# 计算机网络和因特网

## 什么是因特网：

是网络的网络，由软件和硬件组成，并且提供服务。

### 因特网的具体构成：

1. **主机/端系统**：指因特网上的所有设备。
2. **通信链路，路由器和分组交换机**：主机通过他们进行连接，发送分组。
3. 端系统要通过**ISP**：Internet service provider来接入网络
4. 端系统、分组交换机和其他部件都需要运行**协议（如TCP，IP）**

IP定义了路由器和端系统之间收发分组的格式，TCP协议保证数据通信的完整性和可靠性，防止丢包

### 服务描述：

应用程序涉及多个相互交换数据的端系统，所以被称作分布式应用程序（distributed application），因为他们存在于端系统上而不是分组交换机，所以需要考虑运行在一个端系统上的应用程序如何才能通过因特网向另一个端系统上的软件发送数据：**套接字接口（socket interface）**。

套接字接口规定了不同端系统上程序进行数据交付的方式（除了主要数据还需要有数据头来规定数据格式，送往的目的地）。

### 什么是协议

协议：定义了两个或多个通信实体之间交换报文的格式和顺序，以及报文发送和接受采取的动作。

## 网络边缘和网络核心

### 网络边缘：

由于端系统和应用程序位于网络边缘，需要通过物理设备连接到边缘路由器，所以此时需要**接入网**

家庭接入网：DSL、电缆、FTTH、拨号和卫星

DSL(digital subscriber line)数字用户线 和 电缆是最流行的两种宽带接入方式。

**物理媒体**实现具体的比特流传输。氛围引导性和非引导性，包括了双铜绞线，同轴电缆，光纤，陆地无线电信号，卫星无线电信号。

### 网络核心：

**分组交换：**

1. 存储转发传输：

在网络应用中，端系统彼此交换**报文**，而为了从源端系统向目的端发送报文，源端将豹纹切割成很多**小数据块**，称之为**分组**。每个分组通过分组交换机在互联网上进行传输，分组交换机主要有两类：路由器和链路层交换机。

多数分组交换机在链路的输入端使用**储存转发传输（store and forward transmission）,**也就是只有在接受到整个分组之后（store），才会进行向链路转发第一个分组（forward）。

1. 排队时延和分组丢失

每个分组交换机都有**输出缓存**(output buffer)/或者叫**输出队列**(output queue)来存储路由器准备发送到链路上的分组。如果发现这条链路已经被其他的分组交换机占用，则需要等待其他交换机完成发送后，分组才能被传输。于是产生了**排队时延**（queuing delay）。这些时延根据网络拥塞程度变化，因为缓存的大小是有限的，如果在缓存已经满了的情况下接受到分组，此时将出现分组丢失（丢包）packet loss, 到达的分组或者已经排队的分组之一会丢失。

1. 转发表和路由选择协议：

每台路由器都有一个**转发表**，将目的地址映射成为输出链路。当分组到达某个路由器时，路由器检查它的地址，并用这个目的地址搜索转发表，选择适当的链路进行转发。

路由选择协议就是用于自动设置转发表，决定每个路由器到目的地的最短路径，根据路径结果来配置每个路由器的转发表。

**电路交换：**

通过网络交换或者交换机移动数据的两种方式：分组交换，电路交换。

可以把它们看作不需要预定直接排队进入的餐厅，和需要预定的餐厅（doge

发送信息前，需要在发送方和接收方之间建立**端到端**的连接，网络必须在两个端系统之间预留一条电路。

分组交换和电路交换的对比：

分组交换的优势：1提供了比电路交换更好的带宽，2比电路交换简单有效成本低

电路交换的优势：稳定

## 协议层次与服务模型

各个层次的所有协议被称之为**协议栈**，以自顶向下的方式看五层模型：

应用层

运输层

网络层

链路层

物理层

### 应用层

应用层是网络应用程序以及他们的应用层协议存留的地方。

常用的几个应用层协议有：

HTTP（提供Web文档的请求和传送）

SMTP（电子邮件报文的传输）

FTP（端到端的文件传输）

对某些网络功能，如讲域名转换为32比特网络地址，由应用层协议：域名系统DNS完成

应用层之间交换的信息分组为**报文message**

### 运输层

运输层的分组为**报文段segment**

运输层为上层提供服务，其目的是在应用程序端点之间传送应用层的报文，由两种运输协议：TCP和UDP。

**TCP**提供**面向连接**服务，确保传递的同时进行**流量控制**，由于其将长报文切割为报文段并且提供**拥塞控制**，因此网络拥塞时，源端点会抑制传输速率。

**UDP**提供**无连接**服务，是**不提供不必要服务**的服务，无可靠性，无流量控制和拥塞控制，但是比较灵活。

可以类比于上面的电路交换和分组交换。

### 网络层

网络层的传输单位为**数据报datagram**。

源端系统中的运输层协议TCP或者UDP在向网络层递交其报文段和目的主机，网络层需要根据路由将数据报从源端发送到目的端。

网络层包括的著名**IP协议**，IP协议定义了数据报各个字段以及端系统、路由器需要如何运用这些字段。所有网络层的组建必须运行ip协议。

网络层也包括**路由选择协议**

### 链路层

链路层分组为**帧frame**。

网络层通过源端和目的地的一系列路由器路由数据报，为了将分组一个节点（主机或路由）移动到下一个节点，网络层必须依靠链路层服务。在每个节点，网络层将数据下发给链路层，链路层沿着路径将数据报传递给下一个节点，然后在下一个节点将数据上传给网络层。

链路层服务取决于应用于链路的特定链路层协议。链路层的例子包括以太网、Wi-Fi、电缆接入网的DOCSIS协议。因为数据报从源端向目的传输时通常需要经过几条链路，一个数据报会被沿途不同链路上的协议处理。

### 物理层

物理层传输**比特流。**

链路层将帧从一个网络元素移动到邻近的网络元素，而物理层将帧的一个个比特移动

下一个节点。这一层的协议进一步与传输媒体相关，如：双绞铜线、单模光纤和同轴电缆相关协议。跨越这些链路移动比特也是根据当前协议进行。

### 相比于OSI七层模型

五层模型缺少了两个层次：会话层session，表示层Presentation。

会话层提供数据交换的定界和同步功能，包括建立检查点和恢复的方案。

表示层作用是使通信的应用程序能够解释数据含义，包括数据的压缩、加密以及数据描述（表示/存储格式统一）

对于五层协议中缺少两个层的处理方法：

这留给应用程序开发者处理。应用程序开发者决定 一个服务是否是重要的，如果该服务重要，应用程序开发者就应该在应用程序中构建该功能。

### 封装

自顶向下，数据在每一层向下传输时，下层服务会对数据进行封装，所以在每一层的分组都可以分为两个类型的字段：**首部字段（head filed）**和**有效载荷字段（payload filed）**,有效载荷字段通常来自于上一层的分组。

## 网络攻击

### 恶意软件入侵

**恶意软件malware**可以通过主机与互联网收发数据时入侵。一旦入侵，它可以删除文件，安排间谍手机隐私信息等。此时受害主机可能成为数以千计的类似受害设备中的一员，它们被统称为**僵尸网络（botnet）**，黑客可以利用僵尸网络进行分布式拒绝服务攻击DDOS。

至今，多数恶意软件时自我复制（self-replicating）：一旦感染一个主机，则寻求进入其他主机形成新的感染主机，以此来进行指数型快速扩散。其**扩散方式有两种：病毒和蠕虫**。

**病毒virus**：一种需要某种形式的交互来感染用户设备的恶意软件。典型例子是可执行代码的电子邮件，其自我复制方式可以通过向用户地址簿上每一个接收方发送有同样恶意附件的相同报文。

**蠕虫worm**：一种无需明显交互来感染主机的恶意软件。蠕虫可以进入互联网中使用脆弱网络程序的主机。扩散方式是通过新近感染蠕虫的主机，其搜索其他运行相同网络层序的易感染主机，向他们发送蠕虫自身的副本。

### 攻击服务器和网络基础设施

拒绝服务攻击DOS attack。DoS攻击使得网络、主机或其他基础设施部分不能由合法用户使用。大多数Dos攻击属于下列三种类型之一：

1. 弱点攻击：

向一台目标主机上脆弱的应用程序或者操作系统发送制作精细的报文，适当顺序的多个分组发送给一个应用程序或者操作系统后，该服务器可能停止工作，甚至主机可能崩溃。

1. 带宽洪泛：

攻击者向目标主机发送大量的分组，分组数量之多是的目标的接入链路拥塞，合法的分组无法到达服务器。

1. 连接洪泛：

攻击者在目标主机中创建大量的半开/全开TCP连接。主机因为这些伪造的连接陷入困境，停止接受合法的连接。

DDOS分布式拒绝服务则是攻击者控制多个源向目标猛烈发送流量，是的目标难以检测和防范。

### 嗅探

通过**分组嗅探器（packet sniffer）**被动记录每个分组副本信息。

因为其是被动存在，不向信道注入分组，所以难以检测，所以需要通过加密来进行防范。

### 伪装

通过**ip哄骗**（ip spoofing）将虚假源地址的分组注入因特网，冒充另一个用户。

需要通过**端点鉴别**，使得我们确信一个报文源自于我们所信任的地方。