路據口转移分组。某些分组交換机称为*鏈路層交換机*基于*鏈的层字段*中的值做转发决定。机构造的数据报大小不超过最小 MTU; 路由器丟弃超大的数据报,并发送错误报告 其他分组交換机称为*開由體基下回於國際是空*中中的值數若发決定,某些计算制网络中,实际上有*第三种重要的网络功能,即连接建立。* "問題影響理" *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验特性。在发送主机中当运验层向网络层仓 ②四回,此口中超过200円的对点。如为日前"中间大门关节间点上了10时间长了川市空入50 定的源和目的站口间的少<u>的企业</u>整件 万侧塞身,有个知文户"响展集"而意,"确定是一种。 延时地交全性服务,**因特别的规格层**提供了单一的服务,称为*尽力面为服务。* 更新的。 **网络居**他能够在一<u>两台土机</u>之间提供王建旗客旁或建旗服务,互编销层线位 (基于): 重大差异。在网络周中,这些服务是由网络居向运输指理机的上<u>有别子之</u>的服 17万,是人在开。这些服务则是运输层向应用层提供的<u>进程到进程</u>的服务,网络层万<u>亩。</u> 在运输层中,这些服务则是运输层向应用层提供的<u>进程到进程</u>的服务;网络层万<u>亩。</u> 提供这两种服务,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 2000年で大学。 最中級是一条<u>連門経営</u> 其子 传輸分割前建立車車路、传輸結束后所輸車機器 場合発生 大阪 保護 は 内部 できない 100mm 等。同面的对比之后的海中用进步外沿。用面的资格(1922、被针)可以用压缩的。 用于钢头,用电子模式,对比较强度,更加增加的,使用电子模型,使用电子模型,使用电子模型,可以使用的电子。 主机场路是,此后为组织用造场的路径转换,是否分层资源与定约。一条或电路线圈 据处于,深刻目的地上间的路径。但一系列链路和路由圈)。10号,沿着路路径转,但一场中的地上,20位全的地址。指示本则(仅用作源地),网络号为。主 级群市,深刻目的地上间的路径(四十条列链路和路由圈)。10号,沿着路路径转,但与有效的地上,指不是用的电子机,形在1720/1925地,指了是一个10号间,就是 段磁路的一个号码(用于区分经过该磁路的不同意电路,仅有<u>全地度</u>X),沿着该路径的(型线型不地底的分组不输出到线路上,而是这回内部的排收期,于**月 (submar)**,具有 们每个传输分组的 的 VC号,每合中间路由器必须用 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 网掩码中"I"的部分;主机地址:对应于网掩码中"I"的部分。如何确定于两?将网络接口 送路模块修改、约1~5分钟更新一次。 路由爾转发表用分組的目的地址的 前腳与该表中的表项进行匹配: 虚电路和数据报网络的由来: ATM (虚电路网络) 由电信网发展而来; 注重 用户体验(用户付费),追求高质量服务;接架大智能或很少智能、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现 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(如美错控制)推到网络边缘。以保持网络核心简单。数据报网络只提供 表决定路由器的输出端口、到达的分组通过路由器的交换结构将转发到输出端口 些分组。**路由选择处理器,**执行<mark>路由选择协</mark> 能在每个输入端口*本档解出,无*须调用中央路由选择处理器,因此*避免了集中或处理的 盖强*。必须要*用硬件执行资*找,而且需要对大型转发表使用超出简单线性搜索的技术, *接到*能示*网络地*单的长度,如 19424.0.0,255.255.248.0;用7长度"指示*子网地*单的 同时必须*的存存的同时*侧差子特别决注,*果要许多其他动作。*构造为组的版本号、构造 相以及场景中级,并且<u>多工资产了企业。</u>更新历于内阁管理的计数据。 *经*发展:第一代表现,这种技术的企业,是一个表现,这种技术的企业,这些类别的目标。 经发展:第一代表现,这种技术的企业,是一个表现,这种技术的企业,是一个表现,这些类别的目标。 完成: 理代路由器: 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 以*遂归进行。若个别表项不满足路由聚会的多件*: 仍然可以在转发表中绘出一多聚合 性能和代价取决于存储接口数目,仅适合小容量系统,*总转发吞吐量是内容写入或读出* B.C.三类地址的转发表项,用除系表组织;路由器收到数据报后;根据目的地址的类型 *這重的一半*并且*不能同的核支两个分组,越县地在货,交换结构中的总数包括地址线, 輸定要查找的转支表,根据目的地址的类型模型。 载金额和包链线,每个量,外面由油油工等有一种口部并建筑总柱。,每个油油进入一进行带着要发,情毒之形,<i>类而的 自由难的间毒,多类类的复数*等更多 是一个唯一的地址(内部标准)。经数块设计上外询用目时特殊,此效用即分分路度 *Dest_add/prefs_tem_是行起连接。* 由由着原来处,是中国地址的生物,该 pets 用: 各个输入端口在总统上*轮流*广播分组、分组中推带输出端口的地址: 各个输出端口 (en 值)、计算包的目的地址前缀(用地址接码和包的目的地址相与)。与 Dest addr 的 7月 日本代明日上は一般を開始を対象地域。1987年、1987年、1987年(日本代明年)、1987年(日本代明末)(日本代明末)、1987年(日本代明末)(日本代明末 **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**症量负载、交换结构 配的表项中选择前缀最长的表项。在大规模转发表中进行**凭速查找**是一个难题(已经解 基件経緯(現在性地/衛川市場、 政府生物の副川時以 中級イブ推進以底、火災内内 総別投資率以前基準。 急突機能が年度及対時間入園の対象技術等が適当の対象技術等 端口差距域解析。 解析事業的問題「展光機器」以大分園間塞其巨分園的景文。 差台 出意為人別治型性が、皮生死。 宝安機能改革生か分園の出来的自動性の力量が 自動為人別治型性が、皮生死。 宝安機能改革生か分園の出来的自動性の力量が 自動為人別治型性が、皮生死。 宝安機能改革生か分園の出来的自動性の力量が 自動と、可以消除金、淋巴が開発、使用・超速を発生を分類である。 配置を設定しています。 地面に定該する機能の表現を発展が展現を発展する。 条件金、海田同時的一个油 地面に定該する機能の影響を展現解的、最初出外別機と支生死。 宝安機能の、一部を発生を発生を発生を発生を発生を発生を発生しませます。 地面に定該する機能が展現を終め、最初出外別機と支生死の単独的と表現を発生を発生を発生を発生を発生を発生を発生されます。 地面に定該する機能が展現を発展を発展する。 可<u>藏华的、设置多大的输出队列是</u>一个问题:增大输出队列:可以减少毛包的发生, 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,浪费资源);输出 不是該长該好! 分類*丟弃策略: 弃居:* 队列激时,丢弃到达的分组; *主动队列管理:* 主机广播 "DHCP 发现"报文(src0.0.0.0 の是平均以外は企工が一方では、 の単年均以外は企工が一方で表現的時間会議、中国以外长度は大・星科同議法、 中也越大・<mark>自由医療控制平置)</mark> 网络范围的路由选择控制平面因此是**分布式的**,即不同 其 请 求 ℙ 地 址; DHCP 服 务 器 用 "DHCP ack"报 文 (src.223.12: 部分 (例如路由选择算法) 执行在不同的路由器上并且通过彼此发送控制报文进行交互 因特网路由器和路由选择算法是以这种方式运行的。 中的差错和对某些网络层信息请求进行响应的设施,因特网甲县**互联网控制报文协议** 192.168.0.0/16:**网络地址转锋(NAT):Motivation:**使用一个公用 IP 地址支持许多用 度(新遊点 在新) 建辛油片 16 比特。中 数据据的报告继承长度 15535 辛节、参考 物类) 1647 甲基坦 (不幸),从不直口至 (不幸),从不直口至 (不幸)的 (从不是) 《河川共義佛教教服务会会连右周伸系统,经的过去程。 数据的数据形分左交给哪个并完的远离层协议。例如 值为 5 交给「CP 而因为 17 文 数据用中的 (目的 中址、目的词(写) 该以 18 大师 18 大师 17 支贴 18 大师 数 用反码巡算对这些数求和 该和的反码存放在检验和字段中:路由縣臺对每个收到 **外连接。NAT的使用有争议**路由縣应当只处理三层以下的包头(端口号在传输局): 改变。 *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] 绘验和、TOP/UDP 检验和基对整个TCP/UDP 接交提进行的、TCP/UDP 与中不一定部处 须用于同一个协议社,原则:TOP 施公托一个不同的协议(从ATM)上,而下能够制 第547、定分传统社,原则:TOP 施公托一个不同的协议(从ATM)上,而下能够制 第547、定分传统社,原则:10P 的数据,**减和的时间地。域据,成据(有效规**度),数据(10P 上型),主机能由于10P 的数据,根据(1387.527、5001.52度 TCP 主接,MNT 4 数据报承载一个 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 <138.76.29.7.5001> 上收到的 SYN 包转发绘主机。使用中线服务器实现 NAT 穿线: 20字中的中音部加上20字中的17字音影)以及立用层框文、链路层板框未载的最大 30gp中使用:NAT后面的服务器与中域器建立连接。 线接字节接换为1401,47度型的链路可能具有47度的4001,特别过程中,数大的17度超离后中之建建之间较为组。 1897年,数据提供指数的过程,对于1807年, 数据报可以被分片: 数据报在传输的过程中可以被多 ·<mark>器重组。分片的报头</mark>取自原始数据报;与分片有关的字段:*标识*:每个分片必须携 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 深77.15%(67-ΣΕΔ/) 0 + PO \$1 H M A L 位置 0. 基金报头的 MF 位置 1. 计算检查和。 数据报分片的处理过程: 根据报头长度 H 文: 若目的主机收到 发送 Type=

廖四章,问结后网络层的**转发功能和商由选择功能败重要区分;**转发涉及分组在<u>单一</u>的 路由窗中从一条入链路到一条出链路的传送。路由选择涉及一个网络的所有路由高,它 移量器+8+分片总长度;*分片的网面*:分片的开销;降低了路由窗的在吐量;消耗了目 P94 論世· *捷口 interface*:主机/路由器与物理链路的边界;路由器有多个接口,主机常只有一个接口。*IP address*:每个网络接口对应一个IP 地址,IP 地址是一个 32 位的 5月被京旅校之间的旅馆等运动的特性。在发生利用中运动前的网络压停进一个 进机转。该用几个一进特性表示,*基于来的验性* 1994年期*用据号于土机等。4日工造组* 或出*用据据摄影的*发现多点的,我们就是其有技术上的影响发文计像另外。 我们的效性之间的"<u>如果或原子那么多。</u> 1994年,1994 原类似 业除类别标识外,其余比特被划分成*网络号和主机号两部分*:网络号:标识一个物理网 机的服 络:主机号:标识该物理网络上的一个网络接口;同一个物理网络上的网络接口,它们 的 IP <mark>地址具有相同的网络号。*地址分配:*因特网中的每个接口必须具有唯一的 IP 地址</mark> 为在因特网范围内保证 IP 地址的全局唯一性:*网络号*由 (CANN 统一分配,*主机号*由 络边缘的端系蛇中实现的,网络层连接服务除了在*端系蛇中*,也在<u>他于网络练心</u> 每中实现,_随电器网络。*因特用是一个数据报网络*,网络层连接被称为*虚电路*,给管理员练一分配;建立私有网络的组织可以自己选择网络号,但同样必须保证每个F 為了这一个是一次的工作。 即于网地址、不需要通过路由器就可以相互到达的网络推口构成一个子网。 子阿維斯 从概念上说。引入于网仅影频改变了IP 地址的解释: 主机号被进一步划分成于网导和主 机号高部分; 子网号标识网络内的一个子网。主机号标识子网中的一个网络推口; 管理 每台中间路由路必须<u>用一个新的 VC 专替代</u>每个传输分组的 VC 号。该<u>新</u> 机与弗部分;于网与标识网络内的一个于网,主机与标识于网中的一个网络接口;管; *表获得。无论何时跨越一台路由器*创建*一条新的虚电路,*转发表就增加*。员可以根据需要,如子网的数量和规模,选择合适的子网号长度。*子网掩码*,用于指: 与主机/路由醫分开,形成一些分离的网络岛,每个网络岛就是一个子网。路由醫的 不同的端口连接不同的子网。路由器是在子网 网络屏转发数数 #的兩种情形: 直接交付: 节点 (源字机或目的路由器) 将数据包直接发谈绘目的字 《不需要其论的由需转发》;间接交付: 节点将数据包转发验一个路由需去处理。如何 断使用直接交付还是间接交付?直接交付: 数据包的目的地址与节点的某一端口在同 个子网中: 间接交付: 数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。 **维交付的实现**;节点查找转发表。将数据包发送给下一个路由器。记录目的地址到编 端口的映射:取决于目的地址类型的不同,有三类转发表示;目的地址是一个子网络鱼 称造丝前缀表项;目的地址是一个特定的网络接口地址,称特定主机表项(掩码 255.255); 缺省项: 不匹配所有其它表项的地址, 这些地址被映射到一个最高 路由醫端口(0.0.0.0%)。 *IP 采用逐瞬连路*;每个转发表项只记录去往目的地址的下一跳 息(下一个要到达的路由醫端口),而不是一条完整的識到端路由。每**个转发表项包括** 目的地址/掩码、下一跳地址、输出端口等。下一跳地 (不需要通过其它路由器就可以直接到达)。IP 数据报的转发过程 (主机/路由器): 這(扶行確認原协议,封裝)<u>的物理及改</u>值在集入確認上传輸这 第由書端口 elso 宣告德國在第一次 「我們的國家有的」,實的國家可以在第一次 「我們的國家有的」,實的國家可以 又表,扶行兩個管理別能,一台兩個兩份輸入網口,製出網口和,原本學行為的開発,我更表現機變形式開発,**CODA Classistes Intercomain Routing** 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。 立有一个 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** 2.4 \transaction ID:655 \Lifetime:3600 secs) 发证 IP 地址、服务器响应客户的请求、确认所要求的参数; DHCP 服务器使用 UDP 端口 不断分配)) NAT 转维表: 记录每个 (| P地址: 逐端口号) 与 (NAT IP 地址: NAT 海川 日) 的特殊 天系 連入 的最無盤 取 数据版中的 (目的 IP 地址: 目的端口号) 章技 NAT 转换表 然后用转换表中对应的 ((地址: 端口号) 进行替换 16 比特端口号: 炎井一个 NAT IP 地址同时支持 65535 个 2 方可以向任何其它(参与的)对等方发起通信。使用 UPnP 实现 NAT 穿越: 假设主机

D的 Echo Response 报文: 源主机计算 RTT

競路任務的 IP 地址、然后向目的主机发送第二个 Edno Request 报文、IP 报头的 TTL 设 为 2: 若收到第二跳路由器的 TTL expired 报文、记录第二跳路由器的 IP 地址:接着发 由 送一个 TTL 为 3 的 Edno Request 报文:该过程不断重复、直至收到目的主机的 Edno IR ionse 报文 (该目的主机向源发送一个端口不可达的 ICMP 报文)。IPV6: 最初的动 转发数据包; / [2] IPA4 地址将很快耗尽。
2. IPA4 地址将很快耗尽。
2. IPA4 地址将很快耗尽。
2. IPA4 地址将很快耗尽。
2. IPA4 地址将很快耗尽。
3. IPA4 地址将很快耗免。
4. IPA4 电线机构设
4. IPA4 电线机构设 网络议都善客。IPv6 推址: 128 位、使用冒号十六进制表示。 每 16 位以十六进制 由職 (成字机) 称为 BGP speaker。 一对 BGP speaker 通过一条 半永久的 TCP 连接 (首 形式写成一组、组之间用冒号分隔、如"8000: 0: 0: 0: 0: 0123: 4567: 89AB: CDEF"; 地址 表示的零压缩技术: 可将连续的多组 0 压缩为一对冒号,如以上地址可表示为:"8000 123: 4567: 89AB: CDEF"。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(通常是连接特成全连通,它们之间的 BGP 会话称为**内部 BGP (IBGP) 会话**, BGP 定义了 4. 最近的一个)。 **PFG 数据据传式**:以一个 40 字节的基本头开始,后面跟零个或多个扩展 类型的概义: 打开报义: BGP 路由器用来启动与邻居 BGP 路由器的联系;保活报文 然后是数据。PRI(成 traffic class): 作用:发送方在该域定义数据报的优先级。 需发现网络拥塞时,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类 **學欄塞控制的法**; 非实时法属于这一类。优先级 0~7、按照重要性及用户体验设定: 不 安娜**康姓的诗法:** 实时多聚体流属于这一类、优先级8-15、尚无标准。可以按照用产要求的服务质量等级定义。 *捷 (flow)*: 流是具有相同传输特性(源/目的、优先级、透项等)、并要求相同处理(使用相同的路径和资源、具有相同的服务质量和安全要求等) 系列数据句: 流由源地址和流标等 (flow label) 唯一标识: 流标等由发送方分配 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 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 #得 IPv6 具备了对数据包进行区分处理的能力。IPv6 包格式与 IPv4 的区别:与 IF 定头相比。[P66 的基本头中*主解了以下一些字段*。选项:[P66 的基本头总是 40 字节 (但可以通过"下一个首都"),与分片相关的字段:[P66 路由器不负责分片;头校验: 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都有校验和; 代了 ARP 和 IGMP。IPv6 基本头中增加了; 治标答: 支持对数据包区分处理: 改变 段的作用: Type of Service: 代之以 Traffic Class; 总长度: 代之以載荷长度: Proto MP,并取消了 RARP(该协议的功能已被其它协议取代),ICMPv6 仍然使用差错报告 和查询两类报文:为 IPv6 增加了新的类型。如"分组太大"和"未识别的 IPv6 选项"; 夫特 、优先级和流标签允许路由器控制拥塞、王齐不太重要的数据包、去掉 查询报文、增加了一些查询报文、用于实现 ARP (地址解析) 和 IGMP (; 不必要的查询报文,增加了 報管理)的功能。 Al IPv4 対波到 IPv6 地址: 0:00:0:0:FFFF:13:1:68:3(前 80 位 为 0. (位为 1. 点分十进制剩余 32 位); **从 IPv4 过速到 IPv6:** 双静**议**技方辈,支持 IPv6 的 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 DN 回 IPv4 地址,发送 IPv4 分组:若返回 IPv6 地址,发送 IPv6 分组;<mark>双枝节点同时拥</mark>4 1和 IPv6 地址。IPv6 数据何如何穿越 IPv4 网络? 报头转换: 双村节点 (如路由器 E · 将数据报传递给 IPv4 路由醫(如路由醫()之前,將 IPv6 报头转换成 IPv4 □ 报头转换不完全,有信息丢失。**建立嚴道**: IPv6/IPv4 边界路由醫将 IPv6 一个 IPv4 包中, 送入 IPv4 网络,目的边界路由醫取出 IPv6 包继续传输; 优点 的数据报的全部信息。**都由进程复注,什么是最佳路径**,应用评价:路径长度、数据读 分组延迟、通信费用、安全性等: ISP 美心: 网络吞吐量最大、平均包延迟最小、 動情费用最低、网络负载均衡、路由稳定、健壮等。 新由评价指标通常是矛盾的。需要 返送路算法分类:全局算法 or 分布式算法?全局算法所有路由器具有关于拓扑和 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 蓝路代价,通过与邻居交换信息,进行选代计算。 *静态算法 or 动态算法? 静态算法* 由随时间不变或缓慢变化(手工配置); 动态算法。路由器根据拓扑及链路代价的变化 动更新路由。解路状态(LS)选路算法: *解路状态洗路算法*为*全局算法*,其*基本局* 內,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 链路代价信息. 扩散 LS 分類: 向网络中所有节点发送 LS 分组(链路状态广播复决) 个是确保并非所有路由器制 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 7 要求解任意两个节点之间的最小代价路径,主要贡献在于给出了*分布式(透代、异多地)* 作解 B-F 方程的方法。*算法的基本思想*:节点×测量其<u>到各个邻居</u> v 的链路代价(xx); 点 x 估计其到达各个节点 y 的最小代价 Dx(y), 这些代价构成了自己的距离矢 De-Dio_Vip(Vip(N),每个节点周期抽染等它的高数点量 D. 支型物包层。可点,每年每个 格像、的图表气量。De-Dio_Vip(Vip(N),有个节点周期抽染等它的高数点量 D. 支型物包层。可点,每年每个 格像、的图表气量。De-Vip(Vip(N)),有一方点,从各个都是到的目的图表头面上,拥一眼就要分子是一个不知(多维性的人,使用。多维性的人多组形式,这种种类型解析,可能是这些,多维性的人,多维性的人类似的。 日本 方程更新自己的图表头面。De/Vip(Vip(N)),可点的本来计算由以下解析,进程的程度。并为组织是实验,可以发现的 日本 方程更新自己的图表头面。De/Vip(Vip(N)),可由的本来计算由以下解析,进程的程度。并为组织是实验的多维组地址,如何解释者的严格 上,多组织人功论也能解解处,然后就是是一个现代的工程,可以使用。由于是一种工程,可以使用。由于一种工程,可以使用。由于一种工程,可以使用。由于一种工程,可以使用。由于一种工程,可以使用。由于一种工程,可以使用。由于一种工程,可以使用。由于一种工程,可以使用。由于一种工程,可以使用,由于一种工程,由于一种工程,可以使用,由于一种工程,由于 发现距离矢量 dx(y)有变化时通知其邻居。链路代价变化: 好消息传播快, 料 价; 节点计算的路由不传播。错误不扩散; **收拾速度**; O(INIIEI)个报文。O(N2)次计算。 **距离矢量 DV**: 距离矢量仅在发生变化时向邻居发送; 节点传播的信息可能不正确 由陽数目扩大、路由表规模、信息交換开锚; 网络管理员希望对于网络有更多的抑制 数(曾理自治): 选路算法的选择,隐藏网络内部组织。自治系统 (AS): 自治系统 (AS) 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, NNN 分配; 一个 AS 中的路由器运行相同的选路协议 (称 Intra-AS 洗路协议): AS 中的路由器可以运行不同的 Intra-AS 洗路协议。 网关路由器: 在一个 AS 内。 连接到其它 AS 的路由器;网关路由器之间运行 Inter-AS 选路协议,所有 AS & f相同的 Inter-AS 选路协议。Inter-AS 的任务: AS1 内部的路由器需发送数据报到 路由霧应当向哪个网关路由霧发谈? AS1 的网关路由器必 了解哪些目的网络诵言 / 设置未往外网 x 的转发项: 1c 和 1b 分别从 3a 和 2a 了解到网络 x 可达、干是各自 网络×可达"的信息传播到 AS1 内部(inter-AS);1d 决定使用 1c 还是 1b 路由器 土豆炒议: 选择离 1d 最近的网关路由器(intra-AS);从转发表中得知到达最近网会 接口为 I, 添加表項 (x, l)到转发表中。 *涉及两个层次的选路*: 通过哪个网关路由器 何到达该网关路由器 (AS 内洗路)。 转发表由 intra-AS 公里到 AS 内部网络的路由·inter-AS & Intra-As 心里和 的有RIP、较低层 ISP 和企业网使用; OSPF, 较顶层 ISP 使用。Inter-AS 选路协议也称 外部网关协议 EGP. 目前只有: BGP。 选路算法和选路协议: 洗路算法是洗路协议的 分;选路协议还包括路径代价的定义、报文格式 等具体实施方面的问题。 <mark>因特网中自治系统内</mark>首 《、报文格式、报文传输、报文处理、异常事件》 治系统内部的路由选择: RIP: RIP 采用距离失 选路算法。距离 (代价):用路数 (hop count) 衡量。器 (hop): 相邻路由器之间的8 RIP 通告 (RIP 响应报文): 距离向量: 路由器到 AS 内各个子网 短路径的跳数(估计值);构造 RIP 响应报文:距离向量封装在 RIP 响应报文中传输 为 RIP 涌告。每个报文推带一个目的子网列表(最多包含 25 个子网)。以及到每个 子网的最短距离;发送 RIP 响应报文: RIP 报文封装在 UDP 报文中发送 张称为**路由选择表**的 RIP 表,包括该路由器的距离向量和该路由器的 发表。RP 健時失效与恢复: 若超过 180 秒未收到某个邻居的 RP 通告,认为该邻居 据选路: 扩展 RP 协议实现多播选路的困难:除边缘路由器外,其它路由器不知道多播 可达: 今通过该邻居的路径生效(距离设为 16) 发谈 RP 通告:采用 春传光终眠决 组 及 其成员 的存在:DVMRP 采用广播、单枝的能决办法:RPF 广播、确保多播分别 可达: 令通过该邻居的路径失效 (距离设为 16), 3 数至无穷问题: 若选路表中到目的网络 x 的路由是 x 的距离设为 16(阻止 A 使用这条路由)。因特网中自治系统 F 采用**舒誘状态选择意法 舒誘代价**:由管理员配置(反映了管理员的选路策略) SFF 弁用<u>を取り込む即果で、</u> 変形F 分銀、SSFF 放送でより 7 5 神分組美型、分別用于探測邻居、適告链路状态等 SFF 分組被封装在 IP 包中传輸、协议号为 89。路由器周期性地或在链路状态改变时 OSPF 結路通告。OSPF 协议参查: 链路通告分组在网络中的广播及可靠传输。路由 根据收到的链路通告分组构造链路状态数据度。路由器利用链路 计算以太路由器为相的最短路径树。OSPF最重要的优点是支持AS内部的分层的 允许使用多条相同费用的路径(RIP 只能选一条);可以针对不同的 ToS 设置不同费用 亦度: 集成单据路由和多据路由: 一个 ○SPF 自治系统可以配置成多个区域 (area): 铂 区域运行自己的 OSPF 协议,区域内部的临阶状态仅在本区域内广播。区域边界路由 设质区域间的选路。一个 OSPF 自治系统配置为若干区域:一个特殊区域称为主干, 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;路由疆; **区域边界路由器**; 连接本地区域和主干的路由器; ≠**干路由器**; 主干上的路由器。可 对是区域边界路由器: 内部路由器: AS 内部的非区域边界路由器。分层的 OSPF: 每个区域(包括主干)运行自己的OSPF协议; B运行自己的 OSPF; 链路通告只限于区内 去往其他区网络的方向(不知道路径)。 **每个区域边界路由器**,将本区域的洗路信息

磨的原本与服务。因特同规模板其主大且结构非常复杂。每个 AS 可重行自己的内部的 由协议、使用自己的由规模全部目的特别的维护性指码。不同间的制度,被用的电子模型的一个电子 住路由。*边界阿美协议 BGP*: 当一对 AS 同意交換选路信息时,每个 AS 指定一个排 AS 边缘的路由器(或主机),使用 BGP 协议交换选路信息。 *运行 BGP 协议的边界*最 179) 建立 BGP 会话、交换 BGP 报文 (BGP 是应用层协议!)、BGP 会话的两个端点 日 169 建立 567 金融。 文庆 567 张庆 169 朱正 178 189 朱正 189 朱 是**运动效义**:1月7枚人,BOF 时口留加水后引引节后 BOF 时口留的软状,体后放火。 6P 路由器定期交换保活报文,告知对方自己处于工作状态;通知报文:当检测到差错 【路由器打算关闭连接时,发送通知报文;<mark>更新报文</mark>:BOF 路由器使用该报文宣布新题 B. 以及撤销以前通告的路由。可达性信息:以 AS 枚举形式通告的、到达目的前缀的 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 差形式通报完全路径; AS2 的 BGP speaker 通报: 128.96, 192.4.153, 192.4.32, 192.4 从<AS2>到达; AS1 的 BGP speaker 收到后通报: 128.96, 192.4.153, 192.4.32, 192.4 经路径<AS1, AS2>到达。BGP speaker 內部的透路信息库由三部分组成: Adj-RII : 每个 Adj-RIBs-In 对应一个 BGP 对等方,保存从该 BGP 对等方收到的选路信息; OC-RIB: 已被该 BGP speaker 计算出来的最佳路由;Adj-RIBs-Out: 每个 Adj-RIBs-Ou 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 进程的处理过* 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 网络管理员定义) 结果可能是: 丟弃、按原样接受、接受但修改某些属性(如偏好 对于每一个目的前缀,从所有可达的路径中按照 BGP 指定的决策顺序等 各由,装入 LOC-RIB;输出策略引擎根据出境过滤规则(由管理员定义),计算要通告 每一个 BGP 对等方的路由更新。放入对应的 Adi-RIB-Out 中 (路由聚合也在这个阶段 E成);BCF 进程利用 Adj-RIB-Out,向每个 BCF 对等方发送路由更新报文。Intra Tinter-AS 选路协议:Intra-AS 选路协议:用于在 AS 内部交换选路信息,如 OSPF、R 媒个路由测度(代价)选择到目的节点的最优路径;Inter-AS选路协议:用于在不 ;之间交換洗路信息。如 BGP。主要依据策略而不是路由测度去寻找可达路径。 是性路径)。 为什么会有不同的 AS 间和 AS 内部騎由选择协议;对该问题的答案能 AS 内与 AS 间的路由选择目标之间差别的本质: 策略(AS 间在意)、规模(AS 间 意、而 AS 内可以讲一步划分)、性能(AS 内关心)。 广播和多播路由选择:广播路由 **径(broadcast routing)**; 网络层提供了从一种源结点到网络中的所有其他结点交付付 多播路由选择(multicast routing)使单个源结点能够向其他网络结点的 集发送分组的副本。广播路由选择算法: 用 N 次单槽实现广播 (在源节 低效: 相同的分组在某些链路上可能重复传输。需其它机制支持: 源节点需知道所 组<mark>拷贝最少。*在网络中复制分组:洪泛(flooding)*:节点收到广播分组后,向所</mark> 来的链路除外)发送该分组的拷贝、缺点:在有环的网络中,广播分约 共占 (公領 。 「网络中无休止地循环,没费资源。*要控送还*;目标:每个路由器仅转发它之 比的广播分组;*两种方法*;节点记录之前转发过的分组 ID,不重复转发分组(此方法: 源排址+分组 ID): 反向路径转发:利用节点内部的单播转发表。 路径上到来的广播分组(该方法使用最多)。 反向路径 分组的源地址查找单播路由表,找到去往该源地址的输出端口;若分组的输入端口 往该地址的输出端口相同,则扩散该分组,否则丢弃分组;优点;篇法合理,易于3 节点作为核心 (也称汇聚点); 其它节点向核心发送单播的加入报文: 路由器利用单 发表的核心转发加入报文时,记录报文的输入端口及输出端口。这些端口或是位于 时上的端口;当加入报文到达生成树上的一个节点时,报文经过的路径被添加到生 上。实践中的广播算法: 应用层: Gnutella, TCP, 寿命 TTL, 范围受限的洪泛; 📿 或塞开一个组 多樣和管理协议 (IGMP) 允许主机向本地路由器由请加入或塞开 组;如何将多播分组交付给每一个接收者:多播选路协议协调多播路由器建立到达所 有接收者的路径树。 多播组管理 IGMP 协议运行在主机与边缘路 由器之间: 主机利用 SMP 协议向边缘路由器请求加入一个组、或塞开一个组;边缘路由器利用 IGMP 协议 向主机询问组成员关系,边缘的由器通过(GMP 协议可以了解到,在它的某个端口能够的 的主机询问组成员关系,边缘由器通过(GMP 协议可以了解到,在它的某个端口能够 则达的网络上存在着哪些组的成员。由于IGMP 的交互范围被局限在主机与其相连的路 由器之间,需要另一种协议来协调遍及因特网内的多播路由器(包括相连的路由器),以 后一个功能是由 网络原多裸路由选择算法完成的 B特网中的网络服多播是由两个互补的组件组成的: IGMP 与多播路由选择协议。IGM),报文类型:查询(一般查询、特殊查询)、成员报告、退出报告(退出是可选的。 使用了成员报告报文: 当无主机响应一个具有给定组地址的成员报告报文时 という。 接路由器就推断出已没有主机在这个多桶组了)。 **我状态於议要比較状态协议的性态** 第一些 后者不仅要求状态显式地增加成删除,还要求有机制能够负责当实体提早结束 位失败时清除状态。**加入一个组**;每个主机维护一张应用讲程与名器组的对应表:主机 的一个应用讲程想要加入一个多播组时,向主机发送请求; 若这是一个新组、主机 1357 在7500年3000年3000年300日 1000年300日 1000年31日 10 对该多播组的特殊查询报文(询问该端口上还有这个组的成员吗?) 若在规定的时间内 的所有节点:退出报告:多播地址224002 核收者是该子网上的所有路由器:成员 被划分为等长的时隙 每个时隙传一帧:节点只能在时隙开始时发送:节点是时钟同: 上577日7日7日, 长系报告:被报告的多播地址。*多播新由选择算法·目标:*为每个组建立多播转发树 上该组所有成员的路径树),每个组成员应当只收到多播分组的一个拷贝,非本组成 应收到多播分组,从源节点到每一个组成员节点的路径应当是最佳的(最短路径)。**建**时除发送新的帧;若检测到冲突,节点在随后的每一个时除中以概率P重传,直至: **立多播劇的兩種方法: 基于源的制**源节点建立一模到多播组所有成员的最短路径树、源 经过的子网数量。限定一条路径 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 基于源的柯:最短路径树:MOSPF(多播 OSPF)通过扩展 OSPF 协议实现最短路径多 福洗路: 扩展链路状态、使之包含链路上的组成员关系: 基本思想: 所有参与多播的主 加高級は、別版性中の心。 とことは他は一上の自成の人が、最早的心が、175~3~10日 初在局域网上定期通报其所属的多播组(IGMP)、路由服務毎条直達電路上対应的 组集合作为链路状态在网上广播(MOSPF)、当路由爾第一次週到某个<S,G>多播分割 算从源节点 S 到多播组 G 的最短路径多播树(按需计算)。基于源的树:距离矢量多 枝的解决办法: RPF 广播: 确保多播分 域网上通报所属的多播组,局域网上的路由器记录这些信息(GMP); 当路由 關收到发往组 G 的多播分组,但它并没有从局域网上监听到组 G 的报告时, 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 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,当报文到达标 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 G 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 洗路表向核心转发加入报文、并在多播转发表中创建一条共享树记录<*.G 报文章 施造的表例像U等&加入核文、并在多倫特及表刊到建一来共享例に来る。 送的接口: 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: 许接收 G 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,报文统过 路径被添加到树上。如何利用组并重树发送多播分组?当须节点根要发送多播分 原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 组的目的地址为 G,从源节点到核心的路径上,可能有路由器不在多播树 (转发);建立隧道:源节点将多播分组封装到 ·个单播分组中, 单播分组的目的地址为 核心的单播地址。最广泛使用的因特网多播洗路协议是 PIM:不依赖于网络中所使用的 (子河及路径代价),通告给其它区域,将收到的其它区域的远路信息(子河及路径代 通告给某权域的内部由通,对于*主任其它区域*的分组,后头找到其本区域20万 应用,在于上年来到11的区域20万种后,然后将来到180万吨,20万平 6万年 12世,采用至于19的万元(1975年),然后将来到180万吨(1975年),然后被1975年(1975年),但是1975年(1975年),1975年),1975年(1975年),1975年),1975年),1975年(1975年),1975年),1975年),1975年),1975年(1975年),1975年

· *随层:链路、推入网和局域网:<mark>网络层和链路层的关系:网络层:选路:*路由器确定 注目的节点的下一跳,**转发:**在路由器内部将数据报从输入端口转移到输出端口;*链*</mark> *路层:将数据投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8 →下一跳路由器,目的路由器→目的主机。 *福那层模球*:结点:运行链路层协议的任何 设备。*健略,*连接相邻节点的通信信道。*帧,*链路层分组称为*健路层帧。*键路层模 **健路层服务:组帧 (基本服务)** 从原始比特流中提取出完整的帧; **健路接入 (**) *随知因因为* **播経路需要)在广播信道上协调各个节点的发送行为; 差積拾票(基本服务)检测传输** 错误; **差错刘正(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** 它们之间的 BGP 会话称为内部 BGP (IBGP) 会话、BGP 定义了 4 种 议提供) 语过确认、重传等机制确保接收节点正确收到每一个帧(停.等、GBN、SR) 链路 (加半纤 基些型绞线) 上很小使用 高湿和率链路 (加于线链路) 点 *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 可靠交付的链路层协议、需要流量 **全双** T₂ 半双丁通信时、提供收/发转换。每路局在何处实现: **路由器中**链路局在线分 《fine card》中实现,主机链路层主体部分在网络适配器(网卡)中实现。线卡/网络适配器(网卡)中实现。线卡/网络适配器连接物理媒体,还实现物理层的功能。链路层由硬件和软件实理。网卡中的控制器 芯片:组帧、链路接入、检错、可靠交付、流量控制等,主机上的链路层软件:与网络 层接口、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绘网络 活版日,然后日的四位人,可且上的四位人。 是。**网络连西港之间的通信,发送卿将数报报封装到帧中,生成校验比特,执行可靠传输和流量控制,解封装数** 据报,交给上层协议。 *整础绘画和刻正技术。*传输出销的类型,单个错;由随机的信道 ·噪声引起,一次只影响 1 位; **察发错;**由瞬间的脉冲噪声引起,一次影响许多位,使 用突发长度表示突发错影响的最大数据位数。差错控制编码的类型:检错码:只能检测 构成。有效编码集: 由 2^m 个符合编码规则的码字组成。 检 · 若收到的码字为无效码字,判定出现传输错误。 *海明距离* ·若收到的码字为无效码字,判定出现传输错误。海明距离(Hamming Distance)。 个码字的对应位取值不同的位数。**纠错**·将收到的无效码字纠正到距其最近的有效码 检错码与纠错码的*能力都是有限的! 编码集的海阴距离*:编码集中任意两个有效 - 1811年1フラロ8年1日第27年207年207年207年207年20月 - 海母来十七恩内で十分次 180万年8日第19日第 - 日本 1917年1日 - 日本 1918年1日 - 猎枪测的实施: 发送端对要保护的数据 D (包括帧头字段) 牛成校验位 EDC (姜猎枪测 和纠正比特) 添加在帧头中: 接收端对收到的数据 D 计算校验价 EDC'. 根据 EDC'到定 會關模體·单比特奇傳校體:可推測全比特错误、检错率为50%、編码集活 二维奇傳校體:可推測 2 比特错和 到 正 单比特错。编码集海明距离为3。 有利于检测变发错误。前向纠错(FEC); 接收方检测和纠正差错的能力; 优点; 减少所需 的改选方面变换的文载。允许在接收方立即纠正差错,遵负了不得不等待的往返时差,而 这些时延是发送方收到 NAK 分组并向接收方重传分组所需要的,**因转用检验和(Internet** checksum):数据的字节作为 16 比特的整数对待并求和(溢出回卷),这个和的反码形 成了機带在极文段首部的因特网检验和: TCP 和 UDP 对所有字段(包括首部和数据 (2) 计算因特网检验和:优字:检验和方法需要相对小的分组开销,与CRC 相比提供相对弱的差错保护。 为什么运输后使用检验和而链路后使用企业和通常是在主机中 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 快速如检验和这样的差错检测方案是重要的。在另一方面,链路层的差错检测在适置 器中用专用的硬件实现。它能够快速执行更复杂的CRC 操作。 CRC是一种多项式编码,它将一个位电看成是某个一元多项式的系数,如 1011 看成是 一元多项式 X3 + X + 1 的系数。 信息多项式 M/x); 由 m 个信息比特为系数构成的多项 武。*冗余多项式 R(x)*;由(万众宋计特为系数构成的多项式,最多项式 T(x);在 m 个信息比特后加上 r 个冗余比特构成的码字所对应的多项式,表达式为 T(x) = x^r = M(x) + R(x)、生成多项式 G(x):双方确定用来计算 R(x)的一个 r + 1 比特多项式。编码方法:R(x) M(x) ÷ G(x) 的会式 (减法运算定义为异或操作)。检验方法: 若 T(x) ÷ G(x) 余式为0. 判定传输正确。CRC 网络信能/JRE 可用使件实现,是应用最广泛的绘能 BB。CRC 举例:取 G(X) = X^3 + 1. 对信息比特 10110 计算 CRC 码。101110000 + 1001 的余式为 R=011 (CRC code),码字:101110011:取 G(X) = X^3 + 1. 接收端收 (比特出 1001001、问是否有错? 解答: 1001001÷1001 的会式为 001 (不为 0)。有 **健康的面積光剂,占到占健康,**但许该了 下接收方的链路,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**:连排 "许多节点的单一共享链路,任何一个节点发送的数据可被链路上的。 . 当有 M 个节点发送时,每个节点应能以 R/M 的平均读主发送(公平性好 3. 协议是完全分布式的:不需要一个特殊的节点来协调发送 时钟成时隙同步(不需要额外的机制)4. 简单(实现和运行开销小)。 MAC 协议的分 信道划分,将信道划分为若干子信道,每个节点固定分配一个子信道,不会发生冲突 . MAC 协议的分类: 方法的折衷。引入额外机制。信道划分协议: TDMA (时分多址): 将信道的使用时间 成帧,每个节点在帧中被分配一个固定长度的*时间片(一个时间帧 N 个时髦)*。 间片可以发送一个分组,节点只能在分配给自己的时间片内发送,若节点不发达 其时间片**轮空。FDMA(频分多址):**将信道频谱划分为若干<mark>子频带</mark>,每个节点被分配 个固定的子频带(R/N *帶重*),若节点不发送,其子频带空闲。 *TDM 和 FDM 的优劣;* 肖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户 列中的轮次。 *CDMA [码分多数];*将每个比特时间进一步划分为 m 个微时隙(称 chip), 每个节点被分配一个惟一的 m 比特码序列 (称 chip code): 罗漢方鑰码: 罗溪*1"=发溪 code. 发谈"0"=发谈 chip code 的反码; 信号叠加; 多个节点发谈的信号在信道中 发性相加;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 复出原数据; 前提条件: 任意两个 chip code (知道时隙内时开始);所有节点可在时隙结束前检测到是否有冲突发生。操作:节; 上层收到数据后,在下一个时隙发送;若时隙结束前未检测到冲突,节点可在下一 --个时隙发送;若时隙结束前未检测到冲突,节点可在下 功。优点: 单个活跃节点可以信道读率连续发送、分布式: 节点自行决定什么时候 簡单。較点:发生冲突的时隙被决费了,由于概率重传,有些时隙被周围,需要时 同步。**时隙多路访问协议的效率:**当网络中存在大量活跃节点总有帧发送时时,长期 运行过程中 成功时期所占的比例。时分 Aloha 的效率: 假设: 有 N 个活跃节点。每个* 在每个时隙开始时以概率 n 发谈; 给定节点在一个时隙中发谈成功的概率 = n(1-n 7. 核 ALOHA: 基本思想: 取消同步时钟 任何节点有数据发送就可以立即发送: 为海沙水际信诺利斯太灾体龄是不成功 并不成功 今即以解衷 p 雷体 以解室 /1.0 持一个帧时后再决定。(*帧时*:发送一帧的时间,假设帧长度相同)。**发生冲突的情况** 发送的帧与在 [t0 - 1,t0 + 1] 时段内发送的其它帧冲突。统 Aloha 的效率: (给定节点发送成功)=P(节点发送)*P(无其它节点在[t0-1:t0]内发送)*P(无其它节点在[t 两个重要的规则: 发送前监听信道 (carrier sensing 载波侦听), 信道空闲发送整个帧 言道忙则等待至少一段时间没有传输再发说(推迟发说); 碰撞检测, 即当一个传输结点 | 1945日 | 1947日 | 19 听多路访问(CSMA)和具有碰撞检测的 CSMA(CSMA/CD)协议作中。冲察仍可能发生 由于存在端到端信道传播时延,节点可能没有监听到其它节点正在发送,即使忽略传载 E迟,当两个(或多个)节点同时发现信道由忙变为空闲、并都决定立即发送时,仍会 CSMA/CD (Colli etection); 若在发送的过程中检测到冲突, 怎么办? 继续发送会下的部分(消费带宽) 7 (1945年) 18 (1945年) 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, 然后发误帧; 3.若 NIC (误完整个帧而没有检测到冲突, 认为发送成功!; 4.若 NIC 在传输过程中检测到冲突 指数回退) 然后返回步骤 2。我们希望时间间隔应该这样: 当碰撞结点数最较少时, 一个给定帧时,在该帧经历了一连串的n次碰撞后,结点随机地从(C ,中选择一个K值,对于以太网,一个结点等待的实际时间是 K-512

可碰撞,因此,当几个其他适配器处于指数后退状态时,有可能 传输。CSMA/CD 效率: Tprop = 以太网中任意两个节点之 传播延迟的最大值 的最大值; Ttrans = 最长帧的传输时间; efficiency = 1 / (1 + ns)。在以下情况下,以太网的效率趋近于1: Torop 趋近于0. 或 Ttrans 无穷。**结论:应控制以太网的规模。 聽流 MAC 协议:**多路访问 1. 当只有一个结点活跃时,该活跃结点具有 R bps 的吞吐量; 2: 多路访问协议的两个理想 s 的吞吐量; 2. 当有 M 个结 t活跃时,每个活跃结点的吞吐撞接近 R/M bns。ALOHA 和 CSMA 协议具备第一个制 ,但不具备第二个特性。轮询协议:结点之一被指定为主结点、主结点以循环的方式 询每个结点,主结点首: 结点 1 传输了某些帧后 ,主结点首先向结点 1 发送一个报文,告诉它能够传输的帧的最多数量 了某些帧后,主结点告诉结点 2 它能够传输的帧的最多数量(主结点能够 通过观察在信道上是否缺乏信号。来决定一个结点何时完成了帧的发送)。 (体化: 消除 m每一个非活跃的结点: 第二个缺点是单点失效。 **今顾传谢林议**: 没有主结点 ト窓力◆線(token)的小的特殊輔在結占之间以基础固定的次序进行交換: 当-到今牌时,仅当它有一些碗要发送时,它才持有这个今牌。否则,它立即向下一个结点 转发该令牌;一个结点收到令牌时,若它确实有帧要传输,它发送最大数目的帧数,然 后把今牌转发给下一个结点。优化: 今牌传递是分散的、并有很高的效率: 一个结点的 MAC 协议: 雷色载下高效:没有冲突,节点公平使用信道:轻色载下低效:即使只有-个活跃节点也只能使用 I/N 的带宽。髓机接入 MAC 协议。 轻负载时离效:单个活跃节点可以使用整个信道;重负载时低效:频繁发生冲突,信道使用效率低。轮流协议(试 为的计算机及外设连接起来的网络,范围在几公里以内,通常为个人或机构所有;*就*被 阿*MAN*:通常覆盖一个城市的范围(几十公里),要能支持数据、音频和视频在内的综 合业务、服务质量好、支持用户数量多; 广域网 WAN (Wide Area Network): 通常覆 一个国家或一个洲(一百公里以上),规模和容量可任意扩大。 二一百名來 《广·河·一日公至以上),於彼州谷軍 (15思考) 人。 海· 吳阳為左西曆 (阿卡) 固定分配一个地址。除为**原理地址、硬件地址、超時后地址 MAC 楚继等,MAC 楚继长 6 个字节**:由 EEE 负责分配、相块适配器的地址是主线唯一 珍。 阿卡生产海的 EEE 與宗一柴 MAC 地址回 图 3 字字为,生产海绵生产的每一 块网卡有不同的 MAC 地址、MAC 地址图化在网卡的 ROM 中,现在用软件改变网卡的 IAC 地址也是可能的。 有多个网络接口的主机或路由器将具有与之相关联的多个链路层地址; 链路层交换机 是因为链路层交换机的任务是在主机与路由器之间承载数据报;交换机透明地执行该项 任务,这就是说,主机或路由器不必明确地将领寻址到其间的交换机。适配器的MAC I 址具有扁平结构(这与层次结构相反),而且不论适配器到哪里用都不会变化。目的 MA . ■ M MAC 級が有三种类型: 单播地址: 配器的 MAC 地址: 地址最高比特为 0: 多播地址:标识-多播帧 (若将适配器设置成**混收模式**,适配器将收到的所有帧交给主机)。**主机和路由器** 據口條了可能是認公並及於大學之,上於可以可以 可能了可能完整地之外还有 MAC 地址,这有部下几个原则。局域网是为住底网络层 协议而设计的,而不只是用于 IP 和四特网:如果适配器使用网络思地址而不是 MAC 地址的话。网络原址也必有可能本宽距器的 RAM ,并且在每次还距离的不成的 对要重新配置,另一种选择是在适配器中不使用任何地址,让每个适配器将它收到的每 制数据(通常是 IP 数据报)沿协议栈向上传递。然后网络原则能够核对网络地址层是否 匹配,这种选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。 为了使网络体 r的构群模块。不同的层次需要有它们自己的寻址方案。*如何实现直接交付*?当发设 节点 A、接收节点 B 位于同一个物理网络上时、数据报可从 A 直接交付給 B: A 的网络 是所数据报。以及 B 的物理地址交给据链路层:数据链路层将数据报封 装在一个结路层帧中,帧的目的地址=B 的物理地址、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。发送节点如何获得接收节点的物理地址?地址解析 85)。東四級高級公司的經歷。及逐可減回的軟件確保可減回的概定確定「是運輸的 Address Resolution)。同應了過程中差值,如何實際的在的MAC 建設计 進<mark>一般之地的缺点</mark>。主机每次使用的 IP 地址可能不同(DHCP)。主机可能更换同 是並維新的設(ARP)用于动态核母 IP 地址一MAC 地址映射,其基本思想是:若节 A 希望核符节点 B B)MAC 地址、节点 A 「獲 B B D IP 地址(地址解析源录),节点 B 用自己的MAC地址进行响应。ARP 据文格式: 硬件类型: 硬件接口类型; 对于以大网 核值为"1"。协议类型: 高层协议地址类型。对于IP地址,该值为 080016。操作: AF 青求为 1、ARP 响应为 2。在以太网上,ARP 报文封装在以太帧中传输。 *地址解析的过* Br. 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。 每个收到 ARP 请求的节点用目标 IP 地址与自己的 IP 地址比较,地址相符的节点进行 ip (B 响应)。4. B 构造一个 ARP 响应、交换发谈方与目标字段内容、在发谈方硬件 地址字段填入自己的 MAC 地址、修改操作字段为 2: 5, B 将 ARP 响应封装在单层帧 (目 地址为 A 的 MAC 地址)中发送。 改进 ARP 的措施: 一个地址映射 (绑定) 表, 称 ARP 缓存; 每次发送数据报前先查询 ARP 缓存, 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 缓存中的位 河则及这 AIT 明书, TITUS的 CAN THE AIT TO THE AIT THE AIT TO THE AIT THE P 表中; 节点在启动时自动广播自己的地址映射: 节点 A 在启动时主动广播 ,在目标字段内填入自己的 IP 地址,收到 ARP 请求的节点将 A 的地址映射缓存起 若 A 收到 ARP 响应,报告 IP 地址重复错误。 ARP 是即插即用的,这就是说,一个 表是自动建立的。一个 ARP 分组封装在链路层帧中,因而在体系结构上位于链路层 P表是自动建立的。 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 (栈。 **数据报到达子网之外:** 数据报从 A (子网 1) 经过 R (路由器) 到达 B (子网 2) 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 P 数据报, src (P= A, dest (P= B); A 利用 ARP 获得下一號 111.111.111.110 对应的 MAC 地址 (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, des AC = R-1、发送;R 接收帧,取出 IP 数据报,发现目的地址为 B;R 利用 ARP 获得 的网卡接收帧,取出了数据报、交给网络层。ARP与DNS的一个重要区别:DNS共EB特网中任何地方的主机解析主机名,而 ARP 只为在同一个子网上的主机和路由器 6口解析 IP 地址。数据报从 A 主机到 B 主机的过程(跨越局域网) 1.A 创建数据报 srcIP A. DstIP = B 2.A 查找转发表(路由协议)根据 DstIP 获取下一跳的 IP 地址 3.A 根据下-LEP 地址利用 ARP 获取下一跳默认网关的 MAC 地址:A 创建链路层帧,转装 IP 数据 Lep 地址利用 ARP 获取下一跳默认网关的 MAC 电址:A 创建链路层帧,转装 IP 数据 Lep 地址利用 ARP 获取下一跳默认网关的 MAC 电加速链路层帧,解封装得到 IP 数据报,获得 B IP 地址、利用 ARP 获取 B 的 MAC 地址、创建链路层帧、srcMAC = B DstMAC = 路柱 8另一侧接口、涌过 xx 接口转发 5.8 网卡接收帧:取出 IP 数据报交付网络房 6.当路由 8—段为内网一段为公网时,路由870年修改数据设的「P 地址 7路由8万层的链路 协议可能不同;交换机不同端口的链路层协议一定相同<mark>以太同:</mark>第一个广泛应用的局域 网技术, 也是目前占主导地价的有线局域网技术; 与其它的局域网技术相比, 技术简单 成本低,为提高速率,以太网技术不断演化和发展。 *战姓和针,我要或以太阳;*战机比,战机中 中期): 以同轴电缆作为共享传输媒体(总线),所有节点通过特殊接口连接到这条总线 集线器 (hub, 物理层) (1990s 后期): 一个物理层中继器、从一个进口讲入的物 申) 放大后立即从其它端口输出;集线器相当于共享电缆。星型拓扑; 是自己,从是一次,从几至地外的企物。相似,并未被自己,并不是一个地。 董州的"人 操成以太师,交换机(21世纪早期): 主机通过双致线或光纤连接到交换机,交换机 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! 星型拓扑: 各节点仅与中心节点直接通信,各 点之间不直接通信;不同于基于集线器的星型连接。以*太网帧结构;(按顺序)前*周线 010 字节、后跟一个 10101011 字节、用于在发送方和接收方之间建立B 司步。目的地址 (6 字节) + 瀬地址 (6 字节)。Type (2 字节):指出 Data 所属的海 B协议(如 IP、ARP等)。每个协议有一个编号、用于多路分配(和网络居数据报中 臺輪房根文段的端口字段类似)。Data: 46-1500 字节,不足 46-字节填3 ;以太网的最大传输单元(MTU)是 1500 字节,这意味若如果 P 数据报超过了 00 字节,则主机必须将该数据报分片;如果 IP 数据报小于 46 字节,数据报必须被填 夺到 46 字节,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 元到79千户,三元内元元号。 (1955年) 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 dest addr.、src addr.、type 和 data 四个字段计算得到的 CRC 码。所有的以太网技术都 向网络层提供无连接服务,意味着没有握手。以太网技术都向网络层提供不可靠服务。 前检测到冲突,帧的发送时间必须足够长;节点检测冲察需要时间,假设信号在相距摄 一个独立城的,在读帧经历了一连串的。次键接后,组点题则是以(0.1.2.3。 24m 上海上海一 K 组,对于以大同,一个组点等的的实际的同差。5322上线时间,成 全球的基本性。10.9.1.4. 指数面进动的最上层照照的效果或重新的同。类较重,长型、建筑速率21、对什么最小模长为。47字(不包括等等),程度是 実現的基本性。10.9.1.4. 指数面进动的最上层照照的效果或重新的同。类较重(产量)、2523年、3743年

100cc 物理病場方式不同,所不适定以太阳抗大市 EEE 202.3 下电轴系化、 201 电压 202.0 元间 202.0 集结器,光纤素大体宽2009 来,1,000460mg 以末两 (快速放车用),2006用光纤发放 5.45 以及数线器交换器,2008sa-74 (空间用致基础支收器),5.条效效性(2.75 (同元等的),5.条效性(2.75 (同元等的))。 不超近100米;1008sa-74 (可使用数量磁支收料),5.条效效性(3.7),不超近100 要标准(如底牙积的)。4.等此类数较能,无效的、不 5.45 (1.008sa-74 (可使用数量磁支收料)。3.类效效性(4.7),不超近100 要标准(如底牙积的)。4.等就基础设施,无效的、不 5.008sa-87 (以处使用变换的)。5.45 (4.5) (大周、只用交换机,并增加了对流量控制的支持: 1000Base-XX: 多模光纤,不超过 550 等**表表:** 信号在传播过程中能量逐渐减少(路径频矩):**干扰:**受到其它信号强闭干扰 米: 1000Base-IX: 单模或多模光纤,不超过 5000 米: 1000Base-CX (很少用): 2对用 多**各传播:** 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** 蓄双绞线 不超过 25 米: 1000Base-T: 4 对 5 类双绞线 不超过 100 米: 10GBase-- スピカルミド・スピカガーキのより、スピモカガラがルミド・**DIA MARK 30423 特**に 第一十年 - エエロり 2 ALS - A エロリカリ画 上州・ハロ 2 BLS - A PA に DIB では 2 PT - A PA に DIB では 3 PT - A PA に DIB では 2 PT 长度; 这两种格式都可使用,当 type/length 的值大于 1500 財銀程为 type, 否则解释为 节点只能知道其周围是否有节点在发送; 但真正影响此次通信的是接收节点周围是否有 1974年元本版、文版344API (文成519年) (841-27一74-24、サッドローラルでは、 通信、開始発生を完全・今日間の時間之間。 人権大士解文 戸房投援車戸研究機能 (1974年) 開始開始 (1965年) 地址而不是基于 IP 地址&&交换机类与路由器的转发表的构造方式有很大差别。**威的过** 淡的信标帧,主机选择一个 AP 发送<mark>关联请求帧</mark>,AP 向主机发送关<mark>联响应帧;主动扫描</mark> else 扩散帧(未知节点、采用扩散法转发)(向输入端口以外的所有端口转发) **交替机成** 度远小于发送信号的强度),不能检测出所有的冲突(隐藏节点)。**目标**:源变河 新教館が接近程。用機的自給性量数模支表(接受決策):若目的地址所在湖口 = 帧 CSMAC(cdissonA/voidance)、北井南 の2.11 密使用数弦研磨机接入。但这再 的进入湖口、丟弃帧:若目的地址所在湖口 + 帧的进入湖口、转发帧:若目的地址不 MAC 約沒有重要的区別:802.11 使用碰撞避免而率碰撞检测:由于无线信道相对较差 在转发表中、扩散帧。用帧的逐渐非查找转发表(更新转发表); 若找到选业、将对应表的设比特率。802.11(不同于以太网)使用链路层确认/重传(ARO)方案。802.11 的操作 項的主有期限力量大值。若沒有投到该地址,海斯斯地址构建入端口时供卖物。這里地 項的主有期限力量大值。在沒有投到该地址,海斯斯地址构建入端口时供卖物。這里地 項的主有期间发生机。更被制度是自动,这些自由治量之前,*支援机是自手习的* 到支线机模型的方包。200千日每个自由法理之前,支线机是自由于现象。 在该帧源地址字段中的 MAC 地址。该帧到达的接口。当前时间交换机以这种方式在1 的表中记录了发送结点所在的局域网网段。如果在局域向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国有记录。3)如果在一段时间(称为老化期后,交换机没有接收到以该地址作为源地址的帧,就在表中删除这个地址。以这种方式,如果 今 PC 被另一分 PC(具有不同的适配器) 代替、原来 PC 的 MAC 排址搭册终从该交换 使用信道预约机制的 CSMA/CA: 假设 A 欲向 AP 发说一个数据帧: A 向 AP 发说一 转发分组交换机,但它和路由暴星根太不同的,因为它用 MAC 地址转发分组。交换机 「冲突则不会给任何一方发说 CTS):若监听到信道忙则随机浪避 停等协议 2、等待 Di 这格生成可观的 ARP 油量和处理量: 交換机对广播风暴并不提供任何保护措施、交換机 SIFS: 允许正处于会话中的节点优先发说,如收到 RTS 的节点发说一个 CTS. 收到数计 径,它们允许以丰宫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 之后任何节点可以竞争信道。EIFS:如果以上间隔都没有发送,EIFS之后收到坏帧或对 · 由國列等个分組的处理时间進而に交換机更长。因为它们必须处理兩位第三屆的字段。 要改選的,你听信道:13 年-开始就侦听到信道空间,等待DFS 时间后发送线 23 传的化原文线线或格的器,几百年主机/网络、交换机或足够了,因为它们不要求它"地"则,意实一个编码间面,在例示的信道空间时间或过程。在处这样中传统可能偏端,让 进起时代阿拉斯波像是激励感化并渐渐进行者进一程是在由几千日主机组成的关大河,高端计镜域,25 中间,这里含个维持可能的。 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治量區 发送成功,若还有新的帧要发送,从第 2 步开始 CSMA/CA: 若未收到确认, 重新进 可在属于生成树的边上装发制; 当生成树上的交换机或铼路发生故障时,自用冗余铼路。 察对无线网络损害很大、要尽可能避免。 802.11 帧格式: 四个地址字段: Address 1 人员在物理位置上可能很分数(他们的主机连接到在不同的交换机),但是逻辑上,不 网向外路可需要调解,对重的的趋器头分割同风,成本原稿,**或的母域的/XM** 发生为理局域和上的一个逻辑 FFR,他含了配图为该 VAN 成员的所有方点,**命**个 发析 MAC、地址 AP 仅对天线线询见,对于超远网络(BR)最后等的 VIAN 在逻辑上是一个独立的网络: 每个 VIAN 是一个单独的广播域: 一个 VIAN 中的 duration of reserved transmission time (RTS/CTS), frame seg # (for reliable ARC) 子同地址划分 VLAN,**交换机如何在 VLAN 何称变的**,当一个朝到达时,交换机用商店 机械手等V VLAN,**交换机如何在 VLAN** 何**的变动**,一生 VLAN 对自然所有国。 18 AP3 中心转变**发**也需要更加,交换机*通过自主学习更新转变表*,交换机或到 11 上发现,**对是交换的 VLAN** 中国国际发来自任意 VLAN 的统 802.1 相连了所,有阿康逊勒克达。主机师看在同一个 P于两年,因而 P由是模特不变,以晚过至于 有VAND 國家政主 2021年,海加 4 字节 VAN 新型的 医硬物换尿切碎,120VAN 解现得,如此免收2. *随时强强,各种强强一个维持等的* VAN,使用需要的 VAN,至 支援力力,提展中产生的经过发展,在自由的收集表走工资的。 解的 VAN 文教师摄影的的法域口,逐 MAC 经比较减退 P地位(原决于 VAN 的划 生物与混合物性,更多的 B达线 VAN EXE 2018年,2018年 转支表、疾召下一度 IP 地区海道 II 利用 APP 疾得下一致 MAC 地址,用下一致 MAC (e.g., 79129.132)。**通信者**:希望与移动市点通信的市点。**移动方点进步**,移动市点进 地址的磁磁磁磁振频、发起。 西亚文学研发 P 中部分理:将以上第 II 第 2 步约指来受,从海南格后,向外长程全进,移动而直达分地代理向月南代建进**,要转起来** 存到地址三层转发来中,用目的 P 地址**支发三层转发表**,13条件,直接用下一层 MAC / 外先代理加藤场市点在长地网络上:月南代程建筑都多市点的转交地址,还来到地址 HTP: 主要都能测量。Background: 终端(特别是笔记本、智能手机)的处理能力 越来越强,成本越来越低,已经成为大众化的电子设备,用户随时随地上网的意愿非常 通信者将包发送给外地代理,外地代理将包转发给移动节点,移动节点直接向通信者

WiFi, cellular): 2. 多酰有基础设施: 主机通过多个无线节点的中继才能到达固定网络(如无线网状网络)3. 单跳无基础设施: 无基站,不连接到固定网络,节点间通信不得 夢中線(如蓝牙网络)4、单踝无基础设施;无基站,不连接到固定网络、节点间通信器 **正** 无线链路的特性: 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 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 注册—个恒定速率的轮询服务。声明自己希望得到的带意: PCF 的实现是可洗的。DC (Distributed Coordination Function)模式:可用于有基础设施的无线网络和无基设施的无线网络,所有实现必须支持DCF模式;所有节点(AP和无线终端)使用CSMA/(C 文竞争信道。CSMA/CA 支持两种机制:信道预约机制(可选),无信道预约的机制 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。路 知帧的节点可以发送一个错误报告帧。不使用微道预约机制的 CSMA/CA: 当节点有帧 MAC. address 3 = R1 MAC. 将该帧发给 AP; AP 将这个 802.11 帧转换为 802.3 帧 (ARP: 仍在准备: 域内跨由选择到 DNS 服务器: Web 李白一服务器交互: TCP 和 点移动及变换外地网络等对通信者都是透明的: 正在进行的通信可以保持! 直接选路

,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 从外地代理提供的转交地址中选择一个作为自己的转交地址。*移动主机注册*:移动 证信息等: 着认证通过,将移动节点的永久地址及转交地址保存在绑定表中,发 ,外地代理收到有效的注册响应后,将移动节点记录在自己的转发表中 > 3833 当移动节点回到归属网络时、要向归属代理注销。数据报间接选路。 包首先被归属代理得到;归属代理查找地址绑定表、获得移动节点当前的转交地址 · 属代理格數据但发送到转交地址: 外地代理将数据包转发给移动节点。*归属代理和* 學到数据报? 若通信者不在归属网络上: 数据包首先到达移动节点归属网络上的路由 KD) MAC ARM, 对为特别的 MAC ARM, 对数据指数表别胜阳远时不及这, 有雇用有 **1周网络上**: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 R、利用得到的 MAC 地址封装数据报,发送。<u>数据报如何能被归属代理得到</u>? 链路 帧的目的地址必须是归属代理的 MAC 地址;也就是说。移动节点的永久地址应当图 地址。ARP代理: 归属代理为位于外地网络的移动主机发送 ARP I AMC 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 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 刷新其它节点的 ARP 提存。数据报如何到达转交换址? 归属代理如何将数据报发决 \$\$\$\$\frac{\psi_{\text{in}}\text{in}}{\psi_{\text{opt}}\text{in}} \text{Non-transfer} 目的地址=转交地址 (x)(转交地址是外地代理的 IP 地址, 而数据报的最终目的 立是移动节点): 使用**账道(√) 账道技术的又一个应用例子)。** *归属代理通过帐道转送* 数据包: 归属代理向外地代理发送的包: Src P= 归属代理 P, Dst P= 转交地址,里 | 封装着通信者发送的包(这个包的 dest 是永久地址); 外地代理向移动节点发送的包: 涌信者发送的原始包。**外域代理如何转发数据和到移动节点?**外地代理解封装收到的数 語信。得到原始數是根,外地代理如何获得移动节点的 MAC 地址:在参考表达3033 接信,得到原始數是根,外地代理如何获得移动节点的 MAC 地址:在表示表达3033 夏,外地代理获知了移动节点的永久地址和 MAC 地址,记录在其转发表中;外地代3 根据目的 IP 地址查找转发表,得到移动节点的 MAC 地址; 外地代理利用移动节点 AC. 地址、将数据报封势到链路层帧中、发送绘移动节点。**移动节点如何发送数据何** 形动于点种数据包发送给外地代理(映画新曲器):Srchl=移动节点次块地址,Destly 通信者IP地址,SrcMAC=移动节点 MAC,DestMAC=外地代理 MAC;外地代理按照I 常方式转发数据包。移动节点如何得如外地代理的 MAC 地址?代理通告报文的源 MA 外地代理的地址。 的影响: 无线链路带来的问题: 误码率. 能上,有很大影响: 天包率高、传输延迟增大: TCP 将天包 (长亚 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。 十章机网络中的安全:什么是网络安全:网络安全的通用定义:网络安全是指网络系统 《日、《日本》《日本》《日本》《日本》(1985年)《日本》(1985年》(1985年)《日本》(1985年》(1985年)《日本 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 络不受攻击。网络服务可用。**安全攻击的孝型,被动攻击**; 试图从系统中获取信息 387-1-240日,可知成为了扩展。 不对系统产生影响,**两种美型:***给新***:**监听并记录网络中传输的内容;*造量分析*: 信频度、报文长度等流量模式推断通信的性质。*主动政击*;试图改变系统资源或影 个数据单元、经过一段时间后重新发送到网络中: 相文绪改,改变报文的部分内容 能及炎猪及交流交流交流及交换及的发送顺序;*拒絕服务*;阻止通信设施的正常使用或管理。 思*的安全机制:加密*;使用数学算法对数据进行变换,使其不易理解;*鉴别*;通过报文 **鈅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 称加密算法:加密密钥与解密密钥不同。按照明文额处理的方式,加密算法分为:块(向 CA 提供身份证明;CA 验证了 Bob 的身份后创建证书,绑定 Bob 及其公钥;证 操作素码: 保留明文字母不变、但改变字母的位置; 例子; 列操作素码。 療師 30000 水は低間。 将田町スナツイツ、 PB以東子中的区質、 例す: 列映区密码。 **層線** 安全性・传統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 接位两种基本手段、 B型代密码学的基本原则是、加密与解密的算法是公开的、只有 【下两个条件之一:破译密文的代价超过信息本身的价值;破译密文所需的时间超过信息本身的价值;破译密文所需的时间超过信息本身的价值;破译密文所需的时间超过信息。 有双生印刷。现代省码子中,省码的安主性走通以算法的复杂性和省前的长度未成 。**针对加密系统的密码分析攻击:偿密文攻击:**密码分析者仅能根据截获的密文进 分析、以得到明文或密钥(对密码分析者最不利的情况); **巴如明文政赤**; 密码分析者 7 有截該的密文外,还有一些已知的"明文·密文州·来帮助破译密码,以得出密钥;必 明文**攻击**:密码分析者可以任意选择一定数量的明文,用被攻击的加密算法加密,很 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。

全的加密系統必須能抵御选择明文攻击。全表快密码难以实现。DES (Data Encryptic landard):块加密算法,每次以 64 比特的明文块作为输入,输出 64 比特的密文块; ES 是基于迭代的算法,每一轮迭代执行相同的替换和换位操作,但使用不同的密钥 S 使用一个 56 比特的主密钥,每一轮迭代使用的子密钥(48 比特)由主密钥产生 常算法,加密和解密使用相同的函数。两者的不同只是子密钥的次序则好 - 轮今 DES 设备工作于加密模式, 使用密钥 K1 对明文讲行变换; 第二轮今 DE |異:第一彩で VES 改善上作丁加密模式、使用密钥 NI 为明文地行文祭、第一彩で VES 接番工作于解码模式、使用密钥 N2 对第一轮的输出进行变换:第三轮令 DES 设备工作 - 加密模式、用密钥 N1 对第二轮的输出进行变换、输出密文。**有差 3DES 的三个问题**: 个密钥而不是三个密钥? 112 比特的密钥已经足够长。为 而是三重 DES?考虑采用 EE 模式的两重 DES,且攻击者已经拥有了一 | 配的的文 -- 密文対 (F), C1), 即有 C1 = EKZ (EKI (P1)), 令 X = EKI(P1) = DK2(C1), 法者分別计算 EKI(P1)和 DK2(C1), 并寻找使它们相等的 K1 和 K2, 则穷尽整个密钥空 只需 256 的攻击量而不是 2112。(中途攻击) 为什么是 EDE 而不是 EEE S 兼容。3DES 用户解密单次 DES 用户加密的数据,只需令 KI = KZ 就行了。AES Advanced Encryption Standard): 每次处理 128 比特明文块,輸出 128 比特密文块; 钥长度可以是 128、192 或 256 比特;如果使用强力方法破解、假设破解 DES 需要 則破解 AES(128 比特密钥)需要 149 万亿年! 密码块链接(Cipher Block Chaining 每个明又块被独立加密,相同的明文块生成相同的密文块,容易被重放攻击利用。 块链接(CBC):发送方生成一个随机的初始向量 c(0),用明文发送给接收者;每一 月文块加密前,先与前一个密文块进行异或,然后再加密:第一个明文块与 c(0)异或 对称加密算法:要求发送者和接收者使用同 A方选择了一个密钥后,如何将密钥安全地传递给接收方?非对称加密算法:安选者和 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 多收者不共享密钥,发谈者使用加密密钥,接收者使用解密密钥,不存

I密密钥放在一个公开的文件中,解密密钥妥善保管;当 Alice 希望向 Bob 发送一个 指息时: Alice 从公开的文件中查到 Bob 的加密密钥,用 Bob 的加密密钥加密信息。 送给 Bob; Bob 用自己的解密密钥解密信息。**公开密钥和私有密钥**:公开密钥:加密 密钥、由发送者使用:私有密钥:解密密钥、由接收者使用。要求:KB-() 定公销KB+,不可能计算出私钥KB。 **公开密钥算法应满足的条件**;从计算上说 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。 可解密密钥,从密文计算出明文是容易的,从加密密钥推出解密密钥; ②计算出原始明文是不可能的。公开密钥算法两个问题:入侵者知道该公额 加密算法,可以据此发起选择明文政击; 加密密钥是公开的,任何人都可能向 Bob; J加密异法,可以俄武及医选择可义以市,加密密制建公开的,任何人都可能问 800。 他一个已加密的报文,在单一共享密钥情况下,发送方知道共享秘密密钥的事实就已! 接收方隐含地证实了发送方的身份,然而在公钥体制中,这点就行不通了,因为任 个人都可向 Bob 发送使用 Bob 的公开可用密钥加密的报文,这就需要用数字签名把 BB || Data || Kb+ (Ka-b) || signatureA. 8—A: 18 || 16 || 10 A || r/m || Data || Ka+ (Kb-a) || signatureA. 8—A: 18 || 16 || 10 A || r/m || Data || Ka+ (Kb-a) || signatureA. 8—A: 18 || si 发送方和报文明定起来。RSA **算法: 生成節**朝: 选择两个大素数 P和 () () () () 型位为大干 10^100); 计算 n = p·q 和 z = (p·1)·(q·1); 选择一个与 z 互质的数、令其为 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)。 RSA 算法: 加密和

接收方有一个共享的密钥,可以通过加密报文来提供报文鉴别:发送方用共享的密钥密整个报文、发送给接收方;如果接收方能够正确解密收到的报文,则报文必是可信 分介,设想:发送者用明文发送报文,并在报文后附上一个标签,允许接收者利用这 标签来鉴别报文的真伪,用于鉴别报文的标签必须满足两个条件:能够验证报文的完 8性(是否被除改),不能被伪造。 **最假完整性和限义确要:很文确要(数字相收)**,将 个散列函数件用到一个任意长的报文 即上,生成一个固定长度的散列值 H(m),这个 好例格为为诸权分据文确要(messape digest)业称数字指纹。*使用象义需要整位* 2的完整性: 发送者对发送的报文计算一个报文摘要,作为标签和报文一起发始接收者: · 较:缺点:需要使用加密管法。<mark>需碼數列函数: 为什么要开发一个不需要加密算法</mark> 次*鉴别技术*?加密软件通常运行得很慢,即使贝加密少量的数据;加密转件的代价是 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 定的数据块 x,要找到一个 y ≠x 并满足 H(y)=H(x),在计算上是不可能的: 该特性及 使用加密算法的报文鉴别很重要,如果能找到一个不同于 x 的数据块 y,使得 H(y)=H(v B & 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 是不可能的。(抵抗生日政治) 满足前四个特性的散列函数称为弱散列函数、满足所有 个特性的散列函数称为强散列函数。 **散列函数标准**:目前使用最多的两种散列函数 D5: 散列品长度为 128 比特; SHA-1: 美国联邦政府的标准, 散列品长度为 160 比特 前获得最多支持的密码散列函数方案为 HMAC, 已应用到许多安全协议中。 小可以替代手写答名的数字答名必须満足以下三个条件。接收方通讨文档中的数字符 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进过差名的文档(防陆 赖),接收方不可能伪造被签名文档的内容。MAC 无法胜任这项工作,因为有两个人拥 有它。用私钥加密根文牌要;发送方先计算报文编要,然后用自己的私钥加密报文编要 形成数字等名,数字等名附加在报文后面一起发送;接收方线贝—份数字等名。妥善保 ND)。如何可靠地获取公明?考虑下面的例子: Bob 将公明 EB 发布在自己的主页上; lice 获取 Bob 主页的请求被 Trudy 截获,Trudy 将假冒的 Bob 主页发送给 Alice,主页 的公钥是 Trudy 的公钥 ET; Alice 使用 Trudy 的公钥加密会话密钥,发送给 Bob; Trudy Bob 的公司,并有 CA 的签名。近非的验证:当 Aice 需要 Bob 的公司的:获取 Bob 证书;使用 CA 的公钥验证 Bob 的证书,得到 Bob 的公钥。 **X.509 证书**:目前最常月 证书标准:建立在公钥算法和数字签名的基础上:CA对证书内容先进行 SHA-1 散列 。由一个组织运行多个CATen识理器。信任问题。分布或公明基础设施。 作astructure,PKIJ:提供公钥加密和数字签名服务的系统或平台;包含不同组织运行 CA、每个CA拥有自己的私钥,负责为一部分用户签发证书:用户自己决定使用哪一 . 信仔維与信仔鏈: 信仔锚 (trust anchor): 信任的起点 系统中的所有实体都以 CA 的公明作为它们的信任锚,信任锚必须通过安全的物理途径获取;信任链(chain trust):从叶结点到根 CA 的证书序列;根 CA 的选择:有许多根 CA,每个根 CA 都 百自己的一个分级结构, 所有根 CA 间可以进行交叉认证; 用户自行决定信任哪个根 CA; 许多根 CA 的公钥接预装在浏览器上、这些根 CA 由浏览器厂商认证并嵌入到 答: 网络排址: 18.208.0.0 件中,關軟件一起发布。*证明的機構*,每个证书都有有效期,过期后证书自动失效,广播地址:18,223,255,255 也可以显述機構证书,逐聚系CA 定期地及存证书籍研列家(Certificate Revocation 邮/用户地址:18,008.01 8、CEU)。来中的出已整编销的证书评例写,每个用户在使用一个证书新要要丢款取,最大用户地址:18,223,256,254 RI、检查该证书是否在CRL中,*证书存放在哪里*?使用 DNS 作为证书显录,该方案的 准为 DNSSEC;使用专门的目录服务器存放证书。该方案的标准为 LDAP;证书撤销列 通常与证书存放在一起。CA 定期地将 CRL 推进目录服务器,由目录服务器负责将 CRL 列出的证书清除植。 端点基别,端点基别,一个实体经过计算机网络向另一个实体证 明其身份的过程。鉴别应当在报文和数据交换的基础上,并将至24分钟或的一部分独立 完成。鉴别协议通常在两个通信实体运行其他协议(例如,可靠数据传输协议、路由选 择信息交换协议或电子邮件协议)之前运行。鉴别协议首先建立相互满意的各方的标识。 当鉴别完成之后。各方才继续下面的工作。 鉴别协议 ap1.0: 直接发送一个报文。 --个不重数 R. 然后把这个值发误给 Alice: 3) Alice 使用她与 Bob 共享的对称秘格 - 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 60.5 左协议 ap3.1 - 一样、由于 Alics 知道 KA-B 并用它加密一个值、就使得 Bob 知道收到的报文是巾 Alics 生的。这个不重数用于确定 Alics 是活跃的; 4) Bob 解密接收到的报文,如果解密得

一个用户的一次报文传输(接收方鉴别发送方);双向鉴别;通信双方相互鉴别;

鉴别·通信双方相互鉴别,并使报文同步机制,单向鉴别·Gone-way authentication) A→B:tA ||rA|| IDB || Data || Kb+(Ka-b) || signatureA,说明:tA:时间载,由报文的产时间和到期时间组成,rA:A 随机选择的一个不重数,供接收者检测重放攻击;IDB:

Morku、指示报文的接收者,Data: 报文中包含的数据信息: Ka-b :若Data 需要保密 则 Ka-b 为 A 加密 Data 使用的对称密钥; Kb+: B 的公开密钥,用于加密对称密钥 Ka b; signatureA: A 的数字签名,对 tA、rA、IDB 和 Data 的明文生成; 接收方鉴别:

自己的私钥解出 Ka-b、用 Ka-b 解密 Data、计算前面 4 个部分的报文编纂:B 用 A A 公钥从签名中将到原始的报文档。 Zeles Zeles

J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

○曹敬宗、如用于鉴别、数字签名或发进一次性会记者明等。 通知 和 Bob 具有读者明创剧本,这使得分发对称密明显常图束。公开查阅查阅?效率 相对证下,这其对于任意义是是职业,为了复数学事间重要的对象。 《新春光集》目除的美国主义是被参加,是一个概义是有可能的技术。一个概义是可能的 《新春光集》目除的美国主义是被参加,是不是被多类的方面,也就是形,提入是否未,来说:1. 从中。 由于一个规划中的运行部份,这一点还不够称着到时度的模型, 自声称的源:*元整件检查*:报文是否被修改过。方法一:对整个报文加密,如果发达了。3),用 Bob 的公钥 RB-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。 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**:他也 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。*只美心发送方鉴其* s。缺点:<mark>混淆了机密性和报文鉴别两个概念,</mark>有时我们只想知道报文是否可信,而报 成本身并不需要保密,加密整个报文会带来不必要的计算开销。*将报文鉴别与数据机密* 一个散列函数 H(例如 MD5)从而得到一个报文摘要;用她的私钥 KA-对散列函数的结别 进行签名,从而得到一个数字签名,把初始报文(未加密)和该数字签名级联起来生员一个包;向 Bob 的电子部件地址发送这个包。当 Bob 接收到这个包时:他将 Alice 的公 钥 KB+应用到被签名的报文编要上: 将该操作的结果与他自己对该报的散列 H 进行 协 设计一个提供机磨件 发送方案到到报文宗整件的由子邮件系统, 计程结会记字 实现: Alice 首先生成一个预备包,它与图 8-20 中的包完全相同,其中包含她的初始 文和该报文数字签名过的散列;然后 Alice 把这个预备包看作一个报文,再用图 8-19

组的分片中、MF(或 M)位是 0、HLEN 是 10、总长度是 200。

水X、川(水)路各新订单,对于世感或走到面,委托到一个X 海走川(X)-1,在订单上。於 丁相以入事,对正在 NKT 海水到**来在一门 海水中**之36。而从代谢亚达30家在一门 7 不可能的(单向性),该特性对于使用密码数列高数的规文室别很重要,如果根据<mark>繼續中变这?</mark> 答:发送节点利用 ARP 请求查询目标主机的 MAC 地址。由于高不知道的 KS||m|-n 可以投影一个 x、使得 H(x)-n,那么根据 x 和 m 可以推出 KS; 对于任意,联走机的 MAC 地址,所以 ARP 请求封装在广播帧中发送。交送 ARP 响应的节点之经入 ARP 请求中获得了请求节点的 MAC 地址、所以 ARP 响应可以用单播帧发送。5. A fo (4) 或 (3)(2)加密会话密钥 (2) 8. 若一无限用户 slotted ALOHA 信道处于负载 g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 份鉴别、报文完整性和防发送方抵赖的安全机制。请给出数字签名最常见的构造方。 加強力、協力的協力方法。说明数字签名为什么可以提供以上安全服务。等(1)当实为 A需要为报文 M 生成数字签名时,A 首先用一个敵列函数计算 M 的报文摘要,然后) 绘的操作: 四种差型: **伪装:** 一个实体假冒另一个实体: **重放:** 从网络中被动地获取 会量更高的"技术"因为它需要一个如后而描述的,具有认证中心支撑的父钥基础设施 A 的私钥加密该报文接要 生成数字签名。(2) A 的私钥是只有 A 知道的秘密、任何甚至 字体无法得到。因而一个有效的数字签名可提供发送方身份鉴别。报文编要可用于检》 很文的完整性,对报文内容的任何修改将产生不同的报文摘要。用 A 的私机加密后的计 收摘要是不可伪造的,从而数字签名就将 A 与报文 M 紧密关联在一起,既能提供报义 福號 16 <mark>電路层 ACK 的作用 (1) 差错控制,确认,实现可靠传送(2) 流量控制,测动的口 17. 10 若使用一个 256-kbps 的无差错卫星信道(往返传播时延为 512-msec)一个了向上发送 512-byte 数据帧,而在另一个方向上返回很短的确认帧。则对于窗口大小少</mark> 15. 127 的最大吞吐量是多少?512*8/256k=16ms (1)k=1.16/(16+512)*256=7.

| | | 6田农,现收到相邻 新路由器 R1 的路由 | |
|------------|------|--------------------------|--|
| 3-1 路由器 R1 | 的路由表 | | |
| 目的网络 | 距离 | 下一跳 | |
| Net2 | 3 | R5 | |
| Net3 | 4 | R3 | |

Net5 表 3-2 R2 发给 R1 的更新 目的网络 答:路由器 R1 的路由表 目的网络

度早 800 分片偏移值早 300 过来该分片第一个字节和最后 跳"路由器知道剩余的路径信息或网络中的所有路由器信息保持一致。 答: RIP 缺点:(1)更新周期(30s)过短:(2)未进行区域划分 OSPF 缺点: 用回

《的缺点。音:KIP 联点:(1)史斯网邦(いの)にスメヒュ/ピノヘーメムi ッ ニューッ &广播方式在整个区域广播所有节点的链路状态,开销过大 f于下图中的子网,若采用下列方法,从 K 开始广播需要产生多少个分组?



在下图的网络拓扑中, A-F 为路由器, 边上 的数字为链路代价。 (1)给出以 A 为根的最小生成树 (最小生成 树由各个节点到A的最短路径构成 例出合「下京別 A 的版版超程特成) (2) 假设连接到 A 上的一个主机 S (图中未 画出) 向网络中发送了一个广播分组,该网络

发送给 A 的分组不算在内)。答:(1)--(2)共13 个分组副本 若一无限用户 slotted ALOHA 信道处于负载不足与过载的临界点,则(1)信道中空闲时槽 的比例是多少?(2)成功发送一个帧发送次数是多少*答:(1)pi=o°,G=1=pi(空闲比 =36.8% (2)G/S=1/0.368≈2.72(注:S=Ge⁻⁶) <mark>緣 IFFE_802.3 MAC 协议要点</mark>答:发前监听(CS),边发边听(最小帧长),冲突避让 2)802.3u:512+5.12₁x; <mark>EEE 802.11 协议哪个(成几个)控制帧发现隐藏终端与暴露终端的</mark> : (1) 隐藏终端: CTS; (2)暴露终端: RTS/EEE 802.3 MAC 协议中最小帧长的功能与计 答:最小帧长的功能:检测冲突。计算依据:传输速率*2*相距最远两个站点间 报文编要、牛成数字签名。(2) A 的私钥是只有 A 知道的秘密、任何其它实体无法得到 · 个有效的数字签名可提供发说方身价鉴别。据文编票可用于绘测报文的字数代 3100一,有双的数十亚名可提供及应月对印鉴所。极大测安与用了他所放大的无证上, 封报文内容的任何修改将产生不同的报文摘要,用。的私钥加密后的报文摘要是不可伪 结的,从而数字签名就将 A 与报文 M 紧密关联在一起,既能提供报文完整性服务,也

牛成树广播: a)错, b)错 255.240.0 。如果按照 IP 地址从小到大对于网进行编号,写出第 2 个子网的地址范 用 a.b.c.d/x 的形式表示 128.16.16.0/20 。 內路由器收到以下四条新的前缀: 157.6.96.0/21、 /21. 如果这些地址使用同一条输出线路。它们能被聚合吗? 如果能、请给 能, 聚合后的前缀是 157.6.96.0/19 的地址为 200.24.11.4 的数据包,请问应使用哪个表项转发数据包? 3・14/17 2006年7000年2 45 98 78 48 18 g以下格式給出主机 A 和路由器 R 中的转发表,假设图中两个网络的子网掩码均为 255.255.0. 主机 A 的端口编号为 1. 路由縣 R 的端口从左至右编号为 1. 2 目的前缀 111.111.111.0/24 default 或者 222.222.222.0/24 b议?哪一种(或几种)是有冲突的协议 多址接入协议划分为信道划分、随机接入、轮流协议三种类型。 信道划分和轮流 议是无冲突的, 随机接入是有冲突的。 发送节点利用 ARP 请求查询目标主机的 MAC 地址,由于尚不知道目标主机的 MAI ,所以 ARP 请求封装在广播帧中发送。发送 ARP 响应的节点已经从 ARP 请求中获 了请求节点的 MAC 地址,所以 ARP 响应可以用单播帧发送

5点 A、B、C 连接到同一个广播局域网上,A 向 B 发送的单播帧(dest MAC = B), 在器能收到吗?如果能收到,C 的适配器会处理这个帧吗?如果会处理,C 的说 能收到: 会处理: 但不会将 P 包交给自己的网络层。 . 8 .

影防止发送方抵赖。<mark>对于无控制洪泛,受控洪泛和生成树广播三种广播洗路方式。下</mark>

法是否正确。a) 一个节点可能收到同一个广播分组的多个拷贝;b) 一个节点可能飞 同的出链路上多次转发同一个广播分组 答: 无控制洪泛;a)对,b)对。 受控洪泛



を知る。 を如图所示的网络中、路由器 R 连接了两个链路层交换机 S1和 S2。假设主机 A 向主机 B 发送了一个数据报(src IP = A、dest IP = B)、请给出编号①~④的线路上传输的以 太帧的源地址和目的地址,填入下表。MAC地址用符号表示,比如 A 的 MAC地址表示为 A、R 的端口 1 的 MAC地址表示为 B、R 的端口 1 的 MAC地

下-学

(直接交付也可以)

111.111.111.110

- (写直接交付也可以)

別分为嘅三种类型?其中、嘅一种(或几利

| 线路编号 | Src MAC | Dest MAC |
|------|---------|----------|
| 1 | A | R-1 |
| 2 | A | R-1 |
| 3 | R-2 | В |
| 4 | R-2 | В |

DM、TDM 和 CDMA 都是信道分区 MAC 协议

1.19 考虑向具有 700 字节 MTU 的一条链路发送一个 2400 字节的数据报。假定初数据报标有标识号 422。将会生成多少个分片? 在生成相关分片的数据报中的各个字段。 [段数为 [(2400 - 20)/680] = 4 段, 即生成 4 个分片。分片相关的 IPv4 报文字段包 标识 标主和片值路,对于标识字段 其中每一段都会有标识符 422:对于标主字段 7年2月 (東京 中央 1) (東京 中央 1 F是 8 的倍数, 680/8 = 85 因此这四个分片的片偏移字段应为 0, 85, 170, 255 7.78 o 9] (4), 000/0 - 03 000/0 - 10 000/0 - 10 000/0 - 10 00/0 d 使 $ed \mod z = 1$ 此处取 d = 7 此时可以得出生成的公钥 $K^+ = (n, e) = (33.3)$ $SH K^- = (n d) = (33.7)$

| RSA 加密, $n = 33$, $e = 3$ | | | | | | | |
|----------------------------|--------------------|--|------------------|-------|------------------|--|--|
| 明文字母 加:数字表示 | | | m^e | 密文 c: | $c = m^e \mod n$ | | |
| d 4 | | | 64 | | 31 | | |
| 0 | 15 | | 3375 | | 9 | | |
| д | 7 | | 343 | 13 | | | |
| RSA 解密, n = 33, d = 7 | | | | | | | |
| 密文 c | Č c c ^d | | $m = c^d \mod n$ | | 明文字母 | | |
| 31 | 31 27512614111 | | 4 | | d | | |
| 0 4792060 | | | 15 | | | | |

| 32世前 | | | | | | | | |
|-----------------|--------------|------|-------------|------------|---------|--------|-------|-----|
| 本 | 1118 15.8 | 服务类型 | 数据相长度(字节) | | 321£49 | | | |
| | | | 标志 | 标志 13比特片偏移 | 版本 流量类別 | 武量类型 | 投标等 | |
| 寿命 上层协订 | | 上层协议 | | 百开松安和 | - | 了效義荷长度 | 下一个价格 | 跳飛到 |
| 3万比特别作地址 | | | 加油社(128比特) | | | | | |
| | | | 目的地址(128比特) | | | | | |
| 32比特目的P地址 | | 教経 | | | | | | |
| 选项(加票有的话) | | | | | | | | |
| 教務 | | | | | | | | |
| 輔(数字代表該字段的字节长度) | | | | | | | | |

解控制 持续期 地址1 地址2 地址3 序号控制 地址4 有效截荷 CRC 帧控制字段扩展(数字代表孩子字段的比特长度)

物议版本 类型 子类型 到AP 从AP 契多 泉武 物率 更多 WEP 保留