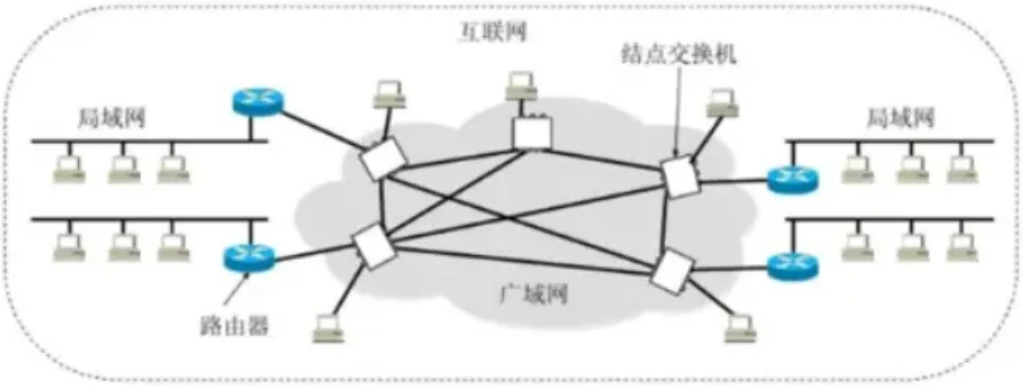
计算机网络

一 计算机网络概述

1 计算机网络的定义

计算机网络是将多台地理位置分散的计算机及其外部设备，通过通信线路连接起来，在网络操作系统、管理软件及通信协议的管理和协调下，实现资源共享、信息传递和协同工作的系统。



2 计算机网络的功能

资源共享

计算机网络资源共享的功能是指通过网络连接，使得不同计算机用户能够共同访问和利用网络中的各种资源，这些资源包括硬件设备、软件应用以及数据信息等。这种共享机制提高了资源的利用效率，降低了成本，并促进了信息的流通与合作。

分布式处理与负载均衡

分布式处理是指将不同地点的、或具有不同功能的、或拥有不同数据的多台计算机通过通信网络连接起来，在控制系统的统一管理控制下，协调地完成大规模信息处理任务的计算机系统。这种处理方式允许网络中的多台计算机各自承担同一工作任务的不同部分，在人的控制下同时运行，共同完成同一件工作任务。

综合信息服务

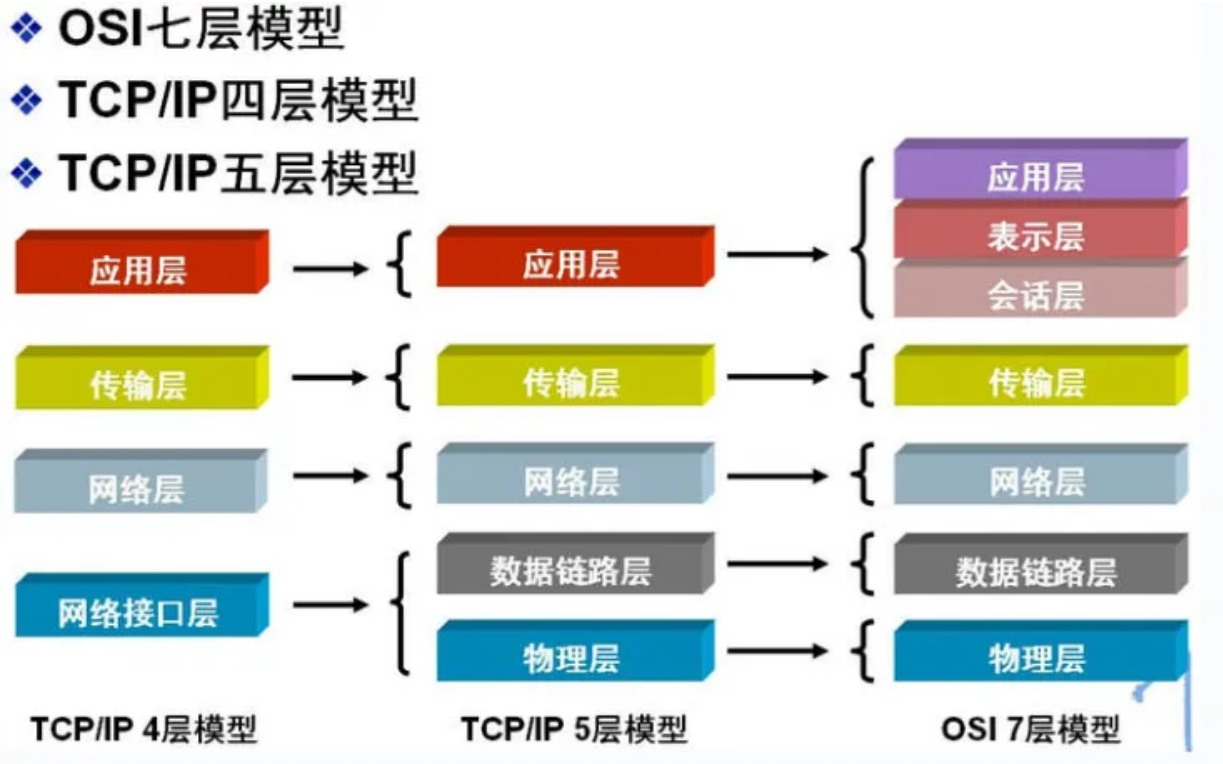
综合信息服务:指利用计算机网络技术，将各种信息资源进行整合、处理，并通过网络向用户提供全面、及时、准确的信息服务。

3 计算机网络的组成

硬件：包括客户端、通信设备、通信线路等。
软件：软件是用户与计算机硬件之间的接口，它使得用户能够方便地操作计算机、管理资源、执行各种任务和应用。
协议：实现通信所需要的一些约定，为使网内各计算机之间的通信可靠有效,通信双方必须共同遵守的规则和约定称为通信协议。

二 网络层次划分

国际标准化组织（ISO）在1978年提出了"开放系统互联参考模型"。它将计算机网络体系结构的通信协议划分为七层，自下而上依次为：物理层、数据链路层、网络层、传输层、会话层、表示层、应用层。其中第四层完成数据传送服务，上面三层面向用户。



OSI七层模型

层名称	功能
应用层	网络服务于最终用户的一个接口
表示层	数据的表示、安全、压缩、加密等
会话层	建立、管理终止会话
传输层	定义传输数据的协议端口号，以及流控和差错校验
网络层	进行逻辑地址寻址，实现到达不同网络的路径选择
数据链路层	建立逻辑连接、硬件地址寻址、差错校验等功能
物理层	建立、维护及断开物理连接

三 常见层次模型中的设备及协议

TCP协议

传输控制协议，面向连接的、可靠的、基于字节流的传输层通信协议。

特点

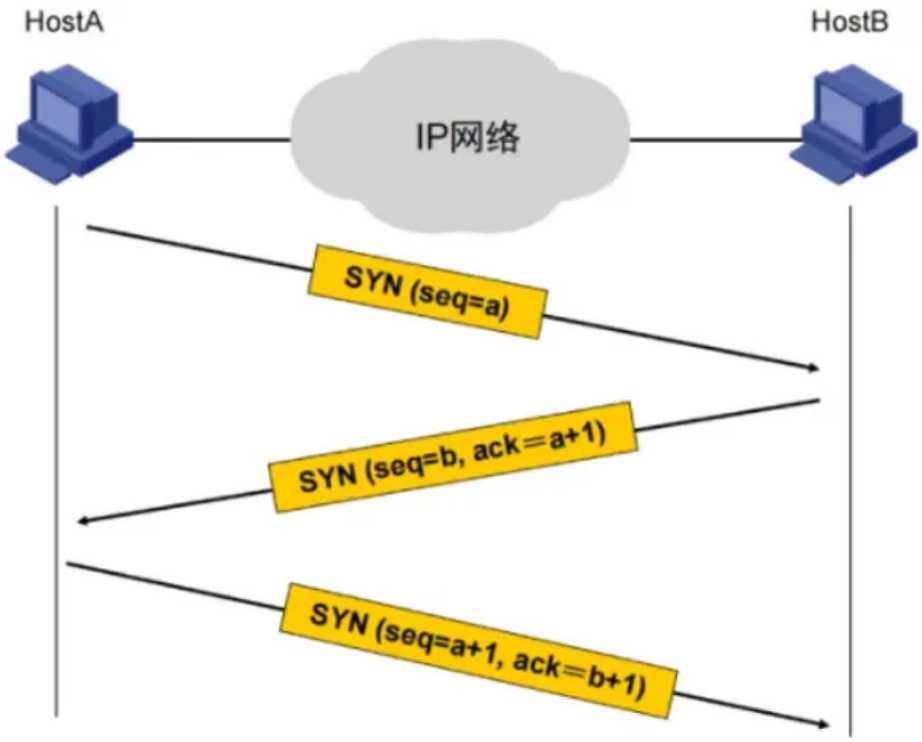
1、面向连接

2、可靠性

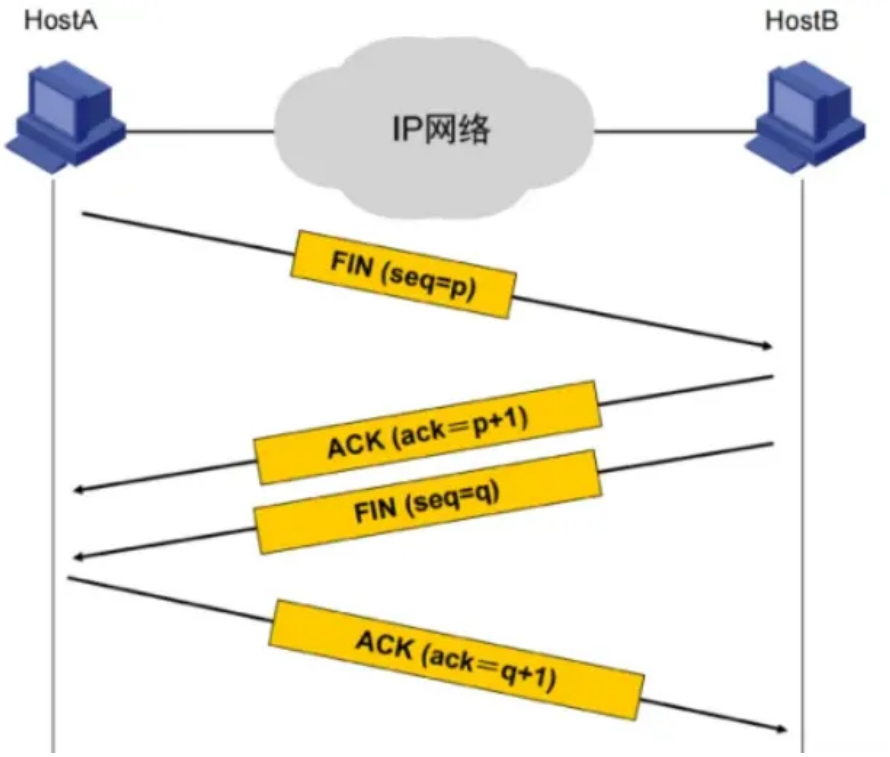
3、数据流控制

4、错误检测和校正

Tcp三次握手发起连接



Tcp四次挥手断开连接



UDP协议

UDP用户数据报协议，是面向无连接的通讯协议，UDP数据包括目的端口号和源端口号信息

TCP 与 UDP 的区别

TCP是面向连接的，可靠的字节流服务；UDP是面向无连接的，不可靠的数据报服务。

交换机和路由器

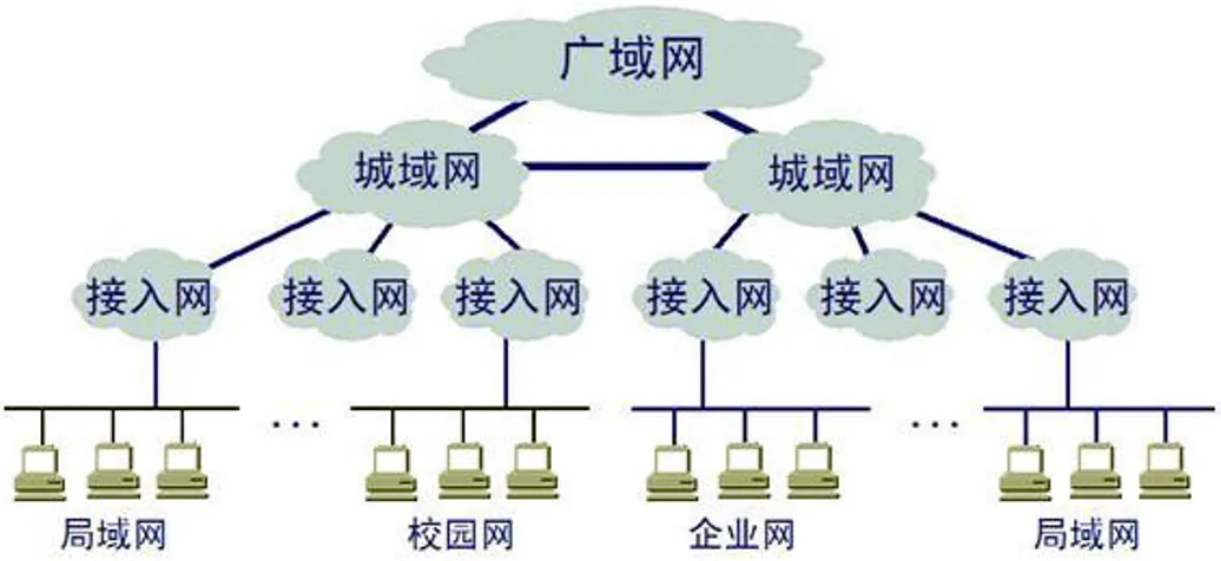
交换机的工作方式

1. **数据包转发**：交换机的主要功能是在网络内部实现数据的快速传输和转发。它根据数据包的MAC地址来转发数据包，将数据包从源地址发送到目的地址。
2. **MAC地址学习**：交换机通过学习MAC地址来确定数据包的目标地址。当交换机接收到一个数据包时，它会检查数据包的源MAC地址，并将其与接收数据包的端口号建立映射关系，存储在交换机的MAC地址表中。
3. **高速数据传输**：交换机通常具有多个LAN端口，用于连接多个设备。它采用高速的数据包转发技术，如直通式交换、存储转发式和碎片隔离方式等，以实现高速数据传输和网络流量控制。

路由器的工作方式

1. **数据包转发**：路由器的主要功能是将数据包从一个网络传输到另一个网络。它根据数据包的IP地址来判断路由，通过查找路由表来确定数据包的最佳路径，然后将数据包转发到下一跳路由器或目的网络。
2. **路由决策**：路由器在转发数据包时，会进行复杂的路由决策。它会根据目的地址来查找路由表，以确定数据包的最佳路径。路由表包含了网络地址、下一跳地址、出接口等信息，路由器根据这些信息来转发数据包。
3. **网络安全**：路由器还可以提供网络安全功能，如防火墙、虚拟专用网络（VPN）等。这些功能可以通过配置路由表、访问控制列表等来实现，以保护网络免受攻击和数据泄露。

网络分类



按照覆盖范围分类主要可以分类如下：（主要的区别就是范围）

局域网（LAN）：局限于较小的地理范围内，如家庭、学校或公司内部的网络。

城域网（MAN）：覆盖范围比局域网大，通常覆盖一个城市或地区。

广域网（WAN）：覆盖范围广泛，可以跨越多个城市、国家或地区，甚至全球

IP地址

IP地址是电子设备（计算机）在互联网上的唯一标识。IP地址分为IPv4和IPv6。IPv4地址由32位二进制组成，采用点分十进制。IP地址由网络号（包括子网号）和主机号两部分组成。网络位相同的IP地址为同一网段。

IP的主要作用

标识节点和链路：用唯一的IP地址标识每一个节点；用唯一的IP网络号标识每一个链路；

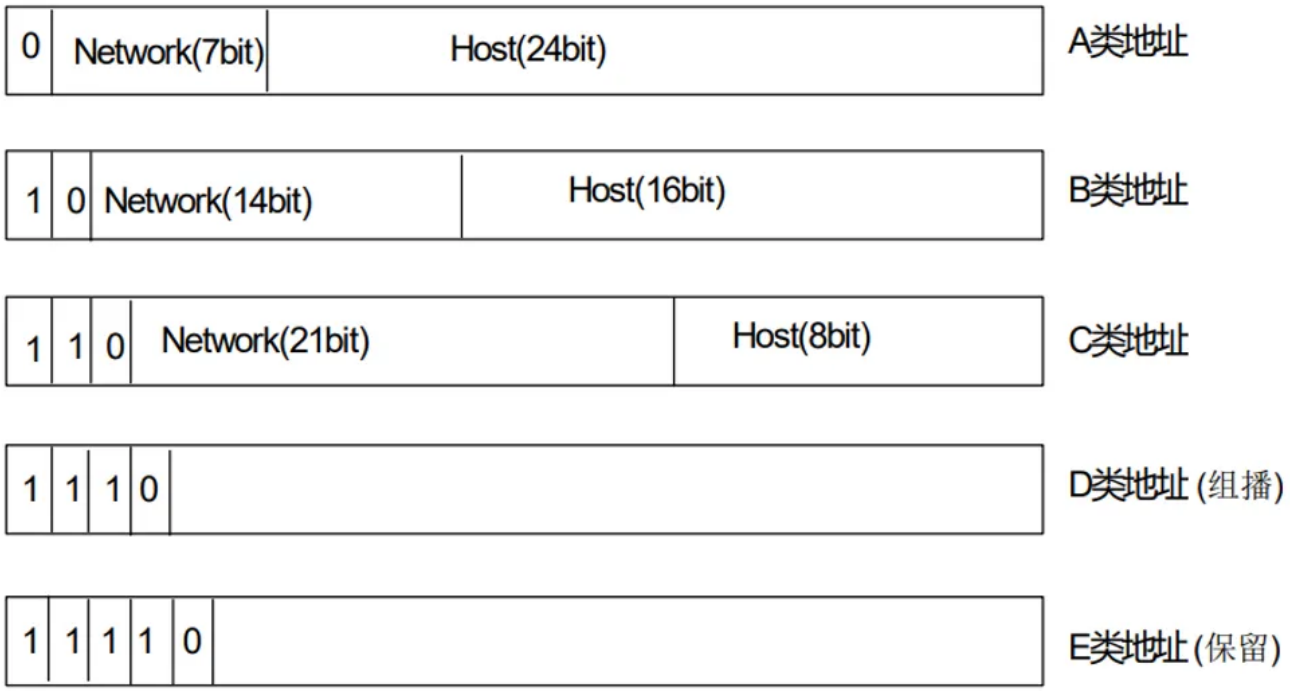
寻址和转发：确定节点所在网络的位置，进而确定节点所在的位置;IP路由器选择适当的路径将IP包转发到目的节点。

IP地址格式和表示方法

网络号用于区分不同的IP网络

主机号用于标识该网络内的一个IP节点

IP地址的分类



A类地址

网络地址的最高位必须是“0”,它主要为大型网络而设计的，地址范围从1.0.0.0 ~126.255.255.255。每个网络能容纳16777214个主机。其中127.0.0.1是一个特殊的IP地址，表示主机本身，用于本地机器的测试

B类地址

网络地址的最高位必须是“10”，地址范围从128.0.0.0到191.255.255.255。每个网络能容纳6万多个主机

C类地址

网络地址的最高位必须是“110”。范围从192.0.0.0到223.255.255.255。C类网络可达209万余个，每个网络能容纳254个主机。

D类地址

组播地址主要在需要向多个目标主机发送相同数据的场景中使用，组播地址在城市安防监控、智能交通、环境监测等领域广泛应用。

E类地址

E类地址为保留地址 用于科研使用。

公网地址及私网地址

公网地址是由互联网注册机构进行分配的，这些地址在Internet上是唯一的，并且具有全球可达性。公网地址用于Internet上的设备，允许设备在Internet上进行通信。

私网地址则是由局域网管理员自行分配的，它们只在局域网内部具有唯一性。私网地址则仅限于局域网内部使用，不能直接在Internet上访问。这种设计有助于保护内部网络的安全性，防止内部网络与公共网络之间的冲突。

私网地址如下

	私有地址范围	子网掩码
A类	10.0.0.1~10.255.255.254	255.0.0.0
B类	172.16.0.1~172.31.255.254	255.255.0.0
C类	192.168.0.1~192.168.255.254	255.255.255.0

子网掩码：用来确定IP地址的网络位，网络号的位都置1，主机号都置0

内网与外网

内网（局域网，LAN）

定义：内网是指在某一特定区域内由多台计算机以及网络设备构成的网络，如校园网、政府网、企业内网等。范围：内网的覆盖范围相对较小，通常仅限于某一建筑物、园区或公司内部，方圆几公里以内。

外网（广域网，WAN）

定义：外网又称广域网、公网，是连接不同地区局域网或城域网计算机通信的远程网。范围：外网的覆盖范围广泛，可以跨越城市、国家甚至全球，提供远距离通信服务。

端口号

端口号的主要作用是表示一台计算机中的特定进程所提供的服务。

网络中的计算机是通过IP地址来代表其身份的，它只能表示某台特定的计算机，但是一台计算机上可以同时提供很多个服务，如数据库服务、FTP服务、Web服务等，我们就通过端口号来区别相同计算机所提供的这些不同的服务。

按端口号范围分类

知名端口

范围是0到1023，这些端口一般固定分配给一些服务，如常见的端口号21表示的是FTP服务，端口号80表示http服务等。

注册端口

范围是1024–49151，分配给用户进程或应用程序，需向IANA注册以避免冲突，如MySQL(3306)、MongoDB(27017)等。

动态/私有端口

范围是49152–65535，临时分配给客户端程序使用，通常用于短暂的通信会话。

常用端口及协议大全 (lddgo.net)

虚拟专用网络

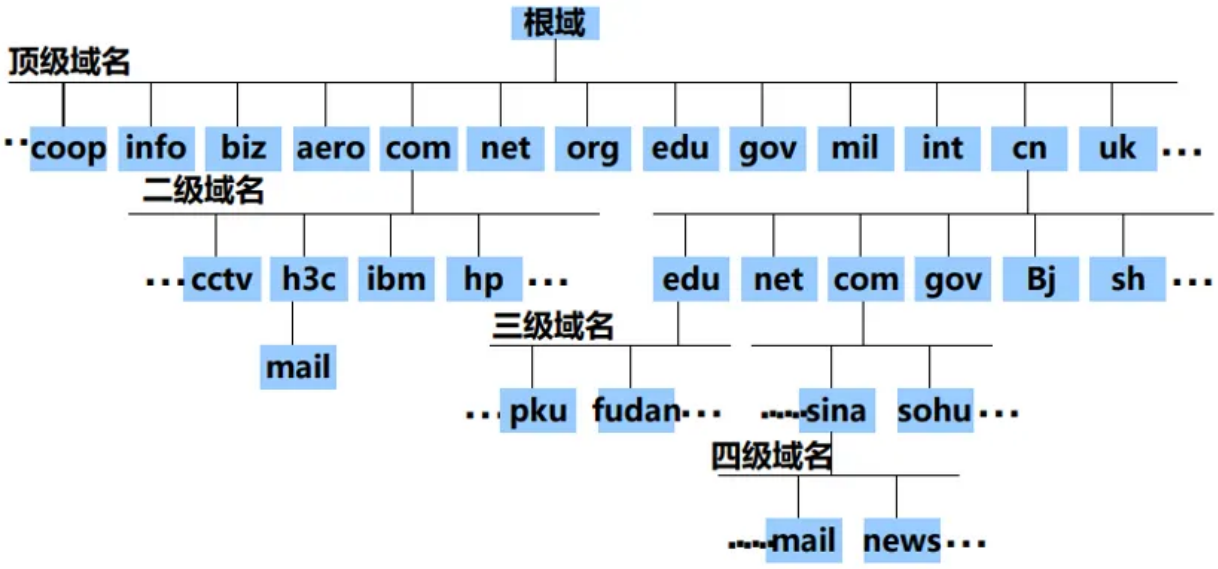
定义：VPN是利用公共网络（如Internet）的基础设施，通过隧道技术为用户提供的与专用网络具有相同通信功能的安全数据通道。

虚拟：用户不需要建立各自专用的物理线路，而是利用公共网络资源和设备建立一条逻辑上的专用数据通道。

专用网络：虚拟出来的网络并非任何连接在公共网络上的用户都能使用，只有经过授权的用户才可以使用。

域名

由一串用点分隔的名字组成的Internet上某一台计算机或计算机组的名称。域名由两个或两个 ·以上的词构成，中间由点号分隔开。最右边的那个词称为顶级域名。常见的域名有www.baidu.com，www.taobao.com，www.jd.com 这些都是域名，域名可以在Godaddy、Gandi、Hover、Namesilo、Namecheap等网站注册。



url 统一资源定位器

Internet上的每一个网页都具有一个唯一的名称标识。它是www的统一资源定位标志，简单地说URL就是web地址，俗称“网址”。

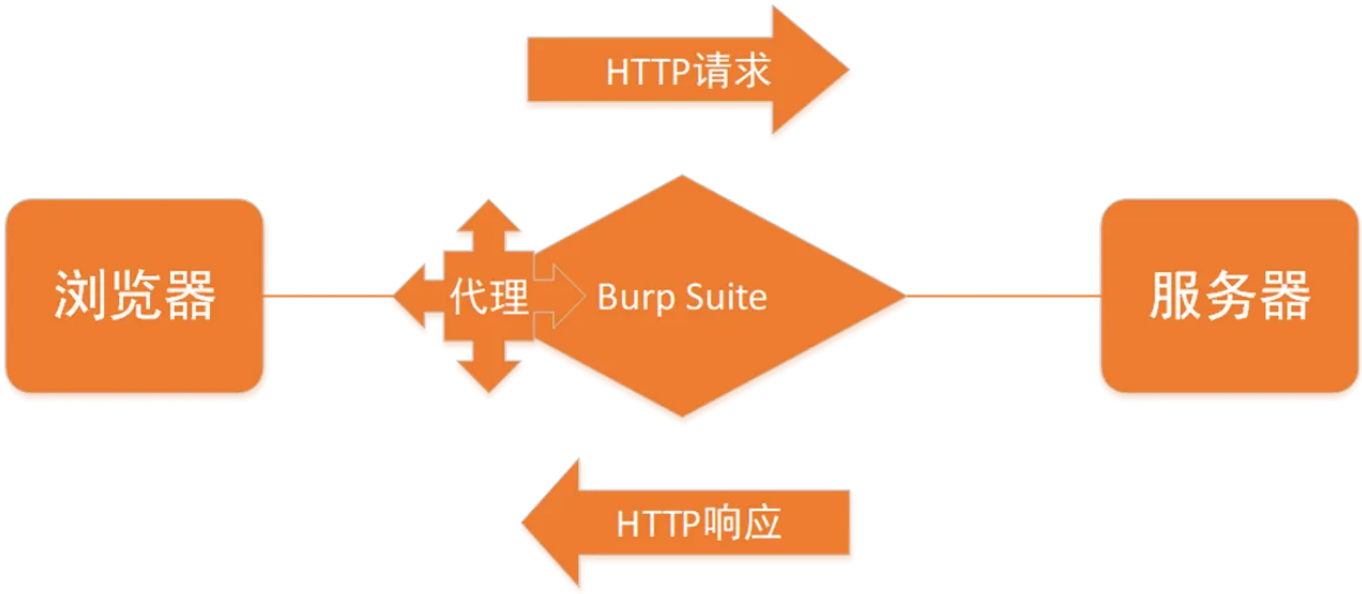
CDN

全称是Content DeliveryNetwork，即内容分发网络。

CDN的基本思路：是尽可能避开互联网上有可能影响数据传输速度和稳定性的瓶颈和环节，使内容传输的更快、更稳定。

代理

网络代理是指允许一个网络终端（通常指客户端）通过这个服务与另一个网络终端（通常指服务器）进行非直接的连接的一种网络服务。提供代理服务的电脑系统或其它类型的网络终端称为代理服务器（Proxy Server）。



HTTP协议

HTTP协议(Hyper Text Transfer Protocol)。它是从WEB服务器传输超文本标记语言(HTML)到本地浏览器的超文本传输协议。HTTP是一个基于TCP/IP通信协议来传递数据的协议，传输的数据类型为HTML文件,、图片文件, 查询结果等。HTTP协议一般用于B/S架构(浏览器/服务器结构)。

版本

HTTP 有多个版本，目前广泛使用的是 HTTP/1.1 和 HTTP/2，以及正在逐步推广的 HTTP/3。

- HTTP/1.1：支持持久连接，允许多个请求/响应通过同一个 TCP 连接传输，减少了建立和关闭连接的消耗。
- HTTP/2：基于二进制分帧，支持多路复用，允许同时通过单一的 HTTP/2 连接发起多重的、独立的、双向的交流。
- HTTP/3：基于 QUIC 协议，旨在减少网络延迟，提高传输速度和安全性。

HTTP 的请求–响应

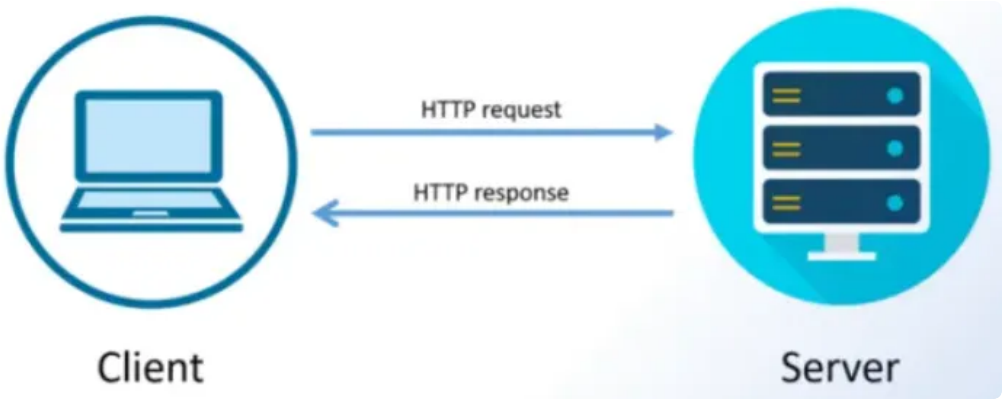
建立连接：客户端与服务器之间建立连接。

发送请求：客户端向服务器发送请求，请求中包含要访问的资源

处理请求：服务器接收到请求后，根据请求中的信息找到相应的资源，执行相应的处理操作

发送响应：服务器将处理后的结果封装在响应中，并将其发送回客户端

关闭连接：在完成请求–响应周期后，客户端和服务器之间的连接可以被关闭



http请求方法

GET：请求从服务器获取指定资源。这是最常用的方法，用于访问页面。

POST：请求服务器接受并处理请求体中的数据，通常用于表单提交。

PUT：请求服务器存储一个资源，并用请求体中的内容替换目标资源的所有内容。

DELETE：请求服务器删除指定的资源。

HEAD：与 GET 类似，但不获取资源的内容，只获取响应头信息

get和post请求的区别

（1）post相对更安全（不会作为url的一部分，不会被缓存、保存在服务器日志、以及浏览器浏览记录中）

（2）post发送的数据更大（get有url长度限制）

（3）post能发送更多的数据类型（get只能发送ASCII字符）

（4）post比get慢

（5）post用于修改和写入数据，get一般用于搜索排序和筛选之类的操作，目的是资源的获取，读取数据

请求报文

报文由三个部分组成，即请求行、请求头部和请求数据。

响应报文结构

响应报文的开始行是响应行、响应头部、响应数据

HTTP 响应头信息：https://www.runoob.com/http/http-header-fields.html

HTTP 状态码

HTTP状态码大全 (lddgo.net)

1xx、2xx、3xx、4xx、5xx

HTTPS

HTTPS 协议是 HyperText Transfer Protocol Secure（超文本传输安全协议）的缩写，是一种通过计算机网络进行安全通信的传输协议。

HTTPS 的主要作用是在不安全的网络上创建一个安全信道，并可在使用适当的加密包和服务器证书可被验证且可被信任时，对窃听和中间人攻击提供合理的防护。

四 网络常用工具介绍

Wireshark

https://www.wireshark.org/download.html

Wireshark是一款开源抓包工具，也被称为网络嗅探器，用于分析网络流量和数据包它以前的名字是Ethereal，于1998年首次开发，直到2006年才改为Wireshark。

功能与特点

提供可视化分析网络包的图形页面，使得数据包分析更加直观。

支持显示网络模型中的第2层到第5层（链路层、网络层、传输层、应用层）的数据包。

拥有丰富的内置过滤器库，帮助用户更好地监控网络。

使用场景

常用于检测网络问题、攻击溯源、分析底层通信机制等。

Tcpdump

是一个命令行格式的网络抓包工具，用于捕获和分析网络数据包。它常用于Linux服务器中抓取和分析网络包。

功能与特点

- 能够捕获网络上传输的数据包，并提供了强大的过滤功能。
- 支持多种过滤条件，如源IP地址、目标IP地址、端口号、协议类型等。
- 提供了详细的数据包信息，包括源IP地址、目标IP地址、端口号、协议类型、数据包大小、时间戳等。
- 支持将捕获的数据包保存到文件中以供后续分析。

使用场景

- 常用于网络故障排查、网络性能优化、网络安全审计等任务。

- 适用于Linux环境，是类UNIX系统下用于网络分析和问题排查的首选工具。

捕获指定接口的所有数据包

```
tcpdump –i eth0
```

捕获指定数量的数据包

```
tcpdump –i eth0 –c 100
```

将捕获的数据包保存到文件中

```
tcpdump –i eth0 –w capture.pcap
```

BurpSuite

BurpSuite是一款集成化的渗透测试工具，它包含了许多功能，可以帮助安全人员快速完成对web应用程序的渗透测试和攻击。BurpSuite是用于Web应用安全测试、攻击Web应用程序的集成平台，它将各种安全工具无缝地融合在一起，以支持整个测试过程，从最初的映射和应用程序的攻击面分析，到发现和利用安全漏洞。BurpSuite为这些工具设计了许多接口，以加快攻击应用程序的过程。

核心模块

模块	主要用途
Proxy	拦截/修改 HTTP(S) 流量
Scanner	自动化漏洞扫描（SQLi、XSS 等）
Intruder	定制化暴力破解与模糊测试
Repeater	手动重放和调试请求
Decoder	编解码工具（Base64、URL 等）

应用场景

Web 漏洞挖掘：结合手动测试（Proxy/Repeater）与自动化扫描（Scanner）。

API 安全测试：检测接口逻辑漏洞。

移动端安全：通过代理抓包分析 App 与后端交互。

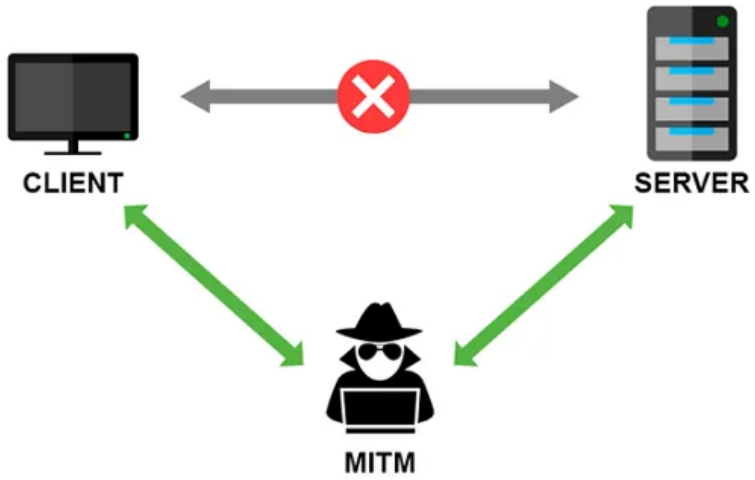
五 网络常见攻击

MITM中间人攻击

MITM（Man-in-the-Middle）中间人攻击是一种网络攻击方式，攻击者通过某种手段将自己插入到通信双方之间，窃取、篡改或者干扰双方的通信内容。

攻击类型

1. **ARP欺骗**：攻击者发送伪造的ARP消息，将攻击者的MAC地址与网络中其他主机的IP地址关联，实现数据流向攻击者机器的重定向。
2. **DNS欺骗**：攻击者干扰DNS查询响应，将受害者导向假冒的服务器。
3. **Wi-Fi劫持**：攻击者创建与本地免费Wi-Fi选项同名的虚假Wi-Fi接入点（AP），一旦受害者连接到了恶意访问点，攻击者就可以监视其一切在线活动。
4. **IP欺骗**：攻击者伪造源IP地址，使目标主机认为数据包来自可信主机。



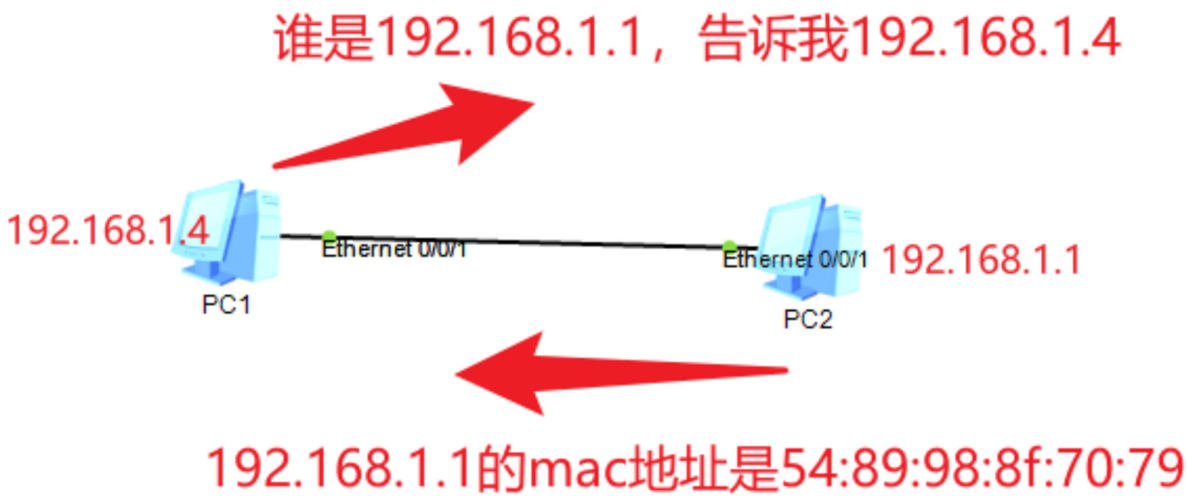
ARP欺骗攻击

ARP协议用于实现IP地址到物理地址（通常是MAC地址）的映射。当一个主机需要知道另一个主机的物理地址时，它会发送一个ARP请求，其他主机收到请求后会检查自己的IP地址是否与请求中的目标IP地址匹配，如果匹配则返回自己的物理地址。

MAC地址，全称为Media Access Control Address，中文称为媒体访问控制地址，是用于识别网络设备的唯一标识符。它由48位二进制数（即6个字节）组成，通常表示为12个十六进制数，格式为XX-XX-XX-XX-XX-XX。

ARP请求，主机在配置新IP地址后，会主动向局域网内发送一个ARP请求，请求自己的IP地址的MAC地址。

ARP攻击就是通过伪造IP地址和MAC地址实现ARP欺骗，能够在网络中产生大量的ARP通信量，攻击者只要持续不断的发出伪造的ARP响应包就能更改目标主机ARP缓存中的IP-MAC条目，造成网络中断或中间人攻击。



Source	Destination	Protocol	Length	Info
HuaweiTe_b1:73:5a	Broadcast	ARP	60	Who has 192.168.1.1? Tell 192.168.1.4
HuaweiTe_8f:70:79	HuaweiTe_b1:7…	ARP	60	192.168.1.1 is at 54:89:98:8f:70:79

僵尸网络与DDOS

僵尸网络 是由黑客集中控制的一群互联网上的计算机。黑客通过各种手段将大量的主机感染僵尸程序，从而在控制者和被感染主机之间形成一对多的控制僵尸网络。

DoS(Denialof Service:拒绝服务攻击):是一种网络攻击手法，短时间内对目标服务器产生大量请求，使服务器链路拥塞或忙于处理攻击请求，导致服务暂时中断或停止，导致其正常用户无法访问。

DDoS(Distributed DenialofService:分布式拒绝服务攻击):强调是将多个计算机(僵尸网络)联合起来作为攻击平台，对一个或多个目标发动DoS攻击。

DOS实验

选择攻击模式

SYN Flood攻击：通过发送大量的SYN数据包来填满目标系统的TCP连接队列，从而耗尽其资源。

ICMP Flood攻击：利用ICMP协议发送大量的ICMP数据包来消耗目标系统的资源。

UDP Flood攻击：通过发送大量伪造的UDP数据包来冲击目标服务器。

配置hping3参数

–c：设置发送数据包的数量。
–d：设置每个数据包的大小。
–i：设置数据包之间的时间间隔。
––flood：开启洪水攻击模式。
–S：在SYN Flood攻击中使用，表示发送TCP SYN数据包。
–p：设置目标端口。
––rand–source：使用随机源地址发送数据包，以避免攻击者的真实IP地址被记录。

```
hping3 –c 10000 –d 120 –S –p 80 ––flood ––rand–source <目标IP地址>
```

这个命令会发送10000个大小为120字节的TCP SYN数据包到目标IP地址的80端口，使用随机源地址，并尽可能快地发送。