转发表 控制面 网络范围上)和转发(路由器根据洗定路由将分组从输入端口转移到输出 端口、根据转发表转运分组、数据面、路由器内)、每台主机和服务器都运行网络层协议、网 **络层的作用**即将报文段从一台发送主机移动到一台接收主机 组交换设备 根据分组首部字段中的值 从输入链路接口到输出链路接口转移分组。某些 分组交换机称为**链路层交换机**基于链路层字 。 **段**中的值做转发决定.其他分组交换机称为 9中的值做转发决定 网络服务模型定义了分组在发送与接收员 系统之间的端到端运输特性,不同架构乃至同一网络都可能提供不同的网络层服务,在 发送主机中当运输层向网络层传递一个分组时能由**网络层提供的特定服务**有具有时延 上界的确保交付:能够为给定的源和目的地之间的分组流提供。有序分组交付。保证最小 带宽•确保最大时延抖动•安全性服务,**因特网的网络层**提 □終日能在 两台主机间提供于连续服务(数据场)或 而向连续服务(申路) 与运输层类似:网络层连接服务以源和目的主机间的握手开始:网络层无连接服务 **/提供**这两种用 系统中实现 成由路(Viernal Circuits)网络:网络层连接被称为成由路 成由路是一条 传输分组前建立虚电路,传输结束后拆除虚电路,所有分组在虚电路上传输(序),如果将路由器资源(带宽、缓存等)分配给虚电路,则虚电路可提供可预期的网络服 建立成电路的本质是预先选好源主机到目的主机的路径,此后分组仅沿选好路径传输, 该链路的不同虑电路 仅有本地意义)+沿途每台路中器中的转发表表项(<讲入端口讲。 号><輸出端口輸出 VC 号>)组成 分组在首部携带 VC 号路由器利用输入端口和 VC 号查找转发表。因为一条虚电路在每条链路。 的化号转发时用输出 在虚由路传输分组只需有 VC 号于需目的地址 无论何时跨制 台路由器创建一条新的虚电路,转发表就增加一个新表项,无论何时终止一条虚电路。 途每个表中的相应项格被删除,分组在每条链路上不简单地保持相同 VC 号是为了虚小 在分组首部中 VC 字段长度,简化了虚电路的建立,否则路由器将不得不交换并处理相当 大量的报文以约定一个共同 VC 号,信令报文专门用于建立、维护、拆除虚电路的控制报文、信令协议交换信令报文的协议。 数据报网络 分组携带目的主机地址路由器按目 的地址转发分组。路由器中转发表记录目的地址到输出端口的映射,转发表被选路模块的 改约1~5分钟更新一次 同一对主机之间传输的分组可能走不同的路径从而可能重 序. 虚电路 VS 数据报 ATM(虚电路网络)由电信网发展而来,注重用户体验(用户付费),追 :高质量服务:终端无智能或很少智能:复杂工作由网络完成,以保持终端简单 Internet(数据报网络)为计算机通信而设计:早期的网络应用均为弹性应用对网络服务 没有严格要求;用户免费使用网络;终端(计算机)具有智能;可将复杂的工作(如差错控制 推到网络边缘 以保持网络核心简单。**数据报网络只提供最小服务**可运行在各种链路: on everything);增加新服务只涉及终端(everything on IP) 组成部分·1输入端口 比特流接收的物理层功能从比特流提取帧 外理帧 提取 IP 数据 报的数据链路层功能转发功能。在本地线卡查拉转发表决定路由器输出端口通过交换结 处理 2.交换结构是路由器中的互联网络用于在输入端口、输出端口和洗路处理 到转运分组·交换速率通常倍于输入输出链路速率。是一个网络B 端口 网络尼功能 若需要 将交换结构输出的信元 组表成分组 若输出端口来不及发送, 组在此排队每次选择一个队头分组 减度发送 <mark>链路层功能</mark>:执行执行链路层协议 封装 ***** 功能:将比特流转换成物理信号.4.路由选择处理器执行 老以及连接的 链路状态信息 并为路由器 计算转发表 执行网络管理功能 路由器的输 **而**而**路由器控制平面**通常用**软件实现**并在路由洗择处理器(CPU) 上执行。 輸入端 [表的拷贝通常会被存放在每个输入端口. 转发表从路由选择处理器经过独立总线复制 1线卡. 转发决策可在每个输入端口.本地做出,无须调用中央路由选择处理器,避免。 查找对大型转发表使用超出简单线性搜索的技术。必须关注 采取许多其他动作。检查分组的版本号、检验和以及寿命字段,并且 更新用于网络管理的计数器。交换结构:1.经内存交换:第一代路由器即传 统计算机。由 CPU 直接控制,数据包拷贝到内存再交换(一进一出 2 次)、交换速率受限于内 带宽、现代路由器每个端口使用一个内存接口硬件连接到存储系统,控制器硬件在端口 司传输控制当息(天 CP() 参与)输入端口将包放入内存输出端口收到控制器发来的消息 B. 内左军 λ 武使出速率的—坐日不能同时转发两个分组 2 经总线交换 数据句通过共享 3线从输入端口缓存转移到输出端口缓存.每个输入和输出端口通过一接口硬件连接到 5.线 F 每个端口被分配—个内部标签·总线协议防止多个端口同时传输 需采用时分多数 复田:各个输入端口在总线上轮流广播分组 各个输出端口根据分组携带内部标答接收发 B电路, 多对端口间可以并行传输; 分阻塞型与非阻塞型两种, 先进设计;将输 入端口和輸出端口连成 N 个并行运行的交换结构,分组划分成固定长度的信元(cell) 送入交换结构 离开交换结构后再组装成分组。输入端口排队与美包:当交换结构不能及 时将输入端口分组转移到输出端口时输入端口处排队,队头阳寒(队头分组阳寒其后分 回(输入队列溢出).当交换结构速率为端口速率的输入端口数倍时可消除 与表包:多个输入端口同时向一输出端口发送时,输出端口处排 出端口排队不可避免增大输出队列虽然可以减少丢包,输出队列并 内存损耗增大延迟(延迟太大的分组最终被重传 浪费资源) **分组丢弃策略·弃尾(**队列法 时丢弃到达的分组)或按优先级/随机丢弃. 主动队列管理在队列满之前就开始丢弃分组 如随机早检测(Random Early Detection)算法和 TCP 拥塞控制机制一起使用,路由器在每 个端口上维护输出队列的平均长度 AvgLen=(1-Weight)×AvgLen+Weight×SampleLen 平均队列长度达到第一个阈值 长度达到第二个间值max,时 丢弃每一个到达的分组、概率 p 是平均队列长度和上一次 丢弃距当前时间的函数分组队列长度越大 丢弃间隔越大 p 也越大 **调度策略**先来先服 务、优先级调度、非抢占式优先级排队、轮询调度、加权公平排队 转发和编址。因特网编址和转发是*网际协议(IP)的重要组件 因特网* 控制而) IP 提供将数据报交付到目的地址和目的协议的服务 不提供任何服务承诺 但 尽量大努力解决(讨大分片,最大转发次数避免循环,包头检错避免误投递)。数据报格: 的首部). • **服务类型**(实际未使用) • 数据报长度(单位 1 字节:首部加上数据长度,该写 长 16 比特对应 P 数据报理论最大长度 65535 字节) · 标识 标志、片偏移,单位 8 字书 这三个字段与分片有关 · 春命(TTL)剩余最大跳数,每次转发减 1. · 上层协议用于解复用 节当作一个数,用反码运算对这些数求和,该和的反码 (被称为因特网检验和)存放在检验和字段中、路由器要对每个收到的 IP 数据报计算其首 部检验和,不一致则检测出是个差错,一般丢弃,注意到在每台路由器上。 首部计算了检验和 TCP/IIDP 检验和是对整 TCP/UDP 报文段进行的.TCP/UDP 与 IP 不一定都必须属于同一个协议栈.原则上 TCF 能运行在一个不同的协议(如 ATM) F 而 IP 能够携带不一定要传递给 TCP/IIDP 的数据 • 源和目的 IP 地址 • 洗项 • 数据/有效 数荷) 如果数据报承载—个 TCP 报文段 则每个行 分片的)数据报共承载了总长 40 字节的首部(各 20 字节的 IP 和 TCP 首部)以及应用层报 文. IP 分片与重组链路层帧能承载的最大数据字节数称为 MaxTrans 划分为若干较小的数据块,每个数据块封装成一独立的数据报传输,数据报在传输的过程 分片的报头取自原始数据报:杨 识每个分片必须携带与原始数据报相同的标识:偏移量指示分片中的数据在原始数据报 载荷中的位置: 标志位:MF(more fragments): 最 ment):DF=1 表示不允许对数据报分片. 分片报头中的*以下字段需要* 修改总长度、偏移量、MF、TTL、头部检查和 除最后一分片外 其余分片数据长度应为 N 应满足 N ▼的最大整数、数据报分片的外理过程根据报头长度和输出线路的MTL 确定分片的最大数据长度 N.将数据报的载荷划分成长度为 N.的若干数据块(最后一个数 据块可能不足 N 字节):将原始报头加到每一个数据块的前面:修改报头中的字段:总长度 =H+数据快长度最后—个报头的 MF 位置 0 其全报头的 MF 位置 1 偏移量 = 数据快在 原始数据报载荷中的字节序号/8.计算头部检查和. 重组将收到的分片重新组装成原始

数据报的过程,重组在目的主机中进行:收集分片:目的主机使用<源 IP 地址:标识>确定属

量重组。分片的问题分片开销:降低了路由器的吞吐量:消耗了目的主机的资源,每个重组 的数据报需要一个重组缓冲区和一个重组定时器。 针对分片的 DoS 攻击:攻击者发送-列奇怪的分片,消耗目的主机资源. IPv6 取消路由器分片的功能源主机发送探测报: 确定路径上的最小 MTU:源主机构造数据报大小不超过最小 MTU:路由器丢弃超大数据 报并发送错误报告 IPv4 编址:接口 interface:主机/路由器与物理链路的边界:路 ・接口.IP address:毎个网络接口对应一个 IP 地址.是· 32 位的二进制数通常用点分十进制数表示,为在因特网范围内保证 IP 地址的全 。每个接口必须具有唯一的 IP 地址. 单播地址结构,除类别标识外其余比特被划分为网 络号(因特网范围内标识物理网络)与主机号(物理网络上一个网络接口)。同 R.主机号由网络管理员统一分配. 建立私有网络组织可自选网络号,同样必须保证每-网络号在私有网络内的唯一性. 地址):32 位全 1 本地广播(仅目的地址):32 位全 0 指示本机(仅源地址):网络号全 0.主机号 有效指代本网主机:形如 127xvz 保留作为回路测试发送到该地址送回内部接收端 干拳的编址(早期):A 类 8bit(第一位 0)子网地址的子网,B 类 16bit(前两位 10),C 多 引。P 编址为这个子网分配了一个地址 xyz.m/h,其中/h 的记法,又是称为**子网掩码**,指示 32bit 中最左侧的 h bit 定义了子网地址 子网地址≠子网号子网 . 如何确定子网? 将网络接口与主机/路由器分开,形成一些分离的网络岛,每个网络 数据报转发音接交付·节占将数据句音接发送绘目的主机(不需要其它路)。 器转发)间接交付:节点将数据包转发给一个路由器去处理。如何判断使用直接交付还是间接交付了直接交付数据包目的地址与节点的某一端口在同一个子网中间接交付数据 图的目的地址不与节点的任何一个端口在同一个子网中.*间接交付的实现*.节点查找转发 点:只能按照三种固定的大小分配地址空间.地址浪费严重(A/B).转发表必须记录每 已分配的网络、转发表规模爆炸式增长(C). CIDR 按照实际需要的地址数量分配地址空 是高地址使用效率。分许将若干多转发表项进行整合减小转发表规模 CIDR 地址分配的 原则 \oplus 计计块的长度 | 必须是 2 的暴次·所有地址的前(32 = $\log L$) 位必须相同 **网络地**拉 的表示方法:用捺码指示网络地址的长度, **机构如何获得网络地址?** 机构通常从 ISP 的地 \$\psi\overline{\psi}\overline{\p 表记录目的地址到输出端口的映射、取决于目的地址类型的不同,有三类转发表项目 州州县—个*子园州州农 州州前缀春顶* 目的州州县—个*特定的园终柱口州州和*特特 不匹配所有其它表项的地址。这些地址被映射到一个默心 **图用逐激洗路**每个转发表项只记录去往日的地址的下一跳信息/下一个要到达的路由器 端口),而不是一条完整的端到端路由. *每个转发表项包括目的地址/掩码、(下一跳地址、)* 到达). 地址聚合:目的地址可以聚合成一个前缀更短的地址:日有相同下一跳. 地址聚合 可以**递归进行。 若个别表项不满足路由聚合的条件**仍可在转发表中给出一条聚合表项 同时给出不能被聚合的表项;最长前缀匹配在所有匹配的路由表项中,选择前缀最长的 支项 查找转发表 为与某个转发表项 Dest addr/prefix len 进行匹配运算路由器需要 先从表项中读出地址掩码(或 prefix-len 值),计算包的目的地址前缀(用地址掩码和包的 的册址相与) 与 Dest addr 的册址前缀(Dest addr 与册址掩码相与)进行比较:引入的简 医地址前缀的长度 prefix len 可以是任意值 Prefix len 无法从地址本 b项中得到,必须从所有匹配的表项中选择前缀最长的表项,在大规模转发表中进行**发** 终端使用动态主机配置协议 Dynamic Host Configuration Protocol 获取 IP 地址。 麻烦(即播即用);可用少量的 IP 地址服务较多的客户(地址重用), DHCP 目标:允许主机加 入网络时自动获取配置信息。DHCP 是一个**客户/服务器模式**的应用协议,每个**子网中**应 有一个 DHCP 服务器或代理 DHCP 步驟: 1 主机广播 "DHCP discover"报文 (dest:255.255.255.255)寻找子网中的 DHCP 服务器 2DHCP 服务器用"DHCP offer"报文 向应给出推荐的 IP 地址及租期,其它配置信息,3主机用"DHCP request"报文请求 IF 址选择一个 DHCP 服务器,向其请求 IP 地址 4DHCP 服务器用 DHCP ack 报文发送 I 地址响应客户的请求确认所要求的参数,DHCP 服务器使用 UDP 端口 67.客户使用 UD 68. DHCP 不足之处:从移动性角度看,节点移动时,不能维持与远 程应用之间的 TCP 连接: 网络地址参拣/NATD使用一个公用 IP 地址支持许多用户同时上网,仅为公共可访 虑). NAT 实现:外出的数据报将数据报中的(源 IP 地址源端口号)替换为(NAT I 下断分配))NAT 转换表记录每个(源 IP 地址:源端口号 业NAT端口号)的转换关系: 进入的数据报职出数据报中的(目的 IP 地址目的端口号)查 找 NAT 转换表。然后用转换表中对应的(IP 地址,端口号)进行替换。 16 比特端口号允许— F的句头/端口号在传输层)·违反端到端原则/节占介入修改 IP 地址和端口号) NAT 妨碍 P2P 応用NAT 只分许内部主动发起的通信 位于 NAT 后面的主机对外不可见 但 P2P 以 用要求任何对等方可以向任何其它(参与的)对等方发起通信 使用IJPnP 实现 NAT 穿刺 條内网主机端口映射到公共 P 地址的端口 − 向外部追踪器通告它在外部端口 − 可用:損 B主机通过追踪器可以看到该主机NAT将外部端口上收到的SYN包转发给主机。使用 中继服务器定理 NAT 穿越在 Skype 中使用NAT 后面的服务器与中继器建立连接外部 客户与中继器建立连接,中继器在两个连接之间转发分组。IPV6:IPV4 地址将很快 尽:IPv4 需要改进:简化头部格式:加快数据报处理和转发;支持服务质量;支持多播;支持移 动性:增强安全性, IPv6 与 IPv4 不兼容,但与其它所有因特网协议都兼容, IPv6 地址:12 IPv6 定义了 三种地址类型 单播地址:一个特定的网络接口;多播地址一组网络接口;任播地址(anycast):一组网络接口中的任意一个(通常是最近的一个). IPv6 数据报以一个40字 节的基本头开始,而后可洗扩展头然后是数据。PRV或 traffic class):作用发送方在该域员 义数据报的优先级 路由器发现网络拥塞时按优先级从低到高的顺序丢弃包 IPv6 将网 各流量划分为两大类:受拥塞控制的流:包括非实时流优先级 0~7.按照重要性及用户体 验设定:*不受拥塞控制的流包括*实时多媒体流优先级 8~15,可以按照用户要求服务质量 等级定义. *流(flow):*流是具有相同传输特性.源/目的、优先级、选项等)、并要求相同处 (使用相同的路径和资源,且有相同的服务质量和安全要求等)的一系 也址和流标签(flow label)唯一标识:流标签由发送方分配,不支持流的节点忽略该域,支持 充的路由器维护一张*流表(flow table)*,记录每一个流需要的处理,收到数据包后,根据源 地址和流标签查找流表进行相应的处理·流的引入使得 IPv6 具备了对数据包进 ☆验计算校验和太花时间,链路层和传输层可以差错检测 IPv6 基本等 中增加了流标签:支持对数据包区分处理;改变了:Traffic Class 代替 Type of Service:载荷长 度代替总长度 Next header 代替 Protocol 允许任意扩展洗项 从 IPv4 计渡到 IPv6:双 24方金支持 IPv6 的主机和路由器同时运行 IPv4 和 IPv6 运行双栈的源节占先对目 节点查询 DNS,若 DNS 返回 IPv4 地址,发送 IPv4 分组,若返回 IPv6 地址,发送 IPv6 分组 同时拥有 IPv4 和 IPv6 地址 IPv6 数据包如何穿越 IPv4 网络? 报头转换双栈节 点(如路由器 B)在将数据报传递给 IPv4 路由器(如路由器 C)之前,将 IPv6 报头转换成 IPv 报头;缺点,报头转换不完全,有信息丢失,建立隧道;IPv6/IPv4 边界路由器将 IPv6 包封装到 一个 IPv4 包中,送入 IPv4 网络,目的边界路由器取出 IPv6 包继续传输,优点,保留原始数据 报的全部信息 第五章 网络层 路由选择算法:什么是最佳路径路径长度、数据速率、分组延迟、通信费用、安全性等:ISI 关心:网络吞吐量最大、平均包延迟最小、平均通信费用最低、网络负载均衡、路由稳定、 健壮等<mark>路由评价指标通常是矛盾的需要折衷。 *选路算法分类,全局算法*所有</mark>路由器具

关于拓扑和链路代价的全部信息,集中式计算:分布式算法。路由器仅知道邻居节点以及 或缓慢变化(手工配置): 动态算法:路由器根据拓扑及链路代价的变化而自动更新路由 编路状态(15)洗路算法。绿路状态洗路算法为全局算法且基本思想为每个节点利用可靠 方法获得全网拓扑信息,抽象成一个带权拓扑图,计算到各个节点的最短路径. 链路状态

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 网络拓扑 计算从本节占到其它各个节占的最短路径(Dijkstra) 可能出现的 可顯光路電 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 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。主要引 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×测量 ξ_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 $D_v(y) \leftarrow min_v \{c(x,v) \in M\}$ 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 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)有变化时通知非 **錄路代价变化:好消息传播快.坏消息传播惯**路由选择环路和无穷计数问题【毒性 S 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)亲自测量的本地链路代价;节点计算的路由不传播,错误不 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]信息<mark>可能不正确:</mark>邻居的距离矢量是"道听途说"的;节点计算的路由要传播: "散收敛较慢,还可能出现路由环路、计算至无穷问题。<mark>层次路由选择。</mark>*平面*; 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 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 itra-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 Inter-AS 域间选路协议,所有 AS 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 IGI* 是常见的有:RIP.较低层 ISP 和企业网使用:OSPF.较顶层 ISP 使用. Inter-AS 选路协议也和 *外部阿关协议 EGP*.目前只有 BGP. <mark>域内选路 Routing Information Protocol 采用*距*。</mark> 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 《谷的默教·从道路由器到日的子网(全)经过的子网数量 限定—条路径的最大化 器 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 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,每个报文的 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 (※窓由果シ间大約毎 30 砂な塩ーカ PIP 幅応収文 毎台窓由果維拍―张致お路由? 學表的 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 180 秒未收到某个邻居的 RIP 通告 认为该邻居不可达。今通过该邻居的路径生效/ 16)发送 RIP 通告:采用表性逆转解决计数至无穷问题:若选路表中到目的网络 x ₩OSPF:OSPF 采用

※部件が

・特路状态洗路

は

は

は

は

を

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・

・ #OSPF 协议定义了 5 种分组类型,分别用于探测邻居、通告链路状态等. OSPF 分组被 **路山哭囯期性州** 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 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 自治系统值 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: # 5 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 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" 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 器,然后再转发到目的子网. OSPF 的其他优点写 络通过自己可达以及将可达性信息的 由器中有最低的路由器到网关代价. 涉及两个点 置intra-AS:设置到 AS 内部网络的路中inter-AS & Intra-As:设置到外部网络的路 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 A 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 原育为其它 AS 转发数据句 能)找到最佳路由 边界阿关协议 Border Gateway Protocol:每个子阿可以发布自己的 存在,当一对 AS 同意交换选路信息时,每个 AS 指 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 speak -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 是应用层协议),BGP 会话的两个端点互为 BGP 对等方 不同 AS 的两个边界路由最 之间建立的BGP 会话称为**外部BGP(eBGP)会话**一个AS 可能有多个<mark>边界路由器</mark>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 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: 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 选择到目的节点的最优路径:Inter-AS 选路协议 F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 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:相同的分组在某些铅 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* ※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 分组);网络中产生的分组拷贝最少. 在网络中复制分组:> 泛(flooding):节点收到广播分组后向所有邻居节点(除分组到来 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. *曼控洪泛*:目 可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 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: 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 ☆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转 出端口:若分组的輸入端口与夫往该地址的輸出端口相同。则扩散该分组.否则丢弃分约 点 算法合理、易于实现日开销不大 生成树方法,使用生成树转发广播分组,路由器知 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:基于机心的方法*: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段 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 新港市的市場社会域可以企業的企業。 就是位于史成树上的端口当加入报文到达生成树上的一个节点时,我文经过的路径被添加到生成树上。 加到生成树上。 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

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 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1 : 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 多播分组的—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B A应当是最佳的(最短路径), 建文多播树的两种方法:基于源的树源节点建立一棵到 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<SG>构成一棵树 多播路F 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.d 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*,每个多样 组使用一棵树 树根为该名播组的核心 源节占先将名播分组发送给核心 核心再在名播林 4.多播路由器只需维护一棵多播树;缺点 《不早最佳的 其子源的树·最有路径树MOSPF 扩展了 OSPF 协议 参与名摄主机 定期》 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 转发确保多播分组到认每一个局域因 各径剪枝: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。 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) 路径加入到树中,如何利用组共享树发送名播分组?当源节点想要发送名播分组时间 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 ※首:酒节占将名攝分组封裝到—个单爆分组由 单爆分组的目的抽册为核心的单数 业 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 寸程,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洗路; 星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。因物 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 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** 据骨干网 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 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 NICMP报文是作为IP有效载荷承载的 滁网络传输必须封装在IP 句中传输 从体系结 ト讲它是位于 IP シ ト的・ICMP 通常被认 为是 IP 协议的一部分 因为 IP 协议使用 ICMP fi 5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: t讲一步的区分:Checksum:ICMP 报文的检查和:内容:与报文类型有关. 报告错误的 ICMP 据文句会触觉该供证的数据据的主部和前 8 个数据字节 Ping 与 ICMPPing 利 CMP 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:源主机发达 ne=8.Code=0 的 Echo Request 报文:若目的主机收到发送 Type=0.Code=0 的 Ech sponse 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 句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约 过的路由器)源主机的 Traceroute 程序向目的主机发送一个 Echo Rec 报文段),IP 报头的 TTL 设为 1;第一跳路由器对),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 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TTI 为 3 的 Echo Request 报文·该过程不断重复 有至此到日的 E机的 Echo Response 报文(该目的主机向源发送一个端口不可达的 ICMF ICMPV61CMPV6 会并了IPM 由的 APP 和 IGMP 并取消了 PAPP(该协议的Th能已被其实 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"分约 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 **各层和链路层的关系: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):**鏈路层将数据报从一个节点传输到相邻的 个节点 蘇路层概述 节点**:字机/路由器,**蘇路**连接相邻节点的通信信道,**帧**等 告流取出完整帖\结路接入/广爆练路需要\在广播信道上协调各个节占的发送行为 美 (測(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)。 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崎(停-等 GBN SR) 低误码率链路(加米纤、某些双绞线)上很少使用高误码率链路(加天线链路)。 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 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 长中的控制器芯片:成帧、链路接入、检错、可靠交付、流量控制等:主机上的链路层 理差错条件和将数据报向上传递绘网络层 **网络活配器之间的通信·发送侧**将数据报 装到帧中 生成校验 P.特 (可洗)执行可靠传输和流量控制: 接收侧提取帧 检测传输 (可选)执行可靠使给和法曼控制 解封装数据据 亦经上层执道 **传输出错的拳型**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。 大影响数据位数. 差錯控制编码的类型: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? 的编码. 差錯检測的实施:码字由m比特数据加r比特冗余位构成,有效编码集由2 合编码规则的码字构成,若收到码字无效。恰错纠错码可将收到的无效码字纠正到距 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。 (直, 为检错d比特, 編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) 2d+1. <mark>奇偶校验. 单比特奇偶校验</mark>可检测奇数比特错误检错率 50%编码集海明距离; 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. <mark>固特网检验和(Internet_checksum);</mark>数据的 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音 的因特网检验和ITCP和LIDP对所有字段(包括首部和数据字段)计算因特网检验和代 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 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<mark>\$</mark> 实现的. 因为运输层差错检测用软件实现.采用<mark>简单而快速</mark>的差错检测方案是重要的 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,它能够快速扩 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。 多项式R(x)由r上特为系数构成的多项式。生成多项式G(x)双方确定用来计 (x)的一个r+1比特多项式。编码方法: $R=M\cdot x^r/G$ 的余式(减法运算定义为异面 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 GE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)1110 计算 CRC 码,101110000 ÷ 1001 的余式为 R=011 (CRC code),码字:10111001 | G(X) = 1001,接收端收到比特串 1001001,问是否有错?解答:1001001÷1001 的余式; ((不当 n) 有传输供证 **多路方间标识 绿路的面釉卷形占到占鳞路**·仅连接了 一个接收方的链路。一条全双丁链路可以看成是由两条单丁链路组成:广播链路; 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 bos 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 的机制)简单(实现和运行开 小). MAC 协议的分类:信道划分:将信道划分为若 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、轻负载的 **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 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。 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. 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-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) 1*时隙(一个时间 N 个时隙*)每个时隙可以发送—个分组,节点只能在分配给自己的时隙

个固定的子频带(R/N 带宽),若节点不发送,其子频带空闲 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(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约 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 等λ的 MAC 协议 当节占有数据要发送时 以信道速率 R 发送 发送前 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.假证 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 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,节点可存 个时隙发送新帧若检测到冲突,节点在随后的每一 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 方间协议的效率: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附 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 $-Np(1-p)^{N-1}$ 最大效率为令 $Np(1-p)^{N-1}$ 最大的概率 p^* 代入 $Np*(1-p)^{N-1}$ 趋向于无穷得到最大效率 1/e 约 37% 维 ALOHA 取消同步时钟 任何节点有数据发送家 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 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.发送的帧! t_n-1,t_n+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 $(10^{-1}, 10^{-1}, 10^{-1}, 20^{-1},$ (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码 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 比信道,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 时传输"循环之前等待一段随机时间 CSMA/CD (Collision Detection)发送的过程中提 则冲突(发生冲突时信号较强)检测到冲突后 立即停止发送剩全的部分 立即启动冲突 夫的过程. 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: 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 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 IF 发送輪 并发送—个阳塞信号(加强冲突):中止传输后等待—个随机时间量(指数回退): 二进制指数后退算法:当传输 撞后、节点随机地从(0,1,2,3,...,2"-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 大再次发生冲突的可能性越小、每次透配器准备传输一个新的帧时。它要运行 CSMA/CD 算法不考虑证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描入一次成功的传输 CSMA/CD 效率 T_{prop} =以太网中任意两节点间传播延迟最大值 T_{tra} efficiency= $1/(1+5T_{prop}/T_{trans})$. 在以下情况下.以太网的效率趋近 760 X年「prop-以入ペートに思考)」に同じて指定と取入に17mas-取り、同様のの のマン(14元) Trpop/Trans)。在以下情况下,以太两的效率趋近于 1.7mas)。在以下情况下,以太两的效率趋近于 1.7mas)。在 最適可于无穷。结论。应控制以太两的规模、影流 MAC 协议ALOHA 和 CSMA 协 1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 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 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。今牌传递协议没有主节点。今牌(token)小的特殊帧在节点之间以固定次序进行传递,节点收到今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 记了释放今牌 则必须调用某些恢复步骤使今牌返回到循环中来 今牌作 文比較信道划分 MAC 协议:重负载下高效:没有冲突:节点公平使用信道:经负载下低效 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 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 负载下的发送冲突)。 交换局域网:局域网 Local Area Network 将 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 Metropolit Area Network 通常覆盖—个城市的范围(月十公里) 要能支持数据。 音频和视频在内间 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 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 MAG 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 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助 这是因为链路层交换机的任务是在主机与路由器 地执行该项任务 这就是说 主机或路 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 快速确定网络接口的位置。而且不论活配器到哪里用都不会变化。目的MAC地址有三 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 助业 助业最高比特为 1·广播地址全 1 网络活配器仅将发送绘本节点 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制

PMAC 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 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 现直接交付? 当发送节点 A、接收节点 B 位于同一个子网络 F 时 数据报可从 A 直接交 付给 BA 的网络层将数据报及 B的 MAC 地址交给酒配器(辖路层),适配器将数据报封家 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:地址和 析(Address Resolution)/可**服静态映射 IP 地址-MAC 地址的缺点**:主机每次使用的 IP 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 过程A 想知道 B 的 MAC 地址·1. A 构造一个 ARP 请求(操作 1) 在发送方字段道入自己的 IAC 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 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 ·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,在发送方面 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MA 掛掛)中发送 **改讲 ARP 的措施:ARP 表**每个节点在内存中维拍一个 ARP 表 每次发送数 記字·APP 经左由的信息 在超时(一般为 15~20 分钟)后删除 *主动学习·*从 APP 违 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 P 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 夏错误. ARP 即插即用.ARP 表是自动建立的. ARP 跨越链路层和网络 ※ 数据報到法子國之外数据報从 A(子國 1)经计 R(路由器)到法 R(子國 2)·A 知道下 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 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 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流 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

相当于共享电缆,因此也是共享式以太网,交换式以太网;交换机(21 世纪早期);主机通过 双绞线或光纤连接到交换机。交换机在端口之间存储转发帧(链路层设备),主机与交换机 之间为全双丁链路 交换式以太网不全产生冲突 不需使用 CS MA/CD 协议! 逻辑星形拓 扑:各节点仅与中心节点直接通信。各节点之间不直接通信:基于集线器的以太网为 星型拓扑,逻辑总线拓扑, 以太网帧结构/按顺序前同步码:7 个 10101010 字节,后跟 011 字节,用于在发送方和接收方之间建立时钟同步,一般不计入以太帧长度 目的地址(6 字节)+源地址(6 字节). Type(2 字节):指出 Data 所属高层协议(如 IP/ARP 等 每个协议一个编号,用于多路分解(和网络层数据报中的) 1500 字节 这意味若如果 IP 数据报报过了 1500 字节 则主机必须将该数据报分片·当采用 填充时传递到网络层的数据包括 IP 数据报和填充部分,网络层使用 IP 数据报首部 CPC(4 字节 循环 〒全松浦)・7 四个字段计算。所有的以太网技术提供无连接(没有握手)不可靠(接收方不发送确认,是 CRC 错误,依靠上层协议错误恢复)服务 (在链路层)缺 长的要求?为确保节点在发送结束前(CSMA/CD)检测到冲突帧的发送时间必须足够长 节点检测冲突需要时间,假设信号在相距最远的两个适配器之间的往返延迟为 2τ.则帧的 于 2τ.即帧的最小长度≧链路速率×2τ;> 码)根据早期以太网的最大直径(2500米)和数据速率(10Mbps)计算得到. 802.3 以太网标准历史上出现讨许多不同的以太网技术。链路层相同 MAC 协议 帧格式 帧处理: | 传输媒体(光纤,同轴电缆,双绞线);数据速率(如 10Mbps,100Mbps, 1Gbps);物 理层编码方式不同。所有这些以太网技术由 IEEE 802.3 工作组标准化形成 IEEE 802.3 标准族 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 宽之和,从根本上解决了网络规模与网络性能的矛盾 网络最小崎长及超校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,由于交换式以为 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**,除了帧格式保持不变外,其它都和共享式以太网不同。 **翻路层交换机,交换机的任务**是接收入链路层帧 将它们转发到出链路。交换机自身没有MAC地址,对子网中的主机和 即插即用 自主学习 交换机输出接口设有缓存 对键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 ※似于数据转发 重要差异导交换机转发分组其于 MAC 抽协而不早其于 IP 抽协日交换 机表与路由器的转发表的构造方式有很大差别,**帧的过滤和转发、自学习:**当帧到来 (转发决策)若目的地址所在端口等于进入端口、丢弃帧、否则转发帧、若目的地址不在转发表中扩散帧、更新转发表)若转发表中有源地址,更新表项,若没有则添加且生存期为最大 值 交換机的表是自动。动态和自治地建立的交换机是即播即用设备。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。使用交换机的优点不同于总线或基 于集线器的星形拓扑那样的广播链路,可消除碰撞:交换机缓存帧且不会在网段上同时们 输名于一个帧 链路异质:交换机将链路彼此隔离.局域网中不同链路能以不同速率运行 日能在不同媒体上运行。管理:提供强化安全性、交换机也易于进行网络管理、交换机 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 为它在链路层 用 MAC 协业转发帧 路由器在网络层根据 IP 协业存储转发数据报 交換 链路(MAC 协议不同),只按原样转发帧路由器可以进 何时使用办施机或路由器:门面会主机小网络 办施机就见够了 因为它们不要或 IP 地址的任何配置就能使流量局部化并增加总计吞吐量,但是在由几千台主机组成的更 大网络中,通常在网络中(除了交换机之外)还包括路由器,路由器提供了更健壮的流量隔 离方式和对广播风暴的控制,并在网络的主机之间使用更"智能的"路由,交换机 播,只能学习单播 MAC 地址会扩散所有广播帧交换机连接所有主机在同一 广播域中路中器可以阻断广播帧传播根据 IP 地址转发(看不到 MAC 地址)每个端口是 个独立广播域。**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 **冲突域**共享同一条广播链路的主机集合,任何一个主机发送的帧名种帧,可被冲突域中的其它主机接收到,广播域:广播帧能到达的主机集合广播风暴为广播帧在网络上大量 传播扩散消耗大量资源,三层交换机:有部分路由器功能。又有二层转发速度的交换机。通 常在机构网络核心层、连接不同子网、专业路由器连接机构网络和外网、三层交换机哈希查找 IP 地址-MAC(路由器 IP 找 IP 后再 MAC)—次洗路多次转发所以快、虚拟局域网 AND 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 网络调到的困难信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),但在逻辑上应连接在同一交换机上;在同一交换机上的主机,在逻辑上,可能需 要隔离:用大量的路中器来分割网段成本很高 成拟局域网 V/AN位于物理局域网上的 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 <u>独立的网络</u>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 VLAN 的名字、每个机器在哪个 VLAN 上:在每个交换机上建立 ↑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 VLAN.基于 IF 地址划分:根据 IP 子网地址划分 VLAN. VLAN 干线连接:将两个 VLAN 交换机互联. 交换 机如何在 VLAN 间转发畅当一个帧到达时,交换机判断该帧属于哪个 VLAN 查找配置表 得到该 VI AN 对应的端口 在该 VI AN 对应的所有端口上转发帧 如何知道一个帧属于哪 如何知道一个帧属于哪 导到该 VLAN 对应的端口,在该 VLAN 对应的所有端 个VLAM领所属的 VLAN = 发送节点所属的 VLAN、交换机根据领的到达端口、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 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 VI AN IFFF 802 10 规定了新的以太帧格式帧 4 中包含一个 VI AN 标答(tan 用于指明帧属于哪个 VLAN. 802.1Q 如何与已有阿卡兼容Q:我们需要抛弃已有的以 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、且支持 VLAN 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 字寸 唐松化·网络作为结路层·多协*议标签交换(MPLS*)是一种分组交换的虚由报网络 *目的*: 使用固定长度标签(而不是 IP 地址)进行高速 IP 转发. 特点使用固定长度标识符(而不 最短前缀匹配) 快速查找·借用虚拟由路(VC)的方法·但 IP 数据报仍然保持 IP 批批 标答? 换路由器:仅根据标签值(不检查 IP 地址)将报文转发到出接口. *灵活性*MPLS 转发决策可 能与 IP 目的地址和源地址不同,以不同的方式将流路由到相同的目的地,如果链路故障 使用预先计算的条价路径快速重新路由流 (对 VoIP 有用). IP 路由:到目的地的路径仅由 目的地地址决定.MPLS路由:到目的地址的路径可以基于源地址和目的地址.一个MPL 加强的帧只能在两个均为 MPLS 使能的路由器之间发送. 回顾:Web 页面请求 DHCP、UDP、IP 和以太阿:仍在准备: DNS 和 ARP:仍在准备:域内路由选择到 服务器:Web 客户-服务器交互:TCP 和 HTTP:

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-基站: 通常连接到固定网络 在无线终端和固定网络之间中继数据包 通常负责协调与 之关联的多个无线主机的传输。 无线链路:连接无线终端和基站需要 MAC 协议协 ,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 · 础设施模式:无线终端通过基站连接到固定网络(网络基础设施),所有传统的网络服务由 固定网络提供自组织模式:网络中没有基站,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中器 切棒于线终端接入到不同基站的 程,*无线网络的分类*: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):多跳有基础设施:主机通过多个无线节点的中继转发才能到达固定网络(如无线网状网络)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缘如蓝 F网络)**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约 ### 无线链路的特性信号衰减:信号在传播过程。 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 能量逐州域之代码工程域代别,TALX工艺会。由 2000日 TALX 经转的传输距离受限、误作用,信号沿多条不同长度路径到达接收端,以上特性导致无线链路的传输距离受限、误工电缆查 结晶比/CMDV亩土的信噪比面容易提取出信号 信暖比与误码率的权衡给定 码率很高. 信噪比(SNR):更大的信噪比更容易提取出信号. 物理层:增加功率->提高信噪比,降低误码率,给定信噪比:选择满足误码率要求的物理员 给出最高的吞叶量:信噪比可随移动性变化:动态适应物理层(调制技术、速率) 无线网络的

言号强度不足以使他们相互检测到对方,但足以在 B 产生冲突 . CSMA 不适合多跳无线 多通过载波侦听 发送节点只能知道其周围是否有节点? F发送·但直正影(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)**CDMA**所有用 ,但每个用户都有自己的 CDMA 代码来编码数据(代码"正交");编 线。2.4-5GHz、<200Mbps. 均使用 CSMA/CA 作为 MAC 协议:都支持基站模式和自组 术·物理是不同 802 11 体系结构·802 11 无线 I AN 的基本组成单元是基本服务集(RSS) 个 BSS 包括若干无线终端。一个 6 MAC 抽計 AP 与路由器相连的有线端口没有 MAI 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-- 个服务集标识符(SSID),并选择 AP 使用的信道:相邻 AP 使用 P装 AP 时 为 AP 分配-信道可能相互干扰。主机必须与一个AP关联:扫描信道,监听各 AP发送的信标帧(周期) 后是可能的量 1%。 文化的 1 MAC 地址)选择—— AP 进行关联 可能需要身份鉴别。 DHCP 获得 AP 所在子网—个 P 地址。 802.11 主动/被动扫描/被动扫描/主机扫描信证 监听 AP 发送的信标帧主机选择—个 AP 发送关联请求帧 AP 向主机发送关联响应制 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。802.11MAC协议:采用CSMA/C(ollision) (voidance):发送前监听信道,不与当前正在进行的发送冲突;发送中 很困难(接收信号的强度远小干发送信号的强度)。不管 隐藏节点). 开始发送帧后,就完全发送该帧. 接收方收到帧后发送链路层 以十回到 902.11 都使用赖油体顺畅机控入 但这面 MAC 协议方面更然 3/80211 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 80211/不同 于以太网)使用链路层确认/重传(ARQ)方案. 操作模式:Point Coordination Function:有基 站 轮询:Distributed CF:通用.所有节点用.CSMA/CA 竞争.支持信道预约(可洗).无信道预约 必须) 使用信道预约处理隐藏终端:Request To Send 和 Clear To Send 操作方法:假设 向 AP 发送一数据帧:A 向 AP 发送一个(暴露)RTS 帧 帧中给出随后要发送数据帧及确 X 问 AF 及这一数路顿X 问 AF 及这一门(泰露KIS 帧,帧平岩占随后安及区数路顿及帧 认帧需要总时间:AP 收到后回复一个 CTS 帧帧中给出同样时间:A 收到 CTS 帧后开始发 送;AP 收到帧后,发送 ACK 帧进行确认;(A 附近)收到 RTS 帧及(AP 附近)收到 CTS 帧的节 均沉默指定时间 计出信道计 A 和 AP 完成发送 若 A 和 B 同时发送 RTS 帧 产生发 下成功的发送方随机等待一段时间后重试。此机制只对长数据帧使用。帧间距机制: 午 PCF/DCF 共存,SIFS:允许正处于会话中节点优先发送,如收到 RTS 的节点发送一 CT 收到数据帧的节点允许发送一个 ACK 帧 PIFS 如 SIFS 后无节点发送 PCF 模式基站可发 送信标/轮询帧 DIFS:如 PIFS 后无基站发送 任节点可竞争信道 EIFS:如以上间隔都没有发 送。收到坏帧或未知帧节点可发送一错误报告帧;*无信道预约链路层确认方案:*发送方:1. 运收到外限级不利限Pinny公面,指码以及可以及10年以及10年以来的企业的对数的设置。 初始时站点监听到信道空闲等待分布式帧间间隔(DIFS)时间段后发送该帧。2.否则选择一幅机间设值,并在临听信道空闲时递减该值如繁忙则冻结计数器。3.计数器减为 0 时 发送整个帧并等待确认 4.如收到确认并且想要发送第二个帧,或(给定时间内)没有收到 **公要用链路层确认**难以检测碰撞且节点不能中断,接收方只会在没有碰撞时确认帧 **"路层确认可以完全避免碰撞吗**不能,可能有隐藏节点的问题,两节点可能洗择了接近 的回退时间。CSMA/CA 与 CSMA/CD 的不同:最根本的不同:CSMA/CD 在发送过程中 测冲率 无确认 而 CSMA/CA 在发送过程中不检测冲率 有确认:由此带来协议处理方面不 同:在CSMA/CD中,节点侦听到信道空闲时立即发送(冲突则停发,影响不大);在CSMA/C 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) 80% · MAC 地址: Address2:帧的目的 MAC 地址; Address2:帧的源 MAC 业;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 帧寻址差例:无线终端 H1 向路由器 R1 发送帧 它的 AP 已知:H1 构造一: MAC,address2=H1 MAC,address3=R1 MAC,发给 AP,AP 将这个 802.11 前 转换为 802.3 帧(有线)。后者 dest addr=R1 MAC.source addr=H1 MAC. AP i 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系 2)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 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。<mark>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</u> 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</mark> 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:**节点讲入休眠.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 域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 与向 AP 请求航 其全节占重新进入休眠 终端在 IP 子圆间移动 终端进入一个新的 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IF かず IP 地址后终端上 生运行的应用将中断 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 个州业与移动节占通信 即使移动业保持不变 "向属代理·当移动节占在外州时 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 可归属代理注册,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 *间接洗路到移* 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. *间接透 路:三角透路问题*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,接交地址(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专行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 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** 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 ※再做)通信者将句发给外地代理:外地代理将包转发会移动节点: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 的转交排排通信者包括固定节占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.原意充当归属代理: ·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 原音充当外地代理的 各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 P 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 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 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 : 当移动节点回到归属网络时.要向归属代理注销 己的转发表中。 数据报间接洗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 归属代理如何得到数据报? 若诵信者不在归属网络 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 数据报机何能被归属代 2/2017 链路层帧的目的地址必须是归属代理的 MAC 地址:

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

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 旧属代理 MAC 地址) 剧新其它节占的 ARP 缓存 数据报如何到达转交出 **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 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 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 f 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 4C ###? 在移动节占注册阶段 外地代理获知了移动节占的永久 ###和 MAC # b中外地代理根据目的 IP 地址查找转发表 得到移动节占的 MAC 地址 N.抽代理利田移动节占的 MAC 抽扯 络数据报封装到结路层帧由 发送经移动节占 凝 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):SrdP=移动节 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 题译码率 手句率 延迟增大 **若占移动带来的问题**手句 延迟增大 逻辑上没什么影 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: 美包率高 传输延迟增大 TCP 将美包(长 。要地域小拥塞窗口、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 ·*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 未自<mark>具头的源,且与输过在中不依修以,确定金剂</mark>及这者和接收者能够证头对了的另历 **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**试图从系统中贫 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) 报文长度等流量模式推断诵信性质) **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)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 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,每次处理一个明文均 生成一个密文块)和**流來码(**处理连续输入明文流并生成连续输出的密文流) **來码的安全** 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 种其太手段 伯那代廖和学的其太值 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** 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其 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。 针对加密表 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: 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 -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 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研 解中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18 击. Data Encryption Standard 算法: 64bit 块加密. 使用 56bit 主密钥,先进行 始换位 然后进行 16 次相同迭代每次使用一个主家组生成的 48hit 子家组 最后再反过来 好相反 墊占 密组长度不够长 进代次数不够多 体加密管法 格 レ 比特的快速射为 レ 比 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* 12bit 已足够长. 为什么不使用 2DES? 中途攻击,若已有明-密文对,寻找Ek1(P1) $D_{lo}(C_1)$ 只需 2^{56} 的攻击量。 为什么 EDE 而非 EEE? 为了与单次 DES 美容 只需令 $K_1=K_2$ AES. 密码块链接(Cipher Block Chaining):若管 世 容易被重放攻击利用 家福捷链接(CBC):发送方生成一个随机初始向量 (V) c(0) 用明文发送给接收者:每一个明文块加密: $c(i) = K_c(m(i) \oplus c(i-1))$ 相 从开家组加索·对我加家質注·更求发送者和按此表使田园—个家组之 发送方洗择了一个密钥后,如何将密钥安全地传递给接收方?非对称加密篇 #详孝和这此者不共享廖组 #详孝使田加廖廖组 这此孝使田解廖廖组 不左右廖组传; 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 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 $K_B^-(K_B^+(m))$ = 不可能计算出私钥K。 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 个问题:入侵者知道该公钥和加密算法,可以据此发起 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: 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 $C = M^c \pmod{n}$,3.解密:对每个密文块C,计算明文 $M = C^d \pmod{n}$ 4.另 - 个重要的特性· $K_{-}^{-}(K_{-}^{+}(m)) = m = K_{-}^{+}(K_{-}^{-}(m))$ 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 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(又称称 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 1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)完整性检验 (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 可以通过加密报文来提供报文鉴别。 就点。混<mark>着了机密性和报文鉴别,不同时</mark>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 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 去一基于加密,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** 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 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+ 48(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),可用已复的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 希运算的报文鉴别很重要如果根据H(mlls) = h可以找到 ,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 $y \neq x$ 满足H(y) = H(x).在计算上不可能:该特性对于使 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 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 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 *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 5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),接收方不可能伪证 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: 的报文摘要H(m) 对收到的报文计算摘要 如果两老相符 表明报文是重 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. 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 主意到在生成 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 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: 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

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 每个 CA 拥有自己的私钥、负责为一部分用户签发证书: 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 的外 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 CRI 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在 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 CRI 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:-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 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代 协议/例如 可靠数据传输协议 路由选择信息交换协议或由子邮件协议/文前法行 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. 253 .<mark>0.</mark>直接发送一个报文. 入侵者可伪装成发送者. <mark>鉴别协议 ap2.0.</mark>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(IF wix 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 Truck 容听到 Alice 发送的明文口令 过后发送给 Bob 鉴别协议 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 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 (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 Alic 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 以如下方式使所 -**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,<mark>鉴别协议 ap5.0:采用公开密钥算法加修 不重数:K=(R), **Bob 计算**: K=(K=(R)) = R.只有 Alice 拥有这个私钥,因而一定是 Alice</mark> 509 单向鉴别服务: $A \rightarrow B$: $t_A ||r_A||IDB||Data||K_b^+(K_{a-b})||signature_A 为什么$ 如何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 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 E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 及的安全性. 例如,一个商业站点不能依赖 IP 层安全性来鉴别——个在该站点购到 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 而等待在网络尼上广泛州部署安全性 可能还需要未来若干在才能解决 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 Rob 且有该网 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 , 为了克服效率间题,我们利用了会话密钥,具体来说:1), Alice 选择 对称会话密钥K. 2).用这个对称密钥加密她的报文m.3).用 Bob 的公钥K.t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。得到对称密钥K。使用这个对称 密钥K.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 对她要发送的报文加应用一个散列函数H(例如MD5)从而得到一个报文摘要用 她的私钥K。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 报的散列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 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 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> 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 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 ode64(<mark>Kg*(K_{A-B})||K_{A-B}(Zip(Sgn||Data))),</mark>压缩,一方面可以减少要加密的数据量 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制 Encode64(K±1) 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示 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 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 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 ps). 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 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 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;服务器从浏览器选择 -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。-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 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 接关研SSL 类型段中指出该记录是否是用于终止该 SSL 会话的 SS 密性·通过加密 SSI 载荷实现 完整性·通过报文奖别码保护 过程;从上层接收—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 SL头,包括内容类型、SSL版本号、压缩数据块的长度等网络 III IPv4 在设计时没有考虑安全性缺少对诵信双方身份的鉴别。容易遭受地址欺骗卫 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. 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". 专用网 专用网诵讨由信专线将分散在各地的计算机(网络)连接而成的网络: 虚拟专用网(Virtual Private Network):建立在公用网上的 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 II参 I/PN 的宏理√PN 的曲 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用 条.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 v4 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,密销管理协议: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(Securit 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 或一对安全网关之间. 两者之间存放该 SA 状态信息:SPI;初始接口和目的拍 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)。 字放所有 SA 的状态信息. IPsec 数据报: IPSec 的使用模式运输模式:IPSec 头被插入至 原始 IP 斗和传输层斗之间 路由器根据原始 IP 斗转发数据句·隧道模式·原始数据句被主 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 乡 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 **阿种模式的比较**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部 来保证:隊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: 方流量分析. **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(陷 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,因而可抵抗重抗 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,准可以运行 改击. 封装安全载荷(Encapsulating Security Payload) ESP 数据包(载荷)大致分为以了

I 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 I 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 首語 初始载荷):ESP尾:包括填充(需要的话)、填充长度和下一 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** 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 舌面附上一个"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, i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 別報刊。版日主以上 新首部附加到戰荷之前(运输模式在第一部分缺少了初始 IP 首部)ESP 紡**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·原始数据句的载荷部分被加密 因而可提供数据机密性 HMAC 覆盖类 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,可抵抗重加 攻击-FSP 隧道模式由 原始 IP 斗曲被 HMAC 覆盖 因而 FSP 隧道模式可提供数据起源鉴 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 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 市。802-11年 選安全机制的 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。 102-11年 103-11年 103-1 重数:天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 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 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_S) IV [I=1,2,...] 第I个密钥K1 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_c, IV) 牛成相同的密钥流执行解密运算 $d_c = c_c XOR k_c^{IV}$ WEP 加密的安全 漏洞:每K。只有224个(Ks, IV)可用:IV会被重复使用:IV用明文传输:攻 的重用 攻击: Trudy(可能通过欺骗方式)让 Alice 加密他选择的明义 (d, d, d, d, d, \dots) :Trudy 能够获得 Alice 加密的密文: $c_i = d$, XOR k!V:Trudy 知道 c_i 和d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 $k_i^{IV} k_2^{IV} k_3^{IV}$. 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名 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(7 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的 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 其木早起由缑的作用,在家户和紫别服务器之间转发报文 31成对主**家组(PMK) 生成** MA 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 8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:防火塘和入侵检测系统: 防火墙: 在可信的内 那网络与不可信的外部网络之间执行访问控制策略的硬⁶ 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: **向过滤防火塘**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 th-TCP/LIDP 源端口号。目的端口号:ICMP 报文类型:TCPSYN 标志和 ACK 标志 句讨论 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 N部发起的 TCP 连接除非访问的具内网的公共 web 服务器→手套讲入的 TCP SVN 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一除 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 th 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 -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** 有相应的连接存在,状态检测防火炉可以跟踪 靈給香连接的狀态 成用网关应用网关除了检查网络层及传输层协议头 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·句讨逃防火炼阳襄所有不源自应用网关的 telnet 连接 应用网关的局限性每个 被代理的应用都需要一个应用网关。应用网关处理开销大速度慢,防火 折御 IP 欺骗攻击: 路由器无法知道句是否来自声称的源:应用网关外理开销大 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: | 容或者之间的关联 IDS: intrusion detection system 深度数据包检查: 查看 四内容(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 代感器? 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 每个使成器仅看到该机构流量的—部分 维拉能够更容易 **其于特征的 ID** 的一些限制:它们要求根据以前的攻击知识来产生一个准确的特征,换言之,对不得不记录的新攻击完全缺乏判断力另一个缺点是即使与一个特征匹配它也可能不是一个攻击 的结果,因此产生了一个虚假告警,最后,因为每个分组必须与范围广泛的特征集合相比 较。IDS 可能处于处理过载状态并因此难以检测出许多恶意分组。 基于异常的 IDS 最大的 特点是它们不依赖现有攻占的以前知识:在另一方面,区分正常流量和统计异常流量是