计算机网络知识点

一、无连接服务与面向连接服务

（1）面向连接服务：

1、当程序使用面向连接服务时，在客户机程序和服务器程序发送具有实际数据的分组前，要彼此发送控制分组。这种所谓的握手过程提醒客户机与服务器，使它们对随后的分组的突然到来做好准备。一旦握手过程结束，就可以说两个端系统之间建立了连接。

2、因特网的面向连接的服务与其他的服务共存，包括可靠数据传送。流控制和拥塞控制。

3、面向连接服务的基本组成部分是：通信实体之间握手的协议。

（2）无连接服务

1、在因特网无连接服务中不存在握手。当应用程序的一方要向应用程序的另一方发送分组时，发送程序直接发送这些分组即可。因为没有数据分组传输之前没有握手过程，数据能更好地传递。

2、数据传送没有可靠性可言，没有流控制和拥塞控制的功能。

3、无连接服务的基本的标志是：没有三次握手的过程。

二、电路交换、分组交换

（1）电路交换

1、在电路交换网络中，沿着端系统通信路径，为端系统之间通信所提供的资源在通讯会话期间将会被预留。

2、缺点：电路交换效率较低，因为在静默期专用电路空闲。

3、电路交换分为：频分复用，时分复用。

（2）分组交换

1、在分组交换网络中，这些为端系统之间通信所提供的资源不会被预留，会话的报文按需使用这些资源，这样将导致可能不得不等待接入通信线路。

2、优点：提供了比电路交换网络更好的带宽共享；比电路交换更简单，更有效，实现成本更低。

三、分组交换网络：数据报网络和虚电路网络

（1）虚电路网络

1、我们称任何根据虚电路号转发分组的网络为虚电路网络

2、每个分组中都有虚电路标识符，对于 VC 而言，一条 VC 的源和目的地仅间接地通过 VC ID 标识出来；源和目的端系统的实际地址并不必执行交换。

each packet carries tag　(virtual circuit ID), tag determines next hop

fixed path determined at call setup time, remains fixed thru call

（2）数据报网络

1、我们将任何根据主机目的地址转发分组的网络称为数据报网络。

2、在数据报网络中，每个通过该网络的分组在它的首部都包含了该分组的目的地址，该地址具有一种等级结构。当一个分组到达网络的分组交换机时，分组交换机检查该分组的目的地址的一部分，并向相邻交换机转发该分组。

四、应用需要的服务与因特网运输协议提供的服务

（1）应用层需要的服务

1、可靠的数据传输

2、带宽

3、定时

（2）因特网提供的服务

1、TCP：面向连接的服务；可靠的传输服务；具有拥塞控制；没有确保最小传输速率；不提供延时保证。

2、UDP：无连接服务；不可靠数据传输服务；没有拥塞控制机制；不提供延时保证。

五、HTTP 协议（超文本传输协议）

（1）非持久连接：

每个 TCP 连接只传输一个请求报文和一个响应报文；每一个请求对象建立和维护一个全新的连接。

（2）持久连接：

服务器在发送响应后保持该 TCP 连接，在相同的客户机与服务器之间的后继请求和响应报文可以通过相同的连接进行传输。

1、非流水线方式：客户机只能在前一个响应接收后才能发出新的请求。

2、流水线方式：在一个响应请求未接收之间可以产生新的请求。

（3）过程

(1) 浏览器分析超链指向页面的 URL。
(2) 浏览器向 DNS 请求解析 www.tsinghua.edu.cn 的 IP 地址。
(3) 域名系统 DNS 解析出清华大学服务器的 IP 地址。
(4) 浏览器与服务器建立 TCP 连接
(5) 浏览器发出取文件命令：
GET /chn/yxsz/index.htm。
(6) 服务器给出响应，把文件 index.htm 发给浏览器。
(7) TCP 连接释放。
(8) 浏览器显示“清华大学院系设置”文件 index.htm 中的所有文本。

五、Cookie

1、第一次访问使用 Cookie 的电子商务网站，在请求报文到达 Web 服务器时，Web 站点产生唯一的标识码，并且作为索引在它的后端数据库的一个项。

2、用包含 Set-cookie 首部行的 HTTP 响应报文对客户机进行相应。

3、当客户机接收到该 HTTP 响应报文时，浏览器将 Cookie 文件中添加 Set-cookie 中的标识码的内容。

4、再次访问该商务网站时，请求报文的首部行中会含有 Cookie 的标识码信息。

六、SMTP

（1）特点及约束条件

1、SMTP 使用的传输层协议是 TCP 的可靠数据传输，端口号 25

2、SMTP 直接传输，一般不使用中间邮件服务器

3、连接建立后：服务器与客户机执行应用层握手；进行 TCP 的可靠数据传输，来传输报文；TCP 关闭连接

4、向服务器发送的命令是 ASCII 码的形式；服务器的回答：回答吗和英文解释

5、邮件报文的主体部分只能采用 ASCII 码表示

uses TCP to reliably transfer email message from client to server, port 25

direct transfer: sending server to receiving server

three phases of transfer

handshaking (greeting)

transfer of messages

closure

command/response interaction

commands: ASCII text

response: status code and phrase

messages must be in 7-bit ASCII

（2）Alice 和 Bob 邮件发送过程

1、Alice 启动邮件代理程序并且提供 Bob 的邮件地址，通过邮件代理发送邮件

2、Alice 的邮件代理程序把报文发给 Alice 的邮件服务器，该邮件在这里被放到报文发送队列中

3、欲行在 Alice 邮件服务器上的 SMTP 客户端发现报文队列中的该报文，创建一个到运行在 Bob 邮件服务器上的 TCP 链接。

4、经过 SMTP 的握手后，SMTP 客户机通过 TCP 连接发送 Alice 的报文

5、在 Bob 服务器端接收该报文，Bob 的邮件服务器然后将该报文放入 Bob 的邮箱中

6、在 Bob 方便的时候，他调用用户代理阅读报文

七、可靠数据传输的原理

（1）rdt 1.0　完全可靠的信道上传输；发送端 TCP 接受应用程数据包以后传输给下层的网络层，接收端 TCP 接收包后直接传递给应用程序。

（2）rdt 2.0　差错检验；接收方反馈；重传；停等协议，没有考虑 ACK 和 NAK 分组受损的情况。

（3）rdt 2.1　进行排序，0、1 号；当收到含糊不清的 ACK 或者 NAK，都重发当前的分组。

（4）rdt 2.2　减少对于 NAK 的使用，用两个 ACK 代表 NAK；

（5）rdt 3.0　考虑到丢包的现象，丢包或者是收到 NAK 后，都进行超时重传；

（6）Go-Back-N 协议（滑动窗口协议）

1、发送方可以发送多个分组而不需要等待确认

2、窗口为 n:1

3、累计应答

4、如果出现超时现象，重发所有已经发送的但是还没有确认过的分组。

5、接收方丢弃所有失序的分组，尽管该分组已经正确的接受

（7）选择重传协议（SR）

1、接收方将确认一个正确接受的分组而不管其是否有序，将失序的分组缓存起来

2、n:n

3、发送方每一个发送的包都有一个定时器，来进行单独的计时

4、窗口的大小和包的序列号数目有关

（8）TCP 协议

1、累计确认：TCP 只确认数据流中至第一个丢失字节为止的字节。

2、估计往返时延 RTT

3、在 TCP 的快速重传机制下，收到一个特定的报文段的 3 个冗余的 ACK 就可以作为对后面报文的一个隐式的 NAK，即超时之前进行对该报文的重传。

4、TCP 确认是累积式的，正确接受但失序的报文不会被接收方逐个确认（可以实现将接受的无序的报文进行缓存）--Go-Back-N

5、Go-Back-N 在 n 号分组丢失时，重传 n-N 所有的分组。TCP 至多传送一个分组，如果报文段 n+1 的确认信号在报文 n 超时之前到达，TCP 不进行 n 号报文的重传。

6、流量控制与拥塞控制

7、TCP 拥塞控制的方法--TCP 拥塞控制算法

加性增；慢启动；对超时事件作出反应。

八、虚电路和数据报网络

（1）虚电路网络

1、定义：　仅在网络层提供连接服务的计算机网络成为虚电路网络

2、VC 组成：　（1）源和目的主机之间的路径

（2）VC 号，沿着该路径的每段链路的一个号码

（3）沿着该路径的每台路由器中的转发表项

3、阶段：　（1）虚电路的建立；（2）数据传送；（3）虚电路拆除。

4、虚电路网络的路由器必须为进行中的连接维持连接状态信息。

（2）数据报网络

定义：在数据报网络中，每当一个端系统要发送分组时，就为改分组加上目的地端系统的地址，然后将该分组推进网络中，完成这些无需建立任何虚电路。在数据包网络中路由器不维护任何有关的虚电路的状态信息。

九、选路算法

（1）分类

- 全局选路算法--链路状态算法
  - 静态选路算法
  - 动态选路算法
- 分散式选路算法--距离向量算法

（2）链路状态算法（LS）--全局算法

1、所有的节点具有该网络的同一个以及完整的视图。
2、Dijkstra 算法
3、防止振荡（避免自同步）-- 对每一个路由器随机化他发送链路通告的时间。

（3）距离限量选路算法（DV）--分散式算法

1、没有计算应该停止的信号，持续到邻居之间没有更多的信息要交换为止。
2、异步的、迭代的、自我终结的
3、节点具有的唯一信息是它到直接相连邻居的链路费用和他从这些邻居接收到的信息。
4、解决无穷计数的问题--独行反转

十、自治系统内部选路

（1）RIP（选择信息协议）

1、是一种距离向量协议
2、RIP 版本使用跳步数作为费用度量

（2）OSPF（开放最短路径优先）

1、使用链路状态信息洪范的链路状态协议和一个 Dijkstra 最低费用路径算法
2、含有多种区域边界路由器：内部路由器，区域边界路由器，主干路由器，边界路由器。

十一、自制系统间的选路：BGP

路由选择：

1、路由被指派一个本地偏好值作为他们的属性之一
2、从余下的路由器中，具有最短 AS-PATH 的路由将被选择
3、从余下的路由中，选择具有最靠近 NEXT-HOP 路由器的路由（热土豆选路）
4、如果任剩下多余的路由，该路由使用 BGP 标识以选择路由

十二、多路访问协议

（1）信道划分协议
1、时分复用：将时间划分为时间频

2、频分复用：将信道划分为不同的频段

3、码分多址：对节点分配不同的编码

（2）随机访问协议

1、时隙 ALOHA：节点只在时隙的开始传输帧

2、ALOHA：非时隙的，完全分散协议

3、载波监听多址访问（CSMA）：载波监听，碰撞检测；发生碰撞后，继续完整的传输它们的帧

（3）轮流协议

1、轮询协议：指定一个主节点，主节点以循环的方式轮询每个节点

2、令牌传递协议：没有主节点，一个小的成为令牌的特殊的目的帧在这些的节点之间以某个固定的次序交换。

十三、动态主机配置协议

（1）DHCP 服务器发现：DHCP 客户端广播（255.255.255.255.68）

（2）DHCP 服务器提供：DHCP 服务器广播（255.255.255.255.67）

（3）DHCP 请求：广播：通知其他 DHCP 的请求者，这个 IP 已经被申请

（4）DHCP ACK：DHCP 服务器广播通知某一个 IP 已经给了某个 DHCP 客户端。

十四、RIP、OSPF、BGP

（1）RIP （选路信息协议）

RIP 是一种距离向量协议，每台路由器维护一张称为选路表的 RIP 表，第一列称为目的子网，第二列指出下一跳路由器标示，第三列指出沿着最短路径到达目的子网的跳数。

D 路由器收到来自 A 的通告，该通告是路由器 A 的选路信息表，该信息表指出到相同子网的跳数的变化，若路由器 D 收到的 A 的选路信息表中到达同样子网的跳数小于 D 现有到达该子网的跳数，则 D 更新其路由表。

（2）OSPF（开放最短路径优先）

像 RIP 一样，OSPF 也广泛应用于因特网内部的区域自治 AS 内部选路。OSPF 的核心是一个使用洪泛链路信息的链路状态协议和一个 Dijkstra 最低费用路径算法。使用 OSPF 一个路由器构建了一个自制系统的完整的拓扑图。路由器在本地运行 Dijkstra 最短路径算法，确定一个以自身为根节点的到所有节点的最短路径树。

使用 OSPF 路由器向自制系统内的所有路由器广播选路信息，而不是仅仅像其邻居路由器广播。每当链路费用发生变化时，路由器就会广播信息。计时链路状态未发生变化，也要周期性的广播信息，以增强其健壮性。

OSPF 的优点包括以下几个方面：

安全。OSPF 路由器之间的交换都是要进过鉴别的。

多条相同费用的路径。当到达某目的的的有相同路径的费用时，OSPF 允许使用多条路径。

对单播选路与多播选路的支持。

支持在单个选路域内的层层次结构。OSPF 最重要的优点是具有按层次结构构造一个自

治系统的能力。

（3）BGP（边界网关协议）

对于每条 TCP 连接，位于连接端点的两台路由器被称为 BGP 对等方，沿着该链接发送的所有报文叫做 BGP 会话。跨越 2 个 AS 之间的会话叫做外部 BGP 会话，同一个 AS 中的两台路由器之间的会话叫做内部会话。

BGP 使得每个 AS 知道其相邻的 AS 哪些是可以到达的。在 BGP 中目的地不是主机而是 CIDR（无类别域间选路）化的前缀，每个前缀表示一个子网或一个子网的集合。

如图 P257 图 4-41.来说明一下 BGP 是怎么建立会话的。在 AS3 和 AS1 之间的 3a 和 1c 之间使用 eBGP 会话交换他们可达性信息，AS3 向 AS1 发送一个可达的前缀列表，AS1 向 AS3 发送一个经 AS1 可达的前缀列表。任何 AS 中的网关路由接收到 eBGP 学习到的前缀后，该网关使用 iBGP 向该 S 中的其它路由器发布这些前缀。当一台路由器得知一个新的前缀时，它为该前缀在其转发表中创建一个项。

BGP 选路规则：

路由被指派一个本地偏好值作为它的属性之一。

在余下的路由中选择具有最短 AS-PATH 的路由。

在余下的路由中选择靠近 NEXT-HOP 的路由。

如果还有余下的路由，在路由使用 BGP 标示符选择路由。

选路策略

P259 图 4-43 所示：X 如果通告其邻居节点 B C 除 X 外没有其它任何目的地，那么 X 则为桩网络。这就是说，计时 X 知道自己有一台路可以到达 Y，X 也不会通知 B，由于 B 不知道通过 X 可以到达 Y，因此 B 不会经由 X 转发目的地 Y 或 C 的流量。这个例子说明了如何使用路由通告策略实现客户-供应商之间的关系。

B 应该将 BAW 告诉 C 吗？如果它这样做，则 C 可以选择 CBAW 到达 W，如果 ABC 都是主干提供商，那么 B 应该觉得他不应该承担 AC 之间的流量。

ISP 遵循一个经验法则：任何穿越主干网的流量必须是其源或目的位于该 ISP 的某个客户网络中，否则这些流量会免费搭乘 ISP 的网络。