

计算机网络与物联网

学习目标：

- (1) 理解计算机网络的概念与体系、数据发送中的封装过程。
- (2) 理解计算机网络的节点身份标识协议和数据传输协议。
- (3) 能够使用交换机和路由器搭建和配置计算机网络。
- (4) 理解物联网的基本概念和特征,能够使用手机进行定位和计步。
- (5) 理解一维码的作用,能够使用 Python 编程实现 EAN-13 码。
- (6) 理解二维码的作用,能够使用库函数生成 QR 二维码。

学习内容：

本章讲述计算机网络的概念、发展历程、分层体系结构和数据封装过程,阐述计算机网络的身份标识、数据传输、链路争用和资源共享协议,介绍交换机、路由器和防火墙等计算机网络设备;讲解物联网的概念和特征,物联网感知、标识和卫星定位技术,特别是条形码技术和射频识别技术。

5.1 计算机网络的概念与体系

计算机网络是计算机技术和信息通信技术相结合的产物,是现代社会重要的基础设施,为人类获取和传播信息发挥了巨大的作用。因此,在学习计算机网络知识之前,需要了解计算机网络的概念、分类及其分层体系。

5.1.1 计算机网络的概念和分类

1. 计算机网络的概念

计算机网络是指将地理位置不同的、具有独立功能的多台计算机及其外部设备,通过通信线路连接起来,实现资源共享和信息传递的计算机系统。

最简单的计算机网络只有两个计算机和一条通信链路。最庞大的计算机网络就是因特网。它由大量计算机网络互连而成,因此因特网也称为“网络的网络”。

计算机网络作为一个复杂的、具有综合性技术的系统,为了允许不同系统实体互连和互操作,不同系统在通信时都必须遵从相互均能接受的规则,这些规则的集合称为通信规程或协议(protocol)。协议需要预先制定(或约定)、相互遵循,否则通信双方无法理解对方信息的含义。在这里,系统是指计算机、终端、应用程

序、数据库管理系统、电子邮件系统等；互连是指不同计算机能够通过通信子网互相连接起来进行数据通信；互操作是指不同的用户能够在通过通信链路连接的计算机上，使用相同的命令或操作，使用其他计算机中的资源与信息，就如同使用本地资源与信息一样。

互联、互操作是计算机网络的基本功能，因此，在不引起概念混淆的情况下，我们通常也把计算机网络简称为网络或**互联网**。

2. 计算机网络的分类

根据不同的用户视角或应用方式，计算机网络可以划分为不同的类型。

1) 按照网络共享服务方式划分

从网络服务的管理角度，网络可以划分为客户/服务器(C/S)网络、对等(P2P)网络、浏览器/服务器(B/S)网络和混合网络。图 5-1 给出了 P2P 网络、C/S 网络和 B/S 网络的工作模式图。

P2P 网络：网络中的每台计算机都是平等的，既可承担客户机功能，也可承担服务器功能。当承担客户机功能时，发出服务请求；当承担服务器功能时，给出服务响应，如图 5-1(a)所示。

C/S 网络：网络中的计算机划分为客户机和服务器，客户机只享受网络服务(发出请求)，服务器提供网络资源服务(提供响应)，如图 5-1(b)所示。

B/S 网络：网络中的用户只需要在自己计算机或手机上安装一个浏览器，就可以通过 Web Server 访问网络资源或与后台数据库进行数据交互。该模式将不同用户的接入模式统一到了浏览器上，让核心业务的处理在服务端完成，是 Web 技术兴起后的一种网络结构模式，如图 5-1(c)所示。

混合网络：网络中同时存在两种或多种网络结构，既提供 P2P 网络服务，也提供 C/S 服务或 B/S 服务。

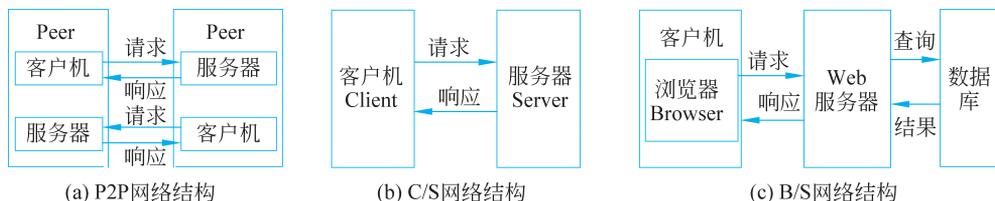


图 5-1 三种网络工作模式图

2) 按照网络节点分布范围划分

按照网络节点分布的地理范围，可以将网络分为局域网、城域网和广域网。

局域网(Local Area Network, LAN)是指网络中的计算机分布在相对较小的区域，通常不超过 10km，如同一房间内的若干计算机，同一楼内的若干计算机；同一校园、厂区内的若干计算机等。在局域网中，当网络节点采用无线连接时，就是无线局域网。

城域网(Metropolitan Area Network, MAN)是指网络中的计算机分布在同一城区内，覆盖范围大约为 10~100km，如一个城市。

广域网(Wide Area Network, WAN)是指网络中的计算机跨区域分布，能够覆盖 100km 以上的范围，比如同一个省、同一个国家或同一个洲甚至跨越几个洲等。广域网也称为互联网(Internet)，通常是由多个局域网或城域网组成的。

3) 根据网络的传输介质划分

根据计算机网络所采用的传输介质,可以将计算机网络分为有线网络和无线网络。

有线网络是指采用双绞线和光纤来连接的计算机网络。双绞线的价格便宜、安装方便,但容易受到干扰;光纤传输距离长、传输速率高、抗干扰能力强,且不会受到电子监听设备的监听,是高安全性网络的理想选择。

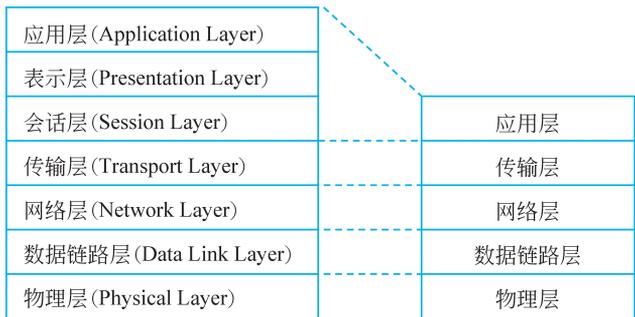
无线网络是指采用电磁波作为载体来实现数据传输的网络类型。由于无线网络联网方式较为灵活,已经成为有线网络的有效补充和延伸。

此外,根据网络的拓扑结构,计算机网络还可以划分为总线型网络(例如以太网)、环状网络(例如令牌环网)、星状网络、树状网络、网状网络和混合网络。

5.1.2 计算机网络的体系结构

计算机网络是相互连接的、以共享资源为目的的、自治的计算机的集合;为了保证计算机网络有效且可靠运行,网络中的各个节点、通信链路必须遵守一整套合理而严谨的结构化管理规则。这些管理规则就包括网络分层体系及其协议规范。

计算机网络按照分层模式建立了一个开放的、能为大多机构和组织承认的网络互联标准,即**开放系统互连**的参考模型(Open System Interconnection Reference Model),简称**OSI/RM**或**OSI参考模型**。OSI参考模型定义了计算机相互连接的标准框架,该框架将网络结构分为七层,如图5-2(a)所示。



(a) 七层OSI参考模型

(b) 五层互联网参考模型

图5-2 计算机网络的层次模型

OSI参考模型的七层具体包括:

1. 物理层

物理层定义信道上传输的原始比特流,例如用多少伏特电压表示“1”,多少伏特电压表示“0”;一个比特持续多少微秒等,从而保证一方发出二进制“1”,另一方收到的也是“1”而不是“0”;此外,还定义网络接插件标准(如针数、各针功能、接头样式等)。

2. 数据链路层

数据链路层负责将数据组合成帧(frame),在两个网络节点之间建立、维持和释放数据链路,控制帧在物理信道上的传输速率、编码方式和差错校验。**帧是数据链路层的传送单位**,包括帧头、数据和帧尾三部分。其中,帧头和帧尾包含一些必要的控制信息,比如同步信息、地址信息、差错控制信息等;数据部分则包含网络层传下来的数据,比如IP数据包等,或从物理层硬件检测后接收的数据。数据链路层通过在帧中引入差错编码(如奇偶校验码、循

环冗余校验)来判定数据帧传输是否出错,如果出错,采用反馈重发的方式来纠正。数据链路层的主要协议包括 HDLC、PPP 等。

3. 网络层

网络层介于传输层和数据链路层之间,其目的是实现两个网络节点或局域网之间的数据包(package)的透明传送,具体功能包括建立、保持和终止网络连接,负责网络的逻辑寻址和路由选择。**包是网络层的传送单位**,包括帧头和数据两部分。其中,帧头包含一些必要的控制信息,比如数据包长、网络地址、校验信息等;数据部分则包含传输层传下来的**数据段(segment)**,或从数据链路层接收的帧。网络层通过**路由选择算法**,为传输层下发的**数据段**选择最适当的通信路径,使得传输层不需要了解网络中的数据传输和交换技术。网络层是计算机网络中通信子网的最高层,主要协议包括 IP、IPX、RIP、OSPF 等。

网络层将来自数据链路层的数据转换为数据分组或包(package),然后通过路径选择、分段组合、流量控制、拥塞控制等将数据包从一台网络设备传送到另一台网络设备。

4. 传输层

传输层是 OSI 参考模型中的第四层,也是整个网络体系结构中最关键的层,因为它是从源节点到目标节点对数据传送进行控制的最后一层。其目的是实现两个网络节点或局域网之间的可靠、有效的报文(message)或数据段传送服务。**报文或数据段是传输层的传送单位**,包括帧头和数据两部分。其中,帧头包含一些必要的控制信息,比如数据端口号、数据包发送或应答序列号、校验和等;数据部分则包含上一层传下来的应用数据,或从网络层接收的数据包。**传输层的主要任务**是将上层应用数据进行分段,形成报文,通过流量控制和差错检测往下传输,防止传输拥堵和保证传输可靠性。在传输层中,最为常见的两个协议分别是传输控制协议(Transmission Control Protocol, TCP)和用户数据报协议(User Datagram Protocol, UDP)。

5. 会话层

会话层位于 OSI 参考模型的第五层,它建立在传输层之上,利用传输层提供的服务,使应用建立和维持会话,并能使会话获得同步。会话层使用校验点可使会话在通信失效时从校验点继续恢复通信。这种能力对于传送大的文件极为重要。会话层支持通信方式的选择、用户间对话的建立和拆除,允许信息同时双向传输。在五层互联网模型中,会话层被合并到了应用层之中。

6. 表示层

表示层位于 OSI 参考模型的第六层,主要作用是异种机通信提供一种公共语言,以便能进行互操作。主要任务包括数据格式转换、数据编码转换、数据加解密、数据压缩和解压等。这种类型的服务之所以需要,是因为不同的计算机体系结构使用的数据表示法不同,如 ASCII、EBCDIC 码等,所以需要表示层协议来保证不同的计算机可以彼此理解。表示层的主要协议包括 JPEG、ASCII、EBCDIC、AES 加密等。在五层互联网模型中,表示层被合并到了应用层之中。

7. 应用层

应用层是 OSI 参考模型的第七层。它向表示层发出请求,为应用程序接口提供常见的网络应用服务。应用层在实现多个系统应用进程相互通信的同时,主要完成一系列业务处理所需的服务。其服务元素分为两类:公共应用服务元素 CASE 和特定应用服务元素

SASE。其中,CASE 主要为应用进程通信、分布系统实现提供基本的控制机制;SASE 则提供文卷传送、访问管理、作业传送、银行事务、订单输入等一些特定的服务。

随着技术的发展,OSI 参考模型中的“会话层”和“表示层”已经被合并到“应用层”之中,所以,目前流行的计算机网络是五层互联网参考模型,如图 5-2(b)所示。

由于计算机网络功能不断壮大,应用种类不断增多,所以,五层互联网参考模型中的应用层协议发展最为迅速,各种新的应用协议不断涌现,这给应用层的功能标准化带来了复杂性和困难性。相比其他层,应用层的标准虽多,但也是最不成熟的一层。目前,应用层的主要协议包括支持网络搜索的超文本传输协议(Hypertext Transfer Protocol,HTTP)、支持文件共享的文件传输协议(File Transfer Protocol,FTP)、支持网络邮箱的简单邮件传输协议(Simple Mail Transfer Protocol,SMTP)等。

5.1.3 计算机网络的数据封装

通过上面 OSI 参考模型的介绍可以发现,计算机网络的每个层次各司其职,负责不同的功能。这些功能组合起来,就可以完成一次完整的数据发送或数据接收过程。数据发送时自顶向下,数据接收时自底向上。下面以五层互联网参考模型为例分别进行介绍。

1. 计算机网络的数据发送

在五层的互联网模型中,数据发送是一个典型的应用数据封装过程。所谓数据封装就是指将每层的协议数据单元(PDU)封装在一组协议头、数据和协议尾中的过程。

图 5-3 给出了计算机网络自顶向下进行数据发送时的数据封装过程。

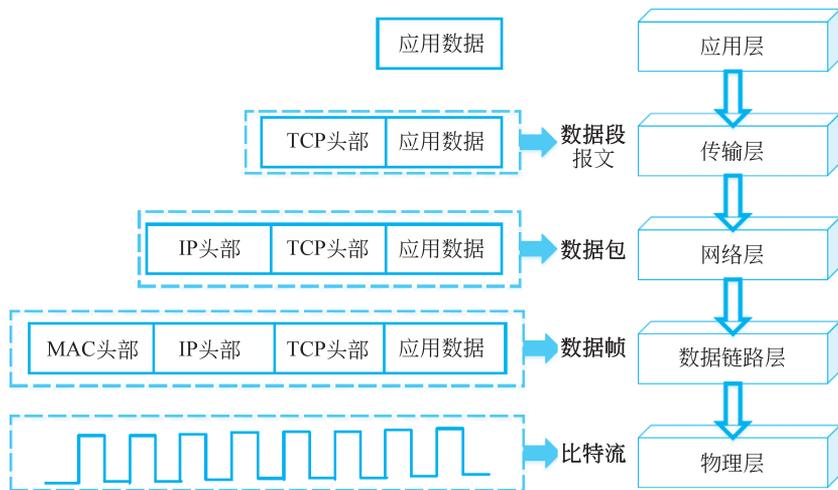


图 5-3 应用数据下发送时的数据封装过程

首先,用户数据通过应用层协议,封装上应用层首部,构成应用数据;应用数据作为整体,在传输层封装上 TCP 首部,成为报文;然后,报文传输到网络层,封装上 IP 首部,成为数据包;封装后的 IP 数据包作为整体传输到数据链路层,数据链路层将其封装上 MAC 头部,成为数据帧。数据帧传输到以太网卡(以太网卡包含了数据链路层的功能和物理层的功能)后,通过硬件加入以太网首部,然后在物理线路上传输。

接收方接到上述数据包后,从以太网卡开始依次解包,获得需要的应用数据。

具体数据发送过程如下。

(1) 在应用层,用户数据添加上一些控制信息(如用户数据大小、用户数据校验码等)后,形成应用数据。如果需要,将应用数据的格式转换为标准格式(如英文的 ASCII 或标准的 Unicode 码),或进行应用数据压缩、加密等,然后发往传输层。

(2) 传输层接收到应用数据后,根据流量控制需要,分解为若干数据段,并在发送方和接收方主机之间建立一条可靠的连接,将数据段封装成**报文**后依次传给网络层。每个报文均包括一个数据段及这个数据段的控制信息(如端口号、数据大小、序列号等)。

(3) 在网络层,来自传输层的每个报文首部被添加上逻辑地址(如 IP 地址)和一些控制信息后,构成一个网络数据包,然后发送到数据链路层。每个数据包增加逻辑地址后,都可以通过互连网络找到其要传输的目标主机。

(4) 在数据链路层,来自网络层的数据包的头部附加上物理地址(即网卡标识,以 MAC 地址呈现)和控制信息(如长度、校验码、类型等),构成一个数据帧,然后发往物理层。需要注意的是:在本地网段上,数据帧使用网卡标识(即硬件地址)可以唯一标识每一台主机,防止不同网络节点使用相同逻辑地址(即 IP 地址)而带来的通信冲突。

(5) 在物理层,数据帧通过网卡上的硬件单元增加链路标志(如 01111110B)后转换为比特流发送到物理链路。比特流的发送需要按照预先规定的数字编码方式和时钟频率进行控制。

2. 计算机网络的数据接收

与发送方的发送数据过程相反,接收方接收数据的过程就是从以太网卡开始逐层依次解包的过程,如图 5-4 所示。

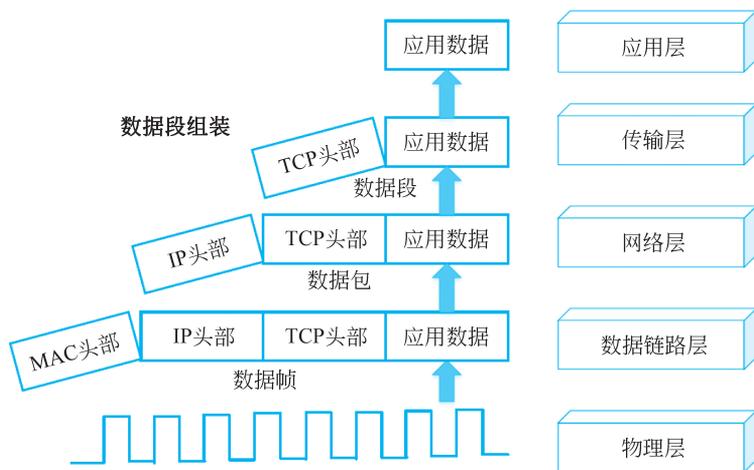


图 5-4 自底向上数据接收的解封装过程

具体过程如下。

(1) 在物理层,连接到物理链路上的网络节点通过网卡上的硬件单元,使用预先规定的数字编码方式和时钟频率对物理链路信息进行读取,形成数据帧,并发往数据链路层。

(2) 在数据链路层,对从物理层接收的数据帧进行校验和物理地址(MAC)比对,如果校验出错或地址比对不符,则抛弃该帧,否则去除物理地址、帧头、帧尾以及校验码后形成数据包,发送到网络层。

(3) 在网络层, 比对数据包头部的逻辑地址(如 IP 地址)与本机设置的 IP 地址是否一致, 如果一致, 则将数据包的 IP 头去除, 形成一个数据报文, 发往传输层, 否则抛弃该数据包。

(4) 传输层收到网络层的数据报文后, 提取报文中的控制信息(如报文系列号等), 将每个报文去除头部信息, 构成数据段后进行缓存。并根据报文的系列号, 将数据段组装成完整的应用数据, 发送到应用层。

(5) 在应用层, 应用数据根据需要进行数据格式转换、解压、解密等处理, 去除一些控制信息(如数据大小、校验码等)后, 转换为用户数据。至此, 数据接收过程完毕。

5.2 计算机网络协议

计算机网络作为一种“信息高速公路”, 面临着“公路”管理同样的难题。在公路管理中, 人、车、路如何协同工作, 长期面临挑战。为了解决上述挑战, 不仅需要通过技术来解决, 更要通过法律、法规来疏导和预防。在计算机网络中也是如此, 必须通过各种规程或协议(类似于法律法规)来保证网络安全、稳定、高效运行。其中就包括网络节点身份标识协议(用来对用户违规和网络故障进行追踪和溯源等)、网络数据传输协议(保证网络节点数据正确到达目标节点)、网络资源竞争协议(保证每个网络节点均有机会使用网络传输信息等)、网络资源共享协议(保证不同组织和个人的信息可以共享和共用等等)。

5.2.1 网络节点身份标识协议

计算机网络的发展是从局域网发展到互联网。为了唯一标识网络中的每个节点, 局域网使用了网络硬件地址(MAC 地址)来标识网络节点, 而由多个局域网互联而成的广域网网络, 则使用了逻辑地址(IP 地址)来标识网络节点。

1. MAC 地址

局域网是计算机网络发展的第一个阶段。为了解决局域网中网络节点的身份标识问题, IEEE 标准规定, 网络中每台设备都要有一个唯一的网络硬件标识, 这个标识就是 MAC 地址。

MAC 地址的直译为媒体存取控制地址, 也称为局域网地址、以太网地址、网卡地址或物理地址, 它用来确认网络节点的身份(或位置), 由网络设备制造商生产时写在硬件内部(一般是网卡内部)。

MAC 地址用于在网络中唯一标识一个网卡。一台设备若有多个网卡, 则每个网卡都需要并会有一个唯一的 MAC 地址。MAC 地址由 48 位(6 字节)组成。书写时通常在每字节之间用“:”或“-”隔开, 如 08-00-20-0A-8C-6D 就是一个 MAC 地址。其中, 前 3 字节是网络硬件制造商的编号, 由 IEEE 分配, 后 3 字节由制造商自行分配, 代表该制造商所生产的某个网络产品(如网卡)的系列号。

查看网络节点的 MAC 地址的流程如下: **控制面板**→**网络和共享中心**→**本地连接**→**详细信息**→**物理地址**。这里的物理地址就是 **MAC 地址**。主要操作过程如图 5-5 所示。

2. IP 地址

随着计算机网络的快速发展, 不同的局域网络连成一体, 出现了互联网。为了屏蔽每个



图 5-5 计算机的 MAC 地址查询方法

局域网络的差异性,做到不同物理网络的互联和互通,就需要提出一种新的统一编址方法,为互联网上每一个子网、每一个主机分配一个全网唯一的地址。

IP 地址被用来给网络上的主机一个编号。IP 地址是一个 32 位的二进制数,通常被分割为 4 字节,书写时用“点分十进制”表示成(a.b.c.d)的形式,其中,a、b、c、d 都是 0~255 的十进制整数。例如,点分十进 IP 地址(128.0.0.7),实际上是 32 位二进制数 10000000.00000000.00000000.00000111。

在 Internet 中,由 NIC 组织统一负责全球 IP 地址的规划、管理,由其下属机构 Inter NIC、APNIC、RIPE 等网络信息中心具体负责美国及全球其他地区的 IP 地址分配。中国申请 IP 地址是通过负责亚太地区事务的 APNIC 进行的。

IP 地址一般包括网络号和主机号两部分。其中网络号的长度决定了整个网络中可包含多少个子网,而主机号的长度决定了每个子网能容纳多少台主机。根据网络号和主机号占用的长度不同,IP 地址可以分为 A、B、C、D 和 E 共 5 类。用二进制代码表示时,A 类地址最高位为 0,B 类地址最高 2 位为 10,C 类地址最高 3 位为 110,D 类地址的最高 4 位为 1110,E 类地址的最高 5 位为 11110。由于 D 类地址分配给多播,E 类地址保留,所以实际可分配的 IP 地址只有 A 类、B 类或 C 类,如图 5-6 所示。

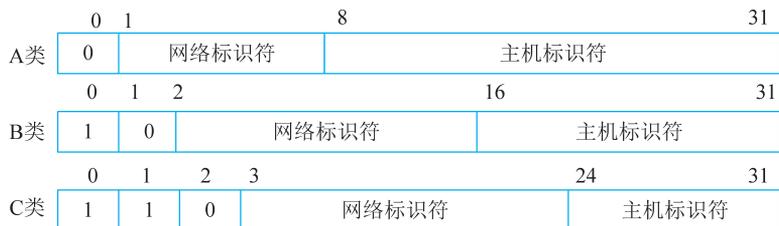


图 5-6 三类可分配的 IP 地址

其中:

A 类地址由最高位的“0”标志、7 位的网络号和 24 位的网内主机号组成。这样,在一个

互联网中最多有 126 个 A 类网络(网络号 1~126, 号码 0 和 127 保留)。而每一个 A 类网络允许有最多 $2^{24} \approx 1677$ 万台主机, 如表 5-1 所示。A 类网络一般用于网络规模非常大的地区网。

B 类地址由最高 2 位的“10”标志、14 位的网络号和 16 位的网内主机号组成。这样, 在互连环境下大约有 16 000 个 B 类网络, 而每一个 B 类网络可以有 65 534 台主机, 如表 5-1 所示。B 类网络一般用于较大规模的单位和公司。

C 类地址由最高 3 位的“110”标志、21 位的网络号和 8 位的网内主机号组成。一个互联网中允许包含约 209 万个 C 类网络, 而每一个 C 类网络中最多可有 254 台主机(主机号全 0 和全 1 有特殊含义, 不能分配给主机), 如表 5-1 所示。C 类网络一般用于较小的单位和公司。

此外, 国际 NIC 组织对 IP 地址还有如下规定: 32 位全“1”表示网络的广播地址, 32 位全“0”表示网络本身; 高 8 位为 1000000 表示回送地址(loopback address), 用于网络软件测试以及本地机进程间通信。最常用的回送地址是 127.0.0.1。

此外, NIC 还为每类地址保留了一个地址段用作私有地址(private address), 专门为组织机构内部使用。三类地址保留的私有地址范围如表 5-1 所示。这些私有地址主要用于企业内部网络之中。

表 5-1 三类地址保留的私有地址范围

类别	最大网络数	IP 地址范围	单个网段最大主机数	私有 IP 地址范围
A	$126(2^7 - 2)$	1.0.0.1~127.255.255.254	16777214	10.0.0.0~10.255.255.255
B	$16384(2^{14})$	128.0.0.1~191.255.255.254	65534	172.16.0.0~172.31.255.255
C	$2097152(2^{21})$	192.0.0.1~223.255.255.254	254	192.168.0.0~192.168.255.255

私有网络由于不与外部互连, 因此可以使用任意的 IP 地址。保留这样的地址供其使用是为了避免以后接入 Internet 时引起的地址混乱。使用私有地址的私有网络在接入 Internet 时, 要使用网络地址转换(Network Address Translation, NAT)协议将私有地址转换成公用合法 IP 地址。在 Internet 上, 这类私有地址是不能出现的。

3. IP 地址和 MAC 地址的异同

由于 IP 地址只是逻辑上的标识, 不受硬件限制, 容易修改(如某些网络节点用户可能基于各种原因使用他人 IP 地址登录网络), 从而出现 IP 地址盗用问题。例如, 我们可以根据需要给一台主机指定任意的 IP 地址。例如, 可以给局域网上的某台计算机分配 IP 地址 202.117.10.191, 也可分配 202.117.10.192。修改网络节点的 IP 地址的具体流程: 控制面板→网络和共享中心→本地连接→属性→Internet 协议版本 4(TCP/IPv4)→IP 地址, 部分流程如图 5-7 所示。

为了解决 IP 地址任意修改或盗用问题, 网络管理者可以将 IP 地址与 MAC 地址绑定。IP 地址和 MAC 地址最大的相同点就是地址都具有唯一性, 主要差异如下。

(1) 可修改性不同: IP 地址是基于网络拓扑设计的, 在一台网络设备或计算机上, 改动 IP 地址是非常容易的; 而 MAC 则是网卡生产厂商烧录好的, 一般不能改动。除非这个计算机的网卡坏了, 在更换网卡之后, 该计算机的 MAC 地址就变了。

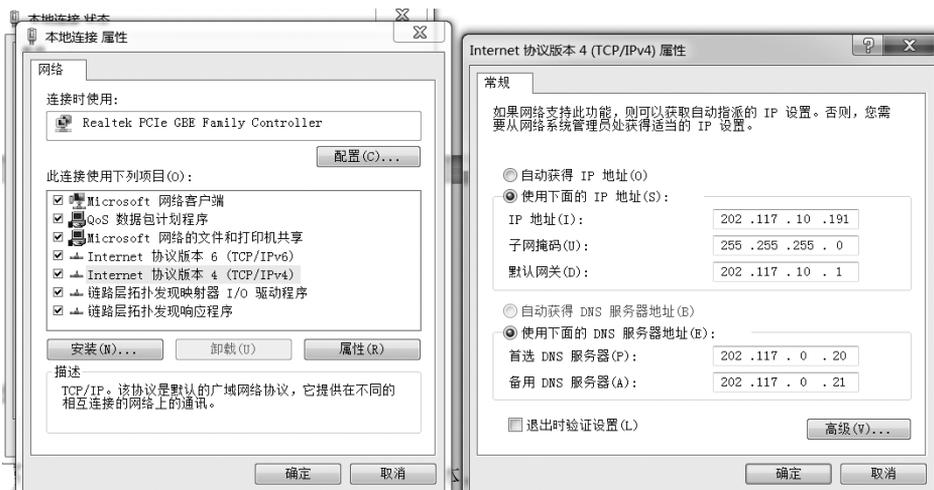


图 5-7 IP 地址查询与修改方法

- (2) 地址长度不同：IP 地址长度为 32 位，MAC 地址为 48 位。
- (3) 分配依据不同：IP 地址的分配是基于网络拓扑的，MAC 地址的分配是基于网卡制造商的。
- (4) 寻址协议层不同：IP 地址应用于 OSI 的网络层，而 MAC 地址应用在数据链路层。
- (5) 传输过程不同：数据链路层通过 MAC 地址将数据从一个节点传输到相同链路的另一个节点；网络层协议通过 IP 地址可以将数据从一个网络传递到另一个网络上，传输过程中可能需要经过路由器等中间节点。

5.2.2 网络节点数据传输协议

实现数据安全、可靠和高效传输是互联网的核心目标。在局域网内部，主要通过数据链路层协议来保障数据可靠传输；在广域网之中，主要通过传输层协议来进一步提高数据传输的可靠性，防止链路拥堵。下面重点介绍其中的 TCP。

1. TCP 报文

TCP 是一种面向连接的、可靠的、基于字节流的传输层通信协议。为了使 TCP 能够独立于特定的网络，TCP 对报文长度有一个限定，即 TCP 传送的数据报长度要小于 64B。因此，对长报文需要进行分段处理后才能进行传输。

TCP 报文是封装在 IP 分组中进行传输的。TCP 报头固定部分的长度为 20 字节，其具体格式如图 5-8 所示。各字段功能说明如下。

源端口和目的端口字段：各占 16 位，分别标志连接两端的应用进程。

序号字段：占 32 位。TCP 的序号不是对每个 TCP 报文的编号，而是对每字节的编号。这样，序号字段指的是该 TCP 报文中数据的起始字节的序号。由于序号长度为 32 位，它可对 2^{32} (4G) 字节进行编号。因此，序号重复时，旧序号数据早已在网络中消失。TCP 在连接建立时还采用了三次握手协议，确保不会把旧的序号当成新的序号。

确认序号字段：占 32 位，采用附载应答方式，指出下一个期望接收的字节序号，也就是告诉对方，这个序号以前的字节都已经正确收到。例如，确认序号为 1024 表示序号为 1023