《TCP/IP详解 卷1：协议（英文版）》

图书基本信息

书名：《TCP/IP详解 卷1：协议（英文版）》

13位ISBN编号：9787115222596

10位ISBN编号：7115222592

出版时间：2010-3

出版社：人民邮电出版社

作者：W.Richard Stevens

页数：598

《TCP/IP详解 卷1：协议（英文版）》

前言

本书介绍的是TCP/IP协议族，但是视角却不同于其他TCP/IP教科书。我们将用一种流行的诊断工具来动态地监视协议，而不仅仅是描述协议及其功能。通过观察不同环境下协议的运作情况，可以更好地理解其工作原理和设计方案的由来。此外，本书还分析了协议的实现，读者无须花费精力去阅读数千行的源代码。　　在网络协议从20世纪60年代到20世纪80年代的发展过程中，必须要使用昂贵的专用硬件才能监视到分组在线路上的传送情况。要理解由硬件显示的分组，还必须对协议极为熟悉。硬件分析器的功能也受限于硬件设计者所提供的内置功能。　　现在的情况有了显著的变化：随处可见的工作站就能监视局域网了[Mogul 1990]。只要在网络上连接一个工作站，然后运行一些公用软件（详见附录A），就能够观察线路上发生的情况。很多人可能会认为这只是一个诊断网络问题的工具，实际上它也非常有助于理解网络协议的工作原理，这正是本书的目标。　　本书面向所有希望了解TCP/IP协议运行原理的读者：编写网络应用的程序员、利用TCP/IP维护计算机系统与网络的系统管理员以及那些需要每天与TCP/IP应用打交道的用户。　　本书的结构　　下图给出了本书涉及的各种协议和应用，方框上的斜体数字指明了该协议或应用在哪一章讨论。　　(图中略去的许多细节将在相应的章节中讨论。例如，DNS和RPC都用到了TCP，但从图中看不出来。)　　我们采用一种自底向上的方式来介绍TCP/IP协议族。第1章介绍TCP/IP的基础知识；随后从链路层（第2章）开始向上介绍协议栈。这样做可以为不熟悉TCP/IP或者网络的读者提供阅读后续章节所需的背景知识。

《TCP/IP详解 卷1：协议（英文版）》

内容概要

《TCP/IP详解.卷1:协议(英文版)》是TCP/IP领域的经典之作！书中主要讲述TCP/IP协议，不仅仅讲述RFC的标准协议，而且结合大量实例讲述了TCP/IP协议族的定义原因，以及在各种不同的操作系统中的应用及工作方式，使读者可以轻松掌握TCP/IP的知识。《TCP/IP详解.卷1:协议(英文版)》内容详尽且具权威性，几乎每章都提供精选的习题，并提供了部分习题的答案。
《TCP/IP详解.卷1:协议(英文版)》适合任何希望理解TCP/IP协议如何实现的人阅读，更是TCP/IP领域研究人员和开发人员的权威参考书。无论是初学者还是功底深厚的网络领域高手，《TCP/IP详解.卷1:协议(英文版)》都是案头必备。

《TCP/IP详解 卷1：协议（英文版）》

作者简介

W. Richard Stevens 国际知名的UNIX和网络专家，备受赞誉的技术作家。他1951年2月5日出生于赞比亚，后随父母回到美国。中学时就读于弗吉尼亚菲什伯恩军事学校，1973年获得密歇根大学航空和航天工程学士学位。1975年至1982年，他在亚利桑那州图森市的基特峰国家天文台从事计算机编程工作，业余时间喜爱飞行运动，做过兼职飞行教练。这期间他分别在1978年和1982年获得亚利桑那大学系统工程硕士和博士学位。此后他去康涅狄格州纽黑文的健康系统国际公司任主管计算机服务的副总裁。1990年他回到图森，从事专业技术写作和咨询工作。写下了多种经典的传世之作，包括《TCP/IP详解》（三卷）、《UNIX环境高级编程》和《UNIX网络编程》（两卷）。Stevens于1999年9月1日去世，年仅48岁。2000年他被国际权威机构USENIX追授“终身成就奖”。

《TCP/IP详解 卷1：协议（英文版）》

书籍目录

章节摘录

The third and major reason is that the room allocated for options in the IP header isnt large enough today to handle most routes. There is room for only nine IP addresses in the IP header options field. In the old days of the ARPANET this was adequate, but it is far too small nowadays. Traceroute uses ICMP and the TTL field in the IP header. The TrL field （time-to-live） is an 8-bit field that the sender initializes to some value. The recommended initial value is specified in the Assigned Numbers RFC and is currently 64. Older systems would often initialize it to 15 or 32. We saw in some of the Ping examples in Chapter 7 that ICMP echo replies are often sent with the TrL set to its maximum value of 255. Each router that handles the datagram is required to decrement the TTL by either one or the number of seconds that the router holds onto the datagram. Since most routers hold a datagram for less than a second, the TrL field has effectively become a hop counter, decremented by one by each router. The purpose of the TTL field is to prevent datagrams from ending up in infinite loops, which can occur during routing transients. For example, when a router crashes or when the connection between two routers is lost, it can take the routing protocols some time （from seconds to a few minutes） to detect the lost route and work around it.During this time period it is possible for the datagram to end up in routing loops. The TTL field puts an upper limit on these looping datagrams. When a router gets an IP datagram whose TTL is either 0 or 1 it must not forward the datagram. （A destination host that receives a datagram like this can deliver it to the application, since the datagram does not have to be routed. Normally, however, no system should receive a datagram with a TTL of 0.） Instead the router throws away the datagram and sends back to the originating host an ICMP "time exceeded" message.The key to Traceroute is that the IP datagram containing this ICMP message has the routers IP address as the source address. We can now guess the operation of Traceroute. It sends an IP datagram with a TTL of 1 to the destination host. The first router to handle the datagram decrements the TTL, discards the datagram, and sends back the ICMP time exceeded. This identifies the first router in the path. Traceroute then sends a datagram with a TrL of 2, and we find the IP address of the second router. This continues until the datagram reaches the destination host. But even though the arriving IP datagram has a TTL of 1, the destination host wont throw it away and generate the ICMP time exceeded, since the datagram has reached its final destination. How can we determine when weve reached the destination？ Traceroute sends UDP datagrams to the destination host, but it chooses the destination UDP port number to be an unlikely value （larger than 30,000）, making it improbable that an application at the destination is using that port. This causes the destination hosts UDP module to generate an ICMP "port unreachable" error （Section 6.5） when the datagram arrives. All Traceroute needs to do is differentiate between the received ICMP messages——time exceeded versus port unreachable——to know when its done.

媒体关注与评论

“这本书必定是TCP/IP开发人员和用户的圣经。Stevens揭秘了此前一些网络专家讳莫如深的许多奥妙。我本人参与过几年TCP/IP的实现工作，以我的观点，这本书堪称目前最详尽的参考书了。”
——Robert A. Ciampa，3COM公司网络工程师　　“Stevens创作了一本很好的教材和参考书。内容组织合理，文字清晰易懂，书中有很多出色的图示详细解读了IP、TCP和辅助协议以及应用的原理与运作中的隐秘细节。”　　——Scott Bradner，哈佛大学OIT/NSD技术顾问　　“比光讲理论强多了。Stevens采用了多主机的配置，带领我们饱览TCP/IP的各种例子和图示。基于实际的例子，这些例子反过来又强化了理论，这一点使其有别于本领域的所有其他书籍，并使本书既有极强的可读性，又蕴涵丰富的信息。”　　——Peter M.Haverlock，IBM TCP/IP技术顾问　　“卷1对于开发人员、网络管理员以及任何想理解TCP/IP技术的人来说，都是极好的参考书。内容非常全面，既能满足专家的需要，也给了新手足够的背景知识和注解。”　　——Bob Williams，NetManage公司营销副总裁
“Stevens写的所有书都相当出色，这部巨著再次令世人称奇。虽然已经有不少书在写TCP/IP了，但是这本书以其深入和详实而领先群伦。Stevens带领读者深入TCP/IP协议的内部，采用了形象化的方法展示协议的运作。”　　——Steven Baker，Unix Review杂志　　“书中的图示好极了，写作风格清新，可读性强。总之，Stevens把一个复杂的问题说得很容易理解。这本书值得每个人关注。你一定要读一读，并把它珍藏在书架上。”　　——Elizabeth Zinkann，Sys Admin杂志　　“作者成功地创作出了又一本不可或缺的网络巨著。这是我所读过的最全面、最完整的TCP/IP著作，写法完全不同于其他书，不仅详细介绍了TCP、IP、ARP、ICMP、路由技术等，还实际展示了这些协议和常见网络工具的用法。”　　——Eli Charne，ConneXions杂志　　“……区别在于Stevens力图向大家清晰地展示协议内幕。他的主要方法是直截了当地阐释、章末提供练习题、对于首部等逐字节解读，并将实际通信流内容列出来作为示例。”　　——Walter Zintz，Unix World杂志

《TCP/IP详解 卷1：协议（英文版）》

精彩短评

1、东西不错，不过一直没时间看
2、有了最新版，老版就不看了。
3、一月读书计划-部分精度部分跳读，看原理比较容易让人犯困，还好没再傻逼的字字揣摩。一直以为，跳读的时候，没有什么收获，其实不是~
4、后面的pearson 防伪标签 残缺不全 纸张的话 感觉对不起这个价 封面的有挤压的痕迹 建议书和别的商品不要放在一起 包装虽好 但是塑料纸 扛不住挤压的

印刷的清晰，在吐槽下纸张 看着让人纠结
至于有人说正不正品 我也不知再怎么看 书字迹清晰 没错别字就可以了 要求不高
总的来说4星
5、非常详细
6、看书的纸张就知道是正版
7、内容很好，不过感觉印刷质量还是差了点点啊
8、想必不用多说了，这本书的经典地位几乎没有什么别的书可以动摇。非常详细地说明了TCP/IP协议族的方方面面，大量的例子和图表。
爱不释手的好书
9、前后断断续续一个半月读完，受益匪浅！

TCP领域无可争议的圣经，应该給十星！美中不足是作者英年早逝，使得本书没有后来与时俱进进行修订，有些内容稍感落后。不过tcp ip的原理还是很透彻的，英语写作也很好
10、书就不用多说了，纸质还OK。虽然快递有点慢，送货员来了好多次都没找到我，不过最后还是送过来了，态度很不错。
11、感受原汁原味的科技作品，过瘾！
12、好书 真是经典！
13、把各种协议的包头看了个遍
14、书质量不错，不过希望包装好点 以免运输过程中损坏
15、Excellent book
16、内容有点老，不过书中举的例子都很经典
17、非常喜欢，虽然有电子版的，还是捧本书比较舒服
18、
19、十分经典的英文读物
20、拿到手一翻 应该是正版的 全部是英文 以我的知识积累 但愿能够看懂 纸张好 速度快
21、书不错，为什么最后一页有类似脚印的泥印
22、此书非常不错,正在阅读中,很喜欢,三册买全了
23、再次orz stenens的好书！太深入了，可惜平时用的不多。
24、经典书籍，那是玩网络必备的。

就是有点贵~~~ 从02年的45上升了10年的79
25、网络的经典之作
26、TCP/IP精髓书籍,英文版仅语言障碍,理解方面,似乎比中译版本更顺畅...
27、经典不容质疑
28、书不赖 质量好
29、不错的书 值得一看～～
30、网络经典，不得不看
31、除了部分已经过时了的应用层协议，精读了余下的绝大部分。小部分未读内容需找第二版补缺。（还需的重要内容有: DHCP，IPv6 众协议，HTTP 众协议，SMTP 等）
32、真是圣书啊。

33、协议经典
34、购买方便，经典书籍。
35、只看了tcp部分，stevens的书写的深入明白。
36、本书针对liux作为平台来讲的,全是英文,呵呵. 耐心看看真的还不错的了
37、看过中文版的! = = 啊. 不对.PDF看了30多页呢
38、中文版有一处错误，这个原版没有
39、纸张质量不错了！
40、10星
41、书的质量非常好，很好很强大...
42、书籍质量不错，快递也给力
43、对学习网络理论的GGJJ有益
44、圣经，必读
45、把前24章读了10遍以上吧，25以后应用层的协议介绍后面再慢慢看了。
46、断断续续读了一年多终于看完了，记了2000多行笔记，收获很大。
47、刚开始的时候，我曾怀疑它是否只是徒有虚名；到最后，我却不得不跟其他人一样不厌其烦地跟周边的朋友说，这本书太TM经典了，学网络你必须得看！看一定要看英文原版！中文版烂得一塌糊涂！
48、阅读后真实的内心感受很好
49、细致系统的讲解了TCP/IP协议族中各个协议，结合具体的网络监测工具，能够更加深入的理解网络协议的运行原理。
50、内容就不评价了，大家都知道，书还是不错的，不过有眯褶皱。。。

《TCP/IP详解 卷1：协议（英文版）》

精彩书评

1、书是1994年出版的，号称是经典。但是呢，很多东西过时了。我刚看了一些，就发现不少过时的内容。比如没有介绍IP的CIDR，没有介绍TCP的ECN。如果要作为教材来学习，我建议还是看一本比较与时俱进的书，相信会有更好的教材。如果是作为权威的参考书，那么还是不错的。另外，当我仔细研读的时候，发现该书的语言怎么竟然不太顺畅呢？比如17.3 TCP Header节226页第3段第1句：The sequence number identifies the byte in the stream of data from the sending TCP to the receiving TCP that the first byte of data in this segment represents. 另外，怎么可以用write做名词呢？

《TCP/IP详解 卷1：协议（英文版）》

章节试读

1、《TCP/IP详解 卷1：协议（英文版）》的笔记-第5页

1.RARP帧类型为0x8035，操作码3，应答操作码为4。
-
ARP/RARP请求都是广播，应答都是单播。
-
RARP协议为无盘工作站提供bootstrap，得到请求的源MAC之后，找到谁有这个MAC的IP，并单播回应。
-
RARP原理是在链路层上广播，能阻止大部分路由转发，确保最少的应答信息。
==========
2.假设sun主机（无盘工作站）需要在网络上引导。bsdi负责RARP服务/tcpdump，我们使用tcpdump -e得到：（1）源地址，目的地址——广播，类型，数据报长度
根据MAC寻找IP，并将返回目标设置为MAC
（2）源地址，目的地址，类型，长度
返回IP给设置的MAC
（3）源地址，目的地址，类型，长度
sun收到IP后，发送一个TFTP读请求（RRQ）给文件8CFC0D21
（收到IP后，立刻发送TFTP请求来读取引导文件）

注意（2）中数据报长度不符合最短长度，是因为此处tcpdump运行在发送端，未经过网卡的填充处理。（14头+28数据）——>网卡补空白直到60——>发送

如果没有bsdi，sun将超时重发：==========
3.RARP的复杂性：
-
（1）ARP服务是TCP/IP协议的一部分，ARP时，容易取得需要返回的MAC；而RARP有依赖性和复杂性，RARP时，需要读取/etc/ethers，而内核操作不能读取，只能交给【用户进程】来完成。
-
（2）RARP需要根据不同的系统，具体实现（参考BSD Packet Filter包过滤/Sun's Network Interface Tap/SVR4 Data Link Provider Interface）。
-
（3）RARP请求用的是链路层广播，所以不能由路由器转发，因此，如果要在此网保证RARP，则只能在此网上，增加冗余RARP服务器。有了多个RARP服务器后，解析时返回的RARP应答可能很多，在时间上引发以太网collisions。

2、《TCP/IP详解 卷1：协议（英文版）》的笔记-第4页

1.ARP协议为IP层的物理寻址提供映射解析。RARP被那些没有磁盘驱动器的系统使用，需手工设置。
ARP适合于很多主机和路由连接到单一节点的情况，这样这个节点就拥有很多解析映射，广播给同一网段的所有主机和路由。
ARP是将32位的IP解析为48位的MAC。
点对点链路不使用ARP，当设置这种链路（引导时），必须告知每一段IP地址，不涉及MAC地址。
ARP高速缓存中每一项的生存时间一般为20min。
==========
2.应用程序的请求实例(ftp bsdi)：

FTP->gethostbyname函数（DNS解析函数、etc/hosts）将bsdi转化为相应IP->FTP调用TCP->TCP发送IP数据报
（如果IP在本地网络）->直接传到主机
（如果IP在远程网络）->IP选路函数->传到路由主机
->出接口时如使用以太网，ARP函数广播IP请求->bsdi收到请求，ARP函数广播IP和对应MAC->主机收到回复，使用得到的IP协议发送IP数据报。==========
3.ARP请求/应答结构-
（-请求解析的目的地址（全1广播）、源地址、以太网帧类型0x0806；）
-硬件类型（1为以太网）、协议类型（0x0800为IP地址= 以太网帧的IP类型值）：组合起来表示按照协议类型地址匹配，返回硬件类型地址；
-硬件地址长度（6为以太网）、协议地址长度（4为IP）；
-OP（操作字段）：四种操作类型——ARP请求（1）、ARP应答（2）、RARP请求（3）、RARP应答（4）；
-发送端硬件地址（与以太网头部发送端相同）、发送端协议地址、目的端硬件地址、目的端协议地址。
-
ARP实例讲解：
对于一个ARP请求来说，除目的端硬件地址外的所有其他的字段都有填充值，当系统接到一份目的端为本机的ARP请求报文之后，他就把硬件地址填进去，然后用两个目的端地址分别替换两个发送端地址，并把炒作字段值为2，最后把它发送出去。
==========
4.ARP实例1（一般情况、删去了结束命令4行）（1）发送端地址、接收端地址（广播）、以太网数据帧类型、数据帧长度（以太网头14+ARP46，有的是64含尾部）、匹配IP、请求地址
（2）在TCPDUMP输出中，第4行svr2发出IP数据报时没有提出ARP请求，是因为它可能已经缓存过bsdi。
==========
5.ARP实例2（不存在的ARP映射、因为已知ARP是广播的所以不加参数-e）（1）大约在5.5秒时进行第一次请求，在29.5秒时进行第三次请求，在76秒时放弃，
（2）ARP请求对应与TCP发送的初始RCPSYN段，
（3）只有有ARP回复确定了MAC之后，才会有TCP数据报发送。
==========
6.ARP代理
（1）当140.252.1上的其他主机（gemini）有一份IP数据报要发送给140.252.1.29（sun）时，gemin比较网络号（140.252）和子网号（1），因为它们是相同的，所以在140.252.1上广播ARP请求。
（2）路由器netb识别出IP属于它的一个拨号主机，于是将自己的MAC通过140.252.1应答。gemin发送IP数据报到netb，netb隐藏了传递给sun的过程。
（3）如果在gemini上ARP解析netb和sun，应答的MAC都是netb的地址。
（4）netb与sun的线路只有一个IP的原因：因为netb不需另一端的IP地址，相反，它通过packets到达时的串行线路端口，来确定分发线路。
（5）netb接收所有140.252.13的ARP请求并应答，netb路由表实现对140.252.13上主机的映射，所有IP数据包转发由netb负责。
==========
7.无偿ARP（gratuitous ARP）
（1）检查同IP，如果有应答，说明IP冲突；
（2）按ARP请求帧里的源IP和源MAC刷新映射（修改此IP对应的MAC）。（因为ARP请求会让所有接收到请求的主机，依照刷新源IP到源MAC的映射）
（除非全网主机都有gratuitous ARP，否则不建议使用gratuitousARP）
==========
8.arp -a/-d/-s

arp -s ip mac
==========
9.总结：
（1）大多数的TCP/IP实现中，ARP是透明的，ARP命令对告诉缓存进行检查和操作。
（2）高速缓存中每一项内容都有一个定时器，根据它删除完整/不完整映射。
（3）委托ARP用于隐藏分支，无偿ARP用于引导过程。

3、《TCP/IP详解 卷1：协议（英文版）》的笔记-第2页

1.链路层的作用：支持网络层的IP模块；发送接收ARP应答；发送接收RARP应答。
-
2.IEEE802 & 以太网
802.3针对CSMA/CD，802.4针对令牌总线，802.5针对令牌环网，802.2针对上述的共同特性。

TCP/IP需求RFC规定，internet主机都与10Mb/s的以太网线连接：必须发送和接受RFC894封装，可以接受RFC894mixedwithRFC1042封装，可能发送RFC1042封装。

注意：RFC894是以太网，RFC1042是IEEE802
--
IEEE802特有：
DSAP——目的服务访问点0XAA
SSAP——源服务访问点0Xaa
ctrl——3
org code——0
-
IEEE802数据帧最小长度——38
以太网数据帧最小长度——46
不足填充PAD
==========
3.尾部封装RFC893
==========
4.SLIP——串行线路IP(RFC1055)
令c0为END，db为ESC，SLIP以0xc0开头和结尾，
中间如果出现0xc0，则以0xdb&0xdc取代；
如果出现0xdb，则以0xdb&0xdd取代。缺陷：
必须知道对方IP；
数据帧没有类型字段，使用SLIP时不能混杂其他协议；
没有数据检验和，CRC由上层协议解决。
==========
5.CSLIP(RFC1144)
针对传输IP/TCP首部进行压缩，不发生改变的首部被抛弃，用小的数字取代发生改变的字段。
现在大多数SLIP都支持CSLIP。
==========
6.PPP——点对点协议()修正了SLIP的缺陷，有点像ISO的HDLC标准（高层数据链路控制），其包括三个部分：
（1）串行封装方法（支持8位数据和无奇偶验的异步模式，支持面向bit的同步模式）(RFC1548)
（2）建立配置测试LCP（链路控制协议）(RFC1548)
（3）支持不同的NCP（网络控制协议——当前有IP/OSI/DECnet/AppleTalk）(RFC1332)
-

以0x7e开始和结尾，地址为0xff，控制0x03，协议类型（IP数据报/链路控制/网络控制）；
当0x7e出现在信息字段中时，通过bit stuffing硬件技术转义为0x7d；
当0x7e出现在数据帧中时，需要将紧接着的字符第6个bit取补码：（1）遇到字符0x7e则传0x7d&0x5e，（2）遇到转义0x7d则传0x7d&0x5d，（3）——默认情况，如果字符值小于0x20，都需要进行转义。例如，遇到0x01，需传送0x7d&0x21，第6bit取补码后变为1，而前面两种会将其变为0。-
PPP>SLIP的理由：
1.PPP支持单根串行的多协议传输（不止IP协议）
2.每帧都有循环冗余检验
3.通信双方可以IP地址动态协商（使用IP网络控制协议）
4.提供类似CSLIP报文首部压缩
5.链路控制协议可以对多个数据链路选项进行设置。
==========
7.环回接口（基于链路层实现）
localhost——127.0.0.1
-（1）传给环回地址的任何数据均作为IP输入；
（2）传给广播地址或多播地址的数据报，复制一份传给环回接口，然后送到以太网（因为广播传送和多播传送的定义包含主机本身）；
（3）任何传给该主机IP地址的数据均传送到环回接口。
==========
8.最大传输单元MTU（指内含数据段）
为保证交互提供足够快的相应时间，将超过MTU的IP数据报分片。==========
9.路径MTU（MTU：最大传输单元）通过多个网络通信俩主机的最小MTU，叫做路径MTU。
俩主机之间的路径MTU，随所选路由改变，且选路不一定对称。
==========
10.串行线路（在IP层检测以太网帧）吞吐量计算

交互的响应时间最好<=100～200ms（更小的MTU值有利于交互体验，而大块数据的线路利用率需要更大的MTU值。）

平均等待时间= 传输MTU所需时间的一半（只适合SLIP/PPP在交互通信和大块数据传输时）
在只使用交互通信时，经过压缩的数据往返时间更小。
==========
小结：
1.对比以太网&IEEE802.2/802.3的封装格式
2.对比SLIP和PPP的封装格式（均常用于低速链路，提供压缩公共字段提升交互通信）
3.通过典型的串行线路MTU，对SLIP/CSLIP链路的传输时延进行计算。

4、《TCP/IP详解 卷1：协议（英文版）》的笔记-第3页

1.IP网际协议为ICMP/IGMP和传输层(TCP/UDP)提供，不可靠、无连接的数据传输。Big Endian字节序传输（网络字节序）——按照一个字节一个字节地传输
-
IP协议版本：4——IPv4
首部长度：首部长度
服务类型TOS：最小时延、最大吞吐量、最高可靠性、最小费用总长度字段：整个IP数据报的长度
-
标识字段：唯一地表示主机发送的报文。
-

TTL：最多路有数，数据报的生存时间。
首部检验和：根据IP首部计算的检验和码
-
32位源地址
-
32位目的地址
-
任选项：==========
2.IP路由选择
host不负责转发，router可以转发，host和router的路由算法有某种程度上的相似，host带有router时一般不负责转发。
-
IP层路由表信息：目的IP、下一跳routerIP/直连网络IP、标志、指定数据报的传输接口。
-
工作机制：接收network接口或本地生成的上层数据->搜索IP路由表
->如果搜索到为本机，则送至IP首部协议指定的，协议模块中处理。
->如果未搜索到，（1）带router功能则进行转发，（2）不带router功能则丢弃数据报。
-
router逐跳机制：
->寻找IP、主机号匹配的主机（是）->转发/处理
->寻找网络地址匹配的条目 （是）->转发
->寻找默认条目（是）->转发
（否）->传送失败（主机不可达）
-
注意：
逐跳过程的数据帧头部地址不断在变（如果是SLIP或PPP则没有MAC头部地址，直接使用IP地址）；
下一跳的IP地址，经过ARP协议转换为MAC地址；
每次寻找命中的时候，查看数据报中的IP是否与本机匹配，如果不匹配则查找路由表。
==========
3.子网寻址
4.子网掩码5.特殊情况的IP地址（空子网号代表未划分）注意：头两个网络号为0只会出现于，类似BOOTP协议中，初始化本机IP地址时的源地址。
==========
6.子网实例
在路由协议支持变长子网的情况下（RIP不支持），针对不同协议的两个子网，可以用掩码对网络进行再划分。sun主机的掩码和子网划分最后一行是sun的子网广播地址（即sun子网，主机号段取值-1）
==========
7.网络层命令——ifconfig==========
8.netstat

5、《TCP/IP详解 卷1：协议（英文版）》的笔记-第1页

==========
1.链路层，网络层，运输层，应用层
-
应用层——网关，连接不同协议簇，为特定应用程序服务（EMAIL/文件传输）
运输层TCP/UDP——端到端协议，路由器，提供可靠，使用端口号区分应用程序
+tcp segment/+udp datagram->packet
网络层IP——逐跳（点对点）协议，路由器，连接不同结构、相同协议簇，不可靠

+ip datagram->ip fragment=packet
链路层ARP/RARP——网桥，网络设备驱动，系统内核负责，+frame=
multihomed system都可以是路由器，或者主机
==========
2.网络层
IP：ICMP——实现与其他主机或路由器交换错误报文和其他重要信息。
IGMP——internet组管理协议，将UDP数据多播到多个主机
-
三类IP：单播地址（目的为单机）、广播地址（目的端为给定网络上所有主机）、多播地址（目的端为同一组内的所有主机）。
==========
3.分级寻址系统
DNS域名系统地址（IP与主机名映射信息）
IP网络层地址
ARP链路物理地址（MAC与IP映射信息）
-
==========
4.封装链路层：网络层IP/ARP/RARP要向链路层传送数据，因此在链路层帧的首部加入网络层标识，16bit，用于指明使用的网络层协议。
-
网络层：运输层ICMP/IGMP/TCP/UDP都要向IP层传送数据，因此在IP首部加入协议标识，用于区别此IPdatagram在网络层的类型：1.ICMP，2.IGMP，6.TCP，17.UDP
注意：ICMP和IGMP是IP的附属协议，属于网络层
-
应用层：应用层要向传输层传送数据，需要在传输层加入应用程序标识，用于区别应用层的不应用程序：TCP/UDP都用一个16bit的端口号来标识，将源端口号、目的端口号存入传输层首部。
==========
5.分用Demultiplexing（解除封装）注意：ICMP和IGMP是网络层IP的附属协议，放在运输层是因为ICMP/IGMP都封装在IPdatagram中。
ARP和RARP都是链路层协议，放在IP层是因为ARP/RARP都封装在链路层frame中。

==========
6.client-server模型
server的分类：
重复型——等待请求->处理客户请求->响应发出请求的客户，等待请求...
并发型(多任务操作系统)——等待请求->启动新服务器来处理请求->等待请求...
TCP服务器是并发的，UDP服务器是重复的。

==========
6.端口号（传输层区分不同应用程序）
服务器TCP/IP知名端口号：1～1023（256~1023：internet扩展服务/unix特定服务）
服务器临时端口号：1024～5000
服务器不常用的internet服务：5001～
-
客户端程序对所使用的端口号不关心，只保证在调用时，是本机唯一即可，临时设定。
==========
7.标准化
（1）ISOC（internet协会）
（2）IAB（internet体系结构委员会）标准最后审核，隶属于ISOC

（3）IETF/IESG（internet工程专门小组/指导小组）开发标准，隶属于IAB
（4）IRIF（internet研究小组）长远研究，隶属于IAB
RFC标准文档：
赋值RFC 1340 [Reynolds 和Postel 1992]、
正式协议标准RFC 1600[Postel 1994]、
主机需求RFC、1122和1123[Braden 1989a, 1989b]
路由需求RFC、1009[Almquist 1993]
==========
8.标准简单服务（应用层）
服务端：（使用的端口号基本都是奇数，因为早期TCP是单工通道，后来全双工）客户端：一般使用telnet
==========
9.互联网
internet——共同协议簇连接的多个网络连接，广义
Internet——全世界范围通过TCP/IP通信的主机集合，专指
==========
10.本书的测试网络==========

==========

==========

6、《TCP/IP详解 卷1：协议（英文版）》的笔记-第6页

1.简介
ICMP属于IP层协议，为IP、更高层协议（TCP/UDP）、用户进程（作为差错报文）提供服务。-
（1）类型

《TCP/IP详解 卷1：协议（英文版）》

版权说明