计算机网络-2025-1-12

各章节知识点

概述

广域网、城域网和局域网的区别

- **局域网 (LAN)：** 就像你家或者办公室里的网络，范围比较小，比如一个房间、一栋楼，主要用来连接附近的电脑、打印机等设备。
- **城域网 (MAN)：** 比局域网大一点，覆盖一个城市或者几个街区，连接多个局域网，比如学校或者公司总部网络。
- **广域网 (WAN)：** 范围非常大，可以跨越城市、国家甚至全球，比如互联网。它用来连接不同地区的网络，让大家可以互相通信。

> **规模从小到大，局域网 < 城域网 < 广域网。**

客户端-服务器和对等P2P的区别

- **客户端-服务器：** 就像餐厅点菜一样，你需要先跟服务员（服务器）点菜，服务员会把你的请求传给厨师，厨师做完菜再给服务员，然后服务员再给你送过来。
  - **客户端**：你的电脑、手机，用来发送请求和接收数据。
  - **服务器**：存储数据、处理请求的电脑，比如网站的服务器。
- **对等P2P：** 就像朋友之间互相分享文件，大家都是平等的，谁都可以请求和提供数据，不需要专门的服务器。比如用BT下载电影。

> **客户端-服务器有专门的“服务中心”，P2P是大家“互相帮助”（去中心化）。**

互联网的三种主要交换方式

- **电路交换：** 就像打电话，双方建立一条专属的“电路”，其他人的数据不能插进来，通话结束再断开连接。这种方式比较固定，但资源利用率不高。
- **报文交换：** 就像寄快递，每个快递（报文）都包含目的地地址，经过不同的菜鸟驿站中转最终到达。这种方式比较灵活，但数据量大的时候可能会慢。
- **分组交换：** 就像把包裹拆分成小件，每个小件（分组）都包含目的地地址，经过不同路径到达，然后再组装成完整的包裹。这种方式效率高、可靠性高，现在互联网主要用这种方式。

> **简单来说，就是打电话(电路交换)、寄快递(报文交换)、拆分包裹(分组交换)。**

OSI的7层体系结构

OSI（开放系统互联）模型，就像一个规范，把网络通信分成七层，每一层负责不同的事情，就像盖房子一样，每一层都有自己的职责：

- **应用层：** 用户能直接看到的一层，比如浏览器、邮件软件。
- **表示层：** 把数据转换成不同的格式，比如加密解密。
- **会话层：** 建立、管理和结束两个程序之间的通信会话。
- **传输层：** 负责把数据从一个地方安全地送到另一个地方，比如TCP和UDP协议。
- **网络层：** 负责给数据包选择最佳路径，比如IP协议。
- **数据链路层：** 负责在网络中传输数据，比如以太网协议。
- **物理层：** 负责传输二进制数据，比如网线、光纤。

> **就像盖房子，从钢筋(物理层)到家电(应用层)，每层都有自己的任务。**

TCP/IP的4层体系结构

- **应用层：** 包含各种应用程序，比如HTTP、FTP。
- **传输层：** 负责可靠或不可靠的数据传输，比如TCP和UDP协议。
- **网络层：** 负责数据包的路由，比如IP协议。
- **网络接口层：** 负责物理连接和数据传输。

> **TCP/IP模型比OSI模型更简洁**

物理层

导引型媒体有哪些？（同轴电缆、光纤、双绞线）有什么特点？

- **同轴电缆：**
  - **特点：** 铜芯，外面包裹着绝缘层和屏蔽层。
  - **优点：** 传输距离相对较远，抗干扰能力较强。
  - **缺点：** 成本较高，体积较大，安装不方便。
- **光纤：**
  - **特点：** 玻璃或塑料，利用光来传输信号。
  - **优点：** 传输速度快，带宽大，抗干扰能力强，损耗小。
  - **缺点：** 成本高，安装维护复杂，接口比较脆弱。
- **双绞线：**
  - **特点：** 将两根绝缘的铜线互相缠绕在一起，减少电磁干扰。就像我们常用的网线。

- **优点：** 成本低，安装方便，应用广泛。
- **缺点：** 传输距离相对较短，抗干扰能力较弱。

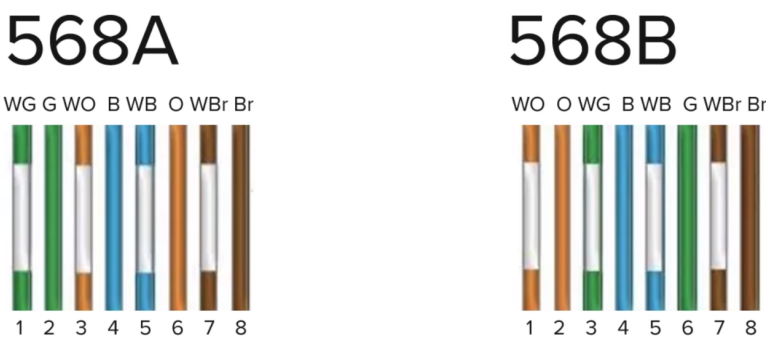
> **同轴电缆：铜芯电线；光纤：细玻璃线；双绞线：类麻花缠绕的线。**

- **568A:**

  绿白 绿 橙白 蓝 蓝白 橙 棕白 棕

- **568B:**

  橙白 橙 绿白 蓝 蓝白 绿 棕白 棕



数据链路层

数据链路层的三个基本问题

- **封装成帧：** 将来自网络层的数据包，加上一些额外信息，变成可以在物理链路上发送的“帧”，就像给包裹贴上标签。
- **透明传输：** 确保数据中包含的特殊字符，不会被误认为是帧的边界，就像寄快递时，不会把包裹上的地址信息当成包裹本身。
- **差错控制：** 在传输过程中，可能会出现数据错误，数据链路层会检查并纠正错误，就像快递员会仔细检查包裹是否完好。

CSMA/CD机制的原理

CSMA/CD (载波侦听多路访问/冲突检测) 是一种早期的网络协议，用于避免多并发。

- **载波侦听 (CS)：** 发送数据之前，先听听信道有没有人说话（是否有其他设备在发送数据）。
- **多路访问 (MA)：** 如果信道空闲，就发送数据。
- **冲突检测 (CD)：** 如果发送数据的时候，同时发现其他设备也在发送数据，就立刻停止发送，等待一段时间，然后重试。

> **“先听再说，边说边看，撞车停下，稍后再来”**。 就像马路上开车，先看看有没有车再起步，如果发现撞车，就先停下，等一会儿再重新开。

MAC地址的格式和特点

> 每一块网卡都有独一无二的MAC地址。

- **格式：** MAC地址是48位的二进制数，通常写成六组两个十六进制数，每两个数之间用冒号或者短横线隔开，比如 `00-1A-2B-3C-4D-5E` 。
- **特点：**
  - **全球唯一：** 每一个网卡的MAC地址都是不同的。
  - **固化：** MAC地址是由厂家写入网卡芯片的，一般不能修改。
  - **用于数据链路层：** MAC地址主要用于局域网内的数据传输。

> **MAC地址独一无二且固定，用于在局域网内找到设备。**

冲突域、广播域的意思和区别

- **冲突域：** 指的是一个区域内，如果多台设备同时发送数据，就会发生冲突（数据互相碰撞），导致数据丢失。就像一条马路上，如果大家不按规则，一起开车，就会撞车。
- **广播域：** 指的是一个区域内，发送一个广播消息，所有设备都能接收到。就像在班级里喊一声，所有同学都能听到。

集线器、交换机和路由器如何切割冲突域和广播域

- **集线器（Hub）：**
  - **特点：** 所有设备共享一个冲突域，一个广播域。
  - **作用：** 像一个“大喇叭”，收到数据就向所有端口转发，容易产生冲突。
- **交换机（Switch）：**
  - **特点：** 每个端口都是独立的冲突域，所有端口共享一个广播域。
  - **作用：** 知道数据应该发给哪个端口，可以减少冲突。
- **路由器（Router）：**
  - **特点：** 每个端口都是独立的冲突域，也是独立的广播域。
  - **作用：** 在不同的网络之间转发数据，可以分隔广播域。

> **集线器是“大家挤在一条路上”，交换机是“大家走自己的路”，路由器是“无视路况走自己的”**

交换机自学习算法的原理（泛洪机制）

- **泛洪（Flooding）：**
  - 当交换机收到一个数据帧，如果不知道目的MAC地址对应的端口，就向所有端口（除了接收端口）转发数据。宿舍窗台收到了一个外卖，你不知道署名“O将军”是谁，就一个一个问室友。
- **学习：**
  - 交换机收到数据帧后，会记录发送数据帧的端口和源MAC地址的对应关系，放到MAC地址表里。外卖给“O将军”后，就知道O将军是谁了
- **转发：**

- 下次收到相同目的MAC地址的数据帧，交换机就可以根据MAC地址表，直接把数据帧转发到对应的端口，不用再泛洪。再收到O将军的外卖直接给O将军了

好的，我们来用简单易懂的方式解释一下图片中的内容：

网络层

IP地址的特点，分类编址方案（A、B、C类如何区分）

- **IP地址的特点：**
  - **逻辑地址：** IP地址是网络层的逻辑地址，用于标识网络中的设备，就像你家的门牌号。
  - **全球唯一性：** 在互联网上，每个设备的IP地址是唯一的，但局域网内可以重复使用。
  - **分层结构：** IP地址分为网络号和主机号两部分，类似于城市的区号和街道门牌号，可以帮助路由。
- **分类编址方案（A、B、C类如何区分）**
  - **A类：** 第一个字节的范围是1-126，网络号占1个字节，主机号占3个字节。适用于大型网络，比如大学和政府机构，拥有很多主机。
  - **B类：** 第一个字节的范围是128-191，网络号占2个字节，主机号占2个字节。适用于中型网络，比如大型公司。
  - **C类：** 第一个字节的范围是192-223，网络号占3个字节，主机号占1个字节。适用于小型网络，比如家庭和小型企业。
  - **区分方法：** 主要看IP地址的第一个字节所在的范围。

> **IP地址就像设备的“网络身份证”，A、B、C类就像是不同大小的“小区”，A类小区最大，C类小区最小。**

如何通过IP地址计算出当前的网络号，和该网络可用地址

- **计算网络号：**
  - 需要知道IP地址和子网掩码。
  - 将IP地址和子网掩码都转换为二进制形式，然后进行“与”运算（AND操作）。
  - “与”运算的结果就是网络号。
- **计算可用地址：**
  - 知道网络号和子网掩码后，剩下的就是主机号的位数。
  - 主机号的位数，去掉全0的网络地址和全1的广播地址，剩下的就是可用主机地址的数量。

如何进行子网划分，如何根据当前网络需求设计合理的子网掩码长度，并计算出每一个子网的可用地址段

- **子网划分：** 将一个大的网络划分成多个小的子网，可以更有效地利用IP地址，更好地管理网络。就像把大公寓分割成多个小房间。
- **设计合理的子网掩码长度：** 根据需要的子网数量和每个子网的主机数量来确定子网掩码的长度。可以通过借用主机号的位数来作为子网号。
- **计算子网的可用地址段：**
  - 计算出子网号。
  - 每个子网的地址范围：网络号 + 子网号 + 主机号。

静态路由协议和动态路由协议的区别

- **静态路由协议：**
  - 管理员手动配置路由，指定数据包的转发路径。
  - 简单、可靠，适用于小型网络，路由不会根据网络变化自动调整。
  - 就像预先规划好的固定路线，不会根据交通状况调整。
- **动态路由协议：**
  - 路由器之间通过互相交换路由信息来动态地计算和更新路由，可以根据网络变化自动调整。
  - 复杂、灵活，适用于大型网络，可以自动适应网络的变化。
  - 就像导航软件，会根据交通状况，实时规划最佳路线。

路由表是如何查找路由的？（最长掩码匹配原则）

- **路由表：** 路由器中存储路由信息的表格，记录着目标网络、下一跳地址、接口等信息。
- **查找路由：** 路由器收到数据包后，会根据目标IP地址，在路由表中查找对应的路由条目。
- **最长掩码匹配原则：** 如果有多个路由条目都能匹配目标IP地址，路由器会选择掩码最长的路由条目，也就是匹配最精确的路由。就像快递员先看门牌号，再看街道名称，精确匹配可以更快找到目的地。

RIP协议、OSPF协议的基本工作原理

- **RIP协议（路由信息协议）：**
  - 是一种基于距离向量的动态路由协议。
  - 路由器每隔一段时间向相邻路由器发送路由信息，计算到目标网络的跳数，跳数越多，路径越远。
  - 简单，容易实现，但只适用于小型网络，收敛速度慢。
  - 就像大家互相传递信息说“我到那个地方要几步”，选择步数最少的。
- **OSPF协议（开放最短路径优先协议）：**
  - 是一种基于链路状态的动态路由协议。

- 路由器之间交换链路状态信息，建立整个网络的拓扑结构，然后通过算法计算出到每个目标网络的最短路径。
- 复杂，效率高，适用于大型网络，收敛速度快。
- 就像大家互相报告说“这条路通不通，有多长”，然后找出最短的路线。

> **RIP就像简单传话，OSPF就像建立完整的地图，再找最佳路线。**

运输层

端口号

- **作用：** 端口号就像你家大门上的房间号，用于标识一台计算机上运行的不同应用程序或服务。
- **范围：** 端口号是一个16位的整数，范围是0到65535。
- **分类：**
  - **知名端口号（0-1023）：** 分配给一些常用的服务，HTTP (80)、HTTPS (443)、FTP (21)。
  - **注册端口号（1024-49151）：** 分配给一些特定的应用程序，比如QQ、微信。
  - **动态/私有端口号（49152-65535）：** 用于客户端临时连接时使用的端口。

UDP协议和TCP协议的区别

- **TCP协议：**
  - **可靠传输：** 类似于打电话，发送数据之前需要先建立连接，保证数据按顺序、可靠地送达。
  - **面向连接：** 需要先进行“三次握手”建立连接，数据传输结束后，需要“四次挥手”关闭连接。
  - **传输速度：** 速度较慢，但可靠性高，适合传输重要数据，比如浏览网页、下载文件。
- **UDP协议：**
  - **不可靠传输：** 类似于发短信，不需要建立连接，只管把数据发送出去，不保证数据一定能到达，也不保证顺序。
  - **无连接：** 不需要建立连接，速度快，但不可靠，适合传输对实时性要求高，但对丢包不敏感的数据，比如直播、csgo。

> **TCP保证数据完整性；UDP不管数据是否完整发出去就不管了爱接不接，延迟很低。**

TCP协议建立连接的三次握手

1. **第一次握手（SYN）：** 客户端向服务器发送一个SYN（同步）包，表示请求建立连接。
2. **第二次握手（SYN+ACK）：** 服务器收到SYN包后，回复一个SYN+ACK（同步+确认）包，表示同意建立连接。

3. **第三次握手（ACK）：** 客户端收到SYN+ACK包后，回复一个ACK（确认）包，表示连接建立完成。

> **“你好，我想跟你说话”，“好的，我收到了，我们开始说话吧”，“好的，开始吧”。**

TCP协议关闭连接的四次挥手：

1. **第一次挥手（FIN）：** 客户端发送一个FIN（结束）包，表示请求关闭连接。
2. **第二次挥手（ACK）：** 服务器收到FIN包后，回复一个ACK包，表示收到了关闭连接的请求。
3. **第三次挥手（FIN）：** 服务器发送一个FIN包，表示服务器的数据也发送完了，请求关闭连接。
4. **第四次挥手（ACK）：** 客户端收到FIN包后，回复一个ACK包，表示连接关闭完成。

> **“我话说完了，再见”，“好的，我知道了，你先走吧”，“我也说完了，再见”，“好的，我也走啦”。**

应用层

DNS协议（域名系统协议）：

DNS协议就像一个“编译器”，负责将我们熟悉的域名（比如www.google.com）转换成计算机可以识别的IP地址（比如172.217.160.142）。

DHCP协议（动态主机配置协议）：

DHCP协议就像一个“自动化IP配置”，负责给局域网内的设备自动分配IP地址、子网掩码、网关等网络配置信息。

HTTP协议（超文本传输协议）：

HTTP协议是用于在Web浏览器和Web服务器之间传输超文本的协议，也就是我们访问网站时所用的协议。

例题

例题1：已知B市的某个互联网公司刚刚从运营商申请到了一段IP地址：`152.23.128.69/27`

1. **这段地址段的网络地址和广播地址分别是多少？.**

计算网络地址：

- 先把IP地址转换成二进制：
  `10011000.00010111.10000000.01000101`
- 子网掩码的二进制表示（前27位是1，后5位是0）：
  `11111111.11111111.11111111.11100000`

- 把IP地址和子网掩码进行按位与操作（AND运算），得到网络地址：
  `10011000.00010111.10000000.01000000`
- 把二进制网络地址转换成十进制：
  `152.23.128.64`

计算广播地址：

- 广播地址的计算方法是：网络地址的主机位全部设为1。
- 网络地址二进制：
  `10011000.00010111.10000000.01000000`
- 将主机位（后5位）全部设置为1：
  `10011000.00010111.10000000.01011111`
- 将二进制广播地址转换成十进制：
  `152.23.128.95`

2. **这段地址段的可用地址数有多少？**

   2（32-掩码位数）-2（减的是网络地址和广播地址）**

   2**(32-27)-2=30

3. **请列出可用地址的范围。（第一个可用 - 最后一个可用）**

   152.23.128.65-152.23.128.94

例题2：已知一台主机的IP地址是128.60.248.21，子网掩码是255.255.255.224.

1. **计算网络号并用CIDR表示：**
   - 先把IP地址和子网掩码转换成二进制：
     - IP地址： `10000000.00111100.11111000.00010101`
     - 子网掩码： `11111111.11111111.11111111.11100000`
   - 将IP地址和子网掩码进行按位与操作（AND运算）得到网络号：

     `10000000.00111100.11111000.00000000`

     `128. 60. 248. 0`
   - 数子网掩码中1的个数，得出子网掩码长度： `27`
   - CIDR表示网络号，即 `128.60.248.0/27`
2. **确定新的子网掩码：**
   - 为了保证每个子网的可用主机数不少于5台，我们需要计算一下每个子网的主机地址需要几位二进制数。
   - 如果主机地址有3位，那么就有 2^3 = 8 个IP地址，减去网络地址和广播地址，剩下6个可用的。

- 如果主机地址有2位，那么就有 2^2 = 4 个IP地址，减去网络地址和广播地址，剩下2个可用的，不够5个。
- 所以，我们需要至少3位作为主机地址，也就是子网掩码的二进制中要有29位是1，剩下的3位是0。
- 所以，新的子网掩码的二进制表示为：`11111111.11111111.11111111.11111000`
- 将二进制子网掩码转换为十进制表示：`255.255.255.248`

3. **列出划分后每个子网的可用地址范围：**
   - 使用子网掩码 `255.255.255.248` 或者 `/29` 进行子网划分。
   - 因为主机地址有3位，所以每个子网包含 2^3 = 8 个IP地址，其中6个是可用地址。

- **第一个子网：**
  - 网络地址：`128.60.248.0/29` 后八位：0000 0000
  - 可用地址范围：`128.60.248.1 - 128.60.248.6`

（128.60.248.7作为第一个子网的广播号，128.60.248.8作为第二个子网的网络号）

- **第二个子网：**
  - 网络地址：`128.60.248.8/29` 后八位：0000 1000
  - 可用地址范围：`128.60.248.9 - 128.60.248.14`
- **第三个子网：**
  - 网络地址：`128.60.248.16/29` 后八位：0001 0000
  - 可用地址范围：`128.60.248.17 - 128.60.248.22`
- **第四个子网：**
  - 网络地址：`128.60.248.24/29` 后八位：0001 1000
  - 可用地址范围：`128.60.248.25 - 128.60.248.30`

例题3：假设某个路由器建立了如下转发表

A	B	C	D
序号	**目的网络**	**子网掩码**	**下一跳地址**
1	10.0.0.0	8	Eth0
2	10.0.0.0	16	Eth1
3	10.0.0.0	17	Eth2
4	10.0.128.0	17	Eth3
5	0.0.0.0	0	Eth4

- **目的地址：`10.0.130.25`，下一跳是多少？**
  - Eth3:
    - 目的网络：`10.0.128.0/17`
    - 二进制IP地址：`00001010.00000000.10000000.00000000`
    - 子网掩码二进制：`11111111.11111111.10000000.00000000`
    - 按位与运算：`00001010.00000000.10000000.00000000`（即`10.0.128.0`）
- **目的地址：`192.168.1.24`，下一跳是多少？**
  - Eth4:
    - 目的网络：`192.168.1.24`
    - 二进制IP地址：`11000000.10101000.00000001.00011000`
    - 子网掩码二进制：`00000000.00000000.00000000.00000000`
    - 按位与运算：`00000000.00000000.00000000.00000000`（即`0.0.0.0`）

例题4：假设某台路由器的路由表如下

	A	B	C
1	**目的网络**	**距离**	**下一跳**
2	N1	7	A
3	N2	5	C
4	N3	2	F
5	N4	8	E
6	N5	4	F

请问，当收到以下路由信息更新时，数据如何变化？

1. **目的网络 N2，距离为 3：**
   - **当前路由表：** N2 的距离是 5，下一跳是 C。
   - **新的路由信息：** N2 的距离是 3。
   - **更新结果：** 由于新的距离 3 小于当前距离 5，因此路由表更新：将 N2 的距离改为 3，下一跳不变，假设为新的下一跳G（根据实际情况）。
2. **目的网络 N3，距离为 5：**
   - **当前路由表：** N3 的距离是 2，下一跳是 F。
   - **新的路由信息：** N3 的距离是 5。
   - **更新结果：** 由于新的距离 5 大于当前距离 2，因此路由表保持不变。
3. **目的网络 N5，距离为 4：**

- **当前路由表：** N5 的距离是 4，下一跳是 F。
- **新的路由信息：** N5 的距离是 4。
- **更新结果：** 由于新的距离 4 等于当前距离 4，路由表保持不变（RIP）或负载均衡（OSPF/EIGRP）。

4. **目的网络 N6，距离为 2：**
   - **当前路由表：** 路由表中没有 N6。
   - **新的路由信息：** N6 的距离为 2。
   - **更新结果：** 由于这是新的目标网络，因此将 N6 添加到路由表，距离为2，假设下一跳为H。

> 距离小于（更优节点）等于（负载均衡）当前距离则会添加进路由表，或者不存在的节点也会添加进路由表。

任何有误请联系Au1Bhi@163.com