TCP/IP 技术浅谈

杨红敏
（中国铁通吉林分公司，吉林 长春 130012）

摘 要：TCP/IP 协议是 Internet 最基本的协议，由底层的 IP 协议和 TCP 协议组成的。分不同层次进行开发，每一层分别负责不同的通信功能。其应用的主要目的是为了在 Internet 上的应用，文章对其在应用中存在的安全性问题等做了简要介绍。
关键词：TCP/IP；WWW 服务；电子邮件
中图分类号：TP316.8 文献标识码：A 文章编号：1000－8136（2011）27－0016－03

1 技术原理概述

1.1 参考模型概述

TCP/IP（Transmission Control Protocol/Internet Protocol 的简写，中文译名为传输控制协议/互联网络协议）协议是 Internet 最基本的协议，简单地说，就是由底层的 IP 协议和 TCP 协议组成的。TCP/IP 协议的开发工作始于 20 世纪 70 年代，是用于互联网的第一套协议。

开放式系统互联模型（OSI）是 1984 年由国际标准化组织（ISO）提出的一个参考模型。作为一个概念性框架，它是不同制造商的设备和应用软件在网络中进行通信的标准。现在此模型已成为计算机间和网络间进行通信的主要结构模型。

1.2 TCP/IP 协议族

网络协议通常分不同层次进行开发，每一层分别负责不同的通信功能。TCP/IP 协议族是一组不同层次上的多个协议的组合。TCP/IP 通常被认为是一个四层协议系统，见图 1。

应用层
传输层
网络层
链路层

图 1 TCP/IP 协议族的 4 个分层

每一层负责不同的功能：

1.2.1 链路层

有时也称作数据链路层或网络接口层，通常包括操作系统中的设备驱动程序和计算机中对应的网络接口卡。它们一起处理与电缆（或其他任何传输媒介）的物理接口细节。

1.2.2 网络层

有时也称作互联网层，处理分组在网络中的活动，例如分组的选路。在 TCP/IP 协议族中，网络层协议包括 IP 协议（网际协议）、ICMP 协议（Internet 互联网控制报文协议）以及 IGMP 协议（Internet 组管理协议）。

1.2.3 传输层

主要为两台主机上的应用程序提供端到端的通信。在 TCP/IP 协议族中，有两个互不相同的传输协议：TCP（传输控制协议）和 UDP（用户数据报协议）。TCP 为两台主机提供高可靠性的数据通信。它所做的工作包括把应用程序交给它的数据分成合适的小块交给下面的网络层，确认接收到的分组，设置发送最后确认分组的超时时钟等。由于传输层提供了高可靠性的端到端的通信，因此应用层可以忽略这些细节。而另一方面，UDP 则为应用层提供一种非常简单的服务。它只是把称作数据报的分组从一台主机发送到另一台主机，但并不保证该数据报能到达另一端。任何必需的可靠性必须由应用层来提供。

1.2.4 应用层

负责处理特定的应用程序细节。几乎各种不同的 TCP/IP 实现都会提供下面这些通用的应用程序：Telnet 远程登录、FTP 文件传输协议、SMTP 简单邮件传送协议、SNMP 简单网络管理协议。

1.3 IP 协议概述

IP 是 TCP/IP 协议族中最为核心的协议。所有的 TCP、UDP、ICMP 及 IGMP 数据都以 IP 数据包格式传输。IP 提供了不可靠和无连接的数据包传送。

不可靠是指它不能保证 IP 数据报能成功的到达目的地。IP 仅提供最好的传输服务。如果发生某种错误时，如某个路由器暂时用完了缓冲区，IP 有一个简单的错误处理算法：丢弃该数据报，然后发送 ICMP 消息报给信源端。任何要求的可靠性必须由上层来提供，如：TCP。

无连接是指 IP 并不维护任何关于后续数据报的状态信息。每个数据报的处理是相互独立的。这也说明，IP 数据报可以不按发送顺序接收。如果信源向相同的信宿发送两个连续的数据报（先是 A，然后是 B），每个数据报都是独立地进行路由选择，可能选择不同的路线，因此 B 可能在 A 到达之前先到达。

1.3.1 传输控制协议（TCP）

传输控制协议（TCP）：为应用程序提供可靠的面向连接的通信服务，适用于要求得到响应的应用程序。目前，许多应用程序都使用 TCP。

TCP 协议通过以下过程来保证端到端数据通信的可靠性：①TCP 实体把应用程序划分为合适的数据块，加上 TCP 报文头，生成数据段。②当 TCP 实体发出数据段后，立即启动计时器，如果源设备在计时器清零后仍然没有收到目的设备的确认报文，重发数据段。③当对端 TCP 实体收到数据，发回一个确认。④TCP 包含一个端到端的校验和字段，检测数据传输过程的任何变化。如果目的设备收到的数据校验和计算结果有误，TCP 将丢弃数据段，源设备在前面所述的计时器清零后重发数据段。⑤由于 TCP 数据承载在 IP 数据包内，而 IP 提供了无连接的、不可靠的服务，数据包有可能会失序。TCP 提供了重新排序机制，目的设备将收到的数据重新排序，交给应用程序。⑥TCP 提供流量控制。TCP 连接的每一端都有缓冲窗口。目的设备只允许源设备发送自己可以接收的数据，防止缓冲区溢出。⑦TCP 支持全双工数据传输。

1.3.2 用户数据报协议（UDP）

UDP 是一个简单的面向数据报的传输层协议：进程的每个输出操作都正好产生一个 UDP 数据报，并组装成一份待发送的 IP 数据报。

UDP 不提供可靠性：它把应用程序传给 IP 层的数据发送出去，但并不保证它们能到达目的地。

1.3.3 TCP/IP 协议栈常用协议介绍

（1）地址解析协议（ARP）。当一台主机把以太网数据帧发送到位于同一局域网上的另一台主机时，需要将数据包封装为以太网帧之后进行发送。在一个 IP 报文被封装为以太网帧的时候，需要根据 IP 报文的目的 IP 地址确认以太网帧的 MAC 地址，用以完成对以太网帧的封装。这就要求在发送设备上有地址解析，即：IP 地址和 MAC 地址之间的映射。

（2）网际控制消息协议（ICMP）。网际控制消息协议 ICMP 是一个网络层的协议，它提供了错误报告和其他回送给源点的关于 IP 数据包处理情况的消息。ICMP 通常为 IP 层或更高层协议使用，一些 ICMP 报文把差错报文返回给用户进程。ICMP 报文通常被封装在 IP 数据包内传输。

（3）动态主机配置协议（DHCP）。随着网络的发展，网络中的主机数量不断增加，管理主机的 IP 地址和相关参数对管理员来说越来越困难，手工分配 IP 地址难免会带来地址冲突问题。主机经常需要从一个地方移动到另一个地方，人工配置 IP 地址相当麻烦。当 IP 地址资源较紧张时，如果每台主机都占用固定的 IP 地址，地址空间会非常紧张，实际上并不是每台机器都是运行的，造成地址的浪费。动态分配是唯一一种允许自动重用地址的机制。因此，这种方法对于有临时上网用户，而且网络的 IP 地址资源又不是多得没法用的时候特别有用。而手工指定对于管理不希望使用动态 IP 地址的用户十分方便，不会因为手工指定而和 DHCP 冲突或和其他已经分配的地址冲突。通过 DHCP 可以给网络中的主机提供配置信息，包括 IP 地址和相关的其他参数。DHCP 可以完美的解决上述问题。

（4）DHCP Relay。当 DHCP 客户机启动并进行 DHCP 初始化时，它会在本网络广播配置请求报文；若本地网络存在 DHCP 服务器则不需要 DHCP 中继就直接可以进行 DHCP 配置；若本地网络中无 DHCP 服务器，则与本地网络相连的、带 DHCP 中继功能的网络设备在收到该广播报文后将做适当处理将之转发给指定的存在于其他网络上的 DHCP 服务器；服务器根据客户机提供的必要信息，为其作响应的配置，并再次通过 DHCP 中继将该配置信息发送给客户机，完成对客户机的动态配置。事实上，从开始到最终完成配置，需要多个这样的交互过程。

2 TCP/IP 存在的问题

2.1 脆弱的 TCP/IP 服务

我们知道 TCP/IP 协议应用的主要目的是为了在 Internet 上的应用，也就是基于 TCP/IP 协议上的服务，虽然 TCP/IP 协议已是事实上通信协议的标准，但仍不可避免的一个问题就是安全性问题，不仅 TCP/IP 协议本身，现在很多基于 TCP/IP 的应用服务都在不同程度上存在着严重的安全问题，一些新的处于测试阶级的服务有更多的安全缺陷。基于 TCP/IP 协议的服务较多，如 WWW 服务、FTP 服务、电子邮件服务、TFTP 服务、NFS 服务、Finger 服务、NDS 服务、DHCP 服务和 WINS 服务等，详细了解这些服务在安全性方面的不足对于用户设置防火墙保护自己的网络有重要意义，平时我们为单位的防火墙时就需要考虑该提供哪些服务、要禁止哪些服务以及哪些服务该如何配置等，在这里仅对一些常用服务做简单介绍。

2.1.1 WWW 服务

WWW 服务相对于其他服务出现较晚，是基于超文本（HTML）传输协议 HTTP 的，它是互联网、多媒体网页制作技术飞速发展的必然产物。它是由瑞士日内瓦欧洲粒子物理实验室发明的，并在短时间内得到迅猛发展，是人们常用的互联网服务，如我们第一线天所进行的网页浏览。随着 Nctscape 公司推出安全套接字层 SSL，WWW 服务器和浏览器的安全性得到大大的提高，现在人们把这种技术应用于电子商务 E－business。例如人们可以在互联网上进行买卖股票和购物。安全套接字层 SSL 使 WWW 服务的安全性得到了提高，但它主要解决的是数据包被窃听和劫持的问题，除此之外 WWW 服务还有其他问题，如 WWW 服务所使用的 CGI 程序、服务器端附件（Server Side Include，SSI）和 Java Applet 小程序等。

最初 WWW 服务只提供静态的 HTML 页面，这种页面显得很呆板，于是人们引入了 CGI 程序，CGI 程序让人们的主页活起来。CGI 程序可以接收用户的输入信息，一般用户是通过表格把输入信息传给 CGI 程序的，然后 CGI 程序可以根据用户的要求进行一些处理，一般情况下会生成一个 HTML 软件包，利用它可做一些非法的事情，如把/etc/passwd 文件传送给黑客、删除服务器上的文件等。另外，很多人在编 CGI 程序时，可能对 CHI 软件包中的安全漏洞并不了解，多数情况下不会重新编写程序的所有部分，只是对其加以适当的修改，这样很多 CGI 程序就不可避免的具有相同的安全漏洞，所以用户若要编写一个安全的 CGI 程序，就应先去了解这些软件包中的安全漏洞。另一个 CGI 程序很多是用 Perl 来编写的，Perl 本身的功能强大，但它同样也很不安全，其中有很多 UNIX 的特殊字符可用来执行 UNIX 的系统命令，一般入侵者就是利用这些特殊字符实施攻击的，这也是造成 CGI 程序不安全的先天性，从某种意义上来讲也是 TCP/IP 协议先天安全性不足的重要因素之一。

2.1.2 电子邮件服务

电子邮件服务给人们提供了一种便宜、方便和快捷的服务，E－mail 地址也开始写在现代都市人的名片上了，但是电子邮件程序本身就存在许多安全性问题。如在 UNIX 环境下的电子邮件 Sendmail，它是一个复杂且功能强大的应用软件，正因如此它的安全漏洞更多。程序越大、越复杂则安全漏洞可能越多，这似乎已是一个不争的事实，以 Windows 系列为例，版本在不断更新，新功能在不断添加，老的 BUG 据说是一个个被 KILL，但新的问题总是层出不穷。如 Win2K 的专业版中竟然在输入法出现了重大安全漏洞，这是以前任何版本 Windows 所未曾出现的！

Sendmail 在 UNIX 环境下以 root 运行，所以如果该程序被黑客利用，用户主机的损失将会是巨大的。互联网蠕虫病毒曾经震惊世界，它使大批的 UNIX 服务于瘫痪之中，这种病毒就是利用 Sendmail 安全缺陷来进攻的。如果要使这些功能以更安全的方式实现，需要对 Sendmail 进行重新设计和重新实现，但人们又会担心新的版本会有更多的人们难以预料的安全漏出现，于是 Sendmail 的开发者们只好对其修修补补。

除此之外，电子邮件附着的 Word 文件或其他文件中有可能带有病毒，如 Word 的宏病毒等。电子邮件炸弹也是一个头疼的问题，但这个问题时至今日人们仍无法有任何有效措施来预防，更不要说彻底解决了。

2.1.3 FTP 服务和 TFTP 服务

这两个服务都是用于传输文件的，但用的场合不同，安全程度也不同。

TFTP 服务用于局域网，在无盘工作站启动时用于传输系统文件，因为它不带有任何安全用证，所以其安全性极差，常被人用来窃取密码文件。

FTP 服务对于局域网和广域网都可以用来下载任何类型的文件，但它允许匿名登录，其实还有许多类似的服务，如 ssh、scp 等，ssh 是一种带有完善加密和认证机制的协议，如果服务器上运行的 ssh 是最新版本，那么使用它应该是安全的。然而如 http、ftp、smtp 和 nntp 则是一般 WWW 服务器实际提供的服务，这些服务是必须运行的，所以有其他文件传输都应最好使用 scp 工具和 ssh 协议完成。

网上有许多匿名 FTP 服务站点，其上有许多免费软件、图片和游戏，匿名 FTP 是人们常使用的一种。FTP 服务的安全性要好一些，至少它需要用户输入用户名和口令，当然匿名 FTP 服务就像匿名 WWW 服务是不需要口令的，但用户权力会受到严格的限制。匿名 FTP 存在一定的安全隐患，因为有些匿名 FTP 被一些人用作存放盗版软件和黄色图片，这会浪费用户的磁盘

窖、网络带宽等系统资源。

2.1.4 Finger 服务

用于查询用户的信息，包括网上成员的真实姓名、用户名、最近登录时间和地点等，也可用来显示当前登录在机器上所有用户名，这对于入侵者来说是无价之宝。因为它能告诉入侵者在本机上有效的登录名，然后入侵就可以注意其活动。

2.2 问题严重性

仔细分析 PSTN、ATM 及 IP 网络结构，可更充分理解 IP 网易受攻击的安全性问题的原委。

一般安全攻击多半在终端发起，PSTN 的终端本质为傻瓜型，兼之 PSTN 的收费模式，在终端入手发起大规模攻击，成本亦很高，难以操作。PSTN 的用户端与网络端接以 UNI 与 NNI 彼此分离，业务提供及控制权均在运营商手中，没有运营商参与，用户难在终端做新花样，播发病毒及发动攻击；就算用户想做手脚，追查亦较方便，因为 PSTN 对所有终端均按 E.164 码号规则赋予全球惟一与公开的编号。此外，当 PSTN 提供 IP 网接入服务时，仅作为 IP 网的链路层接入，IP 数据只是在 PSTN 上透穿，无法在 PSTN 接入 IP 之际从 IP 网攻击 PSTN。由此可以推理 PSTN 的网络与终端安全性较好，相应其丧失的便是灵活有效的宽带多业务增值能力。

ATM 虽然亦同属分组型技术，但 ATM 并无直接的终端业务与用户，对用户而言只是提供一个逻辑“ 专网 ”，用户只能在自己的“ 专网 ”中运作，用户亦无能力与可能发送 ATM 网络能识别与要识别的信令与业务数据。同样，ATM 的 UNI 与 NNI 是分离的，网络只是为用户提供透传功能，其信令、业务数据等对用户为不可见，用户无法产生恶意数据对 ATM 进行攻击；ATM 网络与网络间的安全性则靠运营规则与运营商间的信任关系和协同合作予以保证。而且，由于用户只能在自己所在的网络中运作，即便能发动攻击，也只能攻击自己网络内的有限用户，很容易追查。因此，ATM 网络也有较好的安全性保证，但同时带来了宽带多业务增值不灵活方便与不价廉物美。

再看 IP 网络，它真像信息的明信片传送，没有 UNI 与 NNI 的分离，运营商设备、协议乃至网络拓扑对用户均属开放可见。用户端产生的 IP 信息，无论在用户端或在网络中均可传送终结，从而既可能由用户端与运营商网络交换非法及恶意路由信息，也可能对运营商网络的路由器、接入服务器等设备及三层以上设备实施攻击。与此同时，位于 IP 网络边际的用户侧的网络与业务、应用，一般均使用 TCP/UDP/IP 这一基础技术，这导致用户间在 IP 层及应用层等各层面彼此透明可见，从而亦为恶意用户攻击对方网络及相应业务大开方便之门。IP 网络的终端高度智能化及多业务能力一方面使由终端用户发动攻击变得容易，同时又增加了识别与防范各类花样繁多的安全攻击的难度，因为多种业务综合承载在同一网络上，难以分辨与确立用户间的信任关系，导致恶意用户容易找准对象发动攻击，而被攻击的用户实际上难以分清哪些是合法用户的正常访问，哪些是非法用户侵入或恶意攻击。另一方面，鉴于 IP 网络及技术飞速发展，协议设计及软件开发中的缺陷与漏洞在大规模应用前来不及测试发现与彻底排除，这亦给恶意攻击造成各种可乘之机。对此，一些知名公司的软件漏洞，如微软的 WindowsXPsp2、思科的 IOS 及苹果的 MACOS 均为其明显示例。此外，IP 用户身份难以识别导致很难跟踪及遏止攻击者；而且，IP 的高度智能的终端及其宽带化，加上其计费模式等更有利恶意用户方便与低成本地有效实施大规模攻击，包括分布式拒绝服务（DDOS）攻击在内，而且制造这类攻击的技术难度亦变得愈来愈容易，从而使这类非法入侵及恶意攻击有增无减、肆意蔓延与防不胜防，着实令人担忧。当然，IP 协议的开放透明性导致的安全性弊端，同时带来了其灵活有效的宽带多业务增值能力及容易互联互通和有效降低成本等明显的市场应用优势与吸引力。

现实情况亦确实如此，黑客、病毒似乎愈杀愈烈，泛滥成风，实际已成为 IP 网络安全运作的头等隐患。例如，2004 年，新病毒增加 52%，瑞星报告指出，其中下述十大病毒对用户造成的破坏最大：网络天空（占总病毒数的 39.9%）、爱情后门（占 21.3%）、SCO 炸弹（占 7.7%）、小邮差（占 1.5%）、垃圾桶（占 0.9%）、恶鹰（占 0.8%）、求职信（占 0.5%）、高波（占 0.5%）、震荡波（占 0.4%）及瑞波（占 0.4%）。而且，黑客和病毒威胁呈下述四大发展趋势：变种病毒数量翻番剧增、防不胜防，从漏洞被发现至针对漏洞攻击病毒出现的时间间隔越来越短，国产型木马病毒及后门程序成为主流，目标直指网民真实财产，“ 网络钓鱼 ”形式的诈骗病毒活动明显增加等。十大病毒中有 9 种为蠕虫，从对用户的危害性而言，依然是蠕虫病毒最为严重。病毒变种之所以快速增长蔓延的一个重要原因即在于很多病毒源代码借助网络被病毒作者公开并提供下载，甚至有些代码还包括完整的说明文档及相应工具和示例，易于普及传播。毋需特别技能，仅需修改配置文件和部分源代码便可编译生成一个新的变种病毒。这是对公开性、包括源代码公开在内而产生的负面影响的一种直接讽刺，亦说明如何正确认识与控制一种事物的正反两个方面是何等重要。

由这些分析讨论可充分理解 IP 网络安全问题的本质所在，就像 SARS 一样，只有控制其病源，才能控制其蔓延，因此，寻找 IP 网络的有效安全对策，尤为紧迫、重要。

对此，IP 和 Internet 研究的权威机构——IETF，对现有 Internet 及 IP 协议的缺陷与不足已有足够的认识，曾在其年会提出过主题“ 因特网的十字路口 ”，列举了 Internet 下一步发展面临的 10 大技术问题：身份识别技术、保护 IPR 技术、保护个人隐私技术、新一代 Internet 通信协议 IPv6 技术、下一代 Internet 结构的网格（Grid）技术、无线 Internet 技术、传统电话网与 Internet 融合的技术、更有效地在网上传输的视频技术、防止垃圾邮件的过滤技术及网络安全技术。如果无法在网络安全、个人隐私及 IPR 保护方面取得突破，Internet 将无法成为一种真正可信的商业工具。当然，IETF 相信，在采取一系列有效措施后，如改进 IP 协议，改进 TCP/UDP 协议，缩短路由及传输时延，提高传输效率及质量，实施有效的全球大容量移动扩展、访问与漫游，提高网络安全性及改进网络管理能力等，新的 IP 网能担当起 NGN 重任。十大技术问题中即有一半以上与安全性有关，可见 IP 安全问题的严重性。

参考文献

1 杨延双、张建标、王全民编著.TCP/IP 协议分析及应用［M］. 北京：机械工业出版社，2007.2

2 史蒂文斯（W.Richard Stevens）著.TCP/IP 详解（范建华等译）［M］.北京：机械工业出版社，2007.8

On the TCP / IP Technology

Yang Hongmin

Abstract: TCP/IP protocol is the most basic Internet protocol, which is composed of underlying IP protocol and TCP protocol. It is developed at different levels, and every level is responsible for different communication functions. The main purpose of its application is for the application on Internet. The article briefly introduces its security issues existing in the application.

Key words: TCP/IP; WWW service; E－mail