*第四章：网络层*

***网络层的作用***即为传输层提供主机到主机的通信服务。每一台主机和路由器都运行网络层协议；发送终端将传输层报文段封装到网络层分组中，发送给边缘路由器（接收端相反）；路由器将分组从输入链路转发到输出链路。网络层的**转发功能**和**路由选择功能**做**重要区分：**转发（路由器根据选定的路由，将分组从输入端口传输到输出端口）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。路由选择（确定去往目的路由器的路由）涉及一个网络的*所有*路由器，它们经路由选择协议共同交互，以决定分组从源到目的地结点所采用的路径。**数据面**：执行数据传输功能；转发属于数据面功能，在路由器内部实施；是路由器本地功能。**控制面**：执行控制数据传输功能；选路属于控制面功能，确定分组如何去往目的节点；是网络范围功能；两种控制面实现方法：传统寻路方法（路由器上实现），软件定义网络（服务器上实现）。**单路由控制平面**：一个路由算法在每个路由器中运行；转发和路由功能在每个路由器内都受到约束。每个路由器都有一个路由组件，它与其他路由器中的路由组件通信，以计算其转发表的值。每个路由器作为一个独立的实体来实现自己的控制和数据平面。**逻辑集中控制平面**：逻辑中央路由控制器计算和分配每个路由器使用的转发表，而每个路由器不计算其转发表，这与每个路由器控件不同。控制平面在中央服务器或多个服务器上实现，数据平面在每个路由器中实现。**网络服务模型：*网络服务模型***定义了分组在发送与接收端系统之间的端到端运输特性。**可能的网络服务**：保证交付，具有时延上界的保证交付，有序分组交付，保证最小带宽，安全性。***因特网的网络层***提供了单一的服务，称为***尽力而为服务***。不同架构的网络提供的网络层服务可能不同，同一个网络也可能提供不同的网络层服务。

***概述：*转发和路由选择：*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，从输入链路接口到输出链路接口转移分组。某些分组交换机称为***链路层交换机***，基于*链路层字段*中的值做转发决定。其他分组交换机称为**路由器**,基于*网络层字段*中的值做转发决定。***路由器工作原理：***路由器两个**主要功能**：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）。***路由器的4个组成部分：*1.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：比特流接收；数据链路层：从比特流中提取帧，处理帧，提取IP数据报；分散式交换：*查表*，每块线卡（line card）上都有转发表的一个镜像，查表仅在本地进行；*排队*，当交换结构阻塞时，分组需在此排队（可能带来队头阻塞和丢包。；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。）；*转发*，通过交换结构将分组发送到输出端口。***输入排队交换机中的线路前部(HOL)阻塞***，即在一个输入队列中排队的分组必须等待通过交换结构发送（即使输出端口是空闲的），因为它被位于线路前部的另一个分组所阻塞。**2.交换结构。**路由器中的互联网络，用于在输入端口、输出端口和选路处理器之间转运分组。***方式：*1.经内存交换：**第一代路由器：由传统计算机构成，选路和交换都由CPU完成，交换通过**拷贝**完成；现代路由器：使用多端口内存连接输入端口和输出端口，控制器在端口之间传输控制消息，如存储地址；交换过程：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，总转发吞吐量是内存写入或读出速率的一半并且不能同时转发两个分组。**2.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。**3.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，多对端口间可以并行传输；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；如果来自两个不同输入端口的两个端口目的地为相同的输出端口，一个分组必须等待。**3.输出端口。**输出端口*存储*从交换结构接收的分组；（网络层）*组装：*若需要，将交换结构输出的信元组装成分组；*排队：*若多个输入端口同时向一个输出端口发送时， 输出端口来不及发送，分组在此排队（输出端口排队是不可避免的！可能带来丢包；增大输出队列可以减少丢包，但会增加内存消耗和增大分组延迟，输出队列并不是越长越好！）；*调度：*若有多个等待队列，选择一个队头分组发送；并通过执行*必要的链路层*（执行链路层协议，封装）*和物理层功能*（将比特流转换为物理信号）在输出链路上传输这些分组。**调度策略：**先到先服务，优先级调度，非抢占式优先级排队：分组一旦开始传输，就不能被中断；轮询调度；加权公平排队。**分组丢弃策略：**弃尾：队列满时，丢弃到达的分组；按照优先级丢弃；随即丢弃：如RED（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AvgLen = (1- Weight)×AvgLen + Weight×SampleLen；当平均队列长度达到第一个阈值$min\_{th}$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$max\_{th}$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.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*（选路），执行网络管理功能。**转发表**：记录分组头中某个字段和路由器输出端口之间的映射关系。一台路由器的输入端口、输出端口和交换结构***共同实现了这种转发功能***，并且***总是用硬件实现。***这些转发功能 有时总称为***路由器转发平面***。这些***路由器控制平面***通常用***软件实现***并在路由选择处理器 （CPU）上执行。

**主机和路由器的网络层功能（因特网的网络层的三个主要组件）**：1、**选路协议**（控制面）：路径选择；RIP,OSPF,BGP。2、**IP协议**（数据面）：编址规则，数据报格式，数据报处理规则。3、**ICMP协议**（控制面）：错误报告，路由器信令。

***网际协议：因特网中的转发和编址：***因特网编址和转发是***网际协议(IP)的重要组件***。**IP只提供最小的传输服务**：**IP提供的服务**：将数据报交付到目的地址和目的协议。尽管IP不提供任何服务承诺，但仍尽最大努力解决分组在网络中传输时可能遇到的一些问题：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）。

**数据报格式：**网络层分组被称为**数据报**。***IPv4数据报中的关键字段如下：•版本号。•报头长度***（4字节为单位，一般的 IP 数据报具有20字节的报头，另外一般TCP报头长度也为20字节。）。***•服务类型。•数据报总长度***（1字节为单位；首部加上数据长度，该字段长16比特，IP数据报的理论最大长度65535字节）。•***标识、标志、片偏移***这三个字段与分片有关。•***寿命(TTL)***用来确保数据报不会永远（如由于长时间的路由选择环路）在网络中循环，每当数据报由一台路由器处理时，该字段的值减 l； TTL字段减为0,该数据报丢弃。***•处理载荷的协议***到达其最终目的地才会有用；指示了数据报的数据部分应交给哪个特定的运输层协议（6$\rightarrow $TCP, 17$\rightarrow $UDP）；类似多路分解。***•首部检验和***：将首部中的每2个字节当作一个数，用对这些数求和（wrapround:溢出部分再次求和），该和的反码（被称为因特网检验和）存放在检验和字段中；路由器要对每个收到的IP数据报计算其首部检验和，不一致则检测出是个差错，一般会丢弃；注意到在每台路由器上必须重新计算检验和并再次存放到原处，因为TTL字段以及可能的选项字段会改变。**为什么TCP/IP在运输层与网络层都执行差错检测：**在IP层只对IP首部计算了检验和，TCP/UDP检验和是对整个TCP/UDP报文段进行的。TCP/UDP与IP不一定都必须属于同一个协议栈；原则上TCP能运行在一个不同的协议（如ATM)上，而IP能够携带不一定要传递给TCP/UDP的数据。***•源和目的IP地址。|\*头部结束\*|•选项。•数据（有效栽荷）***。如果数据报承载一个TCP报文段，则每个（无分片的）数据报共承载了总长40字节的首部(各20字节的IP和TCP首部）以及应用层报文。链路层帧能承载的最大数据字节数称为MTU，不同类型的链路可能具有不同的MTU。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，但仅在目的端系统上而非路由器重组。***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，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（所以所有偏移量计算都为前面相对原始数据长度除8）**，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。***数据报分片的处理过程：***根据报头长度和输出线路的MTU，确定分片的最大数据长度N；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）；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；TTL--。***重组：***将收到的分片重新组装成原始数据报的过程称为重组，重组在目的主机中进行：**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；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；**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。***分片的问题：*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；使得系统更为复杂。**针对分片的DoS攻击：**攻击者发送一系列奇怪的分片，消耗目的主机的资源。***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。数据报在传输过程中可以被多次分片，但仅在目的主机上组装，为什么？传输的时候，网络层设备只需要关注寻路、转发的事情，目的主机上的应用程序才会关注应用层数据，故只在应用层组装。

**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。**单播地址**=类别标识+网络号+主机号。***IP address:***每个网络接口对应一个IP地址，IP地址是一个32位的二进制数，通常用点分十进制数表示。为在因特网范围内保证 IP 地址的全局唯一性；每个接口必须具有唯一的IP地址；建立私有网络的组织可以自己选择网络号，但同样必须保证每个网络号在私有网络内的唯一性。***子网（subnet）：***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=网络号+子网号+主机号，子网地址=网络号+子网号）IP编制为这个子网分配了一个地址x.y.z.m/h，其中/h的记法，又是称为**子网掩码**，指示32bit中最左侧的h bit定义了子网地址。***如何确定子网？***将网络接口与主机/路由器分开，形成一些分离的网络岛，每个网络岛就是一个子网。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，子网之间通信必须通过路由器。***基于类的编址（早期）：***A类8bit（第一位0）子网地址的子网，B类16bit（前两位10），C 类 24bit（110），IP广播地址(255.255.255.255)。**特殊网络地址**：网络号有效，主机号全0：网络本身；网络号有效，主机号全1：这个网络中广播（只做目的地址）；全1：发送节点所在网络中广播（只做目的地址）；全0：本机（只做源地址）；网络号全0，主机号有效：本网中主机；127.xx.yy.zz：回路测试。***分类编址的缺点：***只能按照三种固定的大小分配地址空间，地址浪费严重；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）：***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；允许将若干条转发表项进行聚合，减小转发表规模。***按照实际需要分配地址：***若一个网络需要2000个地址，可为其分配一个具有2048个连续地址的地址块。这些地址的前21位必须相同，从而可将其看成是一个具有21位子网地址的网络。***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（$32-log\_{2}L$）位必须相同。***网络地址的表示方法：***用***掩码***指示网络地址的长度，用***/长度***指示子网地址长度。***机构如何获得网络地址？***机构通常从ISP的地址空间中分配地址。**网络层转发数据报的两种情形*：*直接交付：**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）；**间接交付：**节点将数据包转发给一个路由器去处理。**逐跳转发**：每次只转发到下一跳，下一跳必须是直接可达的（在同一个子网内）。***如何判断使用直接交付还是间接交付？***直接交付：数据包的目的地址与节点的某一端口在同一个子网中；间接交付：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。***间接交付的实现：***节点查找转发表，将数据包发送给下一个路由器。***直接交付的实现：***第五章。***转发表：***记录目的地址到输出端口的映射；取决于目的地址类型的不同，有***三类转发表项***：目的地址是一个***子网地址***，称***地址前缀表项***；目的地址是一个***特定的网络接口地址***，称特定主机表项；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（若无缺省项则发送ICMP错误报告）。***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由。***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）。**IP数据报的转发过程（主机/路由器）：**从数据报中提取目的IP地址D，根据地址类别得到网络地址N：1、 D与自己的任何一个IP地址匹配（本节点是数据报的目的节点），将数据包交给protocol域指定的协议实体处理；2、N与自己的任何一个直连网络的地址匹配（直接交付），通过该直连网络把数据包直接交付到目的节点D；3、表中包含到D的特定主机表项（间接交付），把数据包发送到表中指定的下一跳4、表中包含到N的一个地址前缀表项（间接交付），把数据包发送到表中指定的下一跳5、表中包含一个缺省项（间接交付），把数据包发送到表中指定的默认路由器端口6、宣告选路出错，向数据包的源地址发送一条错误报告消息（ICMP)。***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：这些表项的目的地址可以聚合成一个前缀更短的地址；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**。路由聚合意味着ISP使用单个前缀为多个网络做广播。路由聚合很有用，因为ISP可以使用这种技术向Internet的其他部分宣传ISP拥有的多个网络的单一前缀地址。***若个别表项不满足路由聚合的条件：***仍然可以在转发表中给出一条聚合表项；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。***查找转发表***：***为与某个转发表项 Dest\_addr/prefix\_len 进行匹配运算：***路由器需要先从表项中读出地址掩码（或prefix-len值），计算包的目的地址前缀（用地址掩码和包的目的地址相与），与Dest\_addr的地址前缀（Dest\_addr 与地址掩码相与）进行比较；***引入的问题：***地址前缀的长度prefix\_len可以是任意值，Prefix\_len无法从地址本身得到，只能从转发表项中得到，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）。

**主机/路由器如何获得 IP地址？*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（应用层协议）***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：意味着该协议能够自动配置主机的网络相关方面，以便将主机连接到网络中。）；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。***DHCP为主机发现新IP地址的四个步骤：***主机广播“DHCP discover”报文（src:0.0.0.0,68 \dest:255.255.255.255,67 \yiaddr:0.0.0.0 \transaction ID:654），寻找子网中的DHCP服务器；DHCP服务器用 “DHCP offer”报文（src:223.1.2.5,67\dest:255.255.255.255,68\yiaddrr:223.1.2.4\transaction ID:654 \Lifetime:3600secs ）进行响应，给出推荐的IP地址及租期、其它配置信息；主机用“DHCPrequest”报文（src:0.0.0.0,68 \dest:255.255.255.255,67 \yiaddrr:223.1. 2.4 \transaction ID:655 \Lifetime: 3600 secs）请求IP地址，主机选择一个DHCP服务器，向其请求IP地址(223.1.2.4）；DHCP服务器用“DHCP ack”报文（src:223.1.2.5,67\dest: 255.255.255.255,68 \yiaddrr:223.1.2.4 \transaction ID:655 \Lifetime:3600 secs）发送IP地址，服务器响应客户的请求，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。***DHCP不足之处：***从移动性角度看，结点移动时，不能维持与远 程应用之间的TCP连接。***网络地址转换（NAT）：Motivation:***使用一个公用IP地址支持许多用户同时上网，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），网络内部节点对外是不可见的（安全考虑）。地址空间 10.0.0.0/8 用于家庭网络等专用网络或具有专用地址的***地域***。***NAT实现：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））***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:***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。***使用UPnP实现NAT穿越：***假设主机在端口 3345 上运行一个BT程序：BT 程序请求NAT产生一个“洞”，将<10.0.0.1,3345>映射到 <138.76.29.7,5001>上；BT程序向追踪器通告它在<138.76.29.7,5001>上可用；其它主机通过追踪器可以看到该主机，并能向<138.76.29.7, 5001>发起TCP连接；NAT将 <138.76.29.7,5001>上收到的SYN包转发给主机。***使用中继服务器实现NAT穿越：***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。

**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”；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：***以一个40字节的基本头开始，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：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。***流（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，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。***IPv6包格式：***与IPv4首部相比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：Traffic Class代替Type of Service；载荷长度代替总长度；Next header代替Protocol。***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；为IPv6增加了新的类型，如“分组太大”和“未识别的 IPv6 选项”；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，去掉了一些不必要的查询报文，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。***解决IPv4与IPv6共存：***双协议栈+隧道技术。共存***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。

***路由选择算法：什么是最佳路径：***应用评价：路径长度、数据速率、分组延迟、通信费用、安全性等；ISP 关心：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;路由评价指标通常是矛盾的，需要折衷。***选路算法分类：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：*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(**链路状态广播算法**)；**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（**Dijkstra**）。***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）路由选择算法：*距离矢量算法：***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（迭代、异步地）***求解B-F方程的方法。***算法的基本思想：***节点x测量其到各个邻居v的链路代价c(x,v)；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 Dx=[Dx(y):y∈N]；每个节点周期性地将它的距离矢量Dx发送给邻居；节点x拥有每个邻居v的距离矢量 Dv=[Dv(y):y∈N]；当节点x从各个邻居收到它们的距离矢量后，利用BF方程更新自己的距离矢量：$D\_{x}\left(y\right)\leftarrow min\_{v}c\left(x,v\right)+D\_{v}\left(y\right)$。***节点的本地计算由以下两种事件引起:***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)。节点仅在发现距离矢量dx(y)有变化时通知其邻居。***链路代价变化：好消息传播快，坏消息传播慢***（路由选择环路和无穷计数问题：毒性逆转）。***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。

**层次路由选择：*平面结构的网络不具有扩放性:***路由器数目扩大，路由表规模，信息交换开销；***网络管理员希望对于网络有更多的控制权（管理自治）：***选路算法的选择，隐藏网络内部组织。***自治系统（AS）：***自治系统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（域内） 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；所有AS必须运行相同（域间）Inter-AS选路协议。***Intra-AS和Inter-AS选路协议：***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；InterAS 选路协议:用于在不同的 AS 之间交换选路信息（了解哪些目的网络通过自己可达；将可达性信息传播到该AS内部的所有路由器），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）。***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。***热土豆路由选择：***AS尽可能快地扔掉分组，这通过让路由器向某个网关路由器发送分组来完成，同时该网关路由器在到目的地的路径上的所有网关路由器中有最低的**（源）路由器到网关**的费用。***涉及两个层次的选路：***通过哪个网关路由器到达外网 x（AS 间选路），如何到达该网关路由器（AS 内选路）。***转发表由intra-AS和inter-AS配置：***intra-AS：设置到AS内部网络的路由；inter-AS & Intra-As：设置到外部网络的路由。***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）。**AS-PATH：**包含通告已经通过的AS列表。**NEXT-HOP：**AS-PATH起始的路由器接口的IP地址。

***因特网中的路由选择：***Intra-AS 选路协议也称***内部网关协议IGP***，最常见的有:RIP，较低层ISP和企业网使用；OSPF，较顶层ISP使用。Inter-AS选路协议也称***外部网关协议EGP***，目前只有BGP。***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。**因特网中自治系统内部的路由选择：RIP：**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（RIP响应报文）：***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。每台路由器维护一张称为**路由选择表**的RIP表，包括该路由器的距离向量和该路由器的转发表。***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）。**缺点：**定时更新太频繁；缺少分层，对大规模网络不适用；坏消息传得慢；用跳数表示距离。

**因特网中自治系统内部的路由选择：OSPF：**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***。***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。***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； ***路由器：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。***OSPF的其他优点：***安全（所有OSPF报文都要经过鉴别），可以同时使用多条费用相同的路径（可以按照一定比例将流量分配到不同路径上），对单播和多播路由选择的充分支持。**OSPF的不足：**采用可靠洪泛，开销过大；链路状态多，协议复杂。

**自治系统间的路由选择：BGP：*AS间选路的困难与目标：*** 因特网规模极其庞大且结构非常复杂；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；一个AS可能不信任来自某个AS的选路信息；一个AS可能不愿意为其它AS转发数据包；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：***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***。**交换的主要内容**为：可达性信息，不可达性信息，路径属性。**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。****外部BGP（eBGP）会话:***不同AS的两个边界路由器之间建立的BGP会话。***内部BGP（iBGP）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。***边界路由器的选路表：***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。***以AS枚举形式通报完全路径：***AS2的BGP speaker 通报：128.96, 192.4.153, 192.4.32, 192.4.3 可从<AS2>到达；AS1 的 BGP speaker 收到后通报：128.96, 192.4.153, 192.4.32, 192.4.3 可经路径<AS1, AS2>到达。***BGP进程的处理过程：***入境过滤：输入策略引擎对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）；路径选择：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；出境过滤：输出策略引擎根据出境过滤规则（由管理员定义），决定是否向其邻居AS发布某条路径。

**因特网控制报文协议：**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***：**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。***ICMP与IP的关系：***ICMP是IP层协议，是封装在IP包内传输的，因为可能需要经过多个网络才能到达源节点。报文是作为IP有效载荷承载的，从体系结构上讲它是位于IP之上的；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报文格式：*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。**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。***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：源主机发送Type=8，Code=0的Echo Request报文；若目的主机收到，发送Type=0，Code=0的Echo Response报文；源主机计算RTT，并报告；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）：源主机的Traceroute程序向目的主机发送一个Echo Request 报文（包含­了一个具有不可达端口号的 UDP报文段），IP 报头的TTL设为1；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）；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；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；该过程不断重复，直至收到目的主机的Echo Response报文。***ICMPv6：*差错报告：**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；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：**去掉了一些不必要的查询报文；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。

***链路层：链路、接人网和局域网：***

***网络层和链路层的关系：网络层：选路：***路由器确定去往目的结点的下一跳，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：将数据报从一个结点传输到相邻的下一个结点，***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。***链路层概述：结点：***运行链路层协议的任何设备。***链路：***连接相邻结点的通信信道。***帧：***链路层分组称为***链路层帧***。**链路层提供的服务：组帧（基本服务）：**发送：将数据报封装到帧中（加上帧头和帧尾）；接收：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结点的发送行为；**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结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，避免接收结点缓存溢出（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。**链路层在何处实现：路由器中**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。***链路层由硬件和软件实现：***网卡中的控制器芯片：成帧、链路接入、检错、可靠交付、流量控制等；主机上的链路层软件：与网络层之间的接口，组装链路层寻址信息、激活控制器硬件、响应控制器中断、处理差错条件和将数据报向上传递给网络层。***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。

***差错检测和纠正技术：传输出错的类型：***单比特差错；突发差错：差错以突发的形式聚集在一起。***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。**信道编码检错纠错的一般性原理:**信道编码通过在传输数据中引入冗余来防止数字数据在传输过程中出现过失。**海明距离**：两个码字的对应位取值不同的位数（比如，100和101的海明距离为1）。**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（校验位至少1位不同）；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（差错检测和纠正比特），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，在**突发差错**情况下的检错率为50%。***二维奇偶校验：***可*检测2比特错*和*纠正单比特错*（包括校验位错），有利于检测突发错误。**前向纠错(FEC)：**接收方检测和纠正差错的能力；优点：减少所需的发送方重发的次数，允许在接收方立即纠正差错，避免了不得不等待的往返时延，而这些时延是发送方收到NAK分组并向接收方重传分组所需要的。**因特网检验和(Internet checksum)：**数据的字节作为16比特的整数对待并求和（溢出回卷），这个和的反码形成了携带在报文段首部的因特网检验和；TCP和UDP对所有字段（包括首部和数据字段）计算因特网检验和；优劣：检验和方法需要相对小的分组开销，与CRC相比提供相对弱的差错保护。**循环冗余校验（CRC）：**CRC是一种***多项式编码***，它将一个比特串看成是某个一元多项式的系数。**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。**生成多项式G(x)：**双方确定用来计算R(x)的一个r+1比特多项式。**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T(x) = xr·M(x) + R(x)。**编码方法：*R=D\*2^r/G的余式（减法运算定义为异或操作）***。**检验方法：**若生成的编码除以G的余式为 0，判定传输正确。CRC码检错能力极强，可用硬件实现。是应用最广泛的检错码。CRC举例：取G=1001（或者写为G(X)=X^3+1），对信息比特101110计算CRC码。101110000 ÷ 1001的余式为R=011 (CRC code)，码字：101110011；取G(X) = 1001，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？***1、运输层通常是在主机中作为用户操作系统的一部分用软件实现的。因为运输层差错检测用软件实现，采用简单而快速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。2、由于鸽巢原理，即使通过CRC校验，数据报依然可能损坏，为了确保数据完整性，需要checksum对上层再次确认数据报的完整性（能同时通过CRC检验和checksum检验的错误数据报出现概率小）。

***多路访问链路和协议（链路层协议）：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：**连接了许多结点的单一共享链路，任何一个结点发送的数据可被链路上的其它结点接收到。***冲突（collision）：***在广播链路上，若两个或多个结点同时发送，发送的信号会发生干扰，导致接收失败。***多址接入协议（多路访问协议）：***规定结点共享信道（谁可以发送）的方法，多址接入协议也称***媒体接入控制（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.当只有一个结点发送时，它应能以速率R发送（信道利用率高）2.当有M个结点发送时，每个结点应能以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: 不需要一个特殊的结点来协调发送（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，每个结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，每个结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，有数据的结点轮流发送，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。**一、信道划分协议：*TDMA（时分多址）：***将信道的使用时间划分成帧，每个结点在帧中被分配一个固定长度的***时隙（一个时间N个时隙）***，每个时隙可以发送一个分组，结点只能在分配给自己的时隙内发送，若结点不发送，其时隙轮空。***FDMA（频分多址）：***将信道频谱划分为若干子频带，每个结点被分配一个固定的子频带（**R/N带宽**），若结点不发送，其子频带空闲。***TDM和FDM的优劣：***消除碰撞而且非常公平；结点被限制于R/N bps的平均速率，必须总是等待它在传输序列中的轮次。***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），每个结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：**多个结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允许所有结点同时使用整个信道！**二、随机接入的MAC协议：*随机接入的基本思想：***当结点有数据要发送时，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。***时隙（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；结点只能在时隙开始时发送；结点是时钟同步的（知道时隙何时开始）；所有结点可在时隙结束前检测到是否有冲突发生。**操作：**结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，结点可在下一个时隙发送新的帧；若检测到冲突，结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：** 单个活跃结点可以信道速率连续发送，分布式：结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。**时隙多路访问协议的效率：**当网络中存在大量活跃结点总有帧发送时，长期运行过程中**成功时隙**所占的比例。**时隙Aloha的效率：**假设: 有 N 个活跃结点，每个结点在每个时隙开始时以概率p发送；给定结点在一个时隙中发送成功的概率= p(1-p)^(N-1)；给定时隙中有结点发送成功的概率 = Np(1-p)^(N-1)；最大效率: 找到令 Np(1-p)^(N-1) 最大的概率 p\*；代入Np\*(1-p\*)^(N-1)，并令N趋向于无穷，得到：最大效率 = 1/e = 0.37。***纯ALOHA：基本思想：***取消同步时钟，任何结点有数据发送就可以立即发送，结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）等待一个帧传输时间后再决定。**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。**纯Aloha 的效率：**P(给定结点发送成功)=P(结点发送)\*P(无其它结点在[t0-1,t0]内发送)\*P(无其它结点在[t0, t0+1]内发送)=p(1-p)^(N-1)\*(1-p)^(N-1)=p(1-p)^2(N-1)；求出令结点发送成功概率最大的p\*，并令$N\rightarrow \infty $:最大效率 = 1/(2e) = 0.18。***载波侦听多址接入（CSMA）：两个重要的规则：*** **发送前监听信道（carrier sensing 载波侦听）**，信道空闲发送整个帧，信道忙则等待至少一段时间没有传输再发送（推迟发送）；**碰撞检测**，即当一个传输结点在传输时一直在侦听此信道，如果它检测到另一个结点正在传输干扰帧，它就停止传输，在重复＂侦听－当空闲时传输＂循环之前等待一段随机时间。***冲突仍可能发生：***由于存在端到端信道传播时延，结点可能没有监听到其它结点正在发送；即使忽略传输延迟，当两个（或多个）结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。信道传播时延在决定其性能方面起关键作用。***CSMA/CD (Collision Detection)：*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。**以太网采用CSMA/CD协议：1.**NIC（网卡）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.**中止传输后等待一个随机时间量（**指数回退**）然后返回步骤 2。***我们希望时间间隔应该这样：***当碰撞结点数最较少时，时间间隔较短；当碰撞结点数量较大时，时间间隔较长***。二进制指数后退算法：***当传输一个给定帧时，在该帧经历了一连串的n次碰撞后，结点随机地从 { 0, 1, 2, 3,…, （2^n）-1 } 中选择一个 K 值，对于以太网，一个结点等待的实际时间是 K\*512 比特时间，n能够取的最大值在10 以内。**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。每次适配器准备传输一个新的帧时，它要运行 CSMA/CD 算法，不考虑近期过去的时间内可能已经发生的任何碰撞，因此，当几个其他适配器处于指数后退状态时，有可能一个具有新帧的结点能够立刻插入一次成功的传输。**CSMA/CD效率：**Tprop = 以太网中任意两个结点之间传播延迟的最大值；**Ttrans =** 最长帧的传输时间； **efficiency = 1 / (1 + 5\*Tprop/Ttrans)**。**在以下情况下，以太网的效率趋近于 1**：Tprop 趋近于 0，或 Ttrans 趋向于无穷。**结论：**应控制以太网的规模。**三、轮流MAC 协议：** **ALOHA 和 CSMA 协议具备理想多路访问协议的第一个特性，但不具备第二个特性。*轮询协议（蓝牙）：***结点之一被指定为主结点，主结点以循环的方式轮询每个结点，主结点首先向结点1发送一个报文，告诉它能够传输的帧的最多数量，在结点1传输了某些帧后，主结点告诉结点2它能够传输的帧的最多数量（主结点能够通过观察在信道上是否缺乏信号，来决定一个结点何时完成了帧的发送）。**优劣：**消除了碰撞和空时隙，使得轮询取得高得多的效率；第一个缺点是引入了轮询时延，即通知一个结点“它可以传输”所需的时间，例如，如果只有一个结点是活跃的，那么这个结点将以小于R bps的速率传输，因为每次活跃结点发送了它最多数址的帧时，主结点必须依次轮询每一个非活跃的结点；第二个缺点是单点失效，主节点有故障，整个信道都不可操作。***令牌传递协议（FDDI、IBM令牌环、令牌总线）：***没有主结点，一个称为**令牌(token)**的小的特殊帧在结点之间以某种固定的次序进行交换；当一个结点收到令牌时，仅当它有一些帧要发送时，它才持有这个令牌；否则，它立即向下一个结点转发该令牌；一个结点收到令牌时，若它确实有帧要传输，它发送最大数目的帧数，然后把令牌转发给下一个结点。**优劣：**令牌传递是分散的，并有很高的效率；一个结点的故障可能会使整个信道崩溃（单点失效）；如果一个结点偶然忘记了释放令牌，则必须调用某些恢复步骤使令牌返回到循环中来；令牌传递延迟。***MAC协议比较：*信道划分MAC协议:**重负载下高效：没有冲突，结点公平使用信道；轻负载下低效：即使只有一个活跃结点也只能使用 1/N 的带宽。**随机接入MAC协议：**轻负载时高效：单个活跃结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）。

***交换局域网：局域网LAN（Local Area Network）：***将小范围内的计算机及外设连接起来的网络，范围在几公里以内，通常为个人或机构所有；***城域网MAN：***通常覆盖一个城市的范围（几十公里），要能支持数据、音频和视频在内的综合业务，服务质量好，支持用户数量多；***广域网WAN（Wide Area Network）：***通常覆盖一个国家或一个洲（一百公里以上），规模和容量可任意扩大。

**链路层寻址和ARP：**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、链路层地址或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；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。主机或路由器的**适配器（即网络接口）**具有链路层地址，因此，具有多个网络接口的主机或路由器将具有与之相关联的多个链路层地址；**链路层交换机**并不具有与它们的接口（这些接口是与主机和路由器相连的）相关联的链路层地址，这是因为链路层交换机的任务是在主机与路由器之间承载数据报；交换机透明地执行该项任务，这就是说，主机或路由器不必明确地将帧寻址到其间的交换机。适配器的MAC地址具有**扁平结构（这与层次结构相反）**，而且不论适配器到哪里用都不会变化。***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结点的帧交给主机**：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；而若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。为什么有了MAC地址，还需要IP地址？MAC地址是扁平结构的，无法在因特网范围内快速确定接口的位置；IP地址是有结构的，可以在因特网范围内快速确定网络接口的位置。IP地址与MAC地址没有固定的关联关系：MAC地址与网卡绑定，与节点在哪个子网无关；IP地址与所在子网有关，与网卡没有关系。***如何实现直接交付/将数据报发送到下一跳？？***当发送结点A、接收结点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MAC地址交给适配器；适配器将数据报封装在一个链路层帧中，帧的目的地址=B的MAC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。***发送结点获得接收结点的MAC地址方法：地址解析（Address Resolution）问题：*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，网络层协议）***用于动态获得IP地址-MAC地址映射。***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080016。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请求的结点用目标IP地址与自己的IP地址比较，地址相符的结点进行响应（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；**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：***每个结点在内存中维护一个**地址映射表**；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：每个结点可以收到全部的ARP请求报文，可将发送结点的地址映射缓存到自己的ARP表中；结点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请求的结点将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。**ARP 是即插即用的**，一个ARP表是自动建立的。一个ARP分组封装在链路层帧中，因而在体系结构上位于链路层之上。然而，一个ARP分组具有包含链路层地址的字段，因而可认为是链路层协议，但它也包含网络层地址，因而也可认为是为网络层协议。**最好把 ARP 看成是跨越链路层和网络层边界两边的协议**，即不完全符合我们在第1章中学习的简单的分层协议栈。***数据报到达子网之外：***数据报从A（子网1）经过R（路由器）到达B（子网2）：A知道下一跳地址为111.111.111.110（R-1），R知道B从其端口R-2直接可达；A创建IP数据报，src IP＝A, dest IP＝B；A利用ARP获得下一跳111.111.111.110对应的MAC地址（R-1）（而非获得 B 的MAC）；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。**ARP与DNS的一个重要区别：**DNS为在因特网中任何地方的主机解析主机名，ARP只为在同一个子网上的主机和路由器接口解析IP地址。

**以太网：无连接，不可靠的数据传输。**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；与其它的局域网技术相比，技术简单、成本低；为提高速率，以太网技术不断演化和发展；速率持续提高。**共享式以太网：*1、物理总线拓扑：***总线（1970s中期）：以同轴电缆作为共享传输媒体（总线），所有结点通过特殊接口连接到这条总线上。***2、物理星形拓扑（逻辑总线拓扑）：***集线器（hub，物理层）（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。**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！逻辑星形拓扑：**各结点仅与中心结点（交换机）直接通信，各结点之间不直接通信。***以太网帧结构：（按顺序）*前同步码：**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，不计入以太帧长度。**目的地址（6 字节）+源地址（6 字节）**。 **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，用于多路分解（和网络层数据报中的协议字段、运输层报文段的端口字段类似）。**Data：**46～1500 字节，不足46字节填充至46字节；以太网的最大传输单元(MTU)是1500字节，这意味若如果IP数据报超过了1500字节，则主机必须将该数据报分片；当采用填充时，传递到网络层的数据包括IP数据报和填充部分，网络层使用IP数据报首部中的长度字段来去除填充部分。**CRC（4字节，循环冗余检测）：**对 dest addr.、src addr.、type 和 data 四个字段计算得到CRC码。***数据传输特性：*1、所有的以太网技术都向网络层提供无连接服务**，意味着没有握手。**2、以太网技术都向网络层提供**不可靠服务：接收方网卡不发送确认；接收方网卡丢弃CRC错误的帧；依靠上层协议（TCP或应用）进行错误恢复。***为什么有最小帧长的要求？***为确保结点在发送结束前检测到冲突，帧的发送时间必须足够长：结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2τ，则帧的发送时间不应小于2τ，即帧的最小长度≧链路速率×2τ；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，100Mbps， 1Gbps；物理层编码方式不同。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。**以太网的发展：**10Mbps以太网（早期以太网）：同轴电缆、双绞线、光纤、集线器。100Mbps以太网（快速以太网）：光纤/双绞线，集线器/交换机**。**千兆、万兆以太网：光纤/双绞线，使用交换机，并增加了对流量控制的支持。***讨论：共享式以太网和交换式以太网：*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（结点数量）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**。

**链路层交换机：交换机的任务**是存储（输出接口设有缓存）-转发帧：检查输入帧的MAC地址，有选择地将帧转发到一条或多条输出链路。**交换机特性：1、**交换机自身对子网中的主机和路由器是透明的：交换机没有MAC地址，主机不需要了解有关交换机的任何信息，感觉不到交换机的存在。2、即插即用，自主学习：交换机不需要配置。**1)**交换机表初始为空；**2)**对于在每个接口接收到的每个入帧，该交换机在其表中存储：该帧源地址字段中MAC地址，该帧到达的接口，当前时间。**3)**如果在一段时间（称为老化期）后，交换机没有接收到以该地址作为源地址的帧，就在表中删除这个地址。如果一台PC被另一台PC(具有不同的适配器）代替，原来PC的MAC地址将最终从该交换机表中被清除掉。**3、**交换机也是双工的，这意味着任何交换机接口能够同时发送和接收。**交换机的功能：*过滤***是决定一个帧应该转发到某个接口还是应当将其丢弃的交换机功能。***转发***是决定一个帧应该被导向哪个接口，并把该帧移动到那些接口的交换机功能。交换机的过滤和转发**借助于*交换机表(switch table)*完成**：包含某局域网上某些主机和路由器的但不必是全部的表项，交换机表中的一个**表项**包含：一个MAC地址，通向该MAC地址的交换机接口，表项放置在表中的时间。**帧转发的描述类似于数据转发**，**重要差异**是交换机转发分组基于MAC地址而不是基于IP地址且交换机表与路由器的转发表的构造方式有很大差别。***帧的过滤和转发、自学习过程：***当帧到来时，**1.** 记录帧的到来端口；**2.用帧的目的MAC地址查找端口转发表（转发决策）**：if找到目的MAC地址（已知结点）then { if目的地址所在端口=帧的到来端口 then 丢弃（过滤不需要转发的帧）else 转发帧到表项指定的端口（按转发表转发帧） } else 扩散帧（未知结点，采用扩散法转发）（向输入端口以外的所有端口转发）**3.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，将更多或更大范围内的节点连接到一个网段中（也是自学习）**。*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。**机构网络中三层交换机和路由器的使用：**三层交换机：通常用在机构网络的核心层，连接不同的子网或虚拟局域网（每个虚拟局域网是一个独立的子网）。专业路由器：连接机构网络与外网。**三层交换机转发IP包的过程：**1、用目的IP地址查找缓存（一次精确匹配）：1）若命中，直接用下一跳MAC地址构造链路层帧，发送；2）若未命中，执行后续步骤。2、用目的IP地址查找转发表，获得下一跳IP地址及端口，缓存结果（以目的IP地址为索引，哈希表）。3、利用ARP获得下一跳MAC地址，缓存结果。4、用下一跳MAC地址构造链路层帧，发送。**三层交换机转发速度快的原因：**一次选路，多次转发。***有环网络和生成树算法：*实际的网络是有环网络：**实际网络不采用树状结构（可靠性不高），而是存在冗余链路，即网络中存在环；在有环的网络中扩散帧会造成冗余传输，且不能终止。**解决方法（构造网络的生成树）：**在有环的物理网络上建立一个无环的网络拓扑（生成树），正常情况下只使用无环拓扑转发帧。**IEEE 802.1D标准化了构造生成树的分布式算法：**首先选举具有最小序列号的交换机作为生成树的根；按照根到各个交换机的最短路径构造生成树；只有位于生成树中的交换机可以在属于生成树的边上发送；当有节点或链路发生故障时，重新计算一个无环拓扑。***交换机和路由器比较：***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。3、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。***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器中有大的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径，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（它们以及连接到他们的主机都需要配置IP地址），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IP地址的任何配置就能使流量局部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。**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。广播风暴：广播帧在网络中大量传播，消耗大量资源。***为什么交换机可以即插即用而路由器不行：***因为交换机的转发表范围是子网；而路由器的转发表范围是全部因特网，不能控制规模。

***链路虚拟化：网络作为链路层：多协议标签交换（MPLS）:***是一种分组交换的虚电报网络。***目的：***使用固定长度标签(而不是IP地址)进行高速IP转发。***特点：***使用固定长度标识符(而不是最短前缀匹配) 快速查找；借用虚拟电路(VC)的方法；但IP数据报仍然保持IP地址!***标签交换路由器：***仅根据标签值(不检查IP地址)将报文转发到出接口。***灵活性：***MPLS转发决策可能与IP目的地址和源地址不同，以不同的方式将流路由到相同的目的地；如果链路故障，使用预先计算的**备份路径**快速重新路由流 (对VoIP有用)。**IP路由**:到目的地的路径仅由目的地地址决定。**MPLS路由**:到目的地址的路径可以基于源地址和目的地址。一个MPLS加强的帧只能在两个均为MPLS使能的路由器之间发送。

**回顾：Web页面请求的历程：准备：DHCP、UDP、IP 和以太网。仍在准备： DNS 和 ARP。仍在准备：域内路由选择到 DNS 服务器。Web 客户－服务器交互： TCP 和 HTTP。**

**a day in the life of a web request：**（DHCP）1、笔记本电脑需要获取IP地址、第一跳路由器的IP地址、DNS服务器的IP地址：使用DHCP。DHCP discover被封装在UDP/IP/Ethernet中。2、以太帧在局域网中广播 (dest: FFFFFFFFFFFF)，被运行了DHCP服务器的路由器收到。经过层层解封装，DHCP discover到达DHCP服务器 。3、DHCP服务器构造DHCP offer，包含客户可选择的IP地址、第一跳路由器的IP地址、DNS服务器名字和IP地址。DHCP offer被封装，通过LAN转发 (交换机自学习)，到达笔记本。经过层层解封装，客户收到DHCP offer。4、客户构造DHCP request发送给DHCP服务器。5、DHCP服务器构造DHCP ACK发送给客户。客户现在知道了IP地址、第一跳路由器的IP地址、DNS服务器的IP地址。（DNS+ARP+HTTP（TCP））1、浏览器发送HTTP请求前，需要知道www.google.com对应的IP地址：使用DNS。2、解析器构造DNS查询报文，封装到UDP/IP/Eth中；为发送帧，需要第一跳路由器接口的MAC地址：使用ARP。3、ARP查询报文被广播，到达路由器。4、路由器构造ARP响应报文，通过LAN转发，到达笔记本。客户现在知道了第一跳路由器对应接口的MAC地址。5、携带了DNS查询报文的IP包经交换机转发，到达第一跳路由器。IP数据报从校园网经过一系列转发（利用RIP/OSPF、BGP选路协议建立的路由表），进入 Comcast网络, 到达 DNS服务器。6、DNS查询报文经层层解封装到达DNS服务器程序。7、DNS服务器用（缓存的）www.google.com对应的IP地址进行响应。8、为发送HTTP请求，浏览器首先创建到web服务器的TCP socket。TCP SYN报文段（三次握手过程的第一步）到达web服务器。9、Web服务器用TCP SYNACK （三次握手过程的第2步）进行响应。10、TCP连接建立。11、HTTP request送入TCP套接字。12、携带HTTP请求的IP数据报被路由到www.google.com。13、Web服务器用包含网页的HTTP reply 进行响应。14、包含HTTP reply的IP数据报被路由到浏览器。

*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：*1、无线主机：**运行网络应用，可能静止或移动（无线并不一定意味着移动）。**2、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；通常负责协调与之关联的多个无线主机的传输。**3、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；**自组织模式：**网络中没有基站，结点只能与其通信范围内的结点通信，结点相互帮助转发分组，每个结点既是终端又是路由器。***切换：***无线终端接入到不同基站的过程。***无线网络的分类：*1.单跳有基础设施：**主机连接到基站，基站连接到固定网络(如WiFi，cellular)；**2.多跳有基础设施：**主机通过多个无线结点的中继才能到达固定网络（如无线网状网络）**3.单跳无基础设施：**无基站，不连接到固定网络，结点间通信不需要中继（如蓝牙网络）**4.单跳无基础设施：**无基站，不连接到固定网络，结点间通信需要通过其它结点中继（如自组网，车载网）。

***无线链路和网络特征：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。信噪比(SNR):**更大的信噪比更容易提取出信号。***信噪比与误码率的权衡：*给定物理层:**增加功率->提高信噪比,降低误码率；**给定信噪比:**选择满足误码率要求的物理层，给出最高的吞吐量；**信噪比可随移动性变化:**动态适应物理层(调制技术、速率)***无线网络的特性：*隐藏终端问题：**A和C 正在向B发送；由于信号强度衰减，A和C所处的位置使得他们的信号强度不足以使他们相互检测到对方，但足以在B产生冲突。***CSMA不适合多跳无线网络：***通过载波侦听，发送结点只能知道其周围是否有结点在发送；但真正影响此次通信的是接收结点周围是否有结点在发送。**隐藏结点：**不在发送结点的通信范围内、 但在接收结点通信范围内的活跃结点。（发送结点听不到，但影响接收）**暴露结点：**在发送的通信范围内、但不在接收结点通信范围内的活跃结点。（发送结点能听到，但不影响接收）***CDMA：***所有用户共享相同的频率，但每个用户都有自己的CDMA代码来编码数据；许多个用户“共存”并以最小干扰同时传输(代码是“正交的”)；**编码：**$Z\_{i,m}=d\_{i}\*c\_{m}$**解码：**$D\_{i}=\sum\_{m=1}^{M}Z\_{i,m}\*c\_{m}/M$；

***WIFI：802.11无线LAN：*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 体系结构：*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（中央基站）；每个无线接口（终端及 AP）均有一个全局唯一的MAC地址；注意：AP与路由器相连的有线端口没有MAC地址（AP对于路由器是透明的）。***802.11 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11个信道，监听各个AP发送的**信标帧**（周期性发送，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。***802.11主动/被动扫描：*被动扫描**：主机扫描信道和监听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。

**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；**发送过程中不检测冲突(不采用CSMA/CD原因)**：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（隐藏结点）。因此，一旦开始发送一个帧之后，它就完全的发送该帧。**使用链路层确认：**接收方收到帧后需发送确认帧，以便让发送方知道是否发送成功。***目标：***避免冲突 CSMA/C(ollision)A(voidance)。***802.11的操作模式：*PCF**（Point Coordination Function）**模式**（可选）：该模式只能用于有基础设施（基站）的无线网络，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。**DCF**（Distributed Coordination Function）**模式**：可用于有基础设施和无基础设施的无线网络，所有节点（AP和无线终端）使用CSMA/CA协议竞争信道；支持两种机制：信道预约机制（可选），无信道预约的机制（所有实现必须支持）。**使用信道预约机制的CSMA/CA：**假设A欲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帧的结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。当要发送的数据较少时，一般不使用信道预约机制。***帧间距机制：*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，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，任何节点可以竞争信道。**EIFS：**如果以上间隔都没有发送，收到坏帧或未知帧的节点可以发送一个错误报告帧。***以太网和802.11都使用载波侦听随机接入，但这两MAC协议有重要的区别：***802.11使用碰撞避免而非碰撞检测；由于无线信道相对较高的误比特率，802.11(不同于以太网）使用链路层确认／重传(ARQ)方案。**为什么 802. 11 中使用了确认，而有线以太网中却未使用？**因为无线信道具有高误码率，所以使用需要进行确认，以减少数据链路层的数据损坏；有线以太网误码率很低，故不使用确认机制。**不使用信道预约机制的CSMA/CA：发送方：1.**初始时站点监听到信道空闲，它将在一个分布式帧间间隔（DIFS）的段时间段后发送该帧。**2.**否则，该站点选择一个随机回退值，并在监听信道空闲时递减该值，如果繁忙则冻结计数器。**3.**如果计数器减为0,该站点发送整个帧并等待确认。**4.**如果收到确认，并且想要发送第二个帧，或（给定时间内）没有收到确认，都会回到第二步再次执行，后者会选择更大的随机回退时间。**接收方：**如果成功收到帧，则在短帧间间隔(SIFS)后发送ACK。可见，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。***采用随机时间递减的原因：***尽量避免碰撞冲突，当两个站点同时进入随机回退状态时，时间短的先发送并且阻塞时间长的，有效避免了碰撞。***为什么要用链路层确认：***难以检测碰撞且结点不能中断，接收方只会在没有碰撞时确认帧。***链路层确认可以完全避免碰撞吗：***不能。可能有隐藏结点的问题，两结点可能选择了接近的回退时间。***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，结点侦听到信道空闲时立即发送；在CSMA/CA中，结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：*四个地址字段：***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；Address 4：只在自组织模式中使用***。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。***其他字段duration of reserved transmission time (RTS/CTS)，frame seq # (for reliable ARQ)，frame type (RTS, CTS, ACK, data)***。**802.11 终端在IP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（连接AP1和AP2）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：*结点设置功率管理比特，告知AP它将进入休眠状态：**结点进入休眠，并在下一个信标帧之前醒来；在结点休眠期间，AP缓存发往该结点的帧；AP在发送的信标帧中包含一个移动结点列表，这些结点有帧缓存在AP中；列表中的结点向AP请求帧，其余结点重新进入休眠。

***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，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，因为通信的套接字变了。**归属网络：**移动结点的永久“居所”(e.g.128.119.40/24)**。永久地址：**移动结点在归属网络中的地址，总是可以使用这个地址与移动结点通信，即使移动也保持不变（e.g.,128.119.40.186）。**归属代理：**当移动结点在外地时，为移动结点执行移动管理功能的实体。**|| 外部网络：**移动结点当前所在的网络(e.g. 79.129.13/24)。**外部代理：**外地网络上为移动结点执行移动管理功能的实体。**转交地址：**移动节点在外地网络上的地址，由外部代理分配(e.g.79,129.13.2)。**通信者：**希望与移动结点通信的结点。***1、移动结点注册：***移动结点进入外地网络后，向外地代理注册；移动结点通过外地代理向归属代理注册；**最终结果：**外地代理知道移动结点在本地网络上；归属代理知道移动结点的转交地址，记录到地址绑定表中。***2、间接选路到移动结点：***通信者在数据包中使用移动结点的永久地址；归属代理截获数据包，转发给外地代理；移动结点直接将响应发送给通信者。***间接选路：三角选路问题：***移动结点**使用两个地址**：永久地址——通信者用来向移动结点发送数据报（从而移动结点的位置对于通信者是透明的）；转交地址——归属代理用来向移动结点转发数据报；**三角选路：**通信者-归属网络-移动结点；当通信者和移动结点在同一个网络中时很低效。***间接选路：终端在外地网络间移动：***假设结点移动到另一个网络：向新的外地代理注册；新的外地代理向归属代理注册；归属代理更新移动结点的转交地址；归属代理使用新的转交地址向移动结点转发包；结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！***直接选路到移动结点：***通信者向归属代理请求，并获知移动结点的转交地址（此步以后不必再做）；通信者将包发送给外地代理；外地代理将包转发给移动结点；移动结点直接向通信者发送。***直接选路: comments：***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结点的转交地址，通信者（包括固定结点）需要增加对移动通信的支持。

***Mobile IP（RFC 3344）：*具有许多我们已经看到的特性，如：**归属代理，外地代理，永久地址，转交地址，移动结点注册；**标准化了三个部分：**代理发现，向归属代理注册，数据报间接选路。**1、代理发现：**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；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）；移动结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；如果发现在外地网络上，移动结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。**2、移动主机注册：**移动结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、注册寿命等；外地代理记录结点永久IP地址，向归属代理转发注册请求；归属代理处理注册请求，若认证通过，将移动结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；外地代理收到有效的注册响应后，将移动结点记录在自己的转发表中，向移动结点转发注册响应；当移动结点回到归属网络时，要向归属代理注销。**3、数据报间接选路：**数据包首先被归属代理得到；归属代理查找地址绑定表，获得移动结点当前的转交地址；归属代理将数据包发送到转交地址；外地代理将数据包转发给移动结点。***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结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，以获取与移动结点永久节点对应的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结点直接可达，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，移动结点的永久地址应当映射到归属代理的MAC地址。这一点，有两种方法：***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，刷新其它结点的ARP缓存。 ***数据报如何到达转交地址？*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，目的地址为移动结点的永久地址，而移动结点的转交地址位于外地网络。将目的地址在归属网络的数据报送达外地网络：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）**。***归属代理通过隧道转发数据包：*归属代理向外地代理发送的包：**Src IP = 归属代理 IP，Dst IP = 转交地址（通常是外地代理的IP），里面封装着通信者发送的包（这个包的 dest 是永久地址）；**外地代理向移动结点发送的包：**通信者发送的原始包。***外地代理如何转发数据包到移动结点？***外地代理解封收到的数据包，得到原始数据报；外地代理利用移动结点的MAC 地址，将数据报封装到链路层帧中，发送给移动结点。*外地代理如何获得移动结点的MAC地址？*在移动结点注册阶段，外地代理获知了移动结点的永久地址和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，得到移动结点的MAC地址。***移动结点如何发送数据包？***移动结点将数据包发送给外地代理（缺省路由器）：SrcIP=移动结点永久地址，DestIP=通信者IP地址，SrcMAC=移动结点 MAC， DestMAC=外地代理 MAC；外地代理按照正常方式转发数据包。***移动结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：***误码率高：传输距离、环境干扰、多径传输造成信噪比降低。丢包率高：由于误码、发送冲突造成传输失败。延迟增大：由于冲突重传造成延迟增大。***结点移动带来的问题：***丢包增加：切换（AP切换、交换机更新转发表、移动IP注册）造成丢包。延迟增大：切换及间接选路带来延迟增大。**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。 **避免无线链路降低TCP性能方法：**本地恢复，TCP发送方知晓无线链路；分离连接方法。

***计算机网络中的安全：*网络安全的通用定义：**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***具有下列所需要的***特性：*•机密性：**报文内容的机密性：仅发送方和希望的接收方能够理解报文的内容；通信活动的机密性：通信活动或其特征不被外界察觉。**•报文完整性：**报文来自真实的源，且传输过程中未被修改。**• 端点鉴别：**发送者和接收者能够证实对方的身份；**•运行安全性：**网络不受攻击，网络服务可用。***安全攻击的类型：被动攻击：***试图从系统中获取信息，但不对系统产生影响；**两种类型：偷听：**监听并记录网络中传输的内容；**伪装：**一个实体假冒另一个实体；**重放：**从网络中被动地获取一个数据单元，经过一段时间后重新发送到网络中；**报文修改：**改变报文的部分内容、推迟发送报文或改变报文的发送顺序；**拒绝服务：**阻止通信设施的正常使用或管理。***常见的安全机制：*加密：**使用数学算法对数据进行变换，使其不易理解。**鉴别：**通过报文交换证实一个实体的身份，以防假冒。**报文完整性：**验证一个报文是否可信，包括来源和内容。**数字签名：**附加在一个数据单元后面的数据，用来证明数据单元的来源及完整性，以防伪造及抵赖 。**流量填充：**在数据流间隙中插入比特，以挫败流量分析的企图。**访问控制：**通过授权机制限制用户对资源的访问，防止越权行为。

***密码学的原则（加密）：密钥（key）：***加密和解密时需要使用的参数；***密码分析（cryptanalysis）：***破译密文；***按照加密密钥与解密密钥是否相同，加密算法分为：*对称加密算法：**加密密钥与解密密钥相同，且发送者和接收者；**非对称加密算法：**加密密钥与解密密钥不同。***按照明文被处理的方式，加密算法分为：*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，并生成连续输出的密文流。***密码的安全性：*传统**加密方法的安全性建立在算法保密的基础上，现代加密方法也使用替换和换位两种基本手段，但现代密码学的基本原则是：加密与解密的算法是公开的，只有密钥是需要隐藏的。一个加密算法被称为是***计算安全***的，如果由该算法产生的**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。**对称密钥密码体制：*替换密码：***用密文字母替换明文字母，但字母位置不变；例子：凯撒密码；密钥：字母映射表。***换位密码：***保留明文字母不变，但改变字母的位置；例子：列换位密码。***针对加密系统的密码分析攻击：*唯密文攻击：**密码分析者仅能根据截获的密文进行分析，以得到明文或密钥（对密码分析者最不利的情况）；**已知明文攻击：**密码分析者除了有截获的密文外，还有一些已知的“明文-密文对”来帮助破译密码，以得出密钥；**选择明文攻击：**密码分析者可以选择一定数量的明文，用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。块加密算法：**将k比特的块映射为k比特密文。***DES：***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：***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。**3DES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2^56的攻击量而不是2^112（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。***密码块链接（Cipher Block Chaining）：***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；每一个明文块加密算法：$c\left(i\right)=K\_{s}\left(m\left(i\right)\bigoplus\_{}^{}c\left(i-1\right)\right)$；相同的明文块几乎不可能得到相同的密文块，并且不因引入随机性而产生额外的大量带宽（只额外传送 C0），而后果是需要在协议中提供机制分发初始向量（IV）C0。**公开密钥加密：对称加密算法：**要求发送者和接收者使用同一个密钥；存在密钥传递问题：发送方选择了一个密钥后，如何将密钥安全地传递给接收方？**非对称加密算法：**发送者和接收者不共享密钥，发送者使用加密密钥，接收者使用解密密钥，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。**公开密钥和私有密钥：**公开密钥（K+）：加密密钥，由发送者使用；私有密钥(K-)：解密密钥，由接收者使用。***要求：***KB-(KB+(m)) = m，给定公钥KB+，不可能计算出私钥KB-。***公开密钥算法应满足的条件：***从计算上说，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。***公开密钥算法两个问题：***入侵者知道该公钥和加密算法，可以据此发起选择明文攻击；加密密钥是公开的，任何人都可能向Bob发送一个已加密的报文，在单一共享密钥情况下，发送方知道共享秘密密钥的事实就已经向接收方隐含地证实了发送方的身份，然而在公钥体制中，这点就行不通了，因为任何一个人都可向Bob发送使用Bob的公开可用密钥加密的报文，这就需要用数字签名把发送方和报文绑定起来。***RSA算法：*1.生成密钥：**选择两个大素数ｐ和ｑ（典型值为大于10^100）；计算 n＝p\*q 和 z＝(p-1)\*(q-1)；选择一个与z互质的数，令其为d；找到一个e使满足e\*d＝1 (mod z)；公开密钥为(e, n)，私有密钥为 (d, n)。**2.加密方法：**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；对每个数据块M，计算C＝M^e (mod n)，C 即为M的密文；**3.解密方法：**对每个密文块 C，计算M＝C^d (mod n)，M即为要求的明文。**4.另一个重要的特性：**先用公钥再用私钥和先用私钥再用公钥结果相同。**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。

***报文完整性和数字签名：报文完整性（又称报文鉴别）：***用于验证一个报文是否可信的技术。一个报文是可信的，如果它来自声称的源并且没有被修改。报文鉴别涉及***两个方面***：起源鉴别：报文是否来自声称的源；完整性检查：报文是否被修改过。***方法一：*对整个报文加密：**如果发送方和接收方有一个共享的密钥，可以通过加密报文来提供报文鉴别；缺点：混淆了机密性和报文鉴别两个概念，有时我们只想知道报文是否可信，而报文本身并不需要保密；加密整个报文会带来不必要的计算开销。***方法二：采用报文摘要：*报文摘要（数字指纹）：**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)，这个散列值称为该报文的报文摘要（message digest），也称数字指纹。**使用报文摘要验证报文内容的完整性：**发送者对发送的报文计算一个报文摘要，作为标签和报文一起发给接收者；接收者对收到的报文也计算一个报文摘要，和收到的标签（发送方计算的报文摘要）进行比较。**如何保证报文摘要不被修改？**基于加密算法的报文鉴别（法一）：

发送方计算报文摘要，用与接收方共享的密钥加密报文摘要，形成报文鉴别标签（也称报文鉴别码）

接收方用共享的密钥解密报文鉴别码，得到发送方计算的报文摘要，与自己计算的报文摘要进行比较。缺点：需要使用加密算法。***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。基于哈希运算的报文鉴别（法二）：使用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s（鉴别密钥）添加到报文m之前，然后计算报文摘要H ( s || m )形成**报文鉴别码（MAC）**。之后，发送方生成扩展报文$(m,H(s||m))$，并发送给接收方；接收方收到扩展报文$(m,h)$，可用已知的s，计算出报文鉴别码$H(s||m)$，若$H(s||m)=h$，则正常。***散列函数H应满足的特性：***H能够作用于任意长度的数据块，并生成固定长度的输出；对于任意给定的数据块 x，H(x)很容易计算；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(m+s)=h可以找到一个 x，使得 H(x)=h，那么根据x和m可以推出s；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，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。***散列函数标准：***目前使用最多的两种散列函数：**MD5：**散列码长度为128比特；**SHA-1：**美国联邦政府的标准，散列码长度为 160 比特报文摘要；**HMAC：**可与MD5和SHA-1一起使用。**数字签名：*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。MAC无法胜任这项工作，因为有两个人拥有s。***数字签名：***发送方计算$K-(H(m))$形成数字签名，数字签名附加在报文后面一起发送；接收方用发送方的公钥K+得到原始的报文摘要H(m)，对收到的报文计算摘要，如果两者相符，表明报文是真实的。***数字签名与MAC进行比较：***数字签名和MAC都以一个报文（或一个文档）开始。为了从该报文中生成一个MAC，我们为该报文附加一个鉴别密钥，然后取得该结果的散列；注意到在生成MAC过程中既不涉及公开密钥加密，也不涉及对称密钥加密；为了生成一个数字签名，我们首先取得该报文的散列，然后用我们的私钥加密该散列；因此，数字签名是一种“技术含量更高的”技术，因为它需要一个具有认证中心支撑的公钥基础设施(PKI)。***如何可靠地获取公钥？*** Alice 获取 Bob 主页的请求被 Trudy 截获，Trudy 将假冒的 Bob 主页发送给 Alice，主页中的公钥是 Trudy 的公钥 ET；Alice 使用 Trudy 的公钥加密会话密钥；Trudy 截获会话密钥，用 Bob 的公钥加密后再发送给 Bob；Alice 和 Bob 之间通信的报文都被 Trudy 破译。***认证中心（CA）：***将公钥与特定实体绑定，其职责是使识别合法性证书合法化。***证书***包含主体的公钥和公钥所有者全局唯一的身份标识信息，并由CA进行数字签名（私钥），任何人无法伪造或篡改证书的内容；当一个主体获得其公钥证书后，可将证书放在任何一个可公开访问的地方。**证书的获取：**Bob向CA注册其公钥；Bob向CA提供身份证明 ；CA验证了Bob的身份后创建证书，绑定Bob及其公钥；证书包含Bob的公钥，并有CA的签名。**证书的验证：**当Alice需要Bob的公钥时，获取Bob的证书；使用CA的公钥验证Bob的证书，得到Bob的公钥。**证书的撤销：**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（Certificate Revocation List，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。***证书目录：*证书存放在哪里？**使用DNS作为证书目录；使用专门的目录服务器存放证书。证书撤销列表通常与证书存放在一起，CA定期地将CRL推进目录服务器，由目录服务器负责将CRL中列出的证书清除掉。***X.509证书：***目前最常用的证书标准，建立在公钥算法和数字签名的基础上。***使用一个CA签发全世界所有的证书?***流量压力，单点失效。***由一个组织运行多个CA?*** 密钥泄露，信任问题。***谁可以运行CA？分布式公钥基础设施（Public Key Infrastructure，PKI）：***提供公钥加密和数字签名服务的系统或平台；包含不同组织运行的 CA，每个 CA 拥有自己的私钥，负责为一部分用户签发证书；用户自己决定使用哪一个CA。

***端点鉴别：端点鉴别：***一个实体经过计算机网络向另一个实体证明其身份的过程。鉴别协议通常在两个通信实体运行其他协议之前运行。鉴别协议首先建立相互满意的各方的标识；仅当鉴别完成之后，各方才继续下面的工作。**鉴别协议 ap1.0：**直接发送一个报文。入侵者可伪装成发送者。**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）。**鉴别协议 ap3.0：**Alice 向 Bob 发送秘密口令证明自己，口令是鉴别者和被鉴别者之间共享的秘密。Trudy 窃听到 Alice 发送的明文口令，过后发送给 Bob。**鉴别协议 ap3.1：**Alice 将口令加密，发送给 Bob。Trudy 截获数据包，记录口令加密版本，并向Bob回放（重放攻击）**鉴别协议 ap4.0：*目标：***避免回放攻击。***不重数(nonce)：***在一个协议的生存期中只使用一次的数。***协议ap4.0以如下方式使用一个不重数：*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。***失败的情况是因为***Bob不能区分Alice的初始鉴别报文和后来入侵者回放的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。**缺点：**需要一个共享的对称密钥。**鉴别协议 ap5.0：采用公开密钥算法加密不重数：**“I am Alice”→R→KA-(R)→“send me your public key”→KA+。**Bob计算： KA+(KA-(R)) = R**，只有Alice拥有这个私钥，因而一定是 Alice！**X.509提供的单向鉴别服务：单向鉴别：**涉及发送方到接收方的一次报文传输。**A→B：tA ||rA|| IDB || Data || Kb+(Ka-b) || signatureA** 。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。

***为什么要在因特网的多个层次上提供安全性功能呢？仅在网络层提供安全性功能并加以实施还不足够吗？***首先，尽管可以通过加密数据报中的所有数据（即所有的运输层报文段），以及通过鉴别所有数据报的源 IP 地址，在网络层能够提供“地毯式覆盖“安全性，但是却并不能提供用户级的安全性。例如，一个商业站点不能依赖IP层安全性来鉴别一个在该站点购买商品的顾客。第二，在协议栈的较高层上部署新的因特网服务（包括安全性服务）通常较为容易，而等待在网络层上广泛地部署安全性，可能还需要未来若干年才能解决。**安全电子邮件：**电子邮件安全包括真实性和机密性两个方面。 **PGP:** 一个开放源码的安全电子邮件软件包，提供对邮件的保密、鉴别、数字签名和压缩服务，PGP较多地用于个人电子邮件安全（因特网安全电子邮件的事实标准）。**PGP提供五种服务**：鉴别，机密性，压缩，兼容电子邮件，分段。**鉴别：**PGP使用基于公开密钥算法的数字签名提供鉴别服务。生成可供鉴别的电子邮件：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。**机密性服务：**PGP使用对称密钥算法保护邮件的机密性：发送方将选择的一次性会话密钥用接收方的公钥加密，与报文一起发送给接收方。仅使用机密性服务的过程：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(Data)。**压缩服务：**缺省地，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))。在加密报文之前进行压缩，一方面可以减少要加密的数据量，另一方面压缩后的消息冗余很少，增加密码分析的困难。**兼容电子邮件服务：**PGP使用Base64编码将二进制数据流转换成简单ASCII文本，以解决邮件的传输问题。**同时使用以上四种服务的过程：**发送方先对明文报文计算签名，将签名放在报文前面；签名与明文一起被压缩；用会话密钥对压缩后的数据块进行加密；用接收方的公钥加密会话密钥，放在报文的前面；将整个数据块转换成Base64编码格式：EncodeBase64(KB+(KA-B) || KA-B (Zip (Sgn || Data)))。**邮件分段服务：**PGP在完成对报文的全部处理后，自动将超过长度的报文分成小块传输，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。

***使TCP连接安全SSL/TSL：*向基于TCP的网络应用**提供**安全的传输层**服务：如支持Web浏览器和服务器之间的安全通信（https）。***安全服务:*** 服务器鉴别，数据加密，数据完整性，客户鉴别（可选）。**SSL建立在TCP之上，依靠TCP提供可靠的端到端连接。**SSL是***涉及到两个层次的一组协议：***SSL 记录协议（TCP之上，HTTP层之下）：为各种高层协议（如HTTP）提供基本的安全服务；其它三个高层协议（与HTTP同层）：用于SSL交换管理。**宏观描述：*1.握手：***允许服务器和客户之间相互鉴别，并协商加密算法、MAC算法及密钥等。**过程：**SSL version,preference,Ra(A)-> SSL version,preference,Rb(B)->X.509 certificate chain(B)->server done(B)->Eb(用B的公式加密后的预密钥)(A)->发送所有握手报文的MAC(A)->finish(A)-发送所有握手报文的MAC(B)->finish(B)**。更完整描述：握手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支持的加密算法和客户的不重数；服务器从浏览器选择一种对称算法、一种公钥算法和一种MAC算法，它把他的选择以及证书与服务器选择的不重数一起发送给浏览器；客户验证签发证书的CA是否在客户的可信CA列表中，若不在则警告该问题； 如果在则使用该CA的公钥验证证书，提取服务器公钥，生成一个前主密钥（PMS），用服务器的公钥加密该PMS，并将加密的PMS发送给服务器；客户和服务器各自从PMS和不重数中计算主密钥，并进行密钥导出（如果选择CBC，服务器以明文向客户发送IV（两个））；客户发送所有握手报文的一个MAC，服务器发送所有握手报文的MAC（防止握手被篡改）。***2.密钥导出：*两者都生成四个密钥：**Ec,用于客到服的加密；Mc,用于客到服的MAC密钥；Es、Ms，服到客；***3.数据传输：***将数据流分割成为**记录**，对每个记录附加一个MAC用于完整性检查，将“记录+MAC”加密传给服务器。这里的MAC=记录+密钥+TCP序号的散列(防止重排序或重放报文段的攻击)。***4.SSL记录：*提供服务：**机密性：通过加密SSL载荷实现;完整性：通过报文鉴别码保护。**操作过程：**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2^14字节的数据块；（可选）对数据块进行压缩；对数据块生成基于哈希运算的报文鉴别码；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；在处理完的数据块前加上SSL头，包括内容类型、SSL版本号、压缩数据块的长度等。没有字段用于序号（采用隐式序号）。***连接关闭：***SSL类型段中指出该记录是否是用于终止该SSL会话的。***网络层安全性：IPsec和虚拟专用网：IPv4在设计时没有考虑安全性：***缺少对通信双方身份的鉴别，容易遭受地址欺骗攻击；缺少对网络中数据的完整性和机密性的保护，数据很容易被窃听、修改甚至劫持。***IP安全协议（IPSec）：***IETF以RFC形式公布的一组安全协议集；目标是把安全特征集成到IP层，以便对因特网中的安全业务提供低层的支持。***专用网：***通过电信专线将分散在各地的计算机（网络）连接而成的网络；安全性好，但代价高。***虚拟专用网（Virtual Private Network）：***建立在公用网上的一个覆盖网络，在逻辑上与其它流量隔离；数据在发送到公用网之前进行加密。***VPN的实现：***­**VPN的典型结构：**在每个局域网上设置一个安全网关，在每一对安全网关间创建一条穿过因特网的隧道，在隧道中使用IPSec；**VPN的优点：**可以在一对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。传进公用网的 IPsec 被 IPv4 封装，同时拥有 IPv4 和 IPsec 首部。***IPSec提供了一个安全体系框架：*IPSec提供了一个用于集成多种安全服务、加密算法及安全控制粒度的安全体系框架：**IPSec提供的安全服务包括：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；IPSec提供多种安全控制粒度，包括：一条TCP连接上的通信，一对主机间的通信，一对安全网关之间的所有通信。用户可以为数据通信选择合适的安全服务、算法、协议和控制粒度。***IPSec主要包括两个部分：*IPSec 安全协议：**包括鉴别首部协议AH（不提供机密性）和 封装安全性载荷ESP两个安全协议，定义了用于安全通信的IP扩展头和字段，以提供机密性、完整性和源鉴别服务；**密钥管理协议：**定义了通信实体间进行身份鉴别、协商加密算法以及生成共享会话密钥的方法。将以上两部分绑定在一起的是称为安全关联（SA）的抽象。**安全关联（SA） 是两个通信端点间的一个单工连接**，由一个安全参数索引（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；SA是通信对等实体之间对某些要素的协定，如使用的安全协议、协议的操作模式、使用的密码算法、密钥及密钥的生存期等； 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间、一台主机与一个安全网关之间、或一对安全网关之间。***IPSec的使用模式：*运输模式：**IPSec 头被插入到原始IP头和传输层头之间，路由器根据原始IP头转发数据包；**隧道模式：**原始数据包被封装在一个新的IP包中，IPSec头被放在新的IP头和原始IP头之间，路由器根据外层IP头（通常是新IP头）的信息转发数据包。隧道的端点（外层IP头中的地址）通常是一个支持IPSec的安全网关。***两种模式的比较：***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。***鉴别头部（Authentication Header）协议：***AH协议提供无连接完整性、数据起源认证和抗重放攻击，但不提供机密性服务：HMAC 覆盖数据包的载荷部分，因而可提供无连接完整性服务；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；AH 头中有序号，且被 HMAC 覆盖，因而可抵抗重放攻击。***封装安全载荷（Encapsulating Security Payload）：*ESP 数据包(载荷)大致分为以下几个部分：ESP 头：**包含 SPI 和序号，SeqNum：对SA上发送的数据包进行编号，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2^32之前，必须协商一个新的SA和新的密钥；**载荷：**原始数据包中被加密部分的密文（初始IP首部、初始载荷）；**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；**ESPMAC：**覆盖 ESP 头、载荷和 ESP 尾的报文鉴别码。**SPI：**32比特的数，和目的IP地址、安全协议结合起来，唯一标识数据报的SA。**SeqNum：**对SA上发送的数据包进行编号，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。***传输模式下普通IPv4转换为IPSec：***在原始IPv4数据报载荷后面附上“ESP尾部”字段；使用算法和SA规定的密钥加密”载荷+ESP尾“部分；在这个加密量的前面附加上一个称为"ESP 首部”的字段；使用算法和由SA规定的密钥生成一个覆盖ESP首到尾的鉴别MAC；将附加到ESP尾的后面形成载荷；原始IP头添加到ESP头前。***隧道模式路由使用下列方法将这个“普通IPv4数据报”转换成一个IPsec数据报：***在初始IPv4数据报（它包括初始首部字段！）后面附上"ESP尾部”字段；使用算法和SA规定的密钥加密该结果；在这个加密量的前面附加上一个称为"ESP 首部”的字段；得到的包称为"enchilada"；使用算法和由SA规定的密钥生成一个覆盖整个enchilada的鉴别MAC；该MAC附加到enchilada的后面形成载荷；最后，生成一个具有所有经典IPv4首部字段（通常共20字节长）的全新IP首部，该新首部附加到载荷之前。（运输模式在第一部分缺少了初始IP首部）。***ESP协议提供的安全服务：***ESP协议提供数据机密性、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：原始数据包的载荷部分被加密，因而可提供数据机密性；HMAC 覆盖数据包载荷部分，可提供无连接完整性服务；ESP头中有序号，且被HMAC覆盖，可抵抗重放攻击；ESP隧道模式中，原始IP头也被HMAC覆盖，因而ESP隧道模式可提供数据起源鉴别；ESP隧道模式中，原始IP头也被加密，路由器只能看到外层IP头，因而ESP隧道模式可提供数据流机密性服务（ESP隧道模式的安全性强于ESP传输模式）。***AH协议和ESP协议的安全性比较：***数据机密性服务：只有ESP提供，AH不提供；鉴别服务：ESP隧道模式的鉴别服务，安全性强于AH，ESP传输模式的鉴别服务，安全性不如AH；数据完整性服务：两者都提供。

***使无线LAN安全：802.11 WEP（Wired Equivalent Privacy有线等效保密）：***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。***WEP数据加密：***主机与接入点共享一个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{kiIV | i=1,2,…}；第 i 个密钥 kiIV 用来加密帧中的第i个字节di：ci = di XOR kiIV；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 = ci XOR kiIV。***WEP加密的安全漏洞：***每个KS只有224个 (KS, IV) 可用：IV 会被重复使用；IV 用明文传输：攻击者可以观察到 IV 的重用。**攻击：** Trudy（可能通过欺骗方式）让Alice加密他选择的明文(d1 d2 d3 d4 … )；Trudy 能够获得 Alice 加密的密文: ci = di XOR kiIV；Trudy 知道 ci 和 di, 就可以计算出kiIV： di XOR ci = kiIV；Trudy 得到了加密所用的密钥流 k1IV k2IV k3IV……；当过后观察到 IV 被重用时， Trudy 就可以破解密文了！***802.11i增强的安全性：***可以使用各种（较强的）加密算法； 提供了密钥分发机制；使用专门的鉴别服务器（而不是接入点）来提供鉴别服务。***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。**有线等效保密：*主机鉴别过程：***无线主机向接入点请求鉴别；接入点向主机发送一个128比特的不重数；无线主机使用接入点共享的对称密钥加密不重数，发送给接入点；接入点解密不重数，若与接入点发送给主机的不重数相同，完成主机鉴别。利用主机与基站共享密钥这个事实鉴别主机。***802.11i的操作：*1) 安全能力发现。**在发现阶段，接入点（AP）通告它的存在以及它能够向无线客户结点提供的鉴别和加密形式，客户则请求它希望的特定鉴别和加密形式。**2)客户和鉴别服务器相互鉴别和主密钥(MK)生成。** 鉴别发生在无线客户和鉴别服务器（AS）之间。在这个阶段，接入点基本是起中继的作用，在客户和鉴别服务器之间转发报文。**3)成对主密钥(PMK) 生成。**MK是一个仅为客户和鉴别服务器所知的共享密钥，它们都使用 MK 来生成一个次密钥，即成对主密钥(PMK)。鉴别服务器则向接入点发送该PMK。客户和接入点现在具有一个共享的密钥。 **4)临时密钥(TK) 生成。**使用PMK, 无线客户和接入点现在能够生成附加的、将用于通信的密钥。其中的关键是临时密钥，TK 将被用于执行经无线链路向任意远程主机发送数据的链路级的加密。

***运行安全性：防火墙和入侵检测系统：*** **防火墙：**在可信的内部网络与不可信的外部网络之间执行访问控制策略的硬件或软件系统（硬软结合体）；**目的是**保护内部网络免受来自外部网络的攻击。***防火墙的类型：***包过滤防火墙/传统分组过滤器，状态检测防火墙/状态过滤器，应用网关。***包过滤防火墙：***内部网络通过有包过滤功能的路由器（每个接口能够具有自己的访问控制表）连接到因特网上；路由器对数据包进行逐包过滤，基于以下字段决定转发包还是丢弃包：源IP地址，目的IP地址；TCP/UDP源端口号、目的端口号；ICMP报文类型；TCP SYN标志和 ACK 标志。***包过滤策略的例子：***不允许访问外部Web网站→丢弃所有外出的、目的端口为80的包；不允许外部发起的TCP连接，除非访问的是内网的公共web服务器→丢弃进入的TCP SYN包，除非去往130.207.244.203的端口80；防止因特网广播吞噬网络带宽→除DNS包和路由器广播包，丢弃其它进入UDP包；防止网络拓扑被探测（traceroute）/防止网络被跟踪路由→丢弃所有外出的ICMP TTL expired包；阻止外部客户发起到内部服务器的连接→过滤进入的所有ACK比特设为0的报文段，这个策略去除了所有从外部发起的所有TCP连接，但是允许内部发起TCP 连接；防止Web无线电占据可用带宽→丢弃除DNS外所有UDP分组；防止网络被用于smurf Dos攻击→丢弃所有去往某广播地址的ICMP ping分组。***访问控制列表（ACL）：***访问控制列表是一个规则表，包含一系列（动作，匹配条件）；对于每个进出的包，从上到下地匹配规则。***包过滤防火墙孤立地过滤每个包，仍会允许一些异常的包进入：***例如，允许 dest port = 80, ACK=1 的包进入，哪怕并没有相应的连接存在。***状态检测防火墙***可以跟踪 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；扩展 ACL，指示在允许放行一个包前需检查连接的状态。***应用网关：***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。为什么应用程序网关必须与分组过滤器协同工作才能有效？如果没有数据包筛选器。则机构网络内的用户仍将能够直接连接到机构网络外的主机。该筛选器强制用户首先连接到应用程序网关。**例如:** 允许特定的内部用户使用 telnet登录外部主机；所有telnet用户必须连接到应用网关；对于授权用户，应用网关建立与目的主机的telnet会话，并在2个连接之间中继数据；包过滤防火墙**阻塞所有**不源自应用网关的 telnet连接。***防火墙的局限性：***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。**入侵检测系统（IDS）：**由于防火墙的局限性和防火墙不检查数据包之间的**关联**。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。**网络中可以设置多个IDS:** 在不同位置进行不同类型的检查。***为什么使用多个IDS传感器？***IDS 不仅需要做深度分组检查，而且必须要将每个过往的分组与数以万计的“ 特征(signature)"进行比较；这可能导致极大的处理量；将IDS传感器进一步向下游放置，每个传感器仅看到该机构流量的一部分，维护能够更容易。***基于特征的IDS的一些限制：***它们要求根据以前的攻击知识来产生一个准确的特征，换言之，对不得不记录的新攻击完全缺乏判断力；另一个缺点是，即使与一个特征匹配，它也可能不是一个攻击的结果，因此产生了一个虚假告警；最后，因为每个分组必须与范围广泛的特征集合相比较，IDS可能处于处理过载状态并因此难以检测出许多恶意分组。**基于异常的IDS最大的特点**是它们不依赖现有攻占的以前知识；在另一方面，区分正常流量和统计异常流量是一个极具挑战性的问题。**IPS：**滤除可疑流量的设备。属于IDS系统。