第一部分:小测题

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

7.对于无控制洪泛、受控洪泛和生成树广播三种广播选路方式，下列说法是否正确：a) 一个节点可能收到同一个广播分组的多个拷贝；b) 一个节点可能在相同的出链路上多次转发同一个广播分组
答： 无控制洪泛： a)对， b)对。 受控洪泛： a)对， b)错。 生成树广播： a)错， b)错。

8.一个B类网络128.16.0.0/16被网络管理员划分为16个大小相同的子网，则子网掩码为255.255.240.0 。如果按照IP地址从小到大对子网进行编号，写出第2个子网的地址范围，用a.b.c.d/x的形式表示128.16.16.0/20 。

9.一个路由器收到以下四条新的前缀： 157.6.96.0/21、157.6.104.0/21、157.6.112.0/21 和 157.6.120.0/21，如果这些地址使用同一条输出线路，它们能被聚合吗？如果能，请给出聚合后的前缀；如果不能，请说明原因。答：能，聚合后的前缀是157.6.96.0/19

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.多址接入协议（multiple access protocol）划分为哪三种类型?其中，哪一种（或几种）是无冲突的协议? 哪一种（或几种）是有冲突的协议?
答: 多址接入协议划分为信道划分、随机接入、轮流协议三种类型。信道划分和轮流协议是无冲突的，随机接入是有冲突的。

5. 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

6. 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。

7.计算依据:传输速率*相距最远的两个站点间往返传播时延假设节点 A、B、C 连接到同一个广播局域网上，A 向 B 发送的单播帧（dest MAC = B），C 的适配器能收到吗？如果能收到，C 的适配器会处理这个帧吗？ 如果会处理，C 的适配器会把帧中的 IP 数据报交给自己的网络层吗?
答: 能收到; 会处理; 但不会将 IP 包交给自己的网络层

7. 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。

8.交换机是如何提升网络性能的?
划分冲突域

9.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

10. 首先计算 frame 100110101111 及 G(x) = (x4 + x3 +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

11.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

12.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.

13.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))

14.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(根据转发表转运分组)
选路:确定分组从源路由器到目的路由器的路径(计算转发表)
建立连接(某些架构)
传输层连接:进程-进程，连接状态仅保存在端系统中
网络层连接:主机-主机，连接状态保存在源主机、目的主机及所有中间路由器上

下一跳方法: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
可对单个分组提供的服务
保证交付；具有时延上界的保证交付
可对分组流提供的服务
有序交付；保证最小带宽；保证最大时延抖动（分组端到端时延的最大差异）

Network Architecture	Service Model	Guarantees ? Bandwidth	Loss	Order	Timing	Congestion feedback
Internet	best effort	none	no	no	no	no (inferred via loss)
ATM	CBR	恒定速率	yes	yes	yes	无拥塞发生
ATM	ABR	最小速率	no	yes	no	yes

网络层服务:主机-主机；一个网络不能同时提供两种服务；在网络核心实现
传输层服务:进程-进程；可同时提供两种服务；在网络边缘实现

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:1.从源主机到目的主机的端到端路径2.沿途每条链路上的 VC 号(VC 号仅有本地意义)3.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)
注意：对于一个虚电路网络层，沿两个端系统之间路径上的路由器都要参与虚电路的建立，且每台路由器都完全知道经过它的所有虚电路
4、虚电路三阶段：1.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2.数据传送： 基于入接口与入 VC 号决定出接口与出 VC 号3.虚电路拆除：删除路径路由中的转发表
虚电路:是一种信令协议。信令报文:专门用于建立、维护、拆除虚电路的控制报文，信令协议：交换信令报文的协议。

Internet（数据报网络）
计算机之间交换数据。弹性服务，没有严格的时序要求终端（计算机）具有智能。可将复杂的工作（如差错控制）推到网络边缘，以保持网络简单
数据报网络只提供最小服务。可以运行在各种链路之上；增加新服务只涉及终端

ATM（虚电路网络）
由电信网发展而来：严格的时序和可靠性要求；要求保证服务；终端无智能或很少智能：复杂工作由网络完成，保持终端简单
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 路由器组成

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（查表，排队，转发）：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：(组装，排队，调度）：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)
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 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。

Ramdom Early Detection（RED）
主动队列管理的一种，与 TCP 的拥塞控制机制一起使用
路由器在每个端口上维护输出队列的平均长度：
AvgLen = (1- Weight)×AvgLen + Weight×SampleLen
当平均队列长度达到第一个阈值 minth 时，按照丢弃概率p丢弃到来的分组。当平均队列长度达到第二个阈值 maxth 时，丢弃每一个到达的分组。
概率 p 是平均队列长度和上一次丢弃距当前时间的函数，分组队列长度越大，丢弃间隔越大，p 也越大。

假设Rswitch比Rline快n倍，
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；阻塞型与非阻塞型两种，阻塞型互联网络会产生阻塞。先进设计：将分组划分成固定长度的信元（cell）送入交换结构，离开交换结构后再组装成分组

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:通常20字节bytes首部
版本号4bit，报头长度 H(4bits)、服务类型TOS 8 bits、数据报长度(**字节为单位**,16bits)、标识号16bits/标志3bits/片偏移13bits、寿命8bits(剩余最大跳数，转发前-1)、上层协议8bits(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，最后一片标志比特 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 自带分段，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
网络号有效、主机号全为 0 的地址：保留给网络本身。
网络号有效、主机号全为 1 的地址：保留作为定向广播，即在网络号指定的网络中广播（仅用作目的地址）
32 位全 1 的地址：本地广播地址，表示仅在发送节点所在的网络中广播（仅用作目的地址）
32 位全 0 的地址：指示本机（仅用作源地址）
网络号为 0、主机号有效的地址：指代本网中的主机。
3 子网(主机号进一步划分成子网号和主机号两部分)
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。
具有相同子网地址、不需要通过路由器就可以相互到达的网络接口构成一个子网
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

路由器默认网关：第一跳路由器地址

路由表项类型:
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(DHCP 是一个客户/服务器模式的应用协议)
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)
NAT 妨碍 P2P 应用程序：需要 NAT 穿越技术
7 ICMP:因特网控制报文协议 Ping&Traceroute
主要任务:报告差错（主机或路由器使用 ICMP 协议传递网络层上的一些信息），但不能纠错。
ICMP 报文有询问和错误报告两类：
询问：用来请求一些信息，通常采用请求-响应模式交互
错误报告：发现错误的节点向源节点报告错误信息，不需响应
由于 ICMP 报文可能需要经过几个网络才能到达源节点，ICMP 报文被封装在 IP 包中传输。
ICMP 通常被认为是 IP 协议的一部分，因为 IP 协议使用 ICMP 向源节点发送错误报告。

查询：对某些网络问题进行诊断；目前尚在使用的两对查询报文：回送请求与回送应答；时间戳请求与时间戳应答
对于携带 ICMP 差错报文的数据报，不再产生 ICMP 差错报文；对于分片的数据报，如果不是第一个分片，则不产生 ICMP 差错报文；对于具有组播（也称多播）地址的数据报，不产生 ICMP 差错报文；对于具有特殊地址(如 127.0.0.0 或 0.0.0.0)，不产生 ICMP 差错报文
ICMP 报文格式:
首部(8 字节)
前 4 个字节所有类型的报文相同；后 4 个字节与报文类型相关可变长度的数据部分
原始数据报的 IP 首部；该数据报数据部的前 8 个字节：端口号(UDP,TCP)和序号(TCP)

Ping 利用 ICMP 报文测试目的主机是否活跃,以及去往目的主机的路径是否正常

Traceroute 测试到达目的主机的路由（经过的路由器）
8 IPV6:(最初的动机: IPv4 地址将很快耗尽；进一步的动机:简化头部格式，加快数据报处理和转发；支持服务质量；支持多播；支持移动性；增强安全性；IPv6 与 IPv4 不兼容，但与其它所有因特网协议都兼容。)
地址 32 位->128 位
IPv6 定义了三种地址类型:
单播地址:一个特定的网络接口；多播地址:一组网络接口；任播地址(anycast)：一组网络接口中的任意一个（通常是最近的一个
VER,PRI,Flow label,Payload length,Next header,Hop limit,Source address,Dest… address
IPv6 数据报格式: IPv6 数据报以一个 40 字节的基本头开始,后面跟零个或多个扩展头，然后是数据。
PRI(traffic class): 作用：发送方在该域定义数据报的优先级:路由器发现网络拥塞时，按优先级从低到高的顺序丢弃包
IPv6 将网络流量划分为两大类：受拥塞控制的流：非实时流属于这一类，优先级 0~7，按照重要性及用户体验设定
不受拥塞控制的流：实时多媒体流属于这一类，优先级 8~15，尚无标准，可以按照用户要求的服务质量等级定义.
Flow:流是具有相同传输特性（源/目的、优先级、选项等），并要求相同处理(使用相同的路径和资源、具有相同的服务质量和安全要求等)的一系列数据包。流由源地址和流标签（flow label）唯一标识。流标签由发送方分配，不支持流的节点忽略该域。支持流的路由器维护一张流表(flow table),记录每一个流需要的处理；收到数据包后，根据源地址和流标签查找流表，进行相应的处理。流的引入使得 IPv6 具备了对数据包进行区分处理的能力。
不允许中间路由器分片，大大直接丢弃：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。
ICMPv6:合并了 IPv4 中的 ARP 和 IGMP，并取消了 RARP（该协议的功能已被其它协议取代）； 仍然使用差错报告和查询两类报文。从 IPv4 过渡到 IPv6:双协议栈方案：支持 IPv6 的主机和路由器同时运行 IPv4 和 IPv6;源节点先查询 DNS：若 DNS 返回 IPv4 地址，发送 IPv4 分组；若返回 IPv6 地址，发送 IPv6 分组:双栈节点同时拥有 IPv4 和 IPv6 地址
穿越 IPV4 网络:头转换(报头转换不完全，有信息丢失)/建立隧道(IPV6 上套 IPV4 壳)(保留原始数据报的全部信息)

4.5 选路算法(全局算法还是分布式算法;静态算法还是动态算法)

1 链路状态(LS)选路算法:Dijkstra 算法单点广播(错误不扩散)
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
热土豆选路协议：选择最近的网关路由器

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(UDP)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 较顶层 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
3 BGP 应用层协议 端口 179
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，属性值 AS-PATH 包含了该路由已通过的那些 AS 的 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 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

路由选择顺序：偏好->最短AS-PATH->最靠近NEXT-HOP->BGP标签
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 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:(节点记录之前转发过的分组 ID)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(建立隧道:源节点将多播分组封装到一个单播分组中，单播分组的目的地址为核心的单播地址。)
使用基于源的树维护代价大，发送代价为最优(MOSPF、DVMRP)
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：许多或大多数路由器涉及多播选路过程，使用广播+剪枝方式建立多播树
稀疏模式：只有很小一部分路由器涉及多播选路过程，采用共享树的方法；当源节点流量很高时切换到基于源的树

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
网卡中的控制器芯片：组帧、链路接入、检错、可靠交付、流量控制等;主机上的链路层软件：与网络层接口，激活控制器硬件、响应控制器中断等

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:将信道划为若干子频带
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Np(1-p)^(N-1),效率 1/e,0.37
优点:单个活跃节点可以信道速率连续发送;高度分散:节点自行决定什么时候发送;简单；缺点:发生冲突的时隙被浪费了;由于概率发送，有些时隙被闲置;需要时钟同步
纯 ALOHA 立即传输帧,不在时隙传Np(1-p)^(2(N-1)),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(以太网采用):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提升的帧,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能量传播延迟的最大值
Ttrans = 最长帧的传输时间.效率为1/(1+5 * tprop/ttrans)
轮流 MAC 协议:①轮询:主节点轮流“邀请”从节点发送；缺点:引入轮询延迟；单点失效②令牌传递：(主节点)ROM 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.缺点：令牌传递延迟；单点失效（令牌）

MAC 比较：信道划分 MAC 协议:重负载下高效：没有冲突，节点公平使用信道；轻负载下低效：即使只有一个活跃节点也只能使用 1/N 的带宽随机接入 MAC 协议：轻负载时高效：单个活跃节点可以使用整个信道；重负载时低效：频繁发生冲突,信道使用效率低轮流协议（试图权衡以上两者）：按需使用信道（避免轻负载下固定分配信道的低效）；消除竞争（避免重负载下的发送冲突）

随机接入：ALOHA、S-ALOHA (ALOHA 网络) CSMA/CD（早期以太网）CSMA/CA（802.11）
轮流：中心节点轮询（蓝牙）令牌传递（FDDI，IBM 令牌环，令牌总线）

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,没有两块适配器具有相同的地址
必要性 :可以支持各种网络层协议(不只是 IP 协议)
目的 MAC 地址有三种类型:
单播地址：适配器的 MAC 地址，地址最高比特为 0
多播地址：标识一个多播组的逻辑地址，地址最高比特为 1
FF-FF-FF-FF-FF-FF 为广播地址
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. (在以太网上, ARP 报文封装在以太帧中传输)

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. (ARP 请求为 1, ARP 响应为 2)(ARP 缓存)

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

碰撞域描述了一组共享网络访问媒体的网络设备覆盖的区域

广播域是指广播分组直接到达的区域

冲突域:竞争广播信道的一组节点构成一个冲突域

4 以太帧结构 以太帧长 20 字节;以太网技术由 IEEE802.3 工作组标准化

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

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

帧的最小长度≥链路速率×2τ

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.

(自主学习)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

基于交换机端口划分 VLAN;基于 MAC 地址划分 VLAN;基于 IP 地址划分 VLAN

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

VLAN干线连接:每台交换机上一个端口配置为干线端口。

Q:我们需要抛弃已有的以太网卡吗?A:不用,因为只有交换机会使用 VLAN 字段Q:谁来产生 VLAN 字段?A:由第一个接收帧、且支持 VLAN 的交换机添加 VLAN 字段,由路径上最后一个这样的交换机去掉 VLAN 字段Q:帧长度不够怎么办?A:802.1Q 将帧的最大长度提高到 1522 字节

MPLS:

MPLS网络按照标签label进行分组的转发,类似于VC,有基于标签的转发表

初始目的:使用固定长度的标签label进行高速率IP转发 (而不是使用IP address,采用最长前缀匹配)但是IP数据报仍然保留IP地址! 在帧和其封装的分组之间加入一个垫层,标签交换使能的路由器使用垫层信息进行分组转发,不解析分组目标地址.

具有MPLS能力的路由器:基于标签的值进行分组的转发 (而非检查IP地址),MPLS转发表和IP转发表相互独立.

弹性:MPLS转发决策可以和IP不同1.采用源地址和目标地址来路由到达同一个目标的流,不同路径 (支持流量工程) 2.如果链路失效,能够快速重新路由:预先计算好的备份链路.

第六章 无线网络

6.1 概述

基站:连接到固定网络,在无线终端和固定网络间中继数据包

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),所有终端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 1. 单跳+基于基础设施:802.11 网络,3/4G 蜂窝网络2. 单跳+无基础设施 蓝牙3. 多跳+基于基础设施:无线传感器网络,无线网状网络(需中继)4. 多跳+无基础设施 移动自组织网络 车载自组织网络(中继)

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)

信噪比 SNR:信号与噪声强度的相对度量;

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

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.(发送节点听不到,但影响接收)暴露节点:在发送节点范围内,但不在接收节点范围内.(发送节点能听到,但不影响接收)

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 IEEE 802.11 无线局域网

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.

802.11 无线 LAN 的基本组成单元是基本服务集(BSS)

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。

(两种机制不适用或)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

无线站点的盗别:

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

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

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

802.11 链路层确认:目的站点收到通过 CRC 校验的帧;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

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

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

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

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,自组织网络用到

802.11:子网内移动

主机停留在同一个 IP 子网中:IP 地址保持不变

交换机:哪个 AP 与主机关联?自主学习:交换机收到主机发送的帧后,了解到从哪个交换机端口可以到达主机

802.11:高级功能

速率适应:当主机移动或信噪比变化时,基站和主机动态改变传输速率(物理层调制技术)

功率管理:节点设置功率管理比特,告知 AP 它将进入休眠状态:AP 缓存发往该节点的帧,节点在下一个信标帧之前醒来;AP 发送信标帧,其中包含一个移动节点列表——这些节点有帧缓存在 AP中:列表中的节点向 AP 请求帧,其余节点重新进入休眠

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:(三角选路: 通信者-归属网络-移动节点;当通信者和移动节点在同一个网络中时很低效)

移动结点初始到外部网络时,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(节点移动及变换外地网络等对通信者都是透明的:正在进行的通信可以保持)

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(对通信者不透明:通信者需要知道移动节点的转交地址;通信者(包括固定节点)需要增加对移动通信的支持)

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ICMP报文,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,当移动节点回到归属网络时,要向归属代理注销

若通信者在归属网络上,归属代理如何得到发送给移动节点的包?ARP 代理:归属代理为位于外地网络的移动主机发送 ARP 响应,用自己的 MAC 地址进行响应(移动主机永久地址->归属代理 MAC 地址)免费 ARP:当接收到移动主机的注册请求后,归属代理主动发送 ARP 报文,刷新其它节点的 ARP 缓存

归属代理通过隧道转发数据包:外面套层壳

外地代理如何转发数据包到移动节点?外地代理在注册阶段获知移动节点的永久地址和 MAC 地址,记录在其转发表中;外地代理从收到的数据包中取出原始数据包,根据目的 IP 地址查找转发表,得到移动节点的 MAC 地址;外地代理利用原始数据包和移动节点的MAC 地址构造链路层帧,发送给移动节点

移动节点发送数据包:直接发给外地代理.(缺省路由:SrcIP=移动节点永久地址,DestIP=通信者 IP 地址,SrcMAC=移动节点 MAC,DestMAC=外地代理 MAC)

移动节点如何得知外地代理的 MAC 地址?从收到的代理通告报文的源 MAC 得知

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

网络安全是指网络系统的硬件、软件及其系统中的数据受到保护,不受偶然的或者恶意的原因而遭到破坏、更改、泄露,系统连续可靠地运行,网络服务不中断。

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

传统加密方法:替换,换位

现代密码学基本原则:加密与解密的算法是公开的,只有密钥是需要隐藏的

加密算法被称为是计算安全的,该算法产生的密文满足以下两个条件之一:破译密文的代价超过信息本身的价值;破译密文所需的时间超过信息的有效生命期

现代密码学中,密码的安全性是通过算法的复杂性和密钥的长度来保证的

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:有截获的密文,入侵者知道一些“明文-密文对”

选择明文攻击:入侵者可以任意选择一定数量的明文,让被攻击的加密算法加密,得到相应的密文,以利于将来更有效地破解由同样加密算法及相关密钥加密的信息。

一个安全的加密系统必须能抵御选择明文攻击

对称密钥算法:

DES 是一种块加密算法,每次以 64 比特的明文块作为输入,输出 64 比特的密文块;DES 是基于迭代(16 轮)的算法,每一轮迭代执行相同的替换和换位操作,但使用不同的密钥;DES 使用一个 56 比特的主密钥,每一轮迭代使用的子密钥(48 比特)由主密钥产生;DES 是一种对称加密算法,加密和解密使用相同的函数,两者的不同只是子密钥的次序刚好相反

缺点:密钥长度不够长,迭代次数不够多

3DES 使用两个密钥进行三轮 DES 计算:

第一轮令 DES 设备工作于加密模式,使用密钥 K1 对明文进行变换;第二轮令 DES 设备工作于解码模式,使用密钥 K2 对第一轮的输出进行变换;第三轮令 DES 设备工作于加密模式,用密钥 K1 对第二轮的输出进行变换,输出密文

有关 3DES 的三个问题:

为什么使用两个密钥而不是三个密钥?

112 比特的密钥已经足够长

为什么不使用两重 DES(EE 模式)而是三重 DES?

考虑采用 EE 模式的两重 DES,且攻击者已经拥有了一个匹配的明文—密文对(P1, C1),即有 C1=EK2(EK1(P1))

令 X=EK1(P1)=DK2(C1)。攻击者分别计算 EK1(P1)和 DK2(C1),并寻找使它们相等的 K1 和 K2,则穷尽整个密钥空间只需 256 的攻击量而不是 2112。(中途攻击)

为什么是 EDE 而不是 EEE?

为了与单次 DES 兼容。3DES 用户解密单次 DES 用户加密的数据,只需令 K1=K2 就行了。

AES:每次处理 128 比特明文块,输出 128 比特密文块;密钥长度可以是 128、192 或 256 比特

CBC:若每个明文块被独立加密,相同的明文块生成相同的密文块,容易被重放攻击利用。

发送方生成一个随机的初始向量 c(0),用明文发送给接收者;每一个明文块加密前,先与前一个密文块进行异或,然后再加密:第一个明文块与 c(0)异或;相同的明文块几乎不可能得到相同的密文块

非对称加密:不存在密钥传递问题:加密密钥是公开的;解密密钥是私有的

公开密钥算法的使用:

每个用户生成一对加密密钥和解密密钥:加密密钥放在一个公开的文件中,解密密钥妥善保管

当 Alice 希望向 Bob 发送一个加密信息时:Alice 从公开的文件中查到 Bob 的加密密钥,用 Bob 的加密密钥加密信息,发送给 Bob,Bob用自己的解密密钥解密信息

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)

e与z互质,求d,使得ed=1(modz)

加密:C=M^e(modn)(将明文看成是一个比特串,将其划分成一个个数据块 M,且有 0≤M<n)

解密:M=C^d(modn)

优点:安全性好:RSA 的安全性建立在难以对大数提取因子的基础上,这是目前数学家尚未解决的难题;使用方便:免除了传递密钥的麻烦。公钥(n, e)和私钥(n, d)。

缺点:计算开销大,速度慢

RSA 的应用:RSA 一般用来加密少量数据,如用于鉴别、数字签名或发送一次性会话密钥等

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

一个可以替代手写签名的数字签名必须满足以下三个条件:

接收方通过文档中的数字签名能够鉴别发送方的身份(起源鉴别);发送方过后不能否认发送过签名的文档(防抵赖);接收方不可能伪造被签名文档的内容

为什么要开发一个不需要加密算法的报文鉴别技术? 加密软件通常运行得很慢,即使只加密少量的数据;加密硬件的代价是不能忽略的;加密算法可能受专利保护(如 RSA),因而使用代价很高;加密算法可能受到出口控制(如 DES),因此有些组织可能无法得到加密算法

使用密码散列函数(cryptographic hash function)的报文鉴别:

使用密码散列函数计算报文摘要时需要包含一个密钥,但它并不用来做加密运算

发送方用双方共享的一个秘密密钥 KS 添加到报文 m 之前,然后计算报文摘要 H(KS||m)形成报文鉴别码

散列函数 H 应满足的特性:①H 能够作用于任意长度的数据块,并生成固定长度的输出;②对于任意给定的数据块 x,H(x)很容易计算;③对于任意给定的值 h,要找到一个 x 满足 H(x)=h,在计算上是不可能的(单向性):该特性对于使用密码散列函数的报文鉴别很重要;如果根据 H(KS||m)=h 可以找到一个 x,使得 H(x)=h,那么根据 x 和 m 可以推出 KS。④对于任意给定的数据块 x,要找到一个 y≠x 并满足 H(y)=H(x),在计算上是不可能的:该特性对于使用加密算法的报文鉴别很重要;⑤如果能找到一个不同于 x的数据块 y,使得 H(y)=H(x),那么就可以用 y 替换 x 而不被接收方察觉;要找到一对(x, y)满足 H(y)=H(x),在计算上是不可能的。(抵抗生日攻击)

满足前四个特性的散列函数称为弱散列函数,满足所有五个特性的散列函数称为强散列函数。

典型散列函数:MD5(128)和 SHA-1(160)

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.证书上有 CA 的签名.用 CA 的公钥来解密证书,防止偷换.

目前最常用的证书标准是 X.509

X.509 建立在公钥算法和数字签名的基础上:CA 对证书内容先进行 SHA-1 散列,然后用 CA 的私钥对报文摘要加密,形成数字签名。

X.509 定义了三种鉴别程序,供不同的应用选择:

单向鉴别:涉及一个用户到另一个用户的一次报文传输(接收方鉴别发送方)

双向鉴别:通信双方相互鉴别

三向鉴别:通信双方相互鉴别,并提供报文同步机制

为验证公钥证书的真实性:验证方用 CA 的公钥解开证书的签名,得到证书内容的报文摘要;对收到的证书内容计算报文摘要,并与解密得到的报文摘要进行比较,两者相同表明这是合法的公钥证书

信任锚(trust anchor):

信任链是信任的起点,系统中所有实体都以根 CA 的公钥作为它们的信任锚,信任锚必须通过安全的物理途径获取。

信任链(chain of trust):

也称认证路径(certification path),指从叶结点到根 CA 的一个证书序列

根 CA 的选择:

实际中有许多根 CA,每个根 CA 都有自己的一个分级结构,所有根 CA 间可以进行交叉认证;用户可以自行决定信任哪个根 CA;实际上,许多根 CA 的公钥被预装在浏览器上,这些根 CA 由浏览器厂商认证并嵌入到软件中,随软件一起发布

证书撤销:每个证书都有有效期,过期后证书自动失效。;CA 也可以显式地撤销证书,这要求 CA 定期地发布证书撤销列表(CRL),表中给出已经撤销的证书序列号。每个用户在使用一个证书前都要去获取 CRL,检查该证书是否在 CRL 中。

8.4 端点盗别: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.(缺点:需要一个共享的对称密钥)

报文最后还要附上发送方的数字签名.

8.5 SSL(向基于 TCP 的网络应用提供安全的传输层服务)

提供:服务器鉴别,数据加密,客户鉴别(可选)

8.6 IPsec(IPSec 安全协议:包括 AH 和 ESP 两个安全协议;密钥管理协议;安全关联(SA)的抽象)

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:用专用线连接成网络

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 头和传输层之间

IPsec 隧道模式:封装在新 IP 包内,套上新的 IP 头.

传输模式比隧道模式占用较少的带宽

隧道模式更安全:隐藏内部网络的细节(原始 IP 头不可见);内部网络上的主机可以不运行 IPSec,它们的安全性由安全网关来保证;隧道模式可以将一对端点间的通信聚合成一个加密流,从而有效地防止入侵者进行流量分析

802.11WEP: 最初的 802.11 规范使用的安全协议;在主机和基站之间提供较弱的加密及鉴别服务;没有密钥分发机制

802.11i:具有更强安全机制的 802.11 版本;提供较强的加密机制及鉴别机制;提供密钥分发机制

8.8 防火墙

包过滤防火墙:路由器对数据包进行逐包过滤.

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

局限性: 无法抵御 IP 欺骗攻击: 路由器无法知道包是否来自声称的源;应用网关处理开销大,速度慢;每个被代理的应用都需要一个应用网关;应用网关对于用户不透明:客户软件必须设置应用网关的 IP 地址;对于 UDP 包,过滤器或者全部允许,或者全部禁止;和外界的通信强度与网络安全等级是一对矛盾;许多受到高度保护的站点仍然遭到攻击

防火墙:包过滤防火墙仅检查传输层和网络层协议头;应用网关仅检查特定应用的数据包;不检查数据包之间的关联

IDS: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:端口扫描;DoS 攻击

第三部分:田野班小测题.

4.1 IP 报长 3200Byte(20 头,3180 负载),链路层 MTU 804Bytes。MTU 是最大数据长度,无需考虑帧开销。数据内容:804-20=784.所以每次 offset=784/8=98.784*4=3136.最后余 64 进入最后的帧内。

4.2 Dijkstra 算法:每次取源点到 S-U 中最进的点加入 U

4.3

IPV4 校验和是源设置的,而且传播过程中会变。出错/NAT 地址转换, 每次 TTL-1, 校验和也会变

一个子网中可能有多个 DHCP 服务器

路由表中的每个 CIDR 地址都是一个子网? 主机/子网聚合

IPsec 工作在路由器上?

IP 报文段只在接收方重组,不在中间路由器上重组。

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。

5.3 交换机可以即插即用,路由器不行

交换机转发表针对子网;路由器交换表针对整个互联网,不可拓展

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。

另外两种复杂。

6.4(a) 在 802.11 站点传输数据帧之前,它必须首先发送 RTS 帧并接收相应的 CTS 帧。F

(b) 使用 RTS 和 CTS 可以完全避免冲突。F

(c) 使用 RTS 和 CTS 可以完全避免传输数据帧时的冲突。T

(d) 以太网和 802.11 使用相同的帧结构。F

6.5Two users using CDMA to communicate, user A's code = {1,-1,-1,1,-1,1}, user B's code = {1, 1,-1,-1,1,1}. Suppose user A transmits 1, user B transmits -1, show the decoded data using A and B's code to recover from the combined signal.

User A transmit 1	1	-1	-1	1	-1	1
User B transmit -1	-1	-1	1	1	-1	-1
Combine	0	-2	0	2	-2	0
Decode for A	<0,-2,0,2,-2,0>*<1,-1,-1,1,-1,1>= 6/6=1					
Decode for B	<0,-2,0,2,-2,0>*<1,1,-1,-1,1,1>=-6/6=-1					

传输层 TCP 分段网络层 IP 分片链路层 不分片只有目的组装

RIP缺点:(1)定期更新周期过于频繁(或过小或 30s);(2)缺少分层,对大规模网络无法适用;(3)RIP1 存在收敛性问题(或坏消息传的慢);(4)用跳数表示距离(或未使用实际代价表示距离)。OSPF缺点:(1)采用可靠(或带确认)洪泛(或广播)开销过大;(2)协议复杂(或多种链路状态、多种链路)

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