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

2. 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: 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)。

3. 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。

4. 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

5. 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。

6. 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 答: 128.16.16.0/20。

7. 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?

答: (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?

答: 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?

答: 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?

答: 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?

答: 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

8. 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。

9. 交换机是如何提升网络性能的? 答: 划分冲突域

10. 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

11. 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

12. 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

k=1,16/(16+512)*256=7.75

k=15,7.75*15=116.36 (3)k=127,256

13. 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.

14. 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))

15. 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

1. 概 述

网络层三大功能:

转发: 涉及分组在*单一*的路由器中从一条入链路到一条出链路的传送(根据转发表转运分组)

路由选择:确定分组从源路由器到目的路由器的路径，涉及一个网络的*所有*路由器

连接建立(某些架构要求从源到目的地)

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(*端到端*)

- 可对单个分组提供的服务(当运输层向网络层*传递一个分组时*):
  确保交付; 具有时延上界的保证交付
- 可对给定的源和目的地之间*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; 安全性服务

网络层服务(数据报/虚电路): *主机-主机*; 一个网络*不能同时*提供两种服务; 在端系统、网络核心实现

传输层服务(TCP/UDP): *进程-进程*; *可同时*提供两种服务; 在网络边缘实现

虚电路: 仅连接 数据报: 仅无连接

2. 虚电路网络:【有连接、有状态(转发表)、资源预留、VC 号】

*端到端路径。*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。

每台路由器都完全知道经过他的所有虚电路。(与运输层连接的区别)

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)

建立虚电路的本质: 预先选好源主机到目的主机的路径，此后分组仅沿选好的路径传输，是否分配资源是可选的。

一个分组沿着其路由在每条链路上不简单地保持相同的 VC 号的原因: 减少了在分组首部中 VC 字段的长度; 大大简化了虚电路的建立，否则路由器将不得不交换并处理相当大量的报文以约定一个共同的 VC 号。

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

数据报网络【无连接、无状态、不留资源、目的地址】

分组携带*目的主机地址*，路由器按目的地址*转发*分组; 路由器中的*转发表*记录目的地址到输出链路接口的映射; 转发表被*路由选择算法*修改(与虚电路的区别)，并能在任何时间修改(所以一系列分组可能走不同路径而无序到达)。**【最长前缀匹配规则】**

路由器*不维持连接状态信息*，但在其转发表中*维持了转发状态信息。*

数据报网络只提供最小服务的好处: 可运行在各种链路之上; 增加新服务只涉及终端。

3. 路由器工作原理

4 个组成部分: 输入端口、输出端口、交换结构、路由选择处理器

- 输入端口: 将一条输入的物理链路与路由器相连接的*物理层功能*; 需要与位于入链路远端的数据链路层交互的*数据链路层功能*; 查找功能，通过查询转发表决定路由器的输出端口。有转发表的副本，避免了集中式处理的瓶颈。
- 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，并为路由器计算转发表。【软件实现】
- 交换结构: 经内存(经过共享系统总线一次仅能执行一个内存读写); 经总线(标签匹配才保存分组，一次只有一个分组); 经互联网络(由特定总线接受，能并行转发，可能会排队)当交换结构速率至少为端口速率的 n 倍时(n 为输入端口数量)，可以消除输入端口的排队，但路由器成本提高了。*输出端口排队是不可避免的*，增大输出队列: 可以减少丢包的发生，但会增加内存消耗，并增大分组延迟; *输出队列并不是越长越好*。

4. 网络协议(IP 协议、路由选择协议、ICMP 协议)

网络层分组被称为*数据报*

IPV4 数据报格式:

版本号，首部长度(一般的 IP 数据报具有 20 字节的首部)、服务类型、数据报长度(首部加数据)、标识号/标志/片偏移、寿命(TTL 剩余最大跳数，转发前-1，0 则丢弃)、上层协议(数据部分用哪个传输层协议，多路分解，6-TCP，17-UDP)、16 位头部校验和【每台路由器要重新计算】、32 位源/目的 IP 地址，数据(TCP/UDP 报文段)

每个(无分片的)数据报共承载了总长 40 字节的首部(20 字节的 IP 首部加上 20 字节的 TCP 首部)以及应用层报文。

IP 数据报分片:

链路层帧能承载的最大数据字节数称为 MTU。

分片时:每片标识不变，最后一片标志=0，其他标志=1; 偏移量:以 8 字节为单位。

总长 4000 (20+2980)

片	长度	偏移量	标志
1	1480+20=1500	0	1
2	1480+20=1500	1480/8=185	1
3	1020+20=1040	(1480+1480)/8=370	0

终端抽取合并分片而不是路由器!

注:TCP 自带分段，就不用 IP 分片了，但 UDP 不行!

IPV4 编址

IP 要求每台主机和路由器接口有自己的 IP 地址。

8-A 16-B 24-C

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。

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。子网内部通信不需要通过路由器，子网之间通信必须通过路由器。

CIDR: 223.1.1.0/24 表示最左侧 24 比特一样

IP 地址与子网掩码做与运算，可得子网地址。

DHCP(动态主机配置协议，DHCP 是一个客户/服务器模式的应用协议)【即插即用】

子网中应有一个 DHCP 服务器或一个 DHCP 代理。

主机一开始不知道自己的 IP 地址。它用 0.0.0.0 *广播* DHCP 发现报文,寻找子网中的 DHCP 服务器

DHCP 服务器*广播* DHCP 提供报文进行响应,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 请求报文选择一个 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

NAT(网络地址转换)

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。

*外出的数据报:*将数据报中的(源 IP 地址，源端口号)替换为(NAT IP 地址(不变)，NAT 端口号(不断分配))

进入的数据报:取出数据报中的(目的 IP 地址，目的端口号)查找 NAT 转换表，然后用转换表中对应的(IP 地址，端口号)进行替换。

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:*** NAT 只允许内部主动发起的通信，位于 NAT 后面的主机对外是不可见的; 但 P2P 应用要求任何对等方可以向任何其它(参与的)对等方发起通信。

NAT 妨碍 P2P 应用程序: 需要 NAT 穿越技术。

ICMP:因特网控制报文协议 Ping&Traceroute【网络层协议】

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 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

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)

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)

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，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。

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: 将 IPv6 报头转换成 IPv4 报头; 缺点: 报头转换不完全，有信息丢失

建立隧道: IPv6/IPv4 边界路由器将 IPv6 包封装到一个 IPv4 包中，送入 IPv4 网络，目的边界路由器取出 IPv6 包继续传输; 保留原始数据报的全部信息。

5 路由选择算法(全局算法还是分布式算法;静态算法还是动态算法)

全局算法:所有路由器具有关于拓扑和链路代价的全部信息，集中式计算; ***分布式算法:***路由器仅知道邻居节点以及到邻居节点的链路代价，通过与邻居交换信息，进行迭代计算。***静态算法:***路由随时间不变或缓慢变化(手工配置); ***动态算法:***路由器根据拓扑及链路代价的变化而自动更新路由。

链路状态(LS)选路算法:Dijkstra 算法单点广播(错误不扩散)可能出现的问题*: 选路震荡*(可能出现在任何使用拥塞或基于时延的链路测度算法中)，*解决方案*一个是强制费用不依赖拥塞，一个是确保并非所有路由器都运行 LS 算法。

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。路由选择环路和无穷计数问题。

LS 算法和 DV 算法的比较: 链路状态 LS: 链路状态信息在全网传播; 节点仅传播可靠的信息(LS 更健壮): 亲自测量的本地链路代价; 节点计算的路由不传播，错误不扩散; ***收敛速度:*** O(|N||E|)个报文，O(N2)次计算。***距离矢量 DV:*** 距离矢量仅在发生变化时向邻居发送; 节点传播的信息可能不正确: 邻居的距离矢量是"道听途说"的; 节点计算的路由要传播，会造成错误扩散; 收敛较慢，还可能出现路由环路、计算至无穷问题。

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*的自治系统*内部*路由选择协议

不同 AS 中的路由器可以运行不同的自治系统*内部*路由选择协议

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相同的自治系统*间*路由选择协议

所有 AS 必须运行相同的自治系统*间*路由选择协议

热土豆选路协议: 选择最近的网关路由器

6 因特网选路协议

Intra-AS 又称内部网关协议 IGP【内】。常见 路由选择信息 RIP、开放最短路优先 OSPF

Intra-AS 又称外部网关协议 EGP【间】。只有 BGP 边界网关协议

跳: 相邻路由器之间的链路为一跳。***路径的跳数:*** 从源路由器到目的子网(含)最短路径经过*子网数量*。

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。距离向量协议。**【运行 UDP 上的应用层协议】**

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

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)。

OSPF 较顶层 ISP 中使用，洪泛链路状态信息的链路状态协议+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。使用时，路由器向自治系统内*所有*其他路由器广播路由选择信息。**【王湘峰说是运输层协议】**

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。OSPF 最重要的优点是支持 AS 内部的分层选路

AS 内部配置成多个区域，其中一个为主干区域(标识 0)，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

BGP 应用层协议 端口 179【应用层协议】

从相邻 AS 获得子网可达性信息，向本 AS 内部所有路由器传播信息，决定"好"路由

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(Ebgp,iBGP)

可达性信息:以 AS 枚举形式通告的、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。

为什么会有不同的 AS 间和 AS 内部路由选择协议: 对该问题的答案触及了 AS 内与 AS 间的路由选择目标之间差别的本质: 策略(AS 间在意)、规模(AS 间在意，而 AS 内可以进一步划分)、性能(AS 内关心)。

7 广播和多播路由选择

广播路由选择(broadcast routing): 网络层提供了从一种源结点到网络中的所有其他结点交付分组的服务; **多播路由选择**(multicast routing)使单个源结点能够向其他网络结点的一个子集发送分组的副本。

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

洪泛: 节点收到广播分组后，向所有邻居节点(分组到来的链路除外)发送该分组的拷贝

无控制洪泛广播:告诉所有邻居，但会无休止循环(存在环)

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 使用此方法

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。只需要知道在它到发送方的单播最短路径上的下一个邻居。

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

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。封装在 ip 数据报中 协议号 2 *TTL = 1*(IGMP 只在本地工作)

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，也可能包含没有属于某多播组的相连主机的路由器

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(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

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节点

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。**媒体控制协议 MAC。**

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

链路层的主体部分是再网络适配器中实现的。

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

链路层是软件硬件的结合体。

2 差错检测与纠正比特 EDC

保护从网络层传递下来的需要通过链路层传输的数据报，和链路帧首部中的链路级寻址信息等字段。

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，只知道出现奇数个差错。

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。一个 i+j+1 个奇偶比特。不仅可以检测出*单个比特差错*的事实，也可以利用行列索引来纠正。但两个比特差错不能纠正。

循环冗余检测 CRC 校验:

对于 G = r+1 位的生成多项式，G 的最高位有效比特(最左)是 1。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.

加减用异或代替: 1011 XOR 0101 = 1110

检验方法:CRC 码/生成多项式,如果余数 0,无错

能检测任何小于 r+1 比特的突发差错，长度大于 r+1 的以概率 1-0.5^r 被检测到。能检测任何奇数个比特差错。

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:

3 多路访问协议 MAC :规定节点共享信道(谁能发送)的方法

链路层点对点协议: 点对点协议 **PPP**，高级数据链路控制协议 **HDLC**

当碰撞发生时，没有一个接收节点能有效地获得任何传输的帧。

3 个类型: **信道划分协议 随机接入协议 轮流协议**

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

理想特性: 只有一个活跃节点时，具有 R bps 吞吐量。由 M 个活跃节点时，每个 R/M bps

ALOHA 和 CSMA 协议具备第一个特性，但不具备第二个特性。

信道划分协议

时分复用 TDM:时间划为时间帧，每个帧划为 N 个时隙。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。限制在 R/N bps 的平均速率，必须等待轮次。

频分多路复用 FDM:将信道划为频段，把每个频率分配给 N 个节点中的一个，限制 R/N 的带宽。

码分多址 CDMA:每个节点用唯一编码编码数据,不同节点可同时传输,

随机接入协议 发送前不监听信道:ALOHA,监听:CSMA

时隙 ALOHA 【理想化，不能实现】

强假设: 节点同步，只在时隙起点传输。如果碰撞,时隙结束前检测到碰撞，每次重传以概率 p 进行,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

取消强假设，立即传输帧,不在时隙传,效率 1/2e=0.185

载波监听多路访问 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

带碰撞检测的 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).检测到碰撞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:经历 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。n 最大在 10 以内。

dprop = 以太网中任意两个节点之间*传播*延迟的最大值

dtrans = 最长帧的*传输*时间.

效率为 1/(1+5 · dprop/dtrans)

轮流协议: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) 网络中有一个令牌，按照预定的顺序在节点间传递,获得令牌的节点发最大数目帧.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)

链路层协议: DCOSIS CMTS

4 交换局域网

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. 一共 2^(48)的可能。

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)

MAC 地址是扁平的，IP 地址是层次的。

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(48 个 1)

【广播在局域网内，不能穿过路由器!】

主机和路由器接口除了网络层地址之外还有 MAC 地址，这有如下几个原因: 局域网是为任意网络层协议而设计的，而不只是用于 IP 和因特网; 如果适配器使用网络层地址而不是 MAC 地址的话，网络层地址必须存储在适配器的 RAM 中，并且在每次适配器移动(或加电)时要重新配置，另一种选择是在适配器中不使用任何地址，让每个适配器将它收到的每帧数据(通常是 IP 数据报)沿协议栈向上传递，然后网络层则能够核对网络地址层是否匹配，这种选择带来的一个问题是，主机将被局域网上发送的每个帧中断，包括被目的地是在相同广播局域网上的其他结点的帧中断。为了使网络体系结构中各层次成为极为独立的构建模块，不同的层次需要有它们自己的寻址方案。

地址解析协议 ARP:获得与 IP 地址对应的 MAC 地址

每台主机和路由器接口有单一的 IP 地址和 MAC 地址。ARP 只为在*同一个子网*上的主机和路由器接口解析 IP 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

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

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 MTU=1500 字节

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

以太网向网络层提供*无连接*服务 不可靠服务 CSMA/CD 全双工

链路层交换机 它没有 MAC 地址 **【即插即用 全双工】**

对子网中的主机和路由器是透明的

交换机内有一张端口转发表: **交换机表**，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**.

自学习:

交换机表初始为空。帧到达时(入帧)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。

交换机和路由器比较:

尽管交换机也是一个存储转发分组交换机，但它和路由器是根本不同的，因为它用 MAC 地址转发分组。交换机是第二层的分组交换机，而路由器是第三层的分组交换机。

交换机的优点和缺点: 即插即用，能够具有相对高的分组过滤和转发速率; 为了防止广播帧的循环，交换网络的活跃拓扑限制为一棵生成树，一个大型交换网络将要求在主机和路由导异中有大的 ARP 表，这将生成可观的 ARP 流量和处理量; 交换机对广播风暴并不提供任何保护措施，交换机不能连接异构链路(即 MAC 协议不同的网络)，因为交换机只是按原样转发帧。

路由器的优点和缺点: 分组不会被限制到一棵生成树上，并可以使用源和目的地之间的最佳路由，它们允许以丰富的拓扑结构构建因特网，它们对第二层的广播风暴提供了防火墙保护，路由器可以连接异构链路，因为路由器需重新封装链路层帧; 不是即插即用的，路由器对每个分组的处理时间通常比交换机更长，因为它们必须处理高达第三层的字段。

何时使用交换机或路由器: 几百台主机小网络，交换机就足够了，因为它们不要求 CP 地址的任何配置就能使流出阻塞化并增加总计吞吐量; 但是在由几千台主机组成的更大网络中，通常在网络中(除了交换机之外)还包括路由器，路由器提供了更健壮的流量隔离方式和对广播风暴的控制，并在网络的主机之间使用更"智能的"路由。

虚拟局域网 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。动态划分，逻辑上是不同的交换机。

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 字节标签协议标识符、12 比特 VLAN 标识符 3 比特优先权

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: 802.1 将帧的最大长度提高到 1522 字节

多协议标签转换: MPLS

基于固定长度的标签(而不是目的 IP 地址)来转发数据报。

标签转换路由器在转发表中寻找 MPLS 标签，不需要提取 IP 地址与最长前缀匹配。提供了不同路径的可能。

三层交换机: 具有部分路由功能、又有二层转发速度的交换机; 专为加快大型局域网内部的数据交换而设计; 但在安全、协议支持等方面不如专业路由器

三层交换机的使用: 通常用在机构网络的核心层，连接不同的子网或 VLAN; 三层交换机转发速度快的原因: 一次路由，多次转发

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

PPP 由以下三部分组成: 一种在串行通信线路上的组帧方式，用于区分帧的边界，并支持差错检测; 一个用于建立、配置、测试和拆除数据链路的链路控制协议 LCP; 一组网络控制协议(NCP)，用以支持不同的网络层协议。

PPP 帧格式: Flag:帧边界 Address:总是 0xFF(点-点线路) Control: 总是 0x03 Protocol: 指出载荷字段中携带的是哪类分组 Info: 载荷字段 Check: CRC 校验

第六章 无线网络

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(无线并不一定意味着移动)

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(需中继)
多跳+无基础设施 移动自组织网络 车载自组织网络(中继)

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)(与有线的区别)
以上导致传输距离有限, 误码率高

信噪比 SNR, 较大则更容易提取信号。比特差错率(误码率)**BER**。

给定调制方案, SNR 越高, BER 越低; 给定 SNR, 具有较高比特传输率的调制技术(无论差错)具有较高的 BER; 物理层调制技术的动态选择能用于适配对信道条件的调制技术。

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)。C 正在向 B 发送; A 监听到信道空闲, A 向 B 发送; A 和 C 的信号在 B 冲突;

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)。B 准备向 C 发送; B 监听到信道忙(A 在发送); B 不发送, 但其实 B 可以发送(A 和 B 的信号不会在 C 冲突)

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.【信道划分协议题】

$$Z_{i,m}=d_i\cdot c_m$$
$$d_i=1/M\sum Z_{i,m}\cdot c_m$$

例:C=[1, 1, 1, -1, 1, -1, -1, -1] d1=-1, d0=1
Z1=-1, -1, -1, 1, -1, 1, 1, 1 Z2=1, 1, 1, -1, 1, -1, -1, -1
d1=(-1-1-1-1-1-1-1-1)/8=-1

$$Z^*_{i,m}=\sum Z_{i,m}$$
$$d_i=1/M\sum Z^*_{i,m}\cdot c_m$$

3 IEEE 802.11 无线局域网(wifi)

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

802.11 无线 LAN 的基本组成单元是**基本服务集(BSS)**,包括:若干无线站点,一个无线接入点 AP(中央基站)

LAN 和 BSS 的关系: LAN 为广播域,无路由器隔开。而可以一个 BSS 为一个 LAN,也可以多个 BSS 为一个 LAN,取决于连接 BSS 的时交换机还是路由器。

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,管理员为 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)【一次握手】

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)【两次握手】

802.11MAC 协议 CSMA/CA 碰撞避免【随机访问协议】

不能检测碰撞: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。

链路层确认:目的站点收到一个通过 CRC 校验的帧后,等待一个 **SIFS** 发回一个确认帧。

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:1)若一开始就侦听到信道空闲,等待 **DIFS** 时间后发送帧 2)否则,选取一个*随机回退值*,在侦听到信道空闲时递减该值;在此过程中若侦听到信道忙,冻结计数值 3)当计数值减为 0 时,发送整个帧并等待确认 4)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,重新进入第 2 步中的回退阶段,并从一个更大的范围内选取随机回退值;如果有 k 个节点等待发送,它们随机选取的回退值确定了它们的发送顺序。

使用信道预约机制的 CSMA/CA:假设 A 欲向 AP 发送一个数据帧: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*广播*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 和 AP 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。

【RTS/CTS 仅用于长数据】

CSMA/CA 与 CSMA/CD 的不同, 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;**原因:**冲突对无线网络损害很大,要尽可能避免

碰撞是物理现象无法避免,避免的是数据的碰撞!

帧间距机制

802.11 允许 DCF 和 PCF 在一个单元内共存,这是通过帧间距机制实现的。

SIFS:允许正处于会话中的节点优先发送,如收到 RTS 的节点发送一个 CTS,收到数据帧的节点允许发送一个 ACK 帧。

PIFS:如果在 SIFS 后没有节点发送,在 PIFS 之后 PCF 模式的基站可以发送一个信标帧或一个轮询帧。

DIFS:如果 PIFS 后没有基站发送, DIFS 之后任何节点可以竞争信道。

EIFS:如果以上间隔都没有发送, EIFS 之后收到坏帧或未知帧的节点可以发送一个错误报告帧。

802.11 帧格式:

帧的核心是有效载荷,通常由一个 IP 数据报或者 ARP 分组组成。通常小于 1500 字节。

有四个地址字段:

1.接收节点 MAC 地址. 2.发送节点 MAC 地址. 3.连接 AP 的路由器接口的 MAC 地址.

4.自组织模式中相互转发时使用

802.11 帧寻址举例: 无线终端 H1 向路由器 R1 发送帧,它的 AP 已知:H1 构造一个 address 1 = AP MAC, address 2 = H1 MAC, address 3 = R1 MAC,将该帧发给 AP;AP 将这个 802.11 帧转换为 802.3 帧(有线),后者的 dest addr = R1 MAC, source addr = H1 MAC

AP 连接路由器的有线端口没有 MAC 地址! AP 仅对无线终端可见,对于固定网络上的设备是不可见的。

802.11:子网内移动

互联设备为*交换机*:主机停留在同一个 IP 子网中,IP 地址保持不变。切换过程中,终端上的应用正常运行;由于 IP 地址没变,网络层及以上层次感觉不到这个移动,切换过程中产生的延迟及丢包,在上层协议看来是正常的。

互联设备为*路由器*:

自学习: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:高级特色/先进功能

并不完全特定于 802.11 标准

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:一个节点能明显地在睡眠和唤醒之间交替。节点设置功率管理比特 1,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

802.15.1:蓝牙

单跳+无基础设施

在每个时隙,发送方利用 79 个信道中的一个进行传输,同时从*时隙*到*时隙*以一个已知的伪随机方式变更信道, FHSS。

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

外部网络: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)

外部代理:外地网络上为移动节点执行移动管理功能的实体,用于创建 COA 和告诉归属代理移动节点在它的外部代理的网络中具有给定的 COA。

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)对通信者来说是*完全透明*的,正在进行的通信可以保持。目标再移动处理简单。

归属代理*截获*数据报, *封装*在一个新的数据报中,交付给 COA。拥有该 COA 的外部代理接受并*拆封*该数据报,再向移动节点发送原始数据报。【隧道概念】

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.离开外部网络时,向外部代理取消注册,外部代理*不需要*联式地注销 COA。

直接选路:

克服了三角选路的问题;对通信者不透明,增加的复杂性。目标再移动处理复杂。

通信者向归属代理请求,并获知移动节点的 COA(此步以后不必再做);通信者将包封装发送给外地代理;外地代理将包转发给移动节点;移动节点直接向通信者发送。【隧道概念】

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)

外地代理如何获得移动节点的 MAC 地址? 在移动节点注册阶段,外地代理获知了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;外地代理利用移动节点的 MAC 地址,将数据报封装到链路层帧中,发送给移动节点

锚外部代理:*首次*发现移动节点的外部网络中的外部代理。

6 移动 IP:代理发现,向归属代理注册,间接路由选择

代理发现:经代理通告、经代理请求

代理通告:外部代理或归属代理周期性*广播*一个类型字段为 9(路由器发现)的 ICMP 报文。包含代理的 IP 地址。

代理请求:不必等待通告,*广播*一个请求报文,类型字段为 10 的 ICMP 报文,收到请求的代理向移动节点*单播*一个代理通告。

移动 IP 节点收到一个 COA,该地址*必须*向归属代理注册。

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(UDP 报文通过端口 434)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(434 端口)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: 当移动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

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

8 对上层协议的影响

无线链路带来的问题, 误码率、丢包率、延迟增大。***节点移动带来的问题,*** 丢包、延迟增大。**建议上,及什么影响:**为上层协议提供的仍然是尽力而为服务,因此 TCP 和 UDP 也可以运行在无线网络上。**性能上,有很大影响:**丢包率高,传输延迟增大;

TCP 将丢包(长延迟也当作丢包)解释为拥塞,不必要地减小拥塞窗口,导致应用吞吐率很低;

第八章 网络安全

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

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:

唯密文攻击: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

块密码:【重要】

密码块链接 CBC:

相同的明文不同的密文。

发送方产生初始向量 IV: = c0 Ci = Ks(mi XOR ci-1) …

Ks 解密得到 si = mi XOR ci-1 mi = si XOR ci-1

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:【公钥加密 私钥解密】

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)

选一个小于 n 的数 e, e 和 z 互质

求 d, ed = 1 (mod z)

公钥(n,e) 私钥(n,d)

加密:C=M^e(mod n)(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(mod n)

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

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

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)

发送方接收方共享密钥 s,发送方生成报文 m,计算 H(m+s)【报文鉴别码 MAC】,发送(m, h(m+s))

接收方(m,h)计算 H(m+s)与 h 比较。

数字签名:【私钥加密】

发送方先计算报文 H(m),然后用发送方的私钥加密,形成报文鉴别码,发送(m,Kb-(H(m)))。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

典型散列函数:MD5(128) 和 SHA-1(160)

认证:CA 公钥认证

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

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. (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。

基于鉴别协议 ap1.0: 直接发送一个报文。**基于鉴别协议 ap2.0:** 有一个总是用于通信的周知网络地址(IP):Trudy 用 Alice 的 IP 地址创建一个数据包(IP 地址欺骗)。**基于鉴别协议 ap3.0:** Alice 向 Bob 发送口令证明自己,口令是鉴别者和被鉴别者之间共享的秘密。Trudy 监听到 Alice 发送的明文口令,过后发送给 Bob。**基于鉴别协议 ap3.1:** Alice 将口令加密,发送给 Bob。Trudy 截获数据包,过后发送给 Bob(回放攻击)**基于鉴别协议 ap4.0:** ***目标,*** 避免回放攻击。***失败的情况是因为*** Bob 不能区分 Alice 的初始鉴别报文和后来人侵者回放的 Alice 的初始鉴别报文所致;也就是说,Bob 无法判断 Alice 是否还活跃(即当前是否还在连接的另一端),或他接收到的报文是否就是前面鉴别 Alice 时录制的回放。***不重数(nonce)***。在一个协议的生存期中只使用一次的数,也就是说,一旦某协议使用了一个不重数,就永远不会再使用那个数字了。***协议 ap4.0 以如下方式能得一个不重数:*** 1) Alice 向 Bob 发送报文“我是 Alice”; 2) Bob 选择一个不重数 R,然后把这个值发送给 Alice; 3) Alice 使用她与 Bob 共享的对称秘密密钥 KA-B 来加密这个不重数,然后把加密的不重数 KA-B(R)发回给 Bob。与在协议 ap3.1 中一样,由于 Alice 知道 KA-B 并用它加密一个值,就使得 Bob 知道收到的报文是由 Alice 产生的。这个不重数用于确定 Alice 是活跃的; 4) Bob 解密接收到的报文,如果解密得到的不重数等于他发送给 Alice 的那个不重数,则可鉴别 Alice 的身份。**缺点:**需要一个共享的对称密钥。**基于鉴别协议 ap5.0:** **采用公开密钥算法加密不重数**

5 SSL(向基于 TCP 的网络应用提供安全的传输服务)

提供:服务器鉴别,数据加密,客户鉴别(可选)

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:用专有线连接成网络

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 防火墙

软件硬件结合体,自身与网络连接。

传统分组过滤器:路由器对数据包进行逐包过滤.

状态分组过滤器: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

应用程序网关: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 中最近的点加入 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。

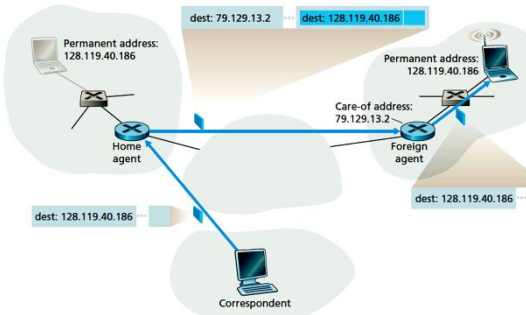
另外两种复杂。

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



小测

Ipv4 的校验和由源主机设置且在转发路径上保持不变(x)

每个子网必须要有 DHCP 服务器(x)

转发表中的每个 CIDR 地址块都是一个子网(x)物理上也要相连

IPsec 协议运行在路由器上(x)运行在主机上

IP 分组在中间路由器上被组装(x)

一个网络层不能同时成为数据报网络和虚电路网络(√)

RIP 和 OSPF 都使用链路状态路由算法(x)

BGP 是域内路由协议(x)

AS 内的非边界路由器的转发表仅由域内路由协议配置(x)

边界路由器的转发表仅由域间路由协议配置(x)

互联网上所有的边界路由器都必须运行相同的域间路由协议(√)

IPv6 的首部比 IPv4 由更多的字段(x)

SSL 是应用层协议(√)

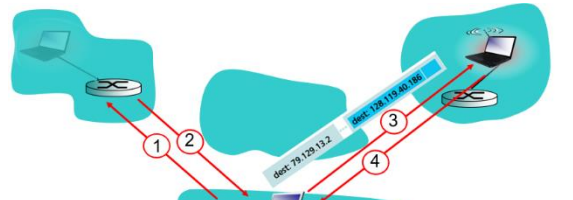
IPsec 是无连接协议(x)

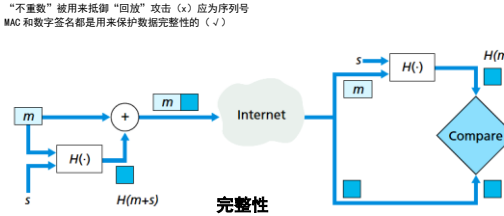
公钥加密信息比对称密钥更快(x)

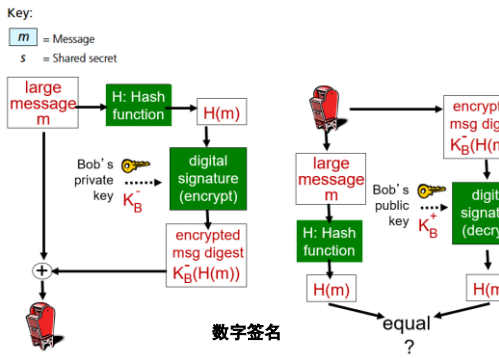
因特网的校验和可以作为哈希函数保证信息完整性(x)

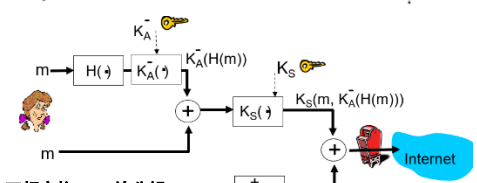
“不重数”被用来抵御“回放”攻击(x)应为序列号

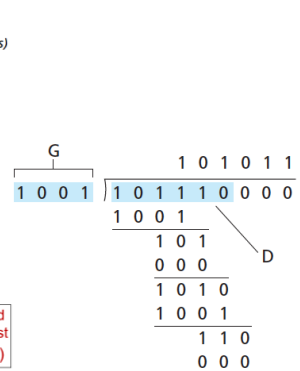
MAC 和数字签名都是用来保护数据完整性的(√)











保密:全文对称密钥
认证:Alice 的私钥
完整:Hash 值

PB19010450 和泳毅