由 IEEE 802.3 工作组标准化，形成 IEEE 802.3 标准族。**10Mbps 以太网（早期以太网）：** 10Base-5：基带同轴电缆（粗），每段电缆最大长度 500 米；10Base-2：基带同轴电缆（细），每段电缆最大长度约 200 米；10Base-T：3 类双绞线和集线器，双绞线最大长度 100 米；10Base-F：多模光纤和集线器，光纤最大长度 2000 米。**100Mbps 以太网（快速以太网）：** 仅能使用光纤/双绞线，以及集线器/交换机：100Base-TX（可使用集线器或交换机）：5 类双绞线（2 对），不超过 100 米；100Base-T4 （可使用集线器或交换机）：3 类双绞线（4 对），不超过 100 米；100Base-FX（只能使用交换机）：多模光纤（2 条），不超过 2000 米。**千兆、万兆以太网：** 只用交换机，并增加了对流量控制的支持：1000Base-SX：多模光纤，不超过 550 米；1000Base-LX：单模或多模光纤，不超过 5000 米；1000Base-CX（很少用）：2 对屏蔽双绞线，不超过 25 米；1000Base-T：4 对 5 类双绞线，不超过 100 米；10GBase-T：只使用光纤，长距离用单模光纤，短距离用多模光纤。**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。***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（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。** **链路层交换机：** ***交换机的任务***是接收入链路层帧并将它们转发到出链路。交换机自身对子网中的主机和路由器是***透明的***。**交换机输出接口设有缓存。** ***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&&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：*** 当帧到来时，**1.** 记录帧的到来端口；**2.** 用帧的目的 MAC 地址查找转发表；**3. if** 找到目的 MAC 地址（已知节点）**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（未知节点，采用扩散法转发）（向输入端口以外的所有端口转发）***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）：** 若目的地址所在端口 = 帧的进入端口，丢弃帧；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。**交换机的表**是自动、动态和自治地建立的，***交换机是自学习的***：**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：在该帧源地址字段中的 MAC 地址，该帧到达的接口，当前时间交换机以这种方式在它的表中记录了发送结点所在的局域网网段。如果在局域网上的每个结点最终都发送了一个帧，则每个结点最终将在这张表中留有记录。**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。以这种方式，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。**交换机是即插即用设备。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。** ***使用交换机的几个优点，它们不同于如总线或基于集线器的星形拓扑那样的广播链路：*** **• 消除碰撞：** 交换机缓存帧并且决不会在网段上同时传输多于一个帧。**• 异质的链路：** 交换机将链路彼此隔离，因此局域网中的不同链路能够以不同的速率运行并且能够在不同的媒体上运行 **• 管理：** 提供强化的安全性（参见插入材料"关注安全性"）交换机也易于进行网络管理。***交换机和路由器比较：*** 尽管交换机也是一个存储转发分组交换机，但它和路由器是根本不同的，因为它用 MAC 地址转发分组，而路由器使用网络层地址。交换机是第二层的分组交换机，而路由器是第三层的分组交换机。***交换机的优点和缺点：*** 即插即用，能够具有相对高的分组过滤和转发速率；为了防止广播帧的循环，交换网络的活跃拓扑限制为一棵生成树，一个大型交换网络将要求在主机和路由器中有大的 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，要人为的配置 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 CP 地址的任何配置就能使流批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。***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。Q: 数据包要从 A 发往 F，交换机 S1 如何知道应转发给 S4，而 S4 如何知道应转发给 S2? A: 通过自主学习！(与单交换机情形相同)。***有环网络和生成树算法：*** 为了提高可靠性，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。***冲突域：*** 第一层，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：*** 第二层，广播帧能够到达的主机集合。**虚拟局域网（VLAN）：** 在大型机构网络中，管理员通常按部门将用户组织到不同的网络中。***管理员配置网络遇到的困难：*** 同一部门的人员在物理位置上可能很分散（他们的主机连接到在不同的交换机上），但是逻辑上，不同的网络可能需要隔离；用大量的路由器来分割网段，成本很高。***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）。***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。***IEEE 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。***802.1Q 如何与已有网卡兼容：*** **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。***三层交换机和路由器：*** 不同子网或 VLAN 之间通过路由器转发，太慢！**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 VLAN；专业路由器：连接机构网络与外网。***三层交换机为什么快：*** 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。三层交换机转发速度快的原因：一次选路，多次转发。***链路虚拟化：网络作为链路层：*** **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 层不是不可见的，对于 IP 来说物理网络只是一条虚拟链路而已！***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：**

无线和移动网络：

Background： 终端（特别是笔记本、智能手机）的处理能力越来越强，成本越来越低，已经成为大众化的电子设备；用户随时随地上网的意愿非常强烈。**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。***概述：无线网络的组成：*无线终端**，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：*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：** 主机通过多个无线节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，节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，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。** ***无线网络的特性：*(a) 隐藏结点问题：** 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；**(b) 暴露节点问题：** 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）***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 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（一个中央基站）；每个无线接口（终端及 AP）均有一个全局唯一的 MAC 地址。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（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；**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)。***以太网和 802.11 都使用载波侦听随机接入，但这两种 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。***802.11 的操作模式：PCF（Point Coordination Function）模式：*** 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。***DCF（Distributed Coordination Function）模式：*** 可用于有基础设施的无线网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 B 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。***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，不使用确认机制；而 CSMA/CA 在发送过程中不检测冲突，使用确认机制；**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：*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，然后再关联到 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：*** **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，不能保留旧 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；即使对方知道终端的新地址，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"(e.g., 128.119.40/24)。**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，即使移动也保持不变（e.g., 128.119.40.186）。**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。**外地网络：** 移动节点当前所在的网络(e.g., 79.129.13/24)。**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。**转交地址(COA)：** 移动节点在外地网络上的地址(e.g., 79,129.13.2)。**通信者：** 希望与移动节点通信的节点。***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：*** 通信者在数据包中使用移动节点的永久地址；归属代理截获数据包，转发给外地代理；外地代理截获数据包，转发给移动节点；移动节点直接将响应发送给通信者。***间接选路：三角选路问题：*** 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（从而移动节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。***间接选路：终端在外地网络间移动：*** 假设节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；归属代理更新移动节点的转交地址；归属代理使用新的转交地址向移动节点转发包；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：*** 通信者向归属代理请求，并获知移动节点的转交地址（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节点；移动节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（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，移动节点注册，**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：*** 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；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：*** 移动节点向外地代理发送一个注册请求，给出自己的永久地址、转交地址、归属代理地址以及认证信息等；外地代理记录相关信息，向归属代理转发注册请求；归属代理处理注册请求，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；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；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：*** 数据包首先被归属代理得到；归属代理查找地址绑定表，获得移动节点当前的转交地址；归属代理将数据包封装后发送到转交地址；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：** 通信者查表得知可以直接交付，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。***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（√）。*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，里面封装着通信者发送的包（这个包的 dest 是永久地址）；**外地代理向移动节点发送的包：** 通信者发送的原始包。***外地代理如何发送数据包到移动节点？*** 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。

计算机网络中的安全：

什么是网络安全：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、通信活动的机密性；**• 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；***流量分析：*** 从通信频度、报文长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；**四种类型：** ***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：*** 附加在一个数据单元后面的数据，用来证明数据单元的起源及完整性，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。***密码学的原则：明文（plaintext）：*** 欲加密的原始数据；***密文（ciphertext）：*** 明文经加密算法作用后的输出；***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；***密码学（cryptology）：*** 设计密码和破译密码的技术统称为密码学。***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；**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。**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，单字母表替换，多字母表替换；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。***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。***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。**全表快密码难以实现。***DES (Data Encryption Standard)：*** 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；一种对称加密算法，加密和解密使用相同的函数，两者的不同只是子密钥的次序刚好相反；缺点：密钥长度不够长，迭代次数不够多。***DES 的计算过程：*** 首先进行一次初始换位（permute），然后进行 16 轮相同的迭代，每轮迭代使用一个不同的子密钥（由主密钥生成），最后再进行一次换位（与初始换位相反）。***3DES*** 使用两个密钥，执行**三次 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 设备工作于解密模式，使用密钥 K2 对第一轮的输出进行变换；第三轮令 DES 设备工作于加密模式，用密钥 K1 对第二轮的输出进行变换，输出密文。***有关 3DES 的三个问题：*** 为什么使用两个密钥而不是三个密钥？112 比特的密钥已经足够长。为什么不使用两重 DES（EE 模式）而是三重 DES? 考虑采用 EE 模式的两重 DES，且攻击者已经拥有了一个匹配的明文--密文对（P1, C1），即有 C1 = EK2 (EK1 (P1))，令 X = EK1(P1) = DK2(C1)，攻击者分别计算 EK1(P1)和 DK2(C1)，并寻找使它们相等的 K1 和 K2，则穷尽两个密钥空间只需 256 的攻击量而不是 2112。（中途攻击）为什么是 EDE 而不是 EEE? 为了与单次 DES 兼容。3DES 用户解密单次 DES 用户加密的数据，只需令 K1 = K2 就行了。***AES（Advanced Encryption Standard）：*** 每次处理 128 比特明文块，输出 128 比特的密文块；密钥长度可以是 128、192 或 256 比特；如果用强力方法破解，假设破解 DES 需要 1 秒，则破解 AES（128 比特密钥）需要 149 万亿年！***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。**密码块链接（CBC）：** c(i)=Ks(m(i) XOR c(i-1))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，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；存在密钥传递问题：加密密钥是公开的，解密密钥是私有的。***公开密钥算法的使用：*** 每个用户生成一对加密密钥和解密密钥：加密密钥放在一个公开的文件中，解密密钥妥善保管；当 Alice 希望向 Bob 发送一个加密信息时：Alice 从公开的文件中查到 Bob 的加密密钥，用 Bob 的加密密钥加密信息，发送给 Bob；Bob 用自己的解密密钥解密信息。**公开密钥和私有密钥：** 公钥：加密密钥，由发送者使用；私有密钥：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以向 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：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 e；找到一个 d 使满足 e*d = 1 (mod z)；公开密钥为(e, n)，私有密钥为 (d, n)。***RSA 算法：加密和解密：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；***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。***RSA：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。***RSA 的特点：*** 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：发送方用共享的密钥加密整个报文，发送给接收方；如果接收方能够正确解密收到的报文，则报文必是可信的。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。***将报文鉴别与数据机密性分开：*** **设想：** 发送者用明文发送报文，并在报文后附上一个标签，允许接收者利用这个标签来鉴别报文的真伪；**用于鉴别报文的标签必须满足两个条件：** 能够验证报文的完整性（是否被修改），不能被伪造。***数据完整性和报文摘要：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的完整性：*** 发送者对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，与收到的标签（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？报文鉴别之方法二：*** 发送方计算报文摘要，然后用与接收方共享的密钥加密报文摘要，形成报文鉴别标签（也称***报文鉴别码***）；接收方使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。**密码散列函数：*为什么要开发一个不需要加密算法的报文鉴别技术？*** 加密软件通常运行得很慢，即使只加密少量的数据；加密硬件的代价是不能忽略的；加密算法可能受专利保护（如 RSA），因而使用代价很高；加密算法可能受到出口控制（如 DES），因此有些组织可能无法得到加密算法。***使用密钥散列函数（cryptographic hash function）生成报文鉴别码：*** 使用密码散列函数计算报文摘要时需要包含一个密钥，但它并不用来做加密运算；发送方用双方共享的一个秘密密钥 KS 添加到报文 m 之前，然后计算报文摘要 H (KS || m)形成报文鉴别码。***散列函数 H 应满足的特性：*** 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(KS||m)=h 可以找到一个 x，使得 H(x)=h，那么根据 x 和 m 可以推出 KS；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，如果能够找到一个不同于 x 的数据块 y，使得 H(y)=H(x)，那么就可以用 y 替换 x 而不被接收方察觉；要找到一对 (x，y) 满足 H(y) = H(x)，在计算上是不可能的。（抵抗生日攻击）满足前四个特性的散列函数称为**弱散列**函数，满足所有五个特性的散列函数称为**强散列**函数。***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；目前获得最多支持的密码散列函数方案为 HMAC，已应用到许多安全协议中。**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，因为有两个人拥有它。***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。***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报文（使用公钥密码）；因此，数字签名是一种"技术含量更高"的技术，因为它需要一个如后面描述的、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？*** 考虑下面的例子：Bob 将公钥 EB 发布在自己的主页上；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，发送给 Bob；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。**问题：** 当 Alice 从公开的途径得到 Bob 的公钥后，Alice 如何确认她得到的就是 Bob 的公钥，而不是其他人的公钥？***公钥证书：*** 为使公钥密码体系有实际应用，每个实体必须能够确认它得到的公钥确实来自声称的实体；解决方案是引入证书机制：使用证书（certificate）来证明某个主体（principal）拥有某个公钥，证书由一个可信任的第三方机构颁发，该机构称为认证权威 CA（certification authority）；证书包含主体的公钥和 CA 的签名，任何人无法伪造或篡改证书的内容；当一个主体获得证书后，可将证书放在任何一个可以公开访问的地方。***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。***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：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；为验证公钥证书的真实性：验证用 CA 的公钥解开证书的签名，得到证书内容的报文摘要；对收到的证书内容计算报文摘要，并与解密得到的报文摘要进行比较，两者相同表明这是合法的公钥证书。***谁可以运行 CA? 世界上有几个 CA?*** 使用一个 CA 签发全世界所有的证书?流量压力，单点失败。由一个组织运行多个 CA? 密钥泄露，信任问题。***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。***信任锚与信任链：信任锚（trust anchor）：*** 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，信任锚必须通过安全的物理途径获取；**信任链（chain of trust）：** 从叶结点到根 CA 的证书序列；**根 CA 的选择：** 有许多根 CA，每个根 CA 都有自己的一个分级结构，所有根 CA 间可以进行交叉认证；用户自行决定信任哪个根 CA；实际上，许多根 CA 的公钥预装在浏览器上，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：*** 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。***证书存放在哪里？*** 使用 DNS 作为***证书目录***，该方案的标准为 DNSSEC；使用专门的目录服务器存放证书，该方案的标准为 LDAP；证书撤销列表通常与证书存放在一起，CA 定期地将 CRL 推送到目录服务器，由目录服务器负责将 CRL 中列出的证书清除掉。***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。鉴别应当在报文和数据交换的基础上，作为某***鉴别协议***的一部分独立完成。鉴别协议通常在两个通信实体运行其他协议（例如，可靠数据传输协议、路由选择信息交换协议或电子邮件协议）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。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 发送口令证明自己，口令是鉴别者和被鉴别者之间共享的秘密。Trudy 监听到 Alice 发送的明文口令，过后发送给 Bob。鉴别协议 ap3.1：Alice 将口令加密，发送给 Bob。Trudy 截获数据包，过后发送给 Bob（重放攻击）鉴别协议 ap4.0：***目标：*** 避免重放攻击。***失败的情况是因为*** Bob 不能区分 Alice 的初始鉴别报文和后来入侵者回放的 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。***不重数(nonce)：*** 在一个协议的生存期中只使用一次的数，也就是说，一旦某协议使用了一个不重数，就永远不会再使用那个数字了。***协议 ap4.0 以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 知道收到的报文是由 Alice 产生的。这个不重数用于确定 Alice 是活跃的；4) Bob 解密接收到的报文，如果解密得到的不重数等于他发送给 Alice 的那个不重数，则可鉴别 Alice 的身份。**缺点：** 需要一个共享的对称密钥。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 定义了三种鉴别程序，供不同的应用选择：*** 单向鉴别：涉及一个用户到另一个用户的一次报文传输（接收方单向鉴别发送方）；双向鉴别：通信双方相互鉴别；三向鉴别：在双向鉴别的基础上增加报文同步机制。***单向鉴别（one-way authentication）：*** A→B：tA ||rA|| IDB || Data || Kb+(Ka-b) || signatureA；**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（two-way authentication）：*** 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（three-way authentication）：*** A→B：tA || rA || IDB || Data || Kb+ (Ka-b) || signatureA；B→A：tB || rB || IDA || rA|| Data || Ka+(Kb-a) || signatureB；A→B：rB || signatureA。***安全电子邮件：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不足以满足一切需要吗？*** 首先，尽管可以通过加密数据报中的所有数据（即所有运输层报文段），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，同时最为期望的安全特性还有"发送方鉴别""报文完整性"和"接收方鉴别"。*提供机密性的方式：*对称密钥算法?** 仅有 Alice 和 Bob 具有该密钥的副本，这使得分发对称密钥非常困难。**公开密钥密码?** 效率相对低下，尤其对于长报文更是如此。**为了克服效率问题，我们利用了会话密钥，具体来说：** 1). Alice 选择一个随机对称会话密钥 Ks；2). 用这个对称密钥加密她的报文 m；3). 用 Bob 的公钥 KB+加密这个对称密钥；4). 级联该加密的报文和加密的对称密钥以形成一个"包"；5). 向 Bob 的电子邮件地址发送这个包。**当 Bob 接收到这个包时：** 他使用其私钥 KB-得到对称密钥 Ks；使用这个对称密钥 Ks 解密报文 m。***只关心发送方鉴别和报文完整性：*** 使用数字签名和报文摘要。**具体说来：** Alice 对她要发送的报文 m 应用一个散列函数 H(例如 MD5),从而得到一个报文摘要；用她的私钥 KA-对散列函数的结果进行签名，从而得到一个数字签名；把初始报文（未加密）和该数字签名级联起来生成一个包；向 Bob 的电子邮件地址发送这个包。**当 Bob 接收到这个包时：** 他将 Alice 的公钥 KB+应用到被签名的报文摘要上；将该操作的结果与他自己对该报文的散列 H 进行比较。***设计一个提供机密性、发送方鉴别和报文完整性的电子邮件系统：*** 过程结合起来而实现：Alice 首先生成一个预备包，它与图 8-20 中的包完全相同，其中包含她的初始报文和该报文数字签名过的散列；然后 Alice 把这个预备包看作一个报文，再用图 8-19 中的发送方的步骤发送这个新报文，即生成一个新包发给 Bob。**当 Bob 接收到这个包后，** 他首先应用图 8-19 中他这一侧的步骤，然后再应用图 8-20 中他这一侧的步骤。注意到在这一方案中，Alice 两次使用了公开密钥密码：一次用了她的私钥，另一次用了 Bob 的公钥。同样，Bob 也两次使用了公开密钥密码：一次用了他的私钥，一次用了 Alice 的公钥。***PGP：目前最流行的两个安全电子邮件协议：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）；**S/MIME：** 基于公钥加密技术对 MIME 所做的安全扩展。S/MIME 较可能作为一种工业标准被商业组织或一些机构使用。***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（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：** 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：** 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))；在压缩报文之前计算数字签名，是为了方便日后对报文的验证；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：** PGP 使用 Base64 编码将二进制数据流转换成可打印 ASCII 文本，以解决邮件的传输问题；PGP 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。***同时使用以上四种服务的过程：*** 发送方先对报文计算签名，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：** 许多电子邮件系统能够接收的最大报文长度不超过 50,000 字节；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：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）。如购物。***安全服务：*** 服务器鉴别，数据加密，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：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：用于 SSL 交换管理。**宏观描述：*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。**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 会话的请求报文，说明可支持的 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。***SSL 记录协议：*** SSL 记录协议为 SSL 连接提供**两种服务：机密性：** 通过加密 SSL 载荷实现；**完整性：** 通过报文鉴别码保护。**SSL 记录协议的操作过程：** 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 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、压缩数据块的长度等。***阻止插入、删除和代替报文段：*** 使用序号；Bob 维护一个序号计数器，计数器开始为 0，Bob 每发送的一个 SSL 记录它都增加 1；Bob 并不实际在记录中包括一个序号，但当他计算 MAC 时，他把该序号包括在 MAC 的计算中；所以，该 MAC 现在是数据加 MAC 密钥 MB 加当前序号的散列；Alice 跟踪 Bob 的序号，通过在 MAC 的计算中包括适当的序号，使她验证一条记录的数据完整性。***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底层的支持。**IPsec 和虚拟专用网：*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（overlay），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。传送公用网的 IPsec 被 IPv4 封装，同时拥有 IPv4 和 IPsec 首部。**安全关联：*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。从技术上讲，***IPSec 主要包括两部分：*** **IPSec 安全协议：** 包括 **AH**（不提供机密性）和 **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。SA 是：*** 通信对等实体之间对某些要素的约定，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。**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。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 数据报：*IPSec 的使用模式：*传输模式：** 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，从而有效防止入侵者进行流量分析。***鉴别头部（Authentication Header）协议：*** **SPI：** 32 比特的数，与目的 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，所有 AH 实现必须支持 HMAC-MD5-96 和 HMAC-SHA-1-96。***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 数据包大致分为以下几个部分：** 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，鉴别数据：覆盖 ESP 头、载荷和 ESP 尾的报文鉴别码。***隧道模式路由 R1 使用下列方法将这个"普通 1Pv4 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)！后面附上一个"ESP 尾部"字段；• 使用算法和由 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 1Pv4 首部字段（通常共 20 个字节）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。***AH 协议和 ESP 协议的安全性比较：*** ESP 隧道模式的安全性强于 ESP 传输模式；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。***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。***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。**有限等效保密：*主机鉴别过程：*** 无线主机向 AP 请求鉴别；AP 向主机发送一个 128 比特的不重数；主机使用与 AP 共享的对称密钥加密不重数，发送给 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。利用主机与基站共享密钥这个事实鉴别主机。***WEP 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 {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 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 AP）来提供鉴别服务。***802.11i 的操作：*** **1) 发现。** 在发现阶段，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)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(Pairwise Master Key，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 AP 发送该 PMK。客户和 AP 现在具有一个共享的密钥。**4)临时密钥(Temporal Key，TK) 生成。** 使用 PMK，无线客户和 AP 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，状态检测防火墙，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，丢弃其它进入的 UDP 包；防止网络拓扑被探测（traceroute）→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。***访问控制列表（Access Control Lists，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。**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：路由器无法知道数据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：** 防火墙不检查数据包之间的关联。***IDS: intrusion detection system：*** 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击的以前知识；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。

分片： 分片序号(从 1 开始) 总长度 MF 偏移量

分片类的问题中，若为电影缓存、音乐等，是应用层，应减去 TCP 头和 IP 头的长度才为数据部分；若为数据报，则为网络层，只需考虑 IP 头

标志： MF **标识：** 分片的标识都是一样的

链路状态算法 LS： 步骤(从 0 开始) N' D(v)，p(v) D(w)，p(w)

路由器转发表： 目的地址(目的网络：如 194.17.20.0/23) 掩码 下一跳(在同一子网内) 端口

若目的地址就在本子网内，则下一跳直接交付，否则写本子网的其他路由器的 ip 地址

R1 到互联网的路由实质上相当于一个**默认路由**（即当某一目的网络 IP 地址与路由表中其他一项都不匹配时，匹配该默认路由表项），默认路由一般写为 0/0，即**目的地址为 0.0.0.0，子网掩码为 0.0.0.0**。

路由协议： RIP、OSPF、BFP

交换机转发表： MAC addr（同一子网内，没有外网的 MAC 地址） interface TTL

交换机 vs 路由器：

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

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

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

链路层设备： 存储-转发帧

网络层功能： 选路和转发

在子网的分配中，要注意减去两个特殊地址

网关的 IP 地址是具有路由功能的设备的 IP 地址，通常**默认网关地址**就是路由器中的 LAN 端口地址

隧道技术的应用： 1.ipv6 数据包穿越到 ipv4 网络。2.多播分组穿越单播网络。3.归属代理通过隧道技术转发数据包。4.直接路由选择的通信者代理(COA)，和归属代理使用的隧道技术相似。5.vpn 隧道技术。6.ipsec 隧道模式

寿命(TTL)第四章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

路径的跳数第五章： 从源路由器到目的子网(含)经过的子网数量