
1101	13	15	D
1110	14	16	E
1111	15	17	F

第 2 课：数制转换与运算

复习笔记中的第 2 课数制转换与运算。需要掌握数制间的转换有：二→十进制、八→十进制、十六→十进制、二→八→十六进制的转换。至于数制之间的运算，很多时候是通过转换到二进制以后再进行计算的。

1）数制的转换

在转换中常用的方法有按权展开多项式法、基数除/乘法和基数为 2^n 的各种进制之间的直接转换法。一般二、八、十六进制转换为十进制采用多项式法；十进制数转换为二、八、十六进制数采用：基数除/乘法；而基数为 2^n 的各种进制间的转换采用：直接转换法。

（1）二进制、八进制、十六进制数转换换为十进制

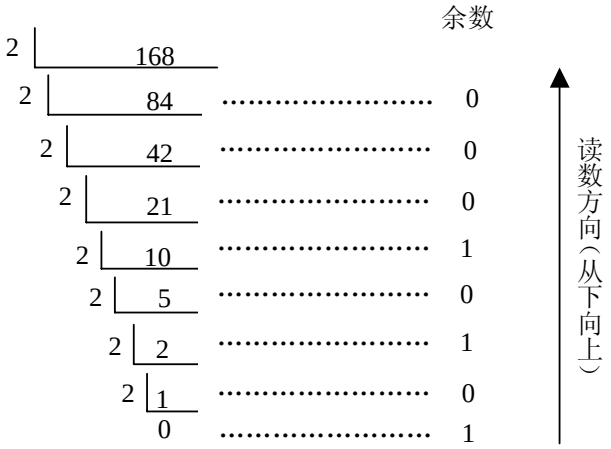
对于任何一个二进制、八进制数、十六进制数，可以写出它的按权展开式，再按十进制进行求和运算即可转换为十进制数，如：

$(1111.11)_2=1\times2^3+1\times2^2+1\times2^1+1\times2^0+1\times2^{-1}+1\times2^{-2}=15.75$

（2）十进制数转换为二进制数

十进制数的整数部分和小数部分在转换时需进行不同的计算，分别求值后在组合。整数部分采用除 2 取余数，即逐次除以 2，直至商为 0，得出的余数倒排，即为二进制各位的数码。小数部分采用乘 2 整数，即逐次乘以 2，从每次乘积的整数部分得到二进制数各位的数码。

小李考试中遇到了“168 转成二进制表示”一题，就可以按照以下步骤计算：



第 1 步：将 168 除以 2，商 84，余数为 0；

第 2 步：将商 84 除以 2，商 42 余数为 0；

第 3 步：将商 42 除以 2，商 21 余数为 0；

第 4 步：将商 21 除以 2，商 10 余数为 1；

第 5 步：将商 10 除以 2，商 5 余数为 0；

第 6 步：将商 5 除以 2，商 2 余数为 1；

第 7 步：将商 2 除以 2，商 1 余数为 0；

第 8 步：将商 1 除以 2，商 0 余数为 1；

第 9 步：读数，因为最后一位是经过多次除以 2 才得到的，因此它是最高位，读数字从最后的余数向前读，即 10101000 。

（3）二进制数转换成八进制

二进制数转换成八进制数的方法是：将二进制数从小数点开始，对二进制整数部分向左每 3 位分成一组，对二进制小数部分向右每 3 位分成一组，不足 3 位的分别向高位或低位补 0 凑成 3 位。每一组有 3 位二进制数，分别转换成八进制数码中的一个数字，全部连接起来即可。

反过来，将八进制数制转换成二进制数，只要将每一位八进制数转换成相应的 3 位二进制数，依次连接起来即可。

（4）二进制数与十六进制数的相互转换

二进制数与十六进制数的相互转换方法和二进制数的转换方法相类似。二进制数转换十六进制数，只要把每次 4 位分成一组，再分别转换成十六进制数码中的一个数字，不足 4 位分别向高位或低位补 0 凑成 4 位，全部连接起来即可。反之，十六进制数转换成二进制数，只要将每一位十六进制数转换成 4 位二进制数，依次连接起来即可。其他数制之间的转换可以通过二进制数作为中间桥梁，先转换为二进制数，再转换为其他进制数。

2）二进制的运算规则

在计算机中，采用二进制数可以非常方便地实现各种算术运算和逻辑运算。

（1）算术运算规则

- 加法规则：0＋0=0；0＋1=1；1＋0=1；1＋1=10。
- 减法规则：0－0=0；10－1=1；1－0=1；1－1=0。
- 乘法规则：0×0=0；0×1=0；1×0=0；1×1=1。
- 除法规则：0/1=0；1/1=1。

（2）逻辑运算规则

- 逻辑与运算（AND）：0∧0=0；0∧1=0；1∧0=0；1∧1=1。
- 逻辑或运算（OR）：0∨0=0；0∨1=1；1∨0=1；1∨1=1。
- 逻辑非运算（NOT）：1=0；0=1。
- 逻辑异或运算（XOR）：0⊕0=0；0⊕1=1；1⊕0=1；1⊕1=0。

第 3 课：比特和字节

通过前两节课的复习，我们知道了计算机中的数据都要采用不同的二进制位来表示，为了方便表示数据量的多少，引入了数据单位概念。

1）位（bit）

简记为“b”，也称为比特，是计算机存储数据的最小单位。一个二进制位只能表示 0 或 1，要想表示更大的数，就得把更多的位组合起来，每增加一位，所能表示的数就增大一倍。

2）字节（Byte）

来自英文 Byte，简记为“B”，规定 1B=8bit，字节是存储信息的基本单位。微型机存储器是由一个个存储单位构成的 ，每一个存储单位的大小就是一个字节。所以存储器容量的大小也可以用字节数来度量。其他常用的度量单位有：KB、MB、GB 和 TB，其换算关系为：1TB=1 024GB；1GB=1 024MB；1MB=1 024KB；1KB=1 024B。

计算机中还有一个常用的数据单位：字（Word）。

计算机处理数据时，CPU 通过数据总线一次存取、加工和传送的数据称为“字”，计算机的运算部件能同时处理的二进制数据的位数称为“字长”。一个字长通常由一个字节或若干字节组成。由于字长是计算机一次所能处理的实际位数长度，所以字长是衡量计算机性能的一个重要指标。字长越大，速度越快，精度越高。

1.4　办公室里的“带宽大战”

任何网络都有一个共同的特点：它们都使用带宽（Bandwidth）来描述它们的传输容量。带宽（Bandwidth）在某一特定的时间内（在给定的条件下）理论上能通过某一特定区域的最大比特量。

1.4.1　为同事解释带宽含义

每天下午大家清闲的时候，都会通过公司的网络下载一些自己喜欢的东西（MP3 和电影居多），上网的速度就会慢如蜗牛。同事每天下午都在发牢骚：“什么破网呀，还不如我家里的 ADSL 快呢!”网管员要是将上面的带宽的定义告诉每个同事，估计有人该怀疑你疯了。所以需要找一种更恰当的比喻。

带宽就像高速公路的车道。公路网络延伸到每个城市、乡镇、小区。车道数较多的公路连接着车道数较少的公路，而这些公路又通向更小、更窄的公路，最终到达住宅时，尤其是小区中只有一条车道，每辆车行驶都慢了许多。最终，当更多的车不断地进入高速公路时，即使有更多的车道，高速公路也会变得拥塞和缓慢。如果将数据网络比喻为高速公路系统，则可以将数据分组相当于车，而带宽相当于高速公路的车道数。

当将数据网络被视为高速公路系统时就很容易看出，为何每天下午大家都在下载东西的时候会引起整个网络的拥塞了。如果你觉得高速公路的概念还不能解释清楚，那么就给同事们说说你堵车的经历吧，这个会引起共鸣的。

1.4.2　网管员的带宽争论

公司新招聘了一位网管员，此人喜好咬文嚼字，北京人将这种同事戏称为“杠头”。在一次技术研讨会上，技术部的主管将“带宽”和“速度”两个词反复交替使用。会议结束前，领导问还有谁补充，下面是这位新同事的发言：

“我有点补充，您刚才的用语不规范。您可以说以 45Mbps 传输的 T3 链路比以 1.544 Mbps 传输的 T1 链路具有更高的速度。但 T3 和 T1 的实际比特传输速度接近于光速，所以实际的比特传输速度不会改变。带宽指的是链路上每秒传输多少比特，而不是比特实际传输有多快。如果只用到它们传输能力内的一小部分时，它们传输数据的速率大致相同，这就像一滴水在细管和粗管里的流速大致相同的道理一样。因此，通常更难准确地说是 T3 的带宽比 T1 的要大，因为它在相同时间内能够传输更多的信息，而不是它有更高的速度。”

笔者很钦佩这位新同事的勇气，他补充的内容笔者非常认可，不过笔者可没有这份勇气，还是将原理补充写在这里吧。

在数字体系中，带宽的基本单位是比特每秒（bps）。带宽是在一个给定的时间（或多少秒）内有多少信息（或 bit）从一个地方流到另一个地方的量度。虽然带宽是以 bps 来描述的，但通常还有一些数倍于 bps 的表示方式。换句话说：网络带宽通常描述为 Kbps、Mbps，甚至 Gbps。

使用公式 T=S/BW（传输时间=文件大小/带宽），可以帮助网络管理员评估网络性能的几个重要方面。如果给定应用的典型文件大小已知，那么用文件大小除以网络带宽就可以估计出这个文件传输所需的最小时间。

进行数据传输计算时，有两个重要方面需要考虑：

（1）结果只是一个估计值，因为文件大小不包括为了使数据能通过网络传输所增加的开销。

（2）结果可能是最佳状态下的传输时间，因为可用带宽永远达不到该网络类型的最大理论值依次用吞吐量取代带宽会更加准确。

虽然数据传输计算相当简单，但如果不注意在公式中使用相同单位的话，也会遇到麻烦。MBps 的含义是兆字节每秒，Mbps 的含义是兆比特每秒，前者是指每秒传输的字节数量，后者是指每秒传输的比特位数。MBps 中的 B 字母是 Byte 的含义，虽然与 Mbps 中的 bit 翻译一样，都是比特，也都是数据量度单位，但二者是完全不同的。

Byte 是字节数，bit 是位数，在计算机中每八位为一字节，也就是 1Byte＝8bit，是 1:8 的对应关系。因此 1MBps 等于 8Mbps。因此，在书写单位时一定要注意“B 字”母的大小写，尤其有些人还把 Mbps 简写为 MBps，此时 B 字母的大小写真可以称为失之毫厘，谬以千里。

1.5　解读网友发言

随着网络的发展，出现了不同和网络类型，这些网络的特征与协议划分定义了不同的用途。其中包括：按网络的地理位置分类、按传输介质分类、内部与外部界线分类，以及专属用途分类等。另外，在局域网中还可以按照介质访问协议、服务方式、网络的拓扑结构进行分类，关于局域网组建与分类的内容将在将在第 2 章的案例中说明。

1.5.1　博客聚会发言

某茶社，51CTO 技术博客网站组织了一次博主见面活动，活动开始之后主持人要求每个人首先介绍一下自己，然后说明一下自己网络的结构和特色。其中一位网管用这样一段话介绍他管理的网络。

第一句：“我现在管理着一家跨国外企公司的网络，北京公司的局域网骨干是新建立的千兆网络，各国分公司的广域网连接都为 DDN 专线接入。”

第二句：“北京公司的写字楼除提供高速有线网络接入，除此以外公司还在各个展室和楼层休息厅设置了无线网络。”

第三句：“公司总部建立了大型的 SAN 存储网络，所有的销售人员都可以通过 VPN 访问方式从外部网络访问道公司内部网络服务，经过安全审核之后这些员工还可访问 SAN 中的核心数据。”

看似轻描淡写的一段介绍，却涉及了很多网络专用名词，如果让你也这样介绍自己的网

络，这些网络名词你是否也能正确使用呢？下面将针对发言中具有下画线的网络基础名称解释一番。

1.5.2　解读第一句话

发言中的第一句话包含了两个网络名词：局域网和广域网。这是将网络按照地理覆盖范围分类的描述方法，根据地理覆盖范围的大小，可以将计算机网络分为局域网、广域网，以及这句话中没有涉及到的“城域网”。它们在网络协议、体系结构、数据传输速率都不相同。

1．名词：局域网（LAN）

LAN（Local Area Network）是一个数据通信系统，其传输范围在中等地理区域使用中、高数据传输速率可连接大量独立设备在物理通信信道上互相通信，如图 1-11 所示。

局域网包含了物理层和数据链路层的功能，所以连到局域网的数据通信设备必须加上高层协议和网络软件才能组成计算机网络。局域网连接的是数据通信设备，包括 PC、工作站、服务器等大、中小型计算机，终端设备和各种计算机外围设备。

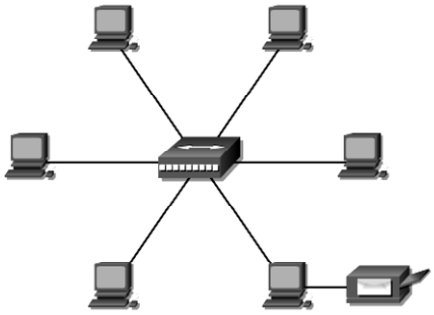


图 1-11　LAN

由于局域网传输距离有限，网络覆盖的范围小，因而具有以下主要特点：

- 局域网覆盖的地理范围比较小。
- 数据传输率高（可到 10 000Mbps）。
- 传输延时小。
- 误码率低。
- 价格便宜。

局域网一般是某一单位或组织所拥有，是网络组建中的重点，同时也是大多数网络管理员日常维护和管理工作的环境之一。

2．名词：广域网（WAN）

广域网（Wide Area Network）是在一个广泛地理范围内所建立的计算机通信网，简称 WAN。其范围可以超越城市和国家以至全球，因而对通信的要求及复杂性都比较高。WAN 的作用范围通常为几十到几千千米，广域网有时也称为远程网（Long Hual Network），如图 1-12 所示。

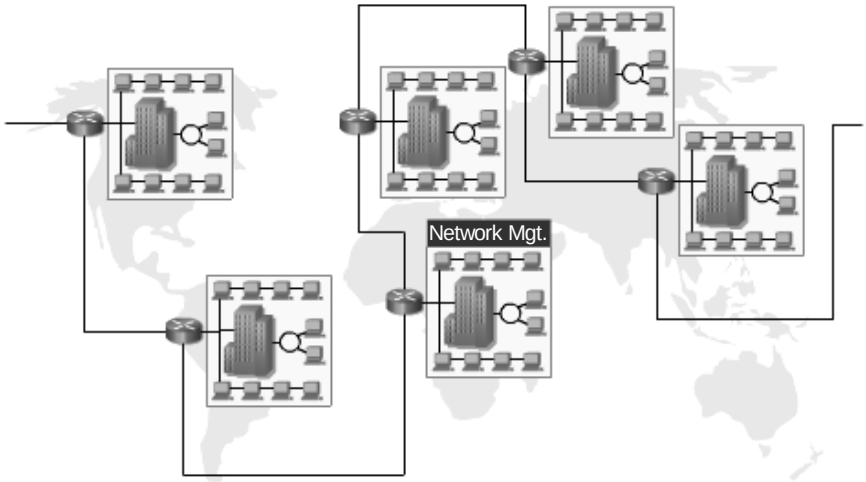


图 1-12　WAN

WAN 由通信子网与资源子网两个部分组成：通信子网实际上是一数据网，可以是一个专用网（交换网或非交换网）或一公用网（交换网）；资源子系统是连在网上的各种计算机、终端、数据库等。这不仅指硬件，也包括软件和数据资源。在实际应用中，LAN 可与 WAN 互连，或通过 WAN 与位于其他地点的 WAN 互连，这时 LAN 就成为 WAN 上的一个端系统。广域网具有以下主要特点：

- 广域网传输距离远、拓扑结构复杂，由此带来的问题是路由选择的复杂性。
- 从一个节点到另一个节点存在着许多可选路径，要选择最佳路由需要复杂的路由策略。
- 广域网面对各种各样的用户需求，需要具有适应大容量和突发性通信及综合业务服务的能力，包括阻塞控制方法、数据传输延迟的解决等。
- 许多广域网是由连接现有网络发展起来的，如公共分组交换网、卫星通信网和无线分组交换网等，这些网络可能使用不同的设备和协议，需要提供开放的设备接口和规范化的协议及协议转换功能。
- 传输速率与局域网相比较低。
- 网络用途多，选用的高层协议复杂，建设成本昂贵。

3．补充知识：城域网（MAN）

城域网 MAN（Metropolitan Area Network）是指在地域上覆盖一个城市及其郊区范围，为城域多业务提供综合传送平台的网络，主要应用于大中型城市地区。基于 LAN 与 WAN 之间。

城域网以多业务光传送网络为基础，实现话音、数据、图像、多媒体、IP 等接入，在功能上主要是指完成接入网中的企业和个人用户与在骨干网络上的运营商之间全方位的协议互通。城域网一般适用于距离为 5km~150km 的范围，建立在光缆通信设施或基础通信服务设施之上。

1.5.3　解读第二句话

发言中的第二句话包含了两个网络名词：有线网络和无线网络，这是按照网络通信介质分类的一种描述方法。

通信介质是指用来连接计算机和网络的电缆、光纤电缆、无线电波或微波。通信介质为

台式计算机、便携式计算机、便携式设备、网络打印机、服务器和路由器等相互连接和通信提供了媒介。

1．名词：有线网络

提供 LAN 中各种设备间的高速连接。现在很多应用程序都要占用大量网络资源，特别是在拥有集中存储和应用程序的企业中尤为突出。有线网络是连接服务器、无线设备和防火墙的基础。

有线网络连接的介质分为两类：第一类为金属导体，例如，同轴电缆、双绞线等，利用铜或铁等金属导体的电流变化来传输数据，第二类为以光纤为代表的透明玻璃或塑胶绳媒体，它们利用光波来传输数据。

2．名词：无线网络

为使用便携式计算机或移动设备的用户提供移动性，提高用户的工作效率。因为在办公室的任何地方用户都能够访问到重要的信息，这对于在会议室参加会议的用户特别有用。另外，无线网络还不需要布线和维护物理网络电缆的成本。无线访问点价格便宜，而且大部分新的便携式计算机、个人数字助理（PDA）和 Tablet PC 都有内置的无线网络适配器。无线网络也可以提供灵活的网络，因为具有无线网络适配器的设备可以放置在办公室或者企业楼宇中的任何位置。

无线网络系统（Wireless Network System）是一种数据传输系统，它是从有线网络系统（Wire Network System）自然发展而来的一种新技术，使用无线射频（RF）技术通过空中接口来收发数据，通常将这种采用无线传输数据或媒体的计算机网络称为无线局域网。

3．补充知识：有线与无线的结合

要实现合理的网络传输和覆盖，必须有线与无线、天空与地面相结合，取长补短。当今的自动化办公环境中，更多地采用有线与无线相结合的方式。表 1-2 中列出了有线与无线组网的特性，以及优缺点。

表 1-2　有线与无线的特点

服　务	主 要 设 备	主 要 用 途	优　点	难　题
有线连接	交换机	连接服务器、设备和桌面	高速 LAN 连接	LAN 布线
无线连接	无线访问点（AP）	连接支持无线功能的设备，（例如，膝上型计算机、Tablet PC 和 PDA）	客户端移动性	安全性 传输速度

1.5.4　解读第三句话

发言中的第三句包含了“网络用途”和“安全管理”两种网络属性描述方法。其中根据网络用途属性描述的是：SAN 与 VPN；根据安全管理划分的网络名词是：内部网络和外部网络，这是利用网络边界的节点进行分类，以确定私有网络和公共网络的界线的一种描述方法。

1．名词：存储区域网（SAN）

SAN 是一种存储设备网络，设计用于更有效地移动数据而不增加 LAN 的负载；SAN 实现这一目标的方式之一是通过使用光纤通道（Fibre Channel）连接来提供强劲的性能。SAN 技术使服务器可与其存储设备的物理距离达到 100km，这一距离比以前所能达到的距离要远的多，对业务恢复情景非常有益。

如图 1-13 所示，SAN 类似于 LAN 体系结构，这样就可以通过集线器、交换机，甚至控制器来连接许多设备，以获得更高可用性。SAN 使服务器可以与存储设备（如磁盘子系统和磁带库）建立多个直接连接。

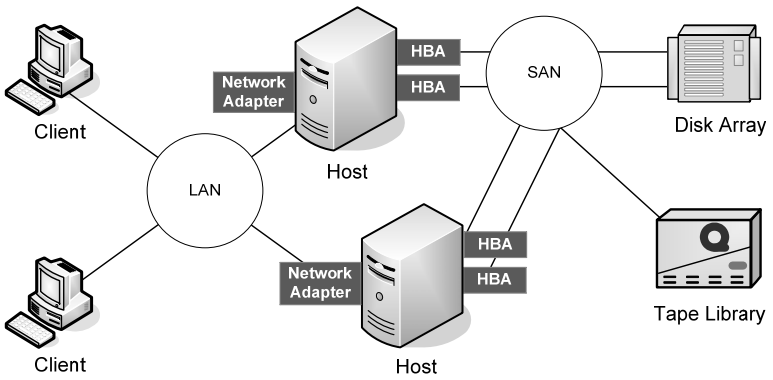


图 1-13　基本形式的 SAN 网络

2．名词：虚拟专用网（VPN）

如图 1-14 中的网络，企业员工需要通过因特网访问企业内部服务器，这就存在了安全问题。虚拟专用网（Virtual Private Network，VPN）就是为了解决这种需求的特殊的网络。它采用一种称为“通道”或“数据封装”的系统，用公共网络及其协议向贸易伙伴、客户、供应商和雇员发送敏感的数据。这种通道是 Internet 上的一种专用通路，可保证数据在网络中安全的传输。

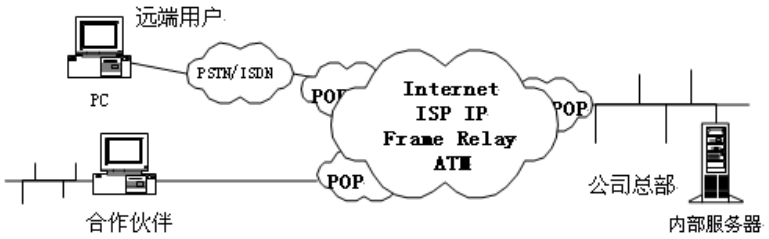


图 1-14　VPN 接入公司网络

企业内部资源享用者只需连入本地 ISP 的 POP（Point Of Presence，接入服务提供点）即可相互通信，利用传统的 WAN 组建技术，彼此之间要有专线相连才可以达到同样的目的。

企业建立 VPN 得到回报非常多。出差员工和外地客户只需拥有本地 ISP 的上网权限就可以访问企业内部资源，如果接入服务器的用户身份认证系统支持漫游的话，甚至不必拥有本地 ISP 的上网权限。VPN 对于流动性很大的出差员工和分布广泛的客户与合作伙伴来说是很有意义的组网方式。

3．名词：内部网络（Intranet）

Intranet 就是建立在企业内部的 Internet，又称内连网，也有人称为“Internal Internet 或

Corporate Internet”。它是一种基于 Internet 的 TCP/IP，采用防止外界侵入的安全措施，为企业内部服务并有连接 Internet 功能的企业内连网络。实际上，它将 Internet 技术运用到企业内部的信息系统中去，以企业内部员工为服务对象，以促进公司内部各个部门的沟通、提高工作效率、增加企业竞争力为目的，使用 Web 协议构建企业级的信息集成和信息服务。

4．名词：外部网络（Extranet）

Extranet 是 Intranet 的延伸和扩展。Intranet 的着眼点在于企业内部，是一种与外部世界完全隔离的内部网络，而 Extranet 是一个使用 Intranet 技术使企业与其客户和其他相关企业相连以完成共同目标的交互式合作网络。外部网络中的信息交流着眼于企业与外部，即企业与客户、企业与贸易伙伴之间的信息交流。

有时 LAN、MAN 和 WAN 间的边界非常不明显，很难确定 LAN 在何处终止，MAN 或 WAN 在何处开始，这就造成了企业外部网络和内部网络的区分问题。确定一个网络边界的主要因素是协议或者说使用的协议。

1.6　利用分层模型解决网络故障

20 世纪 80 年代中期，各大公司逐渐感受到了盲目地大规模扩展网络带来的后果，使用不同标准的网络之间很难通信，于是他们意识到必须摒弃先前的专用网络系统，制定一种网络之间连接的标准。1984 年发布的 OSI-RM 开放体系模型（Open System Interconnection - Reference Model），它为各个厂商提供了一套标准，确保全世界各公司提出的不同类型网络技术之间具有良好兼容性和互操作性。

1.6.1　OSI 模型概述

开放系统互连参考模型（Open System Interconnection - Reference Model）中的关键字“开放”与“互连”就是为解决这个问题。“开放”表示能使任何两个遵守参考模型和有关标准的系统进行连接。“互连”是指将不同的系统互相连接起来，以达到相互交换信息、共享资源、分布应用和分布处理的目的。

1．OSI 各层含义

OSI-RM 开放系统互连参考模型采用分层的结构化技术，共分为 7 层，从低到高为：物理层、数据链路层、网络层、传输层、会话层、表示层、应用层。OSI 参考模型各层功能的简单描述如图 1-15 所示。

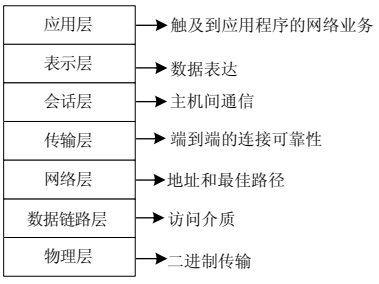


图 1-15　OSI 参考模型分层结构

OSI 参考模型的每一层都有它自己必须实现的一系列功能，以保证数据报文能从源传输到目的地。下面简单介绍一下 OSI 参考模型各层的功能。

1）物理层（Physical Layer）

物理层位于 OSI 参考模型的最底层，它直接面向原始比特流的传输。为了实现原始比特流的物理传输，物理层必须解决好包括传输介质、信道类型、数据与信号之间的转换、信号传输中的衰减和噪声等在内的一系列问题。另外，物理层标准要给出关于物理接口的机械、

电气功能和规程特性，以便于不同的制造厂家既能够根据公认的标准各自独立地制造设备，又能使各个厂家的产品能够相互兼容。

2）数据链路层（Data Link Layer）

数据链路层涉及相邻节点之间的可靠数据传输，数据链路层通过加强物理层传输原始比特的功能，使之对网络层表现为一条无错线路。为了能够实现相邻节点之间无差错的数据传输，数据链路层在数据传输过程中提供了确认、差错控制和流量控制等机制。在数据链路层的设备由二层交换机和网桥。

3）网络层（Network Layer）

网络中的两台计算机进行通信时，中间可能要经过许多中间节点甚至不同的通信子网。网络层的任务就是在通信子网中选择一条合适的路径，使发送端传输层所传下来的数据能够通过所选择的路径到达目的端。网络层提供了路由及其相关功能，可以将众多的数据链路结合成一个互连的网络，这是通过设备的逻辑寻址（与物理寻址相对）来实现的。

4）传输层（Transport Layer）

传输层是 OSI 参考模型中唯一负责端到端节点间数据传输和控制功能的层。传输层是 OSI 参考模型中承上启下的层，它下面的三层主要面向网络通信，以确保信息被准确有效地传输；它上面的 3 个层次则面向用户主机，为用户提供各种服务。

传输层通过弥补网络层服务质量的不足，为会话层提供端到端的可靠数据传输服务。它为会话层屏蔽了传输层以下的数据通信的细节，使会话层不会受到下三层技术变化的影响。但同时，它又依靠下面的 3 个层次控制实际的网络通信操作，来完成数据从源到目标的传输。传输层为了向会话层提供可靠的端到端传输服务，也使用了差错控制和流量控制等机制。

5）会话层（Session Layer）

会话层的主要功能是在两个节点间建立、维护和释放面向用户的连接，并对会话进行管理和控制，保证会话数据可靠传输。会话层是建立在传输层之上，由于利用传输层提供的服务，使得两个会话实体之间不考虑它们之间相隔多远，使用了什么样的通信子网等网络通信细节，从而进行透明的、可靠的数据传输。

6）表示层（Presentation Layer）

在 OSI 模型中，表示层的作用是为通信双方的应用层实体提供共同的表达手段，使双方能正确地理解所传送的信息。

表示层为应用层提供了各种编码和数据转换功能。这些功能可以确保发自某个系统的应用层信息可以被另一个系统的应用层解读出来，表示层的一些编码与转换例子包括公共数据表示格式、字符表示格式的转换、公共数据压缩方案及公共数据加密方案等。

7）应用层（Application Layer）

应用层是 OSI 参考模型中最靠近用户的一层，负责为用户的应用程序提供网络服务。与 OSI 参考模型其他层不同的是，它不为任何其他 OSI 层提供服务，而只是为 OSI 模型以外的应用程序提供服务。

OSI 关心的主要是进程之间的通信行为，因而对应用进程只保留了进程间交互行为的有关部分。这种现象实际上是对应用进程进行了某种程度上的简化，经过抽象（简化）后的应用进程就是应用实体 AE（Application Entity）。应用层为相互通信的 AE 建立连接、进行同步，建立关于错误纠正和控制数据完整性过程的协商等。应用层还包含大量的应用协议，如远程

登录（Telnet）、简单邮件传输协议（SMTP）、简单网络管理协议（SNMP）和超文本传输协议（HTTP）等。

2．层间通信的方法

OSI 使用协议数据单元（Protocol Data Unit，PDU）在层间进行通信。PDU 是加入到用户数据中的信息，这部分控制信息保存在称为“头域”和“尾域”中，进而保持在每个设备上的同样功能，如寻址和控制信息等。因为 PDU 在上下层间传输了修改后的信息，因此根据它负载的信息给出不同的名字。

- 应用层：报文（Message）。
- 传输层：数据段（Segment）。
- 网络层：分组（数据包）（Packet）。
- 数据链路层：数据帧（Frame）。
- 物理层：比特（Bit）。

信号通过网络媒介传送出去，数据沿着堆栈向下传输并加入头和尾的方法称为“封装”。以一封电子邮件的发送和接收为例，其传输过程如图 1-16 所示。

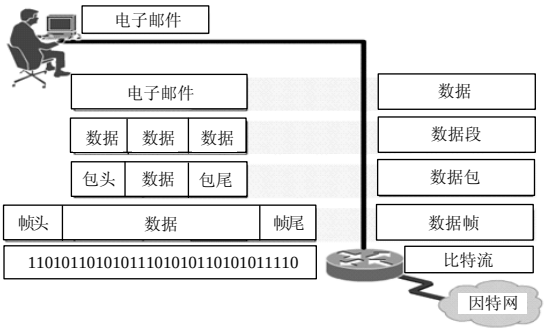


图 1-16　封装过程

第 1 步：创建数据（应用层、表示层、会话层），当用户发送一个电子邮件信息时，它的字母或数字字符被转换成可以通过因特网传输的数据。

第 2 步：为端到端的传输将数据打包（传输层），通过对数据打包来实现因特网的传输。通过使用段，传输功能确保在两端的信息主机的电子邮件系统之间进行可靠的通信。

第 3 步：在报头上附加网络地址（网络层），数据被放置在一个分组或者数据报中，其中包含了带有源和目的逻辑地址（如 IP 地址）的网络报头。这些地址有助于网络设备在动态选定的路径上发送这些分组。

第 4 步：附加本地地址（MAC 地址）到数据链路报头（数据链路层），每一个网络设备必须将分组放置在帧中。该帧的报头包括在路径中下一台直接相连设备的物理地址（如 MAC 地址）。

第 5 步：为进行传输而转换为比特（物理层），帧必须被转换成一种 1 和 0 的模式，才能在介质上（通常为线缆）进行传输。

第 6 步：数据被封装通过网络传送后，接收设备的第一个 OSI 层查看来自对等层的头部信息，除去该头部信息，将余下的信息单元发送到上一个 OSI 层，当应用层完成了这些工作后，接收设备就接收到了需要的数据，这个过程就是“解封装”。

1.6.2　网络故障背景介绍

中铁集团某分公司进行了一次网络改造，分公司的网络用户报告说其中有一台客户端在调整办公室后无法访问总部服务器。由于总公司到分公司的路途遥远，所以采用了电话支持

和网络设备远程排错的方法，最终排除了故障。

1.6.3　选择排查故障的方法

OSI 模型并不只是一项“死”知识，而是指导网络组建和故障排除的一种原则。利用 OSI 模型排除网络错误工作中有 3 种方法可以使用。

（1）从下至上的方法：从 OSI 模型底端开始，顺序向上。

（2）从上至下的方法：从 OSI 模型顶端开始，顺序往下。

（3）分而治之的方法：从 OSI 模型特定层开始，确定问题是在该层、还是上层或下层。

由于分公司的其他客户端都能访问到总部的服务器，而只有一个客户端无法访问，所以应该确认服务器的应用程序是没有问题的，所以可以采用“从下至上”的方法排除网络故障，即从物理层开始。由于是远程管理，在处理此次网络故障时总部工程师并没有到现场，但最终排除了故障。他们并不是通过经验直接判断问题的症结之处，而是根据 OSI 的 7 层模型，从“物理层”开始排除问题的，当确保网卡和网络连接没有问题的时候，再“上升一层”排除问题，直至找到了最终答案。

下面排除故障中用到了一些命令，现在你可能还不了解它们，在学习完成本书后面的一些网络设置配置命令之后，你就会发现原来这些工程师的操作也不是很神奇。

1.6.4　故障解决思路与步骤

客户端无法访问网络的情况在企业网络故障中应该是最常见的一种，但很多管理员在排查故障的时候，不知道从何处入手。并将这台主机搬回到原信息点后能够访问网络，这就使总部工程师首先怀疑到连接这台客户端的物理层链路出现了问题。

1．物理层检查

工程师首先要求用户检查网络客户端网络的物理连接是否正常，查看网线是否与墙上端口和设备相连，连接点是否牢靠等。用户反馈这些连接部件都是正常，所以工程师决定让用户查看交换机端口的工作状态。

由于分公司采用了标准的布线环境，交换机管理良好，有完备的《网络记录文档》。因此，总部查找到这位用户使用的墙上插座端口号为 A201，而且知道 A201 号口与交换机 2 号口相连。

如果工程师在现场就可查看交换机端口的指示灯状态是否正常，但现在是不可能了。所以只能远程登录到这台交换机，利用 show ip interface brief 命令查看其端口是否工作正常。

一般持续绿色代表链路正常运行，如果闪烁绿色则表明正在发送或者接收数据。

```
3750-24#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet1/0/1   unassigned      YES unset  up                    up
GigabitEthernet1/0/2   unassigned      YES unset  up                    up
GigabitEthernet1/0/3   unassigned      YES unset  up                    up
GigabitEthernet1/0/4   unassigned      YES unset  up                    up
GigabitEthernet1/0/5   unassigned      YES unset  down                  down
```

从这条命令的执行结果中看到：GigabitEthernet1/0/2 状态（Status）和协议（Protocol）

工作都是 up 状态，这证明此终端的线缆连接到交换机是正常的，初步可以排除是物理层的问题。

2．检查数据链路层

既然有连接，说明网络是通的，发生物理层错误的可能性很小，所以可以将故障排查上升一层到数据链路层。因此交换机对数据包的转发是建立在 MAC 地址（物理地址）基础之上的，对于 IP 网络协议来说，它是透明的，即交换机在转发数据包时，不知道也无须知道信源机和信宿机的 IP 地址，只需其物理地址，即 MAC 地址。

是不是我们过分相信《网络记录文档》中的接口信息了，交换机的这个接口没有真正连接到这台客户端，而是连接到其他的客户端呢？此时，可以利用第二层信息的排查来确定这个错误是否存在。第二层的关键是 MAC 地址，可以对照交换机接口上的 MAC 地址和客户端的 MAC 地址是否相同，这样也能排除是不是当初施工时《网络记录文档》出现了问题。使用 show mac address-table interface gigabitEthernet 1/0/2 命令可以显示连接此接口计算机的 MAC 地址信息。

```
3750-24#show mac address-table interface gigabitEthernet 1/0/2
          Mac Address Table
-------------------------------------------
Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
  10    0014.2275.57ac    DYNAMIC     Gi1/0/2
Total Mac Addresses for this criterion: 1
```

此时在客户端上查看本机的 MAC 地址，如果不匹配则说明交换机上的接口并不是真的连接了这台客户端。工程师让用户在客户端上执行 IPCONFIG /ALL 命令，然后将 MAC 地址和上面的进行对比，发现 MAC 地址是相同的。可能在数据链路层还有其他的错误，但至少“网络记录文档”并没有欺骗我们，交换机端口和客户端主机是对应的。

3．检查网络层

接下来查看第三层。在 PC 上使用 IPCONFIG /ALL 命令进行检查，输出结果显示如下：

```
C:\Documents and Settings\Administrator>ipconfig /all
Windows IP Configuration
        Host Name . . . . . . . . . . . . : officetm1
        Primary Dns Suffix  . . . . . . . :
        Node Type . . . . . . . . . . . . : Hybrid
        IP Routing Enabled. . . . . . . . : No
        WINS Proxy Enabled. . . . . . . . : No
        DNS Suffix Search List. . . . . . : gwz.edu
Ethernet adapter 本地连接:
        Connection-specific DNS Suffix  . : zt2.cuchina.com.cn
        Description . . . . . . . . . . . : Realtek RTL8168/8111 PCI-E Gigabit Ethernet NIC
        Physical Address. . . . . . . . . : 00-14-22-75-57-AC
        Dhcp Enabled. . . . . . . . . . . : Yes
        Autoconfiguration Enabled . . . . : Yes
        IP Address. . . . . . . . . . . . : 10.10.2.41
        Subnet Mask . . . . . . . . . . . : 255.255.255.192
        Default Gateway . . . . . . . . . : 10.10.2.62
        DHCP Server . . . . . . . . . . . : 10.88.56.1
        DNS Servers . . . . . . . . . . . : 10.88.56.1
        Primary WINS Server . . . . . . . : 10.88.56.1
```

这里，可以看到 PC 有 IP 地址，但是这地址对吗？这台 PC 通过 DHCP 获得 10.88.x.x 范围内的地址，但是现在地址却是 10.10.x.x。

终于发现了问题，DHCP 服务器分发的 IP 地址不属于子网。这种问题多出现在 PC 从某个子网挪到另一个子网时，PC 依然请求旧的 IP 地址就产生了问题，由于这台主机从另外的办公室挪过来才出现的问题，因此可以断定问题出现在网络层。

管理员尝试这样解决问题，让 PC 的网络接口租用的 IP 地址重新交付给 DHCP 服务器（即归还 IP 地址）。使用 IPCONFIG /RELEASE，然后使用 IPCONFIG /RENEW 命令， PC 就会获得正确的 IP 地址，所有的网络应用就都可以使用了。

1.7　网络管理的红宝书——TCP/IP

尽管 OSI 参考模型得到了全世界的认同，但是因特网历史上和技术上的开发标准都是 TCP/IP 模型（传输控制协议/网际协议，Transmission Control Protocol/Internet Protocol）。

从网络设备厂商的研发部门，到各个系统集成公司工程师的桌面，总能发现 TCIP/IP 详解一类的书籍。TCP/IP 技术的学习似乎研究和管理网络的一项业内行规，如果你坐在地铁或公交车上，手里抱着一本 TCP/IP 分析的书本，我们能预知你的明天是光明的，并且有可能是辉煌的。

1.7.1　TCP/IP 模型概述

TCP/IP 起源于 20 世纪 60 年代末美国政府资助的一个网络分组交换研究项目，TCP/IP 是发展至今最成功的通信协议，它被用于当今所构筑的最大的开放式网络系统 Internet 之上。

TCP 和 IP 是两个独立且紧密结合的协议，负责管理和引导数据报文在 Internet 上的传输。二者使用专门的报文头定义每个报文的内容。TCP 负责和远程主机的连接，IP 负责寻址，使报文被送到其该去的地方。TCP/IP 也分为不同的层次开发，每一层负责不同的通信功能。但 TCP/IP 简化了层次设备（只有 4 层），由下而上分别为网络接口层、网络层、传输层、应用层，如图 1-17 所示。

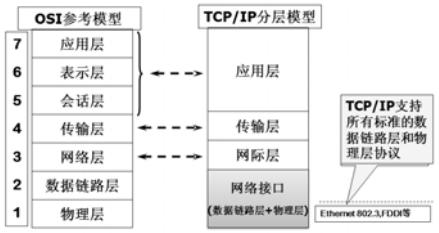


图 1-17　TCP/IP 分层与 OSI 对应关系

由于 TCP/IP 是 OSI 模型之前的产物，所以两者间不存在严格的层对应关系。在 TCP/IP 模型中并不存在与 OSI 中的物理层与数据链路层相对应的部分，相反，由于 TCP/IP 的主要目标是致力于异构网络的互连，所以同 OSI 中的物理层与数据链路层相对应的部分没有进行任何限定。在表 1-3 列出了 TCP/IP 每一层所执行的服务功能和协议。

表 1-3　TCP/IP 模型各层描述

层	描　述	协　议
应用层	定义了 TCP/IP 应用协议及主机程序与要使用网络的传输层服务之间的接口	HTTP、Telnet、FTP、TFTP、SNMP、DNS、SMTP、X-Windows 以及其他应用协议
传输层	提供主机之间的通信会话管理。定义了传输数据时的服务级别和连接状态	TCP、UDP、RTP

Internet 层	将数据装入 IP 数据报，包括用于在主机间及经过网络转发数据报时所用的源和目标的地址信息。实现 IP 数据报的路由	IP、ICMP、ARP、RARP
网络接口层	详细指定如何通过网络实际发送数据，包括直接与网络媒体（如同轴电缆、光纤或双绞铜线）接触的硬件设备如何将比特流转换成电信号	以太网、令牌环、FDDI、X.25、帧中继、RS-232、v.35

TCP/IP 的标准是在名为 Requests for Comments（RFC）的系列文档中发布的。RFC 描述 Internet 的内部运行。TCP/IP 标准总是以 RFC 的形式发布，但并非所有 RFC 都是标准的。一些 RFC 只提供情报信息、实验信息或历史信息。

RFC 最初以 Internet 草案的形式拟定；它们通常由 IETF 职能小组中的一个或多个创作者开发。IETF 职能小组是由一些在 TCP/IP 套件的某一技术领域中具有特定职责的个人所组成的团队。IETF 将以 RFC 的形式发布 Internet 草案的最终版本，并为其分配一个 RFC 编号。

1.7.2　网络接口层中的协议

网络接口层又称为“网络访问层”，主要负责向网络媒体发送 TCP/IP 数据包并从网络媒体接收 TCP/IP 数据包。TCP/IP 独立于网络访问方法、帧格式和媒体，可以使用 TCP/IP 接口层技术组织以太网、无线 LAN 和 WAN 网络之间进行通信。

TCP/IP 支持的网络接口类型包括：标准以太网、令牌环、串行线路网际协议（SLIP）FDDI、串行光学、ATM、点对点协议（PPP）、虚拟 IP 地址等。网络接口层技术将在本书后续章节详细介绍。

1.7.3　Internet 层中的协议

Internet 层的职责包括寻址、打包和路由功能。Internet 层与 OSI 模型的网络层类似。Internet 层包含 ARP、IP（IPv4、IPv6）、ICMP、IGMP 协议，下面将详细地介绍每一种协议。

1．地址解析协议（ARP）

ARP 协议是“Address Resolution Protocol”（地址解析协议）的缩写。ARP 把 IP 地址解析成 LAN 硬件使用的媒体访问控制地址。IP 数据包常通过以太网发送，但以太网设备并不识别 32 位 IP 地址，它们是以 48 位以太网地址传输以太网数据包。因此，必须把 IP 目的地址转换成以太网目的地址。在以太网中，一个主机要和另一个主机进行直接通信，必须要知道目标主机的 MAC 地址。但这个目标 MAC 地址是如何获得的呢？它就是通过地址解析协议获得的。ARP 协议用于将网络中的 IP 地址解析为目标硬件地址（MAC 地址），以保证通信的顺利进行。

RARP 协议，即“Reverse Address Resolution Protocol”（反向地址解析协议）的缩写，RARP 负责将主机的物理地址转换为 IP 地址。例如，局域网中有一台主机只知道物理地址而不知道 IP 地址，那么可以通过 RARP 协议发出征求自身 IP 地址的广播请求，然后由 RARP 服务器负责回答。ARP 和 RARP 使用相同的报头结构，如图 1-18 所示。

硬件类型		协议类型
硬件地址长度	协议长度	操作类型
发送方的硬件地址（0~3 字节）		
源物理地址（4~5 字节）		源 IP 地址（0~1 字节）
源 IP 地址（2~3 字节）		目标硬件地址（0~1 字节）

目标硬件地址（2~5 字节）
目标 IP 地址（0~3 字节）

图 1-18　ARP/RARP 报头结构

另外，为使广播量最小，ARP 维护 IP 地址到媒体访问控制地址映射的缓存以便将来使用。ARP 缓存可以包含动态和静态项目。动态项目随时间推移自动添加和删除。静态项目一直保留在缓存中，直到重新启动计算机为止。

每个动态 ARP 缓存项的潜在生命周期是 10 分钟。新加到缓存中的项目带有时间戳，如果某个项目添加后 2 分钟内没有再使用，则此项目过期并从 ARP 缓存中删除；如果某个项目已在使用，则又收到 2 分钟的生命周期；如果某个项目始终在使用，则会另外收到 2 分钟的生命周期，一直到 10 分钟的最长生命周期。在工作站 PC 的 Windows 环境中，可以使用命令“arp-a”查看当前的 ARP 缓存，如图 1-19 所示。在路由器和交换机中可以用 show arp 完成相同的功能。

下面举个例子：ARP 和 RARP 协议的工作原理。两个位于同一个物理网络上运行 TCP/IP 的主机，如图 1-20 所示，主机 A 和主机 B。主机 A 分配的 IP 地址是 192.168.1.1，主机 B 分配的 IP 地址是 192.168.1.2。

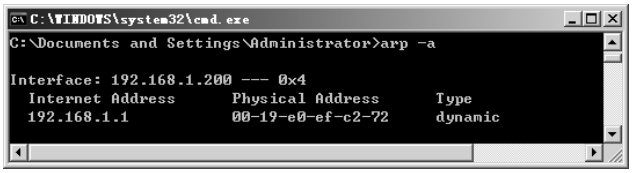


图 1-19　查看 ARP 缓存

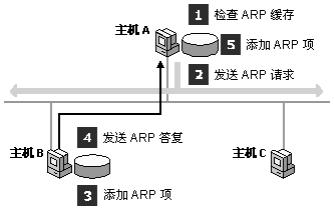


图 1-20　ARP 工作原理解析

当主机 A 要与主机 B 通信时，以下步骤可以将主机 B 软件指定的地址（192.168.1.2）解析成主机 B 硬件指定的媒体访问控制地址。

第 1 步：根据主机 A 上的路由表内容，IP 确定用于访问主机 B 的转发 IP 地址是 192.168.1.2。然后 A 主机在自己的本地 ARP 缓存中检查主机 B 的匹配硬件地址。

第 2 步：如果主机 A 在缓存中没有找到映射，它将询问“192.168.1.2 的硬件地址是什么？”从而将 ARP 请求帧广播到本地网络上的所有主机。源主机 A 的硬件和软件地址都包括在 ARP 请求中。本地网络上的每台主机都接收到 ARP 请求并且检查是否与自己的 IP 地址匹配。如果主机未找到匹配值，它将丢弃 ARP 请求。

第 3 步：主机 B 确定 ARP 请求中的 IP 地址与自己的 IP 地址匹配，将主机的硬件/软件地址映射添加到本地 ARP 缓存中。

第 4 步：主机 B 将包含其硬件地址的 ARP 回复消息直接发送回主机 A。

第 5 步：当主机 A 收到从主机 B 发来的 ARP 回复消息时，会用主机 B 的硬件/软件地址映射更新 ARP 缓存。主机 B 的媒体访问控制地址一旦确定，主机 A 就能向主机 B 发送 IP 通信，为它找到主机的媒体访问控制地址。

2．Internet 协议（IP）

IP 是一个数据报协议，它主要负责在主机之间为数据包进行寻址和路由。但 IP 是无连

接的协议，这意味着它在交换数据之前不建立连接，所以 IP 也是不可靠的，这意味着它不能保证数据包的正确传送。

IP 总是尽“最大努力”来尝试传送数据包，但 IPv4 数据包可能会丢失、错序发送、重复或延迟，所以需要更高层协议（例如，TCP 或某个应用协议）必须能够确认所传送的数据包并根据需要恢复丢失的数据包。图 1-21 显示了 IP 数据包头部结构。

<table>
<tr><td>版本</td><td>头部长度</td><td>服务类型</td><td colspan="3">总长度</td></tr>
<tr><td colspan="3">标识</td><td colspan="2">分段标志</td><td>分段偏移量</td></tr>
<tr><td colspan="2">生存时间</td><td>协议</td><td colspan="3">校验和</td></tr>
<tr><td colspan="6">源地址</td></tr>
<tr><td colspan="6">目标地址</td></tr>
<tr><td colspan="5">选项</td><td>填充</td></tr>
<tr><td colspan="6">数据</td></tr>
</table>

图 1-21　IP 数据包头部信息

IP 数据包头各部分解释如下。

- 版本：用于传输数据的 IP 版本，大小为 4 位。
- 头部长度：用于规定报头长度。
- 服务类型：用于设置数据传输的优先权或者优先级，其大小为 8 位。
- 总长度：指出数据报的总长，数据报总长=报头长度+数据长度，大小为 16 位。
- 标识：用于标识所有的分段，大小为 16 位。
- 分段标志：确定一个数据报是否可以分段，同时也指出当前分段后面是否还有更多分段，大小为 3 位。
- 分段偏移量：由目标计算机用于查找分段在整个数据报中的位置，大小位 13 位。
- 生存时间：在路由器丢弃数据报之前允许数据报通过的网段数；TTL 是由发送主机设置的；路由器在转发 IPv4 数据包时会使 TTL 递减 1，此字段用于防止数据包在 IPv4 网络中无休止地循环传播，长度为 8 位。
- 协议：指定用于创建数据字段中的数据的上层协议，大小为 8 位。
- 校验和：检查所传输数据的完整性，大小为 16 位。
- 源地址：源 IP 地址，字段长度为 32 位。
- 目标地址：目标 IP 地址，字段长度为 32 位。
- 选项：不止一个必须的字段，字段长度具体取决于所选择的 IP 选项。
- 数据：包含网络中传输的数据，IP 数据报还包括上层协议的报头信息。

3．Internet 控制消息协议（ICMP）

ICMP 全称是 Internet Control Message Protocol，中文名为 Internet 控制消息协议。ICMP 负责向数据通信中的源主机报告错误，可以实现故障隔离和故障恢复。

网络本身并不是十分可靠的，在网络传输过程中，可能会发生许多突发事件并导致数据传输失败。前面说到的 IP 是一个无连接的协议，它不会处理网络层传输中的故障，而位于网络层的 ICMP 协议却恰好弥补了 IP 的缺陷，它使用 IP 进行信息传递，向数据包中的源端节点提供发生在网络层的错误信息反馈。另外，通过 ICMP，使用 IP 通信的主机和路由器可以报告错误并交换受限控制和状态信息。

在下列情况中，通常自动发送 ICMP 消息：

- IP 数据报无法访问目标。
- IP 路由器（网关）无法按当前的传输速率转发数据报。
- IP 路由器将发送主机重定向为使用到达目标的更佳路由。

在 IP 数据包中封装和发送 ICMP 消息，如图 1-22 所示。

这里需要注意：由于 ICMP 消息是在 IP 数据包中携带的，因此也是不可靠的。不同类型的 ICMP 消息在 ICMP 报头中标识，表 1-4 列出并说明最常见的 ICMP 消息类型。

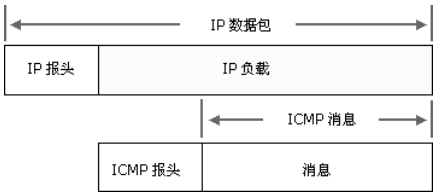


图 1-22　ICMP 在 IP 数据包封装

表 1-4　ICMP 消息类型

ICMP 消息	描　　述
请求回显	确定 IP 节点（主机或路由器）能否在网络上使用
回显答复	回复 ICMP 回显请求
无法连接目标	通知主机数据报无法传递
源结束	通知主机由于拥塞而降低发送数据报的速率
重定向	通知首选路由的主机
超时	指明 IP 数据报的生存时间（TTL）已到期

网络管理员经常使用 Ping 命令发送 ICMP 回显请求消息并记录收到 ICMP 回显答复消息。使用这些消息，可以检测网络或主机通信故障并解决常见的 TCP/IP 连接问题。

4．Internet 组管理协议（IGMP）

IGMP 全称是 Internet Group Multicast Protocol，中文名为 Internet 组管理协议。该协议运行于主机和与主机直接相连的组播路由器之间，是 IP 主机用来报告多址广播组成员身份的协议。通过 IGMP，一方面可以通过 IGMP 主机通知本地路由器希望加入并接收某个特定组播组的信息。另一方面，路由器通过 IGMP 周期性地查询局域网内某个已知组的成员是否处于活动状态。

IGMP 的主要作用是解决网络上广播时占用带宽的问题。在网络中，当给所有客户端发出广播信息时，支持 IGMP 的交换机会将广播信息不经过滤地发给所有客户端。但是这些信息只需要通过组播的方式传输给某一个部分的客户端。

1.7.4　传输层中的协议

传输层（又称主机到主机传输层）为应用层提供会话和数据报通信服务。传输层承担 OSI 传输层的职责。传输层的核心协议是 TCP 和 UDP。TCP 提供一对一的、面向连接的可靠通信服务。TCP 建立连接，对发送的数据包进行排序和确认，并恢复在传输过程中丢失的数据包。与 TCP 不同，UDP 提供一对一或一对多的、无连接的不可靠通信服务。

不论是 TCP/IP 还是在 OSI 参考模型中，任意相邻两层的下层为服务提供者，上层为服务调用者。下层为上层提供的服务可分为两类：面向连接服务和无连接服务。

1）面向连接的网络服务

面向连接的网络服务又称为虚电路（Virtual Circuit）服务，它具有网络连接建立、数据

传输和网络连接释放三个阶段。是按顺序传输可靠的报文分组方式，适用于指定对象、长报文、会话型传输要求。

面向连接服务以电话系统为模式。要和某个人通话，首先拿起电话，拨号码，通话，然后挂断。同样在使用面向连接的服务时，用户首先要建立连接，使用连接，然后释放连接。连接本质上像个管道：发送者在管道的一端放入物体，接收者在另一端按同样的次序取出物体；其特点是收发的数据不仅顺序一致，而且内容也相同。

2）无连接的网络服务

无连接网络服务的两实体之间的通信不需要事先建立好一个连接。无连接网络服务有 3 种类型：数据报（Datagram）、确认交付（Confirmed Delivery）与请求回答（Request reply）。

无连接服务以邮政系统为模式。每个报文（信件）带有完整的目的地址，并且每一个报文都独立于其他报文，由系统选定的路线传递。在正常情况下，当两个报文发往同一目的地时，先发的先到。但是，也有可能先发的报文在途中延误了，后发的报文反而先收到；而这种情况在面向连接的服务中是绝对不可能发生的。

1．传输控制协议（TCP）

TCP 全称是 Transmission Control Protocol，中文名为传输控制协议，它可以提供可靠的、面向连接的网络数据传递服务。传输控制协议主要包含下列任务和功能：

- 确保 IP 数据报的成功传递。
- 对程序发送的大块数据进行分段和重组。
- 确保正确排序及按顺序传递分段的数据。
- 通过计算校验和，进行传输数据的完整性检查。
- 根据数据是否接收成功发送肯定消息。通过使用选择性确认，也对没有收到的数据发送否定确认。
- 为必须使用可靠的、基于会话的数据传输程序，如客户端/服务器数据库和电子邮件程序，提供首选传输方法。

1）TCP 包的结构

TCP 数据包头部总长最小为 20 字节，其结构如图 1-23 所示。

<table>
<tr><td colspan="3">源端口（16）</td><td>目的端口（16）</td></tr>
<tr><td colspan="4">序列号（32）</td></tr>
<tr><td colspan="4">确认号（32）</td></tr>
<tr><td>TCP 偏移量（4）</td><td>保留（6）</td><td>标志（6）</td><td>窗口（16）</td></tr>
<tr><td colspan="3">校验和（16）</td><td>紧急（16）</td></tr>
<tr><td colspan="4">选项（0 或 32）</td></tr>
<tr><td colspan="4">数据（可变）</td></tr>
</table>

图 1-23　TCP 数据包头部结构

- 源端口：指定了发送端的端口。
- 目的端口：指定了接受端的端口号。
- 序列号：指明了段在即将传输的段序列中的位置。
- 确认号：规定成功收到段的序列号，确认序号包含发送确认的一端所期望收到的下

一个序号。

- TCP 偏移量：指定了段头的长度。段头的长度取决于段头选项字段中设置的选项。
- 保留：指定了一个保留字段，以备将来使用。
- 标志：SYN（表示同步）、ACK（表示确认）、PSH（表示尽快地将数据送往接收进程）、RST（表示复位连接）、URG（表示紧急指针）、FIN（表示发送方完成数据发送）。
- 窗口：指定关于发送端能传输的下一段大小的指令。
- 校验和：校验和包含 TCP 段头和数据部分，用来校验段头和数据部分的可靠性。
- 紧急：指明段中包含紧急信息，只有当 URG 标志置 1 时紧急指针才有效。
- 选项：指定了公认的段大小，时间戳，选项字段的末端，以及指定了选项字段的边界选项。

2）TCP 工作原理

TCP 的连接建立过程又称为 TCP 三次握手。首先发送方主机向接收方主机发起一个建立连接的同步（SYN）请求；接收方主机在收到这个请求后向发送方主机回复一个同步/确认（SYN/ACK）应答；发送方主机收到此包后再向接收方主机发送一个确认（ACK），此时 TCP 连接成功建立，如图 1-24 所示。

一旦初始的三次握手完成，在发送和接收主机之间将按顺序发送和确认段。关闭连接之前，TCP 使用类似的握手过程验证两个主机是否都完成发送和接收全部数据。TCP 工作过程比较复杂，包括的内容如下。

- TCP 连接关闭：发送方主机和目的主机建立 TCP 连接并完成数据传输后，会发送一个将结束标记置 1 的数据包，以关闭这个 TCP 连接，并同时释放该连接占用的缓冲区空间。
- TCP 重置：TCP 允许在传输的过程中突然中断连接。
- TCP 数据排序和确认：在传输的过程中使用序列号和确认号来跟踪数据的接收情况。
- TCP 重传：在 TCP 的传输过程中，如果在重传超时时间内没有收到接收方主机对某数据包的确认回复，发送方主机就认为此数据包丢失，并再次发送这个数据包给接收方。
- TCP 延迟确认：TCP 并不总是在接收到数据后立即对其进行确认，它允许主机在接收数据的同时发送自己的确认信息给对方。
- TCP 数据保护（校验和）：TCP 是可靠传输的协议，它提供校验和计算来实现数据在传输过程中的完整性。

3）TCP 与端口号

TCP 和 UDP 都是 IP 层的传输协议，是 IP 与上层之间的处理接口。TCP 和 UDP 端口号被设计来区分运行在单个设备上的多重应用程序的 IP 地址。由于同一台计算机上可能会运行多个网络应用程序，所以计算机需要确保目标计算机上接收源主机数据包的软件应用程序的正确性，以及响应能够被发送到源主机的正确应用程序上。该过程正是通过使用 TCP 或 UDP 端口号来实现的。

在 TCP 和 UDP 头部分，有“源端口”和“目标端口”段，主要用于显示发送和接收过程中的身份识别信息。IP 地址和端口号合在一起被称为“套接字”。TCP 端口比较复杂，其

工作方式与 UDP 端口不同。UDP 端口对于基于 UDP 的通信作为单一消息队列和网络端点来操作，而所有 TCP 通信的终点都是唯一的连接。每个 TCP 连接由两个端点唯一识别。由于所有 TCP 连接由两对 IP 地址和 TCP 端口唯一识别（每个所连主机都有一个地址/端口对），因此每个 TCP 服务器端口都能提供对多个连接的共享访问，如图 1-25 所示。

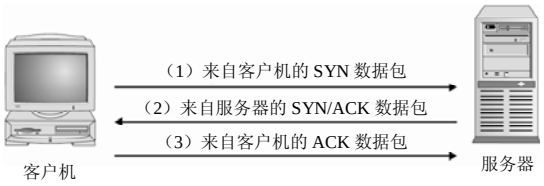


图 1-24　TCP 建立连接

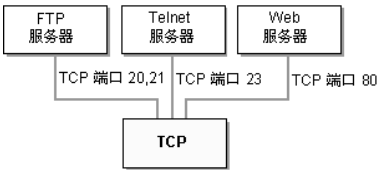


图 1-25　TCP 程序使用保留或已知的端口号

IETF IANA 定义了 3 种端口组。

- 公认端口（Well Known Ports）从 0~1023。
- 注册端口（RegisteredPorts）从 1024~49151。
- 动态和/或专用端口（Dynamic and/or Private Ports）从 49152~65535。

所有小于 1024（当然，也有一些更高的数）的 TCP 服务器端口号都是 Internet 号码指派机构（IANA）保留和注册的。

2．用户数据报协议（UDP）

UDP 全称是 User Datagram Protocol，中文名为用户数据报协议。UDP 提供无连接的网络服务，该服务对消息中传输的数据提供不可靠的、最大努力传送。这意味着它不保证数据报的到达，也不保证所传送数据包的顺序是否正确。UDP 数据包的头部结构如图 1-26 所示。

源端口	目的端口
用户数据包的长度	校验和
数据	

图 1-26　UDP 数据包头部结构

（1）源、目的端口：作用与 TCP 数据段中的端口号字段相同，用来标识源端和目标端的应用进程。

（2）用户数据包的长度：标明 UDP 头部和 UDP 数据的总长度字节。

（3）校验和：用来对 UDP 头部和 UDP 数据进行校验。

这里与 TCP 是不同的，对 UDP 来说，此字段是可选项，而 TCP 数据段中的校验和字段是必须有的。

要使用 UDP，应用程序必须提供源和目标应用程序的 IP 地址和 UDP 端口号。尽管某些 UDP 端口和 TCP 端口使用相同的编号，但这两种端口是截然不同且相互独立的。与 TCP 端口一样，1024 以下的 UDP 端口号是由 IANA 分配的端口。表 1-5 列出了一些常用的 UDP 端口。

表 1-5　UDP 常见端口号

UDP 端口号	描　　述
53	DNS 名称查询
69	TFTP 简单文件传输协议
137	NetBIOS 名称服务
138	NetBIOS 数据报服务
161	简单网络管理协议（SNMP）
520	路由信息协议（RIP）

也许你会问：“既然 UDP 是一种不可靠的网络协议，那么还有什么使用价值或必要呢？”其实不然，在有些情况下 UDP 可能会变得非常有用。因为 UDP 具有 TCP 所望尘莫及的速度优势。虽然 TCP 中植入了各种安全保障功能，但是在实际执行的过程中会占用大量的系统开销，无疑使速度受到严重的影响。反观 UDP 由于排除了信息可靠传递机制，将安全和排序等功能移交给上层应用来完成，极大地降低了执行时间，使速度得到了保证。

1.7.5　应用层中的协议

应用层允许应用程序访问其他层的服务，它定义了应用程序用来交换数据的协议。应用层包含大量的协议，而且人们一直在开发新的协议。人们最熟悉的那些应用层协议可以帮助用户交换信息。

- 超文本传输协议（HTTP）：用于传输那些构成万维网上的页面的文件。
- 文件传输协议（FTP）：用于传输独立的文件，通常用于交互式用户会话。
- 简单邮件传输协议（SMTP）：用于传输邮件和附件。
- 域名系统（DNS）：用于将主机名称（例如，www.microsoft.com）解析为 IP 地址并在 DNS 服务器之间复制名称信息。
- 路由信息协议（RIP）：是路由器用来在 IP 网络上交换路由信息的协议。
- 简单网络管理协议（SNMP）：用于收集网络管理信息并在网络管理控制台和网络设备（例如，路由器、网桥和服务器）之间交换网络管理信息。

1.8　本章小结

本章介绍了网络连接的基本条件及企业组网中常见的网络设备，通过网管员身边的故事解决了一些网络中的数制转换问题，掌握了不同类型网络的特点。应该说，网络基础知识是一个网络管理人员的从业基础，也是阅读后续案例之前的铺垫。

在网络工程和网络管理中，谁都可能遇到一些稀奇古怪的问题，很难从中梳理出头绪，于是网络分层解决问题的方法被认为是最可行的。本章的后两节重点说明了网络分层模型和 TCP/IP 中的核心协议，理解并掌握网络分层的概念，不但能够知道网络数据是如何从一台主机到达另外一台主机的过程。同时，也可以按照这些概念将系统所要实现的复杂功能分化为若干细小模块，每一项分功能以相对独立的方式去实现，这有助于将复杂的问题简化为若干

个相对简单的问题，从而达到分而治之、各个击破的目的。