# 计算机网络与web技术

2013级 高飙

# 第一章

计算机网络基本介绍：计算机网络是由不同通信媒体连接的、物理上独立的多台计算机组成的、在功能完善的网络软件的支持下实现资源共享和信息交换的系统

计算机网络的参考模型：

协议与分层：为实现计算机网络不同主机、不同操作系统之间的通信而规定的、网络全体成员都必须共同遵守的一系列规则和约定，被称为计算机网络协议（protocol）

# 第二章

1 异步通信

广义上讲，如果发送方和接收方之间在发送数据之前无需进行协调（时钟同步），就称这种通信是异步的（asynchronous）

从技术上讲，如果系统允许物理介质在两次传输之间空闲任意长时间，这种传输系统就被归为异步传输系统

由于异步传输机制允许发送器在传输之间空闲任意长时间，所以其在每次传输之前要发送一些额外信息（称为前导位或开始位），以使接收器能和信号同

2 波特率与比特率

波特率(baud rate): 每秒中硬件产生的电信号变化的次数

比特率(bit rate): 每秒钟传送的二进制位数，也叫“位速率”

比特率=波特率\*[log2(电平数)]

3 带宽：

每个传输系统都有自己的模拟带宽（analog bandwidth），称为硬件带宽

带宽的限制起因于物质与能量的物理特性，每一种物理传输系统都只有有限的带宽

带宽为B，使用K种电压进行数据编码的传输系统上，最大数据传输速率D（每秒位数）为：

D = B \* log2（K）

4 香农定理

信号平均功率 S 噪声为N

D = B \* log2(1 + S/N)

5 传输方式 半双工，单工，全双工

6 串行传输与并行传输

串行传输是将组成字符的各个位（bit）串行地发往线路

串行传输的特点：

传输速度较低，一次一位

通信成本也较低，只需一个信道

支持长距离传输，目前计算机网络中所用的传输方式均为串行传输

字符编码的各位(比特)同时传输

并行传输的特点：

传输速度快：一位(比特)时间内就可传输一个字符

通信成本高：每位传输要求一个单独的信道支持；一个字符包含8个二进制位，则并行传输要求8个独立的信道的支持

不支持长距离传输：由于信道之间的电容感应，远距离传输时，可靠性较低。目前、还仅限于计算机内的传输

7远距离通信 各种复用技术

信号电流在传导过程中会逐渐减弱，这称为信号损耗（signal loss），所以它不能沿导线传播任意长的距离

连续的振荡信号要比其他形式的信号能传播更远的距离。这一结果是绝大多数远距离通信系统的基础

远距离通信要发送连续的振荡信号，称为载波（carrier）。

调制与解调：

两种调制技术：

1调幅（amplitude modulation）：使载波的信号强度随待发送信息而变化

2 调频（frequency modulation）：使载波的中心频率随待发送信息而变化

调幅和调频每传送一个码位都需要至少一个载波周期

更为高效的调制：

移相调制（ phase-shift modulation）技术通过突然改变载波的相位来编码数据。每一个变化称为一个相位移动（phase shift）。在一个相位移动之后，载波继续振荡，但它从载波周期的一个新位置开始

奈奎斯特定理指出，如果编码方式允许在单个载波周期内编码多位（bit）数据，则单位时间内允许发送的数据位（bit）将增加

在相位移动调制技术中，通常把相位偏移选择具有2的幂次方大小。若发送器用T个bit建立一个相位移动，则接收器能通过观察相位移动的程度抽取全部T个bit数据。那么在使用这种调相技术后，系统在一秒内能传输的最大位数（也就是比特率）就可以是波特率的若干倍

比特率=波特率\*单个调制状态对应的二进制位数

在某些情况下，比特率也可能小于波特率

调制解调器 解调

多路复用：

1 频分多路复用

两个或多个使用不同载波频率的信号，可以在同一介质上同时传输而互不干扰

频分多路复用（frequency division multiplexing，FDM）允许多对发送器和接收器在一个共享介质上同时通信。每对发送/接收器所使用的载波，都工作在唯一的、互不干扰的频率上

基带与带宽

人们利用频分多路复用建立了许多网络技术，它们允许在同一介质上同时进行相互独立的通信。使用频分多路复用（FDM）的主要动机在于对高吞吐率的需求

为了达到更高的吞吐率，底层的硬件使用电磁频谱中更大的一部分（即更高的带宽）。这样，宽带技术（ broadband technology）这一术语用来描述这些技术

另一方面，任何只使用电磁频谱中很小的一部分，在介质上一次只发送一个信号的技术称为基带技术（ baseband technology）

扩展频谱：FDM还有一个特殊应用，就是使用多个载波来提高可靠性。这一技术被称为扩展频谱（spread spectrum），并被用于多种目的

采用扩频技术的主要原因是为了在某些频率上偶尔会发生干扰的传输系统中提高可靠性

例如采用无线电波的网络

有些拨号调制解调器也使用扩频传输的形式来改善可靠性

2 波分多路复用

技术上，光的FDM称为波分多路复用（wave division multiplexing）

原理：利用波分复用设备将不同信道的信号调制成不同波长的光，并复用到光纤信道上。在接收方，采用波分设备（如棱镜）分离不同波长的光

用途：波分多路复用实质上是利用了光具有不同波长的特征。随着光纤技术的使用，基于光信号传输的复用技术得到越来越多的重视

3 时分多路复用

各个信源轮流使用同一个共享的通信介质

同步时分复用（STDM）：信源以循环（round-robin）方式使用共享介质

统计时分复用：信源轮流发送数据，但如果某个信源没有数据需要发送，复用器就跳过这个信源所占用的那段时隙。大多数计算机网络都采用统计复用形式

4 码分多路复用

正交向量空间中的值可以互不干扰地复合和分离，因此可根据码型结构的不同来实现信号分割

所有用户使用同一频率，占用相同的带宽，各个用户可以同时发送或接收信号，用各自不同的码片序列区分，各个用户相互之间没有干扰

它不是一项新技术，作为一种多址方案它已经成功地应用于卫星通信和蜂窝电话

分组 帧与差错纠正

分组交换：为使发送方和接收方能协调，并保证所有共享网络资源的计算机能公平、迅速地接入网络，大多数计算机网络都把数据分成叫做“分组”（packet）的小块，计算机通过共享资源轮流地发送分组

因为每个分组都很小，所以不会使任何计算机的等待接入时间太长

分组交换使用了统计时分复用技术，来自多个信源的通信竞争使用信道

因为使用了分组技术，所以计算机网络常常被称为分组网络（packet network），或分组交换网络（packet switching network）

物理帧：为了区分分组的一般概念与某个给定网络所采用的分组形式之间的不同，一般使用术语帧（frame）来指数据链路层（或网络接口层）中特定的分组格式

每种网络技术都会确切地定义网络所采用的帧的细节，例如其大小和格式

数据充填：为了允许帧包含任意数据，必须在传输之前修改数据，并在接收之后恢复数据。用来修改数据的技术叫做数据充填（data stuffing），因为它们插入了额外的位或字节

字节充填（byte stuffing）指使用面向字符型硬件的数据充填，如在拨号线上发送IP数据的点对点协议（PPP）采用字节充填

比特（位）充填（bit stuffing）指使用面向比特型硬件的数据充填，如帧中继技术采用比特充填

有面向字符的协议与面向比特的协议：HDLC填充：在发送方，任意时刻发送5个连续的1后，在发送下一个比特前插入一个0

而对于接收方，如果5个连续的1到达了，则：

如果下一个比特是0，则一定是填充的，将被丢掉

如果下一个比特是1，则继续看下一个比特：

如果是0（即最后的8比特是01111110），则它一定是帧结束标记

如果是1，则一定是传输错误，需要丢弃整个帧；并且等到下一个01111110出现才能再次开始接收数据

检错与纠错：

检错：为了检测差错，网络系统通常要随数据一起发送一些附加位，接收端通过这些附加位可以对所接收的数据进行判断看其是否正确。如果存在错误，它不能纠正错误而是通过反馈信道传送一个应答帧，把这个错误的结果告诉给发送端，让发送端重新发送该信息，直至接收端收到正确的数据为止。

常用检错机制：目前比较常见的检错机制

奇偶校验码（parity check）

校验和（checksum）

循环冗余校验（CRC check）

# 第三章

局域网：从点到点到共享信道。

拓扑结构：星型，环型，总线型

介质访问控制办法：

1 CSMA/CD（带冲突检测的载波监听多址访问，802.3）

CSMA/CD是英文carrier sense multiple access with collision detection 的缩写，即“载波侦听多址访问/冲突检测”，或“带冲突检测的载波侦听多址访问”

算法规则：（本质上是改进了的1-坚持型的）

监听总线，等待空闲时发送数据

如果两台（或更多）计算机同时传输，冲突就会发生；当发生冲突时，每个计算机选择一个小于最大延迟x（x是每台计算机自己确定的值） 的随机延迟；这样选择到最小延迟的计算机将首先发送帧

如果一台计算机遇到连续的冲突，那么在随后的每次冲突后，它都把x加倍

2 CSMA/CA

无线局域网使用一种改进的机制—避免冲突的载波侦听多址访问（Carrier Sense Multiple Access with Collision Avoidance，CSMA/CA）

源计算机在传输一个帧之前先发送很短的控制消息

目的计算机接收到控制消息后，发送另一个控制消息表明已经准备好接收数据

当源计算机接收到响应的控制消息后，它就可以开始发送帧

在CSMA/CA中，控制消息的传输可能会发生冲突，但能够很容易地处理。当这种冲突发生时，发送者可以随机等待一段时间，然后重发控制消息。因为控制消息比数据帧要短得多，所以发生第二次冲突的可能性也要比传统以太网要小很多

以太网：以太网：以太网是最早的局域网，也是目前最常见、最具有代表性的局域网

它的核心思想是使用共享的公共传输信道，来源于夏威夷大学的ALOHA无线通信网络

不监听，直接发送；若冲突，则在整帧发完后，再以概率p重发

最早的以太网是由美国施乐公司（Xerox）建立的，其灵感来自“电磁辐射是可以通过发光的以太来传播的”，这也是“以太网”的名字的由来

以太网逐步标准化后形成了802.3协议规范

以太网是一种基于总线的局域网，它使用改进了的1-坚持的CSMA/CD协议；我们通常说到以太网，指的就是那些采用CSMA/CD 协议的局域网

以太网的帧格式：

以太网的新老版本能够保持兼容的主要原因在于帧格式，它自从20世纪70年代DIX被创建后就一直保持不变（82版和79版在帧格式上无变化）

三部分：固定长度的头部、可变长度的载荷以及CRC校验码

帧类型可指明数据中所包含的报文类型，如是IP数据报（0800）还是ARP报文（0806）

网络接口卡：大多数计算机网络以固定的速率通过介质传输数据，这个速率通常比计算机处理位串的速率快。为了解决速度上的不匹配，连接在网络上的每台计算机都包含一种叫做网络接口卡（NIC）的特殊功能的硬件

网卡的功能像一种I/O设备：它为特定的网络技术而制造，并且不需要CPU就能处理帧的发送与接收过程

网卡和计算机之间的通信是通过计算机主板上的I/O总线，以并行传输方式进行的

逻辑拓扑与物理拓扑：双绞线以太网布线物理上形成星型拓扑，而集线器是星型的中心。尽管如此，它的功能像总线--所有计算机共享一个通信介质，计算机必须竞争介质的使用，并且任何时候至多只有一台计算机能传输数据

为了解决这个明显的矛盾及理解网络技术，我们需要区分物理拓扑与逻辑拓扑。从物理上讲，双绞线以太网使用星型拓扑。逻辑上讲，双绞线以太网的功能像总线。这样，双绞线以太网通常叫做星型总线（star-shaped bus），或被称为盒中总线（bus in a box）

局域网的距离控制：局域网的连接距离是设计局域网时考虑的一个基本因素。限制局域网连接距离的主要因素就是公平访问机制

两个最常用的访问机制是CSMA/CD和令牌传递，它们的响应时间都和网络的大小成正比。为了达到较小的网络延迟，局域网的连接距离就会受到限制

另一个限制因素是硬件发射固定能量的电磁波。不幸的是，由于电信号在导线中传输时逐渐变弱，信号不可能被传输到无限远

局域网硬件是为固定的最大电缆长度而设计的，当超过该距离后，局域网便不能正常运行

中继器：限制局域网连接距离的一个因素是电子信号在传输时会衰减。为消除这个限制，一些局域网用中继器来连接两根电缆。中继器并不理解分组或信号编码，它只是放大接收到的信号，并将放大后的信号进行转发

网桥：网桥（bridge）能处理一个完整的帧（因此是数据链路层设备）

网桥以混杂模式（promiscuous mode）侦听每个网段上的信号，当它从一个网段接收到一个帧时，网桥会检查并确认该帧是否已完整地到达，然后根据需要就把该帧传输到其他网段。网桥能够隔离故障两个局域网网段通过网桥连接后，就象一个局域网一样。桥接局域网上任何一对计算机都能互相通信，计算机不知道是否有网桥把它们隔开

交换机：交换局域网的功能就象用网桥连接多个局域网网段。连到交换机的每台计算机就像连到一个专用的局域网网段。许多LAN技术都可以使用交换机

交换或桥接网络的主要优点在于它能提供最大的性能：交换机允许多对计算机间同时交换数据

虚拟交换机：通过加入虚拟化措施，可以对交换机进行扩展，扩展后的交换机称为虚拟局域网交换机（VLAN switch）

允许管理员进行配置，使一台交换机可以仿真多台独立的交换机

管理员划定交换机上的一组端口并将它们指派给VLAN 1，再把另一组端口指派给VLAN

2，

一旦配置完成，一台VLAN交换机看起来就像是多台交换机

比如，当VLAN 2的一台计算机广播一个分组时，只有在同一个VLAN上的计算机才能接收到该广播分组的副本

# 第四章

1 分组交换机

广域网中的基本构件是分组交换机（packet switch）。可以这么理解：广域网由一些分组交换机互连而构成，然后将计算机连接在交换机上

分组交换机：能把完整的分组从一个节点传送到另一个节点的设备

2 存储/转发

不像共享局域网在一个给定时间内只允许一对计算机交换帧，广域网允许许多计算机同时发送分组。广域分组交换系统的基本模式是存储/转发（store and forward）式交换

为完成存储/转发功能，分组交换机必须在存储器中对分组进行缓冲：当分组到达时，分组交换机的输入/输出硬件把一个分组副本放在存储器中并通知处理器，然后进行转发操作

处理器检查分组，决定应该送到哪个接口，并把分组输送到输出硬件

好处：使用存储/转发模式的系统能使分组以硬件所可容许的最快速度在网络中传送

更重要的是，如果有许多分组都必须送到同一个输出设备，分组交换机能将分组一直存储在存储器中排队，等待该输出设备准备好发送。这项技术使分组交换机能对同时到达的短时突发分组进行缓冲在一般情况下，分组不会在存储器中停留时间过长，但如果有很多计算机要同时发送分组时，就会增加延迟。

3 路由算法

存储下一站信息的表通常称为路由表（routing table），转发一个分组到下一站的过程称为路由（routing）

使用两部分层次地址转发分组时，首先检查分组目的地址中的第一部分（对应于分组交换机的那部分）

如果它与本交换机相一致，就利用第二部分地址把分组发送到计算机。否则，利用该地址在路由表中选择下一站

为了使广域网能正确地运行，分组交换机都必须有一张路由表，并且都能转发分组

在较小的网络中，路由表中重复的项不多。然而，表示大型广域网的图中，其路由表会有数百或更多重复的项

大多数广域网系统都允许路由表使用一个单项来代替那些具有相同下一站的项，称为默认路由（default route）或默认路由表项（default routing table entry）

一个路由表中只有一个默认项，并且比其他项的优先级低；如果一个给定的目的地址没有明确的项对应，则使用默认项

有两种方法：

静态路由：分组交换机启动时由程序计算和设置路由，此后路由不再改变

优点是简单、网络开销小

缺点是缺乏灵活性，不能随时应对网络变化

动态路由：分组交换机启动时由程序建立初始路由，当网络变化时随时更新

由于大型网络在设计上都留有冗余连接来应对偶发的硬件故障，所以大多数大型网络都采用动路由选择算法的设计目标：

最优化(Optimization)

简单性与低开销(Simplicity and low overhead)

强壮性和稳定性(Robustness and stability )

快速收敛(Rapid convergence )

灵活性(Flexibility)态路由

4 私有网络与公众网络

单个公司或个人拥有和使用的网络称为私有（ private）的，而公共线路运营商拥有的网络称为公用（public）网络。局域网技术大多数用于私有网络，大单位也可拥有连接多个地点的计算机的私有广域网几乎所有公用网络都是广域网；对于网络来说，公用是指服务上的公用，而非所传输数据的公用。私有网络为使用该网络的人所拥有。公用网络就和电话系统一样，属服务提供者所拥有和操作。任何用户都可以使用公用网络与其他用户通信

5 VPN

虚拟私有网络（Virtual Private Network，VPN）结合了公用和私有网络的优点，它允许具有多个站点的公司拥有一个假想的完全私有的网络，而使用公用网络作为其站点之间交流的传输线路。为建立一个VPN，公司要为其每个站点购买一套特殊的硬件和软件系统，该系统安放在公司的私有（即内部）网络和公用网络之间。每个VPN系统必须配置好该公司的其他VPN系统的地址，使软件只在这些VPN系统之间交换分组。为保护隐私， VPN还在每个分组发送前进行加密

6 面向连接/无连接的服务

从层次上看，广域网中的最高层就是网络层，网络层为连接在网络上的主机提供各种服务。虽然不同网络中接口机制的细节各不相同，但接口的一般类型被称为接口模式（interface paradigm）或称为服务模式（ service paradigm）

网络被划分为两大类：

面向连接型服务（connection-oriented service，COS），也称为虚电路服务

无连接型服务（connectionless service，CLS），也称为数据报服务

面向连接型（虚电路）服务模式

主要优点：记帐方便而且在连接中断时能立即告诉通信的计算机（例如当硬件不能正常工作时）

无连接型（数据报）服务模式

主要优点是初始开销小—无连接网络允许计算机直接发送数据，而不必等待连接

无连接系统中的故障可能不被（立即）发现—计算机在网络故障发生后仍继续发送分组

7 异步传送模式ATM

为了能使分组交换机高速工作又能达到低延迟、低抖动和回波抑制，ATM技术中将所有数据都划分成很小的、固定长度的分组，叫做信元（cell）。ATM采用面向连接型（虚电路）服务模式（connection-oriented service paradigm，COS）。这种模式要求应用进程首先要为通信建立虚拟信道（virtual channel，VC），通信完了要拆除它。ATM为每个VC分配一个24位标识符，前8位是虚通道标识符（virtual path identifier，VPI），后16位是虚信道标识符（virtual channel identifier，VCI）。ATM网络由一个或多个称为ATM交换机的硬件设备构成。每个交换机都要在它的转发中为一条VC设置一个表项。

# 第五章

1 网络协议

规定计算机信息交换中消息的格式和含义的协定称为网络协议（network protocol），或计算机通信协议（computer communication protocol）

2 分层模型

帮助设计者控制协议软件复杂性的基本工具，就是分层模型

通过分层可以把复杂的通信问题划分成若干不同的部分，然后设计者可以每次集中解决一个部分。分层的科学原理为进行分层设计提供了基础。分层原理阐述：在目的端的第N层上，要把源端第N层上进行过的变换，进行逆变换

3 栈：分层软件

协议软件的组织遵循所设计的分层模型。每一层对应于一个软件模块，厂商将模块集总称为栈（stack）

理论上说，发送的数据在发送机上向下通过栈的每一层，在接收机上向上通过栈的每一层

由于每个栈是独立开发的，一个特定栈的协议不能与另一个栈的协议交互

在过去的三十多年里，有不同的厂商开发了一些协议栈，如Novell公司的Netware、苹果公司的AppleTalk以及IBM公司的SNA等，但这些协议栈目前已基本为TCP/IP协议所代替

4 协议采用的通用技术

使用排序来处理乱序和重复分组

无连接网络不保证顺序；硬件设备操作失误可能导致重复的分组

使用确认和重发来处理丢失分组

分组丢失是一个网络的基本问题

使用唯一的会话标识符来防止重传

避免前次会话对后次会话的干扰

使用停-等式协议或滑动窗口机制来控制流量

使用降低速率来处理网络拥塞

5 停等协议

计算机并不都以相同的速度运行。当一台计算机通过网络发送数据的速度比目的计算机接收数据的速度快时，就出现了数据过载，从而导致数据丢失

解决数据过载问题的技术称为流量控制（flow control）机制

最简单的方式是停-等模式：

每发出一个分组便等待接收方的回答；当接收方准备好接收下一个分组时，发送一个控制报文，通常就是某一种形式的确认

这种简单的停-等协议避免了过载，却降低了网络带宽的利用率

6 滑动窗口

程序设置发送方和接收方使用固定的窗口尺寸（ window size），这是在收到确认前可以发送的最大数据量

发送方在开始发送数据时，提取数据填入第一个窗口，并发送每个分组的副本。如果有可靠性要求，发送方应保留一份副本，以备万一需要时重发

接收方必须准备好缓冲区空间以接收整个窗口。当分组顺序到达时，接收方把分组传给应用程序，并返回一个确认给发送方

当确认到达后，发送方丢弃已被确认的副本，并发送下一个分组

可以通过调节窗口大小使计算机充分利用可用的硬件带宽，获得高吞吐率

7 网络拥塞

6台分组交换机。如果到达站点3的数据速率远远快于站点3所能通过连线发到站点4的数据速率，那么站点3就只能把数据放在发送队列中排队，这样队列不断增大，有效延迟增加，从而形成拥塞（congestion）

如果拥塞持续下去，分组交换机将发生内存溢出，开始丢弃分组并导致重发。如果这种情况一直持续，整个网络将变得不可用，这种情况称为拥塞崩溃（congestion collapse）

协议应该监视网络，一旦发现拥塞就迅速地做出反应，避免拥塞崩溃

当拥塞出现时，让分组交换机通知发送方

分组交换机给每个由于拥塞而产生延迟的分组头部设置一个码位，接收该分组的计算机如果发现分组头部中置了该码位，就在确认报文中加入有关消息来通知源发者，或者

当出现拥塞时，让分组交换机发送一个特殊报文给分组的源发者

将分组丢失作为拥塞的估计。这是因为现代网络中，硬件工作良好，大多数的分组丢失是由于拥塞而不是硬件故障引起

对拥塞的适当响应，主要是降低分组传送速率

8 路由器

用于连接异构网络的基本硬件是路由器（ router）

路由器是一台专门完成网络互联任务的专用计算机

路由器可以将多个使用不同技术（包括不同的介质、物理编址方案或帧格式）的网络互联起来

9 互联网体系结构

互联网由一组通过路由器连接起来的网络构成

虽然商用路由器可以连接多个网络，但人们很少使用单个路由器连接所有的网络，因为：

路由器的CPU和内存要用来处理每个被传递的分组，而单个路由器的处理器不足以处理太多的网络之间的通信量

冗余度能改善互联网的可靠性。在某个网络或路由器发生故障时，其他路由器可沿另外的通路传输通信业务

在规划互联网方案的时候，允许使用单位按使用要求来选择

网络的数量和类型

用于互联的路由器数量

以及具体的互联拓扑结构

互联网拓扑结构的具体细节，常常依赖于物理网的带宽、预期的通信量、单位的可靠性要求，以及路由器硬件的费用和性能等

10 TCP/IP协议

TCP/IP协议是Internet的标准通信协议

制定Internet数据分组（packet）格式和规则（对应网络层）

确保数据能传送到目标系统上（对应传输层）

IP协议主要的任务是为数据传送提供正确的路径，以及提供相邻节点之间的数据传送

IP协议实现了主机之间相同格式数据的传输，但不能保证数据分组在传输中不会出现差错

TCP协议功能包括分组重发技术、时序调整和拥塞控制机制等，以保证数据在Internet上的可靠传输

互联层的核心协议是IP，其他协议有ARP、ICMP、IGMP

其中ARP为地址解析协议，负责网络接口层地址的互联层地址解析，比如将互联层地址解析为硬件地址

ICMP为互联网控制报文协议，负责提供诊断功能，报告关于IP数据分组传送的错误或信息

IGMP为Internet组管理协议，负责IP多点传送组的管理

传输层核心协议是传输控制协议TCP和用户数据报协议UDP

其中，TCP 提供一个一对一的、数据无差错的可靠性传输服务

UDP则提供一个一对一或一对多、无连接、不可靠的通信服务，主要用于不要求数据报顺序到达的传输

10 ip编址方案

在TCP/IP协议栈中，编址由互联网协议（ Internet Protocol，IP）规定

目前的IP标准规定每台主机分配一个32位二进制数，作为该主机的互联网协议地址（ Internet Protocol address），常简写为IP地址或互联网地址

在互联网上发送的每个分组中，都含有这种32位的发送方（源）IP地址和接收方（目的）IP地址

为了在使用TCP/IP的互联网上发送信息，一台计算机必须知道接收信息的远程计算机的IP地址

IP地址是一个32位的二进制数。每个地址属于五类地址之一，而地址的类，由地址的头4位决定。一个包含254到65534台主机的网络可分配给一个B类网络号；更小的网络可分配一个C类网络号，更大的网络被分配一个A类网络号 A for0 Bfor 10 cfor110D for 1110 Efor 1111

12 特殊ip地址

本地地址（全0）：当计算机启动时，可以使用TCP/IP中的一个协议来自动获得自己的IP地址；为此，IP保留了全0地址来表示本台计算机

网络地址（网络前缀+后缀为全0）：表示网络本身，如128.211.0.0表示一个已分配给B类前缀为128.211的网络

直接广播（网络前缀+后缀全1）：对指定网络中的所有站点进行直接广播，例如送信息到190.43.255.255，表示将信息送给网络号为190.43中的每一台主机

有限广播（全1）：limited broadcast，在本地物理网内进行广播（路由器不转发）

回送地址：网络号127是用来做循环测试用的，不可拿来做其他用途。例如如果送信息给IP地址127.0.0.1，则此信息将回传给自己

第一个数字W不可高于223，因为它们是给Multicast（多址通信即组播，D类，前缀1110）或保留给将来使用（E类，前缀1111）

13 子网和无类地址

有类编址方案因为因特网的成长而逐渐受到限制

分给的类小则地址不够用，类大则造成许多地址闲置无用

子网编址（subnet addressing）和无类编址（classless addressing）可以在某种程度上克服这种限制

它们不采用三个基本IP地址类，而是改为直接利用前缀和后缀在地址的任意码位上进行分界

例如，对于一个只有9台主机的网络，ISP可以分配28位长的前缀，其余4位作为主机后缀（可容纳14台主机），而不必分配给该网络一个C类地址

无类和子网编址方案要求随同地址一起还要存储一个32位的指定网络前缀和后缀的分界值，这个值称为地址掩码（address mask）或子网掩码（subnet mask）

用位值1来标记网络前缀，用位值0来标记主机后缀

使用掩码来保存分界值，可以把目的地址和地址掩码进行“逻辑与”操作，直接得到目的地址的网络前缀，提高地址计算效率

14 CIDR表示法

CIDR表示法是一种新的语法，它通过在一个地址的后面附加一个斜杠符和一个用十进制数表示的掩码大小值，来指定与此地址相关的掩码

如地址128.10.0.0由16位网络前缀和16位主机后缀组成，用CIDR表示法可以写成：128.10.0.0/16

如果有两个客户都只有12台计算机，那么ISP可以采用CIDR方法将一个C类网络（比如192.211.15.0）划分为三个部分，其中两个，如192.211.15.16/28和192.211.15.32/28，分别分配给客户，而剩余部分留作备用；虽然客户都有同样28位的掩码，但它们前缀不同，所以不会产生混淆

15地址解析

将计算机的协议地址翻译成等效的硬件地址的过程，叫做地址解析（ address resolution），即协议地址被解析（resolved）为正确的硬件地址

主机或路由器当需要向同一物理网络内的另一台计算机发送数据时，要进行地址解析

一台计算机没有必要，同时也不能解析远程网络上的计算机地址

ARP协议

TCP/IP协议组包含了一个标准的地址解析协议（Address Resolution Protocol，ARP）。ARP定义了计算机交换的ARP报文格式和处理ARP报文的规则

这一标准规定了一个 ARP请求报文是全网广播的，但响应报文却是直接发送的

尽管ARP报文格式通用于任何协议和硬件地址，但在实际应用中，此协议主要还是用于将一个IP地址解析成一个以太网地址

当一台计算机给另一台计算机发一个ARP报文时，此报文被嵌入在一个硬件帧中进行传输，即把它当作数据来传输

技术上，把一个报文放在帧中传输叫封装（encapsulation）。ARP被直接封装于一个硬件帧中

网络硬件不了解ARP报文格式，且不检测其中每个域中的内容

第一步，接收方从报文中取出发送方的地址绑定信息，检查cache中是否存在发送方的地址

若无，则将发送方地址绑定信息加入自己的cache中，以便以后加以利用

若已有，则用从报文中取出的绑定信息替代已有的绑定信息

第二步，接收方检查报文中的“操作”域以确认报文类型

若是一个响应报文，接收方以前一定发送过一个请求并在等待所需要的绑定信息

若是一个请求报文，接收方比较“目标协议地址”域与自己的协议地址，如果一样，则要回发一个ARP响应

16动态主机配置协议DHCP

为了帮助一台新加入某网络的主机获得其IP地址

早期使用反向地址解析协议RARP，允许计算机从服务器获得IP地址；同时可以借助ICMP协议发送“Address Mask Request”和“Router Discovery”报文，获得指定网络上使用的地址掩码和路由器地址

后来又有了自举协议（Bootstrap Protocol，BOOTP），允许主机通过一个请求获得多个协议参数

IETF扩展了BOOTP的功能，形成了DHCP

当主机启动时，它广播一个DHCP请求，服务器则发送一个DHCP应答。管理员一般将固定地址分配给服务器，而将动态地址分配给其他主机

按需分配的地址不是永久的，而是由DHCP产生一个有限的地址租用期。当租期满时，主机可以释放地址，也可以与DHCP服务器重新协商延长租期，但服务器拥有绝对的控制权

分组出现丢失或重复时

如果主机没有收到响应，必须重新发送它的请求报文；如果收到重复的响应，则忽略这个多余的副本

对服务器地址进行高速缓存

主机一旦使用DHCP Discover报文找到了一个DHCP服务器，就将服务器的地址存入缓存中以备后用，从而提高租期续约过程的效率

避免因同时出现大量请求而发生阻塞

为防止网络中的大量主机同时发送请求涌入DHCP服务器而导致阻塞，DHCP协议要求每个主机在发送（或重发）请求之前要等待一个随机时间

17 Ipv6改革动机

IPv4定义的有限地址空间将被耗尽

许多企业不得不使用NAT将多个内部地址映射成一个公共IP地址，但使用NAT技术会造成私有地址网络的连接问题

妨碍互联网的进一步发展

需要地址配置自动化、简单化

越来越多的设备使用IP地址地址配置自动化

Internet主干网路由器有维护大型路由表的能力

层次路由机制平面路由机制

IP层安全需求

更好的实时QoS支持的需求

改革难点

由于对IP的依赖性以及IP带来的后续惰性，因而产生了一个重要的问题：

因为IP处于所有因特网通信的中心位置，所以改变IP就会改变整个因特网

下一代IP被称为IPv6

IPv6保留了IPv4很多非常成功的设计特性

无连接，每个数据报都含有目的地址，并可独立选择路径

头部含有最大跳数

此外还保留了IPv4可选项中提供的大多数通用性设施

但IPv6的变化非常大，它几乎修改了所有的细节

# 第六章

1 IP数据报

虚拟分组：传统的硬件帧格式不适合作为互联网上的分组格式

由于路由器可能连接异构的网络，不同类型网络的帧不同，它不能直接将网上送来的帧传给另一个网络

路由器也不能简单地重新格式化帧的头部，因为两个网络可能使用不兼容的地址格式

为了克服异构性，一个互联网必须定义一种与硬件无关的分组格式

结果就产生了一种能无损地在底层硬件中传输的通用的（ universal）、虚拟的（virtual）分组

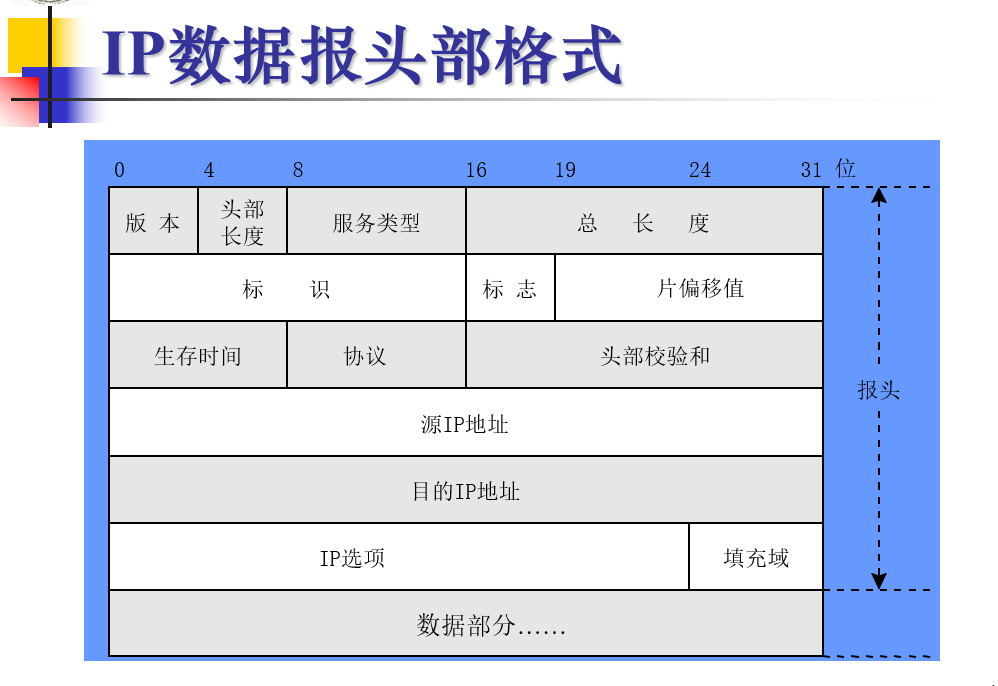
IP数据报：TCP/IP协议使用IP数据报（ IP datagram）这个名字来命名一个互联网分组

IP数据报与硬件帧有着同样的基本格式： IP数据报也是以一个头部开始，后跟数据区

数据报头部中源地址和目的地址都是IP地址

数据报的大小取决于发送数据的应用。大小可变的数据报使得IP可以适应各种应用的需要

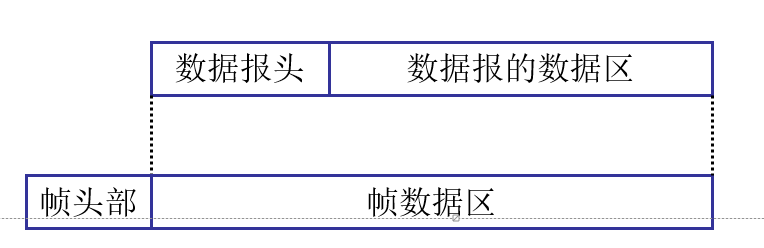
2 IP头部格式



3 IP封装、分片和重装的整个过程

由于在物理网络中，数据是以帧的形式传输的。因此数据报也必须封装成帧来传输。将整个数据报作为数据装入帧的数据区就称为封装。如下图所示

帧中的目的地址是数据报去往的下一站的地址；这个地址是通过将下一站的IP地址翻译成等效的物理地址而得到的



每一种物理网络都规定了一帧所能携带的最大数据量，这一限制称为最大传输单元（maximum transmission unit, MTU）。因此在互联网中，路由器从一个网络上接收到的帧并不意味着能在另一个网络中直接发送。为此，IP协议中采用一种对数据报进行分片的技术

当路由器收到一个数据报，其大小超过所去网络的MTU时，路由器会将它分成若干较小的 “片”（fragment），然后再分别发送这些数据片

每一片都使用IP数据报格式，但只携带了原数据报的一部分数据

在IP数据报的报头中，与一个数据报的分片和组装相关的域有标识域、标志域与片偏移域

标识（identification）域

为一个数据报的所有片分配一个标识ID值

标志（flags）域

占 3 bit。目前只有前两个比特有意义

标志字段中的最低位记为 MF (More Fragment)。MF = 1，表示后面“还有分片”的数据报。MF = 0，表示这已是若干数据报片中的最后一片

标志字段中间的一位记为 DF (Don’t Fragment)，意思是“不能分片”。只有当 DF = 0时才允许分片

片偏移（fragment offset）域，13个bit长

表示该分片在整个数据报中的相对位置（8B为一个单位）

在所有片的基础上重新产生原数据报的过程叫重装（reassembly）

数据报的分片是在传输路径中MTU不同的两个网络间的路由器上发生的，而片的重装在目的主机中进行：

这样做可以减少路由器中的状态信息数量

这样做允许动态改变路径

一个数据报的一部分片到达的同时，很可能仍有一些片被延迟或丢失。尽管这时数据报还不能被重组，接收方仍须保留所有已收到的片，以防未到的片可能只是被延迟

当数据报的某一片第一个到达时，接收方开始一个计时器。引入IP重组计数器的结果是全有/全无（all-or-nothing）：要么所有的片都到达了并且IP重组数据报，要么IP丢弃了整个数据报

分片之后，路由器将每一片转发给它的目的地。如果某片遇到一个MTU值更小的网络时，分片方案规划得很周到，它使得片本身能够再被分片

IP对原来的片与再分的子片并不加以区分，接收方也并不知道收到的是一个第一次分片后形成的片，还是一个已经被多个路由器多次分片后形成的片

同等对待所有片的优点在于：接收方并不需要先重装子片后才能重装原数据报。这样一来就节省了CPU时间，减少了每一片的头部中所需的信息量

4 Ipv6数据报



IPv6数据报分为“不可分片部分”和“可分片部分”

“不可分片部分”指基本头部加上控制路由的头部

IPv6不将包含分片信息的域放在基本头部，而是放在一个单独的扩展头部中，该头部的存在就表示该数据报是一个片（“不可分片部分”+“第N片头部”+“第N片内容”）

在IPv4中，由路由器负责执行分片任务。但在IPv6中，则由发送方主机负责分片，路由器不再参与。如果需要分片，发送方主机将收到中间路由器发送的ICMP差错报文。发送方会不断减小分片长度，一直到分片能最终送达目的端为止

主要原因是IPv6可能根据需要会对路由进行控制，使各片都按同一路径传输。

5 ICMP差错报告机制

尽管IP使用了“尽力而为”（best-effort）的传送语义，但IP还包含了差错检测和报告机制

除了一个头部校验和可用于检测传送错误外， IP还实现了一个差错报告系统叫做互联网控制报文协议（Internet Control Message Protocol，ICMP）

ICMP包含信息报文以及差错报文。当一个数据报出现问题时，路由器将发送一个ICMP差错报文给源主机

ICMP利用8位长的“类型”域来识别每个报文

差错报文例子:

**源抑制（ Source Quench**）。当一个路由器收到太多的数据报以至于用完了缓冲区，就必须丢弃到来的数据报。当丢弃一个数据报时，路由器就会向创建该数据报的主机发送一个源抑制报文。当一台主机收到源抑制报文时，就需要降低传送率

**超时（Time Exceeded）**。有两种情况会发送超时报文。当一个路由器将一个数据报的生存时间（Time To Live）域减到零时，路由器会丢弃这一数据报，并发送一个超时报文。另外，在一个数据报的所有片到达之前，重组计时器到点了，则主机也会发送一个超时报文

**目的不可达（ Destination Unreachable）。**

无论何时，当一个路由器检测到数据报无法传递到它的最终目的地时，就向创建这一数据报的主机发送一个目的不可达报文

这种报文要告知是特定的目的主机不可达，还是目的主机所连的网络不可达。换句话说，这一差错报文能让我们区分是某个网络暂时不在互联网上（例如一个路由器出错），还是某一特定主机临时断线（例如主机关了）

**重定向（Redirect）**

当一台主机创建了一个数据报发往远程网络，主机先将这一数据报发给一个路由器，由路由器将数据报转发到它的目的地

如果路由器发现主机错误地将应发给另一路由器的数据报发给了自己，则使用一个重定向报文通知主机应改变它的路由

一个重定向报文能指出是一台特定主机还是一个特定网络发生了变化，后者更为常见

**参数问题。**指出数据报中的某一参数不正确

ICMP利用IP来传送每一个差错报文。ICMP报文整个被装入IP数据报的数据区中，而IP数据报又被封装进帧中进行传输

每一个ICMP报文的产生总是对应于一个数据报，而数据报在头部中都含有其源主机的IP地址，路由器可取出作为ICMP报文的目的地址

如果携带ICMP差错报文的数据报又出了错，不再有差错报文被发送—以此避免互联网被携带差错报文的差错报文所拥塞

ping使用ICMP回应请求报文和回应答复报文来实现

当调用ping程序时，它发送一个包含ICMP回应请求的报文给目的地，然后等待一段很短的时间。如果没有收到应答，则重新传送请求。如果重传的请求仍没有收到应答（或收到一个ICMP目的不可达报文），ping声称该远程机器为不可达

远端主机上的ICMP软件负责答复该回应请求报文。按照协议，只要收到回应请求， ICMP软件必须发送回应答复报文

Traceroute程序的操作过程（理想状况）

发送一份TTL字段为1的IP数据报给目的主机

处理这份数据报的第一个路由器将TTL值减1，丢弃该数据报，并发回一份ICMP超时报文

这样就得到了该路径中的第一个路由器的地址。然后Traceroute程序发送一份 TTL值为2的数据报，这样我们就可以得到第二个路由器的地址……

由于IP使用尽力传递，数据报还可能丢失、重复、或乱序传递，因而，路由跟踪程序必须准备处理重复响应和重发丢失的数据报

由于路由可能动态地发生变化，路由跟踪程序更适合于一个相对比较稳定的互联网

* **尽管分片解决了异构网络问题，但却常常影响到性能**
* **从源端到目的地的路径上的最小的MTU叫通路MTU（path MTU）。只要数据报不大于通路MTU，就可以直接被传送到目的地而不被分片**
* **如何确定通路MTU呢？**
  + **源端主机上的IP软件发送一系列的探测报文，每一探测报文的数据报的头部的DF标志位都被置为1而防止分片**
  + **如果探测报文的数据报比路径上的某个网络的MTU大，连在此网上的路由器会丢弃探测报文数据报，同时发回一个要求分片的ICMP报文给源主机**
  + **源主机在收到这一差错报文后，就会发送另一个较小的探测报文；----如此这般，直到某一探测报文成功**

6 UDP协议

IP无法区分在同一台计算机中的多个应用程序

在数据报头部中源和目的地址域只是标识计算机主机；它没有包含更多码位来标识主机上的应用程序

能够允许将单个应用程序作为通信端点（endpoint）的协议，被称为端到端协议或者传输协议（end-to-end or transport protocol）

TCP/IP协议的设计者不是采取在IP基础上增加附加特性的方法来标识应用，而是设置一个单独的层次（传输层）来配置端到端协议

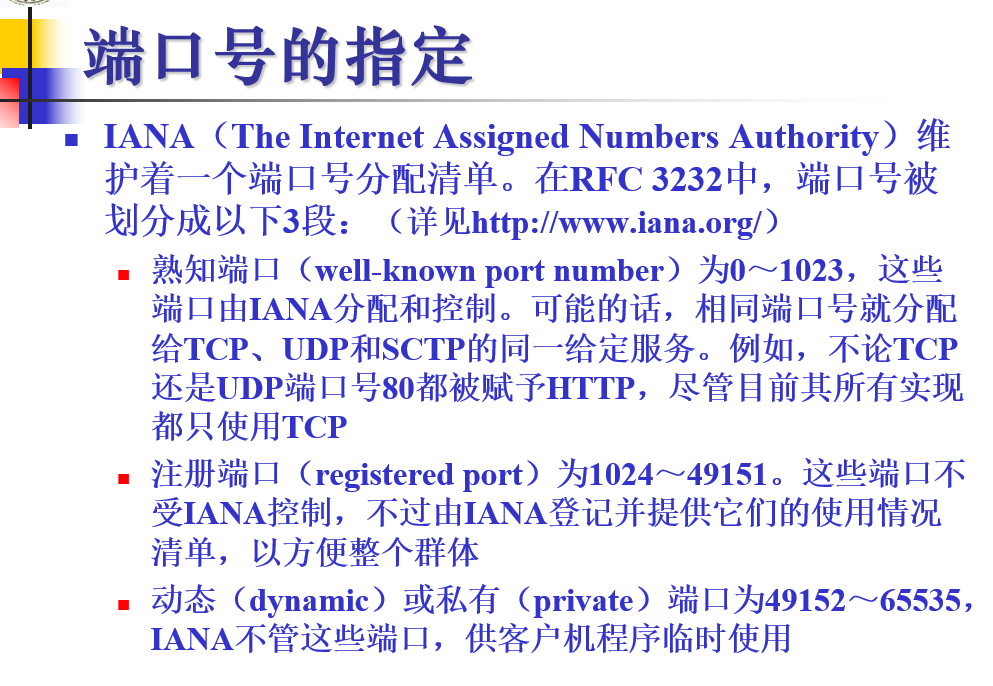
UDP（User Datagram Protocol）是一个简单的面向数据报的传输层协议，它允许应用程序发送和接收单个报文，每个报文用单独的IP数据报传输

端到端：它提供协议端口，使得应用进程能够向其他进程发送数据报，进行进程间的数据通信

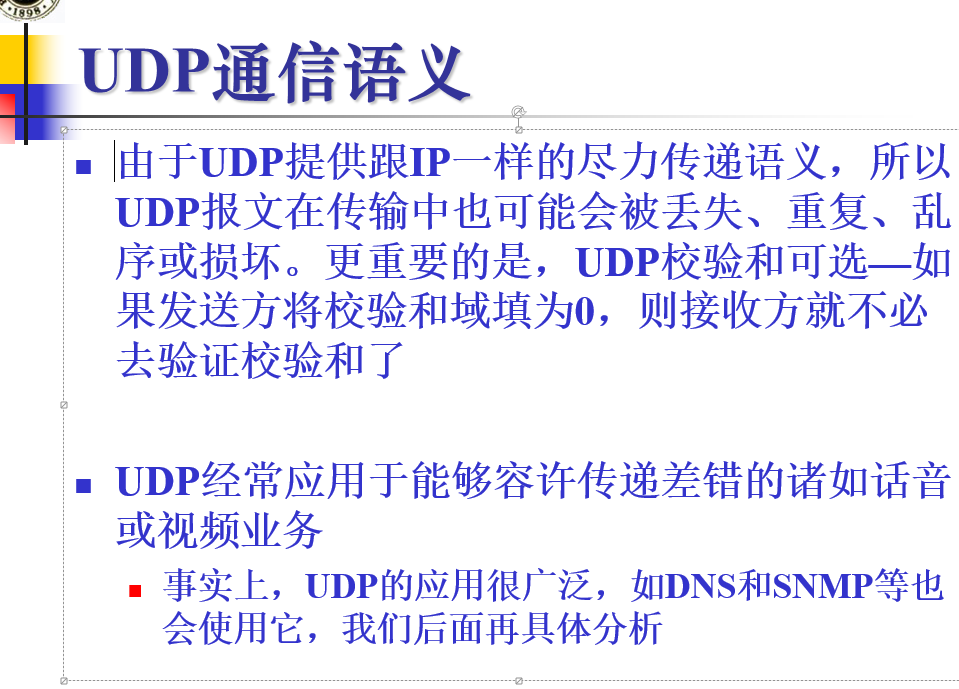
UDP数据报是无连接、不可靠的：UDP不提供确认、消息反馈控制，这一点与IP数据报相同。它的可靠性需要由应用程序本身提供

面向报文：使用UDP的应用进程所发送和接收的数据是单个报文



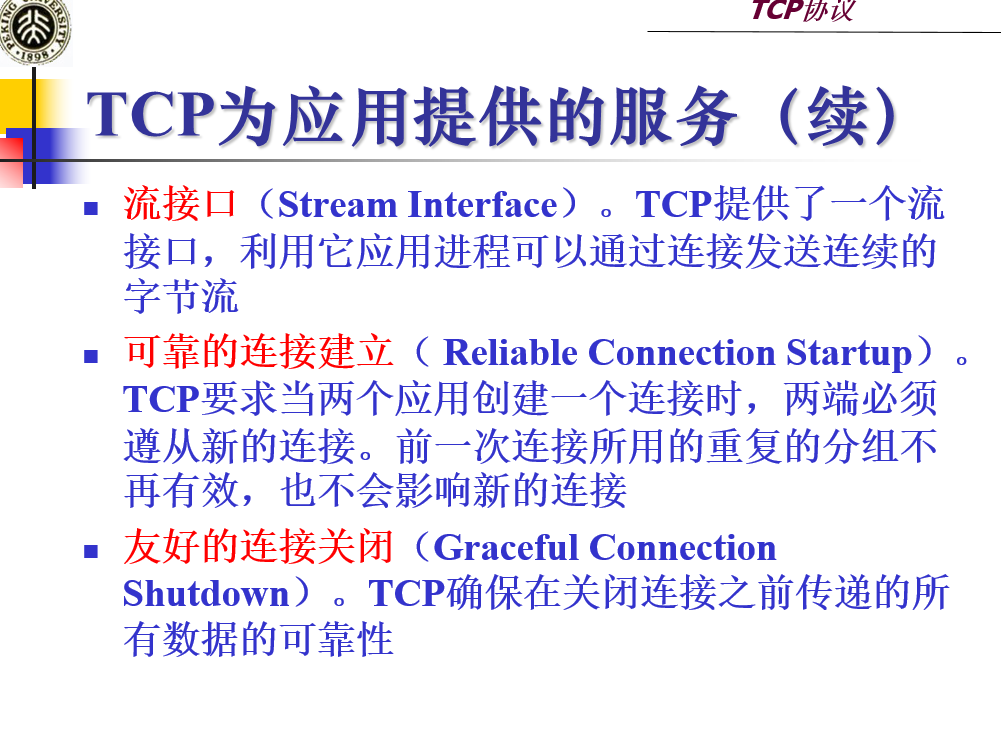


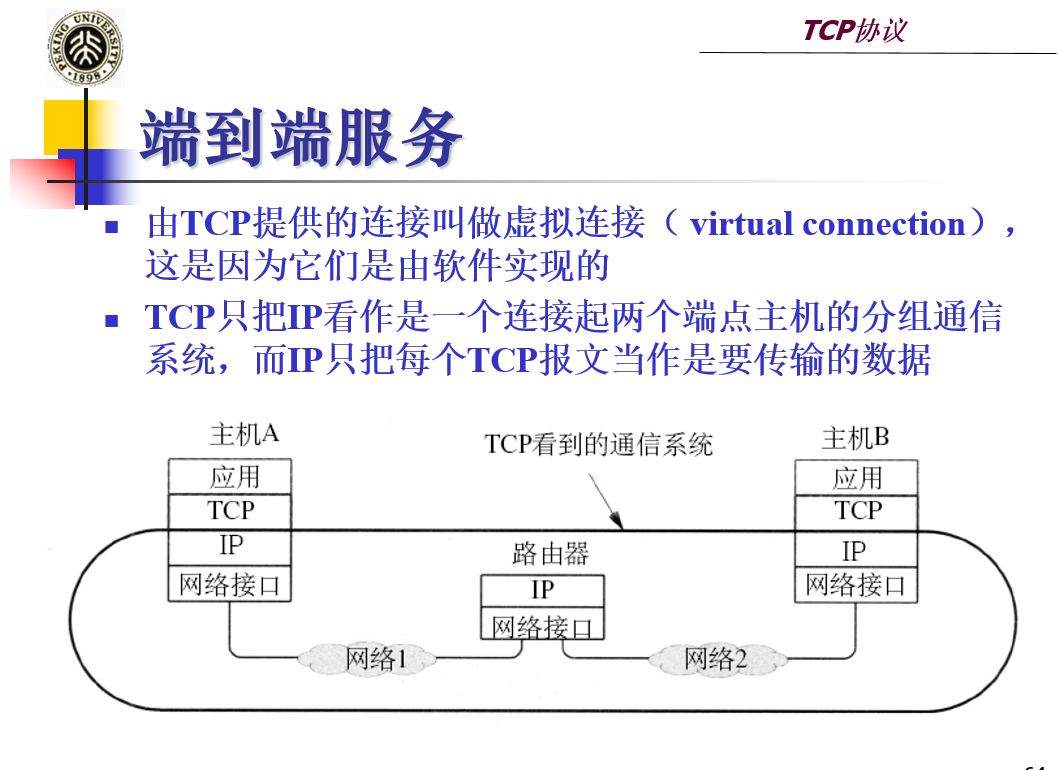


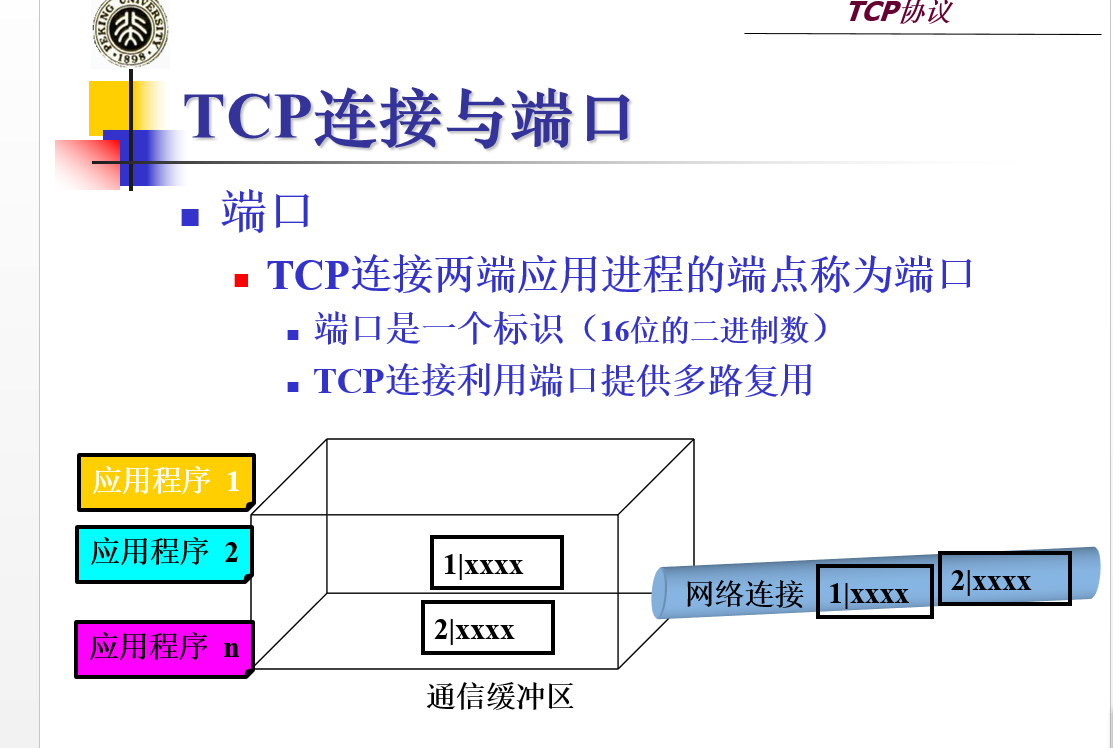


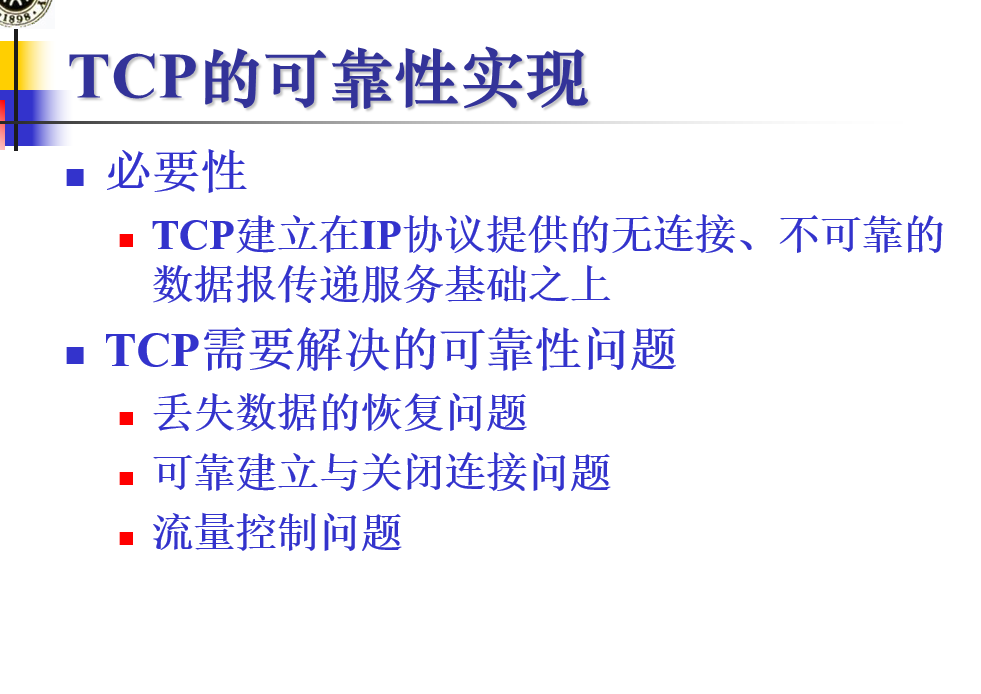
8 TCP协议

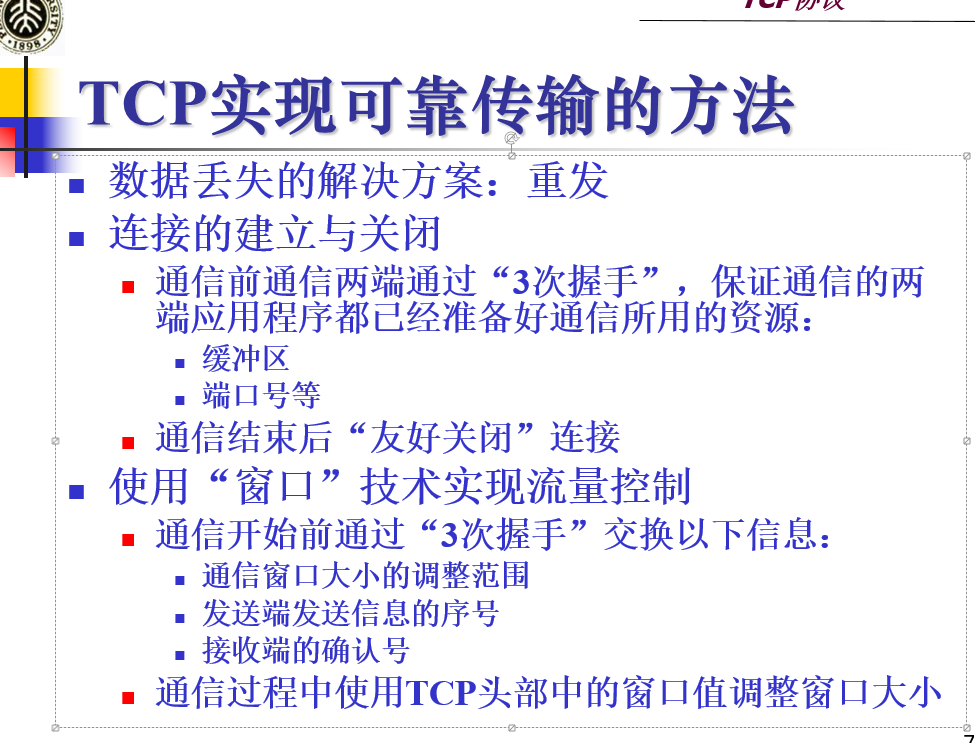


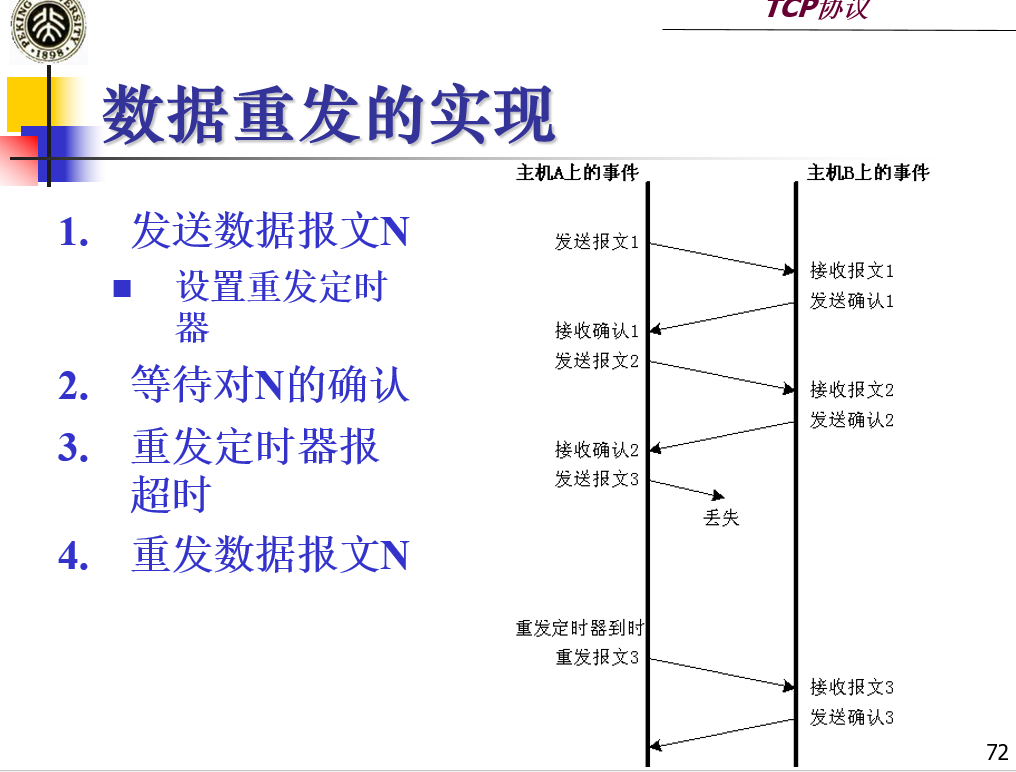




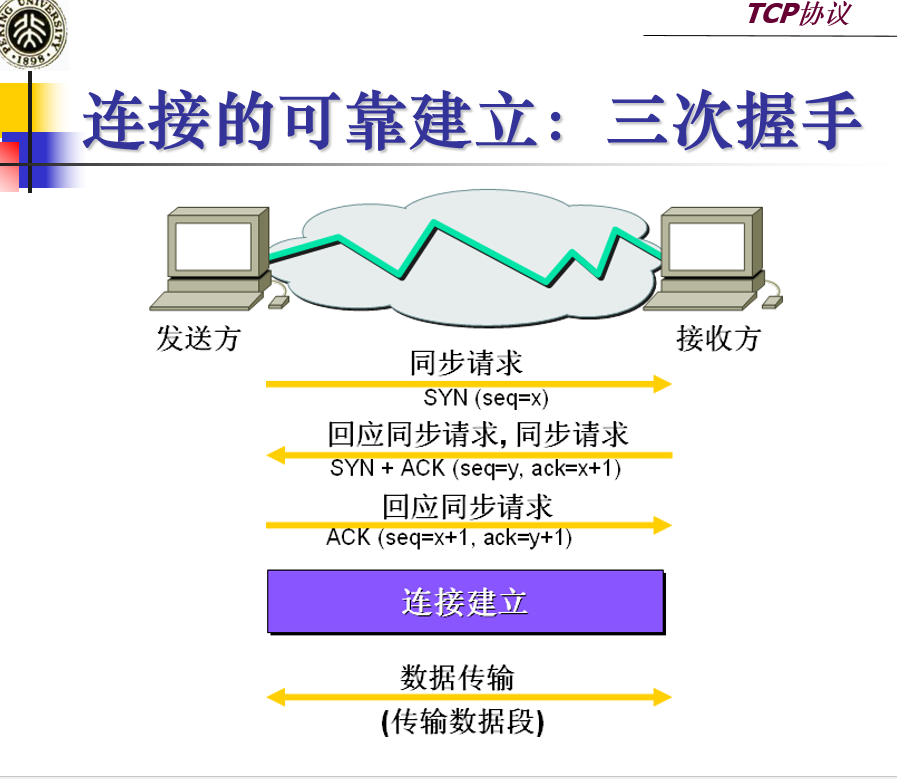


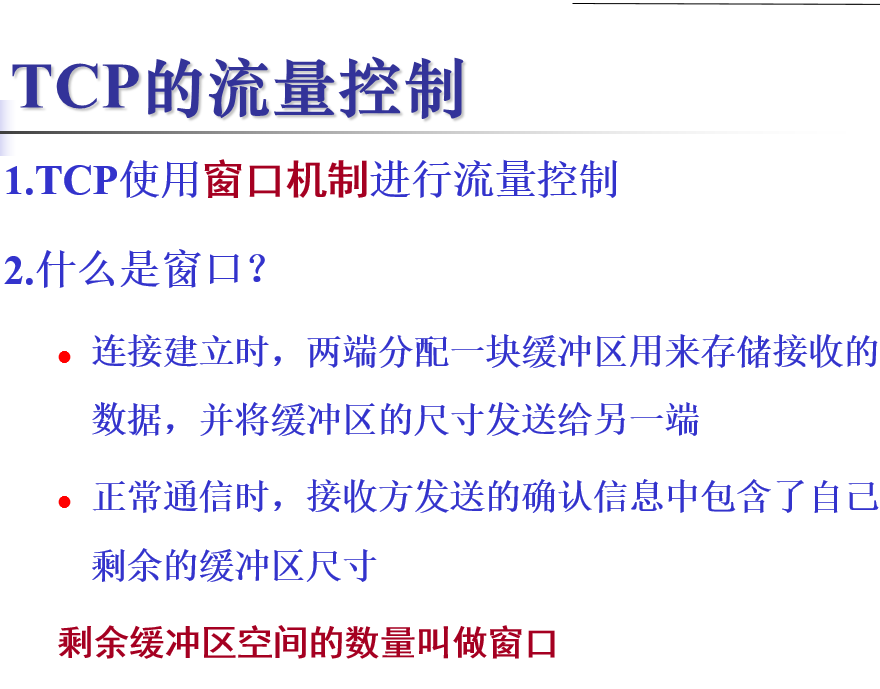






自适应重发





流量控制

* **发送端的主机在确定发送报文段的速率时，既要根据接收端的接收能力，又要从全局考虑不要使网络发生拥塞。因此，对于每一个TCP连接，需要有以下两个状态变量：**
  + **接收端窗口rwnd（receive window）这是接收端根据其目前的接收缓存大小所许诺的最新的窗口值（通知窗口），是来自接收端的流量控制**
  + **拥塞窗口cwnd（congestion window ）这是发送端根据自己估计的网络拥塞程度而设置的窗口值，是来自发送端的流量控制**

第七章

1 网络地址转换 NAT

NAT机制允许一个站点内的多台计算机通过单一的IP地址去使用因特网。NAT：内外有别

为了避免地址冲突，NAT为每台计算机分配一个本地唯一的地址。当对外交换信息时，则把该本地私有地址转换为在整个因特网上能识别的全球IP地址

NAT的目的是要提供虚拟的寻址机制。为此，实现NAT的设备被连接在站点与因特网之间的通路上工作，它要对进入站点和送出到因特网的每个数据报头部域进行重写

只改变IP数据报中的地址域会造成校验和错误。因此，每当改变了源地址或目的地址时，NAT必须重新计算IP校验和

2 NAPT

如果站点中多台计算机要跟同一个目的地进行通信，或者一台计算机的多个应用进程要跟不同的目的地通信，那么前面的基本NAT转换方法就无能为力了

网络地址与端口转换（ NAPT）机制利用IP地址和协议端口号的组合，能够完成这些任务

因为NAPT能理解端口号，所以它能够将每个数据报与TCP连接或某个“一对一”UDP会话关系互相关联起来。也就是说，NAPT针对某一个传输连接而不是某台计算机进行操作

3 静态路由与动态路由

Static routing：静态路由

系统启动时初始化路由表

除非检测到错误，否则路由不变

Dynamic routing：动态路由

系统启动时初始化路由表

同时加载运行路由传播软件（route propagation software）

不同计算机上的路由软件交互作用，从而学习到通往每个站点去的最佳路径，并更新路由表

可能持续改变

为了保证所有路由器能够维持到达每一个可能目的地的有关信息，每个路由器R都要运行采用了路径传播协议的路由软件以查询其他路由器可到达目的地的情况，并通知其他路由器其本身（R）可到达目的地的情况

路由软件利用收到的信息来不断地更新本地的路由表

为了限制路由业务量，因特网采用两级路由层次结构

将因特网中的路由器和网络划分为群组，每个群组内的所有路由器交换信息

每个群组内至少有一个路由器负责收集总结综合信息并发给其他群组

群组的大小和群组内路由协议的采用保持足够灵活

4自治系统

为了掌握路由器的群组概念，我们使用术语自治系统（Autonomous System, AS）

全球因特网中的路由器被划分成群组，每个群组称为自治系统。自治系统内的路由器彼此交换路由信息，然后收集起来再传递给其他自治系统（群组）

自治系统规模的选择可能会涉及到经济、技术或管理等诸多方面。自治系统一般都在单一实体管理控制下

自治系统由因特网号码授权委员会（Internet Assigned Numbers Authority, IANA）分配。一般来说，每个ISP都是单个自治系统；大型的ISP本身还会被划分成多个自治系统

5IGP/EGP

路由选择协议可分为：内部网关协议(Interior Gateway Protocols，IGPs)和外部网关协议(Exterior Gateway Protocols，EGPs)

6 路由软件对每个目的地会找到所有可能的通路，然后选择“最佳”的一条

术语“路由度量”（routing metric）指路由软件选择路径时对所使用通路的测量。典型的因特网路由采用两种度量的组合：

管理成本—需要人工赋值，常用它来控制对通信量合适的通路选择

跳计数—中间网络的个数

7 路由算法

因特网上的路由选择方法尽管多种多样，但它们在本质上都可归属于两种基本的算法：

距离矢量路由算法（Bellman-Ford算法）

链路状态路由算法（Link-status）

距离矢量路由算法是一种基于少量路由信息交换的路由分类算法

路由器中保存着一个到所有可能目的地的路由表，每一项表目里含有到目的地的距离D和到目的地要经过的第一个路由器（下一跳）

每个路由器要向它的邻节点周期性地发送路由更新信息

收到更新信息的路由器将新路由距离D’与原路由比较，如果D’比原来的路由距离D小，则用它替代原来的

上面的讨论中假设网络拓扑是固定不变的，如果是在网络结构变化的情况下（例如其中的一个路由器出现故障），需要对上面的算法做些校正。具体的校正将根据所采用的协议而定

网络中各个节点不必交换通往目的站点的距离，而是维护一张网络拓扑图，在网络拓扑结构发生变化时及时更新拓扑图就行

发现它的邻居节点，并知道其网络地址

测量到其各邻居节点的延迟或开销

组装一个分组，包含它刚刚知道的所有信息

将这个分组发送给所有其他路由器

使用Dijkstra算法计算到每个其他路由器的最短路径

实际上，运行链路状态算法并非一定要采用Dijkstra算法，只要能找出相同的最短路径就行

8路由信息协议（RIP，The Routing Information Protocol ）

路由信息协议（RIP，The Routing Information Protocol ）是一种内部网关协议（IGP）。它采用距离矢量算法传播路由信息。运行RIP的路由器对外通告由它能够到达的目的地及距离，相邻的路由器接收被通告的信息，并用它来更新路由表

按跳数计量距离，源和目标之间的每个网络计为一跳，直接连接计为一跳（无权值！）

使用UDP进行消息传输（有些怪异？）

使用广播或多播传送

采用距离矢量算法（Distance vector algorithm）

支持默认路由传播，方便安装

主机被动模式：允许主机被动地听取和更新路由表

9开放最短路径优先协议

IETF设计出开放最短路径优先协议（OSPF ，The Open Shortest Path First Protocol ）来满足需要

它是一种内部网关路由协议 （IGP）

提供 CIDR 和 subnet 地址格式支持

提供认证的报文交换，安全性增强

采用链路状态算法SPF，无环路

收敛速度快，能够在最短的时间内将路由变化传递到整个自治系统

最主要问题是开销比较大，每台路由器都要维护整个网络的拓扑结构信息

10边界网关协议 （BGP， Border Gateway Protocol ）

是最流行的外部网关协议

提供自治系统级的路由信息 （EGP）

规定政策性条款。管理员可通过配置来限制BGP向外部发布的路由（有些内部信息不向外部发布！）

使用 TCP通信（179端口），提供可靠传输

给出自治系统到其它每个目的地的路径

是目前的Internet所使用的 EGP，所有ISP都参与路由信息的交换，所以从任意一台计算机到任意目标的数据报均会被正确地路由和转发

Current version is four (BGP-4，RFC4271)

11 网关

网关早期不是一个复杂的概念，就是指进出本网络或网段的关口，基本上就是指路由器

随着网络规模和网络技术的发展，目前网关与路由器的概念已经区分开来

路由器：网络层设备，负责不同网络之间的数据转发以及路由选择

网关：使用不同协议族的传输层或应用层程序之间的数据通信，负责协议的转换，如电子邮件网关等；网关经常与一些负责本网安全的应用功能结合起来，如防火墙、VPN等

路由器和网关可以部署在一起，也可以分开

13 组播

* **组播（multicast）：一个主机向特定的多个接收者发送报文的方法；组播群组的成员是动态的**
  + **在Internet上，多媒体业务诸如：流媒体、视频会议和视频点播等，正在成为信息传送的重要组成部分**
  + **点对点传输的单播方式不能适应这一类业务传输特性：“单点发送，多点接收”**
  + **原因：服务器必须为每一个接收者提供一个相同内容的IP报文拷贝，同时网络上也重复地传输相同内容的报文，占用了大量资源**

14 D类地址

* **主机组地址也称为“组播地址”，或者D类地址**
  + **D类地址：前缀1110**
  + **范围：224.0.0.0-239.255.255.255**
  + **每个D类地址标识一组主机**
  + **向某个D类地址发送数据报，即被所有主机组成员接收**

15因特网群组管理协议IGMP

* **IGMP：用于帮助组播路由器识别加入的组成员**
  + **有两个版本：IGMPv1（RFC1112），IGMPv2 (RFC2326)**
  + **该协议只用在主机与路由器之间的网络上，协议只把计算机（而非进程）定义为群组成员**
  + **组播路由器通过IGMP协议为其每个端口都维护一张主机组成员表，并定期地探询表中的主机组的成员，以确定该主机组是否存活**

16域名系统和DNS

* **直接使用IP地址显然不很方便。域名系统（DNS）提供了计算机域名与对等的IP地址之间的自动映射**
* **每个计算机域名是一个由句点分开的字母数字段组成的一个字符串。域名的定位是有层次的，域名中的段对应于层次体系中的层**

**如: www.cis.pku.edu.cn dais.cs.uiuc.edu**

* **域名中段的数量没有标准，因为每个组织都可以自由地选择如何定义它的层次。事实上，一个组织中的两个工作组也可以有不同的层次体系**
  + **域名系统只规定了最重要段的值，称作DNS的顶层域（TLD，Top-level Domain）**
* **在没有优化的情况下，根服务器的通信量是难以忍受的，因为每次有人提到远程计算机的域名时，根服务器都会收到一个请求**
* **实际上可以优化DNS性能**
  + **局部性原理告诉我们，一台给定的计算机会反复地发出同样的请求—如果一个用户输入了一个远程计算机的域名，那么他以后将再次提及相同的域名**
* **在DNS中主要有两方面的优化：**
  + **复制**

**缓存**

* **DNS数据库中的每一项包括三个元素：域名、记录类型、值。当解析器查找一个域名时，它必须指明所希望的类型，一个DNS服务器只返回那些符合类型的项**
* **DNS中的类型体系提供了很大的方便，因为它允许管理者使用单个名字用于多个目的**
* **DNS请求中指定类型带来的结果会很惊讶—一个域名在一个应用里工作正常，而在另一个应用里无法工作**
  + **例如，可以向一台计算机发电子邮件，而试图用ping或traceroute与其通信，将会导致一条“该计算机不存在”的消息。这种明显的不一致性归因于电子邮件的DNS请求类型与其他应用的请求类型不同**

# 第八章

**1 加密算法**

DES算法

* **使用64位密钥（实际上只有56位，每个字节的最后一位是奇偶校验位）加密一个64位明文块**
* **有三个不同阶段：**
  + **把块中64比特完全打乱，以不同次序排列（称为初始变换）**
  + **对结果数据和密钥进行相同的操作循环16次（详见后面阐述）**
  + **将逆初始变换应用于结果**

RSA算法

* **选择两个大素数*p*和*q*，通常要求每个均大于10100**
* **计算*r*＝*p* · *q*和**φ**(r)＝(*p*－1)(*q*－1)**
* **选择一与**φ**(r)互质的数，令其为PK**
* **找到一个SK满足*SK* · *PK*＝1 mod** φ**(r)**

**选好这些参数后，将明文划分成块，使得每个明文报文*P* ∈[0, r-1]**

**加密*P*时，计算密文*C*＝*Ppk*(mod *r*)**

**解密*C*时，计算明文*P*＝*Csk*(mod *r*)**

**由于模运算的对称性，可以证明在确定范围内，加密和解密函数是互逆的**

**为实现加密，需要 (PK, r)，而解密需要(SK, r)**

**报文摘要5MD5**

* **MD5和DES算法相似，都没有正式的数学基础，而是依靠算法的复杂性产生随机的输出来满足要求**
* **摘要计算过程**
  + **把摘要的值初始化为一个常量**
  + **将这个值与报文（message）的前512个比特结合起来生成新的摘要值**
  + **使用同样的变换将这个新值与下一个512比特结合，依次类推，直到生成最终的摘要值**
  + **注：需要将message填充为512 比特的整数倍**

2 安全性内容

* **机密性Confidentiality—防止未授权的数据访问**
* **完整性Integrity—防止数据被改变**
* **真实性Authenticity —认证技术**
  + **报文认证：验证报文的真实性（内容、时间、发送方等）**
  + **身份认证：验证真实身份和所声称身份相符的过程**
* **可用性Availability—防止服务受到破坏（DoS等）**
* **私密性Privacy—发送者保持匿名身份的能力**
* **……**

3完整性机制

* **CRC等不足以保证数据的完整性**
  + **首先，如果出现校验值和报文数据同时破坏，且改变后的校验值和报文又正巧匹配的情况，系统就无法发现错误**
  + **其次，攻击者可能会改变数据而使校验仍然正确**
* **除了报文摘要方案，还可以使用报文鉴别码（message authentication code, MAC）对传输数据进行编码**
  + **典型的编码方案是采用密码散列（cryptographic hashing）机制，如使用只有发送方和接收方才知道的密钥（secret key）。这样，在发送方对信息编码时，密码散列函数像对数据编码一样使用密钥打乱信息中的字节的排列位置。只有接收方才能够恢复这些信息，而没有密钥的攻击者不能解码，也就不能引入错误**

4 公钥私钥

* **很多加密方法中，密钥必须是保密的。而公开密钥加密法给每个用户分配两把密钥：一个称私有密钥，是保密的；一个称公开密钥，是众所周知的**
* **假设M表示一条报文，pub\_u1表示用户1的公开密钥，prv\_u1表示用户1的私有密钥，那么有:**

**M=decrypt(pub\_u1, encrypt(prv\_u1,M))**

**以及**

**M=decrypt(prv\_u1, encrypt(pub\_u1,M))**

* **特点：使用公开密钥（私有密钥）加密的报文除了使用相应的私有密钥（公开密钥）外很难解密**
* **公开密钥加密法还可以用于验证报文发送方，这种技术称作数字签名（ digital signature）**
  + **签名时，使用私有密钥对报文加密**
  + **验证时，使用相应的公开密钥对加密报文进行解密**
* **对一个报文加密两次就可以同时保证报文的可验证性和保密性**
  + **先用发送方的私有密钥加密（可验证性），再用接收方的公开密钥对已加密报文进行再加密（保密性）**

**X=encrypt(pub\_u2, encrypt(prv\_u1, M))**

* + **报文接收方用它的私有密钥解除外层加密，然后用报文发送方的公开密钥解除内层加密**

**M=decrypt(pub\_u1, decrypt(prv\_u2, X))**

5证书

* **证书的思想允许建立一条“信任链”**
  + **如果X证明某个公开密钥属于Y，而Y继续证明另一公开密钥属于Z，那么，尽管X与Z从未相遇，仍然存在一条从X到Z的证书链**
* **证书的主要标准之一称为X.509。这个标准允许留下许多开放的细节，但规定了证书的基本结构**
  + **要证明的实体的名字**
  + **实体的公开密钥**
  + **认证机构的名字**

**数字签名**

6 TLS（Transport Layer Security）

* **TLS分成两部分：**
  + **握手协议，用来协商通信参数。如果必要，可以负责参与者之间的证书交换**
  + **记录协议，用于实际数据的传输。其从应用层下传消息的格式和步骤如下：**
    - **为下面的处理将消息分段或合并成适当大小的块**
    - **可选择地压缩**
    - **使用诸如MD5的散列法保护完整性**
    - **加密**

**传输到较低层（如TCP）**

**7 HTTPs**

* **HTTPS（安全的 HTTP）并没有对HTTP协议做太多的改动，它只是把数据转发到TLS层而不是TCP层，它接收数据也是从TLS层而不是TCP层**
* **为方便起见，指定缺省TCP端口443为“HTTPS”。就是说，如果你试图连接到一个服务器的TCP端口443，那么你可能会发现正与TLS协议会话，它会在鉴别和解密后将数据传给HTTP**

1. **PGP（Pretty Good Privacy）**
   * **由Philip R. Zimmermann设计，对电子邮件提供保密性和完整性保护，并对电子邮件进行认证**
   * **PGP加密由一系列散列、数据压缩、对称密钥加密算法，以及公钥加密算法组合而成**

* **机密性：PGP可以用来发送机密消息，它通过对称的一组“密钥-公钥”组合来实现**
* **数字签名：PGP支持消息认证和完整性检测**
  + **完整性检测被用来检查消息在传输过程中是否被更改（即验证消息完整性）**
  + **消息认证则被用来决定消息是否确由某特定的人或实体发出（即数字签名验证）**
* **商业应用：PGP一般在企业资源规划（即ERP）软件连接到银行系统时使用，防止信息在传输过程中被删改或盗取**

9 SSH

* **SSH提供一种远程登录服务。SSH最常用的功能是提供强有力的客户/服务器鉴别—SSH的客户端程序运行在用户的台式机上，而SSH的服务器端运行在某台用户想登录的远程主机上—但SSH也支持消息完整性和保密性**
* **SSH version2由以下三个协议构成：**
  + **SSH-TRANS：一个传输层协议**
  + **SSH-AUTH：一个鉴别协议**
  + **SSH-CONN：一个连接协议**
* **SSH被拓展支持其他不安全的基于TCP的应用程序**
  + **如XWindows和IMAP邮件阅读程序。其思想是，在一条安全的“SSH隧道”上运行这些程序。这种能力被称为端口转发（port forwarding），其使用SSH-CONN协议**

10 防火墙

* **防火墙是指设置在不同网络或网络安全域（公共网和企业内部网）之间的一系列部件的组合**
* **它是不同网络（安全域）之间的唯一出入口，能根据机构或企业的安全政策，控制（允许 、拒绝 、 监测）出入网络的信息流，且本身具有很高的抗攻击能力，它是提供信息安全服务、实现网络和信息安全的基础设施**
* **防火墙是处理互不信任的单位之间建立网络连接时最重要的安全工具，能以较低的成本提供安全保障**

11 VPN

* **通常VPN用软件来实现：**
  + **VPN按照类似于传统的分组过滤器那样工作，将路由器配置成只允许从机构的其他站点路由器发过来的那些分组通过，而且只允许从本站点路由器发给机构其他站点路由器的分组通过**
  + **分组数据在被传输出去之前，必须由VPN软件对它进行加密处理，这样就可以保证所有的通信业务具有保密性**
* **如果数据报头部不加密，那么外界用户就会知道机构内部的源地址和目的地址；如果加了密，那么因特网路由器就不能在进行转发的时候去解释数据报头部域的内容**
* **为了使机构各站点之间通过因特网传输数据报的时候能保持信息的完全隐蔽性，VPN软件一般采用IP-in-IP隧道机制。亦即发送方VPN软件对全部数据报进行加密，然后把它放置在另一个数据报中进行传输。当该数据报到达机构目的站点路由器后，该路由器的VPN软件从载荷中提取出原始数据报并进行解密，然后把它发给相应的计算机**

IP-in-TCP隧道技术

* **工作原理**
  + **双方先建立TCP连接**
  + **当要发送数据报时，先加密整个数据报，再加上一个小头部用于标记数据报之间的分界点，然后通过TCP连接发送出去**
  + **接收端的VPN软件先获得头部，再对加密的数据报进行解密，即可得到原始数据报**
* **利与弊**
  + **优点：确保数据报的可靠递交**
  + **缺点：如果有TCP报文段丢失或延迟，就无法从后继段继续递交数据—由此，比如第一个数据报成功递交之前，整个要传送的队列都必须等待**

# 第九章

1 吞吐率和延迟

吞吐率（Throughput）

单位时间内所能传输的数据量，是对网络传输能力的度量

但通常被称为网络“带宽”或“速度”

一个类比

“吞吐率”描述的是每秒钟有多少车能进入一条路

“传输延迟”决定一辆车用多长时间从一个地方到达另外一个地方

容量（Capacity）

通常被表示为最大吞吐率

延迟与吞吐率

理论上是独立的

现实中是相关的

D0 表示网络空闲时的延迟，U (在0和1之间)表示当前网络的利用率， D表示有效延迟。以下公式是它们之间关系的简单展示：

这表示，延迟与吞吐率并不独立

随着网络业务量的增加，延迟将随之增加

当吞吐率接近容量的100%时，网络将会经受非常严重的延迟

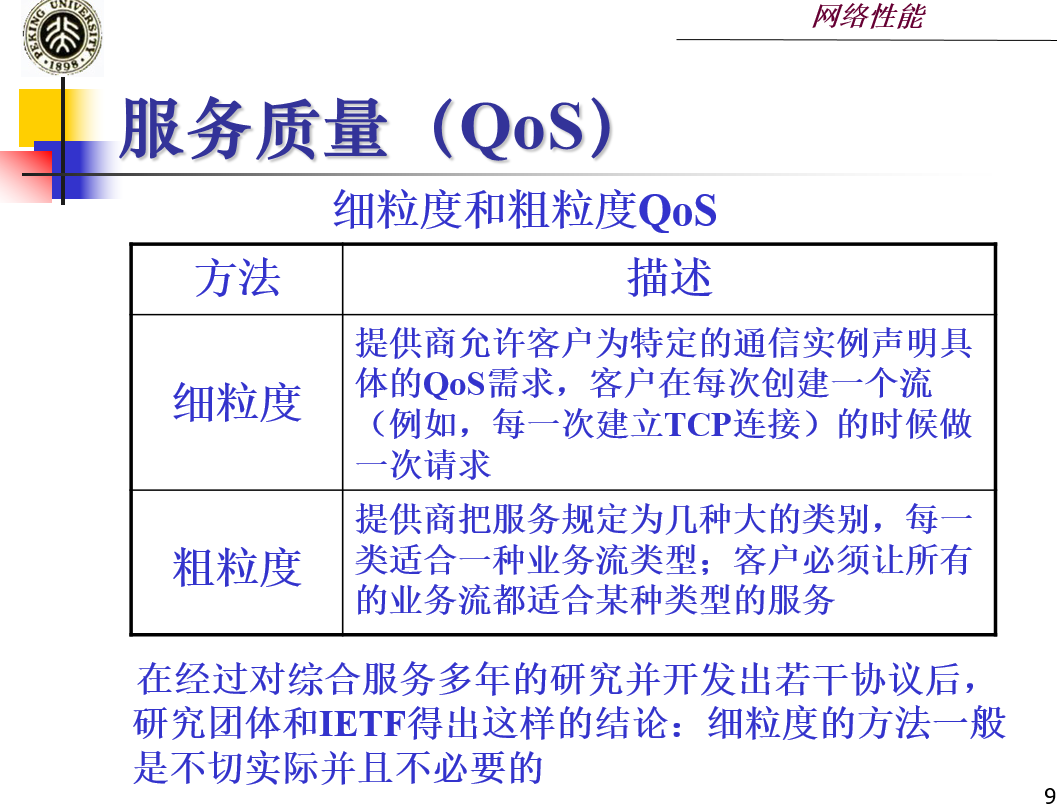
2 抖动

抖动是对延迟变化量的度量，它是数据网络中越来越重要的性能指标

处理抖动的两种方法

设计一个无抖动的等时网络，如传统的电话系统

采用能补偿抖动的协议。在因特网上传播语音和视频，一般采取实时协议（Real-Time Protocols）等来补偿抖动，这比构建等时网络的费用要低得多。当然协议不能补偿太过分的抖动



3**互联网的脆弱性—根源，各种攻击方法**

* **互联网在最初设计时并没有考虑安全问题**
  + **所以，在互联网上的计算机要保证信息的可用性、完整性和保密性就比较困难**
* **网络上的计算机总要提供某些服务才能够与其它计算机相互通信**
  + **但复杂的软件系统不可能没有瑕疵，导致计算机系统和计算机网络的脆弱性不可能完全消除**
* **脆弱性评估的目的**
  + **不是完全消除脆弱性，而是提供出一个安全解决方案**
  + **帮助系统规划者和管理者在“提供服务”和“保证安全”之间找到一个合理的平衡**
* **IP协议的next-hop转发机制不检查源地址**
  + **可以伪造源地址进行攻击**
  + **拒绝服务攻击（DoS）**
* **DNS攻击**
  + **把互联网变成大局域网**
* **对自治系统网关/主路由器的攻击**
  + **服务只能局限于自治系统内部**
* **因特网主干网受到严重破坏**
  + **整个因特网基本瘫痪**

IP路由机制

* **数据报方式**
* **根据最终目的地选择合适的下一站**
  + **理论上可保证整个路径的最优性**
* **不检查源地址**
  + **建立检查机制会造成转发代价急剧增大**
    - **每个路由器都要检查每一个IP数据报**
    - **这将导致连锁反应，在实际中基本不可行**
* **路径追溯很困难**
  + **转发路由器没有“邮戳”，想追溯上一站很困难**
  + **实际操作中，追踪一次袭击要涉及多个组织**

DoS，denial-of-service

向目标服务器发送大量虚假请求，服务器由于不断应付这些无用信息而精疲力尽，合法的用户却因此无法享受到相应服务

DDoS：分布式拒绝服务攻击

首先利用木马程序等控制一些高带宽服务器，然后在这些服务器上安装攻击软件，集数十台、数百台甚至上千台机器对目标服务器发动攻击——即使是高性能的商业网站，也难以逃脱瘫痪的命运

理论上，分清是从很多信源来的合法的过重载荷还是DDoS攻击几乎是不可能的  有效攻击手

4 客户|服务器模式

* **一个应用进程被动地等待另一个应用进程来启动通信过程的这种模式，在分布式计算中普遍采用，叫“客户/服务器交互模式（client-server paradigm of interaction）”**
* **也就是说，网络应用使用一种称为客户/服务器模式的通信方式。服务器应用进程被动地等待通信，而客户应用进程主动地启动通信**

# 第十章

1远程登录与文件传输服务

* **远程登录，即用户由本地机通过网络登录到远端另一台机器的帐号上，作为远程主机的终端用户使用它的资源**
  + **本地机：发起远程登录请求的计算机**
  + **远程机：接受请求并被登录的计算机**
* **TCP/IP定义了两个基本的远程登录协议：Telnet和Rlogin**
* **Telnet有三个步骤**
  + **登录**
  + **将本地输入传输到远端**
  + **将远端输出传输到本地**
* **Telnet提供三种服务**
  + **虚拟终端：用户终端和远程终端之间的标准终端接口**
  + **客户机和服务器协商选项的机制**
  + **对等处理连接的两端**
* **文件传输是指登录到远程机上将其文件传输过来（下载）在本地机上生成一个文件副本，或反之（上载）**
* **文件传输是大多数计算机网络提供的文件访问服务，在TCP/IP中支持文件传输的一个重要协议就是FTP**
  + **FTP基于C/S模式，但建立双重连接**
  + **控制连接——用于维持FTP客户与服务器的会话（使用端口21）**
  + **数据连接——用于维持文件的数据传输，是控制连接派生出来的（使用端口20）**

2 电子邮件

* **邮件传送服务器使用简单邮件传输协议SMTP（Simple Mail Transfer Protocol）。SMTP定义了邮件如何在各个邮件传输系统中，通过发方和收方之间的TCP连接进行传输**
  + **SMTP要求先在客户和服务器之间建立一个会话，然后发方可以发送若干邮件；发送完后中断连接，退出SMTP会话**
  + **SMTP允许发送方询问一个给定的邮箱在服务器所在的计算机上是否存在**
  + **SMTP要求可靠的传递—发方必须保存一个信息的副本直到收方将一个副本放至不易丢失的存储器**
* **许多邮件系统包含一个邮件分发器（mail exploder）或邮件转发器（mail forwarder），这是一个能转发信息副本的程序**
  + **分发器使用数据库来决定如何处理信息。通常称为邮件列表（ mailing list）的数据库中，每一项是一组电子邮件地址。此外，数据库中的每一项本身也被赋予一个电子邮件地址（一对多的一个对应）**
  + **当电子邮件信息到达时，邮件分发器检查目标地址。如果目标地址列表在数据库中出现，分发器就将信息转发给表中的每个地址**
* **虽然邮件分发器可以在任意计算机上进行操作，但将电子邮件信息转发给一个很大的邮件列表中的所有地址，仍需要很长的处理时间。因此，许多机构不允许在一般的计算机上存在分发器或很大的邮件列表**
* **取而代之的是，机构选取一小部分计算机专门运行分发器和转发邮件。这样的专门用于处理电子邮件的计算机程序通常称为电子邮件网关（ e-mail gateway）**
* **在邮件网关内部，分发器程序接收发给邮件列表的信息，并将副本转发给列表中的每个接收者**
* **一个单位可使用邮件网关来统一雇员的电子邮件地址**
* **邮局协议POP （Post Office Protocol）定义了将用户信件从邮件服务器下载到本地客户机的相应规程**
* **Internet消息访问协议（Internet Message Access Protocol，IMAP）是POP的增强版本**
  + **对三种远程邮箱访问（离线、在线和断接）提供了更好的支持**
  + **提供从服务器有选择地收取全部或部分消息的功能，对基于服务器的消息进行处理，并能提供公用电子信箱**

3 IP电话

* **H.323协议是由国际电信联盟电信标准化部门（ITU-T）提出、基于电信网信令和协议制定的IP多媒体标准，它并不是为 IP 电话专门提出的**
* **H.323不是单个协议，而是一组协议**
* **在H.323系统中，终端主要为媒体通信提供数据，功能比较简单，而对呼叫的控制、媒体传输控制等功能的实现则主要由gatekeeper来完成**
* **H.323 协议是一组较为完备的协议，它体现了一种集中式、层次式的控制模式，这种模式与电信网的管理方式是适配的，尤其适用于从终端到终端的 IP 电话网或视频会议网的构建**
* **使用H.323 协议时，各个不同厂商的多媒体产品和应用可以进行互相操作，用户不必考虑兼容性**
* **理论和实践都表明，H.323 有能力做成任意规模的 IP 电话系统和视频会议系统**
* **IETF定义了会话初始化协议SIP**
  + **在应用层上运作**
  + **包含信令的所有方面，包括：对象的定位，通知和建立（即振铃），可用性确认（即对象是否接受呼叫），终结**
  + **提供诸如呼叫转移之类的服务**
  + **会议业务要依赖组播**
  + **允许通话双方协商*能力*并选择所用的*媒体*和*参数***
* **来源**
  + **H.323是ITU提出的，被“借用”为IP电话协议标准；实际上对 IP 多媒体应用（如IP电话或视频会议）来说，不仅要用到H.323 协议，还用了一系列协议，其中有H.225、H.245、H.235、H.450、H.341等，而H.323 协议可以看作是“总体技术要求”**
  + **SIP是IETF提出的，最初的目标是想以现有的 Internet 为基础来构建 IP 电话业务网**
* **系统结构**
  + **在H.323系统中，终端主要为媒体通信提供数据，功能比较简单—体现了一种集中式、层次式的控制模式**
  + **SIP将网络设备的复杂性推向了网络终端设备，因此更适于构建智能型的用户终端—体现的是一种分布式的控制模式**
* **应用领域**
  + **H.323协议的开发目的，是在分组交换网络上，为用户提供取代普通电话的VoIP业务和视频通信系统；H.323 更适合于构建电信级大网，国际上几乎所有的商业性 IP 电话网或视频会议网都是以 H.323 为基础的**
  + **SIP的开发目的是用来提供跨越因特网的高级电话业务；SIP相对简单，目前有许多运营商正在利用 SIP 构建试验网，但若想利用 SIP 构建电信级大网，必须对它进行补充、完善**
* **未来发展**
  + **大多数电信运营商已将 H.323 作为建立新一代视频会议系统的首选，他们正在将传统的基于电路的 H.320 视频会议应用转移到基于 IP 的 H.323 系统中来；H.323 已经成为VoIP 和多媒体通信事实上的主导协议**
  + **在下一代网络中， IP 产品将得到大规模应用和集成，而基于纯 IP 的 SIP结构简单，具有可扩充性和可扩展性， 还提供良好的 QoS（服务质量）支持；SIP有希望成为下一代网络中VoIP 的重要解决方案**

4 多媒体技术

* **狭义的流媒体技术是相对于传统的下载－回放（Download-Playback）方式而言的一种媒体格式，它能从Internet上获取音频和视频等连续的多媒体流，客户端可以边接收边播放，使时延大大减少，而不用等到完全下载完毕再播放**
* **广义的流媒体技术，是指使音频和视频形成稳定和连续的传输流和回放流的一系列技术、方法、协议和软件的总称，我们习惯上称之为流媒体系统**

**实时传输协议RTP**

* **RTP为一些应用提供公共的端到端功能。它规定了音频和视频数据、顺序号和时间戳等信息如何封装在传输层（UDP/TCP）分组中**
* **RTP通常使用UDP来传送数据，但它也可以在TCP或ATM等其他协议之上工作**
* **RTP本身不提供任何机制来确保数据的按时发送或保证服务的质量，甚至不保证分组的顺序递交。它使用顺序号让接收方能检测丢失和乱序的分组**

**实时传输控制协议RTCP**

* **RTCP是RTP的孪生协议，主要功能是定期发送与一个特定的数据流相关的控制流。这个控制流有四个主要功能：**
  + **反馈应用程序和网络的性能**
  + **提供关联和同步来自同一发送方的不同媒体流的一种方法**
  + **在RTP会话期间，各参与者周期性地传送RTCP包，包中含有已发送的数据包的数量、丢失的数据包的数量等统计资料，因此，服务器可以利用这些信息动态地改变传输速率，甚至改变有效载荷类型**
  + **传送发送方标识符到用户界面上显示的一种方法**
* **RTP和RTCP配合使用，能以有效的反馈和最小的开销使传输效率最佳化，特别适合传送网上的实时数据**

**资源预订协议RSVP**

* **资源预订协议RSVP（Resource Reservation Protocol）可预留一部分网络资源（即带宽），能在一定程度上为流媒体的传输提供QoS**
* **RSVP实际运行在IP之上；RSVP的组成元素有发送者、接收者和主机/路由器**
  + **发送者负责让接收者知道数据将要发送，以及需要什么样的QoS**
  + **接收者负责发送一个通知到主机或路由器，这样它们就可以准备接收即将到来的数据**
  + **主机或路由器负责预留出所有合适的资源（路由器会从接收端到发送端连锁通知）**
* **RSVP协议的两个重要概念是流和预订**
  + **流是从发送者到一个或多个接收者的连接特征，通过IP数据报中“流标记”来认证**
  + **发送一个流前，发送者传输一个路径信息到目的接收方，这个信息包括源IP地址、目的IP地址和一个流规格**
  + **流规格由流的速率和延迟组成，这是流的QoS需要的**
  + **接收者记录自己的需要，并通知主机或路由器来实现预订**
* **RSVP支持三种传输类型：尽力传输（best-effort）、速率敏感（rate-sensitive）与延迟敏感（delay-sensitive）**
  + **尽力传输为传统IP传输**
  + **速率敏感传输放弃及时性，而确保传输速率**
  + **延迟敏感传输要求传输及时**
* **RSVP认为它不应该损害我们在无连接网络中已经获得的健壮性，为此它试图在路由器中使用soft state的概念来维持健壮性**
  + **资源预留是“软”的，这意味着需要由接收者周期地更新**
* **RSVP使用面向接收者模式（receiver-oriented），由接收者记录自己的需要；支持多点播送流，使它像单点播送流一样有效**
* **Soft state和receiver-oriented会带来许多好的特性**
  + **例如，每个接收者定期发送刷新消息以保持相称的soft state，所以很容易发送一个请求新级别资源的新预订**

5 组播

* **组播（Multicast）也叫多播，它不同于广播，其传送方式是把相同的数据送到一组选择的目的地站点，而广播是把相同数据传送到其它所有站点**
* **组播技术可以广泛应用于因特网电台、因特网电视、视频会议、股市报价、分布式多媒体游戏等多媒体网络应用中**
* **组播信息传递用的是组（group）地址，组地址是网络上与多个站点相关的一种多目的地址**
* **IP组播地址（也称为组地址）在224.0.0.0到239.255.255.255的D类地址范围内，这是通过将前四个高序位设置为1110来定义的。在网络前缀或无类别域间路由（Classless Inter-Domain Routing，CIDR）表示法中，IP组播地址缩写为224.0.0.0/4**
* **从224.0.0.0到224.0.0.255 (224.0.0.0/24)范围的组播地址保留用于本地子网**
  + **224.0.0.1 - 该子网中所有具有组播功能的主机**
  + **224.0.0.2 - 该子网中所有的组播路由器**
* **几乎所有的LAN采用的都是广播式信道，所以在LAN上可借助于广播机制来实现组播**
* **在LAN上，网络层定义的组播工作方式最终还要借助于MAC子层的组播机制来实现**
* **具体工作过程为：发送方将组播数据帧广播到LAN共享信道上，处在本LAN中的该组播组的成员主机监听到之后将其接收，其它主机则将其丢弃**
* **MAC层也定义了单播MAC地址和组播MAC地址，以使网卡对监听到的数据帧区别对待**
* **组播IP地址要映射为组播MAC地址**
* **单播侦听模式：网卡底层硬件只接收目的MAC地址与本网卡物理地址匹配的数据帧和目的MAC地址为FF-FF-FF-FF-FF-FF（广播地址）的数据帧**
* **单播侦听扩展模式：在单播侦听模式的基础上，网卡底层硬件还接收目的MAC地址与硬件MAC地址过滤器中某个值相匹配的数据帧。硬件MAC地址过滤器中的值可以通过软件配置**
* **混合模式：网卡底层硬件接收所有的数据帧**
* **组播混合模式：网卡底层硬件接收单播/组播标志位为1的所有的数据帧**

**IGMP协议**

* **互联网群组管理协议IGMP工作在主机和直接与其相连的路由器之间。路由器用IGMP协议收集子网内主机的组成员信息**

6 网络管理

* **网络管理的任务主要有：**
  + **配置管理：网络管理的最基本功能，负责监测和控制网络的配置状态**
  + **性能管理：保证有效运营网络和提供约定的服务质量，在保证各种业务的服务质量（QoS）的同时，尽量提高网络资源利用率**
  + **故障管理：迅速发现、定位和排除网络故障，动态维护网络的有效性**
  + **安全管理：提供信息的保密、认证和完整性保护机制，使网络中的服务、数据和系统免受侵扰和破坏**
  + **记账管理：正确地计算和接收用户使用网络服务的费用，进行网络资源的统计和网络成本效益的计算**
* **网络管理并没有被定义为较低层协议的一个必需部分。实际上，一般使用应用层协议进行网络管理。原因如下：**
  + **在由于硬件设备故障而通信困难的情况下，管理员仍然可以跟维持工作的设备进行通信，根据通信成功还是失败来帮助定位故障源**
  + **使用传统的传输协议意味着来自管理员的分组与正常通信业务是在同样的条件下传输。这样，如果网络延迟太大，管理员就可以立即发现问题**
* **管理互联网的标准协议称为简单网络管理协议（ Simple Network Management Protocol，SNMP），目前的版本是第3版，称为SNMPv3**
* **SNMP定义了管理员（manager，在管理人员的计算机上运行的客户程序）传输给代理（agent，网络设备上的应用服务程序）的请求格式以及代理响应的格式等。另外， SNMP还定义了每种可能的请求和响应的确切含义**
* **协议没有定义一个很大的命令集，而是采用存取模式（ fetch-store paradigm）。该模式有两种基本操作：取操作fetch用于取出设备中的数据，存操作store用于给设备赋值**

# 第11章

1 Web页面与浏览—HTTP的变化

* **HTTP是浏览器用于和Web服务器交互的主要传输协议，可被表征如下：**
  + **使用文本控制报文**
  + **传送二进制数据文件**
  + **可以下载或上传数据**
  + **一体化高速缓存**
* **HTTP协议在改变时要兼容以前版本。在使用HTTP协议时，浏览器要发送版本信息，以便使服务器选择使用双方都能理解的最高版本协议**
* **四种主要的HTTP请求类型**

**GET 请求一个文档。服务器响应：发送状态信息，紧接着发送该**

**文档的一个副本**

**HEAD 请求状态信息。服务器响应：发送状态信息，但不发送文档**

**副本**

**POST 发送数据给服务器。服务器将该数据添加到指定的项上**

**例如，将报文添加到一个列表中**

**PUT 发送数据给服务器。服务器用该数据完全替代指定的项，即**

**覆盖或重写原来的数据**

* **由于用户趋向重复地访问相同的网站，因此高速缓存能为Web访问提供优化处理**
  + **浏览器通过在用户硬盘缓存中保存网站图像的副本，以及利用被缓存的副本，就能够明显减少下载的次数**
* **如何应对服务器上的文档更新呢？**
  + **浏览器从服务器获取一个文档时，其头部的“最后更新”（Last-Modified）会指明该文档的最后变更时间**
  + **在使用本地缓存的文档前，浏览器向服务器发出一个HEAD请求，然后比较服务器最新副本与本地副本的“最后更新”时间**
  + **如果发现缓存文档已过时，则下载最新版本**
* **HTTP允许Web站点发送不可缓存的头部，可规定客户端不可缓存某个项；浏览器一般也不缓存小长度内容**
* **HTTP是用来获取网页以及与网页相关的其他信息项（如图像/音频/视频）的标准应用协议**
* **HTTP使用端口80。当浏览器要发送HTTP请求消息时，它建立到URL中指定服务器80端口的新TCP连接，然后通过该连接发送请求消息**
* **在HTTP的早期版本中，浏览器正确接收到相关的响应消息之后，服务器就释放该连接。这种形式的TCP连接称为非持久（nonpersistent）的连接**
* **HTTP的早期版本定义在RFC 1945中**
* **每个请求/响应消息的传输都使用新TCP连接有很多缺点**
  + **当访问包含多个实体（如图像）的网页时，在建立新连接传输每个实体时，会产生一个时间延迟**
  + **每次新传输启动过程缓慢，可能会导致额外延迟**
* **为了减少延迟，当在网页中指定多个实体时，多个进程建立多个TCP连接，使每个实体能并发传输**
  + **这样能减少Web访问的整体时间延迟**
  + **但多个连接的使用会导致在客户端和服务器端的额外开销；这种开销对于繁忙的服务器来说影响很大**
* **HTTPv1.1（定义在RFC 2068中）以上的版本中，除非特殊说明，服务器端在Web会话期间保留初始的TCP连接**
* **这种TCP连接称为持久的（persistent）**
  + **一旦建立连接，浏览器就能发送多个请求而无需等待收到响应**
  + **通常当连接上不再有传输时，此次会话将由计时器超时结束**

**不同版本的HTTP可以一起使用**

* **目前已提出几种扩充的和替代的超文本传输协议，以便增强或替换HTTP**
  + **HTTPS协议与TLS打交道，提供安全的HTTP传输**
  + **W3C曾提出HTTP-NG作为下一代HTTP**
    - **但近年来W3C不再讨论HTTP-NG**

**2 移动IP**

* **移动IP是IP协议的扩展，允许移动计算机在连接可用的任意地点连接至因特网**
* **寻址：当主机从一个网络移动到另一个网络时，IP地址需要修改**
  + **一个简单的解决方案是，当移动主机去往一个新网络时，让移动站点改变它的地址，但使用起来不方便**
  + **更可行的方法是使用两个地址：一个归属地址（home address），一个转交地址（care-of address）；前者永久不变，后者和外地网络（foreign network）相关联**
* **代理**
  + **为了使地址的改变对因特网中其他部分保持透明，需要一个归属代理（home agent）和一个外地代理（foreign agent）**
  + **归属代理通常是附属于移动主机归属网络的路由器**
  + **外地代理接收归属代理发送的分组，并向移动主机转发**
* **和远程主机通信的三个阶段**
  + **代理发现：**

**（1）移动主机必须在离开其归属网络前发现归属代理**

**（2）移动主机必须在它移动到外地网络后也发现外地代理**

**（3）路由器将代理通告添加至ICMP通告分组 ，表明它同意**

**担当代理**

* + **注册：**

**（1）移动主机必须在外地代理上注册**

**（2）移动主机必须在归属代理上注册，这通常由外地代理**

**代为完成**

**（3）如果移动主机已经过期，它必须更新注册**

**（4）当移动主机回到归属网络时，它必须取消注册**

* **和远程主机通信的三个阶段**
  + **数据传输**

**（1）从远程主机到归属代理**

**远程主机使用自己的地址作为源地址，使用移动主机的**

**归属地址作为目的地址；信息被归属代理拦截**

**（2）从归属代理到外地代理**

**使用IP-in-IP的隧道技术**

**（3）从外地代理到移动主机**

**外地代理解除原始分组，获得移动主机的归属地址，**

**然后查阅注册表获得移动主机的转交地址并发送**

**（4）从移动主机到远程主机**

**移动主机准备分组，将自己的归属地址作为源地址，**

**将远程主机的地址作为目的地址**

* **位置透明性**
  + **移动主机的运动对因特网的其余部分是透明的**
* **移动IP的低效**
  + **三角路由：当远程主机和其他网络的移动主机通信时，会发生三角路由或称迂回路由，这是适当的低效**
  + **双重交换：当远程主机和一个移动到与远程主机相同的网络的移动主机通信时，双重交换就发生了，导致严重低效（我就在你身边，你却不知道）**
  + **一种解决低效性的方案是，允许远程主机将转交地址和移动主机的归属地址绑定----如此，其归属代理可以在接收到去往移动主机的第一个分组后，转发的同时也告诉远程主机，以后你可就直接发给转交地址吧（失去透明性）**