14AK4 网络层中的玻璃面 - 1/134 网络层为传输层提供<mark>主机到主机</mark>的通信服务 每一合主机和路由器都运行网络层协议 **发送终端** 将传输层报文段封装到网络层分组中,发送给边

3.发送终端,将传输层报文块封装到网络层分组中,发送给边缘路由器接由器将分组从输入链路转发到输出链路接接,接收线端从边缘路由器接收分组取出报文段交付给传输层 4.网络层的两个功能 选路,确定去目的路由器的路由。(计算转发表,转发,路由器根据选定路由将分组从输入转移到输出根据转发表转运分组) 转数是数据面功能,在路由器内部实施分组转运 转发是数据面功能,在路由器内部实施分组转运 控制面、控制数据传输的和论版图本器由、如能以等程生如独立

转发是数据面功能。在路由器內部实施分组转运 控制面,控制数据传输的功能问路范围的功能)逻辑集中、独立 选路是控制面功能确定为组如何去往目的节点 (传统寻路算法路由器中实现软件定义网络服务器中一) 7 网络服务程型定义分组在发送终端与接收终端之间的传输 特性(保证交付具有时延上界的保证交付有序分组交付、保证 最小带宽安全性)——网络层服务在网络核心实现 **不同架构的网络提供的网络层服务。 "一个网络也可以提供不同的网络层服务" "一个网络也可以提供不同的网络层服务" "一个网络也可以提供不同的网络层服务" "是一个网络也可以提供不同的网络层服务" "一个网络一位"以提供无连接服务)<mark>虚电路</mark>(面向连接) *一个网络不能同时提供无连接服务)虚电路 (边缘)实现。 1 虚电路(网络层)—条编到端路径传输(经)。 "传输层,进程"进程可同时提供且在网络终端(边缘)实现。 1 虚电路(网层)—条编到端路径传输(保),将路由器资 源带宽缓舟;预先分配。可提供可预期的网络服务。 2 本质预先选好从源主机到目的主机的选定(分配资源可选)

源(市宽、聚行)颁先分配,可提供可與期的网络服务。 2本 **成** 预先选好从源注却到目的主机的,选定(分配资源可选) 3 实现、从源注机到目的主机的端到端路径+途经每条链路时 的虚电路号(用于区分绘过该链路的不同虚电路(仅有本地意 以)+沿途每个路由器中的转发表项(人调上+从VCH同理) 4 过程分组只需携带VC号,不带目的地址。路由器利用输入端 1 至402目来地链份,主地产型的似地。路由器利用输入端 1 至402目来地链份。主地产数四份(WCH)

※各、你培育及求从網入強由到面链由特及致婚规(使行所) 全輸入端口力能,物理层(持中交换,查表|本地],排队[阻塞时],转发 (也叫交换),性能要求:以"线速"完成输入端口处理 3交换结构 發由器中的互联网络用于在输入端口输出。 选择是强之间转运分组、交换速率通常是输入/出链路速率的 若干倍三种类型的交换结构(memory, bus, crossbar) (河通·竹皮左旋。)

p是Aklen和上一次丢弃距当前时间的函数以证相关) 先来**先服务价先级调度 i 非抢占式优先级排队**开始传输后不 能被中断**i 轮询调度** i 队列之间轮流提供服务,每次选择一个以 头分组加权公平排队,投每队列带宽权重发进一定数量分组 ²**llternetProtoca**l将数据较分付到目面发达一位协协议 不提供任何服务承诺尽力而为;数据报过大/循环/报头错误



TCP头=20bytesTCP+20IP+应用head length单位是4字

TICP关=Zubytest_verth Zubr+应为mead tengun=业应分子 **享节**)用于分片重组:timetolive剩余最大跳数:每转发前-1.upperlayer处理载荷的协议,用于解复用checksum头部检验。 即分片重组:链路层帧能承载的最大数据字节数.MTUC不定 以太网帧(max1500字节)部分广域网帧(5768)每个数据块 封装成独立数据报传输可多次分片。但仅在目的主机上重组 2.2000年10月以上,自然数据以图显示2000年10月以上,自然数据以图显示2000年10月以上,自然处据,是10月以上,自然处据,是10月以上,自然处据,是10月间, 封裝成独立數据报传輸可多次分片,但仅在目的主机上重组 倫移量、數程原始报头标识(每分片与原始数据报相同标识) 偏移量、數据在原始数据报载前中位置标志位(MF最后一个0 其余1.DF=1不允许分片)<mark>分片修</mark>观息长度=H+数据块长度。 展后报头MF位置0.其余MF位置1.偏移量:第一个为0.数据块 在原始报载前中的字节序号/8.TTL=TTL-1计算头部检查和 分片长度,原始报头长度H分片的数据长度N、H+N SMTU-编 据长度 N 应为满足以上两个条件的最大整数 重组1.收集分片:目的主机用<源P标记-确定属于同一数据 组的公长。为组用最后条件管 简始长度:简单长序:但每条9。0。

32位全0:指示本机(仅用作源地址);网络号为0,主机号有效:本 网中的主机;127.xx.yy.xx的地址:保留作为回路测试,发送到这

特点,路由器每个端口连接一个子网,不同端口连不同子网一 定路由器在子网间转发;子网内部通信无需路由器,之间必须。 IP数据报转发 直接交付:节点将数据包直接发给目的主机,无

需其它路由器转发,目的地址与本节点某端口在同一子网中,间接交付节点转发绘一个路由器处理目的地址不与任一端间接交付节点转发绘一个路由器处理目的地址不与任一端有发表记录目的地址到输出端口的映射:三类转发表项,目的地址是子两地址地址前级表项特定网络接口地址特定上机表项缺省项不匹配其它表项部映射到默认路由器端口即采用。驱烧路,转发表项门记录下一般信息转发表项包括目的地址/掩码、下一跳路由接口沙址输出端口下一般地址须与输出端口在同一子两(无需效现包)转度的交给即位的任何一个直接以下,是一个最大的人员的一个地址前级表现的技术的大量,是一个地址的级度分析。发到下一跳名表中包含到外的一个地址前级表现/间接交付发到下一跳名表中包含到外的一个地址前级表现/间接交付发到下一跳名表中包含到外的一个地址前级表现/间接交付发到下一跳台包含一位连路联系则是的影片以及明末处,发到下一跳台。一个路上被一下,以下,将着干条转发表项进行聚合减小转发表规模,也比较长度是分的需次之所有地址前级2.10点1位必须相同3可以用接码或者"水度来表示行两地址的长度地址接入是是的196章后,是一个数字下一张和一个一个一个一个一个一个路上看一个图本面不需以来一个全面

3.可以用掩码或者/长度/来表示/网地址的长度 地址聚合:目的地址可聚合成更短前缀地址&下一跳相同 若个别表项不满足路由聚合条件,仍可给出一条聚合表 项20023.160/20;同时给出不能被聚合的表项,20023.180/23 分类地址转发表:根据目的地址类型确定要查找的转发表 分类地址转发表:根据目的地址类型确定要查找的转发表 分类地址转发表。根据目的地址类型确定要查找的转发表 从BC)提取网络地址相应转发表中进行印希查找精确匹配) CIDR好1块需分配解决地址空间浪费2地址聚合解决转发表 空间爆炸环1.地址前额长度可为任意值2Prefixlen无法从地 址本身得91.7k能从转发表项得332必须注射缩聚长的表项 获得PP增址路由器管理员手工配置各个接口的IP地址 主机1管理员于正配置车机PID间常服务器2或办套土机配置协 设DHCP按取IP地址子网掩码。缺省路由器本地DNS服务器等 (通常个人终端)免去手工配置麻灰即指面即用,可地面积 目标。公主对加入IMQB中日和共和原理作同序已由至第

(通常个人终端)免去手工配置麻烦(即福即用)。可地址重用 目标允许主机加入网络时**自动获取配置**信息(客户-服务器) 每个子网须有一个DHCP服务器/代理新到主机运行client 过程主机广播"DHCP discover"。寻找子网中的DHCP服务器 服务器用DHCP offer"回应给出推荐的护地址及相拟(及等 跳路由器P(缺省网关,边缘路由器)。本地DNS的P,地址掩码) 主机"DHCP request"选择一个DHCP服务器。向其请求P地址 服务器"DHCP ack"响应客户的请求·输入所要求的参 *DHCP服务器使用业DP端口67条户使用以DP端口68 报文传输:DHCP请求被封装到UDP/IP/以太帧中并广播

<mark>网络地址转换(NAT)</mark> **目的**:1.用一个公用IP支持多用户**同时**上网2.仅为公共可访问 节点分配公用IP(<u>减公用IP数)3.内部节点</u>对外不可见(**安全**)

NAT转换表 因特网侧地址 本地地址 138.76.29.7, 5001 10.0.0.1, 3345 2: NAT路由器排数 10.0.0.2 138.76.29.7 5:128.119.40.186, 80 1, 0:138.76.29.7, 5001 3:响应的数据报到达, 日的格标上。 4: NAT路由嘉将数据报 的目的地址138.76.29.7, 5001

器通告它在<13876297、5001上可用其它主机通过追踪器可以看到该主机,并能向<13876297、5001一发起了它连接的AT7条12876297、5001一收到的SYN包转发给主机1000.12使用中華服务量(Stope) [100] [10

IFVOLUSANI 专制,不则定当专政核总。IFVOLUSE IFVOLUSE 財,未被IPVAI的由器检查处理,推入TTL未减1.SB DE 在路由器在的IPV6看来。IPV6包是从路由器B直接到来的 **CHAPS阿翰是中的控制** 1.TP 两种建立控制面的方法,per-router control (traditional)

设置到该邻居的距离为16;发送RIP通告 毒性逆转:若选路表中到x的路由是A通告的,则向A通告该路

由时,到 x 的距离设为16(阻止A使用这条路由) OSPF: 较顶层ISP使用,LS(还有EIGRP.cisco私有协议,后公有)

在用放射、各种新种的核文化几级补机体企工作时由由非和 拥塞其弄不重要数据包增加PacketTooBig报文; 信息查询:去掉不必要的;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

APP(地址解析和IGMP(多播组管理)的功能

11-14 数据链路上 11-14
建路层 持数据报从一个节点传输到相邻的下一个节点物理层 多种类型传输媒体 传输原始比特流易产生传输错读 节点主机和的由器 链路 连接相邻市点的信道 帧 链路层分组 服务 1 组帧(基本服务)发送将数据报加帧头帧尾封装到帧中 2 链路接入(广播链路需少) 播信道上地景整的帧 2 链路接入(广播链路需少) 播信道上地景整的帧 2 链路接入(广播链路需少) 播信道上地景整的帧 3 差错检测基本服务) 检测传输错误 4 差错到正有些提供,检测并纠正传输错误不使用重传)5 可靠交付部分协议)通过确认,重传等机制确保接收节点正确收到每一个帧停。等 GBN SR) 多用于高误码率链路6流量控制,可专发进度整免接收节点逐转给10分流量控制,不提供可靠交付的链路层协议,无需专门的流量控制不提供可靠交付的链路层协议,需要流量控制机制7 半双工和全双工半双工通信时提供收/皮转换有零实现。1 路由器线卡/2 注机生体在网络适配器/

线卡网络适配器连接物理媒体必头现初埋层的划能 网络**适配器**应间的<mark>通信发送侧</mark>数据报封装到帧中生成校验 比特(可选)执行可靠传输和流量控制;接收侧,提取帧,检测传 输错误(可选)执行可靠传输,流量控制,解封装,交给上层协议 <mark>检错和纠</mark>算

码多项式T: $T(x) = x^{n}M(x) + R(x)$ 生成多项式G(x):双方确定用来计算R(x)的-

共享链路,任一节点发送的数据可被链路上其它节点接收到 多址接入冲突广播链路,若两个或多个节点同时发送,信号会 发生干扰,导致接收失败。多址接入协议MAC(媒体接入控制): 规定节点共享信道(谁可以发送的方法 理想的多址接入协议,在速率为R bps的广播信道上1.只有一个节点发送,能以速率尽发达(信道利用率高)2.M个节点发达, 市场发达,即以PM的平均选率发送(公平性好,信道利用率高) 3.协议是无中心的(分散式),无需特殊节点来协调发送(健壮性) 无需时钟同步,任额外机制)4.简单,实现和运行开销小) (信道划分,为若十子信道,每个节点固定分配一个子 信道、不会发生冲突,关注公平性轻负载时信道利用率不高 (1)TDMA:对外多批,将信管,用时间划分成龄,每个节点,在帧

)MA允许所有节点同时使用整个信道! <mark>机接入</mark>(竞争):不划分信道,节点自行决定何时发送,出现冲

前未检测到冲突,可在下一个时隙及达新的测测。在12/2/32/17人 节点在随后每一个时隙中以概率P重传直至发送成功, 优点单个活跃节点可以信道速率连续送分散式,节点自行 决定什么时候发送,简单、缺点发生冲突的时隙被浪费,由于概 率重传,有些时隙被闲置,需要时钟同步 效率当网络中存在大量,记跃节点时、料运行过程中成功时 隙所占的比例,假设小个活跃节点每个节点在每个时隙开始 时以概率P发送,给定节点在一个时隙中发送成功的概率= p(1-p)N-1.给定时隙中有节点发送成功的概率=Np(1-p)N-1 最大效率(渐进);1/e=3/M。最佳情况仅3/M时间信道有效传输 (2.她ALOHA上无需时钟同步,任何节点有数据就可以立即发送、 深于听师后省到断太次传输是否成功,若不成功、立即以概率P

(2^k)-1}中选择t,延迟t512比特(最小以太帧长度)时间**:6.**回2. **指数回退目的**:根据网络负载调整重传时间:负载越重(冲突次

一物理网络时数据接可从A直接交付给BA的网络层将数据 报B的MAC地址交给数据链路层A的数据链路层接数据接 装在一个链路层帧中,帧的目的地址=B的MAC地址:B的适配 器收到帧根据目的MAC地址判断安给本机取出交给网络层 地址解析了UNPMAC/地址解析或ARPI用干动态获得IP地 址-MAC地址映射若节点A希望获得节点B的MAC地址:节点A

非获得B的MAC);A创建链路层帧,封装IP数据包,src dest MAC = R-1.发送来接收帧取出IP数据报发现目的地址 为BR利用ARP获得B的MAC地址:R创建链路层帧 封装IP数据 报src MAC=R-2 dest MAC = B.发送:B的网卡接收帧取出IP 数据报交给网络层. ARP与DNS的一个重要区别DNS为因特网中任何地方的主机 解析主机名ARP只为同一个子网的主机和路由器接口解析PL 以太网:第一个广泛应用的局域网技术目前占主导地位的有 线局域网技术技术简单成本低为提高速率不断演化和发展 总线拓扑共享式以太厚。线线1970;同轴电缆为共享传输媒 体(总线),所有节点通过特殊接口连到该总线上 集线器(1990)物理层中继器从一个端口进入物理信号(光电),放大后立即从其它端口端出集线器相等十类单电缆 星型拓扑·交换式以太网;交换机(21世纪);主机通过双绞线或 光纤连接到交换机;主机与交换机之间为全双工链路,交换机 在端口之间存储转发帧键路层设备) 个重要区别:DNS为因特网中任

在端口之间存储转发帧(链路层设备)

式以太网不会产生冲突,不需使用CSMA/CD协议! 拓扑。各节点仅与中心节点直接通信,之间不直接通信

各节点仅与中心节点直接通信之间不直接通信 hub的星型连接 g.Preamble(前导码):7个10101010字节,后跟一个 中节用于在发送方和接收方之间建立时钟同步不 旋的长度 Dest Address/SrAddress/E的/濒MAC地 守):指出Data所属的高层协议(PARP等):每个协议 pe(Z子サ)溶缸Data까應的局层까以(IPAKP等),每个阶个编号,Data46-1500字节不**足46填充至46字节**CRC 次对estaddr.srcaddr.type.data四字段计算得到的CRC研 接不可靠的数据传输.无连接发送方网卡与接收方网 没有握手.不可靠.接收方不发送确认,接收方网卡 C错误的帧,依靠上层协议(TCP或应用进行错误恢复 / 女者男.nkk.始更要。CRM/CPA供送法定在任金法法院

路层交换机。 链路层设备。存储、转发帧,检查输入帧MAC地 有选择地将帧转发到一个或多个输出链路,特点、透明(主机 觉不到交换机的存在),即插即用,自主学习(交换机无需配置

/加州內表不完合法自居何代赖辰。例始后公數塘蛙相居。1物理居 它相好了走郊移动內緒。1介留 移动埃滿改变网络接入点。然內格层带来很大问题 无线。在铁路通信始物理层和数据链路层带来很多问题 无线线端。laptop,PDA 手机运行网络应用。无线不一定移动 基站通常连接到固定网络,在无线终端和固定网络之间中级 数据包负责协调与之关联的多个无线生机的传输(20114P) 无线链路,连接无线线端和基础需要MAC协议协调无线链路, 的无线链路具有不同的数据速率和传输距离

同的无弦链路具有一向的数据逐率和付编股品,用就是其它 号源干扰多径传播反射使信号沿多条路径到达接收端 上特性导致无线链路的传输距离受限。误码率很高 厅模式1基础设施模式无线终端通过基站连接固定网络 络基础设施)传统网络服务由固定网络提供切换无线终 接入不同基站的过程之自组织模式没有基础,是

分类	单跳	多跳
有基础设	主机连接到基站连接到固	通过多个无线节点中继才能
施	定网络(wifi,cellular)	到达固定网络(无线网状网络)
无基础设	无基站,不连接到固定网络,	无基站,不连接到固定网络,节
施	节点通信无需中继(蓝牙网	点间通信需通过其它节点中
	络)	继(自组网,车载网)

10年表現一次 但在接收予点通信范围内的活跃节点(发送节点所不到)但影 响接收(2 暴霧节点问题:在发送节点通信范围内,不在接收节 点通信范围内的活跃节点(发送节点循f范围)不影响接收 CSMA在多跳无线网络中作用受限:载波侦听仅知道发送节点 SMA在多线无线网络中作用支限:氧液顶听及知道发达下局 周围是否有节点发送,但影响此次通信的是接收节点周围是

54M);802.11g(2.4-5G;54M)802.11n:多天线(2.4-5G,200M) C协议:CSMA/CA.支持基站模式和自组织模式,物理层不同

同域的朱物元线LAN基本组成半九定率本版分集包 BSS包括若干无线线编一个无线接入点AP 无线接口终端及AP)均有一个全局唯一的MAC地址 跨路由器连的有线端口不MAC地址LAP对路由器是近 与关联通信频段划分成若干信道每个BSS分配一个

信迫与天联,但信则段划分成名十信追率个BS分配一个信息 蔡AP时为AP分配一个服务集标识符(SID),选AP使用的信道 相邻AP的信道可能相互干扰。 主机必须与一个AP关联:1.扫描信道。监听各AP发送的信标制 (含AP的SSID MAC地址)2.选一个AP关联(可能需要身份鉴别) 使用DHCP获得AP所在于网中的一个P地址 被对扫描主机监听AP发送信标帧、主机选一个AP发送关联请 被数据和图像分类的原位。本书过程、中的一模探测语句

求帧:AP向主机发送关联响应帧<mark>主动扫描</mark>: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一个AP发 送关联请求:AP发送关联响应帧

议:CSMA发送前监听信道:不与正在进行的发送冲突

发送过程中不检测冲突(困难,隐藏节点);使用链路层确认;接收方收到帧后需发送确认帧; 目标避免冲突 CSMA/CA操作模式,PCF模式(可选);只用于有基础设施(基站)无线网络,

操作模式PCL模式(可选),只用于有叠磁设施展型,尤线网络自动的节点可以发送帧不会冲突。20CF模式有/无基础设施均同到的节点可以发送帧不会冲突。20CF模式有/无基础设施均可所有。20人和无线终端,使用CSMA/CA协议竞争信道支持两种机制/信道预约/机制(可选),无信道预约的机制(必须)信道预约/向AP发送KTS帧给出施后要发送的数据帧及ACK帧需要的总时间。AP收到DEZCTS帧,给出施后要发送的数据帧及ACK帧等等的总时间。AP收到DEZCTS帧,发送数据帧。AP收到FS发送一个ACK帧进行输入。PV图TSME、发送数据帧。AP收到ES发送一个ACK帧进行输入。PV图TSME、APKSP影长了CTSME、ADMENSME、APKSP影长可以

A收到CTS帧次送数据帧AP收到后发送一个ACK帧进行输入 收到RTS帧(A附近)CTS帧(AP附近)的节点均沉默指定的时间 让出信道让A和AP完成发送活合AE同时发送TS不成功的随 机等待时间重试发送数据较少时,般不使用信道预约机制 帧间距机制分许DCFPC产在一个单元内共存。 SIFS处于会话中的节点优先发送如收到RTS的节点发送CTS, 收到数据帧的节点允许发送一个ACK帧 PIS-若SIFS后节点有发送一个ACK帧 DIS-若PIS后没有基站发送任何节点可以竞争信道 EIS-若以上间隔都没有发送收坏帧或未知帧的节点可以发 送一个错误报告帧

EIFS若以上间隔都没有发送,收环帧或未知帧的节点可以发送一个错误报告帧 无信道预约。当节点要发送时,使听信道 1 若一开始惊听到信道空闲时递减该值,此过程中若像听到信道它,所引信道空闲时递减该值,此过程中若像听到信道忙,永5倍计数值 3.计数值减为0时发送整个帧等待确认,4.若收到确认帧,表明 发送成功,若还有新的帧要发送,从第2步开始CSMAC表表 收到确认重复字中间器阶段从更大范围内选取随村回退值 关着公本选生资经验。详整和选取的温度,每3字卷头选师客

A中侦听到信道空闲随机回退(冲突对网络损害大 格式:Add1目的MAC|Add2:源MAC|Add3:连接AP的路由器 接口MACIAdd4:只在自组织模式中使用 2 2 6 6 6 2 f 6 0 - 2312

寻址举例,AP仅对无线终端可见,对固定网络上的设备不 AP连接路由器的有线端口没有MAC地址! H1主机想通过AP向网络上发送到路由器R1:

71土70/85通过247间份组工及达到附出商标1. 经<mark>端准子网内移动</mark>终端从一个BSS移动到另一个BSS 发生切 按时 终端要关联到新的AD上当11枪迎到来自AP2 信号逐 渐减弱时,开始扫描新的信标帧,当H1收到来自AP2 信号更强 的信标帧时,先解与AP1的关键、然后关联到AP2 发生切换时交换机中的转发表也需要新交换机通过自主 学习更新转发表交换机收到H1(源主机)发送的帧时,更新H1 所存的端口美转发表表次和时垂新可能产生丢包

移如P.私注加冷如P.私还加冷如中。 动节点通过外地代理向归属代理注册归属代理注册多称动 点的外地地址最终结果外地代理知道移动节点在本地网络 上归属代理知道移动节点的转交地址记录到地址绑定表 间接选路到移动节点通信者在数据包中使用移动节点的永

间接选路到移动节点.迪信者在数据包甲使用移动节点的水 丸地址归属代理截获数据包、转发给外地代理移动节点直接 将响应发送给通信者 三角选路通信者-归属网络-移动节点 当通信者和移动节点 在同一个网络中时很低效 间接选路终端在外地网络间移动假设节点移动到另一个同 经企业的发现地位现代现在的

络向新的外地代理注册新的外地代理使用新的转交地址 信息新移动节点的转交地址,归属代理使用新的转交地址 向移动节点转发包。"节点移动及变换外地网络等对通信者都 是透明的正在进行的通信可以保持!

向移动节点转发包。节点移动及变换外地网络等对通信者都是透明的正在进行的通信可以保持! 直接选路到移动节点通信者向归属代理请求并获知移动节点点信者向归属代理请求并获知移动节点通信者向归属代理请求并获知移动节点点转交地址促进以后不必再做)通信者将包发送给外地代理、需要知道移动节点的转交地址通信者(包括固定节点)需要增加对移动通信的支持。Mobile IP移动IP支持移动性的因特网体系结构与协议具有许多我们已经看到的特性归属代理外地代理永少地址转交地址移动节点注册标准化三部分。(1)代理发现2.1愿意充当归属代理或外地代理的路由器定期在网络上爱观主度近代理通传。宣布自己的存在及P地址2.愿意充当

(1)代理发現:原意充当归属代理或外地代理的路由器定期 在网路上安泛代理通告宣布自己的存在及P地址;2.愿意充当 外地代理的路由器在代理通告中会提供一个或多个转交地址 (通常使用自己的IP地址作为转交地址)3.移动节点通过接收 和分析代理通告判断自己是否处于外地网络以及是否切换 的转交地址中选择一个作为自己的转空地址 (2)移动主机注册1移动节点向外地代理发送一个注册请求 经验出自己的京久地址转交地址,归属代理地以及认证证信息 等之外地代理记录相关信息向归属代理转发注册深3.3四 接交地址注册指求,若认证通过将移动节点的永久地址及 展代理处理注册请求,若认证通过将移动节点的永久地址及 时交地址是证册请求,若认证通过将移动节点的永久地址及 到有效的注册响应后,将移动节点记录在自己的转发表中向 即有效的注册响应后,将移动节点记录在自己的转发表中向 移动节点转发注册响应5.当移动节点回到归属网络时,要向 即属代理注语,即响应5.当移动节点

PJ属代理注销。 (3)数据报间接选路1数据包首先被归属代理得到2.归属代理管查地址绑定表。获得移动节点当前转交地址3.归属代理代数据包发送到转交地址4.外地代理将数据包转发给移动节点 归属代理如何得到数据报?1.若诵信者不在归属网络上:数据 交地址?归属代理收到的数据报,目的地址为移动节点的永久 地址,而移动节点的转交地址位于外地网络,**如何将目的地址** 的包:SrcIP=归属代理IP,DstIP=转交地址,里面封装着通信者发送的包(这个包的dest是永久地址);外地代理向移动节点发送的包:通信者发送的原始包:外地代理如何转发数据包到移

地代理如何获得移动节点的MAC地址/在移动节点注册阶段外地代理获知了移动节点的外久地址和MAC地址、记录在其转发表中外地代理根据目的P地址查找转发表得到移动节点的MAC地址,外地代理利用移动节点的MAC地址,将数据报封数1转原域中发送整移动节点第分式的变发送数据包发送给外地代理(被省路由器)SroP-移动节点外域上DesIP—通信者IP地址/SrOMAC—移动行场MAC人estMAC—多小地代理MAC外地代理按照正常方式转发数据包移动节点如何得如外地代理的MAC地址// 代理通信教育的MAC从证据、外域代理的MAC是外地代理的MAC类的地代理的MAC地址// 代理通信教育的海风/是外地代理的MAC、地位/图像的基础 报义的源MAC是外地代建的地址 无线和移动对上层砂块的 影响。无线链带来的问题误码率高、毛包率高,连迟增大 点移动带来的问题。丢包、延迟增大逻辑上,没什么影响为上 层协议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,传输至迟增 大,TCP将丢包(长延迟也当作丢包)解释为拥塞,不必要地减小 拥塞窗口,导致应用吞吐率很低,无线链路、有线/无线混合链 这上位TCP用等。按归 路上的TCP拥塞控制是一个研究问题.

GAAP 安全 网络安全 网络系统硬件 软件,系统数据受保护,不受偶然或恶 意原因被破坏更改 泄露,系统连续可靠运行,网络服务不中断 通信安全 机密性 报文内容(仅发送接收)/通活活特不被察觉 编集鉴别双方都能够证实另一方报文章整性报文自真实来 源传输中未被修改运行安全性网络系统运行正常服务可用

0≤M < n;计算C = M^e (mod n)为M的密文;解密:M=C^c (mod n),为要求的明文.用途:加密少量数据(鉴别,数字签名,发

(mod n) 为要求的明文 用途加密少量数据鉴别数字签名发送一次性会话密钥优点 安全性好基于大数分解,使用方便之于传递密射缺点;计算干绢大速度慢 报文完整性报文鉴别。验证报文可信来自声称的源,未被修改 有用报文加密发送方和接收方用共享的等。如此报文管,不是一个人员的影片用在报文上,是一个人员的影片用在报文上,是一个人员的影片用在报文上,是一个人员的影片用在报文上,是一个人员的影片用在报文中,一个人员的影片用在报文中,一个人员的影片用在报文中,一个人员的影片用在报文中,一个人员的影片,一个人员的影片,一个人员的影片,一个人员的影响,一个人员的影响,一个人员的影响,一个人员们是一个人。

(S/MIME基于公钥加密工业标准,商业组织机构) 服务鉴别机密性压缩,兼容电子邮件,分段 鉴别用基于公开密钥算法的数字签名提供鉴别服务 生成可供鉴别的电子邮件,发送方创建电子邮件(报文);用 SHA-1;计算报文摘要用发送者私钥加密形成数字签名附在报 空邮面 Fiav — # 安治学(Son II Data

SHA-1计算报文摘要用发送者私销加密形成数字签名附在报文前面与报文一起发送:Sopil Data 机密性对称密钥算法发送方外生成报文和随机128比特数/一次性会话密钥别用经话密钥加密报文,再用接收方B公钥加密设定的与场景之一起发送:Mb+(Ka-b)||Ka-b(Data)|加密的压缩1减少要加密的数据显之源之消息完全增加密码分析困难兼容电子邮件Base64编码(二进制数据流转换成ASCII文本)可以配置为仅对报文中某些部分进行编码转换 新用 Encodeasses4(Ki (Ka-B)||Ka-[Cip(Sgn]|Data)))) 邮件分股服务许多邮件最大报文长度不超过50,000字节

安全服务机间整了17亿的网络应价提供安主的17辆运版多 安全服务机够性数据完整性服务器整别客户鉴别可选) SSI建立在TCP上依靠TCP提供可靠端到端连接涉及2个层分 的一组协议1.SSL记录协议,为各种高层协议仅加HTP提供基 本的安全服务(机密性,完整性)其它3个高层协议.SSL交换管理

SSI握手协议,允许服务器客户相互鉴别协商加密算法MAC 算法及密钥由一系列报文交换组成。 能力协商:浏览器间服务器发送建立SSL会话的请求报文说明可支持的SSL协议最高版本、支持的加密算法(按优先级从高

到低利压缩方法等和浏览器选择的一个随机数RC 2服务器从浏览器给出选择中确定合适的SSL版本号,加密算法压缩方法与服务器选择的随机数Rs—起发送给浏览器 服务器鉴别1服务器的浏览器发送上40销证书(和少要的证书链,及其它信息2浏览器检查签发证书CA是否在其可信CA 列表中不在警告岩在则用该CA公钥验证得到账务器的公组数据整整别可选收到服务器容器证书请求则发送其公钥证书。生成密钥1测览器生成一个44字节随机数 称预密钥,用服务器公钥加密后发给服务器2案户服务器各自从预密钥,用服务部公销加密后发给服务器2案户服务器各自从预密钥,用服务器公销加密后发给服务器2、其例AC需要的密钥,以则MAC需要的密钥,以则MAC需要的密钥,是属于浏览器向服务器发送所有提手报文(级联的MAC

于PD9数据外汇(应)数据外压编码 實的报文室列码4用对称密钥算法对压缩的数据块及报文 鉴别码加密(DES,3DES,IDEA,RC等)5.在处理完的数据块前加 LSSL头,包括内容类型、SSL版本号、压缩数据块的长度等

3成设在,例常性等,IPSC 的安全机制效立于算法。因此在选择 成设击,例常性等,IPSC 的安全机制效立于算法。因此在选择 法时不会脚填上它部分的实现。IPSC 提供多种安全控制程度 ITCP 连接上的通信,对其时间的通信,对对全间关心间的所 用户可以为数据通信选择合适的安全服务、算法、协议和控制 术上设 IPSC 基理包括两个部分 cc安全协议。包括AH(不提供机密性)和ESP两个安全协议。定义了

安全通信的IP扩展头和字段 以提供机密性 的操作模式、使用的密码算法、密钥及密钥的生存期等 SA是两个通信 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SASPI携带在数据包中,由数据包

使, 两种模式的比较。传输模式比隧道模式占用较少的带宽,隧道贮隐藏内部网络的细节(原始IP头不可见); 内部网络上的主机 全 隐藏风部网络的细节(原始P)头不可见); 内部网络上的主机可以不运 作门PSc。它们的安全性由安全两类来保证; 能達摸式可以将一对端点间 的通信聚合成一个加密流从而有效地防止入侵者进行流量分析 **鉴别炎** 统/Authentication Header/放安SP1:32比特的数 和目的IP地址、安全协 设结合起来唯一标识极振振的SA、SeqNum对SA上发达的数据包进行 编号,供接收端检测重放攻击一个SA上的序号不能重用见此在传输的数 提包数量达到323之 前,必须协高一个新的SA和新的密钥; Authentication Data:包含指文鉴别局的可要长度域,所名和实现必须支 \$\text{blue}\text{change} Authentication Data:9含指又鉴别码的可变长度或所有科实现必 持HMAC-MDS-96和HMAC-SHA-1-96.AH/放建解先连接完整性 据起源认证和抗重放效击。但不提供机密性服务HMAC覆盖敷据包 荷部分因而可提供还建提完整性服务,HMAC覆盖原始中头中的不 (特翰模式)或整作原始中头保链模式)因而可提收据起源以 中有序号。且被HMAC覆盖。因而可抵抗重放攻击。對赛安全

全性强于AHLEPP传籍模式的鉴别服务,安全性不如AH 28.02.11 WEPWired Equivalent Privacy 存转教教保密,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。802.11版本,提供较强的加 主机向AP请求鉴别。AP向主机发送一个128比特的不重数,主机使用与 AP共享的对称密钥加密不重数,发达给AP、AP解密不重数, 主机使用与 主机的不重数相同。完成主机鉴别,利用主机与基础共享密钥这个等实鉴 别主机 WEP数据加密之机鉴别,利用主机与基础共享密钥这个等实鉴 别主机 WEP数据加密之机等别和发生一个40比特的对称密钥KS(学教及) 对于每个地域学技术也一个2014 统动和检查则以添加图以后面形成 寸于每个帧,发送方生成一个24比特的初始向量IV,添加到KS后面,形成 34 ···); Trudy能够获得Alice加密的密文: ci = di XOR kiIV; Trudy知道c 和di, 就可以计算出kiIV: di XOR ci = kiIV; Trudy得到了加密所用的密钥 流 k1IV k2IV k3IV·····; 当过后观察到IV被重用时,Trudy就可以破解密文 《可附廷接人品差本是起中强的作用任各户和鉴别服务者之间转改整人及 成**对主密银**(Parwisse Master Key, PMK) 生成, MK是一个仅为余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(PMM) 鉴别服务器则向AP发送该产MK等户和AP 现在具有一个共享的 密钥, 4的解析器们任何的对目 Key, TK) 生成, 使用PMK, 无线套产和AP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 特被用 于执行经无线镍路向任意远程主机发法数据的链路级的加密 形**沙楼** 可信, 如然回答。

學型包述的大場、状态性別的大場、应用內容 包述的大場、大态性別的大場、应用內容 包述的大場。由醫对数据包逐包过滤、基于(源P,目的IP TCP/UDP源端口号,目的端口号,ICMP报文类型,TCP SYN标志

讨滤规则 不允许外部发起的TCP连接,除非访问 丢弃进入的TCP SYN包,除非去往 的是内网的公共web服务器 130.207.244.203的端口80

局限性:处理开销大,速度慢,每个应用都需要一个应用网关 IDS:深度数据包检查::查看包内容(如检查包中是否包含已知 向过滤仅检查**传输层和网络层协议头**|应用网关仅检查特定

应用的数据包|不检查数据包的内容及数据包之间的关联

网络作为链路层 在物理网络上增加一个逻辑层次(IP层),在逻辑层上统一编址 包格式,互联在一起的网络看起来像一个网络用网关连接不同的物理网络.在逻辑层上选路到下一个网关,将IP包封装在本地网络帧中发到下一个网关Cerf&kshtnlernetArchitecture,两级维址上网络物理网络:IP层提供统一网络视图.地址,包格式,底层可是任意物理网络,物理网络对于IP层不可见,只是一条虚拟链路.