**CHAP4 网络层中的数据面 -1介绍**

1.网络层为传输层提供**主机到主机**的通信服务

2.每一台主机和路由器都运行网络层协议

3.**发送终端**:将传输层报文段封装到网络层分组中,发送给边缘路由器;**路由器**:将分组从输入链路转发到输出链路;

**接收终端**: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)

5.**数据面:执行**数据传输的功能(路由器**本地**功能)

**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**数据传输的功能(**网络范围**的功能)逻辑集中,独立

**选路**是控制面功能,确定分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~)

7.**网络服务模型**: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可能不同

\*同一个网络也可以提供不同的网络层服务

-2**数据报网络**(提供网络层**无连接**服务)**虚电路**(**面向连接**)

\*一个网络**不能同时**提供无连接服务和面向连接的服务(核心)

\*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**(网络层)一条**端到端路径**:传输分组前建立虚电路,传输结束拆除;所有分组在这条虚电路上传输(**保序**).将路由器资源(带宽,缓存)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)**

3.**实现**:从源主机到目的主机的端到端路径**+**途经每条链路时的虚电路号(用于区分经过该链路的不同虚电路,仅有本地意义)**+**沿途每个路由器中的转发表项(入端口+入VC/出同理)

4.**过程:**分组**只需携带VC号**,**不带目的地址**.路由器利用**输入端口和VC号**查找转发表.转发前用输出链路上的VC号替换

5.**信令协议**: 交换信令报文(用于建立维护拆除虚电路)

6.**数据报网络:**分组携带**目的主机地址**,路由器按目的地址转发分组;路由器中转发表记录**目的地址-输出端口**的映射

转发表被选路模块修改(1~5min更新1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**重排序**

**7.比较:**Internet(**数据报**):为计算机通信而设计;早期的网络应用-弹性应用;用户免费使用网络;终端具有智能,可将复杂的工作(如差错控制)推到网络边缘,保持网络核心简单.

ATM(**虚电路网络**)电信网发展而来;注重用户体验;终端无智能或很少智能;复杂工作由网络完成,以保持终端简单.

数据报网络提供**最小服务**:可运行在各种链路上;为传输层服务的设计增加了灵活性,可简可繁;符合当初**因特网设计的原则**:网络只提供尽力而为的服务;复杂的工作推到网络边缘

-3**路由器:**1.**功能**:**选路:**运行选路协议,计算转发表;(软件ms)

**转发**:依据转发表,从输入链路到输出链路转发数据报(硬件ns)

2.**输入端口**功能:**物理层**(比特流接收);**链路层**(提取处理帧,提取IP数据报);**网络层**(集中交换: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**:路由器中的互联网络,用于在输入端口,输出~,选路处理器之间转运分组;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**)**

①通过**内存交换:**

**传统:**CPU直控制下,数据包拷贝到系统内存中进行交换.交换速率受限于内存带宽:每个数据包**穿过系统总线2次**

**现代**:每端口使用一内存接口硬件连接到存储系统,一控制器硬件在端口间传输消息,**无需CPU**.输入端口将一包放入内存后,接口硬件通过控制器向输出端口发送一个消息,输出端口从内存指定位置读取包,发回响应消息

②通过**总线交换:**1共享总线从输入端口缓存转到输出~

**总线竞争**:防止多端口同时传输(例时分多路复用),各输入端口在总线上轮流广播分组,每输出端口据分组携带的内部标签接收发给本端口的分组.交换速率**受限于总线带宽**

③通过**互联网络交换**:(阻塞型与非阻塞型)

交换结构控制器通过控制交叉点开闭,建立内部**专用电路**.

多对端口间可以**并行传输**(adv:划分成若干固定长度的信元)

4.**输出端口**功能: 物理层处理:将比特流转换成物理信号

链路层处理:执行链路层协议,封装

网络层处理:组装(需要时,输出的信元组装成分组)排队(输出端口来不及发送,在此排队)调度(每次选择一个分组发)

**排队与丢包**:①**输入端口:**交换结构不能及时将输入端口的分组转移到输出端口;问题：**队头阻塞**:队头阻塞其后分组的转发;**丢包**:输入溢出;解决:交换结构速率/入端口速率至少n(输入端口数)②**输出端口**:多输入端口同时向一输出端口发送

**不可避免**的,设置**输出队列长度**:增大输出队列:减少丢包,增加内存消耗,增大分组延迟,导致重传;**输出队列并不是越长越好**.

5.**调度策略:**输出端口选择下一个发送的分组

**分组丢弃策略**:①弃尾:丢弃到来的分组②按照优先级丢弃③随机丢弃:如RED(主动队列管理-满前丢弃)

**随机早检测**(RED):路由器在每个端口上记录输出队列平均长度:AvLen=(1-Weight)×AvLen+ Weight×SampleLen

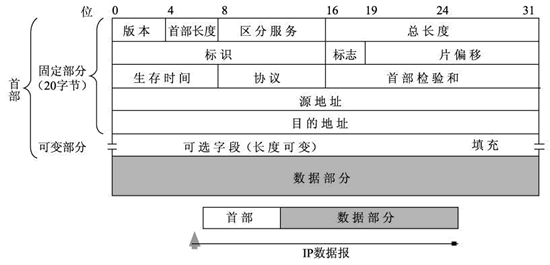
AvLen达第一阈值,按概率p丢弃到来的分组,3ACK,1/2v

AvLen达第二阈值,丢弃每一个到达的分组,超时,v最低

p是AvLen和上一次丢弃距当前时间的函数(均正相关)

**先来先服务|优先级调度|非抢占式优先级排队**:开始传输后不能被中断**|轮询调度**:队列之间轮流提供服务,每次选择一个队头分组**|加权公平排队**:按每队列带宽权重,发送一定数量分组

-3**InternetProtocal**将数据报交付到目的地址和目的协议

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字节**

**数据报格式**:ver协议版本16bitidentiifier,flgs,**fragmentoffset(8字节)**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,

**IP分片与重组:**链路层帧能承载的最大数据字节数:**MTU(不定）**

以太网帧(max1500字节)部分广域网帧（576B）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**

分片报头取自原始报头,**标识**(每分片与原始数据报相同标识)**偏移量**(数据在原始数据报载荷中位置)**标志位**(MF最后一个0其余1;DF=1不允许分片)**分片修改**:**总长度**＝H+数据块长度;最后报头**MF**位置0,其余MF位置1;**偏移量**:第一个为0;数据块在原始报载荷中的**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≦MTU;偏移量13bit;除了最后分片,数据长度应**8字节整倍数**,分片的数据长度 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IP,标识>**确定属于同一数据报的分片;2.利用**最后分片**算原始长度:**原始长度**=偏移量×8+分片总长度;**原始数据报载荷**=原始长度–报头长度3.组装:各分片中数据块按其在原始数据报载荷中偏移量重组

**分片的坏处**:1.降低路由器吞吐量;消耗目的主机资源2.针对分片dos;3.IPv6取消路由器分片:源主机发送探测报文确定路径最小MTU,构造数据报≤MTU;路由器丢弃过大的,发错误报告.

**IP编址**:每**网络接口**(**主机[一个/两个]/路由器[多个]**与物理链路的边界)对应一个IP地址(**32位**的二进制数),用**点分十进制**

**基于类编址:单播地址结构**:**类别标识**|**网络号**(标识**物理网络**,ICANN分配)|**主机号**(标识一个**网络接口**,网络管理员分配)

**特殊:**网络号有效,主机号全0/全1的地址:网络本身/定向广播

32位全1:本地广播地址,仅在发送节点所在网络广播(仅目的)

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,发送到这个地址的分组不输出到线路上,而是送回内部的接收端.

(接口,地址)A类(^24-2, ^7-2)B类(^16-2,^14-2)C(^8-2,21-2)

**子网**:具有同子网地址,**无需路由器即可相互到达**的网络接口

**主机号=子网号+主机号**,子网号表示一个子网. **“孤岛法”**

**子网掩码**:指示IP地址中子网号(1)与主机号(0)的边界, **“与运算”**

**子网地址≠子网号**,子网地址-子网掩码中“1”的部分

**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**:节点转发给一个路由器处理;目的地址不与任一端口在同一子网;节点查找**转发表**,将数据包发给下一个路由器

**转发表:**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**子网地址**:地址前缀表项;**特定网络接口地址**:特定主机表项;**缺省项**:不匹配其它表项都映射到默认路由器端口

**IP采用逐跳选路:**转发表项只记录下一跳信息;**转发表项**包括:目的地址/掩码,下一跳(路由接口)地址,输出端口

**下一跳地址须与输出端口在同一子网**(无需通过其它路由器)**转发过程**:提取目的IP地址D,根据地址类别得到网络地址N;1.D与**自己任一IP匹配**,将数据包交给protocol指定协议实体

2.N与自己的任何一个**直连网络的地址匹配** //直接交付

3.表中包**含到D的特定主机表项**//间接交付,发到下一跳

4.表中包含到N的一个**地址前缀表项**//间接交付, 发到下一跳

5.包含一个**缺省项**//间接交付,发到指定的默认路由器端口

6.宣告选路出错,向源地址发送一条**错误报告**消息(ICMP)

**CIDR**:按照**实际需要**的地址数量分配,提高地址使用效率

允许将若干条转发表项进行**聚合**,减小转发表规模

1.地址块长度L是2的幂次;2.所有地址前(32-logL)位必须相同

3.可以用**掩码或者’/长度’**来表示子网地址的长度

**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:200.23.16.0/20;同时给出不能被聚合的表项:200.23.18.0/23

**最长前缀匹配**:所有匹配的路由表项中,选择前缀最长的表项

**分类地址转发表:**根据目的地址类型确定要查找的转发表(A,B,C),提取网络地址,相应转发表中进行哈希查找(精确匹配)

**CIDR好**:1.按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;**坏**:1.地址前缀长度可为任意值2.Prefixlen无法从地址本身得到,只能从转发表项得到3.必须选择前缀最长的表项

**获得IP地址**:**路由器**:管理员手工配置各个接口的IP地址

**主机**:1.管理员手工配置主机IP(通常服务器)2.**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(通常个人终端),免去手工配置麻烦(即插即用),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”响应:给出推荐的IP地址及租期,(及第一跳路由器IP(缺省网关,边缘路由器),本地DNS的IP,地址掩码)

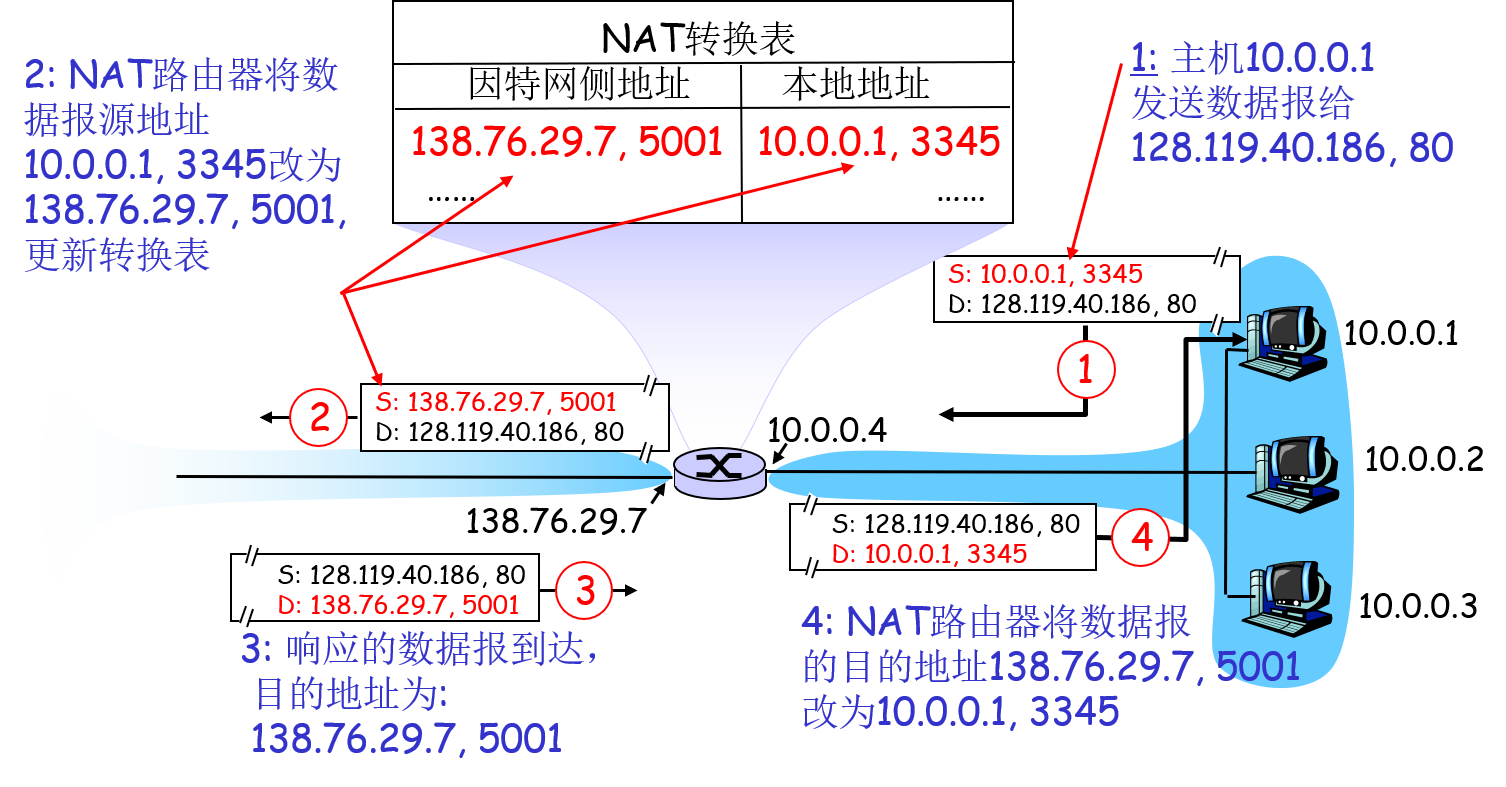
**主机**“DHCP request”:选择一个DHCP服务器,向其请求IP地址

**服务器**“DHCP ack”:响应客户的请求,确认所要求的参数

\*DHCP**服务器**使用**UDP**端口67,客户使用UDP端口68

**报文传输**:DHCP请求被封装到**UDP/IP/以太帧**中并广播.

**网络地址转换(NAT)**

**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(**减公用IP数**)3.内部节点对外不可见(**安全**)

**实现:外出**:(源IP,源端口)→(NATIP,NAT端口);**NAT转换表**:记录(源IP,源端口)和(NATIP,NAT端口)关系;**进入**:目的→对应

**16比特端口号**:允许一个NATIP同时支持65535个对外连接

**争议**:1.路由器应只处理**三层以下**的头(端口号在传输层)2.违反**端到端原则**（节点介入修改IP地址和端口号)

**妨碍P2P**:只允许内部主动发起通信(NAT后主机对外不可见)

NAT穿越问题:1.使用**UPnP**实现NAT穿越:假设主机10.0.0.1在端口3345上运行一个BT程序:请求NAT产生一个洞,将 <10.0.0.1,3345>映射到<138.76.29.7, 5001>上.BT程序向追踪器通告它在<138.76.29.7, 5001>上可用,其它主机通过追踪器可以看到该主机,并能向<138.76.29.7, 5001>发起TCP连接

NAT将<138.76.29.7,5001>收到的SYN包转发给主机10.0.0.1

2.使用**中继服务器**(Skype)

**IPv6**: **IPv6与IPv4不兼容**,但与其它所有因特网协议都兼容

**目的:**IPv4即将耗尽;改进不足:简化头部,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

**128位,8组,2B/组。例子**8000:0:0:0:0123:4567:89AB:CDEF

**零压缩技术**:连续0压缩一对冒号8000**::**0123:4567:89AB:CDEF

**三种地址**:**单播地址**:一个特定网络接口;**多播地址**:一组网络接口;**任播地址**:一组网络接口中任意一个(通常是最近的一个)

**IPv6数据报**:40字节基本头开始,后跟零或多个扩展头,+数据

**1.PRI**:**发送方定义优先级**;IPv6将网络流量分为两类:1.受拥塞控制的流:非实时流,优先级0～7; 2.不受拥塞控制:实时,8～15

**2.流标签**(flow label):标明属于同一个流的数据报;便于分类.

**流**:有相同传输特性,要求相同处理一系列数据包;发送方分配,<源地址,流标签>唯一标识一个流;路由器有流表

**3.对比**:删掉(**IHL:**基本头总是40字节;**不分片**;**无头检验**)增加(流标签)改变(Type of Service改为TrafficClass(PRI);总长度改为**载荷长度**;Protocol改为**Nextheader**,允许任意扩展,拓展头)

VER,PRI,FlowLable,PayloadLength,Nextheader,Hoplimit,SA,DA

**过渡**:**1.IPv4/IPv6双协议栈**:支持IPv6主机和路由器同时运行IPv4和IPv6,双栈源节点查询目的DNS:若IPv4,发IPv4分组,反之亦然;双栈节点同时有IPv4,IPv6地址;**2.建立隧道**:边界路由器将IPv6包封装到IPv4包中,送入IPv4网络,目的边界路由器取出IPv6包继续传输;本质是封装数据包;**IPv6包在IPv4网络中传输时,未被IPv4路由器检查处理,报头TTL未减1;S:B D:E**

在路由器E的IPv6看来,IPv6包是从路由器B直接到来的

**CHAP5网络层中的控制面 -1介绍**

两种建立控制面的方法:per-router control (traditional)

logically centralized control (software defined networking)

**-2选路问题:**路径长度,数据速率,分组延迟,通信费用,安全性

ISP:网络吞吐量最大,平均包延迟最小,平均通信费用最低,网络负载均衡,路由稳定健壮.**路由评价指标通常矛盾,需折衷**

**链路状态LS算法**:**全局**算法,**Dijsktra,选定源点**

发现邻居(链路直接相连);探测链路代价:探测到邻居的代价

构造链路状态分组(邻居及链路代价信息)扩散LS分组:向所有节点发送LS分组;计算路由:用LS分组构造网络拓扑,计算路由

**距离矢量(DV)算法**:

Bellman-Ford方程:,z为下一跳

**过程**:1.节点x测量到各邻居的代价c(x,y)2.x估计到各可达节点的最小路径构成距离矢量Dx;3.每节点周期性发送Dx给邻居

4.节点接收邻居距离矢量,利用B-F方程更新自己的距离矢量.

**特点**:1.迭代,异步,分布. 2.**好消息传得快**

3.**坏消息传得慢**:利用**毒性逆转**:若Z选择经由Y到达X,则Z向Y通告距离向量时将Dz(x)设为无穷大,即阻止Y使用这条路由

**DV和LS比较**:**LS**:链路状态信息在全网传播;O(|N||E|)个报文发送;计算复杂度O(^2);节点仅传播可靠的信息,错误不扩散

**DV**:距离矢量仅发送给邻居,收敛速度差异大,可能出现路由环路;邻居的Dx可能不正确;可能造成错误扩散

**intra-AS(IGP,RIP,OSPF,EIGRP)**将路由器组织到一系列自治系统(AS,由同管理域下网络和路由器组成的集合)中,称为域.

**域内选路**:AS内部进行,同一AS运行相同的协议;**域间选路**:网关路由器(一个AS内部直接连到其他AS的)之间运行相同协议

\*选路协议=选路算法+代价定义,报文格式,传输处理,异常等

**RIP**:一般由较低层ISP和企业网使用;用DV;

距离:跳数(相邻路由器之间的链路为一跳);限定最长距离15跳

路径跳数:从源路由器到目的子网(含)经过的子网数量

**RIP通告**:距离向量(路由器到AS各子网最短路径跳数估计值),封装在RIP响应报文中传输,每报文最多携带25个子网及距离.

RIP是应用层协议,用UDP端口520,相邻路由器约30s交换一次

**接收方**:1.对RIP响应报文中通告的每个目的网络,**跳数加1**

2.对通告的每个目的网络:①目的网络不在选路表中(新子网):

添加到选路表中;②目的网络在选路表中:若目的网络在选路表中下一跳为该邻居,用通告的表项替换选路表中的表项

否则,若通告跳数小于选路表中的跳数,更换选路表中的表项

**链路失效**:超180s未收到某邻居RIP通告,认为不可达:

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)

链路代价:由管理员配置(反映了管理员的选路策略)

定义了5种分组类型,分别用于探测邻居、通告链路状态等

OSPF分组被封装在**IP包**中传输,协议号89

OSPF协议负责链路通告分组在网络中的广播及可靠传输

**特点:**安全:所有OSPF报文需鉴别|允许多条路由代价相同 (RIP仅一条)可按比例分配流量|支持单播多播选路|可用分层

**分层选路**:AS配置成多个区域,每区域运行自己OSPF协议;内部链路状态仅区域内广播;区域边界路由器负责区域间的选路

**特殊区域:主干**,所有区域须连主干;每区域有区域标识,主干:0

区域边界路由器:连本地区域和主干的路由器;主干路由器:可以同时是区域边界路由器;内部路由器:AS内部非区域边界~

**两个选路层次**:本地区域,主干;每区域(含主干)运行自己的OSPF协议;**区域边界路由器**:本区域选路信息汇总,通告其它区域,接收其它区域选路信息通告给本区域的内部路由器

**跨区域分组转发**:先被发给本地区域边界路由器,在主干上转发到目的区域边界路由器,再转发到目的子网

**Inter-AS**: **BGP**哪些目的网络可达；可达信息传播内部所有

**热土豆协议:**选择intraAS中最近的网关路由器.

转发表由intra(到AS内部网络)和inter(到外部网络)配置:

**困难**:因特网规模极庞大,结构复杂|每AS可运行自己内部路由协议,使用自己测度确定到目的网络的最佳路由,不同网络判断标准不同|一个AS可能不信任来自某个AS的信息|一个AS可能不愿意为其它AS转发|AS间选路试**图找到能够到达目的网络的路由**,但**不试图(也不可能)找到最佳路由**

**BGP提供**:每个AS可从邻居获得到各个子网的可达性信息

可以将其它网络的可达性信息传播到所有的内部路由器

可以基于可达性信息和策略确定到其它网络的“好”路由

**BGP对等方**:一对AS同意交换选路信息,每个AS指定一个接近AS边缘的路由器或主机,用BGP协议交换选路信息.运行BGP协议的边界路由器或主机称为BGPspeaker;一对BGPspeaker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会话两个端点互为BGP对等方

**BGP会话**:**外部**BGP(eBGP):不同AS边界路由器间建立的会话.

**内部**BGP(iBGP):一个AS可能有多个边界路由器,之间必须通过半永久TCP连接构成全连通,它们之间的BGP会话

**路径广告**:BGP会话最重要内容是**可达性信息**:以AS枚举形式通告的,到达目的网络前缀的完全路径(便于检测路径环路)

**基于策略的路由**:1.入境过滤:根据输入策略,每条新的路由进行入境过滤,可能丢弃,按原样接受,接受但修改属性(如偏好度)

2.路径选择:对每一个目的前缀,从所有可达的路径中按照BGP指定的决策顺序确定一条最佳路由

3.出境过滤:根据输出策略决定是否向邻居AS发布某条路径

**比较**:IntraAS:用于在AS内部交换选路信息

使用某个路由测度(代价)选择到目的节点的最优路径

InterAS:用于在不同的AS之间交换选路信息

主要依据策略而非路由测度寻找可达路径(不追求最佳路径)

**广播选路**:将数据包从源节点发送到所有其它节点

1.用N次**单播实现**(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

需其它机制支持:源节点需知道所有目的节点的地址

2.**理想的广播选路**: **网络中产生的分组拷贝最少**

源节点不需知其它节点的地址,只需将分组目的地址设为广播地址,路由器负责转发到全网(在网络中复制分组)

**受控洪泛**:每个路由器仅转发它之前未转发过的广播分组

**记录已发送过的分组ID**:OSPF使用(源地址+分组ID识别)

**反向路径转发**:用节点内部的单播转发表,仅转发从本节点到源节点最短路径的反向路径上到来的广播分组(使用最多)

无额外状态和开销,路由器对每个分组扩散一次,有冗余传输

**生成树方法**:路由器知道哪几个端口在生成树上;当从一个端口收到广播分组后,只在属于生成树的其它端口上转发

无冗余的分组拷贝,只在生成树上转发广播分组,无冗余传输

需构造和维护生成树(有额外状态和开销):基于核心的方法.

1.选择一个节点作为核心,也称汇聚点;2.其它节点向核心发送单播加入报文:路由器利用单播转发表向核心转发加入报文时,记录报文输入/出端口,这些端口就是位于生成树上的端口;3.当加入报文到达,报文经过的路径被添加到生成树上

**ICMP**:主机或路由器使用ICMP协议传递网络层上的一些信息

**类型**:**询问**:用于请求信息,通常采用请求-响应模式

e.g.**回声请求/响应:**用于发现对方是否在线;**地址掩码请求/响应**:用于获得本网的地址掩码;**路由器请求**:请求本网路由器的信息;**路由器发现**:路由器定期发送该消息通告自己的信息

**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

e.g.**源抑制**:路由器缓存满,无法容纳新到来的数据报;**超时**:数据报的TTL减为0,或主机的重组定时器超时;**目的不可达**:路由器判断一个数据报不可能到达它的最终目的地;**重定向**:路由器发现主机使用的路由有错或不是最佳路由;**参数错误**

**封装在IP包中传输**: 跨网络传输必须借助IP包

**报文格式**:**type**报文类型(15种);**code**对某类报文进一步的区分**Checksum;**内容:与报文类型有关.报告错误的ICMP报文包含触发该错误的数据报的头部和前8个数据字节

**Ping**:用ICMP测试目的主机是否活跃,目的路径是否正常:

源主机:Type=8,Code=0的Echo Request 报文;目的主机收到,发Type=0,Code=0 的 Echo Response报文;源主机计算RTT,并报告.若源主机连续几次超时(收不到ER),报告目的不可达

**Traceroute**:测试到达目的主机的路由(经过的路由器)

源主机向目的主机发送EchoRequest报文,IP报头的TTL设为k

TTL=0时,向源主机发送TTLexpired(11,0)报文(IP报头中含路由器IP)依次取k=1,2,…**直到收到目标主机的Echo Response**

**ICMPv6**:合并ARP和IGMP,取消RARP(功能已被其它协议取代)

**差错报告**:去掉源抑制报文:优先级和流标签允许路由器控制拥塞|丢弃不重要数据包;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

**CHAP6 数据链路层-1介绍**

**链路层**:将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;易产生传输错误

**节点**:主机和路由器;**链路**:连接相邻节点的信道;**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

接收:从原始比特流中提取出完整的帧

2.链路接入(广播链路需要):广播信道上协调各节点发送行为

3.差错检测(基本服务):检测传输错误

4.差错纠正(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:调节发送速度,避免接收节点缓存溢出

提供可靠交付的链路层协议,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/发转换

**在哪实现**:1.路由器:线卡;2.主机:主体在网络适配器(网卡)实现

线卡/网络适配器连接物理媒体,还实现物理层的功能

**网络适配器之间的通信**:发送侧: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

**检错和纠错:**

传输**出错类型**:1.单个错:随机信道热噪声引起,一次只影响1位

2.突发错:瞬间脉冲噪声引起.影响多位,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**:只检错,不纠错,不确定错误位置与反馈重传机制结合进行差错恢复;纠错码:确定位置;自纠正

**码字**:m比特数据+r比特冗余位(校验位)

有效编码集:2^m个符合编码规则的码字;检错:无效码字,错误

**海明距离**l:两个码字的对应位取值不同的位数->编码集中任意两个有效码字的海明距离的最小值

纠错:将收到的无效码字纠正到距其最近的有效码字

检错码与纠错码的能力都是**有限的！**

检错能力:检测d比特错误,编码集的海明距离至少应为d+1

纠错能力:纠正d比特错误,编码集的海明距离至少应为2d+1

**奇偶校验:**单比特:检测奇数个比特错误,检错率50%,l=2

二维:检测2比特错和纠正单比特错,有利于检测突发错误.l=3

**循环冗余校验CRC**:信息多项式M:m个信息比特构成的多项式

冗余多项式R:由r个冗余比特为系数构成的多项式

码多项式T: 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)的一个多项式

R(x) = x^r·M(x) ÷ G(x) 的余式(减法运算定义为异或操作)

检验方法:若T(x) ÷G(x)的余式为0,判定传输正确

\*检错能力极强,可硬件实现,是链路层上应用最广泛的检错码

链路的两种类型:点到点链路;广播链路:连接许多节点的单一共享链路,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R发送(信道利用率高);2.M个节点发送时,每节点能以R/M的平均速率发送(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(无额外机制);4. 简单(实现和运行开销小)

**信道划分:**信道划分为若干子信道,每个节点固定分配一个子信道,不会发生冲突:关注**公平性**,轻负载时信道**利用率不高**

(1)**TDMA:时分多址**.将信道使用时间划分成帧,每个节点在帧中分配一个固定长度的时间片,每个时间片可以发一个分组;节点只能在分配给自己的时间片内发送;不发送时间片轮空

(2)**FDMA: 频分多址.**将信道频谱划分为若干子频带.;每个节点被分配一个固定的子频带;若节点不发送,其子频带空闲

(3)**CDMA:码分多址.**每个比特时间进一步划分为m个微时隙

每个节点被分配一个惟一的m比特码序列(chip code).发送方编码:发送“1”=发送chip code;发送“0”=发送chip code的反码

信号叠加:多个节点发送的信号在信道中线性相加;接收方解码:用发送方chipcode与信道中混合信号算**内积**,得到原数据

**前提条件:任意两个chip code必须是相互正交的**

CDMA允许所有节点同时使用整个信道！

**随机接入**(竞争):不划分信道,节点自行决定何时发送,出现冲突后设法解决.轻负载时信道利用率高,重负载时冲突严重

发送前不监听信道:ALOHA家族;发送前监听信道:CSMA家族

(1)**时分ALOHA:假设**1.所有帧长度相同2.时间被划分为等长的时隙,每个时隙传一帧3.节点只能在时隙开始时发送4.节点是时钟同步的5.所有节点可在时隙结束前检测到是否有冲突

**操作**:1.节点从上层收到数据后,下一个时隙发送2.若时隙结束前未检测到冲突,可在下一个时隙发送新的帧3.若检测到冲突,**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发送;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t活跃节点时,长期运行过程中成功时隙所占的比例.假设:N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=37%.最佳情况仅37%时间信道有效传输

(2)**纯ALOHA**:无需时钟同步,任何节点有数据就可以立即发送;

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**一个帧时后再决定(帧时:发送一帧的时间,假设帧长相同).**效率**:P(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[t0, t0+1)内发送)=p(1-p)^(2(N-1));最大效率=1/2e.

(3)**载波侦听多址接入(CSMA)**:**发送前监听信道**:1.信道空闲:发送整个帧2.信道忙:推迟发送.但**冲突仍可能发生**:存在传输延迟,节点可能没有监听到其它节点正在发送.即使忽略传输延迟,当两个(或多个)节点同时发现信道由忙变为空闲,都决定立即发送时,仍会发生冲突.

**(4)CSMA/CD:**仅发送的过程中检测冲突(发生冲突时信号强)检测到冲突后,立即停止发送剩余部分,启动冲突解决的过程

**以太网MAC协议:**早期以太网采用CSMA/CD协议:**1.**网卡从网络层接收数据报,构造以太帧;**2.**若网卡监听到信道空闲,立即发送;若信道忙,坚持监听直至发现信道空闲,发送帧**3.**若网卡发送完整个帧没有检测到冲突,认为发送成功**.4**.若网卡传输过程中检测到冲突,立即停止,并发送一个阻塞信号(加强冲突)

**5.**进入**指数回退阶段**,选择等待时间:第k次冲突后:从{0,1,2,..., (2^k)-1}中选择t,延迟t·512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(冲突次数多),等待时间选择范围越大,再次发生冲突的可能性越小

**效率**:Tprop以太网中任意两个节点之间传播延迟的最大值

Ttrans最长帧的传输时间 **效率=1/(1+(5Tprop/Ttran))**

Tprop->0或Ttrans->无穷时,以太网的效率趋近于1

结论:应**控制以太网的规模**

**轮流MAC协议:**不划分信道,有数据的节点轮流发送,不会冲突

信道利用率高,公平性好,但需引入额外机制

**(1)**轮询,缺点:引入轮询延迟;单点失效(主节点) （蓝牙）

(2)令牌传递:网络中有一令牌,按预定顺序在节点间传递

获得令牌的节点可以发送;发送完数据后释放令牌

缺点:令牌传递延迟;单点失效(令牌) (FDDI\IBM令牌环\总线)

**LANs:局域网LAN**:小范围内的计算机及外设连接起来的网络,范围在几公里以内,通常为个人或机构所有

**城域网MAN:**通常覆盖一个城市的范围(几十公里),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**:国家/洲(一百公里以上),规模和容量可任意扩大

**MAC Addressing**:链路层编址:每一块网络适配器(网卡)固定分配一个地址,称为物理地址(硬件地址,链路层地址,MAC地址)

长6个字节,用由“:”或“-”分隔的6个十六进制数表示.由IEEE分配,每块适配器地址全球唯一:网卡生产商购买一块MAC地址空间(前3字节),确保每一块网卡有不同的MAC地址;MAC地址固化在网卡ROM中;现在用软件可以改变网卡的MAC地址

帧的目的MAC地址有三种类型:1.**单播地址**:适配器的MAC地址,地址最高比特为0;2.**多播地址**:标识一个多播组的逻辑地址,地址最高比特为1;3.**广播地址**:ff:ff:ff:ff:ff:ff

网络适配器仅将发送给本节点的帧交给主机:目的地址为适配器MAC地址的单播帧;所有广播帧;指定接收的多播帧

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

MAC VS IP:先有MAC地址,后有IP地址;TCP/IP(互联网)出现之前,只使用MAC地址在单个物理网络中寻址;为什么有了MAC地址,还要IP地址?MAC地址是扁平结构的,无法在因特网范围内快速确定接口的位置;IP地址是有结构的,可以在因特网范围内快速确定网络接口的位置.IP地址与MAC地址无固定关联关系:MAC地址与网卡绑定,与节点所在子网无关

IP地址与所在子网有关,与网卡没有关系

**如何将数据报发送到下一跳**:当发送节点A,接收节点B位于同一物理网络时,数据报可从A直接交付给B:A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的适配器收到帧,根据目的MAC地址判断发给本机,取出交给网络层

**地址解析**:已知IP,MAC?**地址解析协议(ARP)**用于动态获得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广播B的IP地址(地址解析请求),B用自己的MAC地址进行响应

**报文格式**:硬件类型16:以太网为”1”|协议类型:IP地址为”0800\_16”|硬件地址长度8|协议地址长度8|操作:16ARP请求为1,ARP响应为2在以太网上,ARP报文**封装在以太帧中传输.**

**过程:**A想知道B的MAC地址:1.A构造ARP请求,在发送方字段填入自己MAC地址和IP地址,目标字段填入B的IP地址.2.A将ARP请求封装在广播帧中发送3.每个收到ARP请求的节点用目标IP地址与自己的IP地址比较,相符的节点进行响应(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,修改操作字段为2;5.将ARP响应封装在单播帧(目的地址为A的MAC地址)中发送

**ARP缓存**:每个节点在内存中维护一个地址映射表,称ARP缓存

每次发送数据报前先查询,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.超时(15～20分钟)后删除

**改进:主动学习**:1.从ARP请求中获取地址绑定信息:每个节点可以收到全部的ARP请求报文,将发送节点的地址映射缓存到自己的ARP表中2.节点在启动时自动广播自己的地址映射:节点A在启动时主动广播一个ARP请求,在目标字段内填入自己IP地址;收到的节点将A的地址映射缓存起来;若A收到ARP响应,报告IP地址重复错误.;**ARP是即插即用的:**一个ARP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.**所以,最好把ARP看成是跨越链路层和网络层边界两边的协议**.

***数据报到达子网之外:***数据报从A(子网1)经过R(路由器)到达B (子网2):A知道下一跳地址为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, dest MAC = R-1,发送;R接收帧,取出IP数据报,发现目的地址为B;R利用ARP获得B的MAC地址;R创建链路层帧,封装IP数据报,src MAC=R-2, dest MAC = B,发送;B的网卡接收帧,取出IP数据报,交给网络层.

**ARP与DNS的一个重要区别:**DNS为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IP.

**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:共享式以太网**:总线(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输出.集线器相当于共享电缆

**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(**链路层设备**).

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,之间不直接通信

不同于基于hub的星型连接

**以太帧结构**:Preamble(前导码):7个10101010字节,后跟一个10101011字节,用于在发送方和接收方之间建立时钟同步,不计入以太帧的长度.Dest.Address/SrcAddress:目的/源MAC地址;Type(2字节):指出Data所属的高层协议(IP,ARP等),每个协议有一个编号.Data:46-1500字节,**不足46填充至46字节**;CRC(4字节):对destaddr,srcaddr,type,data四字段计算得到的CRC码

**无连接,不可靠的数据传输:**无连接:发送方网卡与接收方网卡之间没有握手;不可靠:接收方网卡不发送确认;接收方网卡丢弃CRC错误的帧;依靠上层协议(TCP或应用)进行错误恢复

**为什么有最小帧长的要求**:CSMA/CD中发送方仅发送过程中检测冲突;为保证发送结束前检测到冲突,帧发送时间须够长:

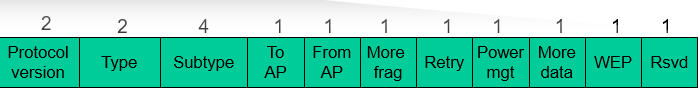
1.节点检测冲突需要时间2.假设信号在相距最远的两个适配器之间往返延迟2τ,则即帧的最小长度≧链路速率×2τ

**为什么最小帧长为64字节**(不含前导码):保证在发送结束前检测到冲突。根据早期以太网的最大直径(2500米)和数据速率(10Mbps)得到;最小长度≧链路速率×往返延迟(2τ）

**IEEE802.3**以太网标准:链路层,物理层

10Mbps以太网(早期以太网):10Base-5:基带同轴电缆(粗),每段最大长度500m;10Base-2:基带同轴电缆(细),最大长度200m;

10Base-T:3类双绞线和集线器,双绞线最大长度100米

10Base-F:多模光纤和集线器,光纤最大长度2000米

100Mbps以太网(快速以太网):仅能用光纤/双绞线,及集线器/交换机.100Base-TX(可用集线器或交换机):5类双绞线(2对),不超过100m;100Base-T4(同上):3类双绞线(4对),不超过100;100Base-FX(只能使用交换机):多模光纤2条,不超过2km

千兆,万兆以太网:使用交换机,并增加了对流量控制的支持

**DIX以太帧与802.3帧**:1.最早的以太帧称为DIX以太帧:type指出处理data域的协议实体;2.符合IEEE802.3标准的帧(802.3帧):

Length:替代DIX帧中type域,指出data长度;两种都可使用,**当type/length的值大于1500时解释为type,否则解释为length**

**共享式以太网**:集线器所有端口位于同一冲突域;任一时刻最多只允许一个主机发送;网络规模(节点数量)与网络性能矛盾

**交换式以太网**:交换机每端口为一个冲突域;多对端口可同时通信;**网络集合带宽=各个端口带宽之和**;从根本解决矛盾

理论上交换式以太网无需限制帧最小长度(不用CSMA/CD).考虑兼容性仍使用;网络直径不受信号最大往返时间的限制.交换式以太网的MAC层除了**帧格式保持不变之外,其他不同**

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

**支持多对传输同时进行**:主机通过**点-点线路**连接到交换机.

交换机缓存分组,在每一条输入链路上执行以太网协议:每条链路是一个冲突域;全双工通信;交换:多对端口可同时传输.

**如何转发**:每个交换机内部有一张端口转发表,每个表项记录以下信息:<MAC地址,到达该MAC地址的端口>

交换机**自主学习**“哪个主机通过哪个端口可达”:当帧到达,交换机从源MAC地址了解发送节点,从帧到来端口了解发送节点位置(从该端口可达),在转发表中记录发送节点和可达端口

帧的**过滤和转发**: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.3.找到目的MAC地址则①目的地址所在端口=帧的到来端口,丢弃帧(过滤不需要转发的帧)②转发帧到表项指定的端口(按转发表转发帧)4.未找到则:扩散帧(未知节点,用扩散法转发).向**输入端口以外**所有端口转发

**处理过程**:1.目的地址查找转发表(转发决策):目的地址所在端口=帧的进入端口,丢弃帧;否则转发(在表转发,不在扩散)

2.用帧的源地址查找转发表(更新转发表):找到地址,将对应表项生存期设为最大值;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

**级联交换机**:多交换机也可级联在一起形成更大范围局域网

也通过自主学习(同单交换机).

**交换机vs路由器**:交换机工作链路层,据MAC地址存储转发帧

路由器工作于网络层,根据IP地址存储转发数据报;交换机不能连接异构链路(MAC协议不同的网络),因为交换机只按原样转发帧,路由器可连异构链路,因为路由器需重新封装链路层帧;交换机不能阻断广播帧的传播:只能学习到单播MAC地址,所有广播帧都会扩散发送,通过交换机连接的所有主机在同一个广播域中;路由器可阻断广播帧的传播:路由器据IP地址转发包(看不到MAC地址),每个路由器端口是一个独立广播域

**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)**,可被冲突域中其它主机接收

**广播域**:广播帧能够到达的主机集合

**三层交换机和路由器**:三层交换机:部分路由功能,二层转发速度|加快大型局域网内部的数据交换而设计|但在安全、协议支持等方面不如专业路由器||三层交换机转发速度快的原因：**一次选路，多次转发(IP索引-Hash)**

路由器可分隔二层网络，但转发速度慢、成本高

7应用6表示层5会话层4传输层3网络层2数据链路层1物理层

**CHAP7无线和移动网络-1介绍**

移动:终端改变网络接入点,给**网络层**带来很大问题

**无线**: 无线链路通信,给**物理层和数据链路层**带来很多问题

**无线终端**: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继数据包;负责协调与之关联的多个无线主机的传输(802.11AP）

**无线链路**:连接无线终端和基站;需要MAC协议协调无线链路;

不同的无线链路具有不同的数据速率和传输距离

**无线链路**:信号衰减:传播中能量减少(路径损耗);干扰:受其它信号源干扰;多径传播:反射使信号沿多条路径到达接收端

以上特性导致无线链路的**传输距离受限、误码率很高**

**运行模式**:1.**基础设施模式**:无线终端通过基站连接固定网络(网络基础设施),传统网络服务由固定网络提供;切换:无线终端接入不同基站的过程;2.**自组织模式**:没有基站;节点只能与通信范围内节点通信;节点相互帮助转发,是终端也是路由器

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

**无线网络的特性:**1.**隐藏节点**问题:不在发送节点通信范围内,但在接收节点通信范围内的活跃节点(发送节点听不到,但影响接收)2.**暴露节点**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(发送节点能听到,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否有节点在发送

**IEEE802.11**:802.11b(范围2.4-5GHz,最高11Mbps);802.11a(5-6G,54M);802.11g(2.4-5G;54M)802.11n:多天线(2.4-5G,200M)

MAC协议:CSMA/CA,支持基站模式和自组织模式,物理层不同

**无线局域网架构**:无线LAN**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**

每个无线接口(终端及AP)均有一个**全局唯一**的MAC地址

AP与路由器连的有线端口无MAC地址(AP对路由器是透明的)

**信道与关联**:通信频段划分成若干信道,每个BSS分配一个信道:

装AP时,为AP分配一个服务集标识符(SSID),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发送的信标帧(含AP的SSID,MAC地址)2.选1个AP关联(可能需要身份鉴别)

使用DHCP获得AP所在子网中的一个IP地址

**被动扫描**:主机监听AP发送信标帧;主机选一个AP发送关联请求帧;AP向主机发送关联响应帧;**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一个AP发送关联请求;AP发送关联响应帧

**MAC协议**: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,基站控制单元内所有通信活动;轮询:基站依次询问节点,被询问到的节点可以发送帧,不会冲突;**DCF**模式:有/无基础设施均可,所有节点(AP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**:A向AP发送RTS帧:给出随后要发送的数据帧及ACK帧需要的总时间;AP收后回复CTS帧:帧中给出同样的时间

A收到CTS帧:发送数据帧;AP收到后:发送一个ACK帧进行确认

**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;**若A,B同时发送RTS,不成功的随机等待时间重试;**发送数据较少时,一般不使用信道预约机制**

**帧间距机制**:允许DCF,PCF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

PIFS:若SIFS后无节点发送,PCF的基站可发送信标帧或轮询帧

DIFS:若PIFS后没有基站发送,任何节点可以竞争信道

EIFS: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

**无信道预约**:当节点要发送时,侦听信道:1.若一开始侦听到信道空闲,等待DIFS后发送帧;2.否则,选取随机回退值,侦听到信道空闲时递减该值,此过程中若侦听到信道忙,冻结计数值

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CSMA/CA;若未收到确认,重复2中回退阶段,从更大范围内选取随机回退值.

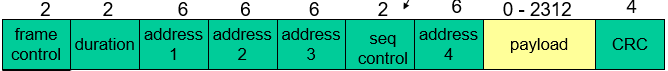
若有k个节点等待发送,其**随机选取的回退值决定发送顺序**

**CSMA/CA与/CD不同**:D在发送过程中检测冲突,无确认机制

A发送过程中不检测冲突,使用确认机制

D中侦听到信道空闲立即发送(不怕冲突,冲突立即停发)

A中侦听到信道空闲随机回退(冲突对网络损害大,尽量避免)

**帧格式**:Add1目的MAC|Add2:源MAC|Add3:连接AP的路由器接口MAC|Add4:只在自组织模式中使用

**寻址举例**:AP仅对无线终端可见,对固定网络上的设备不可见

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:

AP MAC addr + H1 MAC + R1 MAC->R1 MAC+H1 MAC

**终端在子网内移动**:终端从一个BSS移动到另一个BSS.发生切换时,终端要关联到新的AP上:当H1检测到来自AP1的信号逐渐减弱时,开始扫描新的信标帧;当H1收到来自AP2,信号更强的信标帧时,先解除与AP1的关联,然后关联到AP2

发生切换时,交换机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(源主机)发送的帧时,更新H1所在的端口,若转发表未及时更新,可能产生丢包

802.11f规定了AP间漫游的方法

若主机停留在同一个IP子网中,IP 地址保持不变

切换过程中,终端上的应用正常运行:由于IP地址没变,网络层及以上层次感觉不到这个移动,切换过程中产生的延迟及丢包,在上层协议看来是正常的

**先进功能**:**速率适应:**当主机移动或信噪比变化时,基站和主机动态改变传输速率(物理层调制技术)

**功率管理**:节点设置功率管理比特,告知AP它将进入休眠状态:

节点进入休眠,并在下一个信标帧之前醒来;在节点休眠期间,AP缓存发往该节点的帧;AP在发送的信标帧中包含一个移动节点列表,这些节点有帧缓存在AP中

列表中的节点向AP请求帧,其余节点重新进入休眠

**移动**:终端进入新子网后,须分配该子网上一个地址(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.即使对方获知了终端的新地址,应用必须重新建立连接,因为通信的端点(套接字)变了 **改进**?

**归属网络**:移动节点的永久 “居所”(e.g., 128.119.40/24)

**永久地址**:移动节点在归属网络中的地址,总是可以使用这个地址与移动节点通信e.g., 128.119.40.186(保持不变)

**归属代理**:移动节点在外地时,为其执行移动管理功能的实体

**外地网络**:移动节点当前所在的网络;**转交地址**:移动节点在外地网络上的地址;**外地代理**:外地网络上为移动节点执行移动管理功能的实体

**移动节点注册:**移动节点进入外地网络后,向外地代理注册;移动节点通过外地代理向归属代理注册,归属代理记录移动节点的外地地址;**最终结果:**外地代理知道移动节点在本地网络上;归属代理知道移动节点的转交地址,记录到地址绑定表

**间接选路到移动节点:**通信者在数据包中使用移动节点的永久地址;归属代理截获数据包,转发给外地代理;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网络:向新的外地代理注册;新的外地代理向归属代理注册;归属代理更新移动节点的转交地址;归属代理使用新的转交地址向移动节点转发包.;.节点移动及变换外地网络等对通信者都是透明的: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,并获知移动节点转交地址(此步以后不必再做);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发送**.

**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,永久地址,转交地址,移动节点注册;标准化三部分:

**(1)代理发现:1.**愿意充当归属代理或外地代理的路由器定期在网络上发送代理通告,宣布自己的存在及IP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了网络;**4.**如果发现在外地网络上,移动节点从外地代理提供的转交地址中选择一个作为自己的转交地址.

**(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,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等;2.外地代理记录相关信息,向归属代理转发注册请求;3.归属代理处理注册请求,若认证通过,将移动节点的永久地址及转交地址保存在绑定表中,发回一个注册响应;4.外地代理收到有效的注册响应后,将移动节点记录在自己的转发表中,向移动节点转发注册响应;5.当移动节点回到归属网络时,要**向归属代理注销**.

**(3)数据报间接选路**:1.数据包首先被归属代理得到;2.归属代理查地址绑定表,获得移动节点当前转交地址;3.归属代理将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.**若通信者不在归属网络上:数据包首先到达移动节点归属网络上的路由器;路由器查表得知可以直接交付,于是查找ARP缓存或者发送ARP请求,以获取移动节点的MAC地址;利用得到的MAC地址,将数据报封装到链路层帧中发送;**2.**若通信者在归属网络上:通信者查表得知移动节点直接可达,于是查找ARP缓存或者发送ARP请求,利用得到的MAC地址封装数据报,发送.**数据报如何能被归属代理得到**?链路层帧的目的地址必须是归属代理的MAC地址;即,移动节点的永久地址应当映射到归属代理的MAC地址**.ARP代理**:归属代理为位于外地网络的移动主机发送ARP响应,用自己的MAC地址进行响应;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,刷新其它节点的ARP缓存.**数据报如何到达转交地址**?归属代理如何将数据报发送到转交地址?归属代理收到的数据报,目的地址为移动节点的永久地址,而移动节点的转交地址位于外地网络.**如何将目的地址在归属网络的数据报送达外地网络**?方法:修改目的地址=转交地址 (×)(转交地址是外地代理的IP地址,而数据报的最终目的地应是移动节点);使用隧道(√)(隧道技术的又一个应用例子).**归属代理通过隧道转发数据包**:归属代理向外地代理发送的包: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动节点**？外地代理解封装收到的数据包,得到原始数据报;外地代理如何获得移动节点的MAC地址?在移动节点注册阶段,外地代理获知了移动节点的永久地址和MAC地址,记录在其转发表中;外地代理根据目的IP地址查找转发表,得到移动节点的MAC地址;外地代理利用移动节点的MAC地址,将数据报封装到链路层帧中,发送给移动节点.**移动节点如何发送数据包**?移动节点将数据包发送给外地代理(缺省路由器):**SrcIP**=移动节点**永久地址**,DestIP=通信者IP地址,SrcMAC=移动节点MAC,DestMAC=外地代理MAC;外地代理按照正常方式转发数据包.移动节点如何得知外地代理的MAC地址？**代理通告报文的源MAC是外地代理的地址**.**无线和移动对上层协议的影响:无线链路带来的问题**:误码率高,丢包率高,延迟增大.**节点移动带来的问题**:丢包、延迟增大.**逻辑上,没什么影响**:为上层协议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,不必要地减小拥塞窗口,导致应用吞吐率很低;无线链路、有线/无线混合链路上的TCP拥塞控制是一个研究问题.

**CHAP8 安全**-1概述

**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)

**端点鉴别**:双方都能够证实另一方**;报文完整性**: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

**安全攻击种类**:1.**被动攻击**:获取信息,不产生影响(偷听/流量分析)2.**主动攻击**:改变资源或影响系统(伪装:假冒另一个实体;重放:被动获取一个数据单元,之后重新发送;报文修改;拒绝服务)

**安全机制**:1.加密:用数学算法对数据变换;2.鉴别:通过报文交换证实实体身份;3.报文完整性:验证报文是否可信(来源,内容);4.数字签名:附加在数据单元后,证明数据单元来源及完整性,以防伪造,抵赖;5.流量填充:数据流间隙插入比特,挫败流量分析企图;5.访问控制:授权机制限制用户访问,防止越权行为

**2密码学**: (加密密钥=解密密钥?)对称加密/非对称**|**块/流密码

**传统替换密码**:密文字母替换明文字母,位置不变;

eg凯撒密码,单字母表替换,多字母表替换; **密钥:字母映射表**

**传统换位密码:**明文字母不变,改变位置;eg:列换位密码

**密码的安全性**:传统:安全性建立在算法保密基础上

现代:也用替换和换位,但基本原则:算法公开,仅密钥需要隐藏

**计算安全**:破译密文代价超过信息本身价值or破译密文所需时间超过信息有效生命期;现代密码学中,密码的安全性是通过**算法的复杂性**和**密钥的长度**来保证的

**密码分析攻击**:惟密文攻击:仅根据截获密文分析明文或密钥

已知明文攻击:截获密文+一些已知“明文-密文对”分析密钥

选择明文攻击:可任选一定数量明文加密得到相应密文,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**

**现代对称密钥算法**:**1.DES:**块密码,对称,迭代,加解密子密钥次序相反;64入64出 缺点:密钥长度56不够长,迭代次数不够多

**过程:**1.初始换位;2.16轮相同迭代,每轮用不同子密钥(主密钥生成);3.再进行一次换位(与初始换位相反);**3DES**:使用两个密钥进行三轮DES计算:**1.**用K1加密**2.**用K2解密**3.**用K1加密;**1.**Why用两个密钥?112比特密钥足够长**2.**Why三重?中途攻击使穷尽密钥只需2^56而非2^112.**3.**Why EDE而非EEE?与单次DES兼容.3DES用户解密单次DES只用K1=K2.

**1.AES:**对称块加密;每次处理128比特明文块128|192|256;密码块链接(CBC):解决重放攻击(相同明文块不产生相同密文块)

**现代非对称加密:**发送者和接收者不共享密钥;不存在密钥传递问题(加密密钥公开,解密密钥私有)**要求**:公钥无法计算出私钥;公钥和密文无法得到明文;K-(K+(m))=m=K + (K- (m)

**RSA**:n=pq;z=(p-1)(q-1);选择d使(d,z)=1;ed=1(mod z);

公钥(e,n);私钥(d,n);**加密**:明文看作比特串,划分成数据块M,使0≤M＜n;计算C＝M^e (mod n)为M的密文;**解密:**M=C^d (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:免于传递密钥;**缺点**:计算开销大,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

**利用报文加密**:发送方和接收方用共享密钥,如接收到可以解密则可信.混淆了机密性和报文鉴别,带来不必要计算开销.

**报文摘要(数字指纹)**:一个散列函数作用在报文m上,生成固定长度散列值H(m)为报文摘要.发送方发报文+摘要;接收验证.

**基于加密**:发送方计算报文摘要,用与接收方共享密钥加密形成报文鉴别标签(报文鉴别码);接收方用共享密钥解密得到发送方计算的报文摘要,计算验证; 缺点:需要使用加密算法.

**基于哈希**:发送方用共享秘密密钥KS添加到报文m之前,计算报文摘要H(KS||m)形成报文鉴别码(HMAC可与MD5和SHA-1)

**密码散列函数**:易于计算;**单向性**(不可能给定h,找到x,H(x)=h);

单射性(任意数据块x,很难找到y≠x,H(y)=H(x),否则可替换);

计算上无法找到一对(x,y),H(x)=H(y);前3弱散列函数,+4强

标准:MD5:散列码长度128比特;SHA-1:160;鉴别方案HMAC

**数字签名**:条件:1.接收方通过数字签名能鉴别发送方身份(起源鉴别)2.发送方过后不能否认签名过的文档(抵赖);3.接收方无法伪造被签名文档内容

**私钥加密**报文摘要:**发送方**计算报文摘要,用自己私钥加密形成数字签名,附加在报文后发送;**接收方**拷贝数字签名备用;**接收方**用公钥得到原始报文摘要,计算摘要,相符则真实.

**公钥证书**:用证书验证某主体有某公钥;证书由可信第三方机构颁发(认证权威CA);证书含公钥+CA的签名(无法伪造篡改)

**获取证书**:提供身份证明,CA验证后绑定身份与公钥

**验证证书**:获取证书,用CA的公钥验证证书得到公钥

证书标准:X.509.CA对证书内容SHA-1散列,后用CA私钥加密报文摘要形成数字签名.验证公钥证书:验证方用CA公钥解开签名,得到证书内容报文摘要,对收到的证书内容计算验证.

**撤销证书**:有效期/显式撤销:CRL(撤销列表)/使用证书前查CRL

**证书格式**:主体名字:证书被颁给的对象;PubKey:与主体绑定的公钥,及使用该公钥的算法名字及参数等;Signature:证书使用算法及参数,证书签名.证书签名覆盖证书的所有内容

**分布式公钥基础设施**(PKI):提供公钥加密和数字签名服务

含不同组织的CA,每个CA有自己的私钥,为部分用户签发证书

用户自已决定使用哪一个CA;系统:所有实体都有根CA的公钥

**证书目录**:DNSSEC:LDAP专门目录服务器;定期清除CRL所列

**末端鉴别**:**目的**:避免重放攻击; **方法**:使用不重数(Nonce)

4.0:接收给发送方发一个不重数,发送方用共享对称密钥加密

5.0:采用公开密钥算法加密不重数

X.509**单项鉴别服务**:

tA:时间戳(产生+到期时间);rA:A随机选择不重数,供接收者检测重放攻击;IDB:B标识,指示接收者;Data:数据;Ka-b:若需保密,为A加密Data的对称密钥;Kb+:B公钥,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**:B用私钥解Ka-b解密Data,算前面4个部分的报文摘要

B用A的公钥从签名中得到原始的报文摘要,进行比较

**电子邮件安全:**真实性和机密性

**PGP:**因特网安全电子邮件的事实标准,多个人用.

(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**数字签名附在报文前面**,与报文一起发送:Sgn || Data

**机密性**:对称密钥算法:发送方A生成报文和随机128比特数(一次性会话密钥);用会话密钥加密报文,再用**接收方B公钥**加密会话密钥,与报文一起发送:Kb+(Ka-b) || Ka-b(Data)

**压缩:**用ZIP算法:Kb+(Ka-b)||Ka-b(Zip(Sgn||Data))加密前压缩: 1.减少要加密的数据量2.减少消息冗余,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

**都用**:

邮件分段服务:许多邮件最大报文长度不超过50,000字节

PGP完成全部处理后将超长的报文分成小块,会话密钥和签名只在第一片段,接收端去掉每个片段头,将所有片段重新组装

**安全TCP:SSL**:向基于TCP的网络应用提供安全的传输层服务

**安全服务**:机密性,数据完整性,服务器鉴别,客户鉴别(可选)

SSL建立在TCP上,依靠TCP提供可靠端到端连接,涉及2个层次的一组协议:1.SSL记录协议:为各种高层协议(如HTTP)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

**SSL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**:1.浏览器向服务器发送建立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)和压缩方法等,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一起发送给浏览器

**服务器鉴别**:1.服务器向浏览器发送其公钥证书(和必要的证书链)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;若在则用该CA公钥验证,得到服务器的公钥.

**浏览器鉴别**:可选,收到服务器证书请求,则发送其公钥证书.

**生成密钥**:1.浏览器生成一个48字节随机数,称预密钥,用服务器公钥加密后发给服务器2.客户服务器各自从预密钥,Rc,Rs中计算加密数据所需会话密钥,计算MAC需要的密钥

**最后**:1.浏览器向服务器发送所有握手报文(级联)的MAC

2.服务器向浏览器发送所有握手报文(级联)的MAC

**SSL记录协议:**SSL记录协议提供两种服务:1.机密性(通过加密SSL载荷实现)2.完整性:通过报文鉴别码保护

**过程**:1.从上层接收要传输的应用报文,划分成长度不超过214字节的数据块;2.(选)数据块压缩3.对数据块生成基于哈希运算的报文鉴别码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上SSL头,包括内容类型,SSL版本号,压缩数据块的长度等

***网络层安全性:IPsec和虚拟专用网:IPv4在设计时没有考虑安全性:***缺少对通信双方身份的鉴别,容易遭受地址欺骗攻击；缺少对网络中数据的完整性和机密性的保护,数据很容易被窃听、修改甚至劫持.***IP安全协议(IPSec):***IETF以RFC形式公布的一组安全协议集；**目标是**把安全特征集成到IP层,以便对因特网中的安全业务提供低层的支持.**IPsec和虚拟专用网:*专用网:***通过电信专线将分散在各地的计算机(网络)连接而成的网络；安全性好,但代价高.***虚拟专用网(V****irtual* ***P****rivate* ***N****etwork****):***建立在公用网上的一个覆盖网络(overlay),在逻辑上与其它流量隔离；数据在发送到公用网之前进行加密.***VPN的实现:*VPN的典型结构:**在每个局域网上设置一个安全网关,在每一对安全网关间创建一条穿过因特网的隧道,在隧道中使用IPSec；**VPN的优点:**可以在一对局域网间提供完整性控制及机密性服务,甚至对流量分析也有相当的抵御能力；对因特网中的路由器及用户软件是透明的,只要系统管理员设置好安全网关就可以了.传进公用网的IPsec被IPv4封装,同时拥有IPv4和IPsec首部.**安全关联:*IPSec提供了一个用于集成多种安全服务、加密算法及安全控制粒度的安全体系框架:IPSec提供的安全服务包括:***访问控制、无连接完整性、数据起源认证、抗重放攻击、机密性等；IPSec的安全机制独立于算法,因此在选择和改变算法时不会影响其它部分的实现；IPSec提供多种安全控制粒度,包括:一条TCP连接上的通信,一对主机间的通信,一对安全网关之间的所有通信；用户可以为数据通信选择合适的安全服务、算法、协议和控制粒度.从技术上说,***IPSec主要包括两个部分:***

**IPSec安全协议:**包括**AH**(不提供机密性)**和ESP**两个安全协议,定义了用于安全通信的IP扩展头和字段,以提供机密性、完整性和源鉴别服务；**密钥管理协议:**定义了通信实体间进行身份鉴别、协商加密算法以及生成共享会话密钥的方法.*将以上两部分绑定在一起的是称为****安全关联(SA)****的抽象.****SA是****:*通信对等实体之间对某些要素的协定,如使用的安全协议、协议的操作模式、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(SPI)**唯一标识**,如果在两个方向上都需要安全通信,则需要建立两个SA.SPI携带在数据包中,由数据包的处理进程用来查找密钥及相关信息.***SA可以建立在***一对主机之间、一台主机与一个安全网关之间、或一对安全网关之间.**IPsec数据报:*IPSec的使用模式:*传输模式:**IPSec头被插入到原始IP头和传输层头之间,路由器根据原始IP头转发数据包；**隧道模式:**原始数据包被封装在一个新的IP包中,IPSec头被放在新的IP头和原始IP头之间,路由器根据外层IP头的信息转发数据包.隧道的端点(外层IP头中的地址)通常是一个支持IPSec的安全网关.***两种模式的比较:***传输模式比隧道模式占用较少的带宽,隧道模式更安全:隐藏内部网络的细节(原始IP头不可见)；内部网络上的主机可以不运行IPSec,它们的安全性由安全网关来保证；隧道模式可以将一对端点间的通信聚合成一个加密流,从而有效地防止入侵者进行流量分析.***鉴别头部(Authentication Header)协议:*SPI:**32比特的数,和目的IP地址、安全协议结合起来,唯一标识数据报的SA；**SeqNum:**对SA上发送的数据包进行编号,供接收端检测重放攻击.一个SA上的序号不能重用,因此在传输的数据包数量达到232之前,必须协商一个新的SA和新的密钥；**Authentication Data:**包含报文鉴别码的可变长度域,所有AH实现必须支持HMAC-MD5-96和HMAC-SHA-1-96.***AH协议提供***无连接完整性、数据起源认证和抗重放攻击,但不提供机密性服务:HMAC覆盖数据包的载荷部分,因而可提供无连接完整性服务；HMAC覆盖原始IP头中的不变域(传输模式)或整个原始IP头(隧道模式),因而可提供数据起源认证；AH头中有序号,且被HMAC覆盖,因而可抵抗重放攻击.***封装安全载荷(Encapsulating Security Payload):*ESP数据包大致分为以下几个部分:**ESP头:包含SPI和SeqNum；载荷:原始数据包中被加密部分的密文；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；鉴别数据:覆盖ESP头、载荷和ESP尾的报文鉴别码.***隧道模式路由R1使用下列方法将这个“普通1Pv4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；• 使用算法和巾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1Pv4首部字段(通常共20字节长)的全新IP首部,该新首部附加到载荷之前.(*运输模式*在第一部分缺少了初始IP首部).***ESP协议提供的安全服务:ESP协议提供***数据机密性、无连接完整性、抗重放攻击、数据起源鉴别和有限的数据流机密性服务:原始数据包的载荷部分被加密,因而可提供数据机密性；HMAC覆盖数据包载荷部分,可提供无连接完整性服务；ESP头中有序号,且被HMAC覆盖,可抵抗重放攻击；ESP隧道模式中,原始IP头也被HMAC覆盖,因而ESP隧道模式可提供数据起源鉴别；ESP隧道模式中,原始IP头也被加密,路由器只能看到外层IP头,因而ESP隧道模式可提供数据流机密性服务.***AH协议和ESP协议的安全性比较:***ESP隧道模式的安全性强于ESP传输模式；数据机密性服务:只有ESP提供,AH不提供；鉴别服务:ESP隧道模式的鉴别服务,安全性强于AH,ESP传输模式的鉴别服务,安全性不如AH.***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.**有限等效保密:*主机鉴别过程:***无线主机向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,发送给AP；AP解密不重数,若与AP发送给主机的不重数相同,完成主机鉴别.利用主机与基站共享密钥这个事实鉴别主机.***WEP数据加密:***主机与AP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 kiIV；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 kiIV.***WEP加密的安全漏洞:***每个KS只有224个(KS, IV) 可用:IV会被重复使用；IV用明文传输:攻击者可以观察到IV的重用.**攻击:**Trudy(可能通过欺骗方式)让Alice加密他选择的明文(d1 d2 d3 d4 … )；Trudy能够获得Alice加密的密文: ci = di XOR kiIV；Trudy知道ci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AP)来提供鉴别服务.***802.11i的操作:*1) 发现.**在发现阶段,AP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,在客户和鉴别服务器之间转发报文.**3)成对主密钥(Pairwise Master Key , PMK) 生成.**MK是一个仅为客户和鉴别服务器所知的共享密钥,它们都使用MK来生成一个次密钥,即成对主密钥(PMK).鉴别服务器则向AP发送该PMK.客户和AP 现在具有一个共享的密钥.**4)临时密钥(Temporal Key ,TK) 生成.**使用PMK, 无线客户和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将被用于执行经无线链路向任意远程主机发送数据的链路级的加密.

**防火墙**:可信内部网络,不可信的外部网络间执行访问控制策略的硬件或软件系统.**保护内部网络免受来自外部网络攻击.**

**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**:**路由器**对数据包逐包过滤,基于(源IP,目的IP, TCP/UDP源端口号,目的端口号,ICMP报文类型,TCP SYN标志, ACK标志)决定转发包还是丢弃包:会允许一些异常的包进入：

|  |  |
| --- | --- |
| **安全策略** | **过滤规则** |
| **不允许访问外部Web网站** | **丢所有外出,目的端口为80** |
| **不允许外部发起的TCP连接,除非访问的是内网的公共web服务器** | **丢弃进入的TCP SYN包,除非去往130.207.244.203的端口80** |
| **防止因特网广播吞噬网络带宽** | **除DNS包和路由器广播包,丢弃其它进入的UDP包** |
| **防止网络拓扑被探测** | **丢弃所有外出的ICMP TTL expired包** |

**状态检测防火墙**:可以跟踪TCP连接的状态

跟踪连接建立SYN和关闭FIN等状态,判断收到包是否有意义

**应用网关**:不仅检查网络层,传输层协议头,还检查应用层数据

1.所有telnet用户必须连接到应用网关;2.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;3. 包过滤防火墙阻塞所有不源自应用网关的telnet连接

**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病毒特征,攻击特征);检查多个包关联性:端口扫描,DoS攻击

包过滤仅检查**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&Kahn’s InternetArchitecture:两级编址:IP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.