Ch1：

计算机网络由硬件（计算机、网络设备、链路）和软件（操作系统、协议软件）组成

节点：主机（用户终端和服务器）、网络设备；链路：连接两个或多个节点的物理介质（分为点对点链路和共享/多路访问链路）；互联网：一些独立的就三级互相连接；路由器：连接两个或多个计算机网络的节点

操作系统：对节点上的资源进行管理，为软件提供运行环境；协议软件：定义了节点间的通信规则，具体组成包括信息格式、交互流程、解释处理

计算机网络定义：定义为一系列计算机、链路和网络设备的集合，并且满足：物理上，链路和网络设备将计算机连接起来，确保拓扑上的连通性；功能上，提供数据传输功能，确保计算机之间能够交换数据。通过计算机网络，将实现信息服务，资源共享

计算机网络的通用性：一能通过计算机上运行各种软件实现各种网络应用，二能传输多类型数据

网络体系结构目的：构建一个通用的、高效的 、健壮的、能够适应网络技术发展和应用需求变化的网络，指导网络设计，降低网络构建的复杂度；网络体系架构是指计算机网络中层和协议的集合。层表示了网络协议的组织机构。协议定义了通信双方为了实现特定功能所使用的数据格式以及数据处理交互流程。

协议封装：在发送节点每一层都给上层的协议数据单元加上代表协议控制信息的头标or尾部，向下层协议递交；解封装：在目的节点每一层协议根据该层协议控制信息完成PDU处理去掉头or尾向上层提交

网络体系结构分层思想：每一层的构建都是在下一层基础上，每一层都为上一层提供服务。意义：分层将建造一个网络的问题分解为多个可处理的部分，每一层解决一部分问题；分层提供了一种更为模块化的设计，如果添加新的服务，只需要修改一层的功能，而继续使用其它各层提供的功能

OSI（开放系统互连）：主机（物理-数据链路-网络-传输-会话-表示-应用）和路由器（物理-数据链路-网络）

Internet体系结构（基于TCP/IP）：应用层-传输层-互联网层-主机到网络/网络接口层

网络性能指标：1字节B=8比特b，，k、M、G、T，延迟\*带宽又称以bit为单位的链路长度，延迟=发送+传播+处理+排队

网络标准化（意义：不同网络设备可以相互通信、扩大产品市场、遵循相应表纯的产品互联互通）分为事实标准与法定标准，有ITU-国际电信联盟、ISO-国际标准化组织、IEEE-电气和电子工程师协会（IEEE802系列协议）、IETF

Ch2：

1. 常见传输介质：双绞线、同轴电缆、电力线、光纤、无线传输
2. 最大传输速率公式（无噪*nyquist：*、有噪shannon：）其中H为低通滤波器的带宽，本门课的分贝
3. 会有最大传输速率原因：做傅里叶变换会发现，随着频率增高，对应的能量会衰减，我们将衰减到一半的位置定位fc，具体位置由传输介质的材料构成厚度长度决定（这里的周期对应字节分之一而不是比特）
4. 数字速率是数字传输过程中采用物理信道模拟带宽所能获得的最终结果
5. 数字调制：比特和代表他们的信号转换的过程，有基带传输和通带传输和QAM
6. 多路复用：将多路信号（由多个信息源产生或者来自 多条线路）组合在一条物理干线（Trunk）（或者无线链路）上进行传输，分为频分FDM、波分WDM、时分TDM、码分CDM
7. 交换原因：减少网络中节点之间所需的通信线路 → 增强可扩展性,构建更大规模网络

操作：为输入数据选择输出线路/端口，在输入和输出之间建立连接，通过该连接将数据放到输出线路/端口上

交换机：网络中执行交换操作的设备。通过一系列交换机的交换操作，在两个通信节点之间建立一条数据传输路径，这条路径由物理或者逻辑上的链路组成

1. 交换分为数据报交换、电路交换、虚电路网络、消息交换网络（其中数据报（直接发送分组）交换和虚电路（建立连接在发送）属于分组交换）。分组交换：以分组为单元统计复用线路（也称为链路）资源。
2. 公式

|  |  |  |
| --- | --- | --- |
| 分组交换 | 数据报 | 无连接、健壮性（可能沿不同路径因此避开故障）  分组携带的控制信息中包含目的地址，交换机根据路由表来独立地转发分组，使用目的地址来查找  延迟包括发送+路由查找+输入输出端口链接+排队  IP网络采用数据报交换，在网络层执行交换，交换的单元为IP分组，执行交换的设备也被称为IP路由器 |
| 虚电路 | 面向连接（建立的链接叫做虚电路），有序性、基于虚电路表示执行交换，效率高  与电路交换不同，连接不是占用固定的线路资源，只是告诉网络的资源需求，在每个交换机上建立“连接状态”  TM网络采用虚电路交换，交换的单元为固定长度的ATM 信元，执行交换的设备也被称为ATM交换机  延迟=建立链接+发送延迟+断开链接 |
| 分组交换总结 | | 以分组为单元统计复用线路/链路资源。优点：线路利用率高，节点只有在有数据要传输时才占用通信线路，因此多个节点的分组可以共享一条通信线路；支持可变的数据速率。缺点：需要资源管理机制来保证数据传输的速率、延时、可靠性和有序性，增加了复杂性 |

Ch3

1. 为网络层提供的服务类型：无确认无连接、有确认无连接、面向连接
2. 数据链路层的主要功能：向网络层提供良好的服务接口、将物理层的比特流编成帧、数据帧的可靠传输即差错控制和流量控制、信道的多路访问（相关协议：HDLC、PPP、CSMA/CD、CSMA/CA）
3. 成帧的意义：物理层传输比特流时候可能发生错误，此时就要以帧为单位重发；在共享链路上，发送方以帧为单位来竞争对共享链路的访问；方法：（核心都是标识每一帧的起始与结束）

|  |  |
| --- | --- |
| 字符计数法 | 帧的帧头描述帧的长度。缺点：帧头出错不光影响本数据帧，还影响后续的帧 |
| 含字节填充的分界符法 | 帧起始和结束用特殊字节标志，称为标志字节(Flag）  若发送方数据链路层发送的数据中有标志字节，则在它前面插入转义字节（ESC），接收方的数据链路层将数据递交个网络层之前删除转义字节 |
| 含位填充的分界符法 | 帧起始和结束为特殊的位模式: 01111110。发送方出现连续5个“1”则插0 |
| 物理层编码违例法 | 使用没有用来表示数据比特的物理层比特 （即信号形式）来作为帧的起始和结束 |

1. 流量控制的意义：避免一个过快的发送方淹没接收方；方法：基于反馈（通常使用窗口机制控制）、基于速率（通过内置协议控制）
2. 差错控制：检错码、纠错码、纠删码；三种方法：ARQ-检错重发、FEC-前向纠错（不对发送方确认）、HEC-混合纠错检错

对于ARQ和HEC，如果发送的数据丢失：超时重发、对帧编号（一般是序列号）

1. 滑动窗口协议（分为选择重传与回退n）的意义：可靠、适用于各种条件的通用流量控制协议，特别是在效率、复杂性及对缓冲区的需求等方面可作灵活调配。实现链路的高效利用；通过调整发送窗口大小实现流量控制；

发送方最大帧数（B\*D为带宽与延迟）链路利用率上限）

捎带确认：为了提高效率，可以将确认信息放在数据帧中(帧头ACK域)连同数据一起发送给对方

发送窗口尺寸SWS(下边界LAR、上边界LFS), 当发送方收到发送窗口下边界帧的肯定确认时，将发送窗口整体向前滑动，从输出缓冲区中将下边界及其之前的帧副本删除;接收窗口（RWS，下LFR、上LAF）同理，收到窗口外的丢弃，窗口内的缓存，收到LFR则连带后面若干连续的递交网络层

假设序列号nbit，不发生重叠需要SWS+RWS<=2^n，SWS>=RWS一般取SWS=RWS

1. CRC：能够检测到所有的一位错误；若G（X）包含因子X+1，则可以检测到奇数个位发生错误；能检验出所有长度小于等于r的突发错误；若突发长度为r+1，当且仅当错误多项式与G（X）相同时才被整除。根 据突发错误长度的定义，其第1位和最后1位必须是1，因此与G（X）完全相同的概率即误判概率为(1/2)^r-1（所有位模式等概率） ；对于长度大于r+1的突发错误，则误判概率为(1/2)^r（所有位模式等概率）
2. 基本链路协议+全半双工、单工
3. 数据链路层协议（高级数据链路控制HDLC：采用主从结构，一个主站控制多个从，主站发命令，从站返回响应，提供基于滑动窗口、确认和超时机制的可靠数据传输，只有一个地址域，即从站的地址，在命令帧中，它是目的地址，在响应帧中，它是源地址。使用含位填充的分界符法，

根据控制域不同分为信息帧I、管理帧S监控链路，对收到帧确认、无序号帧U对数据链路附加控制

帧=帧标志序列+地址域（全1广播、全0测试地址）+控制域+校验和+帧标志序列）

（PPP由四部分组成1.串行链路上的数据的封装方法2. 链路控制协议（LCP：Link Control Protocol）用来建立、配置、测试数据链路连接 3. 认证协议(可选) 对拨号接入的用户进行认证，以便于计费，例如PAP、CHAP4. 网络控制协议NCP：对不同的网络层协议定义了对应的网络控制协议，例如IPCP

帧=flag+addr+control+protocol+信息+CRC+flag）

Ch4

基于802.3的有线局域网/以太网，基于802.11的无线局域网

1. （局域网LAN是在一个小区域范围内对各种设备提供了互连的网络）和（广播域：在局域网内目的地址为广播地址数据链路层帧会被所有的网络节点接收和处理）LAN被定义为一个广播域早期基于共享链路、现在采用L2交换机
2. IEEE 802参考模型（各子层对应的功能：物理层-用于数据传输的介质+用于设备连接的拓扑结构、介质访问控制MAC-用于共享介质的寻址和访问控制方法+差错校验、逻辑链路控制LLC-与网络层的服务接口+流量控制）

数据链路层划分成LLC和MAC的原因：在传统的数据链路控制中没有管理访问共享（广播式）介质的逻辑需求，MAC子层负责对共享介质的访问控制；对应相同的LLC可以提供不同的MAC

LLC对所有LAN相同，定义了用户之间数据交换机制，提供三种服务与ch3中的三种相同。有信息、监控、无编号三种帧）

MAC：多路访问控制（MAC对由多个节点共享的传输介质（有线介质或者无线信道）的进行访问控制。寻址：在MAC层定义了数据链路层地址，在共享介质上，节点根据帧的目的MAC地址来决定是否处理接收到的帧）。移动管理：在无线局域网中，MAC实现移动管理（切换）。经过局域网络数据链路层处理后的数据单元也被称为MAC帧，MAC帧的通用格式MAC帧=MAC控制+目的MAC地址+源MAC地址+载荷数据LLC PDU+CRC

在网络层LLC PDU=DSAP+SSAP+LLC控制+信息

对于很多数据链层协议，例如以太网，由于使用无确认无连接服务，IP分组直接封装到MAC帧中，没有LLC子层

1. 局域网网络拓扑：星型、环形、总线型、树型；传输介质：电缆、光纤、无限传输
2. MAC地址
3. 多路访问信道：多个用户共享的同一条链路，如果一个用户发送，则其它用户都能侦听到；多路访问协议：控制多个用户对多路访问信道的访问，尽量避免多个用户同时开始帧发送，因为这样会导致冲突。多路访问协议的作用就是在多个竞争的用户之间分配多路访问信道

|  |  |
| --- | --- |
| 静态分配 | 如传统的FDM或TDM，但灵活性差 |
| 动态分配 | 分为随机访问（如ALOHA、CSMA）适用于负载轻的网络  控制访问（轮询和预留两种方式，例如802.11的PCF模式、位图协议等），适用于负载重的网络得到高信道利用率 |

1. ALOHA

|  |  |
| --- | --- |
| 纯ALOHA | 每个站点只要有数据，就可在任意时间发送；通过监听信道来发现是否发生冲突；冲突，则等待一段随机时间，再重新发送；吞吐量= |
| 分槽ALOHA | 每个站点的数据发送只能在某个时槽的开始；通过监听信道来发现是否发生冲突；若冲突，则等待一段随机时间（以时槽为单位）；吞吐量= |

1. CMSA载波侦听多路访问机制

|  |  |
| --- | --- |
| 1-持续CSMA | 当一个站点要发送数据帧时，首先监听信道，若信道忙，就坚持监听，一旦检测信道空闲，就立即发送（发送概率为1）。若有冲突发生， 等待一随机长时间，然后再次检测和发送。发生冲突：信号延迟导致；多个同时监听到空闲并发送 |
| 非持续CSMA | 当一个站点要发送数据帧时，首先监听信道， 若检测到信道空闲，则开始发送；若信道忙， 则随机等待一段时间后再开始监听信道 |
| p-持续CSMA | 当一个站点要发送数据帧时，首先监听信道， 若信道忙则等到下个时槽再开始监听信道；若信道空闲便以概率p发送，而以概率q=1-p推 迟到下个时槽再重复上述过程  可以降低1-持续CSMA协议中多个站点同时发送而造成冲突的概率；采用持续监听是为了克服非持续CSMA协议带来的延迟 |

1. 802.3有线局域网络（以太网）带冲突检测的载波侦听多路访问机制CSMA/CD-（访问控制问题：在共享链路上，需要一种机制协调所有主机之间的数据发送，以公平竞争访问链路）
2. 为什么会有最大最小帧限制：最小是区分有效帧和垃圾数据，因为发生冲突返回时帧不能发送完才能被检测到；最大是因为与RAM的价格有关
3. 检测到冲突的必要条件（冲突返回时帧不能发送完）以及最小帧长计算=
4. 时间槽宽度为
5. 退避算法：当主机检测冲突后，它将等待一个随机的时间，也称作退避，第k次冲突从{0….2^(k-1)}中取一个r等待r个时间槽；k>=10保持集合不变；k>16放弃发送产生一个错误
6. 802.11无线局域网

组成：无线站点STA+无线接入点AP；网络拓扑：Ad Hoc网络，也称为自组织网络（仅由STA之间通过无线传输介质 组成的网络）、基础设施网络（STA之间不能直接通信，所有的通信都必须经过AP，每个AP都配置了一个网络名（SSID），STA必须配置和AP相同的网络名）

1. 访问控制CSMA/CA(冲突避免的载波侦听多路访问机制)用于无线局域网（原因无线无法检测CD）

包括载波侦听（站点在发送帧之前侦听无线信道是否空闲，如果是，则进入冲突避免阶段）和冲突避免（站点在发送帧之前要先等待一个帧间间隔IFS）个过程（为了防止多个站点在等待IFS时间后同时发送而导致冲突，与以太网类似，引入了一个随机退避算法来选择一个退避时间）

不同帧具有不同IFS，IFS越短优先级越高：SIFS：最高优先级，用于ACK等控制帧；PIFS：等于SIFS+1，中等优先级，用于PCF（点协调功能，轮询）操作模式下的帧；DIFS：等于SIFS+2，最低优先级，用于DCF（分布式协调功能，CSMA/CA）操作模式下的数据帧

从0到竞争窗口CW之间的随机选择一个值r，则退避时间为r倍的时槽；初始为2^k-1，下一次为2^(k+1)-1，直到Cwmax

ACK帧：不需要随机退避算法，等一个SIFS发送；发送方未收到ACK：发送方执行指数退避算法，将CW的值加倍，并且将重传计数器（有一个门限值）加1，然后重传数据帧，此时需要再次使用CSMA/CA机制竞争信道

1. MAC帧格式

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| PA-7B | SFD1 | DA6 | SA6 | LEN2 | LLC PDU | Pad | FCS4 |

PA： 先导域用于同步；SFD： 帧起始定界符；DA： 目的MAC地址； SA： 源MAC地址；LEN：数据长度（0-1500但不能小于46）；Pad：填充字段；FCS： 帧校验序列

U/L ：全局(0)还是本地管理(1)；I/G：单播(0)还是组播(1)

组播：I/G为0普通地址，为1组地址。可以将一个数据帧发送给加入组的多台主机

广播：全为1的MAC地址，以太网内所有的主机都会接收该帧

1. 扩展局域网中的帧转发

背景：冲突（碰撞）降低了链路的传输效率；链路共享其实就是带宽共享，用户的带宽得不到保障。解决：采用星型或者树型拓扑结构，用交换机或者网桥连接多用户；交换机和网桥工作在数据链路层，能隔离碰撞域

扩展局域网：一个或者多个网桥或者交换机连接的局域网集合

L2交换机（switch）源自于多端口网桥（bridge），一般采用存储转发方式将来自输入端口的帧交换到对应的输出端口，L2交换机的帧交换基于帧转发表，对于输入端口的帧，根据帧头中的目的地址查找转发表得到输出端口，帧转发表中没有对应的表项，交换机就向所有端口（除接收端口）转发

帧转发格式：每个表项由主机（一般用主机的MAC地址表示）和主机连接的端口组成；生成：源地址学习；每个表项都动态生成。

1. 生成树算法：避免出现环路导致帧永远在局域网中传递

Ch5

1. 数据报网络IP和虚电路网络ATM：是向传输层提供的有无连接到两种服务
2. 路由（找到从源主机到目的主机的 “最佳 ”路径 的过程）和转发（在路由器内部将分组从输入端口转发到输出端口的过程）

|  |  |
| --- | --- |
| 静态路由（用于用户主机、小规模网络） | 非自适应算法，事先计算好每对节点之间的“最优”路径，然后在每个路由器配置好对应的路由表 |
| 动态路由（动态性大的网络、大规模网络） | 自适应算法，根据网络拓扑结构和状态的变化动态调整 “最优”路径，反映到每个路由器就是需要动态更新路由表 |
| 数据报路由：每个分组到达时选择路由 路径，在不同时刻，为相同目的分组选 择的路由路径可能不同 | 虚电路路由：在虚电路建立过程中选择 好路由路径，接下来分组沿建立好的虚 电路路径传输 |

“最优”路径度量：跳数、物理距离、队列长度、排队延迟、可用带宽等

1. 路由算法过程1.距离矢量算法2.链路状态算法

|  |  |
| --- | --- |
| 距离矢量算法 | 每个节点都维护一个包含了到所有其它节点的“距离”的路由表，也称为矢量表；每个节点都将自己的路由表（矢量表）分发给它的邻居节点来更新路由表  故障发现与处理：节点持续发送分组检测另一个节点，收不到预习的更新则确定故障；把消息更新并设置距离无穷大  解决无穷计数问题：1. 选择一个相对小的核实数字作为无限大的代表2. 水平分割 ，当一个节点把路由更新发送给邻居节点时，它并不把从各个邻居节点处学到的路由再回送给该节点 |
| 链路状态算法 | 出现原因：网络拓扑结构发生变化后，DV需要太长时间才能收敛  1.发现邻居，了解网络地址2.设置每个节点的距离3.构建数据包4.发送接收数据包到每一个节点5.计算到每个节点的最短路径（Dijkstra） |
| 在距离矢量算法中，每个节点只和直接相连的节点进行通信，但是它把所知的全部信息（即到所有节点的距离）都告诉它们；在链路状态算法中，每个节点和其余各个节点通过扩散或者 泛洪的方式都进行通信，但是它只告诉它们自己确切知道的 信息（即与其直接相连的链路状态）；距离矢量算法只适用于小规模网络，为了避免计数到无穷问 题，网络直径一般不能超过15跳；距离矢量算法对网络变化反应较慢 | |

|  |  |
| --- | --- |
| 流量控制 | 只与发送方和接收方相关，避免快速的发送方淹没慢速的接收方 |
| 流量管理 | 确保网络能承受注入的流量，可以由网络中的设备完成，或者数据发送方完成 |
| 拥塞控制 | 与发送方和网络中的路由器相关，避免发送方的发送速率超过网络（路由器）能够承载的最大容量 |

1. 拥塞控制

|  |  |
| --- | --- |
| 虚电路 | 用户事先与网络服务提供商协商好服务等级，在虚电路建立过程中预留相应的资源；接纳控制（Admission Control）：如果网络出现拥塞，拒接建立新的虚电路；虚电路建立时绕开发生拥塞的区域 |
| 数据报 | 抑制分组1.源抑制：当路由器发生拥塞时，发送抑制分组给源主机，其中指明原分组的目的地址；源主机收到抑制分组后，减慢到指定目的地的流量2.逐跳抑制：抑制分组将对其通过的每跳都起作用 |

1. 服务质量：度量参数（带宽、延迟、抖动、丢失的QoS服务质量）

服务质量保证原则：1. 需要接纳控制机制2. 路由器需要标记分组，以区分不同类别的业务3. 针对不同类型的业务，需要相应的策略对分组进行处理，确保某些业务的带宽需求4. 当提供业务隔离时，应该尽可能地有效利用网络资源5. 需要一种策略机制来确保发送分组的主机遵循约定的带宽

1. 漏桶：当分组到达的时候，如果队列中还有空间的话，就被添加到对列的尾部，否则该分组将被丢弃；不论输入的速率为多大，输出速率始终是常数。令牌桶：允许突发流量*B+RS=MS*，B容量，R令牌到达速率，M最大输出速率，S突发时间长度。在漏桶算法中，桶中填充的是数据，所以当桶填满后将丢弃分组，而在令牌桶中，桶中填充的是令牌，所以当桶填满后将丢弃令牌，相当于是传输许可，而不是分组

|  |  |
| --- | --- |
| 流量整形 | 调节进入网络的数据流的平均速率和突发性 |
| 流量监管 | 监视用户是否遵守协议，不遵守的数据报被丢弃or标记为低优先级 |

1. 网络互连（目的：实现不同网络节点之间的通信）。分段的原因：不同网络具有不同最大数据传输单元MTU

Ch6

1. IP的优势和IP服务模型1.具有可扩展性，能解决异构性和效率问题2.以IP为核心的细腰体系架构，互连各种异构网络（向下可以互联各种通信技术的网络，向上可以承载各种类型的网络业务）3.采用基于IP的尽力服务模型（一是不可靠，即无连接无确认，二是乱序发送），实现简单，保证大规模网络下的传输效率
2. IP地址的形式：IPv4有32位，分5类，IPv4=网络号/网络前缀+主机号

配置方法（分为地区级RIR、国家级NIR、本地级LIR）：1.手动配置2.拨号用户PPP3.基于DHCP（DHCP又分为自动、动态、手动）

1. IP地址和MAC地址：作用与区别

（作用范围）IP地址在整个网络中标识不同的节点，MAC在链路或局域网内标识不同的节点

（作用）IP地址同时标识身份和位置，IP地址包含网络号，因此节点的IP与他的网络有关，而MAC只用于身份标识与节点位置无关，一般实现固化在网络设备

1. 地址解析协议ARP作用及过程：

网络寻址：数据跨网络传输基于IP地址；链路寻址：数据在网络内传输基于MAC地址。过程：1.目的IP地址所对应的主机和发送主机在同一个网络内（首先，每个主机都有ARP缓存，用来存放一些IP地址与MAC地 址的对应关系。主机根据分组头上的目的IP地址查阅自己的 ARP缓存，如果没查到，就向广播地址发送ARP请求。被请求的IP地址所对应的主机返回一个ARP响应。主机收到响应后，就可发送数据帧，并将该IP地址与MAC地址对存放在ARP缓存中）2.不在同一个（发送主机通过查找转发表得到转发的下一跳网络节点IP地址（第一 跳路由器），对该IP地址执行ARP过程，然后发送数据。第一跳路由器查找转发表得到第二跳路由器的IP地址，对该IP地址执行ARP过程，然后发送数据 .........。目的网络的路由器查找转发表知道目的节点和自己在同一个网络中，对目的IP地址执行ARP过程，然后将数据发送到目的节点）作用：ARP决定了在链路上，封装IP分组的帧会被哪个网络接口接收

1. IP分段原因及原理

每一种物理网络都会规定链路层数据帧的最大长度，称为链路层MTU.IP协议在传输数据包时，若IP数据报加上数据帧头部后长度大于MTU，则将数据报文分为若干分片进行传输，并在目标系统中进行重组。

1. 路由器对IP分组执行的操作

1.检验检校和2.TTL-1。3.重新计算检校和4.根据需要进行分段5.处理需要路由器处理的选项6.分组转发（包括根据目的IP查找转发表和交换）

1. 路由表和转发表

|  |  |
| --- | --- |
| 路由表 | 至少包含：1.目的网络（网络号or前缀）2.下一跳地址。在路由器上，一般通过路由协议来动态建立和维护路由表 |
| 转发表 | 包含比路由表更多的信息包含目的网络的网络号/前缀、输出端口和一些MAC地址  主机上的转发表通过手动orDHCP等动态配置 |
| 关系 | 转发表可以由路由表生成，在路由器上一般先由路由算法生成路由表，然后得到转发表 |

|  |  |
| --- | --- |
| IGP-内部网关路由协议 | 也称为域内路由协议，指路由选择的范围被限制在一个路由选择域内  有距离矢量协议（Bellman-Ford算法）和链路状态协议（Dijkstra（最短路径）算法）  路由信息协议RIP基于距离矢量，开放最短路径优先协议（OSPF）基于状态链路 |
| EGP-外部网关路由协议 | 也称为域间路由协议，指路由选择在不同的路由选择域中的路由器之间进行  边界网关协议BGP基于距离矢量 |

1. ICMP-internet控制保报文协议（是网络层协议，经过IP协议封装、不保证可靠传输）

作用：在网络层提供尽力服务，当分组由于各种原因被丢弃用ICMP发送差错报告。通过ICMP获得网络相关信息（可达性、网络前缀）。定义差错消息和信息消息

|  |  |
| --- | --- |
| 差错消息 | 源抑制、超时、新宿不可达、重定向、参数问题 |
| 信息消息 | 回音请求/相应、路由器发现、地址掩码请求/相应 |
| PING | 功能：测试主机的可到达性和往返延迟  ping程序采用ICMP的回音请求/响应 （Echo request/reply）报文，通过向目的主机发送回音请求，返回响应消息，来测试目的主机的可达性、往返延迟以及丢包率 |
| Traceroute | 功能：发现从源主机到目的主机路径上的网络节点  首先发送TTL=1的echo request，第一跳节点向 源端返回ICMP的Time Exceeded错误，然后发送TTL=2的echo request，第二跳节点返回 Time Exceeded错误，不断递增TTL，直到到达 目的主机 |

1. IPv4的可扩展性问题

原因：1.ip地址不够用，分配粒度太大2. 路由器特别是核心网络路由器路由表(转发表)表项急剧膨胀，从而降低路由效率

解决：1.采用层次结构（划分子网和CIDR）2.网络地址转换（重复利用某些IP地址块）

1. 划分子网步骤

确定子网号/主机号长度子网数量<=2^m，主机数量<=2^n -2；确定子网ID，确定子网掩码；确定主机号；配置转发表

1. CIDR-（无类别域间寻路）：采用可变长度的网络前缀(network prefix)来取代地址分类中网络号长度固定的做法。具有相同前缀的IP地址组成CIDR Block，表示为A.B.C.D/N，其中N为前缀长度

前缀汇聚+前缀最长匹配减少路由表表项

前缀汇集：8个连续的/24的CIDR Block（前缀）可以用一个/21的CIDR Block（前缀）来表示，因此对外汇聚成一条/21的路由

前缀最长匹配（针对汇聚时有些前缀具有不同路由的情况）：规则（在CIDR中，如果路由器上的路由表中有多条表项满足要求，则选择具有最长前缀的那条表项）

1. IPv6改进了：1. 扩展了地址空间（有128位）2. 层次化地址分配（与CIDR类似，通过前缀减少了路由表表项）3. 加那户头标（去掉了检验和、分段等路由器操作）
2. 网络地址转换-NAT：实现网络内的多台主机共享一个或者少量全局的IP地址，在内部可以使用私有地址，但私有地址不能出现在internet的数据报中

网络地址和端口转换NAPT：使用IP地址和TCP/UDP端口号，在NAT设备上，虽然内部网络所有的主机共享同一个全局IP地址，但是它们所使用的端口号不同

NAT局限性：NAPT开销大；IP地址和端口号可能存在于载荷的任何位置，因此需要软件针对具体的应用做额外的处理；并不是说有的数据都是使用UDP或者TCP来传输；破坏了原有的主机到主机的通信模型

Ch7

1. 端到端：在两个应用程序或进程之间的直接数据传输，传输层通过协议如TCP（传输控制协议）或UDP（用户数据报协议）实现这种通信，确保数据可靠性、顺序性和完整性
2. 引入传输层原因：实现运行在不同主机上的进程之间的通信；实现用户对数据传输的控制；屏蔽下层网络的异质性
3. 传输层端口寻址（TCP/UDP中的TSAP对应为端口，端口用来标识应用进程，端口号只具有本地意义，一类是知名端口，其数值一般为 0-1023，一般分配给一些常用的服务进程；另一类则是一般端口，用来随时分配给请求通信的客户进程）
4. TCP和UDP传输的数据单位为传输协议数据单位TPDU，TCP的叫TCP数据段，UDP的叫做数据报
5. TCP中连接建立和释放

TCP中连接：TCP 连接的端点称为套接口（套接口=ip+端口号）即TCP连接用五元组<源端IP地址、源端口号、目的IP地址、 目的端口号、协议>来唯一标识, 五元组常用来标识一个应用层会话（session），包括基于UDP和TCP的会话

TCP在不可靠的IP上为应用进程提供可靠的数据传输服务(包括建立连接、连接管理、连接释放)

三次握手连接建立：SYN（x）、SYN+ACK（x+1，y）、ACK（x+1、y+1）（syn数据段和SYN+ACK数据段都看做1字节数据）作用：通过三步握手，host1和host2之间完成初始序列号、窗口大小、最大数据段尺寸等参数的协商，并且分配连接所需要端点资源

TCP链接碰撞：两个host同时请求链接也能成功，因为建立的五元组唯一

使用对称释放，需要发送FIN且收到回复才能释放，两个host都需要

1. TCP释放连接相关定时器：

闲置定时器：当TCP连接断开后，为防止该连接上的数据段还在网络上，并被后续打开的相同五元组的连接接收，要设置闲置定时器以防止刚刚断开连接的端口号被立即重新使用

保持存活定时器：当一个连接长时间闲置时，保持存活定时器会超时而使一方去检测另一方是否仍然存在，如果它未得到响应，便终止该连接

1. TCP中的流量控制和拥塞控制

滑动窗口机制 ：作用（做到可靠有序传输和流量控制）解决傻瓜窗口（（接受区满了以后导致发送端一个字节一个字节发送）Nagle算法：禁止发送端发送太小的数据段；Clark算法：禁止接收端发送1个字节大小的窗口更新信息）持续定时器（解决发送端等待时接收端新的数据段丢失导致都处于等待的问题。发送端在停止后启动持续定时器，定时器满了后发送端发送1字节的探测数据段，若相应仍为0，则定时器清 0，否则则可以发送数据）重传定时器（TCP在发送数据段的同时， 启动一个重传定时器，如果在超时前该数据段被确认， 就关闭该定时器，否则重传。Timeout太长-导致发送端的等待时间太长；太短 – 重传多余的不必要的数据，RTT=αRTT+(1- α)M，Timeout=βRTT，α一般7/8；D= αD+(1- α)|RTT-M|，Timeout=RTT+4D，α一般3/4）重发后要保持RTT值不变（发送端无法区分ACK是对哪次发送的TCP数据段的确认）ACK延时定时器（当TCP实体收到数据段时它必须返回确认，但并不需要立即回复）选择确认SACK（接收端收到序列号不连续的数据段，把这些信息准确地告诉发送端）

慢启动和拥塞避免（接收窗口 rwnd和拥塞窗口 cwnd，发送窗口的上限值=Min[rwnd, cwnd]）慢启动（设置慢启动阈值ssthresh，拥塞窗口初始化为该连接最大数据段的长度，发送端发送一个最大数据段，得到确认后，其拥塞窗口大小加倍，依次类推，直到发送端认为出现数据段丢失或已达到接收窗口大小）拥塞避免（拥塞窗口增长到ssthresh时，就每次将拥塞窗口加1，如果出现超时或者认为发送的数据段出现丢失时，就将当时拥塞窗口值减半，作为新的ssthresh，同时将拥塞窗口变为1）

加法增大（是指执行拥塞避免算法后，在收到对所有数据段的确认后（即经过一个往返时间），就把拥塞窗口增加一个 MSS）乘法减小（不论在慢启动阶段还是拥塞避免阶段，只要出现一次超时或者认为发送的数据段出现丢失时，就把慢启动阈值ssthresh设置为当前的拥塞窗口乘以 0.5）

AIMD（Additive Increase加法增大, Multiplicative Decrease乘法减小）

快速恢复算法：发送端收到连续三个重复的确认-乘法减小-不执行慢启动算法（cwnd从新的ssthresh开始）-加法增大/拥塞避免

快速重传算法：乘法减小-执行慢启动算法

1. TCP序列号与速率之间的关系

Ch8本章都在客户/服务器模式下

1. 域名系统DNS：负责域名的维护和管理（域名由点和符号构成成员名<=63字符，全长<=255字符）。引入原因：可扩展性问题：1）数量庞大，维护开销大，容易成为性能瓶颈 2）名字管理困难，难以避免重名冲突

需要DNS的服务：www服务、文件传输、电子系统服务

DNS做到层次化命名空间（命名机制遵循的是组织边界）和管理分布化（以域为单位，在网络中分布多个服务器对域名进行管理，这些服务器也被称为名字服务器，某个域如果设置了名字服务器，则该服务器负责此域下的子域的域名的管理）

1. 域名查询类型

迭代查询：本地名字服务器如果没有域名对应的记录，就向更高层次的名字服务器请求，被请求的名字服务器如果也 没有该域名对应的记录就会返回一个可供查询的名字服务器地址。递归查询：被请求的名字服务器如果没有域名所对应的记录，它就会向其它域名服务器查询，并沿着查询的路径逐个返回记录

1. 万维网WWW：由庞大的、分布在世界各地的web页面的集合组成，web页面编写采用HTML等语言；客户端（浏览器）采用HTTP协议访问；使用超链接技术，用户可以访问一个又一个web页面，超链接也用URL；使用URL命名万维网上的各种web页面

URL（统一资源定位符）：每个页面在整个Internet的范围内具有惟一的标识符即URL；URL=<协议>://<主机域名>:<端口>/<路径及文件名>（协议包括FTP、HTTP、mailto；路径及文件名省略则指向缺省页面）

HTTP超文本传输协议：是www能够可靠交换文件的基础，传输层使用TCP协议，工作中客户/服务器模式；有请求消息和响应消息两类

1. 电子邮件

协议：消息交换协议（发送emali的简单邮件传输协议SMTP、接收email的邮局协议POP3和IMAP）、消息格式协议（基本的ASCII文本邮件，多用途Internet邮件扩展MIME）

POP：使用客户/服务器的工作方式；一般假设用户从服务器上把邮件下载到本地主机上，用户对邮件的操作在本机进行

IMAP：邮件存储在邮件服务器上，用户本机IMAP客户端操作与邮件服务器同步

Ch9

1. 网络威胁：非授权访问、信息泄露、拒绝服务。安全服务：鉴别/认证、机密性、完整性、不可否认性。安全性、功能性和易用性
2. 按体质分为对称密钥体制与非对称密钥体制，按模式分位序列、分组密码

|  |  |
| --- | --- |
| 对称密钥体制 | 加密密钥和解密密钥相同，又叫单钥密码体质。包括DES（分组密码）、AES、IDEA  缺点：密钥管理量大，当用户量增大时，密钥空间急剧增大；对称算法无法实现抗否认需求；发送接收方有一个秘密通道共享一个密钥空间 |
| 非对称密钥体制 | 加密密钥和解密密钥不同，又叫双/公钥密码体质。包括RSA、ElGamal、椭圆曲线密码  优点：密钥分为公钥和私钥；需要保存的密钥量大大减少；可以实现数字签名—抗否认，可满足不相识的人之间保密通信；加密速度慢，常用于数字签名或加密对称密钥 |

1. 数字签名系统

要求：不可抵赖、可验证、不可复制、不可篡改

原理：公钥密码体制的一个重要应用就是数字签名，数字签名就是利用私钥生成签名，而用公钥验证签名。由于无法识别数字签名与其拷贝之间的差异，所以，在数字签名前应加上时间戳。但是基于公私钥的加密算法速度慢。

使用单向散列函数（有128bit的MD5、160bit的SHA-1，可以对一个长消息中计算出一个固定长bit串称为MD）的RSA签名：只对信息摘要（MD）进行签名

1. 网络安全相关协议

IPSec-网络层、TLS/SSL-传输层、SHTTP-应用层、S/MIME-应用层；HTTPS与SHTTP是不同的: HTTPS是HTTP over TLS,它依赖于TLS来提供安全的传输服务, HTTP本身没有变化，而SHTTP则是一个应用层安全协议,在HTTP的基础增加了安全性

知道两个IPSec（提供了一个基于IP的网络架构）相关协议：安全服务协议（认证头标AH和封装安全净荷ESP）、密钥协商和管理（internet安全关联和密钥管理协议ISAKMP）

|  |  |
| --- | --- |
| AH | 保证消息完整性，抗重播攻击，但不提供机密性保护  认证范围（IP头标中可变域除外）（认证范围=IP头+AH头+TCP/UDP头+净荷） |
| ESP | 除了保证消息完整性，抗重播攻击，还保证消息的机密性，机密性可以采用3DES等对称加密算法来实现  认证范围不包括IP头标（范围=ESP头+TCP/UDP头+净荷+ESP尾+ESP（认证数据）） |

拒绝服务攻击DoS：过量使用资源导致其他合法用户无法访问；特点：简单有效难以防范；eg：TCP SYN Flood（攻击者：发送大量伪造的用于TCP连接请求的SYN数据段，源IP地址常常是伪造的；目标机：存在大量的半开连接，耗尽系统资源而无法 处理正常连接建立请求）

防火墙的功能：抵挡各种网络攻击的防范手段；过滤不安全的服务和禁止非法访问；控制对特殊站点的访问，可以允许受保护网络的一部分主机被外部访问，而其它部分则禁止；提供访问记录和审计等功能

防火墙分类：分组过滤、状态检测、代理型

DMZ：听获取，一般放置internet上主机能访问的web、FTP服务器

Intranet：受保护的内部网络，禁止internet上的主机直接访问

IDS（入侵检测系统）：通过从计算机网络或计算机系统中的若干关键点收集信息，并对其进行分析，以发现网络或系统中是否有违反安全策略的行为和遭到袭击的迹象；功能：监控网络和系统、发现入侵企图与异常现象、实时报警

DIDS（分布式入侵检测系统）：部署在多个节点上，通过这些节点间的协作来实现快速可靠入侵检测

IPS（入侵防御系统）：等效于防火墙＋IDS，但：IDS一般并联在网络上，被动地监测网络，当检测到入侵时可能来不及做出反应，而IPS串连在网络上，能够在线拦截入侵，预防入侵行为的发生

|  |  |
| --- | --- |
| 物理层 | 功能：激活物理连接以便传送数据；原始比特流传送，分为同步传送和异步传送模式，全双工和半双工传送模式；物理层连接去激活。协议：接口物理规范，设备间信号的传送方式，包括调制方式、编码和使用信号处理与传输线路的特性匹配。设备：信号放大器（Amplifier）、集线器（Hub）。介质：电缆、光纤、无线电波 |
| 数据链路层 | 功能：发送方成帧和接收方帧定界；处理帧破坏、丢失和重复所出现的问题；流量控制：如何避免一个快速的发送方淹没掉一个慢速的接收方；信道（链路）多路访问：；广播式网络中的共享信道的访问控制；广播式网络：所有节点通过一条共享链路连接。相关协议：高级数据链路控制规程HLDCP，点对点协议PPP，CSMA/CD，CSMA/CA。数据链路层的数据传输单元称为帧。设备：网桥（Bridge）、（L2）交换机（Switch）、无线接入点AP |
| 网络层 | 功能：网络互连：处理不同网络互连中存在的问题；路由：根据数据的目的地址，确定到目的网络的“最佳”路 径 ；拥塞控制：网络中出现过多分组如何处理。协议：ATM：发送数据之前需要在发送主机和接收主机之间建立连 接，数据单元为固定长度的信元，信元中携带连接标识，沿 建立好的连接投递；IP：发送数据之前不需要建立连接，数据单元称为分组，大 小可变，分组中携带目标主机地址，可沿不同路径到达目的主机。设备：路由器/L3交换机/ATM交换机 |
| 传输层 | 功能：向上层提供不同类型的传输服务，例如可靠的或者不可靠的；端到端（end-to-end），在两个端点的主机上运行，而不在中间路由器运行；端到端流量控制。服务：面向连接，在数据传输开始之前通过连接建立过程在两个端点 之间协商参数（流量控制参数、最大传输单元等）；无连接，在数据传输开始之前通过连接建立过程在两个端点 之间协商参数（流量控制参数、最大传输单元等）。网络中处理传输层及传输层以上协议数据的设备通称为网关（Gateway） |
| 会话、表示、应用 | 会话：允许不同主机上的用户之间建立会话；会话通常是指各种服务，包括对话控制，记录该由哪一 方来传输数据，令牌管理，禁止双方同时执行同一个关 键操作，以及同步功能。表示：控制数据格式，例如文本、视频、音频或者图像，确保 来自发送主机的数据能够被接收主机理解；表示层还和数据加密和压缩相关。应用：定义了满足各种应用需求的协议 |

|  |  |
| --- | --- |
| 主机到网络层 | 主机通过某个协议连接到网络上，以便将分组发送到 网络上；在Internet中通常将一个广播域称为一条链路，与一 般OSI参考模型中的链路不同。Internet中数据传输的一跳（One Hop）指跨越一个广播域 |
| 互联网层 | 功能上对应着OSI参考模型的网络层。主要是IP协议，因此也称为IP层。它的任务是将分组投递到最终的目的地，提供的是一种无连接的不可靠传输 |
| 传输层 | 功能上对应着OSI参考模型的传输层。定义传输控制协议TCP用户数据报协议UDP。不同的应用可以选择不同的传输服务 |
| 应用层 | 包括了所有的高层协议，没有ISO模型中的会话层和表示层。域名系统DNS：域名⇓→IP地址；HTTP协议：WWW应用；FTP协议：文件传输应用；telnet协议：远程登录应用；SMTP协议：发送电子邮件。应用程序不仅仅要实现相应的应用层协议， 还包括为用户提供操作界面等于其它功能 |

实验：

Exp1：Linux命令行与IP组网

1. PacketTracer搭建网络拓扑结构，分别采用静态路由以及RIP两种方法实现
2. Kernel是操作系统的一层, 它将硬件与计算机上运行的主要程序连接起来；Shell是实际处理命令和返回输出的程序；Terminal是指一个运行shell的包装程序
3. net.ipv4.ip\_forward是一个内核参数，用于控制是否允许IP数据包的转发。当设置为1时 ，表示启用IP转发，即允许Linux系统将从一个网络接口接收的数据包转发到另一个网 络接口。这通常用于路由器或网关设备，它们需要将数据包从一个网络转发到另一个 网络。默认情况下，这个参数是关闭的（设置为0），因为大多数非路由设备不需要转 发数据包。 对于网关设备，通常需要将net.ipv4.ip\_forward设置为1。
4. 交换机接口：通常提供相同类型的接口，如全为以太网端口（10/100/1000Mb ps）或光纤端口等。这些接口用于连接同一网络内的设备，如电脑、打印机等。主要功能是转发数据帧。交换机通过学习MAC地址表来决定将 数据帧转发到哪个接口。 路由器接口：可能包括不同类型的接口，以适应不同的网络环境。除了以太网端口， 还可能有串行接口（Serial）、光纤接口（如SFP、GBIC）、无线接口等，用于连接不 同类型的网络，如广域网（WAN）。功能：不仅转发数据包，还涉及数据包的路由选择。路由器接口会根据路由表 来决定数据包的下一跳地址。

Exp2：

1. struct sockaddr\_in结构体中：1.short sin\_family 表示地址族，本实验中IPv4指定的事AF\_INET  2.u\_short sin\_port 表示端口号 3.struct sin\_addr 表示IP地址 4.char sin\_zero[8] 用来填充剩余空间的0
2. 连接的客户端和非连接的客户端在建立socket时有什么区别：（1）family都使用了AF\_INET表示使用网络协议IPv4且仅限于IPv4 （2）type面向连接的客户端使用了SOCK\_STREAM流套接字,面向连接的套接字,提供可靠的面向流的服务，而面向非连接的客户端使用 SOCK\_DGRAM: 数据报套接字,无连接的套接字, 不能保证顺序和可靠性（3）protocol面向连接的客户端使用了IPPROTO\_TCP，TCP协议, 流套接字的默认协议 ；而面向非连接的客户端使用了IPPROTO\_UDP ，UDP 协议, 数据报套接字的默认协议
3. TCP：（1）优点：可靠性高，面向连接的通信提供了可靠的数据传输服务，确保数据包按顺序到达，没有丢失或重复；通过流量控制机制、拥塞控制机制提高网络的稳定性和效率（2）缺点：建立连接的过程可能会引入额外的延迟；资源消耗，需要更多的资源来建立和维护连接（3）适用于：需要可靠数据传输的应用；对数据传输的顺序和完整性有严格要求的场景

UDP：（1）优点：无连接通信不需要建立连接，因此通常具有较低的延迟和较高的传输速度；协议实现相对简单；资源少（2）缺点：不保证数据的可靠传输；缺乏流量控制和拥塞控制（3）适用于：实时性要求高的应用；可以容忍一定数据丢失的场景

4. 本实验过程中使用的socket工作在阻塞方式。阻塞方式：当socket工作在阻塞模式时，如果调用如accept、connect、recv或send等函数，且当前不能满足执行条件（例如，没有数据可读或写缓冲区满），则当前线程会被挂起，直到条件满足或超时。 阻塞方式的优点是编程模型简单，易于理解和实现。缺点是可能会造成资源浪费。非阻塞方式：在非阻塞模式下，如果调用上述函数时条件不满足，函数会立即返回一个错误码，而不会阻塞当前线程。 非阻塞方式的优点是可以提高程序的并发性能，因为线程可以继续执行其他任务，而不是等待I/O操作完成。缺点是编程模型复杂，需要处理异步逻辑，可能需要使用多线程或I/O多路复用技术来管理多个非阻塞socket。

Exp3：RDT

1. RDT底层是UDP, 为什么程序中可以用recv/send而不是recvfrom/sendto收发数据

在RDT协议的实现中，由于通信双方已经建立了连接，即已经知道对方的地址信息，因此可以使用recv和send函数来简化操作。

1. 停等发送端程序中是如何实现超时重传：停等协议中在一个while(1)中一直发送同一个RDT数据包，在发送一检查poll的状态，如果state == 0，则说明超时，此时需要continue操作即可进入下个while循环，如果state == 1，说明数据发送成功，此时使用break结束发送这个RDT数据包的while循环，即可进入下一个RDT数据包的发送
2. 超时重传机制保证双方正确地结束通信
3. 在选择重传协议中, 为何窗口大小必须小于或等于序列号空间大小的一半：串口大小太多，会导致序列号空间有限，不断递增出现回绕，序列号重叠的现象。

Exp4：

1. HTTP中的幂等（Idempotence）是指一个操作，不论执行多少次，其结果都是相同的。也就是说，多次执行一个幂等操作，和只执行一次的效果是一样的，不会改变资源的状态。
2. GET：在HTTP协议中，GET请求用于从服务器检索数据。GET操作是幂等的，这意味着无论你执行多少次GET请求，它都不会改变服务器上的数据或资源状态。多次执行相同的GET请求，服务器的状态保持不变，返回的结果也相同。POST：POST请求用于向服务器提交数据，通常用于创建新的资源或引发服务器上的状态变化。由于POST操作可能会改变服务器的状态，因此它通常不是幂等的。如果你多次执行相同的POST请求，可能会导致服务器上创建多个资源或引发多次状态变化，这与幂等性的定义相违背。
3. 不同：HTTPS抓包的都是已加密内容，不能直接读取，而HTTP则可以直接读取其中的内容。

原因：HTTPS抓到的数据包与HTTP抓到的数据包的主要区别在于加密和安全性。HTTPS通过SSL/TLS协议对传输的数据进行加密，这使得数据在传输过程中是安全的，不易被窃取或篡改。而HTTP协议以明文方式发送内容，不提供任何方式的数据加密，因此安全性较差，如果攻击者截取了传输报文，就可以直接读懂其中的信息。

此外，HTTPS默认使用443端口，而HTTP默认使用80端口。HTTPS还提供了身份验证机制，通过数字证书验证服务器的身份，防止中间人攻击和伪装。

1. 从输入网址, 到浏览器显示网页, 在应用层依次发生：解析网址- DNS解析-建立连接-发送HTTP请求-服务器处理请求-生成HTTP响应-浏览器接收响应-渲染网页-执行JavaScript-加载资源-完成加载

IP头标格式：版本号（VERS）4bits，IPv4写4，Ipv6写6。2.IP分组头长度，4bits，单位4字节，取值5-15，标准为20字节。3.服务类型（TOS）：优先级+延时+吞吐量+可靠性。4.总长度、16b标识符、3b标志（无作用+DF+MF）、13b段偏移5.TTL：单位s，标识分组的生存时间，没经过一个路由器-1，为0是丢弃分组6.Protocol标识封装在IP分组中的载荷的协议类型header checksum检校和7.source IP：分组的源地址8.destination IP 目的地址9.padding，分组头必须为4字节整数倍，不够时做填充10.options选项（包括安全性、严格/松散的源路由选择、路由记录、时间标记）对于header checksum，由于TTL每个路由器变换因此每次都重新计算