**网络层：**

**4.1概述** 作用：将报文段从发送主机传送到接收主机。(网络层分组：数据报)

重要功能：转发、路由选择、连接建立（仅存在于某些网络架构中,也是握手）。

转发是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（通过转发表，路由选择算法决定插入路由器的转发表值;由路由器接收路由选择协议报文来配置转发表）。路由选择是指网络范围的过程，以决定分组从源到目的地所采取的端到端路径(路由选择协议，路由选择算法是分布式或集中式)。分组交换机是指一台通用分组交换设备，它根据分组首部字段中的值，从输入链路接口道输出链路接口转移分组。某些称为链路层交换机（基于链路层字段），其他称为路由器（基于网络层字段）。网络服务模型定义了分组在发送与接收主机之间端到端传输特性。提供的服务：（对分组）确保交付、具有时延上界的确保交付。（对分组流）有序分组交付、保证最小带宽(低于特定比特率的传输不会丢失，且保证速率/时延)、保证最大时延抖动（两个相继分组发送时间间隔和接受时间间隔的最大差异）、安全性服务(秘密会话密钥来加密数据报;数据完整性、源鉴别服务) 因特网：尽力而为服务；ATM CBR:恒定比特率(电话，端到端时延、时延抖动、丢失、推迟交付比率都有保证)ATM ABR:可用比特率

**4.2虚电路和数据报网络** 网络层与运输层(无)连接服务差异:主机间/进程间;网络层不同时提供连接和无连接服务(二选一)虚电路(VC)网络(如ATM，帧中继)：提供网络层面向连接服务。虚电路包含：1.从源到目的主机的端到端路径。2. VC号,途经该路径每段链路的一个虚电路号(用于区分经过该链路的不同虚电路，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）每条链路不保持相同VC号原因:1.减少分组首部VC字段长度2.每条链路可有不同VC号,即可独立于其他链路选择号码,简化了虚电路建立

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(如带宽); 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

注:沿两端系统间路径上路由器都要参与虚电路建立，且每台路由器都完全知道经过它的所有链路(而运输层连接建立仅涉及两个端系统) 信令报文：专门用于建立,维护,拆除虚电路的控制报文（含修改路由器表中连接状态） 信令协议：交换信令报文的协议

数据报网络：提供网络层无连接服务。（因特网是数据报网络）特点：1.分组携带目的主机地址，路由器按目的地址转发分组2.路由器中的转发表记录目的地址到输出链路的映射（**采用最长前缀匹配**）3.转发表被选择路由算法修改，1-5min更新1次4.同一对主机之间传输的分组可能走不同的路径，从而可能重排序 数据报网络只提供最小服务的好处：1.可运行在各种链路层之上 2.增加新服务只涉及终端。

**4.3路由器工作原理** 路由器功能：选路：运行选路协议，计算转发表。转发：依据转发表，从输入链路到输出链路转发数据报（也称为交换）。转发数据平面(硬件):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 查表：每个输入端口都有转发表的影子副本(通过独立总线从路由选择处理器复制到输入线路卡)，查表仅在本地进行,决定输出端口;快速查找算法,DRAM,SRAM,TCAM(三态内容可寻址存储器)排队: 当交换结构阻塞时，分组需在此排队。转发：将分组从输入端口转移到输出端口（也称交换）,具体方式与交换结构有关;控制分组(带路由选择协议信息，从输入端口转发到路由选择处理器);其他动作:物理层链路层处理；检查分组版本号，检验和，寿命字段，重写后两个字段；更新用于网络管理的计数器。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.传统路由器：选路、转发都由CPU完成。现代路由器：输入端口将一个包放入内存，其接口硬件通过控制器发送一个消息，给出包在内存中的存放地址，输出端口从指定的内存位置读取包，发回响应消息（性能和代价取决于存储接口数目，仅适合小容量系统）。经总线交换：交换结构中的总线包括地址线、数据线和控制线；每个输入和输出端口都有一个接口硬件连接到总线上，每个端口被分配一个唯一的地址（内部标签）；总线协议防止多个端口同时传输，比如采用时分多路复用：各个输入端口在总线上轮流广播分组，分组中携带输出端口的地址；各个输出端口使用地址过滤器检查分组地址，仅将发给本端口的分组缓存起来；除了一个分组占用总线其他必须等待。经互联网络交换：在输入端口与输出端口间建立内部专用电路（如纵横式交换机），多对端口间可以并行传输(但同一输出端口一次只能有一个)。分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。

输出端口功能：网络层处理：1、组装：若需要，将交换结构输出的信元组装成分组。2、排队：若输出端口来不及发送，分组在此排队。3、调度：若有多个等待队列，选择一个队头分组发送。链路层处理：执行链路层协议，封装。物理层处理：将比特流转换成物理信号。管理控制平面(软件):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.网络范围的路由选择控制平面因此是分布式的，即不同部分（例如路由选择算法）执行在不同的路由器上并且通过彼此发送控制报文进行交互。因特网路由器和路由选择算法是以这种方式运行的

排队与丢包：1、**排队的位置和程度**（或者在输入端口排队，或者在输出端口排队）将取决于流量负载、交换结构的相对速率和线路速率。当交换结构不能及时将输入端口的分组转移到输出端口，输入端口处形成排队。带来的问题：队头阻塞(HOL,线路前部阻塞): 队头分组阻塞其后分组的转发。丢包：当输入队列溢出时，发生丢包。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。2、多个输入端口同时向一个输出端口发送时，在输出端口形成排队，需分组调度程序(FCFS,WFQ(加权公平排队))。***设置多大的输出队列***是一个问题：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（延迟太大的分组最终被重传，浪费资源）；输出队列并不是越长越好！分组丢弃策略：**弃尾（drop-tail）**：队列满时，丢弃到达的分组。**主动队列管理(AQM)**：在队列满之前就开始丢弃(或首部加标记)分组，如RED(随机早期检测)算法：设计为和TCP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： ,当平均队列长度达到第一个阈值时，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。

**4.4网际协议:因特网中的转发和编址**IP只提供最小的传输服务，将数据报交付到目的地址和目的协议（多路分解），解决传输中可能出现的几个问题：1、数据报过大无法通过某个中间网络（措施：对数据报进行分片）2、数据报可能因寻路错误在网络中循环（措施：设定数据报的最大转发次数）3、报头出错可能导致误投递（措施：对报头检错）

IP数据报格式：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 版本 | 首部长度 | 服务类型 | 数据报长度（字节） | |
| 16比特标识 | | | 标志 | 13比特片偏移 |
| 寿命(TTL) | | 上层协议 | 首部检验和 | |
| 32比特源IP地址 | | | | |
| 32比特目的IP地址 | | | | |
| 选项（如果有的话） | | | | |
| 数据 | | | | |

IP分片与重组：链路层帧能承载的最大数据字节数称为MTU （Max. Transmission Unit）。传输过程中，较大的IP数据报可以被分片：将数据报载荷划分为若干较小的数据块，每个数据块封装成一个独立的数据报传输，数据报在传输的过程中可以被多次分片，但仅在目的主机上重组。首部长度：单位为4bit。分片的报头取自原始数据报，与分片有关的字段：标识：每个分片必须携带与原始数据报相同的标识。偏移量：指示分片中的数据在原始数据报载荷中的位置。标志位：MF（more fragments）：最后一个分片的MF=0，其余分片的MF=1。DF（don’t fragment）：DF=1表示不允许对数据报分片。分片报头中的以下字段需要修改：总长度，偏移量，MF，头部检查和。由于偏移量只有13比特，将其规定为以8字节块为单位，除最后一个分片外，其余分片的数据长度应为8字节的整倍数。假设原始数据报的报头长度为H，则分片的数据长度 N 应为满足以下条件的最大整数：N ≦ MTU-H，N为8的倍数。

处理过程：1、根据报头长度H和输出线路的MTU，确定分片的最大数据长度N。2、将数据报的载荷划分成长度为N的若干数据块（最后一个数据块可能不足N字节）。3、将原始报头加到每一个数据块的前面，修改报头中的以下字段：总长度＝H+数据块长度，最后一个报头的MF位置0，其余报头的MF位置1，偏移量＝数据块在原始数据报载荷中的字节序号/8，计算头部检查和。

重组：将收到的分片重新组装成原始数据报的过程，在目的主机中进行：1、收集分片：目的主机使用<源IP地址，标识>确定属于同一个数据报的分片。2、利用最后一个分片计算原始数据报长度：原始数据报长度=偏移量×8 +分片总长度。3、组装：将各分片中的数据块按照其在原始数据报载荷中的偏移量重组。

分片的开销：降低了路由器的吞吐量。消耗了目的主机的资源：每个重组的数据报需要一个重组缓冲区和一个重组定时器。

IPv6取消了路由器分片的功能：源主机发送探测报文，确定路径上的最小MTU。源主机构造的数据报大小不超过最小MTU。路由器丢弃超大的数据报，并发送错误报告。

IPv4编址：接口interface:主机/路由器与物理链路的边界，路由器有多个接口，主机通常只有一个接口。每个网络接口对应一个IP地址，是一个32位的二进制数，通常用点分十进制数表示。

单播地址除类别标识外，其余比特被划分成网络号和主机号两部分：网络号：标识一个物理网络。主机号：标识该物理网络上的一个网络接口。同一个物理网络上的网络接口，它们的IP地址具有相同的网络号。

为在因特网范围内保证IP地址的全局唯一性：网络号由ICANN统一分配，主机号由网络管理员统一分配。一个A类、B类及C类地址可提供的接口地址数：A类地址：224-2 = 16777214。B类地址：216-2 = 65534。C类地址：28-2 = 254。A类、B类、C类地址的个数：A类地址：27-2 = 126。B类地址：214-2 = 16382。C类地址：221-2 = 2097152。

特殊IP地址:网络号有效、主机号全为0：保留给网络本身。网络号有效、主机号全为1的地址：定向广播，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，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。形如127.xx.yy.xx的地址：保留作为回路测试，发送到这个地址的分组不输出到线路上，而是送回内部的接收端。

子网：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，从概念上说，引入子网仅略微改变了IP地址的解释：主机号被进一步划分成子网号和主机号两部分，子网号标识网络内的一个子网，主机号标识子网中的一个网络接口。子网掩码用于指示IP地址中子网号与主机号的边界：32比特的数，其中对应主机号的比特为0，其余比特为1，也采用点分十进制表示，如255.255.252.0。路由器的每个端口连接一个子网，不同的端口连接不同的子网。路由器是在子网之间转发数据包的设备。子网内部通信不需要通过路由器。

IP数据包转发：网络层转发数据报的两种情形：1、直接交付（direct delivery）：节点（源主机或目的路由器）将数据包直接发送给目的主机（不需要其它路由器转发），即数据包的目的地址与节点的某一个端口处在同一个子网中；2、间接交付（indirect delivery）：节点将数据包转发给一个路由器去处理，即数据包的目的地址不与节点的任何一个端口在同一个子网中。

转发表：记录目的地址到输出端口的映射。由目的地址类型的不同，有三类转发表项：1、目的地址是一个子网地址，称地址前缀表项；2、目的地址是一个特定的网络接口地址，称特定主机表项；3、缺省项：不匹配所有其它表项的地址，这些地址被映射到一个默认的路由器端口。

IP采用逐跳选路：每个转发表项只记录去往目的地址的下一跳信息（下一个要到达的路由器端口），而不是一条完整的端到端路径。

每个转发表项包括：目的地址/掩码、下一跳地址、输出端口等。下一跳地址必须与输出端口在同一个子网中（不需要通过其它路由器就可以直接到达）

分类编址的缺点：1、只能按照三种固定的大小分配地址空间，地址浪费严重；2、转发表必须记录每个已分配的网络，转发表规模爆炸式增长。

CIDR（Classless InterDomain Routing）：1、按照实际需要的地址数量分配地址空间，提高地址使用效率；2、允许将若干条转发表项进行聚合，减小转发表规模。CIDR地址分配的原则：地址块的长度 L 必须是 2 的幂次。所有地址的前（32-log2L）位必须相同。网络地址的表示方法：1、用掩码指示网络地址的长度，如194.24.0.0 ，255.255.248.0；2、用“/长度”指示子网地址的长度，如194.24.0.0/21。

例：若路由器收到目的地址为194.24.17.4的数据包，其查表过程为：

194.24.17.4 AND 255.255.248.0 = 194.24.16.0，与194.24.0.0不匹配；194.24.17.4 AND 255.255.252.0 = 194.24.16.0，与194.24.8.0不匹配；194.24.17.4 AND 255.255.240.0 = 194.24.16.0，与194.24.16.0匹配选择该转发表项。

地址聚合：转发表中符合以下条件的若干个表项可以合并成一个表项：

1、这些表项的目的地址可以聚合成一个前缀更短的地址；2、这些表项使用相同的下一跳。地址聚合的过程可以递归进行。

若个别表项不满足路由聚合的条件：1、仍然可以在转发表中给出一条聚合表项；2、同时给出不能被聚合的表项。

最长前缀匹配：在所有匹配的路由表项中，选择前缀最长的表项。

路由器收到数据报后：1、根据目的地址的类型确定要查找的转发表（A、B、C三类地址分别有一个转发表）；2、根据目的地址的类型提取网络地址；3、用网络地址在相应的转发表中进行哈希查找（精确匹配）

采用CIDR后出现的问题：1、地址前缀的长度prefix\_len可以是任意值；2、Prefix\_len无法从地址本身得到，只能从转发表项中得到；3、必须从所有匹配的表项中选择前缀最长的表项。在大规模转发表中进行快速查找是一个难题（已经解决）。

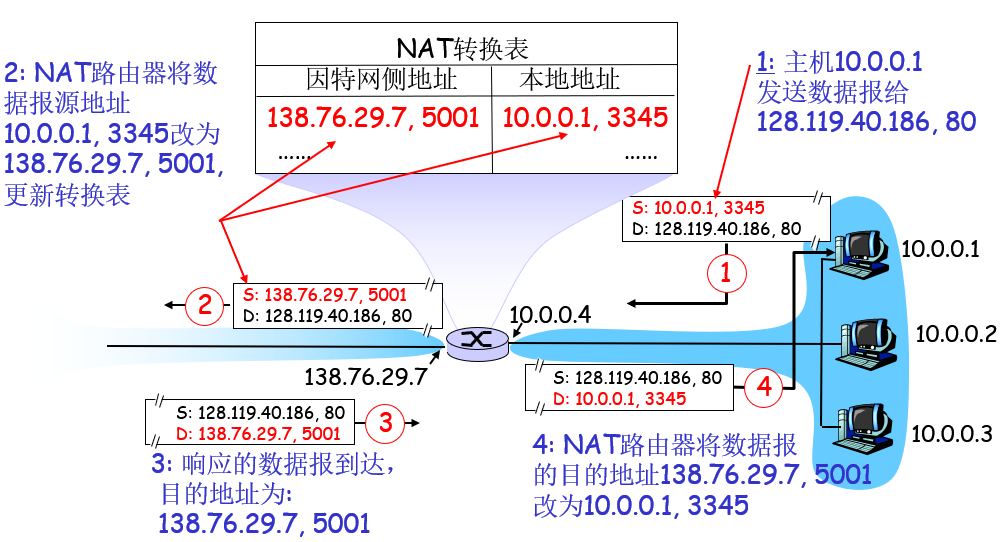
路由器：管理员手工配置路由器各个接口的IP地址

主机：管理员手工配置主机IP地址，服务器通常采用这种方法

主机使用动态主机配置协议DHCP（Dynamic Host Configuration Protocol）获取IP地址、子网掩码、缺省路由器、本地DNS服务器等配置信息

使用DHCP的好处：免去手工配置的麻烦（即插即用）。可用少量的IP地址服务较多的客户（地址重用）。

DHCP：目标: 允许主机加入网络时自动获取配置信息。DHCP是一个客户/服务器模式的应用协议，子网中应有一个DHCP服务器或一个DHCP代理。请求过程：1、主机广播“DHCP discover”报文，寻找子网中的DHCP服务器；2、DHCP服务器用“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；3、主机用“DHCP request”报文请求IP地址，主机选择一个DHCP服务器，向其请求IP地址；4、DHCP服务器用“DHCP ack”报文发送IP地址，服务器响应客户的请求，确认所要求的参数。注：DHCP服务器使用UDP端口67，客户使用UDP端口68。

网络地址转换（NAT）：Motivation：1、使用一个公用IP地址支持许多用户同时上网2、仅为公共可访问的节点分配公用IP地址（减少需要的公用IP地址数）3、网络内部节点对外是不可见的（安全考虑）

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，NAT端口号）。NAT 转换表：记录每个（源IP地址，源端口号）与（NAT IP地址，NAT端口号）的转换关系。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。

16比特端口号: 允许一个NAT IP地址同时支持65535个对外连接。

NAT的使用有争议:1、路由器应当只处理三层以下的包头（端口号在传输层）2、违反端到端原则（节点介入修改IP地址和端口号）。3、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穿越问题：使用中继服务器，在 Skype 中使用：NAT 后面的服务器与中继器建立连接；外部客户与中继器建立连接；中继器在两个连接之间转发分组。

ICMP:（Internet Control Message Protocol）：主机或路由器使用ICMP协议传递网络层上的一些信息。ICMP报文有询问和错误报告两类：1、询问：用来请求一些信息，通常采用请求-响应模式交互；2、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；ICMP与IP的关系：1、ICMP报文被封装在IP包中传输：这是因为ICMP报文可能需要经过几个网络才能到达源节点；2、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。ICMP错误报告的例子：源抑制：路由器缓存满，无法容纳新到来的数据报；超时：数据报的TTL减为0，或主机的重组定时器超时；目的不可达：路由器判断一个数据报不可能到达它的最终目的地；重定向：路由器发现主机使用的路由有错或不是最佳路由；参数错误：数据报中某个参数有错

ICMP信息查询的例子：回声请求/响应：用于发现对方是否在线；地址掩码请求/响应：用于获得本网的地址掩码；路由器请求：请求本网路由器的信息；路由器发现：路由器定期发送该消息通告自己的信息。

ICMP报文格式：

|  |  |  |
| --- | --- | --- |
| Type | Code | Checksum |
| (Contents depends on type and code) | | |

type：报文类型，共定义了15种；code：对某类报文作进一步的区分；

Checksum：ICMP报文的检查和；内容：与报文类型有关。报告错误的

ICMP报文包含触发该错误的数据报的头部和前8个数据字节。

Ping与ICMP：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：1、源主机发送 Type=8，Code=0 的 Echo Request 报文；2、若目的主机

收到，发送 Type=0，Code=0 的 Echo Response报文；3、源主机计算RTT，并报告；

4、若源主机连续几次超时（收不到Echo Response），向调用者报告目的不可达。

Traceroute与ICMP：Traceroute测试到达目的主机的路由（经过的路由器）：1、源主

机的Traceroute程序向目的主机发送一个Echo Request报文，IP报头的TTL设为1

2、第一跳路由器对TTL减1，发现TTL变为0，向源主机发送一个TTL expired报文（IP报头中有路由器的IP地址）3、Traceroute记录第一跳路由器的IP地址，然后向目的主机发送第二个Echo Request报文，IP报头的TTL设为2；4、若收到第二跳路由器的TTL expired报文，记录第二跳路由器的IP地址；接着发送一个TTL为3的Echo Request报文；5、该过程不断重复，直至收到目的主机的Echo Response报文。

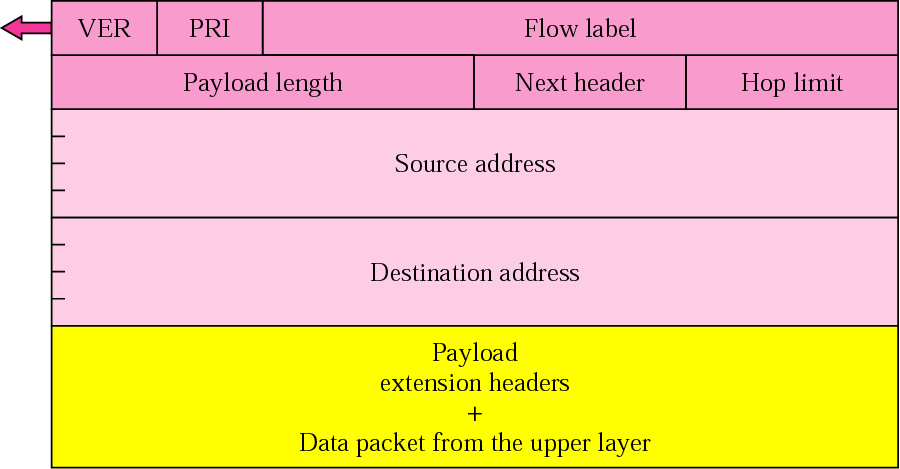
IPv6：最初的动机: IPv4地址将很快耗尽;进一步的动机:简化头部格式，加快数据报;处理和转发;支持服务质量;支持多播;支持移动性;增强安全性 ……

IPv6与IPv4不兼容，但与其它所有因特网协议都兼容。

IPv6地址：128位，使用冒号十六进制表示，每16位以十六进制的形式写成一组，组之间用冒号分隔，如8000:0:0:0:0123:4567:89AB:CDEF

地址表示的零压缩技术：可将连续的多组0压缩为一对冒号，如以上地址可表示为：8000::0123:4567:89AB:CDEF

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（或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：1、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

2、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。

流（flow）：定义：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。标识：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。处理：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。意义：流的引入使得IPv6具备了对数据包进行区分处理的能力。

IPv6包格式：与IPv4固定头相比，IPv6的基本头中去掉了以下一些字段：IHL：IPv6的基本头总是40字节长；与分片相关的字段：IPv6路由器不负责分片；头校验：计算校验和太花时间；现在的网络非常可靠，并且链路层和传输层上往往又都有校验和

IPv6基本头中增加了：流标签：支持对数据包区分处理

改变了以下字段的作用：Type of Service：代之以Traffic Class；总长度：代之以载荷长度；Protocol：代之以Next header，允许任意扩展选项。

ICMPv6：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）。ICMPv6仍然使用差错报告和查询两类报文。功能：差错报告：1、去掉了源抑制报文：优先级和流标签允许路由器控制拥塞，丢弃不太重要的数据包。2、增加了Packet Too Big报文：路由器丢弃长度超过MTU的包，并报告错误。

信息查询：1、去掉了一些不必要的查询报文。2、增加了一些查询报文，用于实现ARP（地址解析）和IGMP（多播组管理）的功能。

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；运行双栈的源节点先对目的节点查询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。

IPv6数据包如何穿越IPv4网络?报头转换：双栈节点（如路由器B）在将数据报传递给IPv4路由器（如路由器C）之前，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。优点：保留原始数据报的全部信息。

选路问题：给定一组路由器和连接路由器的链路，寻找一条从源路由器到目的路由器的最佳路径（应用评价一条路径的好坏可能包括：路径长度、数据速率、分组延迟、通信费用、安全性等。ISP关心一些全局性指标：网络吞吐量最大、平均包延迟最小、平均通信费用最低、网络负载均衡、路由稳定、健壮等）。

图抽象：选路算法: 寻找从源节点到目的节点代价最小的路径。通常考虑无向图，但实际网络中边是有方向的（代价不同）

选路算法分类：全局算法or分布式算法：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 or 动态算法：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：链路状态选路算法为全局算法，其基本思想为：每个节点利用可靠方法获得全网拓扑信息，抽象成一个带权拓扑图，计算到各个节点的最短路径；链路状态选路算法包括五个步骤：1、发现邻居：有链路直接相连的节点为邻居；2、探测链路代价：探测到每个邻居的代价；3、构造链路状态（LS）分组：利用邻居及链路代价信息；4、扩散LS分组：向网络中所有节点发送LS分组；5、计算路由：利用收到的LS分组构造网络拓扑，计算从本节点到其它各个节点的最短路径。

距离矢量（DV）算法：利用Bellman-Ford方程求解任意两个节点之间的最小代价路径，主要贡献在于给出了分布式求解B-F方程的方法。算法的基本思想：1、节点x测量其到各个邻居v的链路代价c(x,v)；2、节点x估计其到达各个节点y的最小代价Dx(y)，这些代价构成了自己的距离矢量 ；3、每个节点周期性地将它的距离矢量Dx发送给邻居；4、节点x拥有每个邻居v的距离矢量 ；5、当节点 x 从各个邻居收到它们的距离矢量后，利用B-F方程更新自己的距离矢量：.

节点的本地计算由以下两种事件引起: 1、本地某条链路的代价c(x,p)发生了变化

收到了某个邻居节点的距离矢量dp(y)；2、节点仅在发现距离矢量dx(y)有变化时通知其邻居。 距离矢量算法是迭代的、异步的、分布式算法。

LS算法和DV算法的比较：链路状态LS：1、链路状态信息在全网传播；2、节点仅传播可靠的信息：亲自测量的本地链路代价；3、节点计算的路由不传播，错误不扩散；4、收敛速度： O(|N||E|)个报文，O(N2)次计算。

距离矢量DV：1、距离矢量仅在发生变化时向邻居发送；2、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；3、节点计算的路由要传播，会造成错误扩散；4、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（AS）是由处于同一个管理域下的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（称Intra-AS选路协议）。不同AS中的路由器可以运行不同的Intra-AS选路协议。

网关路由器：在一个AS内、直接连接到其它AS的路由器。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。

AS1的网关路由器必须:1、了解哪些目的网络通过自己可达。2、将可达性信息传播到 AS1内部的所有路由器。涉及两个层次的选路：1、通过哪个网关路由器到达外网x（AS间选路）；2、如何到达该网关路由器（AS内选路）。采用热土豆协议：选择离1d最近的网关路由器（intra-AS）。

因特网中的选路协议：Intra-AS选路协议也称内部网关协议IGP（Interior Gateway Protocols），最常见的有:RIP（Routing Information Protocol）：较低层ISP和企业网使用。OSPF（Open Shortest Path First）：较顶层ISP使用。Inter-AS选路协议也称外部网关协议EGP（Exterior Gateway Protocols），目前只有：BGP（Border Gateway Protocol）。

选路算法和选路协议：选路算法是选路协议的一部分。选路协议还包括路径代价的定义、报文格式、报文传输、报文处理、异常事件处理等具体实施方面的问题。

RIP ( Routing Information Protocol)：RIP采用距离矢量选路算法，距离（代价）：用跳数（hop count）衡量，跳（hop）：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）经过的子网数量。限定一条路径的最大代价为15跳

RIP通告：距离向量：路由器到AS内各个子网的最短路径的跳数（估计值）。构造RIP响应报文：距离向量封装在RIP响应报文中传输，称为RIP通告。每个报文携带一个目的子网列表（最多包含25个子网），以及到每个目的子网的最短距离。发送RIP响应报文：RIP报文封装在UDP报文中发送，使用UDP端口520（RIP是一个应用层协议！）。相邻路由器之间大约每30秒交换一次RIP响应报文。

路由更新算法：假设：D收到路由器A的RIP响应报文。对RIP响应报文中通告的每个目的网络，跳数加1。对响应报文中通告的每个目的网络，重复以下步骤：

1、若目的网络不在选路表中（邻居报告了一个新的子网），把通告的子网添加到选路表中；2、若目的网络在选路表中。（1）、若目的网络在选路表中的下一跳为A，用通告的表项替换选路表中的表项（使用A最新通告的路径代价（无论增大或减小））。（2）、否则，若通告的跳数小于选路表中的跳数（找到一条更近的路由），更换选路表中的表项。返回。

RIP: 链路失效与恢复: 若超过180秒未收到某个邻居的RIP通告，认为该邻居不可达：令通过该邻居的路径失效（距离设为16）。发送RIP通告。

采用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 (Open Shortest Path First)：OSPF采用链路状态选路算法。链路代价：由管理员配置（反映了管理员的选路策略）。OSPF分组：OSPF协议定义了5种分组类型，分别用于探测邻居、通告链路状态等。OSPF分组被封装在IP包中传输，协议号为89。路由器周期性地、或在链路状态改变时发送OSPF链路通告。功能：OSPF协议负责链路通告分组在网络中的广播及可靠传输。路由器根据收到的链路通告分组构造链路状态数据库。路由器利用链路状态数据库及Dijkstra算法，计算以本路由器为根的最短路径树。

AS内部的分层选路：OSPF最重要的优点是支持AS内部的分层选路。一个OSPF自治系统可以配置成多个区域（area）：每个区域运行自己的OSPF协议，区域内部的链路状态仅在本区域内广播，区域边界路由器负责区域间的选路。

一个OSPF自治系统配置为若干区域：一个特殊区域称为主干，所有区域必须连接到主干上，每一个区域都有区域标识，主干的区域标识为0

区域边界路由器：连接本地区域和主干的路由器。主干路由器：主干上的路由器，可以同时是区域边界路由器。内部路由器：AS内部的非区域边界路由器。

分层的OSPF：两个选路层次：本地区域，主干。每个区域（包括主干）运行自己的OSPF协议。每个区域边界路由器：将本区域的选路信息汇总（子网及路径代价），通告给其它区域，将收到的其它区域的选路信息（子网及路径代价）通告给本区域的内部路由器对于去往其它区域的分组：首先转发到本地区域边界路由器，在主干上转发到目的区域边界路由器，然后再转发到目的子网。

AS间选路的困难与目标：1、因特网规模极其庞大且结构非常复杂；2、每个AS可运行自己的内部路由协议，使用自己的路由测度确定到目的网络的最佳路由，不同网络判断最佳路由的标准不同；3、一个AS可能不信任来自某个AS的选路信息；4、一个AS可能不愿意为其它AS转发数据包；5、AS间选路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。

边界网关协议BGP（Border Gateway Protocol）：当一对AS同意交换选路信息时，每个AS指定一个接近AS边缘的路由器（或主机），使用BGP协议交换选路信息。运行BGP协议的边界路由器（或主机）称为BGP speaker。一对BGP speaker通过一条半永久的TCP连接（端口179）建立BGP会话，交换BGP报文（BGP是应用层协议！）。BGP会话的两个端点互为BGP对等方。

BGP会话：不同AS的两个边界路由器之间建立的BGP会话，称为外部BGP（eBGP）会话。一个AS可能有多个边界路由器，这些边界路由器必须通过半永久TCP连接构成全连通，它们之间的BGP会话称为内部BGP（iBGP）会话。

BGP报文：BGP定义了4种类型的报文：1、打开报文：BGP路由器用来启动与邻居BGP路由器的联系。2、保活报文：BGP路由器定期交换保活报文，告知对方自己处于工作状态。3、通知报文：当检测到差错或路由器打算关闭连接时，发送通知报文。4、更新报文：BGP路由器使用该报文宣布新路由，以及撤销以前通告的路由。

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。边界路由器的选路表中，每个表项包含目的前缀（允许聚合）、下一跳路由器以及到达目的前缀的AS序列。

选路信息库（Routing Information Base）：BGP speaker内部的选路信息库由三部分组成：Adj-RIBs-In：每个Adj-RIBs-In对应一个BGP对等方，保存从该BGP对等方收到的选路信息。LOC-RIB：已被该BGP speaker计算出来的最佳路由。Adj-RIBs-Out：每个Adj-RIBs-Out对应一个BGP对等方，存放准备向该BGP对等方通告的选路信息。

BGP进程的处理过程：接收从各个BGP 对等方发来的更新报文，更新与之相对应的Adj-RIB-In（添加、替换或删除路由）。

输入策略引擎对Adj-RIB-In中每条新的路由进行入境过滤（过滤规则由网络管理员定义），结果可能是：丢弃，按原样接受，接受但修改某些属性（如偏好度）。对于每一个目的前缀，从所有可达的路径中按照BGP指定的决策顺序确定一条最佳路由，装入LOC-RIB。输出策略引擎根据出境过滤规则（由管理员定义），计算要通告给每一个BGP对等方的路由更新，放入对应的Adj-RIB-Out中（路由聚合也在这个阶段完成）BGP进程利用Adj-RIB-Out，向每个BGP对等方发送路由更新报文。

Intra-AS选路协议: 用于在AS内部交换选路信息，如OSPF、RIP，使用某个路由测度（代价）选择到目的节点的最优路径。

Inter-AS选路协议: 用于在不同的AS之间交换选路信息，如BGP。主要依据策略而不是路由测度去寻找可达路径（不追求最佳路径）。

广播选路：广播：将数据包从源节点发送到所有其它节点，用N次单播实现广播（在源节点上复制分组）：低效：相同的分组在某些链路上可能重复传输，需其它机制支持：源节点需知道所有目的节点的地址。理想的广播选路：源节点不需知道其它节点的地址，只需将分组的目的地址设置为广播地址，路由器负责转发到全网（在网络中复制分组）。网络中产生的分组拷贝最少。

在网络中复制分组：洪泛（flooding）：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。缺点：在有环的网络中，广播分组在网络中无休止地循环，浪费资源。

受控洪泛：目标：每个路由器仅转发它之前未转发过的广播分组。两种方法：1、节点记录之前转发过的分组ID，不重复转发分组（OSPF使用此方法：源地址+分组ID）2、反向路径转发: 利用节点内部的单播转发表，仅转发从本节点->源节点的最短路径的反向路径上到来的广播分组（该方法使用最多）。

生成树方法：使用生成树转发广播分组：路由器知道自己的哪几个端口在生成树上。当从一个端口收到广播分组后，只在属于生成树的其它端口上转发该分组。基于生成树的广播不会产生冗余的分组拷贝。

构造方法：选择一个节点作为核心（也称汇聚点）其它节点向核心发送单播的加入报文：

路由器利用单播转发表向核心转发加入报文时，记录报文的输入端口及输出端口，这些端口就是位于生成树上的端口。当加入报文到达生成树上的一个节点时，报文经过的路径被添加到生成树上。

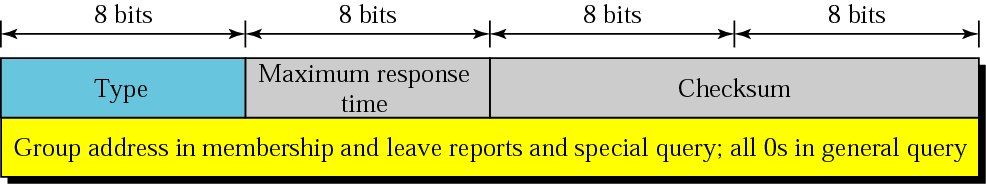
多播：将分组交付给一组接收者的通信模式。如何标识多播通信的接收者？因特网为这组接收者分配一个标识（多播组标识），使用D类地址作为多播组标识。如何设置多播分组的接收者？将分组的目的地址设置为其接收者的多播组地址。

如何将接收者的IP地址与多播组地址关联起来？接收者的IP地址与多播组地址无关。接收者可以在任何时候加入或离开一个组。多播组管理协议（IGMP）允许主机向本地路由器申请加入或离开一个组。如何将多播分组交付给每一个接收者？多播选路协议协调多播路由器建立到达所有接收者的路径树。

多播组管理：IGMP协议运行在主机与边缘路由器之间：主机利用IGMP协议向边缘路由器请求加入一个组、或离开一个组。边缘路由器利用IGMP协议向主机询问组成员关系

边缘路由器通过IGMP协议可以了解到，在它的某个端口能够到达的网络上存在着哪些组的成员。

IGMP报文格式与类型：

报文类型：查询（一般查询，特殊查询），成员报告，退出报告

加入一个组：每个主机维护一张应用进程与多播组的对应表。主机上的一个应用进程想要加入一个多播组时，向主机发送请求；若这是一个新组，主机向其边缘路由器发送一个成员关系报告。

退出一个组：主机发现某个多播组为空时，从表中清除该组，向路由器发送退出报告。路由器收到退出报告后：在该网络接口上发送针对该多播组的特殊查询报文（询问该端口上还有这个组的成员吗？）若在规定的时间内没有收到该多播组的成员关系报告，从表中清除该组。

监视成员关系：路由器周期性地发送通用查询报文（组地址置为0），主机发送成员关系报告作为响应。

IGMP报文的封装：IGMP报文封装在IP包中传输。协议字段值=2。TTL=1（因为IGMP只在本地工作）。封装IGMP报文的IP包使用多播地址作为目的地址：查询报文：多播地址224.0.0.1，接收者是该子网上的所有节点；退出报告：多播地址224.0.0.2，接收者是该子网上的所有路由器；成员关系报告：被报告的多播地址。

多播选路：目标：为每个组建立多播转发树（到达该组所有成员的路径树）。每个组成员应当只收到多播分组的一个拷贝。非本组成员不应收到多播分组。从源节点到每一个组成员节点的路径应当是最佳的（最短路径）。

建立多播树的两种方法：基于源的树:源节点建立一棵到多播组所有成员的最短路径树，源节点S和组G的每一种组合<S,G>构成一棵树。多播路由器必须有每棵<S,G>树的信息，根据多播分组的<S,G>确定使用哪棵多播树。优点：总是使用最佳路径转发多播分组。缺点：路由器需要维护大量的多播树信息。1、MOSPF（多播OSPF）通过扩展OSPF协议实现最短路径多播选路：扩展链路状态，使之包含链路上的组成员关系。基本思想：所有参与多播的主机在局域网上定期通报其所属的多播组（IGMP）。路由器将每条直连链路上对应的多播组集合作为链路状态在网上广播（MOSPF）。当路由器第一次遇到某个<S,G>多播分组时，计算从源节点S到多播组G的最短路径多播树（按需计算）。

2、距离矢量多播选路。扩展RIP协议实现多播选路的困难：除边缘路由器外，其它路由器不知道多播组（及其成员）的存在。DVMRP采用广播+剪枝的解决办法：RPF广播：确保多播分组到达每一个局域网。路径剪枝：路由器删除不包含组成员的路径分支。DVMRP的构建多播树的过程：1、参与多播的主机定期在局域网上通报所属的多播组，局域网上的路由器记录这些信息（IGMP）。2、当路由器收到发往组G的多播分组，但它并没有从局域网上监听到组G的报告时，向上游路由器发送一个剪枝报文，上游路由器停止通过这个接口发送该组的多播分组。3、如果一个路由器从它的每个下游路由器都收到剪枝报文，路由器向其上游路由器转发剪枝报文4、该过程递归进行，直至所有的无关分支都被删除，最终得到一棵<S,G>树

组共享树:每个多播组使用一棵树，树根为该多播组的核心。源节点先将多播分组发送给核心，核心再在多播树上发送。优点：对于每个组，多播路由器只需维护一棵多播树。缺点：多播分组使用的路径可能不是最佳的。当源节点想要发送多播分组时：源节点将多播分组发送给核心，核心在多播树上发送。多播分组如何到达核心？多播分组的目的地址为G，从源节点到核心的路径上，可能有路由器不在多播树上（不知道如何转发）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。

因特网上的多播选路协议:第一个用于因特网的多播选路协议是DVMRP。最广泛使用的因特网多播选路协议是PIM（Protocol-Independent Multicast）：不依赖于网络中所使用的单播选路协议。PIM有两种工作模式：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，采用组共享树的方法；当源节点流量很高时切换到源树。

**链路层：**

网络层和链路层的关系：网络层：选路：路由器确定去往目的节点的下一跳。转发：在路由器内部将数据报从输入端口转移到输出端口。链路层：将数据报从一个节点传输到相邻的下一个节点，如：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：主机和路由器统称为节点。链路：连接相邻节点的通信信道，可分为有线链路，无线链路，局域网。帧：链路层分组称为帧。

链路层服务：组帧（基本服务）：从原始比特流中提取出完整的帧。链路接入（广播链路需要）：在广播信道上协调各个节点的发送行为。差错检测（基本服务）：检测传输错误。差错纠正（有些提供）：检测并纠正传输错误（不使用重传）。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。提供可靠交付的链路层协议，不需要专门的流量控制。不提供可靠交付的链路层协议，需要流量控制机制。半双工和全双工：半双工通信时，提供收/发转换。

链路层的实现位置：路由器：链路层在线卡（line card）中实现。主机：链路层主体部分在网络适配器（网卡）中实现。线卡/网络适配器连接物理媒体，还实现物理层的功能

链路层由硬件和软件实现：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。

网络适配器之间的通信：发送侧:将数据报封装到帧中。生成校验比特。执行可靠传输和流量控制。接收侧：提取帧，检测传输错误。执行可靠传输和流量控制。解封装数据报，交给上层协议。

检错和纠错:传输出错的类型。单个错：由随机的信道热噪声引起，一次只影响1位。突发错：由瞬间的脉冲噪声引起，一次影响许多位，使用突发长度表示突发错影响的最大数据位数

差错控制编码的类型：检错码：只能检测出传输错误的编码，不能确定出错位置，通常与反馈重传机制结合进行差错恢复。纠错码：能够确定错误位置并自行纠正的编码。

如何检测与纠正错误？码字（codeword）：由m比特的数据加上r比特的冗余位（校验位）构成。有效编码集：由 2m 个符合编码规则的码字组成

检错：若收到的码字为无效码字，判定出现传输错误。海明距离（Hamming Distance）：两个码字的对应位取值不同的位数。纠错：将收到的无效码字纠正到距其最近的有效码字。检错码与纠错码的能力都是有限的！

编码集的检错与纠错能力：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，编码集的海明距离至少应为d+1。纠错能力：为纠正所有d比特错误，编码集的海明距离至少应为2d+1。

差错检测的实施：发送端对要保护的数据D（包括帧头字段）生成校验位EDC，添加在帧头中，接收端对收到的数据D’计算校验位EDC’，根据EDC’判定是否有错。

奇偶校验：单比特奇偶校验:可检测单比特错误，检错率为50%，编码集海明距离为2。二维奇偶校验:可检测2比特错和纠正单比特错。编码集海明距离为3。有利于检测突发错误。

循环冗余校验（CRC）：CRC是一种多项式编码，它将一个位串看成是某个一元多项式的系数，如1011看成是一元多项式X3+X+1的系数。

信息多项式M(x)：由m个信息比特为系数构成的多项式。冗余多项式R(x)：由r个冗余比特为系数构成的多项式。码多项式T(x)：在m个信息比特后加上r个冗余比特构成的码字所对应的多项式，表达式为。

生成多项式G(x)：双方确定用来计算R(x)的一个多项式。

编码方法：的余式（减法运算定义为异或操作）。

检验方法：若的余式为0，判定传输正确。

CRC的检错能力：1、单比特差错，只要G(x)含有一个以上的非零项。2、双比特差错，只要G(x)是本原多项式或者1+x乘一个本原多项式的形式。3、任意奇数个比特差错，只要G(x)含有因式(x+1)或(x-1)。4、任意突发差错，当突发差错长度小于或等于r。5、长度为r+1的突发差错片段，这个片段等于。6、长度大于(r+1)的突发差错片段，这个片段等于。

CRC举例：例1：取，对信息比特101110计算CRC码。

解答：101110000 ÷1001的余式为R=011 (CRC code)。码字：101110011

例2：取，接收端收到比特串1001001，问是否有错？

解答：1001001÷1001的余式为001（不为0），有传输错误。

为什么链路层使用CRC，而其上各层使用checksum？

因为运输层差错检测用软件实现，采用简单而快速如检验和这样的差错检测方案是重要的。在另一方面，链路层的差错检测在适配器中用专用的硬件实现，它能够快速执行更复杂的CRC操作。

链路的两种类型：点到点链路：仅连接了一个发送方和一个接收方的链路

一条全双工链路可以看成是由两条单工链路组成。

广播链路：连接了许多节点的单一共享链路，任何一个节点发送的数据可被链路上的其它节点接收到。

多址接入（Multiple Access）：冲突（collision）：在广播链路上，若两个或多个节点同时发送，发送的信号会发生干扰，导致接收失败。

多址接入协议：规定节点共享信道（谁可以发送）的方法。多址接入协议也称媒体接入控制（Medium Access Control，MAC）协议。

理想的多址接入协议：在速率为R bps的广播信道上:1. 当只有一个节点发送时，它应能以速率R发送（信道利用率高）2. 当有M个节点发送时，每个节点应能以 R/M的平均速率发送（公平性好、信道利用率高）。3. 协议是完全分布式的:不需要一个特殊的节点来协调发送（健壮性好）。不需要时钟或时隙同步（不需要额外的机制）。4. 简单（实现和运行开销小）。

MAC协议的分类：信道划分：将信道划分为若干子信道，每个节点固定分配一个子信道，不会发生冲突；关注公平性，轻负载时信道利用率不高。

随机接入（竞争）：不划分信道，每个节点自行决定何时发送，出现冲突后设法解决。轻负载时信道利用率高，重负载时冲突严重。

轮流使用信道：不划分信道，有数据的节点轮流发送，不会出现冲突；信道利用率是以上两种方法的折衷，引入额外机制。

信道划分的MAC协议：TDMA: 时分多址：将信道的使用时间划分成帧，每个节点在帧中被分配一个固定长度的时间片，每个时间片可以发送一个分组；节点只能在分配给自己的时间片内发送；若节点不发送，其时间片轮空。

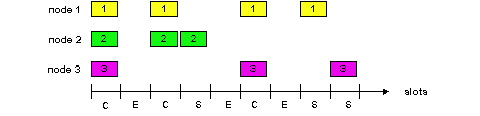
FDMA: 频分多址：将信道频谱划分为若干子频带；每个节点被分配一个固定的子频带；若节点不发送，其子频带空闲。

CDMA: 码分多址：将每个比特时间进一步划分为m个微时隙（称chip）每个节点被分配一个惟一的m比特码序列（称chip code）。发送方编码：发送“1”=发送chip code；发送“0”=发送chip code的反码；信号叠加：多个节点发送的信号在信道中线性相加；接收方解码：用发送方的chip code与信道中收到的混合信号计算内积，恢复出原数据；前提条件：任意两个chip code必须是相互正交的；CDMA允许所有节点同时使用整个信道！

随机接入的MAC协议：随机接入的基本思想：当节点有数据要发送时，以信道速率R发送，发送前不需要协调。随机接入MAC协议规定如何检测冲突，以及如何从冲突中恢复。随机接入MAC协议的例子：发送前不监听信道：ALOHA家族。发送前监听信道：CSMA家族。

时分（Slotted）ALOHA：

假设:所有帧长度相同。时间被划分为等长的时隙，每个时隙传一帧。节点只能在时隙开始时发送。节点是时钟同步的（知道时隙何时开始）。所有节点可在时隙结束前检测到是否有冲突发生。

操作:节点从上层收到数据后，在下一个时隙发送。若时隙结束前未检测到冲突，节点可在下一个时隙发送新的帧。若检测到冲突，节点在随后的每一个时隙中以概率P重传，直至发送成功。

优点：单个活跃节点可以信道速率连续发送。分布式：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。由于概率重传，有些时隙被闲置。需要时钟同步。

时分Aloha的效率：

效率：当网络中存在大量活跃节点时，长期运行过程中成功时隙所占的比例。

假设: 有N个活跃节点，每个节点在每个时隙开始时以概率P发送。。

最大效率: 找到令最大的概率p\* 。代入，并令N趋向于无穷，得到：最大效率 = 1/e。

最佳情况: 信道用于有效传输的时间仅为37%。

纯ALOHA：基本思想：取消同步时钟，任何节点有数据发送就可以立即发送

节点通过监听信道判断本次传输是否成功。若不成功，立即以概率P重传，以概率（1-P）等待一个帧时后再决定。（帧时：发送一帧的时间，假设帧长度相同）。发生冲突的情形：在时刻t0发送的帧与在 [t0-1,t0+1] 时段内发送的其它帧冲突。

P(给定节点发送成功)=P(节点发送)\*P(无其它节点在[t0-1,t0]内发送)\* P(无其它节点在[t0, t0+1]内发送)=p\*(1-p)N-1\*(1-p)N-1=p\*(1-p)2(N-1)

求出令节点发送成功概率最大的，并令N->infty:最大效率=1/(2e)=0.18

载波侦听多址接入（CSMA）:发送前监听信道（carrier sensing）：信道空闲：发送整个帧。信道忙：推迟发送。冲突仍可能发生:由于存在传输延迟，节点可能没有监听到其它节点正在发送。即使忽略传输延迟，当两个（或多个）节点同时发现信道由忙变为空闲、并都决定立即发送时，仍会发生冲突。

CSMA/CD (Collision Detection)：若在发送的过程中检测到冲突，怎么办？继续发送余下的部分（浪费带宽）；停止发送余下的部分

CSMA/CD的基本思想：在发送的过程中检测冲突（发生冲突时信号较强）。检测到冲突后，立即停止发送剩余的部分。立即启动冲突解决的过程。

以太网MAC协议：以太网采用CSMA/CD协议:1、NIC从网络层接收数据报，构造以太帧；2、若NIC监听到信道空闲，立即发送帧；若信道忙，坚持监听直至发现信道空闲，然后发送帧；3、若NIC发送完整个帧而没有检测到冲突，认为发送成功！4、若NIC在传输过程中检测到冲突，立即停止发送帧，并发送一个阻塞信号（加强冲突）；5、NIC进入指数回退阶段，选择一个等待时间: 第一次冲突后: 从{0,1}中选择K，延迟K· 512比特时间

第二次冲突后: 从{0,1,2,3}中选择K，……

第三次冲突后: 从{0,1,2,3,4,5,6,7}中选择K，……

……

第10次冲突后，从{0,1,2,3,4,…,1023}中选择K，……

6. 返回Step 2

指数回退的目的是根据网络负载调整重传时间：负载越重（冲突次数越多），重传时间的选择范围越大，再次发生冲突的可能性越小

CSMA/CD的效率： = 以太网中任意两个节点之间传播延迟的最大值。

= 最长帧的传输时间

在以下情况下，以太网的效率趋近于1： 趋近于 0，或 趋向于无穷。结论：应控制以太网的规模。

轮流MAC协议：轮询：主节点轮流“邀请”从节点发送，邀请到的从节点允许发送。缺点:引入轮询延迟。单点失效（主节点）

令牌传递：网络中有一个令牌，按预定顺序在节点间传递。获得令牌的节点可以发送。发送完数据后释放令牌。缺点：令牌传递延迟。单点失效（令牌）

MAC协议比较：

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），如中心结点轮询、令牌传递（FDDI、IBM令牌环、令牌总线）

链路层编址：每一块网络适配器（网卡）固定分配一个地址，称为物理地址、硬件地址、链路层地址、MAC地址等。MAC地址长6个字节，一般用由“ : ”或“ - ”分隔的6个十六进制数表示。MAC地址由IEEE负责分配，每块适配器的地址是全球唯一的：网卡生产商向IEEE购买一块MAC地址空间（前3字节）生产商确保生产的每一块网卡有不同的MAC地址。MAC地址固化在网卡的ROM中。现在用软件改变网卡的MAC地址也是可能的。

MAC地址类型：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；广播地址：ff:ff:ff:ff:ff:ff 。

网络适配器仅将发送给本节点的帧交给主机：目的地址为适配器MAC地址的单播帧、所有广播帧、指定接收的多播帧。将适配器设置成混收模式，适配器将收到的所有帧交给主机。

如何实现直接交付？

当发送节点A、接收节点B位于同一个物理网络上时，数据报可从A直接交付给B：A的网络层将数据报、以及B的物理地址交给数据链路层；数据链路层将数据报封装在一个链路层帧中，帧的目的地址=B的物理地址；B的适配器收到帧，根据目的地址判断是发给本机的，取出数据报交给网络层

地址解析（Address Resolution）：问题：已知IP地址，如何得到对应的MAC地址？静态映射IP地址-MAC地址的缺点：主机每次使用的IP地址可能不同（DHCP）、主机可能更换网卡。

地址解析协议（ARP）用于动态获得IP地址-MAC地址映射，其基本思想是：

若节点A希望获得节点B的MAC地址，节点A广播B的IP地址（地址解析请求），节点B用自己的MAC地址进行响应。

ARP报文格式：

硬件类型：硬件接口类型。对于以太网，该值为“1”。

协议类型：高层协议地址类型。对于IP地址，该值为。操作：ARP请求为1，ARP响应为2

在以太网上，ARP报文封装在以太帧中传输。

地址解析的过程：A想知道B的MAC地址：1、A构造一个ARP请求，在发送方字段填入自己的MAC地址和IP地址，在目标字段填入B的IP地址。2、A将ARP请求封装在广播帧中发送。3、每个收到ARP请求的节点用目标IP地址与自己的IP地址比较，地址相符的节点进行响应（B响应）。4、B构造一个ARP响应，交换发送方与目标字段内容，在发送方硬件地址字段填入自己的MAC地址，修改操作字段为2。5、B将ARP响应封装在单播帧（目的地址为A的MAC地址）中发送。

改进ARP的措施：ARP缓存：每个节点在内存中维护一个地址映射（绑定）表，称ARP缓存。每次发送数据报前先查询ARP缓存，若找不到则发送ARP请求，并在收到ARP响应后将地址映射缓存起来。ARP缓存中的信息，在超时（一般为15～20分钟）后删除。

主动学习：从ARP请求中获取地址绑定信息：每个节点可以收到全部的ARP请求报文，可将发送节点的地址映射缓存到自己的ARP表中。节点在启动时自动广播自己的地址映射：节点A在启动时主动广播一个ARP请求，在目标字段内填入自己的IP地址。收到ARP请求的节点将A的地址映射缓存起来。若A收到ARP响应，报告IP地址重复错误。

数据报的传输过程：数据报从A经过R到达B：1、A创建IP数据报，src IP＝A, dest IP＝B

2、A利用ARP获得下一跳111.111.111.110对应的MAC地址（R-1）

3、A创建链路层帧，封装IP数据包，src MAC =A, dest MAC = R-1，发送

4、R接收帧，取出IP数据报，发现目的地址为B。

5、R利用ARP获得B的MAC地址。

6、R创建链路层帧，封装IP数据报，src MAC=R-2, dest MAC = B, 发送

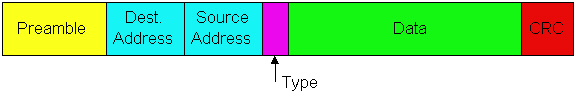
7、B的网卡接收帧，取出IP数据报，交给网络层。

以太网：第一个广泛应用的局域网技术，也是目前占主导地位的有线局域网技术。

总线拓扑（共享式以太网）：总线（1970s中期）：以同轴电缆作为共享传输媒体（总线）。所有节点通过特殊接口连接到这条总线上。集线器（1990s后期）：一个物理层中继器，从一个端口进入的物理信号（光，电），放大后立即从其它端口输出。集线器相当于共享电缆。

星型拓扑（交换式以太网）：交换机（21世纪早期）：主机通过双绞线或光纤连接到交换机。交换机在端口之间存储转发帧（链路层设备）。主机与交换机之间为全双工链路。交换式以太网不会产生冲突，不需使用CSMA/CD协议！星型拓扑：各节点仅与中心节点直接通信，各节点之间不直接通信。不同于基于hub的星型连接。

以太帧结构：

Preamble（前导码）:

7个10101010字节，后跟一个10101011字节，用于在发送方和接收方之间建立时钟同步。Dest.Address/Src Address：目的/源MAC地址。Type（2字节）: 指出Data所属的高层协议（如IP、ARP等），每个协议有一个编号。Data：46～1500字节，不足46字节填充至46字节。CRC（4字节）: 对dest addr.、src addr.、type和data四个字段计算得到的CRC码。

提供无连接、不可靠的数据传输：无连接: 发送方NIC与接收方NIC之间没有握手 。不可靠: 接收方NIC不发送确认，CRC检查出错的帧被丢弃，依靠上层协议（TCP或应用）恢复。

为什么有最小帧长的要求？为确保节点在发送结束前检测到冲突，帧的发送时间必须足够长：

节点检测冲突需要时间。假设信号在相距最远的两个适配器之间的往返延迟为，则帧的发送时间不应小于，即帧的最小长度≧链路速率×

为什么最小帧长为64字节（不包括前导码）：根据早期以太网的最大直径（2500米）和数据速率（10Mbps）计算得到。

802.3以太网标准: 链路层 & 物理层：历史上出现过许多不同的以太网技术：链路层相同：MAC协议，帧格式，帧处理。物理层不同：传输媒体: 光纤，同轴电缆，双绞线；数据速率: 如10Mbps（802.3）, 100 Mbps（802.3u）, 1Gbps(802.3z), …；物理层编码方式。

所有这些以太网技术由IEEE 802.3工作组标准化，形成IEEE 802.3标准族。

DIX以太帧与802.3帧：最早提出的以太帧称为DIX（DEC-Intel-Xerox）以太帧：type：指出处理data域的协议实体。符合IEEE 802.3标准的帧（802.3帧）：length：替代DIX帧中的type域，指出data的长度。这两种格式都可使用，当type/length的值大于1500时解释为type，否则解释为length。

共享式以太网：集线器的所有端口位于同一个冲突域，任一时刻最多只允许一个主机发送，网络规模（节点数量）与网络性能的矛盾无法解决。

交换式以太网：交换机的每个端口为一个冲突域，多对端口可以同时通信，网络的集合带宽=各个端口的带宽之和从根本上解决了网络规模与网络性能的矛盾。

交换式以太网的最小帧长及规模：交换式以太网不再使用CSMA/CD协议，理论上不再需要限制帧的最小长度。但为了向后兼容，帧格式及最小帧长度的限制仍然保持不变。由于交换式以太网不再使用CSMA/CD协议，网络直径不再受到信号最大往返时间的限制。

交换机：每个交换机内部有一张端口转发表，每个表项记录MAC地址以及到达该MAC地址的端口。交换机自主学习“哪个主机通过哪个端口可达”：当一个帧到达时，交换机从源MAC地址了解到发送节点，从帧到来的端口了解到发送节点的位置（从该端口可达）。在转发表中记录发送节点和可达端口。

交换机收到帧的处理过程：用帧的目的地址查找转发表（转发决策）（帧的过滤和转发）：若目的地址所在端口=帧的进入端口，丢弃帧（即过滤掉不需要转发的帧），若目的地址所在端口≠帧的进入端口，转发帧。若目的地址不在转发表中，扩散帧。

用帧的源地址查找转发表（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。

级联交换机：多个交换机也可以级联在一起，形成更大范围的局域网。

有环网络和生成树算法：为提高可靠性，网络中通常存在环（冗余链路），这会导致扩散的帧在网络中循环转发。使用生成树构造无环拓扑：所有交换机运行一个生成树算法，构造一棵覆盖网络中所有主机的生成树，平时只有生成树上的交换机可在属于生成树的边上转发帧。当生成树上的交换机或链路发生故障时，启用冗余链路，重新计算生成树。

交换机 vs. 路由器：1、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；2、交换机是即插即用设备，路由器需要手工配置；3、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）。4、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，路由器可以连接异构链路，因为路由器需重新封装链路层帧；5、交换机需运行生成树算法消除冗余链路，生成树算法假设网络是扁平的，对网络中的节点总数有限制，路由器无此限制。6、交换机不能阻断广播帧的传播：交换机只能学习到单播MAC地址，所有广播帧都会扩散发送通过交换机连接的所有主机在同一个广播域中。路由器可以阻断广播帧的传播：路由器根据IP地址转发包（看不到MAC地址），每个路由器端口是一个独立的广播域。

冲突域：共享同一条广播链路的主机集合，任何一个主机发送的帧（各种帧），可被冲突域中的其它主机接收到。

广播域：广播帧能够到达的主机集合。

虚拟局域网（VLAN）：位于物理局域网上的一个逻辑IP子网，包含了配置为该VLAN成员的所有节点，每个VLAN在逻辑上是一个独立的网络：每个VLAN是一个单独的广播域：一个VLAN中的所有帧流量被限制在该VLAN中，不同VLAN之间的通信要依赖于网络层路由。划分VLAN通过软件配置完成。

VLAN的实现基础是支持VLAN功能的交换机

管理员配置VLAN：管理员决定将物理网络划分成几个VLAN、每个VLAN的名字、每个机器在哪个VLAN上，在每个交换机上建立一个配置表，指出通过哪个端口可以到达哪些VLAN的成员（一个交换机端口可以到达多个VLAN的成员）。

IEEE 802.1Q：802.1Q规定了新的以太帧格式，帧头中包含一个VLAN标签（tag），用于指明帧属于哪个VLAN。

如何划分VLAN？基于交换机端口划分：将某些交换机端口直接、强制性地分配给某个VLAN

基于MAC地址划分：根据用户节点的MAC地址划分VLAN

基于IP地址划分：根据IP子网地址划分VLAN

交换机如何在VLAN间转发帧？当一个帧到达时，交换机判断该帧属于哪个VLAN，查找配置表得到该VLAN对应的端口，在该VLAN对应的所有端口上转发帧。

如何知道一个帧属于哪个VLAN？帧所属的VLAN = 发送节点所属的VLAN。交换机根据帧的到达端口、源MAC地址或源IP地址（取决于VLAN的划分方法），查找VLAN配置表。为避免重复查找 VLAN配置表，交换机将VLAN标识放入帧头中，后续交换机通过检查帧头的VLAN标识，得知这个帧所属的VLAN。

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。

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，通常用在机构网络的核心层，连接不同的子网或VLAN。专业路由器：连接机构网络与外网

三层交换机为什么快？提供本地转发表缓存，一次选路，多次转发。

The Internet: virtualizing networks：多个不连通的网络，他们在编址方法、包格式、差错恢复、选路等方面不同，在物理网络上增加一个逻辑层次（IP层），在逻辑层上统一编址、统一包格式，互联在一起的网络看起来像一个网络。用网关连接不同的物理网络: 在逻辑层上选路到下一个网关，将IP包封装在本地网络帧中，发送到下一个网关。

Cerf & Kahn’s Internetwork Architecture：两级编址: IP网络，物理网络。IP层提供统一的网络视图：地址，包格式。底层可以是任意的物理网络。物理网络对于IP层是不可见的，对于IP来说物理网络只是一条虚拟链路而已！

**无线和移动网络：**

与有线固定网络相比，无线移动上网增加了以下两方面的问题：

无线（wireless）：使用无线链路通信，给物理层和数据链路层带来很多问题。

移动（mobility）：终端改变网络接入点，给网络层带来很大问题

无线网络的组成：无线终端：laptop, PDA, IP电话。运行网络应用。可能静止或移动。无线并不一定意味着移动。基站：通常连接到固定网络，在无线终端和固定网络之间中继数据包，如802.11AP，蜂窝塔。通常负责协调与之关联的多个无线主机的传输。无线链路：连接无线终端和基站，需要MAC协议协调无线链路的使用，不同的无线链路具有不同的数据速率和传输距离。

无线网络的运行模式：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。

无线网络的分类：有基础设施：单跳：主机连接到基站，基站连接到固定网络(如WiFi，cellular)。多跳：主机通过多个无线节点的中继才能到达固定网络（如无线网状网络）。无基础设施：单跳：无基站，不连接到固定网络，节点间通信不需要中继（如蓝牙网络）。多跳：无基站，不连接到固定网络，节点间通信，需要通过其它节点中继（如自组网，车载网）。

无线链路的特性：信号衰减: 信号在传播过程中能量逐渐减少（路径损耗）。干扰: 受到其它信号源的干扰。多径传播: 由于地面或物体的反射作用，信号沿多条不同长度的路径到达接收端。以上特性导致无线链路的传输距离受限、误码率很高。

隐藏节点: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：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不适合多跳无线网络:通过载波侦听，发送节点只能知道其周围是否有节点在发送；但真正影响此次通信的是接收节点周围是否有节点在发送。隐藏节点：不在发送节点的通信范围内、但在接收节点通信范围内的活跃节点。（发送节点听不到，但影响接收）暴露节点：在发送节点的通信范围内、但不在接收节点通信范围内的活跃节点。（发送节点能听到，但不影响接收）.

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，物理层不同。

802.11无线局域网架构：802.11无线LAN的基本组成单元是基本服务集（BSS），一个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。

信道与关联：802.11将通信频段划分成若干信道，每个BSS分配一个信道：管理员安装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。

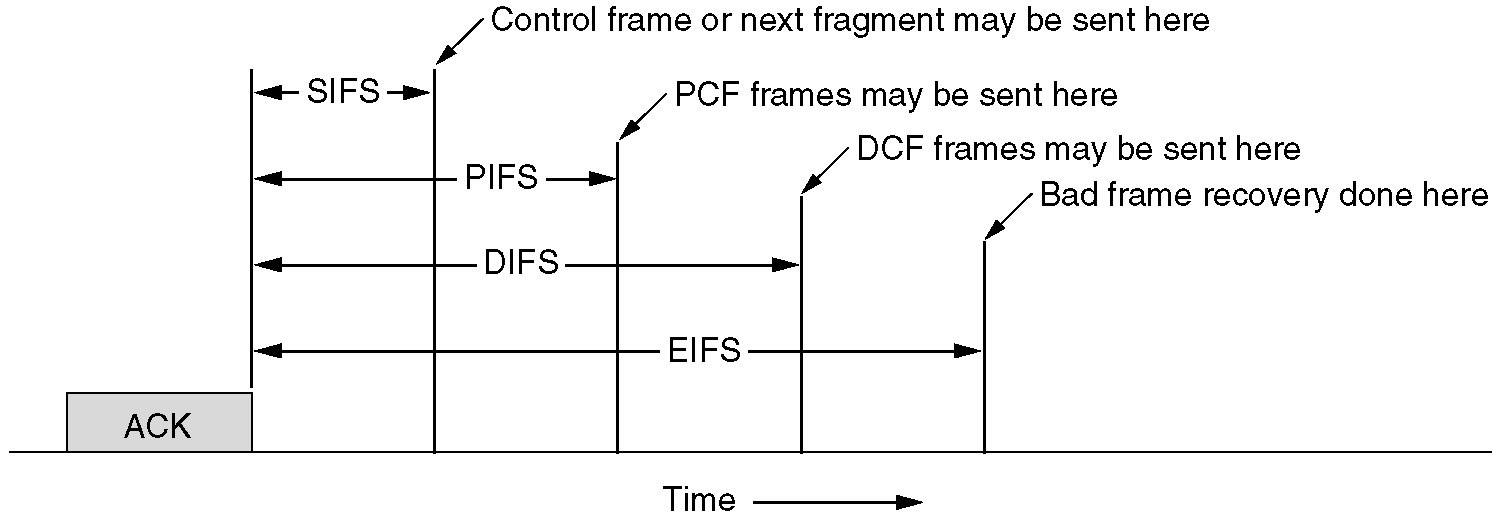
被动扫描: 主机监听AP发送的信标帧，主机选择一个AP发送关联请求帧，AP向主机发送关联响应帧。主动扫描: 主机广播探测请求帧，AP发送探测响应帧，主机从收到的探测响应中选择一个AP发送关联请求，AP发送关联响应帧。

IEEE 802.11：MAC协议:采用CSMA：发送前监听信道，不与当前正在进行的发送冲突。不检测冲突：发送过程中检测冲突很困难（接收信号的强度远小于发送信号的强度），不能检测出所有的冲突（隐藏节点）。目标：避免冲突 CSMA/C(ollision)A(voidance)。

802.11的操作模式—PCF（Point Coordination Function）：该模式只能用于有基础设施（基站）的无线网络，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。PCF的实现是可选的。

802.11的操作模式—DCF（Distributed Coordination Function）：可用于有基础设施的无线网络和无基础设施的无线网络，所有实现必须支持DCF模式，所有节点（AP和无线终端）使用CSMA/CA协议竞争信道。CSMA/CA支持两种机制：信道预约机制（可选），无信道预约的机制。

使用信道预约机制的CSMA/CA：假设A欲向AP发送一个数据帧：1、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。2、AP收到后回复一个CTS帧，帧中给出同样的时间。3、A收到CTS帧后开始发送4、AP收到帧后，发送一个ACK帧进行确认。5、（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。6、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。

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。

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。

CSMA/CA与CSMA/CD的不同：最根本的不同：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。由此带来的协议处理方面的不同：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。

802.11帧格式：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Frame control(2) | Duration(2) | Address2(6) | Address2(6) | Address3(6) |
| Seq control(2) | Address4(6) | Payload(0-2312) | CRC(4) |  |

Duration：duration of reserved transmission time (RTS/CTS)。Address 1: 帧的目的MAC 地址。Address 2: 帧的源MAC地址。Address 3: 连接AP的路由器接口的MAC 地址。

Seq control：frame seq #(for reliable ARQ)。Address 4: 只在自组织模式中使用。

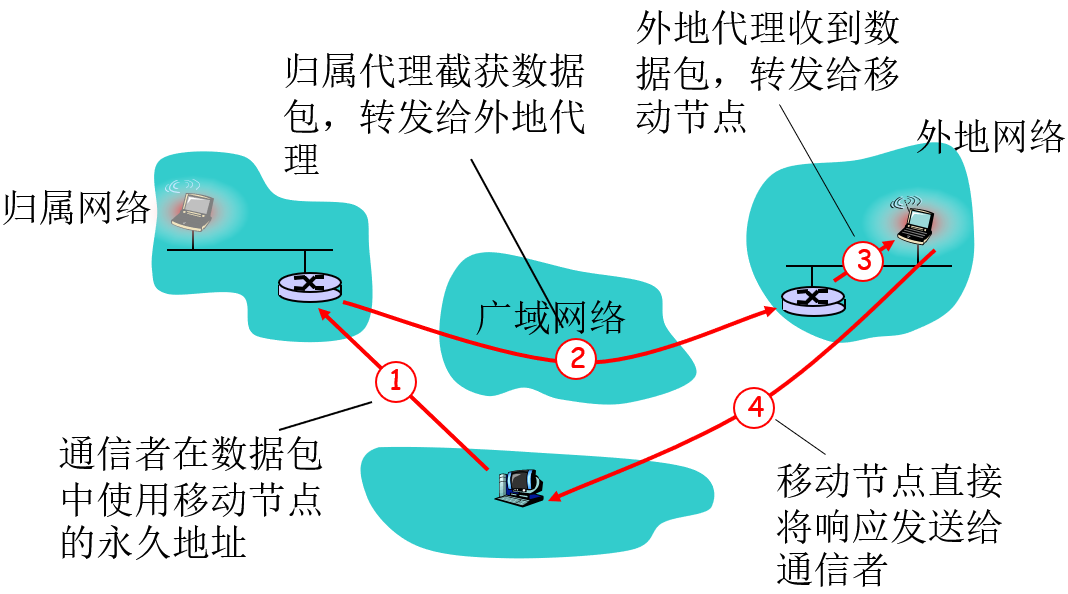
AP仅对无线终端可见，对于固定网络上的设备是不可见的，AP连接路由器的有线端口没有MAC地址！

终端在子网内移动：切换：终端从一个BSS移动到另一个BSS。发生切换时，终端要关联到新的AP上：当H1检测到来自AP1的信号逐渐减弱时，开始扫描新的信标帧，当H1收到来自AP2、信号更强的信标帧时，先解除与AP1的关联，然后关联到AP2。发生切换时，交换机中的转发表也需要更新，交换机通过自主学习更新转发表：交换机收到H1发送的帧时，更新H1所在的端口，若转发表未及时更新，可能产生丢包。802.11f规定了AP间漫游的方法。主机停留在同一个IP子网中，因而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。

802.11: 先进功能：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：节点进入休眠，并在下一个信标帧之前醒来，在节点休眠期间，AP缓存发往该节点的帧，AP在发送的信标帧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。

终端在IP子网间移动：终端进入到一个新的子网后，必须分配该子网上的一个地址（DHCP），并使用新的地址通信：终端在进入新的子网后，不能保留其IP地址，然而，当终端改变IP地址后，终端上正在运行的应用将中断：通信的对方不知道终端的新地址，无法与其通信。即使对方获知了终端的新地址，应用必须重新建立连接，因为通信的端点（套接字）变了。

归属网络:移动节点的永久“居所”。归属代理:当移动节点在外地时，为移动节点执行移动管理功能的实体。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，保持不变。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。通信者:希望与移动节点通信的节点。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。

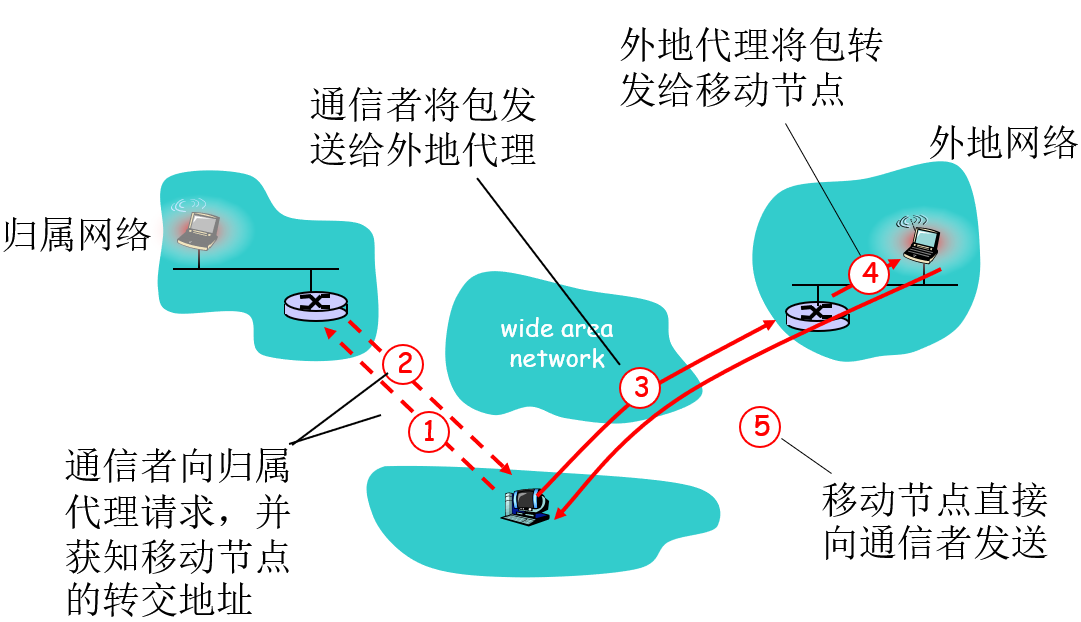
移动节点注册：移动节点进入外地网络后，向外地代理注册，移动节点通过外地代理向归属代理注册。

最终结果:外地代理知道移动节点在本地网络上。归属代理知道移动节点的转交地址，记录到地址绑定表中。

间接选路到移动节点：见左图。

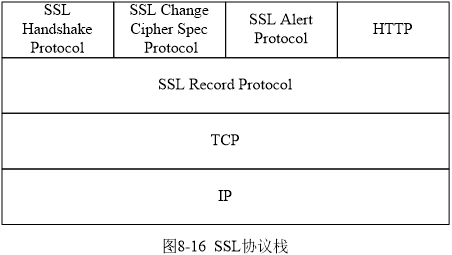
三角选路问题：通信者-归属网络-移动节点。

间接选路：终端在外地网络间移动：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！

直接选路到移动节点：见左图

克服了三角选路的问题：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。

Mobile IP：特性：归属代理，外地代理，永久地址，转交地址，移动节点注册等。标准化了三个部分:代理发现、移动节点注册、数据报间接选路

代理发现：1、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，宣布自己的存在及IP地址2、愿意充当外地代理的路由器在代理通告中会提供一个或多个转交地址（通常使用自己的IP地址作为转交地址）3、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以及是否切换了网络4、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。

移动主机注册：1、移动节点向外地代理发送一个注册请求，给出自已的永久地址、转交地址、归属代理地址以及认证信息等。2、外地代理记录相关信息，向归属代理转发注册请求。3、归属代理处理注册请求，若认证通过，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4、外地代理收到有效的注册响应后，将移动节点记录在自己的转发表中，向移动节点转发注册响应。5、当移动节点回到归属网络时，要向归属代理注销。

数据报间接选路：1、数据包首先被归属代理得到；2、归属代理查找地址绑定表，获得移动节点当前的转交地址；3、归属代理将数据包发送到转交地址；4、外地代理将数据包转发给移动节点。

归属代理如何得到数据报？若通信者不在归属网络上：数据包首先到达移动节点归属网络上的路由器。路由器查表得知可以直接交付，于是查找ARP缓存或者发送ARP请求，以获取移动节点的MAC地址。利用得到的MAC地址，将数据报封装到链路层帧中发送。若通信者在归属网络上：通信者查表得知移动节点直接可达，于是查找ARP缓存或者发送ARP请求，利用得到的MAC地址封装数据报，发送。

数据报如何能被归属代理得到？链路层帧的目的地址必须是归属代理的MAC地址。也就是说，移动节点的永久地址 应当映射到归属代理的MAC地址。

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

也就是说，将移动主机的永久地址映射到归属代理的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请求，刷新其它节点的ARP缓存。

归属代理如何将数据报发送到转交地址？归属代理收到的数据报，目的地址为移动节点的永久地址，而移动节点的转交地址位于外地网络。如何将目的地址在归属网络的数据报送达外地网络？方法：修改目的地址=转交地址 （×）（转交地址是外地代理的IP地址，而数据报的最终目的地应是移动节点）使用隧道（√）（隧道技术的又一个应用例子）。

外地代理如何转发数据包到移动节点？外地代理解封装收到的数据包，得到原始数据报

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。

移动节点如何发送数据包？移动节点将数据包发送给外地代理（缺省路由器）：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，外地代理按照正常方式转发数据包。

移动节点如何得知外地代理的MAC地址？代理通告报文的源MAC是外地代理的地址。

无线和移动对上层协议的影响：

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

逻辑上，没什么影响：为上层协议提供的仍然是尽力而为的服务，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

无线链路、有线/无线混合链路上的TCP拥塞控制是一个研究问题。

**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(不影响系统)：偷听、流量分析;主动攻击(影响)：伪装、重放、报文修改、拒绝服务

安全机制：加密、鉴别、数字签名、报文完整性、流量填充、访问控制

密码学术语：明文(预加密的原始数据)，密文(明文经加密算法后的输出),密钥(加密和解密使用的参数),密码分析(破译密文),密码学(设计密码和破译密码技术)

算法分类：对称加密/非对称加密(加密解密密钥是否相同);块密码/流密码(明文块or明文流)

传统方法：替换、换位。安全性建立在算法保密基础上

现代算法：基本手段同上。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

计算安全：(满足其1)破译密文代价超过信息本身价值or破译密文的时间超过信息有效生命期

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

密码分析攻击：惟密文攻击；已知明文攻击；选择明文攻击[安全加密系统需要能抵御]

对称密钥算法：(问题：如何将密钥安全发送给对方)  
-DES:64bits明文→64bits密文,基于迭代的算法,每轮执行相同替换和换位操作(但不同密钥)；56bits主密钥,每轮迭代的48bits子密钥由之产生[加密解密函数相同，但子密钥次序相反]；缺点：密钥长度不够长，迭代次数不够多。过程：换位→16轮相同迭代(不同子密钥)→换位

-3DES:两个密钥进行三轮DES:1)DES在加密模式,用密钥K1对明文变换.2)DES在解码模式,用密钥K2对第一轮输出做变换.3)DES在加密模式，用K1对第二轮输出做变换→输出。探讨:2个密钥112bits已够长;EDE比EEE更与DES兼容(令K2=K1);EDE(2^112)比EE(2^56)安全性更高

-AES:128bits明文、密文块，密钥长度可以是128、192、256bits

-密码块链接(CBC):发送方生成随机初始向量c(0),明文发送给接收者;每个明文块加密前,先与前一个密文块进行异或,然后再加密(第一个与c(0))。相同明文几乎不可能得到相同密文

非对称加密：(加密密钥公开，解密密钥私有):给定公钥K+,不可能计算出私钥K-.

-RSA:两个大素数p,q.n=p×q,z=(p-1)(q-1).找到一个小于n的e使e和z互素.找到d使e×d=1(mod z).公钥(e,n),私钥(d,n).将明文看成比特串,划分为若干数据块M(M比n小).加密:对每个M,C=M^e(mod n)为密文；解密:M=C^d(mod n)。RSA公私钥先后用结果相同->数字签名中有用

优点:安全性好(难以对大数取因子),使用方便(无需传递密钥);缺点：计算速度慢。一般用来加密少量数据(鉴别、数字签名、一次性会话密钥)

报文完整性(报文鉴别): 1.报文摘要直接验证2.对报文摘要加密，保证不被篡改(a.共享密钥加密[报文鉴别码]；b.发送方私钥加密[数字签名])3.密码散列函数H(K\_S||m)[也是报文鉴别码]。报文是否可信→来自声称的源[起源鉴别]且没有被修改[完整性检查]

方法：-对整个报文加密.(缺点:混淆机密性和鉴别,有时报文无需加密;带来计算开销) -报文摘要(数字指纹):用共享密钥加密报文摘要，形成报文鉴别标签(报文鉴别码),接收方解密得到摘要，和自己计算的做对比(缺点:需要加密算法[代价高,受专利保护和出口限制]) -密码散列函数:用双方共享的一个秘密密钥K\_s添加到报文m之前,然后计算报文摘要H(K\_s||m)形成报文鉴别码.[散列函数H:作用于任意长度的数据块，并生成固定长度的输出;易计算;单向性;计算上不可能找到y≠x且H(y)=H(x)(满足这个特性为强散列函数) 抵抗生日攻击]。常用散列函数:MD5(128bits),SHA-1(160bits),HMAC

数字签名:接收方通过文档中数字签名能够鉴别发送方身份(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。过程:发送方用自己的私钥加密报文摘要形成数字签名，数字签名附加在报文后面一起发送。接收方拷贝一份数字签名，妥善保存，以备将来需要时使用。接收方用发送方的公钥得到原始的报文摘要，对收到的报文计算摘要，如果两者相符，表明报文是真实的。

公钥证书:证明某个主体拥有某个公钥。由认证权威CA颁发.证书包含主体的公钥和CA的签名，任何人无法篡改.证书可放在任何公开访问的地方。证书获取：Bob向CA提供身份证明、CA验证Bob身份后创建证书，绑定Bob及Bob的公钥、证书包含Bob公钥并有CA签名。证书验证: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。常用：X.509证书标准: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。分布式公钥基础设施(PKI):提供公钥加密和数字签名服务,包含不同组织运行的CA，每个CA拥有自己的私钥，用户自已决定使用哪一个CA. CA的组织:树形结构.

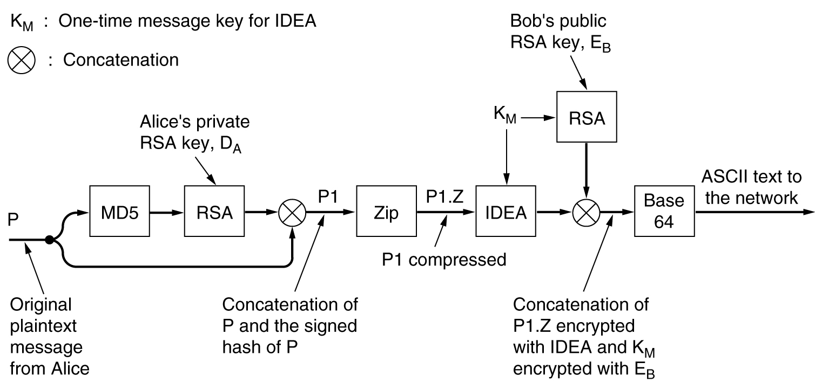
信任锚:信任的起点，系统中的所有实体都以根CA的公钥作为它们的信任锚，必须通过安全的物理途径获取;信任链:从叶结点到根CA的证书序列。根CA的选择:各CA都有自己的一个分级结构，所有根CA间可以进行交叉认证。用户自行决定信任哪个根CA。实际上，许多根CA的公钥被预装在浏览器上，这些根CA由浏览器厂商认证并嵌入到软件中，随软件一起发布

证书的撤销:有效期过后自动失效。CA显式撤销:定期发布证书撤销列表(CRL),给出撤销的证书序列号。用户使用前获取CRL，检查证书是否在CRL中。

鉴别：ap1.0—ap5.0。X.509定义三种鉴别程序: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。

单向鉴别:说明:**tA**：时间戳，由报文的产生时间和到期时间组成;**rA**：A随机选择的一个不重数，供接收者检测重放攻击;IDB：B的标识，指示报文的接收者;Data：报文中包含的数据信息;**Ka-b** ：若Data需要保密，则Ka-b为A加密Data使用的对称密钥;**Kb+**：B的公开密钥，用于加密对称密钥Ka-b;signatureA ：A的数字签名，对tA、rA、IDB和Data的明文生成。接收方鉴别:B用自己的私钥解出Ka-b，用Ka-b解密Data，计算前面4个部分的报文摘要;B用A的公钥从签名中得到原始的报文摘要，进行比较。

双向鉴别：A→B：tA || rA || IDB || Data || Kb+ (Ka-b) || signatureA;B→A：tB || rB || IDA || **rA**|| Data || Ka+(Kb-a) || signatureB。三向鉴别: A→B：tA || rA || IDB || Data || Kb+ (Ka-b) || signatureA; B→A：tB || rB || IDA || rA|| Data || Ka+(Kb-a) || signatureB; A→B：rB || signature

电子邮件安全: S/MIME(基于公钥加密技术,作为工业标准被商业组织或机构使用);PGP协议(因特网安全邮件的事实标准，多用于个人电子邮件)：鉴别、机密性、压缩、兼容电子邮件、分段5种服务。鉴别:基于公开密钥算法的数字签名:发送方创建电子邮件（报文）,用SHA-1计算邮件的报文摘要，然后用发送者的私钥加密报文摘要，形成数字签名,将数字签名附在报文的前面，与报文一起发送:Sgn || Data。机密性:(对称密钥算法)发送方（A）生成一个报文和一个随机的128比特数(一次性会话密钥),先用会话密钥加密报文，再用接收方（B）的公钥加密会话密钥,将加密后的会话密钥放在报文前面，与报文一起发送: KB+(KA-B) || KA-B (Zip (Sgn || Data))。压缩: PGP在完成签名之后、在加密报文之前对报文进行压缩，压缩算法采用ZIP：KB+(KA-B) || KA-B (Zip (Sgn || Data)).[压缩前计算数字签名，方便日后对报文验证;加密前进行压缩，减少要加密的数据量，且压缩后的消息冗余很少，增加密码分析难度]。兼容电子邮件:使用Base64编码将二进制数据流转换成可打印ASCII文本;可被配置为仅对报文中的某些部分（如签名部分）进行Base64编码转换。EncodeBase64(KB+(KA-B) || KA-B (Zip (Sgn || Data)))

邮件分段: PGP处理报文后自动将超过长度的分成小块传输，会话密钥和签名只在第一个片段中出现;接收端去掉每个片段的头部，然后将所有的片段重新组装成一个数据块。

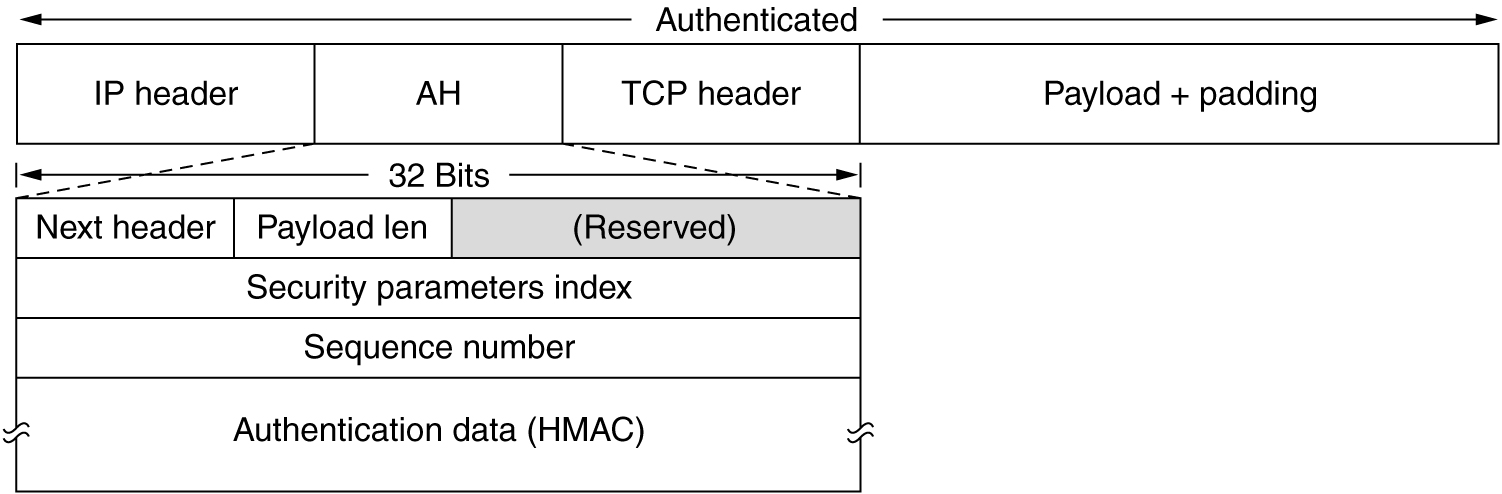
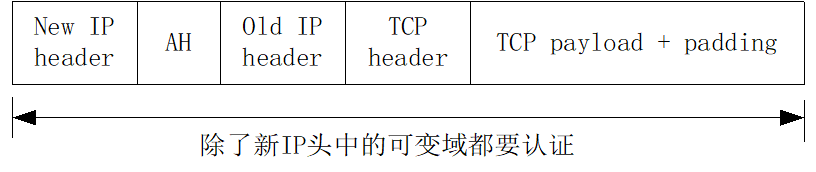
SSL:[应用层和TCP间的sublayer]向基于TCP的网络应用提供安全的传输层服务(如https)。提供服务器鉴别,数据加密,客户鉴别服务。SSL记录协议为高层协议(如http)提供基本的安全服务，其它三个高层协议用于SSL交换管理。握手协议:服务器和客户相互鉴别并协商加密算法、MAC算法及密钥。握手协议由客户和服务器之间的一系列报文交换组成:浏览器向服务器发送建立SSL会话请求，说明支持的SSL协议最高版本、支持的加密算法（按优先级从高到低排列）和压缩方法等，以及浏览器选择的一个随机数Rc。服务器从浏览器给出的选择中确定合适的SSL版本号、加密算法和压缩方法，与服务器选择的一个随机数Rs一起发送给浏览器。服务器向浏览器发送它的公钥证书（和必要的证书链）以及其它信息。浏览器检查签发证书的CA是否在浏览器的可信CA列表中，若不在向用户警告该问题；如果在则使用该CA的公钥验证证书，得到服务器的公钥。如果客户也需要被鉴别（收到服务器的证书请求），则浏览器向服务器发送它的公钥证书。浏览器生成一个48字节的随机数，称预密钥，用服务器的公钥加密后发送给服务器。客户和服务器各自从预密钥、Rc和Rs中计算加密数据需要的会话密钥，以及计算MAC需要的密钥。浏览器向服务器发送一个报文，通知它后面的报文都用这个会话密钥加密，然后发送一个用协商的算法及密钥加密的报文，指示握手协议的浏览器部分完成。 服务器向浏览器发送一个报文，通知它后面的报文都用这个会话密钥加密，然后发送一个用协商的算法及密钥加密的报文，指示握手协议的服务器部分完成。记录协议:机密性[加密SSL载荷]、完整性[报文鉴别码保护]两种服务。流程:从上层接收一个要传输的应用报文，将报文划分成长度不超过214字节的数据块;（可选）对数据块进行压缩;使用密码散列函数对数据块计算报文鉴别码;使用对称密钥算法对（压缩的）数据块及报文鉴别码进行加密，加密算法可以是DES、3DES、IDEA、RC等;在处理完的数据块前加上SSL头，包括内容类型、SSL版本号、压缩数据块的长度

IP安全协议(IPSec):一组安全协议集，将安全特征集成到IP层，以便底层实现因特网安全

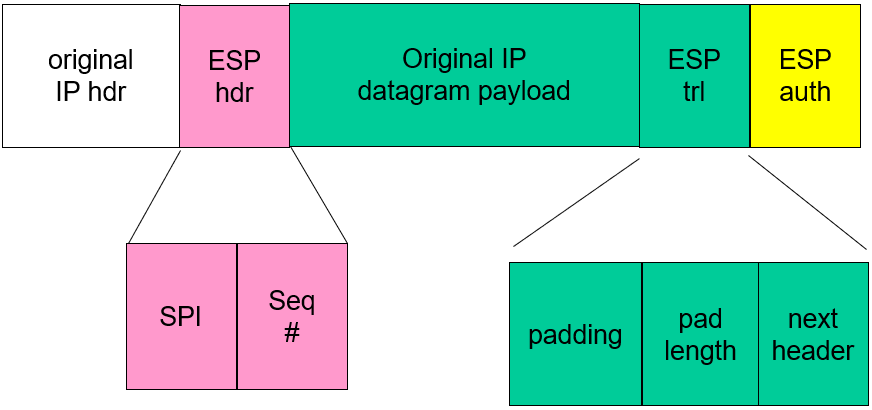
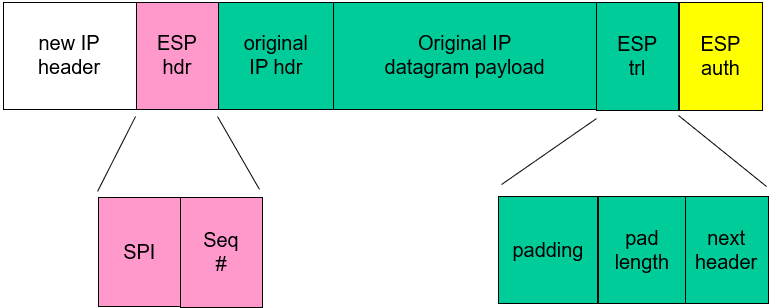
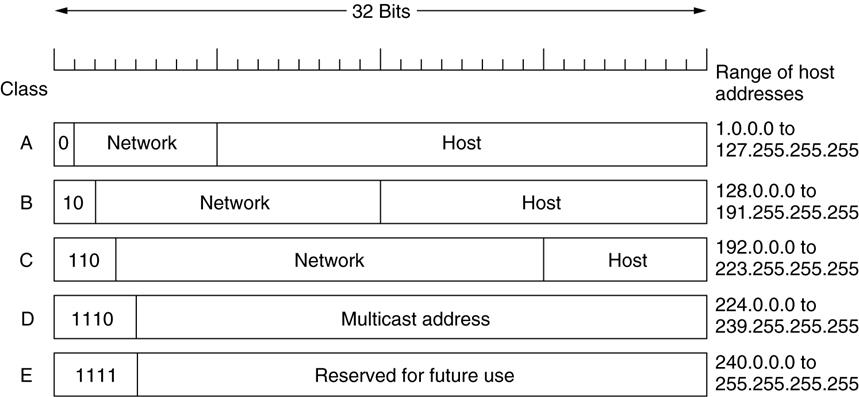
专用网:电信专线连接成的网络，安全性好但代价高;虚拟专用网(VPN):公用网上的一个覆盖网络，逻辑上与其他流量隔离,数据发到公用网前加密。VPN的实现:局域网上设一安全网关，网关间穿过因特网的隧道，隧道中使用IPSec. VPN优点:局域网间提供完整性控制及机密性服务，甚至对流量分析也有相当的抵御能力;对因特网中的路由器及用户软件是透明的，只要系统管理员设置好安全网关就可以了。 IPSec提供安全体系框架:安全服务包括：访问控制、无连接完整性、数据起源认证、抗重放攻击、机密性等。IPSec的安全机制独立于算法，因此在选择和改变算法时不会影响其它部分的实现。提供多种粒度:TCP连接、主机间、网关间的安全通信

IPSec组成:1.安全协议AH和ESP，定义IP扩展头和字段;2.密钥管理协议,定义通信实体身份鉴别、协商加密算法、生成共享密钥的方法.←绑定在一起的是安全关联(SA)。SA:两个通信端点间的一个单工连接，由安全参数索引（SPI）唯一标识，如果在两个方向上都需要安全通信，则需要建立两个SA。SPI携带在数据包中，由数据包的处理进程用来查找密钥及相关信息。SA可以建立在一对主机之、一台主机与一个安全网关、一对安全网关之间。IPSec使用:IPSec头插在IP头和传输层头间(传输模式) or 原始数据包封装在新的IP包中，IPSec头放在新IP头和原始IP头之间，路由器根据外层IP头的信息(地址常是支持IPSec的安全网关)转发数据包.比较:传输模式占用带宽少;隧道模式更安全(隐藏内部细节;内部网络上的主机不运行IPSec,网关保证其安全性;可将一对端点间的通信聚合成一个加密流，防止入侵者进行流量分析)

鉴别头部协议(AH):SPI：32比特的数，和目的IP地址、安全协议结合，唯一标识数据报的SA;SeqNum：对SA上发送的数据包编号，供接收端检测重放攻击,一个SA上的序号不能重用，因此在传输的数据包数量达到232之前，必须协商一个新的SA和新的密钥。Authentication Data：包含报文鉴别码的可变长度域。所有AH实现必须支持HMAC-MD5-96和HMAC-SHA-1-96。

提供服务:无连接完整性(HMAC覆盖数据包的载荷部分)、数据起源认证(HMAC覆盖原始IP头中的不变域（传输模式）或整个原始IP头（隧道模式），因而可提供数据起源认证)和抗重放攻击(AH头中有序号，且被HMAC覆盖)，但不提供机密性服务

封装安全载荷协议(ESP):ESP头：包含SPI和SeqNum;载荷：原始数据包中被加密部分的密文;ESP尾：包括填充（需要的话）、填充长度和下一个头，ESP尾也要被加密;鉴别数据：覆盖ESP头、载荷和ESP尾的报文鉴别码。提供服务:数据机密性(载荷被加密)、无连接完整性、抗重放攻击、数据起源鉴别和有限的数据流机密性服务(隧道模式原始IP头被加密)

安全性对比:ESP隧道>ESP传输;鉴别:ESP隧道>AH,ESP传输<AH;只有ESP提供数据机密性服务

安全WLAN:802.11WEP[主机和基站弱加密和鉴别服务,无密钥分发]、802.11i[密钥分发机制]

WEP:1)主机鉴别:主机向AP请求鉴别;AP向主机发送一128比特不重数;主机使用与AP共享的对称密钥加密不重数，发给AP;AP解密不重数，若与AP发送给主机的不重数相同，完成主机鉴别。2)数据加密:主机与AP共享一个40比特的对称密钥KS（半永久）;对于每个帧，发送方生成一个24比特的初始向量IV，添加到KS后面，形成一个64比特的密钥 (KS, IV);(KS, IV) 用于生成一个密钥流 {ki**IV**|i=1,2,…};第 i 个密钥ki**IV**用来加密帧中的第 i 个字节di:ci *=* diXORki**IV**;IV和加密后的字节ci放在帧中传输;接收方使用相同的 (KS, IV) 生成相同的密钥流，执行解密运算：di *=* ciXORki**IV**。安全漏洞:IV重复使用，攻击者可以观察到

802.11i:使用专门的鉴别服务器而非AP.

防火墙:可信内部网络与不可信外部网络之间执行访问控制策略的硬件或软件系统

-包过滤防火墙:访问控制列表(<动作,匹配条件>)，对每个包自上而下匹配规则

-状态检测防火墙:可以跟踪TCP连接的状态(建立SYN/关闭FIN)，判断收到的包是否有意义

-应用网关:除了检查网络层及传输层协议头，还检查应用层数据

防火墙的局限性:无法抵御IP欺骗;应用网关处理慢;每个代理应用都需要一个应用网关;应用网关对用户不透明,客户软件需要设置网关的IP;对UDP包一刀切;和外界通信强度矛盾

IDS:深度数据包检查: 查看包内容;检查多个包的关联性

1. 一个子网IP地址为10.115.0.0，子网掩码为255.224.0.0的网络，网络地址：10.96.0.0，广播地址：10.127.255.255，最小用户地址：10.96.0.1，最大用户地址：10.127.255.254。

2. 一个IPv4分组的分片中，MF位是0，HLEN是10，总长度是200，分片偏移值是300。试该分片第一字节的位置是2400(300\*8)，最后一个字节的位置为2559(2400+200-10\*4-1)。

3. 基于目的地址转发“下一跳方法”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. IEEE 802.3 MAC协议的全称：1-坚持CSMA/CD。它是如何解决冲突的？发前侦听，边发边听，冲突避让。

6. 若某站点经历了11次连续冲突，则该次冲突导致站点在IEEE 802.3、802.3u网络中站点的平均等待时间分别为多少？

(1)11>10,(2^10)/2=512;802.3:512\*51.2μs;(2)802.3u:512\*5.12μs

7. 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。

8. 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\*最远两站点传播时延x2。

9. 假定生成多项式，帧100110101100 的循环冗余码(CRC)为11101。

10. （1）数字签名最常见的构造方法：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）数字签名为什么可以提供发送方身份鉴别、报文完整性、防抵赖的安全服务？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。

11. IEEE 802.3 MAC协议要点：发前监听（CS），边发边听（最小帧长），冲突避让（BEB）。

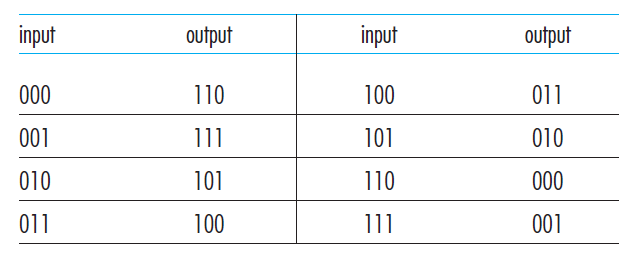
12. 若一无限用户slotted ALOHA信道处于负载不足与过载的临界点，则(1)信道中空闲时槽的比例是多少？ (2)成功发送一个帧发送次数是多少?(1)p0=e-G，G=1≡p0(空闲比例)=36.8% (2)G/S=1/0.368≈2.72(注：S=Ge-G)

13. 多址接入协议划分为信道划分、随机接入、轮流协议。信道划分和轮流协议是无冲突的，随机接入是有冲突的。

14. 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？能收到；会处理；但不会将IP包交给自己的网络层。

15. 描述 的检错能力：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。

16. 为什么以太网交换机能即插即用而路由器不行？交换机：子网的转发表。路由器：全网的转发表。

17. 使用CDMA：A的code={1,-1,-1,1,-1,1}，B的code={1,1,-1,-1,1,1}，假设A传送1，B传送-1。

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 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 | | | | | |

18. Using the following 3-bit block cipher to encrypt a bit string 100100100 (a) without cipher-block chaining (CBC); and (b) with cipher-block chaining (CBC) and IV=111. (a) 011011011 (b) 100 XOR 111 = 011, K(011)=100; 100 XOR 100 = 000, K(000)=110; 100 XOR 110 = 010, K(010) = 101; 100110101。

19. 在下面的空格中填入“谁的什么密钥”：（1）A向B发送一个一次性会话密钥，A用 B的公钥 加密该会话密钥。（2）Certifier.com用 自己的私钥 为foo.com签发公钥证书。（3）A向B发送一个签名的报文，A用 自己的私钥 生成这个数字签名。（4）A向B发送一个可供鉴别的报文，A用 与B共享的密钥 生成报文鉴别码（写出一种方法即可）。

20. 在下面的空格中填入可实现相应安全服务的安全机制：机密性：数据加密；完整性：报文鉴别；防抵赖：数字签名；防假冒：端点鉴别。

21. 在下面的空格中填入需要用到的算法或函数的序号：①对称密钥算法，②公开密钥算法，③散列函数，④密码散列函数。生成数字签名③②数据加密①生成报文鉴别码③① 或 ④ 或 ③②加密会话密钥②

22. 一对主机通过IPSec运行TCP，封装重发的TCP包时，ESP头中的序号不同。 一对主机通过IPSec传输分组流，不用对每个发送的分组都要创建一个新的SA。

|  |  |  |  |
| --- | --- | --- | --- |
| 802.11 | 二面二栏 | hub | 二面一栏 |
| 802.11WEP,802.11i | 二面四栏 | ICMP | 一面二栏中部 |
| 802.3 | 二面一栏 | ICMPv6 | 一面二栏下部 |
| AES | 二面三栏 | IDS | 二面四栏中部 |
| AH | 二面四栏 | IGMP | 一面四栏 |
| ALOHA | 一面五栏 | IGP | 一面三栏中部 |
| ARP | 一面五栏 | IPSec | 二面四栏上部 |
| AS | 一面三栏中部 | LS算法 | 一面三栏上部 |
| CA | 二面三栏 | MAC | 一面五栏 |
| CBC | 二面三栏 | MD5 | 二面三栏 |
| CDMA | 一面五栏 | MOSPF | 一面四栏 |
| CIDR | 一面一栏下部 | NAT | 一面二栏上部 |
| CRC | 一面四栏 | OSPF | 一面三栏中部 |
| CRL | 二面三栏 | PGP | 二面三栏 |
| CSMA、CSMA/CD | 一面五栏 | PIFS | 二面二栏 |
| CSMA/CA | 二面二栏 | PIM | 一面四栏 |
| DES | 二面三栏 | PKI | 二面三栏 |
| DHCP | 一面二栏上部 | RIP | 一面三栏中部 |
| DIFS | 二面二栏 | RSA | 二面三栏 |
| DIX | 二面一栏 | S/MIME | 二面三栏 |
| DVMRP | 一面四栏 | SA | 二面四栏上部 |
| DV算法 | 一面三栏上部 | SHA-1 | 二面三栏 |
| EDE | 二面三栏 | SIFS | 二面二栏 |
| EEE | 二面三栏 | SSL | 二面三栏 |
| EGP、BGP | 一面三栏中部 | TDMA | 一面五栏 |
| EIFS | 二面二栏 | Traceroute | 一面二栏中部 |
| ESP | 二面四栏上部 | VLAN | 二面一栏 |
| FDMA | 一面五栏 | X.509证书 | 二面三栏 |
| HMAC | 二面三栏 |  |  |