2019 年计网期末复习
by @LeBlanc the Deceiver

第一章 计算机网络和因特网
1.3 网络核心
1.3.1 分组交换（不预留资源，需排队）
1. 报文->分组。分组交换机=路由器+链路层交换机。
2. 存储转发传输：缓存完该分组的所有比特后，才能向出链路转发转发。存储转发时延 d=N*L/R。
3. 输出缓存/输出队列。排队时延。分组丢失/丢包。
4. 转发表。转发选择协议。
1.3.2 电路交换（预留资源）
1. 端到端连接。频分复用-带宽。时分复用-帧-时隙。静默期。
2. 区别分组交换&电路交换：①分组交换提供了更好的带宽共享；②分组交换更简单；③分组交换按需分配链路使用，性能更好。
1.3.3 网络的网络
1. 网络结构 1。单一的全球 ISP 去连接所有的接入 ISP。客户。供应商。
2. 网络结构 2。多个互联的全球 ISP+接入 ISP。区域 ISP（每个区域一个）。第一层 ISP。
3. 网络结构 3。多个第一层 ISP+多个区域 ISP（每个区域多个）+接入 ISP。
4. 网络结构 4。存在点 Pop。多宿。对等。因特网交换点 IXP。
5. 网络结构 5。在 4 的顶部增加内容提供商网络。

1.4 分组交换网中的时延、丢包、吞吐量
1.4.1 分组交换网中的时延概述
1. 节点总时延（单台路由器上）=处理时延+排队时延+传输时延+传播时延。
2. 对比传输时延&传播时延。
3. 最大吞吐量
1.4.2 排队时延和丢包
1. 流量强度=La/R。大于 1。≤1。周期性。突发性。平均排队时延与流量强度的关系。
2. 流量强度↑，分组丢失的比例↑。
1.4.3 端到端时延
1. 端到端时延=N（处理时延+传输时延+传播时延）。此时排队时延忽略不计。
2. 其他时延：共享媒体有意时延、媒体分组化时延（IP 语音）
1.4.4 计算机网络中的吞吐量
1. 瞬时吞吐量。平均吞吐量。
2. 瓶颈链路。共享链路的干扰流量。

1.5 协议层次及其服务模型
1.5.1 分层的体系结构
1. 分层。服务：①在这层中执行了某些动作；②使用直接下层的服务。改变服务的实现，而不改变服务本身。服务模型。分层的缺点：①冗余较低层的功能；②某层的功能可能需要仅在其它某层才出现的信息（如时间戳值），这就违背了层次分离。协议栈。自顶向下方法。
2. 应用层-报文-软件。HTTP、SMTP、FTP，DNS。
3. 运输层-报文段-软件。TCP、UDP。

4. 网络层-数据报-软件&硬件。IP、路由选择协议。
5. 链路层-帧-网络接口卡。以太网、DOCSIS 协议。网络层将受到多个不同链路层协议的不同服务。
6. 物理层-比特-网络接口卡。链路相关的、与实际传输媒体（铜、电）相关。
7. 开放系统互联模型 OSI。+表示层+会话层。

1.5.2 封装

1. 源（5 层）。链路层交换机（2 层）。路由器（3 层）。链路层交换机可以识别以太网地址，不能识别 IP 地址。
2. 应用层报文。传输层报文段。网络层数据报。链路层帧。
3. 每一层：分组=首部字段+有效载荷字段（来自上一层的分组）。

第二章 应用层

2.2 Web 和 HTTP

2.2.1 HTTP 概况

1. HTTP=客户程序（Web 浏览器）+服务器程序（Web 服务器）。报文。
2. Web 页面=HTML 基本文件（1 个）+引用对象（多个）
3. URL 地址=存放对象的服务器主机名+对象的路径名。
4. 请求报文。相应报文。TCP 连接。套接字接口。无状态协议。
5. 分层结构的优点：①HTTP 协议不担心数据丢失；②HTTP 协议不关注 TCP 从网络的数据丢失和故障中恢复的细节。
6. HTTP 与客户如何解释 web 页面无关，HTTP 只定义了 HTTP 客户程序和 HTTP 服务器程序之间如何通信。

2.2.2 非持续连接和持续连接（HTTP 默认）

1. 非持续连接：每个 TCP 连接在服务器发送一个对象后关闭，且每个 TCP 连接之传输一个请求报文和一个相应报文。
2. 往返时间 RTT。三次握手。HTTP 总响应时间=RTT*2+服务器传输 HTML 文件的时间。
3. 非持续连接的缺点：①必须为每一个请求的对象建立一个全新的连接；②每一个对象经受 RTT*2 的交付时延，一个用于 RTT 创建连接，另一个 RTT 请求和接收一个对象。
4. （持续连接时）若一条连接经过一定的时间间隔（可配置）仍未被使用，则 HTTP 服务器关闭此连接。

2.2.3 HTTP 报文格式

1. **HTTP 请求报文**=请求行+首部行+空行+实体体（GET 时为空，POST 时为用户输入值）。
2. 请求行=方法字段+URL 字段+HTTP 版本字段。
3. 方法字段：GET、POST、HEAD（开发者调试，仅返回响应，不返回请求对象）、PUT（上传对象到服务器的指定目录）、DELETE（删除服务器上的对象）。
4. Host: 对象所在的主机。Connection: close 非持续连接。User-agent: 浏览器类型。Accept-language: fr 用户想得到该对象的法语版本。
5. 用户提交表单：①POST 实体体；②GET+URL 扩展。
6. **HTTP 响应报文**=状态行+首部行+实体体。
7. 状态行=版本字段+状态码+状态信息。
8. Connection: close 非持续连接。Date: 服务器发送响应报文的时间。Server: 服务器类型。Last-Modified: 对象创建或最后修改的时间。Content-Length: 被发送对象的字节数。Content-Type: 对象的文件类型，注意，必须用这个首部行而不能用文件扩展名。
9. 状态码：200OK 请求成功。301MovedPermanently 请求的对象已被永久转移，新的 URL

定义在响应报文的 Location: 中，客户浏览器可自动获取。400BadRequest 该请求不能被服务器理解。404NotFound 所请求的文档不在服务器上。505HTTPVersionNotSupported 服务器不支持请求报文使用的 HTTP 协议版本。

2.2.4 cookie->标识一个用户

1. cookie=HTTP 响应报文中的 cookie 首部行+HTTP 请求报文中的 cookie 首部行+用户浏览器中储存的 cookie 文件+web 站点的后端数据库。

2. Set-cookie: 1678。Cookie: 1678。

2.2.5 Web 缓存

1. Web 缓冲器/代理服务器。

2. 部署 web 缓冲器的优点：①大大减少对客户请求的响应时间，特别是客户与初始服务器之间的瓶颈带宽远低于客户与 web 缓冲器之间的瓶颈带宽时。②大大减少一个机构的接入链路到因特网的通信量，因此不必增加带宽，降低了费用。③从整体上大大降低了因特网上的 web 流量，改善了所有应用的性能。

3. 内容分发网络：安装许多地理上分散的缓冲器，使大量流量本地化。

2.2.6 条件 GET 方法：允许缓冲器证实它的对象是最新的

1. 条件 GET 方法=请求报文使用 GET 方法+请求报文中包含“If-Modified-Since: ”

2. 304NotModified: 缓存器可以使用该对象

2.4 DNS：因特网的目录服务

2.2.1 DNS 提供的服务

1. 主机标识方法：主机名、IP。域名系统 DNS：DNS 服务器、应用层协议。DNS 运行中 UDP 上，53 号端口。

2. 主机别名。规范主机名。邮件服务器别名。负载分配。

2.4.2 DNS 工作机理概述

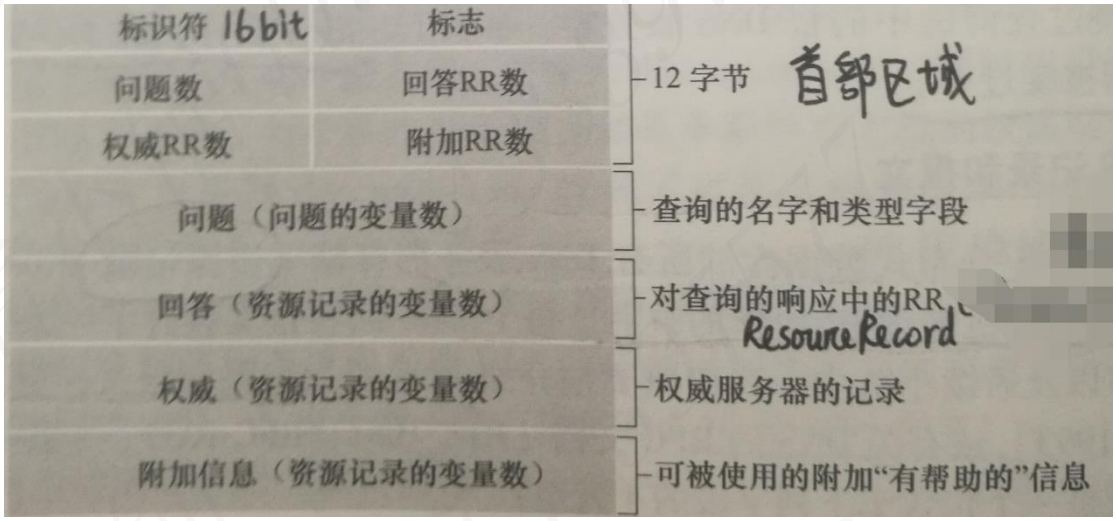
1. 集中式 DNS 设计的缺点：单点故障、通信容量、远距离的集中式数据库、维护。分布式层次数据库。

2. 根 DNS 服务器。顶级域 DNS 服务器（TLD）。权威 DNS 服务器。本地 DNS 服务器。递归查询。迭代查询。

3. DNS 缓存。优点：①改善时延；②减少在因特网上传播的 DNS 报文的数量。DNS 服务器在一段时间后会丢弃缓存的信息。

2.4.3 DNS 记录和报文

1. 资源记录 RR=(Name, Value, Type, TTL)。Type 类型：A 标准主机名->IP 地址。NS 域->权威 DNS 服务器的主机名。CNAME 主机别名->标准主机名。MX 邮件主机别名->标准主机名。



2. 查询报文&回答报文=首部区域（标识符字段、标志字段：查询/回答、权威的、希望递归、递归可用）+问题区域（名字字段、类型字段）+回答区域（可包含多个 RR）+权威区域+附加区域。nslookup 程序。

3. 注册登记机构。提供基本&辅助权威 DNS 服务器的名字、IP 地址。将 web 服务器的 A 资源记录和邮件服务器的 MX 资源记录输入权威 DNS 服务器中。

4. DNS 脆弱性：①分布式拒绝服务（DDoS）带宽洪泛攻击。向根服务器发送大量分组。分组过滤器的保护、本地 DNS 服务器缓存了顶级域名服务器的 IP 地址，绕过了根服务器。②向顶级域名服务器发送。不像根服务器那样容易绕过。③中间人攻击，返回伪造回答，重定向到攻击 web 站点。

2.7 套接字编程：生成网络应用

网络应用=编写客户程序代码+服务器程序代码。分类：开放的&专用的。

2.7.1 UDP 套接字编程：必须把目的地址附在分组上

1. 目的地址=目的主机 IP+目的地套接字的端口号。（UDP 代码完成）
2. 源地址=源主机 IP+源套接字的端口号。（底层操作系统自动完成）
3. 客户发送报文前，服务器必须已作为进程运行。P107 实例。

2.7.2 TCP 套接字编程：只需经过套接字把数据丢进 TCP 连接

1. 客户发送报文前，服务器必须已作为进程运行。
2. 欢迎套接字 serverSocket。连接套接字 connectionSocket。
3. 区别 UDP&TCP 请求报文：①TCP 需要先创建 TCP 连接。②TCP 不需附上目的地址，而 UDP 需要。
4. 区别 UDP&TCP 响应报文：①TCP 不需附上 clientAddress，而 UDP 有。②TCP 将 sercerSocket 套接字与端口号绑定后，还需 serverSocket.litsen(1)，然后 connectionSocket, addr=serverSocket.accept()。③TCP 中，服务器发送完成后，连接套接字关闭，而欢迎套接字保持打开。

第三章 运输层

3.3 无连接运输：UDP

1. UDP 的优点，某些应用更适合 UDP 的原因：①TCP 有拥塞控制，而 UDP 没有。应用不希望时延，可以容忍数据丢失。#UDP 应用也可以实现可靠性，在应用程序自身建立可靠性即可。②UDP 无需建立连接，没有时延。③UDP 不用维护连接状态，不用跟踪这些参数。④

UDP 首部开销小，仅 8 字节，而 TCP 需 20 字节。
2. UDP 的缺点：①UDP 没有拥塞控制，可能有高丢包率。②挤垮 TCP。
3.3.1 UDP 报文段结构=源端口号+目的端口号+长度+检验和

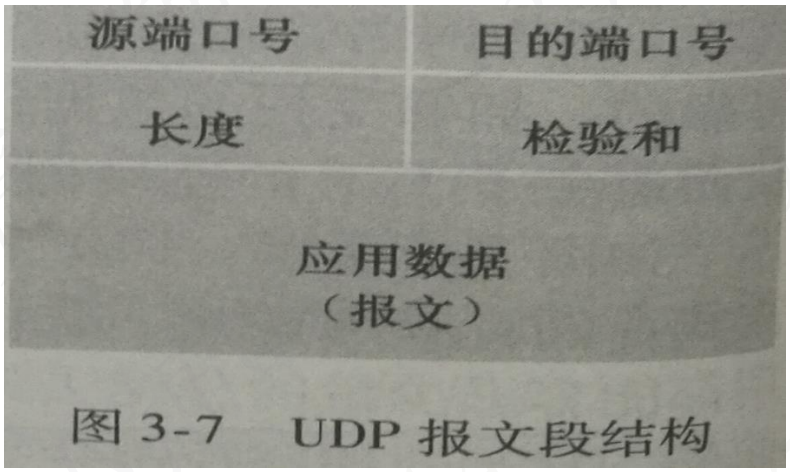


图 3-7　UDP 报文段结构

3.3.2 UDP 检验和（UDP 只有差错检测，没有差错恢复）
1. 算法：对所有 16bit 的字求和，若溢出则回卷，最后反码。接收方加起来得 1111（16 个 1）
2. 端到端原则：①不能保证源和目的地之间的所有链路都提供差错检测。②报文段存储在路由器时可能引入比特差错。

3.4 可靠数据传输原理
3.4.1 构造可靠数据传输协议
1. rdt1.0：底层信道完全可靠。有限状态机 FSM。
2. rdt2.0：有比特差错，但按序。肯定确认。否定确认。自动重传请求协议 ARQ：差错检测、接收方反馈、重传。停等协议：发送方只有在确认接收方已正确接收当前分组时（收到 ACK 后），才会发送新数据。冗余分组。序号。rdt2.1。rdt2.2。
3. rdt3.0/比特交替协议：比特差错+丢包。丢包=发出的分组、传回的 ACK。冗余数据分组。倒计数定时器。性能的核心：停等。
3.4.2 流水线可靠数据传输协议
1. 发送方利用率=(L/R)/(RTT+L/R)。流水线。
2. 每个分组唯一序号。双方缓存多个分组。差错恢复：回退 N 步 GBN、选择重传 SR。
3.4.3 回退 N 步协议/滑动窗口协议
1. 基序号 base。下一个序号 nextseqnum。窗口长度 N。序号范围[0, 2^k-1]
2. GBN 发送方需响应：上层的调用。收到一个 ACK，累积确认。超时事件。GBN 接收方丢弃所有失序分组，不需要缓存。基于事件的编程。
3. GBN 缺点：当串口长度和带宽时延很大时，一个分组的差错就能引起 GNB 重传大量分组。
3.4.4 选择重传 SR
1. 发送方：逐个确认正确接收的分组，仅重传出错的分组。接收方：确认分组，缓存失序的分组。正确接收&正确收到。接收方必须重新确认已收到过的那些序号小于当前窗口基序号的分组。
2. SR 窗口≤½序号空间大小。若 SR 窗口太大：不知道是新分组还是重传。
#窗口长度：接收方接收报文的能力、网络拥塞程度 来决定。
#避免分组重新排序：在分组的存活时间内，不能重用序号。

3.5 面向连接的传输：TCP

3.5.1 TCP 连接

1. 仅在端系统中，中间（路由器、交换机、中继器）无关。全双工服务。点对点。三次握手。

2. 发送缓存。MSS 最大报文段长度 1460。MTU 最大传输单元 1500。TCP 报文段。

3.5.2 TCP 报文段结构=源端口号、目的端口号、序号、确认号、首部长度、保留未用、标志字段（ACK、RST、SYN、FIN、CWR、ECE、PSH、URG）、接收窗口(rwnd)、检验和、紧急数据指针、选项、数据。

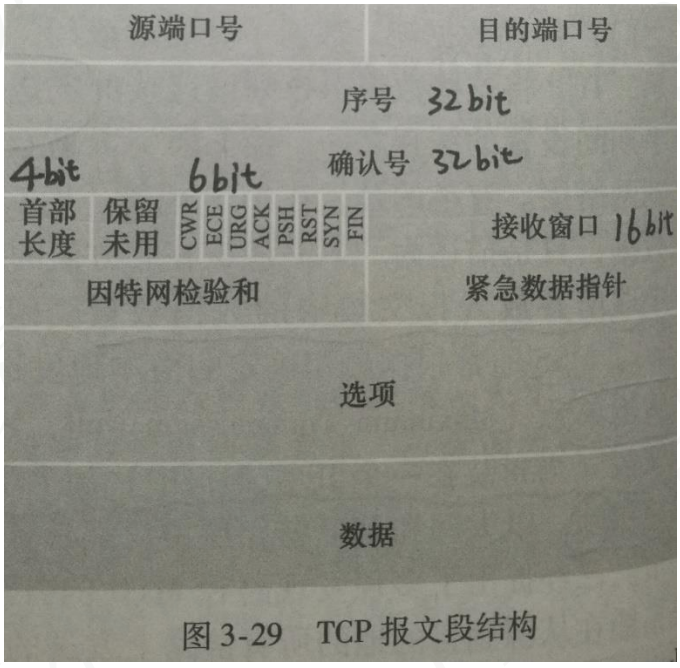


图 3-29 TCP 报文段结构

1. 序号（字节流）。确认号。累积确认。双方可随机选择初始序号。

2. 回显。捎带。

3.5.4 可靠数据传输。

1. 网络层/IP 服务是不可靠的。TCP 提供可靠数据传输服务：无损坏、无间隙、非冗余、按序。单一重传定时器。

2. TCP 发送方：从上层接收数据、定时器超时、收到 ACK。超时间隔加倍。

3. 快速重传：在超时发生之前检测到丢包，一旦收到 3 个冗余 ACK，就执行快速重传。TCP 不使用否定确认，而使用冗余 ACK。

4. 区别 TCP 与 GBN：①相同点：TCP 发送方只需要维护 SendBase 和 NextSeqNum，GBN 发送方只需要维护窗口的上下边界+nextseqnum 在窗口中的位置。②不同点：若丢失 n(n<N)，GBN 将重传 n,n+1,n+2,…,N，而 TCP 只重传 n，甚至不重传（对 n+1 的 ACK 在 n 超时之前到达）。对 TCP 优化：累积确认->选择确认。

3.5.5 流量控制：速度匹配　　#拥塞控制：若网络拥塞，则遏制发送方

1. 接收窗口 rwnd。LastByteRcvd-LastByteRead ≤ RcvBuffer。Rwnd= RcvBuffer-(LastByteRcvd-LastByteRead)。发送方：LastByteSent-LastByteAched≤rwnd。

2. UDP 没有流量控制，缓存会溢出并丢失。

3.5.6 TCP 连接管理

1. 三次握手。SYN 报文段，SYN=1，seq=client_isn。服务器分配缓存、变量。SYNACK 报文段，SYN=1，seq=server_isn，ack=client_isn+1。客户分配缓存、变量。第三次握手：SYN=0，seq=client_isn=1，ack=server_isn+1.

2. TCP 关闭。FIN=1。TIME_WAIT。TCP 状态。
3. SYN 洪泛攻击：发送大量 SYN 报文段，但不完成第三次握手，服务器为这些半开连接分配大量资源。SYNcookie。
4. 请求的端口号与服务器的套接字不匹配：①TCP：发送 RST 报文段。②UDP：发送 ICMP。
5. nmap 扫描：源收到 SNYACK；收到 RST->不匹配，但未被防火墙；没收到->有防火墙。

3.6 拥塞控制原理
3.6.1 拥塞原因与代价
1. 两个发送方+无穷大缓存路由器。每连接的吞吐量。当分组的到达速率接近链路容量时，排队时延巨大。
2. 两个发送方+有限缓存路由器（缓存满时丢弃新到分组）。供给载荷。发送方必须重传以补偿因缓存溢出而丢弃的分组。发送方遇到大时延的不必要重传导致路由器转发不必要的分组副本。
3. 多个发送方+多个有限缓存路由器。当分组被丢弃时，每个上游路由器用于转发该分组的传输容量被浪费了。
3.6.2 拥塞控制方法
1. 端到端拥塞控制（TCP）。网络辅助的拥塞控制（可用比特率 ATM）：直接通知、经接收方反馈。

3.7 TCP 拥塞控制：加性增乘性减 AIMD
1. TCP 发送方如何限制其发送速率：拥塞窗口 cwnd。LastByteSent-LastByteAched ≤ min{cwnd, rwnd}
2. 发送方如何感知出现了拥塞：丢包=超时+3 个冗余 ACK。自计时。
3. 发送方发现拥塞后，采用什么算法来改变发送速率：丢失->拥塞，降速；ACK->加速；带宽检测。 #TCP 分岔：减少时延，前端服务器
4. TCP 拥塞控制算法：慢启动、拥塞避免、快速恢复。
5. 慢启动。指数级。结束：①超时，cwnd 重置为 1MSS，ssthresh=½cwnd。②当 cwnd=ssthresh 时，拥塞避免。③3 个冗余 ACK，快速重传，快速恢复。
6. 拥塞避免： 超时比 3 个冗余 ACK 剧烈。
7. TCP Vegas 算法：观察 RTT 以预测拥塞，在分组丢失之前就线性降低发送速率。
8. 吞吐量两极值：½W/RTT- W/RTT。平均吞吐量=0.75 W/RTT=1.22MSS/(RTT √L)。丢包率 $L=1/(3W^2/8+3W/4)$.
3.7.1 公平性
1. 瓶颈链路（较小 RTT 抢到更高吞吐量）。45°，减半，波动。
2. UDP 没有拥塞控制，不公平。UDP 源可能压制 TCP 流量。
3. TCP 有并行连接。
3.7.2 明确拥塞通告：网络辅助拥塞控制。
1. 明确拥塞通告。
2. 经接收方反馈。路由器发出 ECN，接收方发出 ECE，发送方回答 CWR。

第四章 网络层：数据平面
4.3 网际协议：IPv4、寻址、IPv6 及其他
4.3.1 IPv4 数据报格式
1. 版本、首部长度、服务类型（TOS）、数据报长度（首部+数据，字节）、标识标志片偏移、

寿命 TTL、协议（使用哪种运输层协议）、首部检验和（每台路由器需重新计算，因为 TTL）、源和目的地址、选项、数据（有效载荷）。

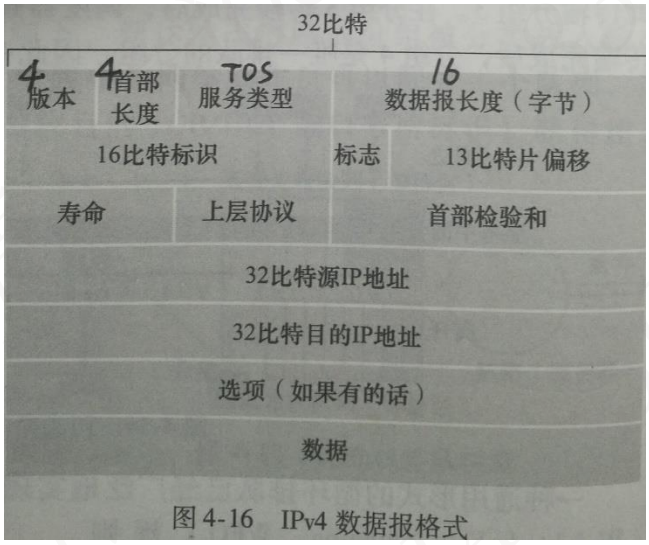


图 4-16　IPv4 数据报格式

4.3.2 IPv4 数据报分片

1. 最大传输单元 MTU：帧。不同链路层协议导致不同的 MTU。片。标识、标志（最后一片为 0）、片偏移。

2. 分片的优点：①减小时延；②避免因单比特差错重传整个大文件；③避免小文件在大文件后排队。分片的缺点：①按序；②首部开销。

4.3.2 IPv4 编址

1. IP 地址与接口关联。32bit/4 字节。点分十进制记法。子网。子网掩码。CIDR 无类别域间路由选择：因特网的地址分配策略。前缀/网络部分。地址聚合/路由聚合/路由摘要。最长前缀匹配。分类编址（ABC 类）。IP 广播地址 255.255.255.255。

2. 动态主机配置协议 DHCP/即插即用协议/零配置协议。DHCP 服务器、DHCP 中继代理。步骤：DHCP 服务器发现（广播）、DHCP 服务器提供（IP 地址租用期）、DHCP 请求、DHCP ACK。缺点：当节点在子网间移动时，不能维持与远程应用之间的 TCP 连接（解决：移动 IP）。

4.3.3 网络地址转换 NAT

1. 专用网络（10.0.0.0/24 仅在给定的网络中才有意义）。中间盒。NAT 转换表：端口号 16bit、IP 地址。缺点：对运行在家庭网络中的服务器会出现问题。解决：NAT 穿越、通用即插即用。

2. 防火墙：检查首部，拒绝可疑。入侵检测系统 IDS：特征数据库。

4.3.5 IPv6

1. 增加：扩大的地址容量 128bit，任播。40 字节首部。流（付费、音频）。

2. IPv6：版本、流量类型、流标签、有效载荷长度、下一个首部（交付给哪个运输层协议）、跳限制、源地址和目的地址、数据。

2. 删去：分片、首部检验和、选项。#IPv4 路由器可以分片，但组装只能在端系统中。IPv6 路由器既不能分片也不能组装。

3. 建隧道：IPv4 向 IPv6 迁移。

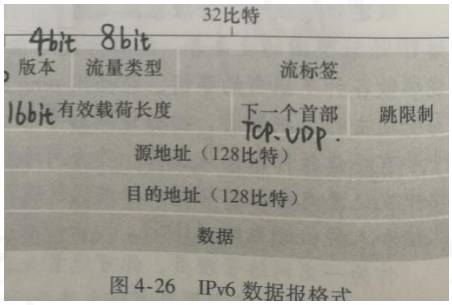


图 4-26 IPv6 数据报格式

第五章：网络层：控制平面

#每路由器控制、逻辑集中式控制

5.2 路由选择算法

1. 图 G=(N,E)，开销。邻居。路径。最低开销路径。

2. 路由选择算法分类：①集中式路由选择算法（链路状态算法 LS）、分散式路由选择算法（距离向量算法 DV）。②动态、静态路由选择算法。③负载敏感（链路开销动态反映了低层链路的拥塞水平）、负载迟钝算法。

5.2.1 链路状态路由选择算法 LS

1. 链路状态广播。Dijkstra 算法。迭代。初始化+循环。N 个节点：搜索节点总数 N(N+1)/2，最差时复杂度 $O(N^2)$，发送 O(N*E)个报文。拥塞敏感，导致振荡。避免自同步：每台路由器发送链路通告的时间随机化。

5.2.2 距离向量路由选择算法 DV

1. 分布式、迭代、异步。最低开销 dx(y)=minv{c(x,v)+dv(y)}。仅当检测到直接相连的链路开销发生变化、从邻居接收到更新，才重新计算自己，若变化，则向邻居发送。

2. 路由选择环路。无穷计数。解决：毒性逆转（≥3 个节点时无效）。

3. 区别 LS&DV：报文复杂性、收敛速度（DV 慢）、健壮性（LS 好）。

5.3 因特网自治系统内部的路由选择：OSPF

1. 自治系统 AS。优点：规模太大时算法失效、管理自治。

2. 开放最短路优先 OSPF。完整拓扑图、周期性广播。优点：安全（简单鉴别、MD5 鉴别）、多条相同开销的路径分摊流量、综合支持单播和多播、支持单个 AS 中的层次结构（主干区域、区域边界路由器）。

5.4 ISP 间的路由选择：BGP

1. 自制系统间路由选择协议。边界网关协议（所有 AS 运行相同）。

5.4.1 BGP 的作用

1. （x, I）（前缀，接口号）。作用：①从邻居 AS 获得前缀的可达性信息。②选择到该前缀的最好路由。

5.4.2 通告 BGP 路由信息

1. 网关路由器。内部路由器。外部 BGP 连接 eBGP-长虚线、内部 BGP 连接 iBGP-短虚线（不总是与物理链路对应）。

5.4.3 确定最好的路由

1. 路由=属性+前缀=NEXT-HOP+ASPATH+目的前缀。

2. 热土豆路由选择。自私的。

3. BGP 实际使用规则不自私：①本地偏好；②最短 ASPATH。用 DV 算 AS 跳的跳数。③热土豆，选最靠近 NEXT-HOP 的路由。④BGP 标识符。

5.4.4 IP 任播

1. 常用于 DNS：①替换不同位置不同服务器上的相同内容。②让用户从最靠近的服务器访问内容，这些服务器都使用相同 IP 地址。如：将 DNS 请求指向最近的根 DNS 服务器。
2. 缺点：相同 TCP 连接的不同分组可能到达不同 Web 服务器。
5.4.5 路由选择策略
1. 多宿接入 ISP。（毒性逆转）维持客户/供应商关系。
2. 区别 AS 内&AS 间路由选择协议：策略（AS 间重策略）、规模（AS 内可扩展性不重要）、性能（AS 间轻性能）
5.4.6 拼装在一起：在因特网中呈现
1. 获得因特网连接，与本地 ISP 签约。网关路由器。ISP 提供 IP 地址范围并用 BGP 向其他 ISP 通告我的前缀，IP 地址我自行分配。
2. 购买域名，提供 DNS 服务器的 IP 地址。在 DNS 服务器中存储主机到 IP 的映射。
5.7 网络管理和 SNMP
1. 管理服务器+被管设备（被管对象）+管理信息库 MIB+网络管理代理（进程）+网络管理协议 SNMP（应用层协议）。
2. SNMP：请求响应模式、陷阱报文。
3. PDU 类型：GetRequest. GetNextRequest. GetBulkRequest. InformRequest. SetRequest. Response. Trap。
4. SNMP PDU 使用 UDP 传输，不可靠。请求编号、响应、超时、重传。

第六章 链路层和局域网
6.2 差错检测和纠正技术 #差错检测和修正比特 EDC
6.2.1 奇偶校验
1. 单比特奇校验。单比特偶校验。只能检验奇数个比特的差错。不能纠正。
2. 二维奇偶校验。检测并纠正单个差错，检测出多个差错单不能纠正。
3. 前向纠错：减少重传次数，允许接收方立即纠正。
6.2.2 检验和方法（运输层）
1. 因特网检验和。运输层用软件，开销小。链路层 CRC 因为有专用硬件。
6.2.3 循环冗余检测编码 CRC/多项式编码
1. 生成多项式 G。求 R=(D 左移 r 位)/G。可检测≤r 比特的差错，以概率 1-0.5^r 检测到大于 r+1 比特的差错。可检测任何奇数个比特的差错。

6.3 多路访问链路和协议
1. 点对点链路&广播链路。多路访问问题。碰撞。
6.3.1 信道划分协议
1. TDM-时间帧-时隙，R/N 速率限制，总是等待轮次。FDM-带宽。码分多址 CDMA：每个节点用自己唯一的编码对发送的数据编码。
6.3.2 随机接入协议：总是以 R 全速发送，碰撞则重发，重发前等待随机时延
1. 时隙 ALOHA 协议：节点同步，等待后重传。优点：唯一活跃节点以 R 全速发送、高度分散。缺点：碰撞、部分时隙空闲。成功时隙。效率=Np(1-p)^(N-1)。P=1/N 时取最大效率 1/e。
2. ALOHA 协议：碰撞后立即重发。效率 p(1-p)^(2N-2)。最大效率 1/2e。
3. 载波侦听多路访问 CSMA->以太网。载波侦听。碰撞检测。信道传播时延。二进制指数后退：n 次碰撞后，从{0,1,2,⋯,2^n-1}选一个 K 值，间隔 K*512 比特时间后重发。效率=1/(1+5*Dprop/Dtrans)，Dprop 是传输任一信号所需的最大时间，Dtrans 传输一个最大长

度帧的时间。Dprop 趋近 0，Dtrans 趋近无穷大时，效率均为 1.

6.3.3 轮流协议

1. 轮询协议。主节点。优点：①消除了碰撞、空时隙，效率高；②M 个活跃节点，吞吐量 R/M。缺点：①轮询时延。②主节点故障则崩溃。

2. 令牌传递协议：仅当需发送时才能持有令牌帧。优点：分散、效率高。缺点：单节点故障使全局崩溃、某节点忘释放令牌需调用恢复。

6.4 交换局域网

6.4.1 链路层寻址和 ARP

1. 交换机没有 MAC 地址(透明)。主机/路由器->适配器/接口->链路层地址/MAC 地址/LAN 地址/物理地址。6 字节，16 进制表示。MAC 广播地址 FF-FF-FF-FF-FF-FF.

2. 需要 MAC 地址的原因：①局域网除了 IP 还适用于其他网络层协议；②网络层地址必须存在适配器中，适配器移动需重新配置。③主机将被每个帧中断。

3. 地址解析协议 ARP。ARP 表：IP、MAC、TTL 寿命。#DNS 可为任何主机，ARP 仅为同一子网解析 IP 地址。ARP 查询报文-广播帧，ARP 响应报文-标准帧。

4. 发送到子网外：ARP 到路由器，路由器转发。

6.4.2 以太网（无连接、不可靠有间隙）

1. 优点：第一个，管理员熟悉、简单便宜、效率高、硬件普及便宜。总线拓扑、星型拓扑、集线器、交换机。

2. 以太网帧结构：前同步码 8 字节（7 个 10101010 同步时钟）、目的地址 6、源地址 6、类型 2（用哪个网络层协议）、数据 46-1500（分片、填充）、CRC4。

3. 速率 10、1000、1000、10G。BASE 以太网。T 铜线。交换机无碰撞，不必使用 MAC。

6.4.3 链路层交换机

1. 过滤。转发。交换机表：MAC 地址、接口、TTL。自学习。即插即用。双工：能同时发送和接收。

2. 优点：缓存帧以消除碰撞、链路隔离、网络管理(检测问题并内部断开)。

3. 区别交换机&路由器：都有流量隔离。①交换机优点：即插即用、只到第二层则过滤和转发速率快。缺点：为避免广播帧循环只能是生成树、大量 ARP 报文、广播风暴单点导致整体崩溃。②路由器优点：拓扑不限制为生成树且可选最优路径、防火墙避免广播风暴。缺点：非即插即用、到第三次速度慢。

6.4.4 虚拟局域网 VLAN。VLAN 干线连接。VLAN 标签。标签协议标识符。