TCP_IP学习笔记:TCP_IP协议介绍 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/142/2021_2022_TCP_IP_E5_AD_A6_E4_c101_142303.htm TCP/IP的通讯协议 这部分简要介绍一下TCP/IP的内部结构，为讨论与互联网有关的安全问题打下基础。TCP/IP协议组之所以流行，部分原因是因为它可以用在各种各样的信道和底层协议（例如T1和X.25、以太网以及RS-232串行接口）之上。确切地说，TCP/IP协议是一组包括TCP协议和IP协议，UDP（User Datagram Protocol）协议、ICMP（Internet Control Message Protocol）协议和其他一些协议的协议组。 TCP/IP整体构架概述 TCP/IP协议并不完全符合OSI的七层参考模型。传统的开放式系统互连参考模型，是一种通信协议的7层抽象的参考模型,其中每一层执行某一特定任务。该模型的目的是使各种硬件在相同的层次上相互通信。这7层是:物理层、数据链路层、网路层、传输层、话路层、表示层和应用层。而TCP/IP通讯协议采用了4层的层级结构，每一层都呼叫它的下一层所提供的网络来完成自己的需求。这4层分别为： 应用层：应用程序间沟通的层，如简单电子邮件传输（SMTP）、文件传输协议（FTP）、网络远程访问协议（Telnet）等。 传输层：在此层中，它提供了节点间的数据传送服务，如传输控制协议（TCP）、用户数据报协议（UDP）等，TCP和UDP给数据包加入传输数据并把它传输到下一层中，这一层负责传送数据，并且确定数据已被送达并接收。 互连网络层：负责提供基本的数据封包传送功能，让每一块数据包都能够到达目的主机（但不检查是否被正确接收），如网际协议（IP）。 网络接口层：对实际的网

络媒体的管理，定义如何使用实际网络（如Ethernet、Serial Line等）来传送数据。TCP/IP中的协议 以下简单介绍TCP/IP中的协议都具备什么样的功能，都是如何工作的： 1. IP 网际协议IP是TCP/IP的心脏，也是网络层中最重要的协议。 IP层接收由更低层（网络接口层例如以太网设备驱动程序）发来的数据包，并把该数据包发送到更高层---TCP或UDP层；相反，IP层也把从TCP或UDP层接收来的数据包传送到更低层。IP数据包是不可靠的，因为IP并没有做任何事情来确认数据包是按顺序发送的或者没有被破坏。IP数据包中含有发送它的主机的地址（源地址）和接收它的主机的地址（目的地址）。 高层的TCP和UDP服务在接收数据包时，通常假设包中的源地址是有效的。也可以这样说，IP地址形成了许多服务的认证基础，这些服务相信数据包是从一个有效的主机发送来的。IP确认包含一个选项，叫作IP source routing，可以用来指定一条源地址和目的地址之间的直接路径。对于一些TCP和UDP的服务来说，使用了该选项的IP包好象是从路径上的最后一个系统传递过来的，而不是来自于它的真实地点。这个选项是为了测试而存在的，说明了它可以被用来欺骗系统来进行平常是被禁止的连接。那么，许多依靠IP源地址做确认的服务将产生问题并且会被非法入侵。 2. TCP 如果IP数据包中有已经封好的TCP数据包，那么IP将把它们向‘上’传送到TCP层。TCP将包排序并进行错误检查，同时实现虚电路间的连接。TCP数据包中包括序号和确认，所以未按照顺序收到的包可以被排序，而损坏的包可以被重传。TCP将它的信息送到更高层的应用程序，例如Telnet的服务程序和客户程序。应用程序轮流将信息送回TCP层，TCP层便

将它们向下传送到IP层，设备驱动程序和物理介质，最后到接收方。 面向连接的服务（例如Telnet、FTP、rlogin、X Windows和SMTP）需要高度的可靠性，所以它们使用了TCP。DNS在某些情况下使用TCP（发送和接收域名数据库），但使用UDP传送有关单个主机的信息。 3.UDP UDP与TCP位于同一层，但对于数据包的顺序错误或重发。因此，UDP不被应用于那些使用虚电路的面向连接的服务，UDP主要用于那些面向查询---应答的服务，例如NFS。相对于FTP或Telnet，这些服务需要交换的信息量较小。使用UDP的服务包括NTP（网落时间协议）和DNS（DNS也使用TCP）。 欺骗UDP包比欺骗TCP包更容易，因为UDP没有建立初始化连接（也可以称为握手）（因为在两个系统间没有虚电路），也就是说，与UDP相关的服务面临着更大的危险。 4.ICMP ICMP与IP位于同一层，它被用来传送IP的的控制信息。它主要是用来提供有关通向目的地址的路径信息。ICMP的‘Redirect’信息通知主机通向其他系统的更准确的路径，而‘Unreachable’信息则指出路径有问题。另外，如果路径不可用了，ICMP可以使TCP连接‘体面地’终止。PING是最常用的基于ICMP的服务。 5. TCP和UDP的端口结构 TCP和UDP服务通常有一个客户/服务器的关系，例如，一个Telnet服务进程开始在系统上处于空闲状态，等待着连接。用户使用Telnet客户程序与服务进程建立一个连接。客户程序向服务进程写入信息，服务进程读出信息并发出响应，客户程序读出响应并向用户报告。因而，这个连接是双工的，可以用来进行读写。 两个系统间的多重Telnet连接是如何相互确认并协调一致呢？TCP或UDP连接唯一地使用每个信息中

的如下四项进行确认： 源IP地址 发送包的IP地址。 目的IP地址 接收包的IP地址。 源端口 源系统上的连接的端口。 目的端口 目的系统上的连接的端口。 端口是一个软件结构，被客户程序或服务进程用来发送和接收信息。一个端口对应一个16比特的数。服务进程通常使用一个固定的端口，例如，SMTP使用25、Xwindows使用6000。这些端口号是‘广为人知’的，因为在建立与特定的主机或服务的连接时，需要这些地址和目的地址进行通讯。 100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com