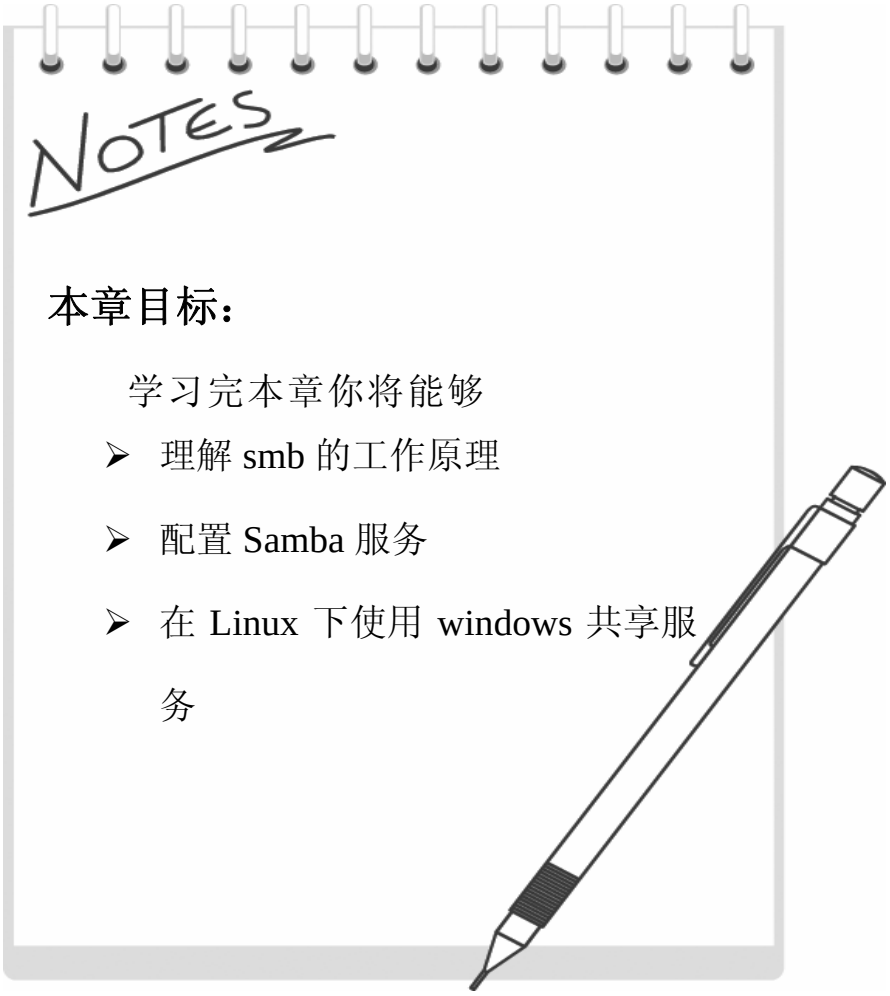
第六章　文件服务器 Samba 的配置

Samba 是一种在 UNIX 环境中运行的免费软件，利用 Samba，Linux 可以创建基于 Windows 的计算机使用共享。另外，Samba 还提供一些工具，允许 Linux 用户从 Windows 计算机进入共享和传输文件。



1. 网上邻居工作原理

网上邻居的工作模式是一个典型的客户端/服务器工作模型，现在，回想一下访问网络邻居的过程，首先，点击网络邻居图标，打开网上邻居列表，其次，点击打开目标服务器图标，列出目标服务器上的共享资源，接下来，点击需要的共享资源图标，进行需要的操作(这些操作包括列出内容，增加，修改或删除内容等。

进当点开网上邻居列表时，这个阶断的实质是列出一个网上的可以访问的服务器的名字列表。在点击一台具体的共享服务器时，这时先发生了一个名字解析过程，我们的电脑会尝试解析名字列表中的这个名称，并尝试进行连接。在连接到该服务器后，我们可以根据服务器的安全设置对服务器上的共享资源进行允许的操作。

下面一步步的来分析这些过程。

1.1 获取网络资源列表

当点击网上邻居图标时，是如何获得当前网络上可以访问的服务器列表的呢?在一个有域的 windows 网络环境下,我们也可以通过活动目录服务来取得这个列表。而在工作组环境中这主要依靠 windows 的浏览服务。

当客户端 A 启动时，如果客户机 A 是域的成员或者有 Wins 服务器，它向域控制器登记自己，或向 Wins 服务器登记自己；如果不是，客户端 A 广播它的名称，当它成功广播自己，并没有其他人和它重名，客户端就登记成功。登记过程如下：

（1）客户端 A 在所有地方广播它自己和它的 NetBIOS 信息 6 到 10 次确保其他网络成员收到信息。(如果有机器没有收到，那该机的网上邻居里就不能看到客户端 A，这也就是为什么在使用 windows 网上邻居时，有时网络是通的，一切配置正常，可是在网上邻居看不到对方的机器。)

（2）如果有另一客户端 B 已用此名，另一客户端 B 发布它自己的广播，包括它正在使用的名字。请求登录的客户端 A 停止所有登记的企图。

（3）无其他客户端反对登记，请求登录的客户端 A 完成登记过程。如果有可用的名称服务器，那么名称服务器会在它的数据库里记上一笔，某机的名称是 A，IP 地址是 XXX.XXX.XXX.XXX

（4）当 A 机正常关机时，重新广播释放刚才注册的这个名字，同一网段上的计算机收到后把这个名字从网上邻居中删除。如果非正常关机，则如果网上有 Wins 服务器的话，客户机非正常关机一定时间以后，Wins 也会注销这个名字；如果没有 wins 服务的话，下次访问 A 服务器时，等待广播应答，没有应答再删除。

在登记完成后，其它计算机中就有了 A 的信息。

如果中途 A 计算机关机了会是什么效果？

这里需要知道的是，浏览服务为各客户机提供的资源列表并不是实时的，也不一定是全局一致的，它依靠每 12 分钟一次的轮询来刷新和同步这个列表，因此，这个列表经常与实际情况不一致。例如：在域环境中，如果域控制器刚确认完 A 主机的信息，A 主机就关机了，那么 A 的资源列表依然存放在域服务器中，其它机器访问网上邻居时，A 主机会被列出，但是不能访问到（废话，已经关机了，当然访问不到）。A 主机要从访问列表中去掉，要等到域控制器（或 Wins 服务器）做下一次轮询时。

1.2 名称解析

当点击网络邻居列表里的一台机器时，这时首先会发生一个名称解析过程。

谈起名称解析，我们常会想到 DNS，事实上，网上邻居的名称解析也是可以使用 DNS 系统的。不过前提是需要架设局域网 DNS 服务器对局域网的各机器名进行解析。

如果没有安装局域网 DNS，也可以使用 NETBIOS 的名字服务还对机器名进行解析，NETBT（TCP/IP 上的 NETBIOS）协议也可以将一台 NETBIOS 机器名解析为 IP 地址，在 windows 下可以用 nbtstat -c 命令查看本机缓存的 NETBIOS 名称和 IP 地址的映射表。也可以使用 nbtstat －r 命令来利用 NETNBT 广播来将指定 NETBIOS 名称解析为 IP 地址。由于广播方式是无法跨子网的，所以当 NETBIOS 要求解析跨子网的名称时，必需要正确设置 WINS 服务器来进行跨网络的 NETBIOS 名称解析。

除以上方式外，网上邻居还允许通过 Lmhost 文件来进行名字解析。

当访问网上邻居时遇到找不到服务器的提示，而又肯定服务器目前是在线的，在排除了网络物理故障的原因后，首先应该考虑的是这是否是名称解析的问题，检查一下网上邻居名称解析相关的各种设置是否正确。（可以直接使用 IP 来访问，看是否成功。）

1.3 网络共享服务的协议和端口

作为网上邻居基础的微软文件和打印服务可以基于多种不同的协议，它们使用不同的端口。

在较早的 WIN98/95 系统下面，主要使用 NETBT(TCP/IP 上的 NETBIOS)协议来完成相关功能，使用 137，138 和 139 端口，同时完成包括列表维护，名称解析和文件传输等多种功能，而 2000 后，网络共享服务也可以通过 TCP/IP 上的 SMB 直接承载实现，使用 445 端口。 名称解析也可以通过 DNS 系统来实现。这样一方面可以

省略 NETBIOS 层，提高工作效率，另一方面免除了 NETBIOS 名称解析引起的广播，减小了网络负荷。但是如果网络中存在一些老版本的 windows 系统或者没有局域网 DNS 服务器，为了名字解析的顺利进行不得不启用 NETBT，否则就只能通过 IP 地址访问网上邻居。

图 6-1 显示了基于 TCP/IP 协议的 windows 文件服务的访问连接：

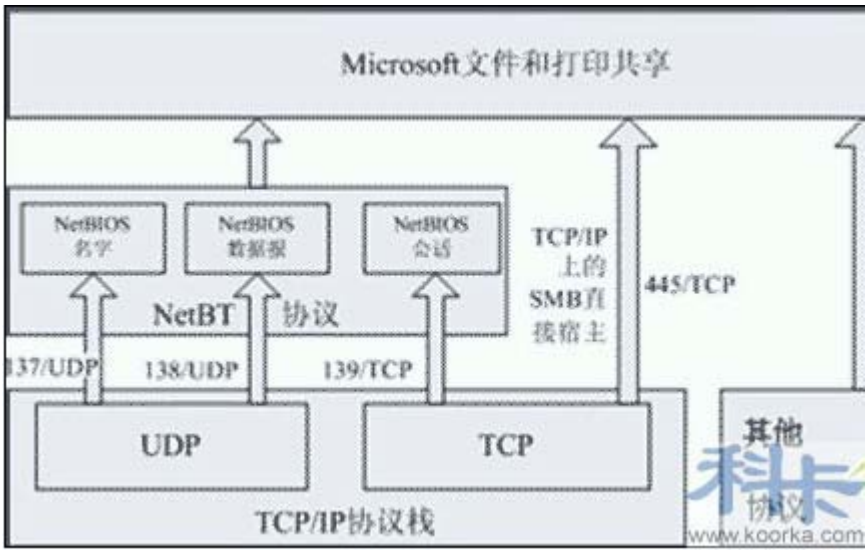


图 6-1

注意：137 端口是 NetBIOS 名称 UDP,138 端口是 NetBIOS 数据报 UDP，139 端口是 NetBIOS 会话 tcp。

1.4 用户身份认证

当客户机发现服务器上的服务与协议都安装正确以后，就开始了用户身份认证过程。也就是确定客户机以什么身份在服务器上进行操作。

关于网上邻居访问过程的身份认证有以下两个原则：

首先是客户机优先以当前登录账户的信息来提交认证信息，例如客户机当前的登录用户为 test，密码为 test，如果这时它访问网上邻居，它用以此为用户名和密码来提交验证信息。

其次，由服务器决定是否将客户机用户身份映射为 guest。

如果 Windows 服务器的本地安全策略——安全选项中“网络访问：本地账户的共享和安全模式”设为仅来宾或者服务器启用了简单文件共享，网络访问的本地用户将以来宾身份验证，这时如果 guest 账户未被禁用，则直接进入下一步本地安全策略验证阶段，如果服务器启用了简单文件共享却没有启用 guest 账户，就会弹出如图 6-2 所示的对话框，用户名为灰色无法更改，密码无论输入什么都无效。

图 6-2

如果服务器上禁用了简单文件共享，或者服务器的本地安全策略——安全选项中的“网络访问：本地账户的共享和安全模式”设为经典，本地账户模式，当客户机连接服务器时，首先以客户机的登录名和密码在服务器上进行验证，如果恰好服务器上存在同名且同密码的账户而且该帐户没有被禁用，客户机将以此用户的身份进入下一本地安全策略的验证阶段；如果服务器上不存在此同名同密码的账户，而服务器上的 guest 账户未被禁用，客户机将以 guest 账户的身分直接进入下一阶段的安全策略验证阶段。如果服务器上禁用了 guest 账户，会弹出要求输入用户名和密码的对话框如图 6-3 所示，这时如果提供了服务器上存在的用户名和密码，则会以此用户的身份进入下一阶段安全策略检查过程。

图 6-3

关于 Windows 的安全策略检查过程，请参考《Windows 系统管理》，它与 Samba 无关，在此不作详细介绍。

1.5 文件权限检查

在通过了本地安全策略检查后，服务器还要检查用户想访问的共享文件夹的共享权限与系统（NTFS）权限是否允许当前登录账户访问。

首先要检查共享权限，然后再检查文件系统权限。用户对该文件（或目录）的有效权限是两个权限的交集。例如，用户 bearzhang 对文件 file1.txt 的共享权限是 r、w、x，在文件系统上的权限是 r，那么最后 bearzhang 对 file2.txt 文件的有效权限是 r。

2. NetBIOS 协议（参考资料）

2.1 简介

Netbios(网络基本输入/输出系统）最初由 IBM,Sytek 作为 API 开发，目的是使用户软件能够使用局域网的资源。自从诞生，Netbois 成为许多其他网络应用程序的基础。严格意义上，Netbios 是接入网络服务的接口标准。

Netbios 原来是作为 THE 网络控制器为 IBM 局域网设计的，是通过特定硬件用来和网络操作系统连接的软件层。Netbios 经扩展，允许程序使用 Netbios 接口来操作 IBM 令牌环结构。Netbios 已被公认为工业标准，通常参照 Netbios-compatible LANs。

它提供给网络程序一套方法，相互通讯及传输数据。基本上，Netbios 允许程序和网络会话。它的目的是把程序和任何类型的硬件属性分开。它也使软件开发员可以免除以下负担：开发网络错误修复，低层信息寻址和路由。使用 Netbios 接口，可以为软件开发员做许多工作。

通过使用 Netbios 的数据报或广播方式，在 Netbios 局域网上的 pc 机建立会话彼此联络。会话允许更多的信息被传送，探测错误，和纠正。通信是在一对一的基础上的。数据报或广播方式允许一台计算机和多台其他的计算机同时通信，但信息大小受限。使用数据报或广播方式没有探测错误和纠正。然而，数据报通信可以不必建立一个会话。

在这种环境下所有的通信以一种称为“网络控制块“的格式提交给 NetBIOS。内存中这些块的分配依赖于用户程序。这些“网络控制块“分配到域中，分别为输入/输出保留。

在当今的环境中，NetBIOS 是使用很普遍的协议。以太网，令牌环，IBM PC 网都支持 NetBIOS。在它原始版本中，它仅作为程序和网络适配器的接口。从那以后，传输类功能加入 NetBIOS，使它功能日益增多。

在 NetBIOS 里，面向连接(tcp)和无连接(udp)通信均支持。它支持广播和复播，支持三个分开的服务：命名,会话，数据报。

2.2 NetBIOS 名称

NetBIOS 名称用来在网络上鉴别资源。程序用这些名称开始和结束会话。你能用多个程序配置一台单独的机器，每个程序都有独特的 NetBIOS 名称。每台支持应用的 pc 机也有用户定义或通过内部方法获得的 NetBIOS 站名。

NetBIOS 能包含至多 16 个阿尔法数字字母。在整个资源路由网络里，字母的组合必须独特。在一台使用 NetBIOS 的 pc 机在网络上能完全工作起来之前，pc 必须先登记 NetBIOS 名称。

NetBIOS 命名允许 16 个字母用在 NetBIOS 名称中。而微软只允许 15 个字母用在 NetBIOS 名称中，第十六个为 NetBIOS 后缀。NetBIOS 后缀用在 Microsoft networking 软件中，区别安装的功能，登记的设备和服务。

2.3 NetBIOS 会话

NetBIOS 会话服务提供给用户程序一种面向连接，可靠的，完全双重的信息服务。NetBIOS 要求一个是客户端程序，一个是服务器端程序。NetBIOS 会话的建立需要双方预定的合作。一个程序必须先发出 listen 命令，其他程序才可以发出 call 命令。listen 命令参考在它的 NetBIOS 名称表中的名称（或 windows 服务器中的），也参考用于作为会话另一端的远端程序的名称。如果聆听者不在聆听，call 命令将不会成功。如果 call 成功，各程序将接到会话 id，以作为会话建立的确认。

send 和 receive 命令操作传输数据。在会话最后，各程序将执行挂起命令。没有为会话服务的实际流控制，因为假定局域网足够快，能够传输需要的数据。

2.4 NetBIOS 数据报

数据报可以发送到特定的地点，或组中所有成员，或广播到整个局域网。与其它数据服务相比，NetBIOS 数据报是无连接，非可靠的。Send_Datagram 命令需要调用者设定目的名。如果目的名是组名，组中每个成员都收到数据。Receive_Datagram 命令的调用者必须确定它接收数据的本地名。除了实际数据外，Receive_Datagram 也返回发送者的名称。如果 NetBIOS 收到数据，但却没有 Receive_Datagram 命令在等待，数据将被丢弃。

Send_Broadcast_Datagram 命令发送信息给本地网上每个 NetBIOS 系统。当

BetBIOS 节点收到广播数据，发布 Receive_Broadcast_Datagram 命令的每个进程都收到数据。如果当广播数据被收到时，没有这些命令在运行，数据将被丢弃。

NetBIOS 使应用程序能和另一个设备建立会话，使网络转发器和处理协议处理收到、发送到另一台机器的请求。NetBIOS 实际上不操作数据。NetBIOS 定义规定了用来到达这些服务的协议的网络接口，而非协议本身。历史上，NetBIOS 曾与叫做 NetBEUI 的协议（网络扩展用户接口）捆绑。接口和协议的结合有时引起混淆，但它们是不同的。

网络协议为定位、连接到网络上特定的服务提供至少一种方法。这通常由将节点和服务名转化为网络地址（名称解析）完成。在连接用 TCP/IP 建立前，NetBIOS 服务名必须解析成 IP 地址。大多数 NetBIOS 的 TCP/IP 实现，用广播或 LMHOSTS 文件完成名称地址的解析。在 Microsoft 环境中，你最可能使用叫做 WINS 的 NetBIOS 名称服务器。

2.5 NetBEUI 解释

NetBEUI 是网络操作系统使用的 NetBIOS 协议的加强版本。它规范了在 NetBIOS 中未标准化的传输帧，还加了额外的功能。传输层驱动器经常被 Microsofts LAN Manager（微软局域网操作器）使用。NetBEUI 执行 OSI LLC2 协议。NetBEUI 是原始的 PC 网络协议和 IBM 为 LanManger（局域网操作器）服务器设计的接口。本协议稍后被微软采用作为它们的网络产品的标准。它规定了高层软件通过 NetBIOS 帧协议发送、接收信息的

方法。本协议运行在标准 802.2 数据链协议层上。

2.6 NetBIOS 范围

NetBIOS 范围 ID 为建立在 TCP/IP（叫做 NBT）模块上的 NetBIOS 提供额外的命名服务。NetBIOS 范围 ID 的主要目的是隔离单个网络上的 NetBIOS 通信和那些有相同 NetBIOS 范围 ID 的节点。NetBIOS 范围 ID 是附加在 NetBIOS 名称上的字符串。两个主机上的 NetBIOS 范围 ID 必须匹配，否则两主机无法通信。NetBIOS 范围 ID 允许计算机使用相同的计算机名，不同的范围 ID。范围 ID 是 NetBIOS 名称的一部分，使名称唯一。

NETBIOS 是不可路由的服务，如果要实现不同网段的主机名服务，需要设置 WINS 来解析。

3. Samba 简介

Samba 是由 Andrew Tridgell 在 1991 年（和 Linux 诞生的时间接近）设计的，当时使用的是 DEC 的 Pathworks 网络，但是他发现无法同时使用 Sun 的 NFS 协议，于是，连 Socket（套接字）都不熟悉的他开始尝试自己在 PC 机上实现 NFS，经过不断的摸索，终于在自己的计算机上实现了 NFS，采用的网络协议是 NetBIOS（因为 NetBIOS 是公开的，可以合法地得到）。到了 1992 年 1 月，他开发出了 0.1 版，称为 Server0.1，随后又开发了一段时间，由于得到了 X 终端，但他放弃了进一步开发 MFS。直到 1992 年底，从一封电子邮件中，Andrew Tridgell 获知了 Linux，一个爱好者将 Server1.0 转换到了 Linux 上，人们很快发现这个程序可以直接使用，应用户的要求，Adrew Tridgell 开始在 Linux 上开发 NFS，同时他发现 smb-server 已经被别人注册了，所以就只好起名为 Samba，这就是 Samba 这个名称的由来。如果感兴趣的话可以访问 http://www.ssc.com/lj/issue7/samba.html 了解这段历史。

1．Samba 服务能够做什么

（1）共享 Linux 磁盘给 Win2000/XP

（2）共享 WinXP/Win2000 磁盘给 Linux 计算机

（3）共享 Linux 打印机给 WinXP/Win2000

（4）共享 WinXP/Win2000 打印机给 Linux 计算机。

2．Samba 的安装

要安装 samba 服务器，可以采用两种方法：从二进制代码安装和从源代码安装。如果干入门，建议使用 RPM 来安装；如果已经入门，建议从源代码来安装。

在 RedHat Linux 系统中，如果下面列出的 3 个软件包都已安装，那么可以开始配置 Samba 服务器了，如果没有安装，请先安装该软件包：

```
[root@koorka ~]# rpm -qa|grep samba
samba-common-3.0.10-1.4E.2
samba-3.0.10-1.4E.2
samba-client-3.0.10-1.4E.2
```

也可以到下面的网址去寻找最新版本：

ftp://metalab.unc.edu/pub/Linux/system/network/samba/

安装的时候，请参考 samba-HOWTO 和软件提供的帮助文件。

Samba 是 SMB 客户程序/服务器软件包，它主要包含以下程序：

SMB 服务器 smbd：为 SMB 客户机如 WindowsXP/2000 等提供 WindowsNT 和

LanManager 风格的文件和打印服务。

Netbios 名字服务器 nmbd：可以提供浏览支持。用户甚至可以用 Samba 作为局域网的主浏览服务器。

SMB 客户程序 smbclient：类似 ftp 程序，用以从 UNIX、Netware 和其他操作系统上访问 SMB 服务器上的资源（如文件、打印机）。

SMB 客户服务程序的 tar 扩展 smbtar：用以方便地拷贝 SMB 服务器上的文件。

在 Linux 上，Samba 还提供了挂卸 SMB 文件系统的工具程序 smbmount（smbmnt）和 smbumount。samba 的内核是 smbd 和 nmbd，如果你用 ps－ef 可以看到这两个进程，那么你的计算机已经在运行 samba 了。

Samba 服务的状态查询、启动和关闭命令分别如下：

#/usr/bin/smbstatus

#/etc/rc.d/init.d/smb start

#/etc/rc.d/init.d/smb stop

4. samba 的配置文件/etc/samba/smb.conf

samba 服务器的配置文件是 smb.conf，在 RedHat 系统中，默认存储在/etc/sambam 目录中。

4.1 常用参数

下面是 Samba 配置文件 /etc/samba/smb.conf 的一些参数说明：
#workgroup=NT 的域名或者工作组名
workgroup=MYGROUP

#server string 等价于 NT 的描述域（description field）
serve rstring=Samba Server

下面的选项对于安全十分重要，它限制连接到当前服务器的本地网络的 IP 地址。下面的例子中，只允许两个 C 类网络地址和本机访问的 SMB 服务器。
;hosts allow=192.168.1.　192.168.2.　127.（允许哪些主机访问）
更多信息，查看 smb.conf 的手册页。如果该选项要激活，把分号去掉。

自动加载打印机，而不是每次单独设置。
printcap name=/etc/printcap（从/etc/printcap 文件中取得打印机的描述信息）

load printers=yes（设置是否自动共享打印机，而不用设置下面的[printer]）

除非你的打印系统的类型不标准，否则不用设置下面的参数，当前支持的打印系统有：bsd，sysv，plp，lprng，aix，hpux，qnx;

printing=lprng（定义打印系统的类型）

如果希望建立游客账号，激活此选项，同时把此账号添加到/etc/passwd 文件中，否则使用用户“nobody”作为游客账号。

;guest account=pcguest

对从不同计算机建立的连接建立不同的日志文件。

log file=/var/log/samba/log.%m（定义日志文件的位置）

限制日志文件的最大尺寸（单位是 KB）。

max log size=50

安全模式，大多数用户希望用户级的安全，详细信息参考 security_level.txt 文件。

security=user

定义 Samba 的安全级别，按从低到高分为四级：share，user，server，domain。它们对应的验证方式如下：

share：没有安全性的级别，任何用户都可以不要用户名和口令访问服务器上的资源。

user：samba 的默认级别，要求用户在访问共享资源之前资源必须先提供用户名和密码进行验证。

server：和 user 安全级别类似，但用户名和密码是递交到另外一个服务器上去验证（比如递交给一台 NT 服务器），如果递交失败，就退到 user 安全级。

Domain：这个安全级别要求网络上存在一台 Windows 的主域控制器，samba 把用户名和密码递交给它去验证。

后面三种安全级都要求用户在本 Linux 计算机上也要系统帐户。否则是不能访问的。

当 security=server 时使用口令服务器选项。

;password server=（NT 服务器的名称）

输入口令应该和真实口令的前面 Password Level 个字符相符合，输入用户名应该和真实用户名的前面 username level 个字符相符合。

;password level=8

;username level=8

用户可能需要使用口令加密，在使用下面的选项之前，请仔细阅读 ENCRYPTION.txt、Win95.txt 和 WinNT.txt 文件。用户密码文件可以存放在/etc/passwd 文件中。

encrypt passwords=yes（因为 windows98 以后都采用加密传输，建议设为 yes）

smb passwd file=/etc/samba/smbpasswd

;ssl CA certFile=/usr/share/ssl/certs/ca-bundle.crt

（当 samba 编译的时候支持 SSL 的时候，需要指定 SSL 的证书的位置）

如果要允许在 Windwos 中的密码改动更新 Linux 系统的密码，就需要下面的选项。

;UNIX password sync=Yes;

;passwd program=/usr/bin/passwd%u;

;passwd chat= *New*UNIX*password* %n *ReType*new*UNIX*password* %n *passwd: *all*authentication*tokens*updated*successfully*

UNIX 用户可以映射成不同 SMB 用户名。

;username map=/etc/samba/smbusers

对每个不同的客户机使用不同的配置文件，%m 代表客户机的 Netbios 名字。

;include=/etc/samba/smb.conf.%m

下面的选项可以提高服务器的性能，特别是使用 smbmount 挂卸 SMB 文件系统时，参考 speed.txt 文件。

Socket options=TCP_NODELAYSO_RCVBUF=8192SO_SNDBUF=8192

如果 SMB 服务器使用了多个网卡，必须在下面列出并进行配置。

;interfaces=192.168.12.2/24 192.168.13.2/24

;remote browse sync=192.168.3.25 192.168.5.255

（这里指定浏览列表同步信息从哪里取得）

;remote announce=192.168.1.255 192.168.2.44

（指定这些计算机向网络宣告自己，而不是有 Browser 得到）

浏览器控制选项。如果你不想让 Samba 服务器成为网络中的主浏览器，那么 local master 设置为 no，否则设置为 yes（此时将参加主浏览器的竞争）。

;local master=no

竞争主浏览器时对自身的评价。

;os level=33

只有在网络中已经安装了一个 NT server 并且已经设置为主域控制器，才使用此项。

;domain controller=

如果你想让 Samba 成为 windows95 工作站的域登录服务器，打开此选项。

;domain logons=yes

如果你打开了 domain logons 选项，你可能想为每台计算机或每个用户创建一个登录脚本，为每个工作站（计算机）创建一个登录脚本。

;logon script=%m.bat

为每个用户创建登录脚本。

;logon script=%U.bat

Windows 的 Internet 命名服务支持区段，WINS 支持要求 Samba 的 nmbd 进程激活 WINS 服务。

;wins support=yes

WINS 服务器—要求 Samba 的 nmbd 进程成为一个 WINS 客户。注意：Samba 可以成为一个 WINS 服务器或者客户，但是不能同时为服务器和客户

;wins server=w.x.y.z

4.2 共享字段说明

[homes]（用户主目录的定义，当以 guest 身份访问时，此字段并不共享）

comment=Home Directories（指的是对共享的备注）

browseable=no

writable=yes

定义打印机共享，使用 BSD 风格的打印系统不必单独定义每一个打印机。

[printers]

comment=All Printers

path=/var/spool/samba（指明打印的文件队列暂时放到/var/spool/samba 目录下）

browseable=no

guest ok=no（指明游客不能打印）

writable=no

printable=yes（这里的 printable 指明该打印机可以打印）

设置网络用户共享文件的临时区域，每个人可以在这里存放文件供别人使用。

;[tmp]

;comment=Temporary file space

;path=/tmp

;readonly=no

;public=yes

一个共享的目录，普通的访问者只能读，属于 staff 组的用户即可以读又可以写。

;[public]

;comment=Public Stuff

;path=/home/samba

;public=yes

;writable=yes

;printable=no

;writelist=@staff

一个私有的打印机，只供 bearzhang 使用，打印缓存存放在 bearzhang 的主目录 #home directory 里。

注意：bearzhang 必须对打印缓存的目录有写的权限。

;[bearzhangsprn]

;comment=Bearzhang's Printer

;valid users=bearzhang

;path=/homes/bearzhang

;printer=bearzhangs_printer

;public=no

;writable=no

;printable=yes

私有的目录，只供用户 bearzhang 使用，bearzhang 需要对该目录有写的权限。

;[bearzhangsdir]

;comment=Bearzhang's Service

;path=/usr/somewhere/private

;valid users=bearzhang

;public=no

;writable=yes

;printable=no

下面的配置，使得每个不同的计算机都有不同的连接。在 path 参数值后面加上%m，代表计算机名，也就是说，主机 host 会连接到 SMB 服务器的/usr/pc/host 目录上。

;[pchome]

;comment=PC Directories

;path=/usr/pc/%m

;public=no

;writable=yes

一个共享目录，对于所有用户都可读可写。注意：目录中创建的文件属于缺省的用户，所以，所有用户都可以在该目录中修改、删除其他用户的文件。

;[public]

;path=/usr/somewhere/else/public

;public=yes

;only guest=yes

;writable=yes

;printable=no

下面的例子解释了如何共享一个目录，从而两个用户可以在里面放置文件。在

下面的配置中，目录应该是对两个用户可写的，并且有 setuid，当然，也可以设置更多的用户共享这一个目录。

;[myshare]

;comment=Mary'sandBearzhang'sstuff

;path=/usr/somewhere/shared（指定共享的路径）

;validusers=mary bearzhang（指定能够使用该共享资源的用户和组）

;public=no（指明该共享资源是否能使游客帐号访问，这个开关有时候也叫 guest ok，所以，有的配置文件中出现 guest ok=yes，其实和 public=yes 是一样的）

;writable=yes（指定了这个目录缺省是否可写，也可以用 read only=no 来设置为可写）

;printable=no

;create mask=0765（指明新建立文件的属性）

4.3 关键步骤

smb 配置文件的关键部分包括以下几个方面：

- 关于 lmhosts 文件和 WINS

在 Windows 网络中，负责计算机的 netbios name 到 IP 地址转换的服务由 WINS 服务器实现，这种转换的静态地址表叫做 lmhosts，WindowsNT 将其存入.mbd 格式的数据库中，在 Linux 中，要担任 WINS 服务器，就只能靠在/etc 目录下的 lmhosts 文件来实现静态地址的转换。lmhosts 文件的格式和 hosts 文件类似，只是这里输入的是计算机的 netbios 名字，而不是 TCP/IP 网络中的主机名。

要让 Linux 主机担任 WINS 服务器，需激活以下参数：

```
wins support=yes
wins server=w.x.y.z
```

强行给 Linux 主机指定一个 netbios 名字：

```
netbios name=Linux
```

- 对连接主机的限制

要允许 IP 为 192.168.0.x 的主机使用 Samba 服务，激活并设置以下参数：

```
hostsallow=192.168.0. 127.
```

- 对连接用户的限制

要允许用户 user 使用 Samba 服务，激活并设置以下参数：

guestaccount=user

➢ 为了提供最大限度的访问，修改安全模式如下：

security=share

➢ 主浏览器（MainBrowser）

在 Windows 的“网上邻居”中，主浏览器负责维护当前网络中的主机列表，但是往往由于刷新过慢，使得重新启动的 smb 服务看不到效果，以为自己设置的仍然不对，这时可以调整 remotebrowsesync 和 remoteannounce 两个参数。remotebrowsesync 将收集网络中其他计算机的信息，remoteannounce 参数将自己声明给当前的子网。例如：

remotebrowsesync=192.168.0.1　192.168.0.26

remoteannounce=192.168.0.1　192.168.0.9

或者调整：

localmaster=yes

参加网络的主浏览器的竞选，调整

oslevel=65

以确保自己能够竞争成功。如果还看不到 SMB 服务器，就单击“开始”-->“运行”命令，在打开的“运行”对话框的“打开”文本框中输入 SMB 服务器的 netbios 名字，例如：\\Linux，这时候一般就会打开 SMB 服务器了。

➢ 关于密码

让 SMB 服务器支持密文登录，必须启用以下参数：

```
encrypt passwords=yes
smbpasswd file=/etc/samba/smbpasswd
```

以 root 的身份执行 smbpasswd 命令，为已经在/etc/passwd 文件中存在的用户设置 smb 的 password，如：

```
[root@koorka ~]# smbpasswd -a bearzhang
New SMB password:
Retype new SMB password:
Added user bearzhang.
```

```
[root@koorka ~]# cat /etc/samba/smbpasswd
bearzhang:502:44EFCE164AB921CAAAD3B435B51404EE:32ED87BDB5FDC5E9CBA88547376818D4:[U          ]:LCT-4540D858:
```

此后，用户 bearzhang 就可以访问 SMB 服务器的资源了。

- 关于 smb 的重启

前面介绍过启动和停止 Samba 服务的命令，当我们修改过 smb.conf 文件后，一是注意用 testparm 命令来进行语法检查，二是不需要重新启动系统，只要重新启动 smb 服务就可以了。

关于 Samba 的设置有很多技术细节，请仔细查看 smb.conf 的手册页和阅读/usr/share/doc/samba*/目录下面的说明文件。另外，在/usr/share/doc/samba*/examples/目录下，还有很多现成的例子供参考。

5. 配置实例

本节以实例的形式介绍 Samba 的应用和实现方法。

学院共分五个部门：教学部、市场部、办公室、后勤部和财务部。为学校建立一个文件共享服务器，要求如下：

1．每个用户可以将自己的工作文件存放到用户主目录中。

2．为每个部门创建一个共享文件夹，该部门的员工可以读写该文件夹，其他部门的员工无权访问。

3．创建一个共享目录 share，使学校内的所有员工都可以读取上面的文件，但是只有办公室主任和教学总监可以往上面存放文件。

4．校长对各部门共享的目录及 share 目录有读写权限。

各部门用户情况如下：

用户组：

教学部：teach

市场部：market

办公室：office

后勤部：logistics

财务部：finance

部门主管：

校长：schoolmaster

教学总监：teachmaster

办公室主任：officemaster

市场总监：marketmaster

后勤主管：logisticmaster

财务总监：financemaster

其他用户：

教学部：john，bear……

市场部：bill，pool……

办公室：lily，anly……

后勤部：jaja……

财务部：

分析：为了方便管理，在创建用户时把 schoolmaster 放入每一个部门的用户组，将每个部门共享目录的拥有者设置为部门主管，各部门共享目录的系统权限设置为 770，将学校的共享目录 share 的拥有者设置为 schoolmaster，属组也设置为 schoolmaster，系统权限设置为 775，并把 teachmaster 和 officemaster 两个用户加入到 schoolmaster 组。

具体操作步骤如下：

1．为各部门创建用户组

分别创建用户组：teach、market、office、logistic、finance。

```
#groupadd teach
#groupadd market
#groupadd office
#groupadd logistic
#groupadd finance
#groupadd schoolmaster
```

2．创建用户

使同一部门的用户属于同一用户组，例如 john 属于 teach 组，bill 属于 market 组。为安全起见，不要给用户设置交互的环境，即将它们的 shell 设置为假，例如 /bin/newshell。

```
#useradd –s /bin/newshell –g schoolmaster –G teach,market,office,logistic,finance schoolmaster
#useradd –s /bin/newshell –g teach –G schoolmaster teachmaster
```

```
#useradd –s /bin/newshell –g market marketmaster
#useradd –s /bin/newshell –g office –G schoolmaster officemaster
#useradd –s /bin/newshell –g logistic logisticmaster
#useradd –s /bin/newshell –g finance financemaster
#useradd –s /bin/newshell –g teach john
#useradd –s /bin/newshell –g teach bear
#useradd –s /bin/newshell –g market bill
#useradd –s /bin/newshell –g market pool
#useradd –s /bin/newshell –g office lily
#useradd –s /bin/newshell –g office anly
#useradd –s /bin/newshell –g logistic jaja
……
```

3．创建共享目录

为各部门创建共享目录，并使该目录的拥有者为部门领导。

（1）在/mnt 目录下创建目录 disk，并将其权限设置为 777，使每个人都有读和写的权限。

```
#mkdir /mnt/disk
#chmod 777 /mnt/disk
```

（2）在/mnt/disk 目录下创建全校的共享目录 share，并将其拥有者改为 schoolmaster，属组改为 schoolmaster，权限设置为 775

```
#mkdir /mnt/disk/share
#chown schoolmaster.schoolmaster /mnt/disk/share
#chmod 775 /mnt/disk/share
```

（3)在/mnt/disk 目录下创建各部门的共享目录,并将其拥有者设置为部门领导，属组设置为部门的用户组，权限设置为 770。

```
#mkdir /mnt/disk/teach
#chown teachemaster.teach /mnt/disk/teach
#chmod 770 /mnt/disk/teach
```

同样方法建立/mnt/disk 下的 market、office、logistic、finance 目录。

4．编辑/etc/samba/smb.conf 文件。

（1）设置工作组名：

```
workgroup = MYGROUP
```

（2）设置主机的 NetBIOS 名：

```
netbios name =file server
```

（3）设置安全级别：

```
security = user
```

（4）设置密码传输方式，并指定 smb 口令存放的文件和位置：

```
encrypt passwords = yes
smb passwd file = /etc/samba/smbpasswd
```

5．设置共享目录。

（1）用户主目录的共享：

```
[homes]
    comment = Home Directories
    browseable = no
    writable = yes
    valid users = %S
    create mode = 0664
    directory mode = 0775
```

（2）学校公共文件的共享：

```
[share]
    comment = for all user
    path = /mnt/disk/share
    valid users = @teach @office @market @logistic @finance @schoolmarket
    public = no
    writable = yes
    write list = teachmaster officemaster schoolmaster
    printable = no
    create mask = 0765
```

（3）教学部共享目录的共享：

```
[teach]
    comment = for teach’s user
    path = /mnt/disk/teach
    valid users = @teach
    public = no
    writable = yes
    printable = no
    create mask = 0765
```

（4）市场部公共目录的共享：

```
[market]
    comment = for market’s user
    path = /mnt/disk/market
    valid users = @market
    public = no
    writable = yes
```

```
    printable = no
    create mask = 0765
```

（5）参照步骤（4）的方法分别设置其它部门的共享目录。

6．设置 smb 用户的口令。

```
#smbpasswd –a schoolmaster
#smbpasswd –a teachmaster
#smbpasswd –a john
……
```

7．启动 smb 服务。

```
#/etc/rc.d/init.d/smb start
```