

计算机网络基础知识简介

主要内容:

- 了解计算机网络的基本概念
- 理解计算机网络体系结构
- 理解数据的封装、解封与传输
- 掌握IP地址&子网划分&超网合并
- 掌握数据线的分类与制作

计算机网络基础知识简介

计算机在人们的日常生活中起着非常重要的作用。每天各个公司以不同的方式使用着计算机和各种软件，其中有一些常用的使用方式：服务器用来存储重要的数据和管理员工帐号；电子制表软件用来组织财务信息；文字处理软件用来生成各种备忘录和文本文档；数据库软件用来存储消费者的详细信息；web浏览器用来访问公司的web站点；计算机在现代生活中扮演着至关重要的角色。

网络是计算机的互联。计算机既可以从网络上获取信息，又可以给网络提供信息。在某种程度上，计算机和网络之间表现出这种相互依赖的关系，计算机可以独立存在，但随着时代发展，计算机越来越依赖网络。

计算机网络概述

- 计算机网络的发展过程
- 计算机网络的组成
- 计算机网络的分类
- 局域网的分类
- 计算机网络的功能与应用

计算机网络的发展过程

- 面向终端分布的计算机系统
- 分组交换数据网(PSDN)出现：
- 局域网（LAN）发展
- 互连网、综合业务数字网ISDN和智能网IN的出现
- 综合业务数字网ISDN
- 智能网IN

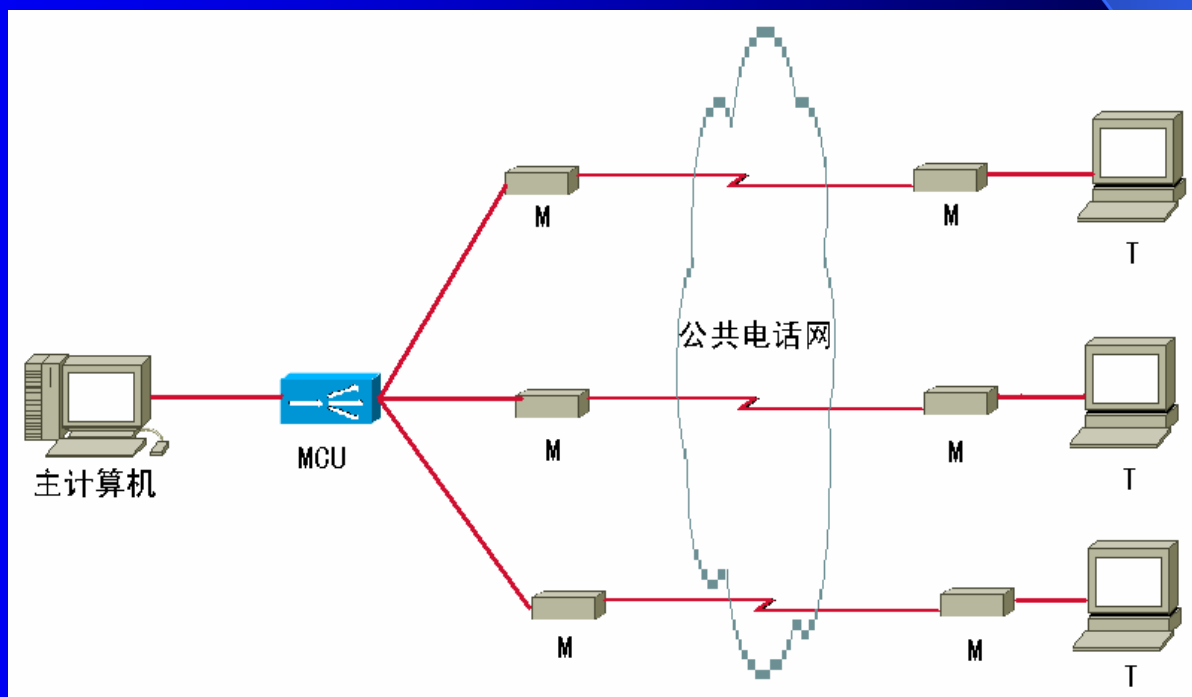
计算机网络的发展过程

计算机与通信（C&C, Computer and Communication）的融合过程就是计算机网络的发展过程，利用通信线路把位于不同地点上的多个计算机系统相互连接起来便形成了计算机网络。在网络中，通过功能完善的网络软件的管理，可以共享某些硬件、软件和数据资源。

计算机网络是计算机技术与通讯技术紧密结合的产物。计算机网络的发展过程经历了三个阶段：具有通信功能的单机系统、具有通信功能的多机系统和计算机网络。

面向终端分布的计算机系统

计算机--终端系统是把多台远程终端设备，通过公用电话网连接到一台中央计算机所构成的面向终端分布的计算机系统，解决远程信息收集、计算和处理。计算机--终端系统提供了计算机通信的许多基本技术，而这种系统本身也成为以后发展起来的计算机网络的组成部分。因此，这种终端联机系统也称为面向终端分布的计算机通信网。也有人称它为第一代的计算机网络。如图1-1所示是这类计算机网的示意图。其中，M--调制解调器，T--终端。



分组交换数据网(PSDN)出现

由于计算机的数据是突发式和间歇性的出现在传输线路上,因此传统的电路交换技术不适合计算机数据的传输。在整个占线期间,真正传送数据的时间往往不到10%甚至1%,所以它对线路的利用率很低,不过它的优点是实时性比较好。20世纪70年代,以美国国防部高级研究计划局DARPA (Defense Advanced Research Project Agency) 的ARPANET为代表,采用崭新的"存贮转发--分组交换"原理,它标志着计算机网络的兴起。ARPANET所采用的一系列技术,为计算机网络的发展奠定了基础。ARPANET中提出的一些概念和术语至今仍被引用。而分组交换网的出现则被公认为现代电信时代的开始。

局域网（LAN）发展

局域网三种基本的拓扑结构是：总线型、环型和星型。市场提供的三种实用的传输介质是双绞线、同轴电缆和光纤。无线传输介质的无线LAN也正在受到重视和发展。介质访问控制技术主要是：载波监听多路访问/冲突监测（CSMA/CD）、令牌传递（Token Passing）、时间片访问控制（Slotted access）。

互连网、综合业务数字网ISDN和智能网IN的出现

- 互连网与OSI的提出

20世纪80年代中，以ISO/OSI七层模型为参照，ISO和国际电报电话咨询委员会CCITT为各个层次制定了一系列协议标准，组成了一个庞大的基本标准集，同时也为OSI的应用和产品的最终实现制定功能标准或轮廓标准ISP（International Standardized profile）。

互连网、综合业务数字网ISDN和智能网IN的出现

- 综合业务数字网ISDN

随着计算机技术、通信技术的发展和应用领域的扩大，通信网络和计算机网络技术一直在迅速发展。综合业务数字网ISDN正是这一发展的体现。

互连网、综合业务数字网ISDN和智能网IN的出现

- 智能网IN

智能网IN（Intelligent Network），是在通信网多种新业务不断发展的情况下，要求运用计算机技术对通信网进行智能化自动管理的形势下产生的。

计算机网络的组成

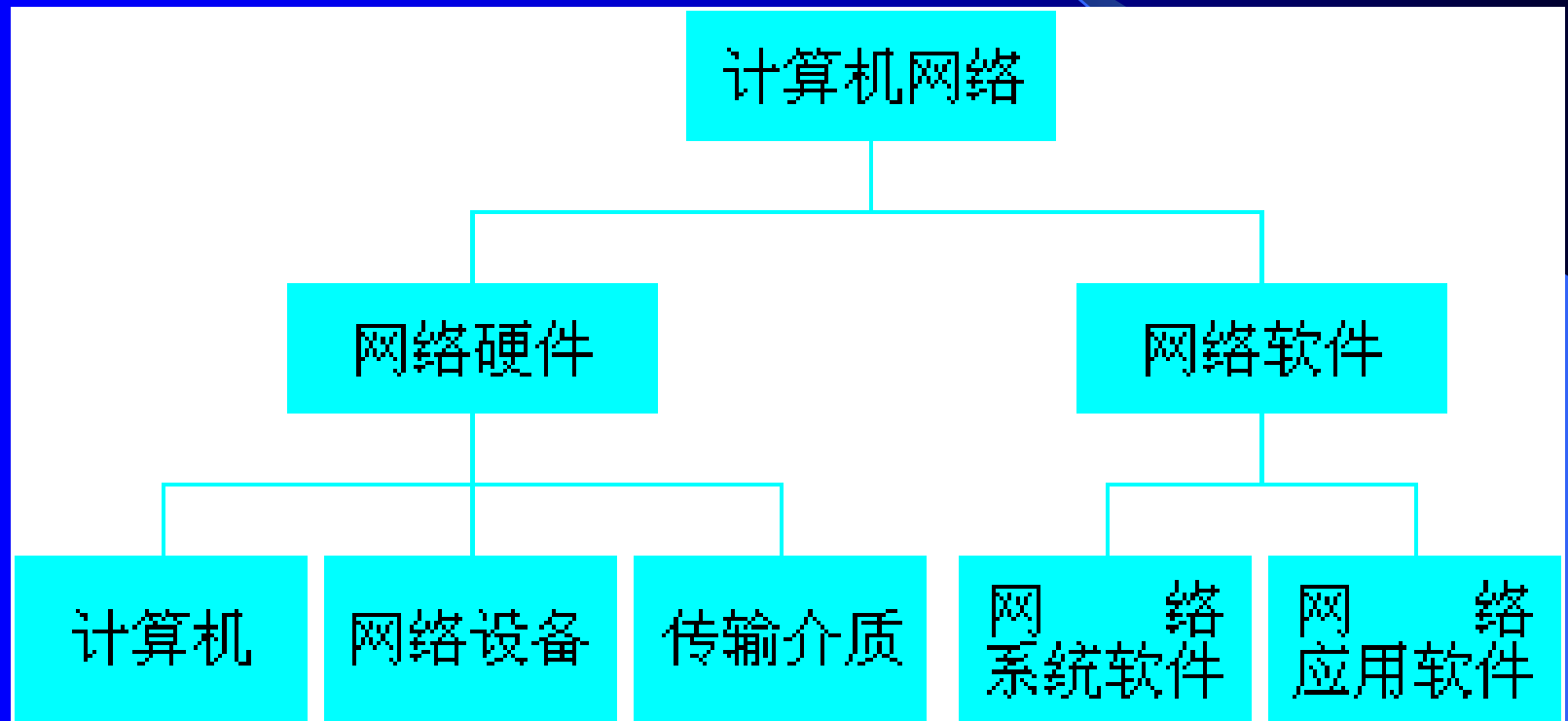
- 计算机网络的逻辑组成
- 计算机网络的物理组成

计算机网络的逻辑组成

计算机网络按逻辑功能可分为资源子网和通信子网两部分。

- 资源子网是计算机网络中面向用户的部分，负责数据处理工作。它包括网络中独立工作的计算机及其外围设备、软件资源和整个网络共享数据。
- 通信子网则是网络中的数据通信系统，它由用于信息交换的网络节点处理机和通信链路组成，主要负责通信处理工作，如网络中的数据传输、加工、转发和变换等。

计算机网络的物理组成



计算机网络的物理组成

- 计算机网络硬件是计算机网络的物质基础，一个计算机网络就是通过网络设备和通信线路将不同地点的计算机及其外围设备在物理上实现连接。因此，网络硬件主要由可独立工作的计算机、网络设备和传输介质等组成。

计算机

独立工作的计算机是计算机网络的核心，也是用户主要的网络资源。根据用途的不同可将其分为服务器和网络工作站。

服务器一般由功能强大的计算机担任，如小型计算机、专用PC服务器或高档微机。它向网络用户提供服务，并负责对网络资源进行管理。一个计算机网络系统至少要有一台或多台服务器，根据服务器所担任的功能不同又可将其分为文件服务器、通信服务器、备份服务器和打印服务器等。

网络工作站是一台供用户使用网络的本地计算机，对它没有特别要求。工作站作为独立的计算机为用户服务，同时又可以按照被授予的一定权限访问服务器。各工作站之间可以相互通信，也可以共享网络资源。在计算机网络中，工作站是一台客户机，即网络服务的一个用户。

网络设备

网络设备是构成计算机网络的一些部件，如网卡、调制解调器、集线器、中继器、网桥、交换机、路由器和网关等。独立工作的计算机是通过网络设备访问网络上的其它计算机。

传输介质

在计算机网络中，要使不同的计算机能够相互访问对方的资源，必须有一条通路使它们能够相互通信。传输介质是网络通信用的信号线路，它提供了数据信号传输的物理通道。传输介质按其特征可分为有线通信介质和无线通信介质两大类，有线通信介质包括双绞线、同轴电缆和光缆等，无线通信介质包括无线电、微波、卫星通信和移动通信等。它们具有不同的传输速率和传输距离，分别支持不同的网络类型。

网络系统软件

网络系统软件是控制和管理网络运行，提供网络通信，管理和维护共享资源的网络软件，它包括网络操作系统、网络通信和协议软件、网络管理软件和网络编程等。

网络应用软件

网络应用软件是指为某一应用目的而开发的网络软件，它为用户提供一些实际的应用。网络应用软件既可用于管理和维护网络本身，也可用于某一个业务领域。例如，以http协议为基础的浏览器软件、网络安全软件、数字图书馆、视频点播、Internet信息服务、远程教学和远程医疗等。

计算机网络的分类

- 局域网 (Local Area Network ; LAN)
- 城域网 (Metropolitan Area Network ; MAN)
- 广域网 (Wide Area Network ; WAN)
- 互联网 (Internet)

局域网 (Local Area Network ; LAN)

通常我们常见的“LAN”就是指局域网，这是我们最常见、应用最广的一种网络。现在局域网随着整个计算机网络技术的发展和得到充分的应用和普及，几乎每个单位都有自己的局域网，有的甚至家庭中都有自己的小型局域网。很明显，所谓局域网，那就是在局部地区范围内的网络，它所覆盖的地区范围较小。局域网在计算机的数量配置上没有太多的限制，少的可以只有两台，多的可达几百台。一般来说在企业局域网中，工作站的数量在几十到两百台次左右。在网络所涉及的地理距离上一般来说可以是几米至10公里以内。局域网一般位于一个建筑物或一个单位内，不存在寻径问题，不包括网络层的应用。

局域网 (Local Area Network ; LAN)

这种网络的特点就是：连接范围窄、用户数少、配置容易、连接速率高。目前局域网最快的速率要算现今的10G以太网了。IEEE的802标准委员会定义了多种主要的LAN网：以太网（Ethernet）、令牌环网（Token Ring）、光纤分布式接口网络（FDDI）、异步传输模式网（ATM）以及最新的无线局域网（WLAN）。这些都将在后面详细介绍。

城域网 (Metropolitan Area Network ; MAN)

这种网络一般来说是在一个城市，但不在同一地理小区范围内的计算机互联。这种网络的连接距离可以在10~100公里，它采用的是IEEE802.6标准。MAN与LAN相比扩展的距离更长，连接的计算机数量更多，在地理范围上可以说是LAN网络的延伸。在一个大型城市或都市地区，一个MAN网络通常连接着多个LAN网。如连接政府机构的LAN、医院的LAN、电信的LAN、公司企业的LAN等等。由于光纤连接的引入，使MAN中高速的LAN互连成为可能。

城域网（Metropolitan Area Network ; MAN）

城域网多采用ATM技术做骨干网。ATM是一个用于数据、语音、视频以及多媒体应用程序的高速网络传输方法。ATM包括一个接口和一个协议，该协议能够在在一个常规的传输信道上，在比特率不变及变化的通信量之间进行切换。ATM也包括硬件、软件以及与ATM协议标准一致的介质。ATM提供一个可伸缩的骨干基础设施，以便能够适应不同规模、速度以及寻址技术的网络。ATM的最大缺点就是成本太高，所以一般在政府城域网中应用，如邮政、银行、医院等。

广域网 (Wide Area Network ; WAN)

这种网络也称为远程网，所覆盖的范围比城域网（MAN）更广，它一般是在不同城市之间的LAN或者MAN网络互联，地理范围可从几百公里到几千公里。因为距离较远，信息衰减比较严重，所以这种网络一般是要租用专线，通过IMP（接口信息处理）协议和线路连接起来，构成网状结构，解决循径问题。这种城域网因为所连接的用户多，总出口带宽有限，所以用户的终端连接速率一般较低，通常为9.6Kbps~45Mbps 如：邮电部的CHINANET，CHINAPAC，和CHINADDN网。

互联网 (Internet)

互联网又因其英文单词“Internet”的谐音，又称为“英特网”。在互联网应用如此发展的今天，它已是我们要每天都要打交道的一种网络，无论从地理范围，还是从网络规模来讲它都是最大的一种网络，就是我们常说的“Web”、“WWW”和“万维网”等多种叫法。从地理范围来说，它可以是全球计算机的互联，这种网络最大的特点就是不定性，整个网络的计算机每时每刻随着人们网络的接入在不变的变化。当您连在互联网上的时候，您的计算机可以算是互联网的一部分，但一旦当您断开互联网的连接时，您的计算机就不属于互联网了。但它的优点也是非常明显的，就是信息量大，传播广，无论您身处何地，只要联上互联网您就可以对任何可以联网用户发出您的信函和广告。因为这种网络的复杂性，所以这种网络实现的技术也是非常复杂的。

局域网的分类

虽然目前我们所能看到的局域网主要是以双绞线为代表传输介质的以太网，那只不过是我們所看到都基本上是企、事业单位的局域网，在网络发展的早期或在其它各行各业中，因其行业特点所采用的局域网也不一定都是以太网，目前在局域网中常见的有：以太网（Ethernet）、令牌网（Token Ring）、FDDI网、异步传输模式网（ATM）等几类，下面分别作一些简要介绍。

以太网（EtherNet）

以太网最早是由Xerox（施乐）公司创建的，在1980年由DEC、Intel和Xerox三家公司联合开发为一个标准。以太网是应用最为广泛的局域网，包括标准以太网（10Mbps）、快速以太网（100Mbps）、千兆以太网（1000Mbps）和10G以太网，它们都符合IEEE802.3系列标准规范。

标准以太网

最开始以太网只有10Mbps的吞吐量，它所使用的是CSMA / CD（带有冲突检测的载波侦听多路访问）的访问控制方法，通常把这种最早期的10Mbps以太网称之为标准以太网。以太网主要有两种传输介质，那就是双绞线和同轴电缆。所有的以太网都遵循IEEE 802.3标准，下面列出是IEEE 802.3的一些以太网标准，在这些标准中前面的数字表示传输速度，单位是“Mbps”，最后的一个数字表示单段网线长度（基准单位是100m），Base表示“基带”的意思，Broad代表“带宽”。

- ·10Base - 5 使用粗同轴电缆，最大网段长度为500m，基带传输方法；
- ·10Base - 2 使用细同轴电缆，最大网段长度为185m，基带传输方法；
- ·10Base - T 使用双绞线电缆，最大网段长度为100m；
- ·1Base - 5 使用双绞线电缆，最大网段长度为500m，传输速度为1Mbps；
- ·10Broad - 36 使用同轴电缆（RG - 59 / U CATV），最大网段长度为3600m，是一种宽带传输方式；
- ·10Base - F 使用光纤传输介质，传输速率为10Mbps。

快速以太网（Fast Ethernet）

- 随着网络的发展，传统标准的以太网技术已难以满足日益增长的网络数据流量速度需求。在1993年10月以前，对于要求10Mbps以上数据流量的LAN应用，只有光纤分布式数据接口（FDDI）可供选择，但它是一种价格非常昂贵的、基于100Mbps光缆的LAN。1993年10月，Grand Junction公司推出了世界上第一台快速以太网集线器FastSwitch10 / 100和网络接口卡FastNIC100，快速以太网技术正式得以应用。随后Intel、SynOptics、3COM、BayNetworks等公司亦相继推出自己的快速以太网装置。与此同时，IEEE802工程组亦对100Mbps以太网的各种标准，如100BASE - TX、100BASE - T4、MII、中继器、全双工等标准进行了研究。1995年3月IEEE宣布了IEEE802.3u 100BASE - T快速以太网标准（Fast Ethernet），就这样开始了快速以太网的时代。

快速以太网（Fast Ethernet）

快速以太网与原来在100Mbps带宽下工作的FDDI相比它具有许多的优点，最主要体现在快速以太网技术可以有效的保障用户在布线基础实施上的投资，它支持3、4、5类双绞线以及光纤的连接，能有效的利用现有的设施。

快速以太网的不足其实也是以太网技术的不足，那就是快速以太网仍是基于载波侦听多路访问和冲突检测（CSMA / CD）技术，当网络负载较重时，会造成效率的降低，当然这可以使用交换技术来弥补。

快速以太网（Fast Ethernet）

100Mbps快速以太网标准又分为：

- 100BASE - TX
- 100BASE - FX
- 100BASE - T4

快速以太网（Fast Ethernet）

100BASE - TX：是一种使用5类数据级无屏蔽双绞线或屏蔽双绞线的快速以太网技术。它使用两对双绞线，一对用于发送，一对用于接收数据。在传输中使用4B / 5B编码方式，信号频率为125MHz。符合EIA586的5类布线标准和IBM的SPT 1类布线标准。使用同10BASE - T相同的RJ - 45连接器。它的最大网段长度为100米。它支持全双工的数据传输。

快速以太网（Fast Ethernet）

- 100BASE - FX：是一种使用光缆的快速以太网技术，可使用单模和多模光纤（62.5和125um） 多模光纤连接的最大距离为550米。单模光纤连接的最大距离为3000米。在传输中使用4B / 5B编码方式，信号频率为125MHz。它使用MIC / FDDI连接器、ST连接器或SC连接器。它的最大网段长度为150m、412m、2000m或更长至10公里，这与所使用的光纤类型和工作模式有关，它支持全双工的数据传输。100BASE - FX特别适合于有电气干扰的环境、较大距离连接、或高保密环境等情况下的适用。

快速以太网（Fast Ethernet）

100BASE - T4：是一种可使用3、4、5类无屏蔽双绞线或屏蔽双绞线的快速以太网技术。它使用4对双绞线，3对用于传送数据，1对用于检测冲突信号。在传输中使用8B / 6T编码方式，信号频率为25MHz，符合EIA586结构化布线标准。它使用与10BASE - T相同的RJ - 45连接器，最大网段长度为100米。

千兆以太网（GB Ethernet）

随着以太网技术的深入应用和发展，企业用户对网络连接速度的要求越来越高，1995年11月，IEEE802.3工作组委任了一个高速研究组（HigherSpeedStudy Group），研究将快速以太网速度增至更高。该研究组研究了将快速以太网速度增至1000Mbps的可行性和方法。1996年6月，IEEE标准委员会批准了千兆位以太网方案授权申请（Gigabit Ethernet Project Authorization Request）。随后IEEE802.3工作组成立了802.3z工作委员会。IEEE802.3z委员会的目的是建立千兆位以太网标准：包括在1000Mbps通信速率的情况下的全双工和半双工操作、802.3以太网帧格式、载波侦听多路访问和冲突检测（CSMA / CD）技术、在一个冲突域中支持一个中继器（Repeater）、10BASE - T和100BASE - T向下兼容技术千兆位以太网具有以太网的易移植、易管理特性。千兆以太网在处理新应用和新数据类型方面具有灵活性，它是在赢得了巨大成功的10Mbps和100Mbps IEEE802.3以太网标准的基础上的延伸，提供了1000Mbps的数据带宽。这使得千兆位以太网成为高速、宽带网络应用的战略性选择。

千兆以太网（GB Ethernet）

1000Mbps千兆以太网目前主要有以下三种技术版本：1000BASE - SX，- LX和 - CX版本。1000BASE - SX 系列采用低成本短波的CD（compact disc，光盘激光器）或者VCSEL（Vertical Cavity Surface Emitting Laser，垂直腔体表面发光激光器）发送器；而1000BASE - LX系列则使用相对昂贵的长波激光器；1000BASE - CX系列则打算在配线间使用短跳线电缆把高性能服务器和高速外围设备连接起来。

10G以太网

现在10Gbps的以太网标准已经由IEEE 802.3工作组于2000年正式制定，10G以太网仍使用与以往10Mbps和100Mbps以太网相同的形式，它允许直接升级到高速网络。同样使用IEEE 802.3标准的帧格式、全双工业务和流量控制方式。在半双工方式下，10G以太网使用基本的CSMA / CD访问方式来解决共享介质的冲突问题。此外，10G以太网使用由IEEE 802.3小组定义了和以太网相同的管理对象。总之，10G以太网仍然是以太网，只不过更快。但由于10G以太网技术的复杂性及原来传输介质的兼容性问题（目前只能在光纤上传输，与原来企业常用的双绞线不兼容了），还有这类设备造价太高（一般为2~9万美元），所以这类以太网技术目前还处于研发的初级阶段，还没有得到实质应用。

令牌环网

令牌环网是IBM公司于20世纪70年代发展的，现在这种网络比较少见。在老式的令牌环网中，数据传输速度为4Mbps或16Mbps，新型的快速令牌环网速度可达100Mbps。令牌环网的传输方法在物理上采用了星形拓扑结构，但逻辑上仍是环形拓扑结构。结点间采用多站访问部件（Multistation Access Unit, MAU）连接在一起。MAU是一种专业化集线器，它是用来围绕工作站计算机的环路进行传输。由于数据包看起来像在环中传输，所以在工作站和MAU中没有终结器。

令牌环网

在这种网络中，有一种专门的帧称为“令牌”，在环路上持续地传输来确定一个结点何时可以发送包。令牌为24位长，有3个8位的域，分别是首定界符（Start Delimiter，SD）、访问控制（Access Control，AC）和终定界符（End Delimiter，ED）。首定界符是一种与众不同的信号模式，作为一种非数据信号表现出来，用途是防止它被解释成其它东西。这种独特的8位组合只能被识别为帧首标识符（SOF）。由于目前以太网技术发展迅速，令牌网存在固有缺点，令牌在整个计算机局域网已不多见，原来提供令牌网设备的厂商多数也退出了市场，所以在目前局域网市场中令牌网可以说是“昨日黄花”了。

FDDI网 (Fiber Distributed Data Interface)

FDDI的英文全称为“Fiber Distributed Data Interface”，中文名为“光纤分布式数据接口”，它是于20世纪80年代中期发展起来一项局域网技术，它提供的高速数据通信能力要高于当时的以太网（10Mbps）和令牌网（4或16Mbps）的能力。FDDI标准由ANSI X3T9.5标准委员会制订，为繁忙网络上的高容量输入输出提供了一种访问方法。FDDI技术同IBM的Tokenring技术相似，并具有LAN和Tokenring所缺乏的管理、控制和可靠性措施，FDDI支持长达2KM的多模光纤。FDDI网络的主要缺点是价格同前面所介绍的“快速以太网”相比贵许多，且因为它只支持光缆和5类电缆，所以使用环境受到限制、从以太网升级更是面临大量移植问题。

FDDI网 (Fiber Distributed Data Interface)

当数据以100Mbps的速度输入输出时，在当时FDDI与10Mbps的以太网和令牌环网相比性能有相当大的改进。但是随着快速以太网和千兆以太网技术的发展，用FDDI的人就越来越少了。因为FDDI使用的通信介质是光纤，这一点它比快速以太网及现在的100Mbps令牌网传输介质要贵许多，然而FDDI最常见的应用只是提供对网络服务器的快速访问，所以在目前FDDI技术并没有得到充分的认可和广泛的应用。

FDDI网 (Fiber Distributed Data Interface)

FDDI的访问方法与令牌环网的访问方法类似，在网络通信中均采用“令牌”传递。它与标准的令牌环又有所不同，主要在于FDDI使用定时的令牌访问方法。FDDI令牌沿网络环路从一个结点向另一个结点移动，如果某结点不需要传输数据，FDDI将获取令牌并将其发送到下一个结点中。如果处理令牌的结点需要传输，那么在指定的称为“目标令牌循环时间”（Target Token Rotation Time, TTRT）的时间内，它可以按照用户的需求来发送尽可能多的帧。因为FDDI采用的是定时的令牌方法，所以在给定时间中，来自多个结点的多个帧可能都在网络上，以为用户提供高容量的通信。

FDDI网 (Fiber Distributed Data Interface)

FDDI可以发送两种类型的包：同步的和异步的。同步通信用于要求连续进行且对时间敏感的传输（如音频、视频和多媒体通信）；异步通信用于不要求连续脉冲串的普通的数据传输。在给定的网络中，TTRT等于某结点同步传输需要的总时间加上最大的帧在网络上沿环路进行传输的时间。FDDI使用两条环路，所以当其中一条出现故障时，数据可以从另一条环路上到达目的地。连接到FDDI的结点主要有两类，即A类和B类。A类结点与两个环路都有连接，由网络设备如集线器等组成，并具备重新配置环路结构以在网络崩溃时使用单个环路的能力；B类结点通过A类结点的设备连接在FDDI网络上，B类结点包括服务器或工作站等。

ATM网

ATM的英文全称为“asynchronous transfer mode”，中文名为“异步传输模式”，它的开发始于20世纪70年代后期。ATM是一种较新型的单元交换技术，同以太网、令牌环网、FDDI网络等使用可变长度包技术不同，ATM使用53字节固定长度的单元进行交换。它是一种交换技术，它没有共享介质或包传递带来的延时，非常适合音频和视频数据的传输。

ATM网

ATM主要具有以下优点：

- ATM使用相同的数据单元，可实现广域网和局域网的无缝连接。
- ATM支持VLAN（虚拟局域网）功能，可以对网络进行灵活的管理和配置。
- ATM具有不同的速率，分别为25、51、155、622Mbps，从而为不同的应用提供不同的速率。

ATM网

ATM是采用“信元交换”来替代“包交换”进行实验，发现信元交换的速度是非常快的。信元交换将一个简短的指示器称为虚拟通道标识符，并将其放在TDM时间片的开始。这使得设备能够将它的比特流异步地放在一个ATM通信通道上，使得通信变得能够预知且持续的，这样就为时间敏感的通信提供了一个预QoS，这种方式主要用在视频和音频上。通信可以预知的另一个原因是ATM采用的是固定的信元尺寸。ATM通道是虚拟的电路，并且MAN传输速度能够达到10Gbps。

无线局域网 (Wireless Local Area Network ; WLAN)

- 无线局域网是目前最新，也是最为热门的一种局域网，特别是自Intel2003年3月份推出首款自带无线网络模块的迅驰笔记本处理器以来。无线局域网与传统局域网的主要不同之处就是传输介质不同，传统局域网都是通过有形的传输介质进行连接的，如同轴电缆、双绞线和光纤等，而无线局域网则是采用空气作为传输介质的。正因为它摆脱了有形传输介质的束缚，所以这种局域网的最大特点就是自由，只要在网络的覆盖范围内，可以在任何一个地方与服务器及其工作站连接，而不需要重新铺设电缆。这一特点使它非常适合那些移动办公一族，有时在机场、宾馆、酒店等（通常把这些地方称为“热点”），只要无线网络能够覆盖到，它都可以随时随地连接上无线网络，甚至Internet。

无线局域网 (Wireless Local Area Network ; WLAN)

无线局域网所采用的是802.11系列标准，它也是由IEEE 802标准委员会制定的。目前这一系列标准主要有4个标准，分别为：802.11b、802.11a、802.11g和802.11z，前三个标准都是针对传输速度地热异常进行的改进，最开始推出的是802.11b，它的传输速度为11MB / s，因为它的连接速度比较低，随后推出了802.11a标准，它的连接速度可达54MB / s。但由于两者不互相兼容，致使一些早已购买802.11b标准的无线网络设备在新的802.11a网络中不能用，所以在今年前些时候正式推出了兼容802.11b与802.11a两种标准的802.11g，这样原有的802.11b和802.11a两种标准的设备都可以在同一网络中使用。802.11z是一种专门为了加强无线局域网安全的标准。因为无线局域网的“无线”特点，致使任何进入此网络覆盖区的用户都可以轻松以临时用户身份进入网络，给网络带来了极大的不安全因素，为此802.11z标准专门就无线网络的安全性方面作了明确规定，加强了用户身份论证制度，并对传输的数据进行加密。

计算机网络的功能与应用

- 计算机网络的功能
- 计算机网络的应用

计算机网络的功能

资源共享

资源共享包括共享硬件、软件和信息资源。通过资源共享，可使网络中各处的资源互通有无、分工协作，从而大大提高系统资源的利用率。例如，计算机网络允许用户使用网上各种不同类型的硬件设备，这些共享的硬件资源有：高性能计算机、大容量磁盘、高性能打印机和高精度图形设备等等。另外，网络上还提供了许多专用软件以及发布了大量信息，供网络用户调用或访问。

信息交换

通过计算机网络，不同地区的用户可以快速和准确地相互传送信息，这些信息包括数据、文本、图形、动画、声音和视频等。用户还可以收发电子邮件、接通可视电话以及举行视频会议等。

均衡负荷

当网络上某台计算机的任务过重时，通过计算机网络可将新的任务交给网上其它计算机去处理，起到均衡负荷的作用。这样，可以减轻局部的负担，提高设备的效率。

分布式处理

当需要处理综合性的大型作业时，通过一定的算法将作业分解并交给多台计算机进行分布式处理，这样就能提高处理速度，充分发挥设备的利用率。协同式计算方式就是利用网络环境的多台计算机来共同完成一个处理任务。

提高可靠性

提高可靠性表现在计算机网络中的各台计算机可以通过网络彼此互为后备机，一旦某台计算机出现故障，其任务可由其它计算机代为处理。避免了单机无后备使用情况下，某台计算机故障导致系统瘫痪的现象，从而提高了整个系统的可靠性。

计算机网络的应用

网络通信

通过Internet收发电子邮件E-mail已经相当普遍，它为人们的快速联系提供了极大的方便。通过IP电话进行长途通话可以大大降低通话费用，随着高速和宽带网络技术的发展，将给传统的电信业务带来很大的变化。

信息检索

随着Internet迅速的扩展，网上的信息越来越多，用户可以通过计算机网络轻松地访问这些信息。

电子商务

电子商务是一种新兴的处于发展的现代商务方式，它是以计算机网络为基础，通过网络完成产品宣传、产品订货、产品营销及货币支付等贸易方式。电子商务和传统的商务活动不同，它不受时间和空间的限制，而且电子商务节省时间，也大大降低了成本。

OA与CIMS

办公自动化OA的真正实现还是在计算机网络建立之后，通过网络可以非常方便地访问和管理各种办公信息，管理效果成倍增加。

计算机集成制造系统CIMS是在计算机网络和数据库技术的支持下，由以计算机辅助设计为核心的工程信息处理系统、以计算机辅助制造为中心的加工、装配、检测、储运、监控自动化工艺系统和经营管理信息系统所组成的综合体。采用CIMS技术是制造业与世界接轨，实现现代化管理，促进企业机制由计划经济向市场经济转变的有效方法。

另外，计算机网络在过程控制、辅助决策、远程医疗、远程教育、数字图书馆、电视会议、视频点播以及娱乐等方面都具有广阔地应用前景。

计算机网络体系结构（OSI与TCP/IP）

分层体系结构与网络协议

本节将会介绍开放通信是如何产生的，以及开放式数据通信的概念，本章节还介绍了两个层次模型，正是这两个模型使得开放式数据通信成为可能。这两个模型是开放式系统互联（Open Systems Interconnect，OSI）参考模型和TCP/IP参考模型。这些模型通过将网络分为各种功能模块，从而大大提高了网络的可理解程度。这些模块被分为层，这些层次的命令以及开放通信的概念，为TCP/IP各种组件和使用的更广泛探索提供了场景和依据。

分层体系结构

计算机网络是一个复杂的系统，相互通信的两个计算机系统必须高度协调工作才行，而这种“协调”是相当复杂的。“分层”可将庞大而复杂的问题，转化为若干较小的局部问题，而这些较小的局部问题就比较易于研究和处理。通常把计算机网络按照一定的功能与逻辑关系划分成一种层次结构。这种层次结构对用户来说是“透明”的，用户不用关心网络是如何工作的，如用户上网并不需要知道网页是如何生成的。但是作为网络研究人员就要知道这种层次关系及其实现的功能。除了计算机网络的层次结构，计算机网络中通常有很多节点，这些节点在计算机之间需要相互交换数据，交换数据时必须遵守的一组约定或规则称为协议。计算机的网络体系结构就是这种层次结构与协议的集合。

分层体系结构

最初的网络与计算解决方案一起是一个享有很高专利权的互联解决方案，这个方案几乎是一个完整的专利。个人计算机出现前，如果某个公司想使他们的数据处理和记帐功能自动化，就必须为其监管系统与某个厂家联系，而且只能与单一厂家联系。

在该专利中，单一厂家产品环境下，应用软件只执行在由单个操作系统支持的平台之上，操作系统只能安全地执行在相同厂家的硬件产品之上，甚至用户的终端设备和与计算机进行连接的设备都必须是一厂家产品的完整解决方案的一部分。

分层体系结构

在单一厂家、完整解决方案时代，美国国防部（D o D）声称需要一个健壮可靠的通信网络，该网络应该可以把所需要的所有计算机（包括所有被接纳为会员的组织所拥有的计算机）互联起来。这些会员包括大学、智能坦克和国防项目的承包人。这听起来不像是一个完整的系统，但它确实是一个大型系统。在计算机网的发展初期，制造商所开发的硬件、软件和网路平台是一个紧密结合的、非开放式系统。一个用户在平台上的数据。因为制造商想靠此永久留住用户。

分层体系结构

让所有DOD的子机构和承包商的研究组织都使用某一厂商的设备是极不现实的。这样，在不同平台间的通信方案就应运而生。结果就诞生了世界上第一个开放通信协议——网际协议（IP）。

因此，一个开放式网络是一种使得在两台不同计算机之间通信和共享数据成为可能的方式。开放性是通过合作开发和技术规范的维护而达到的。这些技术规范，也称为开放式标准，是完全公开的。或许用于解释通信分层模型（包括逻辑链接）的最好工具就是OSI参考模型。

网络协议

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。在网络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。

网络协议是计算机的网络体系结构中的关键要素之一。协议的三要素为：语法、语义、同步。语法是数据与控制信息的结构或格式，即“怎样通信”的问题。语义是需要发出何种控制信息、执行何种动作和返回应答，即“通信内容”，的问题。同步关系“何时通信”的问题。协议与计算机的网络层次结构相对应。协议体系结构的思想是：用一个构造好的模块集合完成不同的通信功能。

网络协议

OSI参考模型是计算机网络的基本体系结构模型。依据网络的不同，通常使用的协议有：TCI/IP协议、IPX/SPX协议、NetBEUI协议等。TCP/IP（传输控制协议/网间协议）是开放系统互连协议中最早的协议之一，也是目前最完全和应用最广的协议，能实现各种不同计算机平台间的连接、交流和通信；IPX/SPX协议同TCP/IP协议一样，可以在局域网中使用，也可路由到另外的局域网。而NetBEUI可以说是专为小型局域网设计的网络协议，没有路由功能。

网络协议

TCP/IP 是“transmission Control Protocol/Internet Protocol”的简写，中文译名为传输控制协议/互联网协议。TCP/IP（传输控制协议/网间协议）是一种网络通信协议，它规范了网络上的所有通信设备，尤其是一个主机与另一个主机之间的数据往来格式及传送方式。TCP/IP是INTERNET的基础协议，也是一种电脑数据打包和寻址的标准方法。在数据传送中，可以形象地理解为有两个信封，TCP和IP就像是信封，要传递的信息被划分成若干段，每一段塞入一个TCP信封，并在该信封面上记录有分段号的信息，再将TCP信封塞入IP大信封，发送上网。在接受端，一个TCP软件包收集信封，抽出数据，按发送前的顺序还原，并加以校验，若发现差错，TCP将会要求重发。因此，TCP/IP在INTERNET中几乎可以无差错地传送数据。对普通用户来说，并不需要了解网络协议的整个结构，仅需了解IP的地址格式，即可与世界各地进行网络通信。

网络协议

IPX/SPX 是基于施乐的 XEROX'S Network System (XNS) 协议，而 SPX 是基于施乐的 XEROX'S SPP (Sequenced Packet Protocol：顺序包协议) 协议，它们都是由 novell 公司开发出来应用于局域网的一种高速协议。它和 TCP/IP 的一个显著不同就是它不使用 ip 地址，而是使用网卡的物理地址即 (MAC) 地址。在实际使用中，它基本不需要什么设置，装上就可以使用了。由于其在网络普及初期发挥了巨大的作用，所以得到了很多厂商的支持，包括 microsoft 等，到现在很多软件和硬件也均支持这种协议。

网络协议

NetBEUI 即 NetBios Enhanced User Interface，或NetBios增强用户接口。它是NetBIOS协议的增强版本，曾被许多操作系统采用，例如Windows for Workgroup、Win 9x系列、Windows NT等。NETBEUI协议在许多情形下很有用，是WINDOWS98之前的操作系统的缺省协议。总之NetBEUI协议是一种短小精悍、通信效率高的广播型协议，安装后不需要进行设置，特别适合于在“网络邻居”传送数据。所以建议除了TCP/IP协议之外，局域网的计算机最好也安上NetBEUI协议。另外还有一点要注意，如果一台只装了TCP/IP协议的WINDOWS98机器要想加入到WINNT域，也必须安装NetBEUI协议。

OSI参考模型简述

创建于1947年的ISO（International Standard Organization, 国际标准组织）是一个由多个国家组成的国际标准化组织。尽管国际标准化组织主要制订技术方面的标准，但它对经济和社会方面的标准化制定也有重要的影响。由于不同的语言对国际标准化组织的名称有不同的缩写方法，该机构决定使用希腊语单词“isos”，该词在希腊语中是平等的意思（Equal），把这个词的前三个字符i、s、o作为该组织的缩写。

20世纪70年代末期，为了解决各种网络之间不兼容的问题，ISO研究了DEC NET、SNA、TCP/IP等协议，于1984年发布了一套描述性的网络模型——开放系统互连参考模型（OSI, Open System Interconnection Reference Model），为生产商们提供了一个大家共同遵守的标准。该标准最大程度上解决了不同网络间的兼容性和互操作性问题。该参考模型非常详细地描述了网络应该具有的功能模块和它们的互连方法，成为当今最主要的参考标准。

OSI参考模型简述

OSI参考模型是一个纯理论分析模型，也就是说OSI参考模型本身并不是一个具体协议的真实分层，也没有任何一个具体的协议栈具有完整的7个功能分层。虽然我们使用的协议没有严格按照OSI分层，但仍然使用OSI的理论来指导我们的工作，尤其在研究和教学方面。

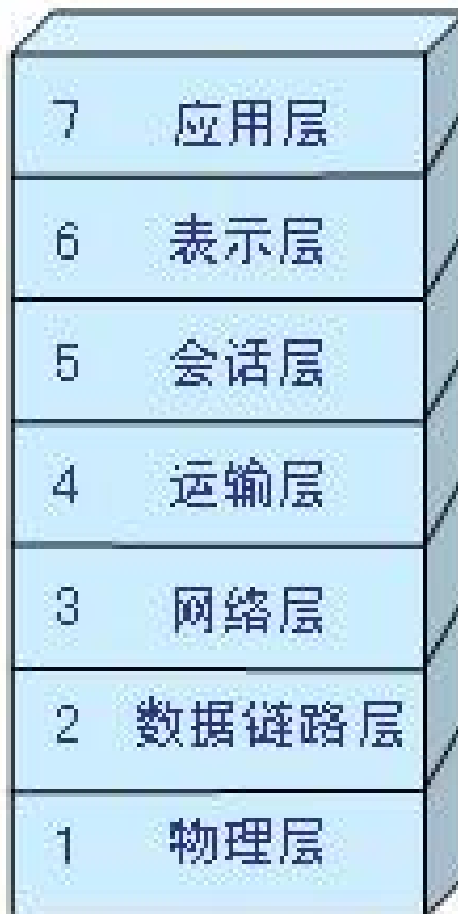
OSI模型将通信会话需要的各种进程划分成7个相对独立的功能层次（Layer），从下到上依次是：第一层,物理层;第二层,数据链路层;第三层，网络层;第四层，传输层;第五层，会话层;第六层,表示层;第七层,应用层。

OSI参考模型简述

分层的一个目的是降低协议的复杂程度。不难想象，把一个复杂的事物分解成若干个部分去分析就会简单得多。分层也有利于加速协议的发展和优化，更好地体现开放性，如可以对某一层做优化修改而不影响其他层的功能。层是根据功能来划分的。如果功能相同或相近就把它们划分在同一层；如果不同，就要分层。不同的层所完成的工作不同。层与层之间并不是孤立的，它们的关系是下层为上层服务。

OSI参考模型

OSI 的体系结构



物理层

最底层称为物理层（Physical Layer），这一层负责传送比特流，它从第二层数据链路层（DDL）接收数据帧，并将帧的结构和内容串行发送即每次发送一个比特，然后这些数据流被传输给DLL重新组合成数据帧。从字面上看，物理层只能看见0和1，它没有一种机制用于确定自己所传输和发送比特流的含义，而只与电信号技术和光信号技术的物理特征相关。这些特征包括用于传输信号，电流的电压、介质类型以及阻抗特征，甚至包括用于终止介质的连接器的物理形状。

物理层

对OSI第一层，人们常常有这样的误解：就是认为OSI第一层应该包括所有产生或发送通信数据信号的机制。其实并非如此，OSI第一层只是一个功能模型，物理层只是一种处理过程和机制，这种过程和机制用于将信号放到传输介质上以及从介质上收到信号。它较低层的边界是连向传输介质的物理连接器，但并不包含传输介质。

物理层

传输介质包含真正用于传输由OSI第一层机制所产生信号的任何方法。一些传输介质是同轴电缆、光纤、双绞线等。人们之所以感到迷惑，主要是因为物理层对介质的性能没有提出任何规范。介质的性能特征对于物理层定义的过程和机制是需要并假定存在的。

物理层为激活、维持和释放端系统之间的物理链路定义了电气、机械、规程的和功能的标准。因此，传输介质处于物理层之外，有时被称为OSI 参考模型的第0层。

数据链路层(DLL)

OSI 参考模型的第二层称为数据链路层 (DLL)。与所有其他层一样，它肩负两个责任：发送和接收。它还要提供数据有效传输的端到端连接。在发送方，DLL需负责将指令、数据等包装到帧中，帧 (frame) 是DLL层生成的结构，它包含足够的信息，确保数据可以安全地通过本地局域网到达目的地。成功发送意味着数据帧要完整无缺地到达目的地。也就是说，帧中必须包含一种机制用于保证在传送过程中内容的完整性。

数据链路层(DLL)

为确保数据传送完整安全到达，必须要做到两点：

- 在每个帧完整无缺地被目标节点收到时，源节点必须收到一个响应。
- 在目标节点发出收到帧的响应之前，必须验证帧内容的完整性。有很多情况可以导致帧的发送不能到达目标或者在传输过程中被破坏或不能使用。DLL有责任检测并修正所有这些错误。

数据链路层(DLL)

DLL的另一个职责是重新组织从物理层收到的数据比特流。不过，如果帧的结构和内容都被发出，DLL并不重建一个帧。相反，它缓存到达的比特流直到这些比特流构成一个完整的帧。

不论哪种类型的通信都要求有第一层和第二层的参与，不管是局域网（LAN）还是广域网（WAN）都是如此，它涉及到物理寻址、网络拓朴、网络介质访问、错误检测、帧的顺序传送和流量控制等问题。

网络层

网络层负责在源机器和目标机器之间建立它们所使用的路由。这一层本身没有任何错误检测和修正机制，因此，网络层必须依赖于端端之间的由DLL提供的可靠传输服务。

网络层用于本地LAN网段之上的计算机系统建立通信，它之所以可以这样做，是因为它有自己的路由地址结构，这种结构与第二层机器地址是分开的、独立的。这种协议称为路由或可路由协议。路由协议包括IP、Novell公司的IPX以及Apple Talk协议。本书将着重讲述IP协议以及与其相关的协议和应用。

网络层

网络层是可选的，它只用于当两个计算机系统处于不同的由路由器分割开的网段这种情况，或者当通信应用要求某种网络层或传输层提供的服务、特性或者能力时。例如，当两台主机处于同一个LAN网段的直接相连这种情况，它们之间的通信只使用LAN的通信机制就可以了（即OSI 参考模型的一二层）。

传输层

传输层提供类似于DLL所提供的服务，传输层的职责也是保证数据在端端之间完整传输，不过与DLL不同，传输层的功能是在本地LAN网段之上提供这种功能，它可以检测到路由器丢弃的包，然后自动产生一个重新传输请求。

传输层的另一项重要功能就是将乱序收到的数据包重新排序，数据包乱序有很多原因。例如，这些包可能通过网络的路径不同，或者有些在传输过程中被破坏。不管是什么情况，传输层应该可以识别出最初的包顺序，并且在将这些包的内容传递给会话层之前要将它们恢复成发送时的顺序。传输层在发送主机系统上对将要发送的数据进行分段，在接收主机系统上完成数据段到数据流的重组。传输层和会话层之间的边界可以认为是应用协议和数据流协议之间的分界。

会话层

OSI的第五层是会话层，相对而言，这一层没有太大用处，很多协议都将这一层的功能与传输层捆绑在一起。

OSI会话层的功能主要是用于管理两个计算机系统连接间的通信流。通信流称为会话，它决定了通信是单工还是双工。它也保证了接收一个新请求一定在另一个请求完成之后，会话层建立、管理和终止两个通信主机之间的会话，会话层为表示层提供服务，它也同步两台主机表示层之间的对话以及管理它们的数据交换。

表示层

表示层负责管理数据编码方式，不是所有计算机系统都使用相同的数据编码方式，表示层的职责就是在可能不兼容的数据编码方式，例如在ASCII和EBCDIC之间，提供翻译。表示层可以用在浮点格式间的调整转换并提供加密解密服务。因此表示层提供加密、翻译、压缩、转换等功能。

应用层

OSI 参考模型的最顶层是应用层，尽管它称为应用层，但它并不包含任何用户应用。相反，它只在那些应用和网络服务间提供接口。

这一层可以看成是初始化通信会话的起因。例如，邮件客户可能会产生一个从邮件服务器检索新消息的请求，客户端应用自动向与之相关的第七层协议发出请求，并产生通信会话，以获取所需要的文件。

TCP/IP参考模型

TCP/IP模型



进程/应用层

应用层协议提供远程访问和资源共享。读者熟悉的应用包括Telnet、FTP、SMTP、HTTP，很多其他应用程序驻留并运行在此层，并且依赖于底层的功能。相似的，需要在IP网络上要求通信的任何应用（包括用户自己开发的和在商店买来的软件）也在模型的这一层中描述。

传输层/运输层

IP的传输层/运输层大致对应于OSI参考模型的会话层和传输层。这一层支持的功能包括：为了在网络中传输对应用数据进行分段，执行数学检查来保证所收数据的完整性，为多个应用同时传输数据多路复用数据流（传输和接收）。这意味着主机到主机层能识别特殊应用，对乱序收到的数据进行重新排序。

当前的主机到主机层包括两个协议实体：传输控制协议（TCP）和用户数据报协议（UDP）。另一个协议正在定义中，这个协议针对于不断增长的面向事务的需要。这个协议称为事务/事务控制协议（Transaction/Transmission Control Protocol，T/TCP）。

网际层

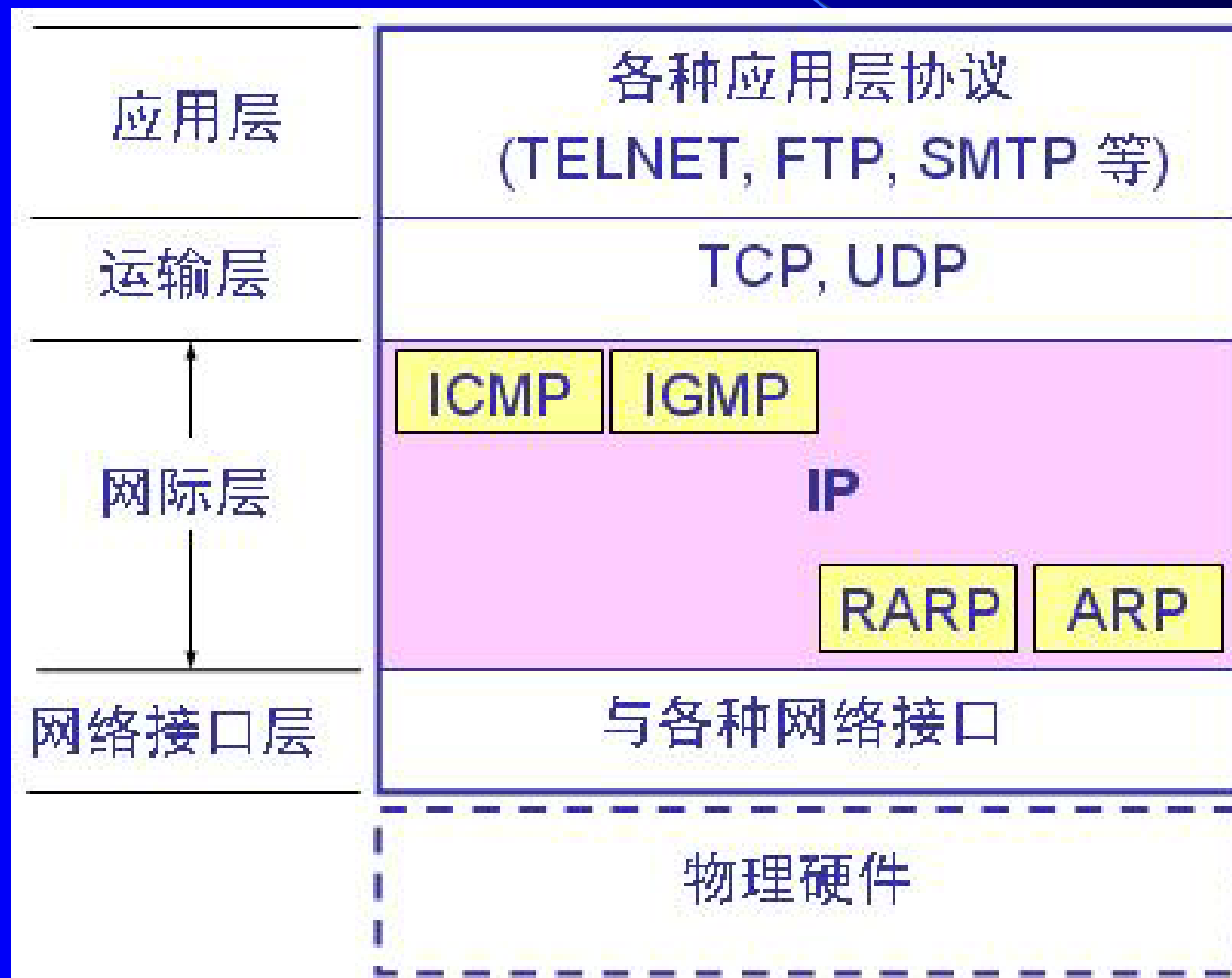
IPv4的网际层由在两个主机之间通信所必须的协议和过程组成。这意味着数据报文必须是可路由的。网际层（IP）负责数据报文路由。网际层也必须支持其他的路由管理功能，它必须提供第二层地址到第三层地址的解析及反向解析。

网际层必须支持路由和路由管理功能。这些功能由外部对等协议提供，称这些协议为路由协议。这些协议包括内部网关协议（IGP）、外部网关协议（EGP），它们标识为对等的这一点很重要，因为它们驻留在网络层中，但却不是IP协议组件与生俱来的部分。实际上，许多路由协议能够在多路由协议地址结构中发现、计算路由。用于其他地址结构的路由协议例子包括IPX和AppleTalk。

网络接口层

网络接口层包括用于物理连接、传输的所有功能。OSI模型把这一层功能分为两层：物理层和数据链路层。由于在同名协议之后创建，TCP/IP参考模型把两层合在一起，是因为各种IP协议中止于网际层。IP假设所有底层功能由局域网或串口连接提供。

协议组件



协议组件

- IP：网际层协议。
- TCP：可靠的主机到主机层协议。
- UDP：尽力转发的主机到主机层协议。
- ICMP：在IP网络内为控制、测试、管理功能而设计的多层协议。

OSI与TCP体系结构的比较

- 显而易见的差异是两种模型的层数不一样，OSI模型有7层，而TCP/IP模型只有4层。两者都有网络层、传输层和应用层，但其他层是不同的。在OSI的七层中，数据链路层不是TCP/IP的一部分，但它是TCP/IP赖以生存的各种通信网络和TCP/IP之间接口。这些通信网包括各种局域网，如以太网、令牌网等，以及多种广域网，如ARPAnet、MILNET和X.25公用数据网等。而IP层内里提供了专门的功能，解决了与各种物理地址的转换。

OSI与TCP体系结构的比较

- TCP/IP参考模型并不十分清晰地区分服务、接口这些概念。想比TCP/IP参考模型,OSI模型中的协议具有更好的隐蔽性并更容易被替换。

OSI与TCP体系结构的比较

- OSI参考模型是先于其协议设计的。这意味着 OSI参考模型不是基于某个特定的协议集而设计的，因而它更具有通用性。但另一方面，也意味着OSI模型的协议实现方面存在某些不足。而TCP/IP参考模型下好相反。先有协议，模型只是现有协议的描述，因而协议与模型非常吻合。但是，TCP/IP参考模型缺乏通用性，不适合描述其他协议栈。

OSI与TCP体系结构的比较

- 在服务类型方面，OSI参考模型的网络层提供面向连接和无连接两种服务，而传输层只提供面向连接服务。TCP/IP参考模型在网络层只提供无连接服务，但在传输层提供两种服务。

OSI与TCP体系结构的比较

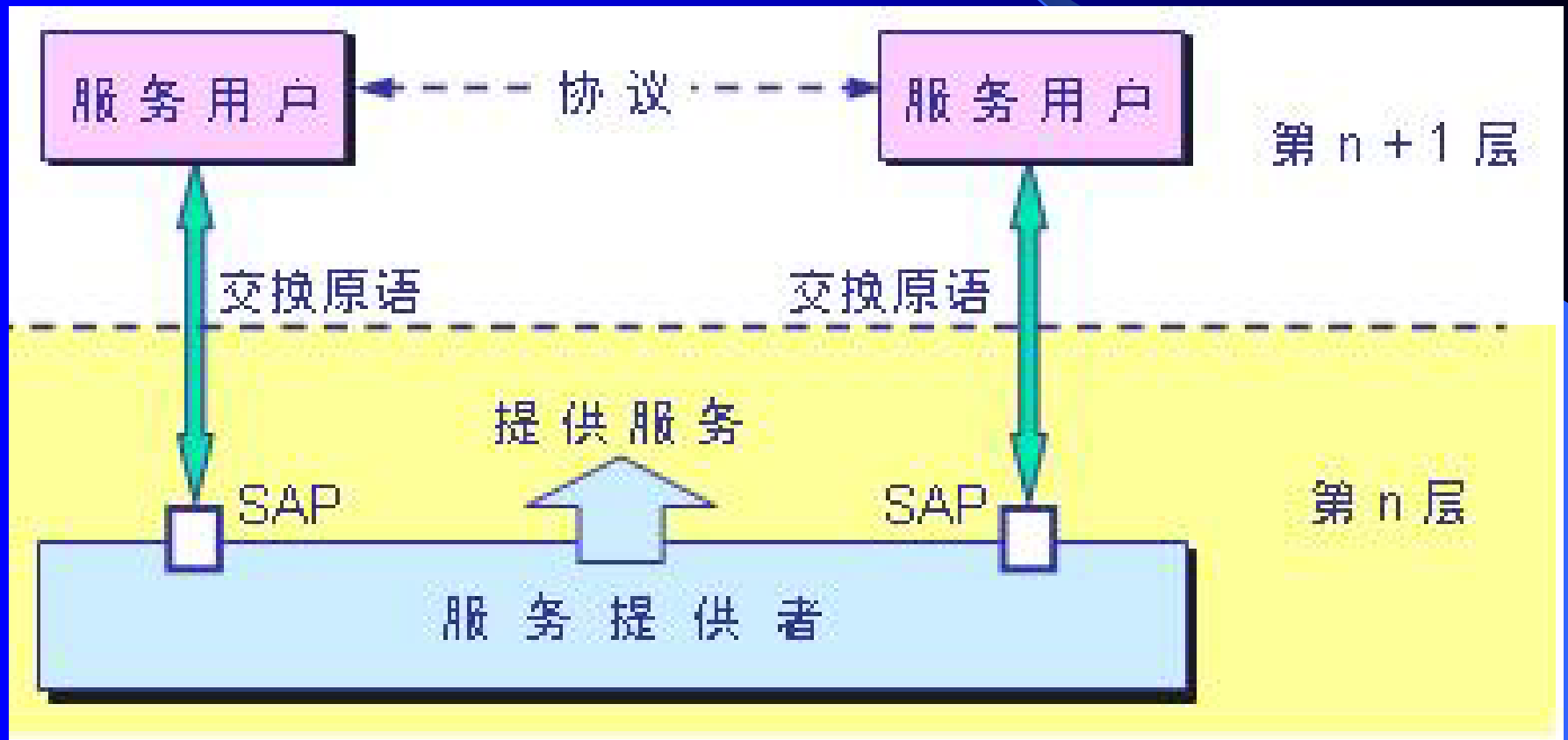
- 使用OSI模型（去掉会话层和表示层）可以很好地讨论计算机网络，但是由于各种原因，OSI协议并未流行。TCP/IP模型正好相反，其模型本身实际上并不存在，只是对现存协议的一个归纳和总结，但TCP/IP协议却被广泛使用。

OSI参考模型和TCP/IP参考模型 比较

OSI参考模型 层描述	OSI 层号	TCP/IP层 描述
应用层	7	进程/应用层
表示层	6	
会话层	5	
传输层	4	主机到主机层
网络层	3	网际层
数据链路层	2	网络访问层
物理层	1	

数据的封装、解封与传输

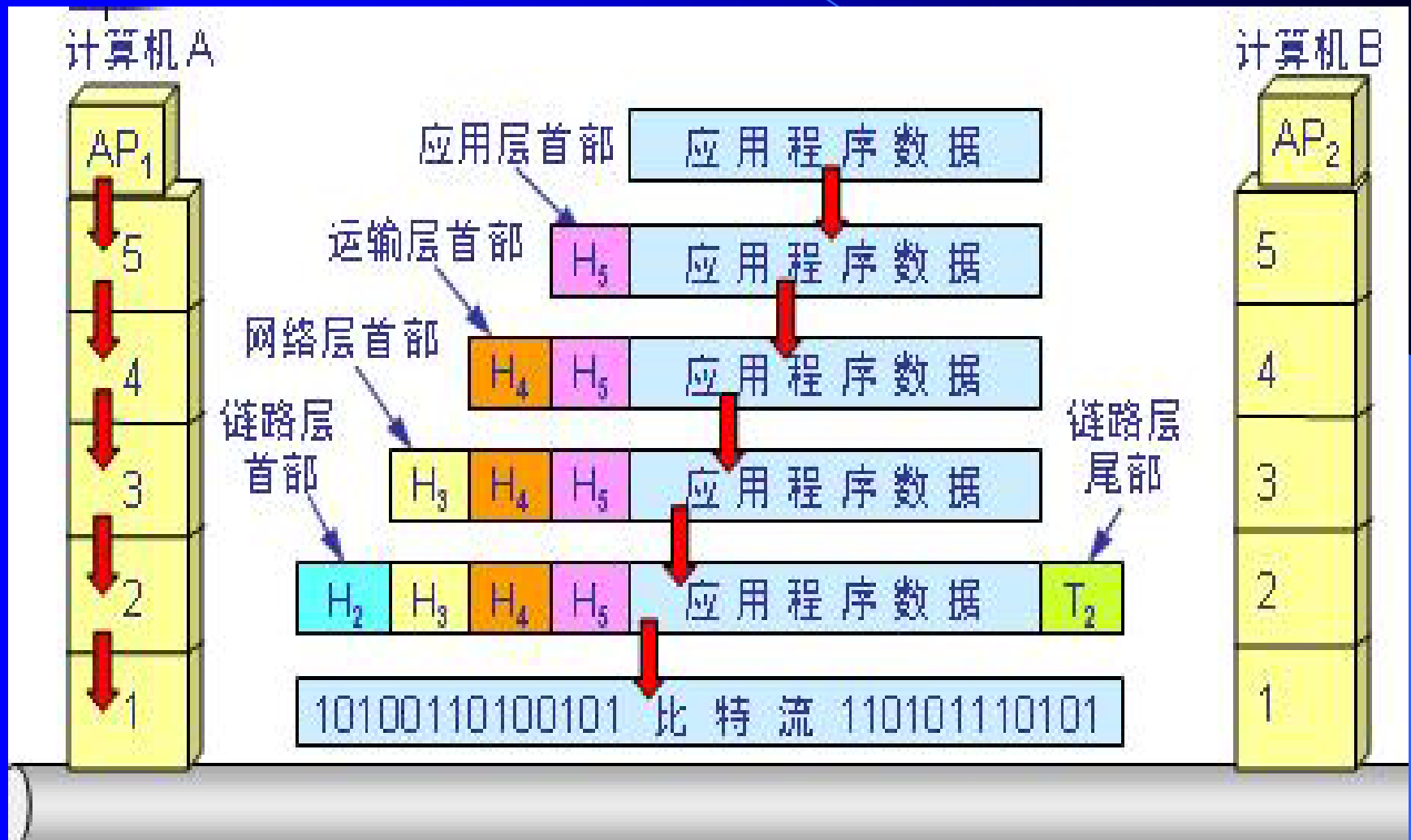
数据的封装解封原理



数据的封装解封原理

- 垂直方向的结构层次是当今普遍认可的数据处理的功能流程。每一层都有与其相邻层的接口。为了通信，两个系统必须在各层之间传递数据、指令、地址等信息，本层的服务用户只能看见服务而无法看见下面的协议，下面的协议对上面的服务用户是透明的，协议是“水平的”，即协议是控制对等实体之间通信的规则，服务是“垂直的”，即服务是由下层向上层通过层间接口提供的，同一系统相邻两层的实体进行交互的地方，称为服务访问点 SAP (Service Access Point)。

数据的封装解封原理



数据的封装解封原理

- 虽然通信流程垂直通过各层次，但每一层都在逻辑上能够直接与远程计算机系统的相应层直接通信。为创建这种层次间的逻辑连接，引发通信机器的每一层协议都要在数据报文前增加报文头。该报文头只能被其他计算机的相应层识别和使用。接收端机器的协议层删去报文头，每一层都删去该层负责的报文头，最后将数据传向它的应用，

IP地址

IP地址介绍

- 地址实际上是一种标识符，在计算机网络中用于标识系统中的某个对象。以太网地址（MAC地址）并不含有位置信息（在这个48比特的数字中没有站点的位置信息），它只是唯一地标识一个对象以区别不同网络站点，对于规模不大的网络环境来说这已经足够了，它能够帮助我们找到目的站点，起到了确定位置的作用。但是在一个规模较大的环境中如果地址中没有位置信息就几乎无法定位站点。试想，在因特网中通过MAC地址寻找目标机器，势必要逐一对比网卡的MAC地址，面对如此大的主机数这几乎是一件无法完成的工作。为了在大网中方便地定位主机，研究人员使用具有结构的地址标识符，这种地址不仅标识主机，还要指出主机所在的位置。IP地址就是当今在因特网中采用的这种所谓结构化的（也称为层次化）地址。

IP地址和MAC地址的比较

- 这两种地址是并存的，IP地址并不能代替MAC地址，前者是在大网中为了方便定位主机所采用的方式，如果网络规模不大，完全可以不使用IP地址，因此，无论什么网络环境物理地址都是要使用的，因为物理地址对应于网卡的接口，只有找到它才算真正到达了目的地。而IP地址是为了方便寻址人为划分的地址格式（注意，管理人员是不能够根据网络设计的要求修改物理地址的），因此IP地址也被称为逻辑地址，又因为这种结构化地址是在OSI的第三层定义的，也被称为三层地址，相应地，物理地址被称为二层地址。IP地址是一种通用格式，无论其下一层的物理网络地址是什么类型，都可以被统一到一致的IP地址形式上。因此IP地址屏蔽了下层物理地址的差异。

IP地址结构

- IP地址是一种层次型地址，它由两个部分组成：网络号和主机号。其中网络号表示互联网网络中的某个网络，而同一网络中有许多主机，由主机号区分。因此给出一台主机的IP地址，就可以知道它所处的网络，就是前面所说的位置信息。这与我们到某个单位去找人非常相似，通常先寻找他所在的部门，再到这个部门中找到这个员工。网络号对应于部门，主机号对应员工本人。这种方式定位一个个体是非常方便和迅速的。

IP地址结构

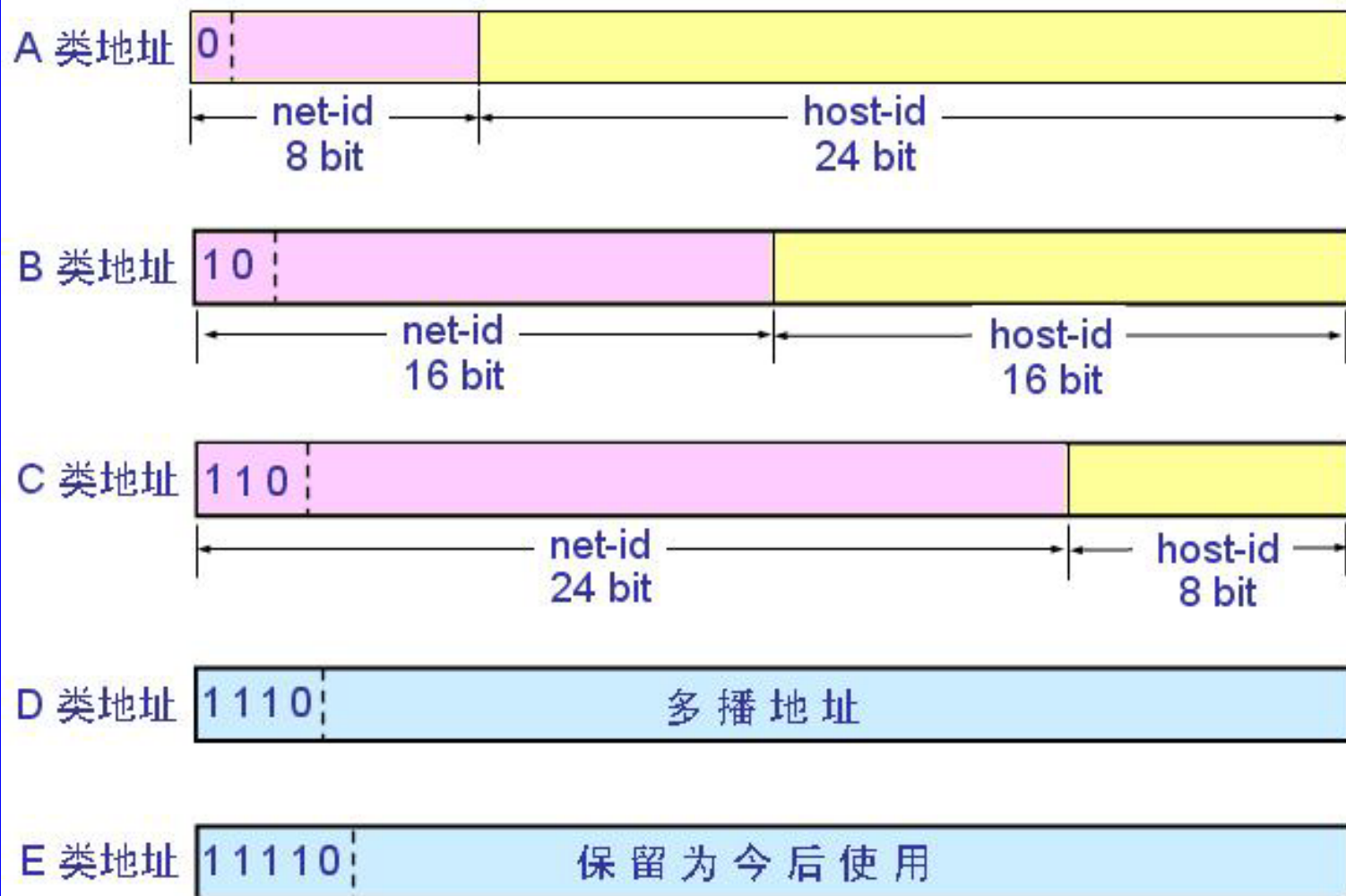
Net ID

Host ID

IP地址结构

- IP地址由一个32位长的二进制数字表示。为了方便表达，这32位又分为4个8比特数,由于我们日常习惯使用十进制表示数字，因此以十进制来表示每个8比特数，它的范围是 0~255。这4个十进制数用小圆点隔开，称为点分十进制表示法，例：
- 10000001 00001011 00000011 00011111
- 129 11 3 31
- IP = 129 . 11 . 3 . 31

IP地址分类



IP地址分类

- A类地址的最高位为0，它用前8比特表示网络号，后24个比特表示主机号，A类网络的网络数相对较少，但在一个网络中可容纳很多主机，每个网络最多可容纳 $(2^{24} - 2)$ 台主机，该类地址适用于大型网，它的首字节取值范围0 - 127；
- B类地址的最高两位为10（以二进制表示），它用前16比特表示网络号，后16个比特表示主机号，此类网络类型的网络数相对较多，每个网络最多可容纳 $(2^{16} - 2)$ 台主机，该类地址适用于中等规模的网络，它的首字节取值范围128 - 191；
- C类地址的最高两位为110（以二进制表示），它用前24比特表示网络号，后8个比特表示主机号，它的网络数量很大，每个网络最多可容纳 $(2^8 - 2)$ 台主机，该类地址适用于小型网，它的首字节取值范围192 - 223；

IP地址使用规则

- 网络号全“0”的地址保留,不能作为标识网络使用。
- 主机号全“0”的地址保留,作为表示网络地址。例如172.16.0.0,表示一个B类网络。
- 网络号全“1”、主机号全“0”的地址代表网络的子网掩码。子网掩码将在下一小节中论述。
- 主机号全1的地址为广播地址,称为直接广播或是有限广播。如172.16.255.255,表示对172.16.0.0里的所有主机进行广播。这类广播地址可以跨越路由器。此外,还有两个特殊的地址:

IP地址的管理

- IP地址要惟一，否则会产生冲突。因此IP地址需要有一个授权机构统一管理，管理IP地址的机构就是InterNic，它负载管理和分配IP地址。如果某台机器要联入因特网就要向它申请IP地址，这些地址也称为注册地址，一旦在InterNic注册后，这个地址就不能再被其他设备使用。但如果是隔离在因特网之外的网络（指未连接到Internet的网络）就没有必要向InterNic申请地址，实际上相互隔离的网络之间没有必要使地址保持惟一，因为它们之间互不通信。所以，在这些隔离的网络中分配IP地址时可以使用私有地址（private address）。所谓私有地址是指InterNic保留给隔离网络中使用的地址，这些地址不能在因特网上使用。比如在企业内部联网时就会用到私有地址，前提是这些主机不访问因特网。

私有地址的范围

10.0.0.0 ~ 10.255.255

172.16.0.0 ~ 172.31.255.255

192.168.0.0 ~ 192.168.255.255

IP地址的子网划分

子网划分方法

原来的IP地址分为网络号和主机号两个部分，划分子网后整个IP地址就分成三个部分：

- 主网络号，它对应于标准A、B、C类的网络号部分；
- 借用主机位而作为网络号的部分，这个被称作子网号；
- 还有一部分就是剩余的主机号。

可变长度的子网掩码

子网掩码的意义

机器在计算一个IP地址的网络号部分时采用IP地址与掩码地址对应位相“与”的算法。首先把IP地址和子网掩码换算成二进制，然后位对位做“与”运算，最后得到IP地址中的网络地址。“与”运算规则如下：

- $1 \text{ AND } 1 = 1$
- $0 \text{ AND } 0 = 0$
- $0 \text{ AND } 1 = 0$

可变长子网掩码VLSM

- VLSM (Variable Length Subnet Mask, 可变长子网掩码), 这是一种产生不同大小子网的网络分配机制, 是指对同一个主网络在不同的位置使用不同的子网掩码。VLSM将允许给点到点的链路分配子网掩码255.255.255.252, 而给Ethernet网络分配255.255.255.0。VLSM技术对高效分配IP地址 (较少浪费) 以及减少路由表大小都起到非常重要的作用。但是需要注意的是使用VLSM时, 所采用的路由协议必须能够支持它, 这些路由协议包括RIP2, OSPF和BGP等。

无类别域间路由（CIDR）

- CIDR（Classless Inter-Domain Routing，无类别域间路由）基本思想是取消地址的分类结构，取而代之的是允许以可变长分界的方式分配网络数。它支持路由聚合，可限制Internet主干路由器中必要路由信息的增长。“无类别”的意思是现在的选路决策是基于整个32位IP地址的掩码操作，而不管其IP地址是A类、B类或是C类，都没有什么区别。

无类别域间路由（CIDR）

- 我们在做IP规划的时候，刻意将子网作成 2^n 模式，目的便是为了尽量支持路由归并，以减少路由表规模， 2^n 子网规划模式也是为了保证IP地址划分的规范性，此外，为进行选路要对多个IP地址进行归并时，这些IP地址必须具有相同的高位地址比特。

无类别域间路由（CIDR）

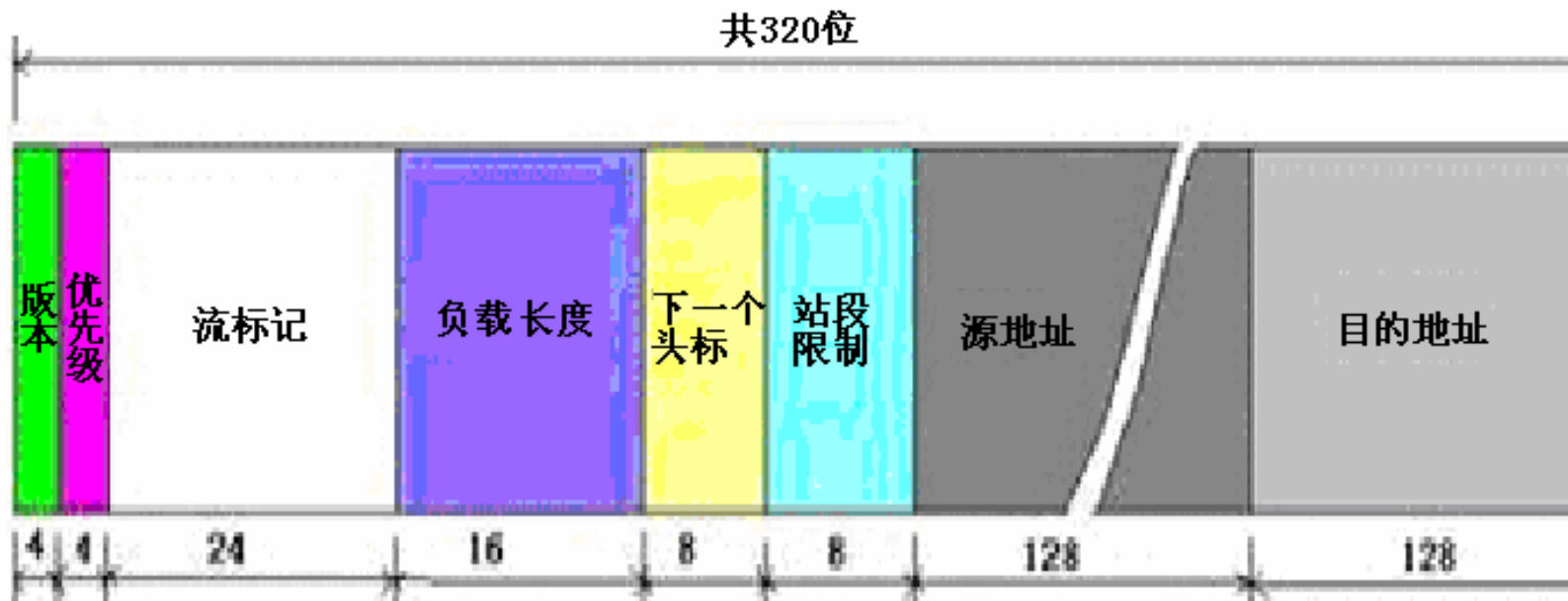
- 路由表和选路算法必须扩展成根据32位IP地址和32位掩码做出选路决策的算法，必须扩展选路协议使其除了32位地址外，还要有32位掩码。CIDR技术用于帮助减缓IP地址耗尽和路由表增大的问题，这种技术使得多个C类地址块可以被组合或聚合在一起以生成更大的无类别IP地址集（也就是说，我们可以用一个CIDR的聚合体来表示一组C类地址）。

IPv6简述

IPv6 地址表示方法

- 在新的IP标准IPv6中，IP地址的表示方法不是这样的了。IPv6的地址在表示和书写时，用冒号将128位分割成8个16位的段，这里的128位表示在一个IPv6地址中包括128个二进制数。每个段包括4位的16进制数字，例如：
1080:0000:0000:0000:0008:0800:200C:123A。

IPv6数据报格式



优先级

在IPv6优先级域中首先要区分二大业务量（ traffic ）：

- 受拥塞控制（ congestion-controlled ）业务量；
- 不受拥塞控制的（ noncongestion-controlled ）业务量。

流标识

- 一个流由其源地地址，目的地地址和流序号来命名。在IPv6规范中规定“流”是指从某个源点向（单目或组播的）信宿发送的分组群中，源点要求中间路由器作特殊处理的那些分组。也就是说，流是指源点、信宿和流标记三者分别相同的分组的集合。任何的流标记都不得在此路由器中保持6秒以上。此路由器在6秒之后必须删除高速缓存（cache）中登录项，当该流的下一个分组出现时，此登录项被重新学习。并非所有的分组都属于流。实际上从IPv4向IPv6的过渡期间大部分的分组不属于特定的流。例如，SMTP、FTP以及WWW浏览器等传统的应用均可生成分组。这些程序原本是为了IPv4而设计的，在过渡期为使IPv4地址和IPv6地址都能处理而进行了改进，但不能处理在IPv4中不存在的流。在这分组中应置入由24位0组成的空流标记。

有效载荷长度

- 有效载荷长度域指示IP基本头标以后的IP数据报剩余部分的长度，单位是字节。此域占16位，因而IP数据报通常应在65535字节以内。但如果使用Hop By Hop选项扩展头标的特大净荷选项，就能传送更大的数据报。利用此选项时净荷长度置0。

下一个头标

- 下一个头标用来标识数据报中的基本IP头标的下一个头标。在此头标中，指示选项的IP头标和上层协议。表6列出了主要的下一个头标值。其中一些值是用来标识扩展头标的。

站段限制

- 站段限制决定了能够将分组传送到多远。主机在生成数据报时，在站段限制域中设置某一初值，然后将数据报送到网上的路由器。各路由器从该值起逐次减1。如数据报到达信宿之前其站段限制变为0，该数据报就被抛弃掉。使用站段限制有二个目的。第一是防止寻路发生闭环（loop）。因IP不能订正路由器的错误信息，故无法使此数据报到达信宿。在IP中可以利用站段限制来防止数据报陷入寻路的死循环中。站段限制还用于其他目的。主机利用它在网内进行检索。PC要向其中一个服务器发送数据报，无论发向哪个都行。为了减轻网络负荷，PC希望搜索到离它最近的服务器。

源地址和目的地址

- 基本IP头标中最后2个域是信源地址和目的地址。它们各占128位。在此域中置入数据报最初的源地址和最后的目的地地址。

IP扩展头标

- 逐项选项头（Hop-by-Hop Option Header）：该字段定义了途经路由器所需检验的信息。
- 目的选项头：含目的站点处理的可选信息。
- 路由选项头(Routing)：提供了到达目的地所必须经过的中间路由器。
- 分段(Fragmentation)头：IPv6对分段的处理类似于IPv4，该字段包括数据报标识符、段号以及是否终止标识符。
- 认证(Authentication)头：该字段保证了目的端对源端的身份验证。
- 加载安全负载(Security encrypted payload)头：该字段对负载进行加密，以防止数据在传输过程中发生信息泄露。

域名概述

IPv4的域名

- 由于IP地址全是数字，为了便于用户记忆，Internet上引进了域名服务系统DNS（Domain Name System）。当您键入某个域名的时候，这个信息首先到达提供此域名解析的服务器上，再将此域名解析为相应网站的IP地址。完成这一任务的过程就称为域名解析。域名解析的过程是：当一台机器a向其域名服务器A发出域名解析请求时，如果A可以解析，则将解析结果发给a，否则，A将向其上级域名服务器B发出解析请求，如果B能解析，则将解析结果发给a，如果B无法解析，则将请求发给再上一级域名服务器C……如此下去，直至解析到为止。Internet域名系统是一个树型结构。DNS将整个Internet划分为多个顶级域，并为每个顶级域规定了通用的顶级域名。网络信息中心NIC将顶级域的管理权授予指定的管理机构，各个管理机构再为它们所管理的域分配二级域名，并将二级域名的管理权授予其下属的管理机构。如此层层细分，就形成了Internet有层次的域名结构。

IPv4的域名

- Internet主机域名的排列原则是低层的子域名在前面，而它们所属的高层域名在后面。Internet主机域名的一般格式为：
- 四级域名.三级域名.二级域名.顶级域名
- 例如：主机域名为 ssky.cuit.edu.cn表示是成都信息工程学院“小天在线”的主机，主机域名为 www.microsoft.com表示是美国微软公司的WWW服务器，美国的主机名可以省略国别代码。

IPv4的域名

- 以机构区分的二级域名原来有7个：com（商业机构）、net（网络服务机构）、gov（政府机构）、mil（军事机构）、org（非盈利性组织）、edu（教育部门）、int（国际机构）。1997年又新增7个最高级标准域名：firm（企业和公司）、store（商业企业）、web（从事与WEB相关业务的实体）、arts（从事文化娱乐的实体）、REC（从事休闲娱乐业的实体）、info（从事信息服务业的实体）、nom（从事个人活动的个体、发布个人信息）。这些域名的注册服务由多家机构承担，CNNIC也有幸成为注册机构之一；按照ISO-3166标准制定的国家域名，一般由各国的NIC(Network Information Center，网络信息中心)负责运行。

IPv4的域名

- 以地域区分的顶级域名有：AQ（南极洲）、AR（阿根廷）、AT（奥地利）、AU（澳大利亚）、BE（比利时）、BR（巴西）、CA（加拿大）、CH（瑞士）、CN（中国）、DE（德国）、DK（丹麦）、ES（西班牙）、FI（芬兰）、FR（法国）、GR（希腊）、IE（爱尔兰）、IL（以色列）、IN（印度）、IS（冰岛）、IT（意大利）、JP（日本）、KR（韩国）、MY（马来西亚）、NL（荷兰）、NO（挪威）、NZ（新西兰）、PT（葡萄牙）、RU（俄罗斯）、SE（瑞典）、SG（新加坡）、TH（泰国）、TW（中国台湾）、UK或GB（英国）、US（美国）（一般可省略）等。

IPv4的域名

- 中国域名体系分为类别域名和行政区域域名两套。类别域名有六个，分别依照申请机构的性质依次分为：AC - 科研机构；COM - 工、商、金融等专业；EDU - 教育机构；GOV - 政府部门；NET - 互联网络、接入网络的信息中心和运行中心；ORG - 各种非盈利性的组织。行政区域域名是按照我国的各个行政区划分而成的，其划分标准依照国家技术监督局发布的国家标准而定，包括“行政区域名”34个，适用于我国的各省、自治区、直辖市。

IPv6的域名系统及解析原理

IPv6与域名系统

- 可聚集全局单播地址是目前主要应用的IPv6地址，因IPv6可聚集全局单播地址是在全局范围内使用的地址，必须进行层次划分及地址聚集。下面就以IPv6 DNS系统对这类地址的解析过程来介绍IPv6 DNS系统的解析原理。
- IPv6全局单播地址的分配方式如下：顶级地址聚集机构TLA（即大的ISP或地址管理机构）获得大块地址，负责给次级地址聚集机构NLA（中小规模ISP）分配地址，NLA给站点级地址聚集机构SLA（子网）和网络用户分配地址。IPv6地址的层次性在DNS中通过地址链技术可以得到很好的支持。

正向解析

- 从以上介绍已经知道，IPv4的地址正向解析的资源记录是“A”，而IPv6地址的正向解析目前有两种资源记录，即“AAAA”和“A6”记录。其中“AAAA”较早提出，它是对IPv4协议“A”记录的简单扩展，由于IP地址由32位扩展到128位，扩大了4倍，所以资源记录由“A”扩大成4个“A”。但“AAAA”用来表示域名和IPv6地址的对应关系，并不支持地址的层次性。
- AAAA资源记录类型用来将一个合法域名解析为IPv6地址，与IPv4所用的A资源记录类型相兼容。之所以给这新资源记录类型取名为AAAA，是因为128位的IPv6地址正好是32位IPv4地址的四倍，下面是一条AAAA资源记录实例：
- host1.microsoft.com IN AAAA
FEC0::2AA:FF:FE3F:2A1C

反向解析

- IPv6反向解析的记录和IPv4一样，是“PTR”，但地址表示形式有两种。一种是用“.”分隔的半字节16进制数字格式（Nibble Format），低位地址在前，高位地址在后，域后缀是“IP6.INT.”。另一种是二进制串（Bit-string）格式，以“\”开头，16进制地址（无分隔符，高位在前，低位在后）居中，地址后加“]”，域后缀是“IP6.ARPA.”。半字节16进制数字格式与“AAAA”对应，是对IPv4的简单扩展。二进制串格式与“A6”记录对应，地址也象“A6”一样，可以分成多级地址链表示，每一级的授权用“DNAME”记录。和“A6”一样，二进制串格式也支持地址层次特性。

IPv6中的即插即用与DNS

- IPv6协议支持地址自动配置，这是一种即插即用的机制，在没有任何人工干预的情况下，IPv6网络接口可以获得链路局部地址、站点局部地址和全局地址等，并且可以防止地址重复。IPv6支持“无状态地址自动配置”和“有状态地址自动配置”两种方式。

IPv6中的即插即用与DNS

- 在无状态地址自动配置方式下，需要配置地址的网络接口先使用邻居发现机制获得一个链路本地地址。网络接口得到这个链路本地地址之后，再接受路由器宣告的地址前缀，结合接口标识得到一个全局地址。而有状态地址自动配置的方式，与IPv4一样的DHCP（动态主机配置协议），需要一个DHCP服务器，通过客户机/服务器模式从DHCP服务器处得到地址配置的信息。

IPv6中的即插即用与DNS

- IPv6节点通过地址自动配置得到IPv6地址和网关地址。但是，地址自动配置中不包括DNS服务器的自动配置。如何自动发现提供解析服务的DNS服务器也是一个需要解决的问题。DNS服务器自动发现的解决方法可以分为“无状态”和“有状态”两类。

IPv6中的即插即用与DNS

- 在无状态的方式下，需要为子网内部的DNS服务器配置站点范围内的任播地址。要进行自动配置的节点以该任播地址为目的地址发送服务器发现请求，询问DNS服务器地址、域名和搜索路径等DNS信息。这个请求到达距离最近的DNS服务器，服务器根据请求，回答DNS服务器单播地址、域名和搜索路径等DNS信息。节点根据服务器的应答配置本机DNS信息，以后的DNS请求就直接用单播地址发送给DNS服务器。

IPv6中的即插即用与DNS

- 另外，也可以不用站点范围内的任播地址，而采用站点范围内的多播地址或链路多播地址等。还可以一直用站点范围内的任播地址作为DNS服务器的地址，所有的DNS解析请求都发送给这个任播地址。距离最近的DNS服务器负责解析这个请求，得到解析结果后把结果返回单播地址、域名和搜索路径等DNS信息告诉节点。从网络扩展性，安全性，实用性等多方面综合考虑，第一种采用站点范围内的任播地址作为DNS服务器地址的方式相对较好。

IPv6中的即插即用与DNS

- 在有状态的DNS服务器发现方式下，是通过类似DHCP这样的服务器把DNS服务器地址、域名和搜索路径等DNS信息告诉节点。当然，这样做需要额外的服务器。

IPv6过渡阶段的DNS

- 在IPv4到IPv6的过渡过程中，作为Internet基础架构的DNS服务也要支持这种网络协议的升级和转换，当然这也要有一个过渡方法，而不是一下子全面改成IPv6的DNS系统。从上面的介绍可以知道，IPv4和IPv6的DNS记录格式等方面有所不同，为了实现IPv4网络和IPv6网络之间的DNS查询和响应，可以采用应用层网关DNS-ALG结合NAT - PT的方法，在IPv4和IPv6网络之间起到一个翻译的作用。例如，IPv4的地址域名映射使用“A”记录，而IPv6使用“AAAA”或“A6”记录。那么，IPv4的节点发送到IPv6网络的DNS查询请求是“A”记录，DNS-ALG就把“A”改写成“AAAA”，并发送给IPv6网络中的DNS服务器。当服务器的回答到达DNS-ALG时，DNS-ALG修改回答，把“AAAA”改为“A”，把IPv6地址改成DNS-ALG地址池中的IPv4转换地址，把这个IPv4转换地址和IPv6地址之间的映射关系通知NAT - PT，并把这个IPv4转换地址作为解析结果返回IPv4主机。IPv4主机就以这个IPv4转换地址作为目的地址与实际的IPv6主机通过NAT - PT通信。

IPv6过渡阶段的DNS

- 对于采用双协议栈方式的过渡方法，在DNS服务器中同时存在“A”记录和“AAAA”（或“A6”）记录。由于节点既可以处理IPv4协议，也可以处理IPv6协议，因此无需类似DNS ALG的转换设备。无论DNS服务器回答“A”记录还是“AAAA”记录，都可以进行通信。

IPv6过渡阶段的DNS

- 随着Internet技术的不断发展，IPv6也已离我们越来越近了。DNS作为IPv4时代的网络基础服务，对Internet起着重要的作用。在即将到来的IPv6时代，新的协议和功能要求DNS不再是仅提供传统意义上的简单资源定位，而是一方面提供类似IPv4 DNS的基础功能，另一方面结合IPv6的新特性，和其它协议有机的结合在一起，提供新的功能，使网络的配置、维护、使用变的更加简单、更加方便，让用户感受到新技术带来的新体验。

数据线的分类与制作

双绞线

- 双绞线是将一对或一对以上的双绞线封装在一个绝缘外套中而形成的一种传输介质，是目前局域网最常用的一种布线材料。从图中我们可以看出双绞线中的每一对都是由两根绝缘铜导线相互缠绕而成的，这是为了降低信号的干扰程度而采取的措施。双绞线一般用于星型网络的布线连接，两端安装有RJ-45头（接口），连接网卡与集线器，最大网线长度为100米，如果要加大网络的范围，在两段双绞线之间可安装中继器，最多可安装4个中继器，如安装4个中继器连5个网段，最大传输范围可达500米。

双绞线

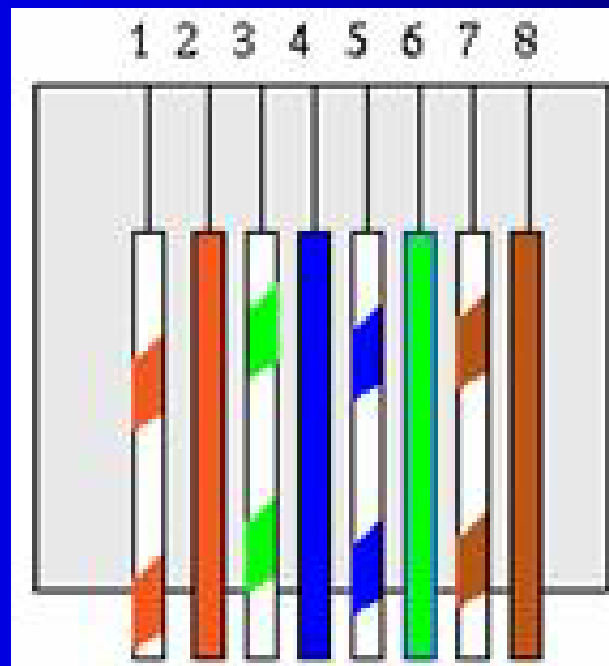


双绞线的分类

- 双绞线分为非屏蔽双绞线（UTP）和屏蔽双绞线（STP）两大类，局域网中非屏蔽双绞线分为3类、4类、5类和超5类4种，屏蔽双绞线分为3类和5类两种。

双绞线线序和RJ-45接口引脚序号

- 双绞线由8根铜导线组成，这8根铜导线的顺序分别橙白—1，橙—2，绿白—3，蓝—4，蓝白—5，绿—6，棕白—7，棕—8，如图1-17所示。

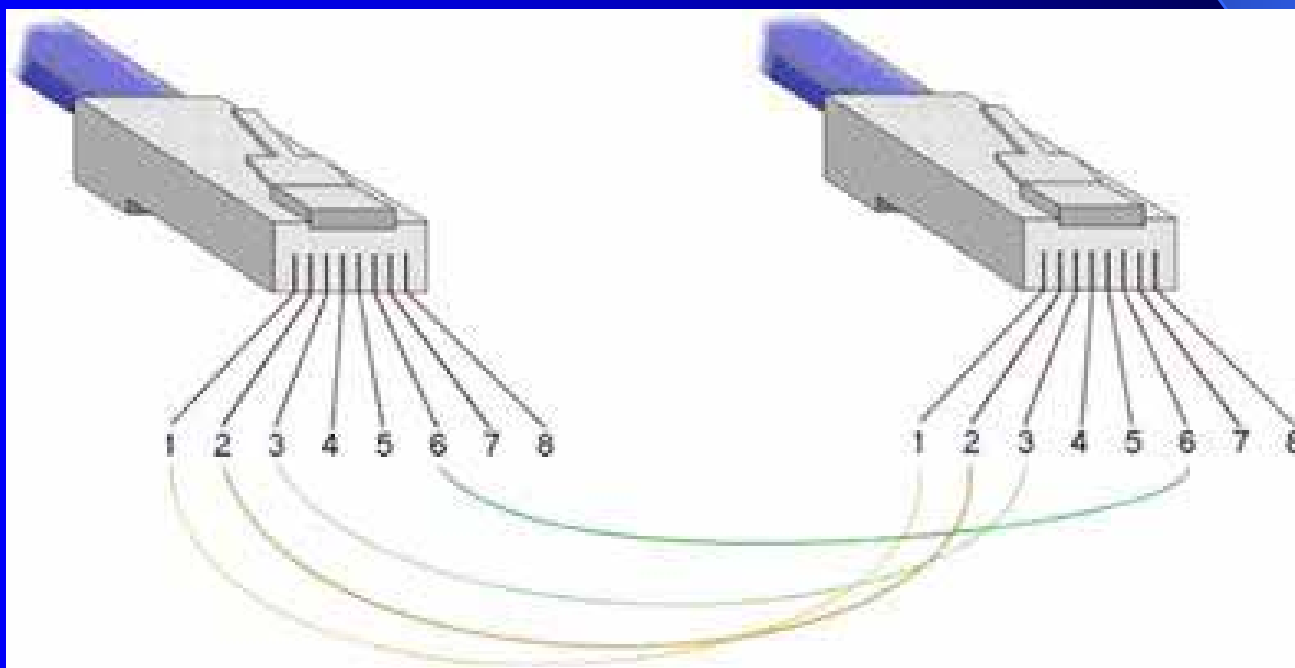


双绞线的连接方式

- 在组建一个网络时，使用双绞线连接网卡和集线器的方式共有3种：网卡到集线器、集线器到集线器和网卡到网卡的连接。3种不同的连接方式下，双绞线两端的RJ-45接口中线的排列也不一样，下面以最常用的5类非屏蔽双绞线为例，分别介绍一下双绞线的3种连接方式。

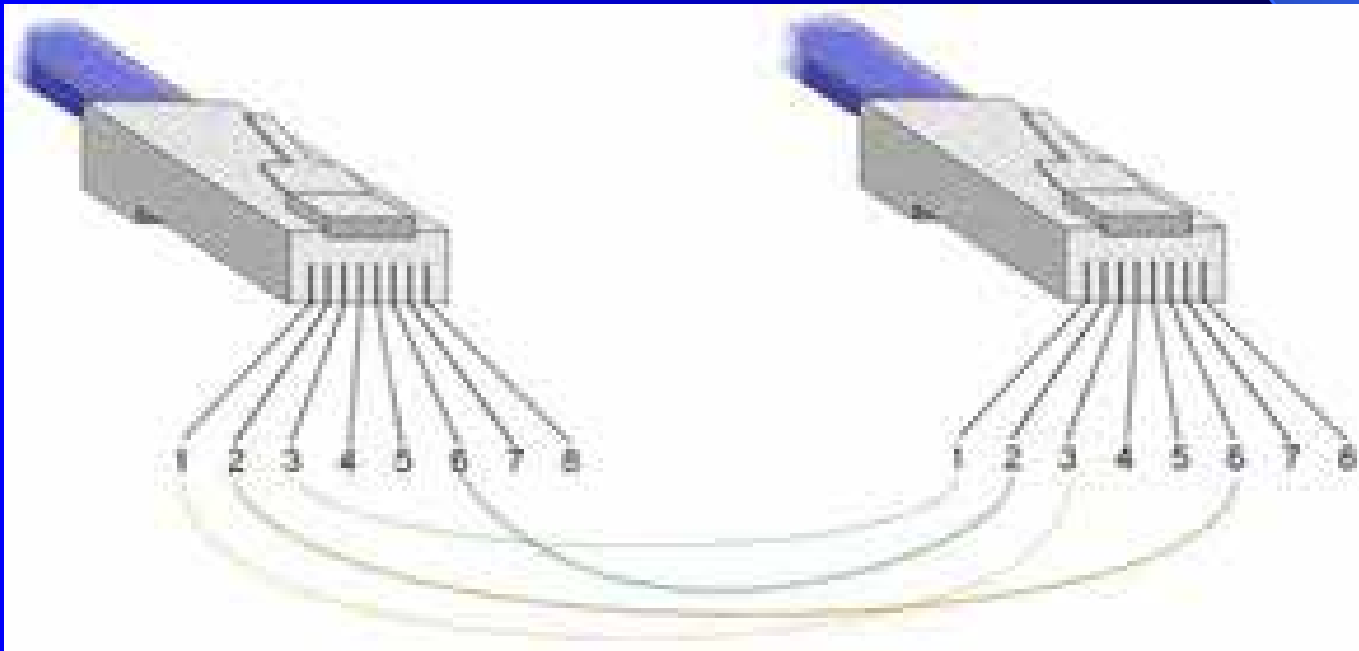
网卡和集线器

- 网卡和集线器的连接，只需要把双绞线与接口引脚对应接入即可。



网卡到网卡连接

- 在某些特定情况下，需要把两台计算机通过网卡直连。此时双绞线需要错位，其顺序与RJ-45接口引脚顺序连接成如图所示。

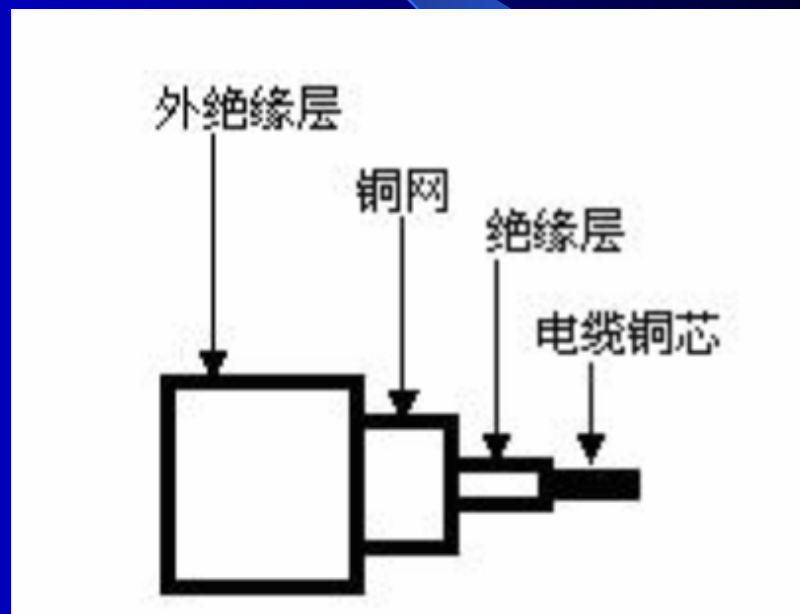


集线器到集线器

- 使用双绞线连接集线器和集线器，可以扩大网络规模，加大网络连接距离。从网卡到集线器，允许的最大网线长度为100米；从集线器到集线器，允许的最大网线长度也是100米。
- 集线器到集线器的双绞线连接方式可以根据集线器上的级联端口分为两种。如果使用集线器上专用的级联端口，则采用网卡到集线器连线方式，如果不使用集线器上专用的级联端口，则采用网卡到网卡连线方式。一般情况下，如果集线器有专用的级联端口，厂商会在该端口旁标注UPLINK字样。

同轴电缆

- 同轴电缆是由一根空心的外圆柱导体（铜网）和一根位于中心轴线的内导线（电缆铜芯）组成，并且内导线和圆柱导体及圆柱导体和外界之间都是用绝缘材料隔开。它的特点是抗干扰能力好，传输数据稳定，价格也便宜，同样被广泛使用，如闭路电视线等。



光缆

- 光缆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。与其他传输介质相比较，光缆的电磁绝缘性能好，信号衰变小，频带较宽，传输距离较大。光缆主要是在要求传输距离较长，用于主干网的连接。光缆通信由光发送机产生光束，将电信号转变为光信号，再把光信号导入光纤，在光缆的另一端由光接收机接收光纤上传输来的光信号，并将它转变成电信号，经解码后再处理。光缆的传输距离远、传输速度快，是局域网中传输介质的佼佼者。光缆的安装和连接需由专业技术人员完成。

3 种UTP线缆的用途与制作

- 双绞线按照是否有屏蔽层可以分为屏蔽双绞线（STP）和非屏蔽双绞线（UTP）。STP抗干扰性较好，但由于价格较贵，因此采用的不是很多。目前布线系统规范通常建议采用UTP来进行水平布线，而将光纤用作主干线缆，同轴电缆已经不再推荐使用。
- UTP按照性能与作用的不同可以分为1、2、3、4、5类、超5类线和6类线，其中适用于计算机网络的是3类、5类和6类UTP。5类UTP的传输速率为10 Mb / s至100 Mb / s，阻抗为100 Ohm，线缆的最大传输距离为100 m。增强型5类UTP线缆通过性能增强设计后可支持1 000 Mb / s的传输速率，又被称为超5类或5e线。6类UTP线缆的标准已经于2003年颁布，这是专为1 000 Mb / s传输制定的布线标准。

UTP线缆的组成

- UTP线缆内部由4对线组成，每一对线由相互绝缘的铜线绞绞而成，绞绞的目的是为了减少电磁干扰，双绞线的名称即源于此。每一根线的绝缘层都有颜色。一般来说其颜色排列可能有两种情况。第一种情况是由4根白色的线分别和1根橙色、1根绿色、1根蓝色、1根棕色的线相间组成，通常把与橙色相绞的那根白色的线称作白橙色线，与绿色线相绞的白色的线称作白绿色线，与蓝色相绞的那根白色的线称作白蓝色线，与棕色相绞的白色的线称作白棕色线。第二种情况是由8根不同颜色的线组成，其颜色分别为白橙（由一段白色与一段橙色相间而成）、橙、白绿、绿、白棕、棕、白蓝、蓝。

三种UTP线缆的作用及线序排列

直连线

- 直连线用于将计算机连入到Hub或交换机的以太网口如图1-22所示，或在结构化布线中由配线架连到Hub或交换机等。如图所示给出了根据EIA / TIA 568—B标准的直连线线序排列说明。EIA / TIA 568—B标准有时被称为端接B标准。

端1	白橙	橙	白绿	蓝	白蓝	绿	白棕	棕
端2	白橙	橙	白绿	蓝	白蓝	绿	白棕	棕

交叉线的作用和线图

- 交叉线用于将计算机与计算机直接相连、交换机与交换机直接相连，有时也被用于将计算机直接接入路由器的以太网口。如图所示，左边为直连线使用方式，右边为交叉线使用方式。



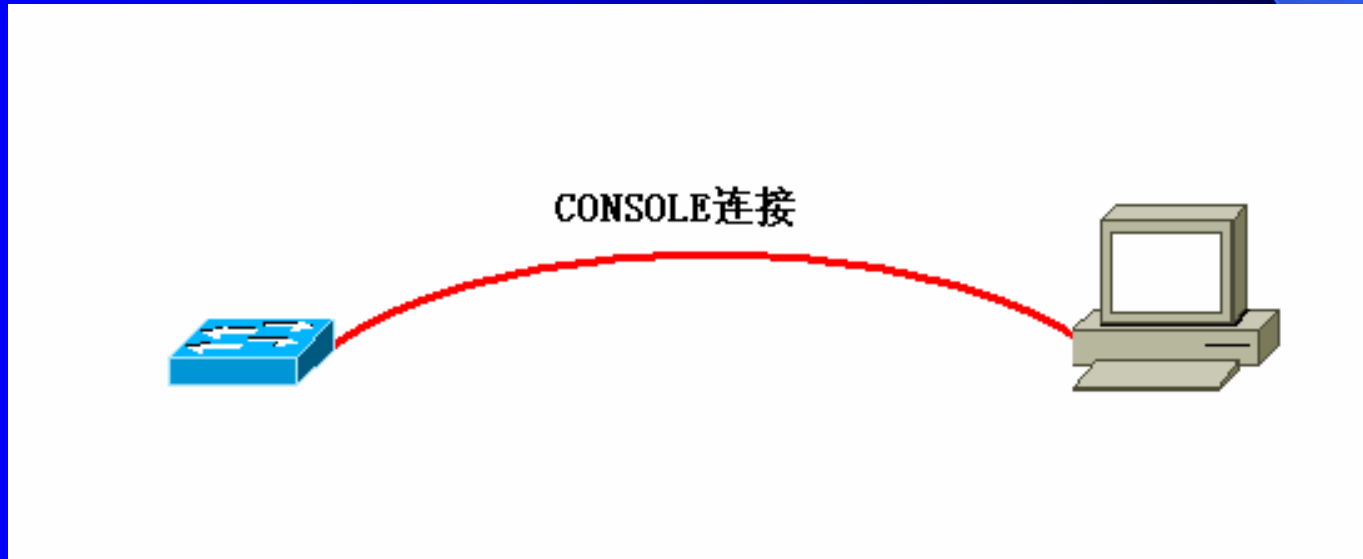
交叉线的作用和线图

另外如图1-24所示给出了EIA / TIA 568—B标准的对接线线序排列

端1	白橙	橙	白绿	蓝	白蓝	绿	白棕	棕
端2	白绿	绿	白橙	蓝	白蓝	橙	白棕	棕

反转线的作用

- 反转线用于将计算机连到交换机或路由器的控制端口，如图所示，在这个连接场合计算机所起的作用相当于它是交换机或路由器的超级终端。



制作步骤

制作直连线

- (1) 计算将要连线的两个设备间的距离，然后在这个距离上至少加上12厘米作为将要截取的电缆的长度。
- (2) 按照算好的长度截取一段5类双绞线。
- (3) 将电缆一端的塑料外皮剥掉2厘米的长度。

制作直连线

- (4) 用手将4对绞在一起的线缆按白橙、橙、白绿、绿、白蓝、蓝、白棕、棕的顺序拆分开来并小心地拉直。注意尽量保持电线绞在一起状态以使噪音可以被抵消。
- (5) 手持电缆，按顺序调整线缆的颜色顺序，即交换蓝线与绿线的位置。
- (6) 捋直并排列好所有的电线，然后在距离电缆外皮0.5厘米到0.75厘米的地方笔直的将电线绞断。应该使得电线没有交织在一起的部分尽量短，因为这一部分要是过长的话，将成为电子噪声的主要来源。

制作直连线

- (7) 将一个RJ-45插头放到电缆的一端，注意插头的叉子应该朝下，橙色的一组电线对着最左边的连接器。
- (8) 轻轻地将插头推倒电线上直到透过插头的顶端可以看到电线的铜线。确认电缆的外皮是否已经进入插头和所有的电线排序是否正确。如果电缆的外皮没有进入插头的话，就不能很好的防止电缆的扭伤。如果没有问题，用力使用钳子夹插头使它可以割破绝缘皮接触电线，完成导电回路。

制作直连线

- (9) 使用相同的方案，重复步骤3~8制作电缆另一端，完成直连线。
- (10) 使用指示器测试刚刚完成的电缆。

制作交叉线

- (1) 按照制作直连线中的步骤1~7制作线缆的一端。
- (2) 用剥线工具在线缆的另一端剥出一定长度的线缆。
- (3) 用手将4对绞在一起的线缆按白绿、绿、白橙、橙、白蓝、蓝、白棕、棕的顺序拆分开来并小心地拉直

制作交叉线

- （4）按顺序调整线缆的颜色顺序，也就是交换橙线与绿线的位置。
- （5）将线缆整平直并剪齐，确保平直线缆的最大长度不超过1.2 厘米。
- （6）将线缆放入RJ45插头，在放置过程中注意RJ45插头的把子朝下，并保持线缆的颜色顺序不变。

制作交叉线

- (7) 检查已放入RJ45插头的线缆颜色顺序，并确保线缆的末端已位于RJ45插头的顶端。
- (8) 确认无误后，用压线工具用力压制RJ45插头，以使RJ45插头内部的金属薄片能穿破线缆的绝缘层，直至完成交叉线的制作。
- (9) 用网线测试仪检查自己所制作完成的网线，确认其达到交叉线线缆的合格要求，否则按测试仪提示重新制作交叉线。

制作反转线

- (1) 按制作直连线的步骤1~7制作线缆的一端。
- (2) 用剥线工具在线缆的另一端剥出一定长度的线缆。
- (3) 用手将4对绞在一起的线缆按白橙、橙、白绿、绿、白蓝、蓝、白棕、棕的顺序拆分开来并小心地拉直，然后交换绿线与蓝线的位置。

制作反转线

- (4) 将线缆整平直并剪齐，确保平直线缆的最大长度不超过1.2 厘米。
- (5) 将线缆放入RJ—45插头，在放置过程中注意RJ—45插头的把子朝上，并保持线缆的颜色顺序不变。
- (6) 翻转RJ—45头方向，使其把子朝上，检查已放入RJ—45插头的线缆颜色顺序是否和另一端颜色顺序全部反序，并确保线缆的末端已位于RJ—45插头的顶端。

制作反转线

- (7) 确认无误后，用压线工具用力压制RJ-45插头，以使RJ-45插头内部的金属薄片能穿破线缆的绝缘层，直至完成反转线的制作。
- (8) 用网线测试仪检查已制作完成的网线，确认其达到反转线线缆的合格要求，否则按测试仪提示重新制作线缆。