远程工作站的协议与安全

蔡吸礼　（杭州广播电视大学　310009）
余日泰　（杭州电子工业学院　310037）

摘要：本文提出一种分析远程工作站通信协议的逆向分析方法，采用这种方法对基于 Netware 异步远程路由器的远程工作站的通信协议进行了详细分析，在此基础上描述了其通信协议的层次结构模型、特点及安全隐患，并提出了针对性的安全策略。

关键词：网络安全　远程工作站　网络协议

一、引言

在 Novell 局域网中，本地工作站与 LAN 的通信过程及其协议已为广大网络用户所熟知，然而某些业务中远程工作站需要共享网络资源，这就超出了局域网网段所许可的距离范围。Novell 公司提供的 Netware 异步远程路由器（NARR）软件包能将物理上离局域网很远的远程工作站通过调制解调器及公共交换电话网与局域网连接在一起，使远程用户可以透明地访问网络资源。

基于 NARR 的远程工作站（以下简称 NARW）与局域网的通信功能是集成在 NARR 软件包中的，Novell 公司并未公开其核心细节。本文基于对通信链路的逆向分析，深入研究了 NARW 与 LAN 的通信过程、协议及其特点，并在这些细节基础上提出了相应的安全策略，可为广域网的产品开发、选型规划及管理提供参考依据。

二、NARW 的配置特点

NARW 与局域网相连，在硬件上要依次通过：站端调制解调器、公共交换电话网、网端调制解调器、NARR，如图 1 所示。

在软件上，工作站最主要的是两个文件：IPX.COM 和 NETX.COM，它们支持工作站与工作站及工作站与文件服务器之间的会话。前者将系统提供的 IPX.OBJ 文件与相应的物理层驱动程序链接后得到，它管理网络站点之间的通信，与物理层共同实现 OSI 参考模型的低三层协议；后者用以进行信息的重定向文件。由于 NARW 物理层使用的是异步串行通信，因而在生成 IPX.COM 后还需用 Aconfig 对 IPX.COM 进行配置[3]，其中包括指定异步串行口速率、对调制解调器的通信协议、对 NARR 的通信协议等等。

NARW 与 LAN 的通信功能被集成在 NARR 软件包中，直接对该软件包进行正向分析有一定的困难，因而我们采用了基于通信链路的逆向分析方法。具体方法是：在 NARW 与站端调制解调器之间接入一台计算机，将其异步串行口 COM1 与 NARW 相连，异步串行口 COM2 与站端调制解调器相连，通过编制软件完成通信速度匹配及双方通信信息的相互转发，同时提取这些原始数据。通过对它们的分析可以清楚的了解 NARW 的工作细节。

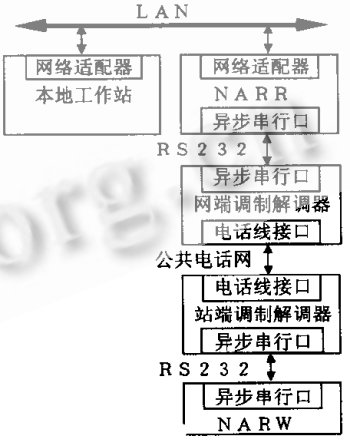

图 1　NARW 的物理连接

三、NARW 与 LAN 建立联系的过程分析

参照图 1 可以将 NARW 与 LAN 的连接过程按其依次通过的物理设备分为以下几个步骤。

1. 建立与站端调制解调器之间的联系

该联系由 IPX.COM 完成，由 NARW 向站端调制解调器发复位命令，等待站端调制解调器返回结果。这一

© 中国科学院软件研究所 http://www.c-s-a.org.cn

过程不但使站端调制解调器复位，而且对智能调制解调器而言还是速度匹配的过程。如图 2 所示：NARW 采用的通信协议是与站端调制解调器相对应的，一般采用 Hayes AT 命令[1]；端口协议由 IPX.COM 生成时配置[3]；站端调制解调器应答"OK"表示连接成功。

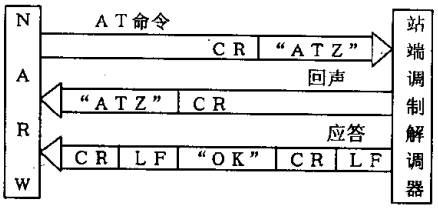

图 2　建立与站端调制解调器之间的联系

2. 建立与网端调制解调器之间的联系

该联系由 IPX.COM 完成，由 NARW 向站端调制解调器发拨号命令（其中包括部分对站端调制解调器的初始化命令），并等待站端调制解调器返回拨号结果，此时由站端调制解调器自动与网端调制解调器取得联系。如图 3 所示：NARW 采用的通信协议仍然与前一阶段相同；调制解调器之间的协议与调制解调器有关，有 CCITT V.32、V.42 等[1]；站端调制解调器应答"10"表示连接成功。

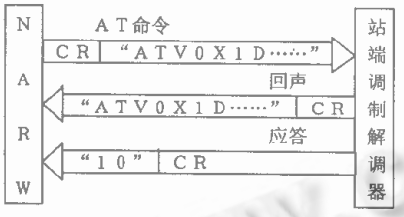

图 3　建立与网端调制解调器之间的联系

3. 建立与 NARR 之间的联系

由于网端调制解调器与 NARR 之间的物理层联系在 NARW 接入 LAN 前就已经由 NARR 完成，因而一旦 NARW 与网端调制解调器之间建立了物理层联系同时也就与 NARR 建立了物理层联系。但是本阶段 NARW 还将与 NARR 建立异步帧数据链路子层的联系。该联系由 IPX.COM 完成，由 NARW 向 NARR 发出访问帧，等待 NARR 发回确认帧和应答帧。如图 4 所示：访问帧的结构参照了基于 IPX 包的异步帧结构（图 6），其帧头及帧校验方式见图 6 说明，而访问包的结构也参照了 IPX 包的结构；"标识串"在 IPX.COM 和 NARR 端软件生成时同时设置且必须一致，作为 NARW 访问许可及身份识别，"工作站名称"在 IPX.COM 生成时设置，"NARR 名称"在 NARR 端软件生成时设置，上述三者均以明文形式传输。

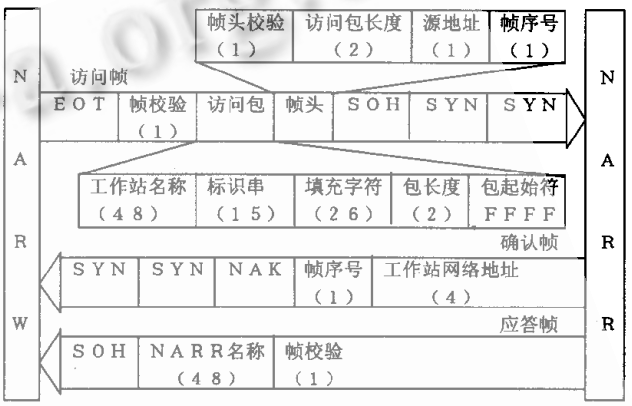

图 4　建立与 LAN 之间联系时的异步帧协议

在以后各阶段，NARW 与 NARR 之间的通信均可通过异步帧数据链路子层完成，也就是说它们在数据链路层建立了透明连接，如图 5 所示。

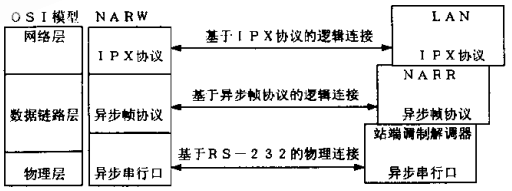

图 5　NARW 与 LAN 通讯的几个层次

4. 建立与 LAN 之间的联系

由于 NARR 与 LAN 之间的数据链路层联系在 NARW 接入 LAN 前就已经由 NARR 完成，而 NARR 负责完成两种不同的数据链路层协议的转换工作，因而

© 中国科学院软件研究所 http://www.c-s-a.org.cn

NARW 与 NARR 建立数据链路层联系的同时也就与 LAN 建立了数据链路层联系。但是本阶段 NARW 还将与 LAN 建立网络层的联系。该联系由 NETX.COM 完成，采用 IPX 协议，其过程和本地工作站与 LAN 建立网络层联系的过程基本相同，本文不再详述[2]。

四、NARW 的通信协议结构及安全隐患

1. NARW 与 LAN 的通信协议结构

在 NARW 与 LAN 建立了联系以后，它即成为了 LAN 的工作站，它与 LAN 的所有通信都可基于 IPX 协议。然而就 NARW 而言，它与 LAN 的通信协议可以分为三个不同的层次，负责与不同设备之间的通信，这些协议与 OSI 参考模型低三层的对应关系如图 5 所示。

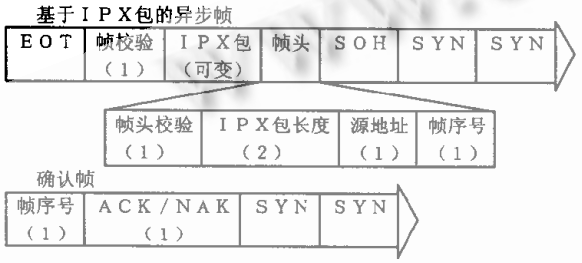

图 6　NARW 中基于 IPX 包的异步帧协议

(1)与 LAN 对应的采用 IPX 协议的网络层协议[2]。在这一层上 NARW 与 LAN 是透明连接的，即 NARW 与本地工作站在逻辑上是基本相同的。

(2)与 NARR 对应的基于 IPX 包的异步帧协议。这是 NARR 方案所特有的协议，由软件 IPX.COM 实现。该协议的两种帧结构如图 6 所示，采用发送/等待的纠错协议，帧校验采用了帧头校验和帧校验的双重校验方式，帧头校验存放帧头(4 个字节)的累加和模 256 的补码，帧校验存放帧的累加和模 256 的补码，对确认帧无校验形式。

(3)与站端调制解调器对应的端口协议。一般由 IPX.COM 生成时设置。

2. NARW 与本地工作站的比较

NARW 与本地工作站在协议层次、建立与 LAN 的通信过程以及软件生成等方面的异同比较见表。

表　NARW 与本地工作站的比较

	NARW	本地工作站
物理接口	异步串行口	网卡
数据通信方式	异步	同步
数据通信速率/带宽	9600bps	10Mbps
数据链路层的帧类型	NARR异步帧	IEEE802.3
数据链路层的帧差错控制方式	发送/等待	IEEE802.3
数据链路层的帧头校验及其方式	累加和补码方式	无
数据链路层的帧校验及其方式	累加和补码方式	CRC
数据链路层大部分协议的实现	主要由软件实现	主要由网卡实现
基于IPX协议的网络层	相	同
软件完成的功能：硬件初始化	针对异步串行口	针对网卡
软件完成的功能：建立与站端调制解调器之间的联系	需要	——
软件完成的功能：建立与网端调制解调器之间的联系	需要	——
软件完成的功能：建立与NARR之间的联系	需要	——
软件完成的功能：工作站身份识别	有	无
软件完成的功能：支持IPX协议	支持	支持
IPX.COM生成后的进一步配置	需要	不需要

3. NARW 的安全隐患

(1)如图 1 所示，NARW 与 LAN 的物理链接环节最脆弱的地方是站端调制解调器与网端调制解调器之间的公共电话网环节，最易受到诸如搭线窃听、拨入端口访问等的攻击。虽然在 NARW 与 NARR 建立联系时要提供"标识串"，在一定程度上增加了 LAN 的安全性，但是，"标识串"不仅用 Aconfig 在 NARW 上和 NARR 上都可读出其明文，而且以明文形式传送，因而极有可能被窃取。

(2)NARW 在网络层上与本地工作站逻辑上基本相同，一旦攻击者攻击成功将获取所有 IPX 包，从而可得到完整的任务信息，而 IPX 协议已被详细分析[2]。

五、针对 NARW 的安全性策略

根据 NARW 的特点，我们认为在安全性要求较高的系统中，可以着重加强以下几个方面的安全措施。

(1)增加保密手段。由于 NARW 与 LAN 的通信过程中含有明文，因此可根据实际情况适当选择一些保密手段，如：采用专线通信方式、使用话路加密设备或链路加密设备等。

© 中国科学院软件研究所 http://www.c-s-a.org.cn

(2)加强网络监控,及时发现攻击者的攻击行为。在LAN环境下启动Netware的监控程序可以及时发现未授权注册企图,但它无法发现对NARR进行的攻击,如对"标识串"的攻击、搭线窃听等,因此还必须对网端调制解调器进行监控,同时可在电话线路上使用渗透检测设备。

(3)加强网络管理。一般LAN安装在一个建筑物或一个部门内,所有用户彼此认识,工作站点位置确定,因而只要采用物理控制方法(如:门锁等)就可获得足够的安全性,但在NARR存在时这些控制方法有可能失去作用,所以更应重视网络管理。例如:对"标识串"采用与通行字相同的安全策略,如定期修改等;对Supervisor的通行字设计尤其重要,因为在Netware中该用户一定存在而且具有很高的权限,受攻击的可能性最大;对远程用户可实行有差别的访问控制,如对网端调制解调器和NARR定时开通、限制特殊用户远程访问等。

(4)加强安全教育。对网络用户进行安全教育,尤其是通行字的选取常识,让他们知道由于NARR的存在,所有用户随时都有可能受到来自LAN地域外的攻击。网络管理者则更应具备安全方面的专业技术知识。

参考文献

[1] Hayes Communication Guide, Hayes Microcompuer Products, Ins., 1994.

[2] [美]L.Chappell著,尹国定等译,Novell指南Netware局域网分析,电子工业出版社,1994.

[3] 庄德秀等编著,Novell网络与通讯技术,清华大学出版社,1994.

(来稿时间:1999年3月)

© 中国科学院软件研究所 http://www.c-s-a.org.cn