计算机网络复习笔记

© 2017-1 熊家靖 PB14011026

第一章 计算机网络和因特网

1.1 什么是因特网

1、因特网的两种描述：组成部分？能够提供的服务？

2、主机 = 端系统

主机连接路径 = 通信链路 + 分组交换机

分组交换机 = 路由器（用于网络核心） + 链路层交换机（用于接入网）

3、因特网服务提供商 ISP

4、协议：定义通信实体之间通信的规范

5、因特网工程任务组 IETF 的标准文档 请求评论 RFC

1.2 网络边缘

1、主机的两种类型：客户、服务器

2、接入网：将端系统连接到其边缘路由器的物理链路

3、边缘路由器：端系统到任何其他远程端系统的路径上的第一台路由器

4、接入方式：数字用户线 DSL、电缆、光纤到户 FTTH、以太网、WiFi、3G、LTE

5、物理媒体：导引型（双绞铜线、同轴电缆、光纤）非导引型（陆地/卫星无线电信道）

1.3 网络核心

1、分组交换：存储转发机制、输出缓存、丢包、转发表、路由选择

2、电路交换：频分复用 FDM、时分复用 TDM（时间划分为帧、帧划分为时隙）

3、分组交换优点：支持更多的端系统 + 快速传输端系统产生的大量数据

电路交换优点：能在请求时间内为端到端保持一个确定量的带宽

TDM 相对 FDM 的优点：FDM 需要复杂的模拟硬件来将信号转换到合适的频带上

4、网络结构：ISP、存在点 PoP、多宿、对等、因特网交换点 IXP、内容提供商

1.4 分组交换网中的时延、丢包和吞吐量

1、吞吐量：每秒能够传送的数据量 单位：bps（b 是 bit 不是 byte）

2、时延：节点处理时延 proc、排队时延 queue、传输时延 trans、传播时延 prop

3、处理时延：检查分组首部、决定将该分组导向何处的时间，微秒或更低数量级

排队时延：分组在链路的输出缓存队列中等待的时间，毫秒到微秒量级

传输时延：将分组的所有比特推向链路的时间，分组长度与链路传输速率的函数
毫秒到微秒量级

传播时延：从链路起点传播到终点的时间，是距离的函数，毫秒量级

4、最大吞吐量：路由器能够转发分组的最大速率

5、流量强度：La/R（a 是分组到达队列的平均速率）设计系统时流量强度不能大于 1

6、平均吞吐量、瓶颈链路（通常都是接入网）

1.5 协议层次及其服务模型

1、协议层用软件、硬件或两者的结合来实现

2、分层优点：概念化、结构化
提供了结构化方式用于讨论系统组件
模块化使更新系统组件更为容易

分层缺点：一层可能冗余较低层的功能

某层的功能可能需要仅在其他某层才出现的信息（如时间戳值）

3、协议栈：物理层 –> 链路层 –> 网络层 -> 运输层 -> 应用层
信息形式：比特 -> 帧 -> 数据报 -> 报文段 -> 报文

4、OSI 模型：应用层、表示层、会话层、运输层、网络层、数据链路层、物理层
表示层：使通信的应用程序能解释交换数据的含义，包括数据压缩、解密、描述
会话层：提供数据交换定界和同步功能，包括建立检查点和恢复方案的方法

5、封装：路由器实现前三层，链路层交换机实现前两层，形式：首部+有效载荷字段

1.6 面对攻击的网络

1、四种攻击类型：侵害计算机、攻击服务器和网络基础设施、嗅探分组、伪装

2、僵尸网络：受害设备形成的网络
病毒：需要某种形式的用户交互来感染用户设备的恶意软件
蠕虫：无需任何明显用户交互就能进入设备的恶意软件

3、拒绝服务攻击 DoS：弱点攻击、带宽洪泛、连接洪泛
分布式拒绝服务攻击 DDoS

4、分组嗅探器：记录每个流经的分组的副本的被动接收机
最好的防御手段都与密码学有关

5、IP 哄骗：将具有虚假源地址的分组注入因特网
采用端点鉴别的方式来防御

第二章 应用层

2.1 应用层协议原理

1、应用程序体系结构：客户—服务器体系结构、对等 P2P 体系结构

2、客户：发起通信的进程　服务器：等待联系的进程

3、套接字：同一台主机内应用层与运输层之间的接口 API

4、应用程序开发者对于运输层的控制：设置运输层协议、设定运输层参数

5、端口号：用于标识运行在主机上的进程的套接字

6、运输层协议提供的服务种类：可靠数据传输、吞吐量、定时、安全性

7、带宽敏感应用：具有吞吐量要求的应用程序
弹性应用：能够根据情况或多或少地利用可供使用的吞吐量

8、TCP 服务：面向连接（全双工连接）、可靠的数据传送服务

9、UDP 服务：无连接、不可靠的数据传送服务

10、应用层协议：定义了运行在不同端系统上的应用程序进程如何相互传递报文

2.2 Web 和 HTTP

1、Web 三要素：Web 浏览器、HTTP 协议、HTML 语言

2、HTTP 使用 TCP 作为支撑运输协议，其不保存状态信息，是无状态协议，端口号 80

3、持续连接：所有的请求及其响应经相同的 TCP 连接发送
非持续连接：每个请求/响应对经一个单独的 TCP 连接发送

4、HTTP 默认使用持续连接，HTTP 客户和服务器也能配置成使用非持续连接

5、往返时间 RTT：指一个短分组从客户到服务器然后再返回客户所花费的时间

6、TCP 每次建立连接需要三次握手，耗费 1.5 个 RTT

7、HTTP 报文种类：HTTP 请求报文、HTTP 响应报文

8、HTTP 请求报文：请求行、首部行、实体
HTTP 响应报文：状态行、首部行、实体

9、Cookie 技术：请求/响应报文中的 cookie 首部行

位于用户端系统中的 cookie 文件，由浏览器进行管理

位于 Web 站点的一个后端数据库

10、Web 缓存器：即代理服务器，既是服务器又是客户

2.3 文件传输协议：FTP

1、FTP 使用两个并行的 TCP 连接来传输文件：控制连接（带外传送） + 数据连接

2、FTP 使用持续的控制连接、非持续的数据连接，会话期间保留用户的状态，端口号 21

2.4 因特网中的电子邮件

1、电邮系统三要素：用户代理、邮件服务器（也是客户端）、简单邮件传输协议 SMTP

2、SMTP 采用 TCP 作为支撑运输协议，使用持续连接，端口号 25

3、SMTP 与 HTTP 对比：

SMTP 基本是一个推协议，HTTP 主要是一个拉协议

SMTP 要求报文按照 7 比特 ASCII 码进行编码，HTTP 无此限制

SMTP 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

SMTP 报文另起一行写上句号作为报文结束，HTTP 通过内容长度域记录长度

4、邮件访问协议：第三版邮局协议 POP3、因特网邮件访问协议 IMAP、HTTP

2.5 DNS:因特网的目录服务

1、主机的标识方式：主机名、IP 地址

2、DNS：一个由分层的 DNS 服务器实现的分布式数据库

一个使得主机能够查询分布式数据库的应用层协议

3、DNS 提供的服务：

主机名到 IP 地址的转换

主机别名、规范主机名

邮件服务器别名（MX 记录允许邮件服务器与 Web 服务器同名）

负载分配：每次用 IP 地址集合的不同置换来响应

4、DNS 采用 UDP 作为支撑运输协议，端口号：53

5、DNS 服务器的类型：根 DNS 服务器、顶级域 DNS 服务器、权威 DNS 服务器

6、利用本地 DNS 服务器进行递归、迭代查询，利用 DNS 缓存改善时延

7、资源记录 RR 提供主机名到 IP 地址的映射：（Name，Value，Type，TTL）

若 Type = A，则 Name 是主机名，Value 是该主机名对应的 IP 地址

若 Type = NS，则 Name 是个域，而 Value 是权威 DNS 服务器的主机名

若 Type = CNAME，则 Value 是别名为 Name 的主机对应的规范主机名

若 Type = MX，则 Value 是个别名为 Name 的邮件服务器的规范主机名

2.6 P2P 应用

1、BitTorrent 协议：

参与特定文件分发的所有对等方的集合称为一个洪流

每个洪流具有一个追踪器，其跟踪洪流中的对等方

加入洪流中的对等方从追踪器获取信息创建并行 TCP 连接，得到邻近对等方

从邻近对等方中按照最稀缺优先的顺序请求资源

采用对换算法，定期随机更新疏通方，每次只响应疏通方的请求

2、分布式散列表：

环形 DHT，即一致性哈希

对等方扰动

第三章 运输层

3.1 概述和运输层服务

1、运输层只工作在端系统中，中间路由器既不处理也不识别运输层所加的报文信息

2、运输层只看得见报文与报文段，看不见数据报

3、网络层提供了主机之间的逻辑通信，而运输层为其进程提供了逻辑通信

4、运输层协议：用户数据报协议 UDP、传输控制协议 TCP

5、运输层最低限度的服务：数据交付、差错检查

3.2 多路复用与多路分解

1、多路复用：为不同套接字中收集到的数据块封装首部信息后推送到网络层

多路分解：将运输层报文段中的数据交付到正确的套接字

2、要求：套接字有唯一标识符

每个报文段有特殊字段来指示该报文段所要交付到的套接字

3、端口号：16 比特的数，大小在 0~65535 之间，0~1023 为周知端口号，使用受限

4、UDP 套接字：使用二元组（目的 IP 地址，目的端口号）标识

TCP 套接字：使用四元组（源 IP 地址，源端口号，目的 IP 地址，目的端口号）标识

3.3 无连接运输：UDP

1、UDP 的优点：应用层能避开 TCP 拥塞控制，从而更精细地控制何时发送什么数据

无需建立连接，不会引入建立连接的时延

无需维持连接状态，能支持更多活跃客户

分组首部开销小（UDP 只有 8 字节，TCP 有 20 字节）

2、使用 UDP 的应用：RIP 路由选择表的更新、网络管理数据 SNMP、域名系统 DNS

3、UDP 报文段结构：源端口号，目的端口号，长度，检验和，均为 16 bits + 报文

长度字段为包括首部在内的 UDP 报文段长度，单位为 byte

检验和字段计算的检验和除了 UDP 报文段以外还包括了 IP 首部的一些字段

UDP 报文段的首部通常为 8 字节

4、UDP 检验和：对 16 比特的字计算带回卷的二进制加法和之后取反

5、使用差错检测的原因：某些链路可能不提供差错检测

报文段存储在某台路由器的内存中时，可能引入比特差错

6、差错处理：丢弃受损的报文段

将受损的报文段交给应用程序并给出警告

3.4 可靠数据传输原理

1、停等协议构建：

rdt 1.0 底层信道可靠

rdt 2.0 底层信道可受损、不丢包（不考虑 ACK、NAK 受损）

checksum 用于差错检测

ACK、NAK 用于接收方反馈，实现重传

rdt 2.1 底层信道可受损、不丢包（考虑 ACK、NAK 受损）

sequence number 用于重传

rdt 2.2 底层信道可受损、不丢包（考虑 ACK、NAK 受损）

ACK 加标号后代替 NAK

rdt 3.0 底层信道可受损、可丢包

countdown timer 用于重传

2、流水线协议构建：

增加序号范围

发送方与接收方两端需要缓存多个分组

3、回退 N 步 GBN 协议（滑动窗口协议）构建：

要求项：发送方维护缓冲区、基序号、下一个序号、计时器
接收方维护下一个按序接收的分组的序号
分组序号段比特为 k 时，序号要对 2^k 取模

发送方：上层调用时，发送方缓存数据
发送窗口未满时，发送下一个包
收到用于累积确认的 ACK 则尽可能滑动窗口
超时则重传所有已发送待确认的分组

接收方：序号为 n 的按序分组被正确收到，为其发送 ACK，并交付给上层
其余情况下，丢弃该分组，并为最近按序接收的分组重新发送 ACK

4、选择重传 SR 协议构建：

要求项：发送方与接收方均需要维护相等长的滑动窗口
滑动窗口的大小小于等于序号空间大小的一半
发送方要为每一个分组维护一个计时器

发送方：上层调用时，发送方缓存数据
发送窗口未满，发送下一个包
收到对特定包的 ACK，则确认它，然后尽可能滑动窗口
哪一个分组超时则重传哪一个分组

接收方：在窗口内的分组被正确接收，为该分组发送 ACK
尽可能滑动窗口，并将数据交付给下层
在窗口左外侧一个窗口大小内的分组被收到，也为该分组发送 ACK
其余情况下，丢弃该分组

5、防止信道突然释放旧分组：

要求项：引入分组在网络中的存活时间
发送方确保一个序号不存在于网络中时，才再次使用该序号

3.5 面向连接的运输：TCP

1、TCP 特性：面向连接、全双工、点对点

2、TCP 三次握手：前两个报文段不承载有效载荷，第三个报文段可以承载有效载荷

3、最大传输单元 MTU：链路层能传输的帧的最大长度
最大报文段长度 MSS：由 MTU 减去 TCP/IP 首部来决定，只包括应用层数据

4、TCP 连接的组成：主机 A（缓存、变量、套接字）+ 主机 B（缓存、变量、套接字）

5、TCP 报文段结构（一般为 20 字节首部）：

源端口号：　用于多路复用/分解
目的端口号：　用于多路复用/分解
序号字段：　为该报文段首字节的字节流编号
确认号字段：　想得到的下一字节的序号，隐含对之前所有字节的累积确认
首部长度：　指示了以 32 bits 的字为单位的 TCP 首部长度
接收窗口：　指示接收方还有多少可用的缓存空间
检验和：　用于差错检查
紧急数据指针：指出紧急数据的最后一个字节
选项字段：　发送/接收方协商 MSS、作为高速网络环境下窗口调节因子
数据字段：　装载应用层报文
标志：　URG： 指示报文段里存在着被发送端置为紧急的数据

PSH： 指示接收方应立即将数据交给上层
ACK： 指示确认号字段有效
RST： 指示不接受连接
SYN： 用于建立连接
FIN： 用于拆除连接

6、往返时间估计：

EstimatedRTT = (1-α)·EstimatedRTT + α·SampleRTT　　α 推荐值为 0.125
DevRTT = (1-β)·DevRTT + β·|SampleRTT - EstimatedRTT|　　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，超时时翻倍，SampleRTT 更新时才按照公式更新

7、TCP 差错恢复：

发送方：每次只对最早的未被确认的报文段启动定时器
超时后，TimeoutInterval 直接翻倍再重传，并不使用公式计算的值
每次只重传最早的未被确认的分组
确认为累积确认，表示之前的字节均已收到
收到三次冗余确认，执行快速重传
接收方：按序到达的的报文段，累积 500ms 内的最多两次确认一起发送 ACK
检测到间隔立即发送冗余 ACK
收到填充间隔低端的报文段，立即发送 ACK

8、TCP 流量控制：

LastByteRcvd – LastByteRead ≤ RcvBuffer
Rwnd = RcvBuffer – [LastByteRcvd – LastByteRead]
LastByteSend – LastByteAcked ≤ rwnd
当主机接收窗口为 0 时，继续发送只有一个字节数据的报文段
通过从该报文段的确认报文中获取接收窗口的更新

9、TCP 连接管理：

连接建立：客户端：向服务器发送 SYN 报文段
服务器：为 TCP 连接分配缓存和变量，并回复 SYNACK 报文段
客户端：为 TCP 连接分配缓存和变量，并回复 ACK 报文段
连接拆除：客户端：向服务器发送 FIN 报文段，等待服务器确认
服务器：向客户端发送 ACK 报文段，确认其请求
服务器：向客户端发送 FIN 报文段，等待客户端确认
客户端：向服务器发送 ACK 报文段，等待一段时间后，结束

10、TCP 的 SYN cookie 机制：

客户端：发送 SYN 报文段，具有四元组（源 IP、目的 IP、源端口、目的端口）
服务器：TCP 序列号 = magic（源 IP、目的 IP、源端口、目的端口、秘密数）
以生成的 TCP 序列号（cookie）回复 SYNACK 报文段
客户端：回复 ACK 报文段，具有四元组（源 IP、目的 IP、源端口、目的端口）
服务器：检查其四元组生成的 cookie 是否刚好比其确认号小 1
确保其合法后，为其分配缓存和变量

3.6 拥塞控制原理

1、拥塞的代价：

分组经历巨大的排队时延

需要重传以补偿因缓存溢出而被丢弃的分组
巨大的时延导致路由器利用链路带宽进行不必要的重传
分组沿路径被丢弃时浪费了上游路由器用于转发它的带宽

2、拥塞控制的方法：

端到端拥塞控制：网络层没有为运输层拥塞控制提供显示支持
网络辅助拥塞控制：网络层构件提供网络中拥塞控制状态的显式反馈信息

3、ATM ABR 的拥塞控制：

默认每 32 个数据信元中夹杂有一个资源管理 RM 信元
拥塞时交换机可以将数据信元的 EFCI 比特置 1
轻微拥塞时，交换机也能直接置位 RM 信元 NI 比特
严重拥塞时，交换机还能直接置位 RM 信元 CI 比特
交换机在拥塞时顺便降低经过的 RM 信元的 ER 值
目的主机根据最近到达的数据信元的 EFCI 比特设置到达的 RM 信元的 CI 比特
经过目的主机处理的 RM 信元被返回给源主机
源主机通过 RM 信元中的 CI、NI、ER 值，调整信元的发送速率

3.7 TCP 拥塞控制

1、TCP 使用端到端拥塞控制，因为 IP 层不提供显式的网络拥塞反馈
具体方法为：让每一个发送方根据所感知到的网络拥塞程度来限制自身速率

2、发送方保证：待确认的数据量 ≤ min { cwnd, rwnd }
其中 cwnd 为拥塞窗口 congestion window，rwnd 为接受窗口 receive window
从而让速率限制在 min { cwnd, rwnd } / RTT 之内

3、指导原则：

超时或者三个冗余都意味着可能丢包，说明网络拥塞，需要降低发送方速率
得到了对未确认报文段的确认，说明网络畅通，应该增加发送方速率
不丢包时，逐渐增长，一旦丢包，迅速回退

4、实现机制：

慢启动： 初始化 cwnd 为 1 MSS，ssthresh 为 64 KB
收到非冗余 ACK，cwnd = cwnd + MSS
cwnd 达到 ssthresh 时，转到拥塞避免
拥塞避免：收到非冗余 ACK，cwnd = cwnd + MSS · (MSS / cwnd)
快速恢复：收到冗余 ACK，cwnd = cwnd + MSS
收到非冗余 ACK，cwnd = ssthresh，回到拥塞避免

任何时候检测到可能出现丢包，都重传，且将 ssthresh 置为 cwnd 的一半
若丢包为超时，cwnd 置为 1 MSS，状态转移到慢启动
若丢包为冗余三次 ACK，cwnd 置为 ssthresh + 3 MSS，状态转移到快速恢复
两种丢包情况对于 ssthresh 的惩罚一样
超时对 cwnd 惩罚最重，需要打回原形
冗余三次 ACK 对于 cwnd 惩罚较轻，只让其回退到原来的一半附近开始

5、平均吞吐量：

（1）$\frac{0.75\times W}{RTT}$，其中 W 为丢包时发送窗口的大小（高度理想化）

（2）$\frac{1.22\times MSS}{RTT\sqrt{L}}$，其中 L 为丢包率

6、公平性：

理想情况：当两连接的吞吐量不相等时，它们也大致具有相等的增长速度，当引发丢包发生时，对大吞吐量的惩罚重于对小吞吐量的惩罚，使得丢包事件的发生，能够缩短两连接吞吐量的差距，最终实现公平

现实情况：具有较小 RTT 的连接比具有较大 RTT 的连接享用更高的吞吐量

第四章 网络层

4.1 概述

1、网络层三大功能：

转发：

将分组从一个输入链路接口转移到适当的输出链路接口的路由器本地动作

路由器通过以分组首部字段的值为索引，在转发表中查询输出链路接口

路由选择：

决定分组从源到目的地所采取的端到端路径，是网络范围内的过程

路由器接收集中式/分布式产生的路由选择协议报文，用于配置转发表

连接建立：

源到目的地沿着所选路径彼此握手，以便在分组流动之前建立起状态

2、路由器：基于网络层字段中的值做转发决定

链路层交换机：基于链路层字段中的值做转发决定

3、网络服务模型：定义了分组在发送与接收端系统之间的端到端运输特性

因特网网络服务模型只提供尽力而为的服务

4.2 虚电路和数据报网络

1、虚电路网络：在网络层提供连接服务（ATM、帧中继）

数据报网络：在网络层提供无连接服务（IP）

2、虚电路组成：

源和目的主机之间的路径（一系列链路和路由器）

沿着该路径每段链路的 VC 号（每条链路的 VC 号可能不同）

沿着该路径的每台路由器的转发表（建立一条虚电路增加相应表项）

3、使用不同 VC 号的原因：

减少了在分组首部中 VC 字段的长度

不同路由器不用就 VC 号进行协商，简化了虚电路的建立

4、虚电路三阶段：

虚电路建立：决定路径、为链路分配 VC 号、填写转发表、预留路径资源

数据传送： 基于入接口与入 VC 号决定出接口与出 VC 号

虚电路拆除：删除路径路由中的转发表

5、信令报文：端系统、路由器之间传递的用于建立虚电路的报文

信令协议：交换信令报文的协议

6、路由转发表：

虚电路：将（入接口，入 VC 号）映射到（出接口，出 VC 号）

数据报：采用最长前缀匹配，将目的地址映射到链路接口

4.3 路由器工作原理

1、路由器组成：

路由器转发平面：用硬件实现

输入端口： 将一条输入的物理链路与路由器相连接

与位于入链路远端的数据链路层交互
查询转发表决定路由器的输出端口
交换结构：连接路由器的输入端口和输出端口
输出端口：类似输入端口
路由器控制平面：用软件实现
路由选择处理器：执行路由选择协议
维护路由选择表以及连接的链路状态信息
为路由器计算转发表
执行网络管理

2、影子副本：路由选择处理器将转发表副本存放在每个端口，避免集中式处理
3、线路前部阻塞：输入队列中排队的分组必须等待其前面正在等待的分组被发送
4、交换结构：
经内存交换：分组从输入端口复制到内存，再复制到输出端口缓存
经总线交换：分组通过总线发往所有输出端口，只有特定输出端口能保存
纵横式交换：能并行转发具有不同输入与输出端的分组

4.4 网际协议：因特网中的转发和编址

1、因特网网络层三组件：
IP 协议：网络层主要协议
路由选择协议：用于计算转发表
ICMP 协议：因特网控制报文协议，用于因特网的网络层差错和信息报告
2、IPv4 数据报格式（首部通常为 20 字节）：
版本号：规定 IP 协议版本，以便让路由器确定如何解释剩余部分
首部长度：以 32 bits 为单位
服务类型：区分不同类型的 IP 数据报
数据报长度：首部加上数据的长度，以字节为单位
标识：发送主机给它发送的每个数据报的标识号加 1
标志：指示某分片是否是数据报的最后一片，0 则是，1 则不是
片偏移：确保目的主机按正确的顺序重新组装片
寿命：还能经过的路由跳数，为 0 时该数据报必须丢弃
上层协议：指示 IP 数据报的数据部分应该交给哪个运输层协议
首部检验和：以 2 字节为单位，相加求和，每台路由器都要重新计算该值
源 IP 地址：
目的 IP 地址：
选项：允许 IP 首部扩展（IPv6 中已删去）
数据：
3、最大传送单元 MTU：链路层帧能承载的最大数据量
4、IP 数据报大于 MTU 时，路由器将其拆分成片，最终全部在端系统重新组装
5、分片的过程：
标识号不变
标识号只有最后一片为 0，其余为 1
片偏移指示前面数据量大小，以 8 字节为单位
6、接口：主机/路由器与链路之间的边界，主机只有一个，路由器有多个
7、IP 地址：与接口相关联，具有全球唯一性（NAT 后面的接口除外）
8、子网：互联主机接口与某个路由器接口的网络

子网掩码：用于划分 IP 地址的网络地址与主机地址

9、因特网的地址分配策略为无类别域间路由选择 CIDR

10、使用单个网络前缀通告多个网络的能力为地址聚合、路由聚合、路由摘要

11、默认网关：第一跳路由器地址

12、动态主机配置协议 DHCP：

DHCP 服务器发现：新加入的主机用广播地址发送 DHCP 发现报文

DHCP 服务器提供：服务器响应以广播地址发送 DHCP 提供报文回馈相关信息

DHCP 请求：客户选择配置参数后向选中的服务器发送 DHCP 请求报文

DHCP ACK：服务器用 DHCP ACK 报文确认

13、保留地址空间：

10.0.0.0/8

172.16.0.0/12

192.168.0.0/16

14、网络地址转换 NAT：

将来自 NAT 背后的（源 IP 地址、端口号）映射为 NAT 面向广域网的（NAT 的 IP 地址、新端口号），即通过使用虚拟端口号的辅助，来扩展寻址能力

通用即插即用 UPnP 协议是一种允许主机发现并配置邻近 NAT 的协议，NAT 穿越正越来越多地由 UPnP 协议提供

15、反对 NAT 的理由：

端口号是用于进程编址的，而不是用于主机编址的

路由器通常仅应当处理到网络层分组

违反了端到端原则，即结点不应介入主机与主机的直接对话

应使用 IPv6 来解决 IP 地址短缺问题

16、因特网控制报文协议 ICMP：

作为 IP 有效载荷承载，用于主机和路由器彼此沟通网络层的信息

17、IPv6 数据报格式：

版本号：

流量类型：类似 IPv4 服务类型字段

流标签：用于标识一条数据报的流

有效载荷长度：有效载荷的字节数

下一个首部：类似 IPv4 上层协议字段

跳限制：类似 IPv4 的 TTL

源地址：扩展到 128 bits

目的地址：扩展到 128 bits

数据：

18、IPv6 特性：

将地址容量从 32 bits 扩展到了 128 bits

不允许中间路由器进行分片，数据报太大时直接丢弃，告知端系统分片

不再计算首部检验和

不再显式包含选项，而将其转移到下一个首部指出的位置上

19、IPv4 向 IPv6 的迁移：双栈、建隧道

4.5 路由选择算法

1、默认路由器：与主机相连接的第一跳路由器

源路由器：源主机的默认路由器

目的路由器：目的主机的默认路由器

2、全局式路由选择算法：具有全局状态信息，也叫链路状态算法

分散式路由选择算法：没有结点拥有关于所有网络链路费用的完整信息

静态路由选择算法：路由随时间流逝变化缓慢

动态路由选择算法：周期性地运行或直接响应拓扑或链路费用的变化

负载敏感算法：链路费用会动态变化以反映出底层链路的当前拥塞水平

负载迟钝算法：链路费用不明显地反映其当前拥塞水平

3、链路状态 LS 算法：即 Dijkstra 算法

4、距离向量 DV 算法：即 Bellman-Ford 算法

每个结点都维护它自身到所有目的地的费用的估计值，作为距离向量

每个结点都存储其所有邻居的距离向量的最新副本

每次收到邻居点或相邻边代价变化时，检查自身是否可以更新

若自身成功更新，则将更新后的距离向量发送给邻居以供其储存

可以通过增加毒性逆转来解决 2 个结点的无穷计数问题

5、链路状态 LS 算法 VS 距离向量 DV 算法

报文复杂性：LS 算法每个结点向所有结点发送报文

DV 算法只在相邻结点之间交换报文

收敛速度： LS 算法相较而言收敛较快

DV 算法收敛较慢，且在收敛时会遇到路由选择环路问题

健壮性： LS 算法的计算在某种程度上是分离的，提供了一定的健壮性

DV 算法中一个不正确的结点的计算值会影响到整个网络

6、自治系统 AS：由一组通常处在相同管理控制下的路由器组成

自治系统路由选择协议：在一个自治系统内运行的路由选择算法

网关路由器：一个 AS 中负责向其他 AS 转发分组的路由器

热土豆路由选择：路由器总是选择一个可到目的地的 AS 内代价最低的网关路由器

4.6 因特网中的路由选择

1、AS 内路由选择协议（内部网关协议）：路由选择信息协议 RIP、开放最短路优先 OSPF

AS 间路由选择协议（外部网关协议）：边界网关协议 BGP

2、RIP 协议：

通常设置于下层 ISP 和企业网中

是一种距离向量协议，运行方式类似于 DV 算法

以经过的子网数量（跳数）作为路径费用

最大费用限制为 15，使得 RIP 的使用限制在网络直径不超过 15 跳的 AS 内

每台路由器维护路由选择表（距离向量 + 转发表）

路由选择信息在邻居间通过 RIP 响应报文（RIP 通告）来交互

RIP 通告大约每 30 秒交互一次，超过 180 秒不交互，默认不可达

RIP 通告即路由选择表，路由器每次收到 RIP 通告后合并进自己的选择表

RIP 使用运输层协议 UDP 上的端口 520 来实现网络层协议的信息维护

3、OSPF 协议：

通常设置于上层 ISP 中

是一种链路状态协议，运行方式类似于 Dijkstra 算法

链路的费用权值由网络管理员配置

路由器向系统内的所有其他路由器广播路由选择信息

链路状态变化时，路由器广播链路状态信息，无变化也会周期性地进行广播

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、可使用等费用的多条路径、支持单播与多播、支持层次结构等优点

4、BGP 协议：

建立了半永久 BGP TCP 连接（BGP 会话）的路由器对成为 BGP 对等方
跨越 AS 的 BGP 会话为外部 eBGP 会话，AS 内的 BGP 会话为内部 iBGP 会话
不作为流量中转的 AS 成为桩网络，除桩网络外的 AS 都具有自治系统号 ASN
路由器通过 BGP 会话交互的信息为前缀与属性值所构成的路由
属性值 AS-PATH 包含了该路由已通过的那些 AS 的 ASN
属性值 NEXT-HOP 为该路由中连接本 AS 的上一个 AS 的路由器的 IP 地址
BGP 是面向策略的 AS 间路由选择协议，除了跳计数外没有费用的概念
路由选择顺序：偏好 –> 最短 AS-PATH –> 最靠近 NEXT-HOP –> BGP 标识符

5、在 AS 间和 AS 内选择不同路由选择协议的原因：

策略：AS 内优先考虑代价，AS 间优先考虑策略
规模：AS 间路由选择要考虑可扩展性，AS 内路由选择不需要
性能：AS 间路由选择能依据策略选择路径，AS 内路由选择要关注于性能

4.7 广播和多播路由选择

1、用单播实现广播：

实现：源结点产生分组的 N 份副本，并利用单播路由向 N 个目的地址传输
缺点：效率不高
接收方地址不一定为发送方所知
广播的目的是生成和更新单播路由，用目的取代手段不够明智

2、无控制洪泛广播：

实现：源结点向它的所有邻居发送分组的副本
当某结点收到一个分组时，保存并向邻居转发
缺点：有圈的情况下将无法停止
广播风暴在网络中产生大量副本压垮网络

3、序号控制洪泛（受控洪泛）广播：

实现：广播分组中加入源结点地址和广播序号
每个结点维护接收到的每个广播分组的序号列表
当收到在列表中的广播分组时，直接丢弃
当收到不在列表中的分组时，保存并向邻居转发
缺点：不能完全避免冗余分组的传输

4、反向路径转发 RPF（受控洪泛）广播：

实现：广播分组中加入源结点地址
每个结点维护它在发送方的单播路径上的前驱结点
当收到来自非前驱结点的分组时，直接丢弃
当收到来自前驱结点的分组时，保存并向邻居转发
缺点：不能完全避免冗余分组的传输

5、生成树广播：

实现：基于中心结点（汇合点/核）建立一棵生成树
每个结点维护它在生成树中的邻居
发送分组时只在生成树链路中进行

6、多播服务：

多播分组仅被交付给网络结点的一个子集

D 类多播地址为表示一组接收方的单一标识

多播组为一个与 D 类多播地址相关联的接收方小组

使用因特网组管理协议 IGMP 与多播路由选择协议

7、IGMP 协议：

运行在一台主机和与其直接相连的路由器之间

membership_query 报文：路由器用于查询接口上的主机已加入的多播组集合

membership_report 报文：主机通知路由器其加入的多播组集合

leave_group 报文：主机通知路由器其离开了某多播组（可以省略）

当无主机响应一个具有给定组地址的查询报文时，则断定无主机还在该多播组

8、软状态机制：

状态若未被显式地更新，则通过超时事件被删除

9、多播路由选择算法：

目标：发现一棵链路的树连接了所有某多播组的路由器

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

10、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：链路、接入网和局域网

5.1 链路层概述

1、结点：运行链路层协议的任何设备（主机、路由器、交换机、WiFi 接入点）

链路：沿着通信路径连接相邻结点的通信信道

2、链路层提供的服务：

成帧

链路接入，使用媒体访问控制协议 MAC

可靠交付，通过确认与重传实现

差错检测与纠正，用硬件实现

3、网络适配器（网卡）：类似于 I/O 设备，连接在 PCI 上，包含控制器和物理传输线路

4、大部分链路层在硬件中实现，部分在软件中实现，链路层是硬件软件结合的地方

5.2 差错检测和纠正技术

1、使用差错检测和纠正比特 EDC 来增强数据 D，可以尽可能地检测出比特差错

2、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，对每行每列使用一维奇偶校验

3、前向纠错：接收方检测差错并纠正

后向纠错：接收方检测差错并请求重传来恢复

4、检验和方法：将数据划分为 k 比特的序列，相加后取反

5、循环冗余检测 CRC：

所有加减采用异或的方式进行

对 r+1 位的生成多项式（二进制串）
在数据后添加 r 个 0，然后除以生成多项式
用所得余数替换数据后添加的 r 个 0，即得 CRC 编码（多项式编码）
每个 CRC 标准都能保证检测出最多 r 比特的差错和任何奇数个的比特差错

5.3 多路访问链路和协议

1、多路访问协议：用于协调多个发送和接收结点对一个共享广播信道的访问

2、理想多路访问协议的特性：

仅有一个结点有数据要发送时，应能让它使用到全部的带宽
多个结点有数据要发送时，平均吞吐量应大致相等
协议是分散的，不会因某主结点故障而使整个系统崩溃
协议简单，实现不昂贵

3、信道划分协议：

时分多路复用 TDM：时间划分为时间帧，帧划分为时隙
频分多路复用 FDM：信道划分为不同频段
码分多址 CDMA：每个结点用其唯一编码来编码数据，可同时传输消除碰撞

4、随机接入协议：

时隙 ALOHA：有新帧要发送时，在下一个时隙开始时传输整个帧
若出现碰撞，则之后的每次重传以概率 p 进行
效率定义为长期运行中成功时隙的份额，约为 0.37

纯 ALOHA：有新帧要发送时，立即传输整个帧
若出现碰撞，则之后的每次重传以概率 p 进行
效率为时隙 ALOHA 的一半，约为 0.185

载波侦听多路访问 CSMA：
结点传输前先听信道，检测到一小段时间没有传输时才开始传输
信道传播时延越大，结点不能及时侦听到传输的机会越大

具有碰撞检测的载波侦听多路访问 CSMA/CD
检测到碰撞时立即停止传输
效率为$1/(1+5\cdot d_{prop}/d_{trans})$

二进制指数后退算法：
经历 n 次碰撞后，随机从 { 0, 1, 2, ……, 2^n - 1 } 中选取 K 值
然后等待发送 512 比特所需时间的 K 倍

5、轮流协议：

轮询：主结点轮询到的结点才可以传输
能传输的帧的最大数量由主结点通知

令牌传递：持有令牌的结点才可以传输
无帧可发或发送完一个帧，将令牌传递给下一个结点

5.4 交换局域网

1、MAC 地址：（LAN 地址、物理地址）

格式：6 字节，以十六进制数表示为 XX-XX-XX-XX-XX-XX
性质：没有两块适配器具有相同的地址
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：

ARP 为同一子网上的主机和路由器将 IP 地址解析为 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 IP、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层的协议

3、发送数据报的过程：

主机查询 ARP 表，是否具有对应 IP 地址的 MAC 地址
若未在 ARP 表中查到相应表项，使用 ARP 查询报文在子网中进行广播
ARP 查询报文中包含目的 IP 地址和目的 MAC 地址 FF-FF-FF-FF-FF-FF
子网中所有适配器拆封 ARP 查询报文的帧，将其上交给自身的 ARP 模块
主机检查自身 IP 地址是否与目的 IP 地址相匹配，匹配则回应 ARP 响应报文
路由器检查目的 IP 地址是否应由自己转发，是则回应 ARP 响应报文
源主机收到 ARP 响应报文后，把 IP 地址到 MAC 地址的映射插入 ARP 表
主机向目的 MAC 地址发送链路层帧
所有适配器都会处理到达自身的帧，但只将 MAC 地址符合要求的帧上交

4、以太网的变革：同轴电缆 + 转发器 –> 集线器星型拓扑 -> 交换机星型拓扑
转发器：物理层设备，在输入端接收信号并在输出端再生信号，使得传输更长距离
集线器：物理层设备，作用于比特，放大传输其受到的信号
交换机：链路层设备，作用于帧，不会出现碰撞

5、以太网帧结构：

数据字段：46—1500 字节，超出需要分片，少于则需要填充
目的地址：目的适配器的 MAC 地址 6 字节
源地址： 源适配器的 MAC 地址 6 字节
类型字段：上层协议号 2 字节（类比 TCP 端口号、IP 协议字段）
CRC： 循环冗余检测码 4 字节
前同步码：前 7 字节为 10101010 用于唤醒和同步，最后 1 字节为 10101011

6、以太网的差错检验：

使用 CRC 校验收到的帧，通过则保留，不通过则丢弃
不管校验结果如何，都不会反馈校验信息

7、以太网标准：例 100BASE-T 代表 100Mbps 传输速率的基带以太网，媒介为双绞铜线

8、链路层交换机：

本身不具有 MAC 地址，对于子网中的主机和路由器是透明的
全双工，交换机和结点可以同时向对方发送帧而不产生碰撞
把接收的所有帧的源 MAC 地址到接口的映射加入交换机表，并加注当前时间
接收的帧的目的 MAC 地址在交换机表中时，按照映射转发到特定接口
接收的帧的目的 MAC 地址不在交换机表中时，广播该帧
及时删除交换机表中已经老化的映射

9、链路层交换机的性质：

消除碰撞，使得最大聚合带宽为交换机所有接口速率之和
隔离异质链路，使得不同链路能以不同速率在不同媒体上运行
强化安全，检测异常适配器并断开连接
方便管理，收集带宽使用的统计数据、碰撞率和流量类型等，提供管理员使用

10、交换机毒化：

向交换机发送大量具有不同伪造源 MAC 地址的分组

交换机表被伪造表项填充满，导致大部分合法分组被广播

嗅探器从而俘获到合法分组

11、交换机 VS 路由器

交换机：优点：即插即用、更高的分组过滤和转发速率

缺点：拓扑有生成树限制、无法抵抗广播风暴

路由器：优点：拓扑无生成树限制、防火墙保护可以抵抗广播风暴

缺点：不是即插即用、对分组的处理时间更长

12、虚拟局域网：

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

不用 VLAN 之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 标签用于跨越 VLAN 干线

VLAN 标签：2 字节标签协议标识符、12 比特 VLAN 标识符、3 比特优先权

第六章 无线网络和移动网络

6.1 概述

1、无线主机：可以移动的端系统设备

无线链路：覆盖区域（传输距离）、链路速率

基站：无线主机与更大网络之间的中继，协调与之相关联的多个无线主机的传输

网络基础设施：无线主机希望与之通信的更大网络

2、基础设施模式：与基站相关联的主机称为以基础设施模式运行

切换：无线主机移动到另一个基站的覆盖范围后将改变与之相关联的基站

3、无线网络分类：

单跳 + 基于基础设施 ：802.11 网络、3G 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 无线链路和网络特征

1、无线链路的特性：

路径损耗：信号强度随着距离的增加而减弱

信噪比 SNR：信号与噪声强度的相对度量；同一频段信号也会相互干扰

多径传播：电磁波经反射在发送方和接收方之间走了多条路径，使得信号模糊

2、物理层调试技术的特征：

给定调制方案下，SNR 越高，BER 越低

给定 SNR 下，使用传输率越高的调制技术，BER 越高

3、无线网络中的干扰：

隐藏终端问题：在某处造成干扰的两方由于物理阻挡互不自知

信号强度衰减：在某处造成干扰的两方信号强度不足以传播到对方处让其察觉

4、CDMA 编码：

0 当成-1，1 还是 1

每个数据比特占一个时隙，一个时隙分 M 个微时隙

每个微时隙一个比特编码，M 个微比特构成一个编码基向量

每个数据比特乘在 M 比特编码基向量上，得到该数据比特的编码向量
不同编码基向量产生的编码向量通过加法叠加在一起，成为编码空间的某向量
编码空间的任一向量在某编码基向量上的投影，即为其在该基向量上的编码

6.3 WiFi：802.11 无线 LAN（WiFi）

1、标准：802.11b　2.4—2.4835 GHz　最高 11 Mbps
802.11a　5.1—5.8 GHz　最高 54 Mbps
802.11g　2.4—2.485 GHz　最高 54 Mbps
802.11n　MIMO

2、体系结构基本构件模块：基本服务集 BSS（多个无线站点 + 接入点 AP）
每个 AP 在安装时，被分配服务集标识符 SSID
85 MHz 的频段被划分为 11 个部分重叠的信道，当两信道间有 4 个信道时才无重叠

3、每个 AP 周期性地发送信标帧（包括其 SSID 和 MAC 地址）
无线站点为了得知正在发送信标帧的 AP，扫描 11 个信道

4、被动扫描：
定义：无线站点扫描信道、监听信标帧
过程：AP 发送信标帧
无线站点收到信标帧，向选择的 AP 发送关联请求帧
被选中的 AP 向无线站点发送关联响应帧

主动扫描：
定义：无线站点向位于无线主机范围内的所有 AP 广播探测帧
过程：无线站点广播探测请求帧
AP 收到探测请求帧，发送探测响应帧
无线站点向选择的 AP 发送关联请求帧
被选中的 AP 向无线站点发送关联响应帧

5、无线站点的鉴别：
基于站点的 MAC 地址允许其接入无线网络
使用用户名和口令，AP 使用鉴别服务器帮助其鉴别

6、802.3 MAC 协议 = 以太网 带碰撞检测的载波侦听多路访问协议 CSMA/CD
802.11 MAC 协议 = 无线网 带碰撞避免的载波侦听多路访问协议 CSMA/CA
区别：802.11 使用碰撞避免而不是碰撞检测
802.11 使用链路层确认/重传 ARQ 方案

7、802.11 不使用碰撞检测的原因：
802.11 适配器接收信号强度远小于发送信号强度，发送接收能力差异大
隐藏终端和信号衰减导致碰撞检测难以实现

8、802.11 链路层确认：
目的站点收到通过 CRC 校验的帧
等待一个短帧间间隔 SIFS 后，发回确认帧
发送站点在给定时间未收到确认帧，执行重传
若干次重传后仍未被确认，放弃发送该帧

9、802.11 碰撞避免：
检测到信道空闲，等待分布式帧间间隔 DIFS 后发送该帧
否则，选择随机回退值，并在信道空闲时递减该值
计数值为 0 时，站点发送整个数据帧并等待确认
成功发送一个帧后，退回第二步，而不是第一步，以保证公平

只要发送开始，不管是否产生碰撞，都将该帧发送完毕

10、处理隐藏终端：

请求发送 RTS 控制帧：发送方使用 RTS 预约一段占用时间

允许发送 CTS 控制帧：接收方广播 CTS 帧同意 RTS 并抑制其他发送方

11、802.11 的 4 个地址字段：

地址 1：要接收该帧的无线站点的 MAC 地址

地址 2：传输该帧的站点的 MAC 地址

地址 3：相应路由器接口的 MAC 地址

地址 4：自组织网络中用到

6.5 移动管理：原理

1、归属网络：移动结点的永久居所

外部网络：移动结点当前所在网络

归属代理：归属网络中代表结点执行移动管理功能的实体

外部代理：外部网络中帮助结点执行移动管理功能的实体（产生 COA / 交代 COA）

永久地址：移动结点在归属网络的地址

转交地址：移动结点在外部网络的地址（COA）

通信者：希望与移动结点通信的实体

2、间接路由选择：

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，并在归属代理处注册

通信者直接将数据报发往归属代理

归属代理将数据报封装在加注目的地址为 COA 的数据报内并转发

外部代理拆封数据报并发送给移动结点

3、直接路由选择：

通信代理从归属代理处获得移动结点的锚外部代理的 COA

通信代理使用 COA 直接与锚外部代理联系

结点移动到新的外部网络时把注册好的 COA 转达给锚外部代理

锚外部代理完成数据报的转发

6.6 移动 IP

1、标准：代理发现、向归属代理注册、数据报的间接路由选择

2、过程：移动结点广播代理请求报文（可省略）

外部代理周期性地在链路上广播 ICMP 报文通告其服务，给出 COA 集合

收到外部代理通告的移动结点选择 COA 并向外部代理发送移动 IP 注册报文

外部代理收到注册报文后记录移动结点永久 IP 地址并向归属代理注册

归属代理接收注册请求并检查真实性和正确性，之后发送注册响应

外部代理接收注册响应，再将其转发给移动结点

6.8 无线和移动性：对高层协议的影响

1、解决无线链路降低 TCP 连接性能的方法：

本地恢复：802.11 ARQ 协议

让 TCP 发送方知晓无线链路，与有线链路进行区分

分离连接：分离成两个运输层连接，为无线链路配置专属协议

第八章 计算机网络中的安全

8.1 什么是网络安全

1、安全通信特性：机密性、报文完整性、端点鉴别、运行安全性

8.2 密码学原则

1、对称密钥系统：发送方与接收方的密钥相同并且保密

公开密钥系统：一个密钥为一方所知，一个密钥为全世界所知

2、入侵者攻击：

唯密文攻击： 入侵者只能得到截取的密文，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：入侵者拥有将明文转换为密文的能力

3、单码代替密码：即凯撒密码，每个字母用偏移量为 k 的字母代替

多码代替密码：在不同位置使用不同单码代替密码

块密码：按比特分块，按照一一对应的映射加密

密码块链接：前一块的输出作为后一块的输入，导致相同明文产生不同的密文

4、RSA 公开密钥系统：

密钥产生：选择大素数 p 和 q

计算 n = pq 和 z = (p – 1)(q – 1)

选择小于 n 的一个数 e，使得 e 和 z 互质

求一个数 d，使得 ed ≡ 1 (mod z)

得到公钥 (n, e) 和私钥 (n, d)

加密过程：$c = m^e \bmod n$

解密过程：$m = c^d \bmod n$

8.3 报文完整性和数字签名

1、密码散列函数：

以 m 为输入，得到固定长度的字符串 H(m)

找到任意两个不同的报文 x 和 y 使得 H(x) = H(y) 在计算上是不可能的

2、报文鉴别码 MAC：

发送者对报文 m 级联鉴别密钥 s 生成 m+s，计算散列 H(m+s)

发送者发送扩展报文(m, H(m+s))

接收者对报文 m 级联鉴别密钥 s 生成 m+s，计算散列 H(m+s)

接收者验证与接收的散列值是否相等

3、数字签名：

发布者对报文 m 计算散列 H(m)，再用自己的私钥对散列加密（签名）

获取者对报文 m 计算散列 H(m)，再与用发布者公钥恢复的签名进行比较

4、公钥认证：

认证中心 CA 验证某实体的身份，为其生成绑定身份和公钥的证书

CA 对证书利用自己的私钥进行数字签名后发布

接收者先递交自己的证书给发送者

发送者使用 CA 的公钥验证证书的合法性后提取接收者的公钥

5、端点鉴别：

访问者声明自己的身份

鉴别者提供一个不重数 R

访问者使用与鉴别者的共享密钥来加密不重数，然后发送给鉴别者

鉴别者解密后验证是否等于使用的不重数 R

附：2016 年秋考试记录

【考试时间】

2017 年 1 月 5 日 下午 2:30 — 4:30（实际情况是大部分同学都在 4:00 做完交卷了）

【命题老师】

张信明老师、田野老师联合命题

【考试题型】

第一大题：选择题（ 4’ × 10 = 40’ ）

1、互联网＋是什么？

2、关于协议栈以下说法错误的是？

3、关于 TCP 协议以下说法错误的是？

4、802.11 没有实现以下哪一项功能？

5、关于路由选择算法说法错误的是？

6、IPv4 和 IPv6 的地址空间大小分别是？

7、（记不全了，总而言之内容很杂，普遍反映选择题不好做）

第二大题：简答题（ 4’ × 5 = 20’ ）

1、给出至少四种应用层协议，并指明其端口号

2、分析网络层转发与路由选择的区别

3、分析链路层交换机是如何提升网络性能的

4、分析 OSPF 和 RIP 协议各自的缺点

5、分析 802.3 与 802.11 协议在处理冲突方面的差异

第三大题：综合题（ 40’ ）

1、分析 TCP 拥塞控制的折线图 14’

2、关于 TCP 握手阶段序号与确认号的变化 6’

3、使用 RIP 算法更新一个结点的转发表 8’

4、设计一套能够确保报文机密性与完整性的方案 12’