第3章 TCP/IP概述

作者：Rima S.Regas

本章内容包括：

- 使用TCP/IP的优点
- TCP/IP的层和协议
- 远程登录
- 文件传输协议(FTP)
- 普通文件传输协议(TFTP)
- 简单邮件传输协议(SMTP)
- 网络文件系统(NFS)
- 简单网络管理协议(SNMP)
- TCP/IP与系统的结合
- Intranet概念

TCP/IP无处不在。它不是某时某地存在的物理事物，它是一组协议，这组协议使任何具有计算机、调制解调器和 Internet服务提供者的用户能访问和共享 Internet上的信息。事实上，使用AOL即时信息服务和ICQ的用户每天可产生超过 7亿5千万条的信息。这是一个非常大的流量，其中绝大部分在Internet上传输。

是TCP/IP协议保证这些数以百万计的信息传输，而几乎没有疏漏，并且没有任何停止的迹象。TCP/IP是一个稳定的、构造优良的、富有竞争性的协议。本章将仔细地考查其中的奥妙。

TCP和IP是两个独立且紧密结合的协议，负责管理和引导数据报文在 Internet上的传输。二者使用专门的报文头定义每个报文的内容。 TCP负责和远程主机的连接。而 IP负责寻址，使报文被送到其该去的地方。下一节将讨论 TCP/IP的优点。

3.1 TCP/IP的优点

TCP/IP使跨平台，或称为异构的网络互联成为可能。举例来说，一个 Windows NT网络可以包含UNIX和Macintosh工作站，甚至可以包含 UNIX网络或Macintosh组成的网络， TCP/IP也有如下的特性：

- 好的破坏恢复机制。
- 能够在不中断现有服务的情况下加入网络。
- 高效的错误率处理。
- 平台无关性。
- 低数据开销。

因为TCP/IP最初的设计目的与国防部有关，所以，上面列出的特性实际上是 TCP/IP的设计要求。“ 好的破坏恢复机制 ”基于下面的想法：当网络被侵入或被攻击而遭到破坏时，它的剩余部分仍能完全工作。在不中止已存在于某一处服务的前提下加入整个网络的能力基于同

样的道理。处理高错误率的能力基于如下考虑：如果报文信息使用一个路由丢失时，应该有一种机制使其能够通过另一路由到达目的地。平台无关性意味着网络和客户端可以是Windows 、UNIX、Macintosh或任何其他的平台或上面所述平台的组合。 TCP/IP如此高效依赖于它的低开销。性能是任何网络的关键。在速度和简单性方面没有其他协议可以与 TCP/IP媲美。

3.2 TCP/IP的层和协议

TCP和IP共同管理网络上流进和流出的数据流。 IP不停地把报文放到以太网上，而TCP负责确信报文到达。TCP负责下面的工作：

- 握手过程
- 报文管理
- 流量控制
- 错误检测和处理

3.2.1 体系结构

TCP/IP是处理上述所有操作并和远程主机通信的一个环境。 TCP/IP由四层组成，这与OSI由七层组成不相同。这四层包括：

- 应用层(Application)
- 传输层(Transport)
- 网络层(Network)
- 链路层(Link)

TCP/IP和OSI之间在层格式方面的主要区别是：传输层不保证任何时刻的传输。 TCP/IP为用户提供用户数据报协议 (UDP)，这是一个更简单的协议，在 UDP中，TCP/IP协议栈中的所有层执行特定的工作或运行应用。

1. 应用层

应用层包括SMTP、FTP、NFS、NIS、LPD、Telnet和Remote Login。对于大多数Internet用户来说这些都是很熟悉的。

2. 传输层

传输层包括UDP和TCP。UDP几乎不进行检查，而TCP提供传输保证。

3. 网络层

网络层由以下协议组成： ICMP、IP、IGMP、RIP、OSPF和用于路由的EGP，用户不必操心这些，因为它们是相当底层的东西。

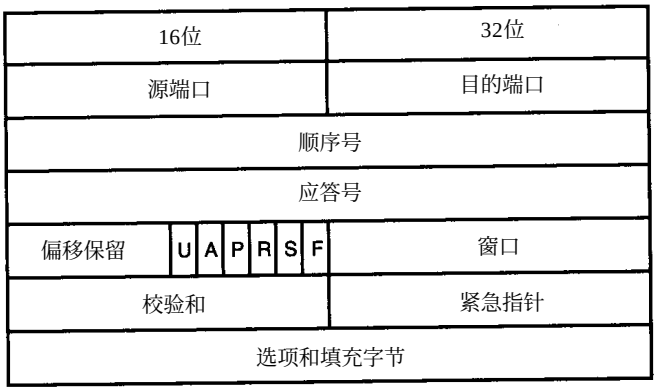
4. 链路层

链路层包括ARP和RARP，负责报文传输。

3.2.2 传输控制协议

传输控制协议(TCP)提供了可靠的报文流传输和对上层应用的连接服务， TCP使用顺序的应答，能够按需重传报文。

TCP头如下所示：



1. 源端口

用于指示源端口的数值。

2. 目的端口

用于指示目的端口的数值。

3. 序号

数据段中第一个数据的序号。

4. 应答号

当ACK位被置之后，这个域包括下一个发送者想要接收到的序号，这个值总被发送。

5. 偏移

这个数指示数据的开始位置。

6. 保留域

保留域不被使用，但是它必须置0。

7. 控制位

控制位是以下各位：

U(URG) 紧急指针域有效

A(ACK) 应答域有效

P(PSH) push操作

R(RST) 连接复位

S(SYN) 同步序号

F(FIN) 发送方已达字节末尾

8. 窗口

这个域指示发送方想要接收的数据字节数，其开始于报文中的 ACK域。

9. 校验和

校验和是报文头和内容按1的补码和计算得到的16位数。假如报文头和内容的字节数为奇数，则最后应补足一个全0字节，形成校验和，注意补足的字节不被送上网络发送。

10. 紧急指针

这个域指出紧急数据相对于跟在URG之后数据的正偏移。

11. 选项

选项可能在头的后面被发送，但是必须被完全实现并且是 8位长度的倍数。两种情况是：

• 情况1 一个单一的选项类型字节。

• 情况2　一个选项类型字节、一个选项长度字节和实际的选项数据。

选项长度包括选项类型和选项长度自身，当然也包括选项数据，这些数据组成选项并被发送。下面显示了三种类型的格式。所有的选项包含在校验和 (checksum)里。一个选项可以开始于任何字节边界，只要对剩余的“死”空间进行填充来满足定义的包长度就可以。

类　型	长　度	描　述
0	-	选项结束
1	-	无操作
2	4	最大段尺寸

0类型选项指示出选项列表的结束，其指示出所有选项的结束而非任一单独选项的结束。只有在选项列表与头结束不一致时才使用这一选项。

1类型选项用于选项的字对齐，这不是一个重要的选项。

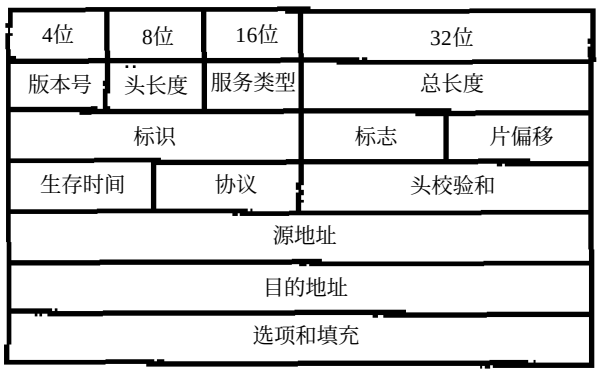
2类型指示其接收段的最大尺寸。这个选项只出现于起始请求段和 SYN位被置了的一段。如果此选项不用，段无尺寸限制。

注意　选项列表可以比数据偏移域指定的短，因为在结束选项之上的头内容必须填充0。

3.2.3 IP协议

IP协议用于管理客户端和服务器端之间的报文传送。

IP头结构如下：



每一个域包含IP报文所携带的信息，下面的描述有助于理解。

1. 版本号

指出此报文所使用的IP协议的版本号，IP版本4(IPv4)是当前广泛使用的版本。

2. 头长度

此域指出整个报文头的长度，接收端通过此域可以知道报文头在何处结束及读数据的开始处。

3. 服务类型

大多数情况下不使用此域，这个域用数值表示出报文的重要程度，此数大的报文优先处理。

4. 总长度

这个域指出报文的以字节为单位的总长度。报文的总长度不能超过 65 535个字节，否则接收方认为报文遭到破坏。

5. 标识

假如多于一个报文(几乎不可避免)，这个域用于标识出报文位置，分段的报文保持最初的ID号。

6. 标志

第一个标志如果被置，将被忽略；假如 DF(Do Not Fragment，不分段)标志设置，则报文不能被分段。假如 MF(More Fragment，段未完)标志被置(1)，说明有报文段将要到达，最后一个段的标志置0。

7. 偏移

假如标志域返回1，此域包括本片数据在初始数据报文区中的偏移量。

8. 生存时间

通常设为15～30秒。表明报文允许继续传输的时间。假如一个报文在传输过程中被丢弃或丢失，则指示报文会发回发送方，指示其报文丢失。发送机器于是重传报文。

9. 协议

这个域指出处理此报文的上层协议号。

10. 校验和

这个域作为头数据有效性的校验。

11. 源地址

这个域指出发送机器的地址。

12. 目的地址

这个域指出目的机器的地址。

13. 选项和填充

选项域是可选的，如果使用，此域包括一些编码，此编码指出安全，严格源路由、松源路由，路由记录及时戳(timestamping)等选项的使用。如果不使用选项，此域称为填充的并且含有1。下面列出了可获得的选项：

类	号	选　项
0	0	选项表结束
0	2	军事安全
0	3	松路由记录
0	7	记录路由(这个选项加入域)
0	9	严格源路由
2	4	时戳

TCP/IP通过翻译层“栈”提供其服务，这个栈称为 TCP/IP。因为TCP和IP是独立的协议，二者需要通用环境来实现其服务。正如本章前面所述， TCP/IP有四层，和OSI的七层相对，其核心是：

- 应用(Application)
- 传输(Transport)
- 网络(Network)
- 链路(Link)

3.2.4 应用层

应用层包括一些服务，这些服务在OSI中由独立的三层实现。这些服务是和端用户相关的认证、数据处理以及压缩。包括电子邮件、浏览器、 Telnet客户以及其他的Internet应用。

3.2.5 传输层

与OSI中传输层不一样， TCP不保证报文的准确传输。其基本作用是管理源和目的之间的报文传输。OSI中传输层保证报文是经过校验的，并且假如报文有错，报文会被要求重传。

3.2.6 网络层

网络层处理报文的路由管理。这一层根据接收报文的信息决定报文的去向。

3.2.7 链路层

链路层管理网络的连接并提供网络上的报文输入 /输出，但是这一层不工作于应用级。

现在读者已对TCP/IP及其功能有了清晰的认识，下一节将讨论 TCP/IP实际提供给用户的巨大好处。

3.3 远程登录(Telnet)

Telnet是TELecommunications NETwork的缩写，其名字具有双重含义，既指应用也是指协议自身。Telnet给用户提供了一种通过其连网的终端登录远程服务器的方式。 Telnet通过端口号23工作。

Telnet要求有一个telnet服务器，此服务器驻留在主机上，等待着远端机器的授权登录。Windows 9x/NT/2000、BeOS、 Linux和其他基于X86平台的操作系统要求安装配置一个 Telnet服务器，接收到达的会晤请求，基于 MacOS的系统也要有一个 Telnet服务器。基于UNIX的计算机是惟一的系统，要求一个 telnetd的应用(“ d ”代表daemon，一个服务器应用程序)。在另一端是一个Telnet应用，作为接口存在，可以是基于文本的也可以是基于图形的。

注意 Windows 2000有一个内嵌的CLI Telnet应用，假如用户点击一个Telnet链接或从终端敲入Telnet，它就会出现。因此Windows 2000不需要第三方的Telnet服务器。

3.4 文件传输协议(FTP)

Telnet具有和远端主机相连接的能力，而 FTP则更具有被动性，它允许用户把文件在远端服务器和本地主机之间移动。这对于想从一个地方把大的文件移动到另一个地方，而又不通过以前建立的“ 热 ”连接的 Web管理员或任何人而言，是非常理想的。 FTP是典型的在所谓被动模式下工作的协议，这种模式把目录树结构下载于客户端然后连接就断开了，但是客户程序周期性地和服务器保持联系以使端口始终是打开的。

注意 基于特定的Web管理员任务，需要配置不同的FTP服务器。有的允许匿名用户不加限制的访问所有内容，而有的只允许以前被认证的用户访问，还有一些允许匿名用户仅在很短的时间周期内访问。假如用户处于不活跃状态，服务器会自动断开连接，

强迫用户在需要时重新连接。

在基于UNIX的系统上，这些程序通常称为 ftpd(“ d ”含义是daemon)和ftp(客户端应用)，FTP的缺省端口是20(用于数据传输)和21(用于命令传输)。在TCP/IP中FTP是独一无二的，因为命令和数据能够同时传输，而数据传输是实时的，在其他协议中不具有这个特性。

所有的操作系统具有FTP客户端和服务器，虽然形式可能不同。所有基于 MacOS的FTP应用是面向图形的，大多数基于窗口的 FTP应用亦是如此。使用基于图形的 FTP客户端的好处是所有的命令，通常通过手动输入，现在被客户程序管理，减小了错误的可能性，使得会话过程更快更容易。另一方面，由于 FTP服务器在初始建立连接之后不需要太多的管理，所以服务器不需要GUI(图形用户接口)。

3.5 普通文件传输协议(TFTP)

TFTP如其名，虽然和FTP有联系但却只具有FTP的非常小的一部分功能。 TFTP使用UDP，就像TFTP与FTP的关系，UDP与TCP相对，TFTP不具有报文监控能力和有效的错误处理能力。但是这些限制同样减小了过程开销。 TFTP不是可靠的协议，仅仅是连接。作为嵌入式的保护机制，TFTP仅仅允许移动可公共访问的文件。这并不意味着 TFTP可被忽视，不具有潜在危险性。

使用TFTP时，安全并不是主要关心的问题， TFTP一般用于嵌入式应用。在这种场合下，空间是首先需要关心的问题，安全问题可用其他方式解决。 TFTP亦用于机器需从远程服务器引导的网络计算机环境。例如，在轿车工厂中，当轿车从生产线上下来从一个责任点移向另一个责任点时，需要在每一个停靠点给特定的轿车提供专门的数据并且需要收集新的数据沿着生产线传到以后各责任点。

3.6 简单邮件传输协议(SMTP)

SMTP是通过网络，主要是Internet传输电子邮件的标准。所有的操作系统具有使用 SMTP收发电子邮件的客户端程序，绝大多数 Internet服务提供者使用 SMTP作为其输出邮件服务的协议。所有的操作系统具有 SMTP服务器，这其中包括，但不仅限于下面所述： Windows 9x/NT/2K、MacOS、UNIX及其变种、 Linux、BeOS，甚至AmigaOS。

SMTP被设计成在各种网络环境下进行电子邮件信息的传输，实际上， SMTP真正关心的不是邮件如何被传送，而只对邮件顺利到达目的地关心。 SMTP能够辗转于进程间通信环境(Interprocess Communication Environment，IPCE)之中，因为IPCE层能够不考虑传输协议和媒体类型进行通信。例如，是邮件信息能够从具有各种传输层协议和媒体类型的 Internet传输至正好相反的Intranet上。

SMTP具有健壮的邮件处理特性，这种特性允许邮件依据一定标准自动路由。 SMTP具有当邮件地址不存在时立即通知用户的能力，并且具有把在一定时间内不可传输的邮件返回发送方的特点(邮件驻留时间由服务器的系统管理员设置)。SMTP使用端口号25。

3.7 网络文件系统(NFS)

NFS是SUN公司为了解决网络环境下各种操作系统之间协调问题而开发的。 NFS仅支持文件共享，并作为许多基于 UNIX的操作系统完整的一部分， NFS也能很好地被许多其他的操作

系统所支持。

NFS不是万能的。和其他协议相比， NFS相当慢。NFS也不能保证文件传输，因为它根本不进行正确性检查。文件遭到破坏是很容易出现的，并且，当同时有大量用户访问系统时，NFS容易当机。最后， NFS没有方法防止各种用户同时写同一个文件，因为 NFS允许用户在不知道其他文件操作的情况下随意破坏文件。

NFS文件访问是无缝透明的。一旦 NFS被安装(mount)，就成为端用户系统的一部分。当然除了输出过程，不需要额外的步骤。输出需要服务器和客户端按 NFS的配置达到同步，这个系统既不简单，对管理员而言也不友好。

3.8 简单网络管理协议(SNMP)

SNMP提供通过简单的协议，如 UDP、IPX或者IP对路由器一级进行监控和管理的能力。简单性是在述及SNMP时需要重点记住的，如果不简单， SNMP就什么也不是。首先，它仅仅支持三个命令 —— GET、GENEXT和SET。前两个支持对报告信息的访问，第三个允许管理员对路由器实现远程控制。

网络设备通过管理信息库(Management Information Base，MIB)提供相关信息。信息数据向SNMP管理者定义了网络设备，传送给 SNMP管理站，管理站会识别每一个设备并存储其信息。所有依附于SNMP的设备都被管理站管理。每一个设备运行一个 SNMP代理，这个代理提供了客户端的操作。当管理站请求一个 GET命令，想得到端口状态时，代理返回该信息。

SNMP并不意味着管理所有的网络设备至细节的高度， SNMP是简单的、每天都进行的管理。这样允许管理员把注意力集中在设备上而不需要装载大量的信息接口。

3.9 TCP/IP和系统结合

读者已经看到TCP/IP能提供什么样的服务， TCP/IP是灵活的并且是被业界接受的协议。Internet使用TCP/IP，因此没有明显的带宽和网络大小的限制。读者已经了解了 TCP/IP的各个方面及其优异的原因。

在你没有主意的情况下考虑使用 TCP/IP的惟一原因是，用户网络不是基于 UNIX的网络环境，因为这种环境已经使用 TCP/IP好多年了。用户很可能使用的是 IPX/SPX的NetWare网络。如果是这样，用户不想升级至完全支持 TCP/IP的NetWare 5.0的惟一原因是：费用问题。

如果用户不想升级 AppleShare，也是出于同样的原因。这种情况不适合 AppleShare IP，因为那个服务器组件已经实现了 TCP/IP，但是价格也是一个因素。 TCP/IP提供了很广泛的功能，服务器、各种服务、客户端，这些功能需要很少的投资，甚至不需投资。

用户可以花大量的钱建一个 TCP/IP的内部网，但是也可以花很少的钱达到同样的目的。首先考虑使用一个服务器操作系统如 Linux，它是免费的，或者花很少的钱买一个发布版。Red Hat、Debian、Caldera是最常见的版本。Linux仍是免费的，但是如果用户想购买 Red Hat、Debian或者Caldera，也会买到它们的服务和支持、专门的安装软件及其他一些通常在 Linux中没有的东西。

注意 如果不想花60美元购买Red Hat Linux也可以从它们的站点上下载获得，但是通过调制解调器下载它需要花费很长的时间，因为Red Hat要占用160M字节空间，而买一个发布版要快得多。

用户也可以使用自己现在的操作系统，因为这些操系统有大量的服务器软件可以获得，这些软件可以运行在MacOS、Windows 9x/NT/2K或其他操作系统上。有些操作系统是免费的，而另一些操作系统的价格在 30美元到2500美元之间，这要依赖于软件自身和用户的许可证。用户也可以重新布线，但是现有的介质类型应足够好，除非用户打算从一个简单的文本应用转到提供24小时服务的3D专业动画应用。

3.10 内部网概述

有三个因素促使TCP/IP成为当今Intranet的主选协议：价格、速度、可扩展性。 TCP/IP实现非常廉价，它能和系统原有的协议一同工作 (AppteTalk、IPX等)，TCP/IP能够快速有效地工作。通过方便的报文交换，能够为 TCP/IP加入一些新的想法。

Internet也在考虑之中，因为用户的公司或网络现在能够访问巨大的资源。电子邮件是今天Internet上使用最广泛的应用，它的使用频率甚至超过了页面浏览。每天有几十亿的信息需要路由。还有成百万的Internet终端容许人们访问放在Internet上的服务。

有许多接入Internet的方式，但主要的方式是拨号方式。任何具有模拟调制解调器的用户可以通过拨打ISP的调制解调器实现与Internet的连接，一旦连接成功，剩下的问题就是使用正确的资源。主要的协议是点到点协议 (Point-to-Point Protocol，PPP)。一个更老的协议是串行线路接口协议 (SLIP)，SLIP允许用户通过串行线路连接到 Internet，但是与PPP不一样，使用SLIP的用户并不是以一台主机的身份出现。

注意 主机能够提供服务，串行客户却不能做到这一点。

3.11 小结

正如读者在本章中所看到的，报文从一个地方传送到另一个地方涉及许多复杂的技术。这就是TCP和IP如此紧密连接在一起的原因。二者在 Internet中担任着重要的角色。读者了解了TCP/IP的分层工作，每一层有特定的功能。假如这些环节中的任何一环遭到破坏，整个系统就会崩溃。幸运的是很少会发生这种情况。

可靠性是TCP/IP在所有操作系统上以这种形式或那种形式存在的原因。有一个称为 QNX的操作系统，它能够存储在一张 1.44M的软盘中，但它却包含了一个 GUI、一个TCP/IP栈、一个浏览器、一个 Web服务器、一个拨号程序和其他一些实用工具。使用 QNX，用户能够从软盘引导连接Internet。毫无疑问，这使得连接 Internet变得非常简单。

TCP/IP是可扩展和可移植的。时刻要记着考虑自身网络所使用的所有可用协议，并且要确信向TCP/IP的转移不会导致对用户访问造成无法补偿的损害。除此之外的其他问题都算不了什么。