网络层的功能：转发（路由器本地）、路由选择(网络范围),连接建立

发送主机的网络层能提供的服务：确保交付、具有时延上界的确保交付、有序分组交付、确保最小带宽、确保最大时延抖动、安全性服务

因特网网络层提供的服务：尽力而为

虚电路网络=源到目的的路径+每段链路的 VC 号+每台路由器转发表表项

虚电路建立的三个阶段：①信令报文建立虚电路（决定 VC 号，增加表项）②数据传送③信令报文拆除虚电路

虚电路与运输层区别：运输层连接建立仅涉及两个端系统，两个端系统独自决定运输层连接参数，路由器不知情连接；虚电路沿着两个端系统之间路径上的路由器都要参与虚电路的建立，且每台路由器都完全知道经过它的所有虚电路。

数据报网络：每个路由器利用目的端系统地址进行转发。

转发表：**目的地址前缀**(prefix)到**链路接口**的映射,1-5min

最长前缀匹配规则：选择与目的地址匹配的最长匹配项。

网络层和运输层的无连接服务和有连接服务的区别

1.网络层:向运输层,主机之间;运输层:向应用层,进程之间 2.网络层不同时提供连接服务的虚电路网络和无连接服务的数据报网络，不同计算机的网络不同。3. 运输层面向连接的服务只在端系统中提供，网络层提供的连接服务也在位于网络核心的路由器中实现

路由器=输入端口（链路层功能+查询转发表决定路由器输出端口+检查分组的版本号等）+交换结构（内存交换/总线交换/互联网络交换（可同时））+输出端口+路由选择处理器

输出端口排队：若输出端口的缓存大小不够，丢包策略：1 丢弃到达的分组（drop-tail）2 删除一个或多个已经排队的分组；缓存大小 B 的设置：B=RTT*C(RTT 为平均往返时延，C 为链路容量)；若有大量的 TCP 流（N）流过一条链路：B=RTT*C/\sqrt{N}(N 通常非常大)。

随机早期检测 RED：一种 AQM 算法：为输出队列长度维护一个加权平均值，当一个分组到达时：如果平均队列长度小于最小阈值 min_{th}，将该分组加入队列；如果平均队列长度大于最大阈值 max_{th}，将该分组标记或丢弃；否则在两者之间，则分组以某种概率被标记或丢弃

因特网网络层=IP 协议+路由选择部分+差错报告和请求响应措施

IPv4 数据报：版本（规定 IP 协议版本），首部长度（标记数据部分从哪里开始，一般为 20 字节）服务类型 TOS（区分 IP 数据类型）数据报长度（=首部+数据，单位字节，最长为 65535 字节）标识、标志、片偏移（与 IP 分片有关）寿命 TTL（每当数据报由一台路由器处理，TTL-1）协议（指示目的端系统数据部分应交给那个运输层协议（6 给 TCP，17 给 UDP））首部检验和（帮助路由器检测 IP 数据报中的比特错误；若路由器计算后不同，会丢弃该数据报；首部中的每 2 个字节当做一个数，用反码运算对他们求和，求和后的反码为检验和）源和目的 IP 地址、选项（允许 IP 首部被扩展（IPv6 以去掉））数据（有效载荷）（TCP/UDP 报文段/ICMP 报文段）

为什么 TCP/IP 在运输层和网络层都执行差错检测?

IP 层只对 IP 首部计算了检验和，而 TCP/UDP 检验和是对整个 TCP/UDP 报文段进行的；TCP/UDP 与 IP 不一定属于一个协议栈，TCP 还可以运行在一个不同的协议上（ATM），而 IP 也可能携带不是 TCP/UDP 的数据。

IP 数据报为什么分片？在发送方与目的地路径上的每段链路可能使用不同的链路层协议，每种协议可能具有不同的 MTU **如何分片？**路由器 1.更改**标志**，最后一个片的标志比特是 0，其他所有片的标志比特被设为 1；2. 更改**偏移字段**，偏移字段指定该片应放在初始 IP 数据报的哪个位置（偏移字段的值会被乘 8 之后再被用来确定真正的偏移量）

如何组装？目的端系统收到了数据报时，它需要判断：此数据报是不是别的数据报的片？如果是，确定何时收到了最后一片，通过发送主机 IP 地址和标识号（发送主机为为数据报贴上唯一标识号）将这些收到的片拼接到一起；当且仅当一个数据报的有效载荷在 IP 层已被完全重构，才会被传递给目的地运输层，否则会被丢弃。

分片的坏处？1.使路由器和端系统更为复杂 2.分片可能被用于生成致命的 DoS 攻击：攻击者发送了一系列古怪的、无法预计的片；攻击者发送交迭的 IP 片

IP 地址：**32bits**（约有 40 亿个 IP 地址）每一个**接口**都有一个 IP 地址

重要观察：子网之内通信不需要经过路由器，子网之间通信需要经过路由器；路由器**每个端口连接一个子网**。

无类别域间路由选择 CIDR：IP 地址=a.b.c.d/x，前缀：x 最高比特构成的 IP 地址的网络部分，剩余 32-x 比特用于区分该组织内部设备，**一个组织通常被分配一块连续的地址，即具有相同前缀的一段地址**。

分类编址（CDIR 之前的做法）：具有 8、16、24 比特的 IP 地址的网络部分被称为 A、B、C 类网络。一个子网只能是这三类中的一类。问题：C 类子网只有 254 台主机（2 个用于特殊用途）B 类子网有 65534 主机

广播地址：255.255.255.255。当一台主机中发出一个目的地址为广播地址的数据报时，该报文会给同一个网络中的所有主机。

组织如何获得自己的地址：从 ISP 获取，ISP 将自己获得的地址块平均分成八块，分别给 8 个组织；IP 地址由 ICANN 管理（它还管 DNS 根服务器、分配域名和解决域名纷争）

主机如何获取自己的地址：**动态主机配置协议 DHCP**：DHCP 允许主机自动获取一个 IP 地址，网络管理员能够配置 DHCP，以使某给定主机每次与网络连接时能够得到一个相同的 IP 地址，或者某主机将被分配一个临时的 IP 地址；DHCP 还允许主机得知**子网掩码、第一跳路由器地址、本地 DNS 服务器地址**。DHCP 是**客户-服务器协议**。新客户接入网络时，DHCP 给它分配一个 IP 地址，客户退出网络时，DHCP 将它的 IP 地址回收。**所以一个采用 DHCP 的组织需要的 IP 地址数量是最多同时在线人数**。每个组织有一个 **DHCP 服务器**，或者 **DHCP 中继代理**。

获取一个 IP 地址的步骤：**1.DHCP 服务器发现**：新到的主机利用 **DHCP 发现报文**获取 DHCP 服务器；发现报文的源地址是 0.0.0.0，表示**本机**；目的地址是 255.255.255.255，即**广播**给所有子网内的主机；**发到 67 端口，是 UDP 报文** **2. DHCP 服务器提供**：DHCP 服务器收到发现报文，以提供报文作为相应 DHCP 服务器也发送一个广播报文，包含收到的**发现报文的事物 ID、向客户推荐的 IP 地址、网络掩码、IP 地址租用期**（若组织中有多台 DHCP 服务器，每一台都会相应，这时就要由客户机去选择一个作为自己的 IP 地址）**3. DHCP 请求**：新到达的客户从一个或多个服务器提供中选择一个，并向选中的服务器提供一个 DHCP 请求报文进行相应，回显配置参数 **4. DHCP ACK**：服务器用 DHCP ACK 报文对 DHCP 请求报文进行相应，证实所要求的参数

DHCP 不足之处：每当结点连接到一个新子网时，要从 DHCP 得到一个新的 IP 地址，当结点在移动式，无法维持 TCP 连接。

NAT 转换表打包和解析过程：1.主机向 NAT-DHCP 发送了一个数据报，源 IP 地址是路由器给主机分配的地址，端口号是主机的端口号。路由器将数据报的源地址改成自己的 IP 地址，端口号新分配一个替换进去，然后再 NAT 表中加入**目的 IP 地址，目的端口号**到**主机 IP 地址，主机端口号**的映射 2.当数据报被发回时，路由器将收到的数据报的**源 IP 地址，源端口号**作为查询依据，得到**主机 IP 地址，主机端口号**，再发送给该主机。由于端口号字段是 16bits，NAT 可支持超过 60000 台主机

NAT 的缺陷：1.端口号不能用于主机编址 2.路由器通常仅应当处理高达第三层的分组 3.NAT 协议违反了端到端原则（主机彼此直接对话），路由器不应修改 IP 地址和端口号 4.应使用 IPv6 解决 IP 地址短缺的问题 5.妨碍 P2P 应用程序，比如 P2P 文件共享应用、P2PIP 语音应用

ICMP 协议：因特网控制报文协议（网络层第三个组件）：ICMP 被主机和路由器用来彼此沟通网络层的信息；ICMP 最典型的用途：**差错报告**；ICMP 报文作为 IP 的有效载荷。若主机收到一个指明上层协议为 ICMP 的 IP 数据报,它分解出该数据报内容给 ICMP,就像给 TCP 和 UDP 一样。

IPv6 数据报格式：<变化>：**扩大的地址容量**：源和目的地址都变成了 128 比特**引入任播地址**：可将数据报交付给一组主机的任何一个 **40 字节首部**（简化高效）**流标签与优先级**：**流**：要求进行特殊处理的一系列报文之一，比如音视频、高优先级用户承载的流量；**流量类型**：给出流中某些数据报的优先级，以便指明某些数据报比其他应用数据报有更高的优先权；<不存在的字段>：**分片/重新组装**，IPv6 不允许路由器分片与重组，只能在源、目的地上执行，若数据报太大不能发送，路由器只能扔掉 **首部检验和**，运输层和数据链路层已经执行了检验操作，所以网络层无需再检验（检验耗时太长）**选项**

链路状态算法(LS)：获取网络拓扑和所有链路费用的方法：让每个节点向网络中所有其他节点广播链路状态分组，包括链路的特征和费用，经常由**链路状态广播算法**来完成。这会使所有结点具有了该网络的等同的、完整的视图。获取全局视图后，用 **Dijkstra 算法**计算最好路径。O(n^2)

分散式路由选择算法：**分布式的**（每个结点从直接相连的邻居接收信息，执行计算，然后把结果返还给邻居），**是迭代的**（此过程一直要持续到邻居之间无更多信息要交换为止。）**是异步的**（不要求所有结点步伐一致地操作。）**是自我终止的**（没有计算停止的信号，算法就停止了。）

距离向量算法(DV)：$$d_x(y) = min_v\{c(x,v) + d_v(y)\}$$

算法过程：1. 每个路由器先初始化自己的距离向量，然后发送给自己的所有邻点。2. 每个路由器接收到邻点发送的他们的距离向量，更新自己的距离向量。3. 若自己的距离向量有所改变，将自己的距离向量再发送给自己所有的邻点。4. 重复 2-3，直到所有路由器的距离向量都不再变动。**链路费用改变**：某一链路费用减少的好消息传播很快；某一链路费用增加（无穷计数问题）的坏消息传播很慢

LS 与 DV 算法比较：1.报文复杂性：LS:LS 要发送 O(|N||E|)个报文；某一链路费用变动时，需要向其他所有结点发送数据 2.收敛速度：LS：O(|N|²)的算法 DV：收敛很慢，有可能遇到无穷奇数问题 3.健壮性：LS：路由计算在每台路由器上都进行，就算一台坏掉，其他也可以进行计算，比较健壮 DV：若出现了一个不正确的费用，它可能会被传向全网络

跳：源路由器到目的子网的最短路径经过的子网数量

自治系统内部路由选择协议：RIP：每条链路的费用为 1；A 路由器到 b 子网的总费用=A 到 b 的最短路径的跳数；一条路径的最大条数=15，所以 RIP 被限制在网络直径不超过 15 跳的自治系统内；**RIP 响应报文/RIP 通告（UDP）**：每对邻接的路由器间每 30s 交换一次，若 180s 还未收到某一邻居的报文，则不再视该邻居路由器为可达，则修改本地选择表，并向邻居通告。包含该路由器或主机所在 AS 内多达 25 个子网列表，和路由器/主机到子网的距离；**RIP 用运输层协议 UDP 实现网络层协议**；**路由选择表**：包含距离向量和转发表，每 30s 收到邻居报文

自治系统内部路由选择协议：OSPF：如何找最短路径？AS 中的每一台路由器都构建一幅关于整个 AS 的完整拓扑图，在图中运行 Dijkstra 算法，确定一个以自身为根结点的到所有子网的最短路径树。**链路费用**：由网络管理员定义：都为 1：实现最小跳数；与链路容量成反比：不鼓励流量使用低带宽链路，**如何构建拓扑图**：路由器向自治系统内**所有**其他路径广播路由选择信息：链路状态（费用、连接状态）发生变化时，路由器会广播状态信息；链路状态未发生变化，每 30min 广播一次 **优点**：安全（只有受信任的路由器能参与一个 AS 的 OSPF 协议，可防止恶意入侵者（利用明文口令或秘钥））多条相同费用的路径（OSPF 允许多条路径，无需仅选择单一路径承载所有流量）对单播与多播路由选择的综合支持 支持在单个路由选择域内的层次结构

自治系统间的路由选择协议：BGP：**交换信息的途径**：在 179 端口的半永久 TCP 连接 **BGP 对等方**：TCP 连接两端点的两台路由器 **BGP 会话**：沿着 TCP 连接发送的所有 BGP 报文**如何知道别的 AS 可达哪些子网**每个 AS 向相邻的 AS 通告与自己相连的子网前缀列表，每个 AS 由 eBGP(外部 BGP 会话)收到相邻的 AS 的通告，利用 iBGP 向本 AS 中的其他路由器发布前缀，一台路由器的值一个新前缀时，为该前缀在转发表中创建一个项 **路由**：包括一些 BGP 属性的前缀。**BGP 属性**：AS-PATH：包含前缀的通告已经通过的那些 AS（防止循环通告）NEXT-HOP：开始某 AS-PATH 的路由器接口，其实是提供一个子网地址（发送方的子网）。**如果一台路由器接收到了许多相同子网前缀的路由，如何选择** 1.每个路由具有一个本地偏好值的属性，先选择本路由器偏好的路由 2.余下的路由中（偏好值相同），最短的 AS-PATH 留下 3.余下的路由中（偏好值和 AS-PATH 长度都相同），选择具有最靠近（具有最低费用路径）NEXP-HOP 路由器的路由【热土豆】4.余下的路由中，使用 BGP 标识符选择

链路层提供的服务：成帧,链路接入,可靠交付,差错检测和纠正

奇偶校验：单个**奇偶校验位(parity bit)**(偶校验方案：选择校验比特的值，使得【数据比特+校验比特】这 d+1 个比特中的 1 的总数为偶数)**,二维奇偶校验**(将 d 个比特信息和划分成 i 行 j 列（d=i*j）对每一行和每一列就进行单奇偶校验，那么帧中就包含了 i+j+1 个比特） **前向纠错 FEC**：接收方监测和纠正差错的能力。

检验和方法：将 d 比特数据视为 k 比特整数的序列。**因特网检验和**：将 d 比特数据视为 16 比特整数的序列，将所有 k 比特整数加起来的结果的反码。接收方：对接收的数据视为 16 比特整数序列，加起来的和取反，若全为 1，则无错。

循环冗余检测 CRC

广播链路：让多个发送和接收结点都连接到相同的、单一的、共享的广播信道上。**多路访问问题**：如何协调**多个发送和接收结点**对**一个**共享广播信道的访问。**碰撞**：一结点同时接到多个帧，那么在该结点处发生碰撞。

信道划分协议：①时分多路复用 TDM：TDM 将时间划成时间帧，把每一帧划分成为多个时隙。**优点**：消除了碰撞/公平：每个结点都有 R/N bps 的带宽**缺点**：每个结点被限制在了 R/N bps 带宽内/每个结点需要等待自己的时隙到来才能发送②频分多路复用 FDM：FDM 把 R bps 的信道划分成了 N 个不同的频段，每个频段具有 R/N bps 的带宽，分配给每个结点。优缺点与 TDM 类似。③码分多址 CDMA：CDMA 对每个结点分配一种不同的编码，每个结点用他唯一的编码来对它发送的数据进行编码。接收方如果知道发送方的编码，那么如果所有结点同时传输，接收方可以辨别哪个出发送方发送的数据。

随机接入协议：①时隙 ALOHA：结点有新的帧发送时，在下一个时隙开始时发送：没有碰撞，不考虑重传；发生碰撞，在时隙结束前检测到碰撞事件，那么以概率 p 在后续的每个时隙中重传此帧，直到该帧无碰撞地传过去。**优点**：若只有一个结点在传输，他可以获得 R 的速率；高度分散，每个结点独立地决定什么时候重传 **效率**：大量结点，最大效率为 1/e=0.37②ALOHA：如果一个传输的帧与一个或多个传输经历了碰撞，这个结点在传输完整个碰撞帧后**立即**以概率 p 重传；否则等待一个帧传输的时间，再以 p 的概率重传或 1-p 的概率等待。**效率**：大量结点，最大效率为 1/2e=0.37③载波侦听多路访问 CSMA：传输前先听信道，若信道被占用，等待直到检测到一小段时间没有传输，再传输④具有碰撞检测的载波侦听多路访问 CSMA/CD（以太网采用此协议）：一个结点在传输时一直侦听此信道，若检测到另一结点在干扰帧，就停止传输，等待一个随机时间，再进入"侦听-空闲时传输"的循环。等待时间的选择：二进制指数后退：经历 n 次碰撞，在[0,...,2^n-1]中选一个值为 K，延迟 K*512 比特时间。CSMA/CD 效率：只有一个帧，该帧能以全速率传输；大量结点传输时有近似式：与上 **结论：应控制以太网的规模**

轮流协议：①轮询协议(蓝牙)：主节点轮询每个结点：告诉它它能够传输的帧的最多数量，它发送完毕后，访问下一个结点，重复。**优点**：清除了碰撞，提高了效率 **缺点**：引入了轮询时延；也要轮询非活跃的结点，降低了效率②令牌传递协议：令牌在结点之间交换。一个结点收到了令牌，若它要传输帧，它就持有并发送最大数目的帧，否则他传输给下一个。**优点**：令牌传递是分散的，效率很高 **缺点**：一个结点故障会使信道崩溃,一个结点偶然忘记释放令牌，需要调用恢复步骤

比较：ALOHA 和 CSMA 都能保证如果只有一个结点活跃，它可以使用 R 的带宽；但不能保证如果有 M 个结点活跃，每个活跃结点的吞吐量接近 R/M。轮流协议可以

MAC 地址：一个网络适配器具有一个 MAC 地址，该 MAC 地址不会改变。没有两块适配器有相同地址。MAC 地址被 IEEE 管理。MAC 地址长度 **6Btyes**，共有 2^{48} 个可能的 MAC 地址。**MAC 广播地址**：FF-FF-FF-FF-FF-FF 可使局域网上所有其他适配器来接受并处理帧

有了 IP 地址为什么还需要 MAC 地址？ 1.如果没有 MAC，对于非 IP 的网络层协议将不能支持 2.如果只用网络层地址的话，它被存在适配器的 RAM 中，每次启动或移动是都要重新配置。3.如果不使用 MAC 地址，每次到网络层去看地址的话，会导致主机将被局域网上发送的每个帧中断

地址解析协议 ARP：用于将同一子网上的网络层地址和链路层地址之间转换。**ARP 表在哪里**：每台主机或路由器的内存中。**ARP 表包含**：IP 地址到 MAC 地址的映射关系，每一个 IP 地址的寿命 TTL **地址解析协议：**ARP 模块到 ARP 表中查找该目的 IP 地址是否有对应的 MAC 地址：若有，把该 MAC 地址加入链路层帧中，发送数据报；若没有：发送方构造一个 ARP 查询分组，发送方适配器用 *MAC 广播地址*发送此分组，发送到子网中（发送方地址段=自己的 MAC 地址和 IP 地址，目标字段=B 的 IP 地址），子网中每个适配器都接收到，并将向上传递给 ARP 模块，每个 ARP 模块都检查自己主机的 IP 地址是否与该目的地址相匹配，若匹配，返回一个 ARP 响应分组。发送方收到响应分组，更新 ARP 表，发送数据报。**注意**：ARP 查询分组是广播帧，ARP 响应分组是标准帧；ARP 表是自动建立的，无需管理员配置 **发送数据报到子网外**：子网 1 的 A 主机想将一个数据报发送给子网 2 的 B 主机：A 主机的适配器需要将 MAC 地址设置成为第一跳路由器的与此子网相连的适配器地址

以太网：以太网提供的是**无连接**（无握手）、**不可靠**（不确认也不否定确认）服务 **以太网帧结构**=数据字段（46-1500Bytes，46 字节<数据报<1500 字节）+目的 MAC 地址（6Bytes）+源 MAC 地址（6Bytes）+类型字段（2Bytes，允许以太网复用多种网络层协议）+CRC（4Bytes）+前同步码（8Bytes，前 7 字节相同用于唤醒适配器和是目的适配器与发送适配器的时钟同步，最后一个字节后两比特警告目的适配器：重要内容来了）**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

链路层交换机：**过滤**：决定一个帧该转发到某个接口还是应当将其丢弃的交换机功能 **转发**：决定一个帧应该被导向哪个接口，并把帧移动到那些接口 **交换机表**：包含某局域网上某些主机和路由器但不必是全部的表项（MAC 地址-通向该 MAC 地址的接口-表项放置在表中的时间）**转发过程**：1.一个帧从交换机的 x 接口到达，交换机取得目的 MAC 地址，在交换机表中索引 2.若表中没有对应表项，交换机广播该帧，即向所有（除去 x）的接口转发该帧 3.若表中有对应表项，且表项是<目的地址-x 接口>，那么将帧过滤，无需转发 4.若表中有对应表项，且表项是<目的地址-y 接口>，y≠x，将帧转发至 y 接口 **自学习配置交换机表**：1.初始表为空 2. 存储每个入帧<源地址的 MAC 地址-该帧到达的接口-当前时间>3. 一段时间后若交换机没有接收到以该地址作为源地址的帧，将该表项删除 交换机是**即插即用设备**，不需要网络管理员或用户干预。**性质**：消除碰撞；异质的电路；管理：安全性

交换机和路由器的比较：1.交换机用 MAC 地址索引，路由器用 IP 地址索引 2. 交换机是第二层的，路由器是第三层的 3. 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 4. 交换机不能阻断广播帧的传播；路由器可以阻断

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。路由器转发 IP 包的过程：用目的 IP 地址查找转发表，获得下一跳 IP 地址及端口，利用 ARP 获得下一跳 MAC 地址，用下一跳 MAC 地址构造链路层帧，发送 三层交换机转发 IP 包的过程：将以上第 1、第 2 步的结果缓存到本地三层转发表中

用目的 IP 地址查找三层转发表：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，执行以上第 1、2、3 步 **速度快的原因**：一次选路，多次转发

无线网络的组成：无线终端+基站+无线链路

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，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. 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

无线链路传播特性：信号衰减、干扰、多径传播

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。**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。

IEEE 802.11 无线局域网：802.11b、802.11a、802.11g、802.11n, 均使用 CSMA/CA 作为 MAC 协议，都支持基站模式和自组织模式

基本服务集（BSS）=若干无线终端+一个无线接入点 AP（基站），是 802.11 无线 LAN 的基本组成单元 **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，主机必须与一个 AP 关联

802.11 的操作模式：PCF 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。DCF 模式：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**：假设 A 欲向 AP 发送一个数据帧：A 向 AP 发送一个 RTS 帧，帧中给出随后要发送的数据帧及确认帧需要的总时间，AP 收到后回复一个 CTS 帧，帧中给出同样的时间，A 收到 CTS 帧后开始发送，AP 收到帧后，发送一个 ACK 帧进行确认。（A 附近）收到 RTS 帧及（AP 附近）收到 CTS 帧的节点均沉默指定的时间，让出信道让 A 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。**无信道预约的机制**：当节点有帧要发送时，侦听信道：若一开始就侦听到信道空闲，等待 DIFS 时间后发送帧；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. 当计数值减为 0 时，发送整个帧并等待确认. 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

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，交换机中的转发表也需要更新；切换过程中，终端上的应用正常运行（因为 IP 地址没变，上层感受不到在切换）；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

间接选路：移动节点使用两个地址：**永久地址**：通信者用来向移动节点发送数据报 **转交地址**：归属代理用来向移动节点转发数据报 **三角选路：通信者-归属网络-移动节点**，当通信者和移动节点在同一个网络中时很低效

直接选路到移动节点：通信者向归属代理请求获知移动节点的转交地址；通信者将包发送给外地代理；外地代理将包转发给移动节点；移动节点直接向通信者发送（问题：对通信者不透明）

Mobile IP：代理发现、移动节点注册、数据报间接选路

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

数据报如何到达转交地址？归属代理通过隧道转发数据包

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，外地代理正常转发数据包

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；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

安全通信需要：机密性、报文完整性、结点鉴别、运行安全性

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（偷听：监听并记录网络中传输的内容；流量分析：从通信频度等流量模式推断通信的性质）主动攻击：试图改变系统资源或影响系统的操作（伪装、重放：从网络中获取一个数据单元，经过一段时间后重新发送到网络中；报文修改：改变报文内容、推迟发送报文或改变发送顺序；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（对数据进行变换，使不易理解）鉴别（通过报文交换确信一个实体的身份，以防假冒）数据完整性（用于保护数据单元或数据单元流的完整性，以防报文修改）数字签名（附加在数据单元后面的数据，用来证明数据单元完整性，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）

针对加密系统的密码分析攻击：惟密文攻击(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（密码分析者可以任意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

对称密钥算法：DES：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

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

非对称加密算法：发送者和接收者不共享密钥：发送者使用公开密钥：接收者使用私有密钥 **RSA 算法（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 $e*d=1 \pmod z$ 公开密钥为 (e, n)，私有密钥为 (d, n) **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 $0 \leq M < n$ 对每个数据块 M，计算 $C = M^e \pmod n$，C 即为 M 的密文。**解密方法**：对每个密文块 C，计算 $M = C^d \pmod n$，M 即为要求的明文。**优点**：安全性好，使用方便；**缺点**：计算开销大，速度慢 **RSA 的应用**：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，也称数字指纹。

报文鉴别：起源鉴别、完整性检查。方法 1:对整个报文加密：双方有共享的密钥（缺点：混淆了机密性和报文鉴别两个概念）。方法 2:发送方计算报文摘要，然后用共享的密钥加密报文摘要，形成报文鉴别标签，接收方解密报文鉴别码得到发送方的报文摘要，与自己算的报文摘要比较（缺点：需要使用加密算法）方法 3:密码散列函数，发送方用双方共享的一个密钥 KS 添加到报文 m 之前，然后计算报文摘要 H(KS || m)形成报文鉴别码

数字签名：用私钥加密报文摘要：发送方先计算报文摘要，然后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。

ap4.0: Bob 向 Alice 发送不重数 R，Alice 用共享密钥加密 R，回送给 Bob。

ap5.0：采用公开密钥算法加密不重数

X.509 的三种鉴别程序：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

安全电子邮件协议：PGP 提供五种服务：鉴别，机密性，压缩，兼容电子邮件，分段

SSL：向基于 TCP 的网络应用提供安全的传输层服务：服务器鉴别，数据加密，客户鉴别；SSL 建立在 TCP 之上，依靠 TCP 提供可靠的端到端连接 SSL 握手协议：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。由客户和服务器之间的一系列报文交换组成：①浏览器向服务器发送建立 SSL 会话的请求报文，说明可支持的 SSL 协议最高版本等，和选择的一个随机数 Rc。②服务器从给出的选择中确定合适的 SSL 版本号、加密算法和压缩方法，与服务器选择的随机数 Rs 发送给浏览器。③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。④浏览器检查签发证书的 CA 是否在浏览器的可信 CA 列表中，如果在则使用该 CA 的公钥验证证书，得到服务器的公钥。⑤如果客户也需要被鉴别，则浏览器向服务器发送它的公钥证书。⑥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。⑦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。⑧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。⑨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。

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；包括 IPSec 安全协议（AH+ESP）和密钥管理协议；**两种模式**：传输模式（用原始 IP 头转发）、隧道模式（用新的 IP 头转发）（传输模式比隧道模式占用较少的带宽；隧道模式更安全）**AH 协议**（鉴别头部协议）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；**ESP**(封装安全载荷)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

防火墙：包过滤防火墙、状态检测防火墙（跟踪连接的建立（SYN）和关闭（FIN）等状态，判断收 到的包是否有意义）、应用网关（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）**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