目　录

计算机网络自顶向下

一、计算机网络和因特网

1.1 What is Intent?

因特网是一个世界范围的计算机网络,即它是一个互联了遍及全世界数十亿计算设备的网络。在不久之前，这些设备多数是传统桌面 PC、Linux 工作站以及所谓的服务器、然而，越来越多的非传统的因特网“物品”（如便携机、智能手机、平板电脑、电视、游戏机、温度调节装置、家用电器、手表、眼镜、汽车和运输控制系统等）正在与因特网相连接。由于大量非传统设备连接到因特网，计算机网络的称谓显的有些过时。用因特网的术语描述整个因特网结构，所有的这些设备都被称谓主机或者端系统，这些设备通过网线相连接，并且在一定的规则和协议下组成现在庞大的网络架构。

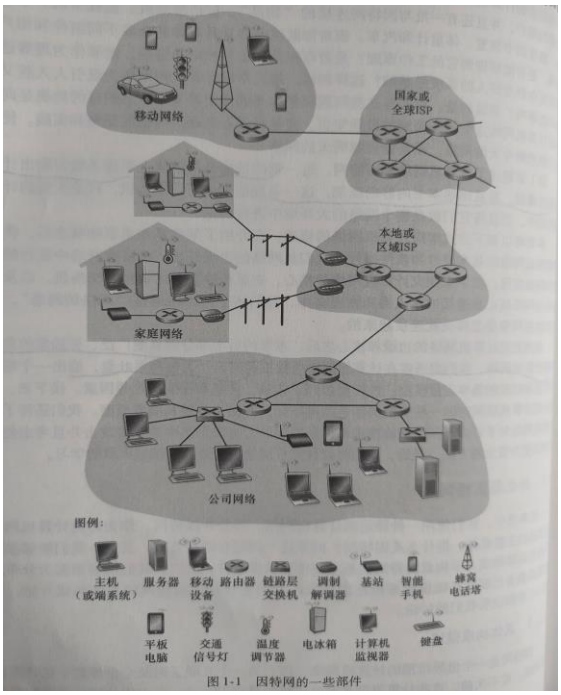


图 1-1　因特网的一些部件

如图所示，端系统通过通信链路和分组交换机连接到一起，通信链路有不同类型的物理媒体组成，这些物理媒体包括同轴电缆、铜线、光纤和无线电频谱，并且不同的链路能够以不同的速率传输数据。当一台端系统要向另一台端系统发送数据的时候，发送端数据将数据分段，并为每段加上首部字节。由此形成的信息包操作被称为分组，这些分组通过网络发送到目的端系统。分组交换机从它的一条入通信链路到达的分组，并从它的一条出通信链路转发到该分组。当今的因特网中，两种最著名的类型是路由器和链路层交换机，这两种类型的叫混迹朝着最终目的地转发分组。链路层交换机通常用于接入网当中，而路由器通常用于网络核心中，从发送端系统和接收端系统，一个分组所经历一系列通信链路和分组交换机成为我那通过该网络的路径。 端系统需要通过因特网服务提供商（Internet Service Provider，ISP）接入因特网，包括本地电缆或电话公司那样的住宅区 ISP、公司 ISP、大学 ISP 等，每个 ISP 自身就是一个由多态分组减缓及和多段通信链路组成的网络。

端系统、分组交换机和其他因特网部件都要运行一系列协议，这些协议控制因特网中信息的发送和接收。TCP(Transmission Control Protocol，传输控制协议)和IP(Internet Protocol，网络协议）是因特网中两个最为重要的协议。IP协议定义了再路由器和端系统之间发送和接收的分组格式。

1.2 网络核心中枢

整个因特网的核心架构就是互联因特网端系统的分组交换机和链路构成的网状网络。在各种网络应用中，端系统彼此交换报文，报文能够包含协议设计者需要的任何东西，报文可以执行一种控制功能，也可以包含数据。为了从源端系统到目的端系统发送一个报文，源将长报文划分为较小的数据块，称之为分组。在源于目的之间，每个分组都通过通信链路和分组交换机传送。

① 存储转发传输

多数分组交换机在链路的输入端使用存储转发传输机制，存储转发传输是指在交换机能够开始向输入链路传输该分组的第一个比特之前，必须接受到整个分组。一台路由器通常由多条繁忙的链路，因为它的任务就是把一个入分组交换到一条出链路。

② 排队时延和分组丢失

每台分组交换机有多条链路与之相连，对于每条相连的链路，该分组交换机具有一个输出缓存，也称为输出队列，它用于存储路由器准备发往那条链路的分组。该输出缓存在分组交换中起着重要的作用，如果到达的分组需要传输到某条链路，但发现该链路正忙于传输其他分组，该到达分组必须在输出分组中等待。因为，处理存储转发时延以外，分组还要承担输出缓存和排队时延，这些时延是变化的，变化的程度取决于网络得额拥塞程度。因为缓存空间是有限的，一个到达的分组可能发现该缓存已被其他等待传输的分组完全充满了。在此情况下，将出现分组丢失（丢包），到达的分组或已经排队的分组之一将被丢弃。

③ 转发表和路由器选择协议

路由器从与它相连的一条通信链路得到分组，然后向与它相连的另一条通信链路转发该分组。在因特网中，每个端系统具备一个成为IP地址的地址。当源主机要向目的端系统发送一个分组时，源在该分组的首部包含了目的地的IP地址。当一个分组到达网络中的路由器的时候，路由器检查该分组的目的地址的一部分，并向一台相邻路由器转发改分组。更特别的是，每台路由器具备一个转发表，用于将目的地址映射为输出链路。当某个分组到达一台路由器的时候，路由器检查该地址，并用这个目的地址搜索其转发表。

1.3 计算机网络分层设计

① 分层设计

计算机网络系统为了给网络协议的设计提供一个结构，网络设计者以分层的方式组织以及实现这些协议的网络硬件和软件，每一个协议属于这些层次之一。在分层模型中，我们关注某层向上一层提供的服务，每层通过在该层执行某些动作或使用下层的服务来提供服务。另外，各层的所有协议被称为协议栈，因特网的协议一共分为五个层次：物理层、链路层、网络层、运输层和应用层。如下图所示，因特网缺少了再OSI参考模型中表示层和会话层，并不是说在具体的因特网中不需要这两层，而是将这两层交给具体应用的开发者来解决，如果该服务是必须并且很重要，相应的开发者自己定制相应的服

务。

1、应用层：应用层是网路应用程序及他们的应用层协议存留的地方，应用层协议分布在多个端系统，而一个端系统中的应用程序使用协议与另一个端系统中的应用程序交换信息分组，我们将这种处于应用层的信息分组称之为报文。

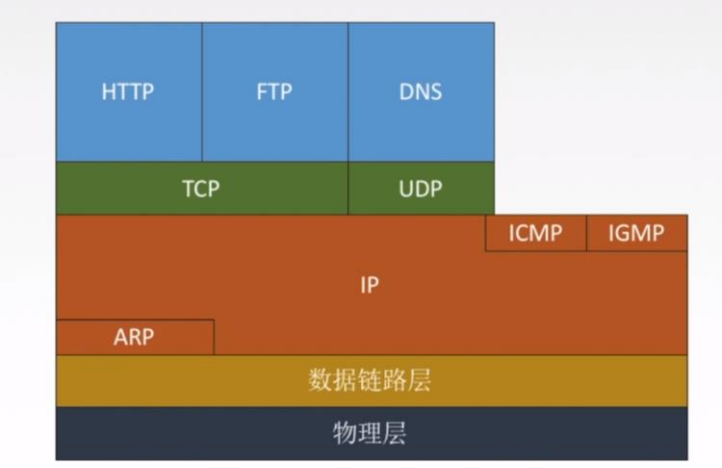
2、运输层：因特网的运输层在应用程序端点之间传送应用层报文，在因特网中，有两种运输协议，即 TCP 和 UDP。这种服务包括了应用层报文向目的地确保传递和流量控制。

3、网络层：因特网网络层负责的被称为数据报的网络分组从一台主机移动到另一台主机当中，在一台源主机中的因特网运输层协议向网络层递交运输层报文段和目的地址，就像我们通过邮政服务寄信件时提供的目的地址一样。

4、链路层：因特网的网络层通过源和目的地之间的一些列路由器路由数据报，为了将分组从一个节点移动到路径的下一个节点，网络层必须依靠该链路层的服务，特别是在每一个节点，网络层将数据报传递给链路层，链路层沿着路径将数据报传递给下一个节点。

5、物理层：虽然链路层的任务是将整个帧从一个网络元素移动到邻近的网络元素，而物理层的任务是将该帧中的一个个比特从一个节点传递到下一个节点。

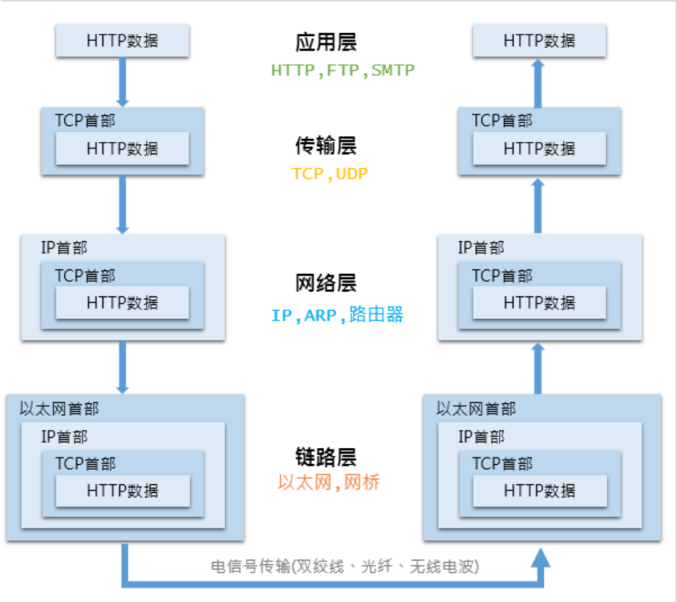
下图是因特网协议栈：



② 逐层封装

如下图所示，数据从发送端系统的协议栈向下，沿着中间的链路层交换机和路由器协议栈上上下下，然后向上到达接收端系统的协议栈。在发送主机端，一个应用层报文

被传送给运输层，在最简单的情况下，运输层收取到报文并附上附加信息，该首部将会被接收端的运输层使用。应用层报文和运输层首部信息一道构成运输层报文段。运输层因此封装了应用层报文，附加的信息也许包括了下列信息：允许接收端运输层向上向适当的应用程序交付报文的信息；差错检测位信息，该信息让接收方能够判断报文中的比特是否在图中已被修改。运输层则向网络层传递该报文段，网络层增加了如源和目的端系统地址等网络层首部信息，生成了网络层数据报。该数据报接下来被传递给链路层，链路层增加了它自己的链路层首部信息并生成链路层帧。



1.4 计算机网络和因特网的发展历史

第一阶段：分组交换的发展

上世纪 60 年代电话网是世界上占领通知地位的通信网络，电话网使用电路交换将信息从发送方传输到接收方。随着计算机的不断普及，以及分时计算器的出现，考虑如何将计算机连在一起，并使他们能够被地理上分布的用户所共享的问题。在这种设计理念的指导下，分组交换技术出现，以作为电路交换技术一种有效的、健壮的替代技术。

第二阶段：专用网络和网络互连

第三阶段：网络的激增

第四阶段：因特网爆炸

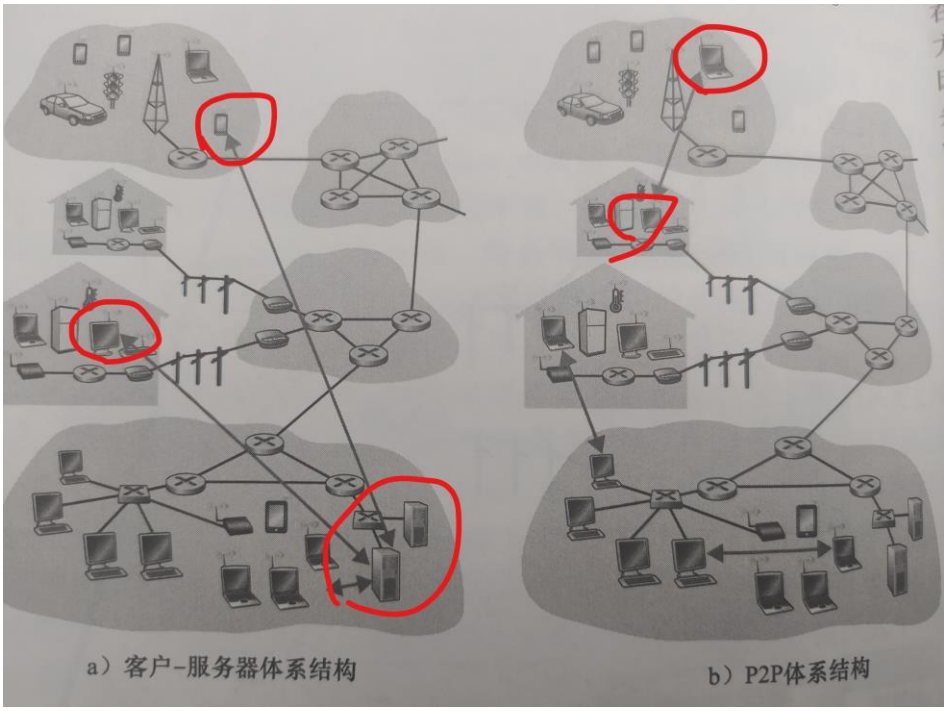
二、计算机网络-应用层

因特网的应用包括基于文本的应用，如文本电子邮件、远程访问计算机、文件传输和新闻组；基于万维网的应用，包括 Web 冲浪、搜索和电子商务，并且现今依然非常流行的及时讯息和对等文件共享。2000 年以来，新型和及其引人入胜的应用持续出现，包括 IP 电话、视频会议、用户生成的视频、点播电影和多方在线游戏等，他们在因特网的网络或路由器通信链路之上创建了引人入胜的人类网络。

1.1 应用层协议原理

① 网络应用层程序体系结构

当进行软件编码之前，应当对应用程序进行一个宽泛的体系结构计划，应用程序的体系结构明显不同于网络的体系结构，从应用程序研发者的角度看，网络体系结构是固定的，并为应用程序提供特定的服务集合。在另一方面，应用程序体系结构有应用程序研发者设计，规定了如何在各种端系统上组织该应用程序。在选择应用程序体系结构时，应用程序研发者很可能利用现代网络应用程序中所使用的的两种主流体系结构之一：客户-服务端体系和对等（P2P）体系结构。



1、客户-服务器体系结构

在客户端-服务器体系结构中，有一个总是打开的主机被称为服务器，部署在提供服务的公司中，客户端也即用户访问公司中的服务器来获取相应的服务。一个典型的例子就是 web 应用程序，浏览器作为客户端访问 web 应用程序的界面，输入网址去寻找相应服务器上的内容，找到以后在浏览器上显示相应的界面来与用户进行实时交互。值得注意的是利用客户-服务器体系结构，客户相互之间不相互通信。具有客户端-服务器体系结构的非常著名的应用程序包括 Web、FTP、Telnet 和电子邮件。

2、对等（P2P）体系结构

在一个 P2P 体系结构当中，对位于数据中心的专用服务器有最小依赖。相反，应

用程序在间断连接的主机对之间使用直接通信，这些主机对被称为对等方。这些对等方并不为服务提供商所有，相反却为用户控制的桌面机和漆上机所有。现今很多目前流行的，流量密集型应用都是 P2P 体系结构的，这些应用包括文件共享、对等方协助下载加速器、因特网电话和视频会议等。

需要提及的是，某些应用具有混合的体系结构，它结合了客户-服务器和 P2P 的元素，例如许多即时通讯应用而言，服务器被用于追踪用户的 IP 地址，但是用户到用户的报文在用户主机之间直接发送。

② 应用程序间进程通信

在构建网络应用程序之前，还需要对运行在多个端系统上的程序是如何相互互相通信的情况有一个基本了解，操作系统的术语来说，进行通信的实际上是进程而不是程序。一个进程可以被认为是运行在一个端系统上的程序，当多个进程运行在相同的端系统上时，他们使用进程间通信机制相互通信。在两个不同的端系统上的进程，通过跨越跨越计算机网络交换报文而相互通信。发送进程生成并向网络中发送报文；接收进程接收这些报文并可能通过回送报文进行响应。

1、客户-服务器进程

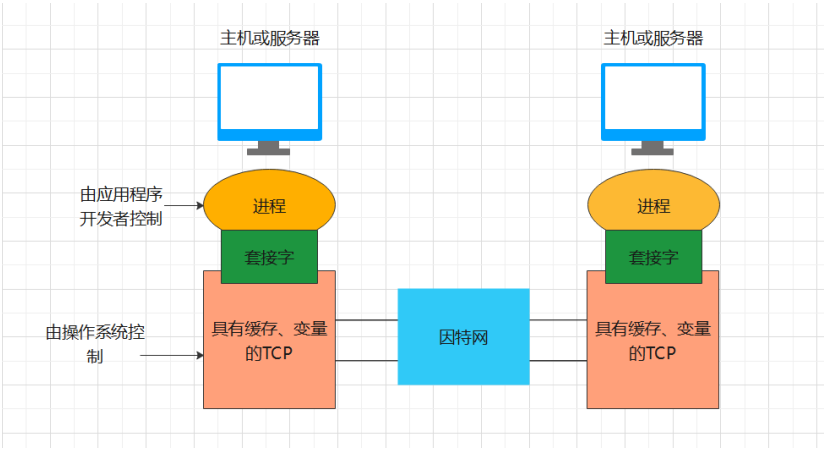
网络应用程序由成对的进程组成，这些进程通过网络相互发送报文。例如，在 web 应用程序中，一个客户浏览器进程与一台 Web 服务器进程交换报文。在一个 P2P 文件共享系统中，文件从一个对等方中进程传输到另一个对等方中的进程。

2、进程与计算机网络之间的接口

多数应用程序是由通信进程对组成，每对中的两个进程互相发送报文从一个进程向另一个进程发送的报文必须通过下面的网络，进程通过一个称为套接字的软件接口向网络中发送报文和从网络中接收报文。由于该套接字是建立在应用程序的可编程接口，因此套接字也称为应用程序编程接口，应用程序开发者可以控制套接字在应用端的一切，但是对该套接字的运输层端几乎没有控制权。

3、进程寻址

为了向特定的目的地发送邮政邮件，目的地需要有一个地址，类似地，在一台主机上运行的进程为了向在另一台主机上运行的进程发送分组，接收进程需要有一个地址，为了识别这个进程，需要定义两种信息：主机地址、在目的主机中指定接收进程的标识符。在因特网中，主机由其 IP 地址标识，进程标识符用端口号标识。



③ 可供应用程序的运输服务

一个运输层协议能够为调用它的应用程序提供的服务，可以从四个方面的要求进行分类：可靠的数据传输、吞吐量、定时和安全性。

根据计算机网络能够提供的通用运输服务，因特网提供具体的运输层传输服务，主要是

TCP 协议和 UDP 协议，TCP 服务模型包括面向连接服务和可靠数据传输服务，UDP 服务模型是一种不提供不必要服务的轻量级运输协议。

1.2 应用层协议实例

应用层定义了运行在不同端系统上的应用程序进程如何相互传递报文，特别是应用层协议定义了：

1、交换的报文类型，例如请求报文和响应报文；

2、各种报文类型的语法，如报文中的各个字段以及这些字段是如何描述的；

3、字段的语义，即这些字段中的信息的含义；

4、确定一个进程何时以及如何发送报文，对报文进行响应的规则。

区分网络应用和应用层协议对理解网络架构十分重要，应用层协议只是网络应用的一部分，例如 Web 是一种客户端-服务器应用，它允许客户按照需求从 web 服务器上获得文档。Web 的应用协议是 Http，它定义了再浏览器和 Web 服务器之间传输的报文格式和序列。

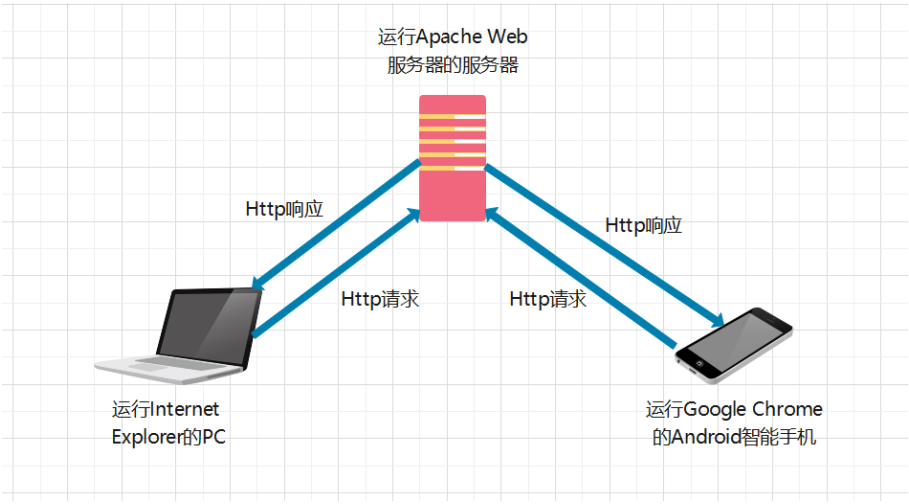
① HTTP 协议

1、web 应用程序

Web 的应用层协议是超文本传输协议（HyperText Transfer Protocol），它是 Web 的核心。Http 由两个程序实现：一个客户端程序和一个服务器程序。客户程序和服务器程序运行在不同的端系统当中，通过交换 Http 报文进行会话。Web 页面是由对象组成，一个对象只是一个文件，诸如一个 HTML 文件、一个 JPEG 图形、一个 Java 小程序或者一个视频片段这样的文件并且它们可以通过一个 URL 地址寻址。多数 Web 页面含有一个 HTML 基本文件以及几个引用对象。因为 Web 浏览实现了 Http 的客户端，所以在 web 环境中我们经常交替使用“浏览器”和“客户”这两个术语。Web 服务器实现了 Http 的服务器端，它用于存储 Web 对象，并且流行的 web 服务器有 Apache Tomcat 和 Microsoft Internet Information Server。

2、Http 协议原理

Http 定义了 Web 客户端向 Web 服务器请求 Web 页面的方式，以及服务器向客户传送 Web 页面的方式。基本思路如下图所示，当用户请求一个 Web 页面时，浏览器向服务器发出该页面的所包含对象的 Http 请求报文，服务器接收到请求并用这些对象的 Http 响应报文进行响应。Http 使用 TCP 作为它的支撑运输协议（而不是在 UDP 上运行）。Http 客户首先发起一个与服务器的 TCP 连接，一旦连接建立，该浏览器和服务器进程就可以通过套接字接口访问 TCP。客户端的套接字接口时客户端进程与 TCP 连接之间的门，在服务端的套接字接口则是服务端进程与 TCP 连接之间的门。



3、Http 协议的特征

网络架构：支持客户端-服务端模式

简单快速：客户向服务器请求服务的时候，只需传送请求方法和路径，请求方法常用的有 GET、HEAD、POST。每种方法规定了客户与服务器联系的类型不同。由于 HTTP 协议简单，使得 HTTP 服务器的规模小，因而通信速度特别快。

灵活：Http 允许传输任意类型的数据对象，正在传输的类型由 Content-Type 加以标记。

无连接：无连接的含义是限制每次连接只处理一个请求。服务器处理完客户端的请求，并收到客户的应答后，即断开连接。采用这种方式可以节省传输时间。

无状态：HTTP 协议是无状态协议。无状态协议是指协议对于事物处理没有记忆能力，缺少意味着如果后续处理需要前面的信息，则它必须重传，这样可能导致每次连接传送的数据量增大，另一方面，在服务器不需要先前信息时它的应答就很快。

4、Http 报文格式解析

Http 协议主要由三大部分组成：起始行（描述请求或相应的基本信息）、头部字段（使用 key-value 形式更详细的说明报文）、消息正文（实际传输的数据，它不一定是纯文本，可以是图片、视频等二进制数据）。具体的 Http 报文如下图所示：

每个报文的起始行都是由三个字段组成：方法、URL 字段和 HTTP 版本字段，如下图所示：

Http 的请求方法一般分为 8 种，他们分别是：

Get 获取资源：Get 方法用来请求访问已被 URI 识别的资源。指定的资源服务器端解析后返回响应内容。也就是说，如果请求的报文是文本，那就保持原样返回。

POST 传输实体：虽然 Get 方法也可以传输实体，但是便于区分，我们一般不用 get 传输实体信息，反而用 POST 传输实体信息。

PUT 传输文件：PUT 方法用来传输文件，就像 FTP 协议的文件上传一样，要求在请求报文的主体中包含文件内容，然后保存到请求 URI 指定的位置。

HEAD 获取响应头部：HEAD 方法和 Get 方法一样，只要不返回报文主体部分，用于确认 URI 的有效性及资源更新的日期时间等。

DELETE 删除文件：DELETE 方法用来删除文件，是与 PUT 方法相反的方法，DELETE 方法按照请求删除指定的资源。

OPTIONS 询问支持的方法：Options 方法用来查询针对请求 URI 指定的资源支持的方法。

TRACE 追踪路径：TRACE 方法是让 WEB 服务器端将之前的请求通信环回给客户端的方法。

CONNECT 要求用隧道协议连接代理：CONNECT 方法要求在与代理服务器通信时建立隧道，实现隧道协议进行 TCP 通信。主要使用 SSL（安全套接层）和 TSL（传输层安全）协议把通信内容加密后经网络隧道传输。

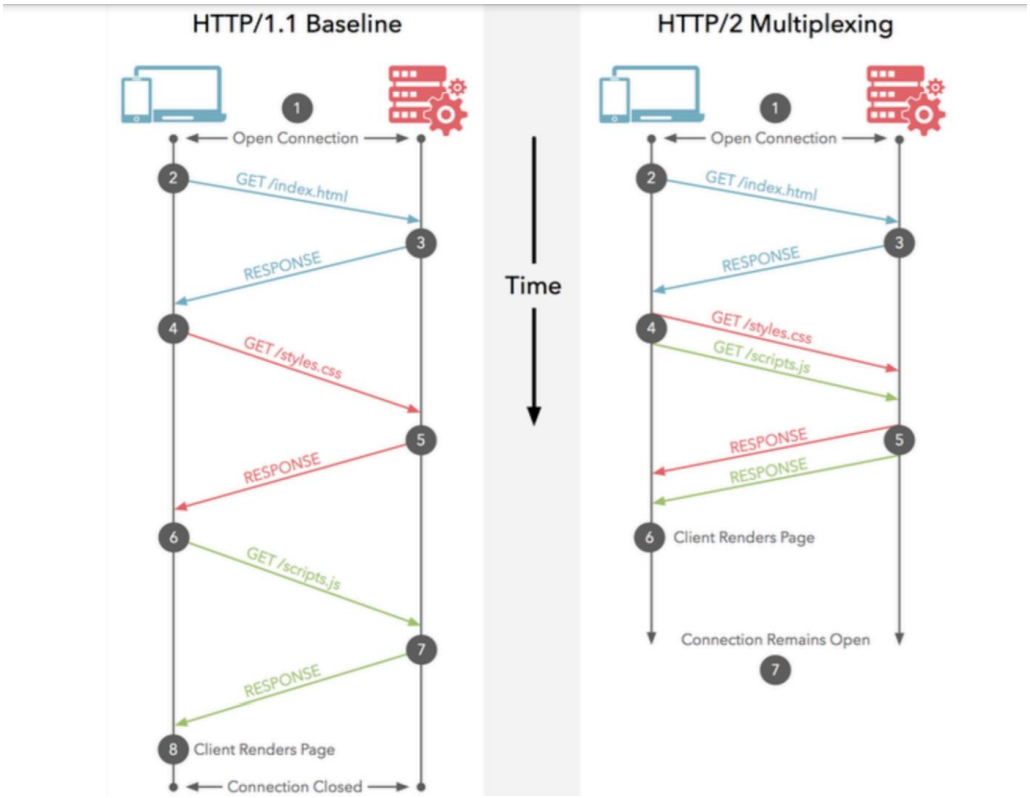
5、Http2.0 新版本所做的改变

头部压缩：由于 HTTP1.1 经常会出现 User-Agent、Cookie、Accept、Server、Range 等字段可能会占用几百甚至几千个字节，而 Body 却经常只有几十个字节，所以导致头部偏重，Http2.0 使用 HPACK 算法进行压缩。

二进制格式：Http2.0 使用了更加靠近 TCP/IP 的二进制格式，而抛弃 ASCII 码，提升了解析效率。

强化安全：由于安全已经成为重中之重，Http2.0 一般都跑在 HTTPS 上。

多路复用：即每一个请求都是用作连接共享，一个请求对应一个 id，这样的连接上可以有多个请求。



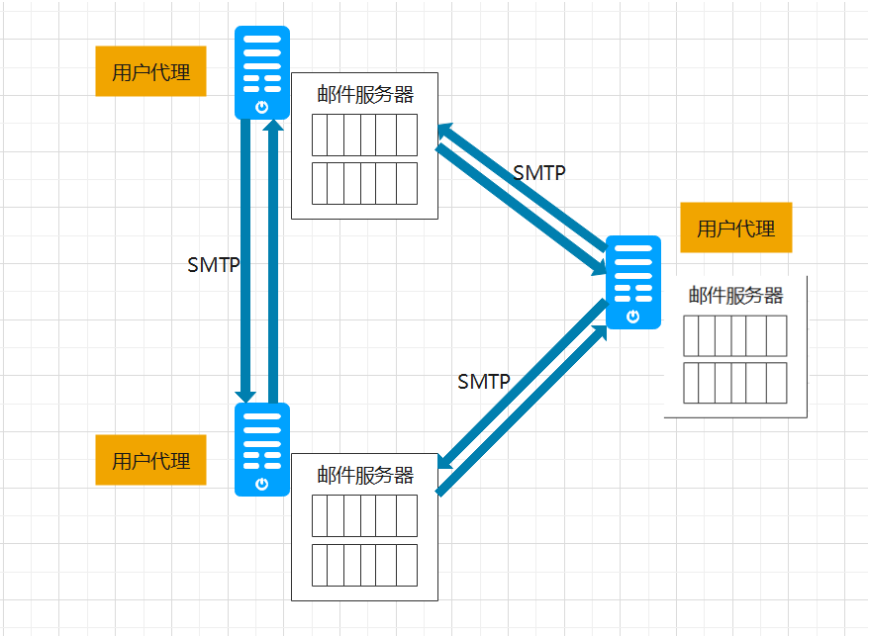
5、Web 缓存

Web 缓存器也叫代理服务器，它是能够代表初始 Web 服务器来满足 Http 网络实体。Web 缓存器有自己的磁盘存储空间，并在存储空间内保存最近请求过的大量对象的副本。通过配置用户的浏览器，使得用户的所有 HTTP 请求首先指向 Web 缓存器。一旦浏览器被配置，每个对象的浏览器被配置，每个对某对象的浏览器请求首先被定向到该 Web 缓存器。

② SMTP 协议

1、电子邮件应用程序

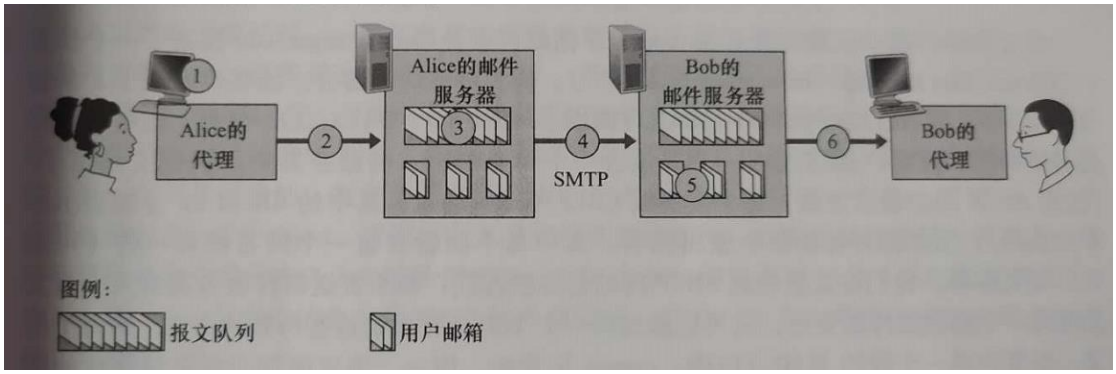
自从有了因特网，电子邮件在因特网上流行起来，当因特网还在襁褓中的时候，电子邮件已经成为最为流行的应用程序。和普通邮件一样，电子邮件是一种异步通信媒介，即当人们方便时就可以收发邮件，不必与他人的计划进行协调。与普通邮件相比，电子邮件更为快速并且易于分发，而且价格便宜。因特网电子邮件系统主要有三个组成部分：用户代理、邮件服务器以及简单邮件传输，如下图所示：



邮件服务器形成了电子邮件体系结构的核心，每个接收方在其中的某个邮件服务器上又一个邮箱。例如 Bob 的邮箱管理和维护着发送给它的报文，一个典型的邮件发送过程是：从发送方的用户代理开始，传输到发送方的邮件服务器，再传输到接收方的邮件服务器，然后在这里分发到接收方的邮箱中。当 Bob 要在它的邮箱中服务报文该报文时，包含它的邮箱的邮件服务器（使用用户名和口令）来鉴别。Alice 须能处理 Bob 的邮件服务器的故障。如果 Alice 的服务器不能将邮件交付给 Bob 服务器，Alice 的邮件的服务器在一个报文队列中保持该报文并在以后尝试再次发送。

2、SMTP 协议原理

SMTP 是因特网电子邮件中的主要协议，它使用 TCP 可靠数据传输服务，从发送方服务器向接收方邮件服务器发送邮件，像大多数应用层协议一样，SMTP 也有两个部分：运行在发送方邮件服务器的客户端和运行在接收方邮件服务器的服务器端。每台邮件服务器上既运行 SMTP 的客户端也运行着 SMTP 的服务器端。当一个邮件服务器向其他邮件服务器发送邮件的时候，它就表现为 SMTP 的客户；当邮件服务器从其他邮件服务器上接收邮件时，它就表现为一个 SMTP 服务器。如下图所示：



SMTP 一般不会使用中间邮件服务器发送邮件，即使这两个邮件服务器处于地球的两端也是如此。假设 Alice 的邮件服务器在中国香港，而 Bob 的邮件服务器在美国圣路易斯，那么这个 TCP 连接也是从香港服务器到圣路易斯服务器之间的直接相连。特别的是，如果 Bob 的邮件服务器没有开机，该报文会保留在 Alice 的邮件服务器上并等待进行重新尝试，这意味着邮件并不在中间的某个邮件服务器上存留。

3、SMTP 与 HTTP 的异同

SMTP 和 HTTP 两个应用层协议都用于从一台主机向另一台主机传送文件，Http 从 Web 服务器向 Web 客户端（通常是一个浏览器）传送文件（也称为对象）；SMTP 从一个邮件服务器向另一个邮件服务器传送文件(即电子邮件报文)。当进行文件传送的时候，持续的 HTTP 和 SMTP 都使用持续连接。另外两个协议之间还有三个主要的区别：

第一个区别是，HTTP 协议主要是一个拉协议，即在方便的时候，某些人在 Web 服务器上装载信息，用户使用 HTTP 从该服务器拉取这些信息。特别是 TCP 连接是由想接受文件的机器发起的。另一方卖弄，SMTP 基本上一个推协议，即发送邮件服务器把文件推向接收邮件服务器，特别是，这个 TCP 连接是由要发送该文件的机器发起的。

第二个区别是，SMTP 要求每个报文采用 7 比特 ASCII 码格式，如果某报文包含了非 7 个比特 ASCII 码进行编码。HTTP 则没有这种限制、

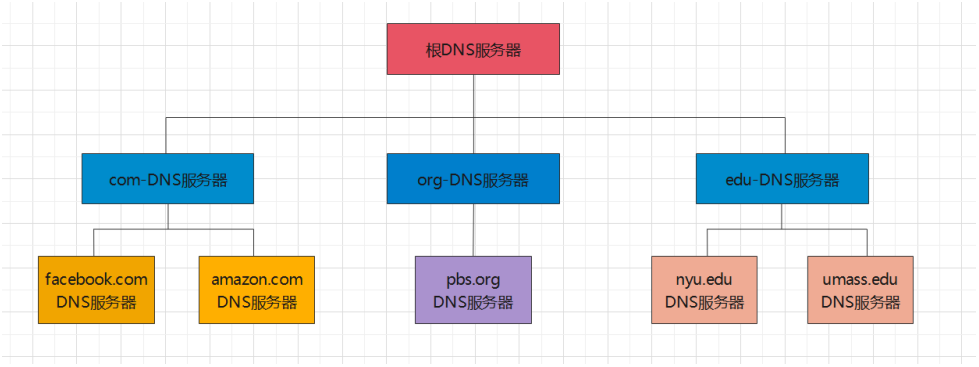
第三个区别是，HTTP 把每个对象封装到它自己的 HTTP 响应报文当中，而 SMTP 则把所有报文对象放在一个报文中。

③ DNS 协议

1、因特网目录应用程序

通常识别主机有两种方式，分别是主机名和 IP 地址，人们更喜欢便于记忆的主机名标识方式，而路由器则喜欢定长的、有着层次机构的 IP 地址。为了折中这些不同的偏好，需要一种能够进行主机名到 IP 地址转换的目录服务，这就是域名系统应用程序的主要任务。DNS 是一个由分层 DNS 服务器实现的分布式数据库，也是一个使得主机能够查询分布式数据库的应用层协议。

DNS 的简单设计是在因特网上只使用一个 DNS 服务器，该服务器包含所有的映射，在这种集中式设计中，客户直接将所有查询直接发往单一的 DNS 服务器，同时该 DNS 服务器直接对所有的查询客户做出响应。尽管这种设计的简单性非常有吸引力，但是不适用于当今的互联网公司，因为因特网有着数量巨大（并持续增长）的主机，这种集中式设计的问题包括：单点故障、通信容量、远距离的几种数据库以及维护等问题。所以现在的 DNS 是一个在因特网实现的分布式的层次数据库，如下图所示：



根 DNS 服务器：有 400 多个根名字服务器遍及全世界，这些根名字服务器的全部清单连同管理他们的组织及其 IP 地址可以在【Root Servers 2016】中找到，根名字服务器提供 TLD 服务器的 IP 地址。

顶级域 DNS 服务器：对于每个顶级域（如 com、org、net、edu 和 gov）和所有国家的顶级域（如 uk、fr、ca 和 jp），都有 TLD 服务器（或服务器集群）。

权威 DNS 服务器，在因特网上具有公共可访问主机（如 Web 服务器和邮件服务器）的每个组织机构必须提供公共访问的 DNS 记录，这些记录将这些主机的名字映射为 IP 地址。

根、TLD 和权威 DNS 服务器都处在该 DNS 服务器层析结构当中，还有另一类重要的

DNS 服务器，成为本地 DNS 服务器。严格说来，一个本地服务器并不属于该服务器的层次结构当中，但是它对 DNS 层次结构是至关重要的。

2、DNS 协议解析

DNS 协议与 HTTP、SMTP 协议一样，都是应用层协议，并且通过客户端-服务器模式提供重要的网络功能，另外在通信的端系统之间通过下面的端到端运输协议来传送 DNS 报文，然而在其他意义上 DNS 的作用非常不同于 Web 应用、文件传输应用以及电子邮件应用。不同之处在于 DNS 是一个不直接跟用户打交道的应用。DNS 协议运行在 UDP 运输服务之上，使用 53 号端口进行传输。DNS 报文结构如下所示：

前 12 个字节是首部区域，其中有几个字段，第一个字段（标识符）是一个 16 比特的数，用于标识查询。这个标识符会被复制到对查询的回答报文中，以便让客户来用它匹配发送的请求和接收到的回答。

问题区域包含着正在进行的查询信息。该区域包括名字字段、类型字段。

在来自 DNS 服务器的回答中，回答区域包含了对最初请求的名字的资源记录。

权威区域包含了其他权服务器的记录。

附加区域包含了其他有帮助的记录。

④ P2P 文件分发

在客户-服务器文件分发中，该服务器必须向每个对等方发送一个该文件的副本，即服务器承受了极大的负担，并且消耗了大量的服务器带宽。在 P2P 文件分发中，每个对等方能够向任何其他对等方重新分发它已经收到的该文件的任何部分，从而在分发过程中协助该服务器。

1、P2P 体系结构的扩展性

如下图所示，对于客户-服务器体系结构，苏子和对等方数量的增加，分发时间呈线性增加并且没有界。然而，对于 P2P 体系结构，最小分发时间不仅总是小于客户-服务体系结构的分发时间，并且对任意的对等方的数量 N，总是小于 1 小时。因此，具有 P2P 体系结构的应用程序能够是字扩展的。这种扩展性的成因是：对等方除了是比特的消费者外还是它们的重新分发者。

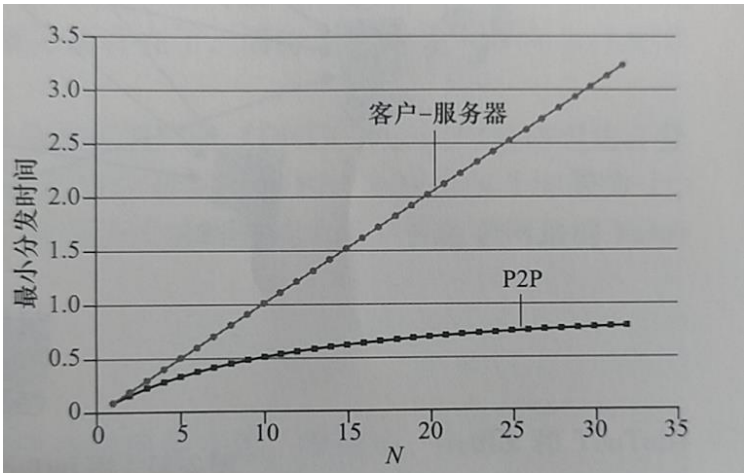


图 2-22　P2P 和客户－服务器体系结构的分发时间

2、BitTorrent-P2P 协议

BitTorrrent 是一种用于文件分发的流行 P2P 协议，用 BitTorrent 的术语来讲，参与一个特定文件分发所有对等方的集合被称为一个洪流。在一个洪流对等方彼此下载等长度的文件块，典型的块长度为 256KB。当一个对等方首次加入洪流时，它没有块，随着时间的流逝，它累积了越来越多的块。当他下载块的时候，也为其他对等方上下载了多个块。随着时间的流逝，它累积了越来越多的块。当下载块时，也为其他对等方上载了多个块，一旦某个对等方获得整个文件，它会自动离开洪流，或者大公无私的留在洪流当中并继续向其他对等方上载块。同时，任何对等方可能任何时候仅具有块的子集就离开洪流，并在以后重新加入洪流。

如下图所示，当一个对等方 Alice 加入洪流以后，追踪器随机的参与对等方的集合中选择对等方的一个子集，并将这 50 个对等方的 IP 地址发送给 Alice。Alice 持有对等方的这张列表，试图与该列表上的所有对等方创建并行的 TCP 连接，我们称所有这样与 Alice 成功建立 TCP 连接的对等方称为“邻近对等方”。随着时间的流逝，这些对等方中的某些可能离开，其他对等方可能试图与 Alice 建立 TCP 连接，因此一个对等方的邻近对等方将随时间波动而波动。

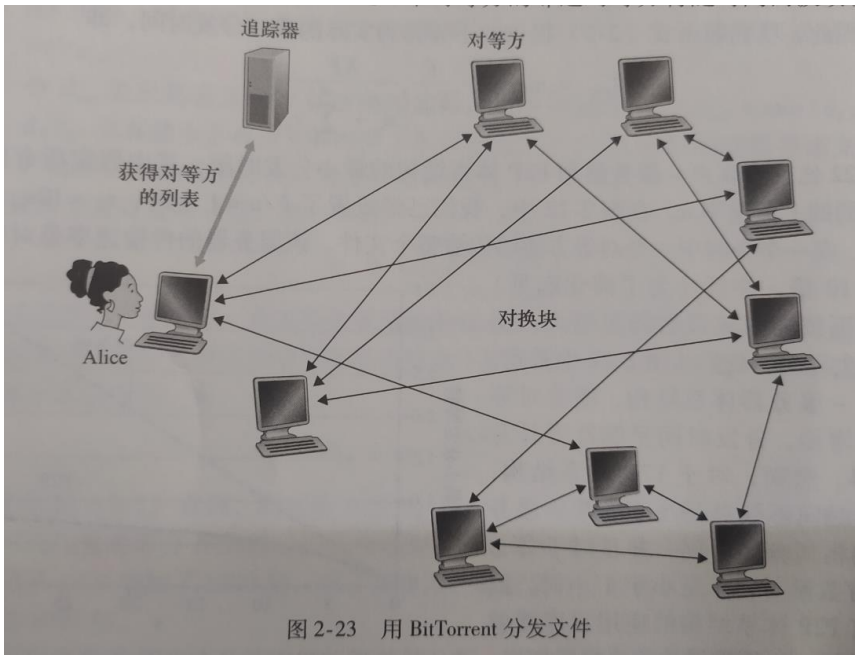


图 2-23　用 BitTorrent 分发文件

⑤ 视频流和内容分发网

在流式存储视频应用中，基础的媒体是预先录制的视频，例如电影、电视节目、录制好的体育赛事事件或者录制好的影虎生成的视频。这些预先录制的好的视频放置在服务器上，用户按需向这些服务器请求来观看视频。许多因特网公司提供流式视频，这些公司包括netfix、Youtobe、亚马逊和优酷等。

在 Http 流中，视频只是存储在 Http 服务器中作为一个普通的文件，每个文件由一个特定的 URL，当用户要看一个视频时，用户和服务器创建一个 TCP 连接并发送对该 URL 的 HTTP 的 get 请求。服务器底层则以网络协议和流量条件允许的尽可能块的速率，在一个 HTTP 响应报文中发送该视频文件。在客户一侧，字节被手机在客户应用缓存中，一旦该缓存中的字节数量超过预定的门限，客户应用程序就开始播放，特别的是，流式视频应用程序周期向的从客户端程序中抓取帧，对这些帧解压缩并且在用户屏幕上展现，因此流式视频应用接收到视频就进行播放，同时放在缓存该视频后面部分的帧。

对于一个因特网视频公司，或许提供流式视频服务最为直接的方法是建立单一的大规模数据中心，在数据中心存储其所有视频，并直接从该数据中心向世界范围的客户传输流式视频。但是这种方法存在三个问题：

1、如果客户远离数据中心，服务器到客户的分组将跨越许多通信链路并很可能通过 ISP，其中很多 ISP 可能谓语不同的大洲。如果这些链路之一提供的吞吐量小于视频消耗速率，端到端吞吐量也将小于该消耗速率，给用户带来恼人的停滞时延。

2、流行的视频很可能经过相同的通信链路发送很多次，这不仅浪费网络带宽，因特网视频公司自己也将向因特网反复发送相同的字节而向其 ISP 运营商支付费用。

3、单个数据中心代表一个单点故障，如果数据中心或其通向因特网的链路奔溃，他将不能够分发任何视频流。

为了应对分布于全世界的用户分发巨量视频数据的挑战，几乎所有的主要视频流都利用视频分发网（Content Distribution Network，CDN）。CDN 管理分布在多个地理位置的副本，并且其所有试图将每个用户请求定向到一个将提供更好用户体验的 CDN 位置。CDN 可以是专用 CDN，即它由内容提供商自己所拥有；例如，谷歌的 CDN 分发 YouTube 视频和其他类型的内容。另一种 CDN 可以和第三方 CDN，它代表多个内容提供商分发内容。

三、计算机网络-运输层

1.1 运输层协议原理

① 运输层概述

运输层协议为运行在不同主机上的应用进程之间提供了逻辑通信功能。从应用者的角度看，通过逻辑通信，运行不同进程的主机好像直接相连一样；应用进程使用运输层提供的逻辑通信功能彼此发送报文，而无须考虑承载这些报文的物理基础设施的细节。在协议栈中，运输层刚好谓语网络层之上，网络层提供了主机之间的逻辑通信，而运输层为运行在不同主机上的进程之间提供了逻辑通信。另外应用层提供了两种截然不同的可用数据运输层协议，这些协议一种是 UDP（用户数据协议），它为调用它的应用程序提供一种不可靠、无连接的服务；另一种是 TCP（传输控制协议），它为调用它的应用程序提供一种可靠的、面向连接的服务。

② 运输层和网络层的联系

运输层协议是在端系统中而不是在路由器上实现的。在发送端，运输层将从发送应用程序接收到的报文转换成运输层分组，用因特网属于来讲该分组被称为运输层报文段。实现的方法是将应用报文划分为较小的块，并为每块加上运输层首部以生成运输层报文段。然后，在报文段。然后，在发送端系统中，运输层将这些报文段传递给网络层，网络层将其封装为网络层分组（即数据报）并且向目的地发送。网络层路由器仅作用于该数据报的网络层字段；即他们不检查封装在该数据报的运输层报文段的字段。在接收端，网络层从数据报中提取运输层报文段，并将该报文段向上交给运输层。运输层则处理接收到的报文段，使该报文段中的数据为接收应用进程使用。

③ 运输层多路分解和多路复用

除此之外运输层考虑的还有接收主机怎样将一个到达的运输层报文段定向到适当的端口。为此目的，每个运输层报文段中有几个字段，在接收端，运输层检查这些字段，标识出接收套接字，进而将报文段定向到该套接字，将运输层报文段中的数据交付到正确的套接字的工作称为多路分解。在源主机从不同套接字中收集数据块，并为每个数据块上封装上首部信息（这将在以后用于分解）从而生成报文段，然后将报文段传递到网络层，所有这些工作被称为多路复用。

1.2 运输层协议实例

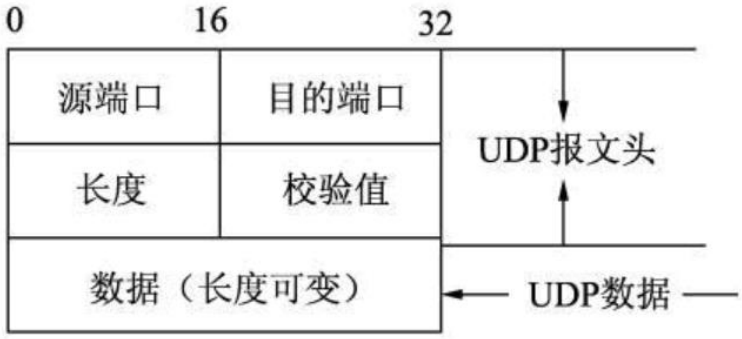
① 无连接运输：UDP

1、UDP 协议

UDP 协议只是做了运输层协议能够做的最少工作，除了复用/分解功能及少量的差错检测外，它几乎没有对 IP 增加别的东西，实际上，如果应用程序开发人员选择 UDP 而不是 TCP。则该应用程序差不多就是直接与 IP 打交道。UDP 从应用程序得到数据，附加上用于多路复用/分解服务的源和目的端口号字段，以及两个其他的小字段，然后将形成的报文段交付给网络层。网络层将此 UDP 报文段封装进一个 IP 数据报中，然后将其发送给一个名字服务器。

DNS 是一个通常使用 UDP 的应用层协议的一个例子，当一台主机中的 DNS 应用程序想要进行一次查询时，它构成了一个 DNS 查询报文并将其交给 UDP。无须执行任何与运行在目的端系统中的 UDP 实体之间握手，主机端的 UDP 为此报文添加首部字段，然后将形成的报文段交给网络层。

2、UDP 协议报文结构



源端口：这个字段占据 UDP 报文头的前 16 位，通常包含发送数据报的应用程序所使用的 UDP 端口。接收端的应用程序利用这个字段的值作为发送响应的目的地址。这个字段是可选的，所以发送端的应用程序不一定会把自己的端口号写入该字段中。如果不写入端口号，则把这个字段设置为 0。这样，接收端的应用程序就不能发送响应了。

目的端口：接收端计算机上 UDP 软件使用的端口，占据 16 位。

长度：该字段占据 16 位，表示 UDP 数据报长度，包含 UDP 报文头和 UDP 数据长度。因为 UDP 报文头长度是 8 个字节，所以这个值最小为 8。

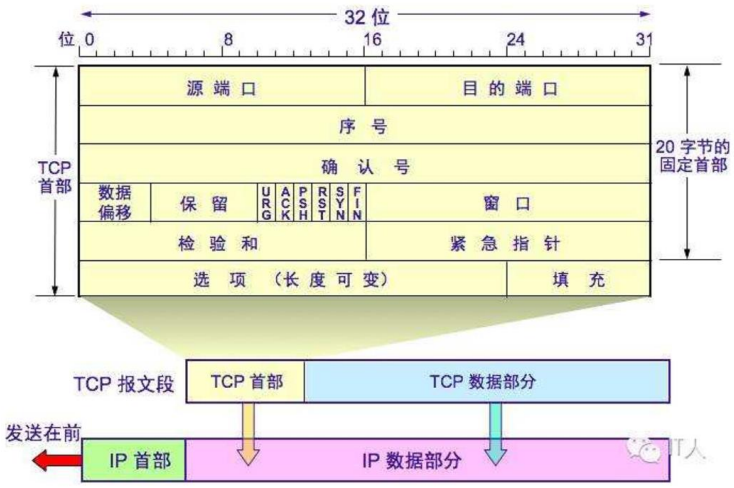
校验值：该字段占据 16 位，可以检验数据在传输过程中是否被损坏。

② 面向连接运输：TCP

1、TCP 协议

TCP 被称为是面向连接的，这是因为在一个应用进程可以开始向另一个进程发送数据之前，这是因为在一个应用进程可以开始向另一个应用进程发送数据之前，这两个进程必须先相互“握手”，即他们必须相互发送某些预备报文段，以确保数据传输的参数，作为 TCP 连接建立的一部分，连接的双方都将初始化与 TCP 连接相关的许多变量。TCP 的“连接”并不是一条在电路交换网络中的端到端 TDM 或 FDM 电路。相反，该“连接”是一条逻辑连接，其共同状态仅保留在两个通信段系统的 TCP 程序当中。由于 TCP 协议只在端系统中运行，而不在中间的网络元素（路由器和链路层交换机）中运行，所以中间网络元素不会维持 TCP 连接状态。事实上，中间路由器对 TCP 连接完全视而不见，他们看到的只是数据报，而不是连接。另外 TCP 连接的组成包括：一台主机上的缓存，变量和与进程连接的套接字，以及另一台主机上的另一组缓存、变量和与进程的套接字。

2、TCP 协议报文结构



32 位比特的序号字段和 32 位比特的确认号字段，这些字段被 TCP 发送方和接收方用来实现可靠的数据传输服务。

16 位比特的接受窗口字段，该字段用于流量控制。

4 比特的首部长度字段，该字段描述了以 32 位比特的字为单位的 TCP 首部字段由于 TCP 选项字段的原因，TCP 首部的长度是可变的。

可选与变长的选项字段，该字段用于发送方与接收方协商最大的报文段长度时，或在高速网络环境之下用作窗口调节因子时使用。

6 比特的标志字段，ACK 比特用于指示确认字段中的值是有效的，即该报文段中包括一个对已被成功接收报文段的确认，RST、SYN 和 FIN 比特用于连接建立和拆除。

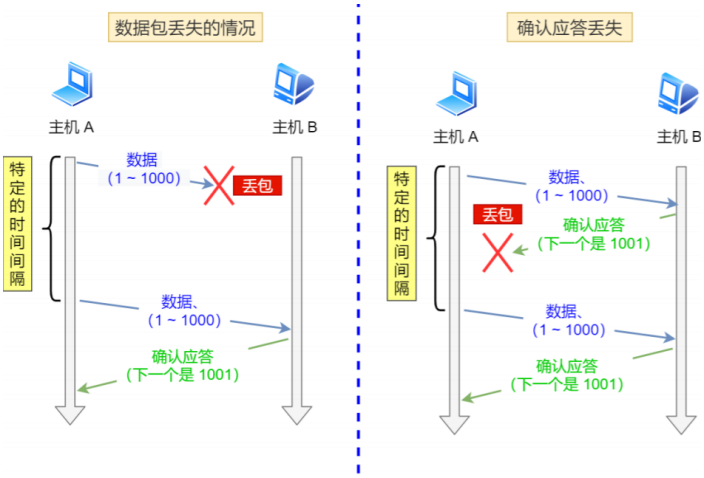
3、TCP 协议可靠数据传输

校验和：发送方在发送数据之前计算检验和，并进行校验和的填充。接收方在收到数据后，对数据以同样的方式进行计算，求出校验和，与发送方的进行比对。在数据传输的过程中，将发送的数据段都当做一个 16 位的整数。将这些整数加起来。并且前面的进位不能丢弃，补在后面，最后取反，得到校验和。

确认应答与序列号：TCP 传输时将每个字节的数据都进行了编号，这就是序列号。TCP 传输的过程中，每次接收方收到数据后，都会对传输方进行确认应答。也就是发送 ACK 报文。这个 ACK 报文当中带有对应的确认序列号，告诉发送方，接收到了哪些数据，下一次的数据从哪里发。有了序列号能够将接收到的数据根据序列号排序，并且去掉重复序列号的数据。这也是 TCP 传输可靠性的保证之一。

超时重传：重传机制是其中的一个机制，设定一个计时器，当超过指定时间后，没有收到对方的 ACK 确认应答报文，就会重发该数据，也就是我们常说的超时重传。TCP

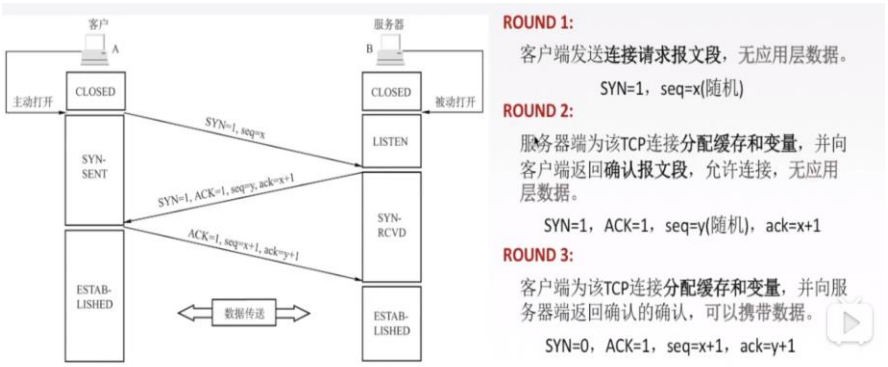
一般在两种情况下发生超时重传，一种是数据报丢失，另一种是确认应答丢失。



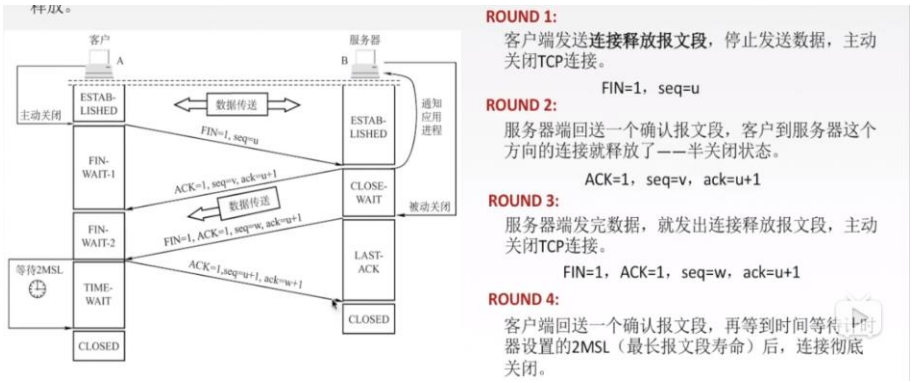
连接管理：连接管理就是三次握手与四次挥手的过程，在前面详细讲过这个过程，这里不再赘述。保证可靠的连接，是保证可靠性的前提。

4、TCP 连接管理

a、三次握手



b、四次分手



为什么 A 在 TIME-WAIT 状态必须等待 2MSL 的时间呢?

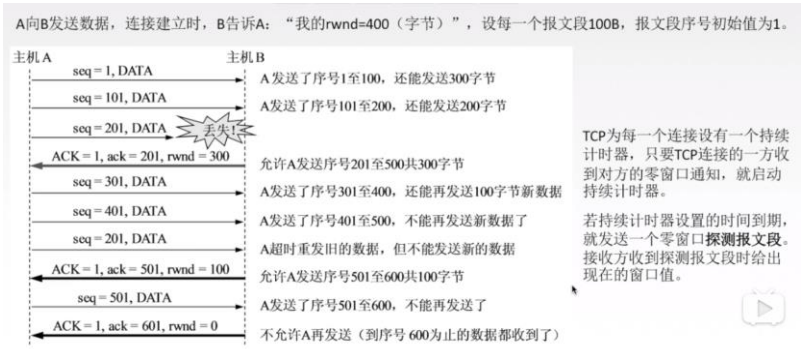
第一、为了保证 A 发送的最后一个 ACK 报文段能够到达 B。这个 ACK 报文段有可能丢失，因而使处在 LAST-ACK 状态的 B 收不到对已发送的 FIN+ACK 报文段的确认。B 会超时重传这个 FIN+ACK 报文段，而 A 就能在 2MSL 时间内收到这个重传的 FIN-ACK 报文段。接着 A 重传一次确认，重新启动 2MSL 计时器。最后，A 和 B 都正常进入到

CLOSED 状态。如果 A 在 TIME=WAIT 状态不等待一段时间，而是在发送完 ACK 报文段后立即释放连接，那么就无法收到 B 重传的 FIN+ACK 报文段，因而也不会再发送一次确认报文段。这样，B 就无法按照正常步骤进入 CLOSED 状态。

第二、防止"已失效的连接请求报文段"出现在本连接中。A 在发送完最后一个 ACK 报文段后，再经过时间 2MSL，就可以使本连接的时间内所产生的所有报文段都从网络中消失。这样就可以使下一个新的连接中不会出现这种旧的连接请求报文段。 B 只要收到了 A 发出的确认，就进入 CLOSED 状态。同样，B 在撤销相应的传输控制块 TCB 后，就结束了这次的 TCP 握手。注意，B 结束 TCP 连接的时间要比 A 早一些。

5、TCP 协议流量控制

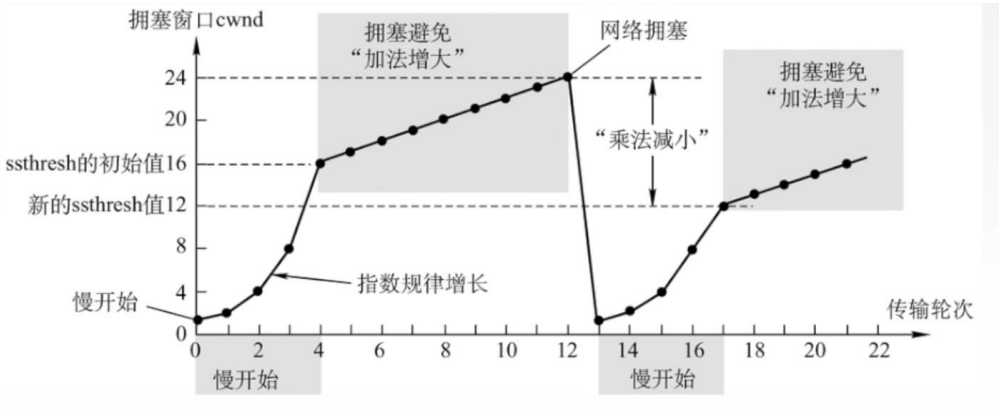
让发送方慢点，要让接收方来得及接收，TCP 利用滑动窗口机制实现流量控制。在控制过程当中，TCP 利用滑动窗口机制来实现流量控制。在通信过程当中，接收方根据自己接收缓存大小，动态调整发送方的发送窗口大小，即接收窗口 rwnd（接收方设置确认报文段的窗口字段来将 rwnd 通知给发送方），发送方的发送窗口取接收窗口 rwnd 和拥塞窗口 cwnd 的最小值。



流量控制只与发送者和接收者之间的端-端通信有关，也就是它是一个局部的控制；但是拥塞控制是一个全局的问题，涉及所有主机、路由器及路由器的存储-转发能力。通俗来说，一个城市，为了缓解拥堵，那么对应应该采取的办法是拥塞控制；但是如果仅仅对于市中心的某一条路避免堵车，那么就是流量控制。

6、TCP 协议拥塞控制

TCP 为运行在不同的主机上的两个进程之间提供了可靠的传输服务。TCP 的另一个关键部分就是其阻塞控制机制。TCP 所采用的方法是让每一个发送方感知从它到目的地之间的路径上没什么拥塞，则 TCP 发送方增加其发送速率；如果发送方感知沿着该路径上面有拥塞，则发送方就会降低其发送速率。TCP 协议拥塞控制算法如下图所示：



慢启动：假设当前发送方拥塞窗口 cwnd 的值为 1，而发送窗口 swnd 等于拥塞窗口 cwnd，因此发送方当前只能发送一个数据报文段（拥塞窗口 cwnd 的值是几，就能发送几个数据报文段），接收方收到该数据报文段后，给发送方回复一个确认报文段，发送方收到该确认报文后，将拥塞窗口的值变为 2。

拥塞避免：也就是每个传输轮次，拥塞窗口 cwnd 只能线性加一，而不是像慢开始算法时，每个传输轮次，拥塞窗口 cwnd 按指数增长。同理，16+1……直至到达 24，假设 24 个报文段在传输过程中丢失 4 个，接收方只收到 20 个报文段，给发送方依次回复 20 个确认报文段，一段时间后，丢失的 4 个报文段的重传计时器超时了，发送发判断可能出现拥塞，更改 cwnd 和 ssthresh.并重新开始慢开始算法。

快速重传：发送方发送 1 号数据报文段，接收方收到 1 号报文段后给发送方发回对 1 号报文段的确认，在 1 号报文段到达发送方之前，发送方还可以将发送窗口内的 2 号数据报文段发送出去，接收方收到 2 号报文段后给发送方发回对 2 号报文段的确认，在 2 号报文段到达发送方之前，发送方还可以将发送窗口内的 3 号数据报文段发送出去，此时，发送方收到了累计 3 个连续的针对 2 号报文段的重复确认，立即重传 3 号报文段，接收方收到后，给发送方发回针对 6 号报文的确认，表明，序号到 6 为至的报文都收到了，这样就不会造成发送方对 3 号报文的超时重传，而是提早收到了重传。

四、计算机网络-网络层

1.1 网络层协议原理

① 网络层概述

网络层实际上就是在实现主机到主机的通信服务，网络层与运输层和应用层不同的是，在网络中每台主机和路由器中都有一个网络层部分。网络层在整个因特网协议栈中是最为复杂的一个层次，网络层能够被分解成两个相互作用的部分，即数据平面和控制平面。每台路由器的数据平面的主要作用是从其输入链路向其输出链路转发数据报；控制平面的主要作用是协调这些本地的每个路由器的转发动作，使得数据报沿着源和目的地主机之间的路由器路径最终能够进行端到端传送。

网络层的作用简而言之就是将分组报文从一台主机移动到另一台主机，实现这个目标的两个核心功能就是转发和路由选择。

转发：当一个分组到达某路由器的一条输入链路时，该路由器必须将该分组移动到适当的输出链路。

路由选择：当分组从发送方向流向接收方时，网路层必须决定这些分组锁采用的路由或路径，计算这些路径的算法被称为路由选择算法。

1、数据平面概述

由上所述，转发是数据平面的主要功能之一，每台路由器中有一个关键元素是它的转发表。路由器检查到达分组首部的一个或多个字段值，进而使用这些首部值在其转发表中索引。通过这种方法来转发分组，这些值对应存储在转发表项中的值，指出了该分组被转发的路由器的输出链接路口。

2、控制平面概述

由上所述，控制平面的主要作用是协调这些本地的每个路由器的转发动作，使得数据报能够沿着源和目的地主机之间的路由器最终能够进行端到端传送。控制平面的实现方法主要有两种，分别是路由传统方法实现和 SDN（Software-Defined Networking，SDN，软件定义网络）方法实现。

a、传统方法

如下图所示，路由选择算法决定了插入该路由器转发表的内容，路由器选择算法运行在每台路由器中，并且每台路由器中都包含了转发和路由选择两种功能。通过考虑网络中的假象情况，也就是说路由器中物理上存在的所有转发表的内容时由人类网络操作员直接配置的，进一步说明转发和路由选择功能的区别和不同目的。在这种情况下，不需要任何路由选择协议。当然，这些操作员将需要彼此交互，以确保该转发表的配置能够分组到达他们想要到达的目的地。

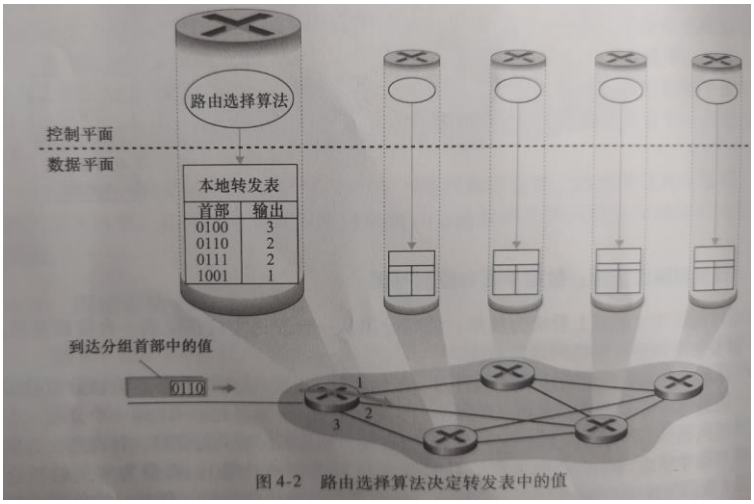


图 4-2 路由选择算法决定转发表中的值

b、SDN 方法

如下图所示，从路由器物理上分离路由选择到统一的远程控制器，在这种方法中路由选择设备尽执行转发，而远程控制器计算并分发转发表。远程控制器可能实现在具有高可靠性和冗余的远程数据中心中，并可能由 ISP 或某些第三方管理。通过减缓包含转发表和其他路由信息的报文，是 SDN 控制平面方法的本质，因为计算转发表并与路由器交互的控制器是用软件实现的，故网络是“软件定义”的。这些软件实现也越来越开放，换言之类似于 Linux 操作系统代码，这些代码可为公众所用，允许 ISP 去创新并对控制网路层功能的软件提出更改性建议。

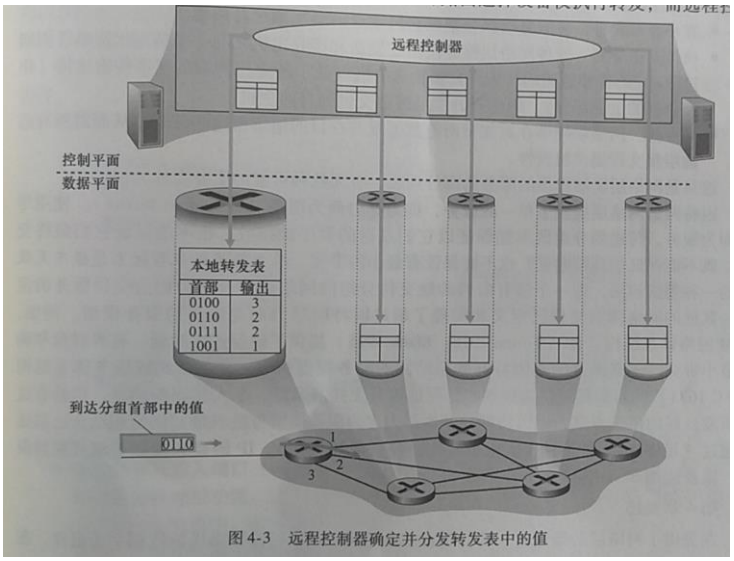
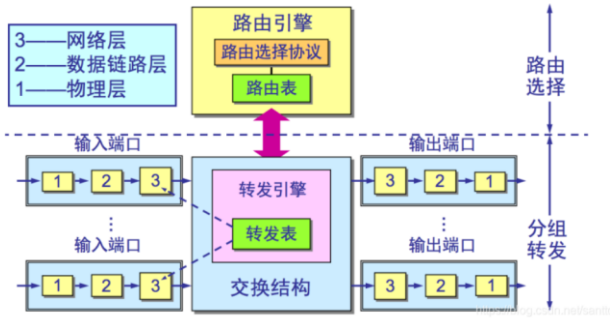


图 4-3 远程控制器确定并分发转发表中的值

② 路由器工作原理

路由器（router）是互联网的枢纽，是连接英特网中各局域网、广域网的设备，它会根据信道的情况自动选择和设定路由，以最佳路径，按前后顺序发送数据。作用在 OSI 模型的第三层，提供了路由与转发两种重要机制。下图是一个通用的路由器体系结构的总体视图：



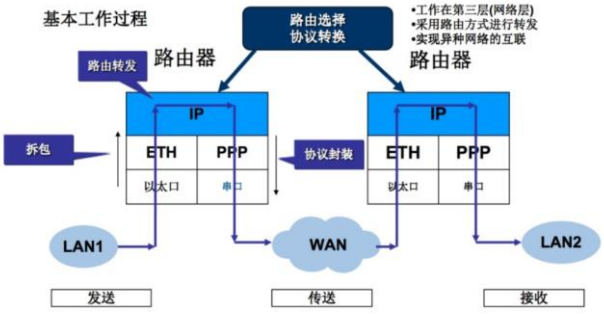
输入端口：输入端口在路由器中执行终结入物理链路的物理层功能，另外它还要位于入链路远端的数据链路层交互来执行数据链路层功能，这显示在输入与输出端口部分中间的方框中。更为重要的是，在输入端口还要执行查找功能，这显示在输入端口最右侧的方框中。

交换结构：交换结构将路由器的输入端口连接到它的输出端口，这种交换结构完全包含在路由器当中，即它是一个网络路由器中的网络。

输出端口：输出端口存储从交换结构接收的分组，并通过执行必要的链路层和物理层功能在输出链路上传输这些分组。当一条链路是双向的时（即承载两个方向的流量），输出端口通常与该链路的输入端口成对出现在同一线路卡上。

路由选择处理器：路由选择处理器执行控制平面的功能，在传统的路由器中，它执行路由选择协议，维护路由选择表与关联链路状态信息，并为该路由器计算转发表。在 SDN 路由器中，路由选择处理器负责与远程控制器通信，目的是接收由远程控制器计算的转发表项，并在该路由器的输入端口安装这些表项。

路由器工作在 OSI 模型三层（网络层）收到数据包后根据 OSI 模型层层将数据包拆开，到网络层后根据 IP 进行路由转发根据接口协议层层封装，实现异种网络的互联。下图是路由器的具体工作过程：



③ 路由选择算法

路由选择算法的目的就是从发送方到接收方的过程当中确定一条通过路由器网络好的路径。通常，一条好的路径指具有最低开销的路径。路由选择算法主要分两种，一种是静态路由选择算法（非自适应选择算法），另一种是动态路由选择算法（自适应选择算法）。

1、静态路由选择算法：管理员手工配置路由信息，其特点是简便、可靠，在符合稳定、拓扑变化不大的网络中运行效果很好，广泛用于高度安全性的军事网络和较小的商业网络，但是它也存在路由更新慢，不适用于大型网络的缺点。

2、动态路由选择算法：自动配置路由信息，其特点是路由器彼此之间交换信息，按照路由算法优化出路由表项，其特点是路由更新快，适用于大型网络，及时响应链路费用或网络拓扑结构变化。但是它也存在算法复杂、增加网络负担的缺点。

由于因特网很大，许多单位不想让外部知道自己的路由协议，但还想连入因特网，由此

诞生自治系统 AS，在单一技术的管理下的一组路由器，而这些路由器使用一种 AS 内部的路由选择协议和共同的度量以确定分组，同时还使用一种与 AS 之间的路由协议以确定在 AS 之间的路由。

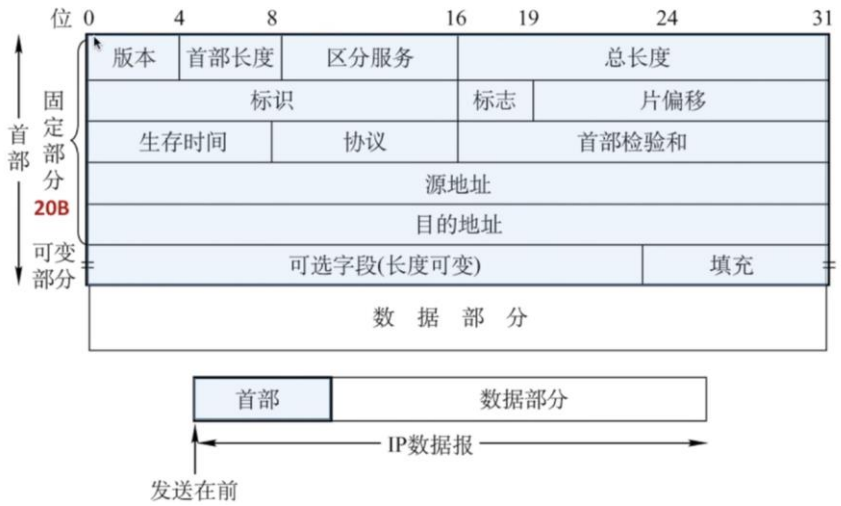
1.2 网络层-数据平面协议实例

① IPV4 协议

1、IPV4 协议

网际协议版本 4（Internet Protocol version 4，IPv4），又称互联网通信协议第四版，是网际协议开发过程中的第四个修订版本，也是此协议第一个被广泛部署的版本。IPv4 是互联网的核心，也是使用最广泛的网际协议版本，其后继版本为 IPv6，直到 2011 年，IANA IPv4 位址完全用尽时，IPv6 仍处在部署的初期。IPv4 是一种无连接的协议，操作在使用分组交换的链路层（如以太网）上。此协议会尽最大努力交付数据包，意即它不保证任何数据包均能送达目的地，也不保证所有数据包均按照正确的顺序无重复地到达。这些方面是由上层的传输协议（如传输控制协议）处理的。

2、IPV4 协议报文格式



版本号：这 4bit 规定了数据报的 IP 协议版本，通过查看版本号，路由器就能确定如何解释 IP 数据报的剩余部分。

首部长度：因为一个 IPV4 数据报可以包含一些可变数量的选项，故需要这 4bit 来确定数据报中的载荷(例如在这个数据报中被封装的运输层的报文段)实际开始的地方。

服务类型：服务类型（TOS）比特包含在 IPV4 首部中，以便使不同类型的 IP 数据报能够相互区别开来。

数据报长度：这是 IP 数据包的总长度（首部加上数据部分），以字节计。因为该字段长为 16bit，所以 IP 数据报的理论最大长度是 65535 字节。

标识、标志、片偏移：这三个字段与所谓的 IP 分片有关。

协议：该字段通常仅当一个 IP 数据报到达最终目的地才会使用。该字段值指示了 IP 数据报的数据部分应当交给哪个协定的运输层协议。

首部检验和：首部检验和用于帮助路由检测收到的 IP 数据报中的比特错误。

源和目的 IP 地址：当某源生成一个数据报时，它在源 IP 字段上插入它的 IP 地址，在目的 IP 地址字段插入其最终目的地的地址。

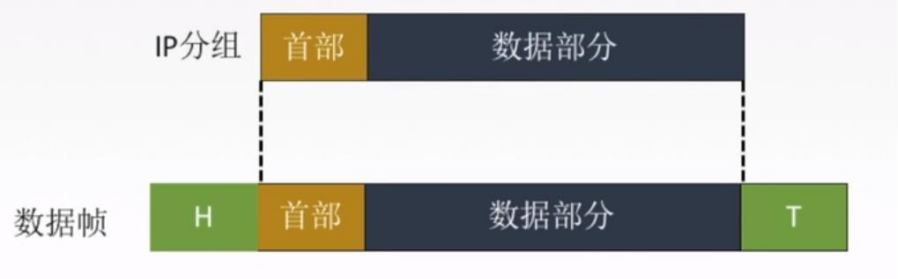
选项：选项字段允许 IP 首部扩展，首部选项意味着很少使用，因此决定对每个数

据报首部不包括选项字段中的信息，这样能够节约开销。

数据：在多数情况下，IP 数据报中的数据字段包含要交付给目的地的运输层报文段（TCP 和 UDP）。然而，该数据报字段也可承载其他类型的数据，如 ICMP 报文段。

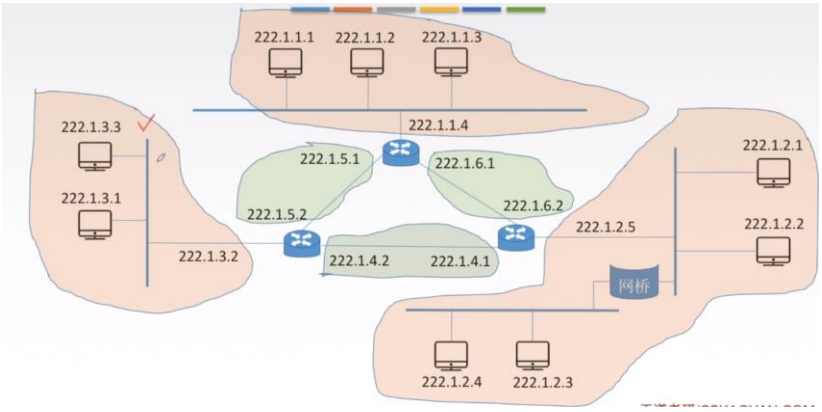
3、IPV4 数据报分片

一个链路层帧能够承载的最大数据量叫做最大传送单元，因为每个 IP 数据报封装在链路层帧中从一台路由器传输到下一台路由器，故链路层协议的 MTU 严格地限制 IP 数据报的长度，对 IP 数据报长度具有严格限制并不是主要问题。问题在于在发送方与目的路径上的每段链路可能使用不同的链路层协议，且每种协议可能具有不同的 MTU。



4、IPV4 编址

主机与物理链路之间的边界叫做接口，路由器的任务就是从链路上接收数据报，并从某些其他链路转发出去，路由器必须拥有两条或者更多条链路与它连接。路由器与它任意一条链路之间的边界也叫作接口，一台路由器因此有多个接口，每个接口都有其链路。因为每台主机与路由器都能发送和接收 IP 数据报，IP 要求每台主机和路由器接口拥有自己的 IP 地址。因此，从技术上讲，一个 IP 地址与一个接口像关联，而不是与包括该接口的路由器相关联。如下图所示：

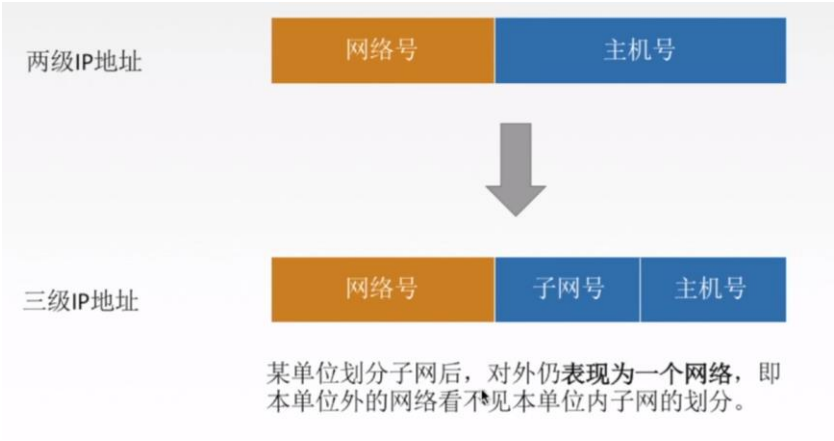


a、分类的 IP 地址

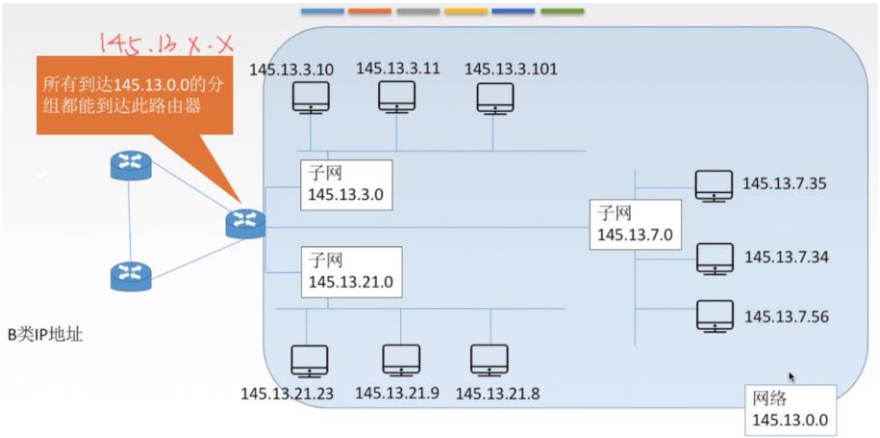
如下图所示：

b、子网划分和子网掩码

IP 术语来说，互联的主机接口与路由器接口的网络形成一个子网，如下图所示是子网号的表示形式：



如下图所示显示的子网划分：

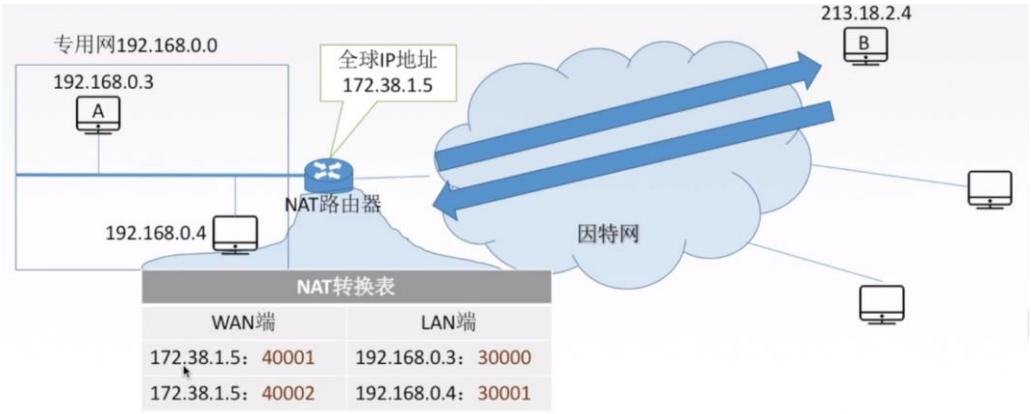


根据子网划分的形式,如果不想让外界知道内部子网的形式与划分提出子网掩码的定义，具体形式如下图所示：

c、无分类编址-构成超网

5、网络地址转换

网络地址转换 NAT（NetWork Address Translation），在专用网连接到因特网的路由器上安装 NAT 软件，安装了 NAT 软件的路由器叫 NAT 路由器，它至少有一个有效的外部全球 IP 地址。如下图所示：



② IPV6 协议

1、IPV6 协议

IPv6 是英文“Internet Protocol Version 6”（互联网协议第 6 版）的缩写，是互联网工程任务组（IETF）设计的用于替代 IPv4 的下一代 IP 协议，其地址数量号称可以为全世界的每一粒沙子编上一个地址。由于 IPv4 最大的问题在于网络地址资源不足，严重制约了互联网的应用和发展。IPv6 的使用，不仅能解决网络地址资源数量的问题，而且也解决了多种接入设备连入互联网的障碍。

2、IPV6 报文格式

扩发的地址容量：IpV6 将 IP 地址长度从 32bit 增加到 128bit，这就确保全世界将不会用尽 IP 地址。另外 Ipv6 还引入一种称为任播地址的新型地址，这种地址可以使数据报交付给一组主机中的任意一个。

简化高效的 40 字节首部：许多 IPV4 字段已被舍弃或作为选项，因而形成的 40 字节定长首部允许路由器更快的处理 IP 数据报。一种新的选项编码允许更灵活的选项处理。

流标签：Ipv6 有一个难以琢磨的流定义。

版本：该 4bit 的比特字段用于标识 IP 版本号。

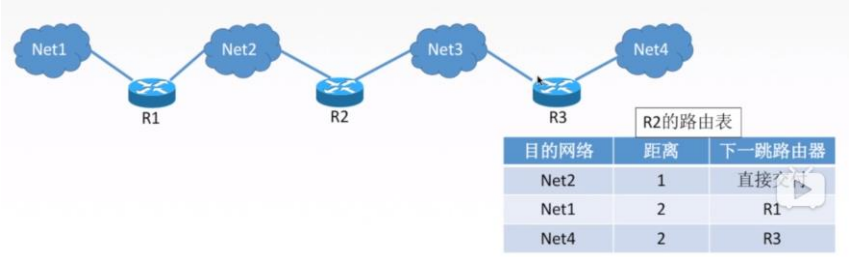
流量类型：该 8 比特于 IPV4 中看到的 TOS 类似。

有效载荷长度：该 16 比特值作为一个无符号整数，给出 IPV6 数据报中跟在定长的 40 字节数据报首部后面的字节数量。

1.3 网络层-控制平面协议实例

① RIP 协议

RIP 协议是一种分布式的基于距离向量的路由选择协议，是因特网的协议标准，最大优点是简单。RIP 协议要求网络中每一个路由器都维护从它自己到其他每一个目的网络的唯一最佳距离记录。RIP 协议只适用于小型网络。



RIP 协议只和相邻的路由器交换信息，路由器交换的信息是自己的路由表。另外每 30

秒交换一次路由信息，然后路由器根据自己更新的信息来更新路由表，若超过 180s 没收到相邻路由器的通告，则判定邻居没了，并更新自己的路由表。

② OSPF 协议

开放最短路径优先 OSPF 协议：“开放”标明 OSPF 不是受某一家厂商控制，而是公开发表的：“最短路径优先”是因为使用了 Dijkstra 提出的最短路径算法 SPF。OSPF 最大的特征就是使用分布式的链路状态协议。

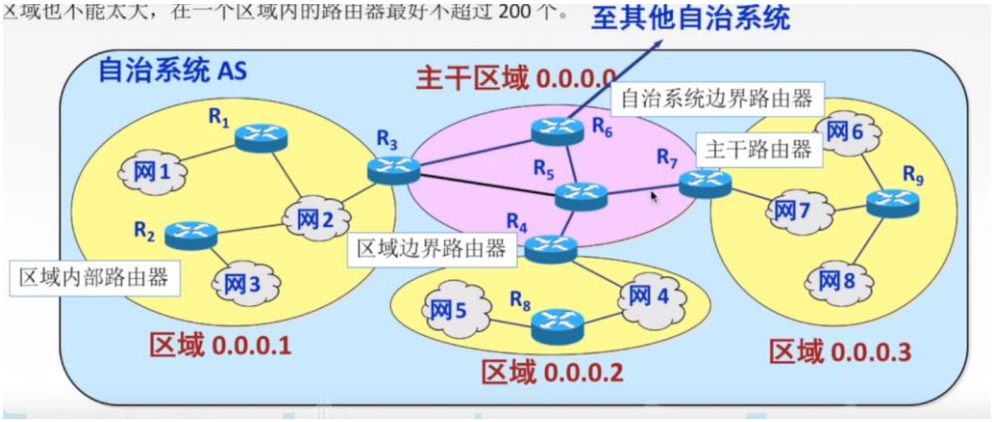
OSPF 的主要特点：

1、使用泛洪法向自治系统内所有路由器发送信息，即路由器通过输出端口向所有相邻的路由器发送信息，而每一个路由器又再次将此信息发往其所有的相邻路由器。最终整个区域内所有路由都得到了这个信息的副本。

2、发送的信息就是与本路由器相邻的所有路由器的链路状态（本路由器与哪些路由器相邻，以及该链路的度量/代价---费用、距离、时延、贷款等）

3、只有当链路状态发生变化的时候，路由器才向所有路由器泛洪发送此信息。最后，所有路由器都能建立一个链路状态数据库，即全网拓扑图。

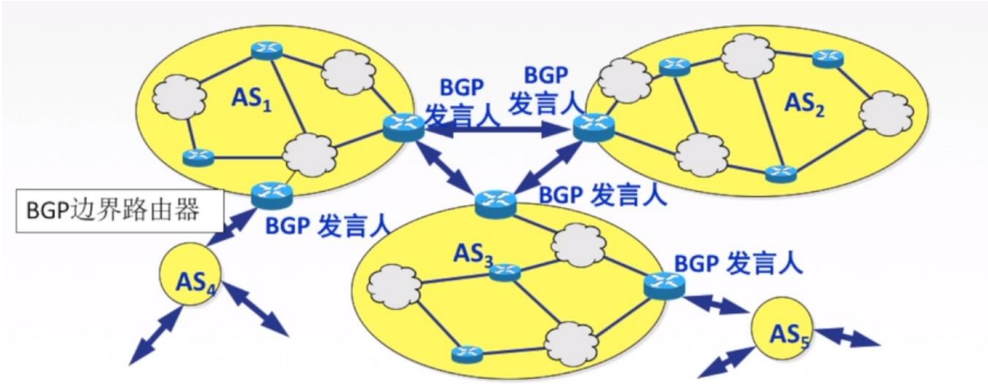
为了使 OSPF 能够用于很大规模的网络，OSPF 将一个自治系统再划分为若干个更小的范围，叫做区域。



③ BGP 协议

OSPF 是一个 AS 内部路由选择协议，当在相同的 AS 内部的源和目的地之间进行分组选路是，分组遵循的路径完全由 AS 内路由选择协议所决定。然而，当分组跨越多个 AS 分组进行路由时，我们需要一个自治系统间路由选择协议。在因特网中，所有的 AS 运行相同的 AS 路由选择协议，成为边界网关协议 BGP。

BGP 所交换的网络可达性的信息就是要到达某个网络所要经过的一系列 AS。当 BGP 发言人互相交换了网络可达性的信息后，各 BGP 发言人就根据所采用的策略从收到的路由信息中找出到达各 AS 的较好路由。



BGP 支持 CIDR，因此 BGP 的路由表也就应当包括目的网络前缀，下一条路由器，以及到达该目的网络所要经过的各个自治系统序列。在 BGP 刚刚运行时，BGP 的邻站是交换整个的 BGP 路由表，但以后只需要发生变化时更新有变化的部分，这样对节省网络带宽和减少路由器处理开销都有好处。

④ ICMP 协议

因特网控制报文协议（ICMP）被主机和路由器用来沟通网络层的信息。ICMP 最典型的用途是差错报告。例如，当运行一个 HTTP 会话时，你也会遇到一些诸如“目的网络不可达”之类的错误报文。这种报文就来自 ICMP，在某各个位置，IP 路由器不能找到一条通往 Http 请求中的指定的主机的路径，该路由器就会向你的主机生成并发出一个 ICMP 报文以指示该错误。

五、计算机网络-数据链路层

1.1 数据链路层协议原理

① 链路层概述

网络层提供的任意两台主机之间的通信服务，在两台主机之间，数据报跨越一系列通信链路传输，一些是有线链路，而一些是无线链路，从源主机起始，通过一系列分组交换机（路由器和交换机），在目的主机结束。当我们沿着协议栈继续往下，从网络层到达链路层，我们自然而然地想到分组是如何通过构成端到端通信路径的各段链路的，这就是链路层要处理的核心问题。

为了方便讨论，将运行链路层协议的任何设备均成为节点，节点包括主机、路由器、交换机、WIFi 接入点。我们也把沿着通信路径连接相邻节点的通信信道成为链路，为了将一个数据报从源主机传输到目的主机，数据报必须通过沿端到端的路径上的各段链路传输。通过特定的链路，传输节点将数据报封装在链路层帧当中，并将该帧传送到链路中。

链路层提供的服务：

1、成帧：在每个网络层的数据报经过链路传送之前，几乎所有的链路层呢个都要将其用链路层帧封装起来，一个帧由一个数据字段和若干个首部字段组成。

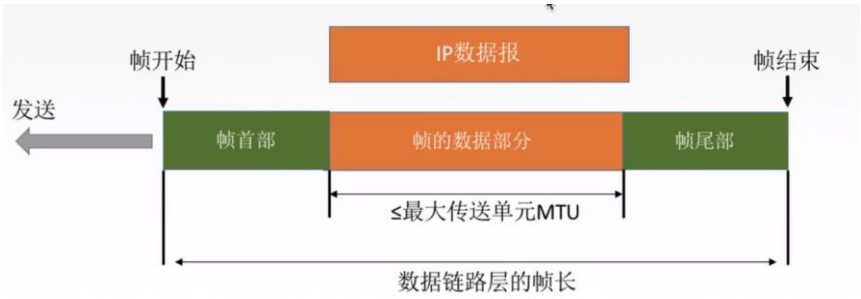
2、链路接入：媒体访问控制（Medium Access Control，MAC）协议规定了帧在链路上传输的规则。对于在链路的一端仅有一个发送方，链路的另一端仅有一个接收方的点对点链路，MAC 协议比较简单，即无论何时链路空闲，发送方都能够成帧。

3、可靠交付：当链路层协议提供可靠交付服务时，它保证无差错地经链路层移动每个网络层的数据报。链路层的可靠交付通常是通过确认和重传取得的，。然而，对于低比特错的链路，包括光纤、同轴电缆和许多双绞铜线链路，链路层可靠交付可能会被认为是一种不必要的开销。所以许多有线的链路层协议不提供可靠交付服务。

4、差错检测和纠正：当帧中的一个比特作为 1 传输时，接收方节点中的链路层层硬件可能不正确地将其判断为 0，反之亦然。这种比特差错是由信号衰减和电磁噪声导致的。

② 封装成帧和透明传输

封装成帧就是一段数据的前后部分添加首部和尾部，这样就构成了一个帧。接收端在收到物理层上交的比特流以后，就能根据首部和尾部的标记，从收到的比特流中识别帧的开始和结束。首部和尾部包含许多的控制信息，他们的一个重要作用是：帧定界（确定帧的边界）。帧同步就是接收方应当能从接收到的二进制比特流区分成帧的起始和终止。



透明传输是指不管所传数据是什么样的比特组合，都应当能够在链路上传送。因此，

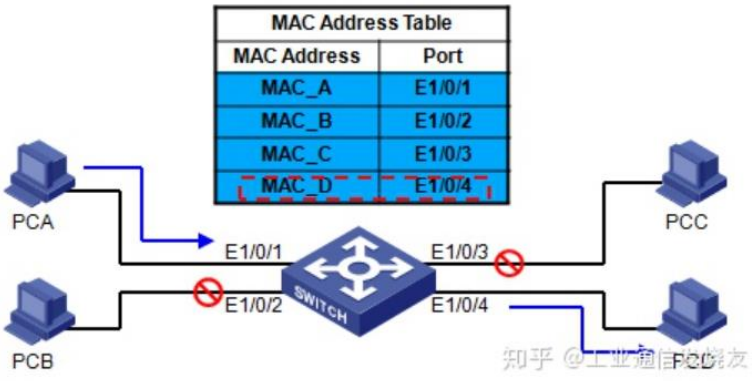
链路层就“看不见”有什么妨碍数据传输的东西。当所传数据中的比特组合恰巧与某一个控制信息完全一样时，就必须采取适当的措施，使收方不会将这样的数据误认为是某种控制信息。这样才能保证数据链路层的传输是透明的。

③ 链路层交换机原理

交换机的任务是接收入链路层帧并将它们转发到出链路，交换机自身对子网中的主机和路由器是透明的，这就是说，某主机/路由器向另一主机/路由器寻址一个帧，顺利地将该帧发送到局域网当中，并不知道某交换机将会接收该帧并将它们转发到另一节点上。

1、交换机转发和过滤

过滤是决定一个帧应该转发到某个接口还是应当将其丢弃的交换机功能。转发是决定一个帧应该被导向那个接口，并将该帧移动到那些接口的交换机功能。交换机的过滤和转发借助交换机表完成。该交换机包含某局域网上某些主机和路由器接口的但不必是全部的表项。



2、自学习

交换机的交换机表是自动、动态和自治地被建立起来，即没有来自网络管理员或来自配置协议的任何干预。换句话说，交换机就是自学习。

1.2 数据链路层协议实例

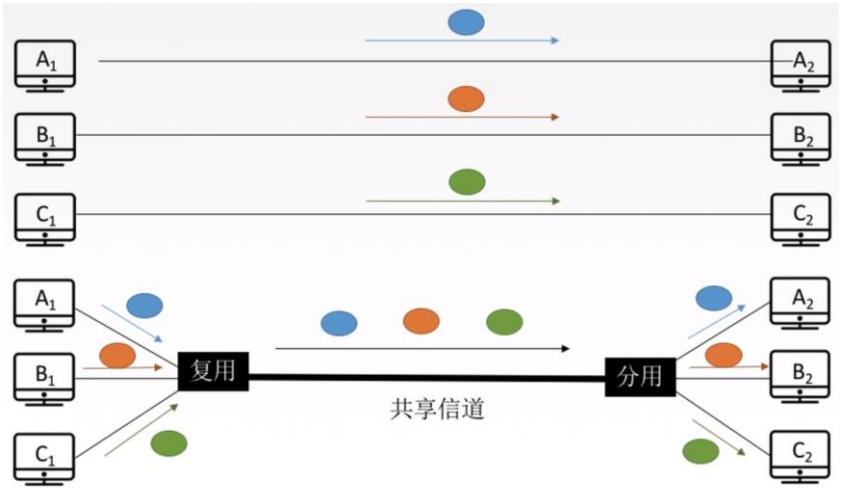
① 多路访问链路与协议

链路层有两种类型的网络连接：点对点链路（用于广域网）和广播链路（用于局域网）。点对点链路由链路一段的单个发送方和链路另一端的单个接收方方法组成。广播链路能够让多个发送和接收节点都连接到相同的、单一的、共享的广播链路。例如在一间教室当中，老师和同学们共享相同的、单一的广播媒体，作为人类，为了共享信道我们遵循这样的规则：“给每个人一个讲话的机会”，“该你讲话的时候在讲话”，“不要一个人独占整个谈话”，“如果有问题请举手”，“当有人讲话时不要打断”，“当其他人讲话时不要睡觉”。计算机网络当中的多路访问协议，即节点通过这些协议来规范它们在共享的广播信道上的传输行为。迄今为止，在大量的链路层技术中已经实现了几十种多路访问协议，尽管如此，我们能够将任何多路访问协议分为 3 种类型之一：信道划分协议、随机接入协议和轮流协议。

1、信道划分协议

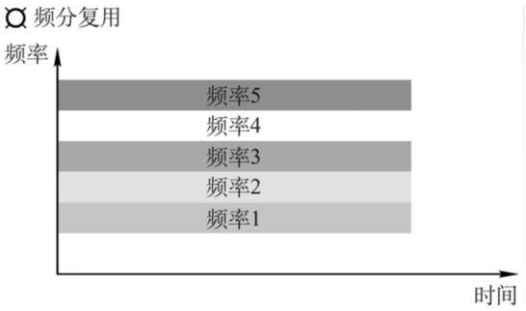
信道划分协议就是将使用介质的每个设备与来自同一信道上的其他设备的通信隔离开，把时域和频域资源合理地分配给网络当中的设备。其中核心就是多路复用技术，把多个信号组合在一条物理线路上进行传输，使得多个计算机或终端设备共享信道资源，提高信道利用

率。

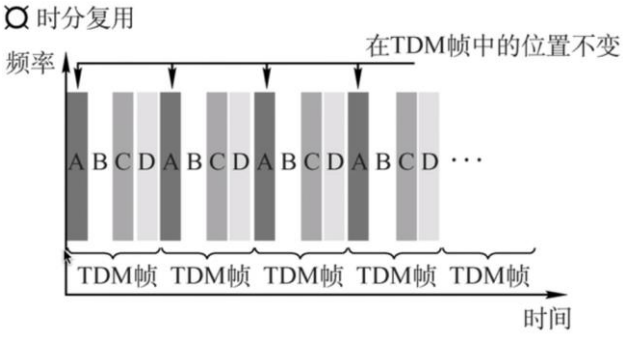


一般静态的划分信道方式主要有四种，分别是：

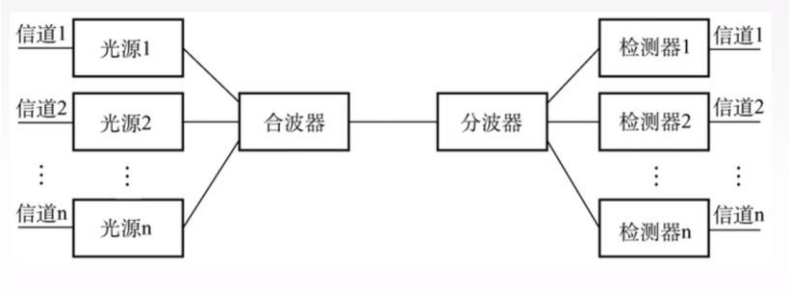
频分多路复用：用户分配到一定的频带后，在通信的过程中自始至终都占用这个频带。频分复用的所有用户在同样的时间占用这个频带。频分复用的所有用户在同样的时间占用不同的带宽（频率带宽）资源。充分利用传输介质带宽，系统效率较高，由于技术比较成熟，实现也比较容易。



时分多路复用：将时间划分为一段段等长的时分复用的用户在每一个 TDM 帧中占用固定序号的时隙，所有用户轮流占用信道。



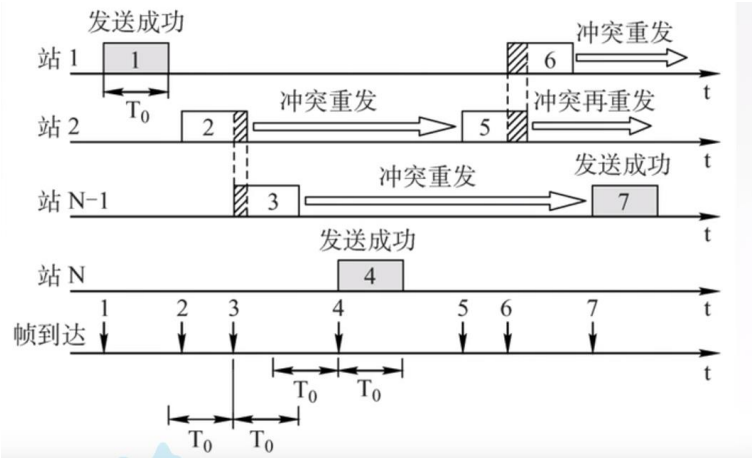
波分多路复用：光的频分多路复用，在一根光纤中传输多种不同波长（频率）的光信号，由于波长（频率）不同，所以各光信号互不干扰，最后再用波长分解复用器将各路波长分解出来。



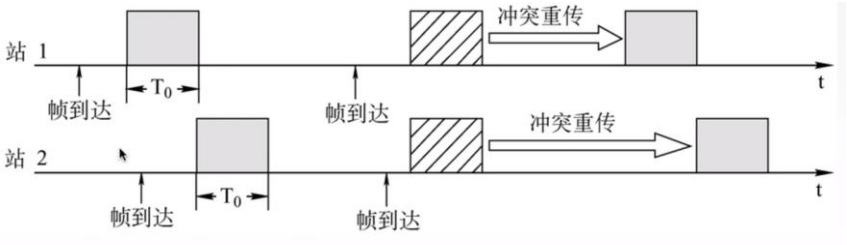
2、随机接入协议

在随机接入协议中，一个传输节点总是以信道的全部速率进行发送。当有碰撞的时候，涉及碰撞的每个节点反复的重发它的帧（也就是分组），到该帧无碰撞地通过为止。但是当一个节点经历一次碰撞的时，它不必立刻重发该帧。虽然迄今为止存在的随机接入协议已有几十种，但是最为常用的随机接入协议即 AlOHA 协议和载波侦听（CSMA）协议。以太网就是一种流行并且广泛部署的 CSMA 协议。

ALOHA 协议（想发就发）：不监听信道，不按时间槽发送，随机重发。如果发生冲突，接收方就会检测出差错，然后不予确认，发送方在一定时间内收不到就判断发生冲突。解决冲突的措施是超时后等一段时间再重传。



时隙 ALOHA 协议：把时间分成若干个相同的时间片，所有用户在时间片开始时刻就进入网络信道，若发生冲突，则必须将下一个时间片开始时刻发送。相比纯 ALOHA 协议，时隙 ALOHA 协议控制了想法就发的随意性。



CSMA 协议：CS 就是载波/监听，每一个站在发送的之前需要检测一下总线上是否有其他计算机在发送数据。MA 就是多点接入，表示许多计算机以多点接入的方式连接在一跟总线上。

CSMA/CA 协议：因为无线局域网无法做到 360° 全面检测碰撞。CSMA/CA 相对于 CSMA 更为礼貌一点，发送之前，先检测信道是否空闲，空闲则发出 RTS，RTS 包括发射端的地址、接收端的地址、下一份数据将持续发送的时间等信息，信道忙则等待。

CSMA/CD 协议：CD 即是碰撞检测（冲突检测），“边发送边监听”，适配器发送数据边检测信道电压的变化情况，以便判断自己在发送数据时其他站是否也在发送数据。

3、轮流协议

多路访问协议的两个理想特性分别是，其一当只有一个节点活跃时，该活跃节点具有 R bps 的吞吐量；其二是当有 M 个节点活跃时，每个活跃节点的吞吐量接近 R/M bps。ALOHA 和 CSMA 协议具备第一个特性，但是不具备第二特性。所以产生轮流协议作为随机接入协议的补充，跟随机接入协议一样，有几十种轮流协议，但是有两种比较重要并且应用范围比较广的协议，分别为轮询协议和令牌传递协议。

轮询协议：轮询协议要求这些节点之一被指定为主节点。主节点以循环的方式轮询每一个节点。特别是，主节点首先向节点 1 发送一个报文，告诉它（节点 1）能够传输帧的最多数量。（主节点能够通过观察在信道上是否缺乏信号，来决定一个节点何时完成了帧的发送）

令牌传递协议：在这种协议中没有主节点，一个称为令牌的小的特殊帧在节点之间以某种固定的次序进行交换。例如：节点 1 可能总是把令牌发送给节点 2，节点 2 可能总是把把令牌发送给节点 3，而节点 N 可能总是把令牌发送给节点。当一个节点收到令牌时，仅当它有一些帧要发送的时候，它才持有这个令牌；否则，它立即向下一节点收到该令牌时，仅当它的一些帧要发送时，如果它确实有帧要传送，它发送的最大数目的帧数，然后把令牌转发给下一节点。

② 链路寻址和 ARP 协议

1、链路寻址 MAC 地址

MAC 地址通常表示为 12 个 16 进制数，每 2 个 16 进制数之间用冒号隔开，如：08:00:20:0A:8C: 6D 就是一个 MAC 地址，其中前 6 位 16 进制数 08:00:20 代表网络硬件制造商的编号，它由 IEEE 分配，而后 3 位 16 进制数 0A:8C:6D 代表该制造商所制造的某个网络产品（如网卡）的系列号。每个网络制造商必须确保它所制造的每个以太网设备都具有相同的前三字节以及不同的后三个字节。这样就可保证世界上每个以太网设备都具有唯一的 MAC 地址。

基于 MAC 地址唯一的特点，局域网采用了用 MAC 地址来标识具体用户的方法。注意：具体实现：在交换机内部通过“表”的方式把 MAC 地址和 IP 地址一一对应，也就是所说的 IP、MAC 绑定（交换机不存在 MAC 地址）。

具体的通信方式：接收过程，当有发给本地局域网内一台主机的数据包时，交换机接收下来，然后把数据包中的 IP 地址按照“表”中的对应关系映射成 MAC 地址，转发到对应的 MAC 地址的主机上，这样一来，即使某台主机盗用了这个 IP 地址，但由于他没有这个 MAC 地址，因此也不会收到数据包。

2、地址转换协议-ARP 协议

因为存在网络层地址（IP 地址）和链路层地址（MAC 地址），所以需要在他们之间进行转换，对于因特网而言，这就是地址转换协议（Address Resolution Protocol，ARP）。

ARP 协议的使用过程（解决下一跳去哪的问题）：

检查 ARP 高速缓存，有对应表项则写入 MAC 帧。没有则使用目的 MAC 地址为 FF-FF-FF-FF-FF-FF-FF 的帧封装并且广播 ARP 请求分组，同一局域网内所有主机都能收到这个请求，目的主机收到请求后就会向源主机单播一个 ARP 响应请求，源主机收到后将此映射写入 ARP 缓存（10-20min 更新一次）

ARP 协议的四种典型情况：

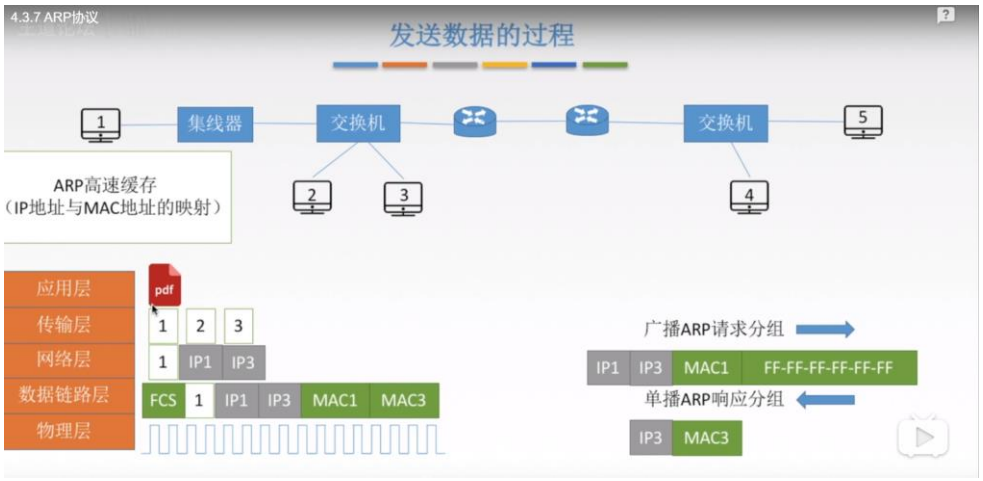
1)、主机 A 发送给本网络中的主机 B，用 ARP 找到主机 B 的硬件地址；

2)、主机 A 发送给另一网络中的主机 B，用 ARP 找到本网络中一个路由器的网关的硬

件地址；

3)、路由器发送给本网络中的主机 A：用 ARP 找到主机 A 的硬件地址；

4)、路由器发送给另一网络中主机 B：用 ARP 找到本网络上的一个路由器硬件地址。



六、无线网络和移动网络

1.1 无线网络原理

① 无线网络概述

无线网络，是指无需布线就能实现各种通信设备互联的网络。无线网络技术涵盖的范围很广，既包括允许用户建立远距离无线连接的全球语音和数据网络，也包括为近距离无线连接进行优化的红外线及射频技术。根据网络覆盖范围的不同，可以将无线网络划分为无线广域网(WWAN：Wireless Wide Area Network)、无线局域网(WLAN：Wireless Local Area Network)、无线城域网(WMAN：Wireless Metropolitan Area Network)和无线个人局域网(WPAN：Wireless Personal Area Network)。

无论是何种无线网络类型，都具备一定体系结构的相关性，如下图所示具备以下几个关键要素：

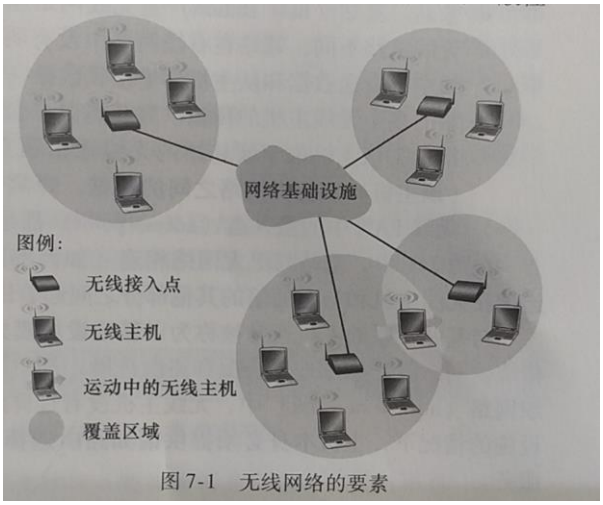


图 7-1　无线网络的要素

无线主机：可以是便携机、掌上机以及智能机或者是桌面计算机。

无线链路：主机通过无线通信链路连接到一个基站或者另一台无线主机。不同的无线链路技术具有不同的传输速率和能够传输不同的距离。

基站：无线网络基础设施中的一个关键部分，与无线主机和无线链路不同，基站在有线网络中没有明确的对应设备。它负责向与之关联的无线主机发送数据和葱主机那里接受数据。基站通常负责协调与之相管理那的多个无线主机的传输。蜂窝网络中的蜂窝塔和 802.11 无线 LAN 中接入点都是基站的实例。

网络基础设施：无线主机希望与之通信更大的网络。

② 无线链路和网络特征

有限网络和无线网络的重要区别在于链路层，其上的层次没有太大变化，有线链路与无线链路的区别体现在以下三个方面：

1、递减的信号强度：电磁波在穿过物体的时候强度将减弱，即使在自由的空间内，信号也将扩散，这使得信号强度随着发送方和接收方距离的增加而减弱。

2、来自其他源的干扰：在同一频段发送信号的电波源相互干扰。

3、多径传播：当电磁波的一部分受物体和地面反射，在发送方和接收方之间走了不同长度的路径，则会出现多径传播。这使得接收方收到的信号变得模糊，位于发送方和接收方之间的物体可导致多径传播随时间而改变。

1.2 无线网络实例

① 个人域网络：蓝牙和 ZigBee

1、蓝牙

IEEE 802.15.1 网络以低功耗和低成本在小范围内运行，它本质是一个低功耗、小范围、低速率的“电缆替代”技术，用于计算机与其无线键盘、鼠标或其他外部设备如蜂窝电话、扬声器、头戴式耳机及其他设备的互联，而 802.11 是一个较高功率、中等范围、较高速率的“接入”技术。为此，802.15.1 网络优势被称为无线个人域网络。

2、ZigBee

IEEE 标准化的第二个个人域网络是 ZigBee，虽然蓝牙提供了一种“电缆替代”的超过每秒兆比特的数据率，但是 ZigBee 较之蓝牙其服务的目标是低功率、低数据率、低工作周期的应用。尽管我们可能倾向于认为“更大、更快就代表更好”，但是并非所有的网络应用都需要高宽带和随之而来的高成本。例如，家庭温度和光线传感器、安全设备和墙上安装的开关都是非常简单、低功率、低工作周期、低成本设备。ZigBee 是非常适合这些设备的。

② 无线局域网：WIFI 无线 LAN

当前，无线 LAN 在工作场所、家庭、教育机构、咖啡屋、机场以及街头无所不在，它已经成为因特网中一种非常重要的接入网技术。802.11 体系结构的节本构建模块是基本服务集（Basic Service Set，BSS）。一个 BSS 包含一个或多个无线站点和一个在 802.11 术语中称为接入点（Access Point，AP）的中央基站。如下图所示，两个 BSS 中的 AP，他们连接到一个互联设备上（如交换机或者路由器），互联设备又连接到因特网中，一个典型的家庭网络中，有一个 AP 和一台将该 BSS 连接到因特网中的路由器。

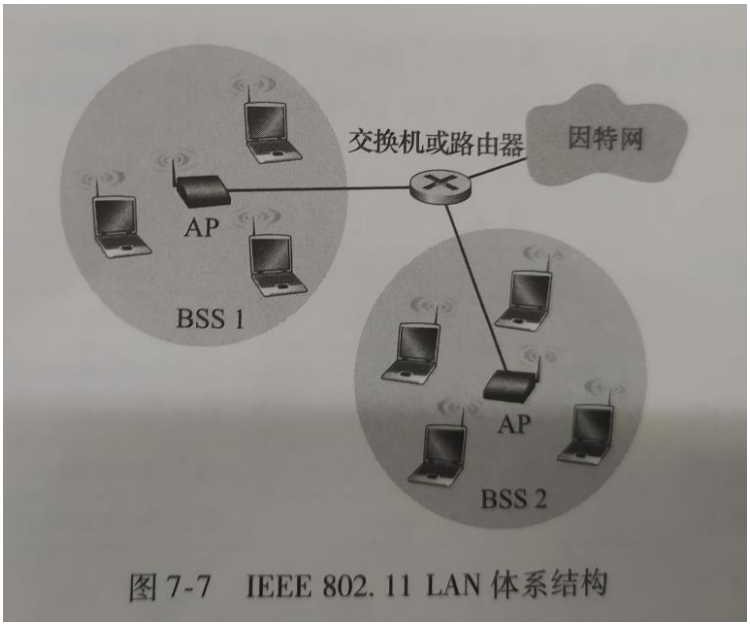


图 7-7　IEEE 802. 11 LAN 体系结构

③ 无线广域网：蜂窝网络

当人们谈论到蜂窝技术的时候，经常将该技术分类为几“代”之一，最早一代的设计主要是用于语音通信，第一代（1G）系统时模拟 FDMA 系统，其专门用于语音通信，这些 1G 系统目前几乎绝迹，他们被数字 2G 系统所代替。初始的 2G 系统也是为语音而设计，但是后来除了语音服务外还扩展了对数据（即因特网）的支持（2.5G），3G 系统也支持语音和数据，但更为强调的是数据能力和更高速的无线接入链路。现今正在运行的 4G 网络基于 LTE 技术，其特征是全 IP 核心网络，并且以几兆比特速率日工了语音和数据的集成。

1、2G 通话：语音通话服务

如下图所示，无线终端通过发行信号到收发基站，再由基站控制器统一发送到移动交换中心，实现处在各地的移动终端实现通信，另外移动交换中心接入公共电话网实现移动终端和电话主机之间的通信，通俗一点来说不仅实现手机和手机之间的通信，还实现了手机和电话座机之间的通信。

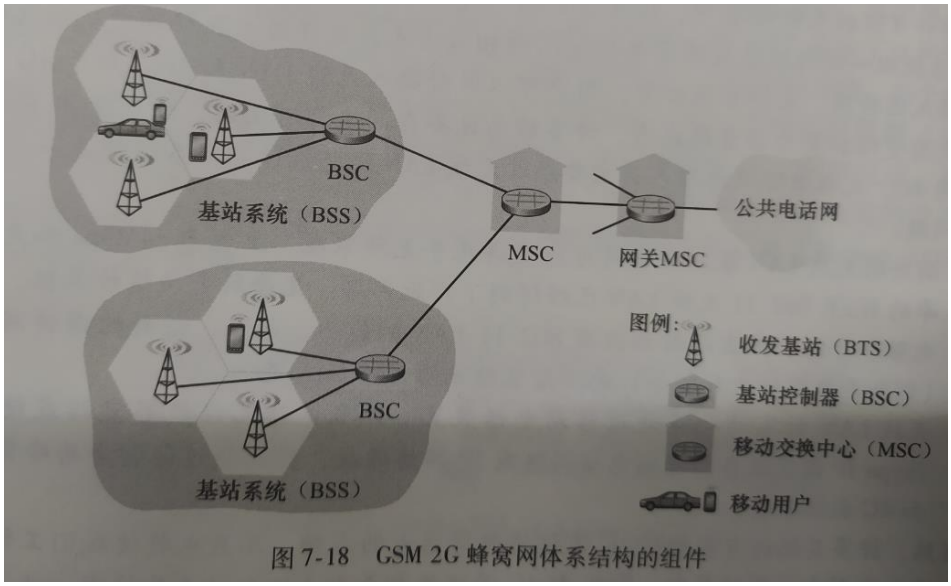


图 7-18　GSM 2G 蜂窝网体系结构的组件

2、3G 上网：接入因特网-网络融合

3G 核心蜂窝数据网将无线电接入网连接到公共因特网。核心网与前面 2G 的网络体系结构遇见过的现有蜂窝语音网的组件协作，由于在现有的蜂窝语音网中具有大量的现有基础设施，3G 数据服务的设计者们所采取的方法非常清楚：不去触动现有核心 GSM 蜂窝语音网，增加与现有蜂窝语音网平行的附加蜂窝数据功能。如果能将新的数据服务直接增加到现有的蜂窝语音网上，这种方式会同样引发在因特网中同样面临的挑战，新的 Ipv6 和 IPV4 的集成技术。

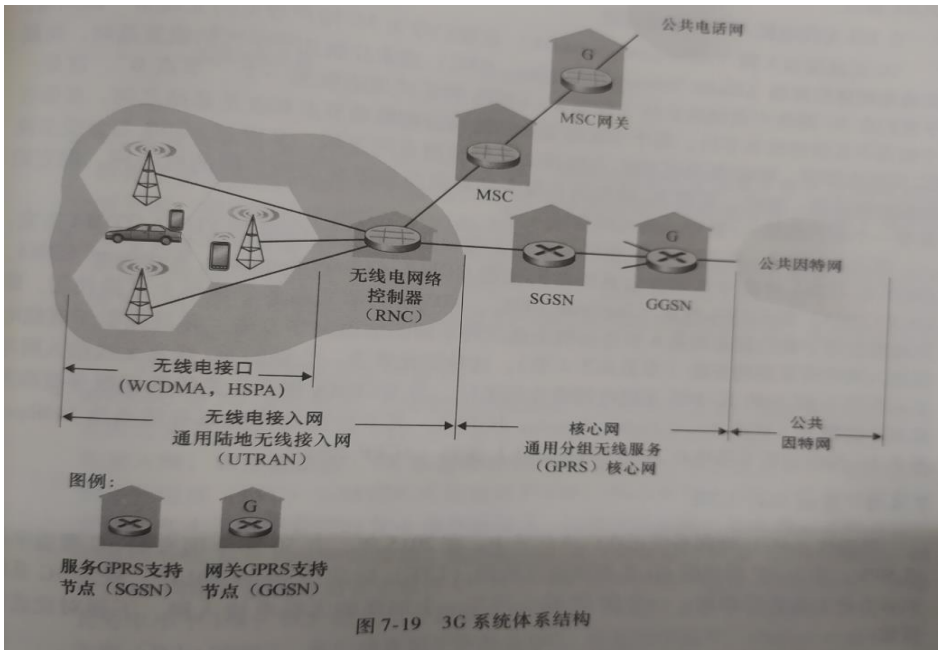


图 7-19　3G 系统体系结构

3、走向 4G：LTE（全 IP）

4G 网络是一种统一的、全 IP 网络体系结构，与 3G 不同的是，3G 网络对于语音和数据流量具有分离的网络组件和路径，但是在 4G 网络体系结构是“全 IP 的”，即语音和数据都承载在 IP 数据报中，来自/去往无线设备（用户设备），到分组开关（P-GW）-该 P-GW 将 4G 边缘网络连接到网络中的其他部分。另外 4G 网络采取数据平面和控制平面全面分离的方式，通过控制层统一分配网络通信路径，数据平面与控制平面职责分离，有利于分组网络融合。

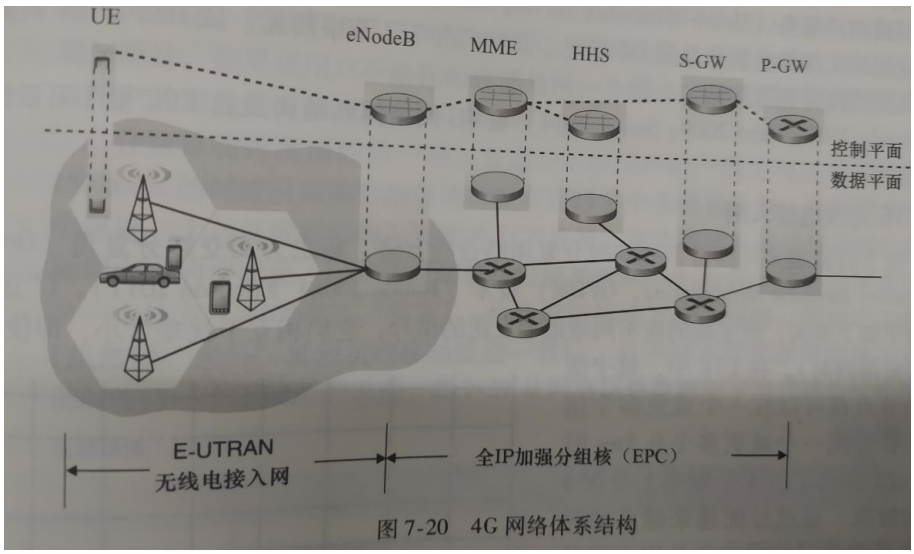


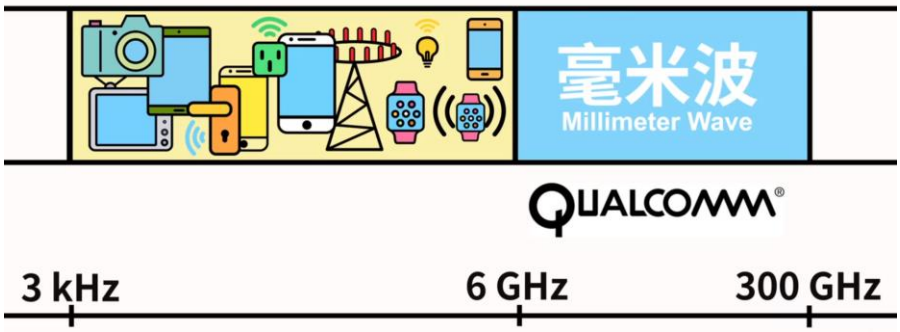
图 7-20　4G 网络体系结构

4、5G 未来：万物互联

5G 作为下一代通信网路技术，它可以以 GB 的速度运行，可以处理千兆级的流量数据，速度比 4G 网络快将近 10 倍，并且 4G 面向个人提供移动宽带服务，5G 提供增强型移动宽带服务。5G 包含增强型移动宽带（eMBB）、大规模机器类型通信（mMTC）以及超可靠和低时延通信（URLCC）三类用例。

5G 的底层核心技术包括毫米波、小基站、大规模 MIMO、波束成形、全双工等五项，具体的内容如下：

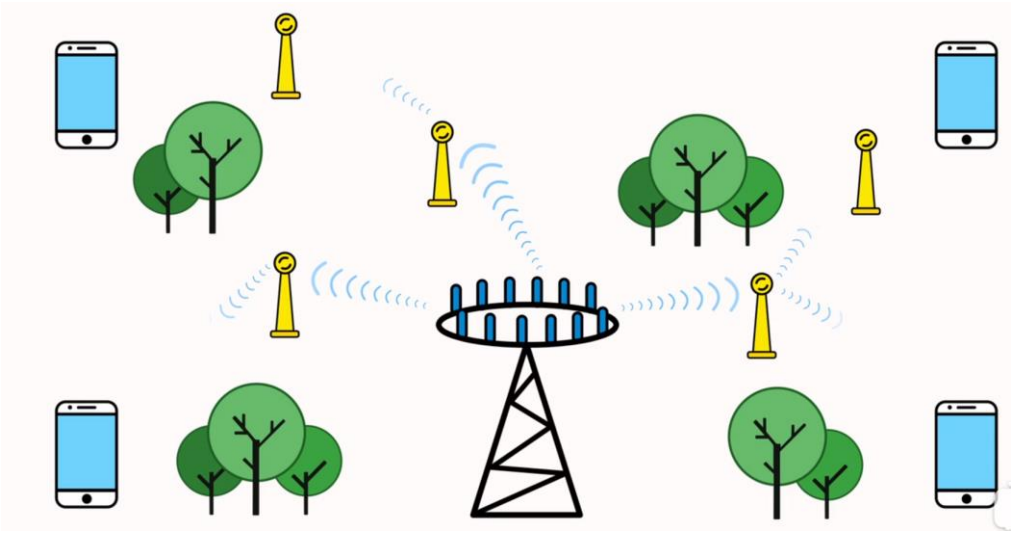
毫米波：目前大部分手机和电子设备都在 3KHz 到 6KHz 频段中工作，但是随着越来越多的设备加入到这个频段当中，而且设备们也在消耗着更多的数据量，这一频段变得拥挤不堪，不仅让我们网速更慢，而且常有掉线的情况，所以我们需要开拓全新的频谱资源，于是高通这样的无线技术专家，就把眼光放在 6GHz 以上的频段，也就是所谓的毫米波。



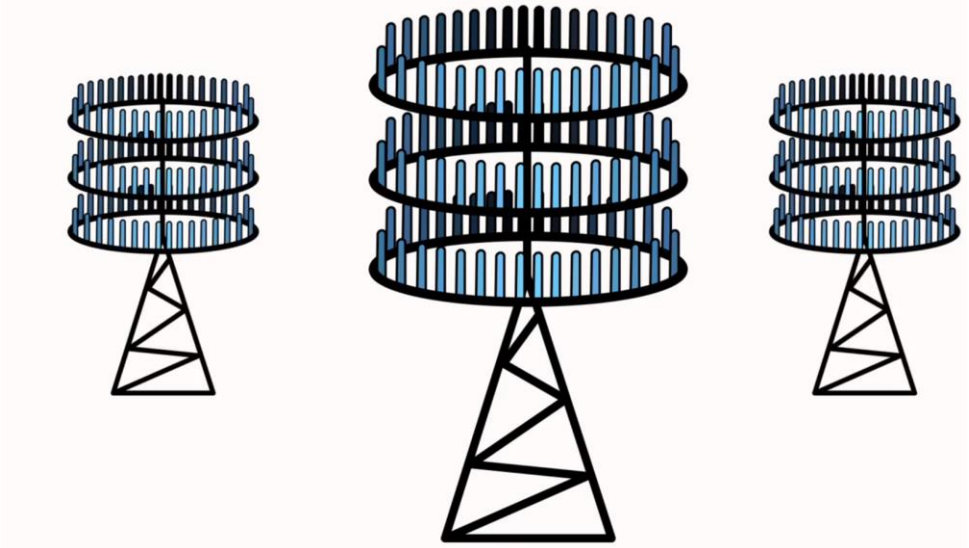
虽然毫米波所在的更高频段具有更大带宽，但是却不能够穿透建筑等介质，甚至会被植物和雨水吸收，为了解决这个问题，其中一个方案就是采用微型基站。

微型基站：现在信号的传输都是通姑一个大型的高功率基站进行传输，由于不会被介质影响，所以通过大功率传输能够覆盖更多的设备，但是在 5G 我们将使用毫米波，如果终端

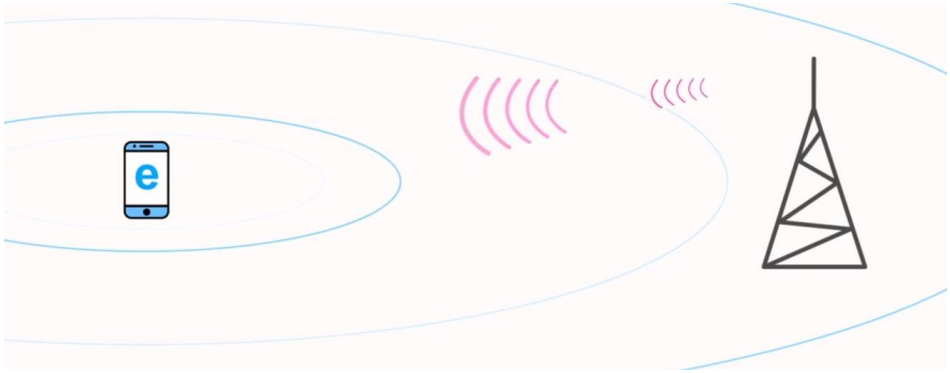
和基站之间有介质格挡，那么终端就接收不到信号。小基站代替大基站就可以解决这个问题，用上千个低功耗的小型基站，进行首发信号来代替现在的大型基站。这种技术特别适用于城市，当终端被建筑物挡住信号以后，手机就会自动切换到另一个小基站来保证传输的稳定性。但是，如果运行商在城市当中，布置那么庞大数量的小型基站，成本会特别高昂，所以像高通就提出了毫米波的移动化，这意味着毫米波需要能在我们走路，或者在车里都能够被服务到。



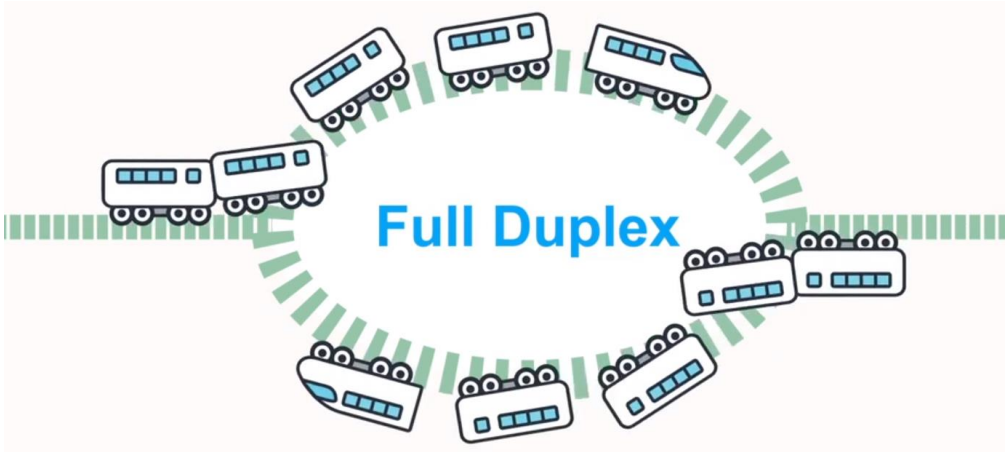
大规模 MIMO：MIMO 指的是多入多出技术，在中国移动的 4G 网络上。基站一侧可能用到了 2 根、4 根到 8 根天线，但是在 5G，超大规模的 MIMO 技术条件下，在基站侧用到最多的是 256 根天线，所以把整个时空上的优越性使用到了极限。



波束成形：波束成形就像一个信号灯，在多个设备之间进行指挥信号应该如何定向传输，当手机上网时，设备发送信号上传，这时信号在空间当中分散式的传播，当基站终端收到信号以后，会根据信号的来源做分析，保证信号全部传输到你的手机，减少信号的丢失。这样上网的速度也就更快。



全双工：实现大量数据的同时上传和下载，无须互相让路。



根据相关研究报告，5G 基础建设将在 2019-2023 年实现，然后渗透到相应的行业应用以及爆发出应有的网络带宽能量在 2022 年-2030 年，具体的基础建设公司和行业应用如下图所示：