计算机网络

Ⅰ.TCP网络模型

应用层

主要任务：位于不同主机中的多个应用进程之间进行通信和协同工作

生成需要传输的数据

（假设遥远的两个公司关系很好，每个公司有着不同的人负责不同的业务）

（告诉下面的部门我XXX做好了一个货物，想从北京x公司发到成都y公司）

（从下面的部门，YYY收到了一个货物，是从北京x公司发来成都y公司的）

传输层

主要任务：向两个主机中进程之间的通信提供通用的数据传输服务

提供应用进程之间的端口

将数据切分成不同段并打好标签便于组装

（给货物附上源地址目标地址，同时对货物进行处理便于运输，并且放到快递箱里，贴好XXX的名字）

（拆开包裹，将货物恢复，根据收货人YYY的名字将货物连同地址一并送到收货人的手里）

网络层

主要任务：分组怎样从一个网络通过路由器转发到另一个网络

为交换网上的不同主机提供通信服务

把传输层产生的报文段或用户数据报封装成分组或包进行传送(IP数据报)

（将要运送的货物二次打包，贴上城市公司地址“北京x公司”，以及目标城市公司地址“成都y公司”）

（确定目标地址是自己的地址才拆开包裹上交）

数据链路层

主要任务：在同一个局域网中，怎样从一个主机传送到另一个主机

将网际层交下来的IP数据报组装成帧，在相邻结点间的链路上传送帧

（将包裹再次封好，贴上两个公司地址对应的唯一的校验码，送到配送部门）

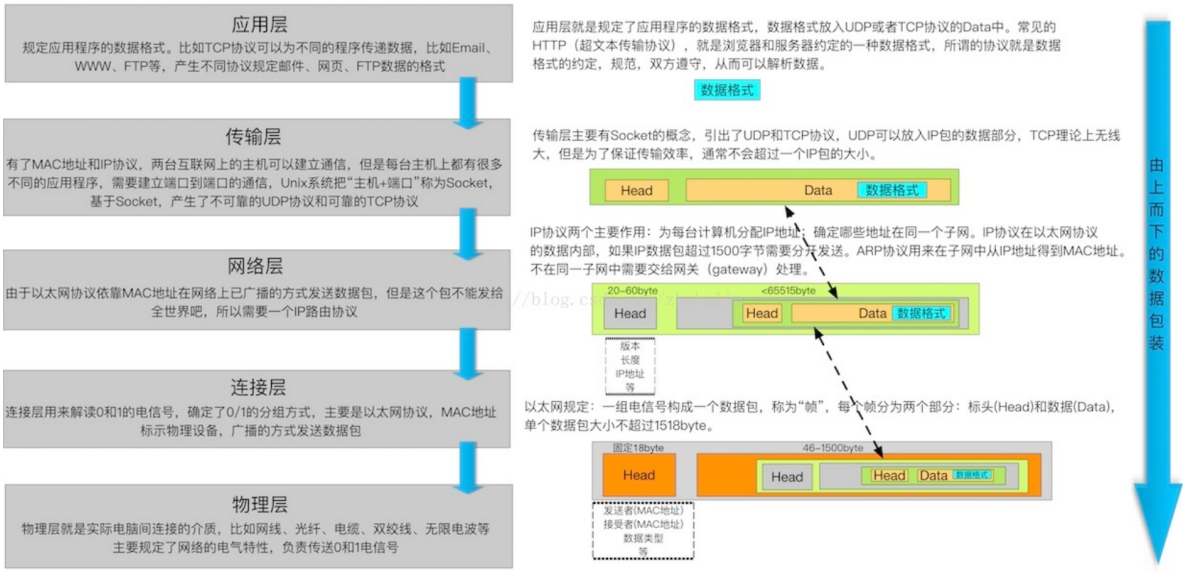
（确定目标校验码是自己的校验码才收好包裹，拆下一层后将包裹上交）

物理层

主要任务：考虑怎样才能在连接各种计算的传输媒体上传输数据比特流

（查询对应的校验码，设定航班定点配送）

TCP/IP 层	网络设备
应用层	
传输层	四层交换机、也有工作在四层的路由器
网络层	路由器、三层交换机
数据链路层	网桥（现已很少使用）、以太网交换机（二层交换机）、网卡（其实网卡是一半工作在物理层、一半工作在数据链路层）
物理层	中继器、集线器、还有我们通常说的双绞线也工作在物理层

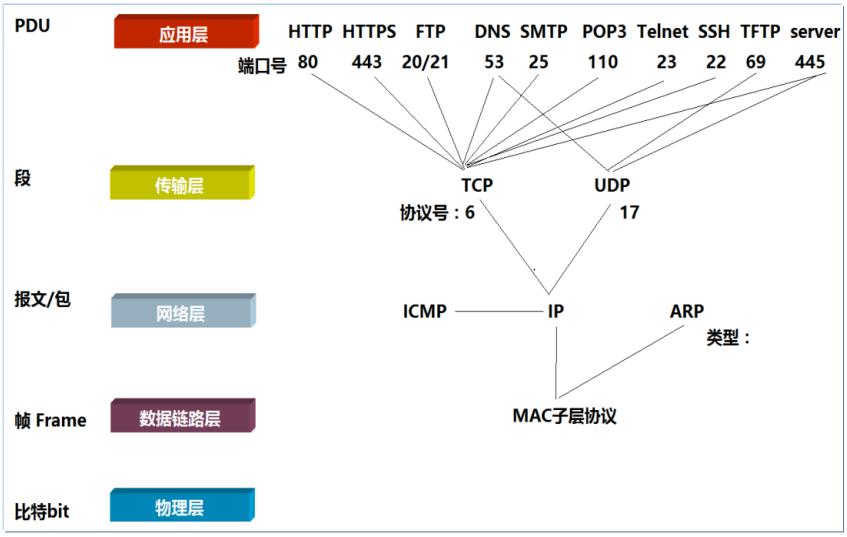


不同服务器的相同层级之间是可见的

同一服务器或不同服务器的不同层级是不可见的（类似于黑箱只接受输入提供输出）

各层级规定各种协议来达到规范统一数据处理方式的目的

TCP/IP协议族的组成



12

一.应用层

规定应用进程通信所遵守的协议

为用于通信的应用程序和用于消息传输的底层网络提供接口

1.http与https协议

基于请求与响应，无状态的，应用层的协议，常基于TCP/IP协议传输数据，互联网上应用最为广泛的一种网络协议,所有的WWW文件都必须遵守这个标准

前者为超文本传输协议（明文传输）默认端口80

后者为带有ssl加密的传输协议，默认端口443

客户端发送的每次请求都需要服务器回送响应，在请求结束后，会主动释放连接。从建立连接到关闭连接的过程称为“一次连接”。

由于HTTP在每次请求结束后都会主动释放连接，因此HTTP连接是一种“**短连接**”，要保持客户端程序的在线状态，需要不断地向服务器发起连接请求。

附：混合加密

混合加密通过对称加密加密明文

非对称加密加密秘钥，形成公钥和私钥

对称加密原理：

M+a=m

m-a=M

非对称加密原理：

M+a（公钥）=m

m+b（私钥）=M

（常用非对称加密有PSA大整数因子分解，及ECC椭圆曲线加密算法）

（无法在一定时间内破解，视为绝对安全）

一台服务器的私钥是**只有自己拥有**，而公钥派发给其他所有人

若要给对应服务器传输数据必须要经过公钥加密

中途即使拦截到文件也由于没有私钥无法解密

附：数字摘要

数字摘要（Digital Digest，数字指纹、数字手印）

将任意长度的消息变成固定长度的短消息，它类似于一个自变量是消息的函数，也就是Hash函数。数字摘要就是采用单向Hash函数将需要加密的明文“摘要”成一串固定长度（128位）的密文这一串密文又称为数字指纹，它有固定的长度，而且不同的明文摘要成密文，其结果总是不同的，而同样的明文其摘要必定一致。

哈希算法单向不可逆，并且公开

每个信息报文按照某种加密算法都会产生一个自己特定的数字摘要，这就可以通过数字摘要来确认所代表的信息报文的真实性和完整性。信息接收方只需要比较信息报文得到的数字摘要和发送方是否一致，就可以确认报文是否被串改。

1、发送方使用hash算法计算得到信息报文的数字摘要

2、发送方将信息报文和数字摘要发送给接收方

3、接收方收到信息报文和数字摘要

4、接收方使用同样的hash算法计算得到信息报文的数字摘要

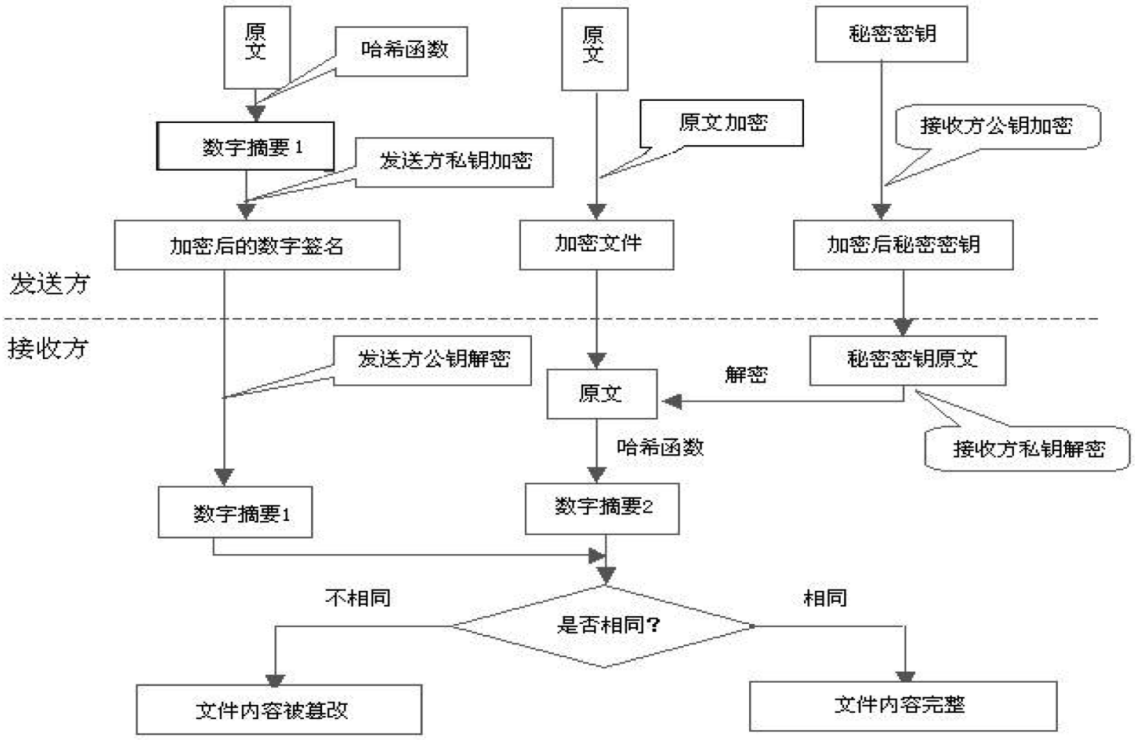
5、比较两个数字摘要的一致性来确认报文是否完整

常见hash算法有md5（有碰撞风险），sha1，sha256

附：数字签名

混合加密技术和数字摘要技术结合形成数字签名技术

- 收方能够证实发送方的真实身份；
- 发送方事后不能否认所发送过的报文；
- 收方或非法者不能伪造、篡改报文。



附：数字证书

数字证书在网络通讯中标志通讯各方身份信息的一系列数据

由受信任的数字证书颁发机构CA发行

证书在验证服务器身份后颁发，证书中包含了一个**密钥对（公钥和私钥）**和所有者识别信息。数字证书被**放到服务端**，具有服务器**身份验证**和数据**传输加密**功能。

2.DNS协议

DNS协议用于域名解析

用户将域名发给域名解析客户端（DNS服务器）

DNS先检查本地是否有对应的IP地址，若找到则返回响应的IP地址。若没找到则请求上级DNS服务器，直至找到或到根节点。

3.FTP协议

文件传输协议（FTP）作为网络共享文件的传输协议

FTP 客户端程序先与服务器建立连接，然后向服务器发送命令。服务器收到命令后给予响应，并执行命令。

FTP 使用 2 个端口，一个数据端口和一个命令端口（也叫做控制端口）。这两个端口一般是21 （命令端口）和 20 （数据端口）。控制 Socket 用来传送命令，数据 Socket 是用于传送数据。

二.传输层

规定端对端的连接和数据传输的协议

负责向两个主机中 进程 之间的 通信 提供服务

定义了应用程序的端口，用以使不同服务的数据包和程序独立

（0-65535）

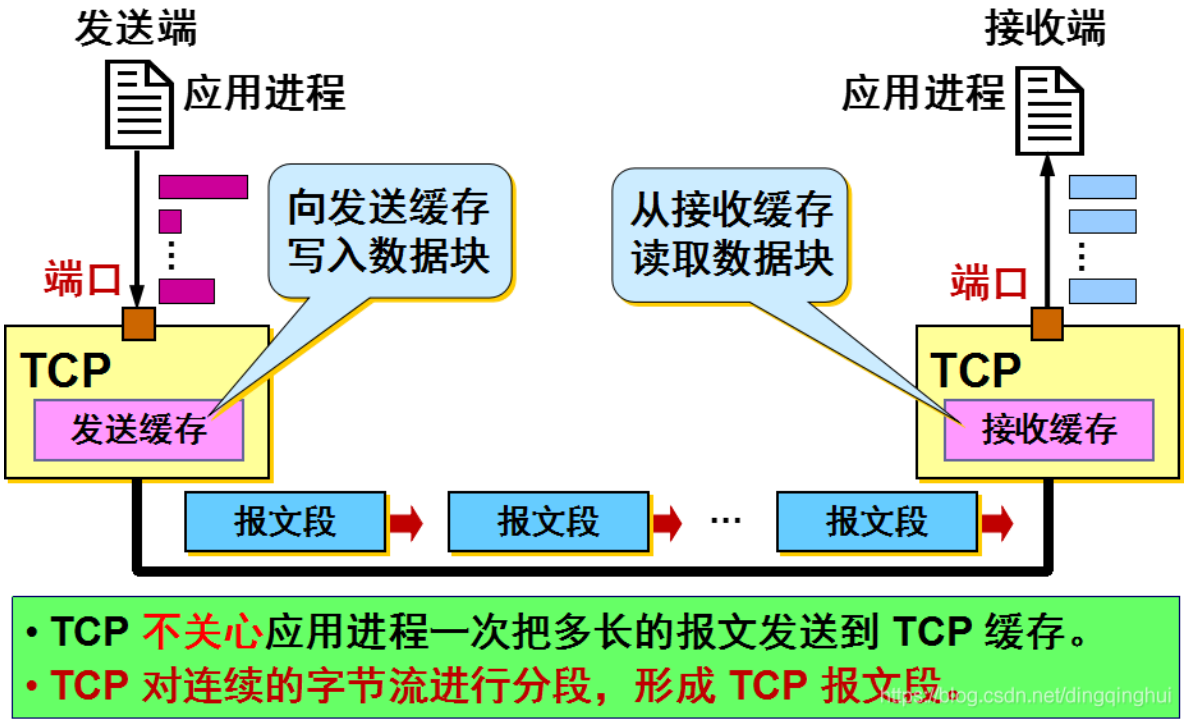
1.TCP协议

一种面向连接，字节流传输的连接传输协议

先将客户端和服务端进行连接，然后建立稳定可靠的传输，同时具有避免丢包处理丢包校验损坏的一系列操作，绝对的安全可靠，但问题是操作繁琐，速度拉胯。

TCP数据包没有长度限制，理论上可以无限长，但是为了保证网络的效率，通常TCP数据包的长度不会超过IP数据包的长度，以确保单个TCP数据包不必再分割。(流式协议，不间断发送)

TCP可靠的缘故：**只要不得到确认，就重新发送数据报，直到得到对方的确认为止。**



TCP将两个端的端口（套接字）进行连接

建立连接时进行三次握手

第一次握手客户向服务器提供开始发包的序列号

服务端确定客户端发送能力正常

第二次握手服务器向客户提供确认的报文和服务器的序列号

客户端确定服务端发送接收能力正常

第三次握手客户端确认让服务端分配缓存，通知自己的应用层发送数据

（防止网络中有延迟的无用连接请求达到服务器端，导致服务器一直在等待客户端的数据，错误的分配网络资源）

改编的抽象例子

第一次握手：

小明送信告诉小红：我喜欢你，这是我给你的礼物。

说明小红知道小明是能把信送过去而不被情敌干爆的

第二次握手：
小红回信告诉小明：我知道了，我喜欢这礼物，我也喜欢你。

此时小红并不确定小明是否收到了告白信

有可能信在送的途中被情敌处理掉了

所以要苦苦的等待~

第三次握手：
小明回信：我也知道了，我们在一起吧。此时才真正建立连接。

断开连接时进行四次挥手

第一次挥手：客户端通知服务端我bb完了，你可以断开连接了

第二次挥手：服务端通知客户端我知道你bb完了，我还得跟你嘱咐几句，我先告诉一下上头准备关掉连接

第三次挥手：服务端告诉客户端我也bb完了，你可以准备关闭连接了

第四次挥手：客户端告诉服务端我知道要关了，你先关

2.UDP协议

无需连接无需确认，单纯的简单打包后送出数据，完全不可靠

但是简洁高效负载小

以牺牲报文完整度的代价换取较低的延迟，实时性以及避免拥塞

适用于视频的传输

三.网络层

网络层是无连接，不可靠尽量交付数据包的服务。由主机的运输层负责对进程提供可靠性的服务。这样设计降低了网络设备的复杂度。

1.IP协议

IP协议根据「IP地址」将数据传输到指定的目标主机

相当于收货地址

同时IP协议将ip数据包传递给链路层

附：IP地址

目前使用最为广泛的是ipv4地址，下面默认ip均为ipv4

ip地址是一串32位二进制数据，8位一组分为四组

每一组的大小为0~2^8-1（255）

产生了2^32个ip地址

ip地址分为5类

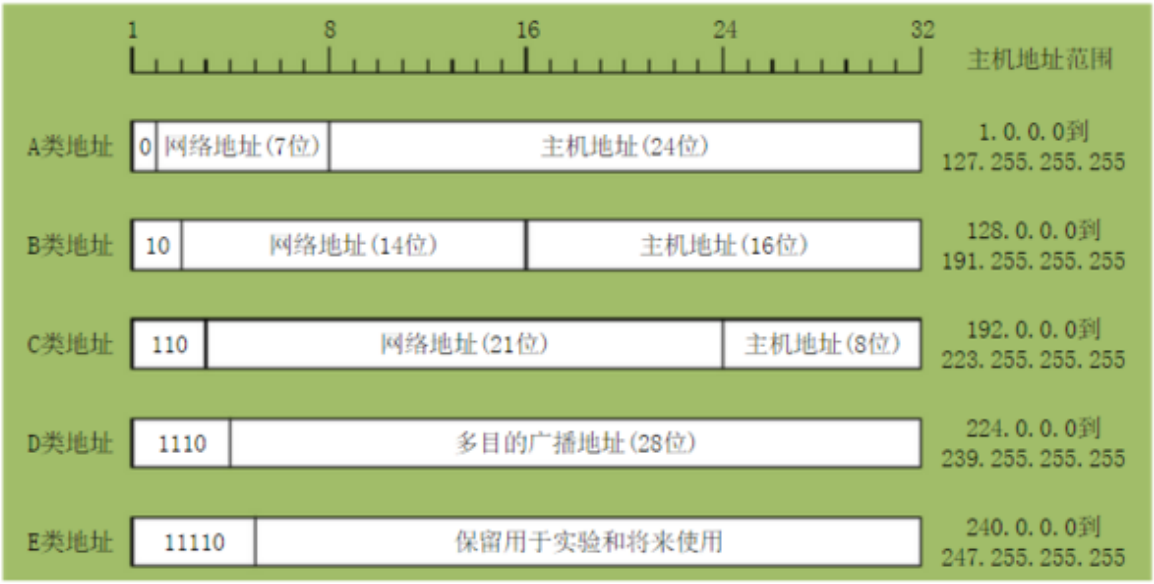
1>. **A类地址**（0.0.0.0 - 127.255.255.255）以”0”头，网络段长度为8位，其中可变部分的长度为7位；主机段长度为24位。7位的可变网络段可识别2^7=128 (0~127)个网络，其中0和127另有用途，故只有126个可用的A类网络地址。另外，主机位全”0”代表网络本身，全”1”代表网内广播，因此一个A类网络地址可识别的可分配地址有 2^24-2 个。

2>. **B类地址**（128.0.0.0 - 191.255.255.255）以”10”开头，网络段长度为16位，可变部分的长度为14位；主机段长度为16位。14位的可变网络段可以识别的网络数为 2^14 个。另外，主机位全”0”与全”1”功能同A类地址，因此一个B类网络可以分配地址有 2^16-2 个。

3>. **C类地址**（192.0.0.0 - 223.255.255.255）以”110”开头，网络段长度为24位，其中可变部分的长度为21位；主机段长度为8位。21位的可变网络段可以识别的网络数为 2^21 个。可分配的主机地址是 2^8-2 个。

4>. **D类地址**（224.0.0.0 - 239.255.255.255）为组播地址，使用”1110”开头，不分网络段和主机段，有 2^28 个组播地址。用于标识预先定义的一组主机。主机使用组播通信时，可以将组播数据报一次性发送给所有同组的主机。

5>. **E类地址**（240.0.0.0 - 255.255.255.255）是保留地址，用于研究使用。以”1111”开头，不区分网络段和主机段，其中32位全1代表本网络内广播，因此E类地址共有 2^28-1 个。



127.x.x.x段地址空间是被保留的回环地址

代表着自己，如127.0.0.1

ip地址又分为**公网ip**和**内网ip**

公网ip是在公网中通过注册购买的ip

在Internet中使用，可以在Internet中随意访问。

私有ip为在内网中相互识别的内部地址

用于组织机构内部使用

内网ip主要有三类

A类IP地址中：`10.0.0.0--10.255.255.255` (大型公司局域网中使用)
B类IP地址中：`172.16.0.0--172.31.255.255` （中型公司局域网中使用）
C类IP地址中：`192.168.0.0--192.168.255.255` （家用/小企业公司局域网中使用）

（两个ip查询网站）

https://zh-hans.ipshu.com/ipv4/

http://ip.yqie.com/

（113不是内网ip，而是教育网提供的外网ip,需要花钱买（学校牛逼））

ip地址可变，是一种逻辑地址

并且一台主机位于多个不同的网络中可以具有不同的ip

（而mac地址唯一）

附：DHCP协议

ip的分配涉及到dhcp协议

服务器控制一段代码范围，使客户机登录时自动获得服务器分配的动态ip与子网掩码

客户机同样也可以自行设置静态ip，但如果ip发生冲突会导致两个人同时收到数据包或都收不到数据包。

附：子网掩码

子网掩码用来指明一个**IP地址（主机地址）**的哪些位标识的是主机所在的子网，以及哪些位标识的是主机的位掩码。

子网掩码用来将某个IP地址划分成**网络号和主机号两部分。**

网络号表示**主机所在的子网**

主机号标识主机

如255.255.255.0

即11111111，11111111，11111111，00000000

说明对应ip有24位网络号，8位主机号

网络（子网）地址即主机号置0

将ip转二进制与子网掩码转二进制进行**按位与运算**

求得的就是对应**网络（子网）地址**

广播地址即主机号置1

广播信道用于将信息发送给当前局域网下所有主机

将ip转二进制与子网掩码转二进制进行**按位异或运算**

求得的就是对应**广播信道地址**

附：IPv6协议

用于替代ipv4的下一代ip协议

IPv6的地址长度为128位，是IPv4地址长度的4倍

1.采用冒分16进制表示法

格式为X:X:X:X:X:X:X:X

每个X的前导0是可以省略的

2.采用0位压缩表示法

某些情况下，一个IPv6地址中间可能包含很长的一段0，可以把连续的一段0压缩为“::”。但为保证地址解析的唯一性，地址中”::”只能出现一次

2.ARP协议

在以太网环境中，**数据的传输所依赖的是MAC地址而非IP地址**，而将已知IP地址转换为MAC地址的工作是由ARP协议来完成的。

一台主机有IP数据报文发送给另一台主机，它都要知道接收方的逻辑（IP）地址。但是IP地址必须封装成帧才能通过物理网络。

这就意味着**发送方必须有接收方的物理（MAC）地址**，因此需要完成逻辑地址到物理地址的映射。而ARP协议可以接收来自IP协议的逻辑地址，将其**映射为相应的物理地址**，然后把物理地址递交给数据链路层。

网关通过广播信道向所有ip发送arp请求

“谁是这个ip”

对应ip的主机将arp相应报文和他的物理地址直接发送给网关

附：arp欺骗

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通信量使网络阻塞，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。

(6条消息) 网络攻防实战--ARP欺骗*vaeloverforever的博客-CSDN博客*arp欺骗

3.ICMP协议

主要用来检测网络通信故障和实现链路追踪

比如经典的ping

通过发送回送请求报文和回送回答报文来检测源主机到目的主机的链路是否有问题，目的地是否可达，以及通信的延迟情况

附：dos攻击

拒绝服务攻击DoS(Denial of Service)：使系统过于忙碌而不能执行有用的业务并且占尽关键系统资源。它是基于这样的思想：用数据包淹没本地系统，以打扰或严重阻止捆绑本地的服务响应外来合法的请求，甚至使本地系统崩溃。

而ddos攻击（分布式拒绝服务攻击）则是通过控制多台主机对服务器进行轰炸

四.数据链路层

将数据封装成帧，根据物理地址进行运输

同时在物理层的基础上提供差错检测，达到可靠传输

五.物理层

电信号的传输

Ⅱ.互联网

一.公网和局域网

互联网分为公网和局域网

公网是最大的局域网，用来定位最基础的一批主机用作服务器

公网ip用于定位服务器

内网ip保留服务器ip的一部分用作子网标识

不同的网络之间通过网关进行传输

附：网关

网关(Gateway)就是一个网络连接到另一个网络的“关口”，既可以用于广域网互连，也可以用于局域网互连。

网关是设备与路由器之间的桥梁，由它将不同的网络间进行访问的控制，转换，交接等等

二.虚拟机的nat与桥接

nat模式表示虚拟机的流量通过物理机发出

物理机作为虚拟机的代理，虚拟机对于外部是透明的

桥接模式表示采用虚拟网卡为虚拟机提供有线网络支持

虚拟机此时和物理机并存

类似于一台真正独立的主机

三.正向/反向代理

1.正向代理

客户端向代理发出请求，代理向目标服务器转交请求

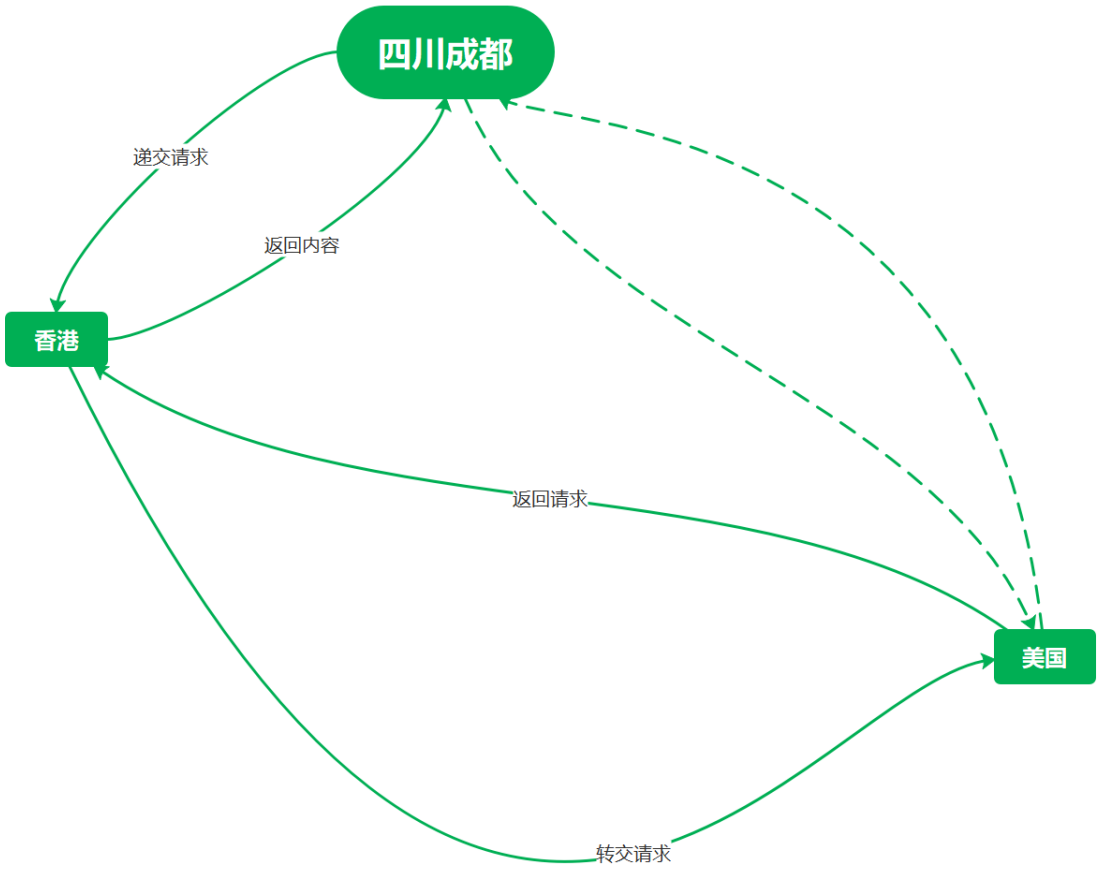
同时将获得的内容返回给客户端

正向代理，其实是"代理服务器"代理了"客户端"，去和"目标服务器"进行交互。

此时对于服务端，只能看到代理的ip，而真正的客户端是透明的

用途：突破防火墙限制，提高访问速度，隐藏ip

例：最简单的梯子



2.反向代理

代理服务器来接受internet上的连接请求，然后将请求转发给内部网络上的服务器，并

将从服务器上得到的结果返回给internet上请求连接的客户端

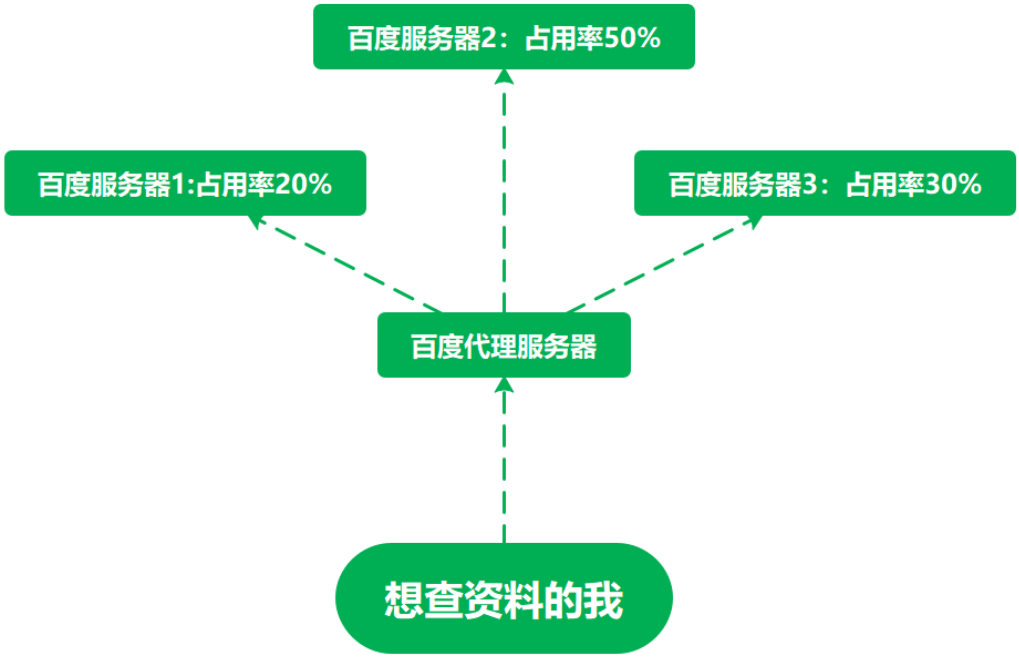
反向代理，其实是"代理服务器"代理了"目标服务器"，去和"客户端"进行交互。

此时目标服务器是透明的，客户端只能看到代理服务器

用途：隐藏服务器真实ip，**负载均衡**，提高访问速度

对于负载均衡

以下面百度的服务器为例



我的请求递交到百度代理之后

会优先被转移到1服务器，使不同的服务器负载均衡