# 第一章 计算机网络和因特网

## 1.1 什么是因特网

**R1 主机和端系统的区别？列举几种不同的端系统。Web服务器是端系统吗？**

没区别；PC，智能手机，Web服务器、电子邮件服务器；是

**R3 标准对协议为什么重要**

标准对于协议很重要，这样人们就可以创造相互连接的网络系统和产品。

## 1.2 网络边缘

**R4 列出六种接入技术。分类为住宅接入、公司接入、广域接入**

住宅接入：DSL、电缆、FTTH、拨号、卫星；

公司接入：以太网、WiFi；

广域无线接入：3G、LTE（蜂窝网络）等

*DSL：Digital Subscriber Line，数字用户线路*

*FTTH：Fiber to the home，光纤入户*

**R5 HFC宽带是专用的还是用户共享的？在下行HFC信道中，有可能发生碰撞吗？**

HFC是用户间共享的。在下行HFC信道中，所有的数据包都是从一个来源发出的，即头端，因此没有碰撞。

*HFC：Hybrid Fiber Coaxial，混合光纤同轴电缆*

**R6 列出身边的住宅接入技术。**

DSL、电缆、FTTH、拨号、以太网、WiFi等。

**R7 以太LAN的传输速率是多少？**

10Mbps、100Mbps、1Gbps、10Gbps。

**R8 能够运行以太网的物理媒体是什么？**

双绞铜线，光纤。

*物理媒体：双绞铜线、同轴电缆、光纤、陆地无线电信道、卫星无线电信道*

**R9 拨号调制解调器、HFC、DSL、FTTH都用于住宅接入，给出每一种的传输速率范围，专用还是公用？**

拨号调制解调器：最高56 Kbps，专用；

HFC：最高42.8 Mbps（下行）和30.7 Mbps（上行），共享；

DSL：最高 24 Mbps（下行）和2.5 Mbps（上行），专用；

FTTH: 最高 4Mbps（上行）和100Mbps（下行），专用。

**R10 列举当今流行的无线因特网接入技术，进行比较**

WiFi是短距离的高速无线网络。4G是远距离的高速无线网络，是3G的下一代产物。

## 1.3 网络核心

**R11 假设发送主机和接收主机中间只有一台分组交换机，交换机与发送主机、接收主机的传输速率分别是R1、R2，交换机采用存储转发分组交换方式，发送一个长度为L的分组的端到端总时延是多少？（忽略排队、传播和处理时延。）**

在*t0*时刻，发送端开始传输，因为没有传输延迟，当*t1=L/R1*时，交换机接收到整个分组，并开始传输分组到接收端，当*t2=t1+L/R2*时，接收端接收到整个分组。因此总的端到端延迟为*L/R1+L/R2*。

*存储转发机制：转发前必须接收到整个分组。*

*排队时延：等待当前分组队列前面的分组全部转发出去的时延。*

*丢包（分组丢失）：如果缓存队列已满，新到达的分组将被丢弃。*

**R12 与分组交换网络相比，电路交换网络有哪些优点？在电路交换网络中，TDM比FDM有哪些优势？**

电路交换网络为通信中的两台主机创建了专用的端到端连接，并预留了资源（带宽、缓存），能确保维持一个恒定的传输速率。而目前的大多数分组交换网络不能做任何的端到端的带宽保证。FDM需要复杂的模拟硬件将信号转换成合适的频段。

*分组交换比电路交换有更好的带宽共享，性能更优，效率更高、成本更低。*

*FDM：Frequency Division Multiplexing，频分复用，频率域。每条电路连续地得到部分带宽。*

*TDM：Time Division Multiplexing，时分复用，时域、帧、时隙。每条电路在时隙中周期地得到全部带宽。*

**R13 假定用户共享一条2Mbps链路。同时假定当每个用户传输时连续以1Mbps传输，但每个用户仅传输20%的时间。**

**A 当使用电路交换时，能够支持多少用户？**

**B 假定使用分组交换。为什么如果两个或更少用户同时传输时，在链路前面基本上没有排队时延？为什么如果3个用户同时传输时，将有排队时延？**

**C 求出某指定用户正在传输的概率**

**D 假定现在有3个用户。求出在任何给定的时间，所有3个用户在同时传输的概率。求出队列增长的时间比率。**

a 电路交换时，用总的链路速率2Mbps除以每个用户的额定速率1Mbps，（与使用的频率无关），得到最大用户数为2。

b 分组交换时，当两个或更少用户同时传输时，需要的最高传输速率为2Mbps，因此没有排队时延。超过两个用户时需要的总带宽大于可用带宽，因此造成排队时延。

c 如题，20%。

d 0.2 \* 0.2 \* 0.2 = 0.008。

**R14 为什么在等级结构相同级别的两个ISP通常互相对等？某IXP如何盈利？**

对等时ISP之间的流量可以直接传输，避免经过上游而造成费用。IXP使多个ISP能够共同对等，收取比上游ISP更少的费用。

*ISP：Internet Service Provider，因特网服务提供商*

*IXP：Internet Exchange Point，因特网交换点*

**R15 某些内容提供商创建自己的网络。描述谷歌的网络。内容提供商构建这些网络的动机是什么？**

谷歌使用专用网络连接它的数据中心。流量经过专用网络传输，因此当谷歌向用户传输数据时，它能绕开高层ISP。

动机：1 减少网络中的转发节点，提高服务质量；2 绕开高层ISP节省流量传输成本。

## 1.4 分组交换网中的时延、丢包和吞吐量

**R16 考虑从某源主机跨越一条固定路由向某目的主机发送一分组。列出端到端时延中的时延组成成分。这些时延中哪些是固定的，那些是变化的？**

处理时延（Processing），排队时延（Queueing），传输时延（Transmission），传播时延（Propagation）；除了排队时延之外都是固定的。

*处理时延由主机性能和分组长度决定；排队时延由缓存中的分组数量决定；传输时延由分组长度和传输速率决定（L/R）；传播时延由物理介质决定。*

**R18 一个长度为1000字节的分组经距离为2500km的链路传播，传播速率为2.5\*10^8 m/s并且传输速率为2Mbps，它需要多长时间？更一般的地，一个长度为L地分组经距离为d的链路传播，传播速率为s并且传输数量为Rbps，它需要多长时间？该时延与传输速率相关吗？**

（题意是在链路上直接传播，不经过交换机、路由器的转发，所以只有传播时延）所以，1 传播时延 = 2500km / 2.5\*10^8m/s = 0.01s；2 传播时延 = d/s；3 此时的总时延与传输速率无关。

**R19 假定主机A要向主机B发送一个大文件，从主机A到主机B的路径上有3段链路，其速率分别为R1=500kbps，R2=2Mbps，R3=1Mbps。**

**A 假定该网络中没有其他流量，该文件传送的吞吐量是多少？**

**B 假定该文件为4MB，传输该文件到主机B大致需要多长时间？**

**C 重复A和B，只是这时R2减小到100kbps。**

a 吞吐量 = 500kbps（取最小值）。

b 传输时长 = 4 \* 10^6 \* 8 bit / 500\*1000 bit/s = 64s。

c 吞吐量 = 100kbps；传输时长 = 4 \* 10^6 \* 8 bit / 100\*1000 bit/s = 320s。

**R20 假定端系统A要向端系统B发送一个大文件。在一个非常高的层次上，描述端系统怎样从该文件生成分组。当这些分组之一到达某分组交换机时，该交换机使用分组中的什么信息来决定将该分组转发到哪一条链路上？因特网中的分组交换为什么可以与驱车从一个城市到另一个城市并沿途询问方向类比？**

端系统A将大文件分解成块，向每个块添加首部信息，从而从文件生成多个分组。每个分组的报头包含目标（端系统B）的IP地址，分组交换机使用分组头部中的目标IP地址来确定转发链路；驱车沿途询问走哪条路与分组询问应该被交换机转发到哪个链路类似。

## 1.5 协议层次及其服务模型

**R22 列出一个层次能够执行的5个任务。这些任务中的一个（或两个）可能由两个（或更多）层次执行吗？**

差错控制，流量控制，多路复用/分解，分段和重组，连接建立；可以，比如差错控制。

**R23 因特网协议栈中的5个层次有哪些？在这些层次中，每层的主要任务是什么？**

互联网协议栈的五层从上到下分别是应用层、传输层、网络层、链路层和物理层。

应用层：网络应用程序及它们的应用层协议存留的地方。

运输层：在应用程序端点之间传送应用层报文。

网络层：将数据报的网络层分组从一台主机向另一台主机移动。

链路层：为了将分组从一个结点（主机或路由器）移动到下一个结点。

物理层：将帧中的一个一个比特从一个结点移到另一结点。

**R24 什么是应用层报文？什么是运输层报文段？什么是网络层数据报？什么是链路层帧？**

应用层报文：应用程序想要发送并传递到传输层的数据；

传输层报文段：封装了传输层首部信息和应用层报文；

网络层数据报：封装了网络层首部信息和传输层报文段；

链接层帧：封装了链接层首部信息和网络层数据报。

**R25 路由器处理因特网协议中的哪些层次？链路层交换机处理的是哪些层次？主机处理的是那些层次？**

路由器：网络层、链路层和物理层 (现代路由器有时充当防火墙或缓存组件，同时还处理传输层)。

链路层交换机：链路层和物理层。

主机：所有五层。

## 1.6 面对攻击的网络

**R26 病毒和蠕虫之间有什么不同？**

病毒需要某种形式的用户互动才能传播。典型的例子：电子邮件病毒。

蠕虫在被感染主机中主动扫描因特网，寻找易受感染的主机，通过发送自己的副本来传播。

**R27 描述如何产生一个僵尸网络，以及僵尸网络是怎样被用于DDoS攻击的？**

攻击者通过直接攻击漏洞或者传播病毒的方式来攻击脆弱的主机，以获得主机的控制权限，这些主机称为僵尸主机。僵尸网络即由大量僵尸主机组成的网络；攻击者拥有僵尸网络所有主机的远程控制权限，攻击者控制僵尸网络中的所有节点向攻击目标发起网络攻击（如发送给攻击目标的TCP SYN消息），对攻击目标造成洪泛攻击。

*僵尸网络：botnet*

*DoS：Denial of Service Attack，拒绝服务攻击*

*DDoS：Distributed DoS，分布式拒绝服务攻击*

**R28 假定Alice和Bob经计算机荷香发送分组。假定Trudy将自己安置在网络中，使得它能够俘获由Alice发送的所有分组，并发送她希望给Bob的东西；她也能够俘获Bob发送的所有分组，并发送她希望给Alice的东西。列出在这种情况下Trudy能够做的恶意的事情。**

Trudy可以伪造、篡改甚至丢弃Alice与Bob之间的通信内容。

# 第二章 应用层

## 2.1 应用层协议原理

**R1 列出5种非专用的因特网应用及它们所使用的应用层协议**

Web服务：HTTP（80端口）；

文件传输：FTP（21、20端口）；

远程登录：Telnet（23端口）、ssh（22端口）

Email：SMTP（25端口）

P2P：BitTorrent

**R2 网络体系结构与应用程序体系结构之间有什么关系？**

网络体系结构是指如五层Internet架构，为应用程序提供了特定的服务集合。应用程序体系结构是由应用程序开发人员设计的，规定了如何在端系统上组织应用程序。

**R3 对两个进程之间的通信会话而言，哪个进程是客户，哪个进程是服务器？**

主动发起请求的是客户端，被动接收请求的是服务器。

**R4 对一个P2P文件共享应用，你同意“一个通信会话不存在客户端和服务端的概念”的说法吗？为什么？**

不。在P2P文件共享应用程序中，接收文件的对等点通常是客户机，发送文件的对等点通常是服务器。

**R5 运行在一台主机上的一个进程，使用什么信息来标识运行在另一台主机上的进程？**

目标主机的IP地址和目标进程中套接字的端口号。

**R6 假定你想尽快地处理从远程客户到服务器的事务，你将使用UDP还是TCP？为什么？**

（题意为尽快处理）使用UDP，事务可以在一个RTT内完成——客户机直接向服务器发送事务的UDP套接字，服务器返回响应。而TCP需要先建立TCP连接再传输事务的TCP套接字，至少需要两个RTT。

*RTT：Round Trip Time，往返时间。即数据发送时刻到接收到确认消息的时刻的差值。*

**R7 如图2-4列出的应用程序没有一个同时既要满足无数据丢失又要求定时的。设想一个既要无数据丢失又高度时间敏感的应用程序。**

电商抢购类应用就同时保证订单数据正确且对时间敏感。

*图2-4列出了一些应用程序与服务要求。*

*文件传输：不能丢失数据，对时间不敏感，带宽弹性；*

*电子邮件：不能丢失数据，对时间不敏感，带宽弹性；*

*Web文档：不能丢失数据，对时间不敏感，带宽弹性；*

*网络电话、视频：容忍丢失数据，对时间敏感，需要保证带宽；*

*存储音频视频：容忍丢失数据，对时间敏感，需要保证带宽；*

*交互式游戏：容忍丢失数据，对时间敏感，需要保证带宽；*

*即时讯息：不能丢失数据，对时间敏感有和没有，带宽弹性；*

**R8 列出一个运输协议能够提供的4种宽泛类型的服务，对于每种服务类型，指出是UDP还是TCP提供的服务？**

可靠数据传输：TCP；

（带宽）吞吐量：都不提供；

定时：都不提供；

安全性：都不提供；

**R9 TCP能用SSL来强化，以提供进程到进程的安全性服务，包括加密。SSL运行在运输层还是在应用层？如果某应用程序研制者想要用SSL来强化UDP，该研制者应当做些什么工作？**

SSL运行在应用层；如果要用SSL强化UDP，研制者需要在应用程序的客户端和服务端代码中插入SSL代码。

## 2.2-2.5 Web和HTTP | 文件传输协议：FTP | 因特网中的电子邮件 | DNS：因特网的目录服务

**R10 握手协议的作用是什么？**

确认身份，是指主要用来让客户端及服务器确认彼此的身份的一类网络协议。

**R11 为什么HTTP、FTP、SMTP及POP3都运行在TCP而不是UDP上？**

TCP具有面向连接服务和可靠数据传输服务，还具有拥塞控制机制，符合HTTP、SMTP 及POP3的对数据传输敏感性的要求。

**R12 考虑一个电子商务网站需要保留每一个客户的购买信息。描述如何使用cookie来完成该功能？**

当用户首次访问站点时，服务器创建并保存一个惟一标识符，该标识符被作为cookie返回并保存到用户的浏览器上。在随后的每次访问中，浏览器将cookie编号发送回站点进行交互。因此站点能识别请求来自哪个用户（浏览器）。

*cookie的四个组件：HTTP响应头的cookie首部行；HTTP请求头的cookie首部行；浏览器中保留的cookie数据或文件；服务器中保留cookie的数据库。*

**R13 描述Web缓存器是如何减少接收被请求的对象的时延的。Web缓存器将减少一个用户请求的所有对象或只是其中的某些对象的时延吗？为什么？**

Web缓存器保存了用户最近请求过的资源且往往比服务器更靠近用户主机，所以能减少请求的时延。Web缓存器能减少所有对象的时延。由于Web缓存器的存在也减少了服务器的链路压力，这种机制也能减少访问时延。

**R14 Telnet到一台Web服务器并发送一个多行的请求报文。在该请求报文中包含if – modified – since: 首部行，迫使响应报文中出现“304 Not Modified”状态编码。**

说法正确。

**R15 为什么说FTP在“带外”发送控制信息？**

FTP使用两个并行TCP连接，一个连接用于发送控制信息（例如传输文件的请求），另一个连接用于实际传输文件。所以说FTP的控制信息是“带外”发送的。

**R16 假定Alice使用一个基于Web的电子邮件账户向Bob发报文，而Bob使用POP3从他的邮件服务器访问自己的邮件。是怎样从Alice主机到Bob主机得到该报文的？要列出在两台主机间移动该报文所使用的各种应用层协议。**

消息首先通过HTTP从Alice的主机发送到她的邮件服务器。然后Alice的邮件服务器通过SMTP将消息发送到Bob的邮件服务器。然后Bob通过POP3将消息从邮件服务器传输到主机。

*SMTP：Simple Mail Transfer Protocol，简单邮件传输协议，是因特网电子邮件应用的核心，用于发送方邮件服务器给接收方邮件服务器传输报文。邮件服务器之间先建立TCP连接后再传输。*

*POP3：Post Office Protocol，第三版邮局协议，解决代理邮件应用从邮件服务器上取邮件的需求（SMTP是推协议，而取邮件需要的是拉协议）。*

*IMAP：Internet Mail Access Protocol，因特网邮件访问协议，比POP3更复杂，功能更多，IMAP能支持邮件报文与文件夹的关联，允许用户代理获取报文组件的命令（获取报文头部信息）。*

**R18 POP3协议中下载并删除模式和下载并保留模式有什么区别？**

通过下载和删除，在用户从POP服务器检索消息之后，这些消息将被删除；在下载和保存配置中，在用户检索消息后不会删除消息。

**R19 一个机构的Web服务器和邮件服务器可以有完全相同的主机别名吗？包含邮件服务器主机名的RR有什么样的类型？**

可以；包含邮件主机名的RR有MX类型和A类型。MX类型记录邮件服务器的别名与规范名的映射，A类型记录邮件服务器的全名和IP地址的映射。

*RR：Resource Record，资源记录，提供了主机名到IP地址的映射。存储在DNS分布式数据库所有DNS服务器中。RR元组包含了4个字段：（Name，Value，Type，TTL）*

*RR的类型：A，标准的主机名与IP地址的映射；NS，当前域名与权威DNS的主机名的映射（当前DNS服务器没有具体IP，但是保留了查询链）；CNAME，别名与规范的主机名的映射；MX，别名与邮件服务器的规范的主机名的映射；*

*DNS协议运行在UDP上，使用53端口。*

## 2.6 P2P应用

**R21 在BitTorrent中，假定Alice向Bob提供一个30秒间隔的文件块吞吐量。Bob将必须进行回报，在相同的间隔中向Alice提供文件块吗？为什么？**

Bob不一定要向Alice提供块。根据BitTorrent的对换算法，Alice必须在Bob的前5个邻居（4个最高速率的和一个试探的对等方）中Bob才能向Alice发送数据块。

*BitTorrent协议中，向对等方请求文件块时采用稀缺优先的技术，向对等方发送文件块时采用最高速率作为优先权，发送方不向可发送范围（4个最高速率的对等方（又叫疏通）和一个试探的对等方）之外的对等方（又叫阻塞）发送文件块。*

**R22 考虑一个新的对等方Alice加入BitTorrent而不拥有任何文件块。没有任何块，因此它没有任何东西可以上载，他无法成为任何其他对等方的前4位上载者。那么Alice将怎样得到她的第一个文件块呢？**

在BitTorrent中，对等方们每过30秒随机选择另外的一个邻居发送块，当Alice被随机选中时，她将得到第一个块。

**R23 覆盖网络是什么？它包括路由器吗？在覆盖网络中边是什么？**

覆盖网路是一种应用层网络（对等方组成的逻辑网络，不是物理链路），在P2P协议中，覆盖网路由文件共享系统的节点与节点间的逻辑联系（两个对等方之间的TCP连接）构成，这条逻辑联系就是“边”，不包括路由器。

**R24 考虑一个具有网状覆盖网络拓扑的DHT（每个对等方跟踪系统中的所有对等方）。这样设计的优点和缺点各是什么？环形DHT（无捷径）的优点和缺点各是什么？**

Mesh DHT：

优点是为了将消息路由到最接近键的对等节点，只需要一次跳转;

缺点是每个对等点必须跟踪DHT中的所有其他对等点。

循环DHT（无捷径）：

优点是每个对等点只需要跟踪几个其他对等点;

缺点是需要O(N)（平均次数为N/2）跳来将消息路由到最接近键的对等点。

**R25 列出至少4个不同的应用，它们本质上适合P2P体系结构。**

文件传输；即时通讯；视频；分布式计算。

## 2.7 TCP套接字编程

**R26 UDP服务器仅需要一个套接字，而TCP需要两个套接字。为什么？如果TCP服务支持n个并行连接，每条连接来自不同的客户主机，那么TCP服务器将需要多少个套接字？**

UDP服务器只有一个serverSocket，来自不同客户机的所有数据都通过这个套接字进入服务器。对于TCP服务器，有一个serverSocket，每当客户机与服务器建立连接时，还会创建一个connectionSocket。因此，为了支持n个并发连接，服务器总共需要n+1个套接字。

**R27 运行在TCP上的客户-服务器应用程序，服务器程序为什么必须先于客户端程序运行？对于运行在UDP上的客户-服务器应用程序，客户程序为什么可以先于服务器程序运行。**

对于TCP应用程序，一旦执行客户程序，它就会尝试启动与服务器建立TCP连接。如果TCP服务器没有运行，那么客户机将无法握手，当然也无法建立连接。对于UDP应用程序，客户程序在执行时不会立即尝试与UDP服务器通信。

# 第三章 运输层

## 3.1 – 3.3 概述与运输层服务 | 多路复用与多路分解 | 无连接运输：UDP

**R1 假定网络层提供了下列服务。在源主机中的网络层接受最大长度1200字节和来自运输层的目的主机地址的报文段。网络层则保证将该报文段交付给位于目的主机的运输层。假定在目标主机上能够运行许多网络应用进程。**

**A 设计可能最简单的运输层协议，该协议将使应用程序数据到达位于目的主机的所希望的进程。假设在目的主机中的操作系统已经为每个运行的应用进程分配了一个4字节的端口号。**

**B 修改这个协议，使它向目的进程提供一个“返回地址”。**

**C 在你的协议中，该运输层在计算机网络的核心中“必须做任何事”吗？**

a 假设这个协议命名为P，在发送端，P接收不超过1196字节的数据块、目的主机地址和端口，以及4个字节报文段首部，存放目的进程端口号。P将报文传递给网络层，网络层将报文传送至目的主机的传输层。目的主机的P检查报文段的数据和端口号，传递给目的进程。

b 在P的报文段首部再加4个字节存放源端口号，P接收不超过1192字节的数据块、目的主机地址、目标端口号、源端口号。目的主机传输层接收到报文段后，P向目标进程提供报文段数据和源端口号。

c 不必须（“必须做任何事”意味着运输层有丰富的功能）。

**R2 考虑有一个星球，每个人都属于某个六口之家，每个家庭都住在自己的房子里，每个房子都有唯一的地址，并且某给定家庭中的每个人有一个独特的名字。假定该星球有一个从源家庭到目的家庭交付信件的邮政服务。该邮政服务要求：1 在一个信封中有一封信；2 在信封上清楚地写上目的家庭的地址（并且没有别的东西）。假设每个家庭有一名家庭成员代表为家庭中的其他成员收集和分发信件。这些信没有必要提供任何有关信的接收者的指示。**

**A 使用对上面R1的解决方案作为启发，描述家庭成员代表能够使用的协议，以从发送家庭成员向接收家庭成员交付信件。**

**B 在你的协议中，该邮政服务必须打开信封并检查信件内容才能提供它们的服务吗？**

a 发送方家庭成员必须将信件内容、目的地址、指定的接收方家庭成员交给家庭成员代表。代表写好信并在信封上写上目的家庭地址。通过邮政服务发给目的家庭。接收家庭成员代表从邮政服务获得信件，读取信件内容，根据信中指定的接收家庭成员，把信件转发给该成员。

b 不需要，信封上有目的家庭的地址。

**R3 考虑在主机A和主机B之间有一条TCP连接。假设从A传送到B的TCP报文段具有源端口号x和目的端口号y。对于从B到A的报文段，源端口号和目的端口号分别是多少？**

y，x。

**R4 描述应用程序开发者为什么可以选择在UDP上运行应用程序而不是在TCP上运行的原因。**

UDP容忍少量的分组丢失，没有拥塞控制机制导致实时性能下降。所以当应用程序开发者不需要TCP的可靠数据传输、拥塞控制时，将选择UDP。通常因特网电话、实时视频会议、流式存储音频与视频应用的开发者可能选择在UDP上运行应用程序。

**R5 在今天的因特网中，为什么语音和图像流量通常是经过TCP而不是UDP发送。**

大量数据传输过程中UDP很有可能会丢失部分分组使整个信息无用，而TCP有完善的分组重传机制。UDP分组最大64k字节；此外大多数防火墙被配置为阻止UDP通信，导致UDP并不常用。

**R6 当某应用程序运行在UDP上时，该应用程序可能得到可靠的数据传输吗？如果成，如何实现？**

能，需要在应用层上设计可靠的数据传输功能。

**R7 假定在主机C上的一个进程有一个具有端口号6789的UDP套接字。假定主机A和主机B都用目的端口号6789向主机C发送一个UDP报文段。这两台主机的这些报文段在主机C都被描述为相同的套接字吗？如果是这样的话，在主机C的该进程将怎样知道源于两台不同主机的这两个报文段？**

相同。UDP套接字时由一个二元组（目的IP地址，目的端口号）来全面标识的，当两个不同来源的UDP报文段有同一个目的IP/端口号时，两个报文段将通过相同的目的套接字被定向到相同的目的进程。网络层IP协议中，两个报文段的IP地址不同，可以被主机C的进程读取。

*套接字（socket）：是进程与网络互相交付数据的门户，一个进程有一个或多个套接字，每个套接字都有唯一标识符。*

*多路分解：在接收端，将运输层报文段中的数据交付到正确的套接字的过程。*

*多路复用：在源端，传输层从不同套接字中收集数据块，为每个数据块封装首部信息生成报文段，最后传递到网络的过程。*

*关于UDP报文首部结构：横向32比特，纵向两格，总长度8字节。第一格是成对的源端口号和目的端口号（各16bit），第二格前16bit是长度字段，意味着UDP报文段（首部+数据）的总字节数，范围是[8, 65535]，后16bit是校验和。【注意，报文段长度字段是一个冗余字段，TCP上就没有，因为在网络层会进行封装，在IP协议中有数据报长度字段】*

**R8 假定主机C端口80上运行的一个Web服务器。假定这个Web服务器使用持续连接，并且正在接收来自两台不同主机A和B的请求。被发送的所有请求都通过位于主机C的相同套接字吗？如果人们通过不同的套接字传递，这两个套接字都有端口80吗？**

Web服务器的TCP套接字用四元组（源IP地址、源端口号、目标IP地址、目标端口号）来标识。因此，来自A和B的请求通过不同的套接字。这两个套接字的标识符中目标端口号都是80。

*如果客户端与服务器使用持续HTTP，则在连接持续期间，客户端与服务器之间经由同一个服务器套接字交换HTTP报文。*

## 3.4 可靠数据传输原理

**R9 在我们的rdt协议中，为什么需要引入序号。**

接收端需要序列号来确定到达的数据包是包含新数据还是重传。

**R10 在我们的rdt协议中，为什么需要引入定时器。**

发送方面对分组丢失的可能情况时，总是选择重传分组。为了实现基于时间的重传机制，因此需要引入定时器。

**R11 假定发送方和接收方之间的往返时延是固定的并且为发送方所知。假设分组能够丢失的话，在协议rdt3.0中，一个定时器仍是必需的吗？试解释。**

仍然需要计时器。发送方还是需要计时器来检测分组丢失，这与时延是否固定是否被发送方所知无关。

## 3.5 面向连接的运输：TCP

**R14 判断题**

**A 主机A通过一条TCP连接向主机B发送一个大文件。假设主机B没有数据发往主机A。因为主机B不能随数据捎带确认，所以主机B将不向主机A发送确认。**

错。接收端都要给收到的分组发送确认。捎带确认指确认ACK被装载在一个服务器到客户端的数据的报文中（Telnet的例子）。

**B 在连接的整个过程中，TCP的rwnd的长度绝不会变化。**

错；接收窗口（rwnd）是动态变化的。

*TCP通过让发送方维护一个接收窗口（rwnd）的变量来提供流量控制，rwnd指示发送方当前接收方还剩余多少可用缓存空间。*

**C 假设主机A通过一条TCP连接向主机B发送一个大文件。主机A发送但未被确认的字节数不会超过接收缓存的大小。**

对。累计确认机制，TCP只确认该流中至第一个丢失字符为止的字节。

**D 假设主机A通过一条TCP连接向主机B发送一个大文件。如果对于这条连接的一个报文段的序号为m，则对于后继报文段的序号将必然是m+1。**

错；重传的情况下序号不变，该序号是期望的待接收分组的序号。

**E TCP报文段在他的首部中有一个rwnd字段。**

对。

*TCP连接两端都各维护一个rwnd。发送数据时，主机B通过把当前rwnd值放入发往主机A的报文段rwnd字段中，通知A在该连接中剩余可用缓存空间。*

**F 假定在一条TCP连接中最后的SampleRTT等于1秒，那么对于该连接的TimeoutInterval的当前值必定大于等于1秒。**

错。

*TCP中，与往返事件相关的概念：SampleRTT（实际采集的RTT），EstimatedRTT（平均的SampleRTT），DevRTT（实际RTT与平均RTT的偏差值），TimoutInterval（超时间隔，会考到它的公式和变化）。*

**G 假设主机A通过一条TCP连接向主机B发送一个序号为38的4个字节的报文段。在这个相同的报文段中，确认号必定是42。**

错。

**R15 假设主机A通过一条TCP连接向主机B发送两个紧接着的TCP报文段。第一个报文段的序号为90，第二个报文段选后为110。**

**A 第一个报文段的有多少数据？**

**B 假设第一个报文段丢失而第二个报文段到达主机B。那么在主机B发往主机A的确认报文中，确认号应该是多少？**

a 20 Bytes；b 90；

**R16 考虑在Telnet的例子中。在用户输入字符C数秒后，用户又输入字符R。那么在用户输入字符R之后，总共发送了多少个报文段，这些报文段中的序号和确认字段应该填入什么？**

前面已经完成了①发送（Seq：42，ACK：79） ②回显（Seq：79，ACK：43） ③确认（Seq：43，ACK：80）；所以新发送的字符R也同样会经历三个步骤：发送（Seq：43，ACK：80），回显（Seq：80，ACK：44），确认（Seq：44，ACK：81）

*3.5 补充内容：*

*rdt的演变：1 可靠数据传输 > 2 经具有比特差错信道的可靠数据传输（rdt2.0） > 3 经具有比特差错的丢包信道的可靠数据传输（rdt3.0） > 4 流水线可靠信道传输。*

*rdt2.0，又叫停等协议（stop-and-wait）：引入确认（肯定/否定），引入自动重传请求（ARQ），引入序号，引入缓存。*

*ARQ功能：差错检测；接收方反馈，重传。*

*rdt3.0，又叫比特交替协议：引入定时器。*

*流水线可靠信道传输协议：（停等协议效率太低）不使用停等协议，允许发送方发送多个分组而无需等待确认。*

*序号范围：分组首部的序号字段长度固定，k比特的序号字段意味着序号范围是[0, 2^k - 1].*

*回退N步（GBN）协议，又叫滑动窗口协议：三个值（base，nextseqnum， N），四类分组（已确认，已发送未确认，未发送，不使用）；触发发送方的三个事件（上层调用，收到确认，超时重传）。*

*选择重传（SR）协议：（单个分组丢包造成的大量分组的重传是没必要的）在接收端，直接返回ACK（不一定按序号），如果窗口前面有未接收的期望分组，则等；等分组到达了再把连续的已接收的一批分组交互出去。*

*关于TCP报文首部结构：横向32bit（4个字节），纵向5格（其实还有可变长度的第六格选项字段，它通常是空的），最小总长度20字节。第一格是成对的源端口号与目的端口号（各16bit），意味着端口范围是[0, 65535]；第二、三格是成对的32bit的序号和确认号，意味着分组序号范围是[0, 2^32-1]；第四格内容最多，主要包含：① 最开头的4bit首部长度（表示首部的最大长度是16单位，一单位为32bit），意味着首部最大长度64字节，② 最末尾的16bit接收窗口，意味着最大接收窗口为65535个分组，③ 6比特标志字段（URG、ACK、PSH、RST、SYN、FIN），URG意味着紧急指针字段有效（不怎么用），ACK指示报文段首部确认号是有效的，PSH意味着分组有数据要交给上层（不怎么用），RST意味着复位（即强制拆除）一个TCP连接，SYN、FIN用于有序地建立和拆除TCP连接；第五个前16bit是校验和和后16bit紧急数据指针。*

*3.6 拥塞控制原理补充内容*

*拥塞控制方法根据网络层是否为运输层拥塞控制提供显示帮助，分为端到端拥塞控制（TCP的拥塞控制方式，因为IP协议不提供拥塞控制能力），网络辅助的拥塞控制（网络层提供显示的拥塞控制辅助）；*

*ATM ABR拥塞控制（网络辅助的拥塞控制）：ATM基于虚电路进行分组交换。信元代替TCP分组概念，分为数据信元和资源管理信元（RM信元），RM信元混在数据信元的流中，用于传递与拥塞相关的信息。交换机代替IP路由器概念。交换机可以生成RM信元。*

*ACR服务在轻负载时充分利用空闲带宽，在网络拥塞时会限制其传输速度为某些预设的最小传输速率。ABR提供三种机制用于从交换机向接收方发送与拥塞相关的信令信息：显示转发拥塞指示比特（EFCI，设置在数据信元上）；拥塞指示比特（CI）和无增长比特（NI）（二者设置在RM信元上，严重拥塞时CI为1，轻微拥塞时NI为1）；显示速率字段（ER），表示虚电路路径上所有交换机的最小速率。*

## 3.7 TCP拥塞控制

**R17 假设两条TCP连接存在于一个带宽为R bps的瓶颈链路上。它们都要发送一个很大的文件（以相同方向经过瓶颈链路），并且两者都是同时开始发送文件。那么TCP将每条连接分配什么样的传输速率？**

R/2。

**R18 考虑TCP的拥塞控制。当发送方定时器超时时，其ssthresh的值将被设置为原来值的一半。**

对。

*3.7 补充内容：*

*流量控制与拥塞控制：二者的手段都是抑制发送方的发送速率。流量控制目的是使发送方速率与接收方匹配，TCP在发送方维护rwnd变量来提供流量控制，rwnd值需要根据接收方的反馈来调整；拥塞控制的目的是调节发送方速率以避免网络拥塞，通过cwnd变量实现，cwnd值由发送方自己通过感知拥塞情况并采取拥塞控制算法来调节。*

*TCP拥塞控制算法：① 慢启动：cwnd从1个MSS指数增长，直到TCP连接出现拥塞或cwnd达到拥塞阈值（ssthresh），当出现拥塞时，ssthresh置为cwnd/2，cwnd重新置为1个MSS，重新转移到慢启动。当cwnd到达ssthresh时，转移到拥塞避免；② 拥塞避免，当cwnd达到ssthresh时，cwnd从指数增长变为线性增长，直到再次出现拥塞，然后转移到慢启动或是快速恢复；③ 快速恢复（推荐但非必要），在收到3个冗余ACK时（并不是所有的拥塞条件），发送端感知到拥塞，ssthresh置为cwnd/2，置新cwnd为ssthresh+3，继续实施拥塞避免的线性增长。；*

*快速重传与快速恢复：发送方一次会批量地发送分组，如果其中一个分组丢失，会引起多个冗余ACK，TCP中，发送方收到3个冗余ACK时被指示为出现了丢包，则执行快速重传（快速是指发送方能在定时器过期之前重传分组）；快速恢复也利用3个冗余ACK来指示丢包，从而感知网络拥塞，并采取优化的方法调整cwnd值（cwnd-3），而不是直接降到1（即慢启动）。*

# 第四章 网络层

## 4.1 – 4.2 概述 | 虚电路和数据报网络

**R1 运输层的分组名称是报文段，数据链路层的分组是帧。网络层分组名称是什么？路由器和链路层交换机都被成为分组交换机，它们的根本区别是什么？**

数据报；交换机数据链路层（二层交换机），路由器属于网络层（三层交换机）。截断的协议栈，没有更上层的协议。

**R2 在数据报网络中，网络层两个最主要功能是什么？虚电路网络中网络层3个最重要的功能是什么？**

数据报网络主要功能是转发和路由选择；虚电路主要功能是建立连接、转发和路由选择。

*数据报网络（因特网的服务类型）：提供无连接的网络层服务；*

*虚电路网络：提供面向连接的网络层服务；虚电路连接建立过程：运输层告知网络层接收方地址，网络层决定发送方与接收方的端到端路径，网络层为每一段链路生成VC号，路径上每台路由器的路由表增加表项（接口号、VC号）*

**R3 路由选择和转发的区别是什么？**

转发涉及分组在单一的路由器内部从一条入链路到一条出链路的传送；路由选择涉及一个网络的所有路由器，它们经路由选择协议共同交互，以决定分组从源到目的结点所采用的路径。

**R4 在数据报网络和虚电路网络中的路由器都是用转发表吗？如果是，描述用于这两类网络的转发表。**

是。虚电路网络面向连接，需要维护VC，路由器转发表包含出与入的VC号，路由表只在连接建立和拆除时修改；数据报网络是无连接的，路由器转发表直接记录分组目的地址的前缀，采用最长前缀匹配规则来匹配转发接口，路由表通过路由选择协议来修改。

**R5 描述网络层能为单个分组提供的某些假象的服务。对分组流进行相同的描述。因特网的网络层提供了这些假想服务吗？ATM的CBR提供了这种假想服务吗？ATM的ABR提供了这种假想服务吗？**

因特网尽力而为模型：无带宽保证，不保证不丢包，分组未必有序，不维护定时，无拥塞指示；

ATM CBR（恒定比特率）：保证恒定速率，保证不丢包，分组有序，维护定时，不出现拥塞情况；

ATM ABR（可用比特率）：保证最小速率，不保证不丢包，分组有序，不维护定时，提供拥塞指示。

## 4.3 路由器工作原理

**R7 为什么在高速路由器的每个输入端口都存储转发表的影子副本？**

因为每个分组可以在输入端口完成查找功能。有了影子副本，转发决策可以在每个输入端口本地做出，无需调用路由选择处理器，避免集中式处理的瓶颈。

**R8 列出并讨论3类交换结构。哪种能跨越交换结构并行发送多个分组？**

经内存交换：在CPU的直接控制下完成的。复制到指定内存，再从内存提取；

经总线交换：输入端口为分组计划一个内部标签，送到总线，所有输出端口可以接收但只有指定端口可以识别标签；

经互联网络交换（纵横式）：由2N条总线组成（N是输入或输出端口的数量），每条输入总线和所有输出总线相连，交叉点通过交换结构控制器开启和闭合，支持并发分组，但是这种并发只限于发往不同输出端口的分组。

**R9 描述在输入端口会出现丢失分组的原因。描述在输入端口如何消除分组丢失。**

如果分组到达的速率大于交换结构的速率，那么就会造成排队，随着队列越来越长，输入端口的缓存被耗尽，将丢弃分组（可能是新到达队尾的分组，也可能是已排队的分组）。消除分组丢失的方法：提升交换结构的速率至N倍的输入线路速率，N为输入端口数。

**R10 描述在输出端口出现丢失分组的原因。通过增加交换结构的速率能够防止这种丢失吗？**

输出端口的缓存被耗尽。增加交换结构的速率有可能加重输出端口内存中的分组队列，对减缓排队现象没有任何帮助。

*关于丢弃和标记分组的策略——主动队列管理（AQM）算法。随机早期检测（RED，AQM的一种），为输出队列长度维护一个加权平均值L，定义长度最小阈值min和最大阈值max，当分组到达，如果：① L< min，分组入队列；② L > max，分组被丢弃；③ L 介于[min, max]，以某种概率标记或丢弃分组。*

**R11 什么是HOL阻塞？它出现在输入端口还是输出端口？**

HOL（head-of-the-line）阻塞：输入队列最前端的分组由于某种原因被阻塞，导致后面的分组即使它对应的输出队列是空的，可以被转发结构立即转发，但仍要等到队列最前端的分组被转发之后才可以被转发。HOL阻塞出现在输入端口。

*4.3 补充内容*

*路由器的四个组成部分：① 输入端口，支持查询和转发功能，查询转发表再通过交换结构把分组转发给输出端口，或者是直接把分组转发到路由选择处理器；② 输出端口，支持分组存储功能，从交换结构接收分组，再向更下层传递分组；③ 交换结构，路由器中的网络，连接输入端口与输出端口；④ 路由选择处理器，执行路由选择协议，维护路由表及链路状态信息。*

*路由器的功能：路由器转发平面（负责转发功能，由硬件实现，即输入端口、交换接口和输出端口）和路由控制平面（执行路由选择协议，对链路进行响应，由软件实现，软件在路由选择处理器上执行）；*

## 4.4 网际协议：因特网中的转发和编址

**R12 路由器有IP地址吗？如果有，有多少个？**

有，每个接口都有一个IP地址。

**R13 IP地址223.1.3.27的32比特二进制等价形式是什么？**

11011111.00000001.00000011.00011011。

*分类编址（classful addressing）方案：把网络按固定比特位数分成A（8bit掩码）、B（16bit掩码）、C（24bit掩码）类子网。此外还有，D类地址用于组播（多播），前面4位1110，后面28位为组播地址id。十进制表示范围：224.0.0.0 - 239.255.255.255；E类地址用于研究使用，前面4位1111，十进制表示范围：240.0.0.0 - 。*

*无分类域间路由选择（Classless Interdomain Routing，CIDR）：一般化的子网寻址方案，格式为A.B.C.D/X。*

**R15 假设在一个源主机和一个目的主机之间有3台路由器。不考虑分片，一个从源主机发送给目的主机的IP报文将通过多少接口？为了将数据报从源发送到目的地需要检索多少个转发表？**

5个网络结点，4段链路，所以有8个接口；路径上有3台路由器，所以有3个转发表。

**R16 假设某应用每20ms生成40字节的数据块，每块封装在一个TCP报文中，TCP报文段再封装在一个IP数据报中。每个数据报的开销有多大？应用数据所占百分比是多少？**

数据报总长度L=20字节（TCP头）+20字节（IP头）+40字节（有效载荷）=80字节；数据占比R=40/80=50%。

**R17 假定主机A向主机B发送封装在IP数据报中的TCP报文段。当主机B收到该数据报时，主机B中的网络层怎样知道它应当将该报文段（即数据报的有效载荷）交付给TCP而不是UDP或某个其他东西？**

网络层从IP头部中读取“上层协议”字段，值为6表明发送给TCP协议，值为17表明发送给UDP协议处理。

**R18 假定有一个无线路由器，将其与电缆调制解调器相连。同时假定ISP动态地为连接的设备（无线路由器）分配一个IP地址。还假定无线路由器使用802.11以无线方式连接了5个主机。怎样为这5台主机分配IP地址？该无线路由器使用NAT吗？为什么？**

分配IP地址的方式：网络管理员手动分配IP地址，或者通过DHCP自动分配IP地址。路由器使用了NAT，因为路由器只有一个公网IP却要给五台主机分配子网IP地址。

*动态主机配置协议（DHCP）：允许主机自动获取（被分配）IP地址、子网掩码、默认网关等信息。DHCP是即插即用协议，主机会频繁地加入和离开网络。DHCP是客户-服务器协议，客户是新加入网络的主机，需要与DHCP服务器请求当前的网络配置信息。*

*DHCP协议客户-服务器交互的四个步骤：① 主机广播DHCP发现报文（最开始主机没有IP地址，所以头两个步骤都是使用广播），② DHCP服务器广播DHCP提供报文（包含事务ID，推荐的IP地址，默认网关，网络掩码，IP地址租用期），③ 主机向指定服务器发送DHCP请求报文（用于回显参数，在上一步客户已经获得了IP地址，所以可以进行端到端请求），④ 服务器用DHCP ACK报文进行响应。*

*网络地址转换（NAT）：用额外的端口映射来弥补IP地址数量少不足以分配给内网使用的问题。然而NAT引入了新的问题，NAT介入、占用且修改了运输层提供给进程使用的端口，违反了端到端原则。*

**R19 比较并对照IPv4和IPv6首部字段。它们有某些字段是相同的吗？**

版本-版本；服务类型（TOS）-流量类型；上层协议-下一个首部；寿命（TLL）-跳限制。

*IPv6数据报首部结构：纵向4格，固定长40（4+4+16+16）字节。第一格（32bit），包含版本（4bit），流量类型（8bit），流标签（20bit）；第二格（32bit），包含有效载荷长度（16bit，注意是数据部分的字节数），下一个首部（8bit），跳限制（8bit），第三、四格是成对的128bit的源地址与目的地址。*

*相比IPv4，IPv6数据报首部弃用的字段有：① 分片/重组相关字段，在源端系统完成分片，遇到数据报太大不兼容链路层时直接丢弃分组并反馈“分组太大”；② 首部校验和，上下两层都做了，网络层就可以节省了；③ 选项字段，本来就是冗余项。*

*IPv6的变化内容：扩大的地址容量；固定的40字节首部；引入流标签与优先级。*

**R20 当IPv6建隧道通过IPv4路由器时，IPv6将IPv4隧道作为链路层协议。说法是否正确？为什么？**

同意，因为IPv6的数据报被封装在IPv4的数据报中，对于IPv6而言，IPv4隧道就是它的下面一层，即链路层。

*4.4 补充内容*

*因特网网络层三个主要组件：IP协议（编制规则，数据报格式，分组处理规则），路由选择协议（路径选择，RIP、OSPF、BGP），ICMP协议（差错报告，路由器“信令”）。*

*关于IP数据报首部结构：与TCP报文段首部结构相似，横向32bit，纵向5格（第六格通常为空），最小长度20字节。第一格包含：版本号（4bit），首部长度（4bit，跟TCP一样），服务类型（8bit），数据报长度（16bit，表示首部+数据的总长度，单位：字节数，意味着IP数据报最大长度是65535字节）；第二格包含16bit标识，3bit标志，13bit片偏移量，这组字段与IP分片有关；第三格包含8bit寿命（TTL，用于确保数据报不会永远存在于网络中），8bit上层协议（指示数据部分交给何种运输层协议处理），16bit校验和；第四、五格是成对的源IP地址和目的IP地址。*

*分片：对IP数据报分片是为了适应各种不同的链路层的帧的MTU。分片由端系统和路由器执行，分片重组由目的地的端系统执行。重组的关键是IP数据报首部第二个那三个字段。注意：IP数据报总长度2^16字节，偏移量为2^13字节，所以规定片长度为8字节的整数倍。分片有安全风险，所以之后的IPv6禁止分片。*

*ICMP与IP协议的关系：ICMP通常被认为是IP的一部分，类似于运输层，ICMP报文承载在IP分组的有效载荷中。*

*ICMP的ping程序：程序可以发送ICMP回显请求报文（类型8编码0）到指定主机，目标主机发回一个ICMP回显回答报文（类型0编码0）；*

*通过ICMP实现的Traceroute程序：程序向目的主机发送一系列普通的IP数据报，每个数据报携带具有一个不可达的UDP端口号的UDP报文段。这些数据报的TLL从1开始递增，源主机也为每个数据报启动定时器。第n个数据报到达第n个路由器时，TLL刚好过期，路由器要丢弃该数据报，并发送ICMP告警报文给源主机。当ICMP报文到达源主机时，源主机从定时器得到RTT，从ICMP报文中得到第n台路由器的名字与IP地址。*

## 4.5 路由选择算法

**R21 比较和对照链路状态和距离向量路由选择算法。**

链路状态算法（LS）是全局式路由选择算法，所有结点都知道关于网络连通性和链路费用方面的完整信息，每个结点通过Dijkstra算法求出到任意结点的最低费用路径。

距离向量算法（DV）是分散式路由选择算法。每个结点与邻居结点交换距离向量信息来维护路由表。结点在每次发现与其直接连接的邻居结点的距离向量更新时，更新自己的距离向量估算（即路由表），然后把更新后的距离向量通知给邻居结点，经过多次迭代将收敛到稳定的实际最低费用路径。

比较：① 报文复杂性，LS算法每个结点都要广播其与邻居的链路信息，要发送O(NE)个报文，DV算法只要求邻居结点互相交换链路费用信息；② 收敛速度，LS算法中每个结点独立执行Dijkstra算法，时间复杂度O(N^2)，DV算法每次迭代的动作仅限于邻接的结点，收敛比较慢；③ 健壮性，LS算法中每个结点独立计算与其他结点的最低费用路径，DV算法则依赖于邻居结点得到最低费用路径的估计，所有LS的健壮性更强。

*LS、DV是路由选择算法的分类方法一种（根据算法是全局式的还是分散式的），此外还有② 是静态的还是动态的，静态通常是人工干预调节实现，动态路由选择算法能够根据网络负载和拓扑变化而调整网络路径；③ 是负载敏感的还是负载迟钝的，敏感型算法中，链路费用会动态地变化以反映出底层链路的当前拥塞水平，相反的即迟钝型，因特网采用的都是迟钝型。*

*Dijkstra寻路算法（图搜索）：从起点开始，每次探索临近的、总路径代价最小的且未被访问过的结点，直至全部结点都被访问过。*

*用于DV算法中的Bellman-Ford方程：dx(y) = minv{c(x, v) + dv(y)}，x到y的最短路径是x到众多邻接点v到y最短距离和的最小值，构成一种迭代关系。对应的距离向量****Dx*** *= [Dx(y): y∈N], 其中Dx(y) = minv{c(x, v) + Dv(y)}。*

*DV算法迭代更新中的路由选择环路和毒性逆转（问题：链路更新前z经过y到达x，更新后y到x的费用增加，已经大于z到x的费用，如不采取措施，z仍保持通过y到达x，z、y会反复更新路径费用。可以采取的措施：当z通过y到达x时，在y的转发表中记录的z到x的距离是无穷大，因为y到了z还要折回去，用无穷大代价来避免环路）*

**R22 讨论因特网的等级制组织是怎样使其能够拓展为数以百万计用户的。**

路由器被组织成AS，在一个AS中，所有路由器运行相同的AS内部协议，在跨越AS时需要使用AS间协议。

**R23 每个自治系统使用相同的AS内部路由选择算法是必要的吗？为什么？**

不必要。每个AS之间互相独立，AS内的路由器只需要知道它到其他路由器的最低费用路径即可。

*4.5补充内容：*

*在路由器（AS内部）的转发表中增加一个AS之外的目的地（一个网络前缀）的步骤：① 从AS间协议（如BGP）知道经多个网关可达子网；② 使用AS内部路由选择算法决定到每个网关的最低费用路径的费用；③ 热土豆路由选择：选择具有最小最低费用的网关（意味着可能存在多个可达x的网关和路径）；④ 从转发表确定通向最低费用网关的接口I，将 (x, I) 添加到该路由器的转发表。*

## 4.6 因特网中的路由选择

**R24 回到图4-37，假设D收到来自A的通告：目的子网：[z, w, x …]，下一跳路由器：[C, -, - …]，跳数：[10, 1, 1 …]。D的转发表会改变吗？如果是，应该如何变化？**

不会，新的值不是最低费用路径。

**R25 比较并对照RIP与OSPF使用的通告。**

RIP在邻居路由器之间交换通告，每30秒一次（如果超过180秒没收到邻居节点的通告，则认为邻居结点已故障），RIP（本质是应用层应用进程）通过UDP来传输RIP请求和响应报文。

OSPF要求路由器对AS内的所有其他路由器广播通告，每30分钟一次，每个路由器根据收到的其他路由器的链路信息独立执行Dijkstra算法来维护转发表。

*OSPF优点：① 引入鉴权；② 支持多条相同费用的路径；③ 支持单播、多播等；④ 支持层次结构（可以在AS内划分下层区域，构成嵌套的层次结构）*

**R26 填空题：RIP通告通常宣称到达各目的地的跳数，而BGP更新却宣称到达各目的地的**可达性信息**。**

*BGP功能：从相邻的AS获得子网可达性信息；向AS内所有路由器传播这些信息；基于可达性信息与AS策略，决定AS间路由。*

**R27 为什么在因特网中用到不同类型的AS间与AS内协议？**

关于策略：AS间路由协议是基于策略的，可以根据策略来控制网络路径和流量。在AS内部，一切都是在相同的管理控制名义下进行的，不涉及策略。

关于可拓展性：扩展对于AS间路由协议至关重要，AS内路由协议对此不关注。

关于网络性能：AS间协议更关心策略，而AS内协议不考虑策略，可以更关注网络性能。

AS间、AS内路由选择协议本质上就不同。

**R29 定义和对比下列术语：子网，前缀，BGP路由。**

子网：通过路由器的接口，将一个大型网络进行划分，从而产生若干个独立的网络区域，叫做子网。

前缀：用CDIR格式来表示的一个子网或者子网集合。

BGP路由：带有BGP属性的前缀叫做一条BGP路由，用于路由器之间的BGP会话通告。

**R30 BGP是怎样使用NEXT-HOP属性的？是怎样使用AS-PATH属性的？**

NEXT-HOP是沿着最低费用路径的AS之外的第一台服务器的IP地址。指示AS内路由器到达目的子网x的最低费用路由。

AS-PATH属性包含了通告已经通过的AS的列表，防止循环通告，如果一台路由器发现自己所在AS被包含在AS-PATH中，路由器将拒绝该通告。

**R31 描述一个较高层ISP的网络管理员在配置BGP时是如何实现策略的。**

书中例子，选择性通告AS之间的路径。

## 4.7 广播和多播路由选择

**R32 通过多个单播（N次单播）实现广播抽象与通过支持广播的单个网络（路由器）实现广播抽象之间有什么重要区别？**

N次单播要求源结点分别给N个网络结点发送点到点的广播分组。这种方法效率低，存在同一条链路上发送着多个相同分组的情况。此外，还要求源结点必须知道所有结点的地址；支持广播的网络中的结点仅通过邻居结点传播广播分组。

**R33 关于广播通信的3种一般方法（无控制洪泛、受控洪泛和生成树广播）中的每一种，下列说法是正确的吗？（可以假设分组不会因为缓存溢出而丢失，所有分组以它们发送的顺序交付给链路）**

**A 一个结点可能接收到同一个分组的多个副本。**

**B 一个结点可能通过相同的出链路转发多个分组的副本。**

a. 在无控制洪泛和受控洪泛方法中都可能接收到同一个分组的多个副本。

b. 在无控制洪泛方法中可能通过相同的出链路转发多个分组的副本。

*无控制洪泛在环路上会重复地发送和接收广播分组的副本。受控洪泛和生成树广播都可以避免环路，受控洪泛是丢弃已转发过的分组副本（序号控制洪泛）或者丢弃不由最短路径发来的分组副本（反向路径转发，RPF），生成树广播是不向生成树结构不相连的结点发送分组副本。*

*RPF方法中，广播源沿着到每个结点的最短路径形成一个数据结构，每个源都不一样。生成树方法中，基于一个中心结点建立一棵共享的生成树。*

**R34 当一台主机加入一个多播组时，它必须将其IP地址改变为它所加入的多播组的地址吗？**

不需要。主机的单播地址独立于它所参与的多播组地址。

*多播的目的地址为一个特殊的IP地址，它位于224.0.0.0 - 239.255.255.255中。*

**R35 IGMP和广域多播路由选择协议所起的作用是什么？**

一台主机通过IGMP通知一台多播路由器想要加入或退出多播组；多播路由选择协议能协调遍及因特网内的多播路由器，以便多播数据报能路由到目的地。

*因特网多播的两个组件，IGMP（因特网组管理协议）和多播路由协议。IGMP组织多播组；多播路由协议负责多播分组的转发。*

**R36 在多播路由选择场合中，一棵组共享的树与一棵基于源的树之间有什么区别？**

组共享树是所有组成员都使用这棵树的路径来发送/接收多播数据报；基于源的树是指每个发送结点都有一棵独立的以自己为根的树，根据这棵树来发送多播数据报。

*每个多播源构建一棵树，借助RPF来传播多播分组，对于组外路由器，采用剪枝来避免流量传输，这是DVMRP的算法。*

# 第五章 链路、接入网和局域网

## 5.1-5.2 链路层概述 | 差错校验和纠正技术

**R1 考虑在5.1.1节中的运输类比。如果一个乘客类比为一个数据报，什么类比成链路层帧？**

汽车、火车等运输方式。

**R2 如果因特网中所有链路都提供可靠的交付服务，TCP可靠传输服务是否多余？为什么？**

链路层可靠服务能保证链路发送的链路层帧能被链路另一端正确接收，主要目的是纠正差错，应用在易于产生高差错率的链路（无线）。但是IP协议提供尽力而为服务，在网络层的接收端收到的IP数据报可能是乱序的、不完整的或是冗余的，因此传输层仍要提供可靠传输服务，TCP提供可靠服务的手段是确认/重传，与链路层不同。

**R3 链路层协议能够向网络层提供哪些可能的服务？在这些链路层服务中，哪些在IP中有对应的服务？哪些在TCP中有对应的服务？**

成帧（IP、TCP）；链接接入；可靠交付（TCP）；差错检测、校正（IP、TCP）；

*5.2 补充内容*

*差错检验的3种技术：奇偶校验，校验和，循环冗余校验。奇偶校验比较简单，采用二维奇偶校验还能纠正最多一位的差错。*

*奇偶校验：数0或1的个数，因此二维奇偶校验不仅可以检查差错，还可以定位出错的编码的为止。*

*校验和方法：把数据D（d bit）作为一个整数序列（k bit），将整数加起来，得到的和用作差错校验比特。因特网中，数据的字节被作为16bit的整数对待并求和。得到的和的反码形成了携带在报文段首部的因特网校验和。接收方同样用数据求和取反码，校验是否有差错。主要应用于校验传输层，网络层的分组首部。算法通过上层应用软件实现，所以检验算法应该尽可能简单快速。*

*循环冗余校验（CRC）；发收双方约定一个G（r+1 bit），要发送的原始数据为D（d bit）。在发送方，通过求D\*2^r/G得到的余数R（r bit），拼接[D, R]一起发送出去。接收方根据[D, R]这d+r位比特除G，如果有余数，说明传输的数据出错了。CRC能够检测小于r+1比特的差错。链路层的差错检验在适配器中用专用的硬件实现，所以能快速执行更复杂的CRC操作。*

## 5.3 多路访问链路和协议

**R4 假设两个结点同时经一个速率为R的广播信道开始传输一个长度为L的分组。用Dprop表示两个结点间的传播时延。如果Dprop < L/R，会出现碰撞吗？为什么？**

画一个时空图可知，A、B同时发送分组，传播时延比传输时间短，意味着B的信号到达A时，A还没有完全发送完分组，发生碰撞。

**R5 在5.3节列出了4中广播信道的4种希望特性。这些特性哪些是时隙ALOHA所具有的？令牌传递具有这些特性中的哪些？**

当仅有一个结点在发送数据时，它拥有全部的Rbps吞吐量。时隙ALOHA满足该特性。令牌传递方法由于轮流机制存在令牌的传递时延，使得结点吞吐量小于R；

当有M个结点要发送数据时，每个结点吞吐量为R/Mbps。时隙ALOHA的出现冲突随机重传机制导致它无法满足该特性。令牌传递是轮流的，每个结点都能利用好令牌的发送机会，满足该特性；

协议是分散的，不会因为一个结点故障导致网络崩溃。时隙ALOHA是分散的，每个结点独立地感知时隙是否冲突，在冲突时自行等待以避免下一次碰撞。令牌传递不是分散的，每个结点发送数据必须依赖于令牌，当出现某个故障结点占用令牌时，网络即崩溃。

协议是简单的。时隙ALOHA、令牌传递方法都是可以简单实现的。

*多路访问协议的主要3个分类：信道划分协议（定义一种信道平均分配的机制，主要有TDM、FDM、CDMA），随机接入协议（个节点独立地往总线发送数据，在发生信号碰撞时等待一个随机的时间再重传，主要有ALOHA、时隙ALOHA、CSMA、CSMA/CD），轮流协议（每个结点都有发送数据的机会，如果当前结点不发送数据，则把机会传递给邻居结点，主要有轮询协议、令牌传递协议）*

*CSMA、CSMA/CD：载波侦听——讲话之前先听，如果有人在说，则等待；碰撞检测——如果与他人同时说话，则停止说话。*

*轮询协议、令牌传递协议：轮询需要主结点来控制各个结点的发送过程，令牌则是以邻居结点之间传递令牌的方式获得发送数据的机会。*

**R6 在CSMA/CD中，在第5次碰撞后，结点选择K=4的概率有多大？结果K=4在10Mbps以太网上对应于多少秒的时延？**

第5次碰撞后，K的可选数的集合有32个元素，K=4的概率是1/32。

K=4时，即4个512比特时间，在10Mbps以太网种的时延时0.2048毫秒。

二进制指数后退算法：n为结点发送分组的碰撞次数，由n得到一个含2^n个整数的集合{0, 1, 2, …, 2^n -1}，K表示结点碰撞后要等待的时间单位，K从整数集合中选一个值，等待时间为K\*512比特时间，然后结合链路传输速度求出实际时间。

**R7 使用人类在鸡尾酒会交互的类比来描述轮询和令牌传递协议。**

轮询协议：主持人（主结点）轮流告诉每个发言者他们是否可以发言以及发言多久。

令牌传递协议：只有拿到麦克风的发言者才可以发言，结束发言后，传递麦克风给下一位发言者。

**R8 如果局域网有很大的周长时，为什么令牌环协议将是低效的？**

当网络周长很大，则令牌的传递就会占用很大的时延，导致网络的效率降低。

## 5.4 交换局域网

**R9 MAC地址空间有多大？IPv4的地址空间？IPv6的地址空间呢？**

MAC地址有48bit，地址空间有2^48个；IPv4：2^32；IPv6：2^128；

**R10 假设结点A、B、C都连接到同一个广播局域网上。如果A向B发送数千个IP数据报，每个封装帧都有B的MAC地址，C的适配器会处理这些帧吗？如果A用广播地址来发送这些帧，C的适配器将会有什么动作？**

当A发送的帧所用的地址是B的地址，因此C会收到该帧，但不会处理，直接丢弃。当A发送的帧所用的地址是广播地址，C会处理并传递给上层协议。

**R11 ARP查询为什么要在广播帧中发送呢？ARP响应为什么要在一个具有特定目的地的MAC地址的帧中发送呢？**

ARP查询报文用于寻找当前ARP表中没有记录的IP地址与对应的MAC地址，只能通过广播来寻找。当目的主机适配器被发现时，交换机知道了源主机的MAC地址，因此它只需要向源主机发送ARP响应报文即可。

**R12 对于图5-19中的网络，路由器有两个ARP模块，每个都有自己的ARP表。同样的MAC地址可能在两个表中都出现吗？**

不可能，MAC地址是唯一的。不存在同一个主机的链路层适配器同时连接两个子网的情况。

*在子网内，链路层通过ARP协议寻址；在子网之间，链路层还是需要通过网络层的IP地址来找到指定的子网，分组到达目的子网后再通过ARP协议找到目的主机。*

**R13 比较10BASE-T、100BASE-T和吉比特以太网的帧结构。它们有什么不同？**

这三种以太网技术具有相同的帧结构。

*以太网帧结构：8字节前同步码（用来“唤醒”交换机并同步时间，分组在传送过程可能存在漂移，所以需要同步），6字节的成对的源与目的地址，2字节类型（用于指示上层协议），46~1500字节的数据部分（如果IP数据报的长度达不到46字节，需要填充。如果超过1500字节，需要在发送端进行分片），4字节的CRC（适配器会直接丢弃不满足的帧）。*

*以太网标准化命名（10BASE-2、100BASE-T、1000BASE-LX、10GBASE-T）：前面的10~10G代表以太网的传输速率，BASE指基带以太网，最后的字母表示物理媒介，T指双绞铜线，FX、SX、BX表示光纤。*

**R15 在一个支持802.1Q的协议交换机上能配置的VLAN的最大数量是多少？**

802.1Q协议中的帧结构比初始以太网帧结构多了4字节VLAN标签（2字节的标签协议标识符，3bit优先级字段，1bit严格标准格式标识字段，12bit VLAN标识符字段），12bit VLAN标识符，意味着支持2^12，即4096个VLAN。

*VLAN：交换机有很多接口，但是这些接口没有隔离性，管理员可以定义多个虚拟局域网（本身有个默认的VLAN），然后把交换机的接口分配到这些VLAN上，实现多个隔离的VLAN。当需要进行VLAN间通信时，通过外接路由器来实现。当一台交换机接口不够时，通过外接一台交换机来拓展，① 每个VLAN外接一条链路到新交换机，② 所有VLAN共用VLAN干线，使用802.1Q协议来拓展。*

**R16 假设支持K个VLAN组的N台交换机经过一个干线协议连接起来。连接这些交换机需要多少端口？**

2N-2个端口，N台交换机串在一起，所以有N-1段链路，因此需要2N-2个端口。

*5.4 补充内容*

*交换机功能（区别广播域的集线器）：转发和过滤。转发依赖于交换机表（项：MAC地址，接口，时间）。当交换机接到的帧目的地址与表不匹配，则广播帧，当匹配时直接转发到指定接口（的缓存）。交换机表项的更新方式，每接收一个帧，记录该帧的源MAC地址、接口号以及接收时间。*

*互联设备的典型特色对比：路由器（流量隔离，不支持即插即用，优化路由），交换机（流量隔离，即插即用，不支持优化路由），集线器（仅支持即插即用）。*

*5.5 链路虚拟化：网络作为链路层 补充内容*

*MPLS（多协议标签交换）：在IP路由器（特制的MPLS使能的路由器）的基础上，使用固定长度的标签代替IP地址来路由。融合了虚电路网络和数据报网络。优点：标签交换比IP寻址效率更高，网络管理员可以介入多条虚电路以实现流量工程，主动引导流量。*

*5.6 数据中心网络 补充内容*

*数据中心网络设备：边界路由器，介入路由器，多层的交换机，机柜（TOR交换机，主机）。*

*数据中心网络组网方式：路由器交换机等级结构，全连接拓扑，模块化数据中心。*

*5.7 Web页面请求的过程（关注链路层）*

*假设链路：学校局域网（Bob的便携主机 – 交换机 – 路由器（运行着DHCP服务器） - ISP网络（路由器 – DNS服务器） - 内容提供商网络（路由器 – Web服务器）。概要过程：① Bob的主机接入局域网，从DHCP服务器获得IP、网关、掩码等信息，另外获得网关路由器的MAC地址（细节：UDP、广播、ARP）；② Bob访问网站，从DNS服务器获得网站IP（细节：DNS服务、域间路由、域内路由）；③ Bob的主机与网站Web服务器建立TCP连接，进行交互（细节：套接字、三次握手）。*

*用到UDP的过程：DHCP请求-响应（68-67）、DNS查询-回答（53）；用到TCP的过程：针对HTTP的连接握手（80）；*

*用到广播的过程：DHCP、ARP、域内路由选择OSPF；*

# 第六章 无线网络和移动网络

## 6.1 概述

**R1 一个无线网络运行在“基础设施模式”下的含义是什么？如果某网络没有运行在基础设施模式下，那么它运行在什么模式下？这种运行模式与基础设施模式之间有什么不同？**

“基础设施模式”是指的主机和基站关联的模式。如果没有运行在基础设施模式下，就运行在自组织网络中。自组织模式没有基站，主机自己提供路由选择、地址分配、DNS服务等服务。

**R2 在6.1节的分类法中，所确定的4种无线网络类型各是什么？**

单跳，基于基础设施（WiFi、蜂窝网络）；单跳，无基础设施（蓝牙）；多跳，基于基础设施（需要无线中继结点才能连接到基站，比如无线网状网络）；多跳，无基础设施（移动自组织网络、车载自组织网络）。

## 6.2 无线链路与网络特征

**R3 下列类型的无线信道损伤之间有什么区别：路径损耗，多径传播，来自其他源的干扰？**

路径损耗：电磁波穿过物体和在空间中减弱和扩散；

多径传播：电磁波由于反射产生了不同长度的路径，使得接收信号变的模糊；

来自其它源的干扰：来自发送源之外其他电波源的干扰。

**R4 随着移动结点离基站越来越远，为了保证传送帧的丢失概率不增加，基站能够采取的两种措施是什么？**

发送方增加传输功率，功率越强，信噪比SNR越少，出错的概率越低。

使用更低比特传输率的调制技术，降低传送速率，单位时间传送的数据越少，出错的概率越低。

*6.2 补充内容*

*CDMA：通过划分编码空间来互传数据。协议中，要发送的每个比特都通过乘以一个信号（编码）的特殊比特来进行编码，这个信号的变化速率比数据的比特序列变化快（每个原始数据的比特都对应一串编码比特），发收双方先预先约定一个编码，数据信号发送前先经过编码转换，接收到数据后再用编码还原回原始数据。*

*CDMA的抗干扰：A、B同时给接收方发送数据，将发生加性干扰，接收方可以用A的编码还原出A的原始数据，B的同理。接收方一次只能处理一个发送源（要么A要么B）的信号。*

## 6.3-6.4 WiFi：802.11 无线LAN | 蜂窝因特网接入

**R5 描述802.11中信标帧的作用。**

802.11标准要求每个AP周期性地发送信标帧，每个信标帧包含该AP地SSID和MAC地址，使无线站点能发现到AP，进而关联AP。

AP发送信标帧刺激无线站点扫描信道地过程是被动扫描。主动扫描则是无线站点向范围内所有AP广播探测请求帧，然后AP用一个探测响应帧应答该请求帧。之后站点选择一个AP进行关联，关联之后还要互发关联请求/响应帧进行二次握手（类似DHCP）。

**R6 判断题：802.11站在传送一个数据帧前，必须首先发送一个RTS帧并收到一个对应的CTS帧。**

错，只有帧长超过门限值的数据帧才会使用RTS/CTS序列。

**R7 为什么802.11中使用了确认，而有线以太网中却未使用？**

无线信道存在较高的勿比特率，因此使用确认/重传机制。有线以太网正确收到的概率较高，因此不使用确认。

**R8 判断题：以太网和802.11使用相同的帧格式。**

错，二者的帧格式完全不相同，只有MAC地址用了6字节这个共同特性。

*802.11帧格式在基础设施模式下用到三个地址，地址1目的MAC，地址2源MAC，地址3网关MAC。*

**R9 描述RTS门限值的工作过程。**

仅当数据帧长超过门限值时，才使用RTS/CTS序列来预约数据帧发送时间。

*RTS/CTS帧用于解决隐藏终端问题，主机在先广播自己的RTS帧，在信号范围内的所有站点都感知到主机想发送数据帧，AP收到RTS帧后广播CTS，因此，不在源主机信号范围内的其他主机也感知到了它的存在和发送动作。其他主机将会推迟发送自己的帧，避免碰撞（CSMA/CA）。为了提高效率，并不是任何时候都要用到RTS/CTS帧序列，而是在数据帧长度超过门限值时才启用。*

**R10 假设IEEE 802.11 RTS和CTS帧与标准的DATA和ACK帧一样长，使用CTS和RTS帧还会有好处吗？**

没有好处，此时使用RTS/CTS还不如直接使用数据帧，如果没有收到确认再重传。

**R11 6.3.4节讨论了802.11移动性，其中无线站点从一个BSS到同一子网中的另一个BSS。当AP是通过交换机互联时，为了让交换机能适当地转发帧，一个AP可能需要发送一个带有哄骗的MAC地址的帧，为什么？**

因为需要更改交换机的转发表，使交换机转发帧到新的AP中。

**R12 在某蓝牙网络中的一个主设备和在802.11网络中的一个基站之间有什么不同？**

蓝牙的主设备和从设备在物理结构上没有不同，都是无线站点，且其它从设备也可以作为主设备。

而802.11网络中的AP有着特殊的物理结构，只有它与外部网络相连，其他无线站点不能作为AP使用。

**R13 在802.15.4 ZigBee标准中超级帧的含义是什么？**

超帧相当于一个往复出现的时间周期，在这个时间周期中有竞争时隙，确保时隙和非活跃时隙，以便各种不同类型的设备能正常通信。

**R14 在3G蜂窝数据体系结构中，“核心网”的作用是什么？**

3G核心网将无线电接入网连接到公共因特网。

*3G系统体系结构：无线电接入网（无线电接口- RNC）-核心网通用分组无线服务-公共因特网；*

*GPRS（通用分组无线服务）：一种蜂窝数据服务；*

*核心网两类结点：SGSN（服务GPRS支持结点）、GGSN（通用GPRS支持结点）；*

**R15 在3G蜂窝数据体系结构中，RNC的作用是什么？在蜂窝语音网中RNC起什么作用？**

RNC（无线电网络控制器）控制几个基站，分别连接MSC（蜂窝语音服务核心网）和SGSN（蜂窝数据服务核心网），共享相同的第一条/z最后一跳无线电接入网；

## 6.5-6.6 移动管理：原理 | 移动IP

**R16 如果某结点与因特网具有无线连接，则该结点必定是移动的吗？试解释之。假设一个使用膝上型电脑的用户携带电脑绕着她的住所散步，并且总是通过相同的接入点接入因特网。从网络的角度看，这是移动用户吗？试解释之。**

物理空间位移与网络接入方式及移动性没有关系。与因特网无线连接的结点不一定是可以移动的，例如接入无线网络的固定主机。便携主机在空间中位移，如果IP没变，意味着它在网络层是没有移动的，如果连接的AP不变，意味着在链路层也没有移动。

**R17 永久地址与转交地址之间的区别是什么？谁指派转交地址？**

永久地址指移动结点的固定地址，即使结点移动到因特网的任何位置，该地址永久固定，其它主机通过永久地址想与移动结点建立连接；转交地址（COA）指移动结点接入到外部网络时临时分配的地址，用于移动结点在外部网络的路由选择与数据传输。

**R18 考虑经移动IP的一条TCP连接。判断：在通信者和移动主机之间的TCP连接阶段经过该移动用户的归属网络，但数据传输阶段直接通过该通信者和移动主机，绕开了归属网络。**

当间接路由选择时，数据报必须经过归属网络，此时说法错误；当直接路由选择时，只在最初寻址阶段需要访问归属网络，之后的数据传输阶段不再经过归属网络，此时说法正确。

6.6 补充内容：

因特网移动IP（代理发现、代理注册、间接路由）：外部代理广播代理通告，分配COA；移动站点收到代理通告，给外部代理发送代理注册请求；外部代理记录注册请求中的地址信息，向归属代理转发注册请求；归属代理验证注册请求，返回注册响应；外部代理转发注册响应；因特网上的通信者通过绕到归属代理与移动结点进行通信。

## 6.7 蜂窝网络中的移动性管理

**R19 在GSM网络中，HLR和VLR的目的是什么？移动IP的什么要素类似于HLR和VLR？**

HLR：归属位置注册器，包含每个用户的个人信息和当前的位置信息。相当于移动IP中的归属代理。

VLR：访问者位置注册，包含当前在该网络中的用户的表项，协调到达或离开的移动用户的呼叫建立。相当于移动IP中的外部代理。

*蜂窝电话网络与移动IP网络有很多相似之处。*

**R20 在GSM网络中，锚MSC的作用是什么？**

锚MSC是呼叫首次开始时移动用户所访问的MSC。之后用户移动时，都用该MSC中转（类似直接路由的锚外部代理）。

## 6.8 无线和移动性：对高层协议的影响

**R21 为了避免单一无线链路降低一条端到端运输层TCP连接的性能，能够采取的三种方法是什么？**

在无线链路中使用重传协议；发送方知晓无线链路，从而调整拥塞控制策略（TCP拥塞丢包与无线ARQ丢包区分）；分离传输层TCP连接为有线和无线两段。

# 第七章 多媒体网络

## 7.1 多媒体网络应用

**R1 重新构造7-1表，满足4Mbps视频，每20秒看一幅100KB图片，以及200kbps音频流。**

应用 比特率 67分钟传输的字节

Victor Video 4Mbps 2GB

Frank Facebook 40kbps 20MB

Martha Music 200kbps 100MB。

**R2 描述视频中有两种类型的冗余，讨论如何能够利用它们进行有效压缩。**

空间冗余：视频中一幅图像的内部冗余。

时域冗余：一幅图像和后续图像的重复。

压缩方法：重复的内容只存储一次。

**R3 假定一个模拟音频信号每秒抽样16000次，并且每个样本量化为1024级之一，该PCM数字音频信号的比特率将是多少？**

16000/s \* 1024 = 16Mbps。

**R4 多媒体应用能够被分为三种类型。阐述它们的名称并对每种类型进行描述。**

流式存储音频和视频，客户播放视频的同时从服务器接收视频的后续部分，流式内容是提前录制的，客户能自由操作；会话式IP语音和视频，时延敏感但容忍丢包；流式实况音频和视频，基于应用层多播技术，其他许多技术都类似于流式存储媒体。

## 7.2 流式存储视频

**R5 流式多媒体系统能够分为三种类型。阐述它们的名称并对每种类型进行描述。**

UDP流，使用UDP传输，使用很小的客户端缓存；HTTP流，使用HTTP传输；适应性HTTP流：使用HTTP传输，媒体被编码为几个版本，用户根据带宽来选择。

**R6 列举UDP流的三种缺点。**

由于无法预测带宽，恒定速率的UDP流不能提供连续的播放；依赖媒体控制服务器（用于处理请求和追踪状态），增加了系统复杂度；UDP流量会因为防火墙阻塞而不可用。

**R7 对于HTTP流，TCP接收缓存和客户应用缓存是相同的东西吗？如果不是，它们如何交互？**

客户缓存从TCP缓存中读取字节，放入客户缓存中，TCP缓存再删掉这些字节。

**R8 考虑对于HTTP流的简单模型。假设服务器以2Mbps的恒定速率发送比特，并且当已经接收到800万比特时开始播放。初始缓存时延tp是多少？**

800万bit 即 8Mb，初始缓存时延为 8Mb / 2Mbps = 4s。

**R9 CDN通常采用两种不同的服务器放置原则之一。阐述它们名称并简要描述这两种原则。**

深入原则，在ISP接入网中部署服务器集群，目标是靠近端用户，改善时延和吞吐量，但是集群管理维护成本高；邀请做客原则，在少量网络关键位置部署集群，通过高速网络与ISP连接，降低维护管理开销，但是可能以时延和吞吐量为代价。

**R10 在7.2.4节中描述了几种集群选择策略。哪个找到了相对客户的LDNS的一个好集群？哪个找到了相对于客户自己的好集群？**

对LDNS的好集群：地理上最为邻近方法，实时测量方法（时延上最短）；对客户的好集群：IP任播方法（利用BGP找最短路由）。

**R11 除了诸如时延、丢包和带宽性能等网络相关的考虑，设计一种集群选择策略时有许多附加的重要因素要考虑。列举之。**

集群上的负载，ISP交付成本等。

## 7.3 IP语音

**R12 端到端时延和分组时延抖动的区别是什么？分组时延抖动的原因是什么？**

端到端时延是路由器中的传输，处理，排队时延链路中的传播，端系统中的处理时延的总和，而时延抖动描述的是端到端时延的变化情况；分组时延抖动的关键原因是路由器中的排队时延是变化的。

**R13 为什么在预定的播放时间之后收到的分组被确认为是丢失的？**

因为播放时间已经过去了，过期的分组对应用程序没有任何意义。

**R14 本节描述了两种FEC方案，简要地总结它们。这两种方案通过增加开销而增加了流的传输速率。交织技术也会增加传输速率吗？**

方案1，每发送n个块之后发送一个由前n个块异或的冗余块；方案2，每个块发送后接着发送它的低音质版本。

交织技术不会增加流的传输速率。

*交织方案：发送方在传输之前对音频数据单元重新排序，使得最初相邻的单元在传输流中以一定距离分离开来。在接收方重新组合，即使丢包，相当于在每个分组中丢失一个音频数据单元，总体上看没有损伤分组（只是得到了质量稍差的分组）。它不需要像FEC那样发送冗余的分组，导致传输速率的增加。*

*差错掩盖：在接收方生成一个音频数据来填补丢失的分组，企图让听者分辨不出。*

## 7.4 实时会话式应用的协议

**R15 接收方如何识别在不同会话中的不同RTP流？同一个会话中的不同流是怎么识别的？**

不同会话通过IP和端口号来识别；同一个会话的不同流用同步源标识符识别。

**R16 SIP注册器的作用是什么？它与移动IP中的归属代理的作用有什么差异？**

SIP注册器：任何时候用户在设备上发起SIP应用时，该应用给注册器发送一个SIP注册报文，通知注册器它现在的IP地址。与SIP代理交互，重定向INVITE报文。

SIP注册器只在连接时指示用户的IP地址，真正开始通信之后，SIP注册器就不参与会话了；归属代理在直接路由的场景下与SIP注册器类似，而在间接路由的场景下将在通信过程中一直充当转交的作用。

## 7.5 支持多媒体的网络

**R17 非抢占优先级排队、抢占优先级排队分别是什么？抢占优先级排队对于计算机网络有意义吗？**

在抢占优先级排队中，目前有低优先级分组正在传输，高优先级分组也可以打断该传输，直接开始传输高优先级分组。

抢占优先级排队对于计算机网络有意义，因为可以做到更快的传输非常重要的分组。

**R18 举一个非保持工作的调度规则的例子。**

时分复用就是非保持工作的调度规则。不管这个时隙是否有数据在传输，时隙都是完整的流逝了，不会被跳过。

**R19 举例说明你的日常生活中所经历的FIFO、优先权、RR和WFQ的排队。**

FIFO：常规的排队。

优先权：坐飞机分VIP舱位。

RR（呼叫一旦开始就要确保给定的服务质量）：类似预约服务。

WFQ（按权值提供服务，这个全职可以是比例可以是概率）：类似于数人头划分资源配额。

# 第八章 计算机网络中的安全

## 8.1 什么是网络安全

**R1 报文机密性和报文完整性之间的区别是什么？通信过程中二者只有其一可以吗？**

机密性要求仅有发送方和期望的接收方能够理解报文内容；完整性要求报文内容不能被篡改；可以，在具体场景具体分析，在网络层链路状态路由选择算法中，路由器并不关心报文机密性，只关心报文完整性。

**R2 因特网实体（路由器、交换机、端系统等）经常需要安全通信。举例。**

路由器-路由器：交换链路状态信息或者距离向量时，需要安全通信，不能被篡改。

主机-Web服务器：浏览网页需要安全通信，不能被篡改。

主机-邮件服务器：发送邮件需要安全通信，保密且不能被篡改。

## 8.2 密码学的原则

**R3 从服务的角度，对称密钥系统和公开密钥系统之间一个重要的差异是什么？**

在对称密钥系统中通信双方的密钥是相同的并且是秘密的。在公开密钥系统中，使用一对密钥通信，一个密钥是公开的，一个密钥只有一方所知。

*对称密钥密码体制：凯撒密码（按字母表偏移得到新的字母映射，但是可用的密钥配对只有25个（或者是字符表的长度））；单码代替密码（凯撒密码的乱序版本，可用的密钥配对有2^26个）；多码代替密码（交替使用单码代替密码）。*

**R4 假定某入侵者拥有一个加密报文以及该报文的解密版本。这个入侵者能够发起已知密文攻击、已知明文攻击和选择明文攻击吗？**

能发起选择明文攻击；

*唯密文攻击：入侵者只能截获到密文，不了解明文报文的内容。*

*已知明文攻击：入侵者知道明文-密文的一些匹配。*

*选择明文攻击：入侵者能够选择某一明文报文并得到该明文报文对应的密文形式。*

**R5 考虑一个8位块密码。这个密码有多少种可能的输入块？有多少种可能的映射？如果我们将每种映射视为一个密钥，则该密码具有多少种可能的密钥？**

2^8种可能的输入块。有(2^8)!种可能的映射。

*块密码（对称密码范畴）：把报文分成k比特的块，每块独立加密。流行的块密码技术：DES、3DES、AES。缺点：相同的明文块得到相同的密文块，容易被猜出明文；*

*引入CBC（块密码链接）技术：改进1，每个块加密之前先与一个随机数（k比特）异或运算, 公式c(i) = Ks( m(i) ⊕ r(i) )，这样每个明文相同的块加密后都不同，之后发送方把密文和随机数发送给接收方。缺点：需要发送的内容增加了一倍；改进2，用c(i-1)代替r(i)，c(i) = Ks( m(i) ⊕ c(i-1))，因此只需要IV（初始向量）c(0)这一个随机数。*

**R6 假定N个人中的每个人都和其他N-1个人使用对称密钥密码通信。任两人（i，j）之间的所有通信对该N个人的组中的所有其他人都是可见的，且该组中的其他人都不应当能够解密他们的通信。则这个系统总共需要多少个密钥？现在假定使用公开密钥密码。此时需要多少个密钥？**

使用对称密钥时，需要N(N-1)/2个密钥；使用公开密钥密码，需要2N个密钥。

**R7 假定n=10000，a=10023，b=10004。使用等同的模算术计算 (a\*b) mod n。**

(a\*b) mod n = [(a mod n) \* (b mod n)] mod n。所以结果为23\*4=92。

*RSA算法：算法基础（mod运算）；步骤：选择两个素数p、q，得到n=pq，z=(p-1)(q-1)，选择e、d满足ed mod z = 1。得到公钥K +=(n, e)，私钥K -=(n, d)。加密过程，使用公钥计算c=m^e mod n。解密过程，使用私钥计算m=c^d mod n。*

*会话密钥：RSA算法次方和求模计算效率太低，通常仅利用RSA算法来加密对称密钥Ks（即会话密钥），通信过程使用会话密钥来加解密报文。*

## 8.3-8.4 报文完整性和数字签名 | 端点鉴别

**R9 散列以何种方式提供比校验和（如因特网校验和）更好的报文完整性校验？**

采用更强有力的散列函数，比如报文摘要算法MD5、SHA-1等。

*MD5编码过程：填充（假设原始报文m长b bit，在b+1位之后填充1及若干0，直到满足b‘ mod 512 = 448）；添加64bit信息（在末尾添加64bit指示原始报文长度b，最后得到的报文M的长度B恰好被512整除）；初始化累加器（报文M按512bit分成N个分组M(i)，i∈[1, N]，每个分组分成16个小组Xi(j)，j∈[1, 16]，每个小组长32bit，即4字节，算法提供一个128bit初始摘要（分成4等分）及4个函数）；循环（依次将Xi(j)代入循环计算过程，最后得到新的128bit摘要）；原报文分成N个分组，有N次主循环。一个分组分成16个小组，每小组需要4次函数运算，因此主循环内有64次小循环。总共循环N\*64次。*

*破解MD5：指的是尝试枚举所有可能的报文来得到与目标摘要匹配的报文摘要，即碰撞；*

**R10 如何解密某报文的散列来得到初始报文？**

不可能。无论初始报文是什么，散列得到的结果（比如MD5摘要）长度固定，散列结果是不可逆的。

**R11 考虑MAC算法（图8-9）的一种变形算法，其中发送方发送（m，H(m)+s），这里H(m)+s是H(m)和s的级联。该变形算法有缺陷吗？为什么？**

有缺陷；把s直接暴露在报文中，让窃听者获取了s，不再是秘密。丢失了鉴别虚假报文的功能。

*图8-9的MAC（报文鉴别码）算法：已知通信双方都约定级联s，通过发送拓展报文(m, H(m+s))，用以(m, H(m))，避免入侵者的伪造。H(x)的值就是MAC。*

**R12 一个签名的文档是可鉴别的和不可伪造的，其含义是什么？**

可证实的：必须能够证明由某个人在一个文档上的签名确实是由该人签署的；无法伪造的：只有该人能够签署那个文件。

**R13 公钥加密的报文散列以何种方式比使用公钥加密报文提供更好的数字签名？**

公钥直接加密报文计算量太大，耗时太长。而只加密散列计算量不大。

**R14 假设certifier.com生成一个用于foo.com的证书。通常这个证书将用certifier.com的公钥加密。这种说法正确吗？**

错误，应该用certifier.com私钥来加密。

*CA生成证书以及Bob与Alice通信过程（原则——私钥签名，公钥验签）：CA向所有人发布自己的公钥，CA也知道所有人的公钥。CA对Bob的公钥进行签名，这个签名就是Bob的证书；Bob向Alice发送Bob使用私钥签名过的报文和CA的证书，Alice使用CA的公钥验签，从证书中提取Bob的公钥，再对Bob的报文进行验签。*

**R15 假设Alice有一个准备发送给任何请求者的报文。数以千计的人要获得Alice的报文，但每个人都要确保该报文的完整性。在这种情况下，基于MAC和基于数字签名的完整性方案哪个更合适？为什么？**

基于数字签名的更合适，因为MAC要求Alice和每个人有独立的鉴别密钥。

**R16 在某端点鉴别协议中，使用不重数的目的是什么？**

防止回放攻击。

*回放攻击（playback attack）：Trudy只需要窃听Alice的通信，并记录下该口令的加密版本，并向Bob回放该口令的加密版本，以假装她就是Alice，因此Bob不能区分Alice的初始报文和Trudy的回放报文。因此Bob需要判断与Alice的会话是否仍活跃，引入不重数（nonce），指示生命周期中只使用一次的数，用于即时证明Alice是活跃的，避免回放攻击。*

*不重数的使用：① Alice向Bob发送身份认证报文；② Bob返回一个不重数R；③ Alice加密这个不重数，再发送给Bob；④ Bob解密该不重数，如果一致，说明Alice是活跃的，身份为真。*

**R17 我们说一个不重数是一个在生存期中只使用一次的值，这意味着什么？其中的生存期是指谁的？**

在协议的生存期内只使用一次。

**R18 基于HMAC的报文完整性方案易受重放攻击影响吗？如果是，能够在方案中综合一个不重数来去除这种脆弱性吗？**

会的；在HMAC后面附加上，改成H(m+s+R)。

## 8.5-8.8 安全电子邮件 | 使TCP连接安全：SSL | 网络层安全性：IPsec和虚拟专用网 | 使无线LAN安全

**R19 假定Bob从Alice处接收一个PGP报文。Bob怎样才能确定Alice（而不是别人）生成了该报文？**

PGP使用数字签名验证完整性。Bob使用Alice的公钥验签，解密得到散列值（也就是报文摘要），再与报文内容得到的散列值相比较，如果一致，就能验证这个报文来自Alice。

*PGP：一个电子邮件加密方案。*

*电子邮件的安全（应用层安全例子）：机密性（会话密钥机制：使用对称密码对报文加密，使用公开密钥通知对称密钥）；报文完整性和端点鉴别（使用散列函数生成报文摘要，连同报文一起加密（私钥签名）后发送出去，接收方验签，对比报文摘要与接收方自己生成的报文摘要，判断报文完整性以及对方的真假）；*

**R20 在SSL记录中，有一个字段用于SSL序号。这种说法是正确的吗？**

错误，序号只用来计算MAC，不包含在报文内。

*SSL加密：SSL记录格式中，头部的类型、版本、长度字段不加密，而使用发送方的会话密钥加密数据和MAC部分。设M为发送方MAC密钥，n为SSL序号，则MAC=H(m+M+n)。*

**R21 在SSL握手中随机不重数的目的是什么？**

防御“连接重放”攻击。

**R22 假设某SSL会话应用了具有CBC的块密码。服务器以明文向客户发送了IV。这种说法正确吗？**

错误的；因为IV是从MS获得的，MS是从PMS获得的，而PMS是客户生成，由公钥加密后发送给服务器的。

*客户端生成PMS（前主密码），用服务器的公钥加密PMS，然后发送给服务器，双方从PMS和不重数中导出MS（主密码），MS被切片生成两个密码和两个MAC密钥。如果使用了CBC技术，两个IV也是从MS中获得（双方各一份）。*

**R23 假设Bob向Trudy发起一条TCP连接，而Trudy正在伪装她是Alice。在握手期间，Trudy向Bob发送Alice的证书。在SSL握手算法的哪一步，Bob将发现他没有与Alice通信？**

在4步，Trudy无法从PMS中计算MS，进而不能生成各种密钥；在6步，Trudy无法发送正确握手报文的MAC，因此被Bob发现。

*SSL的三个阶段：握手（先建立TCP链接，再通告证书，最后交换MS）、密钥导出（双方从MS中生成4个密钥）和数据传输（使用SSL记录格式加密传输）。*

*SSL握手：① 客户发送支持的加密算法列表以及客户的不重数；② 服务器返回所选择的对称加密算法、公钥、MAC算法、证书以及服务器不重数；③ 客户验签，提取服务器公钥，然后生成PMS，发送经服务器公钥加密的PMS；④ 客户与服务器独立地从PMS和不重数中计算出MS，从MS中生成四个密钥；⑤ 客户发送所有握手报文的一个MAC；⑥ 服务器发送所有握手报文的一个MAC。*

**R24 考虑使用IPsec从主机A向主机B发送分组流。通常，为该流中的每个分组将创建一个新SA。这种说法是正确的吗？**

错误。如果A到B，那么最多两个SA。

**R25 假设在图8-28中总部和分支机构之间通过IPsec运行TCP。如果TCP重新传输相同的分组，则由R1发送的两个对应的分组将在ESP首部中具有相同的序号。这种说法是正确的吗？**

错误；对于IPsec来说，这是一个新分组，ESP序号会更新，这个序号用于防御重放攻击。

**R26 IKE SA和IPsec SA是相同的东西。这种说法是正确的吗？**

不是。大型的、地理上分散的部署需要一个自动的机制来生成SA，IKE协议用来从事这项工作。IKE SA与IPsec SA不同，IKE SA是双向的，用于为IPsec提供一个鉴别和加密的信道。

**R27 考虑802.11的WEP。假定数据是10101100并且密钥流是11110000。相应的密文是什么？**

d=10101100，K=11110000，c=d⊕K=01011100。

**R28 在WEP中，每个帧中以明文发送IV。这种说法是正确的吗？**

正确。IV值逐帧变化，以明文的形式出现再每一个WEP加密的802.11帧的首部中。

## 8.9 运行安全性：防火墙和入侵检测系统

**R29 状态分组过滤器维护两个数据结构。给出它们的名字并简单地讨论它们的功能。**

连接表：追踪所有进行中的TCP连接；访问控制列表：实现防火墙规则。

**R32 为什么应用程序网关必须与分组过滤器协同工作才能有效？**

分组过滤器在网络层和传输层分组的粒度进行流量过滤，而应用程序网关则是在应用的角度上进行流量过滤。

*防火墙的3个分类：传统分组过滤器（基于策略过滤分组流量，使用访问控制表实现），状态过滤器（传统分组过滤器是独立地过滤分组，状态过滤器是在TCP连接的基础上过滤分组，维护一个TCP连接表和一个访问控制表），应用程序网关（分组过滤仅针对网络层、传输层，在应用层，还需要结合应用程序网关来实现细分到具体应用类型的过滤）。*

**R33 基于特征的IDS和IPS检查和UDP报文段的载荷。这种说法是正确的吗？**

不一定需要检查载荷，与规则集指定的规则有关。