

一、概论

1、在网络边缘的端系统中运行的程序之间的通信方式通常可划分为两大类：

- 客户服务器方式 (C/S 方式) 即 Client/Server 方式

- 对等方式 (P2P 方式) 即 Peer-to-Peer 方式

(1) 客户(client)和服务器(server)都是指通信中所涉及的两个应用进程。

- 客户服务器方式所描述的是进程之间服务和被服务的关系。

- 客户是服务的请求方，服务器是服务的提供方。

(2) 对等连接(peer-to-peer, 简称为 P2P)是指两个主机在通信时并不区分哪一个是服务请求方还是服务提供方。

- 只要两个主机都运行了对等连接软件 (P2P 软件)，它们就可以进行平等的、对等连接通信。

- 双方都可以下载对方已经存储在硬盘中的共享文档。

特点

- 对等连接方式从本质上看仍然是使用客户服务器方式，只是对等连接中的每一个主机既是客户又同时是服务器。

例如主机 C 请求 D 的服务时, C 是客户, D 是服务器。但如果 C 又同时向 F 提供服务, 那么 C 又同时起着服务器的作用

2、电路交换、分组交换、报文交换

(1) 电路交换的特点：电路交换必定是面向连接的；

电路交换的三个阶段：建立连接、通信、释放连接。

电路交换传送计算机数据效率低

- 计算机数据具有突发性。

- 这导致通信线路的利用率很低。

(2) 分组计划优点

- 高效 动态分配传输带宽，对通信链路是逐段占用。

- 灵活 以分组为传送单位和查找路由。

- 迅速 不必先建立连接就能向其他主机发送分组。

- 可靠 保证可靠性的网络协议；分布式的路由选择协议使网络有很好的生存性。

缺点

- 分组在各结点存储转发时需要排队，这就会造成一定的时延。

- 分组必须携带的首部（里面有必不可少的控制信息）也造成了一定的开销。

3、体系结构

- 计算机网络的体系结构(architecture)是计算机网络的各层及其协议的集合。

- 体系结构就是这个计算机网络及其部件所应完成的功能的精确定义。

- 实现(implementation)是遵循这种体系结构的前提下用何种硬件或软件完成这些功能的问题。

- 体系结构是抽象的，而实现则是具体的，是真正在运行的计算机硬件和软件。

- TCP/IP 是四层的体系结构：应用层、运输层、网际层和网络接口层。

五层协议的体系结构：应用层 运输层 网络层 数据链路层 物理层

4、计算机网络的性能指标

(1) 速率：即数据率(data rate)或比特率(bit rate)是计算机网络中最重要的一性能指标。速率的单位是 b/s, 或 kb/s, Mb/s, Gb/s 等

- 速率往往是指额定速率或标称速率。

(2) “带宽”(bandwidth)本来是指信号具有的频带宽度，单位是赫(或千赫、兆赫、吉赫等)。

- 现在“带宽”是数字信道所能传送的“最高数据率”的同义语，单位是“比特每秒”，或 b/s (bit/s)。

(3) 吞吐量(throughput)表示在单位时间内通过某个网络(或信道、接口)的数据量。

- 吞吐量更经常地用于对现实世界中的网络的一种测量，以便知道实际上到底有多少数据量能够通过网络。

- 吞吐量受网络的带宽或网络的额定速率的限制。

(4) 传输时延(发送时延) 发送数据时，数据块从结点进入到传输媒体所需要的时间。

- 也就是从发送数据帧的第一个比特算起，到该帧的最后一个比特发送完毕所需的时间。

$$\text{发送时延} = \frac{\text{数据块长度 (比特)}}{\text{信道带宽 (比特/秒)}}$$

- 传播时延 电磁波在信道中需要传播一定的距离而花费的时间。

- 信号传输速率(即发送速率)和信号在信道上的传播速率是完全不同的概念。

$$\text{传播时延} = \frac{\text{信道长度 (米)}}{\text{信号在信道上的传播速率 (米/秒)}}$$

- 处理时延 交换结点为存储转发而进行一些必要的处理所花费的时间。
- 排队时延 结点缓存队列中分组排队所经历的时延。
- 排队时延的长短往往取决于网络中当时的通信量。

总时延 = 发送时延 + 传播时延 + 处理时延 + 排队时延

(5) 时 延 带 宽 积

时延带宽积 = 传播时延 × 带宽

- 链路的时延带宽积又称为以比特为单位的链路长度。

(6) 利用率

信道利用率指出某信道有百分之几的时间是被利用的(有数据通过)。完全空闲的信道的利用率是零。

- 网络利用率则是全网络的信道利用率的加权平均值。
- 信道利用率并非越高越好。
- 根据排队论的理论,当某信道的利用率增大时,该信道引起的时延也就迅速增加。
- 若令 D_0 表示网络空闲时的时延, D 表示网络当前的时延,则在适当的假定条件下, D 可以用下面的简单公式表示 D 和 D_0 之间的关系:

$$D = \frac{D_0}{1-U}$$
 U 是网络的利用率,数值在 0 到 1 之间。
-

二、物理层

1、物理层的主要任务描述为确定与传输媒体的接口的一些特性,即:

- 机械特性 指明接口所用接线器的形状和尺寸、引线数目和排列、固定和锁定装置等等。
- 电气特性 指明在接口电缆的各条线上出现的电压的范围。
- 功能特性 指明某条线上出现的某一电平的电压表示何种意义。
- 过程特性 指明对于不同功能的各种可能事件的出现顺序。

2、单向通信(单工通信)——只能有一个方向的通信而没有反方向的交互。

- 双向交替通信(半双工通信)——通信的双方都可以发送信息,但不能双方同时发送(当然也就不能同时接收)。
- 双向同时通信(全双工通信)——通信的双方可以同时发送和接收信息。

3、基带信号(即基本频带信号)——来自信源的信号。像计算机输出的代表各种文字或图像文件的数据信号都属于基带信号。

- 带通信号——把基带信号经过载波调制后,把信号的频率范围搬移到较高的频段以便在信道中传输(即仅在一段频率范围内能够通过信道)。
- 基带信号往往包含有较多的低频成分,甚至有直流成分,而许多信道并不能传输这种低频分量或直流分量。为了解决这一问题,就必须对基带信号进行调制(modulation)。
- 最基本的二元制调制方法有以下几种:
 - 调幅(AM):载波的振幅随基带数字信号而变化。
 - 调频(FM):载波的频率随基带数字信号而变化。
 - 调相(PM):载波的初始相位随基带数字信号而变化。

4、(1) 导向传输媒体

- 双绞线:屏蔽双绞线 STP 无屏蔽双绞线 UTP 同轴电缆(50 Ω 同轴电缆 75 Ω 同轴电缆)
- 光缆

(2) 非导向传输媒体

- 无线传输所使用的频段很广。
- 短波通信主要是靠电离层的反射,但短波信道的通信质量较差。
- 微波在空间主要是直线传播。
 - 地面微波接力通信
 - 卫星通信

5、信道复用技术

(1) 频分复用 FDM 用户在分配到一定的频带后,在通信过程中自始至终都占用这个频带。

- 频分复用的所有用户在同样的时间占用不同的带宽资源(请注意,这里的“带宽”是频率带宽而不是数据的发送速率)。

(2) 时分复用则是将时间划分为一段段等长的时分复用帧(TDM 帧)。每一个时分复用的用户在每一个 TDM 帧中占用固定序号的时隙。

- 每一个用户所占用的时隙是周期性地出现(其周期就是 TDM 帧的长度)。
- TDM 信号也称为等时(isochronous)信号。
- 时分复用的所有用户是在不同的时间占用同样的频带宽度。

时分复用可能会造成线路资源的浪费,使用时分复用系统传送计算机数据时,由于计算机数据的突发性,用户对

分配到的子信道的利用率一般是不高的。

(3) 统计时分复用 STDM

三、数据链路层

1、数据链路层使用的信道主要有以下两种类型：

- 点对点信道。这种信道使用一对一的点对点通信方式。
- 广播信道。这种信道使用一对多的广播通信方式，因此过程比较复杂。广播信道上连接的主机很多，因此必须使用专用的共享信道协议来协调这些主机的数据发

2、数据链路(data link)除了物理线路外，还必须要有通信协议来控制这些数据的传输。若把实现这些协议的硬件和软件加到链路上，就构成了数据链路。

- 现在最常用的方法是使用适配器（即网卡）来实现这些协议的硬件和软件。
- 一般的适配器都包括了数据链路层和物理层这两层的功能。

3、三个基本问题

(1) 封装成帧

- 封装成帧(framing)就是在一段数据的前后分别添加首部和尾部，然后就构成了一个帧。确定帧的界限。
- 首部和尾部的一个重要作用就是进行帧定界。

(2) 解决透明传输问题

- 发送端的数据链路层在数据中出现控制字符“SOH”或“EOT”的前面插入一个转义字符“ESC”（其十六进制编码是 1B）。
- 字节填充(byte stuffing)或字符填充(character stuffing)——接收端的数据链路层在将数据送往网络层之前删除插入的转义字符。
- 如果转义字符也出现数据当中，那么应在转义字符前面插入一个转义字符。当接收端收到连续的两个转义字符时，就删除其中前面的一个。

(3) 差错检测

- 在传输过程中可能会产生比特差错：1 可能会变成 0 而 0 也可能变成 1。
- 在一段时间内，传输错误的比特占所传输比特总数的比率称为误码率 BER (Bit Error Rate)。
- 误码率与信噪比有很大的关系。

循环冗余检验 CRC 的原理

- 在数据链路层传送的帧中，广泛使用了循环冗余检验 CRC 的检错技术。
- 在发送端，先把数据划分为组。假定每组 k 个

比特。

- 假设待传送的一组数据 $M = 101001$ （现在 $k = 6$ ）。我们在 M 的后面再添加供差错检测用的 n 位冗余码一起发送。
- 用二进制的模 2 运算进行 2^n 乘 M 的运算，这相当于在 M 后面添加 n 个 0。
- 得到的 $(k + n)$ 位的数除以事先选定好的长度为 $(n + 1)$ 位的除数 P ，得出商是 Q 而余数是 R ，余数 R 比除数 P 少 1 位，即 R 是 n 位。
- 现在 $k = 6$ ， $M = 101001$ 。
- 设 $n = 3$ ，除数 $P = 1101$ ，
- 被除数是 $2^n M = 101001000$ 。
- 模 2 运算的结果是：商 $Q = 110101$ ，余数 $R = 001$ 。
- 把余数 R 作为冗余码添加在数据 M 的后面发送出去。发送的数据是： $2^n M + R$
即：101001001，共 $(k + n)$ 位。

帧检验序列 FCS

- 在数据后面添加上的冗余码称为帧检验序列 FCS (Frame Check Sequence)。
- 循环冗余检验 CRC 和帧检验序列 FCS 并不同。
 - CRC 是一种常用的检错方法，而 FCS 是添加在数据后面的冗余码。
 - FCS 可以用 CRC 这种方法得出，但 CRC 并非用来获得 FCS 的唯一方法。

接收端对收到的每一帧进行 CRC 检验

- (1) 若得出的余数 $R = 0$ ，则判定这个帧没有差错，就接受(accept)。
- (2) 若余数 $R \neq 0$ ，则判定这个帧有差错，就丢弃。
- 仅用循环冗余检验 CRC 差错检测技术只能做到无差错接受(accept)。
- “无差错接受”是指：“凡是接受的帧（即不包括丢弃的帧），我们都能以非常接近于 1 的概率认为这些帧在传输过程中没有产生差错”。
- 要做到“可靠传输”（即发送什么就收到什么）就必须再加上确认和重传机制。

4、点对点协议 PPP

(1) PPP 协议应满足的需求

简单——这是首要的要求 封装成帧 透明性 多种网络层协议 多种类型链路 差错检测 检测连接状态 最大传送单元 网络层地址协商 数据压缩协商

(2) PPP 协议不需要的功能

纠错 流量控制 序号 多点线路 半双工或单工链路

(3) PPP 协议有三个组成部分

- 一个将 IP 数据报封装到串行链路的方法。
- 链路控制协议 LCP (Link Control Protocol)。
- 网络控制协议 NCP (Network Control Protocol)。

(4) PPP 协议的帧格式

标志字段 F = 0x7E 地址字段 A 只置为 0xFF。

控制字段 C 通常置为 0x03。

PPP 有一个 2 个字节的协议字段。

- 当协议字段为 0x0021 时, PPP 帧的信息字段就是 IP 数据报。
- 若为 0xC021, 则信息字段是 PPP 链路控制数据。
- 若为 0x8021, 则表示这是网络控制数据。

PPP 是面向字节的, 所有的 PPP 帧的长度都是整数字节。

(5) 当 PPP 用在异步传输时, 就使用一种特殊的字符填充法

- 将信息字段中出现的每一个 0x7E 字节转变成成为 2 字节序列 (0x7D, 0x5E)。
- 若信息字段中出现一个 0x7D 的字节, 则将其转变成成为 2 字节序列 (0x7D, 0x5D)。
- 若信息字段中出现 ASCII 码的控制字符 (即数值小于 0x20 的字符), 则在该字符前面要加入一个 0x7D 字节, 同时将该字符的编码加以改变。

(6) PPP 协议用在 SONET/SDH 链路时, 是使用同步传输 (一连串的比特连续传送)。这时 PPP 协议采用零比特填充方法来实现透明传输。

- 在发送端, 只要发现有 5 个连续 1, 则立即填入一个 0。接收端对帧中的比特流进行扫描。每当发现 5 个连续 1 时, 就把这 5 个连续 1 后的一个 0 删除,

(7) PPP 协议之所以不使用序号和确认机制是出于以下的考虑:

- 在数据链路层出现差错的概率不大时, 使用比较简单的 PPP 协议较为合理。
- 在因特网环境下, PPP 的信息字段放入的数据是 IP 数据报。数据链路层的可靠传输并不能够保证网络层的传输也是可靠的。

- 帧检验序列 FCS 字段可保证无差错接受。

(8) PPP 协议的工作状态

- 当用户拨号接入 ISP 时, 路由器的调制解调器对拨号做出确认, 并建立一条物理连接。
- PC 机向路由器发送一系列的 LCP 分组 (封装成多个 PPP 帧)。
- 这些分组及其响应选择一些 PPP 参数, 和进行网络层配置, NCP 给新接入的 PC 机分配一个临时的 IP 地址, 使 PC 机成为因特网上的一个主机。
- 通信完毕时, NCP 释放网络层连接, 收回原来分配出去的 IP 地址。接着, LCP 释放数据链路层连接。最后释放的是物理层的连接。

5、局域网的数据链路层

- 局域网最主要的特点是: 网络为一个单位所拥有, 且地理范围和站点数目均有限。
- 局域网具有如下的一些主要优点:
 - 具有广播功能, 从一个站点可很方便地访问全网。局域网上的主机可共享连接在局域网上的各种硬件和软件资源。
 - 便于系统的扩展和逐渐地演变, 各设备的位置可灵活调整和改变。
 - 提高了系统的可靠性、可用性和残存性。
- 为了使数据链路层能更好地适应多种局域网标准, 802 委员会就将局域网的数据链路层拆成两个子层:
 - 逻辑链路控制 LLC (Logical Link Control) 子层
 - 媒体接入控制 MAC (Medium Access Control) 子层。
- 与接入到传输媒体有关的内容都放在 MAC 子层, 而 LLC 子层则与传输媒体无关, 不管采用何种协议的局域网对 LLC 子层来说都是透明的

6、适配器

- 网络接口板又称为通信适配器 (adapter) 或网络接口卡 NIC (Network Interface Card), 或“网卡”。
- 适配器的重要功能:
 - 进行串行/并行转换。
 - 对数据进行缓存。
 - 在计算机的操作系统安装设备驱动程序。
 - 实现以太网协议。

7、CSMA/CD 协议

(1) 简介

- “多点接入”表示许多计算机以多点接入的方式连接在一根总线上。
- “载波监听”是指每一个站在发送数据之前先要检测一下总线上是否有其他计算机在发送数据，如果有，则暂时不要发送数据，以免发生碰撞。
- 总线上并没有什么“载波”。因此，“载波监听”就是用电子技术检测总线上有没有其他计算机发送的数据信号。
- “碰撞检测”就是计算机边发送数据边检测信道上的信号电压大小。
- 当几个站同时在总线上发送数据时，总线上的信号电压摆动值将会增大（互相叠加）。
- 当一个站检测到的信号电压摆动值超过一定的门限值时，就认为总线上至少有两个站同时在发送数据，表明产生了碰撞。

检测到碰撞后

- 在发生碰撞时，总线上传输的信号产生了严重的失真，无法从中恢复出有用的信息来。
- 每一个正在发送数据的站，一旦发现总线上出现了碰撞，就要立即停止发送，免得继续浪费网络资源，然后等待一段随机时间后再次发送。

(2) 重要特性

- 使用 CSMA/CD 协议的以太网不能进行全双工通信而只能进行双向交替通信（半双工通信）。
- 每个站在发送数据之后的一小段时间内，存在着遭遇碰撞的可能性。
- 这种发送的不确定性使整个以太网的平均通信量远小于以太网的最高数据率。

(3) 争用期

- 最先发送数据帧的站，在发送数据帧后至多经过时间 2τ （两倍的端到端往返时延）就可知道发送的数据帧是否遭受了碰撞。
- 以太网的端到端往返时延 2τ 称为争用期，或碰撞窗口。
- 经过争用期这段时间还没有检测到碰撞，才能肯定这次发送不会发生碰撞。
- 以太网取 $51.2 \mu s$ 为争用期的长度。
- 对于 10 Mb/s 以太网，在争用期内可发送 512 bit，即 64 字节。
- 以太网在发送数据时，若前 64 字节没有发生冲突，则后续的数据就不会发生冲突。

二进制指数类型退避算法

- 发生碰撞的站在停止发送数据后，要推迟（退避）一个随机时间才能再发送数据。

- 确定基本退避时间，一般是取为争用期 2τ 。
- 定义重传次数 k ， $k \leq 10$ ，即

$$k = \text{Min}[\text{重传次数}, 10]$$
- 从整数集合 $[0, 1, \dots, (2^k - 1)]$ 中随机地取出一个数，记为 r 。重传所需的时延就是 r 倍的基本退避时间。
- 当重传达 16 次仍不能成功时即丢弃该帧，并向高层报告。

最短有效帧长

- 如果发生冲突，就一定是在发送的前 64 字节之内。
- 由于一检测到冲突就立即中止发送，这时已经发送出去的数据一定小于 64 字节。
- 以太网规定了最短有效帧长为 64 字节，凡长度小于 64 字节的帧都是由于冲突而异常中止的无效帧。

强化碰撞

- 当发送数据的站一旦发现发生了碰撞时：
 - 立即停止发送数据；
 - 再继续发送若干比特的人为干扰信号（jamming signal），以便让所有用户都知道现在已经发生了碰撞。

8、MAC 帧的格式

- 最常用的 MAC 帧是以太网 V2 的格式。
- 目的地址字段 6 字节 源地址字段 6 字节
- 类型字段 2 字节，类型字段用来标志上一层使用的是什么协议，以便把收到的 MAC 帧的数据上交给上一层的这个协议。
- 数据字段 46 ~ 1500 字节，数据字段的正式名称是 MAC 客户数据字段
 最小长度 64 字节 - 18 字节的首部和尾部 = 数据字段的最小长度
- FCS 字段 4 字节

当数据字段的长度小于 46 字节时，应在数据字段的后面加入整数字节的填充字段，以保证以太网的 MAC 帧长不小于 64 字节。

在帧的前面插入的 8 字节中的第一个字段共 7 个字节，是前同步码，用来迅速实现 MAC 帧的比特同步（为了达到比特同步，在传输媒体上实际传送的要比 MAC 帧还多 8 个字节）。第二个字段是帧开始定界符，表示后面的信息就是 MAC 帧。

1) 无效的 MAC 帧

- 数据字段的长度与长度字段的值不一致；
- 帧的长度不是整数个字节；

- 用收到的帧检验序列 FCS 查出有差错；
- 数据字段的长度不在 46 ~ 1500 字节之间。
- 有效的 MAC 帧长度为 64 ~ 1518 字节之间。
- 对于检查出的无效 MAC 帧就简单地丢弃。以太网不负责重传丢弃的帧。

2) 帧间最小间隔

- 帧间最小间隔为 9.6 μ s, 相当于 96 bit 的发送时间。
- 一个站在检测到总线开始空闲后, 还要等待 9.6 μ s 才能再次发送数据。
- 这样做是为了使刚刚收到数据帧的站的接收缓存来得及清理, 做好接收下一帧的准备。

9、网桥

- 在数据链路层扩展局域网是使用网桥。
- 网桥工作在数据链路层, 它根据 MAC 帧的目的地址对收到的帧进行转发。
- 网桥具有过滤帧的功能。当网桥收到一个帧时, 并不是向所有的接口转发此帧, 而是先检查此帧的目的 MAC 地址, 然后再确定将该帧转发到哪一个接口

1) 使用网桥带来的好处

- 过滤通信量。
- 扩大了物理范围。
- 提高了可靠性。
- 可互连不同物理层、不同 MAC 子层和不同速率 (如 10 Mb/s 和 100 Mb/s 以太网) 的局域网。

2) 使用网桥带来的缺点

- 存储转发增加了时延。
- 在 MAC 子层并没有流量控制功能。
- 具有不同 MAC 子层的网段桥接在一起时时延更大。
- 网桥只适合于用户数不太多 (不超过几百个) 和通信量不太大的局域网, 否则有时还会因传播过多的广播信息而产生网络拥塞。这就是所谓的广播风暴。

3) 网桥和集线器 (或转发器) 不同

- 集线器在转发帧时, 不对传输媒体进行检测。
- 网桥在转发帧之前必须执行 CSMA/CD 算法。
 - 若在发送过程中出现碰撞, 就必须停止发送和进行退避。

4) 透明网桥

- “透明”是指局域网上的站点并不知道所发送的帧将经过哪几个网桥, 因为网桥对各站来说是看不见的。
- 透明网桥是一种即插即用设备, 其标准是 IEEE

802.1D。

5) 网桥应当按照以下自学习算法处理收到的帧和建立转发表

- 若从 A 发出的帧从接口 x 进入了某网桥, 那么从这个接口出发沿相反方向一定可把一个帧传送到 A。
- 网桥每收到一个帧, 就记下其源地址和进入网桥的接口, 作为转发表中的一个项目。
- 在建立转发表时是把帧首部中的源地址写在“地址”这一栏的下面。
- 在转发帧时, 则是根据收到的帧首部中的目的地址来转发的。这时就把在“地址”栏下面已经记下的源地址当作目的地址, 而把记下的进入接口当作转发接口。

6) 网桥在转发表中登记以下三个信息

在网桥的转发表中写入的信息除了地址和接口外, 还有帧进入该网桥的时间。

- 这是因为以太网的拓扑可能经常会发生变化, 站点也可能会更换适配器 (这就改变了站点的地址)。另外, 以太网上的工作站并非总是接通电源的。
- 把每个帧到达网桥的时间登记下来, 就可以在转发表中只保留网络拓扑的最新状态信息。这样就使得网桥中的转发表能反映当前网络的最新拓扑状态。

7) 网桥的自学习和转发帧的步骤归纳

网桥收到一帧后先进行自学习。查找转发表中与收到帧的源地址有无相匹配的项目。如没有, 就在转发表中增加一个项目 (源地址、进入的接口和时间)。如有, 则把原有的项目进行更新。

- 转发帧。查找转发表中与收到帧的目的地址有无相匹配的项目。
 - 如没有, 则通过所有其他接口 (但进入网桥的接口除外) 按进行转发。
 - 如有, 则按转发表中给出的接口进行转发。
 - 若转发表中给出的接口就是该帧进入网桥的接口, 则应丢弃这个帧 (因为这时不需要经过网桥进行转发)。

8) 透明网桥使用了生成树算法 生成树的得出

- 互连在一起的网桥在进行彼此通信后, 就能找出原来的网络拓扑的一个子集。在这个子集里, 整个连通的网中不存在回路, 即在任何两个站之间只有一条路径。
- 为了避免产生转发的帧在网络中不断地兜圈子。

- 为了得出能够反映网络拓扑发生变化时的生成树，在生成树上的根网桥每隔一段时间还要对生成树的拓扑进行更新。

9) 源路由网桥

- 透明网桥容易安装，但网络资源的利用不充分。
- 源路由(source route)网桥在发送帧时将详细的路由信息放在帧的首部中。
- 源站以广播方式向欲通信的目的站发送一个发现帧，每个发现帧都记录所经过的路由。
- 发现帧到达目的站时就沿各自的路由返回源站。源站在得知这些路由后，从所有可能的路由中选择出一个最佳路由。凡从该源站向该目的站发送的帧的首部，都必须携带源站所确定的这一路由信息。

四、网络层

1、虚拟互连网络的意义

- 所谓虚拟互连网络也就是逻辑互连网络，它的意思就是互连起来的各种物理网络的异构性本来是客观存在的，但是我们利用 IP 协议就可以使这些性能各异的网络从用户看起来好像是一个统一的网络。
- 使用 IP 协议的虚拟互连网络可简称为 IP 网。
- 使用虚拟互连网络的好处是：当互联网上的主机进行通信时，就好像在一个网络上通信一样，而看不见互连的各具体的网络异构细节。

2、分类 IP 地址

- 每一类地址都由两个固定长度的字段组成，其中一个字段是网络号 net-id，它标志主机（或路由器）所连接到的网络，而另一个字段则是主机号 host-id，它标志该主机（或路由器）。

IP 地址 ::= { <网络号>, <主机号> }

1) IP 地址的使用范围

网络类别	最大网络数	第一个可用的网络号	最后一个可用的网络号
A	126 ($2^7 - 2$)	1	126
B	16,383 ($2^{14} - 1$)	128.1	191.255
C	2,097,151 ($2^{21} - 1$)	192.0.1	223.255.255

2) IP 地址的一些重要特点

(1) IP 地址是一种分等级的地址结构。分两个等级的好处是：

- 第一，IP 地址管理机构在分配 IP 地址时只分配网络号，而剩下的主机号则由得到该网络号的单位自行分配。这样就方便了 IP 地址的管

理。

- 第二，路由器仅根据目的主机所连接的网络号来转发分组（而不考虑目的主机号），这样就可以使路由表中的项目数大幅度减少，从而减小了路由表所占的存储空间。

(2) 实际上 IP 地址是标志一个主机（或路由器）和一条链路的接口。

- 当一个主机同时连接到两个网络上时，该主机就必须同时具有两个相应的 IP 地址，其网络号 net-id 必须是不同的。这种主机称为多归属主机(multihomed host)。
- 由于一个路由器至少应当连接到两个网络（这样它才能将 IP 数据报从一个网络转发到另一个网络），因此一个路由器至少应当有两个不同的 IP 地址。

(3) 用转发器或网桥连接起来的若干个局域网仍为一个网络，因此这些局域网都具有同样的网络号 net-id。

(4) 所有分配到网络号 net-id 的网络，范围很小的局域网，还是可能覆盖很大地理范围的广域网，都是平等的。

3、地址解析协议 ARP

- 不管网络层使用的是什么协议，在实际网络的链路上传送数据帧时，最终还是必须使用硬件地址。
- 每一个主机都设有一个 ARP 高速缓存(ARP cache)，里面有所在的局域网上的各主机和路由器的 IP 地址到硬件地址的映射表。
- 当主机 A 欲向本局域网上的某个主机 B 发送 IP 数据报时，就先在其 ARP 高速缓存中查看有无主机 B 的 IP 地址。如有，就可查出其对应的硬件地址，再将此硬件地址写入 MAC 帧，然后通过局域网将该 MAC 帧发往此硬件地址。

ARP 高速缓存的作用

- 为了减少网络上的通信量，主机 A 在发送其 ARP 请求分组时，就将自己的 IP 地址到硬件地址的映射写入 ARP 请求分组。
- 当主机 B 收到 A 的 ARP 请求分组时，就将主机 A 的这一地址映射写入主机 B 自己的 ARP 高速缓存中。这对主机 B 以后向 A 发送数据报时就更方便了。

应当注意的问题

- ARP 是解决同一个局域网上的主机或路由器的 IP 地址和硬件地址的映射问题。
- 如果所要找的主机和源主机不在同一个局域网

上，那么就要通过 ARP 找到一个位于本局域网上的某个路由器的硬件地址，然后把分组发送给这个路由器，让这个路由器把分组转发给下一个网络。剩下的工作就由下一个网络来做。

- 从 IP 地址到硬件地址的解析是自动进行的，主机的用户对这种地址解析过程是不知道的。
- 只要主机或路由器要和本网络上的另一个已知 IP 地址的主机或路由器进行通信，ARP 协议就会自动地将该 IP 地址解析为链路层所需要的硬件地址。

4、IP 数据报的格式

- 一个 IP 数据报由首部和数据两部分组成。
- 首部的前一部分是固定长度，共 20 字节，是所有 IP 数据报必须具有的。
- 在首部的固定部分的后面是一些可选字段，其长度是可变的。

5、IP 层转发分组的流程

查找路由表：根据目的网络地址就能确定下一跳路由器，这样做的结果是：

- IP 数据报最终一定可以找到目的主机所在目的网络上的路由器（可能要通过多次的间接交付）。
- 只有到达最后一个路由器时，才试图向目的主机进行直接交付。

特定主机路由

- 这种路由是为特定的目的主机指明一个路由。
- 采用特定主机路由可使网络管理人员能更方便地控制网络和测试网络，同时也可在需要考虑某种安全问题时采用这种特定主机路由。

默认路由

- 路由器还可采用默认路由以减少路由表所占用的空间和搜索路由表所用的时间。
- 这种转发方式在一个网络只有很少的对外连接时是很有用的。
- 默认路由在主机发送 IP 数据报时往往更能显示出它的好处。

如果一个主机连接在一个小网络上，而这个网络只用一个路由器和因特网连接，那么在这种情况下使用默认路由是非常合适的

分组转发算法

- (1) 从数据报的首部提取目的主机的 IP 地址 D ，得出目的网络地址为 N 。
- (2) 若网络 N 与此路由器直接相连，则把数据报直接交付目的主机 D ；否则是间接交付，执行(3)。
- (3) 若路由表中有目的地址为 D 的特定主机路由，则

把数据报传送给路由表中所指明的下一跳路由器；否则，执行(4)。

(4) 若路由表中有到达网络 N 的路由，则把数据报传送给路由表指明的下一跳路由器；否则，执行(5)。

(5) 若路由表中有一个默认路由，则把数据报传送给路由表中所指明的默认路由器；否则，执行(6)。

(6) 报告转发分组出错。

6、子网

1) 划分子网的基本思路

- 划分子网纯属一个单位内部的事情。单位对外仍然表现为没有划分子网的网络。
- 从主机号借用若干个位作为子网号 subnet-id，而主机号 host-id 也就相应减少了若干个位。
IP 地址 ::= {<网络号>, <子网号>, <主机号>}
- 凡是从其他网络发送给本单位某个主机的 IP 数据报，仍然是根据 IP 数据报的目的网络号 net-id，先找到连接在本单位网络上的路由器。
- 然后此路由器在收到 IP 数据报后，再按目的网络号 net-id 和子网号 subnet-id 找到目的子网。
- 最后就将 IP 数据报直接交付目的主机。

2) 子网掩码

- 从一个 IP 数据报的首部并无法判断源主机或目的主机所连接的网络是否进行了子网划分。
- 使用子网掩码(subnet mask)可以找出 IP 地址中的子网部分。

子网掩码是一个重要属性

- 子网掩码是一个网络或一个子网的重要属性。
- 路由器在和相邻路由器交换路由信息时，必须把自己所在网络（或子网）的子网掩码告诉相邻路由器。
- 路由器的路由表中的每一个项目，除了要给出目的网络地址外，还必须同时给出该网络的子网掩码。
- 若一个路由器连接在两个子网上就拥有两个网络地址和两个子网掩码。

使用子网掩码的分组转发过程

- (1) 从收到的分组的首部提取目的 IP 地址 D 。
- (2) 先用各网络的子网掩码和 D 逐位相“与”，看是否和相应的网络地址匹配。若匹配，则将分组直接交付。否则就是间接交付，执行(3)。
- (3) 若路由表中有目的地址为 D 的特定主机路由，则将分组传送给指明的下一跳路由器；否则，执行(4)。
- (4) 对路由表中的每一行的子网掩码和 D 逐位相“与”，若其结果与该行的目的网络地址匹配，则将分组传送

给该行指明的下一跳路由器；否则，执行(5)。

(5) 若路由表中有一个默认路由，则将分组传送给路由表中所指明的默认路由器；否则，执行(6)。

(6) 报告转发分组出错。

7、无分类编址 CIDR

CIDR 最主要的特点

- CIDR 消除了传统的 A 类、B 类和 C 类地址以及划分子网的概念，因而可以更加有效地分配 IPv4 的地址空间。
- CIDR 使用各种长度的“网络前缀”(network-prefix)来代替分类地址中的网络号和子网号。
- IP 地址从三级编址（使用子网掩码）又回到了两级编址。

IP 地址 ::= {<网络前缀>, <主机号>}

CIDR 把网络前缀都相同的连续的 IP 地址组成“CIDR 地址块”

- 128.14.32.0/20 表示的地址块共有 2^{12} 个地址（因为斜线后面的 20 是网络前缀的位数，所以这个地址的主机号是 12 位）。
- 这个地址块的起始地址是 128.14.32.0。
- 在不需要指出地址块的起始地址时，也可将这样的地址块简称为“/20 地址块”。
- 128.14.32.0/20 地址块的最小地址：128.14.32.0
- 128.14.32.0/20 地址块的最大地址：128.14.47.255
- 全 0 和全 1 的主机号地址一般不使用。

构成超网

- 前缀长度不超过 23 位的 CIDR 地址块都包含了多个 C 类地址。
- 这些 C 类地址合起来就构成了超网。
- CIDR 地址块中的地址数一定是 2 的整数次幂。
- 网络前缀越短，其地址块所包含的地址数就越多。而在三级结构的 IP 地址中，划分子网是使网络前缀变长。

最长前缀匹配

- 使用 CIDR 时，路由表中的每个项目由“网络前缀”和“下一跳地址”组成。在查找路由表时可能会得到不止一个匹配结果。
- 应当从匹配结果中选择具有最长网络前缀的路由：最长前缀匹配(longest-prefix matching)。
- 网络前缀越长，其地址块就越小，因而路由就越具体(more specific)。
- 最长前缀匹配又称为最长匹配或最佳匹配。

8、内部网关协议 RIP

工作原理

- 路由信息协议 RIP 是内部网关协议 IGP 中最先得到广泛使用的协议。
- RIP 是一种分布式的基于距离向量的路由选择协议。
- RIP 协议要求网络中的每一个路由器都要维护从它自己到其他每一个目的网络的距离记录。

“距离”的定义

- 从一路由器到直接连接的网络的距离定义为 1。
- 从一个路由器到非直接连接的网络的距离定义为所经过的路由器数加 1。
- RIP 协议中的“距离”也称为“跳数”(hop count)，因为每经过一个路由器，跳数就加 1。
- 这里的“距离”实际上指的是“最短距离”，
- RIP 认为一个好的路由就是它通过的路由器的数目少，即“距离短”。
- RIP 允许一条路径最多只能包含 15 个路由器。
- “距离”的最大值为 16 时即相当于不可达。可见 RIP 只适用于小型互联网。
- RIP 不能在两个网络之间同时使用多条路由。RIP 选择一个具有最少路由器的路由（即最短路由），哪怕还存在另一条高速(低时延)但路由器较多的路由。

RIP 协议的三个要点

- 仅和相邻路由器交换信息。
- 交换的信息是当前本路由器所知道的全部信息，即自己的路由表。
- 按固定的时间间隔交换路由信息，例如，每隔 30 秒。

路由表的建立

- 路由器在刚刚开始工作时，只知道到直接连接的网络的距离（此距离定义为 1）。
- 以后，每一个路由器也只和数目非常有限的相邻路由器交换并更新路由信息。
- 经过若干次更新后，所有的路由器最终都会知道到达本自治系统中任何一个网络的最短距离和下一跳路由器的地址。
- RIP 协议的收敛(convergence)过程较快，即在自治系统中所有的结点都得到正确的路由选择信息的过程。

RIP2 的报文由首部 and 路由部分组成

- RIP2 报文中的路由部分由若干个路由信息组成。每个路由信息需要用 20 个字节。地址族标识符（又称为地址类别）字段用来标志所使

用的地址协议。

- 路由标记填入自治系统的号码，这是考虑使 RIP 有可能收到本自治系统以外的路由选择信息。再后面指出某个网络地址、该网络的子网掩码、下一跳路由器地址以及到此网络的距离。

RIP 协议的优缺点

- RIP 存在的一个问题是当网络出现故障时，要经过比较长的时间才能将此信息传送到所有的路由器。
- RIP 协议最大的优点就是实现简单，开销较小。
- RIP 限制了网络的规模，它能使用的最大距离为 15（16 表示不可达）。
- 路由器之间交换的路由信息是路由器中的完整路由表，因而随着网络规模的扩大，开销也就增加。

9、自治系统 AS

- 自治系统 AS 的定义：在单一的技术管理下的一组路由器，而这些路由器使用一种 AS 内部的路由选择协议和共同的度量以确定分组在该 AS 内的路由，同时还使用一种 AS 之间的路由选择协议用以确定分组在 AS 之间的路由。
- 现在对自治系统 AS 的定义是强调下面的事实：尽管一个 AS 使用了多种内部路由选择协议和度量，但重要的是一个 AS 对其他 AS 表现出的是一个单一的和一致的路由选择策略。

因特网有两大类路由选择协议

- 内部网关协议 IGP (Interior Gateway Protocol) 即在一个自治系统内部使用的路由选择协议。目前这类路由选择协议使用得最多，如 RIP 和 OSPF 协议。
- 外部网关协议 EGP (External Gateway Protocol) 若源站和目的站处在不同的自治系统中，当数据报传到一个自治系统的边界时，就需要使用一种协议将路由选择信息传递到另一个自治系统中。这样的协议就是外部网关协议 EGP。在外部网关协议中目前使用最多的是 BGP-4。

五、运输层

1、传输控制协议 TCP

TCP 最主要的特点

- TCP 是面向连接的运输层协议。
- 每一条 TCP 连接只能有两个端点(endpoint)，每一条 TCP 连接只能是点对点的（一对一）。
- TCP 提供可靠交付的服务。
- TCP 提供全双工通信。
- 面向字节流。

应当注意

- TCP 连接是一条虚连接而不是一条真正的物理连接。
- TCP 对应用进程一次把多长的报文发送到 TCP 的缓存中是不关心的。
- TCP 根据对方给出的窗口值和当前网络拥塞的程度来决定一个报文段应包含多少个字节（UDP 发送的报文长度是应用进程给出的）。
- TCP 可把太长的数据块划分短一些再传送。TCP 也可等待积累有足够多的字节后再构成报文段发送出去。

TCP 的连接

- TCP 把连接作为最基本的抽象。
- 每一条 TCP 连接有两个端点。
- TCP 连接的端点不是主机，不是主机的 IP 地址，不是应用进程，也不是运输层的协议端口。TCP 连接的端点叫做套接字(socket)或插口。
- 端口号拼接到(concatenated with) IP 地址即构成了套接字。
- 套接字= (IP 地址：端口号) 每一条 TCP 连接唯一地被通信两端的两个端点（即两个套接字）所确定。即：TCP 连接 $::= \{socket1, socket2\} = \{(IP1: port1), (IP2: port2)\}$

2、TCP 的流量控制

- 流量控制(flow control)就是让发送方的发送速率不要太快，既要让接收方来得及接收，也不要使网络发生拥塞。
- 利用滑动窗口机制可以很方便地在 TCP 连接上实现流量控制。

持续计时器

- TCP 为每一个连接设有一个持续计时器。
- 只要 TCP 连接的一方收到对方的零窗口通知，就启动持续计时器。
- 若持续计时器设置的时间到期，就发送一个零窗口探测报文段（仅携带 1 字节的数据），而对方就在确认这个探测报文段时给出了现在的窗口值。
- 若窗口仍然是零，则收到这个报文段的一方就重新设置持续计时器。
- 若窗口不是零，则死锁的僵局就可以打破了。

可以用不同的机制来控制 TCP 报文段的发送时机：

- 第一种机制是 TCP 维持一个变量，它等于最大报文段长度 MSS。只要缓存中存放的数据达到 MSS 字节时，就组装成一个 TCP 报文段发送出去。

- 第二种机制是由发送方的应用进程指明要求发送报文段，即 TCP 支持的推送(push)操作。
- 第三种机制是发送方的一个计时器期限到了，这时就把当前已有的缓存数据装入报文段（但长度不能超过 MSS）发送出去。

3、TCP 的拥塞控制

- 在某段时间，若对网络中某资源的需求超过了该资源所能提供的可用部分，网络的性能就要变坏——产生拥塞(congestion)。
- 出现资源拥塞的条件：对资源需求的总和 > 可用资源

拥塞控制与流量控制的关系

- 拥塞控制所要做的都有一个前提，就是网络能够承受现有的网络负荷。
- 拥塞控制是一个全局性的过程，涉及到所有的主机、所有的路由器，以及与降低网络传输性能有关的所有因素。
- 流量控制往往指在给定的发送端和接收端之间的点对点通信量的控制。
- 流量控制所要做的就是抑制发送端发送数据的速率，以便使接收端来得及接收。

慢开始和拥塞避免

- 发送方维持一个叫做拥塞窗口 cwnd (congestion window)的状态变量。拥塞窗口的大小取决于网络的拥塞程度，并且动态地在变化。发送方让自己的发送窗口等于拥塞窗口。如再考虑到接收方的接收能力，则发送窗口还可能小于拥塞窗口。
- 发送方控制拥塞窗口的原则是：只要网络没有出现拥塞，拥塞窗口就再增大一些，以便把更多的分组发送出去。但只要网络出现拥塞，拥塞窗口就减小一些，以减少注入到网络中的分组数。

慢开始算法的原理

- 在主机刚刚开始发送报文段时可先设置拥塞窗口 cwnd = 1，即设置为一个最大报文段 MSS 的数值。
- 在每收到一个对新的报文段的确认后，将拥塞窗口加 1，即增加一个 MSS 的数值。
- 用这样的方法逐步增大发送端的拥塞窗口 cwnd，可以使分组注入到网络的速率更加合理。

传输轮次

- 使用慢开始算法后，每经过一个传输轮次，拥塞窗口 cwnd 就加倍。
- 一个传输轮次所经历的时间其实就是往返时间

RTT。

- “传输轮次”更加强调：把拥塞窗口 cwnd 所允许发送的报文段都连续发送出去，并收到了对已发送的最后一个字节的确认。
- 例如，拥塞窗口 cwnd = 4，这时的往返时间 RTT 就是发送方连续发送 4 个报文段，并收到这 4 个报文段的确认，总共经历的时间。

慢开始门限 ssthresh 的用法如下：

- 当 cwnd < ssthresh 时，使用慢开始算法。
- 当 cwnd > ssthresh 时，停止使用慢开始算法而改用拥塞避免算法。
- 当 cwnd = ssthresh 时，既可使用慢开始算法，也可使用拥塞避免算法。
- 拥塞避免算法的思路是让拥塞窗口 cwnd 缓慢地增大，即每经过一个往返时间 RTT 就把发送方的拥塞窗口 cwnd 加 1，而不是加倍，使拥塞窗口 cwnd 按线性规律缓慢增长。

当网络出现拥塞时

- 无论在慢开始阶段还是在拥塞避免阶段，只要发送方判断网络出现拥塞（其根据就是没有按时收到确认），就要把慢开始门限 ssthresh 设置为出现拥塞时的发送方窗口值的一半（但不能小于 2）。
- 然后把拥塞窗口 cwnd 重新设置为 1，执行慢开始算法。
- 这样做的目的就是要迅速减少主机发送到网络中的分组数，使得发生拥塞的路由器有足够时间把队列中积压的分组处理完毕。

乘法减小

- “乘法减小”是指不论在慢开始阶段还是拥塞避免阶段，只要出现一次超时（即出现一次网络拥塞），就把慢开始门限值 ssthresh 设置为当前的拥塞窗口值乘以 0.5。
- 当网络频繁出现拥塞时，ssthresh 值就下降得很快，以大大减少注入到网络中的分组数。

加法增大

- “加法增大”是指执行拥塞避免算法后，在收到对所有报文段的确认后（即经过一个往返时间），就把拥塞窗口 cwnd 增加一个 MSS 大小，使拥塞窗口缓慢增大，以防止网络过早出现拥塞。

快重传和快恢复

- 快重传算法首先要求接收方每收到一个失序的报文段后就立即发出重复确认。这样做可以让发送方及早知道有报文段没有到达接收方。

- 发送方只要一收到三个重复确认就应当立即重传对方尚未收到的报文段。
- 不难看出，快重传并非取消重传计时器，而是在某些情况下可更早地重传丢失的报文段。

快恢复算法

- (1) 当发送端收到连续三个重复的确认时，就执行“乘法减小”算法，把慢开始门限 $ssthresh$ 减半。但接下去不执行慢开始算法。
- (2) 由于发送方现在认为网络很可能没有发生拥塞，因此现在不执行慢开始算法，即拥塞窗口 $cwnd$ 现在不设置为 1，而是设置为慢开始门限 $ssthresh$ 减半后的数值，然后开始执行拥塞避免算法（“加法增大”），使拥塞窗口缓慢地线性增大。

发送窗口的上限值

- 发送方的发送窗口的上限值应当取为接收方窗口 $rwnd$ 和拥塞窗口 $cwnd$ 这两个变量中较小的一个，即应按以下公式确定：发送窗口的上限值 $= \min[rwnd, cwnd]$
- 当 $rwnd < cwnd$ 时，是接收方的接收能力限制发送窗口的最大值。
- 当 $cwnd < rwnd$ 时，则是网络的拥塞限制发送窗口的最大值。

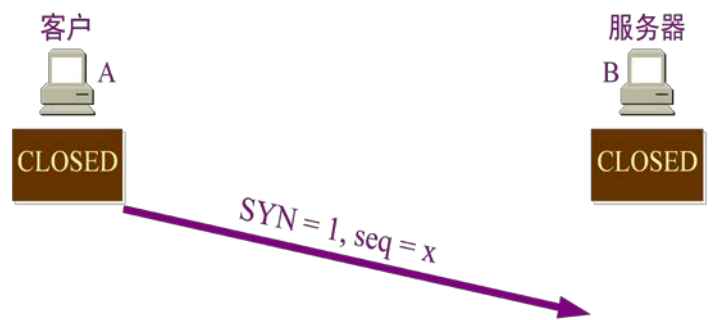
4、TCP 的运输连接管理

- 运输连接就有三个阶段，即：连接建立、数据传送和连接释放。运输连接的管理就是使运输连接的建立和释放都能正常地进行。
- 连接建立过程中要解决以下三个问题：
 - 要使每一方能够确知对方的存在。
 - 要允许双方协商一些参数（如最大报文段长度，最大窗口大小，服务质量等）。
 - 能够对运输实体资源（如缓存大小，连接表中的项目等）进行分配。

客户服务器方式

- TCP 连接的建立都是采用客户服务器方式。
- 主动发起连接建立的应用进程叫做客户（client）。
- 被动等待连接建立的应用进程叫做服务器（server）。

1) TCP 的连接建立



- ①A 的 TCP 向 B 发出连接请求报文段，其首部中的同步位 $SYN = 1$ ，并选择序号 $seq = x$ ，表明传送数据时的第一个数据字节的序号是 x 。
- ②B 的 TCP 收到连接请求报文段后，如同意，则发回确认。B 在确认报文段中应使 $SYN = 1$ ，使 $ACK = 1$ ，其确认号 $ack = x + 1$ ，自己选择的序号 $seq = y$ 。
- ③A 收到此报文段后向 B 给出确认，其 $ACK = 1$ ，确认号 $ack = y + 1$ 。A 的 TCP 通知上层应用进程，连接已经建立。
- ④B 的 TCP 收到主机 A 的确认后，也通知其上层应用进程：TCP 连接已经建立。

2) TCP 的连接释放

- ①数据传输结束后，通信的双方都可释放连接。现在 A 的应用进程先向其 TCP 发出连接释放报文段，并停止再发送数据，主动关闭 TCP 连接。
- ②A 把连接释放报文段首部的 $FIN = 1$ ，其序号 $seq = u$ ，等待 B 的确认。
- ③B 发出确认，确认号 $ack = u + 1$ ，而这个报文段自己的序号 $seq = v$ 。
- ④TCP 服务器进程通知高层应用进程。
- ⑤从 A 到 B 这个方向的连接就释放了，TCP 连接处于半关闭状态。B 若发送数据，A 仍要接收。
- ⑥若 B 已经没有要向 A 发送的数据，其应用进程就通知 TCP 释放连接。

7、A 收到连接释放报文段后，必须发出确认

- ⑧在确认报文段中 $ACK = 1$ ，确认号 $ack = w + 1$ ，自己的序号 $seq = u + 1$
- A 必须等待 $2MSL$ 的时间（TCP 连接必须经过时间 $2MSL$ 后才真正释放掉）

- 第一，为了保证 A 发送的最后一个 ACK 报文段能够到达 B。
- 第二，防止“已失效的连接请求报文段”出现在本连接中。A 在发送完最后一个 ACK 报文段后，再经过时间 $2MSL$ ，就可以使本连接持续的这段时间内所产生的所有报文段，都从网络中消失。这样就可以使下一个新的连接中不会出现这种

旧的连接请求报文段。

六、应用层

1、万维网必须解决的问题

(1) 怎样标志分布在整个因特网上的万维网文档？

- 使用统一资源定位符 URL (Uniform Resource Locator) 来标志万维网上的各种文档。
- 使每一个文档在整个因特网的范围内具有唯一的标识符 URL。

(2) 用何协议实现万维网上各种超链的链接？

- 在万维网客户程序与万维网服务器程序之间进行交互所使用的协议，是超文本传送协议 HTTP (HyperText Transfer Protocol)。
- HTTP 是一个应用层协议，它使用 TCP 连接进行可靠的传送。

(3) 怎样使各种万维网文档都能在因特网上的各种计算机上显示出来，同时使用户清楚地知道在什么地方存在着超链？

- 超文本标记语言 HTML (HyperText Markup Language) 使得万维网页面的设计者可以很方便地用一个超链从本页面的某处链接到因特网上的任何一个万维网页面，并且能够在自己的计算机屏幕上将这些页面显示出来。

(4) 怎样使用户能够很方便地找到所需的信息？

- 为了在万维网上方便地查找信息，用户可使用各种的搜索工具（即搜索引擎）。

鉴于本资料不断发现被转卖/盗卖/分享/转赠，这是对我们劳动成果的亵渎，因此我们极不愿意但却不得不做恶毒的申明以保护我们资料的价值；保证从我们处购买该资料用户的权益（付出的价格）。

申 明

本资料由职场精英工作室所有（唯一旺旺客服：慕蓝小小天使）；我们祝所有从这两处购买资料的用户顺利通过各个公司招聘笔面试取得心仪offer，一堆offer，高大上的offer。祝所有从别处购买/分享获得/获赠该资料的用户笔面试通通挂掉，祝所有转卖/盗卖/分享/转赠我们资料的商家/机构全家人间灭绝，户口销户