2020/08/05_网络编程_第1课_计算机相关的硬件设备、各种协议介绍

笔记本: 网络编程
创建时间: 2020/8/5 星期三 10:13
作者: ileemi

前言

搞明白身边的网络设备的作用，网络数据是怎样传输的。

分组交换技术，一台计算机向另一台计算机传输数据的时候，将传输的数据进行拆分（拆分多分），通过网络传输到目标计算机后，将接收到的拆分数据进行组装。

计算机网络

根据其规模可以分为WAN（广域网）和 LAN（局域网），

ISP（Internet Service Provider）：互联网服务提供商，即向广大用户综合提供互联网接入业务、信息业务和增值业务的电信运营商。

分组传输

> 分组交换十指将大数据分割为个个叫包（ pakcet）的较小单位进行传输的方法。

要传输的数据通过源计算机网卡 --> 分组（数据包） --> 目标计算机网卡 --> 组装
分组需要定义协议

计算机中的协议

在计算机通信中，事先达成一个详细的约定，并遵循这一约定进行处理尤为重要，这种约定其实就是“协议"。

协议标准化

在计算机通信诞生之初，系统化与标准化未得到足够的重视。每家计算机产商都出产各自的网络产品来实现计算机通讯。对于协议的系统化分层化等事宜没有特别强烈的意识。随着积极重要性的不断提高，很多公司逐渐意识到兼容的重要性。人们开始着手研究不同产商的异构机型也能够相互通信的技术。

为了解决上述问题，ISO 制定了一个国际标准 OSI（分层抽象），对通信系统进行了标准化。现在SI所定义的协议虽然并没有得到普及。但是在 OSI 协议设计之初作为其指导方针的 OSI 参考模型却常被用于网络协议的制定当中。

OSI 参考模型 -- 7层抽象层

7 -- **应用层**（针对特定应用的协议 -- 电子邮箱协议，远程登录协议，文件传输协议等） -- 网络开发在应用层
6 -- **表示层**（设备固有数据格式和网络标准数据格式的转换）
5 -- **会话层**（负责通讯管理）

4 -- **传输层**（管理两个结点之间的数据传输。负责可靠传输（确保数据的可靠传送到目标地址））
3 -- **网络层**（解决数据接收，寻址的问题 -- 地址管理与路由选择）
2 -- **数据链路层**（解决数据的分组与组装） -- 硬件（网卡负责）
1 -- **物理层** （数据的传输 -- 0，1）

每层的耦合性比较低，层之间影响较少，每一层都有属于自己的协议，光纤传输的是光信号（反射）要比双绞线（电）传输数据的速度快。

TCP/IP 协议群

正在使用的模型。

20世界60年代，很多大学和研究机构都开始着力于新的通信技术。其中有一家以美国国防部为中心的组织也展开了类似的研究。美国国防部认为研发新的通信技术对于国防军事有着举足轻重的作用。该组织希望我在通信传输的过程中，即使遭到了敌方的攻击和破坏，也可以经过**迂回线路**实现最终的通信，保证通信不中断。

ARPANET 网络

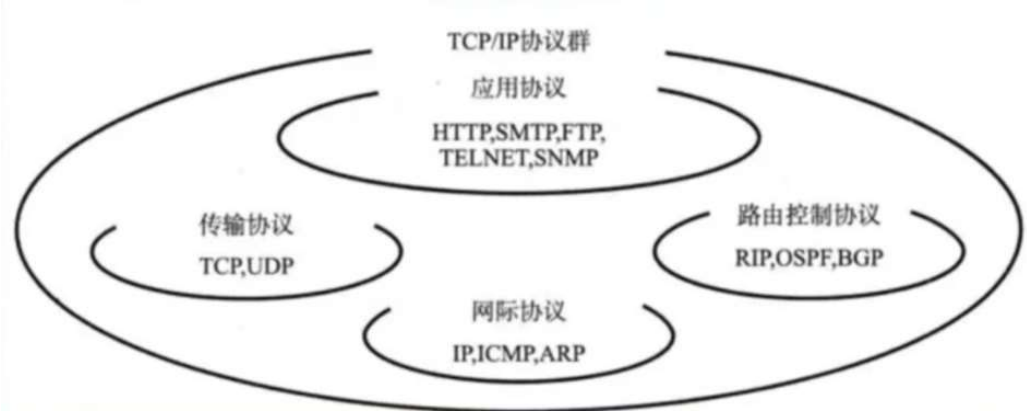
互联网的鼻祖 -- 阿帕网（最早的广域网）

1969年，为严重分组交换技术的实用性，研究人员搭建了一套网络。起初，该网络只连接了美国西海岸的大学和研究所等4个节点。之后，随着美国国防部的重点开发和先关技术的飞速发展，普通用户也逐渐加入其中，发展成了后来的巨大规模的网络。该网络被人们称为 **ARPENET**，也是全球互联网的鼻祖。

TCP/IP的规范

网络编程：自定义协议，使用已存在的标准化的协议

20世纪90年代，ISO 开展了 OSI 这一国际标准协议的标准化进程。然后 OSI 协议并没有得到普及，真正被广泛使用的是 TCP/IP 协议。从字面上意义讲，有人可能会认为 TCP/IP 是指 TCP 与 IP 两种协议。实际生活当中有时也确实指这两种协议。然而在很多情况下，它只是利用IP进行通信时所必须用到的协议群的统称。



互联网

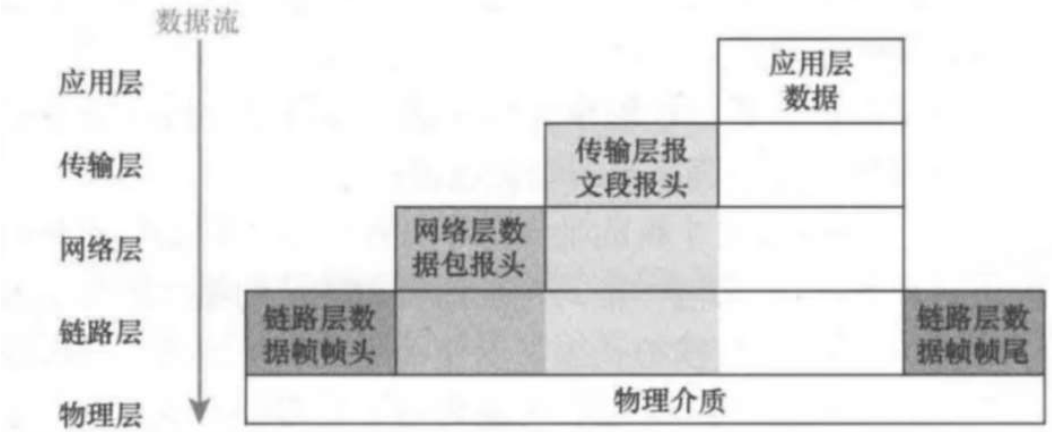
互联网是指由 ARPANET 发展而来、互联全世界的计算机网络。现在，互联网已经是一个专有名词了，其它对应的英文单词为 "The Internet"。

TCP/IP 协议

1 -- **应用层**（应用层，表示层，会话层） -- 应用程序
2 -- **传输层**（各种协议, 学习TCP, UDP） -- 操作系统（操作系统API基于TCP, UDP协议）
3 -- **网络层**（ARP, IP, ICMP协议） -- 操作系统
4 -- **数据链路层（数据链路层，物理层（网卡和网线合并）**） -- 设置驱动程序与网络接口（硬件）网卡
5 -- **物理层** -- 有硬件协议负责

从应用层传输数据的时候，传输层，网络层，数据链路层会在数据头前分别添加包头，用于目标识别。

TCP/IP 协议格式



数据链路层

以太网协议规定了光纤，双绞线或者铜电缆的协议。

> 链路层的传输单元:
> 链路层的数据传输单元成为帧。实体之间通过链路层彼此发送帧数据。
> 链路层的职责包括
> 定义主机的唯一标识方法
> 定义帧的格式
> 定义帧的长短
> 定义一种将帧转为电子信号的物理方法

以太网协议

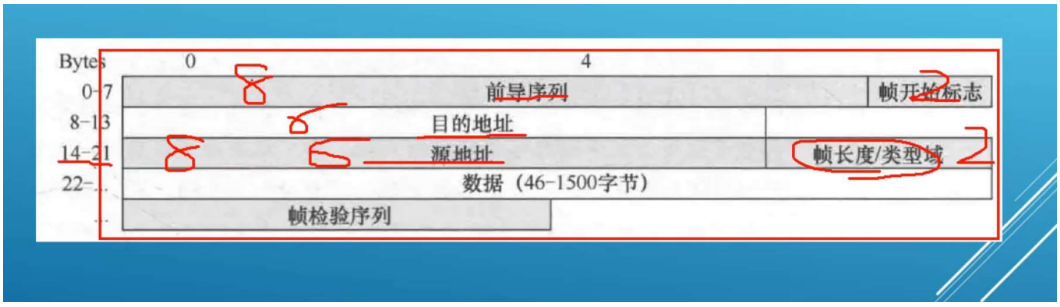
数据链路层

以太网（ Ethernet）不是一个协议，而是基于以太网蓝皮书的一组协议以太网蓝皮书是由美国DEC,Inte1和 Xerox公司于1980年发布的。同时，现代的以太网协议是在IEEE802.3的基础上定义的。用于光纤、双绞线或者铜电缆上的以太网协议各种各样。各种类型的速度也不同。

MAC 地址

在互联网中识别一台计算机的唯一标志就是通过MAC地址。

帧协议



帧最大传输单元（MTU）-- 每一帧可以发送的可行数据（46 - 1500字节）

数据 < 1400的时候通过各层不需要添加头包，此时发送速度最快

交换机

解决局域网的通讯问题（寻址）

交换机内部的 CPU 会在每个端口成功连接时，通过将 MAC 地址和端口对应形成一张 MAC 表。在今后的通讯中，发往该 MAC 地址的数据包将仅送往其对应的端口，而不是所有的端口。因此，交换机可用于划分数据链路层广播，即冲突域；但它不能划分网络层广播，即广播域。

网卡可以和交换机进行连接。

MAC地址

MAC网卡坏的时候，不能和其它计算机进行通讯，MAC地址是唯一的。交换机中的MAC地址表会找不到坏的MAC地址计算机。

解决办法：需要将MAC地址绑定一个编号，当网卡坏的时候，更改编号对应的MAC地址（IP地址）。每个IP地址绑定一个MAC地址。

网络层 IP协议

> 链路层提供了将数据从一台可寻址的主机发送到另外一台或者多台同样可寻址的主机的一种清晰的方式。因此，TCP/IP模型还需要更多的层次来解决问题。

链路层问题：

- 硬件中的MAC地址限制了硬件的灵活性
- 链路层不支持将互联网划分成更小的局域网络
- 链路层不支持不同的链路层协议进行通讯

IP协议版本：IPV4，IPV6

IPV4

实现网络层需求最常用的协议是互联网协议第四版（ Internetprotocol version4,IPv4)。IPv4定义了一个为每台主机单独标识的逻辑寻址系统，一个定义地址空间的逻辑分段作为物理子网的子网系统，一个在子网之间转发数据的路由系统。

IPv4的核心是IP地址。IP地址是32为bit数字，通常以英文句号分割的4个8bit数字的形式展示（4个字节定义一个地址）。例如：192.168.9.1，255.255.255.25

Send(0.0.0.1 "Hello World");

IP地址 --绑定-- MAC地址
0.0.0.1 -- MAC地址1（损坏）
0.0.0.1 -- MAC地址2（不影响发送数据）

IP地址由 **网络标识** 和 **主机标识** 两部分组成

IP地址的分类

A类 -- 广域网（需要自己向美国申请，但是地址已经分配完了）
B类 -- 广域网（个人宽带）
C类 -- 局域网
D类

A类：0.0.0.0 ~ 127.0.0.0 -- 16777214主机
B类：128.0.0.1 ~ 191.255.0.0 -- 35534主机
C类：192.168.0.0 ~ 239.255.255.0 -- 254主机
D类：224.0.0.0 ~ 239.255.255.255 多播

同一个子网（C类）：

192.168.0.0
192.168.0.1

子网掩码

为了局域网而发明的，用 IP 地址和子网掩码解决局域网IP地址分配不够用的情况。

> 同一个子网（与255.255.0.0进行相与）：
> 192.168.1.1
> 255.255.0.0 --> 192.168.0.0
> 192.168.0.1
> 255.255.0.0 --> 192.168.0.0

子网掩码 设置为 0.0.0.0 后，不能联网

路由器

内部有张表，记录 IP 地址，以 IP 地址来区分计算机，通过哪个路径将数据传输到目标计算机中。

路由器内部有一个匹配的网卡地址。

路由器的效率要比交换机低。

网关

路由器的IP地址就是网关（默认网关：192.168.0.1）

网关实质上是一个网络通向其他网络的IP地址。比如有网络A和网络B网络A的IP地址范围为 "192.168.1.1~192.168.1.254"，子网掩码为 255.255.255.0; 网络B的IP地址范围为
192.168.2.1~192.168.2.254", 子网掩码为 255.255.255.。在没有路由器的情况下，两个网络之间是不能进行TCP/IP通信的，即使是两个网络连接在同一台交换机（或集线）上、TCP/P协议也会根据子网掩码（255.255.255.0)判定两个网络中的主机处在不同的网络里。而要实现这两个网络之间的通信，则必须通过网关。如果网络A中的主机发现数据包的目的主机不在本地网络中，就把数据包转发给它自己的网关，再由网关转发给网络B的网关，网络B的网关再转发给网络B的某个主机。网络A向网络B转发数据包的过程。

IPV6

32bit 地址的 IPv4 允许 40亿 个不同的地址。由于子网的存在，使得比 40亿 更多的主机连接在互联网上。虽然如此，由于互联网的发展，32bit的IP地址已经被用完了。VPv6 的创建解决了这个问题。

IPV6 使用 128bit 来表示，可以写成冒号分隔的 8 组数，每一组 4 个十六进制数。

格式	地址
完整形式	2001:4a60:0000:8f1:0000:0000:0000:1013
前导零压缩法	2001:4a60:0:8f1:0:0:0:1013
双冒号法	2001:4a60:0:8f1::1013

ARP（地址解析协议）

只要确定了 IP 地址，就可以向这个目标地址发送数据包。然而，在底层数据链路层，进行实际通信时却又必要连接每个 IP 地址所对应的 MAC 地址。

ARP 是一种解决地址问题的方案。以目标 IP 地址为线索，用来定位下一个应该接收数据分包的网络设备对应的MAC 地址。如果目标主机不再同一链路上时，可以通过 ARP 查找条路由器的 MAC 地址。IPv6 不使用 ART 适用 ICMPVI6.

地址解析协议是建立在网络中各个主机互相信任的基础上的，局域网络上的主机可以自主发送 ARP 应答消息，其他主机收到应答报文时不会检测该报文的真实性就会将其记入本机 ARP 缓存；由此攻击者就可以向某一主机发送伪 ARP 应答报文，使其发送的信息无法到达预期的主机或到达错误的主机，这就构成了一个 ARP 欺骗。ARP 命令可用于查询本机 ARP 缓存中 IP 地址和 MAC 地址的对应关系、添加或删除静态对应关系等。相关协议有RARP、代理 ARP。NDP 用于在 IPv6 中代替地址解析协议。

传输层

网络层的任务是实现远程网络上两台遥远之间的通信，而传输层的任务是实现这些主机上单独进程之间的通信。因为一台主机同时运行很多进程，只知道主机A给主机B发了一个IP数据包是远远不够的。

端口（port）

端口号（2个字节）

> 为了解决这问题，传输层引入了端口（port）的概念。端口是 16bit 的无符号数，是一台特定主机的通信端点。
> 为了避免进程争夺端口，互联网名称与数字分配机构（ ICANN）负责端口号的注册，任何协议和应用开发者都可以注册所需要的端口。每一个传输层协议只能注册一个端口号。
> 0 ~ 1023称为系统端口号
> 124 ~ 49151称为用户端口号
> 19152 ~ 65535 称为动态端口号

UDP

用户数据包协议（ user datagram protoco1,UDP）是一个轻量级的协议，封装数据并将其从一台主机的个端口发送到另一台主机的端口。
UDP 面向无连接，不提供堵塞网络的流量限制服务，不保证数据传输和准确到达。**是一种不可靠的传输协议。**

TCP

传输控制协议（ transmission control protocol,TCP）是在两台主机之间创建持久性的连接，**提供可靠数据流传输。**

应用层

利用网络的应用程序有很多，包括Web浏览器、电子邮件、远程登录、文件传输、网络管理等。能够让这些应用进行特定通信处理正是应用协议。

DHCP（动态主机配置协议）

如果逐一为每一台主机设置 IP 地址会非常繁琐的事情。特别是在移动使用笔记本电脑、只能终端以及平板电脑等设备时，每移动到一个新的地址，都要重新设置IP地址。
为实现自动设置 IP 地址、同一管理IP地址分配，就产生 DHCP(dynamichost configuration protoco1) 协议。有了 DHCP，计算机只要连接到网络，就可以进行 TCP/IP 通讯。

> 由 路由器实现，为计算机自动分配 IP 地址。

DNS 协议

域名系统（英文：Domain Name System，缩写：DNS）是互联网的一项服务。它作为将域名和IP地址相互映射的一个分布式数据库，能够使人更方便地访问互联网。DNS 使用 TCP 和 UDP 端口 53。当前，对于每一级域名长度的限制是 63 个字符，域名总长度则不能超过 253 个字符。

起初有互联网中心整体管理一份 hosts 文件。如果新增加一台计算机接入到 ARPANETE 网或者已有的某台计算机要进行 IP 地址变更，中心的这个 host 文件就的更新，而其它计算机不得不定期下载最新的host文件才能正常使用网络。

在上述背景之下，产生了一个可以有效管理主机名和IP地址之间对应关系的系统，那就是 DNS 系统。在这个系统中主机的管理机构可以对数据进行变更和设定。也就是说，他可以维护一个用来表示组织内部主机名和 IP 地址之间对应关系的数据库。

存在DNS服务器劫持问题

NAT 协议

地址转换协议，端口也需要被转换。

NAT(Network Address Translator）使用用于本地网络中使用私有地址，在连接互联网时转而使用全局IP地址的集数。

端口转发

端口转发（ Port forwarding)，有时被叫做隧道，是安全壳（SSH）为网络安全通信使用的一种方法。端口转发是转发一个网络端口从一个网络节点到另一个网络节点的行为，其使一个外部用户从外部经过一个被激活的NAT 路由器到达一个在私有内部 IP 地址（局域网内部）上的个端口。

NAT协议的一种Bug：**NAT 穿透（内网穿透）**，将外网地址被 NAT 成内网的地址，控制了 NAT 协议的转换表。

连接路由器就需要进行 NAT 穿透，端口转发。NAT内部会做表。

明日任务：怎样通过传输层传输程序数据。