**网络层**

**转发**：input->appropriate output(in router) **路由**：src->dst规划路径(in network)

**Virtual circuits & Datagram:** 1. Host-to-host. (IP to IP) 2. 不可兼得 3. 实现在网络核心

**Virtual circuits(如ATM):** **基于连接**。从电话系统演进而来。1.建立连接 2.包携带VC ID 3.所有路由器维持对每个经过的连接维持状态 4.bandwith, buffer进行分配

VC包含1.path(src->dst) 2.one VC number for each link(每条链路不同) 3.转发表条目

过程：1.建立连接：决定路径、决定VC number、添加转发条目至转发表 2.数据传输 3.拆除连接，更新转发表

**Datagram: connectionless**。没有状态，使用dst address进行转发。

转发表采用**最长前缀匹配**，先分配完整大块，再对小区间进行剔除即可。

转发表由路由算法维护，每1-5分钟进行更新。

一系列src IP,dst IP相同的包可能走不同的路径

**Virtual circuits V.S. Datagram:** datagram:很多链路类型(以太网，802.11)，传输速度没有严格限制，端系统(边缘)复杂 vc:从电话进化而来。有严格的时间可靠性要求。网络内部复杂

**路由器:routing(RIP,OSPF,BGP)+forwarding(table)**

组成：输入端口、交换结构、输出端口、路由处理器

输入端口：物理层->链路层协议接收->查找、转发、排队。线路前部HOL阻塞:指队列中由于前部包的阻塞导致后面包本可以发送但不能发送。输入端口缓存溢出导致排队延时与丢包 交换结构：内存、总线、矩阵开关（N inputs, N outputs, 2N buses）输出端口：datagram缓存，排队->链路层协议发送->物理层。输出端口缓存溢出导致排队延时与丢包。推荐大小RTT\*C/\sqrt{N} bits。RTT往返时延、C链路容量、N tcp连接。

随机早期检测RED算法是主动队列管理AQM的一种，在缓存填满前便丢弃分组通知发送方 处理器：调度排队

**IP协议：IPv4, ICMP, IPv6**

**IPv4:** version(4bit), header length(4bit), 服务类型(8bit),total length(MTU, 16bit), (Id16bit, Flag3bit, Offset13bit)（分片使用，ID相同，Flag=1表示未完，Flag=0表示最后一个，Offset表示当前第一个字节位置/8，**分片只在端处重组拆分**），TTL(先减1，=0则丢弃 8bits)，上层协议8bits，首部校验和（只算首部，16位相加，每次溢出都要回卷，最后取反码）16bits(每个路由器都要更新，原因TTL变化，有错则忽略)，src/dst IP(32+32bits) IP header20bytes,TCP header 20bytes, data=MTU-40bytes。

**IPv4寻址:** 一个接口一个IP地址 子网内部无路由器，通过交换机可达

**CIDR：**a.b.c.d/x x表示子网部分位数。一个CIDR中可能有好几个子网。如ISP分配给Organization就是一个CIDR下将x增大（层次寻址）。可以从ICANN获取一块IP地址

**DHCP:应用层协议，**获取IP地址。即插即用。允许主机IP地址分配，得知子网掩码、第一跳路由器地址、DNS服务器地址。 **步骤**：1.DHCP发现报文。**UDP分组**，端口67，广播目的地址255.255.255.255，源地址0.0.0.0。 2.DHCP提供报文。目的地址255.255.255.255，包含发现报文的ID，向客户推荐的IP地址，网络掩码，IP地址租用期，第一跳路由器IP地址。 3.DHCP请求报文。客户选择服务器发送请求报文进行响应，回显配置的参数。 4.DHCP ACK报文，服务器对请求报文进行响应，证实所要求的参数。 **每个子网内不一定要有DHCP服务器，可通过中继路由器通信**

**NAT：**1.对于外部只需要一个IP地址 2.内部IP改变不需要通知外部 3.可以随意切换ISP，不需要该内部IP 4.外部不可见，安全

需要实现替换向外发包的src IP，记住内部IP地址，替换向内发包的dst IP地址

争议：路由器应该只处理第3层，端口应该只用来寻址，违背端到端原则

外部想要访问内部IP。1. 静态配置某端口进行特定方向转发 2.动态建立公网IP，port和私有IP，port的映射 3.使用中继

**ICMP：网络层协议**error reporting: unreachable host, network, port, protocol; echo request/reply(ping)。**ICMP在IP之上，被IP承载**。Type8字节，code8字节，造成问题的IP数据报前8个字节。(Type,Code)=(0,0)echo reply, (3.0)dest unreachable, (3,3)dest port unreachable, (8,0) echo request(ping), (11,0) TTL expired, (12, 0)bad IP header

ICMP type11, code0，包含路由器名字和IP地址。Traceroute返回port unreachable(3,3)

**IPv6:**32位IPv4地址分配完。格式：version4bit, priority8bit, flow label20bits, payload length16bits, next header, hop limit, src/dst addr(128+128bits) 40字节首部

Payload length数据字节数量，不包括首部。下一个首部即协议值，如TCP，UDP

**与IPv4区别：**IPv6不允许在中间路由器上进行分片与重新组装，只能在源/目的地址上进行操作。无首部校验和。删除选项。ICMPv6，新消息类型，如Packet too large

**IPv4->IPv6:**1.隧道，IPv6包作为IPv4包的payload。2.双栈，将IPv6包转为IPv4，但是转回来会丢失信息，如flow label

**路由算法：链路状态(link state, Dijkstra)，距离矢量(distance vector, Bellman Ford)** 区别：链路状态掌握全局拓扑信息，链路cost。距离矢量去中心化，掌握邻居信息，和邻居交换信息。当前路由均为负载不敏感。

**链路状态**：松弛，最近节点出队O(VlogV)。缺点：导致振荡，原因是所有节点都同时进行了贪心选择，导致最短路径上阻塞。解决办法，所有节点不同时运行LS算法，Link cost不依赖于交通流量

**距离矢量**：d(x->y)=min{w(x, neighbor v)+d(v->y)}。更新即通知所有邻居。优点：好消息（距离减少）传播速度极快。缺点：坏消息传播的很慢。会导致路由环路，即某个包在两个路由器之间来回跳转（无穷计数）。解决方式：毒性逆转，如果z通过y路由到x，则z通知y：z到x的距离是无穷

**LS与DV比较：**复杂性：LS需要每个节点知道每条边的开销，需要O(VE)条报文，DV只需要邻居交换报文。收敛速度：LS需要O(VE)条报文，DV收敛较慢。健壮性：一个LS节点只计算自己的转发表，具有一定程度的健壮性。DV可能导致错误蔓延至整个网络。

**层次路由：**自治系统AS，每个AS在一个ISP中，一个ISP可能有多个AS。相同AS中路由器跑域内(intra-AS)路由协议。不同AS间的路由器可以跑不同域内路由协议。Gateway router(网关路由器)，AS边沿，有和其他AS的链接。

Intra-AS设置内部目的地址条目，intra-AS和inter-AS设置外部目的地址条目

**域间inter-AS路由任务：**AS1必须学习哪些地址可以由AS2可达，哪些由AS3可达。同时将可达性告知AS1内部所有路由器。

如果某子网由AS2,AS3同时可达，则设置转发端口为最近的网关路由器（hot potato）

如果只有AS2可达，则设置为距离网关路由器最近的端口为转发端口

**域内(intra-AS)路由(IGP):**RIP,OSPF,IGRP

**RIP:** DV算法，每30s与邻居交换信息（advertisement）。路由表：目的子网，下一跳路由器，跳数（包括自身）。Advertise跳数信息

如果180s后没有收到邻居advertisment，则认为邻居/链路dead，并进行更新交换信息。使用毒性逆转防止无穷计数问题。Advertisement UDP packets, 520port

**OSPF:** LS算法，知道全局信息，权重由管理员决定。Advertisements泛洪到整个AS。链路状态改变或者30分钟进行链路信息广播。**IS-IS协议**近似于OSPF

**高级特性**（优点）：安全，消息被身份验证。允许许多相同cost路径。支持多播。**层次OSPF**：骨干网、骨干路由器。两层：局域网、骨干网。区域内advertise，骨干路由器OSPF。Area boarder总结距离其他area距离。Boundary routers与其他AS连接

**域间(inter-AS)路由BGP:** eBGP: 从邻居AS获取子网可达性信息。iBGP:将可达性信息宣传到所有域内路由器。BGP session，两个BGP路由器交换BGP信息，advertising paths to different network prefixes, which can be aggregated in one advertisement. 64/24,65/24,66/24,67/24->64/22 一个AS有独一无二的AS number。Sub AS不一定有AS number。**域内非边界路由器的转发表也由域间路由协议iBGP配置。域间路由协议必须相同。**

BGP属性：AS-PATH，advertisement已经经过的AS NEXT-HOP：ASPATH最近AS路由器IP 使用import policy来接受/拒绝advertisement

**BGP路由**：1.本地性能 2.最短ASPATH 3.最近下一跳路由器 4.其他

BGP消息：OPEN(TCP connection)、UPDATE(advertises new path)、KEEPALIVE(keep connection alive)、NOTIFICATION(report errors, close connection)

BGP advertise让路由器知道前缀。BGP route selection知道最佳域间路由。

Best intra-route to BGP route: 1.NEXT-HOP路由器，使用OSPF获取到NEXT-HOP路由器的最短路径，加入转发表。

**域内域间路由区别：**政策：域间路由管理员想控制路由方式。域内不需要政策。规模：层次路由减少路由表大小。性能：域内路由专注性能；域间路由政策>性能

**解决广播重复**：1.记录广播包2.reverse path forwarding，只对最短路径来的包进行转发 3.生成树，定义中心节点，每个节点发加入信息到中心节点。消息直到遇到已经属于生成树的节点才停止转发。

**多播**：只给一个子网发送包，使用多播IP地址表示一组接受者。多播路由：shared-tree，假设中心节点，发送join信息得到树。Source-based tree，使用RFP(reverse path forwarding)

**链路层**

Hosts,routers->nodes,edge->link(wired, wireless, LANs),datagram->frame

**功能**:framing,link access; reliable delivery(wireless link, high error rate); flow control; error detection; error correction; half-duplex & full-duplex。在网卡中实现，附在host系统总线上，硬件，软件，固件的结合。

发送方：添加错误检测位、rdt、流控制。接收方：检错纠错、rdt、流控制，提取包

**奇偶校验：**偶校验，确保1的数量（包括校验位）是偶数。二维奇偶校验需要在右下角添加1位保证奇偶性

**Checksum:**发送方16位整数数组进行相加，得到checksum，接收方也计算，判断是否相等

**CRC循环冗余校验:**G生成多项式r+1比特，r比特CRC码，D\*2^r xor R应该被G整除。可以检查突发的少于r+1比特的错。计算CRC码，D\*2^r/G，除法使用异或运算得到余数，不需要借位

**多路访问链路和协议：**点到点链路PPP，HDLC协议。广播链路：共享线路或介质。碰撞：同时收到多个信号。

**信道划分协议：**TDMA时分多路访问：使用固定长度的时隙。 FDMA频分多路访问：使用固定频率带。CDMA码分多路访问 **随机接入协议：**有碰撞时延后重发。 **两者区别**：信道划分负载低时浪费多。无碰撞。负载高时高效。随机接入高负载效率低。低负载带宽利用率高。

**时隙ALOHA**：1.所有帧由L bits组成。2.时间被划分为L/Rs的时隙。3.节点只在时隙起点开始传输帧。4.节点同步。5.某时隙发送多帧碰撞，所有节点都能检测到。

有新帧要发送，则在下一个时隙进行发送。如果没有碰撞，则成功，可以发送下一个新帧，否则以p的概率在后面时隙中继续发送。

优点:单一活跃节点持续满速率传输。高度去中心化，只需要时隙同步。简单。 缺点：碰撞、空闲时隙、时钟同步

N个节点有一个节点发送成功概率为Np(1-p)^(N-1)，N趋于无穷，最大效率为1/e=0.37

**纯(无时隙)ALOHA**：无同步，碰撞概率相对时隙ALOHA增加。帧首次到达时，立刻完整地被传输至广播信道。如果一个节点在[t,t+1]进行传输，其他节点不能在[t-1,t],[t,t+1]进行传输，概率为p(1-p)^(2(N-1))，最大效率为1/2e

**CSMA载波侦听多路访问**:说话之前先听：载波侦听；如果与其他人同时说话，则停止说话：碰撞检测。距离和信道传播时延在碰撞检测中起到关键作用。越长则检测到碰撞的几率越小。

**传输流程**：1.网卡从网络层接受数据包，创建帧 2.检测信道是否空闲，忙则等待，空则传输 3.如果没有检测到碰撞，则传输完整个帧 4.检测到其他传输信号，异常中止，发送jam阻塞信号，通知其他基站不要传输 5.异常中止后，进行二进制指数回退。在第m次碰撞后，在0~2^m-1中随机选择K，等待K\*512bits时间，返回第2步。 **效率**：1/(1+5t\_{prop} t\_{trans})

**轮流协议：**轮询polling:使用在dumb-slave设备上（如蓝牙），RR算法。缺点：轮询时延、master故障导致整个信道不可用。令牌传递协议：令牌以固定次序在节点间交换（token ring）。缺点：单节点故障导致信道崩溃。时延。

**Cable access**:上行下行FDM，上行channel继续分为TDM时隙

**局域网**：**48bits MAC地址**，烧写在网卡中。**MAC扁平地址->可移植性 IP层次地址不可移植**。广播地址FF-FF-FF-FF-FF-FF(LAN内)。**使用两个地址IP和MAC原因：保持各层独立。局域网为任意网络层协议设计。如果适配器使用IP地址，则不方便支持其他网络层协议；如果使用网络层地址，则地址需要存储在RAM中，移动需要重新配置。适配器不使用任何地址会导致容易被不应被自己处理的帧中断。**

**地址解析协议ARP**:**IP到MAC的映射**。知道IP获取MAC地址。ARP表项<IP, MAC, TTL>，通常过期时间20min。是即插即用的协议 流程：1.A想发数据报给B，但是没有MAC地址 2.A发送arp广播包包含B的IP地址 3.B收到arp包后回复MAC地址 4.A保存该表项。

**发送数据报到子网外**：A->router R->B, A创建IP数据报(src A, dst B)，链路帧(src A, dst R receive interface MAC)发送到R，R提取datagram上传至网络层处理，进行转发，然后在链路层创建链路帧(src R send interface MAC, dst B) **以太网**：mid90s，总线；至今，星状结构。中间从集线器hub到交换机

**以太网帧结构**：前同步码(8bytes)，dst/src MAC addr(6+6bytes), type(2bytes), data(MTU), CRC(4bytes)。前同步码：7bytes10101010+1byte10101011，用于同步收发双方时钟频率

不可靠（丢了就是丢了）、无连接（不握手），CSMA/CD+二进制指数回退

**交换机**：存储转发以太网帧。每条链路无碰撞、**全双工**（可以同时互发消息，半双工不能同时互发消息）。使用CSMA/CD协议。每个交换机有交换表，表项格式为<MAC, interface, time stamp>。 功能：过滤、转发。

**即插即用，具有自学习功能**：从某interface收到帧时，就学习到一个表项。对于不知道的目的MAC，进行泛洪flood操作。如果目的MAC地址找到了，且对应接口不是接收接口，则转发，否则丢弃。

**Router V.S. Switch**:都是存储-转发，都有转发表。路由器在网络层，交换机在链路层。路由器通过路由算法和IP地址得到路由表，交换机通过泛洪、自学习、MAC地址得到转发表。

|  |  |  |  |
| --- | --- | --- | --- |
|  | Hubs | Routers | Switches |
| Traffic isolation | No | Yes | Yes |
| Plug and play | Yes | No | Yes |
| Optimal routing | No | Yes | No |

**VLAN**:动机：一台物理交换机=一台逻辑交换机导致缺乏流量隔离，交换机无效使用（很多端口不能用），管理用户困难。

通过一个将一个物理交换机从一个逻辑交换机变成两个或多个逻辑交换机解决上述问题。

**Ported-based VLAN**:一个路由器的两个接口分拆路由器。对于交换机之间互联，使用VLAN干线连接(trunking)方式，即通过一根线连接两个交换机端口。通过802.1Q协议进行干线通信。802.1Q帧由标准以太网帧+加进首部的4字节VLAN标签组成。VLAN标签由发送方交换机加入，接收方交换机删除。VLAN标签由2字节标签协议标识符和2字节标签控制信息字段和3bit优先权字段组成，CRC需要重新计算。

**链路虚拟化**：**MPLS**多协议标签交换，2.5层协议。通过固定长度标签，改善IP路由器的转发速度。标签交换路由器通过查找MPLS标签进行转发。操作都没有接触IP首部。**允许相同目的IP地址走不同路径**。

**以太网上网**：1.主机发DHCP广播包获得IP地址。2.使用DNS获取网站IP地址，但是在链路层使用ARP获得第一跳路由器MAC地址，发给路由器，然后再路由转发给DNS server（这里使用了RIP，OSPF，BGP创建的转发表）。3.使用TCP SYN和SYNACK建立TCP连接进行HTTP数据通信。4.TCP FIN结束通信

**无线网络和移动网络**

**两大挑战**：无线、移动

**元素**：host，基站BS（连接到有线网，蜂窝塔，802.11AP），无线链路wireless link（用于连接移动设备至基站或另一台无线主机、骨干网连接）。

**基础设施模式**：与基站关联。**自组织网络**：没有基础设施。 改变切入点称为**切换**。

单跳、有基础设施：host<->base station WiFi。单跳、无基础设施：蓝牙802.15 、ad hoc nets。多跳、有基础设施：依赖几个无线节点连接到更大网络mesh net。多跳、无基础设施：移动自组织网络MANET、车载自组织网络VANET

**无线链路特征**：1.递减信号强度（路径损耗） 2.来自其他信号源的干扰 3.多径传播（反射等）

**信噪比**：10log\_10 (P\_{signal}/P\_{noise})。比特差错率BER：对于给定物理层，信噪比越高，误码率越低。对于给定信噪比，比特传输速率越高，BER越高。

**隐藏终端问题**：B可以听见A，C，由于信号衰减，AC相互不能听见。CSMA/CD无法工作。

**使用CDMA解决**：信道划分协议。每个用户有独自的CDMA code。编码信号=原始数据\*CDMA code，解码=编码信号\*CDMA code取平均。

**802.11**：标准：802.11b a g n ax(Wifi6)

基本构建模块：基本服务集BSS。一个BSS包含一个或多个无线站点，以及一个称为接入点AP的中央基站。配置AP的无线LAN是基础设施无线LAN。

**安装AP**时，管理员为AP分配服务集标识SSID。还分配一个信道号。802.11运行在2.4~2.4835GHz频段。在频段中定义了11个部分重叠的信道。两个信道由4个或更多信道隔开时才无重叠。1,6,11无重叠。信道干扰有可能发生。

Host必须**与AP相关联**：host扫描信道，监听信标帧beacon frame，其中包含AP的SSID和MAC地址。选择一个发送关联请求帧。AP返回关联响应帧。可能需要认证。使用DHCP获取IP地址。

**被动扫描**：扫描信道，监听信标帧。**主动扫描**：向无线主机范围内AP广播探测请求帧。AP回复探测响应帧。然后host再选，AP再回复。主动扫描需要二次握手。关于验证，一种是基于MAC地址，一种是基于用户名和口令。

**CSMA/CA**:避免碰撞。传输前先检测是否有传输。没有碰撞检测机制。

802.11使用**链路层确认**检测帧是否无损到达目的地。目的站点（接收方）在收到帧后，等待短帧间间隔SIFS，然后回复ACK帧。

**CSMA/CA过程**：1.某站点检测到信道空闲，在分布式帧间间隔DIFS后发送该帧。 2.否则，选取随机回退值，并且在监听到信道空闲时递减该值，当信道忙时，计数保持不变。3.计数减为0时，发送整个数据帧并等待确认。4.收到确认则表明正确接受。要传输另一帧则从第二步开始循环。如果没有收到，则重新进入第二步，而且随机数范围更大。

使用链路层ACK原因：难以检测碰撞。接收方发ACK如果没有碰撞。

**链路层ACK不能避免碰撞**，两个主机可能互为隐藏终端，两个站点可能选择的回退值相近导致碰撞。

**避免碰撞**：允许发送发预留信道而不是随机访问。避免长数据帧的冲突。使用**短请求发送RTS和短请求允许CTS**控制帧预约信道。1.发送方发长数据，先向AP发送RTS，AP广播CTS帧给发送方明确的发送许可，同时指示其他站点在预约期不要发送。RTS帧仍然会碰撞。RTS/CTS交换引入时延，消耗信道资源，因此只用于长数据帧预约信道。

**802.11帧**：addr1接收者MAC，addr2发送者MAC，addr3第一跳路由器MAC。包含CRC码。Addr4只用在adhoc模式中。

路由器R1知道Host1的IP地址，通过ARP获取Host1的MAC地址。802.3帧发给AP，AP转成802.11帧发给H1，H1回复802.11帧，AP再转成802.3帧回复给R1。

Frame Type(RTS,CTS,ACK,data),WEP加密是否使用，duration持续时间，seq control序列号。通过序列号区别重传帧和新帧。

**相同IP子网内的移动性**：可以保持IP地址与TCP连接。通过交换机自学习构建新转发表。

不同子网移动需要新IP地址（如果没有mobile IP）

**高级特性**：速率适应 功率管理AP为睡眠主机缓存帧，以后再传输

802.15：个人域网络。Ad hoc模式，没有基础设施。蓝牙

**移动性**：归属网络home network，归属代理home agent，永久地址permanent address，家网络中的地址。Care-of-address COA转交地址/外部地址，visited network外部网络，foreign agent外部代理，correspondent通信者

**注册**：外部代理向归属代理注册COA

**间接路由：**通信者将数据报寻址到移动节点的永久地址，移动性对通信者**透明**。步骤：1.通信者寻址永久地址。2.归属代理封装原始数据报发送给外部代理。Dst需要被封装成COA。3.外部代理接收并拆封数据报发给移动节点。4.移动节点直接回应通信者。

缺点：存在三角路由问题，在通信者和移动节点同处一个网络时不高效。

**直接路由：**1.通信者代理首先询问归属代理知道移动节点COA。2.通信者直接通过隧道技术发往移动节点的COA。克服了三角路由问题。对于通信者来说不透明。通信者代理必须知道移动节点的COA。

使用**锚外部代理**解决新外部网络问题。当移动节点移动到新外部网络时，新外部代理提供给锚外部代理新COA。当锚外部代理收到封装数据报时，可以转发给新外部代理。

**间接路由V.S.直接路由**：间接路由是透明的。直接路由更高效。间接路由只需要将新COA告诉home agent即可。直接路由比较复杂。

**移动IP**：间接路由，代理发现，向归属代理注册。

代理通过代理通告(advertisement，ICMP)通告服务。代理注册：1.foreign agent发送ICMP代理通告告知COA。2.移动节点向外部代理发送注册请求报文，包含永久地址和归属代理IP地址。3.外部代理向归属代理发送注册请求报文，包含COA。4.归属代理接收验证绑定IP和COA并返回注册回答报文。包含实际注册时间。5.外部代理接收回答并转发给移动节点。

**无线和移动性对高层协议影响**：丢包、延迟、TCP拥塞控制、带宽限制。

**个人域网络**：802.15.1无线个人域网络。蓝牙

**网络安全 原则**：保密、认证真实性、信息完整性

**攻击框架：**唯密文攻击、已知明文攻击、选择明文攻击

**对称密钥体系**：m=Ks(Ks(m)) 多码代替密码，多个密码本轮换。

**块密码**：分块加密，组合置乱，然后循环。

**密码块链接CBC**：从左往右加密。初始向量c0=IV c(i)=Ks(m(i) xor c(i-1)) 解密m(i)=Ks(c(i)) xor c(i-1)

DES 64bit blocks with 56-bit key AES 128-bit blocks with 128, 192, 256 bits long key 3DES三次DES

**公钥加密体系**：公钥加密，只有私钥能解密，私钥加密，公钥都能解密。

**RSA**：1.大素数p，q，n=pq，z=\Phi(n)=(p-1)(q-1)。2.小于n的数e与z互质。求d使得ed-1被z整除。3.公钥(n,e),私钥(n,d)。4.公钥加密即算m^e同模n的结果c。5.解密即算c^d同模n的结果。原理：欧拉定理。速度慢

可以用公钥加密会话秘钥Ks（对称秘钥）

**端点鉴别**：中间人攻击ap1.0:m -> m ap2.0 IP,m -> IP,m ap3.0 IP, passwd, m -> IP, passwd, m ap3.1: IP, encrypted passwd, m -> IP, encrypted passwd, m

Ap4.0: 使用nonce只会有一次出现的数字。

Ap5.0: m, KA-,KA+ -> m, KT-, KT+转发信息即可，替换私钥公钥

**信息完整性**：使用报文摘要H(m)，checksum不适合做hash函数，因为容易发生冲突。MD5算法通过4步得到128bit散列，SHA-1是美国标准，160bits，也被使用。使用鉴别秘钥s防止被中间人替换消息，H(m+s)成为报文鉴别码(MAC)，可以验证信息完整性。

**数字签名**：KA-(H(m))，为防止数字签名计算开销过大，加入哈希函数将原消息进行哈希，使用KA-(H(m))减少计算量。有完整性和鉴别性。

**公钥认证**：为防止ap5.0漏洞，需要公钥认证。认证中心CA认证公钥，通过KCA-(KB+)对公钥进行证书化。公钥与实体绑定。

**安全邮件**：A->B发邮件。KB+(Ks)发送对称秘钥。Ks(m, KA-(H(m)))提供报文完整性、发送方鉴别功能。 **PGP**几乎和前面一致。

**SSL**：应用层协议，在传输层和应用层间添加SSL层。阶段：1.建立TCP连接。2.验证是否是Alice，通过SSL Hello，Alice需要发送证书。3.发送给Alice主密钥EMS=KA+(MS)。MS为该SSL会话的主密钥。4.秘钥导出：由MS导出4个秘钥EB:Bob->Alice的会话加密秘钥 MB:Bob->Alice的会话MAC秘钥 EA:Alice->Bob的会话加密秘钥 MA:Alice->Bob的会话MAC秘钥s。5.数据传输：中间人可以进行删除或重放导致缺数据或者数据次序错误。解决：使用序号。Bob->Alice。Bob自己维护一个计数器记录序号，从0开始，不在数据报中直接体现，但是包含在MAC的计算中。Alice通过计算MAC得知是否被篡改，所以SSL中MAC是Hash(MB, data || seq || type)。**使用seq阻止重排与一个会话中的重放攻击，使用nonce阻止**连接重放**攻击。**将type也加入防止将类型篡改为TCP connection close,1表示关闭，0表示数据。

**SSL握手**：1.client发送支持的密码算法列表，包括一个client不重数。2.server在列表中选择一个对称算法、公钥算法和MAC算法，将选择、证书、server不重数返回给client。3.client验证证书，获取server公钥KS+，生成前主密钥PMS，将KS+(PMS)发给server。4.使用相同密钥导出函数，client和server独立从PMS和不重数中计算出主密钥MS，然后将MS切片得到两个密码和两个MAC密钥。当选择的对称密码应用于CBC，则两个初始化向量IV也从MS中获得。自此以后，client和server间所有报文均被加密和鉴别。5.client发送所有握手报文的一个MAC。6.server发送所有握手报文的一个MAC。最后两步可以防止握手被篡改。

**SSL结束**：在类型字段指出是否终止SSL会话。TCP FIN不代表终止。

**IPSec**：鉴别首部AH协议、封装安全性荷载ESP协议。AH提供源鉴别和数据完整性服务，不提供机密性服务。ESP都提供。安全关联AS是单工连接。1个总部和n个saler需要2+2n个SA。总部网关路由器R1需要维护：SA的32bit标识符，称为安全参数索引SPI。2.SA的初始接口和目的接口。3.将使用的加密类型。4.加密密钥。5.完整性检查的类型。6.鉴别密钥。一个IPSec实体在安全关联数据库中存储所有SA的状态信息，SDA的数据结构。

数据报形式：隧道模式（更安全，对IP和payload都安全，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。）、运输模式（只对payload安全，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。） **IPSec工作在主机和路由器上，在网络层上。有连接。**

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

**WEP主机鉴别**：ci=di xor ki（ki为初始向量分量）

802.11i增强的安全性，使用各种加密算法，提供密钥分发机制，使用专门鉴别服务器提供鉴别服务。

防火墙：包过滤防火墙（逐包过滤）、状态检测防火墙（跟踪TCP连接状态）、应用网关（检查应用层数据）