[illegible]

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$D_x(y)$,这些代价构成了自己的距离矢量 $D_x = [D_x(y): y \in N]$;每个节点周期性地将它的距离矢量D_x发送给邻居;节点 x 拥有每个邻居 v 的距离矢量$D_v = [D_v(y): y \in N]$;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:$D_x(y) \leftarrow min_v\{c(x,v) + D_v(y)\}$. ***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$d_p(y)$. 节点仅在发现距离矢量$d_x(y)$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,若节点 Z 经 Y 到 X,向 Y 通告距离矢量,将$D_Z(X)$设为无穷大,阻止 Y 使用这条路由】. ***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,$O(N^2)$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(Autonomous System):***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 由 ICANN 分配一个 AS 编号;将路由器组织到一系列 AS 中称域.同一个 AS 中的路由器运行相同的选路协议(称 Intra-AS 域内选路协议);不同 AS 中的路由器可以运行不同的 Intra-AS 选路协议. ***网关路由器:***在一个 AS 内、直接连接到其它 AS 的路由器;网关路由器之间运行 **Inter-AS** 域间选路协议,所有 AS 必须运行相同的 Inter-AS 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定义、报文格式、报文传输、报文处理、异常处理等问题.***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. **域内选路** Routing Information Protocol 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). **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),通常选取不随负载改变的链路特性为代价.. ***OSPF 分组:***OSPF 协议定义了 5 种分组类型,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,可以同时使用多条费用相同的路径,对单播和多播路由选择的充分支持. **Inter-AS 的任务*:***AS1 内部的路由器需发送数据报到 AS1 外,AS1 的网关路由器必须了解哪些目的网络通过自己可达以及将可达性信息传播到 AS1 内部的所有路由器. ***热土豆路由选择:***AS 尽可能快地扔掉分组,这通过让路由器向最近的域内网关路由器发送分组来完成,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路由器到网关代价. ***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. **域间选路: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 Border Gateway Protocol:每个子网可以发布自己的存在,***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***. 不同 AS 的两个边界路由器之间建立的 BGP 会话,称为***外部 BGP(eBGP)会话***;一个 AS 可能有多个边界路由器,这些边界路由器必须通过半永久 TCP 连接构成全连通,它们之间的 BGP 会话称为***内部 BGP(iBGP)会话***. ***BGP 定义了 4 类报文:*****打开报文,保活报文**告知自己处于工作状态,**通知报文,更新报文**. ***可达性信息(路径广告):***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.*** 例:AS3,X. AS2,AS3,X. ***基于策略的路由:***根据输入策略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),可能丢弃/按原样接受/接受但修改某些属性(如偏好度);对于每一个目的前缀,从所有可达的路径中按照 BGP 指定的决策顺序确定一条最佳路由;根据输出策略,决定是否向某个邻居发布某条路径. ***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;Inter-AS 选路协议用于在不同 AS 之间交换选路信息,如 BGP,主要依据策略而不是路由测度去寻找可达路径(不追求最佳路径). ***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). ***广播和多播选路*** ***广播选路(broadcast routing):***网络层提供了从一种源节点到网络中的所有其他节点交付分组的服务;***多播选路(multicast routing)***使单个源节点能够向其他网络节点的一个子集发送分组的副本. **广播路由选择算法:**在**源节点上复制分组:N 次单播**低效:相同的分组在某些链路上可能重复传输,需其它机制支持:源节点需知道所有目的节点的地址. ***理想的广播选路:***源节点不需知道其它节点的地址,只需将分组的目的地址设置为广播地址,路由器负责转发到全网(在网络中复制分组);网络中产生的分组拷贝最少. ***在网络中复制分组:洪泛(flooding):***节点收到广播分组后,向所有邻居节点(除分组到来的链路外)发送该分组的拷贝;缺点:在有环的网络中,广播分组在网络中无休止地循环,浪费资源. ***受控洪泛:***目标:每个路由器仅转发它之前未转发过的广播分组;***两种方法:***节点记录之前转发过的分组 ID,不重复转发分组(OSPF 使用此方法:源地址+分组 ID);**反向路径转发:**利用节点内部的单播转发表,仅转发从本节点->源节点的最短路径的反向路径上到来的广播分组(该方法使用最多). ***反向路径转发 Reverse Path Forwarding:***当广播分组到达路由器时,路由器检查分组的源地址与输入端口;用分组的源地址查找单播路由表,找到去往该源地址的输出端口;若分组的输入端口与去往该地址的输出端口相同,则扩散该分组,否则丢弃分组;优点:算法合理、易于实现且开销不大. ***生成树方法:***使用生成树转发广播分组:路由器知道自己的哪几个端口在生成树上;当从一个端口收到广播分组后,只在属于生成树的其它端口上转发该分组;***基于生成树的广播不会产生冗余的分组拷贝***. ***生成树的构造:基于核心的方法:***选择一个节点作为核心(也称汇聚点);其它节点向核心发送单播的加入报文:路由器利用单播转发表向核心转发加入报文时,记录报文的输入端口及输出端口,这些端口就是位于生成树上的端口;当加入报文到达生成树上的一个节点时,报文经过的路径被添加到生成树上. **多播:** ***如何标识多播通信的接收者:***因特网为这组接收者分配一个标识(多播组标识),使用 D 类地址作为多播组标识;***如何设置多播分组的接收者:***将分组的目的地址设置为其接收者的多播组地址;***如何将接收者的 IP 地址与多播组地址 关联起来:***接收者的 IP 地址与多播组地址无关,接收者可以在任何时候加入或离开一个组,***多播组管理协议(IGMP)***允许主机向本地路由器申请加入或离开一个组;***如何将多播分组交付给每一个接收者:***多播选路协议协调多播路由器建立到达所有接收者的路径树. ***多播路由选择算法:目标***为每个组建立多播转发树(到达该组所有成员的路径树),每个组成员应当只收到多播分组的一个拷贝,非本组成员不应收到多播分组,从源节点到每一个组成员节点的路径应当是最佳的(最短路径). ***建立多播树的两种方法:基于源的树:***源节点建立一棵到多播组所有成员的最短路径树,源节点 S 和组 G 的每一种组合<S,G>构成一棵树,多播路由器必须有每棵<S,G>树的信息,根据多播分组的<S,G>确定使用哪棵多播树,优点:总是使用最佳路径转发多播分组,缺点:路由器需要维护大量的多播树信息. ***组共享树:***每个多播组使用一棵树,树根为该多播组的核心,源节点先将多播分组发送给核心,核心再在多播树上发送. 优点:对于每个组,多播路由器只需维护一棵多播树;缺点:多播分组使用的路径可能不是最佳的. ***基于源的树:最短路径树:***MOSPF 扩展了 OSPF 协议,参与多播主机定期通报所属多播组,将多播组集合作为链路状态广播. ***基于源的树:距离矢量多播选路:***扩展 RIP 协议实现多播选路的困难:除边缘路由器外,其它路由器不知道多播组(及其成员)的存在;***DVMRP 采用广播+剪枝的解决办法:反向路径转发:***确保多播分组到达每一个局域网;路径剪枝:路由器删除不包含组成员的路径分支. ***组共享树:基于核心的树:***指定一个路由器作为组 G 的核心,所有路由器知道该核心所属的组及单播 IP 地址(需要其它的机制),多播路由器向核心发送单播加入报文,当报文到达核心或已在树上的节点时,报文经过的路径加入到树中. ***如何利用组共享树发送多播分组?*** 当源节点想要发送多播分组时:源节点将多播分组发送给核心,核心在多播树上发送;***多播分组如何到达核心?*** 多播分组的目的地址为 G,从源节点到核心的路径上,可能有路由器不在多播树上(不知道如何转发);建立隧道:源节点将多播分组封装到一个单播分组中,单播分组的目的地址为核心的单播地址. ***最广泛使用的因特网多播选路协议是 Protocol Independent M:***不依赖于网络中所使用的单播选路协议. **PIM 有两种模式:**稠密模式:许多或大多数路由器涉及多播选路过程,使用广播+剪枝方式建立多播树;稀疏模式:只有很小一部分路由器涉及多播选路过程,采用组共享树的方法;当源节点流量很高时切换到源树. ***多播分组穿越单播网络:***因特网中只有一小部分路由器是多播路由器,多播分组在从一个多播路由器传递到另一个多播路由器时,通常需要穿越单播网络;在多播路由器之间建立隧道:把多播分组封装在单播分组中传输. 因特网中的多播路由器以及这些多播路由器之间的隧道,构成了***因特网多播骨干网***. **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 报文是作为 IP 有效载荷承载的,跨网络传输必须封装在 IP 包中传输,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. ***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(该目的主机向源发送一个端口不可达的 ICMP 报文). ***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.

第六章 链路层和局域网

网络层和链路层的关系:网络层选路(路由器确定去往目的节点的下一跳),**转发**(在路由器内部将数据报从输入端口转移到输出端口);***链路层将数据报从一个节点传输到相邻的下一个节点***. ***链路层概述:节点:***主机/路由器. ***链路:***连接相邻节点的通信信道. ***帧:***链路层分组称为***链路层帧***. **链路层服务:组帧(基本服务)**(发送,将数据报封装到帧中;接收,从原始比特流取出完整帧);**链路接入**(广播链路需要)在广播信道上协调各个节点的发送行为;**差错检测(基本服务)**检测传输错误;**差错纠正(有些提供)**:检测并纠正传输错误(不使用重传);**可靠交付(部分协议提供)**通过确认、重传等机制确保接收节点正确收到每一个帧(停-等、GBN、SR),低误码率链路(如光纤、某些双绞线)上很少使用,高误码率链路(如无线链路)应当使用;**流量控制:**调节发送速度,避免接收节点缓存溢出(提供可靠交付的链路层协议,不需要专门的流量控制),不提供可靠交付的链路层协议需要流量控制机制;**半双工和全双工:**半双工通信时,提供收/发转换. **链路层在何处实现: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,(可选)执行可靠传输和流量控制;***接收侧:***提取帧,检测传输错误,(可选)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,随机信道热噪声;突发差错,瞬间脉冲噪声,突发长度表示最大影响数据位数. ***差错控制编码的类型:检错码.***只能检测出传输错误的编码,不能确定出错位置,通常与反馈重传机制结合进行差错恢复;***纠错码.***能够确定错误位置并自行纠正的编码. ***差错检测的实施:***码字由m比特数据加r比特冗余位构成,有效编码集由2^m个符合编码规则的码字构成,若收到码字无效,检错.纠错码可将收到的无效码字纠正到距其最近的有效码字. 检错与纠错能力有限,*编码集的海明距离*为任意两有效码字海明距离最小值,为检错d比特,编码集海明距离至少为$d+1$,为纠正d比特,编码集海明距离至少为$2d+1$. **奇偶校验:** ***单比特奇偶校验:***可检测奇数比特错误,检错率 50%,编码集海明距离为 2. ***二维奇偶校验:***可*检测 2 比特错*和*纠正单比特错*有利于检测突发错误,编码集海明距离为 3. **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,避免往返时延. **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. ***为什么运输层使用检验和而链路层使用 CRC:***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. **循环冗余校验(CRC):** ***多项式编码***,将一个比特串看成是某一元多项式系数. **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. **编码方法:*$R = M \cdot x^r / G$的余式(减法运算定义为异或操作)*.** **检验方法:**若生成的编码$T = (x^r \cdot M + R)$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,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. ***多路访问协议: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:**连接了许多节点的单一共享链路,任何一个节点发送的数据可被链路上的其它节点接收到. ***冲突(collision):***在广播链路上,若两个或多个节点同时发送,发送的信号会发生干扰,导致接收失败. ***多址接入协议(多路访问协议):***规定节点共享信道(谁可以发送)的方法,多址接入协议也称***媒体接入控制(Medium Access Control)协议***. ***理想的多址接入协议:***在速率为R bps 的广播信道上当只有一个节点发送时,它应能以速率 R 发送(信道利用率高)当有 M 个节点发送时,每个节点应能以 R/M 的平均速率发送(公平性好、信道利用率高)协议是无中心的,不需要一特殊节点来协调发送(健壮性好),不需要时钟或时隙同步(不需要额外的机制)简单(实现和运行开销小). ***MAC 协议的分类:信道划分:***将信道划分为若干子信道,每个节点固定分配一个子信道,不会发生冲突;关注公平性,轻负载时信道利用率不高;***随机接入(竞争):***不划分信道,每个节点自行决定何时发送,出现冲突后设法解决,轻负载时信道利用率高,重负载时冲突严重;***轮流使用信道:***不划分信道,有数据的节点轮流发送,不会出现冲突,信道利用率是以上两种方法的折衷,需引入额外机制. **信道划分协议:** ***TDMA(时分多址)***将信道的使用时间划分成帧,每个节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,节点只能在分配给自己的时隙内发送,若节点不发送,其时隙轮空. ***FDMA(频分多址):***将信道频谱划分为若干子频带,每个节点被分配一个固定的子频带(**R/N 带宽**),若节点不发送,其子频带空闲. ***TDM 和 FDM 的优劣:***消除碰撞而且非常公平;(节点被限制于 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),每个节点被分配一个惟一的 m 比特码序列(称 chip code);**发送方编码:**发送"1"=发送 chip code,发送"0"=发送 chip code 的反码;**信号叠加:**多个节点发送的信号在信道中线性相加;**接收方解码:**用发送方的 chip code 与信道中收到的混合信号计算内积,恢复出原数据;**前提条件:**任意两个 chip code 相互正交;CDMA 允许所有节点同时使用整个信道. **随机接入的 MAC 协议:**当节点有数据要发送时,以信道速率 R 发送,发送前不需要协调;**随机接入 MAC 协议**规定如何检测冲突,以及如何从冲突中恢复. ***时隙(Slotted)ALOHA:***假设所有帧长度相同;时间被划分为等长时隙,每个时隙传一帧;节点只能在时隙开始时发送;节点时钟同步(知道时隙何时开始);所有节点可在时隙结束前检测到是否有冲突发生. **操作:**节点从上层收到数据后,在下一个时隙发送;若时隙结束前未检测到冲突,节点可在下一个时隙发送新帧;若检测到冲突,节点在随后的每一个时隙以概率 P 重传,直至发送成功. **优点:** 单个活跃节点可以信道速率连续发送,分布式:节点自行决定什么时候发送,简单. **缺点:**发生冲突的时隙被浪费了,由于概率重传有些时隙被闲置,需要时钟同步. **时隙多路访问协议的效率:**当网络中存在大量活跃节点总有帧发送时,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 个活跃节点,每个节点在每个时隙开始时以概率 p 发送;某节点在一时隙中发送成功概率=$p(1-p)^{N-1}$;某时隙有节点发送成功的概率=$Np(1-p)^{N-1}$;最大效率为令$Np(1-p)^{N-1}$最大的概率p^*;代入$Np*(1-p*)^{N-1}$,令 N 趋向于无穷,得到最大效率 1/e 约 37%. ***纯 ALOHA:*****取消同步时钟**,任何节点有数据发送就可以立即发送,节点通过监听信道判断本次传输是否成功,若不成功,立即以概率 P 重传,以概率(1-P)等待一个帧传输时间后再决定. **发生冲突的情形:**在时刻t_0发送的帧与在$[t_0-1, t_0+1]$时段内发送的其它帧冲突. **纯 Aloha 的效率:**P(某节点发送成功)=P(节点发送)*P(无其它节点在$[t_0-1, t_0]$内发送)*P(无其它节点在$[t_0, t_0+1]$内发送)=$p(1-p)^{N-1}(1-p)^{N-1} = p(1-p)^{2(N-1)}$;求出令节点发送成功概率最大$p^*$,并令$N \to \infty$: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);***冲突仍可能发生:***由于存在端到端信道传播时延,节点可能没有监听到其它节点正在发送;即使忽略传输延迟,当两个(或多个)节点同时发现信道由忙变为空闲、并都决定立即发送时,仍会发生冲突. **碰撞检测**,即当一个传输节点在传输时一直在侦听此信道,如果它检测到另一个节点正在传输干扰帧,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. ***CSMA/CD (Collision Detection):***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. **早期以太网采用 CSMA/CD 协议:**网卡从网络层接收数据报,构造以太帧;若网卡监听到信道空闲,立即发送帧;若信道忙,坚持监听直至发现信道空闲后发送帧;若网卡发送完整个帧而没有检测到冲突,认为发送成功;若网卡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);中止传输后等待一个随机时间量(**指数回退**)然后返回监听. ***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,节点随机地从$\{0,1,2,3,\ldots,2^n-1\}$中选择一个 K 值,对于以太网(最小帧长 512bit),一个节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节点能够立刻插入一次成功的传输. ***CSMA/CD 效率:***T_{prop}=以太网中任意两节点间传播延迟最大值;T_{trans}=最长帧传输时间;**efficiency=1/(1+5T_{prop}/T_{trans})**. **在以下情况下,以太网的效率趋近于 1**:T_{prop}趋近于 0,或T_{trans}趋向于无穷. **结论:**应控制以太网的规模. **轮流 MAC 协议:ALOHA 和 CSMA 协议在单个节点活跃时效率高,但多个节点活跃时效率低.** ***轮询协议:***节点之一被指定为主节点,主节点循环轮询每个节点,告诉它能够传输的帧的最多数量. **优劣:**消除了碰撞和空时隙,使得轮询取得高得多的效率;缺点是引入了轮询时延,即通知一个节点"它可以传输"所需的时间,若只有一个节点活跃,传输速率小于 R bps;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:***没有主节点,**令牌(token)**小的特殊帧在节点之间以固定次序进行传递;节点收到令牌时发送最大数目帧,发送后立即释放令牌. **优劣:**令牌传递是分散的,并有很高的效率;一个节点(令牌)的故障可能会使整个信道崩溃;如果一个节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,节点公平使用信道;轻负载下低效:即使只有一个活跃节点也只能使用 1/N 的带宽. **随机接入 MAC 协议:**轻负载时高效:单个活跃节点可以使用整个信道;重负载时低效:频繁发生冲突,信道使用效率低. **轮流协议(试图权衡以上两者):**按需使用信道(避免轻负载下固定分配信道的低效);消除竞争(避免重负载下的发送冲突). ***交换局域网:局域网 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 Metropolitan Area Network*** 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 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 字节;由 IEEE 负责分配,每块适配器地址全球唯一: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;可以用软件改变网卡的 MAC 地址. 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 IP 层次结构相反)**,IP 可以在因特网范围内快速确定网络接口的位置,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:**全 1. **网络适配器仅将发送给本节点的帧交给主机**:目的地址为适配器 MAC 地址的单播帧,所有广播帧,指定接收的多播帧;若设置为混收则转交所有帧. 主机和路由器接口除了网络层地址之外还有 MAC 地址**原因**:先有 MAC 后有 IP,MAC 地址扁平,无法快速确定接口位置,IP 地址有结构,可以快速确定接口位置.IP 地址与所在子网有关与网卡无关.MAC 地址与网卡有关与所在子网无关. 为了使网络体系结构中各层次成为极为独立的构建模块,不同的层次需要有它们自己的寻址方案. ***如何实现直接交付?*** 当发送节点 A、接收节点 B 位于**同一个子网络**上时,数据报可**从 A 直接交付给 B**:A 的网络层将数据报及 B 的 MAC 地址交给适配器(链路层);适配器将数据报封装在一链路层帧中,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. ***发送节点获得接收节点的 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)***用于动态获得 IP 地址-MAC 地址映射. **在以太网(硬件类型 1)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(操作 1),在发送方字段填入自己的 MAC 地址和 IP 地址,在目标字段填入 B 的 IP 地址;**2.** A 将 ARP 请求封装在广播帧中发送;**3.** 每个收到 ARP 请求的节点用目标 IP 地址与自己的 IP 地址比较,地址相符的节点进行响应(B 响应). **4.** B 构造一个 ARP 响应(操作 2),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 表:***每个节点在内存中维护一个 **ARP 表**;每次发送数据报前先查询 ARP 表,若找不到则发送 ARP 请求,并在收到 ARP 响应后将地址映射缓存起来;ARP 缓存中的信息,在超时(一般为 15~20 分钟)后删除. ***主动学习:***从 ARP 请求中获取地址绑定信息:每个节点可以收到全部的 ARP 请求报文,可将发送节点的地址映射缓存到自己的 ARP 表中;节点 A 在启动时主动广播一个 ARP 请求,在目标字段内填入自己的 IP 地址,收到 ARP 请求的节点将 A 的地址映射缓存起来,若 A 收到 ARP 响应,报告 IP 地址重复错误. **ARP 即插即用**,ARP 表是自动建立的. **ARP 跨越链路层和网络层边界两边的协议**. ***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 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 R-1 对应的 MAC 地址(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:**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. ***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),所有节点通过特殊接口连接到这条总线上. ***物理星形拓扑:***集线器(hub,物理层)(1990s 后期):一

[illegible]

中,节点侦听到信道空闲后随机回退(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:***Address1:帧的目的 MAC 地址; Address2:帧的源 MAC 地址;Address3:连接 AP 的路由器接口的 MAC 地址;Address4: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 address1=AP MAC,address2=H1 MAC,address3=R1 MAC,发给 AP;AP 将这个 802.11 帧转换为 802.3 帧(有线),后者 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,对于固定网络设备不可见. ***其他字段预约传输时间(RTS/CTS),帧序号(ARQ),帧类型(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 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. 若主机停留在同一个 IP 子网中,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移动,切换过程中产生延迟及丢包,在上层协议看来正常. **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);**实现:**两帧无 ack,回落到下一个较低的速率;有 10 帧被确认或回落定时器超时,恢复. ***功率管理:*****节点设置功率管理比特,告知 AP 它将进入休眠状态:**节点进入休眠,并在下一个信标帧之前醒来;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),并使用新地址通信,不能保留原 IP 地址. 当终端改变 IP 地址后,终端上正在运行的应用将中断:通信对方不知终端新地址,无法与其通信;即使对方获知终端新地址,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". **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. **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. **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:**移动节点在外地网络上的地址. **通信者:**希望与移动节点通信的节点. ***移动节点注册:***移动节点进入外地网络后,通过外地代理向归属代理注册,归属节点记录移动节点的外地地址. **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;外地代理收到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,移动节点的位置对于通信者透明);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**对通信者都透明,**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,并获知移动节点转交地址(此步以后不必再做);通信者将包发给外地代理;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***克服了三角选路的问题;但对通信者不透明(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:*****支持移动性的因特网体系结构与协议.具有**归属代理,外地代理,永久地址,转交地址,移动节点注册;**标准化三部分: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,宣布自己存在及 IP 地址;愿意充当外地代理的路由器在代理通告中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,以获取移动节点永久地址对应的 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节点直接可达,于是查找 ARP 缓存或者发送 ARP 请求,利用得到的 MAC 地址封装数据报,发送. ***数据报如何能被归属代理得到?*** 链路层帧的目的地址必须是归属代理的 MAC 地址;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;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(将移动主机永久地址关联到归属代理 MAC 地址),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. 将目的地址在归属网络的数据报送达外地网络:不能修改目的地址=转交地址(转交地址为外地代理的 IP 地址,但实际目的应是移动节点);**应使用隧道** ***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. ***外地代理如何转发数据包到移动节点?*** 外地代理解封收到的数据包,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:**为上层协议仍然提供尽力而为的服务,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.

第八章 计算机网络中的安全

什么是网络安全:安全通信特性:**机密性**(报文内容/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,**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性质)***主动攻击:***试图改变系统资源或影响系统操作,**伪装(**一个实体假冒另一个实体)**重放(**从网络中被动获取一个数据单元,经过一段时间后重新发送到网络中)**报文修改(**改变报文部分内容、推迟发送报文或改变报文发送顺序)**拒绝服务(**阻止通信设施正常使用或管理) ***密码学的原则(加密):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*****对称加密和非对称加密**. ***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)和**流密码(**处理连续输入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. ***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. Data Encryption Standard 算法:** 64bit 块加密. 使用 56bit 主密钥,先进行一次初始换位,然后进行 16 次相同迭代每次使用一个主密钥生成的 48bit 子密钥,最后再反过来换位一次. 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. **块加密算法:**将 k 比特的块映射为 k 比特密文. **3DES:**K1 加密一次,K2 解密一次,K1 再加密一次. ***为什么使用两个密钥而不是三个?*** 112bit 已足够长. ***为什么不使用 2DES?*** 中途攻击,若已有明-密文对,寻找$E_{k1}(P_1) = D_{k2}(C_1)$只需$2^{56}$的攻击量. ***为什么 EDE 而非 EEE?*** 为了与单次 DES 兼容,只需令$K_1 = K_2$. **AES.** ***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):**发送方生成一个随机初始向量(IV) $c(0)$,用明文发送给接收者;每一个明文块加密:$c(i) = K_s(m(i) \oplus c(i-1))$;相同的明文块几乎不可能得到相同密文块,并且不因引入随机性而产生额外的大量带宽(只额外传送C_0). **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:加密密钥公开,解密密钥是私有. ***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:加密密钥放在公开的文件中,解密密钥妥善保管. ***要求:***$K_B^-(K_B^+(m)) = m$,给定公钥K_B^+,不可能计算出私钥K_B^-. ***公开密钥算法应满足***从计算上,生成一对加密密钥和解密密钥容易;已知加密密钥,从明文计算出密文容易;已知解密密钥,从密文计算出明文容易;不可能从加密密钥推出解密密钥;不可能从加密密钥和密文计算出原始明文. ***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,无法知道发送方身份,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$n = pq$和$z = (p-1)(q-1)$选择一个与z互质的数d;找到一个e满足$ed = 1(mod\ z)$;公开密钥为(e, n),私有密钥为(d, n). **2.加密:**将明文看成一个比特串,划分成一个个数据块M,且$0 \le M < n$;对每个数据块M,计算密文$C = M^e(mod\ n)$,**3.解密:**对每个密文块C,计算明文$M = C^d\ (mod\ n)$ **4.另一个重要的特性:** $K_B^-(K_B^+(m)) = m = K_B^+(K_B^-(m))$. **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). ***朴素地*****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. ***报文鉴别与数据机密性分开:***附上标签,满足能够验证完整性且不能被伪造. **报文摘要:**将散列函数作用在报文 m 上生成固定长度散列值,发送者计算作为标签,接收者计算比较. 法一基于加密,发送方用与接收方共享密钥加密标签,但需要加密算法. ***开发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. 法二***基于哈希运算,***双方共享密钥s(鉴别密钥),发送方生成扩展报文$(m, H(m||s))$;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$H(m||s)$,若$H(m||s) = h$,则正常. 目前获得最多支持的报文鉴别方案为 HMAC,可与 MD5 和 SHA-1 一起使用. **密码散列函数:** ***满足的特性:***对于任意数据块x,$H(x)$很容易计算.对于任意给定的h,要找到一个x满足$H(x) = h$在计算上不可能(单向性):该特性对于基于哈希运算的报文鉴别很重要,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;对于任意给定数据块x,要找到一个$y \ne x$并满足$H(y) = H(x)$,在计算上不可能: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;[强散列函数需满足]要找到一对(x, y)满足$H(y) = H(x)$在计算上不可能. ***散列函数标准:***目前使用最多两种散列函数:MD5:散列码长度 128 比特;SHA-1:美国联邦政府的标准,散列码长度 160 比特.最多支持 HMAC 和 MD5/SHA-1 一起用. **数字签名:** ***一个可以替代手写签名的数字签名必须满足三个条件:***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(**防伪造**). 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?*** 当 Alice 从公开途径得到 Bob 公钥后,如何确认得到的是 Bob 的公钥,而非其他人的公钥? ***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. ***X.509 证书:***目前最常用的证书标准;***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,单点失效. 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,所有实体都有根 CA 的公钥,所有根 CA 间可交叉认证. **证书的获取:** 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 公钥及 CA 的签名,**验证:** 用 CA 的公钥验证 Bob 的证书得到 Bob 的公钥. **撤销:** 有有效期,或者定期发布证书撤销目录 CRL **证书目录:** 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. ***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. 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(回放攻击) **鉴别协议 ap4.0:** ***目标:***避免回放攻击. ***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K来加密这个不重数,然后把加密的不重数$K(R)$发回给 Bob,与在协议 ap3.1 中一样,由于 Alice 知道K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. **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:**$K_A^-(R)$. **Bob 计算:** $K_A^+(K_A^-(R)) = R$,只有 Alice 拥有这个私钥,因而一定是 Alice! *X.509 单向鉴别服务*: $A \to B: t_A\ ||r_A||IDB||Data||K_b^+(K_{a-b})||signature_A$ ***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***最重要的是**机密性**,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K_s;**2).**用这个对称密钥加密她的报文m;**3).**用 Bob 的公钥K_B^+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K_B^-得到对称密钥K_s;使用这个对称密钥K_s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K_A^-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K_B^+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:***将前两种过程结合起来而实现:Alice 首先生成一个预备包,它与第二方案中的包完全相同,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,再用第一方案中的发送方的步骤发送这个新报文,生成一个新包发给 Bob. **当 Bob 接收到这个包后**,他首先应用第一方案中他这一侧的步骤,然后再应用第二方案中他这一侧的步骤. 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. **Pretty Good Privacy:** 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. Encode64($K_B^+(K_{A-B})||K_{A-B}(Zip(Sgn||Data))$), 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. (因特网安全电子邮件的事实标准);软件生成密钥对;操作与上面第三种方案相同. 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). ***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: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. **SSL 握手协议描述: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 SSL 版本号,加密算法和压缩算法等和客户的不重数R_c; 服务器从浏览器选择一种 SSL、一种加密算法和压缩算法,它把他的选择以及证书与服务器选择的不重数R_s一起发送给浏览器;客户验证该证书,提取服务器公钥,生成一个 48bit 预密钥(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,则初始向量也从这里导出(两个));客户发送所有握手报文的 MAC,服务器发送所有握手报文的 MAC(级联,防止握手被篡改). ***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. **SSL 记录协议描述:** 机密性: 通过加密 SSL 载荷实现,完整性: 通过报文鉴别码保护. **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;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,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***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). 目标把安全特征集成到 IP 层.*** 网络层安全性实现了"地毯覆盖". **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,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. **安全关联 SA:** ***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. **安全关联(Security Association) 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. **两者之间存放该 SA 状态信息:**SPI;初始接口和目的接口;加密类型;加密密钥;完整性检查类型;鉴别密钥. 实体在它的**安全关联数据库(SAD)**中存放所有 SA 的状态信息. **IPsec 数据报:** ***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;**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. ***隧道模式路由 R1 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!)后面附上一个"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. ***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. ***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. ***WEP 数据加密(与 CRC 同时用):***主机与接入点共享一个 40 比特的对称密钥K_S(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K_S后面,形成一个 64 比特的密钥(K_S, IV);(KS, IV)用于生成一个密钥流$\{k_i^{IV} \mid i = 1,2,\ldots\}$;第$i$个密钥$k_i^{IV}$用来加密帧中的第$i$个字节$d_i$:$c_i = d_i\ XOR\ k_i^{IV}$;$IV$和加密后的字节$c_i$放在帧中传输;接收方使用相同的$(K_S, IV)$生成相同的密钥流,执行解密运算:$d_i = c_i\ XOR\ k_i^{IV}$. ***WEP 加密的安全漏洞:***每$K_S$只有$2^{24}$个$(K_S, IV)$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$(d_1\ d_2\ d_3\ d_4\ \ldots)$;Trudy 能够获得 Alice 加密的密文: $c_i = d_i\ XOR\ k_i^{IV}$;Trudy 知道c_i和d_i,就可以计算出k_i^{IV}: $d_i\ XOR\ c_i = k_i^{IV}$;Trudy 得到了加密所用的密钥流 $k_1^{IV}\ k_2^{IV}\ k_3^{IV}$ ...;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 AP)来提供鉴别服务. ***802.11i 的操作:*****1) 发现.** 在发现阶段,接入点通告它的存在以及它能够向无线客户节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(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,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 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[illegible]