服务器知识手册（十八）

狄登峰 主编

需要全本请访问 www.ertongbook.com

目　　录

Windows 系列 1
Win NT、Linux、Unix 等服务器的互连 1
NT Server 无盘站配置技术详解 5
运用主要组设置巧妙阻止受限制组 17
解除"限制组成员"限制 21
Win2000 server 上安装 Office 2000 23
如何本机调试 CGI 28
在 2000 及 NT 中修改密码的到期通知时间 32
runas 使用中的常见错误及对策 33
WindowsNT 和 Linux 的文件权限一个区别 36
RIS 服务的主要软/硬要求 37
WinRoute 拨号参数设置 39
Web 服务器的安全和攻击防范 40
Web 服务器的安全和攻击防范 43
IIS 安全 55
Windows NT 系统安全 65
Win2000 Server 入侵监测 72
远程检测 MS SQL Server 账号安全性 83
Win2000 Server 安全配置入门 95
windows 2000 技巧集成 104
域名服务器 108
架设 DNS 服务器要谨慎 108
Win2000 中 DNS 服务器的设置 109
构建 DNS 服务器简易指南 113

Windows 系列

Win NT、Linux、Unix 等服务器的互连

由于 Novell NetWare 使用的是 IPX/SPX 协议，在 Windows NT 访问 NetWare 资源就要通过协议转换。Windows NT 服务器提供了 GSNW 网关服务，使 Dos/Windows 客户可以通过访问 Windows NT 服务器来间接访问 NetWare 资源。

1、Novell NetWare 服务器的配置

首先，在 NetWare 服务器上创建一个称之为 NTGATEWAY 的用户组，并在你希望共享的目录上赋予 NTGATEWAY 用户组一定的权限，然后，将被用作网关帐号的用户包含在 NTGATEWAY 组中。可使用 NetWare 的 NETADMIN（Dos 版本）或 NWADMIN（Windows 版本）实用程序创建用户组和用户。

2、Windows NT 服务器的配置

Windows NT 服务器的 GSNW 服务需要 Nwlinnk 网络协议支持，所以，首先必需在 Windows NT 服务器上添加 Nwlink 协议。在 NT Server 上运行 Control Panel 中的 NetWare 程序，选择安装 Nwlink 协议即好，要注意的是，Nwlink 所使用的帧类型应与将要访问的 Novell NetWare 服务器上使用的帧类型相匹配。然后，安装 GSNW 服务，同样运行 Control Panel 中的 NetWare 程序，选择安装 GSNW 服务即可。安装完成

后，重新启动计算机，将有一个 GSNW 图标出现在 Control Panel 中，用来选择默认的 NetWare 服务器和 NetWare 打印队列。通过 Control Panel 的 GSNW 图标来激活 NetWare 网关服务程序，激活 GSNW 后，需在 Default Tree 和 Contex 选项中分别输入 NetWare 服务器的树名称和用户账号（NTGATEWAY 组中的用户账号）信息。这样配置之后，NT Server 就可以共享 NetWare 资源，将 NetWare 资源映射到本地盘，NT 的客户端（Dos、Win95/98、NT Workstation、NT Server）便可通过访问该盘来间接存取 NetWare 资源。

使用 GSNW 的优点是：

客户机仅仅需要登录到 Microsoft 网络。

网关仅仅希望一个登录到 NetWare 用户，但是却使许多用户共享 NetWare 资源，这样就合法地扩展了对 NetWare 服务器的访问权限，而不用额外的 NetWare 许可证·客户机仅仅需要一个客户软件包，尤其是在内存受限制的 MS-DOS 系统中，客户机软件包要好节省内存。

·通过消除对支持多种客户机请求程序的需要，减少了管理负担。

使用 GSNW 的缺点是：

由于客户机必须经过 NT 的 GSNW 网关来访问 NetWare 资源，效率不是很高，适用于不经常访问 NetWare 服务器的情况。

Unix、Linux 服务器与 Windows NT 服务器的互连

在 Linux 主机和 Unix 主机使用的都是 TCP/IP 协议，一台 Linux 主机若要同其它 Linux 主机或是 Unix 主机实现信息共享，有很多方便的、成熟的工具如

FTP 或 NFS 等等。同样，Windows NT 也支持 TCP/IP 协议，所以 NT Server 与 Linux 主机或是 Unix 主机的信息交流，也可以通过 FTP 或 NFS。但是，FTP 和 NFS 并不够直观操作。为便于 Windows 与 Linux 及 Unix 更方便地进行信息共享，如同 Windows 与 Windows 之间一样，我们可以通过 Linux 提供的 Samba 服务程序。 Samba 是一组程序，可以使你的 Linux 具备理解 SMB 协议（server message block）的能力。SMB 协议是一种在 os/2、Windows NT、Windows 95 和 Windows for workgroups 等 Windows 系列中广泛使用的协议，该协议主要用来实现文件和打印机共享。使你的 Linux 将会出现在"Network Neighborhood"（网络邻居）中如同其它 Windows 机器一样。Windows 用户可以登录至你的 Linux 机器并且以你赋与他们的权限与 Unix 文件系统进行双向的交流，还可以向 Linux 打印机提交作业。

2.1 Samba 组成

一个 samba 服务器实际上包含了两个服务器程序：smbd 和 nmbd。Smbd 是 samba 的核心。它负责建立对话进程、验证用户身份、提供对文件系统和打印机的访问机制。Nmbd 实现了"network browser"（网络浏览服务器）的功能。它的作用是对外发布 samba 服务器可以提供的服务。Nmbd 可以使 samba 服务器出现在 Windows 95 或 Windows NT 的"Network Neighborhood"（网络邻居）中并且可以客户机浏览到可以访问的资源。完全可以不运行 nmbd 而起动 samba 服务器进程，但是也许客户除了想看到 samba 服务器的 NetBIOS 名外，还想看到 samba 服务器可以提供的服务。

需要全本请访问 www.ertongbook.com

2.2 Samba 配置

由于 SMB 是一个非常复杂的协议，所以配置 samba 是十分繁复的，大约有超过 170 条配置项出现在 smb.conf 文件中。在 RedHat 和 Debian 中 Smb.conf 文件缺省位置是在 /etc/ 下，所有的 samba 程序都要参照这个配置文件。其结构十分类似 Windows 的 *.ini 文件。文件中的每一节都由一个被方括号括起来的标识开始，例如：[global]、[home] 和 [printers]。

每一个配置参数或是一个全局参数（影响或控制整个服务器），或是一个服务参数（影响或控制服务器提供的某项服务）。[global] 节设置全局选项和一些缺省的服务选项。[home] 节是用来动态的映射到每个用户的 home 目录下。[printers] 节用来设置将按照系统 printcap 文件配置的打印机共享至指定用户。

2.3 一个简单的 smb.conf

下面的 smb.conf 描绘了一个简单的但能工作的配置：

[global]

netbios name = ABC workgroup = WORKGROUP server string = Linux

security = user printing = lprng

[homes]

comment = Home Directory browseable = no read only = no

在 [global] 节中设置了主机的 netbios 名，主机所在的工作组的组名和将在 browse list 出现的提示字串。安全参数提示 samba 使用"user level"（用户级）安全级别。SMB 有两种安全级别：share（共享级，对

每个特定的资源使用口令保护和指定每个用户有各自不同的访问权限）和 user level（用户级）。不过在大多数情况下，你使用的是用户级安全级别。由于没有指定特殊的加密方式，samba 缺省使用标准的 unix 口令字验证方式既 plaintext 口令字验证方式验证每个连接。若你的 linux 使用 PAM 模块，那麼你必须修改 PAM 配置使 samba 可以通过口令字数据库验证口令字。RadHat 自动进行这些处理。

[homes] 节中的设置用来控制每个用户 home 目录的共享情况。Comment parameter（注解参数）是在 browse list 中标示该条目的字串。 browseable 参数控制是否该项服务出现在 browse list 中。

下列的配置使每个可以登录至 samba 服务器的用户使用在系统 printcap 文件中定义过的打印机。

[printers]

browseable = no guest ok = yes printable = yes

完成 smb.conf 文件的配置后，可以使用 Testparm 命令来快速检查 smb.conf 文件的语法错误。通过以上配置，在 Linux 主机上运行 Samba 服务程序：smbd 和 nmbd。Windows 与 Unix、Linux 便可以很方便地进行进行数据交换。

NT Server 无盘站配置技术详解

无盘工作站（简称无盘站）即不使用本地磁盘的计算机工作站。由于无盘站具有低配置、低价格、安全性好、易于管理等特点，所以它在我国应用很广。目前，无盘工作站对于学校、网吧、游戏厅和各种计算机培训

中心来说是一种较为理想的选择。

随着客户机/服务器（C/S）结构的兴起，Windows NT 网络以其优异的性能、丰富的软件支持已逐步得到广泛的应用。然而，介绍 Windows NT 无盘站的技术资料很少，给广大网络技术人员建立 Windows NT 无盘站带来一定困难。在此仅是抛砖引玉，希望能给大家帮助。

一、 NT Server 服务器的安装

1. 安装 NT Server 4.0 中文版

安装 NT Server 4.0 中文版，最好使用 NTFS 文件系统。本文假定 NT Server 4.0 装于 C:\WINNT 目录下，服务器名为 NTSERVER，域名为 DOMAIN。

2. 安装 NETBEUI 协议和 DLC 协议

在 NT 服务器"我的电脑"·"控制面板"·"网络"·"协议"选项中添加 NETBEUI 协议和 DLC 协议。

3. 安装远程启动服务（RPL 服务）

在 NT 服务器"我的电脑"·"控制面板"·"网络"·"网络服务"列表中选择"远程启动服务"，单击"确定"进行安装。

4. 启动远程启动服务

在NT服务器"我的电脑"·"控制面板"·"服务"中选"远程启动服务"，单击"启动"，将启动类型改为"自动"，然后重新启动 NT 服务器。

二、RPLCMD 命令简介

NT Server 可支持 3Com、Intel、Novell NE 等系列网卡，对于常见的各种网卡如 Accton、D-Link、TOPSTAR 及各种 NE2000 兼容网卡并不能自动识别。这样，就要求用 RPLCMD 命令手工修改网卡配置文件数据库。

RPLCMD 命令格式为：RPLCMD [\\computername]

其中，computername 为远程启动服务器的计算机名。在程序运行后有下面几个命令：

A：用于修改不完整的网卡记录。

B：用于修改 BOOK BLOCK 记录，可设置 DOSBB.CNF 文件路径。

C：修改配置记录，可用来指出系统目录映射关系文件（DOS622.FIT、DOS622P.FIT、WIN95.FIT、WIN95P.FIT）的路径。

P：用于修改配置文件。

S：用于控制远程启动服务。

V：用于配置网卡厂商编码（网卡 ID 号的前 6 位数字）及网卡名称。

W：用于修改工作站记录。

每个命令执行后又有下面三个命令供选择：

A：添加一条记录。

B：删除一条记录。

E：显示记录。

其中最为常用的是 A、C、V 命令。

三、准备 BOOT ROM

1. 根据实际使用的网卡（ACCTON 16XX、SN2000 等）找到合适的 BOOTROM

Windows NT 常用的 BOOT ROM 为 RPL BOOT ROM，不同于 Novell 网常用的 IPX BOOT ROM 和 ODI BOOT ROM。一种网卡的 BOOTROM 不一定兼容其他网卡，请选择合适的 BOOT ROM。笔者有种 RPL BOOT ROM 可兼容大多数 NE2000 兼容网卡。Accton 16XX 系列网卡使用的 BOOT ROM 型号为 SW7145 。本文将以 NE2000 兼容网卡、NE2000 兼容 RPL BOOT ROM

为例进行配置。

2. 将网卡设置为可远程引导，并将中断设为 3，IO 设为 300

可用网卡驱动盘上 SETUP 之类的程序修改。

3. 将 BOOT ROM 插入网卡

注意将 BOOT ROM 的小缺口和网卡插座的小缺口相对应。

四、DOS 无盘站的安装（以 DOS 6.22、NE2000 兼容网卡为例）

1. 设置远程引导共享目录

NT Server 在远程启动服务（RPL 服务）安装完成后会自动在 C:\WINNT 目录下创建 RPL 目录。将 C:\WINNT\RPL 目录下的 RPLFILES 目录设为共享,共享名为 RPLFILES。

2. 拷贝系统文件

在 NT 服务器上将 DOS 系统文件拷入 C:\RPL\RPLFILES\BINFILES 目录下的 DOS622 目录中（其他 DOS 版本对应相应的目录）,并去掉 IO.SYS、MSDOS.SYS 的所有属性。至少要复制下面三个文件：

IO.SYS

MSDOS.SYS

COMMAND.COM

3. 拷贝 NDIS 驱动文件

将网卡驱动盘上的 NDIS 驱动文件复制为 C:\WINNT\RPL\BBLOCK\NDIS 目录下 NE.DOS 文件。如网卡驱动盘上无 NDIS 驱动文件则将 C:\WINNT\RPL\BBLOCK\NDIS 目录中的 NE2000.DOS 复制为 NE.DOS。

4. 拷贝 DOSBB.CNF 文件

在 C:\WINNT\RPL\BBLOCK\NETBEUI 目录下创建子目录 NE，并将网卡驱动盘上的 DOSBB.CNF 文件拷贝到 C:\WINNT\RPL\BBLOCK\NETBEUI\NE 目录下。如网卡驱动盘上无 DOSBB.CNF，可将 C:\WINNT\RPL\BBLOCK\NETBEUI\NE2000 目录下的 DOSBB.CNF 文件拷贝到 C:\WINNT\RPL\BBLOCK\NETBEUI\NE 目录下，并用 EDIT 修改 DOSBB.CNF，将 DAT BBLOCK\NETBEUI\NE2000\PROTOCOL.INI 一行改为 DAT BBLOCK\NETBEUI\NE\PROTOCOL.INI，将 DRV BBLOCK\NDIS\NE2000.DOS ~ ~ ~一行改为

DRV BBLOCK\NDIS\NE.DOS ~ ~ ~。

5. 拷贝 PROTOCOL.INI 文件

将网卡驱动盘上的 PROTOCOL.INI 文件拷贝到 C:\WINNT\RPL\BBLOCK\NETBEUI\NE 目录下,如网卡驱动盘上无此文件，可将 C:\WINNT\RPL\BBLOCK\NETBEUI\NE2000 目录下的 PROTOCOL.INI 文件拷贝到 C:\WINNT\RPL\BBLOCK\NETBEUI\NE 目录下。

6. 修改网卡远程引导数据库

（1）用网卡设置程序（SETUP 等）查看网卡内部 ID 号，并记录下来。（在 Windows 95 下用 WINIPCFG 命令，在 Windows NT 下用 IPCONFIG /ALL 命令可查看网卡的 ID 号。）

（2）在 WINDOWS NT 命令提示符下运行 RPLCMD 命令。

A）添加网卡厂商编码（即网卡 ID 号前 6 位）

C:\WINNT\RPLCMD

Adapter Boot Config Profile Vender Wksta [Quit]: V

需要全本请访问 www.ertongbook.com

Add Del Enum: A

VenderName=52544C (网卡 ID 号的前 6 位)

VenderComment=ne-compatible

B）添加网卡 BOOK BLOCK 记录

C:\WINNT\RPLCMD

Adapter Boot Config Profile Vender Wksta [Quit] B

Add Del Enum:A

BootName=DOSNE （与下一步 BootName 对应）

VenderName=52544C (网卡 ID 号的前 6 位)

BbcFile=BBLOCK\NETBEUI\NE\DOSBB.CNF

All other parameters are optional

Boot Comment=ne-compatible

WindowsSize=0

C）修改系统配置记录

C:\WINNT\RPLCMD

Adapter Boot Config Profile Vender Wksta [Quit] C

Add Del Enum: A

ConfigName=DOS622NE （自定义的 ConfigName，不能与已有的同名）

BootName=DOSNE （与上一步 BootName 对应）

DirName=DOS

DirName2=DOS622

FitsShared=FITS\DOS622.FIT （共享目录映射关系文件）

FitsPersonal=FITS\DOS622P.FIT （专用目录映射关系文件）

All other parameters are optional

ConfigComment=NE-DOS-BOOT

DirName3=

DirName4=

7．在服务器上建立远程启动配置

（1）打开无盘工作站。

（2）在服务器上配置 Windows NT 支持的网卡。运行"远程启动管理器"，你将看到一台未经配置的无盘站。步骤："开始"·"程序"·"管理工具（公用）"·"远程启动管理器"。

（3）选择菜单"配置"·"检查配置"，然后单击"是"。

（4）选择菜单"远程启动"·"新的配置文件"选择"NE-DOS-BOOT"，配置名键入"DOSRPL"。

（5）选择未经配置无盘站的 ID 号，选择菜单"远程启动"·"转换适配器"选择 DOSRPL，键入 WKSTA 名：USER1，这时你就可发现刚才配置的无盘站已经开始启动了。

五、Windows 无盘站的安装（以中文 Windows 3.2 为例）

1. 在 NT Server 服务器 C 盘上建立"32" 目录，并使之共享，将 Windows 3.2 系统安装文件拷入 32 目录下。

2. 启动该无盘站，以 Admnistrator 帐号登录，执行 C:\>NET USE F: \\ NTSERVER \32。

3. 在无盘站 F 盘执行 SETUP /A，将 Windows 安装到 C:\WIN 目录中。

4. 在无盘站 C 盘 WIN 目录下执行 SETUP/N 命令，选择 EXPRESS 方式安装，将 Windows 安装在 C:\windo

ws 目录下内（勿选择更新任何已存在的 Windows），并以 EXPRESS 安装。

5. 在安装过程中，SETUP 会修改 CONFIG.SYS 与 CONFIG.SYS 文件，如 SETUP 无法修改，选择取消，等复制完成后，将 C:\WINDOWS 目录下的 CONFIG.WIN、AUTOEXEC.WIN 文件内容复制到 C 盘根目录下的 CONFIG.SYS 与 AUTOEXEC.BAT 文件中。

6. 将以下三行加入 C:\WINDOWS\SYSTEM.INI 中的[386enh]区段内。

TimerCriticalSection=5000

UniqueDosPSP=True

PSPIncrement=2

7. 将 C:\WINDOWS 中所有文件复制到 C:\WKSTA.PRO\WIN 目录下(XCOPY /S /E C:\WINDOWS C:\WKSTA.PRO\WIN)，这样所有使用"DOSRPL"配置名的无盘站都可以启动 Windows。

8. 重新启动该工作站，以普通无盘站用户帐号登录，执行 WIN 即可进入 Windows。

六、Windows 95 无盘站的安装（以中文 Windows 95 为例）

1. 简述

目前，Windows 95 可进行无盘站安装，Windows 97、Windows 98 则不行，或许笔者没调试成功，请内行指教。要进行 Windows 95 无盘站的安装，必须有 NETSETUP 软件，在微软原版 Windows 95 光盘上的 ADMIN \ NETTOOLS\NETSETUP 目录下有该软件。

2. 拷贝 W95BB.CNF 文件

将网卡驱动盘上的 W95BB.CNF 文件拷贝到 C:\WI

NNT\RPL\BBLOCK\NETBEUI\NE 目录下。如网卡驱动盘上无 W95BB.CNF，可将 C:\WINNT\RPL\BBLOCK\NETBEUI\NE2000 目录下的 W95BB.CNF 文件拷贝到 C:\WINNT\RPL\BBLOCK\NETBEUI\NE 目录下。并用 EDIT 修改 W95BB.CNF，将 DAT BBLOCK\NETBEUI\NE2000\PROTOCOL.INI 一行改为 DAT BBLOCK\NETBEUI\NE\PROTOCOL.INI，将 DRV BBLOCK\NDIS\NE2000.DOS ~ ~ ~一行改为 DRV BBLOCK\NDIS\NE.DOS ~ ~ ~。（注：如有的网卡驱动盘上有 DOSBB.CNF 而没有 W95BB.CNF 则可将 DOSBB.CNF 拷贝为 C:\WINNT\RPL\BBLOCK\NETBEUI\NE 目录下 W95BB.CNF 文件，然后用 EDIT 编辑 W95BB.CNF，将其中的 EXE BBLOCK\I13.COM~~~一行改为 EXE BBLOCK\W95I13.COM~~~，并和上面一样，要修改 PROTOCOL.INI 文件的路径和 NE.DOS 文件的路径。）

3. 修改网卡远程引导数据库

(1)修改 BOOK BLOCK 记录

C:\WINNT\RPLCMD

Adapter Boot Config Profile Vender Wksta [Quit] B

Add Del Enum:A

BootName=W95NE （与下一步 BootName 对应）

VenderName=52544C (网卡 ID 号的前 6 位)

BbcFile=BBLOCK\NETBEUI\NE\W95BB.CNF

All other parameters are optional

Boot Comment=ne-compatible

WindowsSize=0

（2）修改系统配置记录

C:\WINNT\RPLCMD

Adapter Boot Config Profile Vender Wksta [Quit] C

Add Del Enum: A

ConfigName=WIN95NE （自定义的 ConfigName，不能与已有的同名）

BootName=W95NE （与上一步 BootName 对应）

DirName=DOS

DirName2=WIN95

FitsShared=FITS\WIN95.FIT（共享目录映射关系文件）

FitsPersonal=FITS\WIN95P.FIT （专用目录映射关系文件）

All other parameters are optional

ConfigComment=NE-95-BOOT

DirName3=

DirName4=

4．在服务器上建立远程启动配置

（1）运行"远程启动管理器"，步骤为："开始"·"程序"·"管理工具（公用）"·"远程启动管理器"。

（2）选择菜单"配置"·"检查配置"，然后单击"是"。

（3）选择菜单"远程启动"·"新的配置文件"选择"NE-95-BOOT"，配置名键入"95RPL"。

5．安装 SBS 服务器（Server-Based Setup）

（1）在 NT Server 服务器 C 盘上建立一目录"95SHARE"，并将之设为共享，共享名为"95SHARE"。

（2）启动一台真正的 Windows 95（有盘站），以具有系统管理员权限的用户登录到 NT 服务器。

（3）在真正的 Windows 95 下执行 95 安装光盘上的 ADMIN\NETTOOLS\NETSETUP 目录下的 NETSETUP.EXE 文件，出现"服务器安装"对话框时，单击"设置路径"按钮，输入 SBS 服务器上要保存 Windows 95 文件的路径\\ NTSERVER\ 95SHARE，单击"确定"。

（4）单击"安装"在弹出的对话框中指定 Windows 95 安装文件所在路径（例 D:\WIN95）。开始安装，当询问是否要创建安装脚本，选择不创建，输入 Windows 95 标识码，将 Windows 95 文件复制到 NT 服务器中。

（5）在 NT Server 服务器上执行 NT Server 安装光盘的 CLIENTS\RPL\UPDATE\WIN95 目录下 WIN95SRV.BAT 文件。

例：WIN95SRV \\ NTSERVER\95SHARE

6. 开始安装 Windows 95 无盘站

（1）在服务器上创建 Windows 95 工作目录存放路径"95WORK"并使之共享，共享名为"95WORK"。

（2）启动一台 DOS6.22 无盘工作站 USER1 登录到主域 DOMAIN。

（3）映射网络驱动器

NET USE F: \\ NTSERVER\95SHARE

NET USE G: \\ NTSERVER\95WORK

（4）将工作站与服务器时间同步，执行 C:\>NET TIME \\ NTSERVER /SET /YES。

（5）在 F 盘执行 SETUP /T:G:\USER1.TMP 按照画面提示进行安装。

A）当出现"Server-Based Setup"对话框时选"Set up Windows to run from a network server"。

B）当出现"Startup Method"对话框时，选择"Start

需要全本请访问 www.ertongbook.com