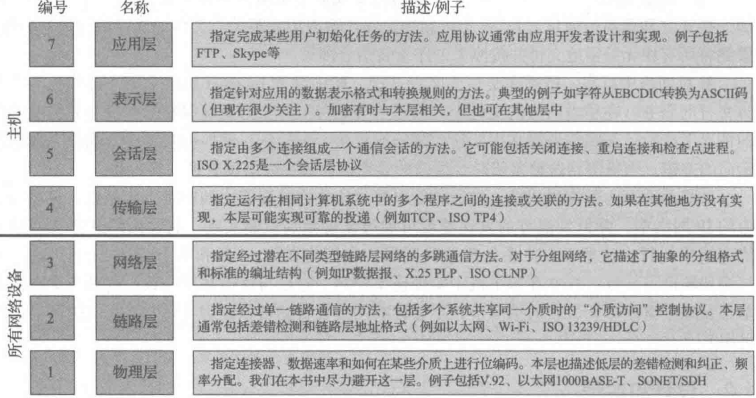
我不得不说，这本书的讲述方式我真的接受不了，太松散了，读着太难受了。

想暑假回去读王道考研那本计算机网络书好了。

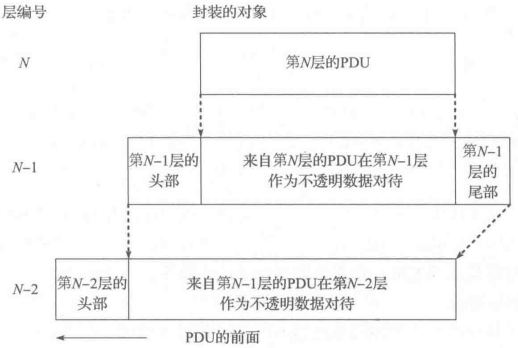
第一章：概述

互联各种网络，由一组网关（后称路由器）来实现，网管可以在互不兼容的网络之间提供翻译功能

分层：层与层之间的关系，只是传递和接收相应的包，然后在本层里面进行各种操作



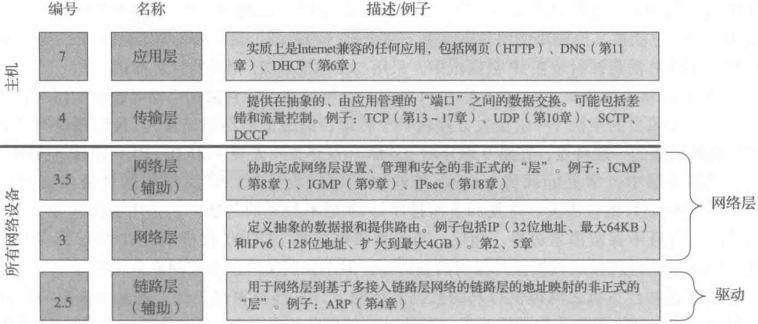
分层中的封装：



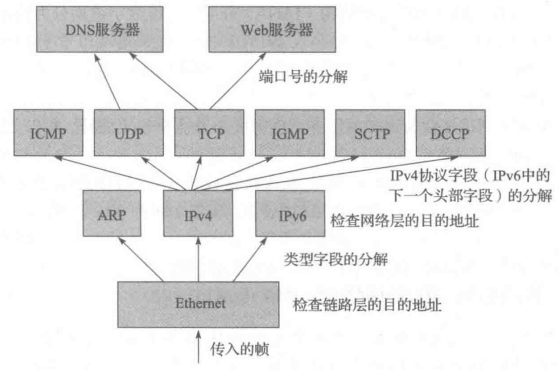
封装：从上到下PDU添加头部尾部，然后保证不看上层传递下来的信息

分层的好处是并不是所有网络设备都要实现所有层，只要实现盒子及相关的层就好

TCP/IP协议族分层结构



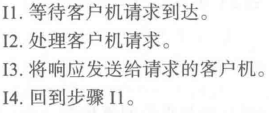
模拟PDU如何在一台Internet主机上进行分解

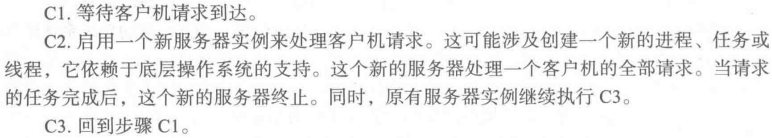


端口号：16位的非负整数。每个ip地址因此有65536个可用的端口号，每个传输协议可使用这些端口号。

常用服务端口号：安全外壳协议22，FTP20 21，Telnet远程终端协议23，电子邮件/简单邮件传输协议SMTP25,域名系统53，超文本传输协议HTTP和HTTPS80和443、交互式邮件访问协议IMAP和IMAPS端口143和993，简单网络管理协议SNMP，端口161和162，轻量级目录访问协议LDAP389

客户机/服务器

迭代：

并发：

并发的优点是每个客户都有自己的服务器实例。大多数服务器是并发的。

对等：每个应用既是客户机也是服务器，又是同时是两者，并能转发请求。

应用程序编程接口：无论是P2P还是客户机/服务器，都需要表述其所需要的网络操作，例如建立一个连接，写入或读取数据。这些通常由主机操作系统使用一个网络应用程序编程接口（API）来实现。最流行的API称为是套接字。

第二章：Internet地址结构

IP地址表示：IPV4点分十进制，32位。IPv6128位，两个字节一分

分类寻址：A 0 B 10 C 110 D 1110 E 1111 ABC单播 D组播 网络号个数不同

子网寻址：一个A/B/C类地址在网络号后在划分一部分作为子网号

子网掩码：用来确定IP地址的网络和子网信息

可变长度子网掩码：看掩码重合的位数的多少

广播地址：主机位全部是1，

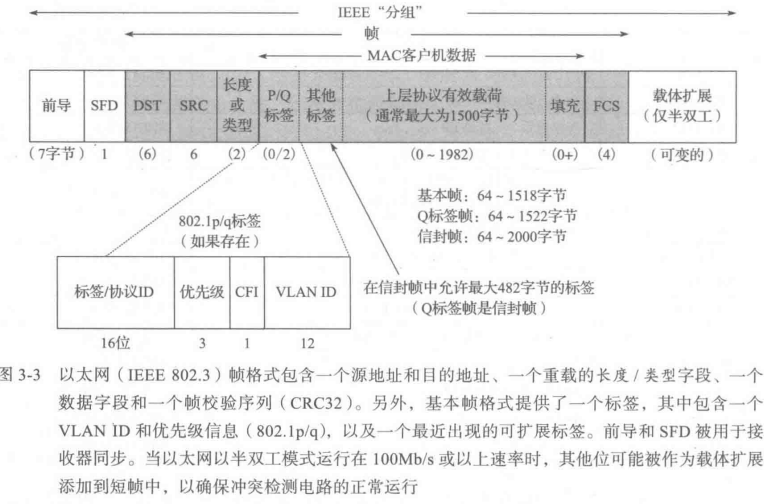
本地地址：主机位全部是0

CIDR和聚合：无类别域间路由，Internet路由器也要有处理掩码的功能，IP地址根据相同掩码的长度数字进行聚合，长掩码比较IP地址后，找到最长相同的位，然后缩短掩码，这就是一个聚合的过程了。

组播：

第三章：链路层

以太网帧格式：



有效载荷部分是放上层PDU的地方，循环冗余校验保证帧在传输过程中没有受损，将要发送的数据与校验码多项式做除法得到余数，然后放到FCS中，到了之后再做一遍，看是否相同

帧最大1518字节，4个CRC和14字节头部，MTU为1500字节。大消息则需要多个帧。

网桥：连接多个物理的链路层网络或成组的站，转发表中是mac地址

交换机：本质上是高性能的网桥

网桥建立转发表使用的协议：生成树协议，快速生成树协议

第四章：地址解析协议

ARP：32位IPv4到48位MAC地址之间的映射

ARP协议用于确定本地可达的IPv4子网使用的IPv4地址对应的硬件地址。

ARP缓存是其运行的基础

ARP每个条目中都有一个计时器，用于清楚不完整的条目和完整的条目。

第五章 IP协议  
IP协议是TCP/IP协议族中的核心协议。所有TCP、UDP、ICMP和IGMP数据都通过IP数据包传输。

提供一种尽力而为、无连接的数据交付服务。它不保证IP数据报能成功到达目的地。



IPv4数据报格式。基本IP头部应该是20字节。

版本号说明v4还是v6

IHL（头部长度）字段保存IPv4头部中32位字的数量，包括任何选项。最多60字节

区分服务字段（DS字段），显式拥塞控制字段（ECN）‘’

总长度字段（IPv4数据报的总长度），通过这个字段以及IHL字段，可以知道IPv4数据报从哪里开始，以及它的长度，16位，因此IPV4数据包最大长度为65535字节。

标识字段帮助标识IPv4主机发送的数据包。为避免将一个数据报分片和其他分片混淆

生存期设置一个数据报可经过的路由器数量的上限

协议字段标识数据报有效载荷部分的数据类型。最常用的是17和6，分别是UDP TCP

头部校验和仅计算IPv4头部，不检查IPv4数据报有效载荷的正确性。

IP转发：本地直连主机或者共享网络，IP数据报直接发送到目的地，不需要或者不使用路由器，否则，主机将数据报交给路由器，如果IP层配置一台路由器，则转发该数据报；还有可能就是将数据报默默丢弃。比如没有路由器，ICMP消息可能发送回源节点，以表明发生了一个错误。

转发表：每一条至少包含，目的地，掩码，下一跳，接口

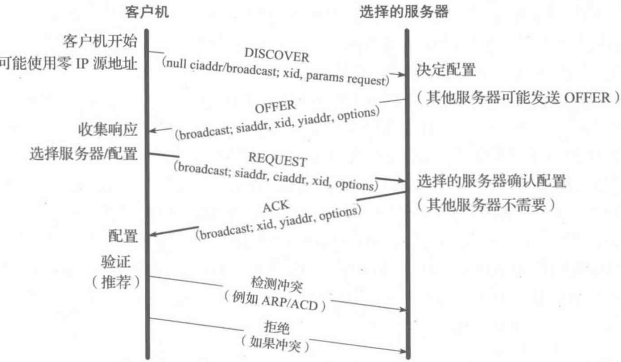
IP转发行动：执行最长前缀匹配算法，在掩码mj中有多少位设置为1。设置为1的位数越多，说明匹配的越好，选择最匹配的条目ek，将其下一跳字段nk作为转发数据报的下一跳IP地址，如果本地出现无法交付的数据报，通常向生成数据报的应用程序返回一个“主机不可达”错误，通过ICMP消息返回给发送数据报的主机

第六章：DHCP和自动配置

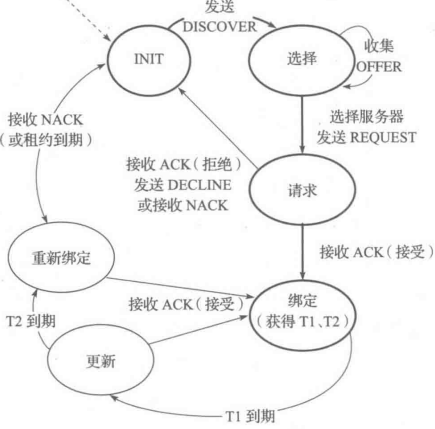
地址池：专门为DHCP用途而分配的一个连续的IP地址范围

租用：DHCP客户机请求分配一个IP地址，服务器从可用的地址池中选择一个地址作为响应。分配给客户机的地址只在一段特定时间内有效，这段时间称为租用期

DHCP协议操作



DHCP状态机



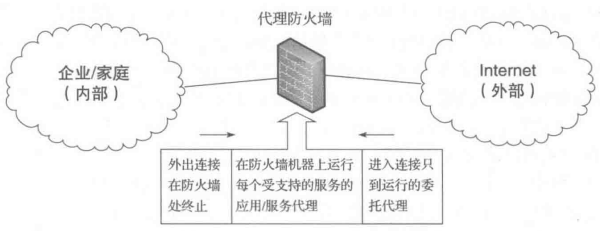
第七章：防火墙和网络地址转换

防火墙：它是一种能够限制所转发的流量类型的路由器

分类：代理防火墙，包过滤防火墙

包过滤防火墙：配置为丢弃或转发数据包头中符合（或不符合）特定标准的数据包

代理防火墙：并不是真正意义上的互联网路由器。本质上是运行一个或多个应用层网关的主机，这种类型的防火墙必须为每一个传输层服务设置一个代理，任何要使用的新服务必须安装一个相应的代理，并通过代理来操作发起连接。最常见的是HTTP代理防火墙，和SOCKS防火墙



网络地址转换（NAT）：本质上是允许在互联网的不同地方重复使用相同的IP地址集的机制。

NAT的工作原理就是重写通过路由器的数据包的识别信息。这种情况常发生在数据传输的两个方向上。

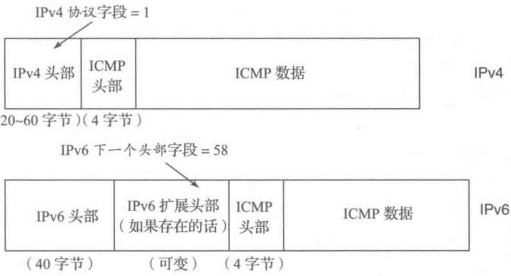
NAT需要重写往一个方向传输的数据包的源IP地址，重写往另一个方向传输的数据包的目的IP地址。

这允许传出的数据包的源IP地址变为NAT路由器中面向Internet的网络接口地址，而不是原始主机的接口地址

第八章：Internet控制报文协议

确切的说ICMP既不是一个网络层协议也不是一个传输层协议，而是位于两者之间

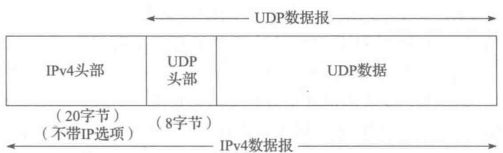
在IPv4和IPv6中的封装



第九章：广播和本地组播

第十章：用户数据报协议和IP分片

UDP保留消息边界的简单的面向数据报的传输层协议，不提供差错纠正，队列管理，重复消除，流量控制，拥塞控制。



UDP头部格式



第十一章：名称解析和域名系统

第十二章：TCP传输控制协议

IP UDP没有实现差错纠正，对于以太网和基于以上的其他协议，协议提供一定次数的重试，如果还是不成功就放弃

当信息出错，就简单的“尝试重新发送”，直到信息最终被接收，这种处理差错的方法，称为自动重复请求（ARQ），构成了许多通信协议的基础，包括TCP

ARQ和重传：

1. 接收方是否收到分组
2. 接收方收到的分组是否与之前发送方发送的一样。接收方给发送方发信号以确定自己已经接收到一个分组，这种方法称为确认，或ACK。最基本的形式是发送方发送一个分组，接收方收到这个分组，再发送对应的ACK。当发送方接收到这个ACK，它再发送另一个分组，这个过程就这样继续。

随之而来的问题：

1. 发送方对一个ACK应该等待多久？
2. 如果ACK丢失了怎么办？
3. 如果分组被接受到了，但是里面有错怎么办？

解决问题的办法

1. 每个分组有一个序列号，定义一个分组窗口作为已被发送方注入但还没完成确认的集合。窗口中分组数量称为窗口大小，控制窗口滑动的协议为滑动窗口协议
2. 为了处理当接收方相对发送方太慢产生的问题，，接收方跟不上时会强迫发送方慢下来，称为流量控制，该控制经常以 基于速率流量控制：给发送方指定某个速率，同时确保数据永远不能超过这个速率发送。这个类型的流量控制最适合流应用程序；另一种是基于窗口流量控制，窗口大小不固定，允许随着时间而发生变动。为了使用这种技术进行流量控制，必须有一种方法让接收方可以通知发送方使用多大的窗口
3. 设置超时重传：让协议实现尝试去估计它们。这称为往返时间估计，一个统计过程。选择一组RTT样本的样本均值作为真实的RTT是最有可能的

TCP和UDP使用相同的网络层，但是TCP提供一种面向连接的，可靠的字节流服务。

TCP头部和封装



头部：

