

计算机网络概述

适用班级：软件设计师、网络工程师

主 讲：刘琳芳

网 址：[www.bitpx.com](http://www.bitpx.com)

比特培训中心

贵州·贵阳

[第1章. 计算机网络概述 1](#_Toc19886701)

[1.1传输媒介 1](#_Toc19886702)

[1.2 网络协议及分层体系结构 3](#_Toc19886703)

[1.2.1 分层体系结构 3](#_Toc19886704)

[1.2.2网络分层模型及协议 3](#_Toc19886705)

[1.3网络设备 5](#_Toc19886706)

[1.3.1 按体系结构划分的网络设备 5](#_Toc19886707)

[1.3.2交换方式 8](#_Toc19886708)

[1.3.3 网络分类 9](#_Toc19886709)

[1.4 IP地址 10](#_Toc19886710)

[1.4.1 网络互联模型 10](#_Toc19886711)

[1.4.2分类IP地址 10](#_Toc19886712)

[1.4.2 IP数据报构成及转发过程 12](#_Toc19886713)

[1.4.3 划分子网 15](#_Toc19886714)

[1.4.4 构成超网 17](#_Toc19886715)

[1.5 TCP/IP协议集 21](#_Toc19886716)

[1.5.1 网络接口层协议 21](#_Toc19886717)

[1.5.2网络层协议 23](#_Toc19886718)

[1.5.3传输层协议 25](#_Toc19886719)

[1.5.4 应用层协议 28](#_Toc19886720)

[1.7 IPV6 33](#_Toc19886721)

[1.8计算机网络概述剩余试题部分 33](#_Toc19886722)

# 第1章. 计算机网络概述

计算机网络，是指两台或多台具有完整功能的如计算机等网络终端设备，使用有线或无线传输媒介通过互联设备进行互连，在约定通信规则下进行有效数据传输和资源共享的组织结构。



图1-1 基本网络结构模型

1.1传输媒介

1.双绞线

双绞线(twisted pair)，由两根相互绝缘的铜线规则地绞合在一起组成，如同一条DNA分子链，相互绞合可以减少对邻近导线的电磁干扰，提高信号传输质量，每根铜线的典型粗细为1mm直径，日常应用最常见的是固定电话系统，几乎所有固定电话都是通过双绞线连接到电话局进行信号传输。

双绞线既能传输模拟信号，也能传输数字信号。其传输能力取决于铜线的粗细，线芯越粗，传输距离和传输质量越优，价格越贵，通常将四对铜线捆成一起构成一根电缆，如果在四对线束外增加一层金属丝编织而成的屏蔽层，这种线缆称为屏蔽双绞线(STP，Shielded Twisted Pair)，没有屏蔽层称为非屏蔽双绞线(UTP，Unshielded Twisted Pair)，如下图，因线路的粗细和绞合密度不同，把双绞线分为多种类别，类别越高，铜线绞合密度越大，线芯越粗，传输距离和传输质量越优,价格越贵，如表，

随着传输距离的增加，信号都会出现不同程度的衰减，使用双绞线进行传输时信号的衰减程度随着信号的频率升高而增大，使用越粗的导线可以降低信号衰减，所以使用双绞线进行传输时信号应有足够的振幅，以及适当的传输距离，以便在噪声干扰下接收端能正确接收信号，双绞线的传输最高速率也和使用的信号编码方式有关。

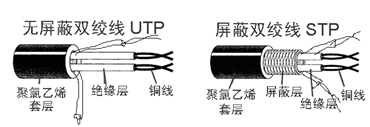


图1-2 双绞线结构模型

表1-1 双绞线类型及其应用

|  |  |  |
| --- | --- | --- |
| 类型 | 带宽 | 典型应用 |
| 3类 | 16MHZ | 低速网络，模拟电话 |
| 4类 | 20MHZ | 短距离的10BASE-T以太网 |
| 5类 | 100MHZ | 10BASE-T以太网(即10Mbit/s)；某些100BASE-T快速以太网(即100Mbit/s) |
| 超5类(5E) | 100MHZ | 100BASE-T快速以太网；某些1000BASE-T吉比特以太网 |
| 6类 | 250MHZ | 1000BASE-T吉比特以太网，ATM网络 |
| 7类 | 600MHZ | 可能用于今后的10吉比特以太网 |

带宽：又称介质带宽，传输介质在传送信号时能够传送电磁波的有效频率范围，单位是HZ，是介质的物理特性；

比特：bit，位，单位名称，一个0称为1bit，一个1也称为1bit。

10BASE-T：10即为10Mbit/s，M=106，读作“兆”，即网络的传输速率为每秒10兆bit，BASE指该网络传输信号为未经过特殊调制的基本频带信号，T指该网络使用双绞线作为传输媒体。

以太网：是应用最为广泛的一种局域网技术，1980年由DEC、Inter和Xerox三家公司合作提出了10Mbps的以太网规范DIX Ethernet V1。1981年，DIX Ethernet V2.0公布并成为世界上第一个局域网产品的规范。

2.同轴电缆：

同轴电缆有内导体铜质芯线、绝缘层、网状屏蔽层以及塑料保护外层组成，具有良好抗干扰特性，用于传输速率较高的环境。

在局域网发展初期层广泛使用同轴电缆作为传输媒体，因其安装和维护不便，已逐渐被双绞线代替。目前主要用于有线电视网中。

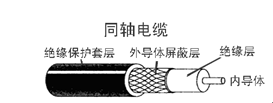


图1-3 同轴电缆结构模型

75欧同轴缆用于有线电视网络，为宽带同轴电缆，用于传输模拟信号。

50欧同轴缆用于局域网的数字信号传输，为基带同轴电缆，粗缆适合大型局域网，传输距离长，可靠性高。造价高，安装难度大。细缆安装简单，造价低。

3.光纤

光纤的纤芯是一种能传播光的石英玻璃或特制塑料拉成的柔软细丝。包层是涂在纤芯外的一层折射率比光纤纤芯低的材料。通常有光脉冲传输表示传输信息为1，没有光脉冲相当于0。在发送端使用发光二极管或半导体激光器产生光信号。因光纤外包层比纤芯折射率低，当光纤从高折射率的媒介射向低折射率的媒介时，其折射角将大于入射角，故当入射角足够大时，光信号将不进入包层，而是被全反射重新进入光纤纤芯内，从而沿着光纤一直传输。

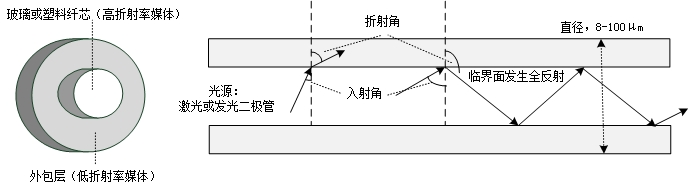


图1-4 光纤通信原理

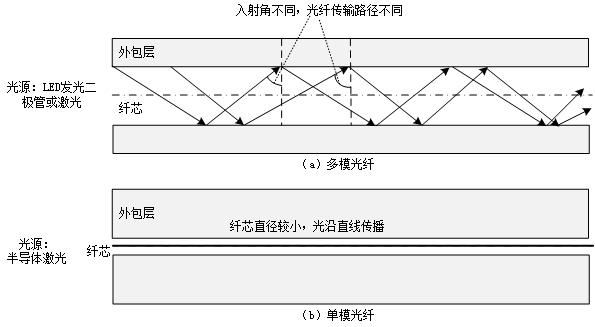


图1-5 单模多模光纤结构图

“模”是指光线的入射角。

* 多模光纤：光线能从多种角度入射，通过不同光路传播，常见的有62.5/125μm和50/125μm两种，其中后面的数值125μm是指光纤的包层直径，前面的数值50μm和62.5μm是指光纤的纤芯直径，一般使用波长为850nm或1310nm的激光，以波长为850nm的激光最为常见。

影响光纤传输带宽度的主要因素是各种色散，如模式色散、材料色散和波导色散等，而以模式色散的影响最为重要。

模式色散，又称模间色散或者多径色散。因一种频率的光波以不同的角度入射到光纤中，形成不同的模式，每种模式具有不同的轴向速度，因而同时发出的不同模式到达输出端的时间是不相同的，从而导致输出端信号的畸变。在一条长度相同的光纤上，不同模式的光到达终点所用的时间差称为光纤时延差。

材料色散，由光纤材料自身特性造成的，例如石英玻璃的折射率，严格来说，并不是一个固定的常数，而是对不同的传输波长有不同的值。

波导色散是对于光纤的某一传输模式，在不同的光波长下的群速度不同引起的脉冲展宽。它与光纤结构的波导效应有关，因此也被成为结构色散。

影响光纤时延差的因素有两个：纤芯－包层相对折射率差和光纤的长度。

光纤的时延差与纤芯－包层相对折射率差成正比。其中是纤芯的折射率和包层的折射率相差越大，光信号传播一定距离后产生的时延差就会越大，光脉冲发生展宽也越大。从减小光纤时延差的观点上看，希望较小为好，这种小的光纤称为弱导光纤。通信用光纤都是弱导光纤。

光纤越长，时延差也越大，色散也越大。

* 单模光纤：纤芯直径比多模光纤要小的多，常见规格是9/125μm，一般采用波长为1310nm或1550nm的激光，传播的光线基本是水平的。

单模光纤能传一种模式的光纤，因此，单模光纤的色散小,故能把光以很宽的频带传输很长距离，适用于远程通讯。

由于单模光纤芯径太小，较难控制光束传输，单模光纤对光源的谱宽和稳定性有较高的要求，如果使用LED作为光源，LED会发放大量不同频宽的光源，如果要取得较好的传输质量，会对光纤制作材料的材料色散要求非常高，故单模光纤使用极为昂贵的激光作为光源体，利用激光才能获得高频宽，即谱宽要窄，稳定性要好。

单模光纤相比于多模光纤可支持更长传输距离，在100Mbps的以太网以至1G千兆网，单模光纤都可支持超过5000m的传输距离。

从成本角度考虑，由于光端机非常昂贵，故采用单模光纤的成本会比多模光纤光缆的成本高。

单模光纤与多模光纤相比：单模光纤有较高的传输率、较长的传输距离、较高的成本，较细的纤芯。且单模光纤的光源采用激光光源，多模的可以采用二极管LED作光源，也可使用激光作为光源。

●(2017.5)以下关于光纤的说法中，错误的是 (11)。

(11)A.单模光纤的纤芯直径更细 B.单模光纤采用LED作为光源

C.多模光纤比单模光纤的传输距离近 D.多模光纤中光波在光导纤维中以多种模式传播

4.无线介质

1. 无线电传输2. 微波传输3. 卫星传输4. 红外线传输5. 激光传输

1.2 网络协议及分层体系结构

1.2.1 分层体系结构

大多数网络按层(layer)的方式来进行组织，不同网络中每一层的名称、功能都不尽相同，以下图生活中常见的快递功能来理解分层、协议、对等实体等抽象网络用语。

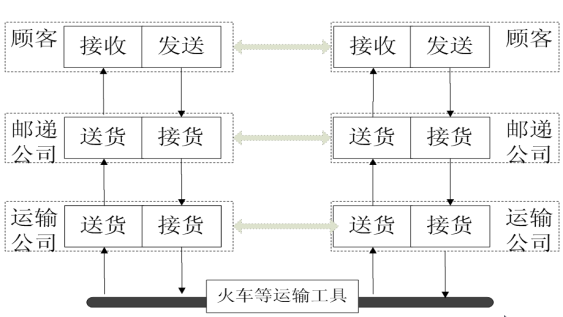


图1-6 协议和服务举例

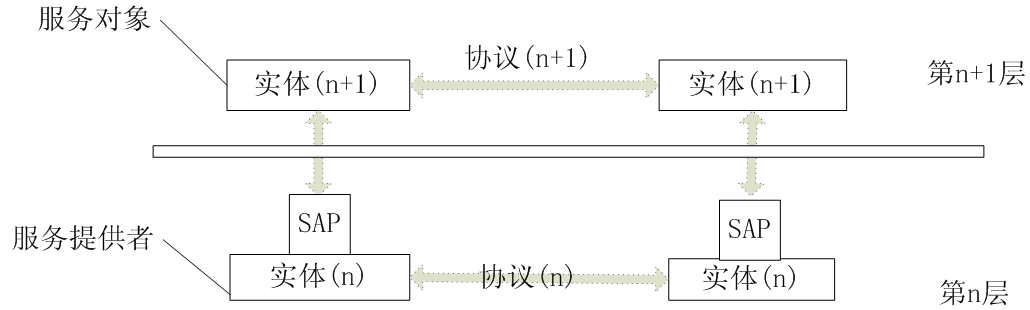


图1-7 网络层次之间的关系

**实体：**发送或接收信息的硬件或软件进程，在同一层中不同设备里运行的实体称为对等实体。

**协议：**控制两个对等实体或多个实体进行通信的规则的集合，不同层次遵循各层的协议。

网络协议的组成要素：

* 语法：数据与控制信息的结构或格式 。
* 语义：需要发出何种控制信息，完成何种动作以及做出何种响应。
* 同步：事件实现顺序的详细说明。

**服务：**在协议的控制下，两个对等实体间的通信使得本层能够向上一层提供服务。要实现本层协议，还需要使用下面一层所提供的服务。

**服务数据单元**(SDU **，service data unit**)：层与层之间交换的数据的单位。

**协议数据单元**(PDU **，potocal data unit**)：每一层传输能力不同，为成功在在n传输SDU，可能需要将SDU分成几部分，每一部分加上一些必要的本层信息后独立进行传输，该种数据称为**协议数据单元**。

**服务访问点(SAP，service access point)**：同一系统中相邻两层的实体交互(即交换信息)的地方，是上层调用下层服务的接口，是服务的唯一标识。

计算机网络的各层及其协议的集合，称为**网络的体系结构**，体系结构是抽象的，而实现则是具体的，是真正运行的计算机硬件和软件。

1.2.2网络分层模型及协议

1. OSI/RM模型七层模型

1984年ISO(国际标准化组织)颁布了OSI/RM(Open Systems Interconnection Reference Model)：开放系统互连参考模型，常简称OSI模型，仅为一种理论模型，现今的互联网并未使用该标准。

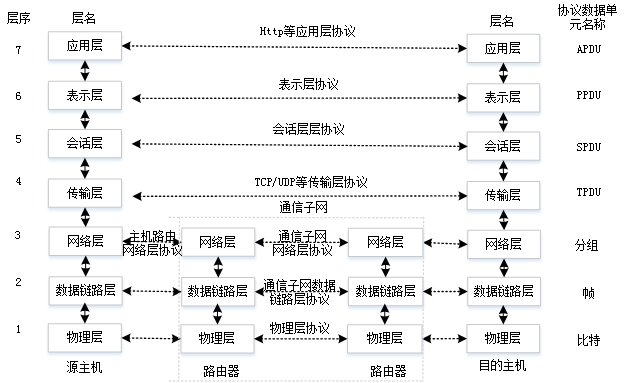


图1-8 OSI/RM 七层模型

(7) 应用层：直接为用户的应用进程服务，协议有万维网应用协议HTTP、电子邮件协议SMTP、文件传输协议FTP等

(6) 表示层：负责两个通信系统之间所交换信息的表示方式，使得两台数据表示结构完全不同的设备能够自由地通信，例如不同的机器有不同的编码来表示字符串(如有些系统使用ASCII编码，有些使用Unicode编码)，表示层使用抽象的方式定义信息，并将其编码进行网络传输，主要任务有：数据编码、处理数据压缩、加密、解压和解密等，实现网络标准法和计算机内部信息表示法质检的转换，提供一种可供应用层选择的服务的集合。

(5) 会话层：为彼此合作的表示层实体建立、维护和结束他们之间的通信会话，可以对同时双向的信息传输提供管理，也可以对任一时刻只能单向传输提供会话管理。

(4) 传输层：TCP和UDP为该层主要协议，为会话层实体提供透明数据传输服务，实现端到端的数据传输，即传输层实现源主机内某程序和目的主机内相应程序之间的连接通信，而下面涉及到的网络层等低层次协议均为网络中每台设备与其相邻设备之间的通信。运输层有复用和分用的功能，复用就是多个上层进程可同时使用下面传输层提供的服务，分用则是运输层把收到的信息分别交付给上层中相应的进程，在这一层，信息的传送单位是报文。

面向连接的服务：在使用该服务时，首先建立连接，接着使用连接，且在信息传输期间需要维护该连接，信息传输完毕后释放连接，保证信息无误、按序到达，可靠性高，通信开销大。

无连接的服务：即传输数据前发送端和接收端不建立连接，只负责将应用程序传给传输层的数据发送出去，不保证他们能可靠交付目的地，只提供尽最大努力交付，数据传输的单位使用户数据报，可靠性欠佳，但通信开销较小，应用于一些可靠性要求不高的地方，如视频点播。

传输层即可以提供面向连接的服务，也可以提供不可靠的无连接的服务，负责流量控制等。核心协议有TCP协议和UDP协议。

(3) 网络层：为传输层实体提供端到端的数据传送功能，使得传输层摆脱路由选择、拥挤控制等网络传输细节，对网络传输中发生的错误予以报告。首先在发送数据时，把上层产生的报文或用户数据包封装成分组或包进行传送，也叫IP数据报。其次要选择适合的路由，使分组能够通过网络中的路由器找到目的主机。使用的主要协议有IP协议、ICMP协议、RIP协议和OSPF协议等。

(2) 数据链路层：负责两个相邻节点间的线路上的数据传输，建立、维持和释放两个相邻节点间的数据链路，将网络层交下来的IP数据报组装成帧(framing)，在相邻结点间传送以帧为单位的数据，每一帧包含数据和必要的控制信息(如地址信息、差错控制等)。使用的主要协议HDLC协议、CSMA/CD、CSMA/CA协议等。

(1) 物理层：为它的上一层提供一个物理连接，以及该物理链路所需的机械、电气、功能和规程特征，如规定电缆和接头类型，传输信息的电压等，但不包含具体的物理传输媒体，传输单位为比特。

●(2016.11)TCP/IP网络中的(13)实现应答、排序和流控功能。

(13)A．数据链路层 B．网络层 C．传输层 D．应用层

●(2005.11)在ISO OSI/RM中，　 (18)　 实现数据压缩功能。

(18)A. 应用层 　 B. 表示层 　 C. 会话层 　　 D. 网络层

2.TCP/IP参考模型

TCP/IP参考模型是目前Internet使用的参考模型。

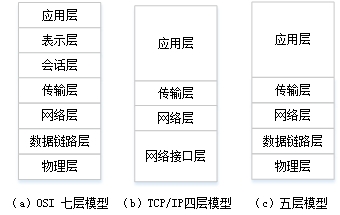


图1-9 OSI/RM模型和TCP/IP模型对比

(1)网络接口层

TCP/IP参考模型没有对该层进行详细的描述，只是指出网络层可以使用某种协议与网络连接，负责实现IP数据报在不同通信系统中传输，实现物理地址(MAC地址)与逻辑地址(IP地址)相互映射的机制。

(2)网际层

是TCP/IP参考模型的核心，负责IP数据报的产生以及IP数据报在逻辑网络上的路由转发，提供数据报的封装、分片和重组，以及路由选择和拥塞控制机制。

(3) 传输层

是TCP/IP参考模型提供端到端通信服务的层次，既可以提供面向连接的可靠通信服务，又可以提供无连接不可靠服务。该层以端口的形式实现通信复用。

(4) 应用层

是TCP/IP参考模型协议数量最多最复杂的层次，面向不同主题向用户提供各种各样的通信服务。

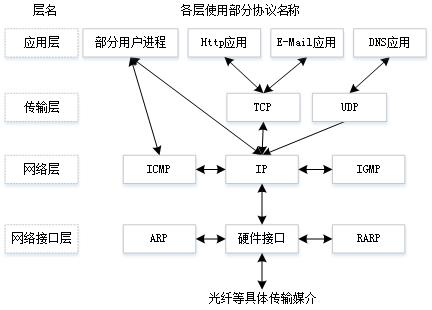


图1-10 TCP/IP协议结构图

1.3网络设备

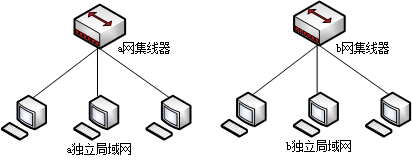
1.3.1 按体系结构划分的网络设备

1. 物理层网络设备

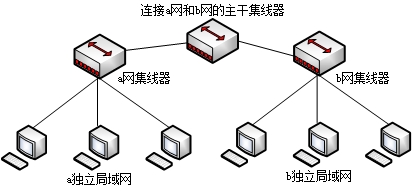
集线器(HUB)或中继器，工作在物理层，是硬件设备，传输的单位为bit，依靠识别电压等信息判断数据，集线器能将多台计算机连接在一起构成共享式局域网，同时它还可以将从任意端口接收到的信号进行整形放大，再复制到其他端口，从而起到对信号进行中继的作用。

集线器的端口带宽主要有10Mbps和lOOMbps两种。集线器是指共享式集线器，其带宽为所有端口共享。例如，从宏观来看，一台16端口、传输速率为100Mbps的集线器，当全部端口都使用时，每一端口的带宽就只有100Mbps的1/16。从微观来看，连接在集线器上的任何一个设备发送数据时，其他所有设备必须等待，此设备享有全部带宽，通讯完毕，再由其他设备使用带宽。所有设备相互交替使用，就好象大家一起过一根独木桥一样。

* 单播通信：指信息的目的地唯一，信息内封装目的地特有的地址信息；
* 广播通信：指信息的目的地为多个对象，信息内封装特有的广播地址信息；
* 冲突域：所有不能同时发送信息的接点设备组成的区域，例如网络上的两台计算机在同时通信时会发生冲突，那么这个网络就是一个冲突域，也叫碰撞域。
* 广播域：能够接收到同一个广播消息的所有设备组成的范围，其中任何一个节点发送一个广播消息，其他设备均能接收到。
* 由集线器连接形成的网络上，所有终端不能有两台及两台以上同时发送信息，集线器连接的网络形成一个冲突域；
* 集线器不能判断数据包的目的地和类型，所以如果是广播数据包也依然转发，而且所有设备发出数据以广播方式发送到每个接口，这样集线器也连接了一个广播域的网络。



1. 两个独立的局域网



1. 一个扩展的局域网

图1-11 网络设备连接图

2. 数据链路层网络设备

网络接口卡NIC(Network Interface Card)：简称网卡，可以将计算机连接到网路上，接口要与传输介质匹配，是[局域网](http://baike.baidu.com/view/788.htm)中连接[计算机](http://baike.baidu.com/view/3314.htm)和传输介质的[接口](http://baike.baidu.com/view/159864.htm)，有自身的网卡地址，即MAC地址，不仅能实现与局域网传输介质之间的物理连接和电信号匹配，还涉及帧的发送与接收、帧的封装与拆封、[介质访问控制](http://baike.baidu.com/view/1324971.htm)、数据的[编 码](http://baike.baidu.com/view/237708.htm)与解码以及[数据缓存](http://baike.baidu.com/view/32571.htm)的功能等，其中一个重要功能就是进行数据串行传输和并行传输的转换。

网桥：连接两个或两个以上的局域网，有选择地将数据帧从一个网络传向另一个网络，网桥要分析帧地址地段，以决定是否把收到的帧转发到另一个网络段上，即具有过滤帧的作用，基于此作用，当一个网络负载很重而性能下降时，可以用网桥把他分城两个网络段，使得各网段间通信量变小，提高网络性能。

交换机**:**工作在OSI/RM的数据链路层。交换机的主要作用是将多台计算机和网络设备连接在一起构成交换式局域网。

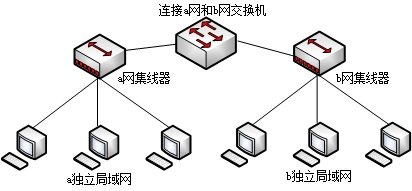


图1-11 用交换机连成更大的局域网

交换机是端口带宽独享，端口之间可以采用全双工进行数据传输，实现数据的线速转发。交换机比集线器先进，允许连接在交换机上的设备并行通讯，好比高速公路上的汽车并行行使一般，设备间通讯不会再发生冲突，因此交换机打破了冲突域。例如，一台lOOMbps全双工交换机在使用时，每对端口之间的数据接收或发送都会以lOOMbps的速率进行传输，不会因为使用端口数的增加而减少每对端口之间的带宽。

交换机的端口带宽有lOMbps、lOOMbps、lO/lOOMbps自适应、1000Mbps、10/100/1000Mbps自适应以及10Gbps等多种，有些交换机只具有其中一种端口，有些则兼有两种或多种端口。

无论如何称呼，交换机最根本的性能都是在第二层实现数据帧的线性交换。名称的不同，体现出来的是用户对交换机工作要求的不同。

交换机与网桥都工作在数据链路层，根据数据帧的目的MAC地址处理数据帧。交换机可以视为多端口的网桥，它们之间存在区别：

交换机通常只要具有帧的转发功能就可以了，而网桥往往还需要具有帧格式转换功能。

3. 网络层网络设备

路由器：传输单位为分组，路由器都有自己的操作系统，但没有交换机那么多接口，一般指具体的硬件设备。具有协议转换能力，主要转发网络层数据包，并在复杂的网络拓扑结构中找出一条最佳的传输路径，采用逐站传递的方式，把数据包从源节点传输到目的节点。

数据链路层剥去帧首部和尾部后，将分组送到网络层的队列中排队等待处理。这会产生一定的时延。

**它不仅能隔离冲突域，还能检测广播数据包(主要指本地广播数据包)，**并丢弃广播包来隔离广播域。在路由器中记录着路由表，路由器以此来转发数据，以实现网络间的通讯。

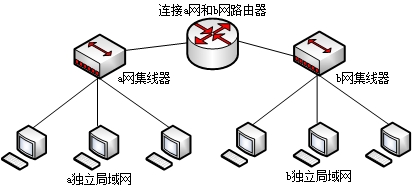


图1-12 用路由器连接

5. 设备区别

集线器与交换机的区别：

(1)在OSI/RM(OSI参考模型)中的工作层次不同

集线器是工作在物理层，而交换机至少是工作到第二层，更高级的交换机可以工作到第三层。

(2)交换机的数据传输方式不同

集线器的数据传输方式是广播(broadcast)方式，而交换机的数据传输是有目的的，数据只对目的节点发送。

(3)带宽占用方式不同

集线器的所有端口是共享集线器的总带宽，集线器只能采用半双工方式进行传输，这样在上行通道上集线器一次只能传输一个任务，要么是接收数据，要么是发送数据。例如，一台16端口、传输速率为100Mbps的集线器，当全部端口都使用时，每一端口的带宽就只有100Mbps的1/16。而交换机是以全双工交换，一台lOOMbps全双工交换机在使用时，每对端口之间的数据接收或发送都会以lOOMbps的速率进行传输，不会因为使用端口数的增加而减少每对端口之间的带宽，所以交换机是端口带宽独享。

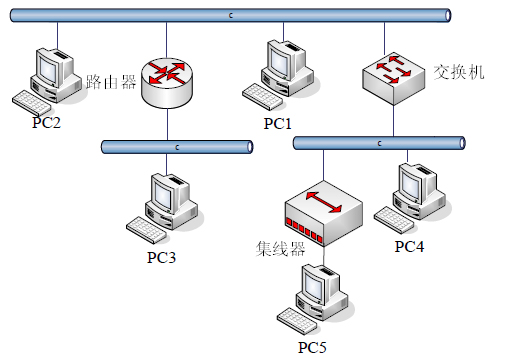
(4)隔离作用域不同

集线器内部是总线结构，不可以隔离冲突域，也不可以隔离广播域。

交换机可以隔离冲突域，但不能隔离广播域。

路由器可以隔离冲突域，也可以隔离广播域

●(2008.5)某IP 网络连接如下图所示，主机PC1 发出一个全局广播消息，无法收到该广播消息的是 (32) 。



(32)A. PC2 B. PC3 C. PC4 D. PC5

●关于网桥和交换机，下面的描述中正确的是(22)。

(22)A.网桥端口数少，因而比交换机转发更快 B.网桥转发广播帧，而交换机不转发广播帧

C.交换机是一种多端口网桥 D.交换机端口多，因而扩大了冲突域的大小

● 使用路由器对局域网进行分段的好处是(23)。

(23)A.广播帧不会通过路由进行转发 B.通过路由器转发减少了通信延迟

C.路由器的价格便宜，比使用交换机更经济 D.可以开发新的应用

●(2015.11)集线器与网桥的区别是：(66)。

(66)A.集线器不能检测发送冲突，而网桥可以检测冲突 B.集线器是物理层设备，而网桥是数据链路层设备

C.网桥只有两个端口，而集线器是一种多端口网桥 D.网桥是物理层设备，而集线器是数据链路层设备

●(2016.11)能隔离局域网中广播风暴、提高带宽利用率的设备是(11) 。

(11)A.网桥 B．集线器 C．路由器 D.交换机

●网络配置如下图所示，其中使用了一台路由器、一台交换机和一台集线器，对于这种配置，下面的论断中正确的是(66)。



(66)A.2个广播域和2个冲突域 B.l个广播域和2个冲突域 C.2个广播域和5个冲突域 D.1个广播域和8个冲突域

●(2018.5)下列网络互连设备中，属于物理层的是(66)。

(66)A.交换机 B.中继器 C.路由器 D.网桥

1.3.2交换方式

1.电路交换

和打电话一样，需要经过建立连接，保持连接和释放连接三个阶段，且连接保持时不可以有其他信号共用信道，电路交换提供面向连接的服务。主要特点：

(1)需要建立通道、维护通道和拆除通道。

(2)信息在传输过程中不用自己寻找目标。

(3)可靠性高，服务质量好。

(4)可确保信息传送的次序。

(5)实现机理比较复杂。

2.存储转发

与邮政系统服务相似，不需要建立起物理的连续通路，提供无连接服务，而是根据报头信息，以接力方式将数据报文在网络节点之间逐段传送，直到目的节点。主要特点：

1. 无须建立通道，信息块自由传输。
2. 每个信息块包含目标地址信息，传输独立。
3. 每个信息块得传输路径可能不一定相同。
4. 可靠性不高，服务质量不好。
5. 信息块不保证顺序到达，容易丢失。
6. 实现机理比较简单。

根据传送数据单元是否存在长度限制，分两种实现方式：

**(1)报文交换**

把要传输的数据称为报文，报文中指明目的地的地址，由交换节点负责寻找路径转发出去，报文完整地在网络中逐个结点向前传输，每一个结点收到整个报文后，检查目标结点地址，再根据网络中的交通情况在适当的时候转发到下一站点，最后经过多次存储-转发，最后到达目标节点。

**(2)分组交换**

把要传输的数据切割成固定长度的分组，该分组比报文要短，给各个分组授予编号，加上源地址和目标地址等分组头信息，这个过程叫做信息的**分片与封装**。然后分组在子网中进行传输，所有分组到达目标结点后，按编号被重新组装成原来的报文，叫信息的**重组**。

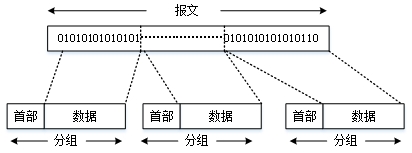


图1-13 报文分片

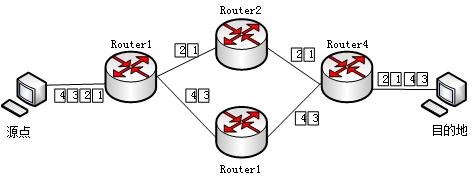
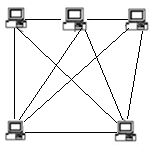
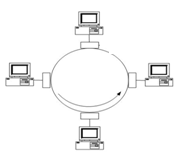
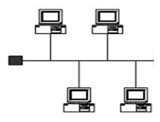


图1-14 分组交换示意图

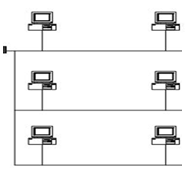
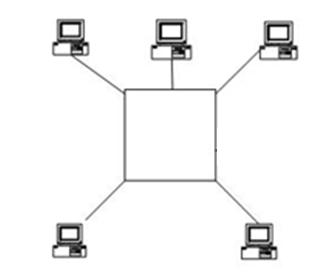
1.3.3 网络分类

1. 按拓扑结构分：

网络的拓扑结构指的就是网络中所有计算机和通信设备、传输媒体之间的物理连接模式。



(a) 总线型(BUS) (b) 环型 (c)网状



(d) 星型 (e) 树型

图1-15 按拓扑结构分类网络

(1)、总线型结构

拓扑结构如图1-6(a)所示，其特点为：结构中只有一条双向通路，进行广播式发送信息，结构简单，节点的增、删和位置的变得容易，系统扩充性能好，使用设备少，价格低，安装使用方便，由于电气信号通路多，信号干扰大，因此对信号的质量要求高，负载重时，线路的利用率低，故障隔离和检测困难。

(2)、环型构

拓扑结构如图1-6(b)所示，其特点为：传输信息的线路构成一个封闭的环，各节点通过中继器连接入网，信息单向沿环路逐点传送，因此信息的流动方向固定，连个节点仅有一条通路，路径控制简单，节点一旦发生故障，系统自动旁路，可靠性高，但是信息要串行通过多个节点，传输效率低，系统响应速度慢，由于环路封闭，扩充交难。

(3)、网状结构

拓扑结构如图1-6(c)所示，其特点为：各节点之间有多条线路相连，故可靠性高，网络响应时间短，但节点之间通路多，节点间路由选择和流量控制难度大，管理软件复杂，硬件成本高。

(4)、星型结构

拓扑结构如图1-6(d)所示，其特点为：使用中央交换单元连接各个节点，维护管理容易，配置灵活，故障隔离和检测容易，各节点之间通信必须经过中央单元转换，线路利用率低，中央单元负荷重。

(5)、树型结构

拓扑结构如图1-6(e)所示，其特点为：是总线型结构的扩充，主要用于多个网络组成的分级结构中，特点同总线型网。

2. 按网络覆盖的不同范围分：局域网、城域网、广域网。

(1)、局域网

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

其特点为：

1. 分布范围有限，通常分分布在一个学校，一个单位，为本单位使用；
2. 较高的数据传输率和数据传输可靠性，误码率低，传输速率一般为1Mb/s，最高已达到1000Mb/s。
3. 通常采用双绞线作为传输介质，跨楼时可使用光纤。
4. 拓扑结构简单，采用星型、环型、和总线型，配置和管理容易。

(2)、城域网

城域网(Metropolitan Area Network)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，主要为接入网络的企业、机关、公司和社会单位提供信息传输的集成服务。

(3)、广域网

广域网(Wide Area Network)又称远程网，是指覆盖范围广、传输速率相对较低、以数据通信为主要任务的网络。其特点为：

1. 分布范围广，加入广域网中的计算机通常处在数公里到数千公里的地方，因此网络所涉及的范围可覆盖地区、省、全国乃至全球。
2. 数据传输率低，一般为几十Mb/s以下。
3. 数据传输可靠性随着传输介质的不同而不同，若使用光纤，误码率较低。
4. 通常借用公共传输网络来实现。
5. 拓扑结构复杂，大多采用“分布式”网络。
6. 布局不规则，对网络的通信控制比较复杂，要求连接到网络上的用户要严格遵守各种标准和规程，要求网络要能够兼容多种网络系统。

## 1.4 IP地址

### 1.4.1 网络互联模型

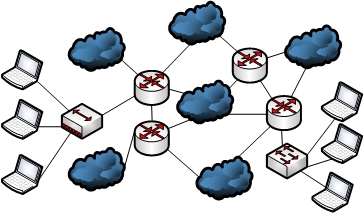


图1-16实际互连网络模型

IP地址：是给每个连接在因特网上的主机(或路由器)分配一个在全世界范围唯一的 32 位的标识符。现在是由因特网名字与号码指派公司ICANN进行分配的，它的编址方法经过三个阶段，这三个阶段是：

(1)分类IP地址。

(2)子网的划分

(3)构成超网

### 1.4.2分类IP地址

二进制数：基数为2，数字符号只有0和1。逢二进一，如“11.1” 按照位权展开：

(11.1)2＝1×21＋1×20+1×2-1＝2+1+0.5=3.5

10000000 B=1\*27=128 01000000 B=1\*26=64 00100000 B=25=32 00010000 B=24=16

00001000 B=23=8 00000100 B=22=400000010 B=21=2 00000001 B=20=1

分类地址即将IP地址划分为若干个固定类，每一类地址由网络号和主机号组成。记为：

IP地址：{<网络号>, <主机号>}

点分十进制表示，即每8位二进制用一个十进制表示。

例如：计算机中存放的IP地址：00000001 00000010 00000011 00000100

采用点分十进制的IP地址： 1 . 2 . 3 . 4

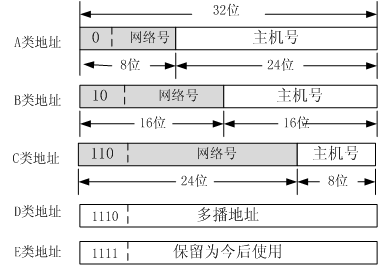


图1-17分类IP地址中网络号字段和主机号字段

1. A类地址：以“0“开头，网络段长为8位，左侧“0“不可变，可变部分为7位。网络号位置的二进制编码变化范围为：00000000-01111111，十进制即0-127，但只有1-126共126个可用的A类网络号，原因是：第一：编码中的二进制全0(即00000000)表示“这个”意思，不表示某个具体的网络，网络号字段全为0的IP地址是个保留地址，意思是“本网络”；第二：网络号以127开头(即二进制表达为01111111开头的)保留作为本地软件环回测试(loopback test)本主机的进程之间的通信之用。

每个网络中所使用的IP地址中左侧网络位不能改变，具体配置时可配置不同的主机位，给定一个网络位，该网络内主机位的二进制编码变化范围为：00000000 0000000 00000000-11111111 11111111 11111111，十进制表示时为0.0.0-255.255.255，一共有224编码方式，其中IP地址 “网络位.0.0.0”表示该网络的网络地址，不用来具体分配给某个站点使用，IP地址 “网络位.255.255.255”表示该网络上所有站点，即该网络的广播地址，不用来具体分配给某个站点使用，可以使用的分配给某个站点的IP地址数量为224-2个。

2. B类地址：以“10“开头，网络段长为16位，左侧“10“不可变，可变部分为14位，左侧第一个字节对应的二进制编码变化范围为10000000-10111111，以点分十进制进行表示为128-191，给定一个B类网络位，该网络内主机位的二进制编码变化范围为： 0000000 00000000-11111111 11111111，十进制表示时为0.0-255.255，一共有216编码方式，其中IP地址 “网络位.0.0”表示该网络的网络地址，不用来具体分配给某个站点使用，IP地址 “网络位.255.255”表示该网络上所有站点，即该网络的广播地址，不用来具体分配给某个站点使用，可以使用的分配给某个站点的IP地址数量为216-2个。通常 128.0.0.0 网络地址不指派。

3. C类地址：以“110“开头，网络段长为24位，左侧“110“不可变，可变部分为21位。左侧第一个字节对应的二进制编码变化范围为11000000-11011111，对应的十进制变化范围为192-223， 192.0.0.0 网络地址不指派。

4. D类地址：多播地址或组播地址，不分网络段和主机段。以“1110“开头，左侧“1110“不可变，即以点分十进制进行表示时，左侧第一个字节对应的十进制变化范围为224-239，对应的二进制编码变化范围为11100000-11101111。

表1-2 IPv4组播地址

|  |  |
| --- | --- |
| 部分IPv4组播地址(Multicast Address) | 说明 |
| 224.0.0.1 | 所有节点地址 |
| 224.0.0.2 | 所有路由器地址 |
| 224.0.0.5 | OSPF路由器 |
| 224.0.0.6 | OSPF IGP路由器 |
| 224.0.0.9 | RIP路由器 |
| 224.0.0.13 | 所有PIM路由器 |
| 224.0.1.1 | 网络时间协议NTP |

5. E类地址：不分网络段和主机段。以“1111“开头，左侧“1111“不可变，即以点分十进制进行表示时，左侧第一个字节对应的十进制变化范围为240-255，对应的二进制编码变化范围为11110000-11111111。

表1-3 各类IP地址汇总表

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 类 | 网络  段长度(bit) | 最大可指派  的网络数(个) | 第一个可指  派的网络地址 | 最后一个可指  派的网络地址 | 主机段长度(bit) | 每个网络可容纳主机IP地址个数 |
| A | 8 | 126(27-2) | 1．0.0.0 | 126.0.0.0 | 24 | 224-2=1677214 |
| B | 16 | 16383(214-1) | 128.1.0.0 | 191.255.0.0 | 16 | 216-2=65534 |
| C | 24 | 2097151(221-1) | 192.0.1.0 | 223.255.255.0 | 8 | 28-2=254 |

表1-4 IP地址汇总表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 网络号 | 主机号 | 源地址使用 | 目的地址使用 | 代表意义 |
| 0 | 0 | 可以 | 不可 | 本网络本主机 |
| 0 | 主机号 | 可以 | 不可 | 本网中的某个主机(host-id) |
| 网络号 | 000…000 | 不可 | 不可 | 该网络的网络地址，代表该网络 |
| 网络号 | 111…111 | 不可 | 可以 | 对该网络(net-id)上所有主机进行广播，为直接广播地址类型，称为该网络的广播地址 |
| 全1 | 全1 | 不可 | 可以 | 对应点分十进制为255.255.255.255，为本地受限广播地址，若目标地址为此，该信息只在本网络内部广播，路由器均不转发 |
| 01111111(即十进制127) | 任何值 | 可以 | 可以 | 回路地址，作还回测试 |

**说明：**

(1)全“0“地址是”这个，0.0.0.0表示本网络上的本主机，0.0.0.0/32可以用作本机的源地址，此外根据RFC文档描述，它不仅是代表本机，0.0.0.0/8可以表示本网络中的所有主机，若该设备可接受来自所有机子的信息，也可设置接收范围为0.0.0.0。

(2)直接广播地址：网络位为某一值，主机位全为“1“的IP地址用于广播，称为直接广播地址。直接广播是对该网络上全部主机进行信息广播发送时所使用的地址，也称该网络的广播地址，该种地址只能作为信息的目的地地址，不能作为源地址使用。

一个A类网络广播地址格式：[网络段].255.255.255 如110.255.255.255

一个B类网络广播地址格式：[网络段].255.255 如130.89.255.255

(3)本地受限广播地址：255.255.255.255，即二进制为32个1，只能作为目的地址，路由器对目的地为该地址的信息不转播，也叫做本地广播地址。

(4)回路地址：形如127.\*.\*.\*，测试本主机的网络配置的测试。如127.0.0.1表示本机的TCP/IP协议，ping 127.0.0.1，测试本机TCP/IP是否正常。

(5)保留的私有地址：该地址不可以在公网上使用，可在局域网使用：若路由器遇到目的地为私有地址数据包，一律不转发到外网。

表1-5 私有IP地址列表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 类别 | 网络个数 | 私网网络地址 | 所有IP地址范围 | 每个网络中主机IP地址数量 |
| A | 1 | 10.0.0.0 | 10.0.0.0—10.255.255.255 | 224-2 |
| B | 16 | 172.16.0.0—172.31.0.0 | 172.16.0.0—172.31.255.255 | 216-2 |
| C | 256 | 192.168.0.0—192.168.255.0 | 192.168.0.0—192.168.255.255 | 28-2 |

1. ****分等级的IP 地址结构。****

**IP 地址被分为网络位和主机位两部分，有以下原因：**

第一，IP 地址管理机构在分配 IP 地址时只分配网络号，而剩下的主机号则由得到该网络号的单位自行分配。方便了 IP 地址在本机构内部的分配和管理。

第二，路由器内的路由表项目包含大量的网络地址，路由器根据自己的路由表进行数据转发时，大部分是依据目的主机所连接的网络号来转发分组，使得路由表中的项目数大幅度减少，从而减小了路由表所占的存储空间，提高路由查询速度。

1. 允许一个设备配置多个IP地址

IP 地址是标志“一个主机(或路由器)和一条链路的接口”，当一个主机同时连接到两个网络上时，该主机就必须同时具有两个相应的 IP 地址，其网络号 net-id 必须是不同的。这种主机称为多归属主机(multihomed host)。

(9)按照因特网的观点，一个网络是具有相同网络号net-id的主机的集合，因此，用集线器、中继器或网桥连接起来的若干个局域网仍为一个网络，这些局域网都具有同样的网络号，具有不同网络号的局域网需使用路由器进行互连。

●(2018.11)下列关于私有地址个数和地址的描述中，都正确的是 (52) 。

(52)A.A类有10个:10.0.0.0—10.10.0.0 B.B类有16个:172.0.0.0—172.15.0.0

C.B类有16个:169.0.0.0—169.15.0.0 D.C类有256个:192.168.0.0—192.168.255.0

●(2018.11)以下IP地址中，既能作为目标地址又能作为源地址，且以该地址为目的地址的报文在Internet上通过路由器进行转发的是 (53) 。

(53)A.0.0.0.0 B.127.0.0 C.100.10.255.255/16 D.202.117.112.5/24

●通常路由器不进行转发的网络地址是 (46) 。

(46)A.101.1.32.7 B.192.178.32.2 C.172.16.32.1 D.172.35.32.244

●(2007.5)以下地址中属于D类地址的是 (27)。

(27)A．224.116.213.0 B．110.105.207.0 C．10.105.205.0 D．192.168.0.7

● (2012.5)IP地址分为公网地址和私网地址，以下地址中属于私网地址的是(52)。

(52)A．10.216.33.124 B．127.O.O.1 C．172.34.21.15 D．192.32.146.23

●(2015.11)如果要检查本机的IP协议是否工作正常，则应该ping的地址是 (55) 。

(55)A.192.168.0.1 B.10.1.1.1 C.127.0.0.1 D.128.0.1.1

●(2017.11)在一台安装好TCP/IP协议的计算机上，当网络连接不可用时，为了测试编写好的网络程序，通常使用的目的主机IP地址为(69).

(69)A. 0.0.0.0 B.127.0.0.1 C.10.0.0.1 D.210.225.21.255/24

### 1.4.2 IP数据报构成及转发过程

IP(Internet Protocol，网络互联协议)：是网际层核心协议，为传输层提供不可靠、无连接的数据报传送服务，无连接的传输即指没有确定目标系统在已做好接受数据准备之前就发送数据。不可靠的服务即指目的系统不对成功接收得分组进行确认，IP只是尽可能地使数据传输成功。主要有IPV4 和IPV6版本，默认情况指IPV4版本。

一个 IP 数据报由首部和数据两部分组成。首部的前一部分是固定长度，共 20 字节，是所有 IP 数据报必须具有的。在首部的固定部分的后面是一些可选字段，其长度是可变的。

1. IP数据报构成

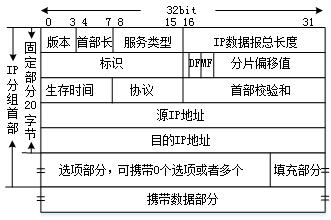


图1-18 IP数据报的格式

1)、固定部分*：*

(1)版本： 4 bit，指IP协议的版本,目前的 IP 协议版本号为 4 (即 IPv4)，即该字段为0100；

(2)首部长——占 4 bit，可表示的最大数值二进制为1111，对应十进制为 15，此时表示首部长度为15个单位，此处一个单位即为 4 字节，因此 IP 的首部长度的最大值是15\*4=60字节，当IP分组的首部长度不是4字节的整数倍时，需要利用最后的填充字段加以填充，以保证整个首部为4字节的整倍数，当首部最短时，即只有固定部分，此时长度部分填写值为5，即二进制0101。

(3)服务类型： 8 bit，使主机告诉网络它希望获得什么样的服务，可以是可靠性和速度的各种组合，通常对于声音、图像等信息希望获得较高的速度，对于文件的传输希望获得更高的可靠性，几乎没有被人们使用。

(4)总长度： 16 bit，指首部和数据之和的长度，单位为字节，因此数据报的最大长度为 216-1=65535 字节。

在IP层下面的每一种数据链路层都有其自己的帧格式，其中包括帧格式中数据字段的最大长度，称为最大传输单元MTU(Maximum Transfer Unit)，当一个IP数据报封装成链路层的帧时，此数据报的总长度(首部加上数据部分)一定不能超过下面的数据链路层的MTU值。当超过时，就不惜把过长的数据报进行分片后才能在网络上传输。这时，数据报首部中的“总长度”字段不是指未分片前的数据报长度，而是指分片后的每一个分片的首部长度和数据长度的总和。

(5)标识(identification)——占 16 bit，它是一个计数器，用来产生数据报的标识，没发送一份报文，该值会增大1，当一个大的数据报被分片后，所有分片具有该总数据报的标识，以便目的主机能够识别每个分片属于哪个总的数据，以便进行合并。

(6)标志(flag)：3 bit，目前只有两个比特有意义。

* 标志字段的最低位是 MF (More Fragment)。若某个分片内MF = 1， 表示该分组后面“还有分片”。MF = 0 表示该分组是若干数据报分片中的最后一个分片。
* 标志字段中间的一位是 DF (Don't Fragment)，意思是“不能分片”，当 DF = 0 时才允许该分组继续分片，若DF=1，则命令路由器不能将其分片，因为目的地不具备重组功能或者该数据有特殊功能不允许分片。

(7)分片偏移值(12 bit) ：13位，指出：较长的分组在分片后，某分片在原分组中的相对位置，即相对用户总片中，该片包含的数据部分相对于总片数据部分向后的偏移长度，即该片是从总数据何处开始，该值计算以 8 个字节为偏移单位进行计算。

例：一个数据报的总长度为3820字节，其数据部分为3800字节长，经过某些网络是由于网络因素，需要分片为长度不超过1420字节的数据报片。经计算总报片只有固定首部，长度为20字节，因此每个数据报片也仅包含20字节首部，每个分片数据部分长度不能超过1400字节。三个分片数据部分长度分别为1400、1400和1000字节数据报，原始数据报首部数据被复制为各数据报片的首部，其中某些字段值进行相应修改。

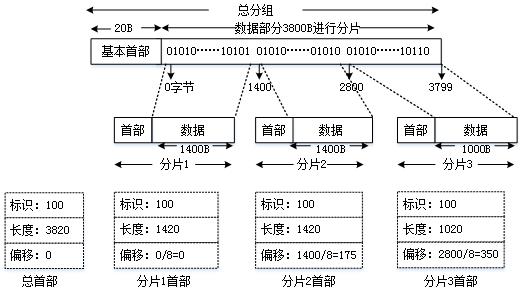


图1-19 数据报的分片举例

表1-8 IP数据报首部中与分片有关的字段中的数值

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | 总长度 | 标识 | MF | DF | 片偏移值 |
| 原始数据报 | 3820 | 100 | 0 | 0 | 0 |
| 数据报片1 | 1420 | 100 | 1 | 0 | 0 |
| 数据报片2 | 1420 | 100 | 1 | 0 | 175 |
| 数据报片3 | 1020 | 100 | 0 | 0 | 350 |

(8)生存时间：8 bit，记为 TTL (Time To Live)，用“跳数”作为 TTL 的单位，最大值为255(即二进制为11111111)，由发出数据报的原点设置这个字段(通常设置为32或64)，指明数据报在因特网中之多可经过多少路由器，数据报每经过一个路由器，路由器就将该分组内 TTL 值减 1，若减1后该分组内TTL为0，则丢弃该分组，此时丢弃该分组的路由器会发送一个特殊的ICMP报文通知源点，该值是为了防止无法交付的数据报无限制地在网络中兜圈子，浪费网络资源。若某IP数据报被源点设置TTL初值为1，经过路由时，TTL为0，路由将不会将该报文转至外网，此时就表示这个数据报只能在本局域网中传送。

(9)协议：8 bit，字段指出此数据报携带的数据使用何种协议，以便目的主机的 IP 层将组装好的整个报文的数据部分上交给哪个处理过程，该协议编号在整个因特网上通用。

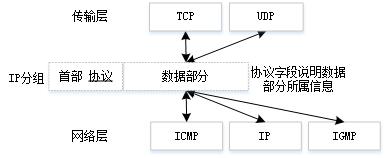


图1-20协议字段用途

表1-9 协议字段值

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 协议名 | ICMP | IGMP | IP | TCP | EGP | IGP | UDP | IPv6 | ESP | OSPF |
| 协议字段值 | 1 | 2 | 4 | 6 | 8 | 9 | 17 | 41 | 50 | 89 |

(10)首部检验和：16 bit，只检验数据报的首部，不包括数据部分，分组在转发过程中每个结点接收数据后都要进行检验和重新计算，若发现收到数据检验结果不正确，将其丢弃，避免错误的数据在网络中继续转发浪费网络资源。

(11)源地址：32 bit，即4 字节。

(12)目的地址：32 bit，即4 字节。

2)、IP 数据报首部的可变部分

IP 首部的可变部分就是一个选项字段，用来支持排错、测量以及安全等措施，内容很丰富。选项字段的长度可变，从 1 个字节到 40 个字节不等，取决于所选择的项目。增加首部的可变部分是为了增加 IP 数据报的功能，但这同时也使得 IP 数据报的首部长度成为可变的。这就增加了每一个路由器处理数据报的开销。实际上这些选项很少被使用。

表1-10 IP数据报可变**选项**

|  |  |
| --- | --- |
| 选项 | 意义描述 |
| 安全性(security) | 指明数据报的机密程度，实际应用中常被忽略不计 |
| 严格的源路由选择(strict soure routing) | 携带一系列IP地址，包含从源端到目的端的完整路径，数据必须严格按照该IP地址顺序和个数进行传输，不能通过其它任何非列表指定的路由，常用于测量源端到目的端时间时使用 |
| 松散源路由选择(loose soure routing) | 携带一系列IP地址，要求数据必遍按照顺序遍历列表中所列IP地址，但数据可以在穿过两个IP地址中间的其它路由器，常用于指定少量必须经过的重点路径信息 |
| 记录路由(record route) | 使沿途路由器能将其IP地址记录其中，用于管理者追踪发现路由选择算法的错误 |
| 时间标记(time stamp) | 使沿途路由器将其IP地址和时间标记记录其中，同样用于为路由选择算法进行排错 |

2.IP数据报转发算法

数据交付到主机网络层时，主机网络层会依据主机内路由信息将信息转发网关，当路由器收到分组后，依次查询路由表内信息，并按照转发算法进行分组转发，分组转发算法如下:

(1)从数据报的首部提取目的站的 IP 地址 ，首先检查该IP地址是否为本机IP地址之一或为广播IP地址，如果是，数据报就交由IP首部中“协议”指明的模块进行处理，如果不是这些地址，开始使用路由表进行路由查找和转发。

(2) 提取目的站的 IP 地址D, 得出目的网络地址为 N若网络 N 与此路由器直接相连，则直接将数据报交付给目的站 D；否则是间接交付，执行(3)。

(3) 若路由表中有目的地址为 *D* 的特定主机路由，则将数据报传送给路由表中所指明的下一跳路由器；否则，执行(4)。

(4) 若路由表中有到达网络 *N* 的路由，则将数据报传送给路由表指明的下一跳路由器；否则，执行(5)。

(5) 若路由表中有一个默认路由，则将数据报传送给路由表中所指明的默认路由器；否则，执行(6)。

(6) 报告转发分组出错。

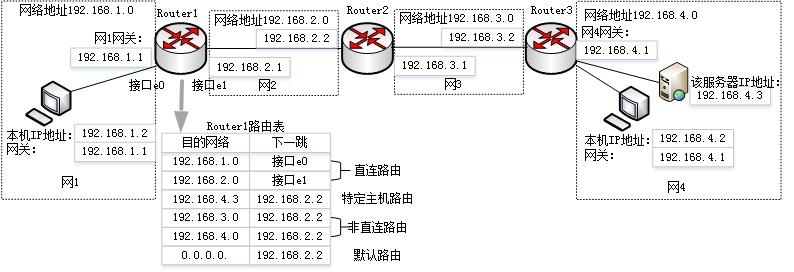


图1-21通过路由器R的路由表转发分组

特定主机路由：即对特定的目的主机指明一个路由；因特网所有的分组转发大多数基于目的主机所在的网络的网络地址，以便减小路由表长度，节约存储空间，采用特定主机路由可使网络管理人员能够更方便地控制网络和测试网络，同时也可在需要考虑某种安全问题时采用这种特定主机路由。

默认路由(default route)：没有其他路由选择时的选择路由，在TCP/IP协议族中，默认路由的网络地址为0.0.0.0。

●(2018.11)IP数据报首部中IHL ( Internet首部长度)字段的最小值为 (65) 。

(65)A.5 B.20 C.32 D.128

●(2013.5)在网络层采用分层编址方案的好处是(18)。

(18)A.减少了路由表的长度 B.自动协商数据速率 C.更有效地使用MAC地址 D.可以采用更复杂的路由选择算法

●(2017.5)IPv4首部中首部长度字段(IHL)的值最小为 (20)，为了防止IP数据报在网络中无限制转发，IPv4首部中通过(21)字段加以控制。

(20)A.2 B.5 C.10 D.15

(21)A.URG B.Offset C.More D.TTL

●(2017.11)IP数据报经过MTU较小的网络时需要分片。假设一个大小为1500的报文分为2个较小报文，其中一个报文大小为800字节，则另一个报文的大小至少为 (22) 字节。

(22)A.700 B.720 C.740 D.800

●(2017.11)IPv4首部中填充字段的作用是 (23) 。

(23)A.维持最小帧长 B.保持IP报文的长度为字节的倍数 C.确保首部为32比特的倍数 D.受MTU的限制

### 1.4.3 划分子网

1. 划分子网

划分子网(subnetting)即从 1985 年起在 IP 地址中又增加了一个“子网号字段”，使两级的 IP 地址变成为三级的 IP 地址的做法。是从主机号借用若干个比特作为子网号 subnet-id，而主机号 host-id 也就相应减少了若干个比特。IP地址结构如下：

IP地址 ::= {<网络号>, <子网号>, <主机号>}

2.子网掩码构成

子网掩码长度为32位数字，由左侧一串1和随后的一串0组成，子网掩码中1对应IP地址中原来的网络号和子网号，子网号的比特宽度由所需要划分的子网，0对应的是划分子网后每个子网中剩余的主机位。



图1-22划分子网后各地址特征

将某IP地址和其配套子网掩码进行逻辑与运算即可获得该机所在网络的网络地址，

AND 运算规则：1 AND 1=1 1AND 0=0 0 AND 0=0

例题1： 某网络上一主机配置IP地址是128.127.72.32，配置子网掩码未255.255.192.0，试求该主机所在网络的网络地址？

过程：将IP地址与子网掩码进行逻辑与运算，以下为计算过程，计算中为简单起见，仅将同时包含主机位和网络位的字节展开形成二进制：

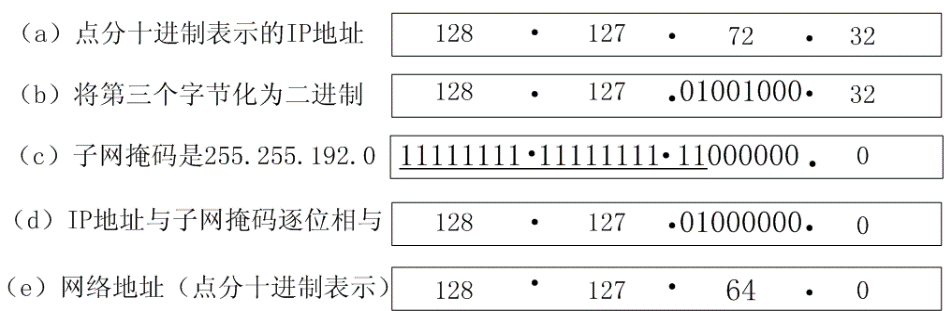


图1-24 网络地址计算例1

例题2：上例中IP地址不变，是128.127.72.32，子网掩码使用255.255.224.0，试求该地址所在子网网络地址？



图1-25 网络地址计算例2

3. 划分子网的情况下路由器转发分组算法

在划分子网的情况下，路由表内记录子网掩码信息，路由器转发分组的算法如下：

(1) 从收到的分组的首部提取目的 IP 地址 D。

(2) 先用各网络的子网掩码和 D 逐比特相“与”，看是否和相应的网络地址匹配。若匹配，则将分组直接交付。否则就是间接交付，执行(3)。

(3) 若路由表中有目的地址为 D 的特定主机路由，则将分组传送给指明的下一跳路由器；否则，执行(4)。

(4) 对路由表中的每一行的子网掩码和 D 逐比特相“与”，若其结果与该行的目的网络地址匹配，则将分组传送给该行指明的下一跳路由器；否则，执行(5)。

(5) 若路由表中有一个默认路由，则将分组传送给路由表中所指明的默认路由器；否则，执行(6)。

(6) 报告转发分组出错。

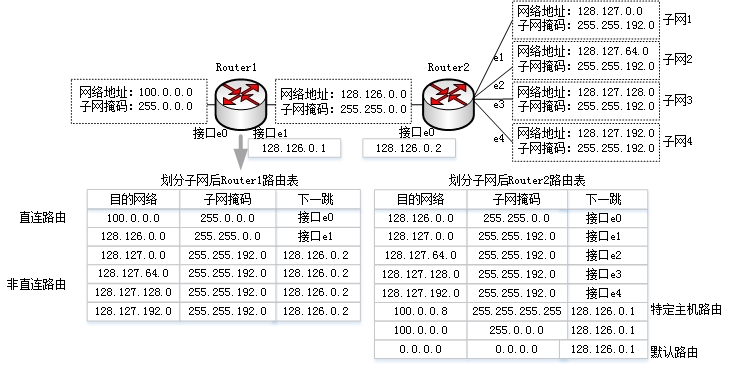


图1-23划分子网后路由表内容

●(2008.11)一个B 类网络的子网掩码为255.255.192.0，则这个网络被划分成了 (52) 个子网。

(52)A. 2 B. 4 C. 6 D. 8

●(2009.5)在Windows系统中设置默认路由的作用是(67)。

(67)A.当主机接收到一个访问请求时首先选择的路由 B.当没有其它路由可选时最后选择的路由

C.访问本地主机的路由 D.必须选择的路由

●(2013.11)在路由表中设置一条默认路由，目标地址应为 (46) ，子网掩码应为 (47) 。

(46)A. 127.0.0.0 　　 B. 127.0.0.1 　 C. 1.0.0.0 　　 D. 0.0.0.0

(47)A. 0.0.0.0 　　　 B. 255.0.0.0　 　 C. 0.0.0.255 　 D. 255.255.255.255

●(2015.5) (18) 时使用默认路由。

(18)A.访问本地Web服务器 B.在路由表中找不到目标网络 C.没有动态路由 D.访问ISP网关

●(2015.11)以下4种路由中，(69)路由的子网掩码是255.255.255.255。

(69)A.远程网络 B.静态 C.默认 D.主机

4.默认子网掩码

现在因特网规定，无论是否划分子网，都要设置子网掩码，若不划分子网，那么该网络的子网掩码就是使用默认子网掩码，即子网掩码中1的位置和二级IP地址中的网络号部分相对应。

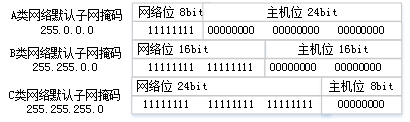


图1-26 A 类B类 C类IP地址的默认子网掩码

**3. 定长子网划分**

例子：某公司获得了C类网络号202.116.94.0，该公司有A.B.C.D共4个部门，各部门的计算机数量均60台.公司要求对获得的网络地址进行划分，每个部门划分到不同的子网中。

定常划分子网，划分子网4个，需要占取2位主机位，主机位有6位，每个子网可分配的IP地址最多为26-2=62个，刚好够用，子网掩码为255.255.255.192.

表1-9各部门IP网段汇总表

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 部门 | 网络地址 | 地址范围 | 子网掩码 | 可分配地址数量 | 广播地址 |
| A | 202.116.94  .0(00000000) | 202.116.94.01(00000001)--  202.116.94.62(00111110) | 255.255.255.192 | 26-2 | 202.116.94  .63(00111111) |
| B | 202.116.94  .64(01000000) | 202.116.94.65(01000001)--  202.116.94.126(01111110) | 255.255.255.192 | 26-2 | 202.116.94  .127(01111111) |
| C | 202.116.94  .128(10000000) | 202.116.94.129(10000001)--  202.116.94.190(10111110) | 255.255.255.192 | 26-2 | 202.116.94  .191(10111111) |
| D | 202.116.94.  192(11000000) | 202.116.94.193(11000001)--  202.116.94.254(11111110) | 255.255.255.192 | 26-2 | 202.116.94  .255(11111111) |

**4．可变子网掩码**

VLSM(Variable Length Subnet Mask)可变子网掩码。

例如,某公司获得了C类网络号202.116.94.0，该公司有A.B.C.D共4个部门，各部门的计算机数量分别为120、60、30和28.公司要求对获得的网络地址进行划分，每个部门划分到不同的子网中。

如果定常划分子网，要划分子网4个，需要占取2位主机位，主机位有6位，每个子网可分配的IP地址最多为26-2=62个，由于A部门有120台主机，不够，需采用VLSM。

A. 120台 需主机位7位 子网掩码：255.255.255.10000000

B. 60台 需主机位6位 子网掩码：255.255.255.11000000

C. 30台 需主机位5位 子网掩码：255.255.255.11100000

D. 28台 需主机位5位 子网掩码：255.255.255.11100000

表1-10 各部门IP网段汇总表

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 部门 | 网络地址 | 地址范围 | 子网掩码 | 可分配地址数量 | 广播地址 |
| A | 202.116.94  .0(00000000) | 202.116.94.0-  202.116.94.127 | 255.255.  255.128 | 27-2 | 202.116.94  .127(01111111) |
| B | 202.116.94  .128(10000000) | 202.116.94.128-  202.116.94.191 | 255.255.  255.192 | 26-2 | 202.116.94  .191(10111111) |
| C | 202.116.94  .192(11000000) | 202.116.94.192-  202.116.94.223 | 255.255.  255.224 | 25-2 | 202.116.94  .223(11011111) |
| D | 202.116.94.  224(11100000) | 202.116.94.224-  202.116.94.255 | 255.255.  255.224 | 25-2 | 202.116.94  .255(11111111) |

**进行网段划分时，通常采用先大后小的策略，先确定大的网段，再逐步确定小网段。**

●(2018.11)把IP网络划分成子网的好处是 (55) 。

(55)A.减小冲突域的大小 B.减小广播域的大小 C.增加可用主机的数量 D.减轻路由器的负担

●A类网络是很大的网络，每个A类网络中可以有 (66)个网络地址。实际使用中必须把A类网络划分为子网，如果指定的子网掩码为255.255.192.0，则该网络被划分为 (67)个子网。(软社)

(66)A. 210  B. 212  C. 220  D. 224

(67)A. 128 B. 256 C. 1024 D. 2048

●(2015.11)采用可变长子网掩码可以把大的网络分成小的子网，例如把A类网络60.15.0.0/16分为两个子网，假设第一个子网为60.15.0.0/17，则另一个子网为(52)。

(52)A.60.15.1.0/17 B.60.15.2.0/17 C.60.15.100.0/17 D.60.15.128.0/17

### 1.4.4 构成超网

CIDR(读音 “dider”)正式名字是无分类域间路由选择,特点：

* CIDR 消除了传统的 A 类、B 类和 C 类地址以及划分子网的概念。IP 地址从三级编址(使用子网掩码)又回到了两级编址：

IP地址 ::= {<网络前缀>, <主机号>}

使用“斜线记法”，即在IP地址后面加上斜线“/”，然后写上网络前缀占的位数，如地址128.14.32.0/20， /20表示该地址中左侧20位为网络前缀。

* CIDR把网络前缀相同的连续的IP地址组成一个“CIDR地址块”。知道该块中任一地址，即可知该块的最小地址和最大地址：如下IP地址，其中前20位是网络前缀，后面的12位为主机号：

128.127.33.0/20=**10000000 01111111 0010** 0001 00000000

该IP地址所在CIDR 地址块记为：128.127.32.0/20 **10000000 01111111 0010** 0000 00000000

该地址块中最小主机IP地址为： 128.127.32.1 **10000000 01111111 0010** 0000 00000001

该地址块中最大主机IP地址为： 128.127.47.254 **10000000 01111111 0010** 1111 11111110

该地址块广播地址为： 128.127.47.255 **10000000 01111111 0010** 1111 11111111

该地址块共包含主机IP地址总数为： 212-2=210\*22-2=1024\*4-2=4094

CIDR的斜线记法中，斜线后的数字就是地址掩码中1的个数，也可叫子网掩码。

如128.127.33.0/20中/20地址块的地址掩码是：

**11111111 11111111 1111**0000 00000000

计算128.127.33.0/20所在CIDR块，即将Ip地址合地址掩码相与即可，同子网掩码计算网络地址方法一样，即：

128 . 127 . 33 . 0

10000000 01111111 0010 0001 00000000

AND

11111111 11111111 1111 0000 00000000

————————————————————

10000000 01111111 0010 0000 00000000

128 . 127 . 32 . 0

CIDR记法多种形式，地址块10.0.0.0/10，可写为10/10，即把点分十进制中低位的连续0省略；

另外一种简化方法是在网络前缀的后面加上一个星号\*，如00001010 00\*

意思为星号之前为网络前缀，而\*表示IP地址中主机地址。

前缀长度不超过 23 bit 的 CIDR 地址块都包含了多个 C 类地址。这些 C 类地址合起来就构成了超网。

如地址块128.127.32.0/23 相当于包含两个c类网：**10000000 01111111 0010000** 0 00000000

第一个C类网的网络号：128.127.32.0 /24 **10000000 01111111 0010000** 0 00000000

第二个C类网的网络号：128.127.33.0 /24 **10000000 01111111 0010000** 1 00000000

表 1-11 常用CIDR前缀

|  |  |  |  |
| --- | --- | --- | --- |
| CIDR前缀长度 | 该前缀点分十进制表示 | 包含地址总个数 | 相当于包含C类网络个数 |
| /21 | 255.255.248.0 | 211=28\*8=2048 | 8个C网 |
| /22 | 255.255.252.0 | 21=28\*40=1024 | 4个C网 |
| /23 | 255.255.254.0 | 29=28\*2=512 | 2个C网 |
| /24 | 255.255.255.0 | 28=28\*1=256 | 1个C网 |

●(2019.5)假设某公司有 8000 台主机，采用 CIDR 方法进行划分，则至少给它分配 (51) 个 C 类网络。如果 192.168.210.181 是其中一台主机地址，则其网络地址 (52) 。

(51)A、8 B、10 C、16 D、32

(52)A、192.168.192.0/19 B、192.168.192.0/20 C、192.168.208.0/19 D、192.168.208.0/20

●(2019.5)路由器收到一个数据报文，其目标地址为 20.112.17.12，该地址属于 (53) 子网。

(53)A、20.112.17.8/30 B、20.112.16.0/24 C、20.96.0.0/11 D、20.112.18.0/23

●(2019.5)某校园网的地址是 202.115.192.0/19，要把该网络分成 30 个子网，则子网掩码应该是 (56) 。

(56)A、255.255.200.0 B、255.255.224.0 C、255.255.254.0 D、255.255.255.0

●(2006.5)是138.138.192.0/20，该校园网被划分为 (48) 个C类子网，不属于该校园网的子网地址是 (49) 。

(48)A.4 B.8 C.16 D.32

(49)A.138.138.203.0 B.138.138.205.0 C.138.138.207.0 D.138.138.213.0

●(2009.5) 某公司网络的地址是133.10.128.0/17,被划分成16个子网，下面的选项中不属于这16个子网的地址是 (53)。

(该题陷阱，要寻找一个非子网网络地址)

(53)A.133.10.136.0/21 B.133.10.162.0/21 C.133.10.208.0/21 D.133.10.224.0/21

地址聚合：将若干个CIDR块聚合成一个CIDE块，这个地址的聚合称为路由聚合，原因如下：

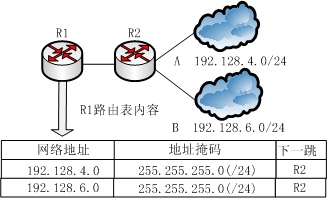


图1-27使用路由汇聚前路由表内容过长

路由汇聚计算过程：

(1) 将需要聚合的几个网段的地址转换为二进制表达方式。

(2) 比较这些网段，寻找他们IP地址前面相同的部分，从发生不同的位置进行划分，相同的部分作为网络段，而不同的部分作为主机段。

例如：有两个C类网址192.128.4.0/24和192.128.6.0/24，使用CIDR技术对他们进行聚合，得到的网络地址？

192.128.4.0/24 11000000 10000000 00000100 00000000

192.128.6.0 /24 11000000 10000000 00000110 00000000

地址聚合结果：192.128.4.0 /22 11000000 10000000 00000100 00000000

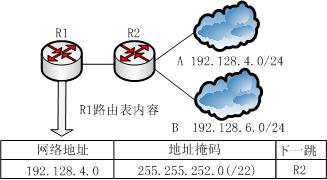


图1-28使用路由汇聚后路由表内容缩短

●(2018.11)网络192.21.136.0/24和192.21.143.0/24汇聚后的地址是 (54) 。

(54)A.192.21.136.0/21 B.192.21.136.0/20 C.192.21.136.0/22 D.192.21.128.0/21

●(2018.11)某主机接口的IP地址为192.16.7.131/26，则该IP地址所在网络的广播地址是 (56) 。

(56)A.192.16.7.255 B.192.16.7.129 C.192.16.7.191 D.192.16.7.252

●(2005.11)设有下面4条路由：172.18.129.0/24、172.18.130.0/24、172.18.132.0/24和172.18.133.0/24，如果进行路由汇聚，能覆盖这4条路由的地址是 (49) 。

(49)A. 172.18.128.0/21　　 B. 172.18.128.0/22　　C. 172.18.130.0/22 　　D. 172.18.132.0/23

●(2009.11)某用户分配的网络地址为192.24.0.0~192.24.7.0，这个地址块可以用 (49) 表示，其中可以分配 (50) 个主机地址。

(49)A．192.24.0.0/20　　 B．192.24.0.0/21 　　 C．192.24.0.0/16 　　 D．192.24.0.0/24

(50)A．2032 B．2048 C．2000 D．2056

●(2012.11)可以用于表示地址块220.17.0.0~220.17.7.0的网络地址是(57)，这个地址块中可以分配(58)个主机地址。

(57)A．220.17.0.0/20　　 B．220.17.0.0/21 C．220.17.0.0/16 D．220.17.0.0/24

(58)A．2032 　　 B．2048 　　 　 C．2000 　　 　　D．2056

●(2015.11)假设用户X有4000台主机，则必须给他分配(53)个C类网络。如果为其分配的网络号为196.25.64.0，则给该用户指定的地址掩码为(54)。

(53)A.4 　　 　　 　　 B.8 　　 　　 　　 　C.10 　　 　　 　　 D.16

(54)A.255.255.255.0 B.255.255.250.0 C.255.255.248.0 D.55.255.240.0

2、最长前缀匹配

* 使用 CIDR 时，路由表中的每个项目由“网络前缀”和“下一跳地址”组成。在查找路由表时可能会得到不止一个匹配结果。
* 应当从匹配结果中选择具有最长网络前缀的路由：最长前缀匹配(longest-prefix matching)，又称为最长匹配或最佳匹配。

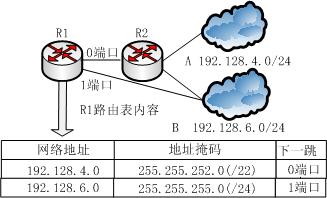


图1-29最长网络前缀匹配

假设R1收到某个数据报目的IP地址D=192.128.6.2，该如何转发，计算其所属地址块。

先计算第一条192.128.4.0/ 22是否匹配

源地址： 192 . 128 . 6 .2

二进制： 19212800000110 2

AND运算 ：11111111 11111111 1111110000000000

二进制结果： 192 . 128. 00000100 . 000000000

十进制结果 192. 128 . 4 . 0

匹配，可以按照路由转发。

再计算第二条路由是否匹配：

源地址： 192 . 128 . 6 .2

二进制： 19212800000110 2

AND运算 ：11111111 11111111 11111111 00000000

二进制结果： 192 . 128. 00000110 . 000000000

十进制结果 192. 128 . 6 . 0

匹配，可以按照路由转发。

此时，选择两个匹配的地址中更具体的一个，即选择最长前缀的地址。

●(2007.5)CIDR技术的作用是 (50) 。

(50)A.把小的网络汇聚成大的超网 B.把大的网络划分成小的子网

C.解决地址资源不足的问题 D.由多个主机共享同一个网络地址

● 地址192.168.37.192/25是 (54)，地址172.17.17.255/23是(55)。

(54)A．网络地址 B．组播地址 C．主机地址 D．定向广播地址

(55)A．网络地址 B．组播地址 C．主机地址 D．定向广播地址

●(2009.5)一个网络的地址为172.16.1.128/26,则该网络的广播地址是　(51)。

(51)A.172.16.1.255　　 B.172.16.7.129 C.172.16.7.191 D.172.16.7.252

●(2011.5)互联网规定的B类私网IP地址为 (51) 。

(51)A. 172.16.0.0/16 B. 172.16.0.0/12 C. 172.15.0.0/16 D. 172.15.0.0/12

●(2011.11) 32位的IP地址可以划分为网络号和主机号两部分。以下地址中，(51)不能作为目标地址，(52)不能作为源地址。

(51)A. 0.0.0.0 B. 127.0.0.1 C. 10.0.0.1 D. 192.168.0.255/24

(52)A. 0.0.0.0 B. 127.0.0.1 C. 10.0.0.1 D. 192.168.0.255/24

●(2012.11)把网络10.1.0.0/16进一步划分为子网10.1.0.0/18，则原网络被划分为(54)个子网。

(54)A．2 B．3 C．4 D．6

●(2013.11)某网络的地址是200.16.0.0，其中包含480台主机，指定给该网络的合理子网掩码是(53)，下面的选项中，不属于这个网络的地址是(54) 。

(53)A. 255.255.255.0 B. 255.255.252.0 C. 255.255.254.0 D. 255.255.248.0

(54)A.200.16.0.23 B. 200.16.3.0 C. 200.16.1.255 D.200.16.1.0

●(2013.11)两个主机的IP地址分别是10.11.7.24和10.11.7.100，要使得这两个主机包含在同一个子网中，则指定的子网掩码长度应该为(55)比特。

(55)A.25 B.26 C.27 D.28

●把网络117.15.32.0/23划分为117.15.32.0/27，则得到的子网是多少个？(26)。每个子网中可使用的主机地址是多少个？(27)

(26) A.4 B.8 C.16 D.32

(27) A.30 B.31 C.32 D.34

●(2014.5)下面的地址中属于单播地址的是 (55) 。

(55)A.125.221.191.255/18 B.192.168.24.123/30 C.200.114.207.94/27 D.224.0.0.23/16

●(2016.5)假设分配给用户U1的网络号为192.25.16.0—192.25.31.0，则U1的地址掩码应该为(54)；假设分配给用户U2的网络号为192.25.64.0/20，如果路由器收到一个目标地址为11000000.00011001.01000011.00100001的数据报，则该数据报应传送给用户(55)。

(54)A. 255.255.255.0 B.255.255.250.0 C.255.255.248.0 **D.255.255.240.0**

(55)A. U1 **B. U2**  C. U1或 U2 D.不可到达

●(2016.11)ISP分配给某公司的地址块为199.34.76.64/28，则该公司得到的IP地址数是(51) 。

(51)A.8 B.16 C.32 D.64

●(2016.11)下面4个主机地址中属于网络110.17.200.0/21的地址是(53) 。

(53)A. 110.17.198.0 B. 110.17.206.0 C. 110.17.217.0 D. 110.17.224.0

●(2016.11)某用户得到的网络地址范围为110.15.0.0～110.15.7.0，这个地址块可以用(54) 表示，其中可以分配(55) 个可用主机地址。

(54)A.110.15.0.0/20 B.110.15.0.0/21 C.110.15.0.0/16 D.110.15.0.0/24

(55)A.2048 B.2046 C.2000 D.2056

●(2016.11)CIDR技术解决了路由缩放问题。例如2048个C类网络组成一个地址块，网络号从192.24.0.0～192.31.255.0,这样的超网号应为 (68) ，其地址掩码应为(69) 。

(68)A．192.24.0.0 B．192.31.255.0 C．192.31.0.0 D．192.24.255.0

(69)A．255.255.248.0 B．255.255.255.0 C．255.255.0.0 D．255.248.0.0

●(2017.5)某单位IP地址需求数如下表所示，给定地址192.168.1.0/24，按照可变长子网掩码的设计思想，部门3的子网掩码是 (52) 。

|  |  |
| --- | --- |
| 二级单位名称 | IP地址需求数 |
| 部门1 | 100 |
| 部门2 | 50 |
| 部门3 | 30 |
| 部门4 | 10 |
| 部门5 | 10 |

(52)A.255.255.255.128 B.255.255.255.192 C.255.255.255.224 D.255.255.255.240

●(2017.5)假设某单位有1000台主机，则至少需分配(53)个C类网络，若分配的超网号为202.25.64.0，则地址掩码是(54)。

(53)A.4 B.8 C.12 D.16

(54)A.255.255.224.0 B.255.255.240.0 C.255.255 .248.0 D.255.255.252.0

●(2017.5)在网络101.113.10.0/29中，能接收到目的地址是101.113.10.7的报文的主机数最多有(55)个。

(55)A.1 B.3 C.5 D.6

●(2017.11)下面的地址中，可以分配给某台主机接口的地址是(54)。

(54)A.224.0.0.23 B. 220.168.124.127/30 C.61.10.191.255/18 D.192.114.207.78/27

●(2017.11)以下IP地址中，于网络201.110.12.224/28的主机IP是 (55)。

(55)A.201.110.12.224 B．201.110.12.238 C.201.110.12.239 D.201.110.12.240

●(2015.11)如果在查找路由表时发现有多个选项匹配，那么应该根据(55)原则进行选择。假设路由表有4个表项如下所示，那么与地址139.17.179.92匹配的表项是(56)。

(55)A．包含匹配 B．恰当匹配 C．最长匹配 D．最短匹配

(56)A．139.17.145.32 B．139.17.145.64 C．139.17.147.64 D．139.17.177.64

## 1.5 TCP/IP协议集

### 1.5.1 网络接口层协议

1、ARP(Address Resolution Protocol，地址转换协议)：用于实现逻辑地址(IP地址)向物理地址(MAC)转换。只能解析其他主机的物理地址。

1. 物理地址(MAC地址)

MAC地址长度为 6字节，即48bit，采用十六进制，如00-E0-50-D9-0D-36，当局域网适配器(网卡)生产时，该地址被写入到适配器中保存，网卡进行数据帧发送时，该地址则被填入到MAC帧的首部，所以是数据链路层使用的地址，

IEEE的注册管理机构RA(Registration Authority)是局域网全球地址的法定管理机构，负责分配6个字节中前三个字节(即左侧24bit)，全球生产适配器的厂商需向IEEE机构购买这三个字节作为公司标识符，MAC地址中后三个字节则由厂家自行设定，但不能重复，称为扩展唯一标识符(Extend Unique Identifier)，这种方式获取的48bit地址即为EUI-48，即MAC地址。

适配器有过滤功能，适配器从网络上每收到一个MAC帧，就使用硬件技术检查MAC帧中目的地址是否为本站允许接收的帧，如果允许则收下继续处理，否则丢弃，避免浪费主机其它过多资源。本站允许接收的帧

1. 单播帧(一对一)：即接收MAC帧中目的地址与本机硬件地址相同；
2. 广播帧(一对全体)：即该帧是发往本网上所有的站点进行接收，即48bit目的地址全为1，十六进制表达为：ff-ff-ff-ff-ff-ff
3. 多播帧(一对多)：即该帧是发往本网上部分的站点进行接收。

所有适配器至少能识别单播帧和广播帧，适配器通常需要使用专门软件识别多播帧。广播和多播地址只能作为目的地址使用。

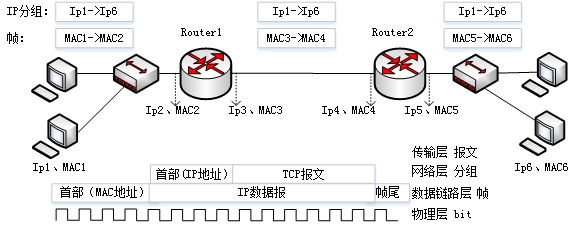


图 1-30 网络数据传输

(2)ARP 高速缓存(ARP cache)

每一个主机都设有一个 ARP 高速缓存(ARP cache)，存放了最近IP 地址到硬件地址的映射记录，为保证记录及时更新，每一项记录通常设置在缓存中的生存时间为20分钟，从记录建立时间算起，超过生存时间的记录被删除。

(3)ARP的请求应答帧格式

在以太网上解析IP地址对应的MAC地址时，发送的请求ARP帧和应答帧的格式如图，请求ARP帧和应答帧不单独传送，需要封装在以太网帧内，即作为以太帧的数据部分，使用该帧类型可完成ARP请求帧、ARP应答帧、RARP请求帧和RARP应答帧。

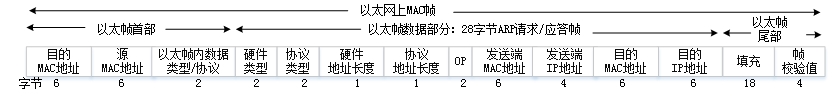


图 1-31 ARP帧格式

**以太帧首部和尾部字段意义：**

* 目的MAC地址：长6字节或2字节长，在10Mbps的基带网使用为6字节地址，若最高位为0，表示该地址是普通地址，若为1，表示地址为组播地址，该组中所有站点都能接收该帧，全1时表示目的地址为广播地址，即十六进制表达为：ff-ff-ff-ff-ff-ff，故当进行ARP请求时，因不明确目的地MAC地址，所以要进行广播询问，即请求该网络上所有站都接收该帧并查看，故此时“目的MAC地址”为全1，即十六进制表达为ff-ff-ff-ff-ff-ff，但只有本机IP地址和帧中目的IP地址一致的站点才给予ARP应答，该应答帧为单播。
* 源MAC地址：信息发源地的MAC地址。
* 以太帧内类型/协议：2个字节，说明帧后数据部分所使用的协议，如IP协议。或为长度字段，是指后边携带数据部分长度。
* 填充：以太网中最小帧长为64字节，当以太帧首和尾部以及数据部分不足64字节时，需进行填充，此处填充18个字节。
* 帧校验值：是4字节循环冗余检验码(CRC)，其检验范围包括从目的地址到数据字段结束的校验，只提供检错，不提供纠错功能。

以太帧封装ARP帧各字段意义：

* 硬件类型：填1时，表明为48bit的以太网地址；
* 协议类型：表明要解析的协议地址类型，为0x0800时，即表示要解析IP地址。
* 硬件地址长度和协议地址长度：表明上述硬件地址和协议地址的长度，使用以太网网址和IP地址时，此两处填写为6和4，表明他们长度分别为6字节和4字节。
* OP：即操作类型，共指明四种操作，分别是ARP请求(值为1)、ARP应答(值为2)、RARP请求(值为3)和RARP应答(值为4)，该字段必须，用以区分当前帧是哪种类型。
* 发送端MAC地址：和以太帧首部中源MAC地址一致，表明该帧来源；
* 发送端IP地址：源MAC地址对应的接口IP地址；
* 目的MAC地址：当该帧为ARP请求帧时，目的地MAC不明确，故此处填写48bit0，00-00-00-00-00-00.当系统收到一份该请求时
* 目的IP地址：当该帧为ARP请求帧时，填写准备解析的IP地址。

注意：当帧为ARP请求帧时，预解析目的IP地址所对应的MAC，故该帧应被该网上所有站点接收并处理，所以该帧发送时为广播帧，**以太帧首部中**目的MAC地址填写为ff-ff-ff-ff-ff-ff，**以太帧数据部分中的**目的MAC地址为00-00-00-00-00-00. 当目的主机给予ARP应答时，因信源和目的地MAC地址和IP地址已明确，该应答帧为单播，以避免其它主机不必要的处理，该应答MAC帧内的MAC地址和IP地址即为本次通信的两个端点的实际地址，帧内OP字段设置为2。

(4)ARP协议工作方式

ARP协议仅解析本网范围内MAC地址。

(1)发送方是主机，要把IP数据报发送到本网络另一个主机B，就先在其 ARP 高速缓存中查看有无主机 B 对应的硬件地址，有即将此硬件地址写入 MAC 帧，然后通过局域网将该 MAC 帧发往此硬件地址，若无，则主机自动运行ARP，获得B的硬件地址后，再发送。

(2)发送方是主机，要把IP数据报发给另一个网络上的一个主机，这时用ARP找到位于本局域网上的某个路由器的硬件地址，然后把分组发送给这个路由器，剩下的工作就由路由器来做。

(3)发送方是路由器，要把数据报转发到本网络上的一个主机，这时用ARP找到目的主机的硬件地址。

(4)发送方是路由器，要把IP数据报转发到另一个网络上的一个主机，这时用ARP找到本网路上一个路由器的硬件地址，剩下的工作就由该路由器来做。

代理ARP：当ARP请求询问的对象为不同网络的其他主机时，此时发送的ARP请求广播帧不能到达外网，而是由连接本网的路由器收到该广播询问帧，并将自己的MAC地址回答给该源主机，源主机会存储并使用该MAC地址，先将数据发送给路由，再由路由代替转发至外网，该路由即称为委托ARP或代理ARP。

说明：

* 路由器在转发数据时，路由表中存储的去往目地的“下一跳路由器的 IP 地址”不会被写入IP 数据报的首部中，而是调用ARP协议， 负责将“下一跳路由器的 IP 地址”转换成硬件地址，将此硬件地址放在链路层的 MAC 帧的首部，然后根据这个硬件地址找到下一跳路由器。
* ARP 是解决同一个局域网上的主机或路由器的IP 地址和硬件地址的映射问题。
* ARP 协议的解析工作是自动地进行，将IP 地址解析为链路层所需要的硬件地址，主机的用户对这种地址解析过程是不知道的。

4. arp命令

arp命令用于显示和修改IP地址和物理地址的映射表，称为ARP表。

格式：arp –a 查看地址解析表，其后可跟一个IP地址，此时就只显示该IP对应的物理地址.

arp –s 在arp缓存中添加项

例如：arp –s 192.168.0.1 ef-23-45-67-89-00

Arp –d删除arp缓存中的项

例如：arp –d 192.168.0.1

●(2018.11)ARP协议数据单元封装在 (23) 中传送。

(23)A.IP分组 B.以太帧 C.TCP段 D.ICMP报文

● (2011.11)ARP表用于缓存设备的IP地址与MAC地址的对应关系，采用ARP表的好处是(22)。

(22)A. 便于测试网络连接数 B. 减少网络维护工作量 C. 限制网络广播数量 D. 解决网络地址冲突

● (2012.5)ARP协议的作用是(18)，它的协议数据单元封装在(19)中传送。ARP请求是采用(20)方式发送的。

(18)A．由MAC地址求口地址 B．由IP地址求MAC地址 C．由IP地址查域名 D．由域名查碑地址

(19)A．IP分组 B．以太帧 C．TCP段 D．UDP报文

(20)A．单播 B．组播 C．广播 D．点播

●(2012.11)所谓“ 代理ARP”是指由(20)假装目标主机回答源主机的ARP请求。

(20)A．离源主机最近的交换机 B．离源主机最近的路由器 C．离目标主机最近的交换机 D．离目标主机最近的路由器

●(2015.5)当一个帧离开路由器接口时，其第二层封装信息中 (17) 。

(17)A.数据速率由10BASE-TX变为100BASE-TX B.源和目标IP地址改变

C.源和目标MAC地址改变 D.模拟线路变为数字线路

●通过CIDR技术，把4个主机地址220.78.169.5、220.78.172.10、220.78.174.15和220.78.168.254组织成一个地址块，则这个超级地址块的地址是(51)。

(51)A.220.78.177.0/21 B.220.78.168.0/21 C.220.78.169.0/20 D.220.78.175.0/20

●(2015.11)下列 (62) 设备可以隔离ARP广播帧。

(62)A. 路由器 B. 网桥 C. 以太网交换机 D. 集线器

●(2016.11)下面哪个协议可通过主机的逻辑地址查找对应的物理地址？ (20) 。

(20)A.DHCP B.SMTP C.SNMP D.ARP

●(2016.11)代理ARP是指(22) 。

(22)A.由邻居交换机把ARP请求传送给远端目标 B.由一个路由器代替远端目标回答ARP请求

C.由DNS服务器代替远端目标回答ARP请求 D.由DHCP服务器分配一个回答ARP请求的路由器

●(2017.5)关于ARP表，以下描述中正确的是(67) 。

(67)A.提供常用目标地址的快捷方式来减少网络流量     B.用于建立IP地址到MAC地址的映射

C.用于在各个子网之间进行路由选择    D.用于进行应用层信息的转换

●(2018.5)若主机hostA的MAC地址为aa-aa-aa-aa-aa-aa，主机 hostB的MAC地址为bb-bb-bb-bb-bb-bb。由hostA发出的查询hostB的MAC地址的帧格式如下图所示，则此帧中的目标MAC地址为(24)，ARP报文中的目标MAC地址为(25)。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 目标MAC地址 | 源MAC地址 | 协议类型 | ARP报文 | CRC |

(24)A.aa-aa-aa-aa-aa-aa B.bb-bb-bb-bb-bb-bb C.00-00-00-00-00-00 D.ff-ff-ff-ff-ff-ff

(25)A.aa-aa-aa-aa-aa-aa B.bb-bb-bb-bb-bb-bb C.00-00-00-00-00-00 D.ff-ff-ff-ff-ff-ff

2. RARP(Reverse Address Resolution Protocol，反向地址转换协议)：

用于实现物理地址向逻辑地址转换。如果本地主机拥有磁盘系统引导时，通常会从磁盘上的系统配置文件读取本机IP地址，对于无磁盘主机，需要调用RARP协议从网络上其它具有管理功能的主机上获取一个IP地址，此时无磁盘主机发送RARP请求，管理功能主机回送RARP应答，给予一个IP地址， RARP协议完成本机MAC地址解析出自身需要的IP地址功能，使用帧格式与ARP协议帧格式相同，主要差别是RARP请求或应答的帧类型代码为0x8035，RARP请求帧中OP值为3，RARP应答中OP值为4。RARP请求为广播，应答为单播。

●(2008.5)ARP协议的作用是由IP地址求MAC地址，ARP请求是广播发送，ARP响应是 (25) 发送。

(25)A．单播 B．组播 C．广播 D．点播

●(2012.11) 以下关于RARP协议的说法中，正确的是 (19) 。

(19)A．RARP协议根据主机IP地址查询对应的MAC地址 B．RARP协议用于对IP协议进行差错控制

C．RARP协议根据MAC地址求主机对应的IP地址 D．RARP协议根据交换的路由信息动态改变路由表

### 1.5.2网络层协议

1.IP协议，即IP数据报构成，略。

2. ICMP(Internet Control Message Protocol，因特网控制消息协议)：用于传输在TCP/IP通信中产生的错误报告、通信控制信息等，通常认为为网络层协议，也可被应用层直接调用。

ICMP 报文作为 IP 层数据报的数据，加上IP数据报的首部，组成一个完整 IP 数据报发送出去。

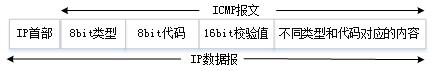


图1-32 ICMP 报文的格式

ICMP 报文的类型有两种，即 ICMP 差错报告报文和 ICMP 询问报文，又由类型字段和代码字段进一步确定该ICMP 报文的种类。

表1-11 ICMP 差错报告报文和 ICMP 询问报文

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 类型 | 报文内类型值 | 报文内代码值 | 报文意义描述 | 备注 |
| 差错类型 | 3 | 0 | 网络不可达 | 终点不可达报文 |
| 1 | 主机不可达 |
| 3 | 端口不可达 |
| 4 | 0 | 源端抑制 | 源站抑制报文 |
| 5 | 0 | 对网络重定向 | 改变路由(重定向)报文 |
| 1 | 对主机重定向 |
| 11 | 0 | TTL为0，即生存期超时 | 时间超过报文 |
| 1 | 数据报分片重组时间超时 |
| 12 | 0 | IP首部损坏 | 参数问题 |
| 1 | IP首部缺少必须项 |
| 询问类型 | 0 | 0 | 回显应答 | Ping命令使用后应答 |
| 8 | 0 | 请求回显 | Ping命令请求 |
| 13 | 0 | 时间戳请求 |  |
| 14 | 0 | 时间戳应答 |  |
| 17 | 0 | 地址掩码请求 | 已不再使用 |
| 18 | 0 | 地址掩码应答 | 已不再使用 |

1)、ICMP 差错报告报文：

ICMP 差错报告报文用于报告IP数据报在网络传输中的某些异常，故ICMP 差错报告报文始终包含它所监督的IP数据报的首部前8个字节。

(1)终点不可达： 报文类型值为3，当路由器或主机不能交付数据报时就向原点发送终点不可达报文，代码值有多种，包含网络不可达、主机不可达、协议不可达、端口不可达等情况，以及需要分片但DF比特已置为1以及源路由失败等情况，此时就向源站发送终点不可达报文。

(2)源站抑制： 报文类型值为4，当路由器或主机由于拥塞而丢弃数据报时，就向源点发送源点抑制报文，使源点知道应当把数据报的发送速率放慢。

(3)改变路由(重定向)：报文类型值为5，路由器把改变路由报文发送给主机，让主机知道下一次应将数据报发送给另外的路由器。

(4)时间超过：报文类型值为11，当路由器收到生存时间为零的数据报时，除丢弃该数据报外，还要向源点发送时间超过报文，此时报文中代码为0；当终点在预先规定的时间内不能收到一个数据报的全部数据报片时，就把已收到的数据报片丢弃，并向源点发送时间超过报文，此时报文中代码为1。

(12)参数问题：报文类型值为12，当路由器或目的主机收到的数据报的首部中有的字段的值不正确时，就丢弃该数据报，并向源点发送参数问题报文。

ICMP 差错报告报文的数据字段的内容

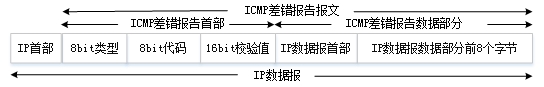


图1-33 ICMP差错报告报文

为避免网络风暴，不应发送 ICMP 差错报告报文的几种情况：

* 对 ICMP 差错报告报文不再发送 ICMP 差错报告报文。
* 对第一个分片的数据报片的所有后续数据报片都不发送 ICMP 差错报告报文。
* 对具有多播地址的数据报都不发送 ICMP 差错报告报文。
* 对具有特殊地址(如127.0.0.0或0.0.0.0)的数据报不发送 ICMP 差错报告报文。

3)ICMP 询问报文

(1)请求回显和回显应答报文 该报文是由路由器向一个特定的目的主机发出的询问，收到此报文的主机必须给源主机或路由发送ICMP回送回答报文。

(2)时间戳请求和应答报文 该报文是请求某个主机或路由器回答当前日期和时间。

(3)地址掩码请求和应答报文 该报文是请求某个主机或路由器回答当前地址掩码。

4) ICMP的应用

(1)PING (Packet InterNet Groper)

Ping 向目标主机(地址)发送一个回迸请求数据包，要求目标主机收到请求后给予答复，从而判断网络的响应时间和本机是否与目标主机(地址)连通性。**PING 使用了 ICMP请求回显和回显应答报文。 是应用层直接使用网络层 ICMP 的例子，它没有通过运输层的 TCP 或UDP。**

有以下常用格式：

例：ping –t 127.0.0.1表示不断的ping该IP地址，直到你按下ctrl+c终止该命令。

例：ping –a 192.168.0.1 表示将地址解析成计算机名

例：ping –n 5 192.168.0.2 表示ping命令将发送5个数据包出去探测，若不写表示默认，默认值是发送4个数据包。

例:Ping –i 120 202.98.192.67 表示设置了TTL＝120的ping命令

例：Ping [www.gzu](http://www.gzu).edu.cn表示ping某主机，与ping该主机IP地址效果是一样的。

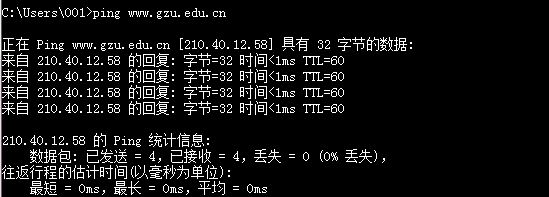


图1-34 ping命令使用

(2)Traceroute(是UNIX的命令)tracert(Windows中命令)

用来跟踪一个分组从源点到终点的路径。操作系统不同，使用的ICMP报文类型有所不同。

有些系统从源主机向目的主机发送一连串的IP数据报，数据报数据部分中封装的是无法交付的UDP数据报，数据报每一个数据报中首部中的生存时间TTL设置数依次递增，第一个数据报的TTL为1，当收到该数据报的路由器收到后会将TTL减1，由于TTL等于零了，故丢弃，由该接收UDP报文的端口向源主机发送一个ICMP时间超过差错报告报文，ICMP时间超过差错报告报文类型值为11(见表1-11)，该类型有两种代码值， 0和1,0表示TTL为0时发送的报文，1表示数据报分片重组时间超时报文，此时发送的为代码为0的报文。当数据报最终到达目的主机时，该数据报内封装一个非法的UDP端口号，目的主机没有任何一个程序使用该端口(通常端口值选择大于30 000)，目的主机丢弃该报文，并向源端发送一个**终点不可达报文中的端口不可达报文，最终探测完成。**

有些系统封装发送一连串的IP数据报数据部分中封装的是**ICMP请求回显报文**，而非UDP报文，同样首部中的生存时间TTL设置数依次递增，路径中间的接收该**ICMP请求回显报文**路由器端口均向源端发送代码值为0的ICMP时间超过差错报告报文，到达终点时由目的主机发送给源主机一个**回显应答报文，以完成探测。**

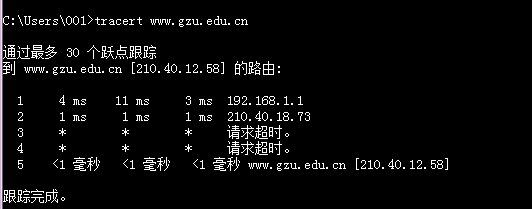


图1-35 路由跟踪图例

●(2009.11)Tracert命令通过多次向目标发送(23)来确定到达目标的路径，在连续发送的多个IP数据包中，(24)字段都是不同的。

(23)A．ICMP地址请求报文 B．ARP请求报文 C．ICMP回声请求报文 D．ARP 响应报文

(24)A．源地址 B．目标地址 C．TTL D．ToS

● (2013.11)下面关于ICMP协议的描述中，正确的是 (19) 。

(19)A．ICMP协议根据MAC地址查找对应的IP地址 B．ICMP协议把公网的IP地址转换为私网的IP地址

C．ICMP协议根据网络通信的情况把控制报文传送给发送方主机 D．ICMP协议集中管理网络中的IP地址分配

● (2013.11)ICMP协议属于TCP／IP网络中的(21)协议，ICMP报文封装在 (22) 协议数据单元中传送，在网络中起着差错和拥塞控制的作用。ICMP有13种报文，常用的ping程序中使用了 (23) 报文，以探测目标主机是否可以到达。如果在IP数据报传送过程中，发现生命期(TTL)字段为零，则路由器发出 (24) 报文。如果网络中出现拥塞，则路由器产生一个\_(25)\_ 报文。

(21)A．数据链路层 　 B．网络层 　 C．传输层 　 D．会话层

(22)A．IP B．TCP 　 C．UDP 　 D．PPP

(23)A．地址掩码请求／响应 B．回送请求应答 C．信息请求／响应 D．时间戳请求／响应

(24)A．超时 B．路由重定向 C．源端抑制 D．目标不可到达

(25)A. 路由重定向　 B．超时 　 C．源端抑制 　 D．目标不可到达

●(2016.5)某校园用户无法访问外部站点210.102.58.74，管理人员在Windows操作系统下可以使用 (43) 判断故障发生在校园网内还是校园网外。

(43)A.ping 210.102.58.74 B.tracert 210.102.58.74

C.netstat 210.102.58.74 D.arp 210.102.58.74

●(2016.5)使用ping命令可以进行网络检测，在进行一系列检测时，按照由近及远原则，首先执行的是(68)。

(68)A.ping默认网关 B.ping本地IP地址 C.ping 127.0.0.1 D.ping远程主机

● (2017.5)在windows操作系统中，采用 (28)命令来测试到达目标所经过的路由器数目及IP地址。

(28)A．ping B．tracert C．arp D．nslookup

●(2017.11)当站点收到“在数据报组装期间生存时间为0”的ICMP报文，说明 (60) 。

(60)A.回声请求没得到响应 B.IP数据报目的网络不可达

C.以为拥塞丢弃报文 D.因IP数据报部分分片丢失，无法组装

●(2017.11)测试网络连通性通常采用的命令是(70)。

(70)A.netstat B.ping C.msconfig D .cmd

●(2019.05)ARP 的协议数据单元封装在 (22) 中传送；ICMP 的协议数据单元封装在 (23) 中传送，RIP 路由协议数据单元封装在 (24) 中传送。

(22)A、以太帧 B、IP 数据报 C、TCP 段 D、UDP 段

(23)A、以太帧 B、IP 数据报 C、TCP 段 D、UDP 段

(24)A、以太帧 B、IP 数据报 C、TCP 段 D、UDP 段

3. IGMP(Internet Group Management Protocol，因特网组管理协议)：IP网络数据传输有两种常见方式：单播和广播，单播是在发送者和接收者之间实现点对点网络传输，广播是指某个IP网络内广播数据包，所有属于该网络的主机都将收到这些数据包，路由器将控制广播数据报的传输范围，防止它传送到其他网络去。组播是介于这两者之间的，是“一对一组“的通信模式，加入该组，就能收到该组其他成员发过来的数据报。

### 1.5.3传输层协议

一台主机可以提供许多服务，比如Web服务、FTP服务、SMTP服务等，唯一标识一个通信，首先要标识传输进程所在主机的NSAP(Network Service Access Point，网络层服务访问点)，即两端的IP地址，其次还要给IP地址对应主机上的每一个传输进程赋予一个本地唯一的标识符，TSAP(Transport Service Access Point 传输层的服务访问点)，即端口，在TCP/IP协议族中，端口号是两个字节长的数值，其取值范围是0—65535。

1.UDP(User Datagram Protocol：用户数据报协议)

一、UDP协议特点

UDP 只在 IP 的数据报服务之上增加了很少一点的功能，即端口的功能和差错检测的功能。虽然 UDP 用户数据报只能提供不可靠的交付，但 UDP 在某些方面有其特殊的优点。

(1)UDP 是无连接的，即发送数据之前不需要建立连接。

(2)UDP 使用尽最大努力交付，即不保证可靠交付，同时也不使用拥塞控制，但通信开销较小，应用于一些可靠性要求不高的地方，很适合多媒体通信的要求，如视频点播。若很多主机同时向网络发送大量高速率的实时视频流时，网络可能拥塞，目的主机都不能正常收到数据，产生严重问题。还有某些实时应用为适当改进UDP的不可靠服务，会增加一些纠错功能或重传部分丢失的报文。

(3)UDP 是面向报文的。UDP 没有拥塞控制，发送方 UDP 对应用程序交下来的报文，在添加首部后就向下交付 IP 层。UDP 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。应用层交给 UDP 多长的报文，UDP 就照样发送，即一次发送一个报文。接收方 UDP 对 IP 层交上来的 UDP 用户数据报，在去除首部后就原封不动地交付上层的应用进程，一次交付一个完整的报文。应用程序必须选择合适大小的报文。

(4)UDP 支持一对一、一对多、多对一和多对多的交互通信。

(5)UDP 的首部开销小，只有 8 个字节。

二、UDP报文首部

用户数据报 UDP 有两个字段：数据字段和首部字段。首部字段有 8 个字节，由 4 个字段组成，每个字段都是两个字节。

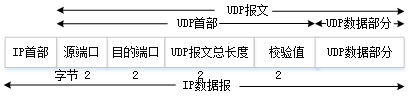


图1-36 UDP用户数据报的首部格式

(1)源端口： 源端口号，在需要对方回信时选用，不需要时可用全0.

(2)目的端口：去往目的地端口号，报文在交付给终点进程时必须使用，如果接收方发现报文中的端口号不正确，就丢弃该报文，并使用ICMP协议(因特网控制消息协议)向源端发送“端口不可达”信息，如从源点追踪目的点的时使用的tracert命令，最终达到目的地的报文中故意封装一个非法的UDP端口号，最终ICMP协议向源端发送“端口不可达”差错报告报文，从而源端达到测试目的地的作用。

(3)长度：UDP用户数据报的长度，当不携带任何数据，仅有首部时，长度为8字节。

(4)检验和：该校验值由发送端计算后填入，最后由接收端进行验证，用来检验首部和数据部分在传输过程中是否有错误，有错就丢弃该报文。但在进行检验和计算时，要使用IP数据报的部分字段临时作为伪首部，将伪首部、UDP报文首部和UDP报文数据部分一起进行计算，将计算的结果填入校验和字段。该伪首部仅仅在计算校验值时临时使用，不用来存储或者向上层交付。

2. TCP(Transmission Control Protocol，传输控制协议)

一、TCP协议特点

(1)TCP是一个面向连接的运输层协议,类似于生活中拨打固定电话一样,数据传送之前需要先建立连接,传送完毕后,必须释放连接，使用三次握手协议进行连接控制。

(2)每一条TCP连接唯一地连接着两个端点，不能提供多播和广播服务。

(3)TCP进行的数据传输保证无差错、不丢失、不重复，并且最终按正确顺序进行交付，即能够提供可靠的交付。

(4)TCP能进行全双工通信，连接的两个端点能同时进行收和发。双方都设置有数据缓冲存储区，用来存放应用层交下来的数据和对方传输过来的数据。

(5)面向字节流，即应用程序交给传输层一个有边界的数据块，但TCP不知道边界的作用和含义，仅仅当做是一连串无结构的字节流，在发送方应用层交下来的数据块个数和大小，不一定和接收方送到应用层的数据块个数和大小一致，TCP会根据相应情况进行调整，组成报文段(segment)进行传输。

(6)TCP使用可变大小的滑动窗口协议进行的流量和拥塞控制。

二、TCP报文首部

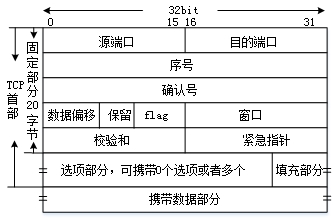


图1-37 TCP首部

(1)源端口和目的端口： 位于首部开头，各占16bit，和UDP端口作用相同。

(2)序号： 比特长度为32bit，范围从0--232-1，使用完毕时从新从0开始编号，为本报文段所发送第一个字节的编号，整个要传输的字节流的起始编号在双方进行三次握手时已设置。例如一共预传输500个字节，起始字节编号为0，本次报文准备传输的第一个字节编号为201，本次报文段准备传输数据量为100字节，则序号处填写201，下一个报文段的序号应填写为301，该序号也称报文段序号。

(3)确认号：比特长度为32bit，即4个字节，以“序号”字段中数据为例，如果接收方全部收到100个字节，则接收方向发送方发送的报文段内确认号填写为301，意即301号字节前的数据全部收到，期望收到的下一个字节序号为301.

(4)数据偏移：比特长度为4bit，是指该报文段中数据的起始位置，也说明该TCP报文段首部的总长度，包括固定部分和后续可变部分。如果该字段填写为1111，即对应十进制为15，不是指首部长度为15个字节，而是15个长度单位，每个长度单位实际表示4个字节，即实际长度为15\*4字节=60字节，表示数据部分相对于该报文段首部向后偏移60个字节，同时说明本报文段的首部固定部分和可变部分一共有60字节，即可变部分占40字节，也是可变部分的最长值。

(5)保留：占6bit，保留为今后扩展应用。

Flag字段包含以下部分：

(6)URG(紧急)：当此报文段中有紧急数据时，该值被设置为1，后面的“紧急指针”指明该报文段中哪个位置的数据为紧急数据，接收方在收到该报文段时将紧急数据放置在该报文段的最前面，优先处理，而其他数据仍为普通数据，如果该位置为0，则无紧急数据，所有数据按照原先顺序排队等待处理。

(7)ACK(确认)：当ACK=0时，说明“确认号”无效，ACK=1时，“确认号”字段有效，TCP中明确规定，连接建立后所有传输的报文段中ACK都必须设置为1.

(8)PSH(推送)：通常接收方会等到接收缓存填满时再将数据一并交给上层应用进程，如果发送方希望接收方立即对某个报文段处理，可发送一个报文段，将PSH设置为1，此时接收方会将这一批数据尽快交给应用进行，而不必等到缓存填满再递交。

(9)RST(复位或重建位)：当TCP出现严重差错，必须释放该连接，而后在重新建立连接时，可将RST设置为1发送给对方，同时该字段还可用来拒绝一个非法的报文段，或拒绝一个连接建立请求。

(10)SYN(同步)： 当一方准备和另一方建立连接时，将SYN=1和ACK=0，若对方同意建立连接，将回复的报文中SYN=1和ACK=1，SYN=1表明该报文是一个连接的建立请求或连接接收报文。

(11)FIN(终止)：当一方数据已经发送完毕，要求释放连接，可将发送的报文段中该字段设置为1.

Flag字段结束

(12)窗口：长度为16比特，2个字节，如果接收发到一个报文，其中窗口值为某一数值，假设为5，表明此时接收方的接收空间只能容纳下5个字节，此时发送方需调整自己的发送窗口值，不能连续发送超过5个字节，以使接收方来得及接收，避免接收方接收空间不足，造成数据丢失。如果经过一段时间，接收方接收空间变大，则向发送方发送的报文中窗口值即可调整为新的窗口值，TCP中使用的可变窗口值使得双方调整发送速率，实现流量控制。

(14)检验和：占16比特，即2个字节，检验范围包括首部和数据两部分，该校验值的计算方法和UDP首部检验和计算方法一致，使用伪首部进行计算，检错效率高，但不能纠错。

(15)紧急指针：占16比特，2字节，只有当URG=1时，该紧急指针才有效，指出本报文段中的紧急数据的结束位置，后边的仍为普通数据。

(16)选项：长度可变，最多可为40字节，当没有可选项目时，TCP报文段只有固定首部，长度为20字节。经常使用的选项包括“最大报文段长度”“选择确认”“时间戳”等。

三、TCP三次握手

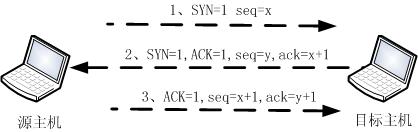


图 1-38 TCP建立连接的“三次握手”过程

第一步：源主机发送一个SYN(同步)标志位为1的TCP数据包，表示想与目的主机进行通信，并选择一个初始序号，如seq=x，TCP规定，SYN报文段(SYN=1的报文段)不能携带数据；

第二步：目标主机愿意进行通信，则响应一个确认，在确认报文段中应把SYN=1和ACK=1，确认号是ack=x+1，同时为自己选择一个初始序号seq=y，这个报文也不能携带数据。

第三步：源主机收到确认后，还要向目标主机给出确认。其中报文段中的ACK=1，确认号ack=y+1，而自己的序号seq=x+1，该报文段可以携带数据，但如果不携带数据则不消耗序号，在这种情况下，则下一个报文段的序号仍是seq=x+1.来想与目标主机的TCP包。

四、**端口分配**

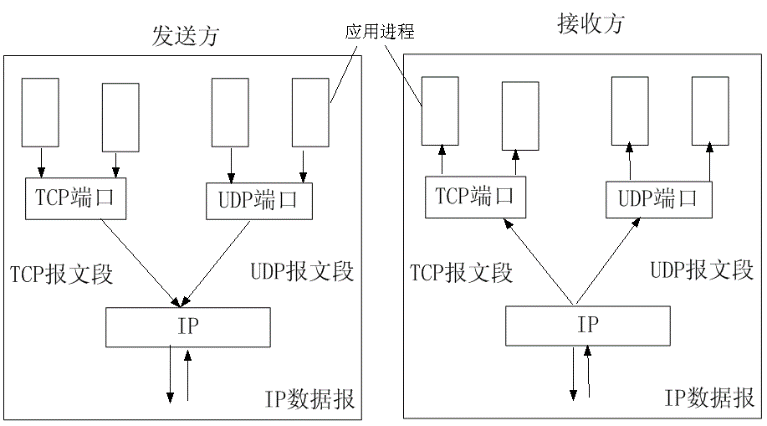


图1-39 端口在通信中所起的作用

在TCP/IP协议族中，端口号是两个字节长的数值，其取值范围是0—65535，作为资源来分配，其端口号的分配方式有：

全局分配： 由权威的中央机构进行统一分配，为常见的协议分配默认的端口号，比如用于浏览网页服务HTTP协议使用[80端口](http://baike.baidu.com/view/416685.htm)，用于FTP服务的[21端口](http://baike.baidu.com/view/416689.htm)。

本地分配： 当进程需要访问传输层服务时，向本地操作系统提出申请得到的端口号。

由于分配方式不同，端口名称也有所不同，如下：

**保留端口**：也称知名端口(Well-Known Port)或熟知端口，只占全部端口数量很小的一部分，不同机器上同样的服务，其端口号相同。TCP和UDP均规定小于1024的端口号(0—1023)才能作为保留端口，**为服务器端使用的端口号。**

**登记端口：**数值为1024-49151，这类端口号是为没有熟知端口号的应用程序使用的。但必须按照规定的手续登记后才能使用，以防重复，也**为服务器端使用的端口号**。

**自由端口**(Free port)：也称短暂端口号，数值为49152-65535，为本地方式分配， 是留给客户进程选择暂时使用。当服务器进程收到客户进程的报文时，就知道了客户进程所使用的端口号，因而可以把数据发送给客户进程。通信结束后，刚才的客户端口号就不存在了，站全部端口的绝大部分。

五. TCP命令

netstat：可以显示协议统计信息和当前的TCP/IP连接。

–a 显示所有连接的监听端口

-n 以数字形式显示监听的IP地址和端口号

-s 按各协议分别显示其统计数据

-r 显示路由表

-e 显示以太网卡统计数据

●(2011.11) TCP是互联网中的 (68) 协议，使用 (69) 次握手协议建立连接。

(68)A. 传输层 B. 网络层 C. 会话层 D. 应用层

(69)A. 1 B. 2 C. 3 D. 4

●(2012.5) TCP协议使用(26)次握手机制建立连接，当请求方发出SYN连接请求后，等待对方回答(27)，这样可以防止建立错误的连接。

(26)A．1 B．2 C．3 D．4

(27)A．SYN,ACK B．FIN，ACK C．PSH,ACK D．RST,ACK

●(2008.5) 在TCP协议中，采用 (22) 来区分不同的应用进程。

(22)A．端口号 B．IP地址 C．协议类型 D．MAC地址

●(2008.11)在TCP/IP 网络中，为各种公共服务保留的端口号范围是 (59) 。

(59)A. 1~255 B. 256~1023 C. 1~1023 D. 1024~65535

●(2012.11)下面哪个字段的信息出现在TCP头部而不出现在UDP头部？(60)。

(60)A．目标端口号 B.顺序号 C．源端口号 D.校验和

●(2015.11)TCP使用的流量控制协议是(68)。

(68)A.固定大小的滑动窗口协议 B.后退N帧的ARQ协议 C.可变大小的滑动窗口协议 D.停等协议

●(2017.11)相比于TCP,UDP的优势为 (66) 。

(66)A.可靠传输 B.开销较小 C.拥塞控制 D.流量控制

### 1.5.4 应用层协议

1. DNS( Domain Name System，实现域名到IP地址的解析)

* 概述：TCP/IP协议创建了一种ASCII码形式的主机命名形式，称为域名(Domain Name)，例如贵州大学主页域名[www.gzu.edu.cn](http://www.gzu.edu.cn), IP地址是210.40.0.58, DNS是一种分布式的网络目录服务，可以实现域名解析为IP地址,使用UDP的53号端口进行通信。
* 工作方式：应用程序需要解析域名时，则调用一个称为解析器的程序，将域名作为参数传递给该程序，解析器通常先在本地DNS缓存中查询对应IP地址，如果没有，再查询本机HOSTS表，如果仍没有，再将域名封装到一个UDP包中，发送给本地域名服务器；域名服务器内存储了大量域名和IP地址映射的目录，经查询，将域名地址映射的IP地址封装到另一个UDP包中，发回给解析器，解析器再将IP地址返回给调用者，有了IP地址后，应用程序和目的方建立一个TCP连接或发送UDP包，开始进行其他业务。 若本地域名服务器不能回答该查询请求，则本地域名服务器作为DNS一个客户向其它根域名服务器发出请求，再顶级域名服务器、权限域名服务器，过程简略。DNS大多数名字都进行本地解析，仅有少量解析需要在网络上通信。
* 域名层次：DNS采用一种层次型的命名机制。用“.”来分隔各层结点，子节点在前，父节点在后，如www.gzu.edu.cn，cn 是顶级域名(中国)，edu是二级域名(中国教育科研网的域名)，gzu是三级域名(贵州大学的域名)，www是四级域名。

表1-12 通用域名

|  |  |
| --- | --- |
| 通用域名 | 分配单位 |
| Com | 商业组织 |
| Edu | 教育机构 |
| Gov | 政府部门 |
| Mil | 军事部门 |

●(2014.5)某用户在使用校园网中的一台计算机访问某网站时，发现使用域名不能访问该网站，但是使用该网站的IP地址可以访问该网站，造成该故障产生的原因有很多，其中不包括 (69)。

(69)A．该计算机设置的本地DNS服务器工作不正常 B．该计算机的DNS服务器设置错误

C．该计算机与DNS服务器不在同一子网 D．本地DNS服务器网络连接中断

●(2017.5)在浏览器地址栏输入一个正确的网址后，本地主机将首先在 (66)查询该网址对应的IP地址。

(66)A.本地DNS缓存 B. hosts文件 C.本地DNS 服务器 D.根域名服务器

2. HTTP(HyperText Transfer Protocol，超文本传输协议)

概述：是应用层上一种请求/响应式的协议，实现客户端与服务器的通信，WWW发布信息的主要协议。HTTP通过URL(统一资源定位符)来定位Web服务器资源。URL是Internet上用来描述信息资源的字符串，包括服务器的域名(或IP地址)、目录和文件，默认连接端口是TCP 80。互联网上的每个文件都有一个唯一的URL，它包含的信息指出文件的位置以及浏览器应该怎么处理它。

基本URL包含模式(或称协议)、服务器名称(或IP地址)、路径和文件名，如“协议://服务器名称(或IP地址)/路径?查询”。

完整的、带有域名部分的普通统一资源标志符语法为“协议://用户名:密码@子域名.域名.顶级域名:端口号/目录/文件名.文件后缀?参数=值#标志”。例如

http：//www.microsoft.com/windows/default.html,其含义如下：

* + http：//：代表超文本传输协议。
    - [www.microsoft.com/](http://www.microsoft.com/)：代表Web服务器的域名，“microsoft.com”称为域名或直接域名，“www”称为主机名或主机头，[www.microsoft.com](http://www.microsoft.com)对应万维网上唯一一台主机。
    - windows/：该服务器上文件目录。
    - default.html：文件目录中的一个HTML文件。
    - 如果要使www.microsoft.com和microsoft.com打开同一页面，需要在Web服务器端进行具体的配置才行，也可配置为打开不同的页面。
* 工作原理：浏览器是用户来获取HTTP服务的软件，Html是一种语言，定义了文档的数据结构和显示方式，通过普通文本嵌入到标识符中，可以显示突破、文本、声音等内容。

用户在浏览器中输入 要访问的站点域名后，浏览器和Web服务器交互过程如下：：

(1) 浏览器分析超链指向页面的 URL。

(2) 浏览器向 DNS 服务器请求解析 www.tsinghua.edu.cn 的 IP 地址。

(3) 域名系统 DNS 解析出清华大学服务器的 IP 地址。

(4) 浏览器与该IP地址的服务器的端口80建立 TCP 连接

(5) 浏览器发出取文件命令：GET /index.htm。

(6) 服务器给出响应，把文件 index.htm 发给浏览器。

(7) TCP 连接释放。

(8) 浏览器显示文件 index.htm 中的所有文本。

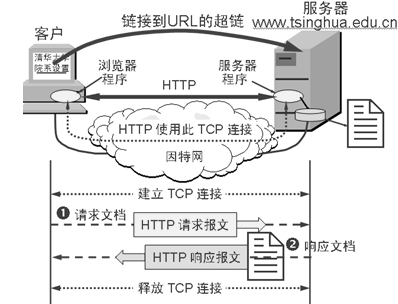


图1-40 HTTP工作过程表

●在地址http://www.dailynews.com.cn/channel/welcome.htm中,www.dailynews.com.cn表示(67)，welcome.htm表示(68)。

(67)A.协议类型 B.主机 C.网页文件名 D.路径

(68)A.协议类型 B.主机域名 C.网页文件名 D.路径

3. FTP( File Transfer Protocol，文件传送协议)

* 概述： FTP是因特网上使用得最广泛的文件传送协议，采用C/S工作模式。通过建立TCP连接，使网络上不同主机之间能够进行高效的文件传输，实现文件资源共享和信息传递。
* FTP传输：因为文件传输的两台计算机可能运行在不同的操作系统下，使用不同的数据类型和文件结构，所以FTP能将本地的数据类型翻译为ASCII码和二进制编码进行传输。
* FTP连接：FTP客户端先通过TCP 21号端口建立控制连接，传输控制信息，在控制连接建立的基础上，每当客户端要下载或上传文件时，再通过TCP 20号端口建立数据连接，传输数据。

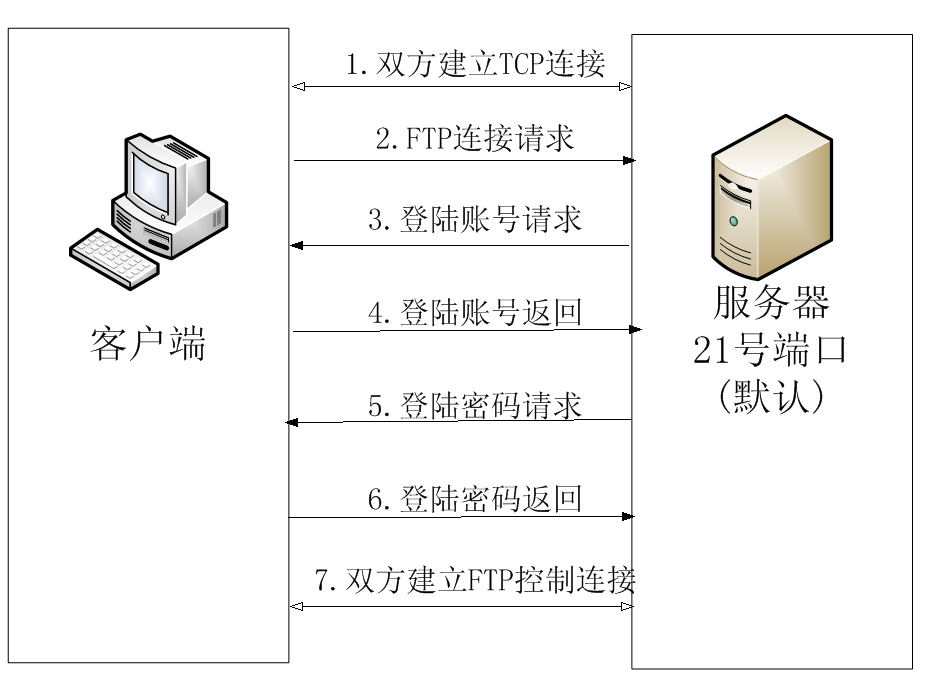


图1-41 FTP控制连接建立过程

* 匿名 FTP 访问通常使用anonymous作为用户名，可以使用认可字符串如guest或者使用者的E-mail作为密码。

因特网上所有的主机之间的通信其实是主机内运行的进程间的通信。按通信方式分为以下三类：

1. 客户/服务器方式(C/S模式)

客户**(client)**是服务请求方，服务器**(server)**是服务提供方，服务器对资源进行集中管理，提供给多个客户端使用，客户端是独立的计算机，能够从服务器获取数据资源。常见的数据处理方式为：客户端从服务器获取数据，然后对数据进行处理，将处理结果返回给服务器，允许多个客户端对数据进行共同访问和处理。客户端必须满足一定的硬件和软件要求，如客户端必须安装相应的数据处理软件，这就提高了客户端的管理和维护要求，增加了计算机网络管理和维护的成本。

2.浏览器/服务器类型(B/S模式)

浏览器/服务器类型，即**Browser/Server**模式，是指在浏览器技术产生后，数据的运算已无需在客户端进行。客户端在安装浏览器之后，只负责显示服务器发来的信息，然后将用户操作返回给服务器，数据的运算可以全部在服务器上进行。客户端只需要通过浏览器，就可以访问和显示任何服务器发来的信息，从而大大降低了网络的管理和维护的成本。这种模型称为浏览器/服务器类型(B/S模式)，又称为瘦客户端模型(Thin Client)，与之相对的C/S模型称为胖客户端模型(Fat Client)。

3.对等连接方式

对等连接(peer-to –peer，简写为P2P)是指两个主机在通信时不区分那一个是服务请求方，哪一个是服务提供方，只要双方都运行了对等连接软件(P2P软件)，他们就可以进行平等或对等连接通信，这是双方都可以下载对方已经存储在硬盘中的共享文档。

4. TFTP(Trivial File Transfer Protocol, 简单文件传送协议)

* TFTP 是一个很小且易于实现的文件传送协议。
* TFTP 采用C/S方式，使用 UDP 数据报，因此 TFTP 需要有自己的差错改正措施。
* TFTP 只支持文件传输而不支持交互。
* TFTP 没有一个庞大的命令集，没有列目录的功能，也不能对用户进行身份鉴别。
* 使用UDP69端口进行通信，利用确认和超时重传机制保证传输的可靠性。

5. DHCP/BOOTP(Dynamic Host Configuration Protocol，动态主机分配协议，Bootstrap Protocol自举协议)

* 概述：

BOOTP是一种基于UDP的协议，主要用于无盘工作站从服务器获得自己的IP地址。DHCP是从原来的BOOTP协议发展而来的，引入“租约“概念，分为两部分：服务器端和客户端。DHCP服务器集中管理IP地址的动态分配以及网络上启用DHCP客户端的其他相关配置信息，并负责处理客户端的DHCP要求；而客户端则使用服务器端分配下来的IP网络配置数据，UDP 67 用于DHCP服务器，UDP 68用于DHCP客户端。

* DHCP的工作过程

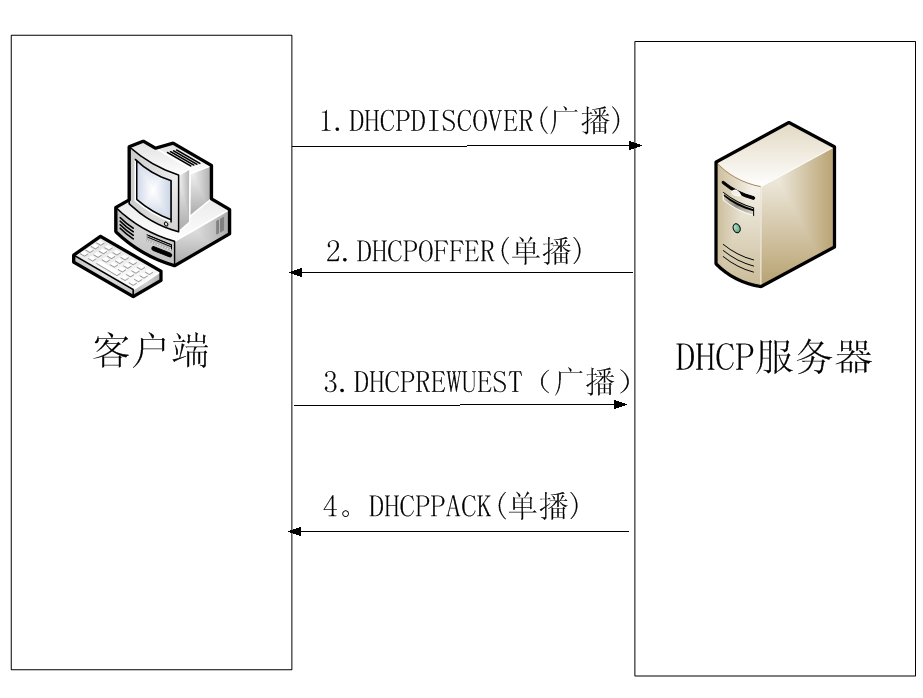


图1-42 DHCP申请过程

(1)IP地址租用申请(DHCPDISCOVER)。DHCP客户端通过UDP68号端口发送DHCPDISCOVER广播信息查找DHCP服务器。只有DHCP服务器作出响应。

(2)IP地址租用提供(DHCPOFFER)。DHCP服务器收到请求后，经过研究可以为该请求提供服务时，从尚未出租的IP地址范围来选择最前面的空闲IP地址，通过UDP67号端口以单播DHCPOFFER的形式来为客户端提供IP信息，可能有多台DHCP服务器收到DHCPDISCOVER请求，向DHCP客户端响应DHCPOFFER.

(3)IP地址租用选择(DHCPREQUEST).DHCP客户端通常是接受收到的第一个DHCPOFFER所提供的信息，并且会向网络发送一个DHCPREWUEST广播包，告诉所有DHCP服务器他将接受哪一台服务器提供的IP地址，其他收到该DHCPREQUEST的服务器将中止相应的分配工作。

(4)IP地址租用确认(DHCPPACK).当被选择的DHCP服务器收到DHCPREQUEST信息之后，便向客户端发送一个单播的DHCPPACK信息，以便确认IP租约的正式生效，然后DHCP客户端便将其TCP/IP协议与网卡绑定。

(5)IP地址租用释放(DHCPRELEASE)。当客户端不需要他的IP地址时，客户端可以发送DHCPRELEASE包来主动释放自己的IP地址。当客户端既不主动释放自己的IP地址，也不续租，等到租期过期就自动释放占用的IP地址。

(6)如果要续租，应在0.5租期的时向服务器提出，如果服务器同意，续租下一个租期，如果不同意，则需要

* DHCP相关命令

ipconfig：获取主机配置信息，包括IP地址、子网掩码和默认网关，也可以获取和释放DHCP租约。

例：在Wsindows系统中，为排除DNS域名解析故障，需要刷新DNS解析器缓存，应使用的命令：ipconfig/flushdns

例：若本机采用DHCP获取地址，需查看所租取IP地址等信息：ipconfig，或ipconfig/all；

例：释放IP地址：ipconfig/release

例：重新获取IP地址： ipconfig/renew

* 自动专用IP地址(APIPA，Autumatic Private IP Address)，

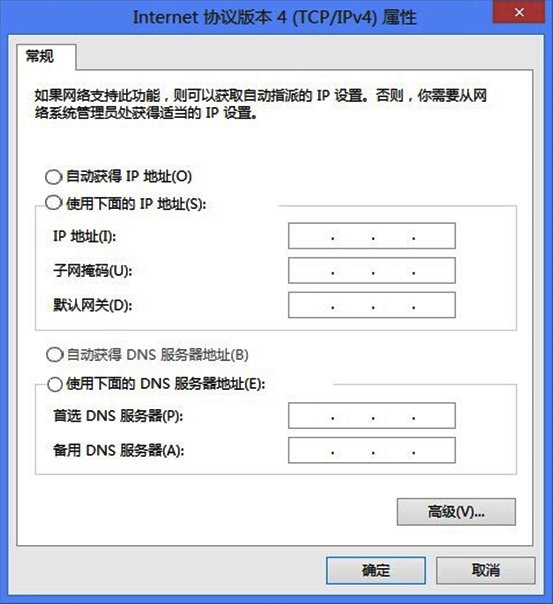
范围：169.254.0.0—169.254.255.255，在基于Windows 98，Windows Me，Windows 2000以及Windows XP的计算机上，如果设置了使用DHCP获取IP地址，当网络中没有架设DHCP服务器时，或者DHCP服务器出了问题的时候，操作系统会自动赋予本机一个类似169.254.x.x的IP地址。

IANA(Internet Assigned Numbers Authority)是负责全球Internet的IP地址编号分配的机构，它把B类地址快169.254.0.0-169.254.255.255定义为自动专用IP地址(Automatic PrivateIP Addressing,APIPA)，这些地址将不能在Internet上使用，所以可以保证不会与其它的Internet上的IP地址冲突。

当网卡被系统赋予一个IP地址后，它就可以与局哉网中其它被系统赋予APIPA IP地址或者手工设定为169.254.x.x的机器通讯了(这些手工设定IP地址的计算机的子网掩码必须是255.255.0.0)。

如果计算机不能访问其它计算机时，检查IP地址，发现IP地址属于169.254.0.0-169.254.255.255的范围时，说明当前的网卡在网络中没有从DHCP服务器租赁到IP地址。

●(2014.5)校园网连接运营商的IP地址为202.117.113.3/30，本地网关的地址为192.168.1.254/24，如果本地计算机采用动态地址分配，在下图中应该如何配置？(68)。



(68)A．选取“自动获得IP地址” B．配置本地计算机IP地址为192.168.1.×

C.配置本地计算机IP地址为202.115.113.× D .在网络169.254.×.×中选取一个不冲突的IP地址

●(2017.5)DHCP服务器给PCl分配IP地址时默认网关地址是202.117.110.65/27，则PC1的地址可能是 (51) 。

(51)A.202.117.110.94 B.202.117.110.95 C.202.117.110.96 D.202.117.110.97

6. 电子邮件协议

(1) SMTP协议： Simple Mail Transfer Protocol ，简单邮件传输协议，建立在TCP基础上，连接端口为25。发信人向源邮件服务器发送邮件使用 SMTP 协议。

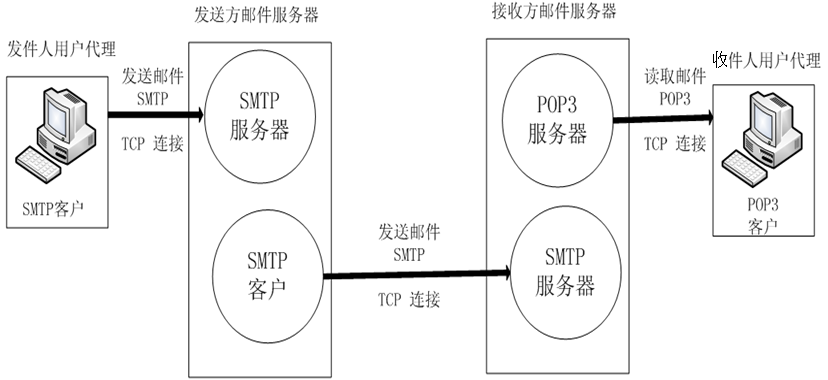


图1-43电子邮件的主要构成模型

(2)POP协议：Post Office Protocol，邮局协议，建立在TCP上，不支持在线阅读，为邮件读取协议，允许用户自己将邮件下载到本地磁盘，再对邮件进行阅读、修改等操作，现在使用的是它的第三个版本 POP3， POP3 服务默认的TCP端口号是110，当使用POP3时，客户端只会连接在服务器上一段的时间，直到它下载完所有新信息，客户端即断开连接。 POP3有三种状态： AUTHORIZATION(授权)，TRANSACTION(处理)，UPDATE(更新).

当TCP建立起来时，POP3进入"授权"状态，客户需要使用USER/PASS进行身份验证. 通过验证后，POP3进入"处理"状态，客户可以发送LIST,RETR等命令来查询，获取邮件. 当客户在此状态下发送"QUIT"命令后，POP3进入"更新"状态，服务器处理完命令后又回到"授权"状态,如 服务器收到客户发送的DELE命令后，仅仅将邮件标记为删除，真正的删除操作在更新状态下执行。

(3)IMAP：Internet Mail Access Protocol,交互式邮件存取协议,一种比POP更高级的消息访问管理协议，建立在TCP连接基础上，当用户 PC 机上的 IMAP 客户程序打开 IMAP 服务器的邮箱时，用户就可看到邮件的首部。若用户需要打开某个邮件，则该邮件才传到用户的计算机上，也是邮件读取协议，IMAP最大的好处就是用户可以在不同的地方使用不同的计算机随时上网阅读和处理自己的邮件。

(4)MIME：Multipurpose Internet Mail Extensions，多功能Internet 邮件扩充协议，规定了通过SMTP传输的非文本电子邮件的标准。

(5)WebMail：登陆服务商的Web站点收发邮件。

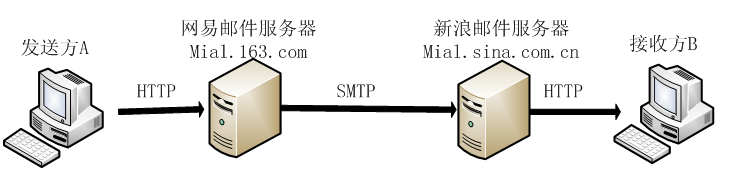


图1-44基于万维网的电子邮件工作过程

7. Telnet (TCP/IP Terminal Emulation Protocol, TCP/IP终端仿真协议)

Telnet是标准的提供远程登陆功能的应用，能够运行于不同操作系统的主机之间。用户通过Telnet 就可在其所在地通过 TCP 连接注册(即登录)到远地的另一个主机上(使用主机名或 IP 地址)。TELNET 能将用户的击键传到远地主机，同时也能将远地主机的输出通过 TCP 连接返回到用户屏幕。这种服务是透明的，因为用户感觉到好像键盘和显示器是直接连在远地主机上，默认使用TCP23号端口。

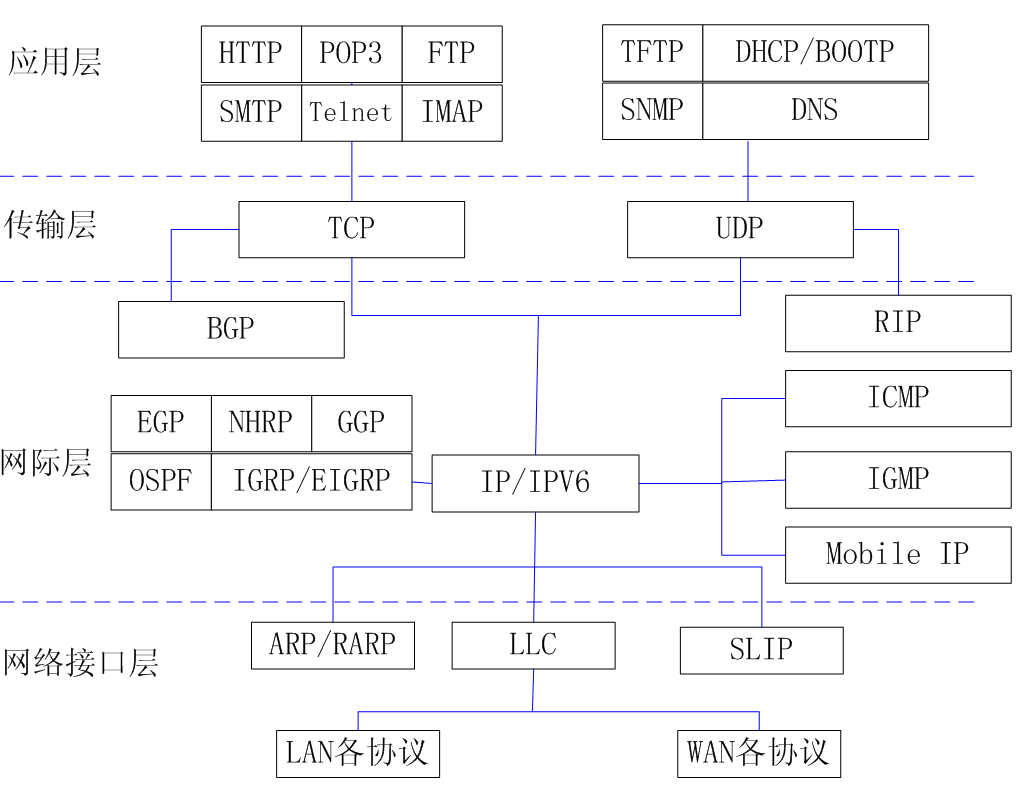


图1-45 TCP/IP协议族的层次模型和协议

端口号总结:

DNS: 默认UDP 53号端口TFTP: 默认UDP 69端口

DHCP: 默认UDP 67端口 用于DHCP服务器，UDP 68端口用于DHCP客户端

http: 默认TCP 80端口SMTP：默认TCP 25端口

POP3 : 默认TCP 110端口Telnet:默认TCP 23号端口

FTP: 客户端先通过TCP 21号端口建立控制连接，传输控制信息。

TCP 20号端口建立数据连接，传输数据。

●(2019.5)下列不属于电子邮件协议的是 (36) 。

(36)A.POP3 B.IMAP C.SMTP D.MPLS

●(2007.11) 简单邮件传输协议(SMTP)默认的端口号是 (20) 。

(20)A.21 B.23 C.25 D.80

● (2007.11)在FTP协议中，控制连接是由 (21) 主动建立的。

(21)A.服务器端 B.客户端 C.操作系统 D.服务提供商

● (2007.11)以下关于FTP和TFTP描述中，正确的是 (39) 。

(39)A.FTP和TFTP都基于TCP协议 B.FTP和TFTP都基于UDP协议

C.FTP基于TCP协议，TFTP基于UDP协议 D.FTP基于UDP协议，TFTP基于TCP协议

●(2007.11)电子邮件应用程序利用POP3协议 (68) 。

(68)A.创建邮件 B.加密邮件 C.发送邮件 D.接收邮件

●(2008.5)运行[Web](http://www.educity.cn/incsearch/search.asp?key=Web) 浏览器的计算机与网页所在的计算机要建立 (66) 连接，采用 (67) 协议传输网页文件。

(66)A.UDP B.TCP C.IP D.RIP

(67)A.HTTP B.[HTML](http://www.educity.cn/incsearch/search.asp?key=HTML) C.[ASP](http://www.educity.cn/incsearch/search.asp?key=ASP) D.RPC

●(2013.5)通常工作在UDP协议之上的应用是(69)。

(69)A.浏览网页 B.Telnet远程登录 C.VoIP(Voice over Internet Protocol) D.发送邮件

●(2014.11)DNS服务器的默认端口号是 (39) 端口。

(39)A.50 B.5l C.52 D.53

●(2015.5) (7) 协议在终端设备与远程站点之间建立安全连接。

(7)A.ARP B.Telnet C.SSH D.WEP

●(2015.5)SNMP协议属于 (46) 层协议。

(46)A.物理 B.网络 C.传输 D.应用

●(2015.5)DHCP协议的功能是 (69) ；FTP使用的传输层协议为 (70) 。

(69)A.WINS名字解析 B.静态地址分配 C.DNS名字登录 D.自动分配IP地址

(70)A.TCP B.IP C.UDP D.HDLC

●(2015.11)POP3协议采用(67)模式，客户端代理与POP3服务器通过建立TCP连接来传送数据。

(67)A.Browser/Server B.Client/Server C.PeertoPeer D.PeertoServer

●(2016.5)默认情况下，FTP服务器的控制端口为 (66)，上传文件时的端口为 (67)。

(66)A.大于1024的端口 B.20 C.80 D.21

(67)A.大于1024的端口 B.20 C.80 D.21

●(2016.11)下面的应用层协议中通过UDP传送的是(21) 。

(21)A．SMTP B.TFTP C.POP3 D.HTTP

●(2016.11)以下协议中属于应用层协议的是(66)，该协议的报文封装在(67)中传送。

(66)A.SNMP B.ARP C.ICMP D.X.25

(67)A.TCP B.IP C.UDP D.ICMP

●(2017.11)若一台服务器只开放了25和110两个端口，那么这台服务器可以提供 (67)服务

(67)A.E-Mail B.WEB C.DNS D.FTP

●(2017.11)下面的应用中，(38) 基于UDP协议。

(38)A.HTTP B.telnet C.RIP D.FTP

## 1.7 IPV6

十六进制数：基数为16，逢十六进一，数字的表示从0到9，10用A表示，以此类推B，C，D，E，F表示15。如“4FD” 按照位权展开：

(4FD)16＝4×162+15×161+13×160＝4FDH

产生的原因是最主要是因为 32 位的 IP 地址不够用， IPV6建立在IPV4基础上，长度改变，各种协议也改变。IPV4地址长度为32位，IPV6长度为128位。

表示方法：将128位分成8组，每组16位二进制，16位二进制转换为十六进制，即使用冒号十六进制记法， “0000”可写作“0”，数字前的0可不写，多个“0：0：0”相连，可写成“：：”，但是，每个IPV6地址中只能有一次将多个“0：0：0”“：：”的压缩：

例：56FA:0000:0000:0000:AAAA:0000:0000:0021

可压缩为：56FA::AAAA:0:0:21或56FA:0:0:0:AAAA::21

●(2008.5)IPv6地址以16进制数表示，每4个16进制数为一组，组之间用冒号分隔，下面的IPv6地址ADBF:0000:FEEA:0000:0000:00EA:00AC:DEED的简化写法是 (20) 。

(20)A. ADBF:0:FEEA:00:EA:AC:DEED B. ADBF:0:FEEA::EA:AC:DEED

C. ADBF:0:FEEA:EA:AC:DEED D. ADBF::FEEA::EA:AC:DEED

●(2009.11)IPv6地址12AB:0000:0000:CD30:0000:0000:0000:0000/60可以表示成各种简写形式，下面的选项中，写法正确的是 (53) 。

(53)A．12AB:0:0:CD30:: /60 B．12AB:0:0:CD3 /60　 C．12AB::CD30 /60 D．12AB::CD3 /60

●2016.11下面关于IPv6的描述中，最准确的是(59) 。

(59)A．IPv6可以允许全局IP地址重复使用 B．IPv6解决了全局口地址不足的问题

C．IPv6的出现使得卫星联网得以实现 D．IPv6的设计目标之一是支持光纤通信

## 1.8计算机网络概述剩余试题部分

●(2007.5)关于路由器，下列说法中错误的是 (66 ) 。

(66)A. 路由器可以隔离子网，抑制广播风暴 B. 路由器可以实现网络地址转换

C. 路由器可以提供可靠性不同的多条路由选择 D. 路由器只能实现点对点的传输

●(2008.11)通过交换机连接的一组工作站 (57) 。

(57)A. 组成一个冲突域，但不是一个广播域 B. 组成一个广播域，但不是一个冲突域

C. 既是一个冲突域，又是一个广播域 D. 既不是冲突域，也不是广播域

● Internet上的DNS服务器中保存有 (70) 。

(70)A. 主机名 B. 域名到IP地址的映射表 C. 所有主机的MAC地址 D. 路由表

● (2011.5)由16个C类网络组成一个超网(supernet)，其网络掩码(mask)应为 (55)。

(55)A. 255.255.240.16 B. 255.255.16.0 C. 255.255.248.0 D. 255.255.240.0

● ARP协议属于(66) 协议，它的作用是 (67) 。

(66)A. 物理层 B. 数据链路层 C. 网络层 D. 传输层

(67)A. 实现MAC地址与主机名之间的映射 B. 实现IP地址与MAC地址之间的变换

C. 实现IP地址与端口号之间的映射 D. 实现应用进程与物理地址之间的变换

● 下面关于集线器与交换机的描述中，错误的是 (68) 。

(68)A. 交换机是一种多端口网桥 B. 交换机的各个端口形成一个广播域

C. 集线器的所有端口组成一个冲突域 D. 集线器可以起到自动寻址的作用

● “三网合一”的三网是指 (69) 。

(69)A. 电信网、广播电视网、互联网 B. 物联网、广播电视网、电信网

C. 物联网、广播电视网、互联网 D. 物联网、电信网、互联网

● SMTP传输的邮件报文采用(31)格式表示。

(31)A．ASCII B．ZIP C．PNP D．HTML

●(2013.5)如下图所示，若路由器C的e0端口状态为down，则当主机A向主机C发送数据时，路由器C发送(13)。



(13)A.ICMP回声请求报文 B.ICMP参数问题报文 C.ICMP目标不可到达报文 D.ICMP源抑制报文

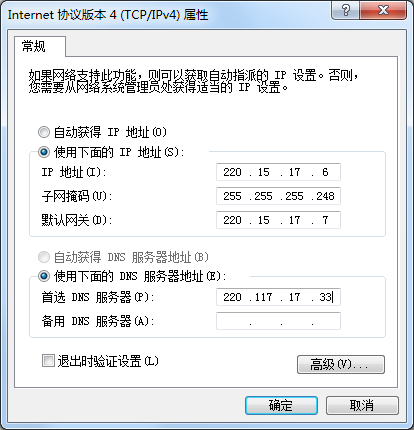
●参见下图，主机Aping主机B，当数据帧到达主机B时，其中包含的源MAC地址和源IP地址是(20)。



(20)A.aaaa.bbbb.0003和10.15.0.11 B.aaaa.bbbb.0002和10.10.128.1

C.aaaa.bbbb.0002和10.15.0.11 D.aaaa.bbbb.0000和10.10.64.1

●一台电脑的本地连接设置如下图所示，结果发现不能ping通任何远程设备，该故障的原因是什么？(51)。



(51)A.默认网关的地址不属于主机所在的子网 B.该主机的地址是一个广播地址

C.默认网关的地址是该子网中的广播地址 D.该主机的地址是一个无效的组播地址

●如果DHCP服务器分配的默认网关地址是192.168.5.33/28，则主机的有效地址应该是(54)。

(54)A.192.168.5.55 B.192.168.5.47 C.192.168.5.40 D.192.168.5.32

●一家连锁店需要设计一种编址方案来支持全国各个门店销售网络，门店有300家左右，每个门店一个子网，每个子网中的终端最多50台，该连锁店从ISP处得到一个B类地址，应该采用的子网掩码是(69)。

(69)A.255.255.255.128 B.255.255.252.0 C.255.255.248.0 D.255.255.255.224

●(2015.5)有较高实时性要求的应用是 (30) 。

(30)A.电子邮件 B.网页浏览 C.VoIP D.网络管理

●工作站A的IP地址是202.117.17.24/28，而工作站B的IP地址是202.117.17.100/28，当两个工作站直接相连时不能通信，怎样修改地址才能使得这两个工作站可以互相通信？ (56)

(56)A.把工作站A的地址改为202.117.17.15 B.把工作站B的地址改为202.117.17.112

C.把子网掩码改为25 D.把子网掩码改为26

●运营商指定本地路由器接口的地址是200.15.10.6/29，路由器连接的默认网关的地址是200.15.10.7，这样配置后发现路由器无法ping通任何远程设备，原因是 (57) 。

(57)A.默认网关的地址不属于这个子网 B.默认网关的地址是子网中的广播网址

C.路由器接口地址是子网中的广播地址 D.路由器接口地址是组播地址