网络层的转发功能和路由选择功能做重要区分:转发涉及分组在单一的路由器中从一条入链路到 条出链路的传送。路由选择涉及一个网络的所有路由器,它们经路由选择协议共同交互,以决定分 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**结路层交换机** 基于*链路层字段*电 的信做转发决定。其他分组交换机称为路由器 基于*网络层字形*中的信做转发决定。网络服务模型 *网络服务模型*定义了分组在发送与接收端系统之间的端到端运输特性。在发送主机中,当运输层向 が、能由网络层提供的特定服务有确保交付: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**提供下列服务: •有序分组交付·确保最小带宽·确保最大时延抖 动•安全性服务,**因特网的网络尼**提供了单一的服务,称为*尽力而为服务*。 **康康縣和數据提阅簿** 机之间提供 无连接服务或连接服务。与运输层类似:网络层连接服务以源 目的主机间的握手开始;网络层无连接服务则没有任何握手预备步骤。运输层与网络层重大差异 1.在网络层中、汶些服务是由网络层向运输层提供的 ÷机到÷机的服务;在运输层中、汶些服务则 称为**虚电路网络**,仅提供无连接服务的称为数据报网络。二者实现面向连接的服务是根本不同的 运输层面向连接服务是在位于风 端系统中实现的,网络层连接服务除了在端系统中 ② 其行为: 传输分组前建立虚电路, 传输结束后拆除虚电路, 每个路由器。 成由路是一条: 为经过它的虚电路维护状态;路由器资源(带宽、缓存等)可以分配给虚电路,从而虚电路能提供 可预期的网络服务。 建文建电路的本质是预先选好源主机到目的主机的路径,此后分组仅沿选好的 路径传输、是否分配资源是可洗的。一条成电路的组成如下;源和目的主机之间的路径(即一系列 链路和路由器); VC号、沿着该路径的每段链路的一个号码(用于区分经计该链路的不同虑由路 沿着该路径的每台路由器中的转发表表面(进入端口 进入 VC 号 输出端口 属于一条虚电路的分组将在它的首部携带一个 VC 号。因为一条虚电路在每条键 每台中间路中器必须用—个新的 VC 号替代每个传输分组的 VC 号、该 表项。无论何时终止一条虚电路,沿着该路径每个表中的相应项将被删除。一个分组沿着其路由在 每条链路 F.不简单地保持相同的 V.C.号的原因: 减少了在分组首部中 V.C. 字段的长度: 大大简化了 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的 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 路由器按目的地址转发分组;路由器中的转发表记录目的地址到输出 链路的除射: 转发表被*迷路提供*修改 约1~5分轴更新一次。同一对主机之间传输的分组可能走 不同的路径,从而可能重线序。路中器转发表用分组的目的地址的**前缀**与该表中的表项进行匹配: 当有多个匹配时,路由器使用**最长前缀匹配规则**,即在该表中寻找最长的匹配项。虽然在数据报网 络中的路由器*不维持连接状态信息,*但它们无论如何*在其转发表*中*维持了转发状态信息。 <mark>康电路和</mark>* 来: ATM (成电路网络) 由电信网发展而来: 注重用户体验(用户付费). 追求高质 曼眼冬·依端于如能请很小如能·复办工作中网络空雨 以保持依端简单 Internet (数据探网络) 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的好处:可运行在各种链路之上;增加新服务只涉及终端。路由部 路由器的 4 个组成部分: 1.输入端口。将一条输入的物理链路与路由器相连接的 功能。需要与位于入铁路远端的数据铁路层交互的数据铁路层功能。查找功能。通过查询转发表决 定路由器的輸出端口。到达的分组通过路由器的交換结构将转发到輸出端口: #BL 当交換结构明 塞时、分组需在此排队; 控制分組(如携带路由洗择协议信息的分组) 从输入端口转发到路中洗 处理器:注意汶里的端□一词。是指路由器的参理输入和输出接□。2.交換结构。交换结构路由 器的输入端口与输出端口相连接,这种交换结构完全包含在路由器中,即它是一 网络13输出端口、输出端口,存储从交换结构接收的分组: 组装: 若需要 将交换结构输出的信息 组装成分组;排队: 若輸出端口来不及发送, 分组在此排队; 调度: 若有多个等待队列, 选择 队头分组发送;并通过执行必要的链路层(执行链路层协议, 封装) 功能在输出链路上传 输这些分组。4.路由选择处理器。执行路由选择协议,维护路由选择表以及连接的维路状态信息 执行网络管理功能。一台路由器的输入端口、输出端口和交换结构共同实 现了这种转发功能,并且总是用硬件实现。这些转发功能 有时总称为路由器转发平面。这些路由 **器控制平面**通常用**软件实现**并在路由选择处理器 (CPU) 上执行。 輸入端口: 转发表的一份**影**子 ■ 本通常会被存的存在分輪 λ端口、转发表从路由洗择外理器经过独立总线(例如一个 PCI 总线) 复制到线路卡。有了影子副本、转发决策能在每个输入端口本地做出、无须调用中央路由洗择处理 的推發。要用硬件执行查找,而且需要对大型转发表使用超出简单线性 搜索的技术 同时必须对内存访问时间除予特别学注,坚固许多其他动作; 检查分组的版本号 检 更新用于网络管理的计数器。交換结构 存交換:第一代路由器: 由传统计算机构成。洗路和交换都由 CPU 完成。交换通过拷贝完成:现 代路由器: 使用多端口内存连接输入端口和输出端口、控制器在端口之间传输控制消息、如存储地 中的存放协业 输出端口从指定的内存位置速取句 发问响应消息: 性能和代价取决于存储接口数 目、仅适合小容量系统、总转发吞吐量是内存写入或读出速率的一半并且不能同时转发两个分组 2经总线办格。交换结构中的总线包括册址线 数据线和控制线:每个输入和输出端口部有一个填 口硬件连接到总线上,每个端口被分配一个唯一的地址(内部标签);总线协议防止多个端口同时 传输,比如采用时分多路复用;各个输入端口在总线上较流广播分组,分组中携带输出端口的地址 各个输出端口使用地址讨滤器检查分组地址, 仅将发给本端口的分组缓存起来; 除了一个分组占用 总线其他必须等待。3.经互联网络交换:在输入端口与输出端口间建立内部专用电路。多对端口间 可以并行传输;分阴寒型与非阴寒型两种,阴寒型互联网络会产生阴寒;先进设计 2000年11日本 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;如果来自两个不同输入端 : 在输入端口和输出端口处 能够形成分组队列。*排队的位置和程度*(或者在输入端口排队、或者在输出端口排队)将**取决于** 流量负载、交换结构的相对速率和线路速率。当交换结构不能及时将输入端口的分组转移到输出端 口 输入端口的形成排队 排队带来的问题。以上阻塞、以上分组阻塞甘后分组的转发、重句。当 输入队列溢出时,发生美句; 当交换结构读率至少为端口读率的 n 倍时 (n 为输入端口数量). 以消除输入端口的排队,但路由器成本提高了。输入排队交换机中的线路前部(HOL)阻塞,即在 个输入队列中排队的分组必须等待通过交换结构发送(即使输出端口是空闲的),因为它被位于线 输出队列进时 发生手句:输出端口排队是不可避免的 设置多大的输出队列是一个问题:增大输 出队列:可以减少丢包的发生,但会增加内存消耗,并增大分组延迟(延迟太大的分组最终被重传 **分组丢弃策略: 弃屋:** 队列满时, 丢弃到达的分组; ≠动 以列管理: 在队列满之前就开始丢弃分组。如 RED 算法: 设计为和 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 (度) 当平均队列长度达到第 套橱索 n 手套到来的分组: 当平均队列长度达到第二个阈值max、时 手套每一个到达的分组: 摄 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 制平面: 网络范围的路由选择控制平面因此是**分布式的**。即不同部分(例如路由选 择管法) 执行在不同的路由器上并且通过彼此发送控制报文讲行交互。 因转网路由器和路由选择管 发和编址: 因特网编址和转发是*网际协议(IP)的* 重要组件。因特网的网络房有三个主要组件、IP 协议 路由选择部分(决定数据报从源到目的地 所流经的路径,算出转发表);报告数据报中的差错和对某些网络层信息请求进行响应的设施。因 产组被称为数据报。IPv4 数据报中的 **羊螺字段加下: • 版本号. • 首部长度** (4 字节为单位 IP./4 数据报可句念一些可变数址的洗项: 大 多数 IP 数据报不包含选项。一般的 IP 数据报具有 20 字节的首部)。\*服务类型。\*数据报长度 字节为单位: 首部加上数据长度 该字段长 16 比特 IP 数据据的理论最大长度 65535 字节). • 标 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 1; TTL 字段减为 ①该数据报丢弃。•6622到达其最终目的地才会有用;指示了数据报的数据部分应交给哪个特定的 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,一般会丢弃;注意到在 →路中器上必须重新计算检验和并再次存放到原外 因为 TD 字段以及可能的洗证 为什么 TCP/IP 在运输层与网络层都执行差错检测:在 IP 层只对 IP 首部计算了检验和. TCP/LIDP 检验和是对整个 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 TCP能运行在一个不同的协议(如 ATM)上,而 IP能够携带不一定要传递给 TCP/UDP 的数据。\*源

和目的 IP 地址。•泷项。•数据 (有效载荷)。如果数据报承载—个 TCP 报文段、则每个 (无分片的)

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。链路层帧能承

数据报可以被分片: 将数据报载荷划分为若干较小的数据块, 每个数据块封装成一个独立的数据报

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):最后一个分片

裁的最大数据字节数称为 MTII

不同类型的链路可能且有不同的 MTII. 传输过程中 较大的 IP

 其余分片的 MF=1: DF (don't fragment): DF=1表示不分许对数据据分片,分片报斗中的 以下字段需要修改: 总长度、偏移量、MF、头部检查和。由于偏移量只有 13 比特、除最后 其余分片的数据长度应为8字节的整倍数。假设原始数据报的报头长度为 H。则分片的数 H. N 为 8 的倍数。数据报分片的处理过程: 根据报头长度和输出线路的 MTU,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 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 申的以下字段: 总长度=H+数据块长度、最后─个报头的 MF 位置 0. 其余报头的 MF 位置: 编移量=数据块在原始数据报载荷中的字节序号/8、计算头部检查和。重组:将收到的分片重新约 装成原始数据报的过程称为重组、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> 确定属于同一个数据报的分片; 利用最后一个分片计算原始数据报长度: 原始数据报长度 值務量×8+分片总长度:细禁。将各分片中的数据快按照其在原始数据报载荷中的值移量重组、49 - 个新组经油区和-- 个新组定时器 · 使得系统面为复态 针对分片的 Dos 17:4: 改丰老贵详一系 列奇怪的分片,消耗目的主机的资源。IPv6 取消了路由器分片的功能:源主机发送探测报文, 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;路由器有多个接口 「接口。IP address.毎个网络接口对应一个 IP 地址、IP 地址是 数、通常用点分十进制数表示。为在因特网范围内保证 IP 地址的全局唯一性 每个将口必须具有 唯一的 IP 地址。子网 (subnet): 具有相同子网地址、不需要通过路由器就可以相互到达的网络相 构成一个子网。IP 编制为这个子网分配了一个地址 xvz.m/h,其中/h 的记法,又是称为**子网**排 码。指示 32bit 中最左侧的 h bit 定义了子网地址。如何确定子网2 将网络接口与主机/路由器分开 形成一些分离的网络岛,每个网络岛就是一个子网。路由器的每个端口连接 16bit (前两位 10), C 类 24bit (110), IP 广播地址(255.255.255.255)。 分类编址的缺点: 只能按 照三种固定的大小分配抽业空间 抽业浪费严重: 转发表必须记录每个已分配的网络 转发表现藏 爆炸式增长。CIDR(Classless InterDomain Routing): 按照实际需要的地址数量分配地址空间 故室: 允许将若干条转发表项讲 行聚合 减小转发表规模。按照实际需要分配地址 一个网络需要 2000 个地址,可为其分配一个具有 2048 个连续地址的地址块。这些地址的前 2. 位必须相同,从而可将其看成是一个具有 21 位子网地址的网络。*CIDR 地址分配的原则:* 地址块的 长度 L 必须是 2 的幂次;所有地址的前( $32 - log_*L$ ) 位必须相同。 网络地址的表示方法:用據碼 发数据报的原始情形: 直接交付: 节占 (源主和或目的路中器) 将数据包直接发送绘目的主机 (2 需要其它路由器转发);**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** 据包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**:节点查找转发表,将 数据包发送给下一个路由器。**直接交付的实现;**第五章。**参发表;**记录目的地址到输出端口的映身 取决于目的地址类型的不同,有*三类转发表项*:目的地址是一个*子网地址*,称*地址前缀表项*;目的 址被映射到一个*默认的*路由器端口。IP 采用逐跳选路:每个转发表项只记录去往目的地址的下一 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** 付其它路由器就可以直接到达)。 **维斯聚合**: 转发表中符合以下条件的若干个表项可以合并成一个 表项:这些表项的目的地址可以聚合成一个前缀更短的地址;这些表项使用相同的下一跳。地址 项;同时给出不能被娶合的表项;最长前缀匹配;在所有匹配的路由表项中,选择前缀最长的表项。 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调 出地址掩码(或 prefix-len 值), 计算包的目的地址前缀 (用地址掩码和包的目的地址相与). Dest\_addr 的地址前缀(Dest\_addr 与地址掩码相与)进行比较;**引入的问题:**地址前缀的长度 refix len 可以是任音值 Prefix len 无法从地址太身得到 只能从转发表项中得到 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**快速查找**是一个难题(已经解决)。*主机* T配置主机 IP 地址、服务器通常采用这种方法; 主机使用动态主机配置协议 DHCP 获取 IP 地址 子网掩码、缺省路由器、本地 DNS 服务器等配置信息。使用 DHCP 的好处:免去手工配置的麻烦 可用小量的IP 地址服务较多的客户(地址重用)。 DHCP 目标: 分许主机加入网络 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,子网中应有一个 DHCP 服务器 或一个 DHCP 代理。 DHCP 为主机发现新 IP 地址的四个步骤: 主机广播 "DHCP discover"报为 5,67 \yiaddr:0.0.0.0 \transaction ID:654),寻找子网中的 DHCP 服务器 Altrangaction ID-654 \Lifetime-3600sacs 讲行响应:给出推荐的IP 地址及租期,其它配置信息:主机用"DHCPrequest"报文(src0.0.00 主机流择—个 DHCP 服务器 向其请求 IP 协址(223124): DHCP 服务器用\*DHCP ack\*报文 \transaction ID:655 \Lifetime:3600 sec 发送 IP 地址 服务器响应客户的语求 确认所要求的参数: DHCP服务器使用 IIDP端口 67 客 使用 UDP 端口 68。 DHCP 不足之外: 从移动性角度看、结点移动时、不能维持与远 程应用之间 网络地址转换 (NAT): Motivation:使用一个公用 IP 地址支持许多用户同时上网 仅为公共可访问的节点分配公用 IP 地址(減小需要的公用 IP 地址数)。网络内部节点对外是不可见 的 (安全考虑)。 地址空间 10.0.0.0/8 用于家庭网络等专用网络或具有专用地址的**地域。NAT 实现 外出的数据据**将数据报中的(源 IP 地址、源端口号)替换为(NAT IP 地址 (不断分配)) NAT 转换表: 记录每个 (源 P 抽址 源端口号) 与 (NAT IP 抽址 NAT 端口号 后用转换表中对应的(IP 地址、端口号)讲行替换。16 比特端口号:允许一个 NAT IP 地址同时支 连后端到端面侧 (节占介 λ 修改 ID 抽址和端口导) NAT 标程 P2P 应用·NAT 口令在由部主动领 起的通信。 位于 NAT 后面的主机对外是不可见的; 但 P2P 应用要求任何对等方可以向任何其它 (参 RT 程序语录 NAT产生—个"洞" 将<10.001.3345>肿射到 <138.76.29.7.5001> 上: RT程序台语院 5001>发起TCP连排: NAT 将 <138 76 29 7 5001> 上收到的 SYN 旬转发给主机。使用中线服务器 实现 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 网络层上的一些信息。ICMP 报文有 询问和错误报告两拳: 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。*ICMI* ICMP 报文号作为 IP 有效整益承载的 从体系结构 F讲字号位于 IP シ F的: ICMP 通常被认为导 I 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: 报文类型有关 报告错误的 ICMP 报文句会触发该错误的数据报的斗架和前 8 个数据字节、Pin 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 Ed esponse 报文:源主机计算RTT,并报告;若源主机连续几次招时(收不到 Echo Response)。 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(经过的路路 器): 源主机的 Traceroute 程序向目的主机发送一个 Echo Request 报文 (包含) 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 TTI expired 报文 (IP报头中有路中器的 IP 排址): Traceroute 记录第一雕路中器的 IP 地址,然后向目的主机发送第二个 Echo Request 报文 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—个端口7 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 8、但与其它所有因特网协议都兼容。IPv6 地址: 128 位、使用冒号十六进制表示。 每 16 位 - 六进制的形式写成一组 组之间用冒号分隔 如"8000·0·0·0123·4567·89AB·CDFF"; IPJ6 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 数据报格式: 以一个 40 字节的基本头升 始、然后是数据。PRI (或 traffic class): 作用: 发送方在该域定义数据报的优先级、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 将网络流量划分为两大拳: 受拥塞控制的流; 非实时流属干汶一类。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; 实时多模 体流属于这一类,优先级 8~15、尚无标准、可以按照用户要求的服务质量等级定义。流 (flow) 特性 (源/目的、优先级、选项等)、并要求相同处理 (使用相同的路径和资源、 传输。数据报本传输的过程中可以被多次分片(但仅在目的端系统上而非路中器重组,分片的报头 具有相同的服务质量和安全要求等)的一系列数据句:途中源地址和途标签(flow label)唯一标识: 取自原始数据报。与分片有关的字段:新说:每个分片必须携带与原始数据报相同的标识:编移量:流标签由发送方分配,不支持流的节点忽略该域,支持流的路由器维护一张*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

、体理 IPv6 具条了对数据句讲行区分外理的能力。 IPv6 包格式: 与 IPv4 首部相比 IPv6 的基本斗 中去掉了以下一些字段: 选项: IPv6 的基本头总是 40 字节长; 与分片相关的字段: IPv6 路由器-负责分片: 头校验: 计算校验和太花时间, 现在的网络非常可靠, 并且链路层和传输层上往往又看 有校验和。IPv6 基本头中增加了: 流标签: 支持对数据包区分处理; 改变了以下字段的作用: Traffi 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 洗项"。 夫掉了源抑制报文,优先级和流标等允许路由器控制拥塞,丢弃不太重要的数据包,夫掉了一些7 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。从 IPv4 过渡到 IPv6: 双协议栈方案: 支持 IPv6 的主机和路由器同时运行 IPv4 和 IPv6; 运行 双栈的源节点先对目的节点查询 DNS: 若 DNS 返回 IPv4 地址, 发送 IPv4 分组; 若返回 IPv6 地址 发送 IPv6 分组: 双枝节 双株共占 (加路由黑 R) 在这颗探探传递绘 ID.// 路由黑 (加路由黑 C) →前 这 ID.6 探头鞋垫 B |Pv4 报头: 缺点: 报头转换不完全,有信息丢失。 **建立隧道:** |Pv6/|Pv4 边界路由器将 |Pv6 包封道 目的边界路由器取出 IPv6 包继续传输 的全部信息。**路由选择算法:** 什么是最佳略径: 应用评价: 路径长度、数据速率、分组延迟、通信 费用、安全性等; ISP 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 衛 路中稳定、健壮等路中评价指标通常是矛盾的 需要折衷。洗路算法分类。全局算法所有路 由器具有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 到邻居节点的链路代价,通过与邻居交换信息,进行迭代计算。*静态算法*路由随时间不变或缓 夸化(手工配置); 动态复法路由器根据拓扑及链路代价的夸化而自动更新路由。链路状态。 路算法: # **辞除状态洗路算法**为 **全局算法** 其 基本思想为: 每个节点利用可靠方法获得全网拓 抽象市一个带权拓扑图 计算到各个节点的最短路径。链路状态洗路算法包括 五个步骤; 发现邻居: 有结路直接相连的节点为邻居: 2 探测结路代价: 探测到每个邻居的代价: 3 构造结晶 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(6) 路状态广播管法): 5 计管路由: 利用收到的 15 分组构造网络拓扑 计简从太节占到其它各个节点 测度算法中)。 解决方案——个是强制费用不依赖拥塞。——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 思想:节点x测量其到各个邻居v的链路代价c(xv); 节点x估计其到达各个节点v的最小代价Dx(v) 这些代价构成了自己的距离矢量 Dx=[Dx(v);v∈N];每个节点周 节点×拥有每个邻居 v 的距离矢量 Dv=[Dv(v),v ∈ N]; 当节点×从各个邻居收到它们的距离。 量后。利用 BF 方程更新自己的距离矢量: $D_v(y) \leftarrow min_vc(x,v) + D_v(y)$ 。 节点的本地计算由以下两 ?在发现距离矢量 dx(v)有变化时涌知其邻民。*链路代价变化;好消息传播快。* 收敛速度: O(INIIEI)个报文、O(N2)次计算。距离矢量 DV: 距离矢量仅在发生变 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 **多的控制权 (管理自治):** 洗路算法的洗择。隐藏网络内部组织。自治系统 (AS): 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 被赋予一个 AS 编号,由 ICANN 分配 中的路由器运行相同的洗路协议(称 Intra-AS 洗路协议);不同 AS 中的路由器可以 T不同的 Intra-AS 洗路协议。 网关路由器: 在一个 AS 内、直接连接到其它 AS 的路由器: 网关 nter-AS 选路协议,所有 AS 必 行相同的 Inter-AS 选路协议。 Inter-AS 的任务 a架的路由器需发送数据报到 AS1 外 路由器应当向哪个网关路由器发送? AS1 的 了解哪些目的网络通过自己可达&&将可达性信息传播到 AS1 内部的所有路由器。 *魏土豆路由* 选择: AS 尽可能快地扔掉分组。这通过让路由器向某个网关路由器发送分组来完成。同时该 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: 置到外部网络的路由。*因特阿中的路由选择:*Intra-AS 选路协议也称*内部阿关协议 IGP*,最常见 有·RIP 较低层 ISP 和企业网使用: OSPE 较简层 ISP 使用、Inter-AS 洗路协议也称外部属学协议 EGP. 目前只有 BGP。选路算法和选路协议: 选路算法是选路协议的一部分; 选路协议还包括路径 <sup>七</sup>价的<mark>定义</mark>、报文格式、报文传输、报文处理、异常事件处理等具体实施方面的问题。 会系统内部的路由选择。RIP:RIP 采用 **距离生量**选路算法。 **距离(任价)**:用降数(ho 量。跳 (hop): 相邻路由器之间的链路为一跳。路径的跳数: 从源图 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: 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 网络最短距离: 发送 RIP 响应报文· RIP 报文封装在 LIDP 报文中发送 使用 LIDP 端口 水为路由选择表的 RIP 表 句括该路由器的距离向量和该路由器的转发表。 RIP 结路生效与恢复 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 发送 RIP 诵告: 采用毒性逆转解决计数至无穷问题: 若洗路表中到目的网络 x 的路由原 通告的、则向 A 通告该路由时、到 x 的距离设为 16 (阳 lt A 使用这条路由)。因特网内 OSPE: OSPE 采用链路状态洗路算法。链路代价: 由管理员配置(反映了管理员 洗路策略)。 OSPF 分相: OSPF 协议定义了 5 种分组类型,分别用干探测邻居、诵告链路状态等 OSPE 分组被封装在 IP 句中传输 协议是为 89。 路中器周期性损 或存链路 改变时发送 OSE 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证 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,计算以本路由器为相 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。 冬个**区域(area)** 每个区域运行自己的 OSDE 协议 区域内部的结路状态仅在太区域内广播 区 域边界路由器负责区域间的洗路。一个 OSPF 自治系统配置为若干区域: 一个特殊区域称为主子 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**的 **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 OSPE 协议: 每个区域边界路中器: 将太区域的洗路信息汇单( 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)通告给本证 域的内部路由器:对于未往其它区域的分组:首先转发到本地区域 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 与目标: 因结网却模拟其庞大日结构非常复杂: 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 (的路由 相不试图 (也不可能) 找到最佳路由。 边界网学练过 RGP: 当一对 AS 同音式 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 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 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) AS 可能有多个协。 R路中器 文些边界路中器必须通过坐永々 TCP 连续构成全连通 ウイ 之间的 BGP 会话称为内部 BGP (iBGP) 会话。BGP 定义了 4 种类型的报文: 1.打开报文: BGP 中器用来自动与邻居 RGP 路中器的群系: 2 保護报文: RGP 路中器定期交换保赁报文 生知对: 报文: BGP 路由器使用该报文宣布新路由、以及撤销以前涌告的路由。可达性信息: 以 AS 枚举用 式诵告的、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 的路由诵告 略表中,每个表项包含目的前缀(允许聚合)、下一跳路由器以及到达目的前缀的 AS 枚举形式通报完全路径: AS2 的 BGP speaker 通报: 128.96, 192.4.153, 192.4.32, 192.4.3 可从 < AS2 到法: AS1 的 BGP speaker 收到后通报: 128 96 192 4 153 192 4 32 192 4 3 可经路径< AS1 AS2: 到达。BGP speaker 内部的选路信息库由三部分组成: Adj-RIBs-In: 每个 Adj-RIBs-In 对应一个 BG 对等方、保存从该 BGP 对等方收到的选路信息; LOC-RIB: 已被该 BGP speaker 计算出来的最低 路由: Adi-RIBs-Out: 每个 Adi-RIBs-Out 对应一个 BGP 对等方。存放准备向该 BGP 对等方通告的 选路信息。BGP 讲程的处理过程: 接收从各个 BGP 对等方发来的更新报文。更新与之相对应的 Adj-RIB-In(添加、替换或删除路由):输入策略引擎对 Adj-RIB-In 中每条新的路由进行入境) (计速抑则中网络管理品定义) 结果可能是· 手套 按原样接受 接受伯修改某些属性(如值) 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低 装入 LOC-RIB: 输出策略引擎根据出籍过滤规则(由管理品定义) 计算要通告绘每一个 RGP 对包 方的路由更新,放入对应的 Adj-RIB-Out 中 (路由聚合也在这个阶段完成); BGP 进程利用

Adj-RIB-Out, 向每个 BGP 对等方发送路由更新报文。Intra-AS 和 Inter-AS 选路协议: Intra-AS

洗路协议·用于在AS 内部交换洗路信息 如 OSPE RIP 使用某个路由测度(代价)洗择到目的 话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) 的最优路径; InterAS 选路协议:用于在不同的 AS 之间交换选路信息,如 BGP,主要依据策 - 种**多项式编码**,它将一个比特串看成是某个一元多项式的系数。 冗余多项式 R(x): 由 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 《悬路由测度去寻找可达路径 (不迫求最佳路径)。 为什么会有不同的 AS 间和 AS 内部路由港 #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) 路由选择(broadcast routing): 网络层提供了从一种源铁点到网络中的所有其他结点交付分组的服 各: **多掃路由洗择(multicast routing)**使单个源结点能够向其他网络结点的一个子集发送分组的副 **路由选择算法:** 在**源节点上复制分组:** 低效: 相同的分组在某些链路上可能重复传输。 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 路由器负责转发到全网(在网络中复制分组); 网 络中产生的分组接贝曼小、在网络中复制分组;进行(flooding);节点收到广播分组后 向降 在有环的网络中,广播分组在网络中 外) 发送该分组的拷贝: 缺点 于休止特征获 浪费咨询 *是的进行*。日标·每个路由器仅转发它为前主转发过的广播分组·**面**数 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); 来的广播分组(该方法使用最多)。 反向路径转发 RPF 基本思想: 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 差分组的输入端口与去往该抽址的输出端口相同 则扩散该分组 否则丢弃分组: (ψ b) 复法合理 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 \*\* <del>据不会产生冗余的分组接贝。生成树的构造:基于核心的方法:</del>洗择一个节点作为核心(也称) 廖点);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。 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 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**。 络分组的目的地址设置为其接收者的**多福组地址**: 如何格格收者的 IP 地址与多福组地址 羊酥起来 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子 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惠开一个组: 如何将多播分组交付价值一个接收者: S福选路协议协调多播路由器建立到达所有接收者的路径树。多播组管理 IGMP 协议运行在主机 缘路由器之间: 主机利用 IGMP 协议向边缘路由器请求加入一个组、或离开一个组; 边缘路由 器利用 IGMP 协议向主机询问组成员关系;边缘路由器通过 IGMP 协议可以了解到,在它的某个端 >问 需要另一种协议来协调追及因特网内的名播路中器 路中到其最终目的地。后一个功能是中*网络尼多福路中港择管注*完成的。 *网络网中的网络尼多*森 是由两个互补的组件组成的: IGMP 与多播路由选择协议。IGMP 报文类型: 路由器到主机。确定主机所加入的所有名播组;membership report; 主机到路由。响应查询 ave group:可洗。不使用时,求助于数状态协议机制(如果状态未被显示地更新,则通过超距 **車件删除) 宏媛路由港报管法,日标**, 当每个组建立名塔鞋骨材(到法该组所有成品的路径树) 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 成员节点的路径向当是最佳的(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 谷转发名播分组。缺点: 路由器需要维护大量的名播树信息。 **组共享树**每个名播组使用一棵树 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: 个组,多播路由器只需维护一棵多播树; \$\dots: 多播分组使用的路径可能不是最佳的。 **基于源的树** 距离失量多据洗路:扩展 RIP 协议实现多播洗路的困难: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: 办法: RPF 广播: 确保名播分组到达每-ト島博園: 路径前枝・路中器删除不句金组成品的路径分支: 参与名場的主机定 所属的多播组,局域网上的路由器记录这些信息(IGMP);当路由器收到发往组 G 的多播分组,但 到组 G 的报告时,向上游路由器发送一个剪枝报文,上游路由器停止通 讨这个接口发送该组的名播分组; 如果一个路由器从它的每个下游路由器都收到前枝报文。路由 <S.G>树。*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 P 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。当报文到这 核心或已在树上的节点时,报文经过的路径加入到树中。组共享树的构造过程:希望加入多播组( 的路由器 S 向组 G 的核心发送单播的加入报文, 收到加入报文的路由器按照单播选路表 发加入报文,并在多播转发表中创建一条共享树记录<\*、G>: 报文到达的接口:标记为转发 G 的多 播分组的接口:向核心进一步转发报文的接口、标记为介许接收 6 的多播分组的唯一接口:当加 入报文到达树上的某个节点或核心时. 报文 分組**?**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 分组如何到达楼心**? 名播分组的目的地址为 G. 从源节点到核心的路径 F. 可能有路由器不在名播 建立隧道: 源节占路名播分组封装到一个单播分组中 单播分组的目的 协业为核心的单摆协业、最广泛使用的网络网络探路协议是 PIM:不依赖于网络中所使用的单摆 选路协议。PIM 有两种工作模式: 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 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。 (中器之间建立隧道: 把名播分组封装在单播分组中传输。 因特网中的名播路中器以及这些名播路 由器之间的隧道,构成了*因特网多播骨干网。SDN: 传统网络:* 每台路由器中的各个路由算法组件 在控制平面上相互作用,计算转发表(物理和逻辑上分布式路中)。控制层面:路中算法、路中表 数据层面: 转发表、SON: 路中器中地路中软件不存在了 路中器之间不在交换信息,在控制层面 有逻辑集中式控制平面: 一个独立的(通常是远程的)控制器与路由器中的本地控制代理(CAs)交互系 计算转发表 (逻辑上集中式路由)。可由多台主机组成。SDN 组成:交换机: 实现快速简单的广 x据平面转发(硬件实现)、存储控制器生成的流表。远程控制器:掌握各主机和整个网络状态 每一个分份计算出最佳的路由 为每个路由器生成正确的资素(链发素) **网络控制软件**。使用I 层 API 实现控制。核心思想:把网络地控制层面和数据层面分离,而让控制层面利用软件来控制裁 三类 OpenFlow 报文: 1.控制器到交换机: 特性: 控制器查询交换机的特性, 交换机响应; 配置 特定的交換机端口,将分组发送出去。2.交換机到控制器:packet-in: 格分组传送给控制器 flow-removed:流表表项在交换机上被删除;端口状态:为控制器提供端口改变信息。3.对等。 **网络层和链路层的关系:网络层:洗路:**路由器确定去往目的结点的下一跳,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: 将数据报从一个结点传输到相邻的下一个结点,**如: 源主机→源路由器 路由器→下一路路由器 目的路由器→目的主机、結構是無減。結点: 法行约

路层协议的任何设备。链路: 连接相邻结点的通信信道。 帧: 链路层分组称为链路层帧。链路层 的服务: 成帧(基本服务);链路接入(广播链路需要)在广播信道上协调各个结点的发送行为 **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结点正确收到每一个帧(停-等 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、避免接收结点缓存溢出(提供可靠交付的链路层协议、不需要专门的运 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 路接入 松错 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 **诱配器之间的通信。发详细,**这数据探封禁到帖由 生成核验补结 执行可靠传输和语言控制: 1 **收欄:** 提取帧、检测传输错误:执行可靠传输和流量控制:解射装数据报、交给上层协议。 **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: 护的数据 D (包括帧斗字段) 生成校验位 FDC (姜鳝检测和纠正比特) 添加在帧斗中: 收到的数据 D计算校验位 EDC'、根据 EDC'判定是否有错。奇偶校验:单比特奇偶校验:可检测单 括校验位错)。有利于检测突发错误。前向纠错(FEC): 接收方检测和纠正差错的能力; 优点 1607 所需的发送方面发的次数。允许在接收方立即纠正差错。避免了不得不等待的往返时延。而这些B 延易发送方此到 NAK 分组并向接收方重传分组所需要的 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图 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 松岭来 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。为什么运输局使用检验和而经 NBE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

法: R=D+2^r/G 的余式 (减法运算定义为异或操作)。检验方法: 若生成的编码除以 G 的余式为 0 对信息比特 101110 计算 CRC 码。101110000 + 1001 的会式为 R=011 (CRC code). 码字: 10111001 X G(X) = 1001,接收端收到比特串 1001001, **結路的兩种类型:** 点到点链路: 仅连接了一个5 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 多结点的单一共享链路。任何一个结点发送的数据可被链路上的其它结点接收到。冲突 (collis 在广播链路上 若两个或多个结占同时发送 发送的信号全发生干扰 导致掠败失败 **多价格入**机 议 (多路访问协议): 规定结点共享信道 (谁可以发送) 的方法 名址接入协议也称*继体接入控*制 (MAC) 协议。理想的多址接入协议: 在速率为 R bps 的广播信道上1.当只有一个结点发送时, 应能以速率 R 发送(信道利用率高)2.当有 M 个结点发送时,每个结点应能以 R/M 的平均速率 利用率高) 3.协议是完全分布式的: 不需要一个特殊的结点来协调发; 不需要时钟或时隙同步 (不需要额外的机制) 4. 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,每个结点固定分配一个子信道 . 轻负载时信道利用率不高; 随机接入 (竞争): 不划分信道。每个结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 分协议: TDMA (时分多址): 将信道的使用时间划分成帧。每个结点在帧中被分配一个周 (一个时间 N 个时隙),每个时隙可以发送一个分组 结点只能在分配给自己的时隙内发 若结点不发送 其时階於空。FDMA (類分多址); 格信道频谱划分为若干子频带 每个结点 被分配——个固定的子频带(R/N 带客) 若结占不发送 其子频带空闲。TDM 和 F 除碰撞而且非常公平; 结点被限制于 R/N bps 的平均速率, 必须总是等待它在传输序列中的轮发 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), 每个结点被分配一个 -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 chi rade 的反似:信号基加:多个结点发送的信号在信道中线性相加:接收方解码:用发送方的 ch 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** 报: 当结点有数据要发送时,以信道速率 R 发送,发送前不需要协调;随机接入 MAC 协议规定包 划分为签长的时隙 每个时降传一帧:结点只能在时隙开始时发送:结点是时轴同步的(知道时) 何时开始): 所有结点可在时隙结束前检测到是否有冲突发生。操作: 结点从上层收到数据后. 一个时隙发送;若时隙结束前未检测到冲突,结点可在下一个时隙发送新的帧;若检测到冲; 个时隙中以概率 P 重传,吉至发送成功。优点。 单个活跃结点可以信道速率语 维发送,分布式:结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,由于概题 新任 有此时除被闲罢 季惠时轴同先 **时除之路访问协议的贫寒**,当网络中存在于曼廷研结点总 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 个活跃结点 每个结点在每个时隙开始时以概率 p 发送; 给定结点在一个时隙中发送成功的概率= p(1-p)^(N-1 给定时隙中有结点发送成功的概率 =  $Np(1-p)^{\wedge}(N-1)$ ; 最大效率; 找到令  $Np(1-p)^{\wedge}(N-1)$  最大的概 基本思想: 取消同步时钟 任何结点有数据发送就可以立即发送 结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X **穿的情形:** 在时刻 t0 发送的帧与在 [t0 - 1:t0 + 1] 时段内发送的其它帧冲突。 P(给定结点发送成功)=P(结点发送)+P(无其它结点在ft0-1:t0)内发送)+P(无其它结点在ft0.t0+1)内发 送)=p(1-p)^(N-1)\*(1-p)^(N-1)=p(1-p)^2(N-1); 求出令结点发送成功概率最大的 p\*, 1/(2e) = 0.18. *载波信听多址接入 (CSMA): 两个重要的规则:* 发送前监听信道 (carrie 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);碰撞检测,即当一个传输结点在传输时一直在侦听此信道,如果它检测到另一个结点正在传 输干状帧 它就停止传输 在重复"你听-当空闲时传输"循环之前等待一段随机 结点可能没有监听到其它结点正在发送; 即使忽略传输 识、当两个(或名个)结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。 传播时延在决定其性能方面起关键作用。CSMA/CD (Collision Detection): 基本思想: 在发送的 付程中检测冲率(发生冲率时信号较强):检测到冲率后 立即停止发送剩余的部分:立即启动;; 突解决的过程。以太网采用 CSMA/CD 协议: 1.NIC 从网络层接收数据报、构造以太帧; 2.若 NIC 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, 然后发送帧; 3.若 NIC: 送完整个航而没有检测到冲突 认为发送成功!: 4 若 NIC 在传输过程中检测到冲突 立即停止发 送帧, 并发送一个阴塞信号(加强冲突); 5.中止传输后等待 回步骤 2。我们希望时间间隔应该这样;当碰撞结点数最较小时、时间间隔较短;当碰撞结点数量 较大时,时间间隔较长。二**讲制指数后误算法**: 当传输一个给定帧时,在该帧经历了一连串的 次碰撞后,结点随机地从 实际时间是 K+512 比特时间 n能够取的最大值在10 以内, 指数同语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, 不考虑近期付金 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 。CSMA/CD 效率: Tprop = 以太网中任意两个结点之间传播延迟的最 大值: Ttrans = 最长帧的传输时间: efficiency = 1/(1 + 5\*Tprop/Ttrans)。在以下情况下,以太 网的效率趋近于 1: Toron 趋近于 0. 或 Trans 趋向于无穷。结论: 应控制以太网的 协议: ALOHA 和 CSMA 协议具备理想多路访问协议的第一个特性, 但不具备第二个 **砂油棉沙**,结占>一被指定为主结占 主结占以循环的方式砂油每个结占 主结占首先向结占 发送一个报文,告诉它能够传输的帧的最多数量,在结点 1 传输了某些帧后,主结点告诉结点 它能够传输的帧的最多数量(主结点能够通过观察存信道上是否缺乏信号、来决定一个结点何时写 □ 下午午午前取得高得多的效率;第一个缺点是 tiff 即通知——个结占"它可以传给"所需的时间 例如 加里只有——个结占是话既的 那么? ↑结点将以小干 R bos 的速率传输,因为每次活跃结点发送了它最多数址的帧时,主结点必须依次 轮询每一个非活跃的结点;第二个缺点是<mark>单点失效</mark>,主节点有故障,整个信道都不可操作。**令牌** 遊协议:没有主结点。一个称为今牌(token)的小的特殊帧在结点之间以某种固定的次序进行交换 一个结点收到令牌时,仅当它有一些帧要发送时,它才持有这个令牌;否则,它立即向 点转发该今牌;一个结点收到今牌时,若它确实有帧要传输,它发送最大数目的帧数,然后把令制 转发给下一个结点。优劣: 令牌传递是分散的,并有很高的效 如果一个结点偶然忘记了释放今晚。则必须调用某些恢复步骤使今晚返回到循环中来 传递证识。MAC 协议比较: 信道划分 MAC 协议: 重负载下高效: 没有冲突。结点公平使用信道 经负载下低效: 即使只有一个活跃结点也只能使用 1/N 的带宽。随机接入 MAC 协议: 经负载 高效· 单个还既结占可以使用整个信道: 面负数时低效· 频繁发生冲突 信道使用效率低, **砂液**量 议(试图权衡以上两者):按需使用信道(避免经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)。 交換局域网: 局域网 LAN (Local Area Network): 将小范围内的计算机及外 设连续起来的网络 范围在几公里以内 通常为个人或机构所有: *城域网 MAN*:通常覆盖—个城 (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 名: 广域网 WAN (Wide Area Network): 诵常覆盖一个国家或一个洲(一百公里以上). 规模和 **坳址、硬件坳址、结路层坳址或 MAC 坳址**等。MAC 坳址长 6 个≤ 配器的地址是全球唯一的: 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; 现在用软件改变网卡的 MAC 地址也是可能的。主机或路中器的循配器(加网络接口)且有铁路层地址 因此 且有名名 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 (沙此接口是与土利和路由奥相连的) 相关联的斜路层操业 汶县因为斜路层交换机的任务县2 主机与路中器之间承载数据报;交换机诱明地执行该项任务。这就是说,主机或路中器不必明确; 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、地址员 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 适配器仅将发送给本结点的帧交给主机:目的地址为适配器 MAC 地址的单播帧,所有广播帧。 定接收的多播帖。主机和路由器接口除了网络尾锄业之外还有 MAC 锄业原因:品域网是为任意风 络层协议而设计的, 而不只是用于 IP 和因特网; 如果适配器使用网络层地址而不是 MAC 地址的设 网络层地址必须存储在话配器的 RAM 中、并且在每次活配器移动(或加电)时要重新配置、另 种洗择是在活配器中不使用任何地址, 让每个活配器将它收到的每帧数据(通常是1)数据报)沿 协议栈向上传递 然后网络层则能够核对网络地址层是否匹配 这种洗择带来的一个问题是 主机 将被局域网上发送的每个帧中断,包括被目的地是在相同广播局域网上的其他结点的帧中断。 **建理直接空付?** 当发送结点 A. 擦收结点 B. 位于同一个子网络上时 数据报可从 A. 直接空付给 B. A 的网络层将数据报、以及 B 的 MAC 地址交给适配器;适配器将数据报封装在一个链路层帧中 帧的目的地址=B的 MAC 地址, B 的话配器收到帧。根据目的地址判断是发绘本机的。取出数据

交给网络层。**发送结点获得接收结点的 MAC 地址方法: 地址解析(Address Resolution)问题:** 交换机根据帧的到达端口、源 MAC 地址或源 IP 地址(取决于 VLAN 的划分方法),查找 VLAN 配 (做);通信者将包发送给外地代理;外地代理将包转发给移动结点;移动结点直接向通信者发送。 <del>節态映射 IP 地址 - MAC 地址的缺</del>点:主机每次使用的 IP 地址可能不同(DHCP),主机可能更换网 置表;为<u>避免重复查找</u> 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 卡。地址解析协议 (ARP) 用于动态获得 IP 地址-MAC 地址映射。在以太网上,ARP 报文封装 以太帧中传输。**增址解析的过程:** A 想知道 B 的 MAC 地址: **1.** A 构造一个 ARP 请求,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 请求的结点用目标 IP 地址与自己的 IP 地址比较。地址相符的结点进行 响应 (B 响应)。4. B 构造一个 ARP 响应, 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: 每个结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 请求中莽取协业继定信息。 每个结点可以收 到全部的 ARP 请求报文,可将发送结点的地址映射缓存到自己的 ARP 表中;结点 A 在启动时主 广播一个 ARP 请求,在目标字段内填入自己的 IP 地址,收到 ARP 请求的结点将 A 的地址映射级存起来,若 A 收到 ARP 响应,报告 IP 地址重复错误。 ARP 是即播即用的,一个 ARP 表是自动建立 - 个 ARP 分组封装在链路层帧中,因而在体系结构上位于链路层之上。然而,一个 ARP 分组 具有包含链路层地址的字段,因而可认为是链路层协议,但它也包含网络层地址,因而也可认为是 为网络层协议。最好把 ARP 看成是跨越链路层和网络层边界两边的协议,即不完全符合我们在第 1 音中学习的简单的分层协议栈。数据报到达子园之外:数据报从 A (子园 1) 经讨 R (路中器) 到达 B (子网2): A 知道下一跳地址为 111.111.111.110 (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 111.111.111.110 对应的 計 (R-1) (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-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。對業 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, 也是目前占主导协位的有线局域网技术:与其它的局域网技术相比 技术简单 成太师: 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),所有结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): 一个物理层中继器, 从一个端口进入的物理信号(光电), 放大后立即从其它端口 输出,集线器相当于共享电缆,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工链路,交换式以太网不会产生冲突,不需使用 CSMA/CD 协议!逻辑星形拓扑: 各结点仅与中心结点直接通信 各结点之间不直接通信: 其于集线器的以太网为物理星型拓扑 報总线拓扑。*以太网帧结构: (按顺序)* 前同步码: 7 个 10101010 字节,后跟一个 10101011 字 用于在发送方和接收方之间建立时钟同步。目的地址 (6 字节) +源地址 (6 字节)。 Type (2 字节): 指出 Data 所属的高层协议(如 IP、ARP等)。每个协议有一个编号。用于多路分解 (和网络层数据报中的协议字段、运输层报文段的端口字段类似)。Data: 46~1500 字节,不 46 字类情态变 46 字类:以太园的最大传统单元(MTIN是 1500 字类,没会味差加果 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数据报首部中的长度字段来去除填充部分。CRC (4 字节,循环冗余检测): 对 destaddr, src addr, type 和 data 四个字段计算得到 CRC 码。所有的以太网技术都向网络层 意味着没有握手。以太网技术都向网络层提供不可靠服务, 对该帧执行 脸。但是当该帧通过 CRC 校验时它既不发送确认帧;而当该帧没有通过 CRC 校验时它也不发送 定确认帧,当某帧没有通过 CRC 校验,适配器 B 只是丢弃该帧。(在链路层)缺乏可靠的 政简单和便宜。但是它也意味着传递到网络层的数据报流能够有问题。 **为什么有最小成** 长的要求? 为确保结点在发送结束前检测到冲突, 帧的发送时间必须足够长; 结点检测冲突需要时 间,假设信号在相距最远的两个适配器之间的往返延迟为 2r、则帧的发送时间不应小于 2r、即帧 的最小长度≥ 链路速率 2r、为什么最小帧长为 64 字节 (不包括前号码):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: 链路层 & 物理层: 历史 上出现过许多不同的以太网技术: <mark>链路层相同:MAC协议,帧格式、帧处理; 物理层不同:传输</mark> 媒体: 光纤, 同轴电缆, 双纹线; 数据速率:如 10Mbps, 100Mbps, 10bps; 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 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(结点数量)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。 交換式以太网的最小較长及规模: 交換式以太网不再使用 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。66
66
67
68
68
68
68
68
69
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70
70 主机和路由器是透明的。交換机輸出接口设有缓存。过滤是决定一个帧应该转发到某个均 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 上型上层上型的发生引发。交换机的过滤和转发槽勒于安全的发展。如此的原理。但含果用原则上某些,然此的交换机功能,交换机的过滤和转发槽助于皮类的感用圆路时间,接收 其初的路由路的E不必是全部的表现。交换机表现的大量,一个MAC单性,通向该 MAC 方。如果成功设置他,则在短时间间隔15万后发达 ACK 采用能物的间路时间,接收 地址的交換机接口,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 发分组其干 MAC 地址而不是其干 IP 地址日交换机表与路由器的转发表的构造方式有很大差别。 的过滤和转发、自学习: 当帧到来时,1. 记录帧的到来端口; 2.用帧的目的 MAC 地址查找端口转 发表(转发决策):if 找到目的 MAC 地址 (已知结点) then { if 目的地址所在端口=帧的到来端口 the 丢弃(讨逑不需要转发的帧) else 转发帧到表项指定的端□(按转发表转发帧) }else 扩散帧(未 知结点,采用扩散法转发)(向输入端口以外的所有端口转发)3.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; 该帧源地址字段中 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 业的帧,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 多干一个帧。•最质的链路:交换机路链路彼此隔离 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、交换机也易于进行网络管理。交 操机和路由器比较。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。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 **为优点和缺点**: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, 换网络的沃旺拓扑限制为一棵生成树 一个大型交换网络将要求在 主机和路内器中有大的 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协之间的最佳路径 它们介许以主意的拓扑结 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(它们以及连接到他们的主机器需要配置 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 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 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"架能的"路由。 **级群交换机**, 多个交换机也可以级群在一起 形成更大范围的局域网。 交換机 S1 如何知道应转发给 S4. 而 S4 如何知道应转发给 S2? 自主学习! (与单交换机情形相同)。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(各种帧),可被冲突域中的其它主机接收到。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)。但在逻辑上应连接在同一交换机上; 在同一交換机上的主机。在逻辑上、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 VI AN: 位于物理局域网上的一个逻辑 IP 子网 句念了配置为该 VI AN 成员的所有结点。 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 較流量被限制在该 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 配置完成。VIAN 的实现基础是支持 VIAN 功能的交换机。管理局配置 VIAN: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 置表。指出涌讨哪个端口可以到达哪些 VI AN 的成员 (一个交换机端口可以到达多个 VI AN 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:根据用户结点的 MAC 地址划 VLAN;基于 IP 地址划分:根据 IP 子网地址划分 VI AN. VI AN 干线连接: 将两个 VI AN 交换机 互联. 交换机 如何在 VI AN 间转发触: 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 所有端口上转发转。如何知道一个转属于哪个 VLAN: 帧所属的 VLAN = 发送结点所属的 VLAN:

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。802.10 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、日支持 VLAN 的交换机添加 VLAN 字段。由路径上最后一个这样的交换机夫掉 网络作为研路层: 多协议标签交换 (MPLS):是一种分组交换的虚电报网络。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(而不是最短前缀匹配) 快速查 找;借用虚拟电路(VC)的方法;但 IP 数据报仍然保持 IP 地址 I 标签交换路由器:仅根据标签值(不检 春 IP 抽址)将报文转发到出接口。 夏溪楼: MPIS 转发决策可能与 IP 目的抽址和源地址不同 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**备价路径**快速重新路由流 (X VolD有田) ID 路由到日的抽的路径仅由日的抽抽补决定 MDIS路由到日的抽补的路径可以其干 源地址和目的地址。一个 MPLS 加强的帧只能在两个均为 MPLS 使能的路由器之间发送。 回廊: 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 客户一服务器交互: TCP 和 HTTP:

**多述。无线网络的组成,无线主机**,运行网络应用。可能静止或移动(无线并不一定音味着移动 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; 通常负责协调与之关联的多 ↑无线主机的传输。**无线链路**:连接无线终端和基站,需要 MAC 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 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,结点只能与其通信范围内的结点通信,结点相互帮助转发分组 每 路由器。切換:无线终端接入到不同基站的过程。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: 主机通过多个无线结点的 中继才能到法周完网络(加于维网法网络)3.单辈子基础设施。于其站 不连接到周定网络 结点 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,结点间通信需 要通过其它结点中继(如自组网、车载网)。 无线链路和网络号配: 无线链路的特性: 信号表減: 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 受限、误码率很高。信噪比(SNR):更大的信噪比更容易提取出信号。信暖比与误码率的权衡; 给定 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层,给出最高 的吞吐量: **信噪比可随移动性变化**:动态诱应物理层(调制技术 读率) **于线网络的结性: 隐藏终端间** 题: A和C正在向B发送;由于信号强度衰减,A和C所处的位置使得他们的信号强度不足以使 他们相互检测到对方,但足以在 B 产生冲突。 CSMA 不适合多號无线网络: 通过载波侦听,发送结点只能知道其周围是否有结点在发送; 但真正影响此次通信的是接收结点周围是否有结点在发送。 隐藏结点:不在发送结点的通信范围内、但在接收结点通信范围内的活跃结点。(发送结点听不到, 但影响接收) 暴露结点: 在发送的通信范围内、但不在接收结点通信范围内的活跃结点。(发送结 点能听到,但不影响接收)CDMA:所有用户共享相同的频率,但每个用户都有自己的 CDMA 代 码来编码数据;许多个用户"共存"并以最小干扰同时传输(代码是"正交的");编码: $Z_{i,m} = d_i * c_m$ 解 码:  $D_i = \sum_{m=1}^{M} Z_{im} * c_m/M$ ; WIFI: 802.11 无线 LAN: 802.11b: 2.4-5 GHz range, up to 11 Mbps. 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 体系结构。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 (中央基站);每个无线接口 AP) 均有一个全局唯一的 MAC 地址。802.11 信道与关联: 802.11 将通信频段划分或若干信证 SSS 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 AP 发送的信标帧(周期性发送,包含 AP 的 SSID 和 MAC 地址),选择 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:被动扫描:被动扫描: 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 《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(隐藏结点)。因此,一旦开始发送一个帧之后,它就完 全的发送该帧。目标: 避免冲突 CSMA/C(ollision)A(voidance)。以太网和802.11 都使用载波侦修 **随机接入,但这两 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(ARO)方案。链路层确认方案: 发送方: 1.初始时站点监听到信道空闲。它将在一个分布式的 IIII (DIFS) 的段时间段后发送该 帧。2.否则 该站点洗择一个随机回退值,并在监听信道空闲时递减该值,如果繁忙则冻结计数器。 3.如果计数器减为 0.该站点发送整个帧并等待确认。4.如果收到确认,并且想要发送第二个帧,或 撞冲突,当两个站点同时进入随机回退状态时,时间短的先发送并且阻塞时间长的,有效避免了碰 撞。 为什么要用链路层磅认: 难以检测碰撞且结点不能中断,接收方只会在没有碰撞时确认帧。 4 雄。另什么安元就看法师的,推议他的观量互动点不能中心,接收刀穴云在汉号被撞的所以他。 *路层确认可以完全避免碰撞吗:*不能。可能有隐藏结点的问题,两结点可能选择了接近的回退时间。 处理隐藏终端: RTS 和 CTS: 操作方法: 假设 A 欲 AP 发送一个数据帧: A 向 AP 发送一个 RTS 帧 帧中给出随后要发送的数据帧及确认帧需要的总时间; AP 收到后回复一个 CTS 帧、帧中给出同样 的时间; A 收到 CTS 帧后开始发送; AP 收到帧后, 发送一个 ACK 帧进行确认; (A 附近) 收到 RTS 帧及(AP 附近)收到 CTS 帧的结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。此机制只对长数据帧使 用。CSMA/CA 与CSMA/CD的不同:最根本的不同:CSMA/CD 在发送过程中检测冲突,而 CSMA/CA 在发送过程中不检测冲突; 由此带来的协议处理方面的不同: 在 CSMA/CD 中, 结点侦听到信道空 闲时立即发送;在 CSMA/CA 中,结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 更尺可能避免 RO2.11 輪旋子, 四个掛か字段, Address 1: 輔約日的 MAC 掛け、 Address : 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 addres . = 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 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 seg # (for reliable ARO), frame type (RTS, CTS, ACK, data)。802.11 终端在 IP 子國内移动: 切棒: 终端从一个 BSS 移动到另一个 BS 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 吉林帧;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 ÷切换时 交換机 (连续 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, # F的应用正常运行: 由于 IP 地址设变 网络黑及以 F E 次成份不到这个移动 切换过程中产生 的延迟及丢包,在上层协议看来是正常的。<mark>802.11 先进功能: *速率适应*: 当主机移动或信噪比变</mark> 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 帧被取消或超时,继续回落。*功率管理*:结点设置功率管理比特,告知 AP 它将进 入休眠状态: 结点进入休眠 并在下一个信标帧之前醒来: 在结点休眠期间 AP 缓存发往该结点 的帧; AP 在发送的信标帧中包含一个移动结点列表,这些结点有帧缓存在 AP 中; 列表中的结点 向 AP 请求帧,其余结点重新进入休眠。 終端在 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,不能保留其 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; 即使对方兹如了效端的新抽址 应用必须重新建立连接 因为通信的套接字本了 内层网络, 移动 结点的永久"居所"(e.g.128.119.40/24)。永久兼址:移动结点在归属网络中的地址,总是可以使用这 个地址与移动结点通信,即使移动也保持不变(e.g.,128.119.40.186)。**归属代理:**当移动结点在外 地时, 为移动结点执行移动管理功能的实体。外部网络: 移动结点当前所在的网络(e.g. 79.129.13/24)。 外部代理:外地网络上为移动结点执行移动管理功能的实体。转交地址:外部代理地址 en 79 129 13 2)。通信書: 希望与移动结占通信的结点。移动结点注册: 移动结点讲入外协网络后 向外地代理注册;移动结点通过外地代理向归属代理注册;最终结果:外地代理知道移动结点在本 地网络上;归属代理知道移动结点的转交地址,记录到地址绑定表中。间接选路到移动结点:通信 者在数据包中使用移动结点的永久地址;归属代理薪蒸数据包、转发给外地代理;移动结点直接将 响应发送给通信者。间接选路:三角选路问题:移动结点使用两个地址:永久地址——通信者用来 向移动结点发送数据报(从而移动结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结点转发数据报;三角选路:通信者-归属网络-移动结点;当通信者和移动结点在同一个网 各中时很低效。*间接选路:终端在外地网络间移动:*假设结点移动到另一个网络:向新的外地代理 地址向移动结点转发包;结点移动及变换外地网络等**对通信者都是透明的:正在进**行

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结点的转 交掛址 通信者(包括固定结点)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、移动结点注册;标准化了 ·个部分:代理发现,向归属代理注册,数据报间接选路。代理发现:愿意充当归属代 理的路由器定期在网络上发送代理诵告,宣布自己的存在及 IP 地址:愿意充当外地代理的路由器 在代理诵告中会提供一个或多个转交地址(诵常使用自己的 IP 地址作为转交地址);移动结点诵讨 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 个作为自己的转交地址。向归属代理注册: 移动的 动结点从外地代理提供的转交地址中选择-<mark>小地代理发送一个注册请求</mark>,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、 冊去念等: 外协作理记录结点永久 IP 协计 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,将移动结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 到有效的注册响应员 络移动结合记录本自己的转发表由 向移动结合转发注册响应 当移动结合 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,获得移动结点当前的转交地址 据包转发给移动结点。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 结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 以菲取移动结点的 MAC 协业:利用得到的 MAC 协业 格数据报酬装到链路层帧中发送: 姜通信 者在归属网络上:通信者查表得知移动结点直接可达、于是查找 ARP 缓存或者发送 ARP 请求、 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: 移动结点的永久地址应当映射到归属代理的 MAC 地址。ARF 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,刷新其它结点的 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, 目的地址为移动结点的永久地址, 计 移动结占的转交册业位于外册网络, 将目的册业在归属网络的数据报送认外册网络, 修改目的册业 =转交地址(×)(不改变目的地址,对上层协议透明; COA 为外部代理地址); 使用隧道(√)( 道技术的又一个应用例子)。归属代理通过隧道转发数据句:归属代理向外地代理发送的句:Sro 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) 外地代理向移动结点发送的包:通信者发送的原始包。外地代理如何转发数据包到移动结点?外1 代理解制收到的数据包。得到原始数据报: 外继代理如何获得移动结点的 MAC 地址? 在移动结点 注册阶段,外地代理获知了移动结点的永久地址和 MAC 地址,记录在其转发表中;外地代理根据 目的 IP 掛价查找转发表 得到移动结点的 MAC 掛价: 外插代理利用移动结点的 MAC 掛价 格数 据报封装到链路层帧中,发送给移动结点。*移动结点如何发送数据包*?移动结点将数据包发送给外 地代理(缺省路由器): SrcIP=移动结点永久地址, DestIP=通信者 IP 地址, SrcMAC=移动结点 MAC DestMAC=外地代理 MAC: 外地代理按照下常方式转发数据句。移动结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 路带来的问题: 误码率、手包率、征识增大。结点移动带来的问题: 手包、征识增大。逻辑上、设 十么影响: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 必要地減小拥塞窗口,导致应用吞吐率很低; 无线链路、有线/无线混合链路上的 TCP 拥塞打

•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 **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 经过一股时间后重要 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。 **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 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 福(分组家福): 每次外理一个旧文块 生成一个家文块 滚家福; 外理连续输入的旧文流 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 · 有家组是要要隐藏的。——个加家管法被称为是**计算安全**的 如果由该管法产生的**家文准足以下**面 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 Papa和学由 - 廖和的中全性具通过管注的复数性和廖知的并度李保证的 - **对数廖**4 **換密码:** 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 母映射表。換位密码:保留明文字母不变,但改变字母的位置;例子:列换位密码 针对加密系统的密码分析改击; 唯密文改击; 密码分析者仅能根据截套的密文进行分析 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 —此户知的"田文-家文对"来帮助破泽家和 以得出家组: 洗择朋女改击,家和分析者可以洗择-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。块加密算法:将 比特的块映射为 k 比特密文。密码块链接(Cipher Block Chaining): 若每个明文块被独立加速 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): 发送方生成一个图 机的初始向量(IV) c(0). 用明文发送给接收者; 每一个明文块加密算法;  $c(i) = K_s(m(1) \oplus c(i-1))$ ○牛類外的大量帯密(只数 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 而后與是要要在協议中提供机制分发初始向量 (IV) CO 要求发送者和接收者使用同一个密钥:存在密钥传递问题:发送方洗择了一个密钥后.如何非 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;加密密钥是公开的、解密密钥是私有的。 公开密钥量 法的使用: 每个用户生成一对加密密钥和超密密钥: 加密密钥放在一个公开的文件中, 超密密钥妥 善保管。公开密钥和私有密钥:公开密钥(K+):加密密钥,由发送者使用;私有密钥(K-):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 #**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 公钥和加密算法,可以据此发起冼择明文攻击; 加密密钥是公开的,任何人都可能向 Bob 发送-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 正实了发送方的身份,然而在公钥体制中,这点就行不通了,因为任何一个人都可向 Bob 发送使 用 Rob 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继定起来。 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 = p+q 和 z = (p-1)+(q-1); 选 接一个与z 互质的数、令其为 d; 找到一个 e 使满足 e-d = 1 (mod z); 公开密钥为(e, n), 私有密钥为 (d, n)。 **2.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; 3.解密方法: 对每个密文块 C, 質 M = C^d (mod n). M 即为要求的明文。4.另一个重要的特件: 先用公钥再用私钥和先用私钥 N公钥结果相同。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。 超文完整 性和數字签名: 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。报文奖别涉及 两个方面 起源奖别。报文是否来自责 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 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。 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。密码散列函数: **列承数 H 心满足的特件:** 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 T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(m+s)=h 可以扎 到一个 x, 使得 H(x)=h, 那么根据 x 和 m 可以推出 s; 对于任意给定的数据块 x, 要找到一个 y≠ 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,如果能指 到一个不同于x的数据续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。**數列函数标准**: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 比特报文 注册: 新的外插代理向归属代理注册: 归属代理更新移动结点的转交曲址: 归属代理使用新的转交 接要: 羅文塞剛福 (MAC) 使用家福教列商教 (contagraphic hash function) 生成报文鉴别码: 发送方用双方共享的一个秘密密钥 s(鉴别密钥),发送方使用H(m+s)生成 MAC。之后,发送方 持! 直接沸路到移动结点; 诵信者向归属代理请求、并获知移动结点的转交地址(此步以后不必再 生成扩展报文(m, H(m+s)),并发送给接收方;接收方收到扩展报文(m,h),可用已知的 s,计算

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 性任这项工作,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—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 接要,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 和以一 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)。 初何可靠地芽取公组? 老成下面的例子: Rob 終公组 FB 发布在自己的主面 F: Alice 芽取 Rob : 面的请求被 Trudy 截获 Trudy 将假冒的 Bob 主页发送给 Alice. 主页中的公钥是 Trudy 的公里 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?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<del>身份标识信息</del>,并由 CA 进行<mark>数字签名</mark>(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银证书后 可将证书放在任何一个可公开访问的协方。 X 509 证书: 目前最常用的证书标准; **淮可以运行 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 每个 CA 拥有自己的私钥、负责为一部分用户等发证书; 用户自己决定 *職点鉴别。端点鉴例*,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 失建立相互滞育的各方的标识: 仅当奖别完成之后 各方才续续下面的工作。 奖别协议 and 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 地址散编)。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 的初始鉴别报文所数; 也就是说 Bob 无法判断 Alice 是否还选择 (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 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 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: "Iam →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! 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及 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 秋式覆盖"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) 通常转为容易 而等待在网络屋上广泛协部署安全性 可能还需要未来若干年才能解决。 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 了克服效率间题,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锁的报文 m; 3).用 Bob 的公钥 KB+加密这个对称密钥; 4).缀联该加密的报文 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。 *只美心发送方鉴别和 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 +(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: 押初始报文 (未加密) 和该数字签名级联起来生成一个句: 向 Bob 的由子邮件抽址发 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:格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 → 再用第一方案中的发送方的先骤发送这个新报文 生成一个新句发绘 Rob. 当 Rob 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。 PGP: 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); 软件生成密钥对; 操作与上面第三 种方案相同。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 --組帥议: 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 交換管理。 索環描述: 1. 握手: 实户需要与服务器创建一条 TCP 连接: 验证服务器是直实 的服务器;发送给服务器一个主密钥,客户和服务器用该主密钥生成 SSL 会话所需的所有对称密钥。 过程: 客户 TCPSYN -> TCPSYNACK -> TCPACK, 客户 SSLhello->证书->EMS = K\$(MS)。2.密 钥导出: 两者都生成四个密钥: Ec, 用于客到服的加密; Mc, 用于客到服的 MAC 密钥; Es、Ms 服到客; 3.数据传输:将数据流分割成为记录,对每个记录附加一个 MAC 用于完整性检查,将证 录+MAC"加密传给服务器。这里的 MAC=记录+密钥+TCP 序号的散列(防止重排序或重放: (击)。4.SSL 记录:由类型字段(hello or 应用)、版本字段(自解释)、长度字段、数据字段和 MAI 字段组成。前三个字段不加密。更字整描述。据手中**宏**户和服务器之间的一系列报文交换组成。治 览器向服务器发送支持的加密算法和客户的不重数,服务器从浏览器选择一种对称算法、一种公舒 算法和一种 MAC 算法,它把他的选择以及证书与服务器选择的不重数一起发送给浏览器,客户验 证该证书、提取服务器公钥、牛成一个前主密钥(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 \*\*择CRC 则初始向量也从这里导出(两个)): 客户发送所有提手报文的一个 MAC 服务器发送 所有握手报文的 MAC(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。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 方身份的奖制 容易遭受地址欺骗改击: 缺少对网络中数据的宗教性和机家性的保护 数据很容易 被窃听、修改甚至劫持。IP 安全协议(IPSec)。网络层安全性实现了"地毯覆盖"。 。 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 的桌现*: VPN 的桌型结构: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 对因结网中的路中器及用户软件是透明的 只要系统管理品设置好安全网关键可以了,传进小田 付拥有 IPv4 和 IPsec 首部。安全关联:IPSec 主要包括两个部分:IPSe 央令体验。包括鉴别首部体验 ALI (不提供却容性) 和 世类中个性类类 FSD 两个中个体验 完成 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(SA) 个通信端点间的一个单工连接,由一个安全参数索引(SP) 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 別密钥。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 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 乡 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 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E 安全网关来保证: 隧道模式可以将一对端占间的通信整合成一个加密流 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

出报文奖则积H(m+s) 若H(m+s)= h 则正堂。 数字答名: 一个可以转代车写答名的数字答 性服名: HMAC 覆盖面绘 IP 斗中的不变域 (传输模式) 或整个面绘 IP 斗(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。對装安全载荷 (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、栽荷和 ESP 尾的 报文鉴别码。除道模式路由 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。(法输槽式在第一部分钟小了初始 IP 首部)。 FSP 植砂 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 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。<mark>利用主机与基站共享密钥</mark>送 下事实鉴别主机。WEP 数据加密:主机与接入点共享一个 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 kilV: 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 kilV。 WEP 加密的安全漏洞:每个 KS 只有 224 个 (KS, IV) 可用: IV 坡重复使用; 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) if Alice 加密他选择的明文(d1 d2 d3 d4 ···); Trudy 能够获得 Alice 加密的密文: ci = di XOR kilV: Trudy 知道 ci 和 di, 就可以计算出 kilV: di XOR ci = kilV; Trudy 得到了加密所用的密钥流 k1N 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(而不是接入点) 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 在李户和鉴别服务器之间转发报文。3)成对主密钥(PMK) 生成。MK 是一个仅为李户和鉴别服务器 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 占发送该 PMK、客户和接入占现在且有一个共享的密钥。 4)临时密钥(TK) 生成。使用 PMK 于线 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 将被用于扩 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: 防火塘和人侵检测系统: [8] 火燒;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(硬软织 体); 目的是保护内部网络免受来自外部网络的攻击。防火塘的类型;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 数据包讲行逐句讨谈。基于以下字段决定转发包还是丢弃包:源 IP 坤址、目的 IP 坤址;TCP/UDE 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→手套所有外出的。目的端口为 80 的句: 不会许外部发起的 TCP 连接 BB 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 拓扑被探測(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 器的连接一过滤进入的所有 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 TCF 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。包拉 滤防火塘孤立地过滤每个包,仍会允许一些异常的包进入:例如、允许 dest port = 80. 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 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 雲松杏连接的状态。 応用開業: 应用同学除了松杏网络尼及传输尼协议斗 还松杏应用尼数据。 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 **塞所有**不源自应用网关的 telnet 连接。 防火糖的局限性: 无法抵御 IP 散骗攻击: 路由器无法知道 包是否来自声称的源;应用网关处理开销大。速度慢;每个被代理的应用都需要一个应用网关;应 用网学对于用户不透明: 客户软件必须设置应用网学的 IP 抽址: 对于 IIDP 句 计滤器或者全部 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 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。而且必须要将每个讨往的分组与数以 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, 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 公正学济曼和统计异学济曼是一个都且地场性的问题