计算机网络复习整理

1 基础

什么是互联网?

互联网是由数量极大的各种计算机网络互连起来而形成的网络。

可以从两种不同的方面来认识互联网：互联网应用、互联网工作原理与特点。

互联网之所以能够向用户提供许多服务，是因为互联网具有两个重要基本特点：

- 连通性（Connectivity）：使上网用户之间都可以交换信息（数据，以及各种音频视频），好像这些用户的计算机都可以彼此直接连通一样。同时，互联网具有虚拟的特点，无法准确知道对方是谁，也无法知道对方的位置。
- 共享（Sharing）：
    - 指资源共享。
    - 资源共享的含义是多方面的。可以是信息共享、软件共享，也可以是硬件共享。
    - 由于网络的存在，这些资源好像就在用户身边一样，方便使用。

互联网基本概念

- 网络把许多计算机连接在一起。
- 互联网则把许多网络通过路由器连接在一起。
- 与网络相连的计算机常称为主机。

互联网的组成

从互联网的工作方式上看，可以划分为两大块：

- 边缘部分：由所有连接在互联网上的主机组成。这部分是用户直接使用的，用来进行通信（传送数据、音频或视频）和资源共享。
- 核心部分：由大量网络和连接这些网络的路由器组成。这部分是为边缘部分提供服务的（提供连通性和交换）。

主机和路由器的作用不同

- 主机是为用户进行信息处理的，并向网络发送分组，从网络接收分组。
- 路由器对分组进行存储转发，最后把分组交付目的主机。

网络协议的三个组成要素

- 语法：数据与控制信息的结构或格式。
- 语义：需要发出何种控制信息，完成何种动作以及做出何种响应。
- 同步：事件实现顺序的详细说明。

> 由此可见，网络协议是计算机网络的不可缺少的组成部分。

分层的好处与缺点

好处：

- 各层之间是独立的。
- 灵活性好。
- 结构上可分割开。
- 易于实现和维护。
- 能促进标准化工作。

缺点：

- 降低效率。
- 有些功能会在不同的层次中重复出现，因而产生了额外开销。

实体、协议、服务和服务访问点

- 实体（Entity）表示任何可发送或接收信息的硬件或软件进程。
- 协议是控制两个对等实体进行通信的规则的集合。
- 在协议的控制下，两个对等实体间的通信使得本层能够向上一层提供服务。
- 要实现本层协议，还需要使用下层所提供的服务。

分组交换

主要特点：

- 分组交换则采用存储转发技术。
- 在发送端，先把较长的报文划分成较短的、固定长度的数据段。

传输单元：

- 分组交换网以“分组”作为数据传输单元。
- 依次把各分组发送到接收端。

核心概念

带宽

- “带宽”（band width）本来是指信号具有的频带宽度，其单位是赫（或千赫、兆赫、吉赫等）。
- 在计算机网络中，带宽用来表示网络中某通道传送数据的能力。表示在单位时间内网络中的某信道所能通过的“最高数据率”。单位是“比特每秒”，或bit/s。

> 在计算机网络中，带宽用来表示网络中某通道传送数据的能力。表示在单位时间内网络中的某信道所能通过的“最高数据率”。单位是“比特每秒”，或*bit/s*。

吞吐量

- 吞吐量（through put）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。

时延

- 时延（delay）是指数据（一个报文或分组，甚至比特）从网络（或链路）的一端传送到另一端所需的时间。
- 有时也称为延迟或迟延。
- 网络中的时延由以下几个不同的部分组成：
    - 发送时延
    - 传播时延
    - 处理时延
    - 排队时延

利用率

- 分为信道利用率和网络利用率：
    - 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。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。

2 物理层

有关信道的几个基本概念

- 信道：一般用来表示向某一个方向传送信息的媒体。
- 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。

基本的带通调制方法

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。

信道复用技术

频分复用、时分复用和统计时分复用

波分复用

码分复用

3 数据链路层

三个基本问题

数据链路层协议有许多种，但有三个基本问题则是共同的。这三个基本问题是：

- 封装成帧
- 透明传输
- 差错控制

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。
- 地理范围和站点数目均有限。

局域网具有如下主要优点：

- 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。

适配器的作用

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。

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，并进行网络层配置，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。

> 可见，*PPP*协议已不是纯粹的数据链路层的协议，它还包含了物理层和网络层的内容。

CSMA/CD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。

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2t（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2t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。

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。

CMSA/CD协议的要点

1. 准备发送。但在发送之前，必须先检测信道。
2. 检测信道。若检测到信道忙，则应不停地检测，一直等待信道转为空闲。若检测到信道空闲，并在96比特时间内信道保持空闲（保证了帧间最小间隔），就发送这个帧。
3. 检查碰撞。在发送过程中仍不停地检测信道，即网络适配器要边发送边监听。这里只有两种可能性：
    - 发送成功：在争用期内一直未检测到碰撞。这个帧肯定能够发送成功。发送完毕后，其他什么也不做。然后回到1。
    - 发送失败：在争用期内检测到碰撞。这时立即停止发送数据，并按规定发送人为干扰信号。适配器接着就执行指数退避算法，等待r倍512比特时间后，返回到步骤2，继续检测信道。但若重传达16次仍不能成功，则停止重传而向上报错。

4 网络层

虚拟专用网VPN

- 利用公用的互联网作为本机构各专用网之间的通信载体，这样的专用网又称为虚拟专用网VPN（Virtual Private Network）。
- “专用网”是因为这种网络是为本机构的主机用于机构内部的通信，而不是用于和网络外非本机构的主机通信。
- “虚拟”表示“好像是”，但实际上并不是，因为现在并没有真正使用通信专线，而VPN只是在效果上和真正的专用网一样。

网络地址转换NAT

- 网络地址转换NAT（Network Address Translation）方法于1994年提出。
- 需要在专用网连接到互联网的路由器上安装NAT软件。装有NAT软件的路由器叫作NAT路由器，它至少有一个有效的外部全球IP地址。
- 所有使用本地地址的主机在和外界通信时，都要在NAT路由器上将其本地地址转换成全球IP地址，才能和互联网连接。

5 传输层TCP与UDP

UDP：一种无连接协议提供无连接服务。

- 在传送数据之前不需要先建立连接。
- 传送的数据单位协议是UDP报文或用户数据报。
- 对方的运输层在收到UDP报文后，不需要给出任何确认。
- 虽然UDP不提供可靠交付，但在某些情况下UDP是一种最有效的工作方式。

TCP：一种面向连接的协议。

- 提供面向连接的服务。
- 传送的数据单位协议是TCP报文段（segment）。
- TCP不提供广播或多播服务。
- 由于TCP要提供可靠的、面向连接的运输服务，因此不可避免地增加了许多的开销。这不仅使协议数据单元的首部增大很多，还要占用许多的处理机资源。

6 应用层

数字签名

用于证明真实性。数字签名必须保证以下三点：

1. 报文鉴别——接收者能够核实发送者对报文的签名（证明来源）；
2. 报文的完整性——发送者事后不能抵赖对报文的签名（防否认）；
3. 不可否认——接收者不能伪造对报文的签名（防伪造）。现在已有多种实现各种数字签名的方法。但采用公钥算法更容易实现。

防火墙

- 防火墙是由软件、硬件构成的系统，是一种特殊编程的路由器，用来在两个网络之间实施访问控制策略。
- 访问控制策略是由使用防火墙的单位自行制订的，为的是可以最适合本单位的需要。
- 防火墙内的网络称为“可信的网络”（trusted network），而将外部的因特网称为“不可信的网络”（untrusted network）。防火墙可用来解决内联网和外联网的安全问题。

防火墙的功能有两个：阻止和允许。

- “阻止”就是阻止某种类型的通信量通过防火墙（从外部网络到内部网络，或反过来）。
- “允许”的功能与“阻止”恰好相反。
- 防火墙必须能够识别通信量的各种类型。不过在大多数情况下防火墙的主要功能是“阻止”。

入侵检测系统

- 防火墙试图在入侵行为发生之前阻止所有可疑的通信。
- 入侵检测系统IDS（Intrusion Detection System）能够在入侵已经开始，但还没有造成危害或在造成更大危害前，及时检测到入侵，以便尽快阻止入侵，把危害降低到最小。
- IDS对进入网络的分组执行深度分组检查，当观察到可疑分组时，向网络管理员发出告警或执行阻断操作（由于IDS的“误报”率通常较高，多数情况不执行自动阻断）。
- IDS能用于检测多种网络攻击，包括网络映射、端口扫描、DoS攻击、蠕虫和病毒、系统漏洞攻击等。

两种入侵检测方法：

- 基于特征的IDS维护一个所有已知攻击标志性特征的数据库。这些特征和规则通常由网络安全专家生成，机构的网络管理员定制并将其加入到数据库中。基于特征的IDS只能检测已知攻击，对于未知攻击则束手无策。
- 基于异常的IDS通过观察正常运行的网络流量，学习正常流量的统计特性和规律。当检测到网络中流量某种统计规律不符合正常情况时，则认为可能发生了入侵行为。

> 至今为止，大多数部署的*IDS*主要是基于特征的，尽管某些*IDS*包括了某些基于异常的特性