第一部分:小测题

第一 二章

1.常用的通信传输介质有哪些？它们之间的主要区别？
(1)有线:双绞线、同轴电缆、光纤:无线
(2)区别:带宽、误码率、传输距离、价格、频谱及复用方式、是否支持移动通信等。

2.面向连接服务能提供什么服务？
(1)可靠传输:(2)有序传输:(3)资源预置(使用)

3.无连接分组交换与面向连接(虚电路)分组交换的区别？
(1)分组格式:前者完全源、目的地址:后者虚电路号
(2)路由表:前者面向整个网络拓扑，转发时顺序查找路由表:后者面向特定路径或源路由，转发基于索引查找路由表。
(3)可靠性、顺序性:前者无:后者有
(4)建立、维护连接:前者无:后者有

4.无连接服务的优点与缺点？
优点:无需知道网络状态(包括网络资源)或只需知道局部网络状态 缺点:具有不确定性(是否有满足服务的网络资源不确定，能否完成服务不确定)

5.分层网络体系结构的不足:
上层协议的性能依赖于下层协议

6.分组交换原理:
(1)存储转发;(2)动态路由(包括每个分组自带源地址、目的地址，拓扑发现、路由选择);(3)出错交由端系统处理

7.若一个 WWW 文档中除有文本外，还有 6 个图像。试问使用 http/1.0 与 1.1 各需要建立几次 TCP 连接？
1.0:7　　1.1:1 次

8.ADSL 通道数(子频带)？其中数据通道数？若每个通道均使用 QAM-128 调制，数据通道总容量？
256,248,248*7*4bk

9.假定要传送的报文共有 x(单位 bit)，从源节点到目的节点共有 k 跳链路，每条链路的传播时延为 d(单位 s)，链路带宽为 b(单位 bit/s):电路交换(包括连接建立与拆除)使用的控制帧(或信令)长度、在各节点的排队时延忽略不计:分组交换使用的分组头、分组长度分别为 h、p(单位 bit)，分组在各节点的排队时延 q(单位 s)。试分析在何种条件下电路交换的总时延要小于分组交换的总时延？
电路交换总时延 D(c):
(1) 连接建立时间:kd　　(2) 连接拆除时间:kd
(3) 数据传输时间:x/b　　(4) 数据传播时间:kd
D(c)=3kd+x/b
分组交换总时延 D(p):
(1) 单个分组传输时间:(p+h)/b
(2) 第 1 跳传输时间(x/p)、((p+h)/b)(x/p 为分组个数)
(3) 传输时间每 1 跳增加 1 个分组的传输时间，所以总的传输时间为　x/p*(p+h)/b+(k-1)*(p+h)/b
(4) 排队时间:kq　　(5) 传播时间:kd
D(p)=x/p*(p+h)/b+(k-1)*(p+h)/b+kd+kq
若 D(c)<D(p)，则…

第三章

1.TCP 协议中 ACK 的作用。
(1)建立连接、拆除连接　　(2)差错控制(或可靠传送)
(3)流量控制　　(4)拥塞控制

2.TCP 连接的目标。
(1)实现进程间通信　(2)实现可靠传送　(3)实现按序传送
(4)进行流量控制　(5)进行拥塞控制

3. 实现 TCP 连接目标的主要机制。
(1)通过传输层地址(端口号)实现进程间通信 (2)通过确认机制实现可靠传送 (3)通过接收方缓存实现按序传送 (4)流量控制 (5)拥塞控制 (6)连接建立与拆除机制

4.在 TCP 连接中，客户端的初始号 215。客户打开连接，只发送一个携带有 200 字节数据的报文段，然后关闭连接。试问下面从客户端发送的各个报文段的序号分别是多少
(1)SYN 报文段:(2)数据报文段:(3)FIN 报文段。
答:(1)215;(2)216;(3)416

5.在一条新建的 TCP 连接上发送一个长度为 32KB 的文件。发送端每次都发送一个最大长度的段(MSS)，MSS 的长度为 1KB，接收端正确收到一个 TCP 段后立即给予确认。发送端的初始拥塞窗口门限设为 16KB。假设发送端尽可能快地传输数据，即只要发送窗口允许，发送端就发送一个 MSS。
(1)已知发生第一次超时后，发送端将拥塞窗口门限调整为 4KB。请问发生超时的时候，发送端的拥塞窗口是多大？此时发送端一共发送了多少数据？其中有多少数据被成功确认了？ (2)发送端从未被确认的数据开始使用慢启动进行重传。假设此后未再发生超时，当文件全部发送完毕时，发送端的拥塞窗口是多大？
(1)第一次超时发生时，发送端拥塞窗口大小=4KB*2= 8KB
在新建立的 TCP 连接上，发送端采用慢启动开始发送，因此当第一次超时发生时，发送端已发送的数据量 = 1KB + 2KB + 4KB + 8KB = 15KB。此时，除最后一批 8 个 TCP 段未获确认外，之前发送的 TCP 段都被确认，因此成功确认的数据量为 7KB。
(2) 发送端采用慢启动重新开始发送，在拥塞窗口达到 4KB 时发送数据量=1KB+2KB+ 4KB=7KB。然后进入拥塞避免阶段:在收到全部 4 个 MSS 的确认后，拥塞窗口增至 5KB，相应地发送端发送了 5KB 数据:收到全部 5 个 MSS 的确认后，拥塞窗口增至 6KB:收到全部 6 个 MSS 的确认后，拥塞窗口增至 7KB:此时刚好发完。因此，文件发送结束时，发送端的拥塞窗口大小为 7KB。

6. TCP 如何发送紧急数据？
(1)紧急标志位 U(URG)置 1:(2)紧急数据置于 TCP 段数据(载荷)前部:(3)紧急指针指向紧急数据的最后一个字节。

7. TCP 接收方何种情形需要立即进行确认？
(1)连续两个段按序到达，且前一个未确认:(2)收到失序段(序号比期望的序号大):(3)收到丢失段:(4)收到重复段。

8.滑动窗口协议中，GBN 与 SR 利用链路缓冲能力连续发送多个帧，令帧的传输时间(transmission time)=1(归一化)、传播时间(propagation time)=a，则链路的缓冲能力为？
a(单向)或 2a(双向)

第四章

1. 一个子网 IP 地址为 10.80.0.0，子网掩码为 255.224.0.0 的网络，这个子网的网络地址、广播地址、最小用户地址、最大用户地址分别是？
答:网络地址:10.64.0.0　广播地址:10.95.255.255
最小用户地址:10.64.0.1　最大用户地址:10.95.255.254

4.一个 IPv4 分组的分片中,MF(或 M)位是 0,HLEN 是 10,总长度是 100,分片偏移值是 200。试求该分片第一个字节和最后一个字节在原分组中的位置。
答:　第一字节的位置是 1600(200*8)，最后一个字节的位置为 1659(1600+100-10*4-1)。

5.基于目的地址转发“下一跳方法”的优缺点。
优点:每个路由表项只需保留“下一跳”的地址，无需给出完整的路由(路径)。缺点:要求“下一跳”路由器知道剩余的路径信息或网络中的所有路由器信息保持一致。

6.RIP、OSPF 协议的缺点
RIP 缺点:(1)更新周期(30s)过短;(2)未进行区域划分
OSPF 缺点:用可靠广播方式在整个区域广播所有节点的链路状态，开销过大

第五-八章

1. 若一无限用户 slotted ALOHA 信道处于负载不足与过载的临界点，则
(1)信道中空闲时槽的比例是多少？
(2)成功发送一个帧发送次数是多少？
(1)p0=e-G，G=1==p0(空闲比例)=36.8%
(2)G/S-1=1/0.368≈2.72

2. IEEE 802.3 MAC 协议的全称？它是如何解决冲突的？
1-坚持 CSMA/CD:发前侦听，边发边听，冲突避让

3. 若某站点经历了 10 次连续冲突，则在 IEEE 802.3、802.3u 网络中站点的平均等待时间分别为多少？
1024/2=512;802.3:512*51.2μs;802.3u:512*5.12μs
802.3U:100Mbps 802.3：10Mbps

4. IEEE 802.11 协议哪个(或几个)控制帧发现隐藏终端与暴露终端的？隐藏终端:CTS:暴露终端:RTS

5. IEEE 802.3 MAC 协议中最小帧长的功能与计算依据？最小帧长的功能:检测冲突。
计算依据:传输速率*相距最远的两个站点间往返传播时延

6. 数字签名是一种可提供发送方身份鉴别、报文完整性和防发送方抵赖的安全机制。
(1)请给出数字签名最常见的构造方法。(2)根据数字签名的构造方法，说明数字签名为何可以提供以上安全服务。
答:(1) 当实体 A 需要为报文 M 生成数字签名时，A 首先用一个散列函数计算 M 的报文摘要，然后用 A 的私钥加密该报文摘要，生成数字签名。(2) A 的私钥是只有 A 知道的秘密，任何其它实体无法得到，因而一个有效的数字签名可提供发送方身份鉴别。报文摘要可用于检测报文的完整性，对报文内容的任何修改将产生不同的报文摘要。用 A 的私钥加密后的报文摘要是不可伪造的，从而数字签名就将 A 与报文 M 紧密关联在一起，既能提供报文完整性服务，也能防止发送方抵赖。

7.交换机是如何提升网络性能的？
划分冲突域

8.链路层 ACK 的作用？
(1)差错控制，确认，实现可靠传送;(2)流量控制，滑动窗口

9. 首先计算 frame 100110101111 及 $G(x)=(x^4+x^3+1)(x+1)$的 CRC,然后描述 G(x)的检错能力.
(1)G(x)=x5+x3+x+1(101011)，CRC=00000
(2)检错能力:①可检测所有单个错误(G(x)多于一项)
②奇数个错误(含 1+x 项)　③2 个错误(说明:该项回答不出不扣分)　④长度不大于 5 的突发错误　⑤(1-2-4)长为 6 的突发错误　⑥(1-2-5)更长和突发错误

10.若使用一个 256-kbps 的无差错卫星信道(往返传播时延为 512-msec)一个方向上发送 512-byte 数据帧，而在另一个方向上返回很短的确认帧。则对于窗口大小为 1, 15, 127 的最大吞吐量是多少？
512*8/256k=16ms
(1)k=1, 16/(16+512)*256=7.75　(2)k=15, 7.75*15=116.36
(3)k=127, 256

11.HDLC 与 PPP 协议的主要区别？
(1)HDLC 使用序列号(滑动窗口协议)，PPP 在控制域为缺省值时不使用序列号(停等协议)且为不可靠传输。
(2)HDLC 面向 bit 填充(同步传输)，PPP 除支持面向比特填充(同步传输，直接使用 HDLC 协议)，还可使用面向 byte 填充(异步传输，使用类 HDLC 协议 RFC1662)
(3)PPP 基于 HDLC，主要用于在点到点链路上传输 IP 流量，并可支持多种网络协议.

12.假设数据帧为 D bits，链路带宽为 b bps，链路出错概率为 p，采用前向纠错策略需要 x bits 的冗余码，采用检错加重传策略需要 y bits 的冗余码。试比较分析两种策略的带宽利用率与时延性能。
(1)前向纠错策略:传输数据量 D+x，传输次数 1，故带宽需求量为(D+x)、传输时延为(D+x)/b
(2)检错加重传策略:一次传输数据量 D+y，传输次数 1/(1-p)，故带宽需求量为(D+y)/(1-p)、传输时延为(D+y)/(b*(1-p))

13.当两个主机采用传输方式使用 IPsec,试问此两台主机是如何建立一条虚拟面向连接的服务？答:SA

第二部分:知识点

第一章 概述

1.1 什么是因特网
1. 因特网的两种描述:
1 按松散的层次结构组织、并且遵循 TCP/IP 协议的 ISP 集合/2 为分布式应用提供通信服务的基础设施
2.终端设备:称为主机或端系统，运行网络应用程序
通信链路:光纤，铜线，射频等，传输速率称为带宽
分组交换机:转发分组，包括路由器和链路层交换机

1.2 网络边缘
1 物理媒体分类
设备之间通过物理媒体相连。分为:导引型/非导引型

1.3 网络核心
1 分组交换
主机将应用报文划分成分组，交换机仅在接收到整个分组后,才可以开始转发(存储-转发)。不考虑信号传播时间,P 个分组经过 N 条链路的总耗时是(P+N-1)L/R
当分组到达速率大于链路输出速率时,会在缓存中排队。若缓存满了，会丢包。
网络核心的重要功能:选路(生成转发表)、转发
分组交换原理:小测 1.6
优点:适合突发数据，简单，不需建立电路支持更多的端系统、能快速传输端系统产生的大量数据
缺点:可能产生严重拥塞(延迟、丢包)
2. 电路交换
通信前预留端-端资源(分组交换不预留)，资源独占。不通信时资源闲置
优点:能在请求时间内为端到端保持一个确定量的带宽
3.ISP
ISP 采用多层结构:局域网连接到区域 ISP，区域 ISP 间直连/用 IXP 相连/连接到更高层 ISP
4. TDM(时分复用)相对 FDM(频分复用)的优点: FDM 需要复杂的模拟硬件来将信号转换到合适频带上

1.4 分组延迟
1.分组延迟的来源
节点处理(查错、确定输出链路)/排队(在缓存处等待传输)/传输延迟(见 1.3.1，分组的发送时间)/传播延迟
最大吞吐量:路由器能够转发分组的最大速率
流量强度:La/R R:链路带宽 L:组长度 a:分组到达速率
L*a<1 越接近 1，延迟越高

1.5 协议层次
分层优点:显式的层次结构易于确定系统的各个部分及其相互关系/模块化使更新系统组件为容易
分层缺点:一层可能冗余低层功能

协议栈
应用层:支持各种网络应用:FTP，SMTP，HTTP
传输层:进程-进程的分组传输:TCP UDP
网络层:源主机-目的主机的分组传输:IP/路由协议
链路层:相邻网络设备之间的分组传输:PPP/以太网
物理层:在物理媒体上传输比特
比特/帧/数据报/报文段/报文
OSI 模型:应用层传输层间加了表示层(顶)与会话层。
表示层:解释交换数据含义，如压缩、解密等
会话层:提供数据交换定界、同步功能.建立检查点,提供恢复方案
封装:路由器顶三层，链路层交换机底二层。形式:首部+有效载荷字段

第二章 应用层

2.1 应用层协议原理
1.网络应用架构:客户-服务器架构，对等架构(P2P)
客户机:发起通信的进程,需要时与服务器通信,不是时时在线,通常使用动态 IP,不与其他客户机直接通信
服务器:等待联系的进程，是总是在线的主机，具有永久 IP 地址。
P2P:没有总是运行的服务器，任意一对端系统可直接通信，每个对等方可以请求服务也可提供服务。对等方间断连接，动态 IP
2.套接字
进程通过套接字收发报文，是应用层、传输层的接口，是应用程序与网络间的 API
为接收报文，每一个进程要有标识(端口号)。因为进程很多，不能用 IP 地址标识进程。HTTP 80 Mail 25
3.传输服务
运输层提供的服务种类:可靠性 吞吐量 定时 安全性
TCP:面向连接的可靠传输，有流量控制、拥塞控制，不提供及时性、最低带宽保证
UDP:无连接、不可靠传输
4.应用层协议 e.g. HTTP SMTP
应用层协议定义了:报文类型、语法、语义、进程发送/响应报文的抑制

2.2 Web、HTTP HTTP1.0 (RFC1945) HTTP1.1(RFC2068)
网页由基本 HTML 文件、对象构成。HTML 文件引用对象。每一个对象有一个 URL
HTTP1.0 (RFC1945) HTTP1.1 (RFC2068)
1.概述
客户发起到服务器 80 端口的 TCP 连接(客户端创建一个套接字)
服务器接受来自客户的连接(服务器端创建一个套接字)
浏览器和服务器交换 HTTP 报文(通过各自的套接字)
关闭 TCP 连接
2.连接方式(小测 1.7)
HTTP/1.0:非持久连接，一个连接一个对象
HTTP/1.1:持久连接，一个连接发送多个对象
RTT (Round-Trip Time)：一个小分组从客户发送到服务器再返回客户的时间。
对于非持久 HTTP，下载一个对象的时间=2RTT+对象传输时间。建立连接:1RTT，发送请求+收到头部:1RTT
对于持久 HTTP，下载一个对象时间=1RTT+传输时间。但传输整个网页还要再加一个 RTT(建立连接)。
3.报文格式:请求行，首部行，回车(表示结束)
上传方法:post(放在报文体内)，get(放在 URL 内)
4. cookie
存储位置:服务器端:返回 ID 给客户/客户端:文件中
5. web 缓存器(代理服务器，proxy)
既是客户端又是服务器，保存最近请求过的对象的拷贝。减少客户请求的响应时间、减少机构接入链路上的流量

2.3 FTP (File Transfer Protocol)，20/21 端口
FTP 采用两个并行的 TCP 连接传输文件:控制连接(端口 21)+数据连接(端口 20).是有状态服务
21 一直保持，20 随文件传输结束而关闭
分开控制、数据连接原因:不会混淆数据与命令/响应，简化协议设计和实现，在传输文件的过程中可以继续执行其它的操作，便于控制传输过程。
用关闭数据连接的方式结束传输:允许动态创建文件

2.4 电子邮件系统
1.三部分:用户代理、邮件服务器、简单邮件传输协议
2.SMTP 端口号 25
使用 TCP 作为传输层协议，持续连接，服务器端口为 25
①SMTP 是一个推协议，只能将邮件从用户代理推送到其邮件服务器，HTTP 主要是一个拉协议　②SMTP 要求报文按照 7 比特 ASCII 码进行编码，HTTP 无此限制　③SMTP 把所有报文对象直接放在一个报文中，HTTP 把对象封装到响应报文中　④SMTP 报文另起一行写上句号作为结束，HTTP 通过内容长度域记录长度。
为了能够传输非 ASCII 内容，编码。
3 邮件访问协议:POP3 IMAP HTTP

2.5 DNS 主机名-IP 地址转换
1 提供的服务:
允许拥有复杂主机名的主机具有一个或多个别名
提供与主机别名对应的规范主机名及 IP 地址
提供邮件服务器的规范主机名及 IP 地址
允许用域名作为邮件服务器别名
允许一个规范主机名对应一组 IP 地址
将 http 请求在一群相同功能的 web 服务器之间分配
2 响应报文<512B,采用 UDP，否则 TCP，端口 53
3 DNS 服务器类型:根(所有)/顶级(.xx)/权威(机构内)DNS 服务器
4 本地 DNS 服务器起代理作用，缓存。DNS 查询是 DNS 服务器间通讯。
5.工作机制:应用程序(如浏览器)调用一个本地例程(称解析器)，主机名作为参数之一传递;解析器向 DNS 服务器发送查询报文(包含要查询的主机名);解析器收到包含 IP 地址的 DNS 响应报文;解析器将 IP 地址返回给调用者(如浏览器)
6 DNS 资源记录:(name, type, ttl, value)
Type=A，Name 是主机名 Value 是对应的 IP 地址
Type=NS Name:域，Value:域的权威 DNS 服务器主机名
Type=CNAME Name:别名，Value 是对应规范名
Type=MX Name:域，Value:该域的邮件服务器名

第三章 传输层

3.1 概述和运输层服务
在应用程序看来，传输层提供了进程间逻辑通信。忽略通信过程，不同主机上的进程可以认为它们是直接相连的
具体怎么传，由网络层管。
1 传输协议运行在端系统上
发送方:将应用报文封装成报文段，交给网络层发送。
接收方:从收到的报文段中取出载荷，交给应用层。
2 因特网的网络服务:
尽力而为的服务:网络层尽最大努力在主机间交付分组，但不提供任何承诺:保证交付，不保证按序交付，不保证数据完整。
3 传输层不能提供的服务:延迟保证 带宽保证
4 传输层可以提供的服务:
保证可靠按序的交付:TCP:不保证:UDP

3.2 多路复用与多路分解
1 多路复用:从多个套接字收集数据，交给网络层发送
多路分解:将收到的报文段交付到正确的套接字
2 主机中每个套接字应分配一个唯一的标识
报文段中有特殊字段指示要交付的套接字
发送方传输层需在报文段中包含目的套接字标识
接收方传输层需将报文段中的目的套接字标识与本地套接字标识进行匹配，将报文段交付到正确的套接字。
3 端口号是套接字标识的组成部分:是一个 16 比特的数,其中 0-1023 保留给公共域协议使用。源/目的端口号
4 UDP 套接字的标识为二元组:(IP 地址，端口号)
5 每个 TCP 连接套接字与一个进程联系,为四元组标识:源 IP 地址,源端口号 目的 IP 地址 目的端口号
6 具有相同套接字标识的 UDP 报文被交付给同一个套接字，与源 IP 地址及源端口号无关。源是用来发响应的。

3.3 UDP
1 UDP 提供:多路复用和多路分解(最基础的)、检测报文错误(但不尝试恢复)
2 不提供:可靠/按序交付、延迟/带宽保证
3 UDP 检验和:所有 16 位比特字的和做反码运算，溢出回卷(检验和+溢出的 1)
检验方法:所有 16 位比特字与检验和加，应当全是 1
4 优点:没有建立连接的延迟
协议简单:发送端和接收端不需要保存连接状态
报头开销小(UDP8B,TCP20B)
没有拥塞控制和流量控制，可以尽可能快地发送报文
5 报文段结构:源端口号、目的端口号、长度、检验和

3.4 可靠数据传输(RDT)原理
RDT1.0:底层信道完全可靠
RDT2.0:可能有比特翻转:检错码查错 ACK/NAK 反馈重传
RDT2.1:ACK/NAK 受损:发送方发现受损就重传。但是接收方会出现冗余。为分组添加序号，发现序号相同就丢弃
RDT2.2:不用 NAK:ACK 中携带序号。NAK 换成上一个 ACK。
发送端发现 ACK 序号不对就重发。
RDT3.0:可能丢包:启动定时器。如果超时前没收到 ACK/没收到期待的 ACK，重发。**注:必须等定时器超时才处理**
RDT3.0 是停等 大慢:一个完了才能传下个。需要流水线。
GoBackN:发送方
发送窗口 = 已发送未确认序号 + 未发送可用序号 = N
ACK 分组携带确认的分组的序号
使用累积确认:若 ACK 包含序号 q，表明 q 前的分组都正确收到，整体滑动发送窗口，使基序号= q+1，视发送窗口是否空启动/终止定时器
发方只对基序号分组使用定时器。如果 ACK 不对，不管。若超时:发送方重传整个发送窗口
接收方:
只对正确收到的序号连续的一系列分组中最高的回 ACK，如果失序，就丢弃，重发前一个 ACK。
选择重传 SR:自动调整失序，避免不必要的重传
发送方:与 GBN 类似，但不累计确认。如果 ACK 的是基序号，滑动发送窗口使基序号=最小未确认分组。
接收方:一旦收到就 ACK。若失序，缓存。若收到的是基序号，滑动接收窗口。如果收到窗口前的冗余分组，说明发送方超时，　发送 ACK(n)，即发送冗余 ACK。
为使接收端不会将重发的分组当成新的分组,窗口[0,N-1]和窗口[N,2N-1]不能重叠。所以 N<序号空间的一半。

3.5 TCP
1 特性:点到点 全双工 面向连接(握手) 可靠有序 流水式发送 流量控制
2 最大传输单元 MTU:链路层帧最大长度
最大报文段长度 MSS:MTU-TCP/IP 头，最大数据字节数，缺省 536 字节
3 窗口比例因子:实际窗口大小=window size*2^ scale
4 TCP 报文段结构
源/目的端口号:多路复用/分解
序号:首字节在字节流中的序号，非报文段序号
确认号:希望的下一字节序号，隐含累计确认
首部长度:32bits 为单位的首部长度
检验和、紧急数据指针(指向最后一个字节)、数据段
标志位:URG:紧急数据　PSH:立即交给上层　RST:不接受连接　SYN:建立连接　FIN:拆除连接
5 往返时间估计
EstimatedRTT=(1-α)EstimatedRTT+αSampleRTT
DevRTT=(1-β)DevRTT+β|SampleRTT-EstimatedRTT|
α 推荐值为 0.125　　β 推荐值为 0.25
TimeoutInterval=EstimatedRTT+ 4·DevRTT
仅为传输一次的报文计算 SampleRTT 再用指数加权移动平均将其累积
TimeoutInterval 初始为 1，超时翻倍,SampleRTT 更新时才按照公式更新
6 传输机制:像一个带累计确认的 SR
接收方(推迟确认):
收到一个期待的报文段,且之前的报均已发过确认:
推迟发送 ACK:500ms 内若无下一个到来,发送 ACK
收到一个期待的报文段，且前一个被推迟确认
立即发送 ACK
收到一个失序的报文段:发送冗余 ACK
收到填充间隙低端的报文段:立即发 ACK
推迟确认优点:减少通信量
缺点:延迟太大时导致不必要的重;RTT 估计不准确
发送方:
流水式发送报文段
仅对最早未确认的报文段使用一个重传定时器(GBN)
仅在超时后重发引起超时(最早未确认)的报文段(选择重传)，收到更新的确认序号后，推进发送窗口
为防止反复重传采用定时器补偿策略，发送方每重传一个报文段,超时值就增大一倍(至一个规定的上限值)。SampleRTT 更新时才再次更新 interval
同一序号收到三次重复 ACK，认为丢包，快速重传 TCP 中的 ACK 序号是期待的报文段第一个字节的序号
7 TCP 流量控制
接收方有个接收缓存,发送方调节速度使缓存不溢出
收方将 Rwnd 放在报文段中,向发方通告缓存可用空间
接收缓存中的可用空间 = RcvWindow　(接收窗口)
= RcvBuffer-[LastByteRcvd - LastByteRead]
LastByteSent-LastByteAcked ≤ RcvWindow
接收窗口为 0 时,发送方停发,但是数据还不能不传,发送方还得知道窗口大小。此时发送方启动坚持定时器,发送零窗口探测报文段，从接收方的响应中获知窗口大小
8 连接管理
三次握手:
客户 TCP 发送 SYN 报文段(SYN=1，ACK=0)
给出客户选择的起始序号，不包含数据
服务器 TCP 用 SYNACK 报文段响应(SYN=ACK=1)
给出服务器选择的起始序号，确认客户的起始序号
不包含数据(服务器端分配缓存和变量)
客户用 ACK 报文段响应(SYN=0，ACK=1)
确认服务器的起始序号
可能包含数据(客户端分配缓存和变量)
四次挥手:
客户端:向服务器发送 FIN，等待服务器确认
服务器:向客户端发送 ACK，确认其请求
服务器:向客户端发送 FIN，等待客户端确认
客户端:向服务器发送 ACK，等待一时间后结束

3.6 TCP 拥塞控制
TCP 使用端到端拥塞控制机制:发送方根据自己感知的网络拥塞程度，限制其发送速度。
发送速度=CongWin/RTT Bytes/sec
乘性减:检测到丢包(3 个冗余 ACK)，将 CongWin 减半(迅速减小)，但不能小于一个 MSS。超时:直接变 1MSS
加性增:若没有丢包，每经过一个 RTT 将 CongWin 增大一个 MSS，直到检测到丢包(缓慢增大)。
慢启动:CongWin<threshold 时，CongWin 每次加倍，否则只+1MSS。丢包时，threshold=CongWin/2
快速重传:收到三个 ACK 后认为丢包，立即重传报文.
Reno 快速恢复:三次 ACK 之后 threshold=CongWin/2，CongWin=threshold.在 Tahoe 中,CongWin = 1.
Tahoe:无论超时还是三次 ACK,都变 1

第四章 网络层

4.1 概述
网络层三大功能:
转发:将分组从路由器的输入端口移到合适的输出端口
选路:确定分组从源路由器到目的路由器的路径
建立连接(某些架构)
下一跳先查:路由表中只保留下一跳地址,各路由器的路由表须保持一致
网络服务模型:定义了分组在发送主机与接收主机之间传输时的特性 因特网只提供尽力而为的服务

4.2 虚电路网络:先选好路，分组只按路传 典型:ATM
传输分组前建立虚电路，传输结束后拆除虚电路
每个路由器为经过它的虚电路维护状态
链路及路由器资源(带宽、缓存等)可以分配给虚电路，从而虚电路能提供可预期的网络服务。
虚电路组成:
从源主机到目的主机的端到端路径
沿途每条链路上的 VC 号(VC 号仅有本地意义)
沿途每个路由器中的转发表项(进入端口,进入 VC 号,输出端口，输出 VC 号)

4.3 路由器架构
主要功能:选路(按协议计算转发表)/转发(按表输入-出)
输入端口
当交换结构不能及时将输入端口的分组转移到输出端口时，输入端口处形成排队。当输入队列溢出时，丢包。
输出端口:
当多个输入端口同时向一个输出端口发送时，形成排队。当输出队列满时，发生丢包。输出端口排队不可避免
丢弃方式:弃尾(满了再丢)/主动管理(到达一定值,按概率丢，满了全丢)
交换结构:内存交换:输入端口->内存->输出端口
总线交换:轮流广播，输入经总线发往输出
互联网络交换:多对并行转发

4.4 网络协议 (IP 协议、路由选择协议、ICMP 协议)
1 IPV4 数据报格式:
版本号，报头长度 H(32bits 为单位)、服务类型、数据报长度(字节为单位)、标识号/标志/片偏移=字节序号/8(用于分片)、寿命(剩余最大跳数，转发前-1)、上层协议(数据部分用哪个传输层协议，多路分解)、16 位头部校验和、32 位源/目的 IP 地址，数据(TCP/UDP 报文段)
数据报总长度=H+分片长度<=MTU-H
链路层帧能承载的最大数据字节数称为 MTU。IP 报文长度>MTU 时，分片，全部在目的主机组装
分片时:每片标识不变，最后一片 MF=0，其余片 MF=1，DF=1:不准分片:偏移量:片在原始数据中的位置
注:TCP 首部分成，就不用 IP 分片了，但 UDP 不行!
2 IPV4 编址
网络号、主机号:A 类编址:0+7 位网络号+24 位主机号　B 类编址:10+14,16;C 类 110+21,8;D 类:1110+组播地址;E 类:1111，预留
网络号:标识一个物理网络，由 ICANN 分配
主机号:标识一个网络接口，由网络管理员分配
主机号全为 0 的地址:给网络自身
主机号全为 1 的地址:作为广播
网络号全为 0 的地址:本网主机
3 子网
用路由器将一个较大的网络划分成若干较小的网络，每个网络使用一部分地址空间。
IP 地址与子网掩码做与运算，可得子网地址
4 IP 数据报转发
直接/间接交付。路由器需要/不需要发给下一个路由器间接交付需要查转发表。
路由表项要素:
网络前缀路由:目的地址是网络而不是一个网络接口
特定主机路由:目的地址是一个特定的网络接口
缺省路由:一个默认的路由器端口,不匹配其它路由表项的数据包发送给该端口
每个路由表项只记录去往目的地址的下一跳信息。目的地址/掩码、下一跳、输出端口
因特网的地址分配策略为 CIDR，按实际需要的地址数量分配地址空间，提高地址使用效率:允许将若干条路由聚合成一条路由，减小路由表规模
一个网络的前 n 位地址是一样的，后面就/n
查表方法:与掩码进行 and 运算。然后匹配表项
5 DHCP
主机一开始不知道自己的 IP 地址。它用 0.0.0.0 广播 DHCP discover 报文，寻找子网中的 DHCP 服务器
DHCP 服务器广播 DHCP offer 报文进行响应,给出推荐的 IP 地址及租期，其它配置信息(带有 MAC 地址，防止发错)
因为子网中可能有多个 DHCP 服务器，主机广播 DHCP request 报文选择一个 DHCP 服务器，向其请求 IP 地址

DHCP 服务器广播 DHCP ack 报文发送 IP 地址，响应客户的请求，确认所要求的参数
DHCP 服务器使用 UDP 端口 67，客户使用 UDP 端口 68
6 NAT
把不同主机数据报的端口号放在一起。原来端口号是用来识别主机进程的，现在也可以识别主机。
端口号为 16 位，允许一个 NAT IP 地址支持 65535 个对外连接。
对外出报文，NAT 将数据报中的(源 IP 地址，源端口号)替换为(NAT IP 地址，新端口号)。
对进入报文，NAT 取出数据报中的(目的 IP 地址，目的端口号)查表换成(IP 地址，端口号)。
路由器应当只处理三层以下的包头(端口号在传输层)
违反端到端原则(节点介入修改 IP 地址和端口号)
7 ICMP:因特网控制报文协议 Ping&Traceroute
主要任务:报告差错，但不能纠错。
8 IPV6:
地址 32 位->128 位
不允许中间路由器分片，太大直接丢弃:不算校验和
引入流，能对数据报进行区分处理，拥塞时按流的优先级丢包。不在显示包含选项。
穿越 IPV4 网络:头转换/建立隧道(IPV6 上套 IPV4 壳)

4.5 选路算法
1 链路状态(LS)选路算法:Dijkstra 算法 单点广播
2 距离向量 DV 算法:Bellman-Ford 算法
Dx(y) ← minv{c(x,v) + Dv(y)} c(x,v)是 xv 距离
每个节点周期性地将它的距离矢量发送给邻居
当节点 x 从其邻居收到距离矢量后，使用 B-F 方程检查是否更新自己的距离矢量。如果更新，发给邻居。好快坏慢
3 自治系统 AS
自治系统是由同一个管理域下网络和路由器组成的集合
每个 AS 被赋予一个 AS 编号，由 ICANN 分配
同一个 AS 中的路由器运行相同的选路协议(Intra-AS)
不同 AS 中的路由器可以运行不同的 Intra-AS
在一个 AS 内直接连接到其它 AS 的路由器是网关路由器
网关路由器之间运行 Inter-AS 选路协议
所有 AS 必须运行相同的 Inter-AS 选路协议

4.6 因特网选路协议
Intra-AS 又称内部网关协议 IGP。常见 RIP OSPF
Intra-AS 又称外部网关协议 EGP。只有 BGP
1 RIP:较低层 ISP 和企业网中使用 应用层协议 端口 520
代价是跳数，最大 15 跳，运行方式类似 DV
每台路由器维护路由选择表(距离向量+转发表)
RIP 通告 30s 交互一次，180s+不交互，认为不可达，距 16 毒性逆转解决计数至无穷问题:若选路表中到目的网络 x 的路由是 A 通告的，则向 A 通告该路由时，到 x 的距离设为 16(阻止 A 使用这条路由)。
2 OSPF 较项层 ISP 中使用，类似 Dijkstra，权值管理员配，广播路由选择信息 封装在 IP 包内，协议号 89
OSPF 使用 IP 承载，需要自行实现可靠报文传输与链路状态广播等功能
AS 内部配置成多个区域，其中一个为主干区域，包含所有区域边界路由器，分组先路由到源区域边界路由器，再通过主干路由到目的区域边界路由器
具有安全、可使用等费的多条路径、支持单播与多播、支持层次结构等优点
3 BGP 应用层协议 端口 179
AS 间选路只试图找到能够到达目的网络的路由，但不试图(也不可能)找到最佳路由。
运行 BGP 协议的边界路由器(或主机)称为 BGP speaker。通过半永久 TCP 连接建立会话，交换 BGP 报文
可达性信息:以 AS 校举形式通告的、到达目的前缀的完全路径(便于检测路径环)。路由器收到相邻 AS 的路由通告，在向下一个 AS 发送该路由之前修改报文，将自己的标识及 AS 号加入到完全路径中。

4.7 广播和多播路由选择
1 N 次单播实现广播:低效(重复传输)，源节点需知所有目的节点地址
2 无控制洪泛广播:告诉所有邻居，但会无休止循环
3 序号控制洪泛:只告诉之前没转发过的 OSPF
4 反向路径转发 RPF:利用单播路由表，只转发最短路径的反向路径上到来的广播
5 生成树广播:每个节点维护生成树中的邻居，广播只在生成树中进行，不会冗余
6 多播
分组交付给网络中的一组节点，所有接收者形成一个多播组:网络层多播地址为一个 D 类地址。
IGMP 协议将组成员关系报告给多播路由器。请求报文、通知报文、退出报文，查询报文
多播路由选择算法
目标:发现一棵链路的树连接了某多播组所有路由器
实现:使用组共享树(即基于核心)，维护代价小，发送代价可能不是最优
使用基于源的树维护代价大，发送代价为最优
因特网中的多播路由选择:
距离向量多播路由选择协议 DVMRP:
反向路径转发+剪枝
协议无关多播路由选择协议 PIM:
稠密模式类似 DVMRP
稀疏模式 使用聚集点来建立多播分发树

第五章 链路层

5.1 链路层概述
链路层任务:将数据报从一个节点传输到相邻的下一个
源主机 -> 源路由器
路由器 -> 下一跳路由器
目的路由器-> 目的主机
节点:主机，路由器
链路:连接相邻节点的通信信道(有线，无线链路，局域网)
帧:链路层分组
链路层服务:
组帧:将数据报封装到帧中、从帧中解封装数据报
链路接入(广播链路):在广播信道上协调各个节点的发送行为
可靠交付(部分协议提供):通过确认、重传等机制确保接收节点正确收到每一个帧(停-等、GBN、SR)。低误码率链路(如光纤，某些双绞线)上很少使用，高误码率链路(如无线链路)应当使用。
流量控制: 调节发送速度，避免接收节点缓存溢出，可以与可靠交付(如 GBN、SR)集成，也可以是单独的机制
差错检测: 检测传输错误
差错纠正(有些提供):检测并纠正传输错误(不是重传)
半双工和全双工:半双工通信时需提供收/发转换
链路层实现位置:线卡(路由器)网卡(主机)，硬软件结合
网络适配器(网卡)同时实现物理层内容

5.2 检错与纠错
单个错:一次一位;突发错:脉冲噪声，一次多位
编码集的海明距离:编码集中任意两个有效码字的海明距离的最小值。
检错能力:为检测出所有 d 比特错误，海明距离>=d+1
纠错能力:为纠正所有 d 比特错误，海明距离>=2d+1
一维奇偶校验:包含附加比特，使得 1 的总数是偶数
二维奇偶校验:划分 i 行 j 列，对每行列使用一维奇偶校验,检测、纠正单比特错误
CRC 校验:
对于 r+1 位的生成多项式:
数据后面加上 r 个 0,然后除以生成多项式,余数替换后面的 r 个 0.
检验方法:CRC 码/生成多项式,如果余数 0,无错
性质:1.任何多于一项的生成多项式 g(x)能检测所有单个错 2.每个被(1+x)除尽的多项式都具有偶数项,能检测所有奇数个错误 3.若码长 n<=g(x)的指数 e，则能够检测所有 1/2 个错 4.若码长 n<=g1(x)的指数,则 g(x)=(x+1)g1(x)产生的码能检测所有 1/2/3 个错误 5.由(n-m)次多项式产生的任一循环码能检测所有长度<=(n-m)的突发错误 6.长度为 b>(n-m)的突发错误中,若 b=n-m+1，则不能检测部分占 2-(n-m-1);若 b>n-m+1,则不能检测部分占 2-(n-m) 。e 是使 g(x)能除尽 x^e+1 的最小正整数:
5.3 多址接入协议:规定节点共享信道(谁能发送)的方法
理想 MAC 协议:
仅有一个结点有数据要发送时,应能让它使用全部带宽;多个结点有数据发送时，平均吞吐量应大致相等;协议是分散的,整个系统不会因某主结点故障而崩溃;协议简单
信道划分协议
时分复用 TDM:节点只能在分配给自己的时间片内发送,如果不发,时间片轮空
频分多路复用 FDM:将信道华为若干子频带
码分多址 CDMA:每个节点用唯一编码编码数据,可同时传输,任意两个 chip code 正交
随机接入协议 发送前不监听信道:ALOHA,监听:CSMA
时隙 ALOHA 在时隙开始时传输整个帧,如果碰撞,每次重传以概率 p 进行,效率 1/e,0.37
纯 ALOHA 立即传输帧,不在时隙传,效率 1/2e,0.185
CSMA 发送前监听信道,信道空闲:发送/忙:推迟发送
但是由于传输延迟,可能没监听到,一旦冲突,浪费
带冲突检测的 CSMA/CD:通过测量信号强度检测冲突(冲突信号强度大).检测到冲突后立即停止传输损坏的帧,并发送阻塞信号
二进制指数后退算法:经理 n 次碰撞后,随机从{0,…,2^n-1}中选取 k,延迟 k*512bit 时间.通过网络负载调整等待时间.
Tprop = 以太网中任意两个节点之间传播延迟的最大值 Ttrans = 最长帧的传输时间.效率为 1/(1+5·t*prop*/t*trans*)
轮流 MAC 协议:网络中有一个令牌，按照预定的顺序在节点间传递,获得令牌的节点一次可以发送一个帧

5.4 交换局域网
1 MAC 地址(LAN 地址、物理地址)
格式:6 字节，以十六进制数表示字节.
性质:地址由 IEEE 分配,没有两块适配器具相同的地址 FF-FF-FF-FF-FF-FF 为广播地址
必要性 :可以支持各种网络层协议(不只是 IP 协议)
2 地址解析协议 ARP:获得与 IP 地址对应的 MAC 地址
主机和路由器的每一个接口都有其 ARP 表，存储 IP 地址到 MAC 地址的映射.ARP 表中的项目通过 ARP 查询、响应报文来更新，且具有寿命值 TTL.
ARP 查询、响应报文包括:发送方、接收方 IP、发送方 MAC、接收方 MAC.ARP 查询报文在广播帧中发送，ARP 响应报文在标准帧中发送.ARP 是跨越链路层和网络的协议.
发送数据报过程:
A 创建 IP 数据报，src IP=A，dest IP=B.
A 查找转发表，得到下一跳地址.
A 利用 ARP 获得下一跳地址对应的 MAC 地址(R-1).
A 创建链路层帧,封装 IP 数据包,src MAC =A，dest MAC = R-1，发送.
R 接收帧，取出 IP 数据报，发现目的地址为 B
R 查找转发表，得知 B 在其端口 R-2 的直连网络上
R 利用 ARP 获得 B 的 MAC 地址
R 创建链路层帧，封装 IP 数据报，src MAC=R-2，dest MAC = B，发送
B 的网卡接收帧，取出 IP 数据报，交给网络层
注:路由器 R 有两个端口 R-1 R-2
3 以太网:基于交换机的星形拓扑，无冲突
交换机在端口之间存储-转发帧,各节点间不直接通信
交换机可以增加总带宽
转发器\集线器:物理层设备
4 以太帧结构 以太帧长 20 字节
前导码 建立时钟同步 7 个 10101010+一个 10101011
目的、源地址:目的/源 MAC 地址，6 字节
类型:数据所属的高层协议(IP/ARP 等)
数据字段 46-1500 字节,超了分片,少了填充
4 字节 CRC 校验码
最小帧长:为在发送结束前检测到冲突，最小 64 字节
5 链路层交换机 它没有 MAC 地址
交换机内有一张端口转发表,每个表项记录以下信息:
MAC 地址，到达该 MAC 地址的端口，时间戳
当一个帧到达时，交换机从源 MAC 地址了解到发送节点从它来的端口可达,在转发表中记录发送节点的 MAC 地址和可达端口.然后交换机用目的 MAC 地址查转发表.如果查到,发送(如果发现目的端口=到来端口,丢弃).否则广播
帧到达时还会更新转发表: 若找到地址，将对应表项的生存期设为最大值;若没有找到该地址,添加源地址和进入端口到转发表，设置表项的生存期为最大值

交换机与路由器区别
均为存储-转发设备:
交换机工作于链路层，根据 MAC 地址存储转发帧
路由器工作于网络层,根据 IP 地址存储转发数据报
内部都有转发表:
交换机:使用“逆向学习法”学习转发表
路由器:运行选路协议计算转发表
交换机是即插即用设备,路由器需要手工配置
交换机转发速度快，成本低(二层设备)
路由器转发速度慢，成本高(三层设备)
交换机不能连接异构链路(即 MAC 协议不同的网络)
路由器可以连接异构链路(重新封装链路层帧)
交换机不能阻断广播帧的传播:交换机会扩散所有的广播帧，通过交换机连接的所有主机在同一个广播域中
路由器可以阻止广播帧的传播:每个路由器端口是一个独立的广播域
VLAN:通过单一的物理局域网基础设施来定义多个虚拟局域网
交换机维护一张端口到 VLAN 的映射表
交换机软件仅在属于相同 VLAN 的端口之间交付帧,不同 VLAN 间需要通过路由器联系;合并不同交换机上的相同 VLAN 可以使用端口互连或干线连接
扩展以太网帧格式 802.1Q 添加 4 字节 VLAN 标签用于指明帧属于哪个 VLAN.VLAN 标签:2 字节标签协议识符、12 比特 VLAN 标识符 3 比特优先权
PPP 协议:点到点护具链路协议,用于 PC-因特网拨号连接和路由器间专线连接

第六章 无线网络

6.1 概述
基站:通常连接到固定网络,在无线终端和固定网络间中继数据包，如蜂窝塔,802.11AP,负责协调关联的多个无线主机的传输
基础设施模式:无线终端通过基站连接到固定网络(网络基础设施),所有传统的网络服务由固定网络提供.切换:无线终端接入到不同基站的过程
自组织模式:网络中没有基站,节点只能与其通信范围内的节点通信,节点相互帮助转发分组,每个节点既是终端又是路由器
分类 单跳+基于基础设施:802.11 网络,3/4G 蜂窝网络
单跳+无基础设施 蓝牙
多跳+基于基础设施:无线传感网络 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 无线链路的特性
信号衰减,其他信号源干扰,多径传播(地面,物体反射作用)
传输距离有限,误码率高
CSMA(载波侦听)不适合多跳无线网络:发送节点只能知道周围是否有节点发送,真正有影响的是接收节点附近是否有节点发送.
隐藏节点:不在发送节点范围内,但在接收节点范围内.
暴露节点:在发送节点范围内,但不在接收节点范围内.

6.3 IEEE 802.11 无线局域网

802.11b	2.4-5 GHz range	up to 11 Mbps
802.11a	5-6 GHz range	up to 54 Mbps
802.11g	2.4-5 GHz range	up to 54 Mbps
802.11n 多天线	2.4-5 GHz range	up to 200 Mbps

均使用 CSMA/CA 作为 MAC 协议,都支持基站模式和自组织模式,但物理层不同
基本组成单元是基本服务集(BSS),包括:
若干无线终端,一个无线接入点 AP
每个无线接口(终端及 AP)均有一个全局唯一的 MAC 地址
安装 AP 时，为 AP 分配一个服务集标识符(SSID)，并选择 AP 使用的信道.相邻 AP 使用的信道可能相互干扰
主机必须与一个 AP 关联:
扫描信道,监听各个 AP 发送的信标帧(包含 AP 的 SSID 和 MAC 地址)选择一个 AP 进行关联(可能需要身份鉴别)使用 DHCP 获得 AP 所在子网中的一个 IP 地址
被动扫描:主机监听 AP 发送的信标帧,主机选择一个 AP 发送关联请求帧，AP 向主机发送关联响应帧(主机找 AP)
主动扫描: 主机广播探测请求帧,AP 发送探测响应帧,主机从收到的探测响应中选择一个 AP 发送关联请求,AP 发送关联响应帧(主机向 AP)
802.11MAC 协议 CSMA/CA 碰撞避免
不能检测冲突:接收信号强度远小于发送信号强度;不能检测隐藏节点.冲突对无线网络损害很大，要尽可能避免。
PCF 模式: 由基站控制单元内的所有通信活动.
轮询:基站依次询问单元中的节点,被询问到的节点可以发送它们的帧，不会有冲突发生。
新节点注册:新加入的节点可以注册一个恒定速率的轮询服务，声明自己希望得到的带宽
DCF 模式:所有节点(AP 和无线终端)使用 CSMA/CA 竞争信道
使用信道预约机制的 CSMA/CA:
A 向 AP 发送一个 RTS 帧，帧中给出随后要发送的数据帧及确认帧需要的总时间;AP 收到后回复一个 CTS 帧，帧中给出同样的时间:A 收到 CTS 帧后开始发送;AP 收到帧后，发送一个 ACK 帧进行确认;(A 附近)收到 RTS 帧及(AP 附近)收到 CTS 帧的节点均沉默指定的时间，让出信道让 A 完成发送;若 A 和 B 同时发送 RTS 帧，产生冲突，不成功的发送方随机等待一段时间后重试
不使用信道预约机制的 CSMA/CA
当节点有帧要发送时，侦听信道:
若一开始就侦听到信道空闲,等待 DIFS 时间后发送帧
若信道忙，选取一个随机回退值，在侦听到信道空闲时开始递减该值;此过程中若侦听到信道忙，冻结计数值
当计数值减为 0 时，发送整个帧并等待确认。
若收到确认帧，表明帧发送成功，若还有新的帧要发送，从第 2 步开始 CSMA/CA;若未收到确认，节点重新进入第 2 步中的回退阶段，并从一更大的范围内选取随机值。
CSMA/CA 与 CSMA/CD 之不同: CSMA/CD 在发送过程中检测冲突,而 CSMA/CA 在发送过程中不检测冲突。在 CSMA/CD 中，节点侦听到信道空闲时立即发送;在 CSMA/CA 中，节点侦听到信道空闲后要随机回退。冲突对无线网络损害很大，要尽可能避免。

802.11 帧格式:有四个地址字段:接收节点 MAC 地址,发送节点 MAC 地址,连接 AP 的路由器接口的 MAC 地址,自组织网络用
6.5 移动网络的地址,路由管理: 移动中维持正在进行的连接
归属网络:移动节点的永久居所
永久地址:移动节点在归属网络中的地址,总是可以使用这个地址与移动节点通信
归属代理:移动节点在外地时为移动节点执行移动管理的实体
外地网络:移动节点当前所在的网络
转交地址:移动节点在外地网络上的地址(COA)
外地代理:外地网络上为移动节点执行移动管理功能的实体
间接选路:
移动结点移动到外部网络时,向外部代理注册 COA,外部代理将注册的 COA 转达给归属代理,在归属代理处注册.通信者将包发送给归属代理,归属代理转发给外地代理,再给移动结点
直接选路:
通信者向归属代理请求并获知移动节点的转交地址,通信者直接将包发送给外地代理,然后发给移动节点
6.6 移动 IP:代理发现,向归属代理注册,间接路由选择
愿意充当归属代理或外地代理的路由器定期在网络上发送代理通告,提供一个或多个转交地址.移动节点通过接收和分析代理通告,判断自己是否处于外地网络/切换了网络.如果发现在外地网络上，移动节点从外地代理提供的转交地址中选择一个作为自己的转交地址
移动节点向外地代理发送一个注册请求，给出自己的永久地址、转交地址、归属代理地址以及认证信息等.外地代理记录相关信息,向归属代理转发注册请求.归属代理处理注册请求，将移动节点的永久地址及转交地址保存在绑定表中,发回一个注册响应.外地代理收到有效响应后，将移动节点记录在转发表中，向移动节点转发注册响应
归属代理通过隧道转发数据包:外面套层壳
移动节点发送数据包:直接发给外地代理.
改进:归属代理将第一个数据包转发给转交地址后,向通信者发送一个消息，告知移动节点当前的转交地址
6.8 对上层协议的影响
丢包率高,应用吞吐率低(TCP 认为是拥塞,不必要的减小窗口)

第八章 网络安全

8.1 什么是网络安全
安全通信特性:机密性\报文完整性\端点鉴别\运行安全性
被动攻击:获取信息但不产生影响 偷听/流量分析
主动攻击:影响系统 伪装/重放/报文修改/拒绝服务
安全机制:加密/鉴别(防止假冒)/数据完整性/数字签名(证明数据起源,完整性,防止伪造/抵赖)/流量填充/访问控制

8.2 密码学原则
对称加密算法:加密密钥与解密密钥相同
非对称加密算法:加密密钥与解密密钥不同
块密码(分组密码):每次处理一个明文块,生成一个密文块
流密码:处理连续输入的明文流,生成连续输出的密文流
攻击:
惟密文攻击:入侵者仅能根据截获的密文进行分析
已知明文攻击:入侵者知道一些“明文-密文对”
选择明文攻击:入侵者拥有将明文转换为密文的能力.
公开密钥算法应满足的条件
生成一对加密密钥和解密密钥是容易的
已知加密密钥，从明文计算出密文是容易的
已知解密密钥，从密文计算出明文是容易的
从加密密钥推出解密密钥是不可能的
从加密密钥和密文计算出原始明文是不可能的
RSA:
选两个大素数 p,q,n=pq,z=(p-1)(q-1)
d 与 z 互质,ed=1(modz)
加密:C=M^e(modn)
解密:M=C^d(modn)

8.3 报文完整性(报文鉴别),数字签名
报文鉴别:起源鉴别/完整性检查.入侵者需不知怎么加密.
将一个散列函数作用到一个任意长的报文 m 上，生成一个固定长度的散列值 H(m)，称为该报文的报文摘要(数字指纹)
发送方计算报文摘要，然后用与接收方共享的密钥加密报文摘要,形成报文鉴别标签(报文鉴别码).接收方用共享的密钥解密鉴别码，得到发送方计算的报文摘要，与自己计算的摘要比较
数字签名:发送方先计算报文摘要,然后用发送方的私钥加密报文摘要,形成报文鉴别码.接收方用公钥解密,比较.
典型散列函数:MD5.先 MD5 一下,然后给 MD5 值加密,传输.对方解密,计算 MD5,比较
为防止公钥被入侵者偷换,需要认证权威(CA)证明公钥.证书卜有 CA 的签名,用 CA 的公钥来解密证书,防止偷换.
8.4 端点鉴别,需要抵御重放攻击
B 向 A 发送不重数 R,A 用私钥加密 R，回送给 B.B 用公钥检查.
报文最后还要附上发送方的数字签名.
8.5 SSL
握供:服务器鉴别，数据加密，客户鉴别(可选)
8.6 IPsec
把安全特征集成到 IP(网络)层,以便提供安全底层支持
专用网:用专线连接成网络
VPN:数据在发送到公用网前经过 VPN 加密，设置隧道
IPsec 传输模式:IPSEC 头插在原始 IP 头]传输层之间
IPsec 隧道模式:封装在新 IP 包内,套上新的 IP 头.
8.8 防火墙
包过滤防火墙:路由器对数报包进行逐包过滤.
状态检测防火墙:跟踪 TCP 连接的状态:跟踪连接的建立(SYN)和关闭(FIN)等状态，判断收到的包是否有意义
应用网关:检查应用层数据
IDS(不是防火墙):深度数据包检查:查看包内容(如检查包中是否包含已知的病毒特征、攻击特征等):检查多个包之间的关联性:防止端口扫描/DoS 攻击

第三部分:田野班小测题

1.1 一条分组交换链路，带宽 10Mbps，现有 20 位用户先后希望建立并保持通信连接，每位用户产生 1Mbps 的数据流量:
20 位用户均建立连接，数据通信产生较多丢包和较大时延
1.2 下面那种不是 ISP 的连接方式:
双方连接内容提供商网络实现连接
1.3 以下那些协议工作在主机/3 层路由器/2 层交换机上?
主机:应-物/路由器:网-物/交换机:链-物
1.4 带宽/吞吐率区别:
带宽:单位时间能够传输的最大数据量
吞吐率:单位时间能够成功实现的最高传输速率
2.1 进程 A 想发数据到另一台主机上的 B 进程,如何识别 B?
IP 地址+端口号
2.2 SSL 工作在应用层上
HTTP/1.0 一次发一个对象
P2P 有服务器进程和客户端进程.但是每个主机既是服务器又是客户端.
HTTP 是无状态服务,FTP 是有状态服务
2.3 你访问百度,哪个 DNS 服务器你一定不会遇到?
百度的 localDNS 服务器
3.1 TCP/UDP 没有提供的服务:
延迟保证/带宽保留
3.2 TCP 中,A seq = 32,给 B 发了 8Byte,A 回 ACK40
然而 B 没收到 A 的 ACK,又给 B 发了 20,A 回 ACK60
3.3
TCP 接收窗口在连接持续的过程中可能会变化.
用户 A 的未确认比特不可能超过接受缓冲区大小.
TCP 中,A 发了序号 m,那么下一个序号不是 m+1.
TCP 段中有接收窗口大小.
TimeoutInterval<SampleRTT
A 的 seq 是 38,发了 4byte 回的 ACK 应该是 42.但是 A 的 seq 和 B 的 seq 没关系。B 是按照 A 的 ACK 回复的。
4.1 IP 报长 3200Byte(20 头，3180 负载)，链路层 MTU 804Bytes。
5.1 如果交换机中间没有路由器直接相连，那么每一个交换机的转发表里都有所有的主机。
5.2
FDM TDM CDMA 是多址接入协议。
CDMA 是多址接入协议，CSMA 是随机接入协议
CSMA/CD 是有线 MAC 协议，检测冲突。
随机接入协议中，如果只有一个节点，它会独享整个信道。
在大量节点收发数据时，CSMA 不可能用 100%的带宽。
6.1
802.11 的 AP 可以设置 RTS 门限值，只有大于的时候才用 RTS 和 CTS
802.11 使用 RTS 和 CTS 不能完全避免冲突。因为可能同时发送 RTS。
但是 802.11 在使用 RTS 和 CTS 在传输数据帧的时候能避免冲突。
以太网和 802.11 帧结构不同。
6.2 CDMA 的编码方式
设 A 的编码是行向量 A，B 的编码是行向量 B。
则，A 传输的 a 被编码为 aA。B 传输的 b 被编为 bB.
传输中的数据 D=aA+bB.
D*A 的转置可得 a，同理可得 b。
6.3 AES 加密方式:
ECB:切成小块，分块加密
CBC:切成小块，与上一块取异或再加密
CTR:有一个自增的算子，把算子加密，与明文异或。
另外两种看复杂。

传输层 TCP 分段
网络层 IP 分片
链路层 不分片
只有目的组装

TCP,IP 头:默认都是 20 个字节，4 个字节计算长度
UDP 头:8 个字节