网络基础

# 10.1网络概述

## 10.1.1计算机网络的概念

* 1. 计算机网络的发展

发展过程大致可以划分为如下4个阶段:

* 1. 具有通信功能的单机系统
  2. 具有通信功能的2机系统
  3. 以共享资源为目的的计算机网络
  4. 以局域网及因特网为支撑环境的分布式计算机系统
  5. 计算机网络的定义

利用**通信设备**和**线路**将地理位置分散的、功能独立的自主**计算机**系统或由计算机控制的外部设备连接起来，在**网络操作系统**的控制下，**按照约定的通信协议**进行信息交换，实现资源共享的系统。

* 1. 计算机网络的功能

计算机网络具有以下功能：

* 1. 数据通信：用以在计算机系统之间传送各种信息。
  2. 资源共享：资源共享包括软件资源共享和硬件资源共享。
  3. 负载均衡
  4. 高可靠性
  5. 按照数据通信和数据处理功能分类

分为两类，内层**通信子网**和外层**资源子网**，通信子网对应于OSI中的低三层（物理层、数据链路层、网络层），而资源子网对应于OSI中的高三层（会话层、表示层、应用层）。

通信子网：

通信子网的节点计算机和高速通信线路组成独立的数据系统，承担全网的数据传输、交换、加工和变换等通信处理工作，即将一台计算机的输出信息传送给另一台计算机。

资源子网：

资源子网包括计算机、终端、通信子网接口设备、外部设备（如打印机、磁带机和绘图机等）及各种软件资源等，它负责全网的数据处理和向网络用户提供网络资源及网络服务。

* 1. 网络操作系统所支持的功能
     1. 硬件支持。支持多种网卡接口卡（现在叫做网卡）。
     2. 多用户多任务支持。
     3. 网络管理。
     4. 用户管理。

## 10.1.2计算机网络的分类（按照通讯距离分类）

* 1. 局域网（Local Area Network, LAN）

局域网（Local Area Network, LAN）是指传输距离有限，传输速度较高，以共享网络资源为目的的网络系统。

特点：

* 1. 分布范围有限
  2. 有较高的通信带宽，数据传输率高。
  3. 数据传输可靠，误码率低。
  4. 通常采用同轴电缆或双绞线作为传输介质。
  5. 拓扑结构简单简洁，大多采用总线、星型和环型等，系统容易配置和管理。
  6. 网络的控制一般趋向于分布式，从而减少了对某个节点的依赖性，避免并减小了一个节点故障对整个网络的影响。
  7. 通常网络归单一组织所拥有和使用。
  8. 城域网（Metropolitan Area Network, MAN）

城域网（Metropolitan Area Network, MAN）是规模介于局域网和广域网之间的一种较大范围的高速网络，一般覆盖临近的多个单位和城市。城域网的概念已经淡化，目前可以认为只有局域网和广域网两种。

* 1. 广域网（Wide Area Network, WAN）

广域网（Wide Area Network, WAN）又称远程网，它是指覆盖范围广、传输速率相对较低、以数据通信为主要目的的数据通信网。

特点：

* 1. 分布范围广。
  2. 数据传输率低。
  3. 数据传输可靠性随着传输介质的不同而不同。
  4. 广域网常常借用传统的公共传输网来实现，因为单独建造一个广域网极其昂贵。
  5. 拓扑结构较为复杂，大多采用“分布式网络”。

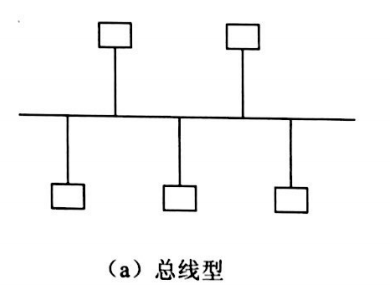
## 10.1.3网络拓扑结构

* 1. 什么是网络拓扑

网络中各个节点相互连接的方法和形式称为网络拓扑。

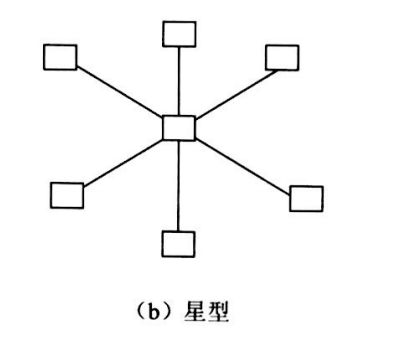
* 1. 总线型结构

其特点为总线型拓扑结构中只有一条双向通路，便于进行广播式传送信息。故结构比较简单，设备少，价格低，安装使用方便，网上的信息延迟时间不确定，故障隔离和检测困难。



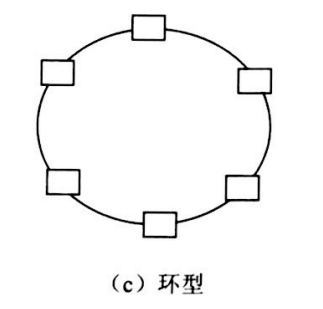
* 1. 星型结构

中央交换单元以放射状连接到网中的各个节点，中央单元采用电路交换方式以建立所希望通信的两节点间专用的路径。其特点为维护管理容易，重新配置灵活；故障隔离和检测容易；网络延迟时间短；网络共享能力差；线路利用率低，中央单元负荷重。局域网多使用星型结构。



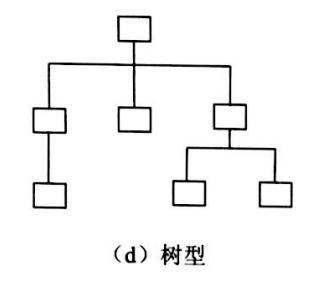
* 1. 环型结构

环型结构的信息传输线路构成一个封闭的环型，各节点通过中继器连入网内，各中继器间首尾相接，信息单向沿环路逐点传送。其特点为环型网中信息的流动方向是固定的，两个节点仅有一条通路，路径控制简单，传输效率低，系统响应速度慢；由于环路封闭，扩充较难。



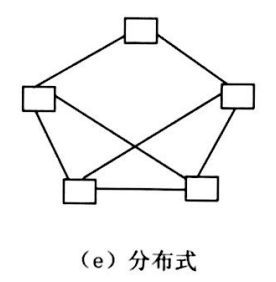
* 1. 树型结构

树型结构是总线型结构的扩充形式，主要用于多个网络组成的分级结构中。其特点同总线型网。广域网多用分布式或树型结构。



* 1. 分布式结构

分布式结构无严格的布点规定和形状，各节点之间有多条线路相连，其特点为分布式网有较高的可靠性，当一条线路有故障时，不会影响整个系统工作；资源共享方便，网络响应时间短；由于节点与多个节点连接，故节点的路由选择和流量控制难度大，管理软件复杂；硬件成本高。广域网多用分布式或树型结构。



* 1. 冲突域和广播域：
  2. 冲突域：

连接在同一导线上的所有工作站的集合，或者说是同一物理网段上所有节点的集合或以太网上竞争同一带宽的节点集合。在OSI模型中，冲突域被看作是第一层的概念，连接同一冲突域的设备有Hub，Reperter或者其他进行简复制信号的设备，能够扩大冲突域，数据链路层及以上的设备可以隔开冲突域。

* 1. 广播域：

接收同样广播消息的节点的集合。广播域被

认为是OSI中的第二层概念，所以像Hub，交换机等第一，二层设备连接的节点集合被认为都是在同一个广播域，三层及以上设备可以隔开广播域。

参考自：<https://blog.csdn.net/ugly_girl/article/details/80901887>

## 10.1.4 ISO/OSI网络体系结构

* 1. ISO/OSI参考模型

IOS/OSI的参考模型共有7层。由低层至高层分别为物理层、数据链路层、网络层、传输层、会话层、表示层和应用层。ISO/OSI的7层参考模型本身不是一个标准，在制定具体网络协议和标准时，要依OSI/RM参考模型作为“参照基准”，并说明与该“参照基准”的对应关系。

协 议 
应 用 层 
表 示 层 
会 话 层 
传 输 层 
网 络 层 
数 据 链 路 层 
物 理 层 
物 理 介 质 
应 用 层 
表 示 层 
会 话 层 
传 输 层 
网 络 层 
数 据 链 路 层 
物 理 层 

特点：

* 1. 是一种将异构系统互连的分层结构。
  2. 提供了控制互连系统交互规则的标准框架。
  3. 定义了一种抽象结构，而并非具体实现的描述。
  4. 不同系统上相同层的实体称为同等层实体。
  5. 同等层实体之间的通信由该层的协议管理。
  6. 相邻层间的接口定义了原语操作和低层向高层提供的服务。
  7. 所提供的公共服务是面向连接的或无连接的数据服务。
  8. 直接的数据传送仅在最低层实现。
  9. 每层完成所定义的功能，修改本层的功能并不影响其他层
  10. ISO/OSI各层的功能
  11. 物理层（Physical Layer）：

提供为建立、维护和拆除物理链路所需的机械、电气、功能和规程的特性；提供有关在传输介质上传输非结构的位流及物理链路故障检测指示。

在这一层，数据还没有被组织，仅作为原始的位流或电气电压处理，单位是位。

* 1. 数据链路层（Data Link Layer）:

数据链路层负责在两个相邻节点间的线路上无差错地传送以帧为单位的数据，并进行流量控制。每一帧包括一定数量的数据和一些必要的控制信息。和物理层相似，数据链路层要负责建立、维持和释放数据链路的连接。传输单位是帧。

* 1. 网络层（Network Layer）：

传输层实体提供端到端的交换网络数据传送功能，使得传输层摆脱路由选择、交换方式和拥挤控制等网络传输细节；可以为传输层实体建立、维持和拆除一条或多条通信路径；对网络传输中发生的不可恢复的差错予以报告。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。传输的单位是包。

* 1. 传输层（Transport Layer）：

为会话层实体提供透明、可靠的数据传输服务，保证端到端的数据完整性。选择网络层能提供最适宜的服务；提供建立、维护和拆除传输连接功能。传送单位是报文。

* 1. 会话层（Session Layer）：

为彼此合作的表示层实体提供建立、维护和结束会话连接的功能；完成通信进程的逻辑名字与物理名字间的对应；提供会话管理服务。

* 1. 表示层（Presentation Layer）：

为应用层进程提供能解释所交换信息含义的一组服务，即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。提供格式化的表示和转换数据服务。数据的压缩、解压缩、加密和解密等工作都由表示层负责

。

* 1. 应用层（Application Layer）：

提供OSI用户服务，即确定进程之间通信的性质，以满足用户需要以及提供网络与用，户应用软件之间的接口服务。例如，事务处理程序、电子邮件和网络管理程序等。

会话层和表示层仅仅是该模型中的规定，在TCP/IP中这两层不存在。

* 1. ISO/OSI参考模型中的数据流向

A 系 统 
应 用 层 
表 示 层 
会 话 层 
传 输 层 
网 络 层 
数 据 链 路 层 
物 理 层 
数 据 
AH 数 据 
应 用 协 议 
表 示 协 议 
会 话 协 议 
传 输 协 议 一 ． 一 ， · 
网 络 协 议 一 ． - ． · 
B 系 统 
应 用 层 
表 示 层 
会 话 层 
传 输 层 
网 络 层 
数 据 链 路 层 
物 理 层 

# 10.2网络互联硬件

## 10.2.1网络设备

* 1. 网络传输介质互联设备

网络线路与用户节点具体衔接时，需要网络传输介质的互联设备。如T型头（细同轴电缆连接器）、收发器、RJ-45（屏蔽或非屏蔽双绞线连接器）。

* 1. 物理层互联设备
  2. 中继器：

在物理层上实现局域网网段互连的，用于扩展局域网网段的长度。由于中继器只在两个局域网网段间实现电气信号的恢复与整形，因此它仅用于连接相同的局域段。在以太网中最多使用4个中继器，中继器的主要优点是安装简便、使用方便、价格便宜。

* 1. 集线器：

可以看成是一种特殊的多路中继器，也具有信号放大功能，与中继器相比集线器可连接多个物理线路，中继器只能连接两个物理线路。优点是当网络系统中某条线路或某节点出现故障时，不会影响网上其他节点的正常工作。集线器上各端口都是共享同一条背板总线的，因此各个端口共同竞争总带宽，并采用广播方式发送信号。

* 1. 数据链路层互联设备
  2. 网桥：

用于连接两个局域网网段，工作于数据链路层。网桥要分析帧地址字段，以决定是否把收到的帧转发到另一个网络段上。确切地说，网桥工作于MAC子层，只要两个网络MAC子层以上的协议相同，都可以用网桥互连，比如802.3有线以太网和802.11无线网络。网桥的两个端口分别有一条独立的交换信道，不是共享一条背板总线，可隔离冲突域。

网桥仅有两个端口。

* 1. 交换机：

交换机是一个具有简化、低价、高性能和高端口密集特点的交换产品，它是按每一个包中的MAC地址相对简单地决策信息转发，而这种转发决策一般不考虑包中隐藏的更深的其他信息。交换机转发数据的延迟很小，操作接近单个局域网性能，远远超过了普通桥接的转发性能。交换机的任意两个网络节点提供独享的电信号通路，多个端口不需要竞争带宽，不广播发送数据帧。

交换机有多个端口，每个端口都具有桥接功能，可以连接一个局域网或一台高性能服务器或工作站。实际上，交换机有时被称为多端口网桥。

交换机的三种交换技术：端口交换，帧交换，信元交换。

* 1. 网络层互联设备
  2. 路由器：

路由器（Router）是网络层互联设备，用于连接多个逻辑上分开的网络。逻辑网络是指一个单独的网络或一个子网，当数据从一个子网传输到另一个子网时，可通过路由器来完成。

路由器具有很强的异种网互连能力，互连的网络最低两层协议可以互不相同，通过驱动软件接口到第三层上而得到统一。

通常把网络层地址信息叫做网络逻辑地址，把数据链路层地址信息叫做物理地址。

路由器最主要的功能是选择路径，其他功能包括过滤、存储转发、流量管理和介质转换等。

路由器工作于网络层，它处理的信息量比网桥要多，因而处理速度比网桥慢。

* 1. 应用层互联设备
  2. 网关：

网关（Gateway）是应用层的互联设备。在一个计算机网络中，当连接不同类型而协议差别又较大的网络时，则要选用网关设备。网关的功能体现在OSI模型的最高层，它将协议进行转换，将数据重新分组，以便在两个不同类型的网络系统之间进行通信。

一般来说，网关只进行一对一转换，或是少数几种特定应用协议的转换，网关很难实现通用的协议转换。

## 10.2.2网络的传输介质

* 1. 有线介质
  2. 双绞线（Twisted—Pair，TP）：

双绞线是现在最普通的传输介质，它分为屏蔽双绞线（STP）和非屏蔽双绞线（UTP）。非屏蔽双绞线有线缆外皮作为屏蔽层，适用于网络流量不大的场合中。屏蔽式双绞线具有一个金属甲套，对电磁干扰具有较强的抵抗能力，适用于网络流量较大的高速网络协议应用。

双绞线还可以分成七类：

网 
线 类 型 
超 5 类 6 类 
超 6 类 
7 类 
类 
3 类 线 
5 类 线 
线 
线 
线 
线 
用 
于 
适 应 
8 0 
年 
用 于 令 适 用 于 
适 用 于 
万 兆 
适 于 的 牌 
用 旧 令 网 
用 持 网 
代 
牌 局 域 
主 要 用 于 传 输 速 主 要 应 用 
10 OBASE—T 
位 以 
作 用 
千 兆 位 以 率 高 于 
于 千 兆 位 太 网 
网 和 以 
和 
太 网 络 
太 网 
网 络 中 
技 术 
的 
IOBASE—T 
1 Gbps 
电 
使 用 
网 络 
的 网 络 
的 应 
用 
话 
线 
传 输 频 率 最 高 传 输 速 率 
比 
200 一 250 可 达 
IMHz 一 
较 
IMHZ 
16MHz 
20MHz 
100MHz 
100MHz 
250MHz 
MHz 
500 
低 
MHz 
比 
较 
4Mbps 10Mbps 
16Mbps 
10 0Mbps 
1000Mbps 
1 Gbps 
1000Mbps 
Gbps 
低 

双绞线需要配合RJ45插头使用。

* 1. 同轴电缆（Coaxial）：

同轴电缆也像双绞线那样由一对导体组成。同轴电缆又分为基带同轴电缆（阻抗为50Ω）和宽带同轴电缆（阻抗为75Ω）。基带同轴电缆用来直接传输数字信号，它又分为粗同轴电缆和细同轴电缆。宽带同轴电缆用于频分多路复用（FDM）的模拟信号发送，还用于不使用频分多路复用的高速数字信号发送和模拟信号发送。

* 1. 光纤（Fiber Optic）：

光导纤维简称光纤，它重量轻，体积小。用光纤传输电信号时，在发送端先要将其转换成光信号，而在接收端又要由光检波器还原成电信号。

光纤分为多模光纤和单模光纤，多模光纤（Multimode Fiber）使用的材料是发光二极管，价格较便宜，但定向性较差；单模光纤（Single Mode Fiber）使用的材料是注入型二极管，定向性好，损耗少，效率高，传播距离长，但价格昂贵。

* 1. 无线介质
  2. 微波：

微波通信是在对流层视线距离范围内利用无线电波进行传输的一种通信方式，频率范围为2～40GHz，微波通信的传输质量比较稳定，影响质量的主要因素是雨雪天气对微波产生的吸收损耗，不利地形或环境对微波所造成的衰减现象。

* 1. 红外线和激光：

有很强的方向性，都是沿直线传播的。对环境气候较为敏感，例如雨、雾和雷电。相对来说，微波一般对雨和雾的敏感度较低。

* 1. 卫星：

卫星通信是以人造卫星为微波中继站，它是微波通信的特殊形式。卫星接收来自地面发送站发出的电磁波信号后，再以广播方式用不同的频率发回地面，被地面工作站接收。卫星通信的优点是容量大、距离远，缺点是传播延迟时间长。

## 10.2.3组建局域网

* 1. 局域网的组成
  2. 服务器（Server）
  3. 客户端（Client）
  4. 网络设备。

主要指一些硬件设备，如网卡、收发器、中继器、集中器、网桥和路由器等。网卡是一种必不可少的网络设备，常用的网卡有Ethernet（以太网）网卡、ARCNET网卡、ESIA总线网网卡和Token-Ring网卡等。

* 1. 通信介质。
  2. 网络软件。

网络软件主要包括底层协议软件、网络操作系统（NOS）等。底层协议软件是由一组标准规则及软件构成，以使实体间或网络之间能够互相进行通信。网络操作系统主要对整个网络的资源和运行进行管理，并为用户提供应用接口。

* 1. 组网例子，软考教材532页

# 10.3网络的协议与标准

## 10.3.1

* 1. IEEE简介

电气和电子工程师协会（Institute of Electrical and Electronics Engineers）。IEEE设置了电子工业标准，分成一些标准委员会（或工作组），每个工作组负责标准的一个领域，工作组802设置了网络上的设备如何彼此通信的标准，即IEEE 802标准委员会划分成的工作组有802.1工作组，协调低档与高档OSI模型；802.2工作组，涉及逻辑数据链路标准；802.3工作组，有关CSMA/CD标准在以太网的应用；802.4工作组，令牌总线标准在LAN中的应用；802.5工作组，设置有关令牌环网络的标准等。

* 1. 协议

协议指的是网络中的计算机与计算机通信时，为了能够实现数据的正常发送与接受必须要遵循的一些事先约定好的规则（标准或约定），在这些规则中明确规定了通信时的数据格式，数据传送时序以及相应的控制信息和应答信号等内容。

## 10.3.2局域网协议

* 1. LAN模型IEEE 802

在IEEE 802局域网（LAN）标准中，只定义了物理层和数据链路层两层，并根据LAN的特点，把数据链路层分成逻辑链路控制（Logical Link Control, LLC）子层和介质访问控制（Medium Access Control, MAC）子层。如图：

OSI/RM 
高 层 
传 输 层 
网 络 层 
数 据 链 路 层 
物 理 层 
逻 辑 链 路 控 制 层 
介 质 访 问 控 制 层 
物 理 层 

* 1. 物理层：

和OSI物理层的功能一样，主要处理在物理链路上发送、传递和接收非结构化的比特流，包括对带宽的频道分配和对基带的信号调制、建立、维持、撤销物理链路，处理机械的、电气的和过程的特性。其特点是可以采用一些特殊的通信媒体，在信息组成的格式上可以有多种。

* 1. MAC：

主要功能是控制对传输介质的访问，MAC与网络的具体拓扑方式以及传输介质的类型有关，主要是介质的访问控制和对信道资源的分配。MAC层还实现帧的寻址和识别，完成帧检测序列产生和检验等功能。

* 1. MAC地址（Media Access Control Address）：

直译为媒体存取控制位址，也称为局域网地址（LAN Address），MAC位址，以太网地址（Ethernet Address）或物理地址（Physical Address），它是一个用来确认网络设备位置的位址。在OSI模型中，第三层网络层负责IP地址，第二层数据链路层则负责MAC位址 。MAC地址用于在网络中唯一标示一个网卡，一台设备若有一或多个网卡，则每个网卡都需要并会有一个唯一的MAC地址 。

MAC地址的长度为48位(6个字节)，通常表示为12个16进制数，如：00-16-EA-AE-3C-40就是一个MAC地址，其中前3个字节，16进制数00-16-EA代表网络硬件制造商的编号，它由IEEE(电气与电子工程师协会)分配，而后3个字节，16进制数AE-3C-40代表该制造商所制造的某个网络产品(如网卡)的系列号。

* 1. LLC：

可提供两种控制类型，即面向连接服务和非连接服务。其中，面向连接服务能够提供可靠的信道。逻辑链路控制层提供的主要功能是数据帧的封装和拆除，为高层提供网络服务的逻辑接口，能够实现差错控制和流量控制。

* 1. IEEE 802标准之间的关系：

802 、 3 
802 」 
$ 02 ， 2 
802 ． 4 
802 」 2 
体 系 结 构 及 网 络 厘 连 
逻 辑 链 路 控 制 
介 质 访 问 控 制 
物 理 介 质 

* 1. 所有的IEEE802标准：



* 1. 以太网 IEEE802.3

采用的“存取方法”是带冲突检测的载波监听多路访问协议（Carrier-Sense Multiple Access with Collision Detection, CSMA/CD）技术。目前以太网主要包括三种类型：

IEEE 802.3中定义的标准局域网，速度为10Mb/s，传输介质为细同轴电缆；

IEEE 802.3u中定义的快速以太网，速度为100Mb/s，传输介质为双绞线；

IEEE 802.3z中定义的千兆以太网，速度为1000Mb/s，传输介质为光纤或双绞线。

* 1. 介质访问技术：

IEEE802.3 [使用CSMA/CD介质访问技术](onenote:" \l "网络基础&section-id={3E6BEB50-15CC-4AFB-BC5E-0A431F1E59DA}&page-id={447B40E1-4CD2-48AB-AE38-ECF8C2B36EDD}&object-id={8C0487C9-F915-0A9A-18A4-247443B7E4D2}&37&base-path=https://d.docs.live.net/62d96054cee15679/文档/信息摘抄/计算机网络.one)。

* 1. IEEE 802.3-10Mbps以太网：

IEEE 802.3所使用的介质访问协议CSMA/CD是让整个网络上的主机都以竞争的方式来抢夺传送数据的权力。

* 1. 工作过程：

首先侦听信道，如果信道空闲，则发送；如果信道忙，则继续侦听，直到信道空闲时立即发送。开始发送后再进行一段时间的检测，方法是边发送边接收，并将收、发信息相比较，若结果不同，表明发送的信息遇到碰撞，于是立即停止发送，并向总线上发出一串阻塞信号，通知信道上各站冲突已发生。已发出信息的各站收到阻塞信号后，等待一段随机时间，等待时间最短的站将重新获得信道，可重新发送。

在CSMA/CD中，当检测到冲突并发出阻塞信号后，为了降低再次冲突概率，需要等待一个退避时间。退避算法有许多种，常用的一种通用退避算法称为二进制指数退避算法。

* 1. 型号的名称含义：

IEEE 802.3——10Mb/s以太网定义过10Base5、10Base2、10Base-T和10Base-F等几种。其型号的含义如下：

10 表示10Mb/s。

Base 表示基带传输，线路编码。

5 代表传输距离500米，传输介质使用同轴粗缆。

T 代表传输介质是双绞线，三类双绞线即可满足。

F 代表光纤。

* 1. 线缆参数对比：

名 称 
电 
缆 
最 大 区 间 长 度 
节 点 数 / 段 
优 点 
用 于 主 干 
10Base5 
5 0 0 m 
1 00 
AU | 
200m （ 185m ） 
10Base2 
纟 田 
缆 
廉 价 
30 
BNC 
易 于 维 护 
双 绞 线 
10Base—T 
RJ—45 
1C24 
1 0 0 m 

拓扑类型为总线型拓扑。

* 1. IEEE 802.3u-100Mbps快速以太网：

采用了非屏蔽双绞线（或屏蔽双绞线、光纤）作为传输媒介，采用与IEEE 802.3一样的介质访问控制层——CSMA/CD，快速以太网可以分为100BaseTX、100BaseFX和100BaseT4三种。

* 1. IEEE 802.3z-1000Mbps千兆以太网：

快速以太网可以分为100BaseTX、100BaseFX和100BaseT4三种。千兆位以太网采用以交换机为中心的星型拓扑结构。

千兆以太网支持如下三种传输介质：

* 1. 光纤系统。支持多模光纤和单模光纤系统，多模光纤的工作距离为500m，单模光纤的工作距离为2000m。
  2. 宽带同轴电缆系统。其传输距离为25m。
  3. 5类UTP电缆。其传输距离为100m。

千兆位以太网采用以交换机为中心的星型拓扑结构。

* 1. 其他以太网协议：

|  |  |  |  |
| --- | --- | --- | --- |
| 1 | Experimental  Ethernet | 1973 | 2.94 Mbit/s (367 kB/s) over coaxial cable (coax) bus，这是最早的实验以太网。 |
| 2 | Ethernet II  (DIX v2.0) | 1982 | 10 Mbit/s (1.25 MB/s) over thick coax. Frames have a Type field. This frame format is used on all forms of Ethernet by protocols in the Internet protocol suite。这个时候EthernetII报文格式基本确定。DIX Ethernet, named after DEC, Intel and Xerox。[EthernetII帧结构](https://www.maixj.net/ict/ethernetii-frame-3426) |
| 3 | IEEE 802.3 standard | 1983 | 10BASE5 10 Mbit/s (1.25 MB/s) over thick coax. Same as Ethernet II (above) except Type field is replaced by Length, and an 802.2 LLC header follows the 802.3 header. Based on the CSMA/CD Process。开始制定802.3系列标准。802.3，后面不带任何数字的，就是第一个标准。传输距离500m。 |
| 4 | 802.3a | 1985 | 10BASE2 10 Mbit/s (1.25 MB/s) over thin Coax (a.k.a. thinnet or cheapernet)。传输距离185米。 |
| 5 | 802.3b | 1985 | 10BROAD36.10 Mbit/s Ethernet signals over standard 75 ohm cable television (CATV) cable over a 3600 meter range。已经废弃的标准。 |
| 6 | 802.3c | 1985 | 10 Mbit/s (1.25 MB/s) repeater spec。HUB的时代。 |
| 7 | 802.3d | 1987 | Fiber-optic inter-repeater link (FOIRL) is a specification of Ethernet over optical fibre. It was replaced by 10BASE-FL. |
| 8 | 802.3e | 1987 | 1BASE5 or StarLAN。StarLAN was the first implementation of 1 megabit per second (1Mbit/s) Ethernet over twisted pair wiring. It was standardized by the standards association of the Institute of Electrical and Electronics Engineers (IEEE) as 802.3e in 1987, as the 1BASE5 version of Ethernet. 这个时候开始使用双绞线传输以太网信号。 |
| 9 | 802.3i | 1990 | 10BASE-T 10 Mbit/s (1.25 MB/s) over twisted pair.传输距离100米。 |
| 10 | 802.3j | 1993 | 10BASE-F 10 Mbit/s (1.25 MB/s) over Fiber-Optic. |
| 11 | 802.3u | 1995 | 100BASE-TX, 100BASE-T4, 100BASE-FX Fast Ethernet at 100 Mbit/s (12.5 MB/s) w/o autonegotiation。进入快速以太网时代。  100base-T4 (twisted pair [4 pair])  100base-TX (twisted pair [2 pair])  100base-FX (fiber, 400m, [MMF光纤](https://www.maixj.net/ict/fiber-2669)) |
| 12 | 802.3x | 1997 | Full Duplex and flow control; also incorporates DIX framing, so there's no longer a DIX/802.3 split。 |
| 13 | 802.3y | 1998 | 100BASE-T2 100 Mbit/s (12.5 MB/s) over low quality twisted pair |
| 14 | 802.3z | 1998 | 1000BASE-X Gbit/s Ethernet over Fiber-Optic at 1 Gbit/s (125 MB/s)。那个时候用的光口应该是[GBIC](https://www.maixj.net/ict/gbic-2640)。 |
| 15 | 802.3-1998 | 1998 | A revision of base standard incorporating the above amendments and errata。1998年应该算是一个以太网发展的里程碑吧。 |
| 16 | 802.3ab | 1999 | 1000BASE-T Gbit/s Ethernet over twisted pair at 1 Gbit/s (125 MB/s)。GE是先有光口的标准，后有电口的标准。传输距离还是100米。 |
| 17 | 802.3ac | 1998 | Max frame size extended to 1522 bytes (to allow "Q-tag") The Q-tag includes 802.1Q VLAN information and 802.1p priority information.VLAN出现。 |
| 18 | 802.3ad | 2000 | Link aggregation for parallel links, later moved to IEEE 802.1AX。链路聚合。Link aggregation addresses two problems with Ethernet connections: bandwidth limitations and lack of resilience. |
| 19 | 802.3-2002 | 2002 | A revision of base standard incorporating the three prior amendments and errata。 |
| 20 | 802.3ae | 2002 | 10 Gigabit Ethernet over fiber; 10GBASE-SR, 10GBASE-LR, 10GBASE-ER, 10GBASE-SW, 10GBASE-LW, 10GBASE-EW。  SR：Short Range;  LR：Long Range;  ER：Extended Range;  他们的传输线路速率都是是10.3124Gbps，编码使用了64B/66B方式。  SW，LW，RW，中的W表示WAN，广域网；这3中规格的速率是9.95328Gbps，同样编码使用了64B/66B方式，之所以速率低，是为了提高与面向WAN被广泛利用的光缆通信规格的SONET/SDH的亲和性，迎合了SONET的OC-192的传输速度。  以太网从局域网开始发展，到ae标准，已经开始跟广域网进行融合，电信的网络和企业的网络开始融合。[10GBASE以太网介绍](https://www.maixj.net/ict/10gbase-ethernet-3315) |
| 21 | 802.3af | 2003 | Power over Ethernet，or PoE (15.4 W) |
| 22 | 802.3ah | 2004 | Ethernet in the First Mile(EFM)。EPON uses a passive optical network. |
| 23 | 802.3ak | 2004 | 10GBASE-CX4 10 Gbit/s (1,250 MB/s) Ethernet over twinaxial cables |
| 24 | 802.3-2005 | 2005 | A revision of base standard incorporating the four prior amendments and errata. |
| 25 | 802.3an | 2006 | 10GBASE-T 10 Gbit/s (1,250 MB/s) Ethernet over unshielded twisted pair (UTP) |
| 26 | 802.3ap | 2007 | Backplane Ethernet (1 and 10 Gbit/s (125 and 1,250 MB/s) over PCB--printed circuit boards)。 |
| 27 | 802.3aq | 2006 | 10GBASE-LRM 10 Gbit/s (1,250 MB/s) Ethernet over multimode fiber |
| 28 | 802.3as | 2006 | Frame expansion |
| 29 | 802.3at | 2009 | Power over Ethernet enhancements (25.5 W) |
| 30 | 802.3av | 2009 | 10 Gbit/s EPON |
| 31 | 802.3au | 2006 | Isolation requirements for Power over Ethernet (802.3-2005/Cor 1) |
| 32 | 802.3aw | 2007 | Fixed an equation in the publication of 10GBASE-T (released as 802.3-2005/Cor 2) |
| 33 | 802.3-2008 | 2008 | A revision of base standard incorporating the 802.3an/ap/aq/as amendments, two corrigenda and errata. Link aggregation was moved to 802.1AX. |
| 34 | 802.3az | 2010 | Energy Efficient Ethernet |
| 35 | 802.3ba | 2010 | 100 Gigabit Ethernet (100GbE) and 40 Gigabit Ethernet (40GbE) are groups of computer networking technologies for transmitting Ethernet frames at rates of 100 and 40 gigabits per second (100 and 40 Gbit/s), respectively. The technology was first defined by the IEEE 802.3ba-2010 standard.  Another variant, 802.3bg, was added in March 2011 to the set of standards. The task force 802.3bj is working on a four lane backplane and a copper 100 Gbit/s standard.  The 802.3bm task force is working on a standard for lower cost 100 Gbit/s optical physical interfaces.[40G/100G Ethernet Background](https://www.maixj.net/ict/40g-100g-ethernet-background-3320) |
| 36 | 802.3bb | 2009 | Increase Pause Reaction Delay timings which are insufficient for 10 Gbit/s |
| 37 | 802.3bc | 2009 | Move and update Ethernet related TLVs (type, length, values), previously specified in Annex F of IEEE 802.1AB (LLDP) to 802.3 |
| 38 | 802.3bd | 2010 | Priority-based Flow Control. An amendment by the IEEE 802.1 Data Center Bridging Task Group (802.1Qbb) to develop an amendment to IEEE Std 802.3 to add a MAC Control Frame to support IEEE 802.1Qbb Priority-based Flow Control. |
| 39 | 802.3.1 | 2011 | MIB definitions for Ethernet. It consolidates the Ethernet related MIBs present in Annex 30A&B, various IETF RFCs, and 802.1AB annex F into one master document with a machine readable extract. (workgroup name was P802.3be) |
| 40 | 802.3bf | 2011 | Provide an accurate indication of the transmission and reception initiation times of certain packets as required to support IEEE P802.1AS. |
| 41 | 802.3bg | 2011 | Provide a 40 Gbit/s PMD which is optically compatible with existing carrier SMF 40 Gbit/s client interfaces (OTU3/STM-256/OC-768/40G POS). |
| 42 | 802.3-2012 | 2012 | A revision of base standard incorporating the 802.3at/av/az/ba/bc/bd/bf/bg amendments, a corrigenda and errata. |
| 43 | 802.3bj | 2014 | Define a 4-lane 100 Gbit/s backplane PHY for operation over links consistent with copper traces on “improved FR-4” (as defined by IEEE P802.3ap or better materials to be defined by the Task Force) with lengths up to at least 1m and a 4-lane 100 Gbit/s PHY for operation over links consistent with copper twinaxial cables with lengths up to at least 5m. |
| 44 | 802.3bk | 2013 | This amendment to IEEE Std 802.3 defines the physical layer specifications and management parameters for EPON operation on point-to-multipoint passive optical networks supporting extended power budget classes of PX30, PX40, PRX40, and PR40 PMDs. |
| 45 | 802.3bm | 2015 | 100G/40G Ethernet for optical fiber |
| 46 | 802.3bp | 2015 | 1000BASE-T1 - Gigabit Ethernet over a single twisted pair, automotive & industrial environments。[802.3bp简介](https://www.maixj.net/ict/ieee-802-3bp-1000base-t1-4819) |
| 47 | 802.3bq |  | 40GBASE-T for 4-pair balanced twisted-pair cabling with 2 connectors over 30 m distances |
| 48 | 802.3bs |  | 400 Gbit/s Ethernet over optical fiber using multiple 25G/50G lanes |
| 49 | 802.3bt |  | Power over Ethernet enhancements up to 100W using all 4-pairs balanced twisted-pair cabling, lower standby power and specific enhancements to support IoT applications (e.g. Lighting, sensors, building automation). |
| 50 | 802.3bw |  | 100BASE-T1 - 100 Mbit/s Ethernet over a single twisted pair for automotive applications |
| 51 | 802.3-2015 | 2015 | 802.3bx - a new consolidated revision of the 802.3 standard including amendments 802.2bk/bj/bm |
| 52 | 802.3by |  | 25G Ethernet.  25 Gigabit Ethernet (25GbE) and 50 Gigabit Ethernet (50GbE) are proposed standards for Ethernet connectivity in a datacenter environment. An industry consortium has been formed to promote the technology and IEEE 802 workgroup has formed to develop the standard. The draft uses technology defined for 100 Gigabit Ethernet implemented as four 25-Gbit/s lanes (IEEE 802.3bj).  IEEE 802.3 has formed an 802.3by task force with the objectives to define:  a single-lane 25 Gbit/s 25GBASE-KR PHY for printed circuit backplanes;  a single-lane 25 Gbit/s 25GBASE-CR PHY for 5 m twin-ax cables;  a single-lane 25 Gbit/s PHY for multi-mode optical fiber. |

来自 <*<https://www.maixj.net/ict/ethernet-ieee802dot3-3241>*>

* 1. 令牌环网 IEEE802.5

令牌环是环型网中最普遍采用的介质访问控制，它适用于环型网络结构的分布式介质访问控制。

IEEE 802.5的介质访问使用的是令牌环控制技术，工作过程为：首先，令牌环网在网络中传递一个很小的帧，称为“令牌”，只有拥有令牌环的工作站才有权力发送信息。令牌在网络上依次顺序传递。当工作站要发送数据时，等待捕获一个空令牌，然后将要发送的信息附加到后边，发往下一站，如此直到目标站。然后将令牌释放。如果工作站要发送数据时，经过的令牌不是空的，则等待令牌释放。

当信息帧绕环通过各站时，各站都要将帧的目的地址与本站地址相比较，如果地址符合，说明是发送给本站的，则将帧复制到本站的接收缓冲器中，同时将帧送回到环上，使帧继续沿环传送；如果地址不符合，则简单地将信息帧重新送到环上即可。

* 1. FDDI 光纤分布式数据接口 IEEE802.7

FDDI（Fiber Distributed Data Interface，光纤分布式数据接口）类似令牌环网的协议，它用光纤作为传输介质，数据传速可达到100Mb/s。

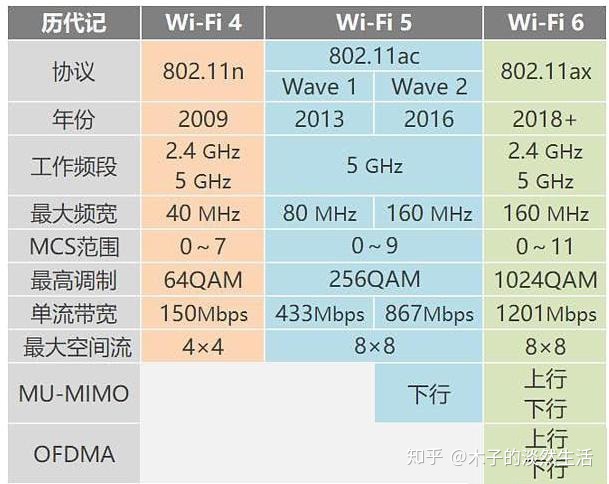
FDDI采用双环体系结构，两环上的信息反方向流动。双环中的一环称为主环，另一环称为次环。在正常情况下，主环传输数据，次环处于空闲状态。双环设计的目的是提供高可靠性和稳定性。FDDI定义的传输介质有单模光纤和多模光纤两种。

* 1. 无线局域网 IEEE802.11

无线局域网使用的是带冲突避免的载波侦听多路访问方法（CSMA/CA)）。冲突检测(Collision Detection)变成了冲突避免（Collision Avoidance)，这一字之差是很大的。因为在无线传输中侦听载波及冲突检测都是不可靠的，侦听载波有困难。另外，通常无线电波经天线送出去时，自己是无法监视到的，因此冲突检测实质上也做不到。在802.11中侦听载波是由两种方式来实现的，一个是实际去听是否有电波在传，然后加上优先权控制;另一个是虚拟的位听载波，告知大家待会有多久的时间我们要传东西，以防止冲突。

IEEE802.11常见标准：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 协议 | 频率 | 速率 | 频宽 | 别称 |
| 802.11b | 2.4GHz | 11Mbps |  |  |
| 802.11a | 5GHz | 54Mbps |  |  |
| 802.11g | 2.4GHz | 54Mbps |  | WIFI3 |
| 802.11n | 2.4 GHz或5 GHz | 72Mbps(1×1, 20MHz)  150Mbps(1×1, 40MHz)  288Mbps(4×4，20MHz)  600Mbps(4×4, 40MHz) | 20MHz/40MHz(信道绑定) | WIFI4 |
| 802.11ac | 5 GHz | 433Mbps(1×1, 80MHz)  867Mbps(1×1,160MHz)  6.77Gbps(8×8,160MHz) | 40MHz  80MHz  160MHz | WIFI5 |
| 802.11ax | 5GHz |  | 1600MHz | WIFI6 |



## 10.3.3 CSMA/CD的冲突检测方法

* 1. CSMA/CD简述

CSMA/CD即**载波侦听多路访问/冲突检测**，是广播型信道中采用一种随机访问技术的竞争型访问方法，具有多目标地址的特点，属于数据链路层协议。它处于一种总线型局域网结构，其物理拓扑结构正逐步向星型发展。CSMA/CD采用分布式控制方法，所有结点之间不存在控制与被控制的关系。

* 1. 工作过程

各工作站在发送数据前，需先侦听信道是否空闲。若空闲，则立即发送数据；若信道忙碌，则等待一段时间至信道中的信息传输结束后再发送数据；若在上一段信息发送结束后，同时有两个或两个以上的节点都提出发送请求，则判定为冲突；若侦听到冲突，则所有节点立即停止发送数据，等待一段随机时间，再重新尝试发送。

* 1. 1和P坚持的CSMA

1坚持的CSMA：线路忙，继续侦听；不忙时，立即发送；信道利用率提高，冲突增大。

p坚持的CSMA：线路忙，继续侦听；不忙时，根据p概率进行发送，以1-p的概率继续侦听。

* 1. 注意

如果两个连接到同一总线的节点间距离超过2500米，数据传播将发生延迟，这种延迟将阻止CSMA/CD的冲突检测程序的正确进行。正因为这个原因，网络中中继器和集线器的使用受到限制，网络拓扑的总长度受限。

在金属介质中，**电信号的传递速度只有光速的65%**，由于传输信号的频率很高，所以传输介质就变成了分布参数电路，一个信号在主机A发出后，B主机需要等待一段时间后才能收到，发送于接受之间的时间间隔不可忽略。

## 10.3.4最大传输单元MTU

* 1. MTU

最大传输单元（Maximum Transmission Unit，MTU）是指一种通信协议的某一层上面所能通过的最大数据包大小（以字节为单位）。作用于数据链路层

如果在IP层要传输一个数据报比链路层的MTU还大，那么IP层就会对这个数据报进行分片。一个数据报会被分为若干片，每个分片的大小都小于或者等于链路层的MTU值。

当同一网络上的主机互相进行通信时，该网络的MTU对通信双方非常重要。但当主机间要通过很多网络才能通信时，对通信双方最重要的是通信路径中最小的MTU，因为在通信路径上不同网络的链路层MTU不同。通信路径中最小的MTU被称为路径MTU。

* 1. 常见链路层协议MTU的缺省数值
     1. FDDI协议：4352字节
     2. 以太网（Ethernet）协议：1500字节
     3. PPPoE（ADSL）协议：1492字节 //IEEE802.2/802.3
     4. IEEE 802.3/802.2：1492字节
     5. X.25协议（Dial Up/Modem）：576字节
     6. Point-to-Point：4470字节

## 10.3.5多路复用技术：

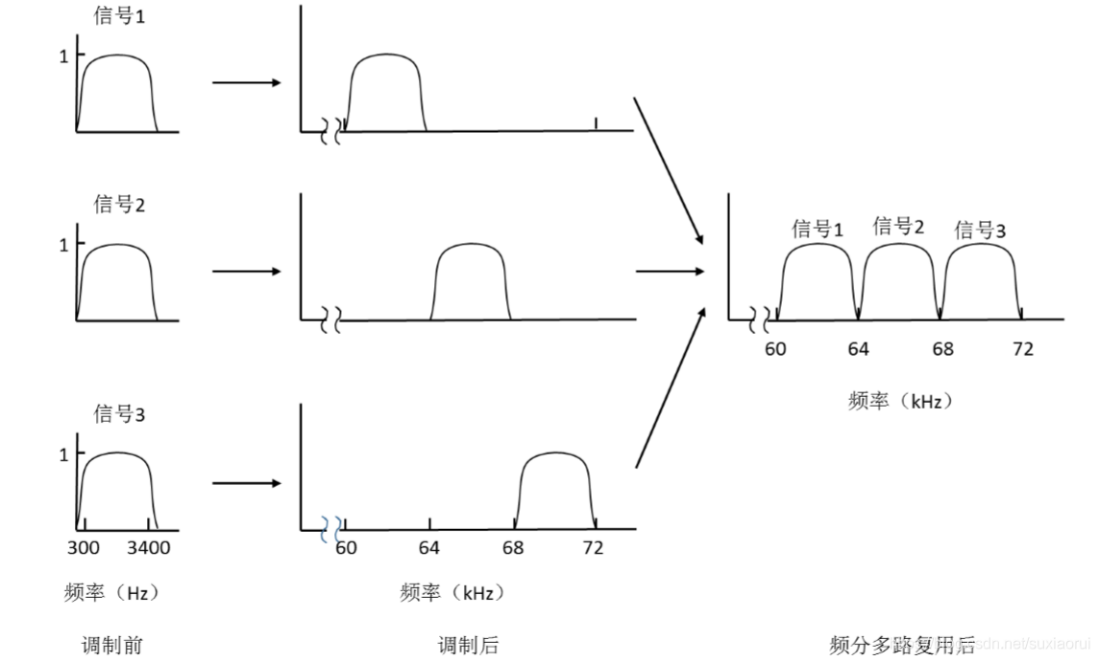
* 1. 什么是多路复用

把通信资源或者说是链路、信道资源进行的划分，分成一系列的资源片。把这些资源片分配给每一路通信。每一路通信在通信过程中就独占它分配到的分配资源。作用于物理层。

来自 <*<https://blog.csdn.net/suxiaorui/article/details/87096375>*>

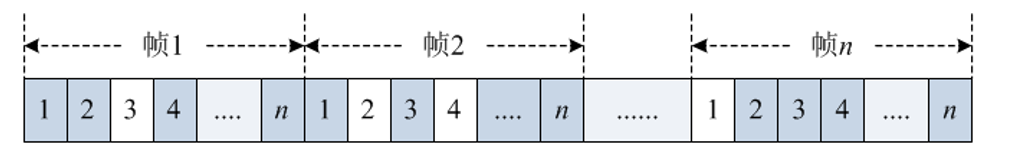
* 1. 频分多路复用( frequency division multiplexing-FDM )

传输结束能够传输的频带很宽，将频带分割成一个个不同的小的频段，再将各个小的频段分给不同的用户使用。



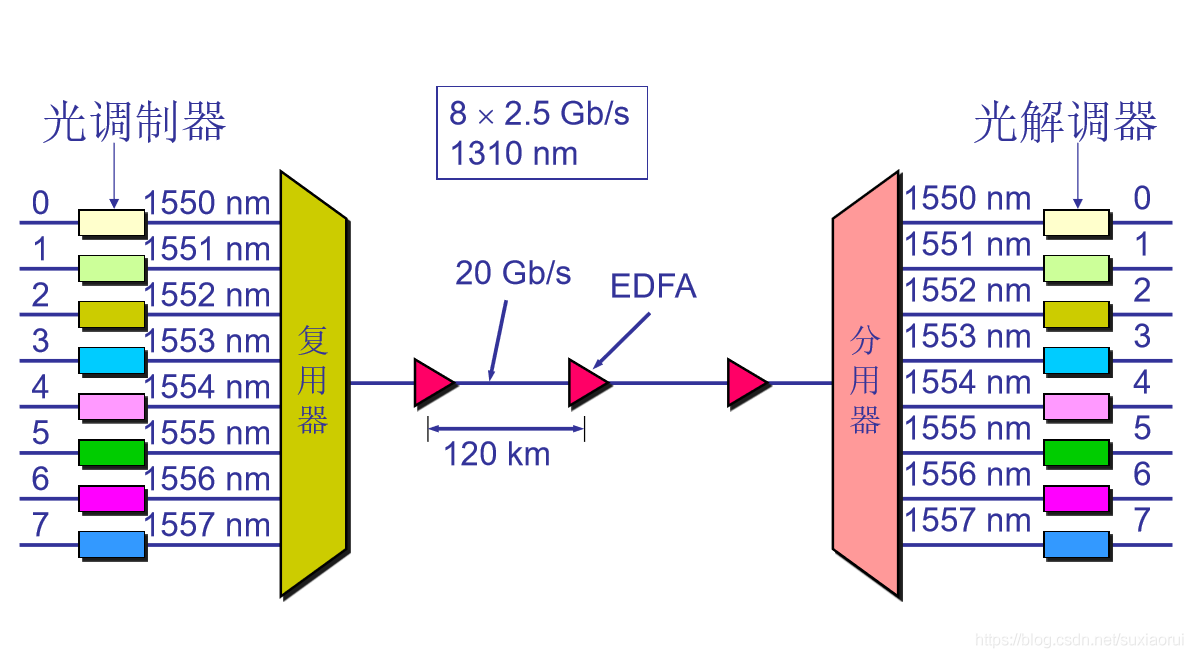
* 1. 时分多路复用( time division multiplexing-TDM )

采用分时技术，把传输线路的可用时间分成若干个时间片。此种复用方法不适用于传输语音信号（模拟信号），仅适用于传输数字信号。



* 1. 波分多路复用(Wavelength division multiplexing-WDM)

光的频分复用



* 1. 码分多路复用( Code division multiplexing-CDM ) 波分多路复用WDM

允许使用整个频段来发送信号，而且没有任何时间限制。在CDMA中，每个比特被细分为m个更短的时间间隔，这些时间间隔称为码片。通常每个比特被分为64个或者128个。

每个用户分配得到一个码片序列，且这些码片序列两两正交，归一化内积为零。

当一个主机要发送“1”时，就发送属于该主机的码片，当要发送“0”时，就发送码片的反码。接收方只要计算复用信号和发送方的码片的归一化内积就能够知道发生方发送了什么。

## 10.3.6广域网协议

1. 点对点协议 PPP

点对点协议主要用于“拨号上网”这种广域连接模式。它的优点在于简单、具备用户验证能力、可以解决IP分配等。它主要通过拨号或专线方式建立点对点连接发送数据，使其成为各种主机、网桥和路由器之间简单连接的一种共通的解决方案。

家庭拨号上网就是通过PPP在用户端和运营商的接入服务器之间建立通信链路。典型的应用是在ADSL（Asymmetrical Digital Subscriber Line，非对称数据用户线）接入方式当中，PPP与其他的协议共同派生出了符合宽带接入要求的新的协议，如PPPoE和PPPoA。

利用以太网（Ethernet）资源，在以太网上运行PPP来进行用户认证接入的方式称为PPPoE。PPPoE既保护了用户方的以太网资源，又完成了ADSL的接入要求，是目前ADSL接入方式中应用最广泛的技术标准。同样，在ATM网络上运行PPP来管理用户认证的方式称为PPPoA。

1. 数据用户线 xDSL

xDSL是各种数字用户线的统称，根据各种宽带通信业务需要，目前还有DSL技术和产品，如ADSL（Asymmetric DSL，不对称数字用户线）、SDSL（Single pair DSL，单对线数字用户环路）、IDSL（ISDN DSL，ISDN用的数字用户线）、RADSL（Rate adaptive DSL，速率自适应非对称型数字用户线）和VDSL（Very high Bit rate DSL，甚高速数字用户线）等。

ADSL是研制最早，发展较快的一种。它是在一对铜双绞线上为用户提供上、下行非对称的传输速率（即带宽）。ADSL接入服务能做到较高的性能价格比，ADSL接入技术较其他接入技术具有其独特的技术优势：它的速率可达到上行1兆／下行8兆，速度非常快。它把线路按频段分成语音、上行和下行三个信道，故语音和数据可共用1对线。

1. 数字专线

数字数据网（Digital Data Network, DDN）是采用数字传输信道传输数据信号的通信网，可提供点对点、点对多点透明传输的数据专线出租电路，为用户传输数据、图像和声音等信息。数字数据网是以光纤为中继干线网络，组成DDN的基本单位是节点，节点间通过光纤连接，构成网状的拓扑结构。户做资料传输使用后，它们就变成用户的专线，直接进入电信的DDN网络，因为这种电路是采用固定连接的方式，不需经过交换机房，所以称之为固定DDN专线。

1. 帧中继

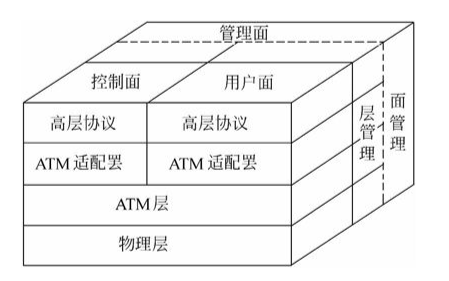
帧中继（Frame Relay, FR）是在用户网络接口之间提供用户信息流的双向传送，并保持顺序不变的一种承载业务。用户信息以帧为单位进行传输，并对用户信息流进行统计复用。帧中继是综合业务数字网标准化过程中产生的一种重要技术，它是在数字光纤传输线路逐渐代替原有的模拟线路，用户终端智能化的情况下，由X25分组交换技术发展起来的一种传输技术。

1. 异步传输模式ATM

异步传输模式（Asynchronous Transfer Mode, ATM）是B-ISDN的关键核心技术，它是一种面向分组的快速分组交换模式，使用了异步时分复用技术，将信息流分割成固定长度的信元。

1. ATM的分层

ATM的参考模型由4层构成，分别是用户层、ATM适配层、ATM层和物理层：

****

1. 用户层

由用户平面、控制平面和管理平面组成。

1. 用户平面。指用户要求的应用、协议及服务。如通常的数据协议、语音和视频应用等。
2. 控制平面。包含连接建立、维护和拆除等有关功能。
3. 管理平面。负责层次和平面的协调，通过层次管理支持用户平面和管理平面。
4. ATM适配层

负责将用户层的信息转换成ATM网络可用的格式。等用户层把较长的数据分组交给ATM适配层后，ATM适配层按规定的长度将数据分成若干信元体，再传给ATM层。

1. ATM层

基本功能是负责生成信元，它不管信元体的内容，只为信元体生成信元头并附给信元体，以形成标准的信元格式。跨越ATM层到物理层的信息单元只能是53个字节的信元。

1. 物理层

负责对信元进行编码，并将其交给物理介质。它汇集了各种被认可的物理线路协议，如SDH（STM-1、STM-4、STM-16）和同步光纤网等。

1. ATM连接类型

ATM连接有两种类型，即永久虚电路（PVC）和交换虚电路（SVC）。

永久虚电路：其连接由管理员建立和拆除。

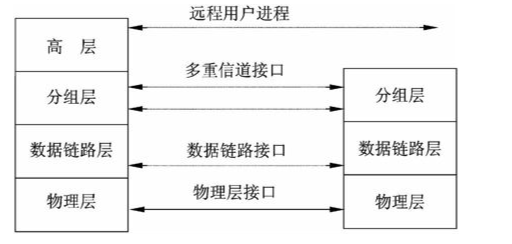
交换虚电路：通过终端系统和ATM网络以及ATM网络内部的信令协议的操作来建立和拆除。

1. 优缺点：

ATM技术适用的范围为多媒体和视频应用；适合构架骨干网；无缝地集成广域网和局域网。ATM的主要缺点是成本较高，不适合于小网络。

1. X.25协议

X.25在本地DTE和远程DTE之间提供一个全双工、同步的透明信道，并定义了三个相互独立的控制层：物理层、数据链路层和分组层，它们分别对应于ISO/OSI的物理层、链路层和网络层，如图5-12所示。

****

X.25是在公用数据网上，以分组方式进行操作的DTE（数据终端设备）和DCE（数据通信设备）之间的接口。X.25只是对公用分组交换网络的接口规范说明，并不涉及网络内部实现，它是面向连接的，支持交换式虚电路和永久虚电路。

## 10.3.7TCP/IP协议簇

* 1. 特性
  2. 逻辑编址:

每一块网卡在出厂时就由厂家分配了一个独一无二的永久性的物理地址。在Internet中，为每台连入因特网的计算机分配一个逻辑地址，这个逻辑地址被称为IP地址。

* 1. 路由选择:

在TCP/IP中包含了专门用于定义路由器如何选择网络路径的协议，即IP数据包的路由选择。

* 1. 域名解析:

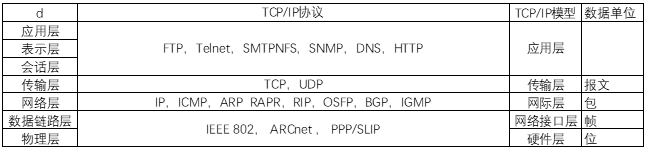
将域名映射为IP地址的操作，称为域名解析。域名具有较稳定的特点，而IP地址则较易发生变化。

* 1. 错误检测与流量控制

TCP/IP具有分组交换确保数据信息在网络上可靠传递的特性，这些特性包括检测数据信息的传输错误（保证到达目的地的数据信息没有发生变化），确认已传递的数据信息已被成功地接收，监测网络系统中的信息流量，防止出现网络拥塞。

* 1. TCP/IP分层模型

TCP/IP分层模型由4个层次构成，即应用层、传输层、网际层和网络接口层



TCP/IP协议(Transfer Controln Protocol/Internet Protocol)叫做传输控制/网际协议，又叫网络通讯协议，TCP/IP实际上是一组协议。

* 1. 应用层：

应用层处在分层模型的最高层，用户调用应用程序来访问TCP/IP互联网络，以享受网络上提供的各种服务。应用程序负责发送和接收数据。

* 1. 传输层：

传输层的基本任务是提供应用程序之间的通信服务。这种通信又叫端到端的通信。传输层既要系统地管理数据信息的流动，还要提供可靠的传输服务，以确保数据准确而有序地到达目的地。

* 1. 网际层：

网际层又称IP层，主要处理机器之间的通信问题。它接收传输层请求，传送某个具有目的地址信息的分组。

该层主要功能：

* 1. 把分组封装到IP数据报（IP Datagram）中，填入数据报的首部（也称为报头），使用路由算法选择把数据报直接送到目标机或把数据报发送给路由器，然后再把数据报交给下面的网络接口层中对应的网络接口模块。
  2. 处理接收到的数据报，检验其正确性。使用路由算法来决定是在本地进行处理，还是继续向前发送。
  3. 适时发出ICMP的差错和控制报文，并处理收到的ICMP报文。
  4. 网络接口层：

网络接口层又称数据链路层，处于TCP/IP协议层之下，负责接收IP数据报，并把数据报通过选定的网络发送出去。

* 1. 网络接口协议

TCP/IP协议不包含具体的物理层和数据链路层，只定义了网络接口层作为物理层与网络层的接口规范。这个物理层可以是广域网，也可以是局域网。任何物理网络只要按照这个接口规范开发网络接口驱动程序，都能够与TCP/IP协议集成起来。

* 1. 网际层协议 IP

TCP/IP协议簇的重点。IP所提供的服务通常被认为是无连接的（connectionless）和不可靠的（unreliable），是一种尽力传送的通信协议，即传送的数据报可能丢失、重复、延迟或乱序，把差错检测和流量控制之类的服务授权给了其他的各层协议。

什么是无连接：

无连接是指没有确定目标系统在已做好接收数据准备之前就发送数据。

IP的主要功能包括将上层数据（如TCP、UDP数据）或同层的其他数据（如ICMP数据）封装到IP数据报中；将IP数据报传送到最终目的地；为了使数据能够在链路层上进行传输，对数据进行分段；确定数据报到达其他网络中的目的地的路径。

工作过程：

* 1. 当发送数据时，源计算机上的IP协议软件必须确定目的地是在同一个网络上，还是在另一个网络上。如果目的地在本地，那么IP协议软件就启动直达通信；如果目的地是远程计算机，那么IP必须通过网关（或路由器）进行通信，在大多数情况下，这个网关应当是默认网关。当源IP完成了数据报的准备工作时，它就将数据报传递给网络访问层，网络访问层再将数据报传送给传输介质，最终完成数据帧发往目的计算机的过程。
  2. 当数据抵达目的计算机时，网络访问层首先接收该数据。网络访问层要检查数据帧有无错误，并将数据帧送往正确的物理地址。假如数据帧到达目的地时正确无误，网络访问层便从数据帧的其余部分中提取数据有效负载（Payload），然后将它一直传送到帧层次类型域指定的协议。在这种情况下，可以说数据有效负载已经传递给了IP。
  3. ARP和RARP

地址解析协议（Address Resolution Protocol, ARP）及反地址解析协议（RARP）是驻留在网际层中的另一个重要协议。数据传输过程中，必须对IP地址与物理地址进行相互转换，ARP的作用是将IP地址转换为物理地址，RARP的作用是将物理地址转换为IP地址。

IP到ARP转换过程：

当计算机需要与任何其他的计算机进行通信时，首先需要查询ARP高速缓存，如果ARP高速缓存中这个IP地址存在，便使用与它对应的物理地址，直接将数据报发送给所需的物理网卡；如果ARP高速缓存中没有该IP地址，那么ARP便在局域网上以广播方式发送一个ARP请求包。如果局域网上IP地址与某台计算机中的IP地址相一致，那么该计算机便生成一个ARP应答信息，信息中包含对应的物理地址。ARP协议软件将IP地址与物理地址的组合添加到它的高速缓存中，这时即可开始数据通信。

* 1. 网际层协议ICMP

Internet控制信息协议（Internet Control Message Protocol, ICMP），工作在网际层，一个专门用于发送差错报文的协议。ICMP定义了5种差错报文（源抑制、超时、目的不可达、重定向和要求分段）和4种信息报文（回应请求、回应应答、地址屏蔽码请求和地址屏蔽码应答）。

IP在需要发送一个差错报文时要使用ICMP，而ICMP也是利用IP来传送报文的。ICMP是让IP更加稳固、有效的一种协议，它使得IP传送机制变得更加可靠。而且利用ICMP还可以用于测试因特网，以得到一些有用的网络维护和排错的信息。

* 1. 传输层协议TCP

TCP（Transmission Control Protocol，传输控制协议），是整个TCP/IP协议族中最重要的协议之一。它在IP提供的不可靠数据服务的基础上，为应用程序提供了一个可靠的、面向连接的、全双工的数据传输服务。

* 1. 实现可靠性的原理：

在TCP传输过程中，发送方启动一个定时器，然后将数据包发出，当接收方收到了这个信息就给发送方一个确认（acknowledgement）信息。而如果发送方在定时器到点之前没收到这个确认信息，就重新发送这个数据包。

* 1. TCP三次握手：

源主机和目的主机之间建立和关闭连接操作时，均需要通过三次握手来确认建立和关闭是否成功。

* 1. 源主机发送一个SYN=1的TCP数据包，表示想与目标主机进行通信，并设定该数据包的同步序列号进行同步，如设置SEQ=200，即发送一个SYN=1，ACK=0，SEQ=200的TCP数据包。
  2. 目标主机愿意进行通信，则响应一个确认，并以下一个序列号为参考进行确认。即发送一个SYN=1，ACK=201，SEQ=100的TCP数据包。
  3. 源主机接收目标主机的TCP包，并发出一个包进行确认，这个确认中包括它想要接收的下一个序列号，即SYN=0，SEQ=201，ACK=101。至此连接建立完成。

三次握手建立连接是一个同步过程，交换初始序列号，保证后续的每一个字节的可靠传输。

TCP 连 接 的 建 立 
一 z 
Host2 
连 接 请 求 数 据 段 
这 是 第 一 次 握 手 
SYN=I ， ACK=I 
这 是 第 二 次 握 手 
二 一 
后 的 确 认 

* 1. 传输层协议UDP

用户数据报协议（User Datagram Protocol, UDP）是一种不可靠的、无连接的协议，可以保证应用程序进程间的通信。与同样处在传输层的面向连接的TCP相比较，UDP是一种无连接的协议，它的错误检测功能要弱得多。

UDP协议软件的主要作用就是将UDP消息展示给应用层，它并不负责重新发送丢失的或出错的数据消息，不对接收到的无序IP数据报重新排序，不消除重复的IP数据报，不对已收到数据报进行确认，也不负责建立或终止连接。

UDP与TCP的区别：

* 1. TCP有助于提供可靠性，这在网络不可靠的时候，通过牺牲一些时间换来达到网络的可靠；UDP则有助于提高传输的高速率性，但不保障可靠性；
  2. TCP是面向连接的传输协议；UDP是无连接的传输协议。
  3. TCP头部开销大；UDP头部开销小。
  4. TCP仅支持单播传输；UDP 提供了单播，多播，广播的功能。
  5. TCP提供拥塞控制，当网络出现拥塞的时候，TCP能够减小向网络注入数据的速率和数量，缓解拥塞；UDP没有拥塞控制。
  6. TCP面向字节流传输，在不保留报文边界的情况下以字节流方式进行传输；UDP面向报文传输，对应用层交下来的报文，既不合并，也不拆分，而是保留这些报文的边界。
  7. TCP适用于要求可靠传输的应用；UDP。适用于实时应用。
  8. 应用层协议

为了让不同平台的计算机能够通过计算机网络获得一些基本的、相同的服务，也就应运而生了一系列应用级的标准，实现这些应用标准的专用协议被称为应用级协议，相对于OSI参考模型来说，它们处于较高的层次结构，所以也称为高层协议。

# 10.4 Internet及应用

## 10.4.1概述

* 1. 从用户的角度来看，整个Internet在逻辑上是统一的、独立的，在物理上则由不同的网络互连而成。
  2. 从技术角度看，Internet本身不是某一种具体的物理网络技术，它是能够互相传递信息的众多网络的一个统称，或者说它是一个网间网，只要人们进入了这个互联网，就是在使用Internet。
  3. 连入Internet的计算机网络种类繁多，形式各异，且分布在世界各地，因此，需要通过路由器（IP网关）并借助各种通信线路或公共通信网络把它们连接起来。
  4. 在Internet中，分布着一些覆盖范围很广的大网络，这种网络称为“Internet主干网”，它们一般属于国家级的广域网。主干网一般只延伸到一些大城市或重要地方，在那里设立主干网节点。每一个主干网节点可以通过路由器将广域网与局域网联接起来，一个节点还可以通过另外的路由器与其他局域网再互连，由此形成一种网状结构。

## 10.4.1Internet地址

Internet地址能唯一确定Internet上每一台计算机、每个用户的位置。Internet地址格式主要有两种书写形式：域名格式和IP地址格式。

* 1. 域名

域名（Domain Name）通常是用户所在的主机名字或地址。

域名格式是由若干部分组成，每个部分又称子域名，它们之间用“.”分开，每个部分最少由两个字母或数字组成。域名通常按分层结构来构造，每个子域名都有其特定的含义。通常情况，一个完整、通用的层次型主机域名由如下4部分组成：

计算机主机名．本地名．组名．最高层域名

从右到左，子域名分别表示不同的国家或地区的名称（只有美国可以省略表示国家的顶级域名）、组织类型、组织名称、分组织名称和计算机名称等。域名地址的最后一部分子域名称为高层域名（或顶级域名），它大致上可以分成两类：一类是组织性顶级域名；另一类是地理性顶级域名。

例如：

[www.dzkjdx.edu.cn](http://www.dzkjdx.edu.cn)　cn是地理性顶级域名，表示“中国”。

[www.263.net](http://www.263.net)　net是组织性顶级域名，表示“网络技术组织机构”。

如果一个主机所在的网络级别较高，它可能拥有的域名仅三部分：本地名．组名．最高层域名。现在，Internet地址管理机构（Internet PCA Registration Authority, IPRA）和（Internet Assigned Number Authority, IANA）负责Internet最高层域名的登记和管理。

* 1. IPv4地址

Internet中的主机地址是用IP地址来唯一标识的。每个IP地址都由4个小于256的数字组成，数字之间用“.”分开。Internet的IP地址共有32位，4个字节。它表示时有两种格式：二进制格式和十进制格式（点分十进制）。二进制格式是计算机所认识的格式，十进制格式是由二进制格式“翻译”过去的，主要是为了便于使用和掌握。

一般情况下域名和IP地址是一一对应的，域名易于记忆，便于使用，因此得到比较普遍的使用。当用户和Internet上的某台计算机交换信息时，只需要使用域名，网络则会通过访问DNS服务器自动地将其转换成IP地址，找到该台计算机。一个域名对应多个IP地址的时候，智能DNS服务器会根据请求的线路、地理位置等信息综合考虑，返回对于该请求最快的IP。

IPv4地址分为5类：A类、B类、C类、D类和E类

01 
012 
10 
0123 
110 
01234 
1110 
01234 
78 
16 
15 16 
(14) 
(21) 
24 
(24) 
24 
(16) 
24 
24 
(28) 
24 
(28) 
31 
31 
31 
31 
31 

* 1. A类:

A类网络地址占有1个字节（8位），定义最高位为0来标识此类地址，余下7位为真正的网络地址，后面的3个字节（24位）为主机地址，A类全部地址有（27-2）×（224-2）个。A类网络地址范围：0.0.0.0-127.255.255.255。

* 1. B类:

B类网络地址占有2个字节，使用最高两位为10来标识此类地址，其余14位为真正的网络地址，主机地址占后面的2个字节（16位），所以B类全部的地址有（214－2）×（216－2）＝16382×65534个。B类网络地址范围：128.0.0.0-191.255.255.255。

* 1. C类:

它是最通用的Internet地址，C类网络地址占有3个字节，使用最高三位为110来标识此类地址，其余21位为真正的网络地址，主机地址占最后1个字节，C类地址有（221－2）×（28-2）个，C类网络地址范围：192.0.0.0-233.255.255.255。

* 1. D类:

组播地址，保留。D类地址是相当新的。它的识别头是1110，用于组播，例如用于路由器修改。D类网络地址范围：224.0.0.0-239.255.255.255。

* 1. E类:

E类地址为实验保留，其识别头是1111。E类网络地址范围：240.0.0.0-247.255.255.255

* 1. IPv4特殊地址：
     1. 直接广播地址：

在A,B,C类地址中，主机号全为1的地址为广播地址。它是用来使路由器将一个分组以广播的方式发送给特定网络上的所有主机，例如地址：192.168.1.255。

* 1. 受限广播地址（32位全1地址）：

又叫做“泛洪广播地址”32全为1的地址为受限地址，用来将一个分组以广播的方式发送给本网络中所有主机，路由器则阻挡该分组通过，将其广播功能限制在本网内部。该地址原来表示互联网上所有的主机，后来退化成受限广播地址。

* 1. “这个网络上的特定主机”地址：

当一个主机或一个路由器向本地网络的某个特定的主机发送一个分组，那么他需要使用“这个网络上的特定主机”地址。该地址的网络好全为0，主机号为确定的值。这样的分组被限制在本网内部，由主机号对应的主机接受。例如向本网络主机201.161.20.18，需要使用地址：0.0.0.18。

* 1. 回送地址：

回送地址又称为环回地址，本地回环地址，Lookback Network。127.0.0.0

A类地址中的127.0.0.1-127.255.255.254都是环回地址，效果相同，用于网络软件测试和本地进程间通信。

TCP/IP规定：

含网络号为127的分组不能出现在任何网络上；主机和路由器不能为该地址广播任何寻址信息。

* 1. 网络地址：

IP地址中主机位全为0的地址为网络地址，用该地址表示这个网络。

* 1. 广播地址：

IP地址中主机位全为1的地址为广播地址，用来向该网络中的所有主机发送信息。

网 络 地 址 ： 
一 网 络 部 分 一 主 机 部 分 一 
1 2 3 4 5 6 7 8 9 11 瞠 13 14 巧 16 17 四 差 四 川 四 31 
i 攫 0 磊 磊 到 的 湖 的 0 思 盟 溯 0000000000000000000 
广 播 地 址 ： 
1 2 3 4 5 6 7 8 9 加 11 瞠 13 14 巧 16 17 四 差 川 四 31 
柒 0 到 到 的 0 000 能 总 思 0000000000000000 

* 1. 全零地址：0.0.0.0

表示这个主机，这个网络。当作路由表中默认路由的目的地址。

* 1. 169.254.0.0非正常地址：

在主机启用了DHCP，但是没有DHCP Server为它分配地址，回默认配置一个169.254.0.0的地址。

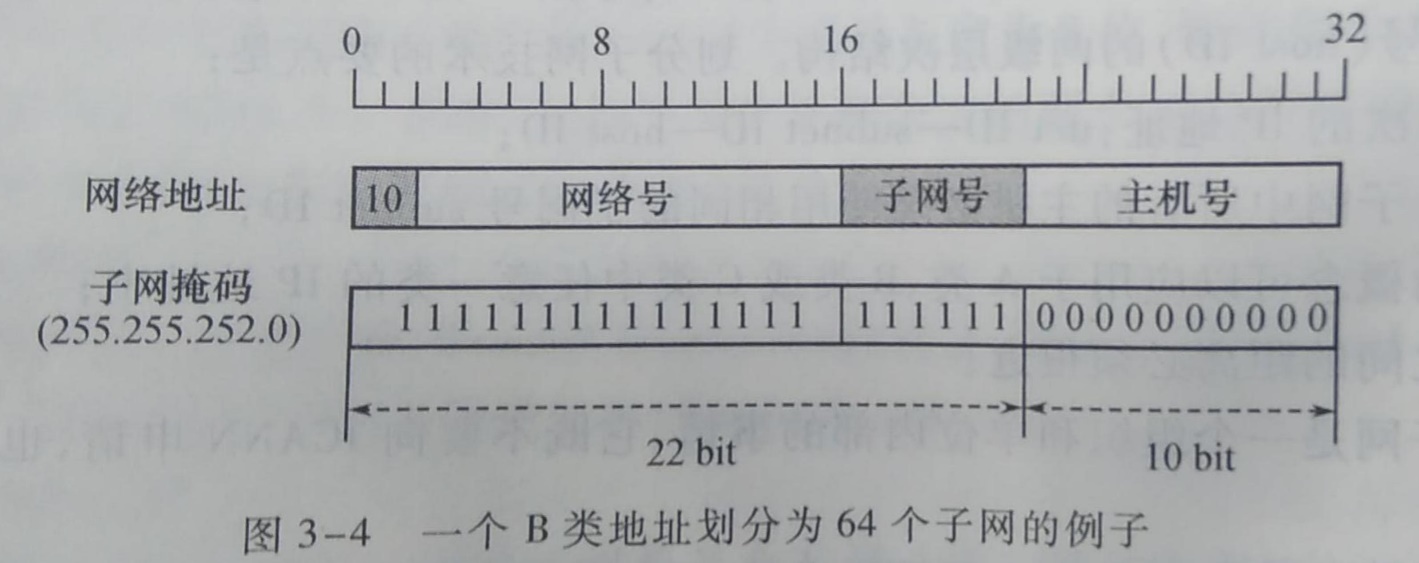
* 1. 子网：

标准分类的IP地址存在两个主要问题：IP地址的有效利用率问题和路由器的工作效率问题。为此人们提出了子网的概念。其基本思想是：允许将网络划分成多个部分供内部使用，但是对于外部网络仍然像象一个网络一样。子网划分有利于优化网络性能，改善网络管理。

* 1. 划分子网的地址结构：
     1. 三级层次结构：net -ID-subnet ID-host ID，而在标准分类中是：net ID-hostID。实际上，三层结构中的子网号subnet ID是从标准分类中的主机号host ID中划分出来的。
     2. 同一个子网中的所有主机必须使用相同的子网号subnetID。
     3. 子网的概念可以应用于A类，B类和C类中任意一类地址中。
     4. 子网之间的距离必须非常近。
     5. 分配子网是一个组织内部的事情，不需要向ICANN申请。
  2. 网络掩码：

又叫子网掩码，当三层次地址提出后需要解决一个问题：如何从一个IP地址中提取出子网号，或者说如何知道这个IP地址的网络号和主机号。

子网掩码的长度和IPv4地址的长度一样，都是32位，子网掩码中用1表示网络位，1的个数代表网络位的长度，用0表示主机位，0的个数代表主机位的长度，很容易理解所有的1都在地址的左边，0都在地址的右边。例如：



A类网络默认子网掩码：255.0.0.0

B类网络默认子网掩码：255.255.0.0

C类网络默认子网掩码：255.255.255.0

* 1. 网络掩码的两种：

点分十进制法：255.255.255.0

/表示法：/24

* 1. 全局IP地址和专用IP地址：

使用IP地址的情况可分为两种：一种是将网络直接连接到Internet，另一种是需要使用TCP/IP协议的内部网络。主机直接连接Internet网络需要使用全局IP地址，全局IP地址是分组在Internet上传输时使用的地址。专用IP地址只能用于一个公司或组织内部网络，而不能用于Internet上，路由器不会将专用IP地址转发到Internet上，专有地址又被称为私有地址。

异同：

* 1. 使用全局地址需要申请，使用专用地址不需要申请。
  2. 全局地址必须保证Internet上的唯一性，专用IP地址在某一个网络内部是唯一的，在不同的网络中可以相同。

专用地址分类：

A类：10.0.0.0-10.255.255.255，掩码/8，255.0.0.0

B类：172.16.0.0-172.31.255.255，掩码/16，255.255.0.0

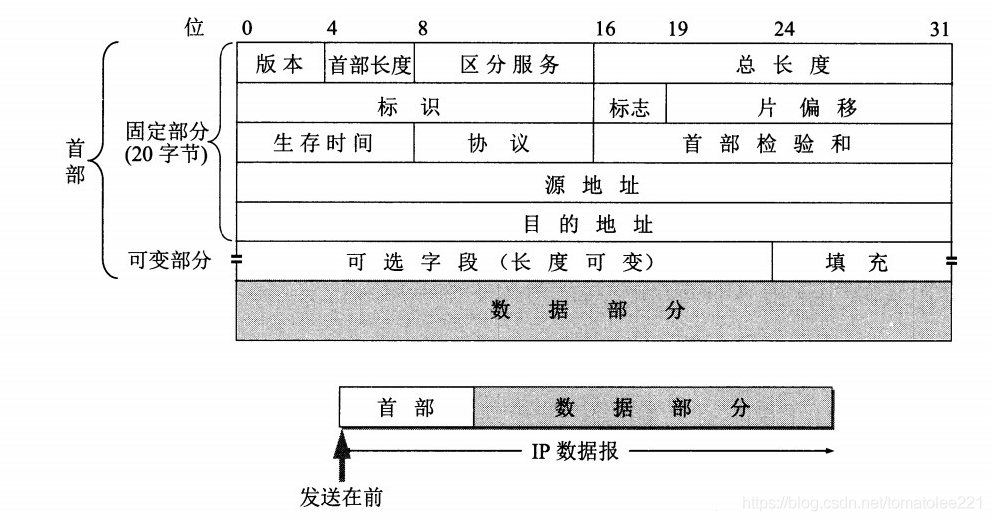
C类：192.168.0.0-192.168.255.255，掩码/24，255.255.255.0

* 1. 全零全幺的含义：

在主机位中，主机位全为 1 的IP地址代表这个网络内部的广播地址，主机位全为 0 的IP地址代表这个网络。因为这两个全为1或全为0的地址的特性用途，所以任何主机都不能分配到这两个地址。

子网号全0或者全1要看网络设备所使用的路由器协议支持不支持，很多有关IP规划的题目中会让你计算出合法的网段数，这个时候要排除全0以及全1子网。

* 1. IPv4数据包的格式：



* 1. 版本(Version)：

该字段长度为4比特位。标识IP报头的版本和格式，IPv4数据包的该字段设置为：0100。

* 1. 首部长度(IHL)：又称为报头长度

该字段长度为4比特位。它标识报头的总长度，以32比特位为一个单位，在IPv4中头部被限制为最多15个32位字。有效报头的最小值为5，即0101。

* 1. 区分服务(Type of Service)：又称为服务类型

表示分组的传输优先级，但是在目前互联网中基本没用。该字段长度为8比特位，被分为俩个部分，前6位被称为区分服务字段—DS字段，后2位是显示拥塞通知字段—ECN字段，用于QS。

* 1. 总长度(Total Length)：又称为数据包总长度

该字段长度为16比特位。它标识数据报和数据包的总长度，单位为字节，所以ipv4的数据最大为65535。

* 1. 标识(Identification)：又称为数据报识别号

该字段长度为16比特位。它标识分段所属的组，所属为同一组则标识符相同。在网络层中也可把流量区分开来，用于流量分片。

* 1. 标记(Flags)：

该字段长度为3比特位。它分为三分部分，保留位（reserved bit）为0；分片位（Don`t fragent）当为1时标识未分片，0则标识被分片；更多位（more fragments)为0标识最后分段，为1标识更多分段。

* 1. 分段偏移(Fragment Offset)：又叫做分片偏移

该字段长度为13位比特位。用来重排序，它标识分段在当前数据包的位置，单位为字节。

* 1. 生存时间(Time to Live，TTL):

该字段长度为8比特位。在网络中标识数据包最大存活时间，用来防止路由环路，每经过一台路由器则TTL字段减去1，直到为0，此数据包直接被丢弃。其值最大为255，单位为s。然而现在路由器转发数据包都是用跳数来作为衡量单位。

* 1. 协议(Protocol):

该字段长度为8比特位。它用来标识上层协议（0—255），6表示TCP协议，17表示UDP协议。

* 1. 报头校验和(Header Checksum):

该字段长度为16比特位。 这个16位字段只对首部查错，不包括数据部分。在每一跳，路由器都要重新计算出的首部检验和并与此字段进行比对，如果不一致，此报文将会被丢弃。重新计算的必要性是因为每一跳的一些首部字段（如TTL、Flag、Offset等）都有可能发生变化，不检查数据部分是为了减少工作量。数据区的错误留待上层协议处理——（UDP）和（TCP）都有检验和字段。此处的检验计算方法不使用CRC。

* 1. 源地址(Source address): 该字段长度为32比特位。它标识发送者的IP地址。
  2. 目的地址(Destination address): 该字段长度为32比特位。它标识接受者的IP地址。
  3. 选项(options):

该字段长度可变，很少被使用。该字段提供某些控制功能，但在大部分情况下不需要这些功能。里面包括机制有松散路由，严格路由，路由记录及时间戳。

* 1. 填充(padding): 通过options字段后面补充0来补齐32位比特位，padding的和位0或者是32的倍数。

<https://blog.csdn.net/tomatolee221/article/details/82985440>

* 1. NAT技术(Network Address Translators)

因特网面临IP地址短缺的问题。解决这个问题有所谓长期的或短期的两种解决方案：

* 1. 长期的解决方案就是使用具有更大地址空间的IPv6协议。
  2. 短期方案时使用网络地址翻译（Network Address Translators, NAT）。

NAT技术最初提出的建议是在子网内部使用局部地址，而在子网外部使用少量的全局地址，通过路由器进行内部和外部地址的转换。NAT是一种快速的IP地址耗尽修补方案。NAT的实现主要有两种形式:

* 1. 动态地址翻译（Dynamic Address Translation）

为此，首先引入存根域的概念，所谓存根域（Stub Domain），就是内部网络的抽象，这样的网络只处理源和目标都在子网内部的通信。任何时候存根域内只有一部分主机要与外界通信，甚至还有许多主机可能从不与外界通信，所以整个存根域只需共享少量的全局IP地址。存根域有一个边界路由器，由它来处理域内与外部的通信。假定：

* + 1. m：需要翻译的内部地址数。
    2. n：可用的全局地址数（NAT地址）。

当m∶n翻译满足条件（m≥1 and m≥n）时，可以把一个大的地址空间映像到一个小的地址空间。所有NAT地址放在一个缓冲区中，并在存根域的边界路由器中建立一个局部地址和全局地址的动态映像表，如图：

SRC 138.201.148.32 
SRC 138.201.148.151 
DST 138.201.148.151 : 
138.201.148.32 
138.201.148.151 
*NAT 
NATIP 
178.201.112.34 
178.201.112.11 
SRC 178.201.112.34 
SRC 178.201.112.11 
DST 178.201.112.11 
SRC "UtUhl: 
DST: Flbid1Ui1E 

这个图显示的是把所有B类网络138.201中的IP地址翻译成C类网络178.201.112中的IP地址。

特点：

* 1. 只要缓冲区中存在尚未使用的C类地址，任何从内向外的连接请求都可以得到响应，并且在边界路由器的动态NAT表中为之建立一个映像表项。
  2. 如果内部主机的映像存在，就可以利用它建立连接。
  3. 从外部访问内部主机是有条件的，即动态NAT表中必须存在该主机的映像。
  4. 网络地址和端口翻译（Network Address Port Translation, NAPT）

这种特殊的NAT应用是m∶1翻译，也叫做伪装（masquerading），因为用一个路由器的IP地址可以把子网中所有主机的IP地址都隐藏起来。如果子网中有多个主机要同时通信，那么还要对端口号进行翻译，所以这种技术更经常被称为网络地址和端口翻译。在很多NAPT实现中，专门保留一部分端口号给伪装使用，叫做伪装端口号。如图：

SRC 138.201.148.32 :1275 
DST 193.46.94.1 15:80 
SRC 138.201.160.201:4192 
DST 53.12.198.15:23 
SRC 195.112.12.161:63451 
NAT _ 
DST 193.46.94.115:80 
NAT 
SRC195.112.12.161 :63452 
DST53.12.198.15:23 
NAT 
NAT NCI 
138.201.148.32:1275 
138.201.160.201 :4192 
SRC: 
63451 
DST: HbJUÜl: 
63452 

该图显示了对端口号进行翻译，从而隐藏了内部网络138.201中的所有主机。

特点：

* 1. 出口分组的源地址被路由器的外部IP地址所代替，出口分组的源端口号被一个未使用的伪装端口号所代替。
  2. 如果进来的分组的目标地址是本地路由器的IP地址，而目标端口号是路由器的伪装端口号，则NAT路由器就检查该分组是否为当前的一个伪装会话，并试图通过它的伪装表对IP地址和端口号进行翻译。
  3. 伪装技术可以作为一种安全手段使用，借以限制外部对内部主机的访问。另外，还可以用这种技术实现虚拟主机和虚拟路由，以便达到负载均衡和提高可靠性的目的。
  4. NAT的缺点：
     1. 打破了IP地址的唯一性。
     2. 破坏了IP网络的无连接特性，NAT转换器维持着网络连接状态。
     3. 违背了基本的协议分层原则。
     4. 如果传输层不是采用TCP或UDP，NAT将不能正常工作。
     5. NAT让一个共有IP地址可以承载6144（65535-4096）个私人地址，严重超载。
  5. IPv6
  6. IPv4地址不足问题的描述：

IPv4（IP version 4）标准是20世纪70年代末期制定完成的。20世纪90年代初期，WWW的应用导致因特网爆炸性发展，随着因特网应用类型日趋复杂，终端形式特别是移动终端的多样化，全球独立IP地址的提供已经开始面临沉重的压力。IPv4将不能满足因特网长期发展的需要，必须立即开始下一代IP网络协议的研究。由此，IETF于1992年成立了IPNG（IP Next Generation）工作组；1994年夏，IPNG工作组提出了下一代IP网络协议（IP version 6, IPv6）的推荐版本；1995年夏，IPNG工作组完成了IPv6的协议文本；1995年—1999年完成了IETF要求的协议审定和测试；1999年成立了IPv6论坛，开始正式分配IPv6地址，IPv6的协议文本成为标准草案。

由于IPv4地址是32位二进制，所能表示的IP地址个数为232＝4294967296≈40亿个，因而在因特网上约有40亿个IP地址。由32位的IPv4升级至128位的IPv6，因特网中的IP地址从理论上讲会有2128 ＝3.4×1038 个，可以为地球上的每一粒沙子分配一个IPv6地址，在想象得到的将来，IPv6的地址空间是不可能用完的。除此之外，IPv6还采用分级地址模式、高效IP包首部、服务质量、主机地址自动配置、认证和加密等许多技术。

* 1. IPv6数据包的格式：

IPv6数据包有一个40字节的基本首部（base header），其后可允许有0个或多个扩展首部（extension header），再后面是数据。每个IPv6数据包都是从基本首部开始。IPv6基本首部的很多字段可以和IPv4首部中的字段直接对应。

0 
4 
16 
] 2 
24 
31 
版 本 号 通 信 类 型 
流 标 号 
字 节 的 基 本 首 部 
净 负 荷 长 度 
下 一 个 首 部 跳 数 限 制 
128 位 源 地 址 
128 位 目 的 地 址 
4 个 字 节 

* 1. 版本号：该字段占4位，说明了IP协议的版本。对IPv6而言，该字段值是0110，也就是十进制数的6。
  2. 通信类型：

该字段占8位，其中优先级字段占4位，使源站能够指明数据包的流类型。首先，IPv6把流分成两大类，即可进行拥塞控制的和不可进行拥塞控制的。每一类又分为8个优先级。优先级的值越大，表明该分组越重要。对于可进行拥塞控制的业务，其优先级为0～7。当发生拥塞时，这类数据包的传输速率可以放慢。对于不可进行拥塞控制的业务，其优先级为8～15。这些都是实时性业务，如音频或视频业务的传输。这种业务的数据包发送速率是恒定的，即使丢掉了一些，也不进行重发。

* 1. 流标号：

该字段占20位。所谓流，就是因特网上从一个特定源站到一个特定目的站（单播或多播）的一系列数据包。所有属于同一个流的数据包都具有同样的流标号。源站在建立流时是在224－1个流标号中随机选择一个流标号。流标号0保留作为指出没有采用流标号。源站随机地选择流标号并不会在计算机之间产生冲突，因为路由器在将一个特定的流与一个数据包相关联时，使用的是数据包的源地址和流标号的组合。

从一个源站发出的具有相同非0流标号的所有数据包，都必须具有相同的源地址和目的地址，以及相同的逐跳选项首部（若此首部存在）和路由选择首部（若此首部存在）。这样做的好处是当路由器处理数据包时，只要查一下流标号即可，而不必查看数据包首部中的其他内容。任何一个流标号都不具有特定的意义，源站应将它希望各路由器对其数据包进行的特殊处理写明在数据包的扩展首部中。

* 1. 净负荷长度（payload length）：

该字段占16位，指明除首部自身的长度外，IPv6数据包所载的字节数。可见，一个IPv6数据包可容纳64K字节长的数据。由于IPv6的首部长度是固定的，因此没有必要像IPv4那样指明数据包的总长度（首部与数据部分之和）。

* 1. 下一个首部（next header）：

该字段占8位，标识紧接着IPv6首部的扩展首部的类型。这个字段指明在基本首部后面紧接着的一个首部的类型。

* 1. 跳数限制（hop limit）：该字段占8位，用来防止数据包在网络中无限期地存在。源站在每个数据包发出时即设定某个跳数限制。每一个路由器在转发数据包时，要先将跳数限制字段中的值减1。当跳数限制的值为0时，就要将此数据包丢弃。这相当于IPv4首部中的生存期字段，但比IPv4中的计算时间间隔要简单些。
  2. 源站IP地址：该字段占128位，是数据包的发送站的IP地址。
  3. 目的站IP地址：该字段占128位，是数据包的接收站的IP地址。
  4. IPv6的地址表示：
     1. 常规表示法：

为了使地址的表示简洁些，IPv6使用冒号十六进制记法（colon hexadecimal notation, colon hex），它把每个16位用相应的十六进制表示，各组之间用冒号分隔。例如：2409:8a28:84c:79a0:2068:c643:4408:3e1b。

* 1. 零压缩表示法：

冒号十六进制记法允许0压缩（zero compression），即一连串连续的0可以用一对冒号所取代，例如：FF05:0:0:0:0:0:0:B3可以改成FF05::B3，即中间的很多个0用 :: 表示。

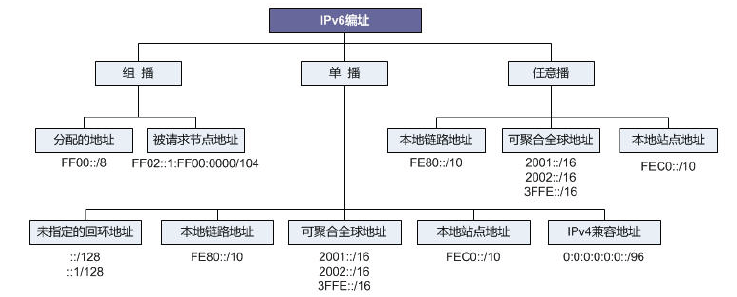
为了保证0压缩有一个清晰的解释，建议中规定，在任一地址中，只能使用一次0压缩。

* 1. IPv4地址结合表示法:

冒号十六进制记法可结合有点分十进制记法的后缀。这种结合在IPv4向IPv6的转换阶段特别有用。例如：::1可以表示为 ::0.0.0.1。

虽然为冒号所分隔的每个值是一个16位的量，但每个点分十进制部分的值则指明一个字节的值

* 1. IPv6的地址分类：
     1. 单播（unicast）：传统的点对点通信。
     2. 多播（multicast）：一点对多点的通信，数据包交付到一组计算机中的每一个。IPv6没有采用广播的术语，而是将广播看作多播的一个特例。
     3. 任播（anycast）：这是IPv6增加的一种类型。任播的目的站是一组计算机，但数据包在交付时只交付给其中的一个，通常是距离最近的一个。
  2. IPv6地址的结构，特性和特殊地址：



IPv6地址的前64位为网络位，后64位为主机位，不需要象IPv4那样使用子网掩码划分子网等。64位的网络地址一般称为前缀。

当用户使用IPv6连接互联网时，运营商只为用户分配前缀地址（一般是网络位的前60位或者56位，剩下的几位由用户自行安排），主机位的地址由用户主机按照一定规则生成，或者自定义设置。

IPv6不再按照IPv4中的ABC分来，而是按照用途和具体功能分类，如上图。

详细内容：<https://blog.csdn.net/wangcg123/article/details/97398709>

## 10.4.2Internet服务

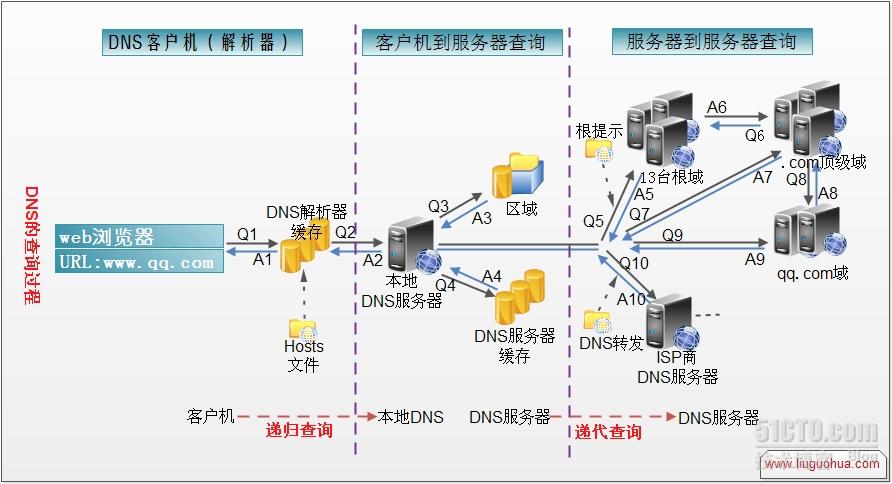
* 1. 域名服务DNS
  2. 概述：

Internet中的域名地址与IP地址是等价的，它们之间是通过域名服务来完成映射变换的。实际上，DNS是一种分布式地址信息数据库系统，服务器中包含整个数据库的某部分信息，并供客户查询。

* 1. 工作模式：

域名系统采用的是客户端／服务器模式，整个系统由解析器和域名服务器组成。解析器是客户方，它负责查询域名服务器、解释从服务器返回来的应答、将信息返回给请求方等工作。域名服务器是服务器方，它通常保存着一部分域名空间的全部信息，这部分域名空间称为区（zone）。一个域名服务器可以管理一个或多个区。域名服务器可以分为主服务器、Caching Only服务器和转发服务器（Forwarding Server）。

* 1. 工作过程：
     1. 解析器向本地域名服务器发出请求查阅用户B的域名。
     2. 本地域名服务器向最高层域名服务器发出查询地址的请求。
     3. 最高层域名服务器返回给本地域名服务器一个IP地址。
     4. 本地域名服务器向组域名服务器发出查询地址的请求。
     5. 组域名服务器返回给本地域名服务器一个IP地址。
     6. 本地服务器向刚返回的域名服务器发出查询域名地址请求。
     7. IP地址返回给本地域名服务器。
     8. 本地域名服务器将该地址返回给解析器。



本地域名服务器为了得到一个IP地址常常需要查询多个域名服务器。于是，在查询地址的同时，本地域名服务器也就得到了许多其他域名服务器的信息，像它们的IP地址、所负责的区域等。本地域名服务器将这些信息连同最终查询到的主机IP地址全部存放在它的Cache中，以便将来参考。当下次解析器再查询与这些域名相关的信息时，就可以直接引用。这样就大大减少了查询时间。

* 1. 远程登录服务Telnet
  2. 概述：

远程登录服务是在Telnet协议的支持下，将用户计算机与远程主机连接起来，在远程计算机上运行程序，将相应的屏幕显示传送到本地机器，并将本地的输入送给远程计算机。由于这种服务基于Telnet协议且使用Telnet命令进行远程登录，故称为Telnet远程登录。

* 1. 工作模式：

Telnet是基于客户端／服务器模式的服务系统，它由客户端软件、服务器软件以及Telnet通信协议三部分组成。

* 1. 电子邮件服务

E-mail系统基于客户端／服务器模式，整个系统由E-mail客户端软件、E-mail服务器和通信协议三部分组成。E-mail客户端软件也称用户代理（User Agent），是用户用来收发和管理电子邮件的工具；E-mail服务器主要充当“邮局”的角色，它除了为用户提供电子邮箱外，还承担着信件的投递业务，当用户发送一个电子邮件后，E-mail服务器通过网络若干中间节点的“存储—转发”式的传递，最终把信件投递到目的地（收信人的电子邮箱）；E-mail服务器主要采用SMTP（简单邮件传输协议），本协议描述了电子邮件的信息格式及其传递处理方法，保证被传送的电子邮件能够正确地寻址和可靠地传输，它是面向文本的网络协议，其缺点是不能用来传送非ASCII码文本和非文字性附件，在日益发展的多媒体环境中以及人们关注的邮件私密性方面，更显出它的局限性。后来的一些协议，包括多用途Internet邮件扩充协议（MIME）及增强私密邮件保护协议（PEM），弥补了SMTP的缺点。而SMTP是用在大型多用户、多任务的操作系统环境中，将它用在PC上收信是十分困难的，所以在TCP/IP网络上的大多数邮件管理程序使用SMTP来发信，且采用POP（Post Office Protocol）（常用的是POP3）来保管用户未能及时取走的邮件。

POP协议有两个版本：POP2和POP3。目前使用的POP3既能与STMP共同使用，也可以单独使用，以传送和接收电子邮件。POP协议是一种简单的纯文本协议，每次传输以整个E-mail为单位，不能提供部分传输。

* 1. 万维网服务WWW

万维网是基于客户端／服务器模式的信息发送技术和超文本技术的综合，WWW服务器把信息组织为分布的超文本，这些信息节点可以是文本、子目录或信息指针。WWW浏览程序为用户提供基于超文本传输协议（Hyper Text Transfer Protocol, HTTP）的用户界面，WWW服务器的数据文件由超文本标记语言（Hyper Text Markup Language, HTML）描述，HTML利用统一资源定位器（URL）的指标是超媒体链接，并在文本内指向其他网络资源。

超文本传输协议是一个Internet上的应用层协议，是Web服务器和Web浏览器之间进行通信的语言。所有的Web服务器和Web浏览

器必须遵循这一协议，才能发送或接收超文本文件。HTTP是客户端／服务器体系结构，提供信息资源的Web节点（即Web服务器），可称作HTTP服务器，Web浏览器则是HTTP服务器的客户。WWW上的信息检索服务系统就是遵循HTTP运行的。在HTTP的帮助下，用户可以只关心要检索的信息，而无须考虑这些信息存储在什么地方。

一个URL（Web地址）包括以下几部分：协议、主机域名、端口号（任选）、目录路径（任选）和一个文件名（任选）。

* 1. 文件传输服务FTP

文件传输协议用来在计算机之间传输文件。

* 1. 匿名FTP服务:

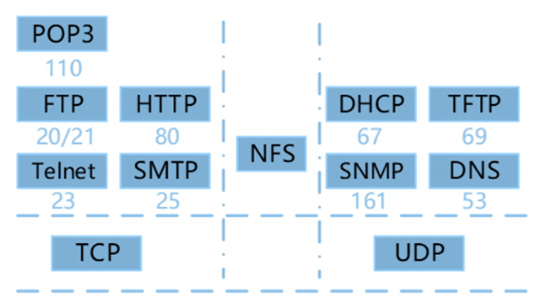
匿名FTP服务设置了一个特殊的用户名——anonymous，供公众使用，任何用户都可以使用这个用户名与提供这种匿名FTP服务的主机建立连接，并共享这个主机对公众开放的资源。匿名FTP的用户名是anonymous，而密码通常是guest或者是使用者的E-mail地址。当用户登录到匿名FTP服务器后，其工作方式与常规FTP相同。通常，出于安全的目的，大多数匿名FTP服务器只允许下载（download）文件，而不允许上传upload）文件。

* 1. 工作模式：

FTP是基于客户端／服务器模式的服务系统，它由客户端软件、服务器软件和FTP通信协议3部分组成。FTP客户端软件运行在用户计算机上，在用户装入FTP客户端软件后，便可以通过使用FTP内部命令与远程FTP服务器采用FTP通信协议建立连接或文件传送；FTP服务器软件运行在远程主机上，并设置一个名叫anonymous的公共用户账号，向公众开放。

FTP在客户端与服务器的内部建立两条TCP连接：一条是控制连接，主要用于传输命令和参数（端口号为21）；另一条是数据连接，主要用于传送文件（端口号为20）。

1. 应用层服务的端口号



1. 常用Windows网络命令
   1. ping 用于检测网络是否通畅和网络延迟
   2. ipconfig 查看网络配置信息
   3. tracert 路由跟踪
   4. nslooukup 查看域名解析情况
   5. route 系统路由设置
   6. netstat -a 查看端口的分配和网络连接