计算机网络复习纲要

软日1009出品
刘毅，胡俊宇，王琰，王领，方强

目　　录

1 计算机网络和因特网

1.1 什么是协议

为计算机网络中进行数据交换而建立的规则、标准或约定的集合。

1.2 分组/电路交换

电路交换：电路交换在通信之前要在通信双方之间建立一条被双方独占的物理通路（由通信双方之间的交换设备和链路逐段连接而成），从而在这条链路上的数据交换成为电路交换。

分组交换：分组交换也称包交换，它是将用户传送的数据划分成一定的长度，每个部分叫做一个分组。在每个分组的前面加上一个分组头，用以指明该分组发往何地址，然后由交换机根据每个分组的地址标志，将他们转发至目的地，这一过程称为分组交换。

1.3 网络传输中的时延

1. 处理时延：检查分组首部和决定将该分组导向何处所需要的时间。
2. 排队时延：在队列中，当分组再链路上等待传输时，他经受排队时延。
3. 传输时延：将所有分组的比特推向链路路所需要的时间。
4. 传播时延：从该链路的起点到目的路由器传播所需要的时间是传播时延。

1.4 吞吐量

吞吐量可近似为沿着源和目的地址之间路径的最小传输速率。

1.5 ISO / OSI参考模型

1. 物理层：透明地传输比特流。
2. 数据链路层：同一物理介质上的两个接口之间的数据传输；地址标识方法；数据单元表示（帧格式）；差错检测/校正；流量调节；介质访问控制。
3. 网络层：因特网上的任何两个计算机之间的分组传输；地址标识；分组转发；路由发现。
4. 传输层：因特网上的任何两个进程之间的可靠数据传输；流量调节。
5. 会话层：对通信对象进行统一编码。
6. 表示层：向应用进程提供信息表示方式，使不同表示方式的系统之间能进行通信。
7. 应用层：各类应用软件，确定进程之间通信的性质以满足用户的需要。

2 应用层

2.1 C/S 与 P2P 的比较

1. C/S结构是一种客户端/服务器结构，客户端与服务器之间是主从关系，是一种一对多的模式。它的信息和数据需要保存在服务器上，若用户要浏览和下载信息，必须先访问服务器，才能浏览和下载信息，而且客户机之间没有交互的能力。相反，P2P模式不分提供信息服务器和索取信息的客户端，每一台电脑都是信息的发布者和索取者，对等点之间能交互，无需使用服务器。

2. C/S模式中信息的存储和管理比较集中、稳定，服务器只公布用户想公布的信息，并且会在服务器中稳定地保存一段时间，该服务器通常也不间断的运行在网络间。而P2P缺乏安全机制，P2P是能给用户带来方便，但也会带来大量垃圾信息，而且各个对等点可以随便进入或者退出网络，会造成网络的不稳定。

3. 从安全的角度来说，因为系统会出现漏洞，而C/S 模式采用集中管理模式，客户端只能被动地从服务器获取信息，所以一旦客户端出了差错，并不会影响整个系统。

4. C/S模式的管理软件更新的较快，要跟上技术，必须花费大量精力和金钱在软件的更新换代上，而且工作人员要维护服务器和数据库，也要耗费大量资金。相反的P2P 不需要服务器，也就不必耗费大量资金，而且每个对等点都可以在网络上发布和分享信息，这使得闲散资源得以充分的利用。

2.2 套接字

多个TCP连接或多个应用程序进程可能需要通过同一个 TCP协议端口传输数据。为了区别不同的应用程序进程和连接，许多计算机操作系统为应用程序与TCP／IP协议交互提供了称为套接字(Socket) 的接口。

2.3 Web应用和HTTP协议

2.3.1 定义

Web的应用层协议是超文本传输协议(HTTP)，他是Web的核心。

2.3.2 特点

1. HTTP使用的是TCP协议作为他的支持运输层协议

2. HTTP服务器并不保存关于客户机的任何信息，他是一个无状态协议。

3. 分为非持久连接和持久连接

4. 使用cookie 来把内容与用户关联起来，记录用户状态。

5. 使用Web缓存可以大大减少对客户及请求的响应时间，还可以大大减少一个机构内部网域内特网接入链路上的通信量，不必急于增加带宽，从而降低费用，改善性能。

2.4 文件传输协议FTP

2.4.1 特点

1. 使用两个并行的TCP链接来传输文件，一个是控制连接，一个是数据连接，因为FTP协议使用了一个分离的控制连接，所以我们也称FTP是带外传送的。
2. 在整个会话期间保留用户的状态信息，是一个有状态协议。
3. 控制连接贯穿了整个用户会话期间，但是针对会话中的每一次文件传输都需要建立一个新的数据连接（即数据连接是非持久的)。

2.5 因特网中的电子邮件

2.5.1 SMTP 与HTTP的区别

1. SMTP是一个推协议，HTTP 是一个拉协议。
2. SMTP要求每个报文都是用7位ASCII码格式。HTTP 没有这个限制。
3. 在处理既包含文本又包含图形的文档时，SMTP把所有报文对象放在一个报文之中，HTTP 把每个对象封装到他自己的HTTP 响应报文中。

2.5.2 MIME

支持发送非ASKII文本格式，即支持附件。

2.5.3 POP3

POP3是一个非常简单的邮件访问协议，它使用的是下载并删除的方式来访问邮件服务器，这让如果用户希望从不同的机器访问他的邮件报文，如从办公室的PC、家里的PC或他的便携机来访问邮件。如果最先是从他办公室的PC机上收取了一个邮件，那么用户回到家时，通过他的便携机将不能再次收取该邮件。为了解决这个问题，出现了IMAP 协议。

2.5.4 IMAP

IMAP服务器把每个报文与一个文件夹联系起来，当报文第一次到达服务器时，它是放在收件人的收件箱文件夹里。收件人则可以把邮件移到一个新的、用户创建的文件夹中，或阅读邮件，删除邮件等，IMAP 协议为用户提供了创建文件夹以及在文件夹之间移动邮件的命令。

2.6 DNS

2.6.1 定义

DNS是一个有分层的DNS 服务器实现的分布是数据库。是一个允许聚集查询分布是数据库的应用层协议。DNS协议一般运行在UDP之上。其用于把主机名解析为IP 地址。

2.6.2 服务器类型

根DNS服务器，顶级域服务器，权威DNS服务器，本地DNS服务器

2.6.3 递归查询与迭代查询

一般来说，主机到本地DNS服务器的查询是递归的，其余的查询是迭代的。

2.7 P2P应用

2.7.1 定义

在P2P文件分发中，每个对等方都能够重新分发其所有的该文件的任何部分，从而协助服务器进行分发。即每个对等方既是客户机又是服务器。

2.7.2 最稀罕优先

根据他没有的块从他的邻居中确定最稀罕的块（最稀罕的块就是他在邻居中拷贝数量最少的那些块），并优先请求那些最稀罕的块。按照此方式，最稀罕的块更迅速的重新分发，其目标大致是均衡每个块在洪流中的拷贝数量。

2.7.3 搭免费车

是指对等方从文件共享系统中下载文件而不上载文件。其解决办法是利用BitTorrent中的一种机灵的兑换算法。其基本想法是Alice确定其邻居的优先权，这些邻居是那些当前能够以最高的速率共给他数据的。特别是，Alice对于他的每个邻居持续测量接收到的比特的速率，确定以最高速流入的四个邻居。然后，他将数据块发给这四个邻居。每过十秒，它重新计算给速率并可能修改这四个对等方，每过三十秒，Alice 将随机的选择一名新的兑换伙伴进行兑换。如果这两个对等方满足此兑换要求，那么他们会将对等方放入其前四位列表中并继续与对方进行兑换，知道对等方之一发现了一个更好的伙伴为止。因此Alice为了能在一段较长的时间内以较快的速率从Bob 下载比特，就必须同时以一种较快的速率向Bob上载比特。

2.7.4 在P2P区域中搜索信息

集中式索引，查询洪泛，层次覆盖

3 运输层

3.1 多路复用与多路分解

运输层协议只工作在端系统中（即TCP/UDP不在路由等设备中占有任何资源)。

3.1.1 多路复用

从源主机的不同数据套接字中搜集数据块，并为每个数据块封装上首部信息从而生成报文段，然后将报文段传递给网络层。

3.1.2 多路分解

将运输层报文段中的数据交付到正确的套接字。

3.1.3 多路分解实现条件

1. 主机上每个套接字被分配一个端口号。
2. 每个报文段具有源端口字段和目的端口字段。
3. 报文到达主机，有运输层检查报文的目的端口号，并定向到相应的套接字。

3.1.4 端口号

16bit大小的数字，0–1023为周知端口号

3.2 UDP

3.2.1 UDP的优点

1. 运输层能更好地控制要发送的数据和发送时间。
2. 无需连接建立。
3. 无连接状态，不用缓存和拥塞控制等，以便支持更多的活动客户机。
4. 分组首部开销小。

3.2.2 UDP报文结构

共8字节。源端口号（2字节)、目的端口号（2字节)、长度（2字节)、检验和（2字节)。其中UDP检验和，对报文段中的所有16位比特字求和，进位回卷，对和进行反码运算，结果作为检验和部分。

3.3 可靠传输原理

3.3.1 GBN

GO BACK N(GBN):常被称为滑动窗口协议。

基序号（base）：最早的未确认分组序号。

下一个序号（nextseqnum）：最小的未使用序号。

N：窗口长度。

GBN响应以下三类事件：

1. 上层的调用：若发送窗口未满，则发送，否则返回数据给上层
2. 收到ACK：若是一个失序的分组则丢弃，并为最近按序接受的分组重传ACK（比如已经收到分组0,1,2,3,4，下一个应该收5，却收到了6，丢弃，并返回ACK4）累积确认，便是接收方已正确收到序号n以前的所有分组
3. 超时事件：重传所有已发送单还未被确认的分组

3.3.2 SR

选择重传（SR）:要求接受方逐个地确认正确接受的分组，仅重传可能出错了的分组。

选择重传同样响应以下三类事件：

1. 从上层收到数据：同GBN。
2. 超时：每个分组有自己的定时器，只发送超时的分组。
3. 收到ACK：若该分组在窗口内，则标记为已收，若该分组序号等于base,则窗口后移至具有最小序号的未确认分组处，同时用多出来的序号发送未发送数据。

由于发送方窗口和接收方窗口会出现不一致的情况，为保证不出现问题，窗口长度必须小于或等于序号空间大小的一半（原因详见课本152、153页三个图）。

3.4 TCP

3.4.1 TCP特点

全双工，端对端，都有发送缓存和接收缓存。

3.4.2 TCP头

在不包含选项时是20字节。源端口号（2字节）、目的端口号（2字节）、序号（4字节）、确认号（4字节）、首部长度（4位）、保留未用（6位），标志字段（6位），接收窗口（2字节），检验和（2字节），紧急数据指针（2字节）

序号：不是报文段的编号，而是该报文段首字节流的编号。

确认号：期望收到的下一个字节序号。

序号和确认号不好区分，我的个人理解是序号为我给你的当前这个报文的起始号，而确认号是我希望得到你给我的数据的起始地址。

3.4.3 快速重传

快速重传：只返回对下一个有序报文的ACK，三次冗余的ACK 即重传。

3.4.4 流量控制服务

消除发送方使接收方缓存溢出的可能（不同于拥塞控制）。

3.4.5 TCP建立过程

1. 客户机发送一个SYN报文段。
2. 服务及收到该报文，为该TCP分配缓存和变量，并发送允许连接的报文，SYN=1。
3. 客户机收到后，也要分配缓存和变量。发送一个报文，确认建立连接，SYN=0。

3.4.6 TCP关闭过程

请求方发送一个FIN=1的报文，接收方收到后返回ACK，并发送一个FIN报文，请求方收到该报文后，也发送一个ACK。所有资源释放。

3.5 拥塞控制

3.5.1 拥塞网络的开销

1. 当分组到达速率接近链路容量时，分组经历的巨大排队延时。
2. 发送方必须执行重传以补偿因为缓存溢出而丢弃的分组。
3. 发送方在遇到延时所进行的不必要重传引起的路由器利用其他链路宽带来转发不必要的分组拷贝。
4. 当一个分组沿一条路径被丢弃时，每个上游路由器用于转发该分组到丢弃该分组而使用的传输容量被浪费。

3.5.2 TCP拥塞控制

加性增、乘性减、慢启动、对超时事件作出反应。

1. 加性增、乘性减:当TCP发送方感受到端到端路径无拥塞时就加性增加其发送速率，当察觉到路径拥塞时（通过丢包事件）就乘性地减小其发送速率。

2. 慢启动：TCP发送方在初始阶段不是线性地增加其发送速率，而是以指数的速度增加，直到发生一个丢包事件为止。

3. 对超时事件作出反应：TCP发送方在一个超时事件发生后就进入慢启动阶段，从而对超时事件做出反应p。

4 网络层

4.1 虚电路网络和数据报网络

4.1.1 虚电路网络

仅在网络层提供连接服务的计算机网络（ATM，帧中继），通讯前需预先建立逻辑连接的虚电路。整个通讯过程分为：虚电路建立，数据传输与虚电路拆除阶段。报文分组不必带目的地址、源地址等辅助信息。节点只要做差错检验，而不需要做路径选择。但当线路中单个节点失效会造成整个虚电路失效。

4.1.2 数据报网络

仅在网络层提供无连接服务的计算机网络（因特网是数据报网络)。数据报网络中，分组传输之间不需要预先建立线路连接，每个分组都可以独立选择传输路径，每个分组在通信子网中可能是通过不同的传输路径到达目的主机。但可能出现乱序，重复与丢失现象。每个分组必须带有目的地址与原地址，传输延迟较大，适用于突发性通信不适用于长报文，会话式通信。

4.2 路由器

4.2.1 路由器体系结构

1. 输入端口。

2. 交换结构：将路由器的输入端口连接到它的输出端口（一台路由器中的网络)。内存，纵横制，总线。

3. 输出端口。

4. 选路处理器：维护选路信息与转发表，并执行路由器中的网络管理功能。

5. 输入输出端口缓存量。

4.3 IP（因特网中的转发和编址）

4.3.1 网络层三个主要组件

IP协议，选路组件，互联网控制报文协议（ICMP）

4.3.2 差错检验

为什么TCP/IP在运输层与网络层都执行差错检验?

答：首先，在IP层只对首部进行了检验，而TCP/UDP检验和是对整个TCP/UDP报文段进行的。其次，TCP/UDP与IP不一定属于同一个协议栈。

4.3.3 IP数据报分片

一条链路层帧能承载的最大数据量叫做最大传输单元（MTU)。

为了让目的主机执行这些重新组装任务，IPv4设计者将标识、标志和片偏移字段放在IP数据报中。见书P219表4-2，注：片偏移字段的单位是8字节。

4.3.4 IPv4 编址

每个IP地址32比特，一般按点分十进制记法的方式书写。

因特网的地址分配策略被称为无类别域间选路（CIDR）,CIDR将子网寻址的概念一般化了。因为对于子网地址，32 比特的IP地址被划分为两部分，并且也具有点分十进制形式a.b.c.d/x，其中x指示了在地址的第一部分中的比特数。(第一部分网络地址，第二部分主机地址)

4.3.5 可变长子网掩码

RFC 1878中定义了可变长子网掩码，VLSM 规定了如何在一个进行了子网划分的网络中的不同部分使用不同的子网掩码。这对于网络内部不同网段需要不同大小子网的情形来说很有效。VLSM可以对子网进行层次化编址，这种高级的IP寻址技术允许网络管理员对已有子网进行划分，以便最有效的利用现有的地址空间。

子网掩码：网络地址全为1，主机地址全为0

4.3.6 IP地址分类

A:1.0.0.0–127.255.255.255

B:128.0.0.0–191.255.255.255

C:192.0.0.0–223.255.255.255

D:224.0.0.0–239.255.255.255

E:240.0.0.0–255.255.255.254

4.4 DHCP动态主机配置协议

DHCP协议的4个步骤

1. DHCP服务器发现：新到达的主机在UDP分组中向端口67 发送DHCP发现报文（DHCP客户机生成包含DHCP 发现报文的IP数据报)，其中使用广播地址255.255.255.255 并且使用“本主机”源地址0.0.0.0。

2. DHCP服务器提供：DHCP服务器收到一个DHCP发现报文时，用一个DHCP提供报文对客户机做出响应，仍然使用IP广播地址255.255.255.255。p每个服务器提供报文中含有收到的发现报文的事物ID，向客户机推荐的IP地址，网络掩码以及IP地址租用期。

3. DHCP请求：新到达的客户机从一个或多个服务器中选择一个，并用一个DHCP请求报文对选中的服务器进行响应，配置参数。

4. DHCP ACK：服务器用DHCP ACK报文对DHCP 请求报文进行响应，证实所需求得参数。

4.5 网络地址转换（NAT）

NAT路由器对外界的行为就如同一个具有单一IP地址的单一设备。NAT路由器维护一张NAT 转换表，表项中包含了端口号和IP地址，保证路由器一侧的家庭网络与外界的通讯。 NAT穿越正越来越多地由通用即插即用（UPnP）提供，UPnP是一种允许主机发现并配置邻近NAT的协议。UPnP 要求主机和NAT是UPnP 兼容的。

4.6 ICMP：互联网控制报文协议

ICMP报文有一个类型字段和一个编码字段，并且包含引起该ICMP报文首次生成的IP数据报的首部和前8字节内容。

4.7 IPv6

4.7.1 IPv6的改进

1. IPv6简化了IP分组的首部格式.

2. IPv6增强了对进一步扩展的支持。

3. IPv6增强了对QoS (Quality of Service) 的支持。

4. IPv6增强了对安全的支持。

5. IPv6增加了对 Anycast 通信方式的支持。

4.8 IPv4到IPv6的迁移

1. 双栈：IPv6节点也具有完整的IPv4实现，这样的节点被称为：IPv6/IPv4节点，它有发送和接受IPv4 与IPv6 两种数据报的能力。确定另一个节点是IPv6 使能的还是仅IPv4 的，通过DNS来解决。

2. 建隧道：我们将两台IPv6路由器中间的IPv4 路由器集合称为一个隧道。该隧道的发送端可以将整个IPv6 数据报放到IPv4数据报的数据（有效载荷）字段中。接受端的IPv6 节点收到该IPv4数据报，再从中取出其中的IPv6数据报。

4.9 IPv4与IPv6的区别

1. IPV6地址长度由32比特增加为128比特。
2. 首部由以前的20-60字节，变为高效的40字节。取消了选项字段。
3. IPv6在路由器中禁止分片。取消首部检验和。
4. IPV6简化了报文头部格式，字段只有7个，加快报文转发，提高了吞吐量；
5. 提高安全性。身份认证和隐私权是IPV6的关键特性。
6. 支持更多的服务类型；
7. 允许协议继续演变，增加新的功能，使之适应未来技术的发展。

4.10 选路算法

4.10.1 分类

根据全局性还是分布式分类：

1. 全局选路算法：用完整的、全局性的网络知识来计算从源到目的之间的最低费用路径。这就要求在算法真正开始计算以前以某种方式获得这些信息。实际上，具有全局状态信息的算法常被称作链路状态算法（LS）。
2. 分布式选路算法：以迭代的、分布式的方式计算出最低费用路径。没有节点拥有所有网络链路费用的完整信息，而每个节点仅有与其直接相连链路的费用知识即可开始工作。距离向量选路算法（DV）就是分布式的。

4.10.2 链路状态选路算法（LS 算法）

类似Dijkstra 算法，书P240例子

4.10.3 距离向量选路算法（DV 算法）

类似Floyd 算法，书P243-P245例子

4.11 因特网中的选路

4.11.1 自制系统（AS）

一组在相同管理下的路由器组成。

4.11.2 网关路由器

负责向本AS之外的目的地转发分组的路由器

4.11.3 热土豆选路

当AS中的几个网关路由器都能到达目的地x，该要发送的分组经离它路径费用最小的网关路由器转发。

4.11.4 因特网中的自治系统内部选路

1. 选路信息协议（RIP）（用DV算法）：使用跳数作为费用测度，运行方式类似DV算法。
2. 开放最短路径优先（OSPF）（用LS算法）：各条链路费用由管理员配置，一台路由器构建一幅关于整个自治系统的完整拓扑图，路由器在本地运行Dijkstra 算法，以确定一个以自身为根节点到所有子网的生成树。

4.12 广播选路算法

1. 无控制洪泛：要求源节点向它所有的邻居发送该分组，会产生广播风暴。
2. 受控洪泛：序号控制洪泛（收到相同广播序号的则丢弃），反向转发路径（仅当该分组是自己到其源的最短单播路径上的，才接受）
3. 生成树广播：构建最小生成树，按生成树发送广播分组。

5 链路层和局域网

5.1 CRC校验和

即是循环冗余校验，具体实现见书本的P287-288页。

5.2 CSMA

载波侦听多路访问在发送前，会先进行侦听，如果没有，就会发送，但是有信号的话，就会等待，如果在传输的过程中检测到碰撞，就会随机停止一段时间，进行等待，然后再发送。

5.3 CSMA/CD

CSMA/CD是一种分布式介质访问控制协议，网中的各个站（节点）都能独立地决定数据帧的发送与接收。每个站在发送数据帧之前，首先要进行载波监听，只有介质空闲时，才允许发送帧。这时，如果两个以上的站同时监听到介质空闲并发送帧，则会产生冲突现象，这使发送的帧都成为无效帧，发送随即宣告失败。每个站必须有能力随时

检测冲突是否发生，一旦发生冲突，则应停止发送，以免介质带宽因传送无效帧而被白白浪费，然后随机延时一段时间后，再重新争用介质，重发送帧。CSMA/CD协议简单、可靠，其网络系统（如Ethernet）被广泛使用。

5.4 MAC Address

MAC Address：mac地址是由6字节组成的。是用来标示硬件地址。其与IP地址不同，具有扁平结构。

5.5 ARP

是地址解析协议，是通过ip地址来标示出mac地址。

假设主机A和B在同一个网段，主机A要向主机B发送信息。具体的地址解析过程如下

1. 主机A首先查看自己的ARP表，确定其中是否包含有主机B 对应的ARP表项。如果找到了对应的MAC地址，则主机A 直接利用ARP表中的MAC地址，对IP数据包进行帧封装，并将数据包发送给主机B。

2. 如果主机A在ARP表中找不到对应的MAC地址，则将缓存该数据报文，然后以广播方式发送一个ARP请求报文。ARP 请求报文中的发送端IP地址和发送端MAC地址为主机A的IP 地址和MAC地址，目标IP地址和目标MAC地址为主机B的IP地址和全0的MAC地址。由于ARP请求报文以广播方式发送，该网段上的所有主机都可以接收到该请求，但只有被请求的主机（即主机B）会对该请求进行处理。

3. 主机B比较自己的IP地址和ARP请求报文中的目标IP地址，当两者相同时进行如下处理：将ARP请求报文中的发送端（即主机A）的IP地址和MAC地址存入自己的ARP 表中。之后以单播方式发送ARP响应报文给主机A，其中包含了自己的MAC地址。

4. 主机A收到ARP响应报文后，将主机B的MAC地址加入到自己的ARP表中以用于后续报文的转发，同时将IP数据包进行封装后发送出去。

5.6 以太网帧结构

是由前同步码，目的地址，这个地址是mac 地址，源地址，是自己的mac地址，类型是可以支持多种类型的网络。CRC是数据校验码。其中数据的范围是46字节–1500字节，整个帧的范围是64字节–1518字节。

5.7 链路层交换机

交换机为链路层和物理层设备，与路由器相比其拥有即插即用的特性

5.7.1 自学习过程

1. 交换机表初始为空。
2. 对于在某接口收到的每个入帧，该交换机在其表中储存：a在该帧源地址字段中的MAC地址，b该帧到达的接口，c当前的时间。交换机以这种方式在他的表中记录发送节点所在的LAN网段。如果在LAN上的每个节点最终都发送了一个帧，每个节点将在这张表中被记录下来。
3. 如果在一段时间之后，交换机没有接受到该址作为原地址的帧，就在表中删除这个地址。

6 结语

这份提纲是我们5个人用了4天时间总结的，每个人完成一章的内容，里面涉及了计算机网络的重点和考点，希望能够对大家有所帮助。由于时间紧凑，免不了错误和纰漏，欢迎大家指出与改正。特别感谢胡俊宇，王琰，王领和方强同学对我的支持和帮助。最后祝大家能取得一个好成绩!