系统管理指南：网络服务

文件号码 E22299
2011 年 8 月

ORACLE

120418@25097

目录

图

表

示例

前言

《系统管理指南：网络服务》是多卷集的一部分，该多卷集包含 Oracle Solaris 系统管理信息的重要部分。本书假设您已经安装了 Oracle Solaris 10 操作系统，并且设置了计划使用的所有网络软件。

注 – 此 Oracle Solaris 发行版支持使用 SPARC 和 x86 系列处理器体系结构的系统。支持的系统可以在 Oracle Solaris OS: Hardware Compatibility Lists（Oracle Solaris OS：硬件兼容性列表）中找到。本文档列举了在不同类型的平台上进行实现时的所有差别。

在本文档中，这些与 x86 相关的术语表示以下含义：

- x86 泛指 64 位和 32 位的 x86 兼容产品系列。
- x64 特指 64 位的 x86 兼容 CPU。
- “32 位 x86”指出了有关基于 x86 的系统的特定 32 位信息。

有关支持的系统，请参见Oracle Solaris OS: Hardware Compatibility Lists（Oracle Solaris OS：硬件兼容性列表）。

目标读者

本书适用于所有负责管理一个或多个运行 Solaris 10 发行版的系统的人员。要使用本书，您应当具备一到两年的 UNIX 系统管理经验。参加 UNIX 系统管理培训课程可能会对您有所帮助。

系统管理指南系列书籍的结构

下表列出了系统管理指南系列中各本书包含的主题。

书名	主题
《系统管理指南：基本管理》	用户帐户和组、服务器和客户机支持、关闭和启动系统、管理服务以及管理软件（软件包和修补程序）
《系统管理指南：高级管理》	终端和调制解调器、系统资源（磁盘配额、记帐和 crontab）、系统进程以及 Oracle Solaris 软件问题故障排除

书名	主题
《系统管理指南：设备和文件系统》	可移除介质、磁盘和设备、文件系统以及备份和还原数据
《系统管理指南：IP 服务》	TCP/IP 网络管理、IPv4 和 IPv6 地址管理、DHCP（动态主机配置协议）、Ipsec（Internet 协议安全）、IKE（Internet 密钥交换）、Solaris IP 过滤器、移动 IP、IP 网络多路径 (IP network multipathing, IPMP) 以及 IPQoS
《系统管理指南：名称和目录服务（DNS、NIS 和 LDAP）》	DNS、NIS 和 LDAP 命名和目录服务，包括从 NIS 转换到 LDAP 以及从 NIS+ 转换到 LDAP
《System Administration Guide: Naming and Directory Services (NIS+)》	NIS+ 命名和目录服务
《系统管理指南：网络服务》	Web 高速缓存服务器、与时间相关的服务、网络文件系统（NFS 和 Autofs）、邮件、SLP 和 PPP
《系统管理指南：打印》	打印主题和任务，使用服务、工具、协议和技术来设置及管理打印服务和打印机
《系统管理指南：安全性服务》	审计、设备管理、文件安全、BART、Kerberos 服务、PAM、Solaris 加密框架、权限、RBAC、SASL 和 Solaris 安全 Shell
《系统管理指南：Oracle Solaris Containers－资源管理和 Oracle Solaris Zones》	资源管理主题项目和任务、扩展记帐、资源控制、公平份额调度器 (fair share scheduler, FSS)、使用资源上限设置守护进程 (rcapd) 的物理内存控制，以及资源池；使用 Solaris Zones 软件分区技术和 `lx` 标记区域的虚拟功能
《Oracle Solaris ZFS 管理指南》	ZFS（Zettabyte 文件系统）存储工具以及文件系统的创建和管理、快照、克隆、备份、使用访问控制列表 (Access Control List, ACL) 保护 ZFS 文件、在安装区域的 Oracle Solaris 系统中使用 ZFS、仿真卷以及故障排除和数据恢复
《Oracle Solaris Trusted Extensions 管理员规程》	特定于 Oracle Solaris Trusted Extensions 功能的系统管理
《Oracle Solaris Trusted Extensions 配置指南》	从 Solaris 10 5/08 发行版开始，介绍如何规划、启用及初始配置 Oracle Solaris Trusted Extensions 功能

相关书籍

以下是本书中引用的相关文档的列表。

- 《系统管理指南：高级管理》
- 《系统管理指南：基本管理》
- 《系统管理指南：IP 服务》
- 《系统管理指南：名称和目录服务（DNS、NIS 和 LDAP）》
- 《System Administration Guide: Naming and Directory Services (NIS+)》

- 《系统管理指南：Oracle Solaris Containers－资源管理和 Oracle Solaris Zones》
- 《系统管理指南：安全性服务》
- 由 Anderson、Bart、Bryan Costales 和 Harry Henderson 合著的UNIX Communications。Howard W. Sams & Company 出版，1987。
- 由 Costales, Bryan 编著的sendmail, Third Edition。O'Reilly & Associates, Inc. 出版，2002。
- 由 Frey、Donnalyn 和 Rick Adams 合著的!%@:: A Directory of Electronic Mail Addressing and Networks。O'Reilly & Associates, Inc. 出版，1993。
- 由 Krol 和 Ed 合著的The Whole Internet User's Guide and Catalog。O'Reilly & Associates, Inc. 出版，1993。
- 由 O' Reilly、Tim 和 Grace Todino 合著的Managing UUCP and Usenet 。O'Reilly & Associates, Inc. 出版，1992。

相关信息

有关 PPPoE 许可条款的信息，请参阅以下位置的相关资料：

/var/sadm/pkg/SUNWpppd/install/copyright

/var/sadm/pkg/SUNWpppdu/install/copyright

/var/sadm/pkg/SUNWpppg/install/copyright

获取 Oracle 技术支持

Oracle 客户可以通过 My Oracle Support 获取电子支持。有关信息，请访问 `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info`，或访问 `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs`（如果您听力受损）。

印刷约定

下表介绍了本书中的印刷约定。

表 P–1 印刷约定

字体或符号	含义	示例
`AaBbCc123`	命令、文件和目录的名称；计算机屏幕输出	编辑 `.login` 文件。 使用 `ls -a` 列出所有文件。 `machine_name% you have mail.`

表 P–1 印刷约定 （续）

字体或符号	含义	示例
AaBbCc123	用户键入的内容，与计算机屏幕输出的显示不同	`machine_name% su` `Password:`
aabbcc123	要使用实名或值替换的命令行占位符	删除文件的命令为 `rm` *filename*。
AaBbCc123	保留未译的新词或术语以及要强调的词	这些称为 *Class* 选项。 **注意**：有些强调的项目在联机时以粗体显示。
新词术语强调	新词或术语以及要强调的词	**高速缓存**是存储在本地的副本。 请**勿**保存文件。
《书名》	书名	阅读《用户指南》的第 6 章。

命令中的 shell 提示符示例

下表显示了 Oracle Solaris OS 中包含的缺省 UNIX shell 系统提示符和超级用户提示符。请注意，在命令示例中显示的缺省系统提示符可能会有所不同，具体取决于 Oracle Solaris 发行版。

表 P–2 shell 提示符

shell	提示符
Bash shell、Korn shell 和 Bourne shell	`$`
Bash shell、Korn shell 和 Bourne shell 超级用户	`#`
C shell	`machine_name%`
C shell 超级用户	`machine_name#`

第 1 部 分

网络服务主题

本节对全书进行了概述，并提供有关 NCA 和 NTP 服务的概述、任务和参考信息。

◆ ◆ ◆ 第 1 章

1 网络服务（概述）

本章列出了本书包含的主要主题。此外，还对此发行版包含的 PERL 服务进行了说明。

Oracle Solaris 10 Update 10 发行版的主题

本书介绍以下服务和实用程序：

第 42 页中的 “Perl 5”	实用摘录与报告语言 (Practical Extraction and Report Language, Perl) 是一种工具，它可以生成用以辅助完成系统管理任务的脚本。
第 2 章，管理 Web 高速缓存服务器	NCA（网络高速缓存和加速器）可通过高速缓存 Web 页来改善 Web 服务器性能。
第 3 章，与时间有关的服务	NTP（网络时间协议）和与时间相关的实用程序可为许多系统同步时间。
第 4 章，管理网络文件系统（概述）	NFS（网络文件系统）是一种协议，可以提供从远程主机访问文件系统的功能。
第 7 章，SLP（概述）	SLP（服务定位协议）是一种动态服务搜索协议。
第 12 章，邮件服务（概述）	邮件服务允许在将邮件路由至所需任何网络的同时将邮件发送给一个或多个用户。
第 15 章，Solaris PPP 4.0（概述）	PPP（点对点协议）是一种在远程主机之间提供点对点链接的协议。
第 24 章，UUCP（概述）	UUCP（UNIX 对 UNIX 复制程序）允许主机交换文件。

第 27 章，使用远程系统（概述）	这些命令可用于访问远程系统中的文件。这些命令包括 ftp、rlogin 和 rcp。

Perl 5

此 Solaris 发行版中包括实用摘录与报告语言 (Practical Extraction and Report Language, Perl) 5.8.4，它是一个功能强大的通用编程语言，通常作为免费软件提供。由于 Perl 具有出色的进程、文件和文本处理功能，因此已逐渐成为适用于复杂系统管理任务的标准开发工具。

Perl 5 包括一个可动态装入的模块框架，这样便可为特定任务添加新功能。在网址为 http://www.cpan.org 的综合 Perl 典藏网 (Comprehensive Perl Archive Network, CPAN) 上可以免费获取许多模块。如果要想使用 gcc 从 CPAN 生成并安装附加模块，可以使用 /usr/perl5/5.8.4/bin/perlgcc 脚本来执行此操作。有关详细信息，请参见 perlgcc(1) 手册页。

访问 Perl 文档

此 Solaris 发行版提供了有关 Perl 的几个信息来源。通过以下两种机制可以获得相同的信息。

可以通过向 MANPATH 环境变量中添加 /usr/perl5/man 来访问手册页。以下示例显示了 Perl 概述。

```
% setenv MANPATH ${MANPATH}:/usr/perl5/man
% man perl
```

可以使用 perldoc 实用程序来访问其他文档。以下示例显示相同的概述信息。

```
% /usr/perl5/bin/perldoc perl
```

perl 概述页列出了此发行版包含的所有文档。

Perl 兼容性问题

通常，Perl 的 5.8.4 版本可与以前的版本兼容。脚本不需要重新生成或重新编译便可使用。但是，任何基于 XSUB 的 (.xs) 模块都需要重新编译和重新安装。

Solaris 版本的 Perl 的更改

Solaris 版本的 Perl 编译为可对 malloc 系统、64 位整数和大文件提供支持。此外，还应用了相应的修补程序。有关所有配置信息的完整列表，请查看此命令的结果。

```
% /usr/perl5/bin/perlbug -dv
---
Flags:
    category=
    severity=
---
Site configuration information for perl v5.8.4:
 .
 .
```

使用 `perl -V` 可以生成更短的列表。

◆ ◆ ◆ 第 2 章

管理 Web 高速缓存服务器

本章概述了 Solaris 网络高速缓存和加速器 (Network Cache and Accelerator, NCA)，介绍了 NCA 的使用过程和有关 NCA 的参考资料。此外，还针对 Solaris 10 6/06 发行版介绍了安全套接字层 (Secure Sockets Layer, SSL) 的使用以及使用 SSL 内核代理来改进 SSL 包处理性能的过程。

网络高速缓存和加速器（概述）

Solaris 网络高速缓存和加速器 (Network Cache and Accelerator, NCA) 可通过保留 HTTP 请求期间所访问的 Web 页的内核内部高速缓存来改善 Web 服务器性能。此内核内部高速缓存使用系统内存来显著改善通常由 Web 服务器处理的 HTTP 请求的性能。使用系统内存来保存用于 HTTP 请求的 Web 页会降低内核与 Web 服务器之间的开销，从而可以改善 Web 服务器的性能。NCA 提供一个套接字接口，通过该接口，只需进行最少的修改，任何 Web 服务器都可与 NCA 通信。

从内核内部高速缓存恢复请求页（高速缓存命中）时，性能会得到显著改善。请求页不在高速缓存中（高速缓存未命中）并且必须从 Web 服务器恢复时，性能也会得到显著改善。

此产品设计用于在专用的 Web 服务器上运行。如果在运行 NCA 的服务器上运行其他大型进程，将会出现问题。

NCA 将记录所有高速缓存命中，因此 NCA 提供日志记录支持。此日志以二进制格式存储，以改善性能。`ncab2clf` 命令可用来将日志由二进制格式转换为一般日志格式 (common log format, CLF)。

Solaris 发行版包括以下增强功能：

- 套接字接口。
- 支持向量化的 sendfile，它提供对 AF_NCA 的支持。有关更多信息，请参见 `sendfilev(3EXT)` 手册页。
- 利用 `ncab2clf` 命令的新选项，可以跳过选定日期 (`-s`) 之前的记录并处理指定数量的记录 (`-n`)。
- `ncalogd.conf` 中的 `logd_path_name` 可以指定原始设备、文件或两者的组合。
- 支持 Web 服务器打开多个 AF_NCA 套接字。通过多个套接字，可在一台服务器上运行不同的 Web 服务器。
- 新增一个名为 `/etc/nca/ncaport.conf` 的配置文件。该文件可用来管理 NCA 使用的 IP 地址和端口。您的 Web 服务器可能不提供对 AF_NCA 套接字的本机支持。如果服务器缺少此支持，请使用该文件和 NCA 套接字实用程序库将 AF_INET 套接字转换为 AF_NCA 套接字。

使用安全套接字层协议的 Web 服务器

在 Solaris 10 6/06 发行版中，可将 Apache 2.0 和 Sun Java System Web Server 配置为使用安全套接字层 (Secure Sockets Layer, SSL) 协议。该协议可在两个应用程序之间提供保密性、消息完整性和端点身份验证。为了加速 SSL 流量，已对内核进行更改。

SSL 内核代理实现 SSL 协议的服务器端。该代理通过使用用户级 SSL 库的应用程序为服务器应用程序（如 Web 服务器）提供更好的 SSL 性能。性能提高可能会达到 +35%，这取决于应用程序的工作负荷。

SSL 内核代理支持 SSL 3.0 和 TLS 1.0 协议，以及最常见的加密套件。有关完整列表，请参见 `ksslcfg(1M)` 手册页。该代理可配置为回退到任何不支持的加密套件的用户级 SSL 服务器。

以下过程说明如何配置服务器以使用 SSL 内核代理：

- 第 53 页中的 “如何配置 Apache 2.0 Web 服务器以使用 SSL 内核代理”
- 第 55 页中的 “如何配置 Sun Java System Web Server 以使用 SSL 内核代理”
- 第 56 页中的 “在区域中使用 SSL 内核代理”

管理 Web 高速缓存服务器（任务列表）

下表介绍了使用 NCA 或 SSL 所需的过程。

任务	说明	参考
规划 NCA	要在启用 NCA 之前解决的问题的列表。	第 47 页中的 “规划 NCA”

任务	说明	参考
启用 NCA	启用 Web 服务器中 Web 页的内核内部高速缓存的步骤。	第 48 页中的 “如何启用 Web 页的高速缓存”
禁用 NCA	禁用 Web 服务器中 Web 页的内核内部高速缓存的步骤。	第 51 页中的 “如何禁用 Web 页的高速缓存”
管理 NCA 日志记录	启用或禁用 NCA 日志记录进程的步骤。	第 51 页中的 “如何启用或禁用 NCA 日志记录”
装入 NCA 套接字库	在 AF_NCA 套接字不受支持的情况下使用 NCA 的步骤。	第 52 页中的 “如何装入 Socket Utility Library for NCA”
将 SSL 内核代理用于 Apache 2.0 Web 服务器	将 SSL 内核代理用于 Web 服务器以改善 SSL 包处理的步骤。	第 53 页中的 “如何配置 Apache 2.0 Web 服务器以使用 SSL 内核代理”
将 SSL 内核代理用于 Sun Java System Web Server	将 SSL 内核代理用于 Web 服务器以改善 SSL 包处理的步骤。	第 55 页中的 “如何配置 Sun Java System Web Server 以使用 SSL 内核代理”
将 SSL 内核代理用于本地区域中的 Web 服务器	将 SSL 内核代理用于本地区域中的 Web 服务器的步骤。	第 56 页中的 “在区域中使用 SSL 内核代理”

规划 NCA

以下各节介绍了启动 NCA 服务之前需要解决的问题。

NCA 的系统要求

要支持 NCA，系统必须满足以下要求：

- 必须安装 256 MB 的 RAM。
- 必须安装 Solaris 10 或 9 发行版，或 Solaris 8 升级发行版之一。
- 需支持可对 NCA 提供本机支持的 Web 服务器或为使用 Socket Utility Library for NCA 而修改了启动脚本的 Web 服务器：
  - Apache Web 服务器，随 Solaris 8 升级版、Solaris 9 和 Oracle Solaris 10 发行版一起提供。
  - Sun Java System Web Server
  - 可从 Zeus Technology `http://www.zeus.com` 获得的 Zeus Web 服务器

此产品设计用于在专用的 Web 服务器上运行。如果在运行 NCA 的服务器上运行其他大型进程，将会出现问题。

NCA 日志记录

可将 NCA 服务配置为记录 Web 活动。通常，如果已启用 Web 服务器日志记录，则应启用 NCA 日志记录。

可为门服务器提供守护进程支持的插入库

许多 Web 服务器都使用 AF_INET 套接字。缺省情况下，NCA 使用 AF_NCA 套接字。为更正此情况，提供一个插入库。这一新库在标准套接字库 `libsocket.so` 之前装入。库调用 `bind()` 由新库 `ncad_addr.so` 插入。假设已在 `/etc/nca/ncakmod.conf` 中启用状态。Solaris 9 和 Solaris 10 发行版所包含的 Apache 的版本已设置为调用此库。如果您使用的是 IWS 或 Netscape 服务器，请参见第 52 页中的 “如何装入 Socket Utility Library for NCA”以使用新库。

多个实例支持

安装了 NCA 的系统通常需要运行多个 Web 服务器实例。例如，一个服务器可能需要既支持用于外部访问的 Web 服务器，又支持 Web 管理服务器。要分隔这些服务器，需要将每个服务器配置为使用单独的端口。

管理 Web 页的高速缓存（任务）

以下各节介绍了启用或禁用服务的各个部分的过程。

▼ 如何启用 Web 页的高速缓存

1 **成为超级用户或承担等效角色。**

角色包含授权和具有特权的命令。有关角色的更多信息，请参见《系统管理指南：安全性服务》中的“配置 RBAC（任务列表）”。

2 **注册接口。**

在 `/etc/nca/nca.if` 文件中键入每个物理接口的名称。有关更多信息，请参见 `nca.if(4)` 手册页。

```
# cat /etc/nca/nca.if
hme0
hme1
```

每个接口都必须有一个附带的 `hostname.`*interface-name* 文件，并在 `/etc/hosts` 文件中具有一个表示 `hostname.`*interface-name* 内容的项。要在所有接口中都启动 NCA 功能，请在 `nca.if` 文件中放置一个星号 `*`。

3 **启用 ncakmod 内核模块。**

将 /etc/nca/ncakmod.conf 中的 status 项更改为 enabled。

```
# cat /etc/nca/ncakmod.conf
#
# NCA Kernel Module Configuration File
#
status=enabled
httpd_door_path=/var/run/nca_httpd_1.door
nca_active=disabled
```

有关更多信息，请参见 ncakmod.conf(4) 手册页。

4 **可选启用 NCA 日志记录。**

将 /etc/nca/ncalogd.conf 中的 status 项更改为 enabled。

```
# cat /etc/nca/ncalogd.conf
#
# NCA Logging Configuration File
#
status=enabled
logd_path_name="/var/nca/log"
logd_file_size=1000000
```

可通过更改 logd_path_name 项表示的路径来更改日志文件的位置。日志文件可以是原始设备或文件。有关 NCA 日志文件路径的样例，请参见以下示例。有关配置文件的更多信息，请参见 ncalogd.conf(4) 手册页。

5 **可选为多个实例支持定义端口。**

在 /etc/nca/ncaport.conf 文件中添加端口号。此项将使 NCA 在所有已配置的 IP 地址中监视端口 80。

```
# cat /etc/nca/ncaport.conf
#
# NCA Kernel Module Port Configuration File
#
  .
  .
ncaport=*/80
```

6 **仅适用于 x86：增加虚拟内存大小。**

使用 eeprom 命令设置系统的 kernelbase。

```
# eeprom kernelbase=0x90000000
# eeprom kernelbase
kernelbase=0x90000000
```

第二个命令用于验证已设置的参数。

注 – 通过设置 kernelbase，可将用户进程可以使用的虚拟内存量减小至 3 GB 以下。此限制意味着系统与 ABI 不兼容。引导系统时，控制台会显示一条警告消息，指明不兼容。大多数程序实际需要的虚拟地址空间都不到 3 GB。如果某一程序需要 3 GB 以上的虚拟地址空间，则需在未启用 NCA 的系统中运行该程序。

7 重新引导服务器。

示例 2–1 使用原始设备作为 NCA 日志文件

ncalogd.conf 中的 logd_path_name 字符串可将原始设备定义为存储 NCA 日志文件的位置。使用原始设备的优点在于，访问原始设备的开销很小，因此服务可以运行得更快。

NCA 服务将测试文件中列出的所有原始设备，以确保没有使用任何文件系统。此测试可确保不会意外重写任何活动的文件系统。

为了防止此测试找到文件系统，请运行以下命令。此命令将销毁任何磁盘分区中已配置为文件系统的文件系统部分。在此示例中，/dev/rdsk/c0t0d0s7 是正在使用旧文件系统的原始设备。

```
# dd if=/dev/zero of=/dev/rdsk/c0t0d0s7 bs=1024 count=1
```

运行 dd 之后，便可将该原始设备添加到 ncalogd.conf 文件中。

```
# cat /etc/nca/ncalogd.conf
#
# NCA Logging Configuration File
#
status=enabled
logd_path_name="/dev/rdsk/c0t0d0s7"
logd_file_size=1000000
```

示例 2–2 将多个文件用于 NCA 日志记录

ncalogd.conf 中的 logd_path_name 字符串可将多个目标定义为存储 NCA 日志文件的位置。当第一个文件已满时，将使用第二个文件。以下示例显示如何选择先写入 /var/nca/log 文件，然后再使用原始分区。

```
# cat /etc/nca/ncalogd.conf
#
# NCA Logging Configuration File
#
status=enabled
logd_path_name="/var/nca/log /dev/rdsk/c0t0d0s7"
logd_file_size=1000000
```

▼ 如何禁用 Web 页的高速缓存

1 **成为超级用户或承担等效角色。**

角色包含授权和具有特权的命令。有关角色的更多信息，请参见《系统管理指南：安全性服务》中的“配置 RBAC（任务列表）”。

2 **禁用 ncakmod 内核模块。**

将 /etc/nca/ncakmod.conf 中的 status 项更改为 disabled。

```
# cat /etc/nca/ncakmod.conf
# NCA Kernel Module Configuration File
#
status=disabled
httpd_door_path=/var/run/nca_httpd_1.door
nca_active=disabled
```

有关更多信息，请参见 ncakmod.conf(4) 手册页。

3 **禁用 NCA 日志记录。**

将 /etc/nca/ncalogd.conf 中的 status 项更改为 disabled。

```
# cat /etc/nca/ncalogd.conf
#
# NCA Logging Configuration File
#
status=disabled
logd_path_name="/var/nca/log"
logd_file_size=1000000
```

有关更多信息，请参见 ncalogd.conf(4) 手册页。

4 **重新引导服务器。**

▼ 如何启用或禁用 NCA 日志记录

在启用 NCA 之后，可根据需要打开或关闭 NCA 日志记录。有关更多信息，请参见第 48 页中的 “如何启用 Web 页的高速缓存”。

1 **成为超级用户或承担等效角色。**

角色包含授权和具有特权的命令。有关角色的更多信息，请参见《系统管理指南：安全性服务》中的“配置 RBAC（任务列表）”。

2 **更改 NCA 日志记录。**

要永久性地禁用日志记录，需要将 `/etc/nca/ncalogd.conf` 中的状态更改为 `disabled` 并重新引导系统。有关更多信息，请参见 `ncalogd.conf(4)` 手册页。

a. **停止日志记录。**

```
# /etc/init.d/ncalogd stop
```

b. **启动日志记录。**

```
# /etc/init.d/ncalogd start
```

如何装入 Socket Utility Library for NCA

仅当您的 Web 服务器不提供对 AF_NCA 套接字的本机支持时，才应遵循此过程。

在 Web 服务器的启动脚本中，添加一个用于预装库的行。该行应与以下行类似：

```
LD_PRELOAD=/usr/lib/ncad_addr.so /usr/bin/httpd
```

▼ 如何向 NCA 服务中添加新端口

1 **成为超级用户或承担等效角色。**

角色包含授权和具有特权的命令。有关角色的更多信息，请参见《系统管理指南：安全性服务》中的“配置 RBAC（任务列表）”。

2 **添加一个新端口。**

向 `/etc/nca/ncaport.conf` 中添加一个新端口项。此示例在 IP 地址 `192.168.84.71` 中添加端口 `8888`。有关更多信息，请参见 `ncaport.conf(4)`。

```
# cat /etc/nca/ncaport.conf
#
# NCA Kernel Module Port Configuration File
#
  .
  .
ncaport=*/80
ncaport=192.168.84.71/8888
```

3 **启动一个新的 Web 实例。**

地址需要位于包含 NCA 端口配置的文件中，Web 服务器才能将该地址用于 NCA。如果 Web 服务器正在运行，则定义新地址后必须将其重新启动。

▼ 如何配置 Apache 2.0 Web 服务器以使用 SSL 内核代理

应使用此过程来改善 Apache 2.0 Web 服务器上的 SSL 包进程的性能。

开始之前 以下过程要求已安装并配置 Apache 2.0 Web 服务器。发行版中包括 Apache 2.0 Web 服务器。

要使用 SSL 内核代理，服务器私钥和服务器证书需要位于一个文件中。如果只在 `ssl.conf` 文件中指定了 `SSLCertificateFile` 参数，则指定的文件可直接用于内核 SSL。如果还指定了 `SSLCertificateKeyFile` 参数，则需要合并证书文件和私钥文件。合并证书文件和私钥文件的一种方法是运行以下命令：

```
# cat cert.pem key.pem >cert-and-key.pem
```

1. **成为超级用户或承担等效角色。**

   角色包含授权和具有特权的命令。有关角色的更多信息，请参见《系统管理指南：安全性服务》中的“配置 RBAC（任务列表）”。`ksslcfg` 命令包括在 `Network Security`（网络安全性）配置文件中。

2. **停止 Web 服务器。**

   此命令将停止将服务器配置为使用 SMF 运行的系统中的 Web 服务器。

   ```
   # svcadm disable svc:/network/http:apache2
   ```

   如果服务尚未转换，请使用以下命令语法停止该服务：`/usr/apache2/bin/apachectl stop`

3. **确定要用于 `ksslcfg` 命令的参数。**

   `ksslcfg(1M)` 手册页中列出了所有选项。必须了解的参数包括：

   - `key-format`－与 `-f` 选项一起定义证书和密钥格式。对于 SSL 内核代理，该值应为 `pem` 或 `pkcs12`。
   - `key-and-certificate-file`－与 `-i` 选项一起设置存储服务器密钥和证书的文件位置。
   - `password-file`－与 `-p` 选项一起选择文件的位置，该文件中应包括用于加密私钥的口令。此口令用来允许无人参与的重新引导。对该文件的权限应为 `0400`。
   - `proxy-port`－与 `-x` 选项一起设置 SSL 代理端口。请选择标准端口 `80` 之外的其他端口。Web 服务器侦听 SSL 代理端口。
   - `ssl-port`－选择要侦听的 SSL 内核代理的端口。通常，将此参数设置为 `443`。

注 – 不能为 NCA 配置 `ssl-port` 和 `proxy-port` 值，因为 SSL 内核代理以独占方式使用这些端口。通常，端口 80 用于 NCA，端口 8443 用于 `proxy-port`，端口 443 用于 `ssl-port`。

4 创建服务实例。

使用 `ksslcfg` 命令指定 SSL 代理端口和相关参数。

`ksslcfg create -f` *key-format* `-i` *key-and-certificate-file* `-p` *password-file* `-x` *proxy-port ssl-port*

5 验证是否已正确创建该实例。

以下命令报告的服务状态应为 "online"。

```
# svcs svc:/network/ssl/proxy
```

6 配置 Web 服务器以在 SSL 代理端口上侦听。

编辑 `/etc/apache2/http.conf` 文件并添加一行，以定义 SSL 代理端口。如果使用服务器 IP 地址，Web 服务器将只在该接口上侦听。该行应如下所示：

`Listen 0.0.0.0:`*proxy-port*

7 为 Web 服务器设置 SMF 相关性。

Web 服务器只应在 SSL 内核代理实例之后启动。以下命令将建立该相关性。

```
# svccfg -s svc:/network/http:apache2
svc:/network/http:apache2> addpg kssl dependency
svc:/network/http:apache2> setprop kssl/entities = fmri:svc:/network/ssl/proxy:kssl-INADDR_ANY-443
svc:/network/http:apache2> setprop kssl/grouping = astring: require_all
svc:/network/http:apache2> setprop kssl/restart_on = astring: refresh
svc:/network/http:apache2> setprop kssl/type = astring: service
svc:/network/http:apache2> end
```

8 启用 Web 服务器。

```
# svcadm enable svc:/network/http:apache2
```

如果未使用 SMF 启动该服务，请使用以下命令：`/usr/apache2/bin/apachectl startssl`

示例 2–3 配置 Apache 2.0 Web 服务器以使用 SSL 内核代理

以下命令将使用 `pem` 密钥格式创建一个实例。

```
# ksslcfg create -f pem -i cert-and-key.pem -p file -x 8443 443
```

▼ 如何配置 Sun Java System Web Server 以使用 SSL 内核代理

应使用此过程来改善 Sun Java System Web Server 上的 SSL 包进程的性能。有关此 Web 服务器的信息，请参见《Sun Java System Web Server 6.1 2005Q4 SP4 管理员指南》。

开始之前 以下过程要求已安装并配置 Sun Java System Web Server。

1. **成为超级用户或承担等效角色。**

   角色包含授权和具有特权的命令。有关角色的更多信息，请参见《系统管理指南：安全性服务》中的"配置 RBAC（任务列表）"。`ksslcfg` 命令包括在 `Network Security`（网络安全性）配置文件中。

2. **停止 Web 服务器。**

   使用管理员 Web 界面停止服务器。有关更多信息，请参见《Sun Java System Web Server 6.1 2005Q4 SP4 管理员指南》中的 "Starting and Stopping the Server"。

3. **禁用加密框架的 metaslot。**

   需要此步骤以确保在创建内核 SSL 服务实例时已禁用 metaslot。

   ```
   # cryptoadm disable metaslot
   ```

4. **确定要用于 `ksslcfg` 命令的参数。**

   `ksslcfg(1M)` 手册页中列出了所有选项。必须了解的参数包括：

   - `key-format`－与 `-f` 选项一起定义证书和密钥格式。
   - `token-label`－与 `-T` 选项一起指定 PKCS#11 令牌。
   - `certificate-label`－与 `-C` 选项一起选择 PKCS#11 令牌的证书对象中的标签。
   - `password-file`－与 `-p` 选项一起选择文件的位置，该文件中应包括用于使用户登录到 Web 服务器所使用的 PKCS#11 令牌的口令。此口令用来允许无人参与的重新引导。对该文件的权限应为 `0400`。
   - `proxy-port`－与 `-x` 选项一起设置 SSL 代理端口。请选择标准端口 `80` 之外的其他端口。Web 服务器侦听 SSL 代理端口。
   - `ssl-port`－定义要侦听的 SSL 内核代理的端口。通常，将此值设置为 `443`。

   注 – 不能为 NCA 配置 `ssl-port` 和 `proxy-port` 值，因为 SSL 内核代理以独占方式使用这些端口。通常，端口 80 用于 NCA，端口 8443 用于 `proxy-port`，端口 443 用于 `ssl-port`。

5 **创建服务实例。**

使用 `ksslcfg` 命令指定 SSL 代理端口和相关参数。

```
ksslcfg create -f key-format -T PKCS#11-token -C certificate-label -p password-file -x proxy-port ssl-port
```

6 **启用加密框架的 metaslot。**

```
# cryptoadm enable metaslot
```

7 **验证是否已正确创建该实例。**

以下命令报告的服务状态应为 "online"。

```
# svcs svc:/network/ssl/proxy
```

8 **配置 Web 服务器以在 SSL 代理端口上侦听。**

有关更多信息，请参见《Sun Java System Web Server 6.1 2005Q4 SP4 管理员指南》中的 "Adding and Editing Listen Sockets"。

9 **启动 Web 服务器。**

示例 2–4 配置 Sun Java System Web Server 以使用 SSL 内核代理

以下命令将使用 `pkcs11` 密钥格式创建一个实例。

```
# ksslcfg create -f pkcs11 -T "Sun Software PKCS#11 softtoken" -C "Server-Cert" -p file -x 8443 443
```

在区域中使用 SSL 内核代理

SSL 内核代理在区域中工作时具有以下限制：

- 所有内核 SSL 管理都必须从全局区域中执行。全局区域管理员需要访问本地区域证书和密钥文件。使用 `ksslcfg` 命令在全局区域中配置服务实例后，便可以启动本地区域 Web 服务器。
- 通过运行 `ksslcfg` 命令来配置实例时，必须指定特定的主机名或 IP 地址。需要特别指出的是，该实例不能使用 INADDR_ANY。

示例 2–5 在本地区域中配置 Apache Web 服务器以使用 SSL 内核代理

在本地区域中，先停止 Web 服务器。在全局区域中，执行配置服务的所有步骤。要为名为 `apache-zone` 的本地区域创建实例，请使用以下命令：

```
# ksslcfg create -f pem -i /zone/apache-zone/root/keypair.pem -p /zone/apache-zone/root/pass \
    -x 8443 apache-zone 443
```

在本地区域中，运行以下命令，以启用服务实例：

```
# svcadm enable svc:/network/http:apache2
```

高速缓存 Web 页（参考）

以下各节介绍了使用 NCA 所需的文件和组件。而且，还提供了有关 NCA 如何与 Web 服务器交互的特定信息。

NCA 文件

为了支持 NCA 功能，您需要多个文件。其中许多文件是 ASCII 格式的，但也有一些文件是二进制格式的。下表列出了需要的所有文件。

表 2–1 NCA 文件

文件名	功能
`/dev/nca`	NCA 设备的路径名。
`/etc/hostname.*`	可列出服务器中配置的所有物理接口的文件。
`/etc/hosts`	可列出与服务器关联的所有主机名的文件。此文件中的项必须与 `/etc/hostname.*` 文件中的项匹配，NCA 才能起作用。
`/etc/init.d/ncakmod`	用于启动 NCA 服务器的脚本。此脚本在引导服务器时运行。
`/etc/init.d/ncalogd`	用于启动 NCA 日志记录的脚本。此脚本在引导服务器时运行。
`/etc/nca/nca.if`	可列出 NCA 运行所在接口的文件。有关更多信息，请参见 `nca.if(4)` 手册页。
`/etc/nca/ncakmod.conf`	可列出用于 NCA 的配置参数的文件。有关更多信息，请参见 `ncakmod.conf(4)` 手册页。
`/etc/nca/ncalogd.conf`	可列出用于 NCA 日志记录的配置参数的文件。有关更多信息，请参见 `ncalogd.conf(4)` 手册页。
`/etc/nca/ncaport.conf`	可列出用于 NCA 的 IP 地址和端口的文件。有关更多信息，请参见 `ncaport.conf(4)` 手册页。
`/usr/bin/ncab2clf`	用于将日志文件中的数据转换为一般日志格式的命令。有关更多信息，请参见 `ncab2clf(1)` 手册页。
`/usr/lib/net/ncaconfd`	用于配置 NCA 以在引导期间在多个接口上运行的命令。有关更多信息，请参见 `ncaconfd(1M)` 手册页。

表 2–1 NCA 文件 （续）

文件名	功能
/usr/lib/nca_addr.so	使用 AF_NCA 套接字而非 AF_INET 套接字的库。此库必须用在使用 AF_INET 套接字的 Web 服务器上。有关更多信息，请参见 ncad_addr(4) 手册页。
/var/nca/log	保存日志文件数据的文件。该文件为二进制格式，因此不要对其进行编辑。
/var/run/nca_httpd_1.door	门路径名。

NCA 体系结构

NCA 功能包括以下组件。

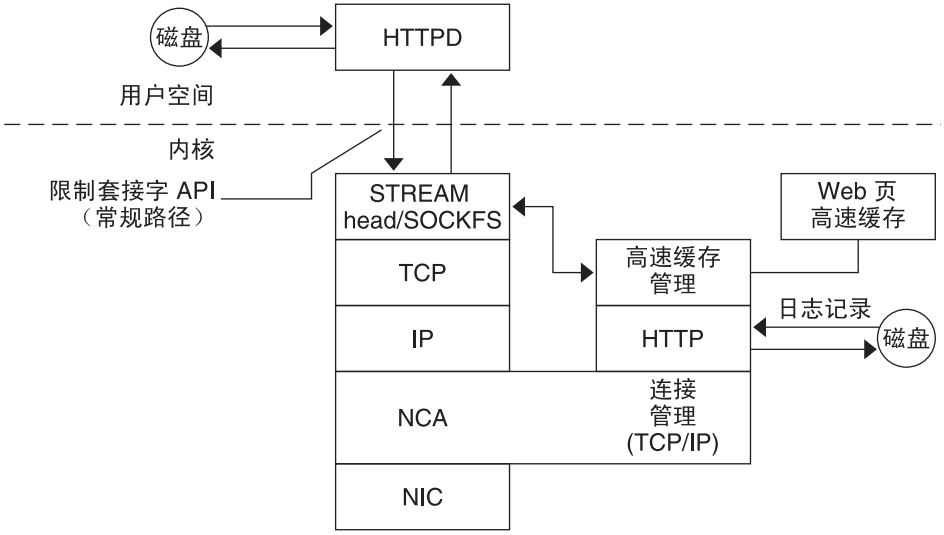
- 内核模块，ncakmod
- Web 服务器，httpd

内核模块 ncakmod 可在系统内存中维护 Web 页的高速缓存。该模块通过套接字接口与 Web 服务器 httpd 通信。系列类型为 PF_NCA。

该内核模块还提供一种可记录所有 HTTP 高速缓存命中的日志记录功能。NCA 日志记录将 HTTP 数据以二进制格式写入磁盘。NCA 提供一种转换实用程序，以将二进制日志文件转换为一般日志格式 (common log format, CLF)。

下图显示了常规路径以及启用 NCA 时所用路径的数据流。

图 2–1 NCA 服务的数据流



NCA 到 Httpd 的请求流

以下列表显示在客户机与 Web 服务器之间的请求流。

1. 从客户机向 Web 服务器发出 HTTP 请求。
2. 如果页面在高速缓存中，则返回内核内部的高速缓存 Web 页。
3. 如果页面不在高速缓存中，则请求转到 Web 服务器，以恢复或更新页面。
4. 根据响应中所用的 HTTP 协议语义，决定是否对页面进行高速缓存。然后将该页面返回客户机。如果 HTTP 请求中包含 Pragma: No-cache 头，页面将不会被高速缓存。

◆ ◆ ◆ 第 3 章

3 与时间有关的服务

许多数据库和验证服务都要求在网络中始终保持系统时钟同步。本章包含以下主题：

时钟同步（概述）

Solaris 软件中包含由特拉华大学开发的网络时间协议 (Network Time Protocol, NTP) 公共域软件。`xntpd` 守护进程设置并维护系统时间。`xntpd` 守护进程完全实现了 RFC 1305 定义的版本 3 标准。

`xntpd` 守护进程在系统启动时读取 `/etc/inet/ntp.conf` 文件。有关配置选项的信息，请参见`xntpd(1M)`。

在网络中使用 NTP 时请记住以下几点：

- `xntpd` 守护进程占用的系统资源非常少。
- NTP 客户机在引导时将自动与 NTP 服务器同步。如果客户机未同步，则客户机与时间服务器通信时将再次重新同步。

同步时钟的另一种方法是在使用 `cron` 的同时运行 `rdate`。

管理网络时间协议（ 任务 ）

以下过程说明如何设置和使用 NTP 服务。

▼ 如何设置 NTP 服务器

1 **成为超级用户或承担等效角色。**

角色包含授权和具有特权的命令。有关角色的更多信息，请参见《系统管理指南：安全性服务》中的“配置 RBAC（任务列表）”。

2 **创建 `ntp.conf` 文件。**

要确保正确执行 `xntpd` 守护进程，必须首先创建 `ntp.conf` 文件。可以将 `ntp.server` 文件用作模板。

```
# cd /etc/inet
# cp ntp.server ntp.conf
```

3 **启动 `xntpd` 守护进程。**

```
# svcadm enable network/ntp
```

▼ 如何设置 NTP 客户机

1 **成为超级用户或承担等效角色。**

角色包含授权和具有特权的命令。有关角色的更多信息，请参见《系统管理指南：安全性服务》中的“配置 RBAC（任务列表）”。

2 **创建 `ntp.conf` 文件。**

要激活 `xntpd` 守护进程，必须首先创建 `ntp.conf` 文件。

```
# cd /etc/inet
# cp ntp.client ntp.conf
```

3 **启动 `xntpd` 守护进程。**

```
# svcadm enable network/ntp
```

使用其他与时间有关的命令（任务）

需要时可以使用以下过程更新当前时间，而不必设置 NTP。

▼ 如何与其他系统同步日期和时间

1. **成为超级用户或承担等效角色。**
   角色包含授权和具有特权的命令。有关角色的更多信息，请参见《系统管理指南：安全性服务》中的“配置 RBAC（任务列表）”。

2. **使用 `rdate` 命令可重置日期和时间，以便与其他系统同步。**
   `# rdate` *another-system*
   another-system　其他系统的名称

3. **确认已使用 `date` 命令正确重置了系统日期。**
   输出中显示的日期和时间应与其他系统的日期和时间一致。

示例 3–1 与其他系统同步日期和时间

以下示例说明了如何使用 `rdate` 使一个系统与另一个系统的日期和时间同步。在本示例中，晚几个小时运行的系统 `earth` 被重置为与服务器 `starbug` 的日期和时间一致。

```
earth# date
Tue Jun  5 11:08:27 MDT 2001
earth# rdate starbug
Tue Jun  5 14:06:37 2001
earth# date
Tue Jun  5 14:06:40 MDT 2001
```

网络时间协议（参考）

为使 NTP 服务运行，需要具备以下文件。

表 3–1 NTP 文件

文件名	功能
`/etc/inet/ntp.conf`	列出 NTP 的配置选项。
`/etc/inet/ntp.client`	NTP 客户机的配置文件样例。
`/etc/inet/ntp.server`	NTP 服务器的配置文件样例。

表 3–1 NTP 文件 （续）

文件名	功能
/etc/inet/ntp.keys	包含 NTP 验证密钥。
/usr/lib/inet/xntpd	NTP 守护进程。有关更多信息，请参见 xntpd(1M)。
/usr/sbin/ntpdate	用于根据 NTP 设置本地日期和时间的实用程序。有关更多信息，请参见 ntpdate(1M)。
/usr/sbin/ntpq	NTP 查询程序。有关更多信息，请参见 ntpq(1M)。
/usr/sbin/ntptrace	用于将 NTP 主机追溯到主 NTP 服务器的程序。有关更多信息，请参见 ntptrace(1M)。
/usr/sbin/xntpdc	xntpd 守护进程的 NTP 查询程序。有关更多信息，请参见xntpdc(1M)。
/var/ntp/ntpstats	用于保存 NTP 统计信息的目录。
/var/ntp/ntp.drift	在 NTP 服务器上设置初始频率偏移。

第 2 部分

访问网络文件系统主题

本节提供NFS服务的概述、任务和参考信息。

◆ ◆ ◆ 第 4 章

管理网络文件系统（概述）

本章概述了可用于通过网络访问文件系统的 NFS 服务。本章论述了了解 NFS 服务所必需的概念，并介绍了 NFS 和 autofs 的最新功能。

注 – 如果系统启用了区域，但您希望在非全局区域中使用此功能，请参见《系统管理指南：Oracle Solaris Containers－资源管理和 Oracle Solaris Zones》以了解更多信息。

NFS 服务的新增功能

本节提供了 Solaris OS 发行版中新增功能的信息。

Solaris 10 11/06 发行版中的变化

Solaris 10 11/06 发行版支持文件系统监视工具。请参见以下内容：

此外，本指南还提供了有关 `nfsmapid` 守护进程的更详细的说明。有关 `nfsmapid` 的信息，请参见以下内容：

有关新增功能的完整列表，请参见《Oracle Solaris 10 8/11 新增功能》。

Solaris 10 发行版中的变化

从 Solaris 10 发行版开始，NFS 版本 4 为缺省版本。有关 NFS 版本 4 的功能及其他变化的信息，请参阅以下内容：

- 第 71 页中的 “NFS 版本 4 协议”
- 第 124 页中的 “`/etc/default/autofs` 文件”
- 第 125 页中的 “`/etc/default/nfs` 文件的关键字”
- 第 128 页中的 “`lockd` 守护进程”
- 第 130 页中的 “`nfs4cbd` 守护进程”
- 第 131 页中的 “`nfsmapid` 守护进程”
- 第 140 页中的 “NFS 文件系统的 `mount` 选项”
- 第 157 页中的 “NFS Over RDMA”
- 第 159 页中的 “NFS 中的版本协商”
- 第 159 页中的 “NFS 版本 4 的功能”
- 第 186 页中的 “Autofs 如何为客户机选择最近的只读文件（多个位置）”

另请参见以下内容：

- 第 86 页中的 “设置 NFS 服务”，可获取任务信息
- 《Oracle Solaris 10 8/11 新增功能》，可获取新增功能的完整列表

此外，还可通过服务管理工具管理 NFS 服务。可以使用 `svcadm` 命令对此服务执行启用、禁用或重新启动等管理操作。可以使用 `svcs` 命令查询该服务的状态。有关服务管理工具的更多信息，请参阅 `smf(5)` 手册页以及《系统管理指南：基本管理》中的第 18 章 “管理服务（概述）”。

NFS 术语

本节介绍使用 NFS 服务时必须了解的一些基本术语。第 6 章，访问网络文件系统（参考）中包括 NFS 服务的扩展适用范围。

NFS 服务器和客户机

术语**客户机**和**服务器**用于说明计算机在共享文件系统时承担的角色。通过网络共享其文件系统的计算机担当服务器。访问文件系统的计算机称为客户机。使用 NFS 服务，任何计算机都可以访问其他任何计算机的文件系统。同时，NFS 服务还提供对其自身文件系统的访问。网络中的计算机可以在任何特定时间承担客户机或服务器的角色，也可以同时承担客户机和服务器的双重角色。

客户机通过挂载服务器的共享文件系统来访问服务器上的文件。客户机挂载远程文件系统时，不会复制该文件系统。不过，挂载进程会使用一系列远程过程调用，客户机将通过这些调用对服务器磁盘上的文件系统进行透明访问。该挂载与本地挂载类似。用户键入命令就像这些文件系统是本地文件系统一样。有关文件系统挂载任务的信息，请参见第 81 页中的 “挂载文件系统”。

通过 NFS 操作在服务器上共享文件系统后，即可从客户机对该文件系统进行访问。可以使用 autofs 自动挂载 NFS 文件系统。有关涉及 share 命令和 autofs 的任务，请参见第 78 页中的 “自动文件系统共享”和第 95 页中的 “Autofs 管理的任务概述”。

NFS 文件系统

可使用 NFS 服务共享的对象包括任何整个或部分目录树或文件分层结构（包括单个文件）。计算机共享的文件分层结构不能与已共享的文件分层结构重叠。不能共享外围设备（如调制解调器和打印机）。

在大多数 UNIX 系统环境中，可共享的文件分层结构与文件系统或部分文件系统对应。但是，NFS 支持可跨多个操作系统运行，并且文件系统的概念在其他非 UNIX 环境中可能是没有意义的。因此，术语**文件系统**是指可使用 NFS 共享和挂载的文件或文件分层结构。

关于 NFS 服务

使用 NFS 服务，不同体系结构的计算机（运行不同的操作系统）可以通过网络来共享文件系统。从 MS-DOS 到 VMS 操作系统的许多平台上都已实现 NFS 支持。

由于 NFS 定义的是抽象的文件系统模型，而不是体系结构规范，因此可以在不同的操作系统上实现 NFS 环境。每个操作系统都会将 NFS 模型应用于其文件系统语义。此模型意味着文件系统操作（如读取和写入）可以正常进行，就像这些操作访问本地文件一样。

NFS 服务具有以下优点：

- 使多台计算机可以使用同一文件，从而使网络中的每个人都可以访问相同的数据
- 通过使计算机共享应用程序而无需每个用户应用程序的本地磁盘空间来降低存储成本
- 实现数据的一致性和可靠性（因为所有的用户都可以读取同一组文件）
- 使文件系统挂载对用户透明
- 使远程文件访问对用户透明
- 支持异构环境
- 减少系统管理开销

NFS 服务使文件系统的物理位置与用户无关。通过使用 NFS 实现，用户无论处于什么位置，都可以查看所有相关的文件。使用 NFS 服务，可以将常用文件的一个副本放在一台计算机的磁盘上，而不是将副本放在每个系统上。所有其他系统将通过网络访问这些文件。在 NFS 操作下，远程文件系统与本地文件系统几乎没有区别。

关于 Autofs

可以使用自动挂载功能挂载通过 NFS 服务共享的文件系统。Autofs（一种客户端服务）是可提供自动挂载功能的文件系统结构。autofs 文件系统通过 `automount` 进行初始化，引导系统时会自动运行该命令。自动挂载守护进程 `automountd` 将持续运行，可根据需要挂载和取消挂载远程目录。

只要运行 `automountd` 的客户机尝试访问远程文件或远程目录，守护进程就会挂载远程文件系统。该远程文件系统可根据需要持续挂载很长时间。如果在一段时间内未访问远程文件系统，则会自动取消挂载该文件系统。

无需在引导时进行挂载，并且用户不再需要知道用于挂载目录的超级用户口令。用户无需使用 `mount` 和 `umount` 命令。autofs 服务会根据需要挂载和取消挂载文件系统，无需用户的任何介入。

使用 `automountd` 挂载某些文件分层结构不会排除使用 `mount` 挂载其他分层结构的可能性。无盘计算机**必须**通过 `mount` 命令和 `/etc/vfstab` 文件来挂载 `/`（根目录）、`/usr` 和 `/usr/kvm`。

有关 autofs 服务的更具体的信息，请参见第 95 页中的 “Autofs 管理的任务概述”和第 182 页中的 “Autofs 如何工作”。

NFS 服务的功能

本节介绍了 NFS 服务中包括的重要功能。

NFS 版本 2 协议

版本 2 曾经是广泛使用的 NFS 协议的第一个版本。版本 2 现在仍可在多种平台上使用。所有的 Solaris 发行版都支持 NFS 协议版本 2，但 Solaris 2.5 之前的 Solaris 发行版仅支持版本 2。

NFS 版本 3 协议

NFS 版本 3 协议的实现是 Solaris 2.5 发行版的一个新增功能。为了提高互操作性和性能，已进行了几处更改。为了获得最佳使用效果，版本 3 协议必须同时在 NFS 服务器和客户机上运行。

与 NFS 版本 2 协议不同，NFS 版本 3 协议可以处理大于 2 GB 的文件。以前的限制已被取消。请参见第 73 页中的 “NFS 大文件支持”。

使用 NFS 版本 3 协议，可在服务器上安全地进行异步写入；该功能允许服务器在内存中高速缓存客户机写入请求，从而提高性能。客户机无需等待服务器将更改提交到磁盘，因此响应时间更快。另外，服务器还可以对请求进行批处理，这样就改进了服务器上的响应时间。

许多 Solaris NFS 版本 3 操作都会返回文件属性，这些属性存储在本地高速缓存中。由于高速缓存更新的频率提高了，因此需要进行单独操作来更新此数据的情况就减少了。因此，对服务器的 RPC 调用的数量也会减少，从而提高了性能。

验证文件访问权限的过程也得到了改进。如果用户尝试在没有适当权限时复制远程文件，版本 2 即会生成“写入错误”消息或“读取错误”消息。在版本 3 中，会在打开文件之前检查权限，因此报告的错误为“打开错误”。

NFS 版本 3 协议取消了 8 KB 传输大小限制。客户机和服务器可以协商它们所支持的任意传输大小，而不用遵循版本 2 强制规定的 8 KB 限制。请注意，在 Solaris 2.5 实现中，协议的传输大小缺省为 32 KB。从 Solaris 10 发行版开始，对线路传输大小的限制更加宽松了。传输大小取决于底层传输的能力。

NFS 版本 4 协议

NFS 版本 4 具有以前版本中未提供的功能。

NFS 版本 4 协议将用户 ID 和组 ID 表示为字符串。客户机和服务器使用 `nfsmapid` 执行以下操作：

- 将这些版本 4 ID 字符串映射为本地数字 ID
- 将本地数字 ID 映射为版本 4 ID 字符串

有关更多信息，请参阅第 131 页中的 “nfsmapid 守护进程”。

请注意，在 NFS 版本 4 中，ID 映射器 `nfsmapid` 用于将服务器上的 ACL 项中的用户 ID 或组 ID 映射为客户机上的 ACL 项中的用户 ID 或组 ID。相反的映射也能实现。有关更多信息，请参见第 166 页中的 “NFS 版本 4 中的 ACL 和 nfsmapid”。

使用 NFS 版本 4 取消共享文件系统时，将破坏该文件系统中任何打开文件或文件锁定的所有状态。在 NFS 版本 3 中，服务器会保留客户机在取消共享文件系统之前获取的任何锁定。有关更多信息，请参阅第 160 页中的 “在 NFS 版本 4 中取消共享和重新共享文件系统”。

NFS 版本 4 服务器使用伪文件系统为客户机提供访问服务器上导出对象的权限。在 NFS 版本 4 之前，伪文件系统不存在。有关更多信息，请参阅第 160 页中的 “NFS 版本 4 中的文件系统名称空间”。

在 NFS 版本 2 和版本 3 中，服务器返回持久性文件句柄。NFS 版本 4 支持可变文件句柄。有关更多信息，请参阅第 162 页中的 “NFS 版本 4 中的可变文件句柄”。

委托是服务器用于将文件委托给客户机进行管理的一项技术，客户机和服务器上均支持该技术。例如，服务器可以授予客户机读取委托或写入委托。有关更多信息，请参阅第 165 页中的 “NFS 版本 4 中的委托”。

从 Solaris 10 发行版开始，NFS 版本 4 不支持 LIPKEY/SPKM 安全风格。

另外，NFS 版本 4 也不使用以下守护进程：

- `mountd`
- `nfslogd`
- `statd`

有关 NFS 版本 4 的完整功能列表，请参阅第 159 页中的 “NFS 版本 4 的功能”。

有关与使用 NFS 版本 4 相关的过程信息，请参阅第 86 页中的 “设置 NFS 服务”。

控制 NFS 版本

`/etc/default/nfs` 文件使用关键字来控制客户机和服务器都使用的 NFS 协议。例如，可以使用关键字来管理版本协商。有关更多信息，请参阅第 125 页中的 “`/etc/default/nfs` 文件的关键字”或 `nfs(4)` 手册页。

NFS ACL 支持

Solaris 2.5 发行版中添加了访问控制列表 (access control list, ACL) 支持。ACL 提供了一种用于设置文件访问权限的机制，该机制比通过标准 UNIX 文件权限提供的机制更加精细。NFS ACL 支持提供了一种将 ACL 项从 Solaris NFS 客户机更改到 Solaris NFS 服务器并查看它们的方法。

NFS 版本 2 和版本 3 协议支持旧的 POSIX 草案样式 ACL。UFS 可本地支持 POSIX 草案 ACL。有关 UFS ACL 的更多信息，请参见《系统管理指南：安全性服务》中的“使用访问控制列表保护 UFS 文件”。

NFS 版本 4 协议支持新的 NFSv4 样式 ACL。ZFS 可本地支持 NFSv4 ACL。对于功能齐全的 NFSv4 ACL 功能，ZFS 必须用作 NFSv4 服务器上的底层文件系统。NFSv4 ACL 具有一组丰富的继承属性，以及一组除标准读取、写入和执行之外的权限位。有关新 ACL 的概述，请参见《Oracle Solaris ZFS 管理指南》中的第 8 章 “使用 ACL 和属性保护 Oracle Solaris ZFS 文件”。有关 NFS 版本 4 中 ACL 支持的信息，请参见第 166 页中的 “NFS 版本 4 中的 ACL 和 `nfsmapid`”。

NFS Over TCP

在 Solaris 2.5 发行版中，NFS 协议的缺省传输协议已更改为传输控制协议 (Transport Control Protocol, TCP)。TCP 有助于提高慢速网络和广域网的性能。TCP 还提供拥塞控制和错误恢复功能。NFS over TCP 可用于版本 2、版本 3 和版本 4。在 Solaris 2.5 发行版之前，缺省的 NFS 协议为用户数据报协议 (User Datagram Protocol, UDP)。

NFS Over UDP

从 Solaris 10 发行版开始，NFS 客户机不再使用过多的 UDP 端口。以前，通过 UDP 进行的 NFS 传送为每个未解决的请求使用单独的 UDP 端口。现在，缺省情况下，NFS 客户机仅使用一个 UDP 保留端口。但是，此支持是可配置的。如果同时使用多个端口会通过增强可伸缩性来提高系统性能，则可将系统配置为使用多个端口。此功能也反映在 NFS over TCP 支持中，这种可配置性是 NFS over TCP 一开始就有的。有关更多信息，请参阅《Oracle Solaris Tunable Parameters Reference Manual》 。

注 – NFS 版本 4 不使用 UDP。如果使用 `proto=udp` 选项挂载文件系统，则会使用 NFS 版本 3 而不是版本 4。

NFS Over RDMA 概述

Solaris 10 发行版包括远程直接内存访问 (Remote Direct Memory Access, RDMA) 协议，这是一种通过高速网络实现内存到内存数据传输的技术。具体来说，RDMA 可提供不受 CPU 干预而直接进出内存的远程数据传输。为提供此功能，RDMA 将 InfiniBand-on-SPARC 平台的互连 I/O 技术与 Solaris 操作系统相结合。有关更多信息，请参阅第 157 页中的 “NFS Over RDMA”。

网络锁定管理器和 NFS

Solaris 2.5 发行版还包括经过改进的网络锁定管理器版本。网络锁定管理器为 NFS 文件提供了 UNIX 记录锁定和 PC 文件共享功能。现在，用于 NFS 文件的锁定机制可靠性提高了，因此使用锁定的命令挂起的可能性也降低了。

注 – 网络锁定管理器仅用于 NFS 版本 2 和版本 3 挂载。文件锁定内置于 NFS 版本 4 协议。

NFS 大文件支持

Solaris 2.6 对 NFS 版本 3 协议的实现经过了更改，可以正确处理大于 2 GB 的文件。NFS 版本 2 协议和 Solaris 2.5 对版本 3 协议的实现不能处理大于 2 GB 的文件。

NFS 客户机故障转移

Solaris 2.6 发行版中添加了只读文件系统的动态故障转移。故障转移可为已复制的只读资源（如手册页、其他文档和共享的二进制文件）提供高级别的可用性。挂载文件系统后，随时可能发生故障转移。现在，手动挂载可以列出多个副本，这与以前发行版中的自动挂载程序非常相似。除了无需等到重新挂载文件系统后再进行故障转移的情况外，自动挂载程序没有变化。有关更多信息，请参见第 84 页中的 “如何使用客户端故障转移”和第 170 页中的 “客户端故障转移”。

对 NFS 服务的 Kerberos 支持

Solaris 2.0 发行版中包括对 Kerberos V4 客户机的支持。在 2.6 发行版中，`mount` 和 `share` 命令已有更改，可以支持使用 Kerberos V5 验证的 NFS 版本 3 挂载。另外，还更改了 `share` 命令，可针对不同的客户机启用多种验证风格。有关涉及安全风格的更改的更多信息，请参见第 74 页中的 “RPCSEC_GSS 安全风格”。有关 Kerberos V5 验证的信息，请参见《系统管理指南：安全性服务》中的“配置 Kerberos NFS 服务器”。

WebNFS 支持

Solaris 2.6 发行版还包括使 Internet 上的文件系统可通过防火墙访问的功能。此功能是通过使用 NFS 协议的扩展实现的。使用 WebNFS 协议进行 Internet 访问的优点之一是该协议的可靠性。该服务是作为 NFS 版本 3 和版本 2 协议的扩展而构建的。此外，WebNFS 实现还提供了在不产生匿名 `ftp` 站点管理开销的情况下共享这些文件的功能。有关与 WebNFS 服务相关的更多更改的说明，请参见第 75 页中的 “WebNFS 服务的安全协商”。有关更多任务信息，请参见第 93 页中的 “WebNFS 管理任务”。

注 – NFS 版本 4 协议优先于 WebNFS 服务。NFS 版本 4 完全集成了已添加到 MOUNT 协议和 WebNFS 服务中的所有安全协商。

RPCSEC_GSS 安全风格

Solaris 7 发行版支持一种名为 RPCSEC_GSS 的安全风格。此风格使用标准的 GSS-API 接口来提供验证、完整性和保密性，并实现了对多种安全机制的支持。有关 Kerberos V5 验证支持的更多信息，请参见第 74 页中的 “对 NFS 服务的 Kerberos 支持”。有关 GSS-API 的更多信息，请参见《Oracle Solaris 开发者安全性指南》。

Solaris 7 对 NFS 挂载的扩展

Solaris 7 发行版包括对 `mount` 命令和 `automountd` 命令的扩展。通过扩展，挂载请求可以使用公共文件句柄，而不使用 MOUNT 协议。MOUNT 协议是 WebNFS 服务使用的同一种访问方法。通过避免使用 MOUNT 协议，可通过防火墙进行挂载。此外，由于服务器与客户机之间需要发生的事务更少，因此挂载速度应该会更快。

通过这些扩展，还可以使用 NFS URL 而不使用标准路径名。另外，也可以使用带有 `public` 选项的 `mount` 命令以及自动挂载程序映射来强制使用公共文件句柄。有关 WebNFS 服务更改的更多信息，请参见第 74 页中的 “WebNFS 支持”。

WebNFS 服务的安全协商

Solaris 8 发行版中添加了一种新的协议，用于使 WebNFS 客户机可与 NFS 服务器协商安全机制。此协议可提供在使用 WebNFS 服务时使用安全事务的功能。有关更多信息，请参见第 173 页中的 “WebNFS 安全协商如何工作”。

NFS 服务器日志记录

在 Solaris 8 发行版中，通过 NFS 服务器日志记录，NFS 服务器可以提供已对其文件系统执行的文件操作记录。该记录包括有关访问哪个文件、何时访问文件以及谁访问文件的信息。可以通过一组配置选项来指定包含此信息的日志位置,也可以使用这些选项来选择应该记录的操作。对于使匿名 FTP 归档文件可用于 NFS 和 WebNFS 客户机的站点而言，此功能特别有用。有关更多信息，请参见第 80 页中的 “如何启用 NFS 服务器日志记录”。

注 – NFS 版本 4 不支持服务器日志记录。

Autofs 功能

Autofs 可用于本地名称空间中指定的文件系统。此信息可以在 NIS、NIS+ 或本地文件中进行维护。

Solaris 2.6 发行版中包括 `automountd` 的完全多线程版本。此增强功能使 autofs 更可靠，并且可以启用多个挂载的并发服务，这可防止服务在服务器不可用时挂起。

新的 `automountd` 还提供了更好的即时挂载功能。如果文件系统具有分层结构关系，则以前的发行版将挂载一组完整的文件系统。现在，仅挂载顶层文件系统。如果需要，可以挂载与此挂载点相关的其他文件系统。

autofs 服务支持间接映射的浏览功能。用户可通过此支持查看可以挂载的目录，而不必实际挂载每个文件系统。`-nobrowse` 选项已添加到 autofs 映射中，因此不能自动浏览大文件系统，如 `/net` 和 `/home`。另外，还可以使用带有 `-n` 选项的 `automount` 命令关闭每个客户机上的 autofs 浏览功能。有关更多信息，请参见第 107 页中的 “禁用 Autofs 浏览功能”。

◆ ◆ ◆ 第 5 章

网络文件系统管理（任务）

本章介绍了有关如何执行设置 NFS 服务、添加要共享的新文件系统和挂载文件系统等 NFS 管理任务的信息。此外，还介绍了如何使用安全 NFS 系统和 WebNFS 功能。本章最后一部分包括故障排除过程以及一些 NFS 错误消息及其含义的列表。

作为 NFS 管理员，您的责任取决于您的站点的要求和您的计算机在网络中的角色。您可能要负责本地网络中的所有计算机，在这种情况下您可能要负责确定以下配置项：

- 哪些计算机应该用作专用服务器
- 哪些计算机应该可同时用作服务器和客户机
- 哪些计算机应该仅用作客户机

设置服务器后对其进行维护涉及以下任务：

- 根据需要共享和取消共享文件系统
- 修改管理文件以更新计算机自动共享或挂载的文件系统列表
- 检查网络状态
- 诊断和解决出现的与 NFS 相关的问题
- 设置对 autofs 的映射

请记住，计算机既可以是服务器，也可以是客户机。因此，计算机可用于与远程计算机共享本地文件系统，并挂载远程文件系统。

注 – 如果系统启用了区域并且您要在非全局区域中使用此功能，请参见《系统管理指南：Oracle Solaris Containers－资源管理和 Oracle Solaris Zones》以了解更多信息。

自动文件系统共享

服务器通过在 NFS 环境中共享其文件系统来提供对这些文件系统的访问。可以使用 `share` 命令或 `/etc/dfs/dfstab` 文件指定要共享的文件系统。

只要启动了 NFS 服务器操作，就会自动共享 `/etc/dfs/dfstab` 文件中的各项。如果需要定期共享同一组文件系统，则应设置自动共享。例如，如果您的计算机是支持起始目录的服务器，则需要使起始目录随时可用。大多数文件系统共享应自动执行。仅在测试或故障排除期间才应手动执行共享。

`dfstab` 文件列出了服务器与其客户机共享的所有文件系统。此文件还对可以挂载文件系统的客户机进行控制。可以修改 `dfstab` 以添加或删除文件系统，或更改进行共享的方式。只需使用受支持的任何文本编辑器（如 `vi`）来编辑文件即可。下次计算机进入运行级 3 时，系统会读取已更新的 `dfstab`，以确定应自动共享的文件系统。

`dfstab` 文件中的每一行都包含 `share` 命令，该命令与在命令行提示符下键入以共享文件系统的命令是同一命令。`share` 命令位于 `/usr/sbin` 中。

表 5–1 文件系统共享任务列表

任务	说明	参考
建立自动文件系统共享	配置服务器以便重新引导服务器时自动共享文件系统的步骤	第 78 页中的 “如何设置自动文件系统共享”
启用 WebNFS	配置服务器以便用户可使用 WebNFS 来访问文件的步骤	第 79 页中的 “如何启用 WebNFS 访问”
启用 NFS 服务器日志记录	配置服务器以便在选定的文件系统上运行 NFS 日志记录的步骤	第 80 页中的 “如何启用 NFS 服务器日志记录”

▼ 如何设置自动文件系统共享

1 **成为超级用户或承担等效角色。**

角色包含授权和具有特权的命令。有关角色的更多信息，请参见《系统管理指南：安全性服务》中的“配置 RBAC（任务列表）”。

2. **为要共享的每个文件系统添加项。**

   编辑 `/etc/dfs/dfstab`。向要自动共享的每个文件系统的文件中添加一个项。各项本身在文件中必须占据一行且使用以下语法:

   ```
   share [-F nfs] [-o specific-options] [-d description] pathname
   ```

   有关 `/etc/dfs/dfstab` 的说明，请参见 `dfstab(4)` 手册页；有关完整的选项列表，请参见 `share_nfs(1M)` 手册页。

3. **共享文件系统。**

   将项添加到 `/etc/dfs/dfstab` 中之后，可通过重新引导系统或使用 `shareall` 命令来共享文件系统。

   ```
   # shareall
   ```

4. **验证信息是否正确。**

   运行 `share` 命令检查是否列出了正确选项：

   ```
   # share
   -        /export/share/man   ro   ""
   -        /usr/src     rw=eng    ""
   -        /export/ftp    ro,public  ""
   ```

另请参见 下一步是设置 autofs 映射，以便客户机可以访问已在服务器上共享的文件系统。请参见第 95 页中的 “Autofs 管理的任务概述”。

▼ 如何启用 WebNFS 访问

从 Solaris 2.6 发行版开始，缺省情况下，可用于 NFS 挂载的所有文件系统都可自动用于 WebNFS 访问。需要使用此过程的唯一条件是以下情况之一：

- 允许在尚未允许 NFS 挂载的服务器上进行 NFS 挂载
- 使用 `public` 选项来重置公共文件句柄以缩短 NFS URL
- 使用 `index` 选项强制装入特定的 HTML 文件

有关在启动 WebNFS 服务之前应考虑的问题的列表，请参见第 94 页中的 “规划 WebNFS 访问”。

1. **成为超级用户或承担等效角色。**

   角色包含授权和具有特权的命令。有关角色的更多信息，请参见《系统管理指南：安全性服务》中的“配置 RBAC（任务列表）”。

2. **使用 WebNFS 服务向要共享的每个文件系统添加项。**

   编辑 `/etc/dfs/dfstab`。向每个文件系统的文件中添加一个项。以下示例中显示的 `public` 和 `index` 标记是可选的。

   ```
   share -F nfs -o ro,public,index=index.html /export/ftp
   ```

有关 /etc/dfs/dfstab 的说明，请参见 dfstab(4) 手册页；有关完整的选项列表，请参见 share_nfs(1M) 手册页。

3 **共享文件系统。**

将项添加到 /etc/dfs/dfstab 中之后，可通过重新引导系统或使用 shareall 命令来共享文件系统。

```
# shareall
```

4 **验证信息是否正确。**

运行 share 命令检查是否列出了正确选项：

```
# share
-       /export/share/man   ro   ""
-       /usr/src     rw=eng   ""
-       /export/ftp    ro,public,index=index.html  ""
```

▼ 如何启用 NFS 服务器日志记录

1 **成为超级用户或承担等效角色。**

角色包含授权和具有特权的命令。有关角色的更多信息，请参见《系统管理指南：安全性服务》中的“配置 RBAC（任务列表）”。

2 **可选更改文件系统配置设置。**

可以采用以下两种方法之一更改 /etc/nfs/nfslog.conf 中的设置。可以通过更改与 global 标记关联的数据来编辑所有文件系统的缺省设置。此外，也可以为此文件系统添加新的标记。如果不需要这些更改，则无需更改此文件。nfslog.conf(4) 中介绍了 /etc/nfs/nfslog.conf 的格式。

3 **使用 NFS 服务器日志记录向要共享的每个文件系统中添加项。**

编辑 /etc/dfs/dfstab。向要启用 NFS 服务器日志记录的文件系统的文件添加一个项。必须在 /etc/nfs/nfslog.conf 中输入 log=*tag* 选项中所使用的标记。本示例使用 global 标记中的缺省设置。

```
share -F nfs -o ro,log=global /export/ftp
```

有关 /etc/dfs/dfstab 的说明，请参见 dfstab(4) 手册页；有关完整的选项列表，请参见 share_nfs(1M) 手册页。

4 **共享文件系统。**

将项添加到 /etc/dfs/dfstab 中之后，可通过重新引导系统或使用 shareall 命令来共享文件系统。

```
# shareall
```

5 **验证信息是否正确。**

运行 share 命令检查是否列出了正确选项：

```
# share
-        /export/share/man   ro   ""
-        /usr/src     rw=eng   ""
-        /export/ftp    ro,log=global  ""
```

6 **检查 NFS 日志守护进程 nfslogd 是否正在运行。**

```
# ps -ef | grep nfslogd
```

7 **可选如果 nfslogd 尚未运行，则启动它。**

- **可选如果存在 /etc/nfs/nfslogtab，请键入以下内容来启动 NFS 日志守护进程：**

  ```
  # svcadm restart network/nfs/server:default
  ```

- **可选如果不存在 /etc/nfs/nfslogtab，请运行任何 share 命令以创建该文件，然后启动守护进程。**

  ```
  # shareall
  # svcadm restart network/nfs/server:default
  ```

挂载文件系统

可以采用多种方法挂载文件系统。引导系统时，根据需要使用命令行或通过自动挂载程序都可以自动挂载文件系统。自动挂载程序提供了在引导时挂载或使用命令行挂载的许多优点。但是，许多情况下需要结合使用所有这三种方法。此外，还存在多种启用或禁用进程的方法，具体取决于挂载文件系统时使用的选项。有关与文件系统挂载关联的任务的完整列表，请参见下表。

表 5–2 挂载文件系统的任务列表

任务	说明	参考
在引导时挂载文件系统	每次重新引导系统时即挂载文件系统的步骤。	第 82 页中的 “如何在引导时挂载文件系统”.
使用命令挂载文件系统	在系统正在运行时挂载文件系统的步骤。此过程在测试时非常有用。	第 82 页中的 “如何通过命令行挂载文件系统”.
使用自动挂载程序挂载	在不使用命令行的情况下根据需要访问文件系统的步骤。	第 83 页中的 “使用自动挂载程序挂载”.
阻止大文件	阻止在文件系统上创建大文件的步骤。	第 83 页中的 “如何在 NFS 服务器上禁用大文件”.
启动客户端故障转移	服务器出现故障时实现自动切换至工作文件系统的步骤。	第 84 页中的 “如何使用客户端故障转移”.

表 5–2 挂载文件系统的任务列表 （续）

任务	说明	参考
禁用对客户机的挂载访问	禁用某台客户机访问远程文件系统的步骤。	第 85 页中的 “如何禁用对某台客户机的挂载访问”.
提供穿过防火墙访问文件系统的权限	允许使用 WebNFS 协议穿过防火墙对文件系统进行访问的步骤。	第 85 页中的 “如何穿过防火墙挂载 NFS 文件系统”.
使用 NFS URL 挂载文件系统	允许使用 NFS URL 来访问文件系统的步骤。此过程允许在不使用 MOUNT 协议的情况下访问文件系统。	第 86 页中的 “如何使用 NFS URL 挂载 NFS 文件系统”.

▼ 如何在引导时挂载文件系统

如果要在引导时挂载文件系统，而不使用 autofs 映射，请遵照以下过程执行操作。必须在每台对远程文件系统具有访问权限的客户机上完成此过程。

1 **成为超级用户或承担等效角色。**

角色包含授权和具有特权的命令。有关角色的更多信息，请参见《系统管理指南：安全性服务》中的“配置 RBAC（任务列表）”。

2 **向 `/etc/vfstab` 中添加文件系统的项。**

`/etc/vfstab` 文件中的各项使用以下语法：

```
special  fsckdev  mountp  fstype  fsckpass  mount-at-boot  mntopts
```

有关更多信息，请参见 `vfstab(4)` 手册页。

注意 – 另外还包含 NFS 客户机 `vfstab` 项的 NFS 服务器必须始终指定 `bg` 选项，以避免系统在重新引导过程中挂起。有关更多信息，请参见第 140 页中的 “NFS 文件系统的 `mount` 选项”。

示例 5–1 客户机的 vfstab 文件中的项

客户机需要从服务器 `wasp` 挂载 `/var/mail` 目录。文件系统需要作为 `/var/mail` 挂载在客户机上，并且客户机需要具有读写访问权限。向客户机的 `vfstab` 文件中添加以下项。

```
wasp:/var/mail - /var/mail nfs - yes rw
```

▼ 如何通过命令行挂载文件系统

为了测试新的挂载点，通常要通过命令行来挂载文件系统。这类挂载允许对不能通过自动挂载程序使用的文件系统进行临时访问。

1. **成为超级用户或承担等效角色。**

   角色包含授权和具有特权的命令。有关角色的更多信息，请参见《系统管理指南：安全性服务》中的“配置 RBAC（任务列表）”。

2. **挂载文件系统。**

   键入以下命令：

   ```
   # mount -F nfs -o ro bee:/export/share/local /mnt
   ```

   在本实例中，服务器 bee 中的 /export/share/local 文件系统挂载在本地系统的只读 /mnt 上。从命令行挂载可临时查看文件系统。可以使用 umount 或通过重新引导本地主机来卸载此文件系统。

注意 – mount 命令的所有版本均不会对无效选项发出警告。该命令将默认忽略所有无法解释的选项。要防止意外行为，请确保验证已使用的所有选项。

使用自动挂载程序挂载

第 95 页中的 “Autofs 管理的任务概述”包括有关使用自动挂载程序来建立和支持挂载的特定说明。在不对普通系统进行任何更改的情况下，客户机应该能够通过 /net 挂载点来访问远程文件系统。要挂载上一个示例中的 /export/share/local 文件系统，请键入以下内容：

```
% cd /net/bee/export/share/local
```

由于自动挂载程序允许所有用户挂载文件系统，因此不需要 root 访问权限。自动挂载程序还提供对文件系统进行自动取消挂载，因此完成后无需取消挂载文件系统。

▼ 如何在 NFS 服务器上禁用大文件

对于支持某些客户机的服务器（这些客户机无法处理超过 2 GB 的文件），可能需要禁用创建大文件的功能。

注 – Solaris 2.6 发行版以前的版本不能使用大文件。如果客户机需要访问大文件，请检查 NFS 服务器的客户机是否正在运行 2.6 发行版（最低版本）。

1. **成为超级用户或承担等效角色。**

   角色包含授权和具有特权的命令。有关角色的更多信息，请参见《系统管理指南：安全性服务》中的“配置 RBAC（任务列表）”。

2. **检查文件系统上是否不存在大文件。**

   例如：

   ```
   # cd /export/home1
   # find . -xdev -size +2000000 -exec ls -l {} \;
   ```

   如果文件系统上存在大文件，则必须删除这些文件或将其移至其他文件系统。

3. **取消挂载文件系统。**

   ```
   # umount /export/home1
   ```

4. **如果已使用 `largefiles` 挂载了文件系统，则重置该文件系统状态。**

   如果文件系统上不存在大文件，则 `fsck` 会重置文件系统状态：

   ```
   # fsck /export/home1
   ```

5. **使用 `nolargefiles` 挂载文件系统。**

   ```
   # mount -F ufs -o nolargefiles /export/home1
   ```

   可以通过命令行进行挂载，但要使选项更为持久，请将类似以下内容的项添加到 `/etc/vfstab` 中：

   ```
   /dev/dsk/c0t3d0s1 /dev/rdsk/c0t3d0s1 /export/home1  ufs  2  yes  nolargefiles
   ```

▼ 如何使用客户端故障转移

1. **成为超级用户或承担等效角色。**

   角色包含授权和具有特权的命令。有关角色的更多信息，请参见《系统管理指南：安全性服务》中的“配置 RBAC（任务列表）”。

2. **在 NFS 客户机上，使用 `ro` 选项挂载文件系统。**

   可以通过命令行、自动挂载程序或通过向 `/etc/vfstab` 中添加类似以下内容的项来挂载：

   ```
   bee,wasp:/export/share/local  -  /usr/local  nfs  -  no  ro
   ```

   自动挂载程序允许使用此语法。但是，文件系统已挂载后不能进行故障转移，仅在选择了服务器时才能进行此操作。

注 – 不能使用命令行或 `vfstab` 项来混用运行不同版本 NFS 协议的服务器。只能使用 autofs 来混用支持 NFS 版本 2、版本 3 或版本 4 协议的服务器。autofs 中会使用版本 2、版本 3 或版本 4 服务器中最适用的一种版本。

▼ 如何禁用对某台客户机的挂载访问

1 **成为超级用户或承担等效角色。**

角色包含授权和具有特权的命令。有关角色的更多信息，请参见《系统管理指南：安全性服务》中的“配置 RBAC（任务列表）”。

2 **在 /etc/dfs/dfstab 中添加一个项。**

第一个示例允许对 eng 网络组中除名为 rose 的主机之外的所有客户机进行挂载访问。第二个示例允许对 eng.example.com DNS 域中除 rose 之外的所有客户机进行挂载访问。

```
share -F nfs -o ro=-rose:eng /export/share/man
share -F nfs -o ro=-rose:.eng.example.com /export/share/man
```

有关访问列表的其他信息，请参见第 148 页中的 “使用 share 命令设置访问列表”。有关 /etc/dfs/dfstab 的说明，请参见 dfstab(4)。

3 **共享文件系统。**

再次共享文件系统或重新引导 NFS 服务器之前，NFS 服务器不会使用对 /etc/dfs/dfstab 所做的更改。

```
# shareall
```

▼ 如何穿过防火墙挂载 NFS 文件系统

要穿过防火墙访问文件系统，请使用以下过程。

1 **成为超级用户或承担等效角色。**

角色包含授权和具有特权的命令。有关角色的更多信息，请参见《系统管理指南：安全性服务》中的“配置 RBAC（任务列表）”。

2 **使用如下命令手动挂载文件系统：**

```
# mount -F nfs bee:/export/share/local /mnt
```

在本示例中，文件系统 /export/share/local 是通过使用公共文件句柄挂载到本地客户机上的。可以使用 NFS URL 来代替标准路径名。如果服务器 bee 不支持公共文件句柄，则挂载操作将会失败。

注 – 此过程要求使用 public 选项来共享 NFS 服务器上的文件系统。此外，客户机与服务器之间的所有防火墙都必须允许在端口 2049 上使用 TCP 连接。共享的所有文件系统都允许公共文件句柄访问，因此缺省情况下将应用 public 选项。

▼ 如何使用 NFS URL 挂载 NFS 文件系统

1. **成为超级用户或承担等效角色。**

   角色包含授权和具有特权的命令。有关角色的更多信息，请参见《系统管理指南：安全性服务》中的“配置 RBAC（任务列表）”。

2. **可选如果使用的是 NFS 版本 2 或版本 3，请使用如下命令手动挂载文件系统：**

   ```
   # mount -F nfs nfs://bee:3000/export/share/local /mnt
   ```

   在本示例中，`/export/share/local` 文件系统是使用 NFS 端口号 `3000` 从服务器 `bee` 中挂载的。端口号不是必需的，缺省情况下会使用标准 NFS 端口号 `2049`。可以选择在 NFS URL 中包括 `public` 选项。如果没有 `public` 选项，则在服务器不支持公共文件句柄的情况下会使用 MOUNT 协议。`public` 选项会强制使用公共文件句柄，如果不支持公共文件句柄，则挂载将失败。

3. **可选如果使用的是 NFS 版本 4，请使用如下命令手动挂载文件系统：**

   ```
   # mount -F nfs -o vers=4 nfs://bee:3000/export/share/local /mnt
   ```

设置 NFS 服务

本节介绍了完成以下操作必须执行的一些任务：

- 启动和停止 NFS 服务器
- 启动和停止自动挂载程序
- 选择不同版本的 NFS

注 – 从 Solaris 10 发行版开始，NFS 版本 4 为缺省版本。

表 5–3 NFS 服务任务列表

任务	说明	参考
启动 NFS 服务器	启动 NFS 服务的步骤（如果该服务尚未自动启动）。	第 87 页中的 “如何启动 NFS 服务”
停止 NFS 服务器	停止 NFS 服务的步骤。通常无需停止该服务。	第 87 页中的 “如何停止 NFS 服务”
启动自动挂载程序	启动自动挂载程序的步骤。更改某些自动挂载程序映射时需要使用此过程。	第 88 页中的 “如何启动自动挂载程序”
停止自动挂载程序	停止自动挂载程序的步骤。更改某些自动挂载程序映射时需要使用此过程。	第 88 页中的 “如何停止自动挂载程序”
在服务器上选择不同版本的 NFS	在服务器上选择不同版本的 NFS 的步骤。如果选择不使用 NFS 版本 4，请使用此过程。	第 88 页中的 “如何在服务器上选择不同版本的 NFS”

表 5–3 NFS 服务任务列表 （续）

任务	说明	参考
在客户机上选择不同版本的 NFS	通过修改 `/etc/default/nfs` 文件在客户机上选择不同版本的 NFS 的步骤。如果选择不使用 NFS 版本 4，请使用此过程。	第 89 页中的 “如何通过修改 `/etc/default/nfs` 文件在客户机上选择不同版本的 NFS”
	使用命令行在客户机上选择不同版本的 NFS 的替代步骤。如果选择不使用 NFS 版本 4，请使用此替代过程。	第 90 页中的 “如何使用 `mount` 命令在客户机上选择不同版本的 NFS”

▼ 如何启动 NFS 服务

1 **成为超级用户或承担等效角色。**

角色包含授权和具有特权的命令。有关角色的更多信息，请参见《系统管理指南：安全性服务》中的“配置 RBAC（任务列表）”。

2 **在服务器上启用 NFS 服务。**

键入以下命令。

```
# svcadm enable network/nfs/server
```

此命令可启用 NFS 服务。

注 – 引导系统时会自动启动 NFS 服务器。此外，引导系统后，可随时通过共享 NFS 文件系统来自动启用 NFS 服务守护进程。请参见第 78 页中的 “如何设置自动文件系统共享”。

▼ 如何停止 NFS 服务

1 **成为超级用户或承担等效角色。**

角色包含授权和具有特权的命令。有关角色的更多信息，请参见《系统管理指南：安全性服务》中的“配置 RBAC（任务列表）”。

2 **在服务器上禁用 NFS 服务。**

键入以下命令。

```
# svcadm disable network/nfs/server
```

▼ 如何启动自动挂载程序

1 **成为超级用户或承担等效角色。**

角色包含授权和具有特权的命令。有关角色的更多信息，请参见《系统管理指南：安全性服务》中的“配置 RBAC（任务列表）”。

2 **启用 autofs 守护进程。**

键入以下命令：

```
# svcadm enable system/filesystem/autofs
```

▼ 如何停止自动挂载程序

1 **成为超级用户或承担等效角色。**

角色包含授权和具有特权的命令。有关角色的更多信息，请参见《系统管理指南：安全性服务》中的“配置 RBAC（任务列表）”。

2 **禁用 autofs 守护进程。**

键入以下命令：

```
# svcadm disable system/filesystem/autofs
```

▼ 如何在服务器上选择不同版本的 NFS

如果选择不使用 NFS 版本 4，请使用此过程。

1 **成为超级用户或承担等效角色。**

角色包含授权和具有特权的命令。有关角色的更多信息，请参见《系统管理指南：安全性服务》中的“配置 RBAC（任务列表）”。

2 **编辑 `/etc/default/nfs` 文件。**

例如，如果要使服务器仅提供版本 3，请将 NFS_SERVER_VERSMAX 和 NFS_SERVER_VERSMIN 的值都设为 3。有关关键字及其值的列表，请参阅第 125 页中的 “`/etc/default/nfs` 文件的关键字”。

```
NFS_SERVER_VERSMAX=value
NFS_SERVER_VERSMIN=value
```

value　　提供版本号。

注 – 缺省情况下，将对这些行加以注释。另外，请记住删除井号 (#)。

---

3 **可选如果要禁用服务器委托，请在 /etc/default/nfs 文件中包括以下行。**

```
NFS_SERVER_DELEGATION=off
```

注 – 在 NFS 版本 4 中，缺省情况下将启用服务器委托。有关更多信息，请参见第 165 页中的 “NFS 版本 4 中的委托”。

---

4 **可选如果要为客户机和服务器设置公共域，请在 /etc/default/nfs 文件中包括以下行。**

NFSMAPID_DOMAIN=*my.comany.com*

my.comany.com　　提供公共域

有关更多信息，请参阅第 131 页中的 “nfsmapid 守护进程”。

5 **检查 NFS 服务是否正在服务器上运行。**

键入以下命令：

```
# svcs network/nfs/server
```

此命令将报告 NFS 服务器服务是处于联机状态还是禁用状态。

6 **可选如有必要，请禁用 NFS 服务。**

如果发现在前面的步骤中 NFS 服务处于联机状态，请键入以下命令来禁用该服务。

```
# svcadm disable network/nfs/server
```

注 – 如果需要配置 NFS 服务，请参阅第 78 页中的 “如何设置自动文件系统共享”。

---

7 **启用 NFS 服务。**

键入以下命令以启用该服务。

```
# svcadm enable network/nfs/server
```

另请参见 第 159 页中的 “NFS 中的版本协商”

▼ 如何通过修改 /etc/default/nfs 文件在客户机上选择不同版本的 NFS

以下过程说明如何通过修改 /etc/default/nfs 文件来控制在客户机上使用的 NFS 版本。如果希望使用命令行，请参阅第 90 页中的 “如何使用 mount 命令在客户机上选择不同版本的 NFS”。

1. **成为超级用户或承担等效角色。**

   角色包含授权和具有特权的命令。有关角色的更多信息，请参见《系统管理指南：安全性服务》中的“配置 RBAC（任务列表）”。

2. **编辑 `/etc/default/nfs` 文件。**

   例如，如果要使客户机上仅提供版本 3，请将 NFS_CLIENT_VERSMAX 和 NFS_CLIENT_VERSMIN 的值都设为 3。有关关键字及其值的列表，请参阅第 125 页中的 “`/etc/default/nfs` 文件的关键字”。

   ```
   NFS_CLIENT_VERSMAX=value
   NFS_CLIENT_VERSMIN=value
   ```

   value　提供版本号。

   注 – 缺省情况下，将对这些行加以注释。另外，请记住删除井号 (#)。

3. **在客户机上挂载 NFS。**

   键入以下命令：

   ```
   # mount server-name:/share-point /local-dir
   ```

   server-name　提供服务器的名称。

   /share-point　提供要共享的远程目录的路径。

   /local-dir　提供本地挂载点的路径。

另请参见 第 159 页中的 “NFS 中的版本协商”

▼ 如何使用 mount 命令在客户机上选择不同版本的 NFS

以下过程说明如何使用 `mount` 命令来控制在客户机上使用的用于进行特定挂载的 NFS 版本。如果希望为客户机挂载的所有文件系统修改 NFS 版本，请参见第 89 页中的 “如何通过修改 `/etc/default/nfs` 文件在客户机上选择不同版本的 NFS”。

1. **成为超级用户或承担等效角色。**

   角色包含授权和具有特权的命令。有关角色的更多信息，请参见《系统管理指南：安全性服务》中的“配置 RBAC（任务列表）”。

2. **在客户机上挂载所需的 NFS 版本。**

   键入以下命令：

   ```
   # mount -o vers=value server-name:/share-point /local-dir
   ```

value	提供版本号。
server-name	提供服务器的名称。
/share-point	提供要共享的远程目录的路径。
/local-dir	提供本地挂载点的路径。

注 – 此命令使用 NFS 协议来挂载远程目录并忽略 `/etc/default/nfs` 文件中的客户机设置。

另请参见 第 159 页中的 “NFS 中的版本协商”

管理安全 NFS 系统

要使用安全 NFS 系统，您负责的所有计算机都必须具有域名。域是一个管理实体，通常包含多台计算机，它是大型网络的一部分。如果运行的是名称服务，则还应为域建立名称服务。请参见《系统管理指南：名称和目录服务（DNS、NIS 和 LDAP）》。

NFS 服务支持 Kerberos V5 验证。《系统管理指南：安全性服务》中的第 21 章 “Kerberos 服务介绍”介绍了 Kerberos 服务。

还可以配置安全 NFS 环境，以使用 Diffie-Hellman 验证。《系统管理指南：安全性服务》中的第 16 章 “使用验证服务（任务）”介绍了此验证服务。

▼ 如何设置使用 DH 验证的安全 NFS 环境

1. **为域指定域名，并使域中的每台计算机都可识别该域名。**
   如果使用 NIS+ 作为名称服务，请参见《系统管理指南：名称和目录服务（DNS、NIS 和 LDAP）》。

2. **使用 `newkey` 或 `nisaddcred` 命令为客户机用户创建公钥和私钥。使每个用户使用 `chkey` 命令建立其各自的安全 RPC 口令。**

注 – 有关这些命令的信息，请参见 `newkey(1M)`、`nisaddcred(1M)` 和 `chkey(1)` 手册页。

生成公钥和私钥后，公钥和已加密的私钥会存储在 `publickey` 数据库中。

3 **验证名称服务是否正在响应。**

如果运行的是 NIS+，请键入以下内容：

```
# nisping -u
Last updates for directory eng.acme.com. :
Master server is eng-master.acme.com.
        Last update occurred at Mon Jun  5 11:16:10 1995

Replica server is eng1-replica-replica-58.acme.com.
        Last Update seen was Mon Jun  5 11:16:10 1995
```

如果运行的是 NIS，请验证 `ypbind` 守护进程是否正在运行。

4 **验证密钥服务器的 `keyserv` 守护进程是否正在运行。**

键入以下命令。

```
# ps -ef | grep keyserv
root    100      1  16    Apr 11 ?        0:00 /usr/sbin/keyserv
root   2215   2211   5  09:57:28 pts/0    0:00 grep keyserv
```

如果守护进程未运行，请键入以下内容以启动密钥服务器：

```
# /usr/sbin/keyserv
```

5 **解密并存储私钥。**

通常，登录口令与网络口令相同。在这种情况下，不需要 `keylogin`。如果口令不同，则用户必须登录，然后运行 `keylogin`。您仍然需要以 `root` 身份使用 `keylogin -r` 命令，将已解密的私钥存储在 `/etc/.rootkey` 中。

注 – 如果 root 私钥发生更改或如果 `/etc/.rootkey` 丢失，则需要运行 `keylogin -r`。

---

6 **更新文件系统的挂载选项。**

对于 Diffie-Hellman 验证，请编辑 `/etc/dfs/dfstab` 文件并向相应项中添加 `sec=dh` 选项。

```
share -F nfs -o sec=dh /export/home
```

有关 `/etc/dfs/dfstab` 的说明，请参见 `dfstab(4)` 手册页。

7 **更新文件系统的自动挂载程序映射。**

编辑 `auto_master` 数据，将 `sec=dh` 作为挂载选项包括在 Diffie-Hellman 验证的相应项中：

```
/home    auto_home    -nosuid,sec=dh
```

注 – Solaris 2.5 前后的发行版有一个限制。如果客户机未安全地挂载安全共享的文件系统，则用户有权以 `nobody` 身份而不是以其自身身份进行访问。对于使用版本 2 的后续发行版，如果安全模式不匹配，NFS 服务器将拒绝访问，除非 `share` 命令行中包括 `-sec=none`。如果使用版本 3，则可从 NFS 服务器中继承该模式，因此客户机无需指定 `sec=dh`。用户有权以其自身身份访问文件。

重新安装、移动或升级计算机时，如果未建立新的密钥或更改了 `root` 的密钥，请记住保存 `/etc/.rootkey`。如果确实删除了 `/etc/.rootkey`，则可以始终键入以下内容：

```
# keylogin -r
```

WebNFS 管理任务

本节提供有关管理 WebNFS 系统的说明。以下是相关任务。

表 5–4 WebNFS 管理的任务列表

任务	说明	参考
规划 WebNFS	启用 WebNFS 服务之前应考虑的问题。	第 94 页中的 “规划 WebNFS 访问”
启用 WebNFS	通过使用 WebNFS 协议来启用 NFS 文件系统挂载的步骤。	第 79 页中的 “如何启用 WebNFS 访问”
启用可穿过防火墙的 WebNFS	允许使用 WebNFS 协议穿过防火墙对文件进行访问的步骤。	第 95 页中的 “如何启用可穿过防火墙的 WebNFS 访问”
使用 NFS URL 进行浏览	有关在 Web 浏览器中使用 NFS URL 的说明。	第 94 页中的 “如何使用 NFS URL 进行浏览”
在 autofs 中使用公共文件句柄	使用自动挂载程序挂载文件系统时强制使用公共文件句柄的步骤。	第 107 页中的 “如何在 Autofs 中使用公共文件句柄”
在 autofs 中使用 NFS URL	向自动挂载程序映射添加 NFS URL 的步骤。	第 107 页中的 “如何在 Autofs 中使用 NFS URL”
提供穿过防火墙访问文件系统的权限	允许使用 WebNFS 协议穿过防火墙对文件系统进行访问的步骤。	第 85 页中的 “如何穿过防火墙挂载 NFS 文件系统”
使用 NFS URL 挂载文件系统	允许使用 NFS URL 来访问文件系统的步骤。此过程允许在不使用 MOUNT 协议的情况下访问文件系统。	第 86 页中的 “如何使用 NFS URL 挂载 NFS 文件系统”

规划 WebNFS 访问

要使用 WebNFS，首先需要能够运行和装入 NFS URL（例如 `nfs://server/path`）的应用程序。下一步是选择可针对 WebNFS 访问导出的文件系统。如果应用程序具有 Web 浏览功能，则通常会使用 Web 服务器的文档根目录。选择要针对 WebNFS 访问导出的文件系统时，需要考虑以下几个因素。

1. 每台服务器都有一个公共文件句柄，缺省情况下该句柄与服务器的根文件系统关联。系统将相对于与公共文件句柄关联的目录确定 NFS URL 中的路径。如果该路径指向导出的文件系统中的一个文件或目录，则服务器将提供访问权限。可以使用 `share` 命令的 `public` 选项将公共文件句柄与特定的导出的目录相关联。使用此选项可使 URL 可相对于共享的文件系统，而不是相对于服务器的根文件系统。根文件系统不允许进行 Web 访问，除非共享根文件系统。
2. 使用 WebNFS 环境，已具有挂载权限的用户可通过浏览器访问文件。无论文件系统是否是使用 `public` 选项导出的，都可启用此功能。由于用户已经通过 NFS 设置拥有了访问这些文件的权限，因此这种访问不会导致任何其他安全风险。如果无法挂载文件系统的用户需要使用 WebNFS 访问权限，只需使用 `public` 选项来共享该文件系统即可。
3. 对公众开放的文件系统比较适于使用 `public` 选项。例如，ftp 归档文件中的顶层目录或 Web 站点的主 URL 目录。
4. 可以使用带有 `index` 选项的 `share` 命令来强制装入 HTML 文件。另外，也可以在访问 NFS URL 时列出目录。

   选定文件系统后，请检查文件并根据需要将访问权限设置为限制查看文件或目录。请根据需要，为正在共享的所有 NFS 文件系统建立权限。对于许多站点，目录的 `755` 种权限和文件的 `644` 种权限可提供正确的访问级别。

   如果要同时使用 NFS URL 和 HTTP URL 访问某个 Web 站点，则需要考虑其他因素。第 174 页中的 “Web 浏览器使用的 WebNFS 限制”中介绍了这些因素。

如何使用 NFS URL 进行浏览

能够支持 WebNFS 服务的浏览器应允许对类似于以下形式的 NFS URL 进行访问：

`nfs://`*server*`<:`*port*`>/`*path*

server　文件服务器的名称

port　要使用的端口号（缺省值为 `2049`）

path　文件的路径，可以相对于公共文件句柄，也可以相对于根文件系统

注 – 在大多数浏览器中，后续事务可以记住前一个事务的 URL 服务类型（例如 `nfs` 或 `http`）。如果装入了包括不同服务类型的 URL，则会出现异常。使用 NFS URL 后，可能会装入对 HTTP URL 的引用。如果装入了这类引用，则后续页面将通过 HTTP 协议而不是 NFS 协议进行装入。

如何启用可穿过防火墙的 WebNFS 访问

通过将防火墙配置为允许在端口 `2049` 上使用 TCP 连接，可以对不属于本地子网的客户机启用 WebNFS 访问。如果仅允许 `httpd` 访问，则不允许使用 NFS URL。

Autofs 管理的任务概述

本节介绍在您自己的环境中可能会遇到的一些最常见任务。其中包括针对每种情况的建议步骤，以帮助您配置 autofs，从而最好地满足客户机的需要。

注 – 从 Solaris 10 发行版开始，还可以使用 `/etc/default/autofs` 文件来配置 autofs 环境。有关任务信息，请参阅第 97 页中的 “使用 `/etc/default/autofs` 文件配置 autofs 环境”。

Autofs 管理的任务列表

下表提供了与 autofs 相关的许多任务的说明和链接。

表 5–5 Autofs 管理的任务列表

任务	说明	参考
启动 autofs	启动自动挂载服务而不必重新引导系统	第 88 页中的 “如何启动自动挂载程序”
停止 autofs	停止自动挂载服务而不禁用其他网络服务	第 88 页中的 “如何停止自动挂载程序”
使用 `/etc/default/autofs` 文件配置 autofs 环境	为 `/etc/default/autofs` 文件中的关键字赋值	第 97 页中的 “使用 `/etc/default/autofs` 文件配置 autofs 环境”
使用 autofs 访问文件系统	使用自动挂载服务访问文件系统	第 83 页中的 “使用自动挂载程序挂载”

表 5–5 Autofs 管理的任务列表 （续）

任务	说明	参考
修改 autofs 映射	修改主映射的步骤，这些步骤应该用于列出其他映射	第 99 页中的 “如何修改主映射”
	修改间接映射的步骤，这些步骤应该用于大多数映射	第 99 页中的 “如何修改间接映射”
	修改直接映射的步骤，需要在客户机上的挂载点与服务器之间建立直接关联时应该使用这些步骤	第 99 页中的 “如何修改直接映射”
修改 autofs 映射以访问非 NFS 文件系统	使用 CD-ROM 应用程序项设置 autofs 映射的步骤	第 100 页中的 “如何使用 Autofs 访问 CD-ROM 应用程序”
	使用 PC-DOS 软盘项设置 autofs 映射的步骤	第 101 页中的 “如何使用 Autofs 访问 PC-DOS 数据软盘”
	使用 autofs 访问 CacheFS 文件系统的步骤	第 102 页中的 “如何使用 CacheFS 访问 NFS 文件系统”
使用 `/home`	如何设置公用 `/home` 映射的示例	第 102 页中的 “设置 `/home` 的通用视图”
	设置引用多个文件系统的 `/home` 映射的步骤	第 103 页中的 “如何设置包含多个起始目录文件系统的 `/home`”
使用新的 autofs 挂载点	设置与项目相关的 autofs 映射的步骤	第 104 页中的 “如何在 `/ws` 下整合与项目相关的文件”
	设置支持不同客户机体系结构的 autofs 映射的步骤	第 105 页中的 “如何设置不同的体系结构来访问共享名称空间”
	设置支持不同操作系统的 autofs 映射的步骤	第 106 页中的 “如何支持不兼容的客户机操作系统版本”
使用 autofs 复制文件系统	提供对故障转移的文件系统的访问	第 106 页中的 “如何在多台服务器之间复制共享文件”
在 autofs 中使用安全限制	限制对文件的远程 `root` 访问时提供对文件系统的访问	第 106 页中的 “如何应用 Autofs 安全限制”
在 autofs 中使用公共文件句柄	挂载文件系统时强制使用公共文件句柄	第 107 页中的 “如何在 Autofs 中使用公共文件句柄”
在 autofs 中使用 NFS URL	添加 NFS URL 以便自动挂载程序可以使用它	第 107 页中的 “如何在 Autofs 中使用 NFS URL”
禁用 autofs 浏览功能	在单台客户机上禁用浏览功能使得 autofs 挂载点不会自动填充的步骤	第 108 页中的 “如何在单台 NFS 客户机上完全禁用 Autofs 浏览功能”
	在所有客户机上禁用浏览功能使得 autofs 挂载点不会自动填充的步骤	第 108 页中的 “如何针对所有客户机禁用 Autofs 浏览功能”

表 5–5 Autofs 管理的任务列表 （续）

任务	说明	参考
	在客户机上禁用浏览功能使得特定 autofs 挂载点不会自动填充的步骤	第 108 页中的 “如何在选定的文件系统上禁用 Autofs 浏览功能”

使用 /etc/default/autofs 文件配置 autofs 环境

从 Solaris 10 发行版开始，可以使用 `/etc/default/autofs` 文件来配置 autofs 环境。具体来说，此文件提供了配置 autofs 命令和 autofs 守护进程的其他方法。在命令行上制定的规范也可以通过此配置文件实现。通过为关键字提供值，可以制定规范。有关更多信息，请参阅第 124 页中的 “`/etc/default/autofs` 文件”。

以下过程说明如何使用 `/etc/default/autofs` 文件。

▼ 如何使用 /etc/default/autofs 文件配置 autofs 环境

1 **成为超级用户或承担等效角色。**

角色包含授权和具有特权的命令。有关角色的更多信息，请参见《系统管理指南：安全性服务》中的“配置 RBAC（任务列表）”。

2 **在 `/etc/default/autofs` 文件中添加或修改项。**

例如，如果要关闭对所有 autofs 挂载点的浏览，可以添加以下行。

```
AUTOMOUNTD_NOBROWSE=ON
```

此关键字与 `automountd` 的 `-n` 参数等效。有关关键字的列表，请参阅第 124 页中的 “`/etc/default/autofs` 文件”。

3 **重新启动 autofs 守护进程。**

键入以下命令：

```
# svcadm restart system/filesystem/autofs
```

涉及映射的管理任务

下表介绍了管理 autofs 映射时需要注意的几个因素。选择的映射和名称服务将影响对 autofs 映射进行更改时需要使用的机制。

下表介绍了映射类型及其使用。

表 5–6 autofs映射类型及其使用

映射类型	使用
主	将目录与映射关联
直接	将 autofs 定向至特定文件系统
间接	将 autofs 定向至面向引用的文件系统

下表介绍了如何对基于名称服务的 autofs 环境进行更改。

表 5–7 映射维护

名称服务	方法
本地文件	文本编辑器
NIS	`make` 文件
NIS+	`nistbladm`

下表提示您何时运行 `automount` 命令，具体取决于对映射类型已做的修改。例如，如果添加或删除了某个直接映射，则需要在本地系统上运行 `automount` 命令。通过运行该命令，可使更改生效。但是，如果修改了现有项，则无需运行 `automount` 命令以使更改生效。

表 5–8 何时运行 automount 命令

映射类型	重新启动 `automount`？	
	添加或删除	修改
`auto_master`	Y	Y
直接	Y	N
间接	N	N

修改映射

以下过程要求使用 NIS+ 作为名称服务。

▼ 如何修改主映射

1. **以具有更改映射权限的用户身份登录。**
2. **使用 `nistbladm` 命令对主映射做出更改。**
   请参见《System Administration Guide: Naming and Directory Services (NIS+)》。
3. **对于每台客户机，成为超级用户或承担等效角色。**
   角色包含授权和具有特权的命令。有关角色的更多信息，请参见《系统管理指南：安全性服务》中的"配置 RBAC（任务列表）"。
4. **对于每台客户机，运行 `automount` 命令以确保更改生效。**
5. **通知用户所做的更改。**
   通知是必需的，以便用户还可以在其各自的计算机上以超级用户身份运行 `automount` 命令。请注意，只要运行 `automount` 命令，即会从主映射中收集信息。

▼ 如何修改间接映射

1. **以具有更改映射权限的用户身份登录。**
2. **使用 `nistbladm` 命令，对间接映射进行更改。**
   请参见《System Administration Guide: Naming and Directory Services (NIS+)》。请注意，更改将在下次使用映射时（即下次执行挂载时）生效。

▼ 如何修改直接映射

1. **以具有更改映射权限的用户身份登录。**
2. **使用 `nistbladm` 命令，添加或删除对直接映射的更改。**
   请参见《System Administration Guide: Naming and Directory Services (NIS+)》。
3. **通知用户所做的更改。**
   通知是必需的，以便用户可以在需要时在其各自的计算机上以超级用户身份运行 `automount` 命令。

注 – 如果仅修改或更改现有直接映射项的内容，则无需运行 `automount` 命令。

例如，假定修改了 auto_direct 映射，以便从其他服务器挂载 /usr/src 目录。如果此时未挂载 /usr/src，则尝试访问 /usr/src 时新的项会立即生效。如果现在已挂载了 /usr/src，则可以等到进行自动取消挂载，然后再访问该文件。

注 – 请尽可能使用间接映射。间接映射更容易构造，并且对计算机文件系统的要求较少。另外，间接映射也不会像直接映射那样在挂载表中占用很多空间。

避免挂载点冲突

如果已在 /src 上挂载了本地磁盘分区并且计划使用 autofs 服务来挂载其他源目录，则可能会遇到问题。如果指定挂载点 /src，则只要尝试访问本地分区，NFS 服务便会隐藏该分区。

需要在其他某个位置（例如在 /export/src 上）挂载该分区。然后，需要在 /etc/vfstab 中添加如下项：

```
/dev/dsk/d0t3d0s5 /dev/rdsk/c0t3d0s5 /export/src ufs 3 yes -
```

还需要在 auto_src 中添加此项：

```
terra        terra:/export/src
```

terra 是计算机的名称。

访问非 NFS 文件系统

Autofs 还可以挂载 NFS 文件以外的其他文件。Autofs 会将文件挂载在可移除介质上，如软盘或 CD-ROM。通常，可使用卷管理器将文件挂载在可移除介质上。以下示例说明如何可以通过 autofs 完成此挂载。卷管理器和 autofs 不会同时运行，因此必须先停用卷管理器，然后才能使用这些项。

可以将介质放入驱动器并从映射中引用文件系统，而不要从服务器挂载文件系统。如果计划访问非 NFS 文件系统并且使用的是 autofs，请参见以下过程。

▼ 如何使用 Autofs 访问 CD-ROM 应用程序

注 – 如果**未**使用卷管理器，请使用此过程。

1. **成为超级用户或承担等效角色。**

   角色包含授权和具有特权的命令。有关角色的更多信息，请参见《系统管理指南：安全性服务》中的“配置 RBAC（任务列表）”。

2 **更新 autofs 映射。**

为 CD-ROM 文件系统添加如下项：

```
hsfs      -fstype=hsfs,ro      :/dev/sr0
```

要挂载的 CD-ROM 设备必须显示为冒号后跟一个名称。

▼ 如何使用 Autofs 访问 PC-DOS 数据软盘

注 – 如果**未**使用卷管理器，请使用此过程。

1 **成为超级用户或承担等效角色。**

角色包含授权和具有特权的命令。有关角色的更多信息，请参见《系统管理指南：安全性服务》中的“配置 RBAC（任务列表）”。

2 **更新 autofs 映射。**

为软盘文件系统添加如下项：

```
pcfs      -fstype=pcfs      :/dev/diskette
```

使用 CacheFS 访问 NFS 文件系统

高速缓存文件系统 (cache file system, CacheFS) 是一种普通的非易失性高速缓存机制。CacheFS 利用小而快速的本地磁盘提高了某些文件系统的性能。例如，可以使用 CacheFS 改进 NFS 环境的性能。

CacheFS 在不同版本的 NFS 上的工作方式不同。例如，如果客户机和后台文件系统运行的是 NFS 版本 2 或版本 3，则文件将在前台文件系统中进行高速缓存以便客户机访问。但是，如果客户机和服务器运行的都是 NFS 版本 4，则其功能如下：当客户机最初请求访问 CacheFS 文件系统的文件时，请求将绕过前台的（即高速缓存的）文件系统，并直接访问后台文件系统。使用 NFS 版本 4 后，文件将不再在前台文件系统中进行高速缓存。后台文件系统将提供所有文件访问权。另外，由于前台文件系统中没有高速缓存任何文件，因此特定于 CacheFS 的挂载选项（这些选项旨在影响前台文件系统）会被忽略。特定于 CacheFS 的挂载选项不适用于后台文件系统。

注 – 第一次在系统上配置 NFS 版本 4 时，控制台上将出现一条警告，表明高速缓存不再起作用。

▼ 如何使用 CacheFS 访问 NFS 文件系统

1 **成为超级用户或承担等效角色。**

角色包含授权和具有特权的命令。有关角色的更多信息，请参见《系统管理指南：安全性服务》中的“配置 RBAC（任务列表）”。

2 **运行 `cfsadmin` 命令在本地磁盘上创建高速缓存目录。**

```
# cfsadmin -c /var/cache
```

3 **将 `cachefs` 项添加到相应的自动挂载程序映射中。**

例如，将此项添加到主映射中可以高速缓存所有起始目录：

```
/home auto_home -fstype=cachefs,cachedir=/var/cache,backfstype=nfs
```

将此项添加到 `auto_home` 映射中仅会高速缓存名为 `rich` 的用户的起始目录：

```
rich -fstype=cachefs,cachedir=/var/cache,backfstype=nfs dragon:/export/home1/rich
```

注 – 随后搜索的映射中包括的选项会覆盖之前搜索的映射中设置的选项。最后找到的选项即是使用的选项。在前面的示例中，如果某些选项需要更改，则向 `auto_home` 映射添加其他项时只需在主映射中包括这些选项即可。

定制自动挂载程序

可以采用多种方式设置自动挂载程序映射。以下任务给出了有关如何定制自动挂载程序映射以提供易用目录结构的详细信息。

设置 /home 的通用视图

理想情况是，所有的网络用户均可以在 `/home` 下找到其各自的或任何人的起始目录。此视图应该在所有计算机（无论是客户机还是服务器）中是通用的。

每个 Solaris 安装都附带一个主映射：`/etc/auto_master`。

```
# Master map for autofs
#
+auto_master
/net     -hosts     -nosuid,nobrowse
/home    auto_home  -nobrowse
```

另外，还会在 `/etc` 下安装 `auto_home` 的映射。

```
# Home directory map for autofs
#
+auto_home
```

除了对外部 auto_home 映射的引用，此映射为空。如果要使 /home 下的目录对于所有计算机通用，请勿修改此 /etc/auto_home 映射。所有的起始目录项都应出现在名称服务文件 NIS 或 NIS+ 中。

注 – 不应允许用户从其起始目录运行 setuid 可执行文件。如果没有此限制，任何用户在任何计算机上都可具有超级用户权限。

▼ 如何设置包含多个起始目录文件系统的 /home

1. **成为超级用户或承担等效角色。**

   角色包含授权和具有特权的命令。有关角色的更多信息，请参见《系统管理指南：安全性服务》中的"配置 RBAC（任务列表）"。

2. **在 /export/home 下安装起始目录分区。**

   如果系统具有多个分区，请将这些分区安装在单独的目录下，例如 /export/home1 和 /export/home2。

3. **使用 Solaris Management Console 工具创建并维护 auto_home 映射。**

   每次创建新的用户帐户时，请在 auto_home 映射中键入用户起始目录的位置。映射项可以非常简单，例如：

   ```
   rusty        dragon:/export/home1/&
   gwenda       dragon:/export/home1/&
   charles      sundog:/export/home2/&
   rich         dragon:/export/home3/&
   ```

   请注意使用 &（和符号）替代映射关键字。和符号是以下示例中第二次出现的 rusty 的缩写。

   ```
   rusty         dragon:/export/home1/rusty
   ```

   如果提供了 auto_home 映射，则用户可以引用路径为 /home/*user* 的任何起始目录（包括其本身的起始目录）。*user* 是它们在映射中的登录名和关键字。登录到其他用户的计算机时，此所有起始目录的通用视图非常重要。Autofs 将为您挂载起始目录。同样，如果在其他计算机上运行远程窗口系统客户机，则该客户机程序具有与 /home 目录视图相同的视图。

   此通用视图还将扩展到服务器。以前面的示例为例，如果 rusty 登录到服务器 dragon，则 autofs 会通过将 /export/home1/rusty 回送挂载到 /home/rusty 上来提供对本地磁盘的直接访问。

   用户无需知道其起始目录的实际位置。如果 rusty 需要更多磁盘空间，并且需要将其起始目录重新定位到其他服务器，则简单更改就足够了。只需更改 auto_home 映射中 rusty 的项，即可反映新的位置。其他用户可以继续使用 /home/rusty 路径。

▼ 如何在 /ws 下整合与项目相关的文件

假定您是某个大型软件开发项目的管理员。您计划在名为 /ws 的目录下提供所有与项目相关的文件。此目录将在站点上的所有工作站中通用。

1 向站点 auto_master 映射 NIS 或 NIS+ 添加 /ws 目录的项。

```
/ws     auto_ws     -nosuid
```

auto_ws 映射可确定 /ws 目录的内容。

2 为防万一，添加 -nosuid 选项。

此选项可阻止用户运行任何工作区可能存在的 setuid 程序。

3 向 auto_ws 映射中添加项。

auto_ws 映射已经过组织，因此每项都能描述一个子项目。首次尝试添加时将生成如下映射：

```
compiler   alpha:/export/ws/&
windows    alpha:/export/ws/&
files      bravo:/export/ws/&
drivers    alpha:/export/ws/&
man        bravo:/export/ws/&
tools      delta:/export/ws/&
```

每项结尾的和符号 (&) 是该项关键字的缩写。例如，第一项与以下内容等效：

```
compiler        alpha:/export/ws/compiler
```

首次尝试添加时会提供一个外观简单的映射，但该映射不适合。项目组织者决定应提供 man 项中的文档作为每个子项目下的子目录。另外，每个子项目都要求子目录描述该软件的多个版本。必须将其中的每个子目录都指定给服务器上的整个磁盘分区。

请按如下所示修改映射中的各项：

```
compiler \
    /vers1.0    alpha:/export/ws/&/vers1.0 \
    /vers2.0    bravo:/export/ws/&/vers2.0 \
    /man        bravo:/export/ws/&/man
windows \
    /vers1.0    alpha:/export/ws/&/vers1.0 \
    /man        bravo:/export/ws/&/man
files \
    /vers1.0    alpha:/export/ws/&/vers1.0 \
    /vers2.0    bravo:/export/ws/&/vers2.0 \
    /vers3.0    bravo:/export/ws/&/vers3.0 \
    /man        bravo:/export/ws/&/man
drivers \
    /vers1.0    alpha:/export/ws/&/vers1.0 \
    /man        bravo:/export/ws/&/man
tools \
    /           delta:/export/ws/&
```

尽管现在映射看起来比较大，但是映射仍然仅包含五个项。由于每项都包含多个挂载，因此每项都比较大。例如，对 /ws/compiler 的引用要求挂载 vers1.0、vers2.0 和 man 三个目录。每一行结尾的反斜杠将通知 autofs 该项会继续进入下一行。实际上，尽管使用了换行符和一些缩进以使该项更具可读性，但该项仍是较长的一行。tools 目录包含所有子项目的软件开发工具，因此该目录不遵循相同的子目录结构。tools 目录仍然表示单个挂载。

这种安排为管理员提供了许多灵活性。软件项目通常会占用大量磁盘空间。在项目的整个生命周期内，可能需要重新定位并扩展各种磁盘分区。如果这些更改反映在 auto_ws 映射中，则无需通知用户，因为 /ws 下的目录分层结构未被更改。

由于服务器 alpha 和 bravo 查看的是同一个 autofs 映射，因此登录到这些计算机的任何用户都可以找到预期的 /ws 名称空间。系统将为这些用户提供通过回送挂载（而不是 NFS 挂载）对本地文件的直接访问。

▼ 如何设置不同的体系结构来访问共享名称空间

您需要为本地可执行文件和应用程序（如电子表格应用程序和字处理软件包）汇编一个共享名称空间。此名称空间的客户机使用要求不同可执行文件格式的多个不同的工作站体系结构。另外，某些工作站运行的是不同发行版的操作系统。

1. **创建 auto_local 映射。**

   请参见《系统管理指南：名称和目录服务（DNS、NIS 和 LDAP）》。

2. **为共享名称空间选择单个站点特定名称。**

   此名称可使属于此空间的文件和目录易于识别。例如，如果选择 /usr/local 作为名称，则路径 /usr/local/bin 显然属于此名称空间。

3. **为使用户群易于识别，请创建 autofs 间接映射。**

   在 /usr/local 中挂载此映射。在 NIS auto_master 映射中设置以下项：

   ```
   /usr/local      auto_local      -ro
   ```

   请注意，-ro 挂载选项表明客户机不能对任何文件或目录执行写入操作。

4. **在服务器上导出相应的目录。**

5. **在 auto_local 映射中包括 bin 项。**

   目录结构如下：

   ```
   bin      aa:/export/local/bin
   ```

6. **可选要为不同体系结构的客户机提供服务，请通过添加 autofs CPU 变量来更改相应的项。**

   ```
   bin      aa:/export/local/bin/$CPU
   ```

   - 对于 SPARC 客户机－将可执行文件放入 /export/local/bin/sparc 中。

- 对于 x86 客户机－将可执行文件放入 /export/local/bin/i386 中。

▼ 如何支持不兼容的客户机操作系统版本

1. **将体系结构类型与确定客户机操作系统类型的变量合并。**

   可以将 autofs OSREL 变量与 CPU 变量合并，以形成可同时确定 CPU 类型和 OS 发行版的名称。

2. **创建以下映射项。**

   ```
   bin      aa:/export/local/bin/$CPU$OSREL
   ```

   对于运行操作系统版本 5.6 的客户机，请导出以下文件系统：

   - 对于 SPARC 客户机－导出 /export/local/bin/sparc5.6。
   - 对于 x86 客户机－将可执行文件放入 /export/local/bin/i3865.6 中。

▼ 如何在多台服务器之间复制共享文件

共享已复制的只读文件系统的最佳方法是使用故障转移。有关故障转移的说明，请参见第 170 页中的 “客户端故障转移”。

1. **成为超级用户或承担等效角色。**

   角色包含授权和具有特权的命令。有关角色的更多信息，请参见《系统管理指南：安全性服务》中的“配置 RBAC（任务列表）”。

2. **修改 autofs 映射中的项。**

   创建用逗号分隔的所有副本服务器的列表，如下所示：

   ```
   bin      aa,bb,cc,dd:/export/local/bin/$CPU
   ```

   Autofs 会选择距离最近的服务器。如果服务器具有多个网络接口，请列出每个接口。Autofs 会选择距离客户机最近的接口，从而避免路由不必要的 NFS 流量。

▼ 如何应用 Autofs 安全限制

1. **成为超级用户或承担等效角色。**

   角色包含授权和具有特权的命令。有关角色的更多信息，请参见《系统管理指南：安全性服务》中的“配置 RBAC（任务列表）”。

2. **在名称服务 auto_master 文件（NIS 或 NIS+）中创建以下项：**

   ```
   /home      auto_home      -nosuid
   ```

nosuid 选项可阻止用户创建设置了 setuid 或 setgid 位的文件。

此项将覆盖普通的本地 /etc/auto_master 文件中的 /home 的项。请参见前面的示例。由于对外部名称服务映射的 +auto_master 引用出现在该文件中的 /home 项之前，因此会发生覆盖。如果 auto_home 映射中的项包括挂载选项，则会覆盖 nosuid 选项。因此，在 auto_home 映射中不应使用任何选项，或者如果使用，则每项都必须包括 nosuid 选项。

注 – 请勿在服务器的 /home 上或下挂载起始目录磁盘分区。

▼ 如何在 Autofs 中使用公共文件句柄

1 **成为超级用户或承担等效角色。**

角色包含授权和具有特权的命令。有关角色的更多信息，请参见《系统管理指南：安全性服务》中的“配置 RBAC（任务列表）”。

2 **在 autofs 映射中创建如下项：**

```
/usr/local      -ro,public     bee:/export/share/local
```

public 选项会强制使用公共句柄。如果 NFS 服务器不支持公共文件句柄，则挂载将失败。

▼ 如何在 Autofs 中使用 NFS URL

1 **成为超级用户或承担等效角色。**

角色包含授权和具有特权的命令。有关角色的更多信息，请参见《系统管理指南：安全性服务》中的“配置 RBAC（任务列表）”。

2 **创建如下的 autofs 项：**

```
/usr/local      -ro     nfs://bee/export/share/local
```

服务会尝试在 NFS 服务器上使用公共文件句柄。但是，如果该服务器不支持公共文件句柄，则会使用 MOUNT 协议。

禁用 Autofs 浏览功能

安装的缺省版本的 /etc/auto_master 会向 -/home 和 /net 的项添加 nobrowse 选项。此外，如果尚未修改 /etc/auto_master 中的 /home 和 /net 项，则升级过程还会向这些项中添加 -nobrowse 选项。但是，可能必须手动进行这些更改，或在安装后针对站点特定的 autofs 挂载点关闭浏览功能。

可以采用多种方式关闭浏览功能。使用 automountd 守护进程的命令行选项禁用该功能，此方式可针对客户机完全禁用 autofs 浏览功能。或者使用 NIS 或 NIS+ 名称空间中的 autofs 映射针对所有客户机上的每个映射项禁用浏览功能。另外，还可以在未使用网络范围名称空间的情况下使用本地 autofs 映射，针对每台客户机上的每个映射项禁用该功能。

▼ 如何在单台 NFS 客户机上完全禁用 Autofs 浏览功能

1. **在 NFS 客户机上成为超级用户或承担等效角色。**

   角色包含授权和具有特权的命令。有关角色的更多信息，请参见《系统管理指南：安全性服务》中的“配置 RBAC（任务列表）”。

2. **编辑 /etc/default/autofs 文件以包括以下关键字和值。**

   ```
   AUTOMOUNTD_NOBROWSE=TRUE
   ```

3. **重新启动 autofs 服务。**

   ```
   # svcadm restart system/filesystem/autofs
   ```

▼ 如何针对所有客户机禁用 Autofs 浏览功能

要针对所有客户机禁用浏览功能，必须使用名称服务，如 NIS 或 NIS+。否则，需要手动编辑每台客户机上的自动挂载程序映射。在本示例中，/home 目录的浏览功能已禁用。必须对需要禁用的每个间接 autofs 节点遵照以下过程执行操作。

1. **向名称服务 auto_master 文件中的 /home 项添加 -nobrowse 选项。**

   ```
   /home      auto_home      -nobrowse
   ```

2. **在所有客户机上运行 automount 命令。**

   在客户机系统上运行 automount 命令后或重新引导后，新的行为才会生效。

   ```
   # /usr/sbin/automount
   ```

▼ 如何在选定的文件系统上禁用 Autofs 浏览功能

在本示例中，/net 目录的浏览功能已禁用。对于 /home 或其他任何 autofs 挂载点可以使用同一过程。

1. **检查 /etc/nsswitch.conf 中的 automount 项。**

   要使本地文件项具有较高的优先级，名称服务转换器文件中的项应将 files 列在名称服务之前。例如：

   ```
   automount:  files nis
   ```

此项会显示标准 Solaris 安装中的缺省配置。

2 **检查 /etc/auto_master 中 +auto_master 项的位置。**

除使本地文件优先于名称空间中的项以外，还必须将 +auto_master 项移至 /net 后面：

```
# Master map for automounter
#
/net    -hosts     -nosuid
/home   auto_home
/xfn    -xfn
+auto_master
```

标准配置会将 +auto_master 项置于文件的顶部。此放置方式可防止使用任何本地更改。

3 **向 /etc/auto_master 文件中的 /net 项添加 nobrowse 选项。**

```
/net     -hosts     -nosuid,nobrowse
```

4 **在所有客户机上运行 automount 命令。**

在客户机系统上运行 automount 命令后或重新引导后，新的行为才会生效。

```
# /usr/sbin/automount
```

NFS 故障排除的策略

跟踪 NFS 问题时，请记住可能出现故障的主要位置：服务器、客户机和网络。本节概括的策略会力求隔离每个单独的组件，以找到运行不正常的组件。在所有情况下，要使远程挂载成功，mountd 和 nfsd 守护进程必须正在服务器上运行。

缺省情况下，将为所有挂载设置 -intr 选项。如果程序挂起时出现 server not responding 消息，则可以使用键盘中断组合键 Ctrl-c 中止该程序。

网络或服务器出现问题时，访问硬挂载远程文件的程序将会失败，其方式与访问软挂载远程文件的程序不同。硬挂载远程文件系统会导致客户机的内核在服务器再次响应之前一直重试请求。软挂载远程文件系统会导致客户机的系统调用在尝试片刻后返回错误。由于这些错误会导致意外的应用程序错误和数据损坏，因此应避免软挂载。

硬挂载文件系统时，如果服务器无法进行响应，则尝试访问该文件系统的程序将挂起。在这种情况下，NFS 系统会在控制台上显示以下消息：

```
NFS server hostname not responding still trying
```

服务器最终响应时，控制台上会出现以下消息：

```
NFS server hostname ok
```

访问软挂载文件系统（其服务器未响应）的程序会生成以下消息：

```
NFS operation failed for server hostname: error # (error-message)
```

注 – 由于可能的错误，请勿软挂载包含读写数据的文件系统或用于运行可执行文件的文件系统。如果应用程序忽略这些错误，则可写数据可能会被损坏。挂载的可执行文件可能无法正确装入，从而会失败。

NFS 故障排除过程

要确定 NFS 服务出现故障的位置，需要遵照几个过程执行操作以隔离故障。请检查以下各项：

- 客户机是否可以访问服务器?
- 客户机是否可以访问服务器上的 NFS 服务?
- NFS 服务是否正在服务器上运行?

在检查上述各项的过程中，您可能会注意到网络的其他部分未正常运行。例如，名称服务或物理网络硬件可能未正常运行。《系统管理指南：名称和目录服务（DNS、NIS 和 LDAP）》包含几个名称服务的调试过程。另外，在该过程中，您可能还会了解到问题不在客户端。例如，如果从工作区域的每个子网中至少获得了一个故障呼叫。在这种情况下，应该假定问题出在服务器上或服务器附近的网络硬件上。因此，应该在服务器而不是客户机上启动调试过程。

▼ 如何检查 NFS 客户机上的连接

1 检查是否可以从客户机访问 NFS 服务器。请在客户机上键入以下命令。

```
% /usr/sbin/ping bee
bee is alive
```

如果此命令报告服务器处于活动状态，请以远程方式检查 NFS 服务器。请参见第 111 页中的 “如何远程检查 NFS 服务器”。

2 如果不能从客户机访问服务器，请确保本地名称服务正在运行。

对于 NIS+ 客户机，请键入以下内容：

```
% /usr/lib/nis/nisping -u
Last updates for directory eng.acme.com. :
Master server is eng-master.acme.com.
        Last update occurred at Mon Jun  5 11:16:10 1995

Replica server is eng1-replica-58.acme.com.
        Last Update seen was Mon Jun  5 11:16:10 1995
```

3 如果名称服务正在运行，请通过键入以下内容确保客户机已收到正确的主机信息：

```
% /usr/bin/getent hosts bee
129.144.83.117    bee.eng.acme.com
```

4 **如果主机信息正确，但不能从该客户机访问服务器，请从其他客户机运行 `ping` 命令。**

如果从第二台客户机运行的命令失败，请参见第 112 页中的 “如何验证服务器上的 NFS 服务”。

5 **如果可以从第二台客户机访问服务器，请使用 `ping` 检查第一台客户机到本地网络中的其他系统的连接。**

如果此命令失败，请检查客户机上的网络软件配置，例如 `/etc/netmasks` 和 `/etc/nsswitch.conf`。

6 **可选检查 `rpcinfo` 命令的输出。**

如果 `rpcinfo` 命令未显示 `program 100003 version 4 ready and waiting`，则服务器上未启用 NFS 版本 4。有关启用 NFS 版本 4 的信息，请参见表 5–3。

7 **如果软件正确，请检查网络硬件。**

尝试将客户机移至第二个网络断开位置。

▼ 如何远程检查 NFS 服务器

请注意，如果使用的是 NFS 版本 4 服务器，则不必同时支持 UDP 和 MOUNT 协议。

1 **通过键入以下命令，检查 NFS 服务是否已在 NFS 服务器上启动：**

```
% rpcinfo -s bee|egrep 'nfs|mountd'
 100003  3,2    tcp,udp,tcp6,upd6                nfs     superuser
 100005  3,2,1  ticots,ticotsord,tcp,tcp6,ticlts,udp,upd6  mountd  superuser
```

如果尚未启动守护进程，请参见第 113 页中的 “如何重新启动 NFS 服务”。

2 **检查服务器的 `nfsd` 进程是否正在响应。**

在客户机上，键入以下命令以测试来自服务器的 UDP NFS 连接。

```
% /usr/bin/rpcinfo -u bee nfs
program 100003 version 2 ready and waiting
program 100003 version 3 ready and waiting
```

注 – NFS 版本 4 不支持 UDP。

如果服务器正在运行，则它将列出程序和版本号的列表。使用 `-t` 选项可以测试 TCP 连接。如果此命令失败，请前进至第 112 页中的 “如何验证服务器上的 NFS 服务”。

3 **通过键入以下命令，检查服务器的 `mountd` 是否正在响应。**

```
% /usr/bin/rpcinfo -u bee mountd
program 100005 version 1 ready and waiting
program 100005 version 2 ready and waiting
program 100005 version 3 ready and waiting
```

如果服务器正在运行，则它将列出与 UDP 协议关联的程序和版本号的列表。使用 -t 选项可以测试 TCP 连接。如果任何尝试都失败，请前进至第 112 页中的 “如何验证服务器上的 NFS 服务”。

4 **检查本地 autofs 服务是否正在使用：**

```
% cd /net/wasp
```

选择已知应该正常工作的 /net 或 /home 挂载点。如果此命令失败，请在客户机上以 root 身份键入以下内容以重新启动 autofs 服务：

```
# svcadm restart system/filesystem/autofs
```

5 **验证是否在服务器上按照预期方式共享文件系统。**

```
% /usr/sbin/showmount -e bee
/usr/src                                        eng
/export/share/man                          (everyone)
```

请检查服务器上的项和本地挂载项中是否有错误。另外，还要检查名称空间。在本实例中，如果第一台客户机不在 eng 网络组中，则该客户机不能挂载 /usr/src 文件系统。

请检查所有本地文件中所有包括挂载信息的项。此列表包括 /etc/vfstab 和所有的 /etc/auto_* 文件。

▼ 如何验证服务器上的 NFS 服务

1 **成为超级用户或承担等效角色。**

角色包含授权和具有特权的命令。有关角色的更多信息，请参见《系统管理指南：安全性服务》中的“配置 RBAC（任务列表）”。

2 **检查服务器是否可以访问客户机。**

```
# ping lilac
lilac is alive
```

3 **如果不能从服务器访问客户机，请确保本地名称服务正在运行。**

对于 NIS+ 客户机，请键入以下内容：

```
% /usr/lib/nis/nisping -u
Last updates for directory eng.acme.com. :
Master server is eng-master.acme.com.
        Last update occurred at Mon Jun  5 11:16:10 1995

Replica server is eng1-replica-58.acme.com.
        Last Update seen was Mon Jun  5 11:16:10 1995
```

4 **如果名称服务正在运行，请检查服务器上的网络软件配置，例如 /etc/netmasks 和 /etc/nsswitch.conf。**

5 **键入以下命令以检查 rpcbind 守护进程是否正在运行。**

```
# /usr/bin/rpcinfo -u localhost rpcbind
program 100000 version 1 ready and waiting
program 100000 version 2 ready and waiting
program 100000 version 3 ready and waiting
```

如果服务器正在运行，则它将列出与 UDP 协议关联的程序和版本号的列表。如果 rpcbind 似乎被挂起，请重新引导服务器。

6 **键入以下命令以检查 nfsd 守护进程是否正在运行。**

```
# rpcinfo -u localhost nfs
program 100003 version 2 ready and waiting
program 100003 version 3 ready and waiting
# ps -ef | grep nfsd
root    232      1  0  Apr 07     ?     0:01 /usr/lib/nfs/nfsd -a 16
root   3127   2462  1  09:32:57  pts/3  0:00 grep nfsd
```

注 – NFS 版本 4 不支持 UDP。

如果服务器正在运行，则它将列出与 UDP 协议关联的程序和版本号的列表。另外，还应使用带有 -t 选项的 rpcinfo 来检查 TCP 连接。如果这些命令失败，请重新启动 NFS 服务。请参见第 113 页中的 “如何重新启动 NFS 服务”。

7 **键入以下命令以检查 mountd 守护进程是否正在运行。**

```
# /usr/bin/rpcinfo -u localhost mountd
program 100005 version 1 ready and waiting
program 100005 version 2 ready and waiting
program 100005 version 3 ready and waiting
# ps -ef | grep mountd
root    145      1 0 Apr 07  ?     21:57 /usr/lib/autofs/automountd
root    234      1 0 Apr 07  ?     0:04  /usr/lib/nfs/mountd
root   3084 2462 1 09:30:20 pts/3  0:00  grep mountd
```

如果服务器正在运行，则它将列出与 UDP 协议关联的程序和版本号的列表。另外，还应使用带有 -t 选项的 rpcinfo 来检查 TCP 连接。如果这些命令失败，请重新启动 NFS 服务。请参见第 113 页中的 “如何重新启动 NFS 服务”。

▼ 如何重新启动 NFS 服务

1 **成为超级用户或承担等效角色。**

角色包含授权和具有特权的命令。有关角色的更多信息，请参见《系统管理指南：安全性服务》中的“配置 RBAC（任务列表）”。

2 **在服务器上重新启动 NFS 服务。**

键入以下命令。

```
# svcadm restart network/nfs/server
```

识别提供 NFS 文件服务的主机

运行带有 -m 选项的 nfsstat 命令可收集当前的 NFS 信息。当前服务器的名称会输出在 "currserver=" 之后。

```
% nfsstat -m
/usr/local from bee,wasp:/export/share/local
 Flags: vers=3,proto=tcp,sec=sys,hard,intr,llock,link,synlink,
        acl,rsize=32768,wsize=32678,retrans=5
 Failover: noresponse=0, failover=0, remap=0, currserver=bee
```

▼ 如何验证用于 mount 命令的选项

不会对无效选项发出警告。以下过程有助于确定在命令行上或通过 /etc/vfstab 提供的选项是否有效。

对于本示例，假定以下命令已运行：

```
# mount -F nfs -o ro,vers=2 bee:/export/share/local /mnt
```

1 通过运行以下命令来验证选项。

```
% nfsstat -m
/mnt from bee:/export/share/local
Flags:  vers=2,proto=tcp,sec=sys,hard,intr,dynamic,acl,rsize=8192,wsize=8192,
        retrans=5
```

bee 中的文件系统已挂载了版本设置为 2 的协议。不过，nfsstat 命令不会显示有关所有选项的信息。但是，使用 nfsstat 命令是验证选项的最准确的方法。

2 检查 /etc/mnttab 中的项。

mount 命令不允许将无效选项添加到挂载表中。因此，请验证文件中列出的选项是否与命令行中列出的选项匹配。采用这种方式，即可检查 nfsstat 命令未报告的选项。

```
# grep bee /etc/mnttab
bee:/export/share/local /mnt nfs    ro,vers=2,dev=2b0005e 859934818
```

Autofs 故障排除

有时，您可能会遇到与 autofs 有关的问题。本节将改进问题解决过程。本节分为两个小节。

本节提供了 autofs 生成的错误消息的列表。该列表分为两部分：

- automount 的详细 (-v) 选项生成的错误消息
- 随时可能出现的错误消息

每条错误消息后都有说明和该消息的可能原因。

进行故障排除时，请使用详细 (-v) 选项启动 autofs 程序。否则，可能会遇到问题却不知道原因。

以下段落标有 autofs 失败时可能出现的错误消息，以及可能的问题的说明。

automount -v 生成的错误消息

`bad key` *key* `in direct map` *mapname*
描述: 扫描直接映射时，autofs 找到了不带前缀 / 的项关键字。

解决方法: 直接映射中的关键字必须是全路径名。

`bad key` *key* `in indirect map` *mapname*
描述: 扫描间接映射时，autofs 找到了包含 / 的项关键字。

解决方法: 间接映射关键字必须是简单的名称，而不是路径名。

`can't mount` *server*:*pathname: reason*
描述: 服务器上的挂载守护进程拒绝为 *server*:*pathname* 提供文件句柄。

解决方法: 请检查服务器上的导出表。

`couldn't create mount point` *mountpoint*: *reason*
描述: Autofs 无法创建挂载所需的挂载点。尝试以分层结构方式挂载服务器的所有导出文件系统时，经常会出现此问题。

解决方法: 所需的挂载点只能存在于无法挂载的文件系统中，这意味着不能导出文件系统。由于导出的父文件系统是以只读方式导出的，因此无法创建挂载点。

`leading space in map entry` *entry* `text in` *mapname*
描述: Autofs 在自动挂载映射中发现了包含前导空格的项。此问题通常表明不正确的连续映射项。例如：

```
fake
/blat           frobz:/usr/frotz
```

解决方法: 在本示例中，autofs 遇到第二行时就会生成警告，因为第一行应该以反斜杠 (\) 终止。

mapname `: Not found`
描述: 无法找到所需的映射。仅当使用 `-v` 选项时，才会产生此消息。

解决方法: 请检查映射名的拼写和路径名。

`remount` *server*:*pathname* `on` *mountpoint* `: server not responding`
描述: Autofs 无法重新挂载以前已取消挂载的文件系统。

解决方法: 请联系 Oracle 以获取帮助。此错误消息非常少见，并且没有直接的解决方法。

`WARNING: mountpoint already mounted on`
描述: Autofs 正在尝试通过现有的挂载点进行挂载。此消息意味着 autofs 中出现了内部错误（异常）。

解决方法: 请联系 Oracle 以获取帮助。此错误消息非常少见，并且没有直接的解决方法。

各种错误消息

`dir mountpoint must start with '/'`
解决方法: 必须以全路径名提供自动挂载程序的挂载点。请检查挂载点的拼写和路径名。

`hierarchical mountpoint: pathname1 and pathname2`
解决方法: Autofs 不允许其挂载点具有分层结构关系。autofs 挂载点决不能包含在其他自动挂载的文件系统中。

`host server not responding`
描述: Autofs 尝试访问 *server*，但未收到任何响应。

解决方法: 请检查 NFS 服务器的状态。

hostname`: exports: rpc-err`
描述: 从 *hostname* 获取导出列表时出现错误。此消息表明服务器或网络出现问题。

解决方法: 请检查 NFS 服务器的状态。

`map mapname, key key: bad`
描述: 该映射项格式错误，autofs 无法解释该项。

解决方法: 请重新检查该项。该项或许包含需要转义的字符。

mapname`: nis-err`
描述: 在 NIS 映射中查找项时出现错误。此消息表明 NIS 出现问题。

解决方法: 请检查 NIS 服务器的状态。

`mount of server:pathname on mountpoint:reason`
描述: Autofs 执行挂载失败。这种情况表明服务器或网络出现问题。*reason* 字符串定义了该问题。

解决方法: 请联系 Oracle 以获取帮助。此错误消息非常少见，并且没有直接的解决方法。

mountpoint: Not a directory
描述: Autofs 无法将其本身挂载在 *mountpoint* 上，因为它不是一个目录。

解决方法: 请检查挂载点的拼写和路径名。

nfscast: cannot send packet: *reason*
描述: Autofs 无法将查询包发送至复制文件系统位置列表中的服务器。*reason* 字符串定义了该问题。

解决方法: 请联系 Oracle 以获取帮助。此错误消息非常少见，并且没有直接的解决方法。

nfscast: cannot receive reply: *reason*
描述: Autofs 无法接收来自复制文件系统位置列表中的任何服务器的回复。*reason* 字符串定义了该问题。

解决方法: 请联系 Oracle 以获取帮助。此错误消息非常少见，并且没有直接的解决方法。

nfscast: select: *reason*
描述: 所有这些错误消息都表明尝试检查服务器中已复制的文件系统时出现问题。此消息表明网络出现问题。*reason* 字符串定义了该问题。

解决方法: 请联系 Oracle 以获取帮助。此错误消息非常少见，并且没有直接的解决方法。

pathconf: no info for *server*:*pathname*
描述: Autofs 无法获取路径名的 pathconf 信息。

解决方法: 请参见 fpathconf(2) 手册页。

pathconf: *server* : server not responding
描述: Autofs 无法访问为 pathconf() 提供信息的 *server* 上的挂载守护进程。

解决方法: 请避免在此服务器中使用 POSIX 挂载选项。

使用 Autofs 时的其他错误

如果 /etc/auto* 文件设置了执行位，则自动挂载程序会尝试执行映射，它将创建如下消息：

/etc/auto_home: +auto_home: not found

在这种情况下，auto_home 文件具有的权限不正确。该文件中的每一项会生成一条与此消息类似的错误消息。应通过键入以下命令来重置该文件的权限：

```
# chmod 644 /etc/auto_home
```

NFS 错误消息

本节显示了错误消息，后跟会产生该错误的条件的描述和至少一种修正方法。

`Bad argument specified with index option - must be a file`
解决方法: 必须在 index 选项中包含文件名。不能使用目录名。

`Cannot establish NFS service over /dev/`*tcp*`: transport setup problem`
描述: 如果尚未更新名称空间中的服务信息，则通常会产生此消息。还可向 UDP 报告此消息。

解决方法: 要解决此问题，必须更新名称空间中的服务数据。

对于 NIS+，各项应如下所示：

```
nfsd nfsd tcp 2049 NFS server daemon
nfsd nfsd udp 2049 NFS server daemon
```

对于 NIS 和 /etc/services，各项应如下所示：

```
nfsd    2049/tcp    nfs    # NFS server daemon
nfsd    2049/udp    nfs    # NFS server daemon
```

`Cannot use index option without public option`
解决方法: 在 share 命令中使用 index 选项时需要同时指定 public 选项。要使 index 选项生效，必须定义公共文件句柄。

注 – Solaris 2.5.1 发行版要求使用 share 命令来设置公共文件句柄。Solaris 2.6 发行版中已对此进行了更改，缺省情况下，公共文件句柄将被设置为 root (/)。此错误消息不再表明相关问题。

`Could not start `*daemon*`: `*error*
描述: 如果守护进程异常终止或者如果系统调用发生错误，则会显示此消息。*error* 字符串定义了该问题。

解决方法: 请联系 Oracle 以获取帮助。此错误消息很少见，并且没有直接的解决方法。

`Could not use public filehandle in request to` *server*
描述: 如果指定了 `public` 选项，但是 NFS 服务器不支持公共文件句柄，则会显示此消息。在这种情况下，挂载将失败。

解决方法: 要修正这种情况，可尝试在不使用公共文件句柄的情况下挂载请求，或重新配置 NFS 服务器以支持公共文件句柄。

daemon `running already with pid` *pid*
描述: 守护进程已运行。

解决方法: 如果要运行新的副本，请中止当前版本并启动新版本。

`error locking` *lock file*
描述: 如果不能正确锁定与守护进程关联的 *lock file*，则会显示此消息。

解决方法: 请联系 Oracle 以获取帮助。此错误消息很少见，并且没有直接的解决方法。

`error checking` *lock file*`:` *error*
描述: 如果无法正常打开与守护进程关联的 *lock file*，则会显示此消息。

解决方法: 请联系 Oracle 以获取帮助。此错误消息很少见，并且没有直接的解决方法。

`NOTICE: NFS3: failing over from` *host1* `to` *host2*
描述: 如果发生故障转移，则控制台上会显示此消息。该消息仅作为建议。

解决方法: 不需要执行任何操作。

filename`: File too large`
描述: NFS 版本 2 客户机正在尝试访问超过 2 GB 的文件。

解决方法: 请避免使用 NFS 版本 2。请使用版本 3 或版本 4 来挂载文件系统。另外，请参见第 140 页中的 “NFS 文件系统的 `mount` 选项”中的 `nolargefiles` 选项的说明。

`mount: ... server not responding:RPC_PMAP_FAILURE - RPC_TIMED_OUT`
描述: 共享尝试挂载的文件系统的服务器已关闭或无法访问、处于错误的运行级，或其 `rpcbind` 已停用或挂起。

解决方法: 等待服务器重新引导。如果服务器已挂起，请重新引导该服务器。

`mount: ... server not responding: RPC_PROG_NOT_REGISTERED`
描述: 已使用 `rpcbind` 注册了挂载请求，但是未注册 NFS 挂载守护进程 `mountd`。

解决方法: 等待服务器重新引导。如果服务器已挂起，请重新引导该服务器。

`mount: ... No such file or directory`
描述: 远程目录或本地目录都不存在。

解决方法: 请检查目录名的拼写。同时在两个目录中运行 `ls`。

`mount: ...: Permission denied`
描述: 您的计算机名称可能不在客户机或网络组的列表中，通过该列表可对尝试挂载的文件系统进行访问。

解决方法: 请使用 `showmount -e` 验证该访问列表。

`NFS file temporarily unavailable on the server, retrying ...`
描述: NFS 版本 4 服务器可以委托客户机管理文件。此消息表明服务器正在为与您的客户机请求冲突的其他客户机重新调用委托。

解决方法: 必须先重新调用，然后服务器才可以处理您的客户机请求。有关委托的更多信息，请参阅第 165 页中的 “NFS 版本 4 中的委托”。

`NFS fsstat failed for server` *hostname*`: RPC: Authentication error`
描述: 许多情况都会导致此错误。要调试的最困难情况之一即是由于用户属于太多组而出现此问题。目前，如果用户通过 NFS 挂载来访问文件，则该用户最多可以属于 16 个组。

解决方法: 同样存在另一种情况，即用户需要属于 16 个以上的组。可以使用访问控制列表提供所需的访问特权。

`nfs mount: ignoring invalid option “-`*option*`”`
描述: *-option* 标志无效。

解决方法: 要验证所需的语法，请参阅 `mount_nfs(1M)` 手册页。

注 – 如果运行的是 Solaris 2.6 发行版到当前发行版中或已修补的早期版本中包括的任何版本的 `mount` 命令，则不会显示此错误消息。

`nfs mount: NFS can’t support “nolargefiles”`
描述: NFS 客户机已尝试使用 `-nolargefiles` 选项从 NFS 服务器挂载文件系统。

解决方法: NFS 文件系统类型不支持此选项。

`nfs mount: NFS V2 can’t support “largefiles”`
描述: NFS 版本 2 协议不能处理大文件。

解决方法: 如果需要访问大文件，则必须使用版本 3 或版本 4。

`NFS server` *hostname* `not responding still trying`
描述: 如果程序在执行与文件相关的工作时挂起，则 NFS 服务器可能出现了故障。此消息表明 NFS 服务器 *hostname* 已关闭，或者服务器或网络出现了问题。

解决方法: 如果正在使用故障转移，则 *hostname* 是一个服务器列表。要开始故障排除，请参见第 110 页中的 “如何检查 NFS 客户机上的连接”。

`NFS server recovering`
描述: 在 NFS 版本 4 服务器重新引导过程中，一些操作不允许执行。此消息表明客户机正在等待服务器允许此操作继续进行。

解决方法: 不需要执行任何操作。请等待服务器允许执行该操作。

`Permission denied`
描述: 由于以下原因，`ls -l`、`getfacl` 和 `setfacl` 命令会显示此消息：

- 如果 NFS 版本 4 服务器上的访问控制列表 (access control list, ACL) 项中存在的用户或组不能映射为 NFS 版本 4 客户机上的有效用户或组，则不允许该用户读取客户机上的 ACL。
- 如果 NFS 版本 4 客户机上设置的 ACL 项中存在的用户或组不能映射为 NFS 版本 4 服务器上的有效用户或组，则不允许该用户写入或修改客户机上的 ACL。
- 如果 NFS 版本 4 客户机和服务器的 NFSMAPID_DOMAIN 值不匹配，则 ID 映射将失败。

有关更多信息，请参见第 166 页中的 “NFS 版本 4 中的 ACL 和 `nfsmapid`”。

解决方法: 请执行以下操作：

- 确保 ACL 项中的所有用户 ID 和组 ID 都存在于客户机和服务器上。
- 确保在 `/etc/default/nfs` 文件中正确设置了 NFSMAPID_DOMAIN 的值。有关更多信息，请参见第 125 页中的 “`/etc/default/nfs` 文件的关键字”。

要确定是否无法在服务器或客户机上映射任何用户或组，请使用第 167 页中的 “检查是否存在未映射的用户 ID 或组 ID”中提供的脚本。

`port` *number* `in nfs URL not the same as port` *number* `in port option`
描述: NFS URL 中包含的端口号必须与 `-port` 选项包含的端口号匹配才能进行挂载。如果端口号不匹配，则挂载将失败。

解决方法: 更改命令以使端口号相同，或者不要指定不正确的端口号。通常，无需同时使用 NFS URL 和 `-port` 选项来指定端口号。

`replicas must have the same version`
描述: 要使 NFS 故障转移工作正常，NFS 服务器副本必须支持相同版本的 NFS 协议。

解决方法: 不允许运行多个版本。

`replicated mounts must be read-only`
描述: NFS 故障转移在以读写方式挂载的文件系统上不能正常工作。以读写方式挂载文件系统会增加文件更改的可能性。

解决方法: NFS 故障转移取决于文件系统是否相同。

`replicated mounts must not be soft`
描述: 复制的挂载要求等到超时后再进行故障转移。

解决方法: `soft` 选项要求超时开始时挂载即失败，因此不能对复制的挂载使用 `-soft` 选项。

`share_nfs: Cannot share more than one filesystem with 'public' option`
解决方法: 检查 `/etc/dfs/dfstab` 文件是否只选中了一个文件系统以使用 `-public` 选项进行共享。每台服务器上只能建立一个公共文件句柄，因此使用此选项在每台服务器上只能共享一个文件系统。

`WARNING: No network locking on` *hostname*`:` *path*`: contact admin to install server change`
描述: NFS 客户机未能成功尝试与 NFS 服务器上的网络锁定管理器建立连接。生成此警告旨在提醒您锁定不起作用，而不是表明挂载失败。

解决方法: 请使用提供完全锁定管理器支持的新版本的 OS 来升级服务器。

◆ ◆ ◆ 第 6 章

访问网络文件系统（参考）

本章介绍 NFS 命令，以及 NFS 环境的各个部分和这些部分协同工作的方式。

注 – 如果系统启用了区域并且您要在非全局区域中使用此功能，请参见《系统管理指南：Oracle Solaris Containers－资源管理和 Oracle Solaris Zones》以了解更多信息。

NFS 文件

任何计算机上的 NFS 活动都需要若干文件来支持。其中许多文件是 ASCII 文件，但也有一些文件是数据文件。表 6–1 中列出了这些文件及其功能。

表 6–1 NFS 文件

文件名	功能
`/etc/default/autofs`	列出 autofs 环境的配置信息。
`/etc/default/fs`	列出本地文件系统的缺省文件系统类型。
`/etc/default/nfs`	列出 `lockd` 和 `nfsd` 的配置信息。有关更多信息，请参阅第 125 页中的 “`/etc/default/nfs` 文件的关键字”和 `nfs(4)` 手册页。
`/etc/default/nfslogd`	列出 NFS 服务器日志记录守护进程 `nfslogd` 的配置信息。

表 6–1 NFS 文件 （续）

文件名	功能
/etc/dfs/dfstab	列出要共享的本地资源。
/etc/dfs/fstypes	列出远程文件系统的缺省文件系统类型。
/etc/dfs/sharetab	列出共享的本地资源和远程资源。请参见 sharetab(4) 手册页。请勿编辑此文件。
/etc/mnttab	列出当前挂载的文件系统，包括自动挂载的目录。请参见 mnttab(4) 手册页。请勿编辑此文件。
/etc/netconfig	列出传输协议。请勿编辑此文件。
/etc/nfs/nfslog.conf	列出 NFS 服务器日志记录的常规配置信息。
/etc/nfs/nfslogtab	列出与 nfslogd 进行日志后期处理相关的信息。请勿编辑此文件。
/etc/nfssec.conf	列出 NFS 安全服务。
/etc/rmtab	列出由 NFS 客户机远程挂载的文件系统。请参见 rmtab(4) 手册页。请勿编辑此文件。
/etc/vfstab	定义要本地挂载的文件系统。请参见 vfstab(4) 手册页。

/etc/dfs/fstypes 中的第一项通常用作远程文件系统的缺省文件系统类型。此项将 NFS 文件系统类型定义为缺省类型。

/etc/default/fs 中只有一项：本地磁盘的缺省文件系统类型。通过检查 /kernel/fs 中的文件，可以确定客户机或服务器支持的文件系统类型。

/etc/default/autofs 文件

从 Solaris 10 发行版开始，可以使用 /etc/default/autofs 文件来配置 autofs 环境。具体来说，此文件提供了配置 autofs 命令和 autofs 守护进程的其他方法。在命令行上制定的规范也可以通过此配置文件实现。但是，与命令行上制定的规范不同的是，此文件将保留您的规范，即使在升级操作系统时也是如此。另外，不再需要更新关键的启动文件即可确保保留 autofs 环境的现有行为。可通过为以下关键字提供值来制定规范：

AUTOMOUNT_TIMEOUT
: 设置在取消挂载文件系统之前文件系统保持空闲的持续时间。此关键字与 automount 命令的 -t 参数等效。缺省值为 600。

AUTOMOUNT_VERBOSE
: 提供有关 autofs 挂载、取消挂载和其他不重要事件的通知。此关键字与 automount 的 -v 参数等效。缺省值为 FALSE。

AUTOMOUNTD_VERBOSE
在控制台上记录状态消息。此关键字与 automountd 守护进程的 -v 参数等效。缺省值为 FALSE。

AUTOMOUNTD_NOBROWSE
针对所有 autofs 挂载点打开或关闭浏览功能。此关键字与 automountd 的 -n 参数等效。缺省值为 FALSE。

AUTOMOUNTD_TRACE
扩展每个远程过程调用 (remote procedure call, RPC) 并在标准输出中显示扩展的 RPC。此关键字与 automountd 的 -T 参数等效。缺省值为 0。取值范围为 0 到 5。

AUTOMOUNTD_ENV
允许您将不同的值指定给不同的环境。此关键字与 automountd 的 -D 参数等效。可以多次使用 AUTOMOUNTD_ENV 关键字。但是，必须对每个环境赋值使用单独的行。

有关更多信息，请参阅 automount(1M) 和 automountd(1M) 手册页。有关过程信息，请参阅第 97 页中的 “如何使用 /etc/default/autofs 文件配置 autofs 环境”。

/etc/default/nfs 文件的关键字

在 NFS 版本 4 中，可以在 /etc/default/nfs 文件中设置以下关键字。这些关键字控制客户机和服务器使用的 NFS 协议。

NFS_SERVER_VERSMIN
设置要注册且由服务器提供的 NFS 协议的最低版本。从 Solaris 10 发行版开始，缺省值为 2。其他有效值包括 3 或 4。请参阅第 86 页中的 “设置 NFS 服务”。

NFS_SERVER_VERSMAX
设置要注册且由服务器提供的 NFS 协议的最高版本。从 Solaris 10 发行版开始，缺省值为 4。其他有效值包括 2 或 3。请参阅第 86 页中的 “设置 NFS 服务”。

NFS_CLIENT_VERSMIN
设置由 NFS 客户机使用的 NFS 协议的最低版本。从 Solaris 10 发行版开始，缺省值为 2。其他有效值包括 3 或 4。请参阅第 86 页中的 “设置 NFS 服务”。

NFS_CLIENT_VERSMAX
设置由 NFS 客户机使用的 NFS 协议的最高版本。从 Solaris 10 发行版开始，缺省值为 4。其他有效值包括 2 或 3。请参阅第 86 页中的 “设置 NFS 服务”。

NFS_SERVER_DELEGATION
控制是否对服务器启用 NFS 版本 4 委托功能。如果启用此功能，则服务器将尝试对 NFS 版本 4 客户机提供委托。缺省情况下，会启用服务器委托。要禁用服务器委托，请参见第 88 页中的 “如何在服务器上选择不同版本的 NFS”。有关更多信息，请参阅第 165 页中的 “NFS 版本 4 中的委托”。

NFSMAPID_DOMAIN
为客户机和服务器设置公共域。将忽略使用本地 DNS 域名的缺省行为。有关任务信息，请参阅第 86 页中的 “设置 NFS 服务”。另请参见第 131 页中的 “nfsmapid 守护进程”。

/etc/default/nfslogd 文件

此文件定义了使用 NFS 服务器日志记录时所使用的某些参数。可以定义以下参数。

CYCLE_FREQUENCY
确定在循环使用日志文件之前必须经过的小时数。缺省值为 24 小时。此选项用于防止日志文件变得太大。

IDLE_TIME
设置 `nfslogd` 在检查缓冲区文件中是否存在更多信息之前应处于休眠状态的秒数。此参数还确定检查配置文件的频率。此参数与 MIN_PROCESSING_SIZE 一同确定处理缓冲区文件的频率。缺省值为 300 秒。增加该秒数即可通过减少检查次数来提高性能。

MAPPING_UPDATE_INTERVAL
指定对文件句柄到路径映射表中的记录进行更新的间隔秒数。缺省值为 86400 秒，即一天。此参数有助于保持文件句柄到路径映射表始终处于最新状态，而不必不断更新这些表。

MAX_LOGS_PRESERVE
确定要保存的日志文件数目。缺省值为 10。

MIN_PROCESSING_SIZE
设置在处理和写入日志文件之前缓冲区文件必须达到的最小字节数目。此参数与 IDLE_TIME 一同确定处理缓冲区文件的频率。缺省值为 524288 字节。增加该字节数即可通过减少处理缓冲区文件的次数来提高性能。

PRUNE_TIMEOUT
选择文件句柄到路径映射记录超时之前必须经过的、并可以缩减的小时数。缺省值为 168 小时，即 7 天。

UMASK
为 `nfslogd` 创建的日志文件指定文件模式创建掩码。缺省值为 0137。

/etc/nfs/nfslog.conf 文件

此文件定义了 `nfslogd` 使用的日志记录的路径、文件名和类型。每个定义都与 *tag* 相关联。启动 NFS 服务器日志记录时，需要您标识每个文件系统的 *tag*。全局标记定义了缺省值。可以根据需要将各个标记与以下参数一起使用。

defaultdir=*path*
指定日志记录文件的缺省目录路径。除非您指定了不同的目录，否则缺省目录为 `/var/nfs`。

log=*path/filename*
设置日志文件的路径和文件名。缺省值为 `/var/nfs/nfslog`。

fhtable=*path/filename*
选择文件句柄到路径数据库文件的路径和文件名。缺省值为 `/var/nfs/fhtable`。

buffer=*path/filename*
确定缓冲区文件的路径和文件名。缺省值为 `/var/nfs/nfslog_workbuffer`。

logformat=*basic*|*extended*
选择创建用户可读日志文件时使用的格式。基本 (basic) 格式产生的日志文件与某些 `ftpd` 守护进程类似。扩展 (extended) 格式提供了更详细的视图。

如果未指定路径，则使用由 `defaultdir` 定义的路径。另外，还可以使用绝对路径覆盖 `defaultdir`。

为了更容易地识别文件，请将文件置于单独的目录中。下面的示例列出了所需的更改。

```
% cat /etc/nfs/nfslog.conf
#ident  "@(#)nfslog.conf        1.5     99/02/21 SMI"
#
  .
  .
# NFS server log configuration file.
#

global  defaultdir=/var/nfs \
        log=nfslog fhtable=fhtable buffer=nfslog_workbuffer

publicftp log=logs/nfslog fhtable=fh/fhtables buffer=buffers/workbuffer
```

在本示例中，以 `log=publicftp` 形式共享的任何文件系统都使用以下值：

- 缺省目录为 `/var/nfs`。
- 日志文件存储在 `/var/nfs/logs/nfslog*` 中。
- 文件句柄到路径数据库表存储在 `/var/nfs/fh/fhtables` 中。
- 缓冲区文件存储在 `/var/nfs/buffers/workbuffer` 中。

有关过程信息，请参阅第 80 页中的 “如何启用 NFS 服务器日志记录”。

NFS 守护进程

为了支持 NFS 活动，在系统进入运行级 3 或多用户模式时将启动多个守护进程。mountd 和 nfsd 守护进程在作为服务器的系统上运行。服务器守护进程的自动启动取决于 /etc/dfs/sharetab 中是否存在带有 NFS 文件系统类型标签的项。为了支持 NFS 文件锁定，应该在 NFS 客户机和服务器上运行 lockd 和 statd 守护进程。但是，与以前版本的 NFS 不同，在 NFS 版本 4 中，不使用守护进程 lockd、statd、mountd 和 nfslogd。

本节介绍以下守护进程。

automountd 守护进程

该守护进程处理来自 autofs 服务的挂载和取消挂载请求。该命令的语法如下：

```
automountd [ -Tnv ] [ -D name= value ]
```

该命令采用以下几种方式运行：

- -T 启用跟踪。
- -n 对所有 autofs 节点禁用浏览功能。
- -v 选择将所有的状态消息记录到控制台。
- -D *name*=*value* 将替换 *name* 指示的自动挂载映射变量的 *value*。

自动挂载映射的缺省值为 /etc/auto_master。可使用 -T 选项进行故障排除。

lockd 守护进程

此守护进程支持对 NFS 文件进行记录锁定操作。lockd 守护进程针对网络锁定管理器 (Network Lock Manager, NLM) 协议管理客户机与服务器之间的 RPC 连接。该守护进程通常不使用任何选项即可启动。可将三个选项与此命令一起使用。请参见 lockd(1M) 手册页。可以在命令行中或通过编辑 /etc/default/nfs 中的相应字符串来使用这些选项。以下是可在 /etc/default/nfs 文件中设置的关键字的说明。

注 – 从 Solaris 10 发行版开始，LOCKD_GRACE_PERIOD 关键字和 -g 选项已过时。过时的关键字将由新的关键字 GRACE_PERIOD 取代。如果同时设置了这两个关键字，则 GRACE_PERIOD 的值将覆盖 LOCKD_GRACE_PERIOD 的值。请参见以下有关 GRACE_PERIOD 的说明。

与 LOCKD_GRACE_PERIOD类似，/etc/default/nfs 中的 GRACE_PERIOD=*graceperiod* 设置服务器重新引导后客户机回收 NFS 版本 3 锁定（由 NLM 提供）和版本 4 锁定所需的秒数。因此，GRACE_PERIOD 的值可控制 NFS 版本 3 和 NFS 版本 4 的锁定恢复的宽延期长度。

/etc/default/nfs 中的 LOCKD_RETRANSMIT_TIMEOUT=*timeout* 参数选择将锁定请求重新传输到远程服务器之前等待的秒数。此选项将影响 NFS 客户端服务。*timeout* 的缺省值为 15 秒。减小 *timeout* 值可以改善“嘈杂”网络上的 NFS 客户机的响应时间。但是，这种更改可能会增大锁定请求的频率，进而会导致增加服务器负载。使用 -t *timeout* 选项来启动该守护进程，即可在命令行中使用相同的参数。

/etc/default/nfs 中的 LOCKD_SERVERS= *nthreads* 参数指定服务器对于每个连接可处理的并发线程的最大数目。应根据 NFS 服务器上的预期负载来确定 *nthreads* 的值。缺省值为 20。使用 TCP 的每台 NFS 客户机都使用与 NFS 服务器之间的单一连接。因此，每台客户机最多可使用服务器上的 20 个并发线程。

使用 UDP 的所有 NFS 客户机都共享与 NFS 服务器之间的单一连接。在上述情况下，可能必须增加可用于 UDP 连接的线程数。对于每台 UDP 客户机而言，至少要有两个线程。但是，此数目具体取决于客户机上的工作负荷，因此每台客户机两个线程可能是不够的。使用更多线程的缺点是：使用线程越多，占用的 NFS 服务器内存就越多。但是，如果从不使用线程，则增加 *nthreads* 没有任何效果。通过使用 nthreads 选项来启动该守护进程，即可在命令行中使用相同的参数。

mountd 守护进程

该守护进程处理来自远程系统的文件系统挂载请求并提供访问控制。mountd 守护进程将检查 /etc/dfs/sharetab，以确定哪些文件系统可用于远程挂载，以及哪些系统允许执行远程挂载。可以将 -v 选项和 -r 选项与此命令结合使用。请参见 mountd(1M) 手册页。

-v 选项以详细模式运行该命令。NFS 服务器每次确定应授予客户机的访问权限时，都会在控制台上输出一条消息。在尝试确定客户机为何不能访问文件系统时，生成的信息可能非常有用。

-r 选项拒绝来自客户机的所有未来的挂载请求。此选项不会影响已挂载文件系统的客户机。

注 – NFS 版本 4 不使用该守护进程。

nfs4cbd 守护进程

`nfs4cbd` 专用于 NFS 版本 4 客户机，可管理 NFS 版本 4 回调程序的通信端点。该守护进程没有用户可访问的接口。有关更多信息，请参见 `nfs4cbd(1M)` 手册页。

nfsd 守护进程

该守护进程可处理其他客户机文件系统请求。可以将多个选项与此命令一起使用。有关完整列表，请参见 `nfsd(1M)` 手册页。可以在命令行中或通过编辑 `/etc/default/nfs` 中的相应字符串来使用这些选项。

`/etc/default/nfs` 中的 `NFSD_LISTEN_BACKLOG=`*length* 参数为 NFS 和 TCP 设置基于面向连接传输的连接队列的长度。缺省值为 32 项。使用 `-l` 选项来启动 `nfsd`，即可在命令行中执行相同的选择。

`/etc/default/nfs` 中的 `NFSD_MAX_CONNECTIONS=`*#-conn* 参数选择每个面向连接传输的最大连接数。*#-conn* 的缺省值没有限制。使用 `-c` *#-conn* 选项来启动该守护进程，即可在命令行中使用相同的参数。

`/etc/default/nfs` 中的 `NFSD_SERVER=`*nservers* 参数选择服务器可以处理的并发请求的最大数目。*nservers* 的缺省值为 16。使用 `nservers` 选项来启动 `nfsd`，即可在命令行中执行相同的选择。

与旧版本的该守护进程不同，`nfsd` 不会产生用于处理并发请求的多个副本。使用 `ps` 检查进程表时，将仅显示正在运行的守护进程的一个副本。

nfslogd 守护进程

该守护进程提供有关操作的日志记录。服务器上的哪些 NFS 操作将写入记录，取决于 `/etc/default/nfslogd` 中定义的配置选项。启用 NFS 服务器日志记录时，选定文件系统上的所有 RPC 操作的记录将由内核写入缓冲区文件。然后，`nfslogd` 将对这些请求进行后期处理。名称服务转换器用于帮助将 UID 映射为登录名，并将 IP 地址映射为主机名。如果无法通过确定的名称服务找到任何匹配项，则记录该数字。

还可以通过 `nfslogd` 来处理文件句柄到路径名的映射。该守护进程将跟踪文件句柄到路径映射表中的这些映射。对于在 `/etc/nfs/nfslogd` 中标识的每个标记，都存在一个映射表。经过后期处理后，这些记录将被写入 ASCII 日志文件中。

注 – NFS 版本 4 不使用该守护进程。

nfsmapid 守护进程

版本 4 的 NFS 协议 (RFC3530) 更改了用户标识符或组标识符（UID 或 GID）在客户机与服务器之间的交换方式。该协议要求分别采用 `user@nfsv4_domain` 或 `group@nfsv4_domain` 格式将文件的所有者属性和组属性作为字符串在 NFS 版本 4 客户机与 NFS 版本 4 服务器之间进行交换。

例如，用户 `known_user` 在 NFS 版本 4 客户机上具有 UID 123456，该客户机的完全限定主机名为 `system.example.com`。客户机为了向 NFS 版本 4 服务器发出请求，必须将 UID 123456 映射为 `known_user@example.com`，然后将此属性发送到 NFS 版本 4 服务器。NFS 版本 4 服务器希望接收 `user_or_group@nfsv4_domain` 格式的用户和组文件属性。服务器从客户机收到 `known_user@example.com` 后，就会将该字符串映射为底层文件系统可以识别的本地 UID 123456。此功能假设网络中的每个 UID 和 GID 都是唯一的，并且客户机中的 NFS 版本 4 域与服务器上的 NFS 版本 4 域匹配。

注 – 如果服务器不能识别给定的用户名或组名，即使 NFS 版本 4 域匹配，服务器也不能将该用户名或组名映射为其唯一 ID（整数值）。在这类情况下，服务器会将传入的用户名或组名映射为 `nobody` 用户。为了防止这类情况出现，管理员应避免创建仅在 NFS 版本 4 客户机上存在的特殊帐户。

NFS 版本 4 客户机和服务器都能执行整数到字符串和字符串到整数的转换。例如，在对 GETATTR 操作进行响应时，NFS 版本 4 服务器会将从底层文件系统获取的 UID 和 GID 映射到其各自的字符串说明中，并将此信息发送到客户机。此外，客户机也必须将 UID 和 GID 映射到字符串说明中。例如，在对 `chown` 命令进行响应时，客户机在将 SETATTR 操作发送到服务器之前会先将新的 UID 或 GID 映射到字符串说明中。

但是请注意，客户机和服务器将以不同的方式对不能识别的字符串做出响应：

- 如果用户不在服务器上，即使在同一 NFS 版本 4 域配置中，服务器也会拒绝远程过程调用 (remote procedure call, RPC) 并向客户机返回错误消息。这种情况将限制远程用户可以执行的操作。
- 如果用户同时存在于客户机和服务器中，但它们的域不匹配，服务器将拒绝属性修改操作（例如 SETATTR），这些操作要求服务器将传入的用户字符串映射为底层文件系统可以识别的整数值。要使 NFS 版本 4 客户机和服务器运行正常，它们的 NFS 版本 4 域（即 `@` 符号后的字符串部分）应相互匹配。
- 如果 NFS 版本 4 客户机不能识别来自服务器的用户名或组名，则客户机无法将字符串映射为其唯一的 ID（整数值）。在这类情况下，客户机会将传入的用户字符串或组字符串映射为 `nobody` 用户。映射为 `nobody` 将为不同的应用程序带来各种问题。至于 NFS 版本 4 功能，修改文件属性的操作将会失败。

可以将 sharectl 命令和以下选项配合使用来更改客户机和服务器的域名。

nfsmapid_domain
为客户机和服务器设置公共域。将忽略使用本地 DNS 域名的缺省行为。有关任务信息，请参阅第 86 页中的 “设置 NFS 服务”。

配置文件和 nfsmapid

下面介绍了 nfsmapid 守护进程使用 /etc/nsswitch.conf 和 /etc/resolv.conf 文件的方式：

- nfsmapid 使用标准的 C 库函数从后端名称服务中请求口令和组信息。这些名称服务由 /etc/nsswitch.conf 文件中的设置控制。对 nsswitch.conf 文件的任何更改都会影响 nfsmapid 操作。有关 nsswitch.conf 文件的更多信息，请参见 nsswitch.conf(4) 手册页。
- 为确保 NFS 版本 4 客户机能够从不同的域挂载文件系统，nfsmapid 将依赖于 DNS TXT 资源记录 (resource record, RR) _nfsv4idmapdomain 的配置。有关配置 _nfsv4idmapdomain 资源记录的更多信息，请参见第 133 页中的 “nfsmapid 和 DNS TXT 记录”。另外，还要注意以下几点：
  - 应该使用所需的域信息在 DNS 服务器上显式配置 DNS TXT RR。
  - 为了使 resolver 能够找到 DNS 服务器并搜索客户机和服务器 NFS 版本 4 域的 TXT 记录，应该使用所需的参数配置 /etc/resolv.conf 文件。

  有关更多信息，请参见以下内容：
  - 第 132 页中的 “优先级规则”
  - 第 135 页中的 “配置 NFS 版本 4 缺省域”
  - resolv.conf(4) 手册页

优先级规则

为了使 nfsmapid 能正常工作，NFS 版本 4 客户机和服务器必须具有相同的域。为了确保与 NFS 版本 4 域匹配，nfsmapid 将遵循以下严格的优先级规则：

1. 守护进程先检查 /etc/default/nfs 文件中是否有已指定给 NFSMAPID_DOMAIN 关键字的值。如果找到了值，则指定的值将优先于其他任何设置。指定的值将附加到外发属性字符串上，并与传入属性字符串进行比较。有关 /etc/default/nfs 文件中的关键字的更多信息，请参见第 125 页中的 “/etc/default/nfs 文件的关键字”。有关过程信息，请参见第 86 页中的 “设置 NFS 服务”。

   注 – 使用 NFSMAPID_DOMAIN 设置不具备可伸缩性，因此建议不要用于大型部署。

2. 如果未对 NFSMAPID_DOMAIN 指定值，则守护进程会从 DNS TXT RR 中查找域名。nfsmapid 将依赖于 /etc/resolv.conf 文件中由 resolver 中的一组例程所使用的指令。resolver 将在已配置的 DNS 服务器中搜索 _nfsv4idmapdomain TXT RR。请注意，使用 DNS TXT 记录具备更强的伸缩性。出于此原因，继续使用 TXT 记录比在 /etc/default/nfs 文件中设置关键字更好。
3. 如果未配置用于提供域名的 DNS TXT 记录，则 nfsmapid 守护进程将使用 /etc/resolv.conf 文件中的 domain 或 search 指令所指定的值，最后指定的指令优先级最高。

   在下面的示例中，同时使用了 domain 和 search 指令，nfsmapid 守护进程使用 search 指令后列出的第一个域 company.com。

   ```
   domain example.company.com
   search company.com foo.bar.com
   ```
4. 如果 /etc/resolv.conf 文件不存在，则 nfsmapid 将按照 domainname 命令的行为获取 NFS 版本 4 域名。具体来说，如果 /etc/defaultdomain 文件存在，则 nfsmapid 将该文件的内容用于 NFS 版本 4 域。如果 /etc/defaultdomain 文件不存在，则 nfsmapid 将使用由网络已配置名称服务提供的域名。有关更多信息，请参见 domainname(1M) 手册页。

nfsmapid 和 DNS TXT 记录

DNS 普遍存在的这一特性为 NFS 版本 4 域名提供了有效的存储和分配机制。此外，由于 DNS 固有的可伸缩性，使用 DNS TXT 资源记录是为大型部署配置 NFS 版本 4 域名的首选方法。您应该在企业级 DNS 服务器上配置 _nfsv4idmapdomain TXT 记录。此类配置可确保任何 NFS 版本 4 客户机或服务器都能通过遍历 DNS 树找到其 NFS 版本 4 域。

以下是用于使 DNS 服务器能够提供 NFS 版本 4 域名的首选项的示例：

```
_nfsv4idmapdomain        IN        TXT            "foo.bar"
```

在本示例中，要配置的域名是用双引号引起来的值。请注意，未指定 ttl 字段，且未将域附加到 _nfsv4idmapdomain（owner 字段中的值）中。此配置使 TXT 记录能够使用区域的颁发机构开始 (Start-Of-Authority, SOA) 记录中的 ${ORIGIN} 项。例如，在域名称空间的不同级别上，该记录的值可能为：

```
_nfsv4idmapdomain.subnet.yourcorp.com.    IN    TXT    "foo.bar"
_nfsv4idmapdomain.yourcorp.com.           IN    TXT    "foo.bar"
```

在使用 resolv.conf 文件搜索 DNS 树分层结构方面，此配置为 DNS 客户机提供了更大的灵活性。请参见 resolv.conf(4) 手册页。此功能提高了找到 TXT 记录的概率。为了获得更大的灵活性，较低级别的 DNS 子域可以定义其各自的 DNS TXT 资源记录 (resource record, RR)。此功能使较低级别的 DNS 子域可以覆盖由最高级别 DNS 域定义的 TXT 记录。

注 – TXT 记录指定的域可以是任意字符串，该字符串不一定与使用 NFS 版本 4 的客户机和服务器的 DNS 域匹配。您可以选择不与其他 DNS 域共享 NFS 版本 4 数据。

检查 NFS 版本 4 域

为网络 NFS 版本 4 域指定值之前，请检查是否已为网络配置 NFS 版本 4 域。下面的示例提供了标识网络 NFS 版本 4 域的方法。

- 要通过 DNS TXT RR 标识 NFS 版本 4 域，请使用 `nslookup` 命令或 `dig` 命令：

  以下是 `nslookup` 命令的样例输出：

  ```
  # nslookup -q=txt _nfsv4idmapdomain
  Server:         10.255.255.255
  Address:        10.255.255.255#53

  _nfsv4idmapdomain.example.company.com text = "company.com"
  ```

  请参见此 `dig` 命令的样例输出：

  ```
  # dig +domain=example.company.com -t TXT _nfsv4idmapdomain
  ...
  ;; QUESTION SECTION:
  ;_nfsv4idmapdomain.example.company.com. IN    TXT

  ;; ANSWER SECTION:
  _nfsv4idmapdomain.example.company.com. 21600 IN TXT   "company.com"

  ;; AUTHORITY SECTION:
  ...
  ```

  有关设置 DNS TXT RR 的信息，请参见第 133 页中的 “nfsmapid 和 DNS TXT 记录”。

- 如果网络没有配置 NFS 版本 4 DNS TXT RR，请使用以下命令从 DNS 域名中标识 NFS 版本 4 域：

  ```
  # egrep domain /etc/resolv.conf
  domain example.company.com
  ```

- 如果未配置 `/etc/resolv.conf` 文件以为客户机提供 DNS 域名，请使用以下命令从网络 NFS 版本 4 域配置中标识域：

  ```
  # cat /var/run/nfs4_domain
  company.com
  ```

- 如果正在使用其他名称服务（如 NIS），请使用以下命令标识为网络配置的命名服务的域。

  ```
  # domainname
  it.example.company.com
  ```

有关更多信息，请参见以下手册页：

- nslookup(1M)
- dig(1M)

- resolv.conf(4)
- domainname(1M)

配置 NFS 版本 4 缺省域

本节介绍网络如何获取所需的缺省域：

- 有关最新发行版，请参见第 135 页中的 “配置 NFS 版本 4 缺省域”。
- 对于初始 Solaris 10 发行版，请参见第 136 页中的 “在 Solaris 10 发行版中配置 NFS 版本 4 缺省域”。

配置 NFS 版本 4 缺省域

在初始 Solaris 10 发行版中，会在安装操作系统后首次重新引导系统过程中定义域。在以后的发行版中，将在安装操作系统过程中定义 NFS 版本 4 域。为提供此功能，添加了以下功能：

- `sysidtool` 命令包括 `sysidnfs4` 程序。此程序会在安装过程中运行以确定是否已为网络配置 NFS 版本 4 域。请参见 sysidtool(1M) 和 sysidnfs4(1M) 手册页。
- `sysidcfg` 文件具有一个新的关键字 `nfs4_domain`。此关键字可用于定义 NFS 版本 4 域。请注意，也可以在 `sysidcfg` 文件中定义其他关键字。请参见 sysidcfg(4) 手册页。

以下内容介绍该功能的运行方式：

1. `sysidnfs4` 程序检查 `/etc/.sysIDtool.state` 文件以确定是否已标识 NFS 版本 4 域。
   - 如果 `.sysIDtool.state` 文件显示已为网络配置 NFS 版本 4 域，则 `sysidnfs4` 程序将不会进行进一步的检查。请参见以下 `.sysIDtool.state` 文件的示例：

     ```
     1       # System previously configured?
     1       # Bootparams succeeded?
     1       # System is on a network?
     1       # Extended network information gathered?
     1       # Autobinder succeeded?
     1       # Network has subnets?
     1       # root password prompted for?
     1       # locale and term prompted for?
     1       # security policy in place
     1       # NFSv4 domain configured
     xterms
     ```

     `# NFSv4 domain configured` 前面显示的 `1` 确认已配置了 NFS 版本 4 域。
   - 如果 `.sysIDtool.state` 文件显示尚未为网络配置 NFS 版本 4 域，`sysidnfs4` 程序将进行进一步的检查。请参见以下 `.sysIDtool.state` 文件的示例：

     ```
     1       # System previously configured?
     1       # Bootparams succeeded?
     1       # System is on a network?
     1       # Extended network information gathered?
     1       # Autobinder succeeded?
     ```

```
1       # Network has subnets?
1       # root password prompted for?
1       # locale and term prompted for?
1       # security policy in place
0       # NFSv4 domain configured
xterms
```

`# NFSv4 domain configured` 前面显示的 `0` 确认尚未配置 NFS 版本 4 域。

2. 如果尚未标识 NFS 版本 4 域，`sysidnfs4` 程序将检查 `sysidcfg` 文件中的 `nfs4_domain` 关键字。
   - 如果 `nfs4_domain` 存在一个值，会将该值指定给 `/etc/default/nfs` 文件中的 NFSMAPID_DOMAIN 关键字。请注意，指定给 NFSMAPID_DOMAIN 的任何值都会覆盖 `nfsmapid` 守护进程的动态域选择功能。有关 `nfsmapid` 的动态域选择功能的更多信息，请参见第 132 页中的 “优先级规则”。
   - 如果 `nfs4_domain` 没有值，`sysidnfs4` 程序将标识 `nfsmapid` 从操作系统的已配置名称服务派生的域。此派生值作为缺省域显示在一个交互式提示中，通过该提示，您可以选择接受该缺省值，或指定其他 NFS 版本 4 域。

具备此功能后，以下功能将过时：

- 初始 Solaris 10 介质分发中提供的 JumpStart 样例脚本 `set_nfs4_domain` 已不再需要，不建议使用。
- 由 `sysidnfs4` 程序的旧版实现所创建的 `/etc/.NFS4inst_state.domain` 文件已不再需要。

注 – 由于 DNS 固有的普遍存在性和可伸缩性，使用 DNS TXT 记录配置大型 NFS 版本 4 部署域始终是首选和强烈建议的方法。请参见第 133 页中的 “`nfsmapid` 和 DNS TXT 记录”。

有关 Solaris 安装过程的特定信息，请参见以下内容：

- 《Oracle Solaris 10 9/10 安装指南：基本安装》
- 《Oracle Solaris 10 9/10 安装指南：基于网络的安装》

在 Solaris 10 发行版中配置 NFS 版本 4 缺省域

在 NFS 版本 4 的初始 Solaris 10 发行版中，如果您的网络包括多个 DNS 域，但只有单个 UID 和 GID 名称空间，则所有的客户机都必须对 NFSMAPID_DOMAIN 使用一个值。对于使用 DNS 的站点，`nfsmapid` 通过从您分配给 `_nfsv4idmapdomain` 的值中获取域名来解决此问题。有关更多信息，请参见第 133 页中的 “`nfsmapid` 和 DNS TXT 记录”。如果未将网络配置为使用 DNS，则在首次引导系统期间，OS 将使用 `sysidconfig(1M)` 实用程序为 NFS 版本 4 域名提供以下提示：

```
This system is configured with NFS version 4, which uses a
domain name that is automatically derived from the system's
name services. The derived domain name is sufficient for most
```

```
configurations. In a few cases, mounts that cross different
domains might cause files to be owned by nobody due to the
lack of a common domain name.

Do you need to override the system's default NFS verion 4 domain
name (yes/no)? [no]
```

缺省响应为 [no]。如果选择 [no]，将看到以下信息：

```
For more information about how the NFS version 4 default domain name is
derived and its impact, refer to the man pages for nfsmapid(1M) and
nfs(4), and the System Administration Guide: Network Services.
```

如果选择 [yes]，将看到以下提示：

```
Enter the domain to be used as the NFS version 4 domain name.
NFS version 4 domain name []:
```

注 – 如果 NFSMAPID_DOMAIN 的值存在于 /etc/default/nfs 中，则您提供的 [domain_name] 将覆盖该值。

有关 nfsmapid 的其他信息

有关 nfsmapid 的更多信息，请参见以下内容：

- nfsmapid(1M) 手册页
- nfs(4) 手册页
- http://www.ietf.org/rfc/rfc1464.txt
- 第 166 页中的 “NFS 版本 4 中的 ACL 和 nfsmapid”

statd 守护进程

该守护进程使用 lockd 为锁定管理器提供崩溃和恢复功能。statd 守护进程可跟踪在 NFS 服务器上保存锁定的客户机。如果服务器崩溃，则在重新引导时，服务器上的 statd 将与客户机上的 statd 进行联系。随后，客户机 statd 便会尝试回收服务器上的所有锁定。客户机 statd 还会通知服务器 statd 客户机发生崩溃的时间，以便可以清除服务器上的客户机锁定。使用此守护进程时没有可选择的选项。有关更多信息，请参见 statd(1M) 手册页。

在 Solaris 7 发行版中，statd 跟踪客户机的方式已改进。在所有早期的 Solaris 发行版中，statd 使用客户机的未限定主机名在 /var/statmon/sm 中为每台客户机创建文件。如果两台客户机在不同的域中，但共享同一主机名，或者如果客户机与 NFS 服务器不在同一个域中，则此文件命名将导致问题。因为未限定的主机名仅列出主机名，而不含任何域或 IP 地址信息，因此旧版本的 statd 无法区分这些类型的客户机。为了解决此问题，Solaris 7 statd 使用客户机的 IP 地址在 /var/statmon/sm 中创建了一个指向未限定主机名的符号链接。新的链接如下所示：

```
# ls -l /var/statmon/sm
lrwxrwxrwx   1 daemon          11 Apr 29 16:32 ipv4.192.168.255.255 -> myhost
lrwxrwxrwx   1 daemon          11 Apr 29 16:32 ipv6.fec0::56:a00:20ff:feb9:2734 -> v6host
--w-------   1 daemon          11 Apr 29 16:32 myhost
--w-------   1 daemon          11 Apr 29 16:32 v6host
```

在本示例中，客户机主机名为 `myhost`，客户机的 IP 地址为 `192.168.255.255`。如果另一台名为 `myhost` 的主机正在挂载文件系统，则两个符号链接都将指向该主机名。

注 – NFS 版本 4 不使用该守护进程。

NFS 命令

必须以 `root` 身份运行这些命令才能使其完全生效，但所有用户都可以发出信息请求：

- 第 138 页中的“`automount` 命令”
- 第 139 页中的“`clear_locks` 命令”
- 第 139 页中的“`fsstat` 命令”
- 第 140 页中的“`mount` 命令”
- 第 145 页中的“`mountall` 命令”
- 第 152 页中的“`setmnt` 命令”
- 第 146 页中的“`share` 命令”
- 第 150 页中的“`shareall` 命令”
- 第 151 页中的“`showmount` 命令”
- 第 144 页中的“`umount` 命令”
- 第 145 页中的“`umountall` 命令”
- 第 150 页中的“`unshare` 命令”
- 第 151 页中的“`unshareall` 命令”

automount 命令

此命令安装 autofs 挂载点，并将 automaster 文件中的信息与每个挂载点相关联。该命令的语法如下：

`automount [ -t` *duration* `] [ -v ]`

`-t` *duration* 用于设置文件系统持续处于挂载状态的时间（以秒为单位），而 `-v` 用于选择详细模式。在详细模式下运行此命令可以更容易排除故障。

如果未明确地进行设置，则持续时间值将设置为 5 分钟。在多数情况下，该值是合适的。但是，在具有许多自动挂载文件系统的系统上，可能需要增大持续时间值。特别是，如果服务器具有许多活动用户，则每 5 分钟检查一次自动挂载文件系统可能效率不高。每 1800 秒（即 30 分钟）检查一次 autofs 文件系统可能更理想。如果没有每 5 分

钟进行一次取消挂载文件系统，/etc/mnttab 就会变得很大。要减少 df 检查 /etc/mnttab 中每一项时的输出，可以使用 -F 选项（请参见 df(1M) 手册页）或使用 egrep 来过滤 df 的输出。

您应该考虑到，调整持续时间还会更改反映对自动挂载程序映射所做更改的速度。取消挂载文件系统之前，无法查看更改。有关如何修改自动挂载程序映射的说明，请参阅第 98 页中的 “修改映射”。

clear_locks 命令

通过此命令，可以删除 NFS 客户机的所有文件、记录和共享锁定。您必须是 root 才能运行此命令。从 NFS 服务器，可以清除对特定客户机的锁定。从 NFS 客户机，可以清除特定服务器上对该客户机的锁定。以下示例将清除对当前系统上名为 tulip 的 NFS 客户机的锁定。

```
# clear_locks tulip
```

使用 -s 选项可以指定要从中清除锁定的 NFS 主机。必须从创建锁定的 NFS 客户机运行此选项。在这种情况下，将从名为 bee 的 NFS 服务器中删除客户机锁定。

```
# clear_locks -s bee
```

注意 – 只有在客户机崩溃且无法清除其锁定时，才应运行此命令。为避免数据损坏问题，请不要清除对活动客户机的锁定。

fsstat 命令

从 Solaris 10 11/06 发行版开始，使用 fsstat 实用程序可以按文件系统类型和按挂载点监视文件系统操作。可以使用各种选项定制输出。请参见以下示例。

本示例显示 NFS 版本 3、版本 4 和 root 挂载点的输出。

```
% fsstat nfs3 nfs4 /
  new     name    name    attr    attr   lookup   rddir   read   read   write   write
 file    remov   chng     get     set      ops     ops    ops  bytes     ops   bytes
3.81K       90  3.65K   5.89M   11.9K    35.5M   26.6K   109K   118M   35.0K   8.16G  nfs3
  759      503    457   93.6K   1.44K     454K   8.82K  65.4K   827M     292    223K  nfs4
25.2K    18.1K  1.12K   54.7M    1017     259M   1.76M  22.4M  20.1G   1.43M   3.77G  /
```

本示例使用 -i 选项提供有关 NFS 版本 3、版本 4 和 root 挂载点的 I/O 操作的统计信息。

```
% fsstat -i nfs3 nfs4 /
 read     read    write    write    rddir    rddir    rwlock    rwulock
  ops    bytes      ops    bytes      ops    bytes       ops        ops
```

```
 109K    118M    35.0K   8.16G   26.6K   4.45M     170K      170K  nfs3
65.4K    827M      292    223K   8.82K   2.62M    74.1K     74.1K  nfs4
22.4M   20.1G    1.43M   3.77G   1.76M   3.29G    25.5M     25.5M  /
```

本示例使用 -n 选项提供有关 NFS 版本 3、版本 4 和 root 挂载点的命名操作的统计信息。

```
% fsstat -n nfs3 nfs4 /
lookup   creat   remov  link   renam  mkdir  rmdir   rddir  symlnk  rdlnk
 35.5M   3.79K      90     2   3.64K      5      0   26.6K      11   136K  nfs3
  454K     403     503     0     101      0      0   8.82K     356  1.20K  nfs4
  259M   25.2K   18.1K   114    1017     10      2   1.76M      12  8.23M  /
```

有关更多信息，请参见 fsstat(1M) 手册页。

mount 命令

使用此命令，可以将已命名的文件系统（本地或远程）附加到指定的挂载点。有关更多信息，请参见 mount(1M) 手册页。在不使用参数的情况下，mount 将显示当前在计算机上挂载的文件系统列表。

标准 Solaris 安装中包括许多类型的文件系统。每个文件系统类型都有特定的手册页，其中列出了适用于该文件系统类型的 mount 选项。NFS 文件系统的手册页为 mount_nfs(1M)。对于 UFS 文件系统，请参见 mount_ufs(1M)。

Solaris 7 发行版可以使用 NFS URL（而不是标准的 server:/pathname 语法）从 NFS 服务器选择要挂载的路径名。有关详细信息，请参见第 86 页中的 “如何使用 NFS URL 挂载 NFS 文件系统”。

注意 – 该 mount 命令版本不会对无效选项发出警告。该命令将默认忽略所有无法解释的选项。请确保验证所有已使用的选项，以防止出现意外行为。

NFS 文件系统的 mount 选项

以下内容列出了挂载 NFS 文件系统时可跟在 -o 标志后面的某些选项。有关完整的选项列表，请参阅 mount_nfs(1M) 手册页。

bg|fg
: 可以使用这些选项来选择挂载失败时的重试行为。bg 选项将导致挂载尝试在后台运行。fg 选项将导致挂载尝试在前台运行。缺省值为 fg，对于必须可用的文件系统而言，这是最佳选择。此选项可防止在挂载完成之前进行进一步处理。对于非关键文件系统，bg 是适合的选择，因为客户机在等待挂载请求完成的同时可以执行其他处理。

forcedirectio
: 此选项可改进大型连续数据传输的性能。数据将直接复制到用户缓冲区。不会在客户机的内核中执行任何缓存操作。缺省情况下，此选项处于关闭状态。

以前，所有写入请求都由 NFS 客户机和 NFS 服务器进行串行化。NFS 客户机已被修改，允许应用程序向单个文件发出并发写入以及并发读取和写入。您可以使用 `forcedirectio` 挂载选项在客户机上启用此功能。使用此选项时，您将为已挂载文件系统中的所有文件启用此功能。您还可以通过使用 `directio()` 接口在客户机的单个文件中启用此功能。除非启用了此功能，否则对文件的写入一定是串行化的。而且，如果正在进行并发写入或并发读取和写入，该文件将不再支持 POSIX 语义。

有关如何使用此选项的示例，请参阅第 143 页中的 “使用 `mount` 命令”。

largefiles
: 使用此选项，可以访问大于 2 GB 的文件。由于只能在服务器上控制是否可以访问大文件，因此在 NFS 版本 3 挂载中将默认忽略此选项。缺省情况下，所有的 UFS 文件系统都使用 `largefiles` 进行挂载。对于使用 NFS 版本 2 协议的挂载，`largefiles` 选项将导致挂载失败，且会出现错误。

nolargefiles
: 此选项用于 UFS 挂载，可以保证文件系统中不会存在大文件。请参见 `mount_ufs(1M)` 手册页。由于只能在 NFS 服务器上控制大文件的存在，因此使用 NFS 挂载时不存在用于 `nolargefiles` 的选项。系统将拒绝使用此选项尝试对文件系统进行 NFS 挂载，且会显示错误。

nosuid|suid
: 从 Solaris 10 发行版开始，`nosuid` 选项与指定 `nodevices` 选项和 `nosetuid` 选项等效。指定 `nodevices` 选项时，禁止在已挂载的文件系统上打开特定于设备的文件。指定 `nosetuid` 选项时，系统将忽略位于文件系统中的二进制文件的 `setuid` 位和 `setgid` 位。进程将使用执行该二进制文件的用户的权限运行。

  `suid` 选项与指定 `devices` 选项和 `setuid` 选项等效。指定 `devices` 选项时，允许在已挂载的文件系统上打开特定于设备的文件。指定 `setuid` 选项时，内核将接受位于文件系统中的二进制文件的 `setuid` 位和 `setgid` 位。

  如果这两个选项都没有指定，则缺省选项为 `suid`，这将提供指定 `devices` 选项和 `setuid` 选项这一缺省行为。

  下表介绍了将 `nosuid` 或 `suid` 与 `devices` 或 `nodevices`，以及 `setuid` 或 `nosetuid` 组合的效果。请注意，在每个选项组合中，限制性最强的选项将确定行为。

组合选项的行为	选项	选项	选项
与使用 `nosetuid` 和 `nodevices` 等效	`nosuid`	`nosetuid`	`nodevices`
与使用 `nosetuid` 和 `nodevices` 等效	`nosuid`	`nosetuid`	`devices`
与使用 `nosetuid` 和 `nodevices` 等效	`nosuid`	`setuid`	`nodevices`

组合选项的行为	选项	选项	选项
与使用 nosetuid 和 nodevices 等效	nosuid	setuid	devices
与使用 nosetuid 和 nodevices 等效	suid	nosetuid	nodevices
与使用 nosetuid 和 devices 等效	suid	nosetuid	devices
与使用 setuid 和 nodevices 等效	suid	setuid	nodevices
与使用 setuid 和 devices 等效	suid	setuid	devices

nosuid 选项为访问可能不可信服务器的 NFS 客户机提供了附加安全性。使用此选项挂载远程文件系统会减少通过导入不可信设备或导入不可信 setuid 二进制文件来升级特权的机会。所有这些选项在所有的 Solaris 文件系统中都是可用的。

public
与 NFS 服务器联系时，此选项将强制使用公共文件句柄。如果服务器支持公共文件句柄，则由于不使用 MOUNT 协议，挂载操作会比较快。此外，由于不使用 MOUNT 协议，公共选项允许穿过防火墙进行挂载。

rw|ro
-rw 和 -ro 选项指示文件系统以读写方式挂载还是以只读方式挂载。缺省值为读写，该选项适用于远程起始目录、邮件假脱机目录或需要由用户更改的其他文件系统。只读选项适用于不应该由用户更改的目录。例如，用户不应写入手册页的共享副本。

sec=*mode*
可以使用此选项指定在挂载事务期间使用的验证机制。*mode* 的值可以是以下之一。

- 对 Kerberos 版本 5 验证服务使用 krb5。
- 对具备完整性的 Kerberos 版本 5 使用 krb5i。
- 对具备保密性的 Kerberos 版本 5 使用 krb5p。
- 不进行验证时，使用 none。
- 对于 Diffie-Hellman (DH) 验证，使用 dh。
- 对于标准的 UNIX 验证，使用 sys。

上述模式还在 /etc/nfssec.conf 中进行了定义。

soft|hard
如果服务器没有做出响应，则使用 soft 选项挂载的 NFS 文件系统将返回错误。hard 选项将使挂载继续重试，直到服务器做出响应为止。缺省值为 hard，大多数文件系统都应该使用此选项。应用程序不会经常检查从使用 soft 选项挂载的文件系统返回的值，这可能会使应用程序出现故障或可能导致文件损坏。如果应用程序检查返回值，则在使用 soft 选项的情况下，路由问题和其他情况可能仍然会干扰应用程序或

导致文件损坏。在大多数情况下，不应该使用 soft 选项。如果文件系统是使用 hard 选项挂载的且不可用，则使用该文件系统的应用程序将挂起，直到该文件系统可用为止。

使用 mount 命令

请参阅以下示例。

- 在 NFS 版本 2 或版本 3 中，这两个命令以只读方式从服务器 bee 挂载 NFS 文件系统。

```
# mount -F nfs -r bee:/export/share/man /usr/man
```

```
# mount -F nfs -o ro bee:/export/share/man /usr/man
```

在 NFS 版本 4 中，以下命令行将完成同样的挂载。

```
# mount -F nfs -o vers=4 -r bee:/export/share/man /usr/man
```

- 在 NFS 版本 2 或版本 3 中，即使已挂载了 /usr/man，此命令也会使用 -O 选项强制在本地系统上挂载服务器 bee 中的手册页。请参见以下内容。

```
# mount -F nfs -O bee:/export/share/man /usr/man
```

在 NFS 版本 4 中，以下命令行将完成同样的挂载。

```
# mount -F nfs -o vers=4 -O bee:/export/share/man /usr/man
```

- 在 NFS 版本 2 或版本 3 中，此命令使用客户机故障转移。

```
# mount -F nfs -r bee,wasp:/export/share/man /usr/man
```

在 NFS 版本 4 中，以下命令行使用客户机故障转移。

```
# mount -F nfs -o vers=4 -r bee,wasp:/export/share/man /usr/man
```

注 – 在命令行中使用时，列出的服务器必须支持同一版本的 NFS 协议。在命令行中运行 mount 时，请不要同时使用版本 2 和版本 3 服务器。可以同时将这两个服务器与 autofs 一起使用。Autofs 会自动选择最合适的版本 2 或版本 3 服务器。

- 以下示例将 NFS URL 与 NFS 版本 2 或版本 3 中的 mount 命令结合使用。

```
# mount -F nfs nfs://bee//export/share/man /usr/man
```

以下示例将 NFS URL 与 NFS 版本 4 中的 mount 命令结合使用。

```
# mount -F nfs -o vers=4 nfs://bee//export/share/man /usr/man
```

- 使用 forcedirectio 挂载选项，客户机可以对文件进行并发写入以及并发读取和写入操作。下面是一个示例。

```
# mount -F nfs -o forcedirectio bee:/home/somebody /mnt
```

在本示例中，命令从服务器 bee 挂载 NFS 文件系统，并对目录 /mnt 中的每个文件启用并发读取和写入。启用对并发读取和写入的支持时，将发生以下情况。

- 客户机允许应用程序并行写入文件。
- 客户机上禁用缓存。因此，来自读取和写入的数据将保留在服务器上。更明确地说，由于客户机不会高速缓存已读取或写入的数据，所以将从服务器读取应用程序尚未为其自身高速缓存的所有数据。客户机的操作系统不会具有此数据的副本。通常，NFS 客户机将在内核中高速缓存数据以供应用程序使用。

  由于在客户机上禁用了缓存，因此将禁用读前进程和写后进程。当内核预料应用程序下一步可能请求的数据时会发生读前进程。然后，内核将提前启动收集该数据的进程。内核的目标是在应用程序请求数据之前将数据准备就绪。

  客户机使用写后进程增加写吞吐量。数据将被高速缓存到内存中，而不是在应用程序每次将数据写入文件时立即启动 I/O 操作。随后，数据将被写入磁盘。

  写后进程很可能会允许以较大的块写入数据，或者允许从应用程序异步写入数据。通常，使用较大块的结果是会增大吞吐量。异步写入允许应用程序处理和 I/O 处理之间有重叠。此外，异步写入可通过提供更好的 I/O 序列来允许存储子系统优化该 I/O。同步写入强制在存储子系统上使用可能不是最佳的 I/O 序列。
- 如果应用程序不准备处理未被高速缓存的数据语义，则性能可能会大大降低。多线程应用程序可以避免此问题。

注 – 如果未启用对并发写入的支持，则对所有的写入请求进行串行化。串行化请求时，将发生以下情况。如果正在处理写入请求，则第二个写入请求必须等待第一个写入请求完成之后才能继续进行。

- 使用不含参数的 `mount` 命令可以显示客户机上挂载的文件系统。请参见以下内容。

```
% mount
/ on /dev/dsk/c0t3d0s0 read/write/setuid on Wed Apr 7 13:20:47 2004
/usr on /dev/dsk/c0t3d0s6 read/write/setuid on Wed Apr 7 13:20:47 20041995
/proc on /proc read/write/setuid on Wed Apr 7 13:20:47 2004
/dev/fd on fd read/write/setuid on Wed Apr 7 13:20:47 2004
/tmp on swap read/write on Wed Apr 7 13:20:51 2004
/opt on /dev/dsk/c0t3d0s5 setuid/read/write on Wed Apr 7 13:20:51 20041995
/home/kathys on bee:/export/home/bee7/kathys
  intr/noquota/nosuid/remote on Wed Apr 24 13:22:13 2004
```

umount 命令

使用此命令，可以删除当前已挂载的远程文件系统。`umount` 命令支持 `-V` 选项，以便进行测试。您还可以使用 `-a` 选项一次取消挂载多个文件系统。如果 *mount-points* 中包括 `-a` 选项，则会取消挂载这些文件系统。如果不包括挂载点，则系统会尝试取消挂载 `/etc/mnttab` 中列出的所有文件系统，但“必需的”文件系统（如 `/`、`/usr`、`/var`、`/proc`、`/dev/fd` 和 `/tmp`）除外。由于文件系统已挂载并且在 `/etc/mnttab` 中应有一个对应项，因此无需包括一个表示此文件系统类型的标志。

`-f` 选项可强制取消挂载繁忙的文件系统。可以使用此选项来取消挂起因尝试挂载无法挂载的文件系统而处于挂起状态的客户机。

注意 – 如果强制取消挂载文件系统，则在写入文件的情况下会导致数据丢失。

请参见以下示例。

示例 6–1 取消挂载文件系统

本示例取消挂载在 `/usr/man` 上挂载的文件系统：

```
# umount /usr/man
```

示例 6–2 使用 umount 的选项

本示例显示了 `umount - a -V` 的运行结果：

```
# umount -a -V
umount /home/kathys
umount /opt
umount /home
umount /net
```

请注意，此命令实际上不会取消挂载文件系统。

mountall 命令

使用此命令可挂载文件系统表中列出的所有文件系统或特定的一组文件系统。此命令提供了执行以下操作的方法：

- 使用 `-F` *FSType* 选项选择要访问的文件系统类型
- 使用 `-r` 选项选择文件系统表中列出的所有远程文件系统
- 使用 `-l` 选项选择所有本地文件系统

由于所有标记为 NFS 文件系统类型的文件系统均为远程文件系统，因此在上述选项中，有一些是多余的。有关更多信息，请参见 `mountall(1M)` 手册页。

请注意，以下两个用户输入示例是等效的：

```
# mountall -F nfs
```

```
# mountall -F nfs -r
```

umountall 命令

使用此命令可取消挂载一组文件系统。`-k` 选项运行 `fuser -k` *mount-point* 命令来中止所有与 *mount-point* 关联的进程。`-s` 选项表示不会并行执行取消挂载。`-l` 指定将仅使用本地文件系统，`-r` 指定将仅使用远程文件系统。`-h` *host* 选项表示应取消挂载已命名主机中的所有文件系统。不能将 `-h` 选项与 `-l` 或 `-r` 合并使用。

以下是取消挂载从远程主机挂载的所有文件系统的示例：

```
# umountall -r
```

以下是取消挂载当前从服务器 bee 挂载的所有文件系统的示例：

```
# umountall -h bee
```

share 命令

使用此命令，可以在 NFS 服务器上挂载本地文件系统。另外，还可以使用 share 命令显示当前在系统上共享的文件系统列表。NFS 服务器必须处于运行状态才能使用 share 命令。如果 /etc/dfs/dfstab 中存在一项，则在系统引导过程中会自动启动 NFS 服务器软件。如果 NFS 服务器软件未运行，则此命令不会报告错误，因此必须验证此软件是否正在运行。

可以共享的对象包括任意目录树。但是，每个文件系统分层结构会受到文件系统所在的磁盘分片或磁盘分区的限制。例如，共享根 (/) 文件系统将不会同时共享 /usr，除非这些目录位于相同的磁盘分区或磁盘分片上。标准安装将根目录置于分片 0 中，将 /usr 置于分片 6 中。另外，共享 /usr 时将不会共享在 /usr 子目录上挂载的其他任何本地磁盘分区。

如果某个文件系统是一个已共享的更大文件系统的一部分，则不能共享此文件系统。例如，如果 /usr 和 /usr/local 位于同一磁盘分片上，则可以共享 /usr 或 /usr/local。但是，如果这两个目录需要使用不同的共享选项进行共享，则必须将 /usr/local 移到单独的磁盘分片上。

通过读写共享的文件系统的文件句柄，可以获取对只读共享的文件系统的访问权限。但是，这两个文件系统必须位于同一磁盘分片上。您可以创建更为安全的环境。请将那些需要读写的文件系统置于单独的分区或磁盘分片中，使其与需要以只读方式共享的文件系统分隔开来。

注 – 有关取消共享文件系统之后再重新共享此系统时 NFS 版本 4 如何运行的信息，请参阅第 160 页中的 “在 NFS 版本 4 中取消共享和重新共享文件系统”。

特定于非文件系统的 share 选项

以下是可以用于 -o 标志的一些选项。

rw|ro
: *pathname* 文件系统针对所有客户机是读写共享或只读共享。

rw=*accesslist*
: 文件系统仅对列出的客户机是读写共享。其他所有请求均被拒绝。从 Solaris 2.6 发行版开始，*accesslist* 中定义的客户机列表已进行了扩展。有关更多信息，请参见第 148 页中的 “使用 share 命令设置访问列表”。可以使用此选项来覆盖 -ro 选项。

特定于 NFS 的 share 选项

以下是可以用于 NFS 文件系统的选项。

aclok
: 使用此选项，可以将支持 NFS 版本 2 协议的 NFS 服务器配置为对 NFS 版本 2 客户机进行访问控制。如果不使用此选项，则会为所有客户机提供最低访问权限。如果使用此选项，则客户机具有最高访问权限。例如，在使用 `-aclok` 选项进行共享的文件系统上，如果某个用户具有读取权限，则所有用户均具有读取权限。但是，如果不使用此选项，本应具有访问权限的客户机也会被拒绝访问。确定是允许较多访问还是较少访问取决于已设置的安全系统。有关访问控制列表 (access control list, ACL) 的更多信息，请参见《系统管理指南：安全性服务》中的“使用访问控制列表保护 UFS 文件”。

注 – 要使用 ACL，请确保客户机和服务器运行的软件支持 NFS 版本 3 协议和 NFS_ACL 协议。如果该软件仅支持 NFS 版本 3 协议，则客户机可获取正确的访问权限，但不能处理 ACL。如果该软件支持 NFS_ACL 协议，则客户机可获取正确的访问权限，并且可处理 ACL。

---

anon=*uid*
: 可以使用 *uid* 来选择未验证的用户的用户 ID。如果将 *uid* 设置为 `-1`，则服务器会拒绝未验证的用户进行访问。通过设置 `anon=0` 可以授予超级用户访问权限，但是由于此选项允许未验证的用户具有超级用户访问权限，因此请改用 `root` 选项。

index=*filename*
: 用户访问 NFS URL 时，`-index=`*filename* 选项会强制装入 HTML 文件，而不是显示目录列表。如果在 HTTP URL 正在访问的目录中找到 `index.html` 文件，则此选项会模拟当前浏览器的操作。此选项相当于为 `httpd` 设置 `DirectoryIndex` 选项。例如，假定 `dfstab` 文件项与以下内容类似：

```
share -F nfs -o ro,public,index=index.html /export/web
```

这些 URL 随后会显示相同的信息：

```
nfs://<server>/<dir>
nfs://<server>/<dir>/index.html
nfs://<server>//export/web/<dir>
nfs://<server>//export/web/<dir>/index.html
http://<server>/<dir>
http://<server>/<dir>/index.html
```

log=*tag*
: 此选项可指定 `/etc/nfs/nfslog.conf` 中的标记，该文件中包含文件系统的 NFS 服务器日志记录配置信息。必须选择此选项才能启用 NFS 服务器日志记录。

nosuid
: 此选项表示应忽略所有启用 `setuid` 或 `setgid` 模式的尝试。NFS 客户机不能创建启用了 `setuid` 或 `setgid` 位的文件。

public
: -public 选项已添加到 share 命令中，以启用 WebNFS 浏览功能。使用此选项在一台服务器上只能共享一个文件系统。

root=*accesslist*
: 服务器会向列表中的主机提供超级用户访问权限。缺省情况下，服务器不会向任何远程主机提供 root 访问权限。如果选定的安全模式不是 -sec=sys，则只能在 *accesslist* 中包括客户机主机名。从 Solaris 2.6 发行版开始，*accesslist* 中定义的客户机列表已进行了扩展。有关更多信息，请参见第 148 页中的 “使用 share 命令设置访问列表”。

注意 – 授予其他主机超级用户访问权限会涉及许多安全问题。请慎用 -root= 选项。

root=*client-name*
: *client-name* 值可用于 AUTH_SYS 验证，以便对照 exportfs(1B) 提供的地址列表来检查客户机的 IP 地址。如果找到匹配项，则可以向共享的文件系统提供 root 访问权限。

root=*host-name*
: 对于安全 NFS 模式（如 AUTH_SYS 或 RPCSEC_GSS），服务器会对照访问列表派生的基于主机的主体名称列表来检查客户机的主体名称。客户机主体名称的通用语法为 root@*hostname*。对于 Kerberos V，语法为 root/*hostname.fully.qualified* @REALM。使用 *host-name* 值时，访问列表中的客户机必须具有某个主体名称的凭证。对于 Kerberos V，客户机必须具有其 root/ *hostname.fully.qualified*@REALM 主体名称的有效密钥表项。有关更多信息，请参见《系统管理指南：安全性服务》中的“配置 Kerberos 客户机”。

sec=*mode*[:*mode*]
: *mode* 选择获取对文件系统的访问权限所需的安全模式。缺省情况下，安全模式为 UNIX 验证。可以指定多种模式，但是每个命令行一次只能使用一种安全模式。每个 -mode 选项都应用于所有后续的 -rw、-ro、-rw=、-ro=、-root= 和 -window= 选项，直至遇到其他 -mode 为止。使用 -sec=none 可将所有用户映射为用户 nobody。

window=*value*
: *value* 选择 NFS 服务器上某个凭证的最长生命周期（以秒为单位）。缺省值为 30000 秒，即 8.3 小时。

使用 share 命令设置访问列表

在 Solaris 2.6 之前的发行版中，用于 share 命令的 -ro=、-rw= 或 -root= 选项的 *accesslist* 仅限于主机名或网络组名列表。从 Solaris 2.6 发行版开始，访问列表还可以包括域名、子网号或用于拒绝访问的项。由于不需要更改名称空间或维护较长的客户机列表，这些扩展简化了单个服务器上的文件访问控制。

以下命令为大多数系统提供只读访问权限，但是允许 rose 和 lilac 进行读写访问：

```
# share -F nfs -o ro,rw=rose:lilac /usr/src
```

在下面的示例中，只读访问权限指定给了 eng 网络组中的任意主机。专门为客户机 rose 提供了读写访问权限。

```
# share -F nfs -o ro=eng,rw=rose /usr/src
```

注 – 不能同时指定不带参数的 rw 和 ro。如果未指定读写选项，则缺省情况下会为所有客户机指定读写访问权限。

要使多台客户机共享一个文件系统，必须在同一行中键入所有选项。针对同一对象多次调用 share 命令时，将仅“记住”最后一个运行的命令。以下命令为三台客户机系统启用读写访问权限，但是仅为 rose 和 tulip 提供以 root 身份访问文件系统的权限。

```
# share -F nfs -o rw=rose:lilac:tulip,root=rose:tulip /usr/src
```

共享使用多种验证机制的文件系统时，请确保在正确的安全模式之后包含 -ro、-ro=、-rw、-rw=、-root 和 -window 选项。在本示例中，会为名为 eng 的网络组中的所有主机选择 UNIX 验证。这些主机只能以只读模式挂载文件系统。如果主机 tulip 和 lilac 使用 Diffie-Hellman 验证，则它们可以以读写模式挂载文件系统。使用这些选项时，即使主机 tulip 和 lilac 不使用 DH 验证，也可以以只读模式挂载文件系统。但是，必须在 eng 网络组中列出这些主机名。

```
# share -F nfs -o sec=dh,rw=tulip:lilac,sec=sys,ro=eng /usr/src
```

尽管 UNIX 验证是缺省安全模式，但如果使用 -sec 选项，也不会包含 UNIX 验证。因此，如果要将 UNIX 验证与其他任何验证机制一起使用，就必须包含 -sec=sys 选项。

通过在实际域名的前面添加一个点，可以在访问列表中使用 DNS 域名。点后面的字符串是域名，而不是全限定主机名。以下项允许挂载访问 eng.example.com 域中的所有主机：

```
# share -F nfs -o ro=.:.eng.example.com /export/share/man
```

在本示例中，单个 "." 与通过 NIS 或 NIS+ 名称空间匹配的所有主机相匹配。从这些名称服务返回的结果中不包括域名。".eng.example.com" 项与所有使用 DNS 进行名称空间解析的主机相匹配。DNS 始终返回全限定主机名。因此，如果使用了 DNS 和其他名称空间的组合，则需要较长的项。

通过在实际网络号或网络名的前面添加 "@"，可以在访问列表中使用子网号。此字符可将网络名与网络组或全限定主机名区分开来。必须在 /etc/networks、NIS 或 NIS+ 名称空间中标识子网。如果 192.168 子网已标识为 eng 网络，则以下各项具有相同效果：

```
# share -F nfs -o ro=@eng /export/share/man
# share -F nfs -o ro=@192.168 /export/share/man
# share -F nfs -o ro=@192.168.0.0 /export/share/man
```

最后两项表明无需包括完整的网络地址。

如果网络前缀不是按字节对齐的，即与无类别域间路由 (Classless Inter-Domain Routing, CIDR) 一样，则可以在命令行中显式指定掩码长度。掩码长度可通过在网络名或网络号后添加一条斜杠和地址前缀中的有效位数进行定义。例如：

```
# share -f nfs -o ro=@eng/17 /export/share/man
# share -F nfs -o ro=@192.168.0/17 /export/share/man
```

在上述示例中，"/17" 表示地址中的前 17 位将用作掩码。有关 CIDR 的其他信息，请查阅 RFC 1519。

另外，还可以通过在项的前面放置 "-" 来选择拒绝访问。请注意，各项是从左到右读取的。因此，必须将拒绝访问项放置在应用了拒绝访问项的项之前：

```
# share -F nfs -o ro=-rose:.eng.example.com /export/share/man
```

本示例将允许对 eng.example.com 域中除了名为 rose 的主机之外的任何主机进行访问。

unshare 命令

使用此命令，可使以前可供挂载的文件系统不能再由客户机挂载。可以使用 unshare 命令取消共享任何文件系统，无论此文件系统使用 share 命令进行显式共享还是通过 /etc/dfs/dfstab 自动共享。如果使用 unshare 命令取消共享通过 dfstab 文件共享的文件系统，请务必谨慎。请记住，退出再重新进入运行级 3 时，会再次共享文件系统。如果要保持这一更改，则必须从 dfstab 文件中删除此文件系统的项。

取消共享 NFS 文件系统时，将禁止从具有现有挂载的客户机进行访问。文件系统可能仍挂载在客户机上，但是无法再访问其中的文件。

注 – 有关取消共享文件系统之后再重新共享此系统时 NFS 版本 4 如何运行的信息，请参阅第 160 页中的 “在 NFS 版本 4 中取消共享和重新共享文件系统”。

以下是取消共享某个特定文件系统的示例：

```
# unshare /usr/src
```

shareall 命令

使用此命令可共享多个文件系统。如果在不带选项的情况下使用此命令，则可以共享 /etc/dfs/dfstab 中的所有项。您可以包括一个文件名来指定其中列出了 share 命令行的文件的名称。如果没有包括文件名，则会检查 /etc/dfs/dfstab。如果使用 "-" 来替换文件名，则可以从标准输入中键入 share 命令。

以下是共享本地文件中列出的所有文件系统的示例：

```
# shareall /etc/dfs/special_dfstab
```

unshareall 命令

此命令可使所有当前共享的资源不可用。-F *FSType* 选项可选择 /etc/dfs/fstypes 中定义的文件系统类型的列表。使用此标志，可以仅选择要取消共享的某些文件系统类型。/etc/dfs/fstypes 中定义了缺省的文件系统类型。要选择特定的文件系统，请使用 unshare 命令。

以下是取消共享所有 NFS 类型的文件系统的示例：

```
# unshareall -F nfs
```

showmount 命令

此命令可显示以下内容之一：

- 已经远程挂载了通过 NFS 服务器共享的文件系统的所有客户机
- 仅由客户机挂载的文件系统
- 具有客户机访问信息的共享文件系统

注 – showmount 命令仅显示 NFS 版本 2 和版本 3 的导出内容。此命令不显示 NFS 版本 4 的导出内容。

此命令的语法如下：

showmount [-ade] [*hostname*]

-a	输出所有远程挂载的列表。每项都包括客户机名称和目录。
-d	输出由客户机远程挂载的目录的列表。
-e	输出共享或导出的文件的列表。
hostname	选择要从中收集信息的 NFS 服务器。

如果未指定 *hostname*，则会对本地主机进行查询。

以下命令列出了所有客户机以及这些客户机已挂载的本地目录：

```
# showmount -a bee
lilac:/export/share/man
lilac:/usr/src
rose:/usr/src
tulip:/export/share/man
```

以下命令列出了已挂载的目录：

```
# showmount -d bee
/export/share/man
/usr/src
```

以下命令列出了已共享的文件系统：

```
# showmount -e bee
/usr/src                                (everyone)
/export/share/man                     eng
```

setmnt 命令

此命令可创建 /etc/mnttab 表。mount 和 umount 命令会查阅该表。通常不必手动运行此命令，因为它会在系统引导时自动运行。

用于解决 NFS 问题的命令

这些命令在解决 NFS 问题时会非常有用。

nfsstat 命令

可以使用此命令来收集有关 NFS 和 RPC 连接的统计信息。该命令的语法如下：

```
nfsstat [ -cmnrsz ]
```

-c　显示客户端信息

-m　显示每个已挂载 NFS 文件系统的统计信息

-n　指定要同时显示在客户端和服务器端的 NFS 信息

-r　显示 RPC 统计信息

-s　显示服务器端信息

-z　指定应将统计信息设置为零

如果未在命令行中提供任何选项，则使用 -cnrs 选项。

向计算环境中添加新的软件或硬件时，收集服务器端统计信息对于调试问题非常重要。每周最少运行一次此命令并存储运行结果可以保留以前执行情况的完整历史记录。

请参阅以下示例：

```
# nfsstat -s

Server rpc:
Connection oriented:
calls      badcalls   nullrecv   badlen     xdrcall    dupchecks  dupreqs
719949194  0          0          0          0          58478624   33
Connectionless:
calls      badcalls   nullrecv   badlen     xdrcall    dupchecks  dupreqs
73753609   0          0          0          0          987278     7254

Server nfs:
calls                badcalls
787783794            3516
Version 2: (746607 calls)
null       getattr    setattr    root       lookup     readlink   read
883 0%     60 0%      45 0%      0 0%       177446 23% 1489 0%    537366 71%
wrcache    write      create     remove     rename     link       symlink
0 0%       1105 0%    47 0%      59 0%      28 0%      10 0%      9 0%
mkdir      rmdir      readdir    statfs
26 0%      0 0%       27926 3%   108 0%
Version 3: (728863853 calls)
null          getattr       setattr       lookup        access
1365467 0%    496667075 68% 8864191 1%    66510206 9%   19131659 2%
readlink      read          write         create        mkdir
414705 0%     80123469 10%  18740690 2%   4135195 0%    327059 0%
symlink       mknod         remove        rmdir         rename
101415 0%     9605 0%       6533288 0%    111810 0%     366267 0%
link          readdir       readdirplus   fsstat        fsinfo
2572965 0%    519346 0%     2726631 0%    13320640 1%   60161 0%
pathconf      commit
13181 0%      6248828 0%
Version 4: (54871870 calls)
null                compound
266963 0%           54604907 99%
Version 4: (167573814 operations)
reserved            access              close               commit
0 0%                2663957 1%          2692328 1%          1166001 0%
create              delegpurge          delegreturn         getattr
167423 0%           0 0%                1802019 1%          26405254 15%
getfh               link                lock                lockt
11534581 6%         113212 0%           207723 0%           265 0%
locku               lookup              lookupp             nverify
230430 0%           11059722 6%         423514 0%           21386866 12%
open                openattr            open_confirm        open_downgrade
2835459 1%          4138 0%             18959 0%            3106 0%
putfh               putpubfh            putrootfh           read
52606920 31%        0 0%                35776 0%            4325432 2%
readdir             readlink            remove              rename
606651 0%           38043 0%            560797 0%           248990 0%
renew               restorefh           savefh              secinfo
2330092 1%          8711358 5%          11639329 6%         19384 0%
setattr             setclientid         setclientid_confirm verify
453126 0%           16349 0%            16356 0%            2484 0%
write               release_lockowner   illegal
3247770 1%          0 0%                0 0%

Server nfs_acl:
Version 2: (694979 calls)
```

```
null         getacl       setacl       getattr      access       getxattrdir
0 0%         42358 6%     0 0%         584553 84%   68068 9%     0 0%
Version 3: (2465011 calls)
null         getacl       setacl       getxattrdir
0 0%         1293312 52%  1131 0%      1170568 47%
```

以上列出的是 NFS 服务器统计信息的示例。前五行与 RPC 有关，其余行则报告 NFS 活动。在两组统计信息中，了解 `badcalls` 或 `calls` 的平均数以及每周的调用次数有助于确定问题。`badcalls` 值报告来自客户机的错误消息数。该值可以表明网络硬件问题。

某些连接会在磁盘上生成写入活动。这些统计信息的突然增加可能表明出现了问题，应该对这一现象进行调查。对于 NFS 版本 2 的统计信息，要注意的连接包括 `setattr`、`write`、`create`、`remove`、`rename`、`link`、`symlink`、`mkdir` 和 `rmdir`。对于 NFS 版本 3 和版本 4 的统计信息，要注意 `commit` 的值。如果 `commit` 在某台 NFS 服务器中的级别高于在另一台几乎相同的服务器中的级别，请检查 NFS 客户机是否具有足够的内存。客户机没有可用资源时，服务器上的 `commit` 操作数将增加。

pstack 命令

此命令可显示每个进程的栈跟踪。`pstack` 命令必须由相应进程的所有者或 `root` 运行。可以使用 `pstack` 来确定进程挂起的位置。此命令允许使用的唯一选项是要检查的进程的 `PID`。请参见 `proc(1)` 手册页。

以下示例检查正在运行的 `nfsd` 进程。

```
# /usr/bin/pgrep nfsd
243
# /usr/bin/pstack 243
243:    /usr/lib/nfs/nfsd -a 16
 ef675c04 poll     (24d50, 2, ffffffff)
 000115dc ???????? (24000, 132c4, 276d8, 1329c, 276d8, 0)
 00011390 main     (3, effff14, 0, 0, ffffffff, 400) + 3c8
 00010fb0 _start   (0, 0, 0, 0, 0, 0) + 5c
```

此示例显示进程正在等待新的连接请求，这是正常响应。如果栈显示在发出请求之后进程仍在轮询，则此进程可能被挂起。请遵照第 113 页中的 “如何重新启动 NFS 服务”中的说明来解决此问题。请查看第 110 页中的 “NFS 故障排除过程”中的说明来充分验证问题是否是程序已挂起。

rpcinfo 命令

此命令可生成有关系统上正在运行的 RPC 服务的信息。另外，还可以使用此命令来更改 RPC 服务。许多选项都可用于此命令。请参见 `rpcinfo(1M)` 手册页。以下是可用于此命令的某些选项的简短概要。

`rpcinfo [ -m | -s ] [ hostname ]`

`rpcinfo -T` *transport hostname* [*progname*]

`rpcinfo [ -t | -u ]` [*hostname*] [*progname*]

`-m` 显示 `rpcbind` 操作的统计信息表

`-s` 显示所有已注册的 RPC 程序的简明列表

`-T` 显示有关使用特定传输或协议的服务的信息

`-t` 探测使用 TCP 的 RPC 程序

`-u` 探测使用 UDP 的 RPC 程序

transport 为服务选择传输或协议

hostname 选择需要其中信息的服务器的主机名

progname 选择收集有关其信息的 RPC 程序

如果未指定 *hostname* 的值，则使用本地主机名。可以将 *progname* 替换为 RPC 程序编号，但是很多用户可能会记住名称而记不住编号。可以在不运行 NFS 版本 3 软件的系统上使用 `-p` 选项（而非 `-s` 选项）。

此命令生成的数据可包括以下内容：

- RPC 程序编号
- 特定程序的版本号
- 正在使用的传输协议
- RPC 服务的名称
- RPC 服务的所有者

以下示例收集有关正在服务器上运行的 RPC 服务的信息。此命令生成的文本将通过 `sort` 命令过滤，以便使输出更具可读性。多个列出 RPC 服务的行已从本示例中删除。

```
% rpcinfo -s bee |sort -n
   program version(s) netid(s)                         service     owner
    100000  2,3,4     udp6,tcp6,udp,tcp,ticlts,ticotsord,ticots rpcbind     superuser
    100001  4,3,2     ticlts,udp,udp6                   rstatd      superuser
    100002  3,2       ticots,ticotsord,tcp,tcp6,ticlts,udp,udp6 rusersd     superuser
    100003  3,2       tcp,udp,tcp6,udp6                 nfs         superuser
    100005  3,2,1     ticots,ticotsord,tcp,tcp6,ticlts,udp,udp6 mountd      superuser
    100007  1,2,3     ticots,ticotsord,ticlts,tcp,udp,tcp6,udp6 ypbind      superuser
    100008  1         ticlts,udp,udp6                   walld       superuser
    100011  1         ticlts,udp,udp6                   rquotad     superuser
    100012  1         ticlts,udp,udp6                   sprayd      superuser
    100021  4,3,2,1   tcp,udp,tcp6,udp6                 nlockmgr    superuser
    100024  1         ticots,ticotsord,ticlts,tcp,udp,tcp6,udp6 status      superuser
    100029  3,2,1     ticots,ticotsord,ticlts           keyserv     superuser
    100068  5         tcp,udp                           cmsd        superuser
    100083  1         tcp,tcp6                          ttdbserverd superuser
    100099  3         ticotsord                         autofs      superuser
    100133  1         ticots,ticotsord,ticlts,tcp,udp,tcp6,udp6 -           superuser
    100134  1         ticotsord                         tokenring   superuser
```

```
    100155  1         ticots,ticotsord,tcp,tcp6        smserverd   superuser
    100221  1         tcp,tcp6                         -           superuser
    100227  3,2       tcp,udp,tcp6,udp6                nfs_acl     superuser
    100229  1         tcp,tcp6                         metad       superuser
    100230  1         tcp,tcp6                         metamhd     superuser
    100231  1         ticots,ticotsord,ticlts          -           superuser
    100234  1         ticotsord                        gssd        superuser
    100235  1         tcp,tcp6                         -           superuser
    100242  1         tcp,tcp6                         metamedd    superuser
    100249  1         ticots,ticotsord,ticlts,tcp,udp,tcp6,udp6 -           superuser
    300326  4         tcp,tcp6                         -           superuser
    300598  1         ticots,ticotsord,ticlts,tcp,udp,tcp6,udp6 -           superuser
    390113  1         tcp                              -           unknown
 805306368  1         ticots,ticotsord,ticlts,tcp,udp,tcp6,udp6 -           superuser
1289637086  1,5       tcp                              -           26069
```

以下两个示例说明如何通过在服务器上选择特定的传输来收集有关特定 RPC 服务的信息。第一个示例检查通过 TCP 运行的 `mountd` 服务。第二个示例检查通过 UDP 运行的 NFS 服务。

```
% rpcinfo -t bee mountd
program 100005 version 1 ready and waiting
program 100005 version 2 ready and waiting
program 100005 version 3 ready and waiting
% rpcinfo -u bee nfs
program 100003 version 2 ready and waiting
program 100003 version 3 ready and waiting
```

snoop 命令

此命令通常用于查看网络中的包。必须以 `root` 身份运行 `snoop` 命令。使用此命令是一种确保网络硬件在客户机和服务器上都正常运行的好方法。可以使用许多选项。请参见 snoop(1M) 手册页。以下是此命令的简短概要：

`snoop [ -d` *device* `] [ -o` *filename* `] [ host` *hostname* `]`

`-d` *device*　　指定本地网络接口

`-o` *filename*　　将所有捕获到的包存储在已命名的文件中

hostname　　显示仅进出特定主机的包

`-d` *device* 选项在具有多个网络接口的服务器上非常有用。除了设置主机之外，还可以使用许多表达式。命令表达式与 `grep` 的组合通常可以生成极其有用的数据。

排除故障时，请确保包进出相应的主机。另外，还应查找错误消息。将包保存到文件中可以简化查看数据的过程。

truss 命令

使用此命令可以检查某个进程是否已被挂起。`truss` 命令必须由相应进程的所有者或由 `root` 运行。可以将许多选项用于此命令。请参见 `truss(1)` 手册页。以下是此命令的简短语法。

`truss [ -t` *syscall* `] -p` *pid*

`-t` *syscall*　　选择要跟踪的系统调用

`-p` *pid*　　指明要跟踪的进程的 PID

syscall 可以是要跟踪的系统调用的列表，各系统调用之间以逗号分隔。另外，在 *syscall* 前面添加 ! 可选择不跟踪所列出的系统调用。

本示例说明进程正在等待来自新客户机的另一个连接请求。

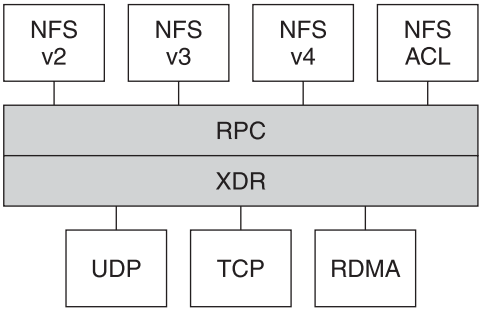
```
# /usr/bin/truss -p 243
poll(0x00024D50, 2, -1)         (sleeping...)
```

以上示例表示一个正常响应。如果在发出新连接请求之后该响应未发生更改，则此进程可能会被挂起。请遵照第 113 页中的 “如何重新启动 NFS 服务”中的说明来修复被挂起的程序。请查看第 110 页中的 “NFS 故障排除过程”中的说明来充分验证问题是否是程序已挂起。

NFS Over RDMA

Solaris 10 发行版中包括远程直接内存访问 (Remote Direct Memory Access, RDMA) 协议，这是一种通过高速网络实现内存到内存数据传输的技术。具体来说，RDMA 可提供不受 CPU 干预而直接进出内存的远程数据传输。RDMA 还可提供直接数据放置，这消除了数据副本，因此进一步消除了 CPU 干预。这样，RDMA 不仅减轻了主机 CPU 的负担，而且还减少了主机内存和 I/O 总线的争用。为提供此功能，RDMA 将 SPARC 平台上 InfiniBand 的互连 I/O 技术与 Solaris 操作系统相结合。下图说明了 RDMA 与其他协议（如 UDP 和 TCP）的关系。

图 6–1 RDMA 与其他协议的关系



NFS 是位于 RPC 层之上的一组协议。
XDR（外部数据表示，eXternal Data Representation）层将 RPC 参数和 RPC 结果编码到几个 RPC 传输协议（如 UDP、TCP 和 RDMA）之一。

如果 RDMA 传输在客户机和服务器上都不可用，则 TCP 传输为首选备用传输协议，如果 TCP 不可用，则会再使用 UDP。但是请注意，如果使用 `proto=rdma` 挂载选项，则会强制 NFS 挂载仅使用 RDMA。

有关 NFS 挂载选项的更多信息，请参见 `mount_nfs(1M)` 手册页和第 140 页中的 “mount 命令”。

注 – 用于 InfiniBand 的 RDMA 会使用 IP 寻址格式和 IP 查找基础结构来指定对等点。但是，由于 RDMA 是单独的协议栈，因此它没有完全实现所有的 IP 语义。例如，RDMA 并不使用 IP 寻址来与对等点进行通信。因此，RDMA 可能会跳过基于 IP 地址的各种安全策略配置。但是，不会跳过 NFS 和 RPC 管理策略，如 `mount` 限制和安全 RPC。

NFS 服务如何工作

以下各节介绍了 NFS 软件的一些复杂功能。请注意，本节说明的某些功能仅适用于 NFS 版本 4。

- 第 173 页中的 “WebNFS 服务如何工作”
- 第 174 页中的 “Web 浏览器使用的 WebNFS 限制”
- 第 174 页中的 “安全 NFS 系统”
- 第 175 页中的 “安全 RPC”

注 – 如果系统启用了区域并且您要在非全局区域中使用此功能，请参见《系统管理指南： Oracle Solaris Containers－资源管理和 Oracle Solaris Zones》以了解更多信息。

NFS 中的版本协商

NFS 启动过程包括协商服务器和客户机的协议级别。如果未指定版本级别，则缺省情况下将选择最佳级别。例如，如果客户机和服务器都可以支持版本 3，则会使用版本 3。如果客户机或服务器只能支持版本 2，则会使用版本 2。

从 Solaris 10 发行版开始，可以在 `/etc/default/nfs` 文件中设置关键字 NFS_CLIENT_VERSMIN、NFS_CLIENT_VERSMAX、NFS_SERVER_VERSMIN 和 NFS_SERVER_VERSMAX。为服务器和客户机指定的最小值和最大值将取代这些关键字的缺省值。对于客户机和服务器，最小缺省值为 2，最大缺省值为 4。请参见 第 125 页中的 “`/etc/default/nfs` 文件的关键字”。为查找服务器所支持的版本，NFS 客户机会从 NFS_CLIENT_VERSMAX 的设置开始，然后依次尝试每个版本，直到遇到 NFS_CLIENT_VERSMIN 的版本设置为止。一旦找到所支持的版本，此过程便会终止。例如，如果 NFS_CLIENT_VERSMAX=4 而 NFS_CLIENT_VERSMIN=2，则客户机会首先尝试版本 4，然后尝试版本 3，最后尝试版本 2。如果 NFS_CLIENT_VERSMIN 和 NFS_CLIENT_VERSMAX 设置为相同的值，则客户机会始终使用此版本，而不会尝试任何其他版本。如果服务器不提供此版本，挂载将会失败。

注 – 可以使用带有 `vers` 选项的 `mount` 命令来覆盖通过协商确定的值。请参见 `mount_nfs(1M)` 手册页。

有关过程信息，请参阅第 86 页中的 “设置 NFS 服务”。

NFS 版本 4 的功能

在版本 4 中对 NFS 进行了许多更改。本节介绍这些新功能。

- 第 160 页中的 “在 NFS 版本 4 中取消共享和重新共享文件系统”
- 第 160 页中的 “NFS 版本 4 中的文件系统名称空间”
- 第 162 页中的 “NFS 版本 4 中的可变文件句柄”
- 第 163 页中的 “NFS 版本 4 中的客户机恢复”
- 第 164 页中的 “NFS 版本 4 中的 `OPEN` 共享支持”

- 第 165 页中的 “NFS 版本 4 中的委托”
- 第 166 页中的 “NFS 版本 4 中的 ACL 和 nfsmapid”
- 第 171 页中的 “NFS 版本 4 中的客户端故障转移”

注 – 从 Solaris 10 发行版开始，NFS 版本 4 不支持 LIPKEY/SPKM 安全风格。另外，NFS 版本 4 也不会使用 `mountd`、`nfslogd` 和 `statd` 守护进程。

有关与使用 NFS 版本 4 相关的过程信息，请参阅第 86 页中的 “设置 NFS 服务”。

在 NFS 版本 4 中取消共享和重新共享文件系统

如果同时使用 NFS 版本 3 和版本 4，则客户机尝试访问一个已经取消共享的文件系统时，服务器会以错误代码响应。但是，如果使用 NFS 版本 3，则服务器会保留客户机在取消共享文件系统之前所获取的所有锁定。这样，重新共享文件系统时，NFS 版本 3 客户机即可访问此文件系统，就好像从未取消共享此文件系统一样。

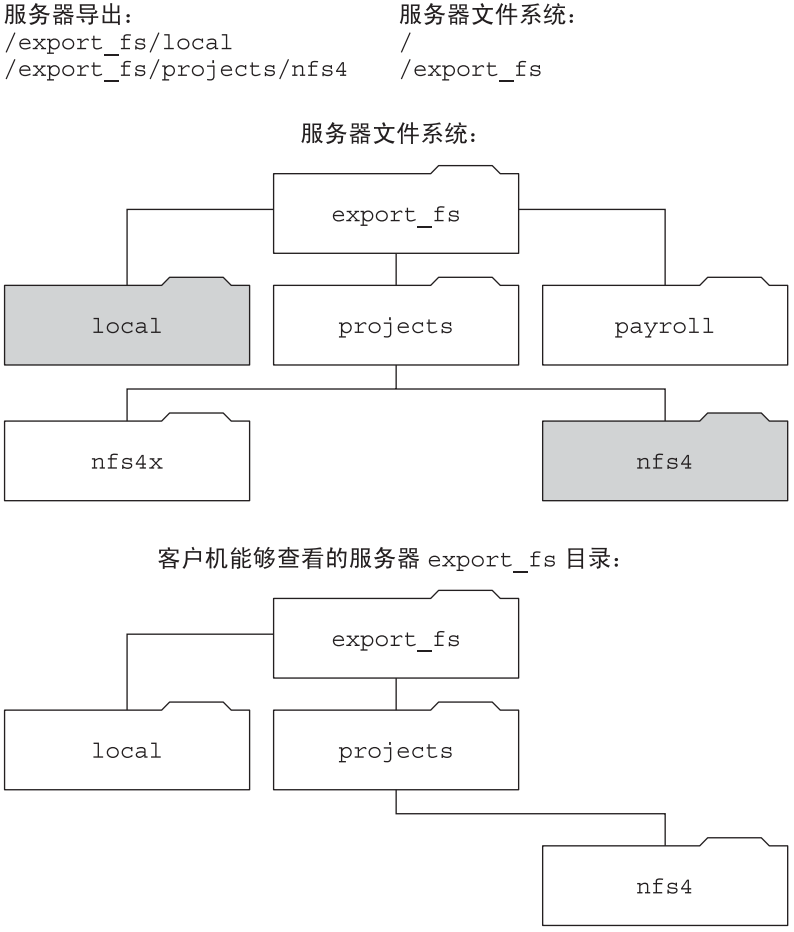
如果使用 NFS 版本 4，则取消共享文件系统时，将破坏此文件系统中任何已打开文件或文件锁定的所有状态。如果客户机尝试访问这些文件或锁定，则会收到一条错误消息。通常会将此错误消息作为 `I/O` 错误报告给应用程序。但是请注意，通过重新共享当前共享的文件系统来更改选项不会破坏服务器上的任何状态。

有关信息，请参阅第 163 页中的 “NFS 版本 4 中的客户机恢复” 或参见 `unshare_nfs(1M)` 手册页。

NFS 版本 4 中的文件系统名称空间

NFS 版本 4 服务器可创建并维护一个伪文件系统，此系统使客户机能够对服务器上所有导出的对象进行无缝访问。在 NFS 版本 4 之前，不存在伪文件系统。客户机会强制挂载每个共享服务器文件系统来进行访问。请参考以下示例。

图 6–2 服务器文件系统和客户机文件系统的视图



请注意，客户机无法看到 `payroll` 目录和 `nfs4x` 目录，因为这些目录未被导出，也没有通向导出目录。但是，客户机可以看到 `local` 目录，因为 `local` 是一个导出的目录。客户机还可看到 `projects` 目录，因为 `projects` 通向导出目录 `nfs4`。因此，未显式导出的服务器名称空间的部分内容会与伪文件系统桥接，该文件系统仅显示导出目录和那些通向服务器导出目录的目录。

伪文件系统是服务器创建的仅包含目录的结构。伪文件系统允许客户机浏览已导出文件系统的分层结构。因此，客户机的伪文件系统视图限制为仅显示通向已导出文件系统的路径。

以前的 NFS 版本不允许客户机在未挂载每个文件系统的情况下遍历服务器文件系统。但是，在 NFS 版本 4 中，服务器名称空间可进行以下操作：

- 将客户机的文件系统视图限制为仅显示通向服务器导出的目录。
- 使客户机能够对服务器导出目录进行无缝访问，而不要求客户机挂载每个底层文件系统。请参见前面的示例。但是请注意，某些操作系统可能会要求客户机挂载每个服务器文件系统。

由于与 POSIX 相关的原因，Solaris NFS 版本 4 客户机不会跨越服务器的文件系统边界。如果尝试进行这类操作，则客户机会使目录显示为空。要修正这种情况，必须针对服务器的每个文件系统执行挂载。

NFS 版本 4 中的可变文件句柄

文件句柄是在服务器上创建的，其中包含唯一标识文件和目录的信息。在 NFS 版本 2 和 3 中，服务器会返回持久性文件句柄。这样，客户机即可确保服务器会生成始终引用同一文件的文件句柄。例如：

- 如果删除某个文件并将其替换为同名文件，则服务器会为新文件生成新的文件句柄。如果客户机使用旧的文件句柄，则服务器会返回一条错误消息，说明此文件句柄已过时。
- 如果重命名文件，则文件句柄将保持不变。
- 如果必须重新引导服务器，则文件句柄将保持不变。

因此，当服务器从客户机收到包括文件句柄的请求时，解决方案会非常简单，并且文件句柄会始终引用正确的文件。

这种为 NFS 操作标识文件和目录的方法对大多数基于 UNIX 的服务器都很有效。但是，此方法不能在依赖其他标识方法（如文件的路径名）的服务器上实施。为了解决此问题，NFS 版本 4 协议允许服务器声明其文件句柄为可变句柄。这样，即可更改文件句柄。如果文件句柄确实已更改，则客户机必须找到新的文件句柄。

与 NFS 版本 2 和 3 一样，Solaris NFS 版本 4 服务器始终提供持久性文件句柄。但是，访问非 Solaris NFS 版本 4 服务器的 Solaris NFS 版本 4 客户机必须在服务器使用可变文件句柄时支持这些句柄。具体来说，当服务器通知客户机文件句柄可变时，客户机必须高速缓存路径名和文件句柄之间的映射。客户机会一直使用可变文件句柄，直到句柄过期为止。文件句柄过期后，客户机会执行以下操作：

- 刷新引用此文件句柄的高速缓存信息
- 搜索此文件的新文件句柄
- 重试此操作

注 – 服务器会始终通知客户机哪些文件句柄为持久性句柄，哪些文件句柄为可变句柄。

可变文件句柄可能会由于以下任一原因过期：

- 关闭文件
- 迁移文件句柄的文件系统
- 客户机重命名文件
- 服务器重新引导

请注意，如果客户机无法找到新的文件句柄，则会在 `syslog` 文件中放入一条错误消息。进一步尝试访问此文件会失败，并显示 `I/O` 错误。

NFS 版本 4 中的客户机恢复

NFS 版本 4 协议为有状态协议。如果客户机和服务器都保留有关以下内容的当前信息，协议即为有状态协议。

- 打开的文件
- 文件锁定

出现故障（如服务器崩溃）时，客户机和服务器会协同工作，重新建立故障前已存在的打开状态和锁定状态。

服务器崩溃并重新引导时，会丢失其状态。客户机检测到服务器已经重新引导后，将启动帮助服务器重建其状态的进程。此进程称为客户机恢复，因为由客户机引导此进程。

客户机发现服务器已经重新引导后，便会立即暂停其当前活动并启动客户机恢复进程。启动恢复进程时，系统错误日志 `/var/adm/messages` 中会显示如下消息。

```
NOTICE: Starting recovery server basil.example.company.com
```

在恢复进程中，客户机会向服务器发送有关客户机以前状态的信息。但是请注意，在此期间，客户机不会向服务器发送任何新请求。任何打开文件或设置文件锁定的新请求都必须等到服务器完成其恢复期之后才能继续进行。

客户机恢复进程完成时，系统错误日志 `/var/adm/messages` 中会显示以下消息。

```
NOTICE: Recovery done for server basil.example.company.com
```

现在，客户机已经成功地将其状态信息发送给服务器。不过，尽管此客户机已经完成了此进程，但是其他客户机可能尚未完成将其状态信息发送给服务器这一进程。因此，在一段时间内，服务器不会接受任何打开或锁定请求。指定这段时间（称为宽延期）旨在允许所有客户机完成其恢复。

在宽延期内，如果客户机尝试打开任何新文件或建立任何新锁定，服务器都会拒绝请求并显示 `GRACE` 错误代码。收到此错误后，客户机必须等到宽延期结束，然后才能向服务器重新发送请求。在宽延期内，会显示以下消息。

```
NFS server recovering
```

请注意，在宽延期内，可以继续执行不打开文件或不设置文件锁定的命令。例如，ls 和 cd 命令不会打开文件或设置文件锁定。因此，不会暂停执行这些命令。但是，cat 之类可打开文件的命令会暂停执行，直到宽延期结束为止。

宽延期结束后，会显示以下消息。

```
NFS server recovery ok.
```

现在，客户机即可向服务器发送新的打开和锁定请求。

客户机恢复会因为各种原因而失败。例如，如果服务器重新引导后存在网络分区，则客户机可能无法在宽延期结束之前与服务器重新建立其状态。宽延期结束后，服务器不允许客户机重新建立其状态，因为新的状态操作可能会产生冲突。例如，新的文件锁定可能会与客户机尝试恢复的旧的文件锁定发生冲突。发生这种情况时，服务器会将 NO_GRACE 错误代码返回到客户机。

如果恢复某个特定文件的打开操作失败，客户机会将此文件标记为不可用，并显示以下消息。

```
WARNING: The following NFS file could not be recovered and was marked dead
(can't reopen:  NFS status 70):  file :  filename
```

请注意，数字 70 仅是一个示例。

如果在恢复过程中重新建立文件锁定失败，则会显示以下错误消息。

```
NOTICE: nfs4_send_siglost:  pid PROCESS-ID lost
lock on server SERVER-NAME
```

在这种情况下，会向进程发送 SIGLOST 信号。SIGLOST 信号的缺省操作是终止此进程。

要从此状态恢复，必须重新启动所有在失败时打开文件的应用程序。请注意，可能会出现以下情况。

- 一些没有重新打开文件的进程可能会收到 I/O 错误消息。
- 在恢复失败之后已重新打开文件或执行打开操作的其他进程可顺利访问文件。

因此，一些进程可以访问其他进程无法访问的特定文件。

NFS 版本 4 中的 OPEN 共享支持

NFS 版本 4 协议提供了几种文件共享模式，客户机可以使用这些模式控制其他客户机对文件的访问。客户机可以指定以下内容：

- DENY_NONE 模式，用于允许其他客户机对文件进行读写访问。
- DENY_READ 模式，用于拒绝其他客户机对文件进行读取访问。
- DENY_WRITE 模式，用于拒绝其他客户机对文件进行写入访问。

- DENY_BOTH 模式，用于拒绝其他客户机对文件进行读写访问。

Solaris NFS 版本 4 服务器完全实现了这些文件共享模式。因此，如果客户机尝试打开文件的方式与当前共享模式冲突，则服务器会通过使操作失败来拒绝此尝试。如果这类尝试在打开或创建操作开始时失败，则 NFS 版本 4 客户机会收到一条协议错误消息。此错误会映射为应用程序错误 EACCES。

尽管此协议提供了几种共享模式，但目前 Solaris 中的打开操作不提供多种共享模式。打开文件时，Solaris NFS 版本 4 客户机只能使用 DENY_NONE 模式。

另外，尽管 fcntl 系统调用使用 F_SHARE 命令来控制文件共享，但是 fcntl 命令无法在 NFS 版本 4 中正常实现。如果在 NFS 版本 4 客户机上使用这些 fcntl 命令，则客户机会向应用程序返回一条 EAGAIN 错误消息。

NFS 版本 4 中的委托

NFS 版本 4 为委托同时提供客户机支持和服务器支持。委托是服务器用于将文件管理委托给客户机的一种技术。例如，服务器可以授予客户机读取委托或写入委托。读取委托可以同时授予多台客户机，因为这些读取委托不会彼此冲突。写入委托只能授予一台客户机，因为写入委托会与其他任何客户机进行的任何文件访问相冲突。虽然客户机拥有写入委托，但是它不会向服务器发送各种操作，因为客户机保证具有对文件的独占访问权限。同样，客户机在拥有读取委托时也不会向服务器发送各种操作。这是因为服务器保证任何客户机都不能以写入模式打开文件。通过委托，可显著减少服务器和客户机之间针对被委托文件的交互。因此，可降低网络通信流量，并且提高客户机和服务器的性能。但是请注意，性能提高的程度取决于应用程序使用的文件交互的类型以及网络和服务器的拥塞量。

是否授予委托完全由服务器决定。客户机不会请求委托。服务器可根据文件的访问模式来决定是否授予委托。如果几台不同的客户机最近以写入模式访问了文件，则服务器可能不会授予委托。原因是此访问模式表明将来可能会发生冲突。

当客户机访问文件的方式与当前授予此文件的委托不一致时，便会发生冲突。例如，如果一台客户机拥有对文件的写入委托，同时另一台客户机打开此文件来进行读取或写入访问，则服务器会撤销第一台客户机的写入委托。同样，如果一台客户机拥有读取委托，同时另一台客户机打开同一个文件进行写入，则服务器会撤销读取委托。请注意，在这两种情况下都不会将委托授予第二台客户机，因为此时存在冲突。发生冲突时，服务器会使用回调机制来联系当前拥有委托的客户机。收到此回调后，客户机会向服务器发送文件的更新状态并返回委托。如果客户机无法对重新调用做出响应，则服务器会撤销委托。在此类情况下，服务器会拒绝客户机对此文件进行的所有操作，客户机将已请求的操作报告为失败。通常，这些失败会作为 I/O 错误报告给应用程序。要从这些错误中恢复，必须关闭文件，然后再重新打开。当客户机和服务器之间存在网络分区并且客户机拥有委托时，撤销委托会失败。

请注意，一台服务器不能解决对其他服务器上存储的文件的访问冲突。因此，NFS 服务器仅解决它自己存储的文件的冲突。此外，要响应由运行各种 NFS 版本的客户机导

致的冲突，NFS 服务器只能对运行 NFS 版本 4 的客户机启动重新调用。NFS 服务器不能对运行早期 NFS 版本的客户机启动重新调用。

检测冲突的进程会有所变化。例如，与 NFS 版本 4 不同，因为版本 2 和版本 3 不包括打开过程，所以仅会在客户机尝试读取、写入或锁定文件之后检测冲突。服务器对这些冲突的响应也会有所不同。例如：

- 对于 NFS 版本 3，服务器会返回 `JUKEBOX` 错误消息，这会导致客户机停止访问请求并稍后重试。客户机会输出消息 `File unavailable`。
- 对于 NFS 版本 2，因为不存在与 `JUKEBOX` 错误消息等效的消息，所以服务器不做任何响应，这会导致客户机等待然后再重试。客户机会输出消息 `NFS server not responding`。

解决了委托冲突之后，便不会存在这些情况。

缺省情况下，会启用服务器委托。可以通过修改 `/etc/default/nfs` 文件来禁用委托。有关过程信息，请参阅第 88 页中的 “如何在服务器上选择不同版本的 NFS”。

客户机委托不需要任何关键字。NFS 版本 4 回调守护进程 `nfs4cbd` 在客户机上提供回调服务。只要启用对 NFS 版本 4 的挂载，此守护进程就会自动启动。缺省情况下，客户机会针对 `/etc/netconfig` 系统文件中列出的所有 Internet 传输向服务器提供必需的回调信息。请注意，如果在客户机上启用了 IPv6 并且可以确定客户机名称的 IPv6 地址，则回调守护进程可接受 IPv6 连接。

回调守护进程使用临时的程序编号以及动态指定的端口号。此信息提供给服务器，服务器会在授予任何委托之前测试回调路径。如果回调路径测试不成功，则服务器不会授予委托，这是唯一可从外部看到的行为。

请注意，因为回调信息嵌在 NFS 版本 4 请求中，所以服务器不能通过使用网络地址转换 (Network Address Translation, NAT) 的设备来联系客户机。另外，回调守护进程还会使用动态端口号。因此，即使防火墙在端口 2049 上启用了正常的 NFS 流量，服务器可能仍然无法遍历防火墙。在此类情况下，服务器不会授予委托。

NFS 版本 4 中的 ACL 和 nfsmapid

访问控制列表 (access control list, ACL) 通过使文件的所有者可以为文件所有者、组以及其他特定用户和组定义文件权限来提供更好的文件安全性。ACL 是使用 `setfacl` 命令在服务器和客户机上设置的。有关更多信息，请参见 `setfacl(1)` 手册页。在 NFS 版本 4 中，ID 映射器 `nfsmapid` 用于将服务器上的 ACL 项中的用户 ID 或组 ID 映射为客户机上的 ACL 项中的用户 ID 或组 ID。相反的映射也能实现。ACL 项中的用户 ID 和组 ID 必须同时存在于客户机和服务器上。

ID 映射失败的原因

以下情况可能导致 ID 映射失败：

- 如果存在于服务器上 ACL 项中的用户或组不能映射为客户机上的有效用户或组，则不允许该用户读取客户机上的 ACL。

  例如，对于服务器上其用户 ID 或组 ID ACL 项不能映射为客户机上的用户 ID 或组 ID 的文件，在发出 `ls -lv` 或 `ls -lV` 命令时，会收到 `Permission denied` 错误消息。ID 映射器无法映射 ACL 中的用户或组。如果 ID 映射器能够映射该用户或组，则在通过 `ls -l` 生成的文件列表中，权限后面会显示一个加号 (+)。例如：

  ```
  % ls -l
  -rw-r--rw-+   1 luis    staff      11968 Aug 12  2005 foobar
  ```

  同样，`getfacl` 命令也会因为同样的原因返回 `Permission denied` 错误消息。有关此命令的更多信息，请参见 `getfacl(1)` 手册页。
- 如果不能将客户机上设置的任何 ACL 项中的用户 ID 或组 ID 映射为服务器上的有效用户 ID 或组 ID，则 `setfacl` 或 `chmod` 命令可能会失败，并返回 `Permission denied` 错误消息。
- 如果客户机和服务机的 NFSMAPID_DOMAIN 值不匹配，则 ID 映射将失败。有关更多信息，请参见第 125 页中的 “/etc/default/nfs 文件的关键字”。

避免 ACL 出现 ID 映射问题

为避免 ID 映射问题，请执行以下操作：

- 确保在 `/etc/default/nfs` 文件中正确设置了 NFSMAPID_DOMAIN 的值。
- 确保 ACL 项中的所有用户和组 ID 同时存在于 NFS 版本 4 客户机和服务器上。

检查是否存在未映射的用户 ID 或组 ID

要确定是否有无法在服务器或客户机上映射的用户或组，请使用以下脚本：

```
#! /usr/sbin/dtrace -Fs

sdt:::nfs4-acl-nobody
{
     printf("validate_idmapping: (%s) in the ACL could not be mapped!",
stringof(arg0));
}
```

注 – 此脚本中使用的探测器名称是一个接口，该接口以后可以更改。有关更多信息，请参见《Solaris 动态跟踪指南》中的“稳定性级别”。

有关 ACL 或 nfsmapid 的其他信息

请参见以下内容：

- 《系统管理指南：安全性服务》中的“使用 ACL 保护 UFS 文件（任务列表）”
- 《Oracle Solaris ZFS 管理指南》中的第 8 章 “使用 ACL 和属性保护 Oracle Solaris ZFS 文件”
- 第 131 页中的 “nfsmapid 守护进程”

UDP 和 TCP 协商

启动过程中，还会协商传输协议。缺省情况下，将选择客户机和服务器同时支持的第一个面向连接的传输。如果此选择未成功，则使用第一个可用的无连接传输协议。/etc/netconfig 中列出了系统支持的传输协议。TCP 是该发行版支持的面向连接的传输协议。UDP 是无连接传输协议。

如果 NFS 协议版本和传输协议都是通过协商确定的，则 NFS 协议版本优先于传输协议。使用 UDP 的 NFS 版本 3 协议比使用 TCP 的 NFS 版本 2 协议具有更高的优先级。可以使用 mount 命令手动选择 NFS 协议版本和传输协议。请参见 mount_nfs(1M) 手册页。在大多数情况下，允许协商选择最佳选项。

文件传输大小协商

文件传输大小确定在客户机与服务器之间传输数据时使用的缓冲区的大小。一般情况下，最好使用较大的传输大小。NFS 版本 3 协议的传输大小没有限制。但是，从 Solaris 2.6 发行版开始，软件规定缺省缓冲区大小为 32 KB。如果需要，客户机可以在挂载时规定较小的传输大小，但是在大多数情况下，此规定是没有必要的。

系统不会与使用 NFS 版本 2 协议的系统协商传输大小。在这种情况下，最大的传输大小将设置为 8 KB。

可以在 mount 命令中使用 -rsize 和 -wsize 选项来手动设置传输大小。对于某些 PC 客户机，可能需要减小传输大小。另外，如果将 NFS 服务器配置为使用较大的传输大小，则还可以增加传输大小。

注 – 从 Solaris 10 发行版开始，放宽了对线路传输大小的限制。传输大小取决于底层传输的能力。例如，对于 UDP，NFS 的传输限制仍然是 32 KB。但是，因为 TCP 是流协议，不受 UDP 的数据报限制，因此通过 TCP 的最大传输大小已经增加到 1 MB。

如何挂载文件系统

以下说明适用于 NFS 版本 3 挂载。NFS 版本 4 挂载过程既不包括端口映射服务，也不包括 MOUNT 协议。

客户机需要从服务器挂载文件系统时，客户机必须从服务器获取文件句柄。文件句柄必须与文件系统对应。此过程需要在客户机与服务器之间处理多项事务。在本示例中，客户机正在尝试从服务器挂载 /home/terry。此事务的 snoop 跟踪如下。

```
client -> server PORTMAP C GETPORT prog=100005 (MOUNT) vers=3 proto=UDP
server -> client PORTMAP R GETPORT port=33492
client -> server MOUNT3 C Null
server -> client MOUNT3 R Null
client -> server MOUNT3 C Mount /export/home9/terry
server -> client MOUNT3 R Mount OK FH=9000 Auth=unix
client -> server PORTMAP C GETPORT prog=100003 (NFS) vers=3 proto=TCP
server -> client PORTMAP R GETPORT port=2049
client -> server NFS C NULL3
server -> client NFS R NULL3
client -> server NFS C FSINFO3 FH=9000
server -> client NFS R FSINFO3 OK
client -> server NFS C GETATTR3 FH=9000
server -> client NFS R GETATTR3 OK
```

在此跟踪中，客户机首先从 NFS 服务器上的端口映射服务请求挂载端口号。客户机收到挂载端口号 (33492) 后，会使用该端口号测试服务器上服务的可用性。客户机确定服务正在该端口号上运行后，便会请求挂载。服务器对此请求做出响应时，服务器中会包含正在挂载的文件系统 (9000) 的文件句柄。随后，客户机将针对 NFS 端口号发送请求。客户机收到来自服务器的端口号后，客户机便会测试 NFS 服务 (nfsd) 的可用性。此外，客户机还会请求有关使用该文件句柄的文件系统的 NFS 信息。

在以下跟踪中，客户机正在使用 public 选项挂载文件系统。

```
client -> server NFS C LOOKUP3 FH=0000 /export/home9/terry
server -> client NFS R LOOKUP3 OK FH=9000
client -> server NFS C FSINFO3 FH=9000
server -> client NFS R FSINFO3 OK
client -> server NFS C GETATTR3 FH=9000
server -> client NFS R GETATTR3 OK
```

通过使用缺省的公共文件句柄（即 0000），系统将跳过所有要从端口映射服务获取信息并要确定 NFS 端口号的事务。

注 – NFS 版本 4 提供对可变文件句柄的支持。有关更多信息，请参阅第 162 页中的 “NFS 版本 4 中的可变文件句柄”。

挂载时 -public 选项和 NFS URL 的作用

使用 -public 选项可能会造成导致挂载失败的条件。添加 NFS URL 也可产生导致失败的情形。以下列表介绍了如何使用这些选项挂载文件系统的具体细节。

带有 NFS URL 的 public 选项－强制使用公共文件句柄。如果系统不支持公共文件句柄，则挂载将失败。

带有常规路径的 public 选项－强制使用公共文件句柄。如果系统不支持公共文件句柄，则挂载将失败。

仅 NFS URL－使用公共文件句柄（如果在 NFS 服务器上启用了此文件句柄）。如果在使用公共文件句柄时挂载失败，则尝试使用 MOUNT 协议进行挂载。

仅常规路径－不使用公共文件句柄，而使用 MOUNT 协议。

客户端故障转移

通过使用客户端故障转移，NFS 客户机可以识别使相同数据可用的多台服务器，并且在当前服务器不可用时可以切换到备用服务器。如果发生以下情况之一，则文件系统就会变得不可用。

- 文件系统连接到的服务器崩溃
- 服务器过载
- 出现网络故障

在上述情况下执行的故障转移通常对用户是透明的。因此，故障转移可以随时进行，而不会中断客户机上正在运行的进程。

故障转移要求采用只读方式挂载文件系统。文件系统必须相同，故障转移才能成功进行。有关使文件系统相同的原因说明，请参见第 171 页中的 “什么是复制的文件系统？ ”。静态文件系统或不常更改的文件系统是故障转移的最佳候选系统。

您不能对同一 NFS 挂载同时使用 CacheFS 和客户端故障转移。系统针对每个 CacheFS 文件系统存储了额外信息。故障转移期间不能更新此信息，因此挂载文件系统时只能使用这两个功能之一。

需要为每个文件系统建立的副本数目取决于许多因素。理想的情况是，应该至少具有两台服务器。每台服务器都应该支持多个子网。此设置比每个子网中具有唯一一台服务器更好。该过程要求检查列出的每台服务器。因此，列出的服务器越多，每个挂载的速度就越慢。

故障转移术语

要完全领会该过程，需要了解两个术语。

- **故障转移**－从支持复制的文件系统的服务器列表中选择服务器的过程。通常，使用已排序列表中的下一台服务器，除非该服务器无法做出响应。
- **重映射**－使用新的服务器。在正常使用中，客户机在远程文件系统上存储每个活动文件的路径名。在重映射期间，系统将评估这些路径名以在新的服务器上找到这些文件。

什么是复制的文件系统？

为了实现故障转移，当其中每个文件大小都相同且文件大小或文件类型与原始文件系统相同时，可以将这样的文件系统称为**副本**。不考虑权限、创建日期和其他文件属性。如果文件大小或文件类型不同，则重映射将失败，且该过程将挂起，直到旧的服务器可用为止。在 NFS 版本 4 中，该行为是不同的。请参见第 171 页中的 “NFS 版本 4 中的客户端故障转移”。

可以使用 `rdist`、`cpio` 或其他文件传输机制来维护复制的文件系统。由于更新复制的文件系统会导致不一致，因此为实现最佳效果，应考虑以下预防措施：

- 在安装新版本的文件之前，先重命名旧版本的文件
- 在夜间运行更新，此时客户机使用率较低
- 使更新始终很小
- 将副本数目降到最少

故障转移和 NFS 锁定

某些软件包需要对文件进行读取锁定。为防止这些产品被破坏，允许对只读文件系统进行读取锁定，但是只有客户端可查看读取锁定。这些锁定在重映射后不会发生变化，因为服务器不“知晓”有关锁定的信息。由于文件不会发生更改，因此您不需要在服务器端锁定文件。

NFS 版本 4 中的客户端故障转移

在 NFS 版本 4 中，如果由于文件大小不同或文件类型不同而无法建立副本，将发生以下情况。

- 文件被标记为停用。
- 输出警告信息。
- 应用程序收到系统调用故障信息。

注 – 如果重新启动应用程序并再次尝试访问该文件，则应该会成功。

在 NFS 版本 4 中，您不会再收到因目录大小不同而导致的复制错误。在以前的 NFS 版本中，这种情况被视为错误且会阻碍重映射过程。

此外，在 NFS 版本 4 中，如果目录读取操作未成功，则将由列出的下一台服务器执行该操作。在以前的 NFS 版本中，未成功的读取操作将导致重映射失败且挂起该过程，直到原始服务器可用为止。

大文件

操作系统支持大于 2 GB 的文件。缺省情况下，UFS 文件系统是使用 `-largefiles` 选项挂载的，以便支持此新功能。如有需要，请参见第 83 页中的 “如何在 NFS 服务器上禁用大文件”以获取说明。

如果服务器的文件系统是使用 `-largefiles` 选项挂载的，则 Solaris 2.6 NFS 客户机可以访问大文件，而不需要进行更改。但是，并不是所有的 Solaris 2.6 命令都可以处理这些大文件。有关可处理大文件的命令的列表，请参见 `largefile(5)`。不能支持具有大文件扩展的 NFS 版本 3 协议的客户机不能访问任何大文件。尽管运行 Solaris 2.5 发行版的客户机可以使用 NFS 版本 3 协议，但是该发行版不提供大文件支持。

NFS 服务器日志记录如何工作

NFS 服务器日志记录提供 NFS 读写记录，以及修改文件系统的操作记录。此数据可用于跟踪对信息的访问。此外，记录可以提供用于度量信息重要性的定量方法。

访问启用了日志记录的文件系统时，内核会将原始数据写入缓冲区文件。此数据包括以下内容：

- 时间标记
- 客户机 IP 地址
- 申请者的 UID
- 正在访问的文件或目录对象的文件句柄
- 已执行操作的类型

`nfslogd` 守护进程会将此原始数据转换为日志文件中存储的 ASCII 记录。转换期间，IP 地址将被修改为主机名，UID 将被修改为登录名（如果已启用的名称服务可以找到匹配项）。文件句柄也被转换为路径名。为了完成转换，该守护进程将跟踪文件句柄并在单独的文件句柄到路径表中存储信息。这样，每次访问文件句柄时，就不必再次识别路径了。由于在 `nfslogd` 关闭时不会在文件句柄到路径表中对映射进行任何更改，因此必须始终使该守护进程保持运行状态。

注 – NFS 版本 4 不支持服务器日志记录。

WebNFS 服务如何工作

WebNFS 服务通过使用公共文件句柄使目录中的文件可用于客户机。文件句柄是内核生成的地址，可标识 NFS 客户机的文件。**公共文件句柄**具有预定义的值，因此服务器不需要为客户机生成文件句柄。通过删除 MOUNT 协议，可以使用此预定义文件句柄来减少网络通信流量。此功能还会加速客户机的进程处理。

缺省情况下，系统将在根文件系统上建立 NFS 服务器上的公共文件句柄。此缺省设置为 WebNFS 提供了对已在服务器上具有挂载权限的任何客户机的访问权限。通过使用 share 命令，可以更改公共文件句柄以指向任意文件系统。

当客户机具有与文件系统对应的文件句柄时，将会运行 LOOKUP，以确定要访问的文件的文件句柄。NFS 协议一次只允许评估一个路径名组件。目录分层结构的每个附加层都需要运行一次 LOOKUP。当 LOOKUP 与公共文件句柄有关时，WebNFS 服务器可以使用单个多组件查找事务来评估整个路径名。多组件查找使 WebNFS 服务器可以将该文件句柄传送到所需的文件，而不针对路径名中的每一目录层交换文件句柄。

此外，NFS 客户机还可以通过单一 TCP 连接启动并发下载。此连接提供快速访问，而不会在服务器上产生因设置多个连接而导致的负载增加。尽管 Web 浏览器应用程序支持件并发下载多个文件，但每个文件都有各自的连接。通过使用某个连接，WebNFS 软件可以减少服务器上的开销。

如果路径名中的最终组件是指向其他文件系统的符号链接，则客户机可以访问文件（如果客户机已具备通过正常的 NFS 活动进行访问的权限）。

通常，NFS URL 是相对于公共文件句柄进行评估的。通过在路径的开始位置添加一个附加的斜杠，可以更改评估，使其与服务器的根文件系统有关。在本示例中，如果已在 /export/ftp 文件系统上建立了公共文件句柄，则这两个 NFS URL 是等效的。

```
nfs://server/junk
nfs://server//export/ftp/junk
```

注 – NFS 版本 4 协议优先于 WebNFS 服务。NFS 版本 4 完全集成了已添加到 MOUNT 协议和 WebNFS 服务中的所有安全协商。

WebNFS 安全协商如何工作

NFS 服务包括一个协议，该协议使 WebNFS 客户机可以与 WebNFS 服务器协商选定的安全机制。新协议使用安全协商多组件查找功能，该功能是对早期版本的 WebNFS 协议中使用的多组件查找功能的扩展。

WebNFS 客户机通过使用公共文件句柄来发出常规多组件查找请求，进而启动进程。由于客户机不知道服务器保护路径的方式，因此将使用缺省的安全机制。如果缺省的安全机制不够，则服务器将回复 AUTH_TOOWEAK 错误。此回复表明缺省机制无效。客户机需要使用更强大的缺省机制。

客户机收到 AUTH_TOOWEAK 错误后，会向服务器发送请求，以确定需要哪种安全机制。如果请求成功，则服务器将使用指定路径所需的安全机制数组进行响应。根据安全机制数组的大小，客户机可能必须发出更多请求才能获取完整的数组。如果服务器不支持 WebNFS 安全协商，则请求将失败。

请求成功后，WebNFS 客户机将从其支持的数组中选择第一个安全机制。然后，该客户机将使用选定的安全机制发出常规多组件查找请求，以获取文件句柄。所有后续的 NFS 请求都是使用选定安全机制和文件句柄发出的。

注 – NFS 版本 4 协议优先于 WebNFS 服务。NFS 版本 4 完全集成了已添加到 MOUNT 协议和 WebNFS 服务中的所有安全协商。

Web 浏览器使用的 WebNFS 限制

使用 HTTP 的 Web 站点可以提供的多项功能不受 WebNFS 软件的支持。这些差异源自 NFS 服务器仅发送文件这一事实，因此必须在客户机上执行所有的特殊处理。如果需要为 WebNFS 和 HTTP 访问配置一个 Web 站点，则应考虑以下问题：

- NFS 浏览不运行 CGI 脚本。因此，带有活动 Web 站点（该站点使用许多 CGI 脚本）的文件系统可能不适用于 NFS 浏览。
- 浏览器可能会启动不同查看器来处理不同文件格式的文件。如果可以通过文件名来确定文件类型，则通过 NFS URL 访问这些文件便可启动外部查看器。使用 NFS URL 时，浏览器应该识别标准 MIME 类型的任何文件扩展名。WebNFS 软件不会为了确定文件类型而在文件内部进行检查。因此，确定文件类型的唯一方法就是通过文件扩展名。
- NFS 浏览不能利用服务器端图像映射（可单击的图像）。但是，NFS 浏览可以利用客户端图像映射（可单击的图像），因为 URL 是使用位置定义的。不需要来自文档服务器的任何其他响应。

安全 NFS 系统

NFS 环境是用于在具有不同计算机体系结构和操作系统的网络中共享文件系统的一种强大而便捷的方式。但是，这些通过 NFS 操作使文件系统共享变得非常便利的功能同时还会造成一些安全问题。以前，大多数 NFS 实现使用 UNIX（或 AUTH_SYS）验证，但是也可以使用更强大的验证方法（如 AUTH_DH）。使用 UNIX 验证时，NFS 服

务器通过验证发出请求的计算机（而不是用户）来验证文件请求。因此，客户机用户可以运行 su 并模仿文件的所有者。如果使用 DH 验证，则 NFS 服务器将验证用户，这使得此类模仿非常困难。

凭借超级用户访问权限和对网络编程的了解，任何人都可以将任意数据引入网络，并从网络中提取任何数据。最危险的攻击就是涉及数据引入的攻击。例如，通过生成适当的包或通过记录“会话”并稍后重放来模仿用户。这些攻击将影响数据的完整性。涉及被动窃听（仅侦听网络通信流量，而不模仿任何人）的攻击不是很危险，因为不会损害数据完整性。用户可通过对通过网络发送的数据进行加密来保护敏感信息的保密性。

解决网络安全问题的常见方法是针对每个应用程序都单独制定解决方案。更好的方法是在涉及所有应用程序的级别上实现标准验证系统。

Solaris 操作系统包括位于远程过程调用 (remote procedure call, RPC) 级别的验证系统（NFS 操作所依赖的机制）。此系统（称为安全 RPC）可以大大提高网络环境的安全性，并能为 NFS 系统等服务提供附加安全性。当 NFS 系统使用由安全 RPC 提供的功能时，该系统称为安全 NFS 系统。

安全 RPC

安全 RPC 是安全 NFS 系统的基础。安全 RPC 的目标是建立至少与分时系统一样安全的系统。在分时系统中，所有用户共享单台计算机。分时系统通过登录口令验证用户。使用数据加密标准 (Data Encryption Standard, DES) 验证，可以完成相同的验证过程。用户可以登录任何远程计算机，就像登录本地终端一样。用户的登录口令是其网络安全的保证。在分时环境中，系统管理员出于道义不会更改口令以模仿某人。在安全 RPC 中，网络管理员是可信的，不会更改存储有**公钥**的数据库中的项。

为了解 RPC 验证系统，您需要熟悉两个术语：凭证和检验器。以 ID 证件为例，凭证就是标识用户的具体内容：姓名、地址和生日。检验器就是附加到证件上的照片。通过对照携带该证件的人员检查该证件上的照片，可以确定该证件未被盗用。在 RPC 中，客户机进程会通过每个 RPC 请求将凭证和检验器发送到服务器。服务器仅发回检验器，因为客户机已经“知晓”服务器的凭证。

RPC 验证是开放式的，这表示可以在其中插入各种验证系统，如 UNIX、DH 和 KERB。

当网络服务使用 UNIX 验证时，凭证包含客户机的主机名、UID、GID 和组访问列表。但是，检验器不包含任何内容。由于不存在检验器，因此超级用户可以使用如 su 等命令来伪造相应的凭证。UNIX 验证的另一个问题是 UNIX 验证将认为网络中的所有计算机都是 UNIX 计算机。UNIX 验证在应用于异构网络中的其他操作系统时将会中断。

为克服 UNIX 验证问题，安全 RPC 将使用 DH 验证。

DH 验证

DH 验证使用数据加密标准 (Data Encryption Standard, DES) 和 Diffie-Hellman 公钥密码学来验证网络中的用户和计算机。DES 是标准加密机制。Diffie-Hellman 公钥密码学是包含两个密钥的密码系统：一个公钥和一个私钥。公钥和私钥存储在名称空间中。NIS 将密钥存储在公钥映射中。这些映射包含所有潜在用户的公钥和私钥。有关如何设置映射的更多信息，请参见《系统管理指南：名称和目录服务（DNS、NIS 和 LDAP）》。

DH 验证的安全性依赖于发件人加密当前时间的能力，随后收件人可以对该时间进行解密，并对照自己的时钟进行检查。时间标记是使用 DES 进行加密的。使此方案正常工作的要求如下所示：

- 两个代理必须就当前时间达成一致。
- 发件人和收件人必须使用相同的加密密钥。

如果网络运行时间同步程序，则系统将自动同步客户机和服务器上的时间。如果时间同步程序不可用，则可以使用服务器的时间（而不是网络时间）来计算时间标记。启动 RPC 会话之前，客户机将询问服务器时间，然后计算其自己的时钟与服务器时钟之间的时间差值。计算时间标记时会使用该差值来调整客户机的时钟。如果客户机与服务器的时钟未同步，则服务器将开始拒绝客户机的请求。客户机上的 DH 验证系统将与服务器重新进行同步。

客户机和服务器使用同一个加密密钥，具体方法是：生成一个随机的**对话密钥**（也称为**会话密钥**），并使用公钥密码学推导**公用密钥**。公用密钥是只有客户机和服务器才能推导的密钥。对话密钥用于加密和解密客户机的时间标记。公用密钥用于加密和解密对话密钥。

KERB 验证

Kerberos 是 MIT 开发的验证系统。Kerberos 提供各种加密类型，包括 DES。Kerberos 支持不再作为安全 RPC 的一部分来提供，但是此发行版中包含服务器端和客户端实现。有关 Kerberos 验证实现的更多信息，请参见《系统管理指南：安全性服务》中的第 21 章 “Kerberos 服务介绍”。

在 NFS 中使用安全 RPC

如果计划使用安全 RPC，请注意以下几点：

- 如果在周围无人的情况下服务器发生崩溃（例如，在断电后），则存储在系统中的所有私钥都将被删除。此时，所有进程都不能访问安全网络服务或挂载 NFS 文件系统。重新引导期间的重要进程通常以 `root` 身份运行。因此，如果已妥善存储了超级用户的私钥，且没有人可以键入该私钥的解密口令，则这些进程可以正常工作。`keylogin -r` 允许 `root` 在 `keyserv` 可读取的 `/etc/.rootkey` 中存储明文形式的私钥。
- 某些系统以单用户模式引导，控制台上会显示超级用户登录 shell，但不显示口令提示。在这类情况下，物理安全性是非常必要的。

- 无盘计算机引导并不是绝对安全的。他人可以模拟引导服务器并引导不正当的内核，例如，在远程计算机上记录您的私钥。安全 NFS 系统仅在内核和密钥服务器都处于运行状态之后，才会提供保护。否则，无法验证引导服务器提供的回复。此限制可能会是一个严重的问题，不过，只有使用内核源代码的复杂攻击才能利用此限制。此外，犯罪行为会留下证据。如果轮询网络查找引导服务器，则会发现不正当引导服务器的位置。
- 大多数 setuid 程序都归 root 所有。如果 root 的私钥存储在 /etc/.rootkey 中，则这些程序会正常工作。但是，如果用户拥有 setuid 程序，则 setuid 程序可能有时无法正常工作。例如，假设 setuid 程序归 dave 所有，并且在引导计算机之后 dave 未登录计算机。在这种情况下，该程序可能无法访问安全网络服务。
- 如果使用 login、rlogin 或 telnet 登录远程计算机并且使用 keylogin 获取访问权限，则可以访问您的帐户。原因是您的私钥会被传递给该计算机的密钥服务器，该服务器随后会存储您的私钥。只有在不信任远程计算机的情况下才考虑使用此过程。但是，如果存在疑问，请勿在远程计算机要求口令时登录远程计算机。请使用 NFS 环境来挂载与远程计算机共享的文件系统。此外，也可以使用 keylogout 从密钥服务器中删除私钥。
- 如果使用 -o sec=dh 选项共享起始目录，则远程登录可能会有问题。如果未将 /etc/hosts.equiv 或 ~/.rhosts 文件设置为提示输入口令，将成功登录。但是，用户不能访问其起始目录，因为没有在本地进行验证。如果系统提示用户输入口令，则当该口令与网络口令匹配时，用户有权访问其起始目录。

Autofs 映射

Autofs 使用三种类型的映射：

- 主映射
- 直接映射
- 间接映射

Autofs 主映射

auto_master 映射将目录与映射相关联。该映射是指定 autofs 应检查的所有映射的主列表。以下示例说明 auto_master 文件可能包含的内容。

示例 6–3 /etc/auto_master 文件样例

```
# Master map for automounter
#
+auto_master
/net            -hosts           -nosuid,nobrowse
/home           auto_home        -nobrowse
/-              auto_direct     -ro
```

本示例说明在常规 auto_master 文件中额外增加了 auto_direct 映射。主映射 /etc/auto_master 中的每一行都具有以下语法：

mount-point map-name [*mount-options*]

mount-point *mount-point* 是目录的全（绝对）路径名。如果目录不存在，则 autofs 将创建该目录（如果可能）。如果目录存在且不为空，则在该目录上挂载会隐藏该目录的内容。在这种情况下，autofs 将发出警告。

作为挂载点的表示法 /- 指示此特定映射是直接映射。该表示法还表示没有特定的挂载点与该映射关联。

map-name *map-name* 是用于查找位置目录或挂载信息的 autofs 映射。如果名称前面带有斜杠 (/)，autofs 会将该名称解释为本地文件。否则，autofs 会使用在名称服务转换器配置文件 (/etc/nsswitch.conf) 中指定的搜索项来搜索挂载信息。特殊映射还可用于 /net。有关更多信息，请参见第 179 页中的 “挂载点 /net”。

mount-options *mount-options* 是可选的以逗号分隔的选项列表，其中的选项适用于挂载 map-name 中指定的项，除非 map-name 中的项列出了其他选项。每种特定类型的文件系统的选项都列在该文件系统的挂载手册页中。例如，有关特定于 NFS 的挂载选项，请参见 mount_nfs(1M) 手册页。对于特定于 NFS 的挂载点，bg（后台）和 fg（前台）选项都不适用。

以 # 开头的行是注释。# 之后直到行尾的所有文本都将被忽略。

要将较长的行拆分为较短的行，请在行尾放置一个反斜杠 (\)。项的最大字符数为 1024。

注 – 如果在两个项中使用了同一挂载点，则 automount 命令会使用第一项。第二项将被忽略。

挂载点 /home

挂载点 /home 是 /etc/auto_home（间接映射）中列出的项将要挂载到的目录。

注 – 缺省情况下，Autofs 可以在所有计算机上运行且支持 /net 和 /home（自动挂载的起始目录）。可以使用 NIS auto.master 映射或 NIS+ auto_master 表中的项或通过本地编辑 /etc/auto_master 文件来覆盖这些缺省值。

挂载点 /net

Autofs 将在目录 /net 下挂载特殊映射 -hosts 中的所有项。该映射是仅使用主机数据库的内置映射。假设计算机 gumbo 位于主机数据库中，且可以导出其任何文件系统。以下命令会将当前目录更改为计算机 gumbo 的根目录。

```
% cd /net/gumbo
```

Autofs 只能挂载主机 gumbo 的**已导出的**文件系统，即服务器上可供网络用户使用的文件系统，而不是本地磁盘上的文件系统。因此，gumbo 中的所有文件和目录可能都无法通过 /net/gumbo 使用。

使用 /net 访问方法时，服务器名称位于路径中，且与位置相关。如果要将导出的文件系统从一台服务器移动到另一台服务器，则该路径可能无法再正常工作。应针对所需的文件系统在映射中特别设置一项，而不应使用 /net。

注 – Autofs 仅在挂载时检查服务器的导出列表。挂载服务器的文件系统之后，在自动取消挂载该服务器的文件系统之前，autofs 不会再次检查服务器。因此，只有在取消挂载客户机上的文件系统，然后重新挂载之后，才能“看到”新导出的文件系统。

Autofs 直接映射

直接映射是自动挂载点。使用直接映射时，客户机上的挂载点与服务器上的目录之间存在直接关联。直接映射具有全路径名并显式表示这种关系。以下是典型的 /etc/auto_direct 映射：

```
/usr/local          -ro \
   /bin                   ivy:/export/local/sun4 \
   /share                 ivy:/export/local/share \
   /src                   ivy:/export/local/src
/usr/man            -ro    oak:/usr/man \
                           rose:/usr/man \
                           willow:/usr/man
/usr/games          -ro    peach:/usr/games
/usr/spool/news     -ro    pine:/usr/spool/news \
                           willow:/var/spool/news
```

直接映射中的行具有以下语法：

key [*mount-options*] *location*

key — *key* 是直接映射中挂载点的路径名。

mount-options — *mount-options* 是要应用于此特定挂载的选项。仅当这些选项不同于映射缺省值时，才需要这些选项。每种特定类型的文件系统的选项都列在该文件系统的挂载手册页中。例如，有关特定于 NFS 的挂载选项，请参见 mount_nfs(1M) 手册页。

location *location* 是文件系统的位置。对于 NFS 文件系统和 High Sierra 文件系统 (High Sierra file system, HSFS)，分别以 *server*:*pathname* 和 :*devicename* 形式指定一个或多个文件系统的位置。

注 – *pathname* 不应包括自动挂载的挂载点。*pathname* 应该为文件系统的实际绝对路径。例如，起始目录的位置应列为 *server*:/export/home/ *username*，而不是 *server* :/home/*username*。

与主映射中相同，以 # 开头的行是注释。# 之后直到行尾的所有文本都将被忽略。要将较长的行拆分为较短的行，请在行尾放置一个反斜杠。

在所有的映射中，直接映射中的项与 /etc/vfstab 中相应的项最相似。/etc/vfstab 中可能存在如下所示的项：

```
dancer:/usr/local - /usr/local/tmp nfs - yes ro
```

等效的项则以如下形式出现在直接映射中：

```
/usr/local/tmp     -ro     dancer:/usr/local
```

注 – 自动挂载程序映射之间不会出现任何选项关联。添加到自动挂载程序映射中的任何选项将覆盖以前搜索到的映射中列出的所有选项。例如，auto_master 映射中包含的选项将被任何其他映射中的相应项所覆盖。

有关与此类型的映射关联的其他重要功能，请参见第 186 页中的 “Autofs 如何为客户机选择最近的只读文件（多个位置）”。

挂载点 /–

在示例 6–3 中，挂载点 /- 通知 autofs 不要将 auto_direct 中的项与任何特定挂载点关联。间接映射使用在 auto_master 文件中定义的挂载点。直接映射使用在已命名映射中指定的挂载点。请记住，在直接映射中，关键字或挂载点是全路径名。

NIS 或 NIS+ auto_master 文件只能具有一个直接映射项，因为在名称空间中挂载点必须是唯一的值。作为本地文件的 auto_master 文件可以具有任意数目的直接映射项（如果这些项不重复）。

Autofs 间接映射

间接映射使用关键字的替代值在客户机上的挂载点与服务器上的目录之间建立关联。间接映射对于访问特定文件系统（如起始目录）非常有用。auto_home 映射便是间接映射。

间接映射中的行具有以下通用语法：

key [*mount-options*] *location*

key — *key* 是间接映射中的简单名称（不含斜杠）。

mount-options — *mount-options* 是要应用于此特定挂载的选项。仅当这些选项不同于映射缺省值时，才需要这些选项。每种特定类型的文件系统的选项都列在该文件系统的挂载手册页中。例如，有关特定于 NFS 的挂载选项，请参见 mount_nfs(1M) 手册页。

location — *location* 是文件系统的位置。可以 *server*:*pathname* 形式指定一个或多个文件系统的位置。

注 – *pathname* 不应包括自动挂载的挂载点。*pathname* 应该为文件系统的实际绝对路径。例如，目录的位置应列为 *server*:/usr/local ，而不是 *server*:/net/ *server*/usr/local。

与主映射中相同，以 # 开头的行是注释。# 之后直到行尾的所有文本都将被忽略。要将较长的行拆分为较短的行，请在行尾放置一个反斜杠 (\)。示例 6–3 显示了一个包含以下项的 auto_master 映射：

```
/home      auto_home        -nobrowse
```

auto_home 是间接映射的名称，该映射包含要在 /home 下挂载的项。典型的 auto_home 映射将包含以下内容：

```
david                   willow:/export/home/david
rob                     cypress:/export/home/rob
gordon                  poplar:/export/home/gordon
rajan                   pine:/export/home/rajan
tammy                   apple:/export/home/tammy
jim                     ivy:/export/home/jim
linda    -rw,nosuid     peach:/export/home/linda
```

例如，假设上面的映射位于主机 oak 上。假设用户 linda 在口令数据库中有一项，该项将她的起始目录指定为 /home/linda。只要 linda 登录计算机 oak，autofs 就会挂载位于计算机 peach 上的目录 /export/home/linda。她的起始目录以读写方式结合 nosuid 选项进行挂载。

假设发生以下情况：用户 linda 的起始目录在口令数据库中列为 /home/linda。任何人（包括 Linda）都可以从使用特定主映射（引用上一个示例中的映射的主映射）设置的任何计算机访问此路径。

在上述情况下，用户 linda 可以在其中的任何一台计算机上运行 login 或 rlogin，并且已为自己挂载了起始目录。

而且，此时 Linda 还可以键入以下命令：

```
% cd ~david
```

autofs 将为她挂载 David 的起始目录（如果允许所有权限）。

注 – 自动挂载程序映射之间不会出现任何选项关联。添加到自动挂载程序映射中的任何选项将覆盖以前搜索到的映射中列出的所有选项。例如，将使用任何其他映射中对应的项来覆盖 auto_master 映射中包含的选项。

在没有名称服务的网络中，必须更改网络中所有系统上的所有相关文件（如 /etc/passwd）以允许 Linda 访问自己的文件。在运行 NIS 的网络中，应在 NIS 主服务器上进行更改并将相关的数据库传播到从属服务器。在运行 NIS+ 的网络中，执行更改后会自动将相关的数据库传播到从属服务器。

Autofs 如何工作

Autofs 是一项可自动挂载相应文件系统的客户端服务。以下是协同工作以完成自动挂载的组件：

- automount 命令
- autofs 文件系统
- automountd 守护进程

自动挂载服务 svc:/system/filesystem/autofs 是在系统启动时调用的，它可读取主映射文件 auto_master 以创建最初的一组 autofs 挂载。这些 autofs 挂载在启动时不会自动挂载。这些挂载是一些点，以后将会在这些点之下挂载文件系统。这些点也称为触发节点。

设置 autofs 挂载后，这些挂载可以触发在其下挂载文件系统。例如，当 autofs 收到对当前尚未挂载的文件系统的访问请求时，autofs 会调用 automountd，实际上由该命令挂载请求的文件系统。

初始挂载 autofs 挂载后，必要时会使用 automount 命令更新 autofs 挂载。该命令将比较 auto_master 映射中的挂载列表和挂载表文件 /etc/mnttab（以前为 /etc/mtab）中的已挂载文件系统的列表。然后，automount 会做出相应更改。该进程允许系统管理员更改

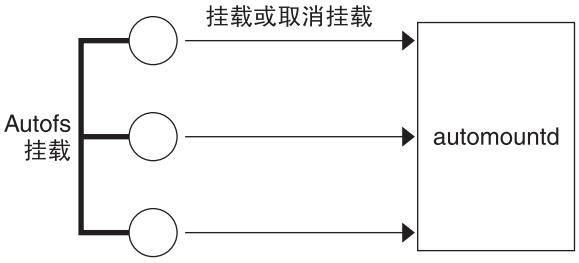
auto_master 中的挂载信息，并使 autofs 进程可以使用这些更改，而无需停止并重新启动 autofs 守护进程。挂载文件系统后，在自动取消挂载文件系统之前，进一步进行访问不需要 automountd 执行任何操作。

与 mount 不同，automount 并不会从 /etc/vfstab 文件（该文件特定于每台计算机）中读取要挂载的文件系统列表。在域中或在计算机上，automount 命令是通过名称空间或本地文件进行控制的。

以下是有关 autofs 工作方式的简要概述。

自动挂载守护进程 automountd 是在引导时由服务 svc:/system/filesystem/autofs 启动的。请参见图 6–3。此服务还运行 automount 命令，该命令读取主映射并安装 autofs 挂载点。有关更多信息，请参见第 184 页中的 “Autofs 如何启动导航进程（主映射）”。

图 6–3 svc:/system/filesystem/autofs 服务启动 automount



Autofs 是支持自动挂载和取消挂载的内核文件系统。

请求访问 autofs 挂载点处的文件系统时，将发生下列情况：

1. Autofs 拦截请求。
2. Autofs 将消息发送到 automountd，以便挂载请求的文件系统。
3. automountd 在映射中查找文件系统信息，创建触发节点并执行挂载。
4. Autofs 允许继续处理被拦截的请求。
5. 当文件系统在一段时间内没有活动后，Autofs 将取消挂载该文件系统。

注 – 不应手动挂载或取消挂载通过 autofs 服务管理的挂载。即使手动操作成功，autofs 服务也不会检查是否已取消挂载该对象，从而可能导致不一致。重新引导时将清除所有 autofs 挂载点。

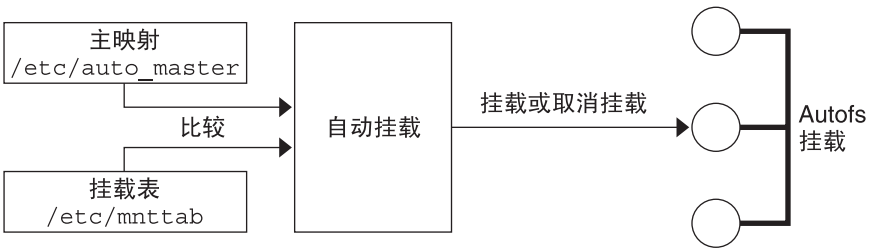
Autofs 如何在网络中进行导航（映射）

Autofs 将搜索一系列映射以在网络中进行导航。映射是包含诸如网络中的所有用户的口令项或网络中的所有主机名称等信息的文件。实际上，这些映射包含网络范围内与 UNIX 管理文件等效的文件。可以在本地使用映射，或通过网络名称服务（如 NIS 或 NIS+）使用映射。请参见第 191 页中的“修改 Autofs 导航网络的方式（修改映射）”。

Autofs 如何启动导航进程（主映射）

`automount` 命令在系统启动时读取主映射。主映射中的项包括直接映射名或间接映射名、映射路径和映射的挂载选项，如图 6–4 所示。项的具体顺序并不重要。`automount` 会将主映射中的项与挂载表中的项进行比较，以生成最新列表。

图 6–4 在主映射中进行导航



Autofs 挂载过程

触发挂载请求时，autofs 服务执行的具体操作取决于自动挂载程序映射的配置方式。一般情况下，挂载过程对于所有挂载都是相同的。然而，最终结果会随指定的挂载点和映射复杂性的不同而不同。挂载过程包括创建触发器节点。

简单的 Autofs 挂载

为帮助说明 autofs 挂载过程，假设已安装了以下文件。

```
$ cat /etc/auto_master
# Master map for automounter
#
+auto_master
/net        -hosts        -nosuid,nobrowse
/home       auto_home     -nobrowse
/share      auto_share
$ cat /etc/auto_share
# share directory map for automounter
#
ws          gumbo:/export/share/ws
```

访问 /share 目录时，autofs 服务将为 /share/ws 创建一个触发节点，/share/ws 是 /etc/mnttab 中类似于以下项的项：

```
-hosts  /share/ws     autofs  nosuid,nobrowse,ignore,nest,dev=###
```

访问 /share/ws 目录时，autofs 服务将通过以下步骤完成该过程：

1. 检查服务器的挂载服务的可用性。
2. 在 /share 下挂载请求的文件系统。此时，/etc/mnttab 文件包含以下项。

```
-hosts  /share/ws     autofs  nosuid,nobrowse,ignore,nest,dev=###
gumbo:/export/share/ws /share/ws   nfs   nosuid,dev=####    #####
```

有层次挂载

在自动挂载程序文件中定义了多层后，挂载过程将变得更加复杂。假设您对上一个示例中的 /etc/auto_shared 文件进行了扩展，使其包含以下内容：

```
# share directory map for automounter
#
ws        /       gumbo:/export/share/ws
          /usr    gumbo:/export/share/ws/usr
```

该挂载过程基本上与上一个示例中访问 /share/ws 挂载点时的情况相同。此外，下一层 (/usr) 的触发节点是在 /share/ws 文件系统中创建的，因此可以挂载下一层（如果可以对其进行访问）。在本示例中，/export/share/ws/usr 必须存在于 NFS 服务器上，才能创建触发节点。

注意 – 指定有层次的层时，请勿使用 -soft 选项。有关此限制的说明，请参阅第 185 页中的 “Autofs 取消挂载”。

Autofs 取消挂载

一段空闲时间后将按相反的顺序（与挂载顺序相反）执行取消挂载过程。如果分层结构中较高级别的某个目录处于繁忙状态，则只取消挂载该目录下面的文件系统。在取消挂载过程中，将先删除所有触发节点，然后再取消挂载文件系统。如果文件系统处于繁忙状态，则取消挂载将失败并将重新安装触发节点。

注意 – 指定有层次的层时，请勿使用 -soft 选项。如果使用 -soft 选项，则重新安装触发节点的请求可能会超时。如果重新安装触发节点失败，将不能再访问下一级别的挂载。解决此问题的唯一方法是让自动挂载程序取消挂载分层结构中的所有组件。自动挂载程序通过等待文件系统自动取消挂载或重新引导系统来完成取消挂载。

Autofs 如何为客户机选择最近的只读文件（多个位置）

该直接映射示例包含以下内容：

```
/usr/local          -ro \
   /bin                    ivy:/export/local/sun4\
   /share                  ivy:/export/local/share\
   /src                    ivy:/export/local/src
/usr/man            -ro   oak:/usr/man \
                          rose:/usr/man \
                          willow:/usr/man
/usr/games          -ro   peach:/usr/games
/usr/spool/news     -ro   pine:/usr/spool/news \
                          willow:/var/spool/news
```

挂载点 /usr/man 和 /usr/spool/news 列出了多个位置，第一个挂载点有三个位置，第二个挂载点有两个位置。任何复制的位置都可以向任何用户提供相同的服务。只有在挂载只读文件系统时此过程才有意义，因为您必须对要写入或修改的文件的位置进行某些控制。您需要避免在某个时候修改某个服务器上的文件，然后在几分钟后又去修改其他服务器上的“同一个”文件。这样做的优点是，将自动使用可用性最佳的服务器，而无需执行用户所需的任何工作。

如果已将文件系统配置为副本（请参见第 171 页中的“什么是复制的文件系统？”），则客户机可以利用故障转移。这样，不仅可以自动确定最佳的服务器，而且在该服务器不可用时，客户机还会自动使用下一个最佳服务器。

将好的文件系统配置为副本的一个示例是手册页。在大型网络中，多台服务器可以导出当前的一组手册页。如果服务器正在运行且正在导出其文件系统，则从哪个服务器挂载手册页并不重要。在前面的示例中，多个挂载位置在映射项中被表示为挂载位置的列表。

```
/usr/man -ro oak:/usr/man rose:/usr/man willow:/usr/man
```

在本示例中，可以从服务器 oak、rose 或 willow 挂载手册页。哪个服务器最佳取决于很多因素，其中包括：

- 支持特定 NFS 协议级别的服务器的数目
- 服务器的邻近度
- 加权

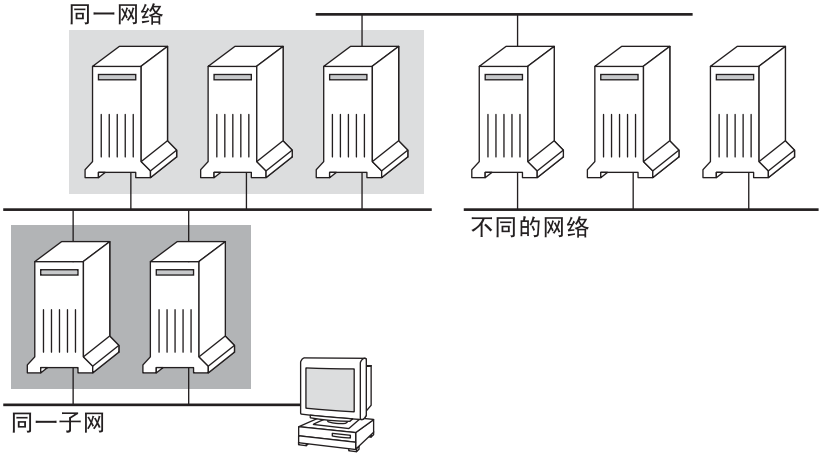
排序期间，将对支持各版本 NFS 协议的服务器进行计数。大多数服务器支持的协议版本将成为要使用的缺省协议。此选择为客户机提供最多的可依赖的服务器。

找到使用同一版本协议的服务器的最大子集后，会按邻近度对该服务器列表进行排序。为确定临近度，将检查 IPv4 地址。IPv4 地址会显示每个子网中包含哪些服务器。本地子网中的服务器优先于远程子网中的服务器。首选最近的服务器可以减少延迟时间和网络通信流量。

注 – 不能确定使用 IPv6 地址的副本的邻近度。

图 6–5 说明了服务器的邻近度。

图 6–5 服务器邻近度



如果支持同一协议的多台服务器位于本地子网中，则系统将确定连接每台服务器的时间并使用最快的服务器。使用加权也会影响排序（请参见第 188 页中的 “Autofs 和加权”）。

例如，如果版本 4 服务器比较多，则版本 4 将成为要使用的缺省协议。但是，现在排序过程更加复杂了。以下是如何进行排序的一些示例：

- 本地子网中的服务器优先于远程子网中的服务器。因此，如果版本 3 服务器位于本地子网中，而最近的版本 4 服务器位于远程子网中，则版本 3 服务器优先级更高。同样，如果本地子网包含版本 2 服务器，则它们优先于包含版本 3 和版本 4 服务器的远程子网。
- 如果本地子网包含数目不同的版本 2、版本 3 和版本 4 服务器，则需要进行更多排序。自动挂载程序将优先使用本地子网上的最高版本。在这种情况下，版本 4 是最高版本。但是，如果本地子网具有的版本 3 或版本 2 服务器比版本 4 服务器多，则自动挂载程序将从本地子网上的最高版本“向下移动”一个版本。例如，如果本地子网有三台版本 4 服务器、三台版本 3 服务器和十台版本 2 服务器，则会选择版本 3 服务器。
- 同样，如果本地子网包含数目不同的版本 2 和版本 3 服务器，则自动挂载程序将首先查看哪个版本代表本地子网上的最高版本。接下来，自动挂载程序将对运行每个版本的服务器进行计数。如果本地子网中的最高版本同时代表最多的服务器，则选

择最高版本。如果较低版本具有更多服务器，则自动挂载程序将从本地子网上的最高版本向下移动一个版本。例如，如果本地子网上的版本 2 服务器比版本 3 服务器更多，则选择版本 2 服务器。

注 – `/etc/default/nfs` 文件中的关键字值也会影响加权。具体来说，NFS_SERVER_VERSMIN、NFS_CLIENT_VERSMIN、NFS_SERVER_VERSMAX 和 NFS_CLIENT_VERSMAX 的值可以使某些版本从排序过程中排除。有关这些关键字的更多信息，请参见第 125 页中的 “`/etc/default/nfs` 文件的关键字”。

选择服务器之后，可以在挂载时使用故障转移检查排序方式。在单个服务器可能无法临时导出其文件系统的环境中，多个位置非常有用。

在具有许多子网的大型网络中，故障转移特别有用。Autofs 将选择适当的服务器，并且能够将 NFS 网络通信流量限制在本地网络段。如果服务器具有多个网络接口，则可以列出与每个网络接口关联的主机名，就像接口是单独的服务器一样。Autofs 将选择离客户机最近的接口。

注 – 对于手动挂载，不会执行任何加权和邻近度检查。`mount` 命令将对从左到右列出的服务器设置优先级。

有关更多信息，请参见 `automount(1M)` 手册页。

Autofs 和加权

对 autofs 映射增加加权值可影响对处于同一邻近度级别的服务器的选择。例如：

```
/usr/man -ro oak,rose(1),willow(2):/usr/man
```

括号中的数字表示加权。不含加权的服务器的值为零，因此最有可能被选中。加权值越高，服务器被选中的几率越低。

注 – 所有其他的服务器选择因素都比加权重要。只有在网络邻近度相同的服务器之间进行选择时，才需考虑加权。

映射项中的变量

通过在客户机名称前加一个美元符号 ($) 前缀可以创建特定于该客户机的变量。该变量有助于了解正在访问同一个文件系统位置的不同体系结构类型。还可以使用花括号将变量名与附加字母或数字分隔开。表 6–2 显示了预定义的映射变量。

表 6–2 预定义的映射变量

变量	含义	源自	示例
ARCH	体系结构类型	uname -m	sun4
CPU	处理器类型	uname -p	sparc
HOST	主机名	uname -n	dinky
OSNAME	操作系统名称	uname -s	SunOS
OSREL	操作系统发行版	uname -r	5.8
OSVERS	操作系统版本（发行版的版本）	uname -v	GENERIC

可以在项所在行的任何位置使用变量，但不能使用关键字。例如，假设您的文件服务器分别从 /usr/local/bin/sparc 和 /usr/local/bin/x86 中导出 SPARC 和 x86 体系结构的二进制文件。客户机可以通过如下映射项进行挂载：

```
/usr/local/bin        -ro     server:/usr/local/bin/$CPU
```

现在，所有客户机的同一项将应用于所有体系结构。

注 – 针对任何 sun4 体系结构编写的大多数应用程序可以在所有 sun4 平台上运行。-ARCH 变量硬编码为 sun4。

引用其他映射的映射

文件映射中使用的映射项 *+mapname* 将导致自动挂载读取指定的映射，就好像该映射包含在当前文件中一样。如果 *mapname* 前面没有斜杠，则 autofs 会将映射名视为字符串，并使用名称服务转换器策略查找映射名。如果路径名是绝对路径名，则 automount 将检查该名称的本地映射。如果映射名以破折号 (-) 开头，则 automount 将访问相应的内置映射，如 hosts。

此名称服务转换器文件包含标记为 automount 的 autofs 的一个项，其中包含搜索名称服务的顺序。以下文件是名称服务转换器文件的示例。

```
#
# /etc/nsswitch.nis:
#
# An example file that could be copied over to /etc/nsswitch.conf;
# it uses NIS (YP) in conjunction with files.
#
# "hosts:" and "services:" in this file are used only if the /etc/netconfig
# file contains "switch.so" as a nametoaddr library for "inet" transports.
# the following two lines obviate the "+" entry in /etc/passwd and /etc/group.
```

```
passwd:         files nis
group:          files nis

# consult /etc "files" only if nis is down.
hosts:          nis [NOTFOUND=return] files
networks:       nis [NOTFOUND=return] files
protocols:      nis [NOTFOUND=return] files
rpc:            nis [NOTFOUND=return] files
ethers:         nis [NOTFOUND=return] files
netmasks:       nis [NOTFOUND=return] files
bootparams:     nis [NOTFOUND=return] files
publickey:      nis [NOTFOUND=return] files
netgroup:       nis
automount:      files nis
aliases:        files nis
# for efficient getservbyname() avoid nis
services:       files nis
```

在本示例中，会在搜索 NIS 映射之前先搜索本地映射。因此，可以在本地 `/etc/auto_home` 映射中为最常访问的起始目录添加几个项。然后，可以使用转换器回退到 NIS 映射以查找其他项。

```
bill                cs.csc.edu:/export/home/bill
bonny               cs.csc.edu:/export/home/bonny
```

搜索已包含的映射后，如果找不到匹配项，`automount` 将继续扫描当前映射。因此，可以在 + 项之后添加更多项。

```
bill                cs.csc.edu:/export/home/bill
bonny               cs.csc.edu:/export/home/bonny
+auto_home
```

包含的映射可以是本地文件，也可以是内置映射。请记住，只有本地文件可以包含 + 项。

```
+auto_home_finance      # NIS+ map
+auto_home_sales        # NIS+ map
+auto_home_engineering  # NIS+ map
+/etc/auto_mystuff      # local map
+auto_home              # NIS+ map
+-hosts                 # built-in hosts map
```

注 – 不能在 NIS+ 或 NIS 映射中使用 + 项。

Autofs 可执行映射

可以创建能够执行某些命令以生成 autofs 挂载点的 autofs 映射。如果需要能够根据数据库或平面文件创建 autofs 结构，则使用 autofs 可执行映射将非常有用。使用可执行映射的缺点是，需要在每台主机上安装该映射。可执行映射不能包含在 NIS 或 NIS+ 名称服务中。

可执行映射必须在 auto_master 文件中有一个对应项。

```
/execute    auto_execute
```

以下是可执行映射的示例：

```
#!/bin/ksh
#
# executable map for autofs
#

case $1 in
             src)  echo '-nosuid,hard bee:/export1' ;;
esac
```

为使本示例正常工作，该文件必须作为 /etc/auto_execute 进行安装，且必须设置可执行位。将权限设置为 744。在上述情况下，运行以下命令将导致从 bee 挂载 /export1 文件系统：

```
% ls /execute/src
```

修改 Autofs 导航网络的方式（修改映射）

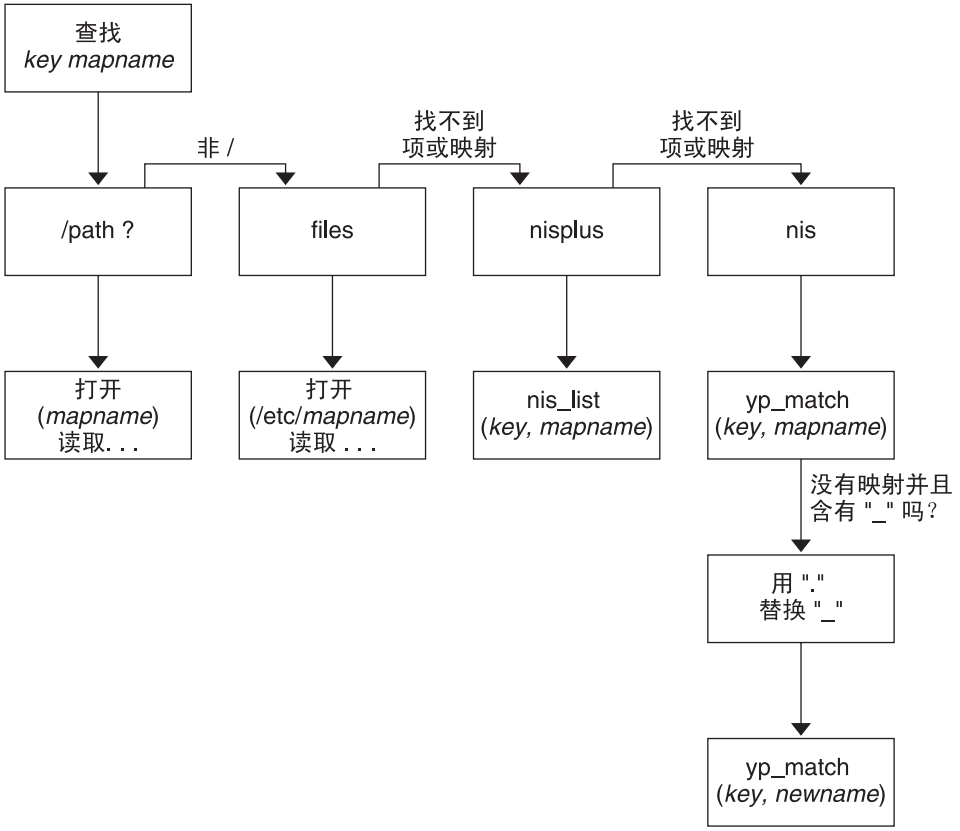
可以在映射中修改、删除或添加项，以满足环境的需要。当用户所需的应用程序和其他文件系统更改其位置时，映射必须反映这些更改。可以随时修改 autofs 映射。所做修改在 automountd 下次挂载文件系统时是否生效取决于修改的映射和修改类型。

使用名称服务时的缺省 Autofs 行为

引导时服务 svc:/system/filesystem/autofs 将调用 autofs，然后 autofs 将查找 auto_master 主映射。Autofs 遵循下文讨论的规则。

Autofs 使用在 /etc/nsswitch.conf 文件的自动挂载项中指定的名称服务。如果指定了 NIS+（而不是本地文件或 NIS），则使用所有映射的原有映射名。如果选择了 NIS，且 autofs 找不到其所需的映射，而找到包含一个或多个下划线的映射名，则会将下划线改为点。这种更改允许旧的 NIS 文件名仍然有效。然后，autofs 将再次检查映射，如图 6–6 所示。

图 6–6 Autofs 使用名称服务的方式



此会话的屏幕活动将与以下示例类似。

```
$ grep /home /etc/auto_master
/home           auto_home

$ ypmatch brent auto_home
Can’t match key brent in map auto_home.  Reason: no such map in
server’s domain.

$ ypmatch brent auto.home
diskus:/export/home/diskus1/&
```

如果选择 "files" 作为名称服务，则所有的映射都被假定为 `/etc` 目录中的本地文件。Autofs 会将以斜杠 (/) 开头的映射名解释为本地文件，无论 autofs 使用哪种名称服务。

Autofs 参考

本章的其余几节介绍更高级的 autofs 功能和主题。

Autofs 和元字符

Autofs 会将某些字符识别为具有特殊含义。某些字符用于替换，而某些字符用于保护其他字符不被 autofs 映射解析器解析。

和符号 (&)

如果您的映射中指定了许多子目录（如下所示），请考虑使用字符串替换。

```
john        willow:/home/john
mary        willow:/home/mary
joe         willow:/home/joe
able        pine:/export/able
baker       peach:/export/baker
```

可以使用和符号 (&) 替换所有关键字。如果使用和符号，则上一个映射会更改为以下形式：

```
john        willow:/home/&
mary        willow:/home/&
joe         willow:/home/&
able        pine:/export/&
baker       peach:/export/&
```

在以下情况下，还可以在直接映射中使用关键字替换：

```
/usr/man                        willow,cedar,poplar:/usr/man
```

也可以按照以下方式进一步简化项：

```
/usr/man                        willow,cedar,poplar:&
```

请注意，和符号替换使用整个关键字字符串。因此，如果直接映射中的关键字以 / 开头（按原样），则替换中应包括斜杠。因此，例如，您不能按照以下方式使用：

```
/progs                &1,&2,&3:/export/src/progs
```

原因是 autofs 会将示例解释为以下内容：

```
/progs                 /progs1,/progs2,/progs3:/export/src/progs
```

星号 (*)

可以使用通用替换字符星号 (*) 与任何关键字匹配。可以通过以下映射项从所有主机挂载 /export 文件系统。

```
*                       &:/export
```

每个和符号均替换为任何给定关键字的值。Autofs 会将星号解释为文件结束字符。

Autofs 和特殊字符

如果您的映射项包含特殊字符，则可能必须挂载其名称令 autofs 映射解析器迷惑的目录。autofs 解析器对于包含如冒号、逗号和空格等的名称非常敏感。应该用双引号括住这些名称，如下所示：

```
/vms    -ro    vmsserver: -  -  - "rc0:dk1 - "
/mac    -ro    gator:/ - "Mr Disk - "
```

第 3 部 分

SLP 主题

本节提供有关服务定位协议 (Service Location Protocol, SLP) 服务的概述、规划、任务和参考信息。

◆ ◆ ◆ 第 7 章

7 SLP（概述）

服务定位协议 （Service Location Protocol, SLP) 为已启用 SLP 的网络服务的搜索和置备提供了与平台无关的便捷框架。本章介绍用于 IP 内联网的 SLP 体系结构和 SLP 的 Solaris 实现。

SLP 体系结构

本节概括了 SLP 的基本操作，并介绍了 SLP 管理中所用的代理和进程。

只需进行少量配置或无需进行任何配置，SLP 便可自动提供下面的所有服务。

- 旨在获取访问服务所需信息的客户机应用程序请求
- 对网络硬件设备或软件服务器的服务通知；例如，打印机、文件服务器、摄像机和 HTTP 服务器
- 从主服务器故障中进行托管恢复

此外，还可以根据需要执行以下操作以管理和调整 SLP 操作。

- 将服务和用户组织到由逻辑组和功能组构成的**范围**中
- 启用 SLP 日志记录，以监视网络中的 SLP 操作或对其进行故障排除
- 调节 SLP 时间参数以提高性能和可伸缩性
- 将 SLP 配置为：在不支持多播路由的网络中部署 SLP 时，它不发送和处理多播消息
- 部署 SLP 目录代理以提高可伸缩性和性能

SLP 设计摘要

SLP 库向可识别网络的代理告知通知服务，以便在网络中搜索这些服务。SLP 代理负责维护有关服务类型和位置的最新信息。这些代理也可以使用代理注册来通知未直接启用 SLP 的服务。有关更多信息，请参见第 10 章，引入传统服务。

客户机应用程序依赖于 SLP 库，该库可直接向通知服务的代理发出请求。

SLP 代理和进程

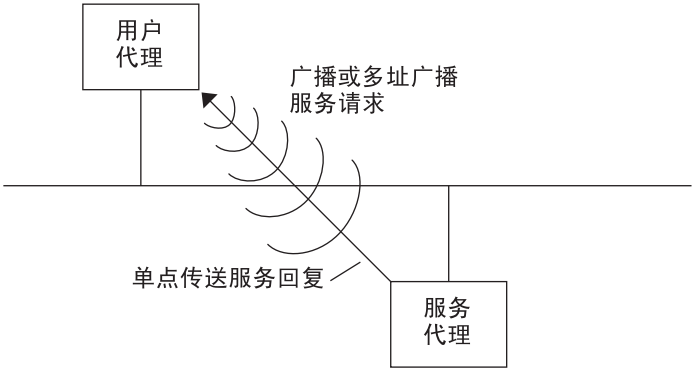
下表描述了 SLP 代理。有关本卷中使用的这些术语和其他术语的扩展定义，请参阅词汇表。

表 7–1 SLP 代理

SLP 代理	说明
目录代理 (Directory Agent, DA)	对服务代理 (Service Agent, SA) 注册的 SLP 通知进行高速缓存的进程。DA 会根据需要，将服务通知转发给用户代理 (User Agent, UA)。
服务代理 (Service Agent, SA)	代表服务来分发服务通知并向目录代理 (Directory Agent, DA) 进行注册的 SLP 代理。
用户代理 (User Agent, UA)	代表用户或应用程序获取服务通知信息的 SLP 代理。
范围	服务的管理或逻辑分组。

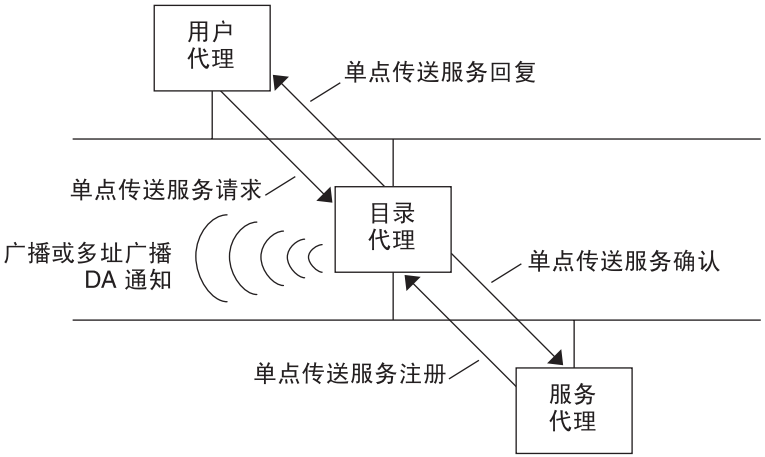
下图显示了实现 SLP 体系结构的基本代理和进程。该图表示了 SLP 的缺省部署。未进行任何特殊配置。只需要两个代理：UA 和 SA。SLP 框架允许 UA 向 SA 多播服务请求。SA 会向 UA 单点传送应答。例如，当 UA 发送服务请求消息时，SA 将以服务应答消息来响应。服务应答包含与客户机要求相匹配的服务的位置。属性和服务类型还可能具有其他请求和应答。有关更多信息，请参见第 11 章，SLP（参考）。

图 7–1 SLP 基本代理和进程



下图显示在框架中部署 DA 时用于实现 SLP 体系结构的基本代理和进程。

图 7–2 用 DA 实现的 SLP 体系结构代理和进程



部署 DA 时，网络中发送的消息较少，因此 UA 可以更快速地检索信息。当网络规模增大或者不支持多播路由时，DA 是基本要素。DA 用作已注册的服务通知的高速缓存。SA 发送注册消息 (SrvReg)，其中列出它们向 DA 通知的所有服务。然后，SA 将在应答中收到确认 (SrvAck)。服务通知将由 DA 刷新，或到期（根据为通知设置的生命周期）。UA 搜索到 DA 后，会向 DA 单点传送请求，而不向 SA 多播请求。

有关 Solaris SLP 消息的更多信息，请参阅第 11 章，SLP（参考）。

SLP 实现

在 Solaris SLP 实现中，表 7–1 中的 SLP SA、UA、DA、SA 服务器、范围和其他体系结构组件将部分映射到 `slpd` 中，部分映射到应用程序进程中。SLP 守护进程 `slpd` 会组织一些脱离主机的 SLP 交互，以执行以下操作：

- 使用被动和主动目录代理搜索，以便搜索网络中的所有 DA
- 维护更新的 DA 表，以便在本地主机上使用 UA 和 SA
- 用作传统服务通知的代理 SA 服务器（代理注册）

可以通过设置 `net.slpisDA` 属性，将 `slpd` 也配置为用作 DA。请参见第 9 章，管理 SLP（任务）。

有关 SLP 守护进程的更多信息，请参见 `slpd(1M)`。

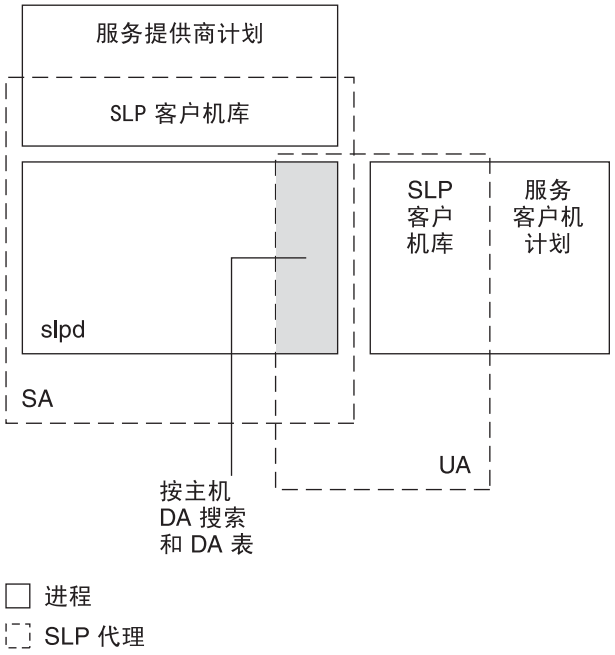
除了 slpd 之外，通过 C/C++ 和 Java 客户机库（libslp.so 和 slp.jar），也可访问 UA 和 SA 客户机的 SLP 框架。客户机库提供以下功能：

- 提供可注册和注销服务通知等网络服务的软件
- 可通过发出针对服务通知的查询来请求服务的客户机软件
- 可用于注册和请求的 SLP 范围的列表

要在 slpd 与提供上述服务的客户机库之间启用进程内通信，不必进行任何特殊配置。但是，必须在装入客户机库之前先运行 slpd 进程，该库才能正常运行。

在下图中，服务提供商计划中的 SLP 客户机库使用 SA 功能。服务提供商计划使用 SLP 客户机库来向 slpd 注册和注销服务。服务客户机计划中的 SLP 客户机库使用 UA 功能。该服务客户机计划使用 SLP 客户机库来发出请求。SLP 客户机库或者向 SA 多播请求，或向 DA 单点传送请求。此通信对应用程序是透明的，但以单点传送方式发送请求时速度更快。设置不同的 SLP 配置属性会对客户机库的行为产生影响。有关详细信息，请参见第 9 章，管理 SLP（任务）。slpd 进程可以处理所有 SA 功能，例如应答多播请求和向 DA 注册。

图 7–3 SLP 实现



其他 SLP 信息源

有关 SLP 的详细信息，请参阅以下文档：

- Kempf、James 和 Pete St. Pierre 合著的 Service Location Protocol for Enterprise Networks。John Wiley & Sons, Inc. ISBN 编号：0–471–31587–7。
- 《Authentication Management Infrastructure Administration Guide》。文件号码：805–1139–03。
- Guttman、Erik、Charles Perkins、John Veizades 和 Michael Day 合著的 Service Location Protocol, Version 2, RFC 2608，Internet 工程任务组 (Internet Engineering Task Force, IETF) 发布。[http://www.ietf.org/rfc/rfc2608.txt]
- Kempf、James 和 Erik Guttman 合著的 An API for Service Location, RFC 2614，Internet 工程任务组 (Internet Engineering Task Force, IETF) 发布。[http://www.ietf.org/rfc/rfc2614.txt]

◆ ◆ ◆ 第 8 章

规划和启用 SLP（任务）

本章介绍有关规划和启用 SLP 的信息。以下各节介绍了 SLP 配置以及 SLP 的启用过程。

SLP 配置注意事项

SLP 守护进程已预先配置为使用缺省属性。如果您的企业使用缺省设置可以正常运行，则 SLP 部署实际上不需要进行任何管理。

但在某些情况下，可能要修改 SLP 属性，以调整网络运行或激活某些功能。例如，通过一些配置更改可以启用 SLP 日志记录。SLP 日志和 snoop 跟踪中的信息有助于确定是否需要进行其他配置。

SLP 配置属性位于 `slp.conf` 文件中；该文件位于 `/etc/inet` 目录中。如果决定更改缺省属性设置，请参阅第 9 章，管理 SLP（任务）以了解相应过程。

在修改 SLP 配置设置之前，请考虑以下与网络管理的关键方面有关的问题：

- 企业中正在运行何种网络技术?
- 该技术可以顺利处理多大网络通信流量?
- 该网络可以提供多少种服务，分别是什么类型?
- 网络中有多少用户？他们需要什么服务？用户相对于他们最常访问的服务而言在哪个位置?

确定需要重新配置的内容

可以使用启用 SLP 的 snoop 实用程序和 SLP 日志记录实用程序，确定是否需要重新配置以及需要修改的属性。例如，可能需要通过重新配置某些属性来执行以下操作：

- 适应具有不同延迟和带宽特性的混合网络介质
- 从网络故障或未规划的分区中恢复企业
- 添加 DA 以减少 SLP 多播的扩散
- 实现新范围，根据用户最常访问的服务来组织用户

使用 snoop 监视 SLP 活动

snoop 实用程序是一种用于提供网络通信流量信息的被动管理工具。此实用程序自身只生成最小流量，并可使您在活动发生时监视网络中的所有活动。

snoop 实用程序可提供对实际 SLP 消息流量的跟踪。例如，在运行带有 slp 命令行参数的 snoop 时，该实用程序将在跟踪中显示有关 SLP 注册和注销的信息。通过检查哪些服务正在注册以及正在发生的重新注册活动量，可以使用此信息测量网络负载。

snoop 实用程序对于观察企业中 SLP 主机之间的通信流量也很有用。运行带有 slp 命令行参数的 snoop 时，可以监视以下类型的 SLP 活动，以确定是否需要重新配置网络或代理：

- 使用特定 DA 的主机数量。使用此信息来确定是否需要为了负载平衡而部署其他 DA。
- 使用特定 DA 的主机数量。使用此信息可帮助您确定是否为某些主机配置新范围或不同范围。
- 是 UA 请求超时还是 DA 确认较慢。可以通过监视 UA 超时并重新传输来确定 DA 是否过载，也可以检查 DA 是否需要比几秒钟长的时间来向 SA 发送注册确认。如果需要，可利用此信息通过部署其他 DA 或更改范围配置，重新平衡 DA 中的网络负载。

使用 snoop 和 -V（详细模式）命令行参数，可以获得注册生命周期和 SrvReg 中的刷新标志值，以确定是否应减少重新注册数量。

还可以使用 snoop 来跟踪其他种类的 SLP 通信流量，例如：

- UA 客户机与 DA 之间的通信流量
- 多点传送 UA 客户机与应答 SA 之间的通信流量

有关 snoop 的更多信息，请参阅 snoop(1M)。

提示 – 结合使用 netstat 命令和 snoop，查看流量和拥塞统计信息。有关 netstat 的更多信息，请参阅 netstat(1M)。

▼ 如何使用 snoop 运行 SLP 跟踪

1 **成为超级用户或承担等效角色。**

角色包含授权和具有特权的命令。有关角色的更多信息，请参见《系统管理指南：安全性服务》中的“配置 RBAC（任务列表）”。

2 **结合 slp 命令行参数运行 snoop。**

```
Brief Mode:
# snoop slp
```

在缺省的**简短**模式下运行 snoop 时，屏幕中会显示正在运行的输出。SLP 消息会被截断，以便每个 SLP 跟踪的消息占一行。

```
Verbose Mode:
# snoop -v slp
```

在**详细**模式下运行 snoop 时，snoop 会在屏幕中显示正在运行的、未缩写的输出，该输出提供以下信息：

- 服务 URL 的完整地址
- 所有服务属性
- 注册生命周期
- 所有安全参数和标志（如果可用）

注 – 可以将 slp 命令行参数与其他 snoop 选项一起使用。

分析 snoop slp 跟踪

在以下示例中，slpd 在 *slphost1* 上以缺省模式作为 SA 服务器运行。SLP 守护进程会将 *slphost2* 初始化并注册为回显服务器。然后，在 *slphost1* 上调用 snoop slp 进程。

注 – 为简化对跟踪结果的说明，以下 snoop 输出中的各行都用行号作为标志。

```
(1) slphost1 -> 239.255.255.253 SLP V@ SrvRqst [24487] service:directory-agent []
(2) slphost2 -> slphost1 SLP V2 DAAdvert [24487] service:directory-agent://129
(3) slphost1 -> 239.255.255.253 SLP V2 SrvRqst [24487] service:directory-agent []
(4) slphost1 -> 239.255.255.253 SLP V2 SrvRqst [24487] service:directory-agent []
```

```
(5) slphost1 -> slphost2 SLP V2 SrvReg [24488/tcp]service:echo.sun:tcp://slphost1:
(6) slphost2 -> slphost1 SLP V2 SrvAck [24488/tcp] ok
(7) slphost1 -> slphost2 SLP V2 SrvDereg [24489/tcp] service:echo.sun:tcp://slphost1:
(8) slphost2 -> slphost1 SLP V2 SrvAck [24489/tcp] ok
```

1. 显示 *slphost1* 上的 `slpd`，该守护进程通过向 SLP 多播组地址进行多播，执行活动目录代理搜索来搜索目录代理。在跟踪显示中，用于主动搜索的消息编号 24487 在方括号中表示。
2. 表示来自跟踪 1 的主动搜索请求 24487 由 `slpd` 应答，该守护进程作为 DA 在主机 *slphost2* 上运行。*slphost2* 中的服务 URL 已被截断，以便显示在一行中。DA 已发送 DA 通知作为对多播目录代理搜索消息的应答，如跟踪 1 和 2 中匹配的消息编号所示。
3. 显示 *slphost1* 中的 UA 对于其他 DA 的多播。由于 *slphost2* 已对请求做出应答，因此它将禁止再次响应，不会进行其他的 DA 应答。
4. 重复上一行中显示的多播操作。
5. 在向 *slphost2* 中的 DA转发 SA 客户机注册的 *slphost1* 上显示 `slpd`。*slphost1* 向 *slphost2* 上的 DA 进行回显服务器的单播服务注册 (`SrvReg`)。
6. 显示 *slphost2* 对 *slphost1* `SrvReg` 的响应，该响应带有指示注册已成功的服务确认 (`SrvAck`)。

   `snoop` 跟踪中不显示运行 SA 客户机的回显服务器与 *slphost1* 上的 SLP 守护进程之间的流量。缺少此信息的原因是 `snoop` 操作通过网络回送执行。
7. 在注销回显服务通知的 *slphost1* 上显示回显服务器。*slphost1* 中的 SLP 守护进程会将注销转发给 *slphost2* 上的 DA。
8. 显示 *slphost2* 对 *slphost1* 的响应，该响应带有指示取消注册成功的服务确认 (`SrvAck`)。

   第 5、6、7 和 8 行的消息编号后附加的 `/tcp` 参数指示通过 TCP 进行了消息交换。

下一步执行的操作

监视 SLP 通信流量后，可以使用从 `snoop` 跟踪中收集的信息来确定是否需要对 SLP 缺省值进行任何重新配置。使用第 9 章，管理 SLP（任务）中的相关信息来配置 SLP 属性设置。有关 SLP 消息和服务注册的更多信息，请参阅第 11 章，SLP（参考）。

◆ ◆ ◆ 第 9 章

9 管理 SLP（任务）

以下各节介绍用于配置 SLP 代理和进程的信息和任务。

配置 SLP 属性

SLP 配置属性控制网络交互、SLP 代理的特性、状态和日志记录。在大多数情况下，无需对这些属性的缺省配置进行任何修改。但当网络介质或拓扑结构发生更改时，可以使用本章中的过程实现以下目标：

- 补偿网络延迟
- 减轻网络拥塞
- 添加代理或重新指定 IP 地址
- 激活 SLP 日志记录

可以编辑 SLP 配置文件 `/etc/inet/slp.conf`，来执行下表列出的操作。

表 9–1 SLP 配置操作

操作	说明
指定 `slpd` 是否应用作 DA 服务器。SA 服务器是缺省设置。	将 `net.slpisDA` 属性设置为 `True`。
为 DA 多播消息设置时间。	设置 `net.slp.DAHeartBeat` 属性可控制 DA 多播未经请求的 DA 通告的频率。
启用 DA 日志记录以监视网络通信流量。	将 `net.slp.traceDATraffic` 属性设置为 `True` 。

SLP 配置文件：基本元素

当您每次重新启动 SLP 守护进程时，`/etc/inet/slp.conf` 文件都会定义和激活所有 SLP 活动。该配置文件由以下元素组成：

- 配置属性
- 注释行和表示法

配置属性

所有基本 SLP 属性（如 `net.slp.isDA` 和 `net.slp.DAHeartBeat`）都按以下格式命名。

```
net.slp.<keyword>
```

SLP 行为由 `slp.conf` 文件中的一个属性或一组属性的值来定义。在 SLP 配置文件中，属性的结构类似于关键字-值对。如以下示例所示，关键字-值对由属性名称和相关设置组成。

```
<property name>=<value>
```

每个属性的关键字都是指属性名称。值可为属性设置数值（距离或时间）、true/false 状态或字符串值参数。属性值可以为下列数据类型之一：

- True/False 设置（布尔值）
- 整数
- 整数列表
- 字符串
- 字符串列表

如果不允许使用定义的值，则使用该属性名称的缺省值。此外，还会使用 syslog 记录一条错误消息。

注释行和表示法

可向 `slp.conf` 文件中添加注释，以介绍该行的特性和功能。文件中的注释行是可选的，但对于管理很有用。

注 – 配置文件中的设置不区分大小写。有关更多信息，请参阅：Erik Guttman、James Kempf 和 Charles Perkins 合著的 "Service Templates and Service:Schemes"，即 Internet 工程任务组 (Internet Engineering Task Force, IETF) 中的 RFC 2609。[http://www.ietf.org/rfc/rfc2609.txt]

▼ 如何更改 SLP 配置

使用此过程可以更改 SLP 配置文件中的属性设置。启用 SLP 的客户机或服务软件也可以使用 SLP API 来更改 SLP 配置。Internet 工程任务组 (Internet Engineering Task Force, IETF) 中的 RFC 2614 "An API for Service Location" 中介绍了此 API。[http://www.ietf.org/rfc/rfc2614.txt]

1. **成为超级用户或承担等效角色。**

   角色包含授权和具有特权的命令。有关角色的更多信息，请参见《系统管理指南：安全性服务》中的“配置 RBAC（任务列表）”。

2. **停止 `slpd` 和主机上的所有 SLP 活动。**

   ```
   # svcadm disable network/slp
   ```

3. **在更改配置设置之前，先备份缺省的 `/etc/inet/slp.conf` 文件。**

4. **根据需要在 `/etc/inet/slp.conf` 文件中编辑属性设置。**

   有关 SLP 属性设置的一般信息，请参阅第 208 页中的 “配置属性”。有关可能需要更改 `slp.conf` 属性的不同情况的示例，请参见此过程之后的各节。请参见 `slp.conf(4)`。

5. **保存更改并关闭文件。**

6. **重新启动 `slpd` 以激活更改。**

   ```
   # svcadm enable network/slp
   ```

注 – 当您停止或启动 `slpd` 时，SLP 守护进程将从配置文件中获取信息。

示例 9–1 设置 slpd 以将其用作 DA 服务器

通过在 `slpd.conf` 文件中将 `net.slp.isDA` 属性设置为 `True`，可以更改 SA 服务器缺省值，将 `slpd` 用作 DA 服务器。

```
net.slp.isDA=True
```

在每个区域中，不同属性可以控制配置的不同方面。以下各节介绍了可能需要更改 SLP 配置中所用的缺省属性设置的不同情况。

修改 DA 通告和搜索频率

在下列情况下，可以修改用于控制 DA 通告和搜索请求的时间的属性。

- 当您希望 SA 或 UA 从 `slp.conf` 文件的 `net.slp.DAAddresses` 属性中静态获取 DA 配置信息时，可以禁用 DA 搜索。
- 当网络经常进行分区时，可以更改被动通告和主动搜索的频率。
- 如果 UA 和 SA 客户机在拨号连接的另一端访问 DA，则可降低 DA 心跳频率和主动搜索间隔，以减少激活拨号线的次数。
- 如果网络拥塞严重，则可限制多播。

本节中的过程说明如何修改以下属性。

表 9–2 DA 通告时间和搜索请求属性

属性	说明
`net.slp.passiveDADetection`	布尔值，指定 `slpd` 是否侦听未经请求的 DA 通告。
`net.slp.DAActiveDiscoveryInterval`	一个值，指定 `slpd` 执行主动 DA 搜索以发现新 DA 的频率
`net.slp.DAHeartBeat`	一个值，指定 DA 多播未经请求的 DA 通告的频率

将 UA 和 SA 限制为静态配置的 DA

有时可能需要将 UA 和 SA 限制为从 `slp.conf` 文件的静态配置信息中获取 DA 地址。在下一个过程中，可以修改两个属性，以使 `slpd` 只从 `net.slp.DAAddresses` 属性中获取 DA 信息。

▼ 如何将 UA 和 SA 限制为静态配置的 DA

使用以下过程更改 `net.slp.passiveDADetection` 和 `net.slp.DAActiveDiscoveryInterval` 属性。

注 – 只能在执行 UA 和 SA（限制为静态配置）的主机上使用此过程。

---

1 成为超级用户或承担等效角色。

角色包含授权和具有特权的命令。有关角色的更多信息，请参见《系统管理指南：安全性服务》中的“配置 RBAC（任务列表）”。

2 停止 `slpd` 和主机上的所有 SLP 活动。

```
# svcadm disable network/slp
```

3. **在更改配置设置之前，先备份缺省的 `/etc/inet/slp.conf` 文件。**

4. **在 `slp.conf` 文件中将 `net.slp.passiveDADetection` 属性设置为 `False`，以禁用被动搜索。此设置会使 `slpd` 忽略未经请求的 DA 通告。**

   ```
   net.slp.passiveDADetection=False
   ```

5. **将 `net.slp.DAActiveDiscoveryInterval` 属性设置为 `-1`，以禁用初始和定期的主动搜索。**

   ```
   net.slp.DAActiveDiscoveryInterval=-1
   ```

6. **保存更改并关闭文件。**

7. **重新启动 `slpd` 以激活更改。**

   ```
   # svcadm enable network/slp
   ```

为拨号网络配置 DA 搜索

如果 UA 或 SA 通过拨号网络与 DA 分隔，则可配置 DA 搜索，以减少或消除搜索请求和 DA 通告的数量。激活拨号网络通常需要收费。最大程度地减少多余调用可以降低使用拨号网络的成本。

注 – 使用第 210 页中的 “将 UA 和 SA 限制为静态配置的 DA”中介绍的方法可以完全禁用 DA 搜索。

▼ 如何为拨号网络配置 DA 搜索

使用以下过程，可以通过增大 DA 心跳周期和主动搜索间隔来减少未经请求的 DA 通告和主动搜索。

1. **成为超级用户或承担等效角色。**

   角色包含授权和具有特权的命令。有关角色的更多信息，请参见《系统管理指南：安全性服务》中的“配置 RBAC（任务列表）”。

2. **停止 `slpd` 和主机上的所有 SLP 活动。**

   ```
   # svcadm disable network/slp
   ```

3. **在更改配置设置之前，先备份缺省的 `/etc/inet/slp.conf` 文件。**

4. **在 `slpd.conf` 文件中增大 `net.slp.DAHeartbeat` 属性的值。**

   ```
   net.slp.DAHeartbeat=value
   ```

   value　　一个 32 位整数，用于设置被动 DA 通告心跳的秒数

缺省值 = 10800 秒（3 小时）

值的范围 = 2000–259200000 秒

例如，在执行 DA 的主机上，可将 DA 心跳设置为大约 18 小时：

```
net.slp.DAHeartbeat=65535
```

5 **在 `slpd.conf` 文件中增大 `net.slp.DAActiveDiscoveryInterval` 属性的值。**

`net.slp.DAActiveDiscoveryInterval` *value*

value 一个 32 位整数，用于设置 DA 主动搜索查询的秒数

缺省值 = 900 秒（15 分钟）

值的范围 = 300–10800 秒

例如，在执行 UA 和 SA 的主机上，可将 DA 主动搜索间隔设置为 18 小时：

```
net.slp.DAActiveDiscoveryInterval=65535
```

6 **保存更改并关闭文件。**

7 **重新启动 `slpd` 以激活更改。**

```
# svcadm enable network/slp
```

为常用分区配置 DA 心跳

SA 需要向支持其范围的所有 DA 进行注册。在 `slpd` 执行主动搜索后，会出现一个 DA。如果此 DA 支持 `slpd` 范围，则 SLP 守护进程会向此 DA 注册其主机上的所有通告。

`slpd` 搜索 DA 的一种方法是使用 DA 在引导时发送的第一份未经请求的通告。SLP 守护进程使用此周期性的未经请求通告（心跳）来确定 DA 是否仍处于活动状态。如果心跳未能出现，则守护进程将删除它使用的 DA 以及它为 UA 提供的 DA。

最后，当 DA 遇到受控制的关机时，将发送一份特殊的 DA 通告，通知侦听 SA 服务它将不在服务范围。SLP 守护进程还使用此通告从高速缓存中删除非活动 DA。

如果网络经常进行分区并且 SA 长期存在，则当未接收到心跳通告时，`slpd` 可在分区期间删除缓存的 DA。通过减少心跳时间，可以减少分区修复后、取消激活的 DA 恢复到高速缓存之前的延迟。

▼ 如何为常用分区配置 DA 心跳

使用以下过程可以更改 net.slp.DAHeartBeat 属性，从而缩短 DA 心跳周期。

注 – 如果 DA 搜索完全禁用，则必须在执行 UA 和 SA 的主机上的 slp.conf 中设置 net.slp.DAAddresses 属性，主机才能访问正确的 DA。

---

1. **成为超级用户或承担等效角色。**

   角色包含授权和具有特权的命令。有关角色的更多信息，请参见《系统管理指南：安全性服务》中的“配置 RBAC（任务列表）”。

2. **停止 slpd 和主机上的所有 SLP 活动。**

   ```
   # svcadm disable network/slp
   ```

3. **在更改配置设置之前，先备份缺省的 /etc/inet/slp.conf 文件。**

4. **将 net.slp.DAHeartBeat 值减小为 1 小时（ 3600 秒 ）。缺省情况下，DA 心跳周期设置为 3 小时（ 10800 秒 ）。**

   ```
   net.slp.DAHeartBeat=3600
   ```

5. **保存更改并关闭文件。**

6. **重新启动 slpd 以激活更改。**

   ```
   # svcadm enable network/slp
   ```

减轻网络拥塞

如果网络拥塞很严重，则可限制多播活动量。如果网络中尚未部署 DA，则部署 DA 会显著减少与 SLP 相关的多播量。

但即使在部署 DA 之后，DA 搜索仍然需要多播。通过使用第 211 页中的 “如何为拨号网络配置 DA 搜索”中介绍的方法可以降低 DA 搜索所需的多播量。通过使用第 210 页中的 “将 UA 和 SA 限制为静态配置的 DA”中介绍的方法可以完全消除用于 DA 搜索的多播。

适应不同的网络介质、拓扑结构或配置

本节介绍可以通过更改以下属性来调节 SLP 性能的可能情况。

表 9–3 SLP 性能属性

属性	说明
net.slp.DAAttributes	DA 接受通告的最短刷新间隔。
net.slp.multicastTTL	为多播包指定的**生存时间**值。
net.slp.MTU	为网络包设置的字节大小。该大小包括 IP 以及 TCP 或 UDP 数据包头。
net.slp.isBroadcastOnly	布尔值，设置该值以指示是否应将广播用于 DA 搜索和不基于 DA 的服务搜索。

减少 SA 重新注册

SA 在生命周期到期之前，需要定期刷新其服务通告。如果 DA 需要处理来自许多 UA 和 SA 的大量负载，则频繁刷新会导致 DA 过载。如果 DA 过载，UA 请求将开始超时，然后将被删除。UA 请求超时可能有多种原因。在您断定 DA 过载是导致 UA 请求超时的原因之前，应先使用 snoop 跟踪来检查已进行服务注册的服务通告的生命周期。如果生命周期很短并且重新注册频繁发生，则超时很可能是由频繁重新注册引起的。

注 – 如果未设置 FRESH 标志，则注册服务时就会造成服务的**重新注册**。有关服务注册消息的更多信息，请参见第 11 章，SLP（参考）。

▼ 如何减少 SA 重新注册

使用以下过程可以增大 SA 的最短刷新间隔，以减少重新注册。

1. **成为超级用户或承担等效角色。**

   角色包含授权和具有特权的命令。有关角色的更多信息，请参见《系统管理指南：安全性服务》中的“配置 RBAC（任务列表）”。

2. **停止 slpd 和主机上的所有 SLP 活动。**

   ```
   # svcadm disable network/slp
   ```

3. **在更改配置设置之前，先备份缺省的 /etc/inet/slp.conf 文件。**

4. **增大 net.slp.DAAttributes 属性的 min-refresh-interval 属性的值。**

   缺省的最短重新注册周期是零。缺省值零允许 SA 在任意时刻注册。在以下示例中，该间隔增大到 3600 秒（1 小时）。

   ```
   net.slp.DAAttributes(min-refresh-interval=3600)
   ```

5 保存更改并关闭文件。

6 重新启动 slpd 以激活更改。

```
# svcadm enable network/slp
```

配置多播生存时间属性

多播生存时间属性 (net.slp.multicastTTL) 决定了多播包在内联网中的传播范围。多播 TTL 是通过将 net.slp.multicastTTL 属性设置为 1 与 255 之间的整数来配置的。多播 TTL 的缺省值为 255，这意味着从理论上讲，包路由不受限制。但是，TTL 为 255 时会使多播包穿透内联网，到达管理域边缘的边界路由器。需要在边界路由器上正确配置多播，才能防止多播包泄漏到 Internet 的多播主干中，或泄露给您的 ISP。

多播 TTL 作用域设置与标准 IP TTL 相似，区别在于要进行 TTL 比较。对于启用了多播的路由器上的每个接口，都会为其指定一个 TTL 值。当多播包到达时，路由器会将该包的 TTL 与接口的 TTL 进行比较。如果包的 TTL 大于或等于接口的 TTL，包 TTL 将减小 1，这与标准 IP TTL 相同。如果 TTL 变为零，将放弃该包。将 TTL 作用域设置用于 SLP 多播时，必须对路由器进行正确配置，以将包限制到内联网的特定子段。

▼ 如何配置多播生存时间属性

使用以下过程可以重置 net.slp.multicastTTL 属性。

1 成为超级用户或承担等效角色。

角色包含授权和具有特权的命令。有关角色的更多信息，请参见《系统管理指南：安全性服务》中的“配置 RBAC（任务列表）”。

2 停止 slpd 和主机上的所有 SLP 活动。

```
# svcadm disable network/slp
```

3 在更改配置设置之前，先备份缺省的 /etc/inet/slp.conf 文件。

4 在 slpd.conf 文件中更改 net.slp.multicastTTL 属性：

net.slp.multicastTTL=*value*

value 小于或等于 255 的正整数，用于定义多播 TTL

注 – 通过减小 TTL 值可以缩小多播传播的范围。如果 TTL 值为 1，包将限制到子网。如果该值为 32，包将限制到该站点。不过，术语**站点**不是由 RFC 1075 定义的，RFC 1075 探讨了多播 TTL。大于 32 的值表示 Internet 上的理论路由，不应使用。如果路由器正确配置了 TTL，则小于 32 的值可用来将多播限制到一组可访问的子网。

---

5 保存更改并关闭文件。

6 **重新启动 slpd 以激活更改。**

```
# svcadm enable network/slp
```

配置包大小

SLP 的缺省包大小为 1400 字节。对于大多数局域网而言，该大小应该足够。对于无线网络或广域网而言，可以减小包大小，以避免消息分段并减少网络通信流量。对于具有较大包的局域网而言，增大包大小可以改善性能。通过检查网络的最小包大小可以确定是否需要减小包大小。如果网络介质具有较小的包大小，则可相应减小 `net.slp.MTU` 的值。

如果网络介质具有较大的包，则可增大包大小。但是，除非来自 SA 的服务通告或来自 UA 的查询频繁使缺省包大小溢出，否则不应更改 `net.slp.MTU` 值。可以使用 `snoop` 来确定 UA 请求是否经常使缺省包大小溢出，并滚动使用 TCP 而非 UDP。

`net.slp.MTU` 属性会度量完整的 IP 包大小，包括链路层头、IP 数据包头、UDP 或 TCP 数据包头以及 SLP 消息。

▼ 如何配置包大小

使用以下过程通过调节 `net.slp.MTU` 属性来更改缺省包大小。

1 **成为超级用户或承担等效角色。**

角色包含授权和具有特权的命令。有关角色的更多信息，请参见《系统管理指南：安全性服务》中的“配置 RBAC（任务列表）”。

2 **停止 slpd 和主机上的所有 SLP 活动。**

```
# svcadm disable network/slp
```

3 **在更改配置设置之前，先备份缺省的 /etc/inet/slp.conf 文件。**

4 **在 slpd.conf 文件中更改 net.slp.MTU 属性。**

`net.slp.MTU=`*value*

value 一个 16 位整数，用于指定网络包大小（以字节为单位）

缺省值 = 1400

值范围 = 128–8192

5 **保存更改并关闭文件。**

6 **重新启动 slpd 以激活更改。**

```
# svcadm enable network/slp
```

配置仅限广播路由

设计 SLP 的目的是使用多播来进行服务搜索（不存在 DA 时）和 DA 搜索。如果网络不部署多播路由，则可通过将 net.slp.isBroadcastOnly 属性设置为 True 来将 SLP 配置为使用广播。

与多播不同，广播包缺省情况下不在子网中传播。因此，在非多播网络中没有 DA 的服务搜索只适用于单个子网。此外，在使用广播的网络中部署 DA 和范围时，需要考虑特殊的注意事项。多宿主主机上的 DA 可在禁用多播的多个子网之间桥接服务搜索。有关在多宿主主机上部署 DA 的更多信息，请参见第 229 页中的 “DA 放置和范围名称指定”。

▼ 如何配置仅限广播路由

使用以下过程可将 net.slp.isBroadcastOnly 属性更改为 True。

1 **成为超级用户或承担等效角色。**

角色包含授权和具有特权的命令。有关角色的更多信息，请参见《系统管理指南：安全性服务》中的“配置 RBAC（任务列表）”。

2 **停止 slpd 和主机上的所有 SLP 活动。**

```
# svcadm disable network/slp
```

3 **在更改配置设置之前，先备份缺省的 /etc/inet/slp.conf 文件。**

4 **在 slpd.conf 文件中将 net.slp.isBroadcastOnly 属性更改为 True：**

```
net.slp.isBroadcastOnly=True
```

5 **保存更改并关闭文件。**

6 **重新启动 slpd 以激活更改。**

```
# svcadm enable network/slp
```

修改 SLP 搜索请求的超时

在以下两种情况下，可能需要更改 SLP 搜索请求的超时：

- 如果 SLP 代理被多个子网、拨号线路或其他 WAN 分隔，则网络延迟可能太高，导致请求或注册无法在缺省超时时间内完成。相反，如果网络为低延迟，则可通过减小超时来改善性能。
- 如果网络通信流量很大或冲突率很高，则 SA 和 UA 在发送消息前需要等待的最长时间可能不足以确保事务无冲突。

更改缺省超时

高网络延迟可能导致 UA 和 SA 在请求和注册的响应返回之前超时。如果多个子网、拨号线路或 WAN 将 UA 与 SA 分隔，或者同时将 UA 和 SA 与 DA 分隔，则延迟可能会导致问题。通过检查 SLP 请求是否因 UA 和 SA 请求和注册的超时而失败，可以确定延迟是否是问题所在。也可使用 `ping` 命令来度量实际延迟。

下表列出了用于控制超时的配置属性。可以使用本节中的过程来修改这些属性。

表 9–4 超时属性

属性	说明

`net.slp.multicastTimeouts`
`net.slp.DADiscoveryTimeouts`
`net.slp.datagramTimeouts`
	这些属性可以控制在放弃传输之前用于重复的多播和单播 UDP 消息传输的超时。

`net.slp.multicastMaximumWait`	该属性可以控制放弃多播消息之前传输该消息的最长时间。
`net.slp.datagramTimeouts`	DA 超时的上界，由为此属性列出的值的总和来指定。会向 DA 重复发送 UDP 数据报，直到收到响应或达到超时界限为止。

如果在多播服务搜索或 DA 搜索期间频繁出现超时现象，可增大 `net.slp.multicastMaximumWait` 属性的值，其缺省值为 15000 毫秒（15 秒）。增大最长等待时间可以留出更多时间，以便完成高延迟网络中的请求。在更改 `net.slp.multicastMaximumWait` 之后，还应该修改 `net.slp.multicastTimeouts` 和 `net.slp.DADiscoveryTimeouts`。这些属性的超时值之和等于 `net.slp.multicastMaximumWait` 值。

▼ 如何更改缺省超时

使用以下过程可以更改用于控制超时的 SLP 属性。

1 **成为超级用户或承担等效角色。**

角色包含授权和具有特权的命令。有关角色的更多信息，请参见《系统管理指南：安全性服务》中的“配置 RBAC（任务列表）”。

2 **停止 `slpd` 和主机上的所有 SLP 活动。**

```
# svcadm disable network/slp
```

3 **在更改配置设置之前，先备份缺省的 `/etc/inet/slp.conf` 文件。**

4 **在 `slpd.conf` 文件中更改 `net.slp.multicastMaximumWait` 属性。**

`net.slp.multicastMaximumWait=`*value*

value 32 位整数，它列出为 `net.slp.multicastTimeouts` 和 `net.slp.DADiscoveryTimeouts` 设置的值之和

缺省值 = 15000 毫秒（15 秒）

值范围 = 1000 至 60000 毫秒

例如，如果确定多播请求需要等待 20 秒（20000 毫秒），则需要调整为 `net.slp.multicastTimeouts` 和 `net.slp.DADiscoveryTimeouts` 属性列出的值，使两者之和等于 20000 毫秒。

```
net.slp.multicastMaximumWait=20000
net.slp.multicastTimeouts=2000,5000,6000,7000
net.slp.DADiscoveryTimeouts=3000,3000,6000,8000
```

5 **如果需要，请在 `slpd.conf` 文件中更改 `net.slp.datagramTimeouts` 属性：**

`net.slp.datagramTimeouts=`*value*

value 32 位整数的列表，它以毫秒为单位指定将单播数据报传输实现到 DA 时的超时

缺省值 = 3000,3000,3000

例如，可将数据报超时增大到 20000 毫秒，以避免频繁超时。

```
net.slp.datagramTimeouts=2000,5000,6000,7000
```

在高性能网络中，可以减小多播和单播 UDP 数据报传输的超时界限。如果减小超时界限，则同时会减小满足 SLP 请求所需的延迟。

6 **保存更改并关闭文件。**

7 **重新启动 slpd 以激活更改。**

```
# svcadm enable network/slp
```

配置随机等待界限

如果网络通信流量很大或冲突率很高，与 DA 的通信可能会受到影响。冲突率很高时，发送代理必须重新传送 UDP 数据报。通过使用 snoop 来监视作为 SA 服务器运行 slpd 的主机和作为 DA 运行 slpd 的主机网络中的流量，可以确定是否正在重新传输。在作为 SA 服务器运行 slpd 的主机的 snoop 跟踪中，如果出现同一服务的多个服务注册消息，则可能存在通知冲突。

在引导时，冲突特别容易引起问题。当 DA 最初启动时，它会发送未经请求的通告，并且 SA 以注册进行响应。SLP 要求 SA在接收 DA 通告后随机等待一段时间再进行响应。随机等待界限分布均匀，最大值由 net.slp.randomWaitBound 控制。缺省的随机等待界限为 1000 毫秒（1 秒）。

▼ 如何配置随机等待界限

使用以下过程在 slp.conf 文件中更改 net.slp.RandomWaitBound 属性。

1 **成为超级用户或承担等效角色。**

角色包含授权和具有特权的命令。有关角色的更多信息，请参见《系统管理指南：安全性服务》中的“配置 RBAC（任务列表）”。

2 **停止 slpd 和主机上的所有 SLP 活动。**

```
# svcadm disable network/slp
```

3 **更改配置设置之前，先备份缺省的 /etc/inet/slp.conf 文件。**

4 **在 slpd.conf 文件中更改 net.slp.RandomWaitBound 属性：**

net.slp.RandomWaitBound=*value*

value 用于计算在尝试联系 DA 之前的随机等待时间的上界

缺省值 = 1000 毫秒（1 秒）

值范围 = 1000 至 3000 毫秒

例如，可将最长等待时间延长至 2000 毫秒（2 秒）。

```
net.slp.randomWaitBound=2000
```

延长随机等待界限时，注册中将出现更长的延迟。SA 可以用新搜索到的 DA 以更慢的速度完成注册，以避免冲突和超时。

5 **如果需要，请在 slpd.conf 文件中更改 net.slp.datagramTimeouts 属性：**

```
net.slp.datgramTimeouts=value
```

value 32 位整数的列表，它以毫秒为单位指定将单播数据报传输实现到 DA 时的超时

缺省值 = 3000,3000,3000

例如，可将数据报超时增大到 20000 毫秒，以避免频繁超时。

```
net.slp.datagramTimeouts=2000,5000,6000,7000
```

在高性能网络中，可以减小多播和单播 UDP 数据报传输的超时界限。此设置可减小满足 SLP 请求时的延迟量。

6 **保存更改并关闭文件。**

7 **重新启动 slpd 以激活更改。**

```
# svcadm enable network/slp
```

部署范围

借助范围可对依赖于用户的逻辑、物理和管理分组的服务进行调配。使用范围可对服务通告的访问进行管理。

使用 net.slp.useScopes 属性创建范围。例如，在主机上的 /etc/inet/slp.conf 文件中，添加一个名为 newscope 的新范围，如下所示：

```
net.slp.useScopes=newscope
```

例如，您的公司可能在 6 号楼的 2 层的南厅一端有一个联网设备室，联网设备包括打印机和传真机等。2 层的所有人都可以使用这些设备，也可以将这些设备的使用权限定给某个部门的成员。通过范围可对这些计算机的服务通告的访问进行调配。

如果设备专供一个部门使用，则可用该部门的名称创建一个范围，例如 mktg。属于其他部门的设备可用不同的范围名称来配置。

在另一种情况下，部门可能是分散的。例如，机械工程部门和 CAD/CAM 部门可能分散在 1 层和 2 层。但是，可将 2 层的计算机提供给这两层的主机，方法是为其指定相同的范围。可以通过适用于网络和用户的其他任何方式来部署范围。

注 – 实际上，并不禁止具有特定范围的 UA 使用在其他范围内通告的服务。配置范围只控制 UA 检测哪些服务通告。该服务负责强制实施所有访问控制限制。

何时配置范围

无需进行任何范围配置，SLP 便可正常工作。在 Solaris 操作环境中，SLP 的缺省范围是 `default`。如果没有配置任何范围，则 `default` 是所有 SLP 消息的范围。

可在以下任何情况下配置范围。

- 您支持的组织要将服务通告访问限制为自己的成员。
- 您所支持的组织的物理布局表明，某一区域中的服务只能由特定用户访问。
- 适合特定用户查看的服务通告必须进行分区。

第 211 页中的“为拨号网络配置 DA 搜索”中列举了第一种情况的示例。第二种情况的示例是，组织分布于两个大楼内，您希望大楼内的用户访问本大楼内的本地服务。可为 1 号楼内的用户配置 `B1` 范围，而为 2 号楼的用户配置 `B2` 范围。

配置范围时的注意事项

当您在 `slpd.conf` 文件中修改 `net.slp.useScopes` 属性时，便会为主机上的所有代理配置范围。当主机正在运行任何 SA 或用作 DA 时，如果要将 SA 或 DA 配置到 `default` 之外的范围中，则必须配置此属性。如果只有 UA 在计算机中运行，并且 UA 应搜索 `default` 之外的 SA 和 DA 支持范围，则除非要限制 UA 使用的范围，否则无需配置此属性。如果未配置该属性，UA 可以通过 `slpd` 自动搜索可用的 DA 和范围。SLP 守护进程使用主动和被动 DA 搜索来查找 DA，如果没有 DA 在运行，则使用 SA 搜索。另外，如果已配置上述属性，UA 将只使用已配置的范围，而不会将其废弃。

如果您决定要配置范围，则应考虑将 `default` 范围保留在已配置范围的列表中，除非您确信网络中的所有 SA 都配置了范围。如果有任何 SA 未配置，则已配置范围的 UA 将无法找到这些 SA。出现这种情况的原因是，未配置的 SA 会自动以 `default` 为范围，而 UA 会使用已配置的范围。

如果您还决定通过设置 `net.slp.DAAddresses` 属性来配置 DA，请确保已配置的 DA 所支持的范围与您使用 `net.slp.useScopes` 属性配置的范围相同。如果这两个范围不同，`slpd` 将在重新启动时输出错误消息。

▼ 如何配置范围

使用以下过程在 `slp.conf` 文件中为 `net.slp.useScopes` 属性添加范围名称。

1. **成为超级用户或承担等效角色。**

   角色包含授权和具有特权的命令。有关角色的更多信息，请参见《系统管理指南：安全性服务》中的“配置 RBAC（任务列表）”。

2 **停止 `slpd` 和主机上的所有 SLP 活动。**

```
# svcadm disable network/slp
```

3 **在更改配置设置之前，先备份缺省的 `/etc/inet/slp.conf` 文件。**

4 **在 `slpd.conf` 文件中更改 `net.slp.useScopes` 属性：**

`net.slp.useScopes=`*<scope names>*

scope names 字符串列表，表示 DA 或 SA 发出请求时可使用的范围或表示 DA 必须支持的范围

缺省值 = 缺省值（SA 和 DA）/未指定 (UA)

注 –

使用以下各项来构造范围名称：

- 任何字母数字字符（大写或小写）
- 任何标点符号（"、\、!、<、=、> 和 ~ 除外）
- 被视为名称一部分的空格
- 非 ASCII 字符

  使用反斜杠可对非 ASCII 字符进行转义。例如，UTF-8 编码使用 `0xc3a9` 十六进制代码来表示具有法语 *aigue* 重音的字母 *e*。如果平台不支持 UTF-8，则可使用 UTF-8 十六进制代码作为转义序列 `\c3\a9`。

例如，要为 `bldg6` 中的 `eng` 组和 `mktg` 组指定范围，请对 `net.slp.useScopes` 行进行如下更改。

```
net.slp.useScopes=eng,mktg,bldg6
```

5 **保存更改并关闭文件。**

6 **重新启动 `slpd` 以激活更改。**

```
# svcadm enable network/slp
```

部署 DA

本节介绍 DA 在运行 SLP 的网络中的战略部署。

只需具有基本代理（UA 和 SA），无需部署 DA 或配置范围，SLP 便可正常运行。缺少特定配置的所有代理都使用 `default` 范围。DA 用作服务通告的高速缓存。部署 DA 会减少在网络中发送的消息数，并可缩短接收消息响应所需的时间。此功能使 SLP 可以适应更大型的网络。

部署 SLP DA 的原因？

部署 DA 的主要原因是减小多播流量和缩短与收集单播应答有关的延迟。在具有许多 UA 和 SA 的大型网络中，服务搜索所涉及的多播流量可能会很大，从而导致网络性能下降。通过部署一个或多个 DA，UA 必须为服务向 DA 进行单播，并且 SA 必须使用单播向 DA 注册。网络中唯一向 DA 进行注册的 SLP 多播是用于主动和被动 DA 搜索的。

SA 会自动向其在一组通用范围内搜索到的任何 DA 进行注册，而不是接受多播服务请求。但是，在 DA 不支持的范围内的多播请求仍然直接由 SA 来应答。

在 UA 的范围内部署 DA 时，来自 UA 的服务请求将单播至 DA，而非多播至网络。因此，UA 范围中的 DA 将减少多播。通过减少用于正常 UA 请求的多播，可以大大减少获得查询应答所需的时间（从若干秒减少到若干毫秒）。

DA 用作 SA 和 UA 活动的焦点。为范围集合部署一个或多个 DA 可提供用于监视 SLP 活动的集中点。打开 DA 日志记录比从网络中分散的多个 SA 中检查日志更容易监视注册和请求。根据平衡负载的需要，可以为特定的一个或多个范围部署任意数量的 DA。

在未启用多播路由的网络中，可以将 SLP 配置为使用广播。但广播的效率很低，因为它需要每台主机都处理消息。广播还无法在路由器间正常传播。因此，在没有多播路由支持的网络中，只能在同一子网中搜索服务。对多播路由的部分支持会导致在网络中搜索服务的能力不一致。多播消息用于搜索 DA。因此，对多播路由的不完全支持暗示了 UA 和 SA 向 SA 范围内的所有已知 DA 注册服务。例如，如果一个 UA 查询名为 `DA1` 的 DA，而 SA 已向 `DA2` 注册了服务，则 UA 将无法搜索服务。有关如何在未启用多播的网络中部署 SLP 的更多信息，请参见第 217 页中的 “配置仅限广播路由”。

在站点范围内对多播路由的支持不一致的网络中，必须使用 `net.slp.DAAdresseses` 属性以一致的 DA 位置列表配置 SLP UA 和 SA。

最后，SLPv2 DA 支持与 SLPv1 的互操作性。缺省情况下，DA 中会启用 SLPv1 互操作性。如果您的网络包含打印机等 SLPv1 设备或者需要与 Novell Netware 5（它将 SLPv1 用于服务搜索）进行互操作，则应部署 DA。如果没有 DA，Solaris SLP UA 将找不到 SLPv1 通告的服务。

何时部署 DA

如果以下任何条件成立，则请在您的企业中部署 DA：

- 按 snoop 的度量，多播 SLP 流量超过网络带宽的 1%。
- UA 客户端在多播服务请求期间经历较长时间的延迟或超时。
- 您要集中监视一个或多个主机上的特定范围内的 SLP 服务通告。
- 您的网络未启用多播，并且由必须共享服务的多个子网构成。
- 网络所使用的设备支持 SLP (SLPv1) 的早期版本，或者您希望 SLP 服务搜索与 Novell Netware 5 进行交互操作。

▼ 如何部署 DA

使用以下过程在 `slp.conf` 文件中将 `net.slp.isDA` 属性设置为 `True`。

注 – 只能为每个主机指定一个 DA。

---

1. **成为超级用户或承担等效角色。**

   角色包含授权和具有特权的命令。有关角色的更多信息，请参见《系统管理指南：安全性服务》中的“配置 RBAC（任务列表）”。

2. **停止 `slpd` 和主机上的所有 SLP 活动。**

   ```
   # svcadm disable network/slp
   ```

3. **在更改配置设置之前，先备份缺省的 `/etc/inet/slp.conf` 文件。**

4. **在 `slpd.conf` 文件中将 `net.slp.isDA` 属性设置为 `True`：**

   ```
   net.slp.isDA=True
   ```

5. **保存更改并关闭文件。**

6. **重新启动 `slpd` 以激活更改。**

   ```
   # svcadm enable network/slp
   ```

放置 DA 的位置

本节针对不同的情况对放置 DA 的位置提供了建议。

- 当未启用多播路由并且需要 DA 在子网之间桥接服务搜索时

在此情况下，必须在有多个接口并与共享服务的所有子网相连的主机上放置 DA。除非 IP 包不在这些接口间路由，否则**无**需设置 `net.slp.interfaces` 配置属性。有关配置 `net.slp.interfaces` 属性的更多信息，请参见第 227 页中的“用于 SLP 的多宿主配置”。

- 当为改善可伸缩性而部署 DA 并且主要考虑的是优化代理访问时

  UA 通常会向 DA 发出许多服务请求。一个 SA 向 DA 注册一次，并且以固定但不频繁的间隔刷新通告。因此，UA 对 DA 的访问要比 SA 访问频繁得多。而且，服务通告数通常小于请求数。因此，如果针对 UA 访问优化部署，则大多数 DA 部署的效率都会提高。

- 设置 DA 使其拓扑结构与网络中的 UA 接近，从而优化 UA 访问

  毫无疑问，必须用 UA 和 SA 客户机共享的范围来配置 DA。

为平衡负载而放置多个 DA

作为一种负载平衡的方法，可为同一范围集合部署多个 DA。可在下列任一情况下部署 DA：

- 到 DA 的 UA 请求超时，或返回 `DA_BUSY_NOW` 错误。
- DA 日志显示，正在删除许多 SLP 请求。
- 在范围内共享服务的用户网络跨越多个建筑或物理站点。

可以运行 SLP 流量的 `snoop` 跟踪，以确定多少 UA 请求返回 `DA_BUSY_NOW` 错误。如果返回的 UA 请求数很高，则在物理和拓扑结构上远离 DA 的建筑内的 UA 可能响应很慢，或者出现过多超时现象。在此情况下，可在每个建筑内都部署一个 DA，以改善对该建筑内的 UA 客户机的响应。

连接建筑的链接通常比建筑内的局域网慢。如果您的网络跨越多个建筑或物理站点，请在 `/etc/inet/slp.conf` 文件中将 `net.slp.DAAddresses` 属性设置为特定主机名或地址的列表，以使 UA 只访问您指定的 DA。

如果特定 DA 在服务注册中使用大量主机内存，则可通过减少 DA 支持的范围数来减少 SA 注册数。可将该范围分割为具有多个注册的两个范围。然后通过在另一主机上部署另一个 DA 来支持其中一个新范围。

SLP 和多宿主

多宿主服务器在多个 IP 子网中用作主机。该服务器有时可以有多个网络接口卡，并可用作路由器。包括多播包在内的 IP 包将在接口之间进行路由。在有些情况下，会禁用接口之间的路由。以下各节介绍如何为此类情况配置 SLP。

用于 SLP 的多宿主配置

无需进行任何配置，slpd 便可侦听缺省网络接口上的多播和 UDP/TCP 单播。如果在多宿主计算机的接口之间启用了单播和多播路由，则无需进行额外配置。这是因为到达另一接口的多播包正确路由至缺省接口。因此，对 DA 或其他服务通告的多播请求将到达 slpd。如果由于某种原因未打开路由，则需要进行配置。

何时配置非路由的多个网络接口

如果下面的任何一个条件存在，都可能需要配置多宿主计算机。

- 在接口之间启用了单播路由，而禁用了多播路由。
- 在接口之间同时禁用了单播路由和多播路由。

接口之间的多播路由被禁用时，通常是因为网络中尚未部署多播。在此情况下，广播通常用于不基于 DA 的服务搜索和个别子网上的 DA 搜索。通过将 net.slp.isBroadcastOnly 属性设置为 True 来配置广播。

配置非路由的多个网络接口（任务列表）

表 9–5 配置非路由的多个网络接口

任务	说明	参考
配置 net.slp.interfaces 属性	设置此属性，以使 slpd 侦听指定接口上的单播和多播/广播 SLP 请求。	第 227 页中的 “配置 net.slp.interfaces 属性”
安排代理服务通告，以使子网上的 UA 获得具有可访问地址的服务 URL	将代理通告限定到正在运行 slpd 且与单个子网而非多宿主主机连接的计算机。	第 229 页中的 “多宿主主机上的代理通告”
放置 DA 并配置范围，以确保 UA 和 SA 之间的可访问性	在具有一个接口主机名或地址的多宿主主机上配置 net.slp.interfaces 属性。 在多宿主主机上运行 DA 但配置范围，以使每个子网上的 SA 和 UA 使用不同的主机。	第 229 页中的 “DA 放置和范围名称指定”

配置 net.slp.interfaces 属性

如果设置了 net.slp.interfaces 属性，slpd 将侦听该属性所列接口而非缺省接口上的单播和多播/广播 SLP 请求。

通常，设置 net.slp.interfaces 属性时会同时通过设置 net.slp.isBroadcastOnly 属性来启用广播，原因是网络中尚未部署多播。但是，如果已经部署多播，而多播未在此

特定多宿主主机上路由，则多播请求可从多个接口到达 slpd。当包的路由由与子网（接口为这些子网提供服务）连接的另一台多宿主主机或路由器处理时，会出现这种情况。

出现此类情况时，发送请求的 SA 服务器或 UA 将收到来自多宿主主机上的 slpd 的两个响应。然后，客户机库对响应进行过滤，客户机将看不到这些响应。但这些响应在 snoop 跟踪中可见。

注 –

如果关闭单播路由，则所有子网都无法访问多宿主主机上的 SA 客户机通告的服务。如果这些服务无法访问，SA 客户机可以执行以下操作：

- 对每个子网通告一个服务 URL。
- 确保用可访问的 URL 应答来自特定子网的请求。

SA 客户机库不执行任何操作来确保对可访问的 URL 进行通告。服务计划（它可能处理也可能不处理无路由的多宿主主机）将负责确保对可访问的 URL 进行通告。

在禁用单播路由的多宿主主机上部署服务时，请使用 snoop 来确定服务是否可以正确处理来自多个子网的请求。此外，如果计划在多宿主主机上部署 DA，请参见第 229 页中的 “DA 放置和范围名称指定”。

▼ 如何配置 net.slp.interfaces 属性

使用以下过程在 slp.conf 文件中更改 net.slp.interfaces 属性。

1. **成为超级用户或承担等效角色。**

   角色包含授权和具有特权的命令。有关角色的更多信息，请参见《系统管理指南：安全性服务》中的“配置 RBAC（任务列表）”。

2. **停止 slpd 和主机上的所有 SLP 活动。**

   ```
   # svcadm disable network/slp
   ```

3. **在更改配置设置之前，先备份缺省的 /etc/inet/slp.conf 文件。**

4. **在 slpd.conf 文件中更改 net.slp.interfaces 属性：**

   net.slp.interfaces=*value*

   value 网络接口卡的 IPv4 地址或主机名的列表，DA 或 SA 应在该网络接口卡上侦听端口 427 上的多播、单播 UDP 和 TCP 消息

例如，具有三个网络接口卡和已关闭多播路由的服务器将连接至三个子网。这三个网络接口的 IP 地址为 192.147.142.42、192.147.143.42 和 192.147.144.42。子网掩码为 255.255.255.0。以下属性设置将使 slpd 侦听所有三个接口上的单播和多播/广播消息：

```
net.slp.interfaces=192.147.142.42,192.147.143.42,192.147.144.42
```

注 – 可以为 net.slp.interfaces 属性指定 IP 地址或可解析的主机名。

5 **保存更改并关闭文件。**

6 **重新启动 slpd 以激活更改。**

```
# svcadm enable network/slp
```

多宿主主机上的代理通告

如果具有多个接口的主机通过使用 slpd 和代理注册来通告服务，slpd 通告的服务 URL 必须包含可访问的主机名或地址。如果在接口之间启用单播路由，则所有子网上的主机都可以访问其他子网上的主机。还可以对任何子网上的服务进行代理注册。但是，如果已禁用单播路由，则一个子网上的服务客户机将无法通过多宿主主机来访问另一子网上的服务。但是，那些客户机也许可以通过另一个路由器来访问服务。

例如，假设缺省主机名为 bigguy 的主机在三个不同的非路由子网上有三个接口卡。这些子网上的主机名分别是 bigguy（IP 地址是 192.147.142.42）、bigguy1（IP 地址是 192.147.143.42）以及 bigguy2（IP 地址是 192.147.144.42）。现在，假设传统打印机 oldprinter 连接至 143 子网，并且用 net.slp.interfaces 将 URL service:printing:lpr://oldprinter/queue1 配置为侦听所有接口。oldprinter URL 在所有接口上都通告代理。142 和 144 子网中的计算机将接收 URL 以响应服务请求，但无法访问 oldprinter 服务。

对此问题的解决方案是用只与 143 子网连接的计算机（而非多宿主主机）上运行的 slpd 来执行代理通告。只有 143 子网上的主机可以获得通告，以作为对服务请求的响应。

DA 放置和范围名称指定

为了确保客户机获得可访问的服务，在具有多宿主主机的网络中放置 DA 和指定范围名称时必须格外谨慎。当禁用了路由且配置了 net.slp.interfaces 属性时，要特别小心。此外，如果在多宿主计算机的接口之间启用了单播路由，则不需要进行任何特殊的 DA 和范围配置。将以从任何子网中都可访问的 DA 标识服务对通告进行高速缓存。但是，如果禁用了单播路由，则不合适的 DA 放置将产生问题。

要确定上一个示例会导致什么问题，请考虑 bigguy 运行 DA 并且所有子网中的客户机都具有相同范围时可能出现的情况。143 子网中的 SA 将向 DA 注册其服务通告。即使 143 子网中的主机无法访问，144 子网上的 UA 也可以获得这些服务通告。

此问题的一个解决方案是在每个子网而非多宿主主机上运行 DA。在此情况下，多宿主主机上的 net.slp.interfaces 属性应配置一个接口主机名或地址，或者应将其保留为不配置，从而强制使用缺省接口。此解决方案的一个缺点是，多宿主主机通常是可以更好处理 DA 的计算负载的大型计算机。

另一个解决方案是在多宿主主机上运行 DA 但配置范围，以使每个子网上的 SA 和 UA 具有不同范围。例如，在前面的情况下，142 子网上的 UA 和 SA 可能具有一个名为 scope142 的范围。143 子网上的 UA 和 SA 可能具有名为 scope143 的另一个范围，而 144 子网上的 UA 和 SA 可能具有名为 scope144 的第三个范围。可在具有三个接口的 bigguy 中配置 net.slp.interfaces 属性，以使 DA 对这三个子网中的三个范围提供服务。

配置非路由的多个网络接口时的注意事项

配置 net.slp.interfaces 属性可使多宿主主机上的 DA 在子网之间桥接服务通告。如果网络中关闭了多播路由，但在多宿主主机的接口之间启用了单播路由，此类配置将很有用。由于单播在接口之间进行路由，因此服务所在子网之外的子网中的主机可在收到服务 URL 时联系服务。没有 DA 时，特定子网上的 SA 服务器只能接收同一子网上的广播，因此，它们无法找到其子网之外的服务。

使得必须配置 net.slp.interfaces 属性的最常见情形是网络中未部署多播而改用广播时。在其他情况下，需要慎重地考虑和规划，以避免不必要的重复响应或无法访问的服务。

◆ ◆ ◆ 第 10 章

10 引入传统服务

传统服务是早于 SLP 的开发和实现的网络服务。行式打印机守护进程 (`lpsched`)、NFS 文件服务和 NIS/NIS+ 名称服务等服务不包含用于 SLP 的内部 SA。本章介绍通告传统服务的时间和方式。

何时通告传统服务

通过传统服务通告，可使 SLP UA 在网络中查找如下所示的设备和服务。可以查找不包含 SLP SA 的硬件设备和软件服务。例如，具有 SLP UA 的应用程序需要查找不包含 SLP SA 的打印机或数据库时，可能需要使用传统通告。

通告传统服务

可以使用以下任一方法来通告传统服务。

- 修改服务以引入 SLP SA。
- 编写小型程序，以代表未启用 SLP 的服务进行通告。
- 使用代理通告让 `slpd` 通告服务。

修改服务

如果软件服务器的源代码可用，则可引入 SLP SA。用于 SLP 的 C 和 Java API 使用起来相对简单。有关 C API 的信息和有关 Java API 的文档，请参见手册页。如果服务是硬件设备，则制造商可能会有可引入 SLP 的更新 PROM。有关更多信息，请与设备制造商联系。

通告未启用 SLP 的服务

如果没有源代码或包含 SLP 的更新的 PROM，则可编写一个使用 SLP 客户机库通告服务的小型应用程序。此应用程序可用作小型守护进程，可在用来启动和停止服务的同一 Shell 脚本中启动或停止。

SLP 代理注册

Solaris `slpd` 支持用代理注册文件通告的传统服务。代理注册文件是采用可移植格式的服务通告的列表。

▼ 如何启用 SLP 代理注册

1. **在主机文件系统或可通过 HTTP 访问的任何网络目录中创建代理注册文件。**

2. **确定是否存在用于该服务的服务类型模板。**

   模板是对服务 URL 和服务类型的属性的说明。模板用于为特定服务类型定义通告的组成部分：

   - 如果存在服务类型模板，请使用该模板来构造代理注册。有关服务类型模板的更多信息，请参见 RFC 2609。
   - 如果没有该服务的服务类型模板，可选择可以准确描述该服务的属性集合。对通告使用命名授权而非缺省设置。缺省的命名授权只允许用于已标准化的服务类型。有关命名授权的更多信息，请参见 RFC 2609。

     例如，假设一个名为 *BizApp* 的公司有一个用于跟踪软件缺陷的本地数据库。为通告该数据库，该公司可能会使用服务类型为 `service:bugdb.bizapp` 的 URL。此后，命名授权将会是 `bizapp`。

3. **按照后续步骤，使用在前面步骤中创建的注册文件的位置，在 `/etc/inet/slp.conf` 文件中配置 `net.slp.serializedRegURL` 属性。**

4. **成为超级用户或承担等效角色。**

   角色包含授权和具有特权的命令。有关角色的更多信息，请参见《系统管理指南：安全性服务》中的“配置 RBAC（任务列表）”。

5. **停止 `slpd` 和主机上的所有 SLP 活动。**

   ```
   # svcadm disable network/slp
   ```

6. **在更改配置设置之前，先备份缺省的 `/etc/inet/slp.conf` 文件。**

7 **在 `/etc/inet/slp.conf` 文件的 `net.slp.serializedRegURL` 属性中指定代理注册文件的位置。**

`net.slp.net.slp.serializedRegURL=`*proxy registration file URL*

例如，如果串行化的注册文件是 `/net/inet/slp.reg`，则可按如下所示来配置属性：

```
net.slp.serializedRegURL=file:/etc/inet/slp.reg
```

8 **保存更改并关闭文件。**

9 **重新启动 `slpd` 以激活更改。**

```
# svcadm enable network/slp
```

使用 SLP 代理注册进行通告

服务通告由标识服务 URL、可选范围和一系列属性定义的行构成。SLP 守护进程将完全按照与 SA 客户机相同的方式来读取、注册和维护代理通告。下面是某个代理注册文件中的通告示例。

在此示例中，通告了支持 LPR 协议和 FTP 服务器的传统打印机。为了便于说明，添加了行号，但它们不是文件的构成部分。

```
(1) #Advertise legacy printer.
(2)
(3) service:lpr://bizserver/mainspool,en,65535
(4) scope=eng,corp
(5) make-model=Laserwriter II
(6) location-description=B16-2345
(7) color-supported=monochromatic
(8) fonts-supported=Courier,Times,Helvetica 9 10
(9)
(10) #Advertise FTP server
(11)
(12) ftp://archive/usr/src/public,en,65535,src-server
(13) content=Source code for projects
(14)
```

注 – 像配置文件一样，代理注册文件支持同样的非 ASCII 字符转义约定。有关代理注册文件格式的更多信息，请参见 RFC 2614。

表 10–1 SLP 代理注册文件说明

行号	说明
1 和 10	注释行以井号 (#) 开头，不影响文件操作。从注释行开头一直到结束的所有字符都将被忽略。

表 10–1 SLP 代理注册文件说明 （续）

行号	说明
2、9 和 14	分隔通告的空白行。
3、12	具有用逗号分隔的三个必需字段和一个可选字段的服务 URL： ■ 通告的通用 URL 或 `service:URL`。有关如何形成 service: URL 的说明，请参见 RFC 2609。 ■ 通告的语言。在前面的示例中，此字段指定为英语，即 *en*。语言是 RFC 1766 语言标记。 ■ 注册的生命周期，以秒为单位度量。生命周期限制为 16 位的无符号整数。如果生命周期小于最大值 65535，`slpd` 将使通告超时。如果生命周期为 65535，`slpd` 将定期刷新通告，并且在 `slpd` 退出之前，一直将生命周期视为永久。 ■ （可选的）服务类型字段－如果使用此字段，它将定义服务类型。如果定义了服务 URL，则可更改通告 URL 所用的服务类型。在前面的代理注册文件示例中，第 12 行包含一个通用 FTP URL。可选类型字段会使 URL 以服务类型名称 *src-server* 进行通告。缺省情况下，类型名称中不会添加 `service` 前缀。
4	范围指定。 可选行包括标记 `scope`，后跟等号以及用逗号分隔的范围名称列表。范围名称由 `net.slp.useScopes` 配置属性定义。此列表中只应包括为主机配置的范围。如果未添加范围行，则在配置了 `slpd` 的所有范围内进行注册。范围行必须紧随 URL 行之后。否则，系统会将范围名称识别为属性。
5–8	属性定义。 在可选的范围行之后，批量服务通告中包含属性/值列表对行。每个对都包含属性标记，其后是等号以及属性值或以逗号分隔的值列表。在前面的代理注册文件示例中，第 8 行显示了具有多个值的属性列表。所有其他列表都是单值。属性名称和值的格式与在线 SLP 消息的格式相同。

通告传统服务时的注意事项

通常，修改源代码来添加 SLP 的方法，优于编写启用 SLP 的服务（该服务使用 SLP API 代表其他服务进行通告）。修改源代码的方法也优于使用代理注册的方法。修改源代码时，可以添加特定于服务的功能并密切跟踪服务的可用性。如果源代码不可用，则编写代表其他服务进行通告的启用 SLP 的帮助器服务的方法，优于使用代理注册的方法。此帮助器服务最好集成到用于控制激活和取消激活服务启动/停止过程中。没有源代码可用并且编写单独的 SA 不可行时，代理通告通常是第三种选择。

仅当运行 `slpd` 以读取代理注册文件时，才能维护代理通告。代理通告与服务之间没有直接的联系。如果通告超时或 `slpd` 停止，代理通告将不再可用。

如果服务关闭，则必须停止 slpd。编辑序列化注册文件以注释掉或删除代理通告，然后重新启动 slpd。重新启动或重新安装服务时，必须遵循相同的过程。代理通告与服务之间缺少联系是代理通告的主要缺点。

◆ ◆ ◆ 第 11 章

11 SLP（参考）

本章介绍 SLP 状态代码和消息类型。SLP 消息类型与其缩写和功能代码一起列出。展示 SLP 状态代码的同时还展示了其说明和功能代码；功能代码用于表示已接收请求（代码 0）或接收器繁忙。

注 – SLP 守护进程 (`slpd`) 只为单点传送消息返回状态代码。

SLP 状态代码

表 11–1 SLP 状态代码

状态类型	状态代码	说明
无错误	0	已处理请求，未出现错误。
LANGUAGE_NOT_SUPPORTED	1	对于 AttrRqst 或 SrvRqst，在范围内有该服务类型的数据，但使用的不是指定的语言。
PARSE_ERROR	2	消息未遵循 SLP 语法。
INVALID_REGISTRATION	3	SrvReg 存在问题。例如，生命周期为零或省略了语言标记。
SCOPE_NOT_SUPPORTED	4	SLP 消息的范围列表中不包括应答请求的 SA 或 DA 所支持的范围。
AUTHENTICATION_UNKNOWN	5	DA 或 SA 接收到来自不受支持的 SLP SPI 的请求。
AUTHENTICATION_ABSENT	6	UA 或 DA 期望在 SrvReg 中出现 URL 和属性验证但未收到。
AUTHENTICATION_FAILED	7	UA 或 DA 在验证块中检测到验证错误。

表 11–1 SLP 状态代码 （续）

状态类型	状态代码	说明
VER_NOT_SUPPORTED	9	消息中的版本号不受支持。
INTERNAL_ERROR	10	DA 或 SA 中出现未知错误。例如，操作系统没有剩余的文件空间。
DA_BUSY_NOW	11	UA 或 SA 应使用指数补偿进行重试。DA 正忙于处理其他消息。
OPTION_NOT_UNDERSTOOD	12	DA 或 SA 收到来自强制范围的未知选项。
INVALID_UPDATE	13	对于未注册的服务或具有不一致服务类型的服务，DA 收到未设置 FRESH 的 SrvReg。
MSG_NOT_SUPPORTED	14	SA 收到 AttrRqst 或 SrvTypeRqst，但不支持它。
REFRESH_REJECTED	15	SA 以比 DA 的最短刷新间隔更频繁的频率向 DA 发送 SrvReg 或部分 SrvDereg。

SLP 消息类型

表 11–2 SLP 消息类型

消息类型	缩写	功能代码	说明
服务请求	`SrvRqst`	1	由 UA 发出，用于查找服务；或由 UA 或 SA 服务器在主动 DA 搜索期间发出。
服务应答	`SrvRply`	2	DA 或 SA 对服务请求的响应。
服务注册	`SrvReg`	3	允许 SA 注册新通知，利用新增和更改的属性更新现有通知，以及刷新 URL 生命周期。
服务注销	`SrvDereg`	4	通知表示的服务不再可用时，由 SA 用来注销其通知。
确认	`SrvAck`	5	DA 对 SA 的服务请求或服务注销消息的响应。
属性请求	`AttrRqst`	6	由 URL 或服务类型发出，用于请求属性列表。
属性应答	`AttrRply`	7	用于返回属性列表。
DA 通告	`DAAdvert`	8	DA 对多播服务请求的响应。
服务类型请求	`SrvTypeRqst`	9	用来查询具有特定的命名授权并且处于特定范围集合中的已注册服务类型。
服务类型应答	`SrvTypeRply`	10	为响应服务类型请求而返回的消息。
SA 通告	`SAAdvert`	11	UA 使用 `SAAdvert` 在未部署 DA 的网络中搜索 SA 及其范围。

第 4 部分

邮件服务主题

本节提供有关邮件服务的概述、任务和参考信息。

◆ ◆ ◆ 第 12 章

12 邮件服务（概述）

设置和维护电子邮件服务涉及对日常网络操作而言非常重要的复杂任务。作为网络管理员，您可能需要扩展现有的邮件服务。或者，您可能需要在新的网络或子网中设置邮件服务。有关邮件服务的各章节可帮助您规划和设置网络的邮件服务。本章提供了指向 sendmail 中新功能的说明的链接，及其他信息源的列表。本章还将概述建立邮件服务所需的软件和硬件组件。

有关如何设置和管理邮件服务的过程信息，请参见第 13 章，邮件服务（任务）。有关详细信息，请参阅第 249 页中的 “邮件服务任务列表”。

有关邮件服务组件的更详细说明，请参见第 14 章，邮件服务（参考）。本章还将介绍邮件服务程序和文件、邮件路由过程、sendmail 与名称服务的交互，以及 sendmail 8.13 版的功能。请参见第 325 页中的 “sendmail 版本 8.13 中的更改”。

邮件服务的新增功能

本节介绍有关各种 Solaris 发行版中新功能的信息。

此发行版中的更改

Oracle Solaris 10 Update 10 发行版中进行了如下更改：

- sendmail 的缺省版本更新为 8.14 版。
- sendmail 实例分割为两个实例，以更好地管理传统守护进程 (svc:/network/smtp:sendmail) 和客户机队列运行器 (svc:/network/smtp:sendmail-client)。

- 可以将系统配置为自动重新生成 sendmail.cf 和 submit.mc 配置文件。第 263 页中的“如何自动重新生成配置文件”中说明了所需的步骤。
- 缺省情况下，sendmail 守护进程以新的本地守护进程模式运行。仅本地模式只接受本地主机的传入邮件或回送 SMTP 连接。例如，将接受 cron 作业中的邮件或本地用户之间的邮件。按预期路由外发邮件，仅更改传入邮件。-bl 选项用于选择仅本地模式，也称为“成为本地”模式。有关此模式的更多信息，请参见 sendmail(1M) 手册页。有关如何更改回 -bd（成为守护进程）模式，请参见第 263 页中的“如何在打开模式下使用 sendmail”。

Solaris 10 1/06 发行版中的变化

从 Solaris 10 1/06 发行版开始，sendmail 支持使用传输层安全性 (Transport Layer Security, TLS) 的 SMTP。有关更多信息，请参见以下内容：

- 第 325 页中的“sendmail 版本 8.13 支持运行 SMTP 时使用 TLS”
- 第 264 页中的“设置 SMTP 以使用 TLS”

有关 Solaris 10 1/06 发行版中功能的完整列表，请参见《Oracle Solaris 10 8/11 新增功能》。

Solaris 10 发行版中的变化

sendmail 版本 8.13 是缺省设置。有关 8.13 版和其他变化的信息，请参见以下内容：

- 第 294 页中的“编译 sendmail 时使用和未使用的标志”
- 第 295 页中的“MILTER（用于 sendmail 的邮件过滤器 API）”
- 第 296 页中的“配置文件的版本”
- 第 305 页中的“vacation 实用程序的增强功能”
- 第 308 页中的“/etc/mail/cf 目录的内容”
- 第 325 页中的“sendmail 版本 8.13 中的更改”
- 第 333 页中的“sendmail 版本 8.12 支持 TCP 包装”

另外，邮件服务由服务管理工具管理。使用 svcadm 命令可以对此服务执行启用、禁用或重新启动等管理操作。可以使用 svcs 命令查询该服务的状态。有关服务管理工具的更多信息，请参见 smf(5) 手册页和《系统管理指南：基本管理》中的第 18 章“管理服务（概述）”。

其他 sendmail 信息源

以下是有关 sendmail 的其他信息源的列表。

- 由 Costales, Bryan 编著的 sendmail, Third Edition。 O'Reilly & Associates, Inc. 出版， 2002。
- sendmail 主页－http://www.sendmail.org。
- sendmail 常见问题解答－http://www.sendmail.org/faq。
- 新 sendmail 配置文件的自述文件－http://www.sendmail.org/m4/readme.html。
- 与迁移到最新版本的 sendmail 有关的问题指南－http://www.sendmail.org/vendor/sun/。

邮件服务组件介绍

建立邮件服务需要许多软件和硬件组件。以下各节对这些组件进行了简要介绍。这些节中还提供了用于说明这些组件的一些术语。

第一节第 245 页中的 “软件组件概述”定义了在讨论邮件传送系统的软件部分时使用的术语。下一节第 246 页中的 “硬件组件概述”集中介绍邮件配置中硬件系统的功能。

软件组件概述

下表介绍了邮件系统的一些软件组件。有关所有软件组件的完整说明，请参阅第 296 页中的 “软件组件”。

组件	说明
.forward 文件	可以在用户的起始目录中设置以重定向邮件，或将邮件自动发送到程序的文件
邮箱	邮件服务器（电子邮件的最终目标）上的文件
邮件地址	包含收件人姓名和邮件将传送到的系统的地址
邮件别名	邮件地址中使用的备选名称
邮件队列	需要邮件服务器处理的邮件的集合
postmaster	用于报告问题和询问有关邮件服务问题的特殊邮件别名
sendmail 配置文件	包含邮件路由需要的所有信息的文件

硬件组件概述

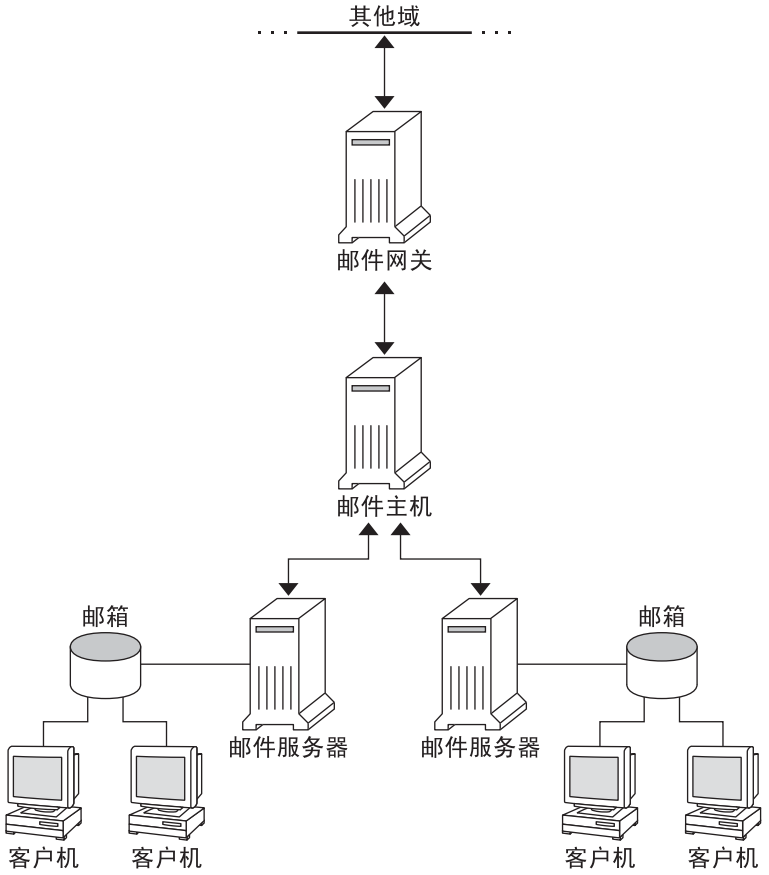
邮件配置需要以下三种元素，您可以在同一系统中合并这三者，也可以在不同的系统中提供。

- 邮件主机－被配置为用于处理难以解析的电子邮件地址的系统
- 最少一个邮件服务器－被配置为用于保存一个或多个邮箱的系统
- 邮件客户机－访问邮件服务器中邮件的系统

如果用户要与所在域之外的网络通信，则还必须添加第四种元素，邮件网关。

图 12–1 说明了一种典型的电子邮件配置，该配置使用三种基本邮件元素和一个邮件网关。

图 12–1 典型电子邮件配置



第 303 页中的 “硬件组件”中将详细介绍每一元素。

◆ ◆ ◆ 第 13 章

13 邮件服务（任务）

本章介绍如何设置和管理邮件服务。如果您对邮件服务管理不熟悉，请阅读第 12 章，邮件服务（概述），以了解有关邮件服务组件的介绍。本章还将介绍典型的邮件服务配置，如图 12–1 中所示。通过以下列表，可以帮助您查找本章中所介绍的多组相关过程。

- 第 249 页中的 “邮件服务任务列表”
- 第 253 页中的 “设置邮件服务（任务列表）”
- 第 260 页中的 “更改 sendmail 配置（任务列表）”
- 第 270 页中的 “管理邮件别名文件（任务列表）”
- 第 279 页中的 “管理队列目录（任务列表）”
- 第 282 页中的 “管理 `.forward` 文件（任务列表）”
- 第 285 页中的 “邮件服务故障排除过程和技巧（任务列表）”

有关邮件服务组件的更详细说明，请参见第 14 章，邮件服务（参考）。此外，本章还将介绍邮件服务程序和文件、邮件路由进程、`sendmail` 与名称服务的交互，以及 `sendmail(1M)` 手册页中未全面介绍的 `sendmail` 8.13 版功能。

邮件服务任务列表

下表将指向着重介绍某一组特定过程的其他任务列表。

任务	说明	参考
设置邮件服务	使用这些过程可设置邮件服务的各个组件。了解如何设置邮件服务器、邮件客户机、邮件主机和邮件网关。了解如何使用 DNS 和 `sendmail`。	第 253 页中的 “设置邮件服务（任务列表）”
更改 sendmail 配置	使用这些过程修改配置文件或服务属性。	第 260 页中的 “更改 sendmail 配置（任务列表）”

任务	说明	参考
管理邮件别名文件	使用这些过程通过网络提供别名。了解如何管理 NIS+ 表中的项。另外，了解如何设置 NIS 映射、本地邮件别名、加密的映射文件以及邮件管理员的别名。	第 270 页中的“管理邮件别名文件（任务列表）”
管理邮件队列	使用这些过程可顺利进行队列处理。了解如何显示和移动邮件队列、强制进行邮件队列处理以及运行邮件队列的子集。另外，了解如何运行旧邮件队列。	第 279 页中的“管理队列目录（任务列表）”
管理 `.forward` 文件	使用这些过程可禁用 `.forward` 文件或更改 `.forward` 文件的搜索路径。另外，还可了解如何通过创建和填充 `/etc/shells`，允许用户使用 `.forward` 文件。	第 282 页中的“管理 `.forward` 文件（任务列表）”
邮件服务故障排除过程和技巧	使用这些过程和技巧可解决邮件服务问题。了解如何测试邮件配置、检查邮件别名、测试 `sendmail` 规则集、验证与其他系统的连接以及记录消息。另外，了解在何处查找其他邮件诊断信息。	第 285 页中的“邮件服务故障排除过程和技巧（任务列表）”
解决错误消息	借助此部分中的信息可解决一些与邮件相关的错误消息。	第 289 页中的“解决错误消息”

规划邮件系统

以下列表说明了在规划过程中应考虑的一些问题。

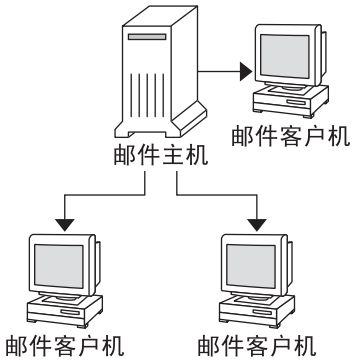
- 确定符合要求的邮件配置类型。本节介绍了两种基本类型的邮件配置，并简要列出了设置每种配置所需的信息。如果您需要设置一个新邮件系统或扩展现有系统，则可能会发现本节信息很有帮助。第 251 页中的“仅本地邮件”介绍了第一种配置类型，第 252 页中的“本地邮件和远程连接”介绍了第二种配置类型。
- 根据需要，选择将充当邮件服务器、邮件主机和邮件网关的系统。
- 列出要为其提供服务的所有邮件客户机，并包含它们的邮箱位置。当您准备为用户创建邮件别名时，此列表可以提供帮助。
- 确定如何更新别名和转发邮件。您可以设置一个 `aliases` 邮箱，作为用户发送邮件转发请求的位置。此外，用户还可以使用此邮箱来发送更改其缺省邮件别名的请求。如果您的系统使用的是 NIS 或 NIS+，则您可以管理邮件转发，而不需要用户来管理邮件转发。第 270 页中的“管理邮件别名文件（任务列表）”中列出了与别名相关的任务。第 282 页中的“管理 `.forward` 文件（任务列表）”中列出了与管理 `.forward` 文件相关的任务。

完成该规划过程后，请在站点中对系统进行设置，以执行第 253 页中的 “设置邮件服务（任务列表）”中描述的各种功能。有关其他任务信息，请参阅第 249 页中的 “邮件服务任务列表”。

仅本地邮件

如图 13–1 中所示，最简单的邮件配置是将两个或多个工作站连接到一台邮件主机。邮件完全是本地的。所有客户机均在其本地磁盘中存储邮件，并且由客户机充当邮件服务器。邮件地址使用 `/etc/mail/aliases` 文件进行解析。

图 13–1 本地邮件配置



要设置此类邮件配置，您需要满足以下条件：

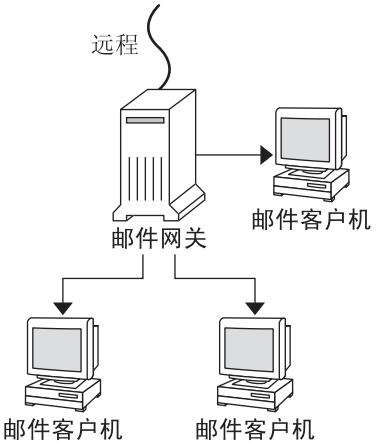
- 在每个邮件客户机系统上提供缺省的 `/etc/mail/sendmail.cf` 文件，该文件无需编辑。
- 指定一台服务器为邮件主机。如果运行的是 NIS 或 NIS+，则可通过为邮件主机中的 `/etc/hosts` 文件添加 `mailhost.`*domain_name* 来进行指定。如果运行的是其他名称服务（如 DNS 或 LDAP），则必须在 `/etc/hosts` 文件中提供其他信息。请参见第 257 页中的 “如何设置邮件主机”。
- 如果使用的是 NIS 或 NIS+ 以外的名称服务，则需要在具有本地邮箱的任何系统上拥有匹配的 `/etc/mail/aliases` 文件。
- 每个邮件客户机系统的 `/var/mail` 需要具有足够的空间来存储邮箱。

有关设置邮件服务的任务信息，请参阅第 253 页中的 “设置邮件服务”。如果要查找与邮件服务设置相关的特定过程，请参阅第 253 页中的 “设置邮件服务（任务列表）”。

本地邮件和远程连接

在小型网络中，最常见的邮件配置如图 13–2 所示。在此配置中，一个系统包含邮件服务器、邮件主机和提供远程连接的邮件网关。邮件通过使用邮件网关中的 `/etc/mail/aliases` 文件进行分发。无需使用名称服务。

图 13–2 采用 UUCP 连接的本地邮件配置



在此配置中，可以假定邮件客户机从邮件主机中的 `/var/mail` 挂载其邮件文件。要设置此类邮件配置，您需要满足以下条件：

- 在每个邮件客户机系统上提供缺省的 `/etc/mail/sendmail.cf` 文件。此文件无需进行任何编辑。
- 指定一台服务器为邮件主机。如果运行的是 NIS 或 NIS+，则可通过为邮件主机中的 `/etc/hosts` 文件添加 `mailhost.`*domain_name* 来进行指定。如果运行的是其他名称服务（如 DNS 或 LDAP），则必须在 `/etc/hosts` 文件中提供其他信息。请参见第 257 页中的“如何设置邮件主机”。
- 如果使用的是 NIS 或 NIS+ 以外的名称服务，则需要在具有本地邮箱的任何系统上拥有匹配的 `/etc/mail/aliases` 文件。
- 邮件服务器的 `/var/mail` 需要具有足够的空间来存储客户机邮箱。

有关设置邮件服务的任务信息，请参阅第 253 页中的“设置邮件服务”。如果要查找与邮件服务设置相关的特定过程，请参阅第 253 页中的“设置邮件服务（任务列表）”。

设置邮件服务（任务列表）

下表介绍了设置邮件服务的过程。

任务	说明	参考
设置邮件服务器	用于启用服务器以路由邮件的步骤	第 253 页中的“如何设置邮件服务器”
设置邮件客户机	用于使用户接收邮件的步骤	第 255 页中的“如何设置邮件客户机”
设置邮件主机	用于建立可解析电子邮件地址的邮件主机的步骤	第 257 页中的“如何设置邮件主机”
设置邮件网关	用于管理与域外部网络之间的通信的步骤	第 258 页中的“如何设置邮件网关”
使用 DNS 和 `sendmail`	用于启用 DNS 主机查找的步骤	第 260 页中的“如何使用 DNS 和 `sendmail`”

设置邮件服务

如果站点不提供与公司外部的电子邮件服务的连接，或者公司位于单个域中，则您可以轻松设置邮件服务。

对于本地邮件，邮件需要两种类型的配置。有关这些配置的说明，请参阅第 251 页中的“仅本地邮件”中的图 13–1。对于与域外部网络之间的通信，邮件需要两种以上的配置。有关这些配置的说明，请参阅第 246 页中的“硬件组件概述”中的图 12–1，或第 252 页中的“本地邮件和远程连接”中的图 13–2。可以在同一系统上合并这些配置，也可以在不同系统上提供这些配置。例如，如果邮件主机和邮件服务器功能位于同一系统上，请按照本节中的指示将该系统设置为邮件主机。然后，按照本节中的指示将同一系统设置为邮件服务器。

注 – 以下用于设置邮件服务器和邮件客户机的过程在邮箱挂载了 NFS 的情况下适用。但是，邮箱通常保存在本地挂载的 `/var/mail` 目录中，因此无需执行以下过程。

▼ 如何设置邮件服务器

设置仅为本地用户提供邮件服务的邮件服务器时，无需采取任何特殊步骤。在口令文件或名称空间中，必须包含用户项。另外，对于要传送的邮件，用户应具有用于检查 `~/.forward` 文件的本地起始目录。为此，通常会将起始目录服务器设置为邮件服务器。有关邮件服务器的更多信息，请参阅第 14 章，邮件服务（参考）中的第 303 页中的“硬件组件”。

该邮件服务器可以路由许多邮件客户机的邮件。此类型的邮件服务器必须为客户机邮箱提供足够的假脱机空间。

注 – 首次传送消息时，mail.local 程序会自动在 /var/mail 目录中创建邮箱。因此，无需为邮件客户机创建单独的邮箱。

对于访问其邮箱的客户机，/var/mail 目录应可用于远程挂载。或者，可使用该服务器提供的邮局协议 (Post Office Protocol, POP) 或 Internet 消息访问协议 (Internet Message Access Protocol, IMAP) 等服务。以下任务说明了如何通过 /var/mail 目录设置邮件服务器。提供 POP 或 IMAP 配置指南超出了本文档范围。

对于以下任务，请确保 /etc/dfs/dfstab 文件会显示已导出 /var/mail 目录。

1 **成为超级用户或承担等效角色。**

角色包含授权和具有特权的命令。有关角色的更多信息，请参见《系统管理指南：安全性服务》中的“配置 RBAC（任务列表）”。

2 **停止 sendmail。**

```
# svcadm disable -t network/smtp:sendmail
```

3 **检查 /var/mail 目录是否可用于远程访问。**

```
# share
```

如果列出了 /var/mail 目录，请转到步骤 5。

如果未列出 /var/mail 目录或没有显示列表，请继续执行相应的子步骤。

a. **可选如果未显示列表，请启动 NFS 服务。**

按照过程第 78 页中的 “如何设置自动文件系统共享”，使用 /var/mail 目录启动 NFS 服务。

b. **可选如果列表中未包含 /var/mail 目录，请将该目录添加到 /etc/dfs/dfstab。**

将以下命令行添加到 /etc/dfs/dfstab 文件中。

```
share -F nfs -o rw /var/mail
```

4 **使文件系统可进行挂载。**

```
# shareall
```

5 **确保已启动名称服务。**

a. **可选如果运行的是 NIS，请使用以下命令。**

```
# ypwhich
```

有关更多信息，请参阅 ypwhich(1) 手册页。

b. **可选如果运行的是 NIS+，请使用以下命令。**

```
# nisls
```

有关更多信息，请参阅 nisls(1) 手册页。

c. **可选如果运行的是 DNS，请使用以下命令。**

```
# nslookup hostname
```

hostname 使用您的主机名。

有关更多信息，请参阅 nslookup(1M) 手册页。

d. **可选如果运行的是 LDAP，请使用以下命令。**

```
# ldaplist
```

有关更多信息，请参阅 ldaplist(1) 手册页。

6 **重新启动 sendmail。**

```
# svcadm enable network/smtp:sendmail
```

▼ 如何设置邮件客户机

邮件客户机是一个在邮件服务器上具有邮箱的邮件服务用户。此外，邮件客户机在指向邮箱位置的 /etc/mail/aliases 文件中还具有邮件别名。

注 – 通过邮局协议 (Post Office Protocol, POP) 或 Internet 消息访问协议 (Internet Message Access Protocol, IMAP) 等服务，还可以执行邮件客户机设置任务。但是，提供 POP 或 IMAP 配置指南超出了本文档范围。

---

1 **成为邮件客户机系统的超级用户或承担等效角色。**

角色包含授权和具有特权的命令。有关角色的更多信息，请参见《系统管理指南：安全性服务》中的“配置 RBAC（任务列表）”。

2 **停止 sendmail。**

```
# svcadm disable -t network/smtp:sendmail
```

3 **确保邮件客户机系统上存在 /var/mail 挂载点。**

该挂载点应已在安装过程中创建。您可以使用 ls 来确保此文件系统存在。以下示例显示了在未创建此文件系统时收到的响应。

```
# ls -l /var/mail
/var/mail not found
```

4 **确保 /var/mail 目录中没有任何文件。**

如果此目录中存在邮件文件，则应移动这些文件，以便在通过服务器挂载 /var/mail 目录时不会覆盖它们。

5 **通过邮件服务器挂载 /var/mail 目录。**

您可以自动挂载或在引导时挂载该邮件目录。

a. **可选自动挂载 /var/mail。**

将如下所示的项添加到 /etc/auto_direct 文件中。

```
/var/mail -rw,hard,actimeo=0 server:/var/mail
```

server 使用指定的服务器名。

b. **可选在引导时挂载 /var/mail。**

将以下项添加到 /etc/vfstab 文件中。此项允许指定的邮件服务器中的 /var/mail 目录挂载本地 /var/mail 目录。

```
server:/var/mail - /var/mail nfs - no rw,hard,actimeo=0
```

重新引导系统时，会自动挂载客户机邮箱。如果不重新引导系统，请键入以下命令挂载客户机邮箱。

```
# mountall
```

注意 – 为正常使用邮箱锁定和邮箱访问，必须在从 NFS 服务器挂载邮件时包含 actimeo=0 选项。

6 **更新 /etc/hosts。**

编辑 /etc/hosts 文件，并为邮件服务器添加项。如果使用名称服务，则无需此步骤。

```
# cat /etc/hosts
#
# Internet host table
#
..
IP-address    mailhost   mailhost   mailhost.example.com
```

IP-address 使用指定的 IP 地址。

example.com 使用指定的域。

mailhost 使用指定的邮件主机。

有关更多信息，请参阅 hosts(4) 手册页。

7 **将客户机项添加到其中一个别名文件。**

有关管理邮件别名文件的任务列表，请参阅第 270 页中的 “管理邮件别名文件（任务列表）”。请注意，首次传送消息时，mail.local 程序会自动在 /var/mail 目录中创建邮箱。因此，无需为邮件客户机创建单独的邮箱。

8 **重新启动 sendmail。**

```
# svcadm enable network/smtp:sendmail
```

▼ 如何设置邮件主机

邮件主机用于解析电子邮件地址并在域内重新路由邮件。合适的邮件主机候选系统是可为网络提供远程连接或将网络连接到父域的系统。以下过程说明了如何设置邮件主机。

1 成为邮件主机系统的超级用户或承担等效角色。

角色包含授权和具有特权的命令。有关角色的更多信息，请参见《系统管理指南：安全性服务》中的"配置 RBAC（任务列表）"。

2 停止 sendmail。

```
# svcadm disable -t network/smtp:sendmail
```

3 验证主机名配置。

运行 check-hostname 脚本，验证 sendmail 是否可以识别此服务器的全限定主机名。

```
% /usr/sbin/check-hostname
hostname phoenix OK: fully qualified as phoenix.example.com
```

如果此脚本无法成功识别全限定主机名，则需要将该全限定主机名作为主机的第一个别名添加到 /etc/hosts 中。

4 更新 /etc/hosts 文件。

选择适合您的步骤。

a. 可选如果使用的是 NIS 或 NIS+，请在要作为新邮件主机的系统上编辑 /etc/hosts。

在 IP 地址和邮件主机系统的系统名之后，添加单词 mailhost 和 mailhost.*domain*。

IP-address mailhost mailhost mailhost.*domain* loghost

IP-address 使用指定的 IP 地址。

mailhost 使用邮件主机系统的系统名。

domain 使用扩展的域名。

现在，系统即被指定为邮件主机。*domain* 应与以下命令输出中指定为子域名的字符串相同。

```
% /usr/lib/sendmail -bt -d0 </dev/null
Version 8.13.1+Sun
 Compiled with: LDAPMAP MAP_REGEX LOG MATCHGECOS MIME7TO8 MIME8TO7
                NAMED_BIND NDBM NETINET NETINET6 NETUNIX NEWDB NIS
                NISPLUS QUEUE SCANF SMTP USERDB XDEBUG

============ SYSTEM IDENTITY (after readcf) ============
      (short domain name) $w = phoenix
  (canonical domain name) $j = phoenix.example.com
         (subdomain name) $m = example.com
              (node name) $k = phoenix
```

```
=====================================================
```

有关 hosts 文件应如何检查这些更改，请参见以下示例。

```
# cat /etc/hosts
#
# Internet host table
#
172.31.255.255   localhost
192.168.255.255  phoenix mailhost mailhost.example.com loghost
```

b. 可选如果未使用 NIS 或 NIS+，请在网络中的所有系统上编辑 /etc/hosts 文件。

创建以下项。

IP-address mailhost mailhost *mailhost.domain* loghost

5 重新启动 sendmail。

```
# svcadm enable network/smtp:sendmail
```

6 测试邮件配置。

有关说明，请参见第 286 页中的 “如何测试邮件配置”。

注 – 有关邮件主机的详细信息，请参见第 14 章，邮件服务（参考）中的第 303 页中的 “硬件组件”。

▼ 如何设置邮件网关

邮件网关用于管理与域外部网络之间的通信。发送邮件网关中的邮件程序可以与接收系统中的邮件程序匹配。

适合作为邮件网关的系统是指连接到以太网和电话线的系统。此外，还可以是配置为 Internet 路由器的系统。可以将邮件主机或其他系统配置为邮件网关。您可能会选择为域配置多个邮件网关。如果使用 UNIX 对 UNIX 复制程序 (UNIX-to-UNIX Copy Program, UUCP) 连接，则应将采用 UUCP 连接的系统配置为邮件网关。

1 成为邮件网关的超级用户或承担等效角色。

角色包含授权和具有特权的命令。有关角色的更多信息，请参见《系统管理指南：安全性服务》中的“配置 RBAC（任务列表）”。

2 停止 sendmail。

```
# svcadm disable -t network/smtp:sendmail
```

3 **验证主机名配置。**

运行 `check-hostname` 脚本，验证 `sendmail` 是否可以识别此服务器的全限定主机名。

```
# /usr/sbin/check-hostname
hostname phoenix OK: fully qualified as phoenix.example.com
```

如果此脚本无法成功识别全限定主机名，则需要将该全限定主机名作为主机的第一个别名添加到 `/etc/hosts` 中。如果需要有关此步骤的帮助，请参阅第 257 页中的 “如何设置邮件主机”中的步骤 4。

4 **确保已启动名称服务。**

a. **可选如果运行的是 NIS，请使用以下命令。**

```
# ypwhich
```

有关更多信息，请参阅 `ypwhich(1)` 手册页。

b. **可选如果运行的是 NIS+，请使用以下命令。**

```
# nisls
```

有关更多信息，请参阅 `nisls(1)` 手册页。

c. **可选如果运行的是 DNS，请使用以下命令。**

```
# nslookup hostname
```

hostname 使用您的主机名。

有关更多信息，请参阅 `nslookup(1M)` 手册页。

d. **可选如果运行的是 LDAP，请使用以下命令。**

```
# ldaplist
```

有关更多信息，请参阅 `ldaplist(1)` 手册页。

5 **重新启动 `sendmail`。**

```
# svcadm enable network/smtp:sendmail
```

6 **测试邮件配置。**

有关说明，请参见第 286 页中的 “如何测试邮件配置”。

注 – 有关邮件网关的更多信息，请参阅第 14 章，邮件服务（参考）中的第 303 页中的 “硬件组件”。

▼ 如何使用 DNS 和 sendmail

DNS 名称服务不支持单个别名。此名称服务支持使用邮件交换器 (Mail Exchanger, MX) 记录和 CNAME 记录的主机或域的别名。您可以在 DNS 数据库中指定主机名、域名或同时指定这两个名称。有关 sendmail 和 DNS 的更多信息，请参见第 14 章，邮件服务（参考）中的第 321 页中的 “sendmail 与名称服务的交互”或参见《系统管理指南：名称和目录服务（DNS、NIS 和 LDAP）》。

1. **成为超级用户或承担等效角色。**

   角色包含授权和具有特权的命令。有关角色的更多信息，请参见《系统管理指南：安全性服务》中的“配置 RBAC（任务列表）”。

2. **启用 DNS 主机查找（仅限 NIS+）。**

   编辑 /etc/nsswitch.conf 文件，并从包含 dns 标志的 hosts 定义中删除 #。如下例所示，主机项必须包含 dns 标志，以便使用 DNS 主机别名。

   ```
   # grep hosts /etc/nsswitch.conf
   #hosts:     nisplus [NOTFOUND=return] files
   hosts:      dns nisplus [NOTFOUND=return] files
   ```

3. **检查 mailhost 和 mailhost.*domain* 项。**

   使用 nslookup 确保 DNS 数据库中存在 mailhost 和 mailhost.*domain* 项。有关更多信息，请参阅 nslookup(1M) 手册页。

更改 sendmail 配置（任务列表）

任务	说明	参考
生成 sendmail 配置文件	使用此过程修改 sendmail.cf 文件。包括如何启用域伪装的示例。	第 261 页中的 “如何生成新的 sendmail.cf 文件”
设置虚拟主机	用于配置 sendmail 以便接收多个域的邮件的步骤。	第 262 页中的 “设置虚拟主机”
设置 sendmail 配置文件的自动重新生成	使用此过程修改 sendmail 服务，以便在升级后自动重新生成 sendmail.cf 和 submit.mc 配置文件。	第 263 页中的 “如何自动重新生成配置文件”
以打开模式运行 sendmail。	使用此过程修改 sendmail 服务属性以启用打开模式。	第 263 页中的 “如何在打开模式下使用 sendmail”
设置 SMTP 以使用传输层安全性 (Transport Layer Security, TLS)	使用此过程启用 SMTP 以与 TLS 建立安全连接。	第 264 页中的 “设置 SMTP 以使用 TLS”

任务	说明	参考
使用备用配置管理邮件传送	使用此过程以防止在主守护进程禁用时可能会发生的邮件传送问题。	第 269 页中的“如何使用 sendmail.cf 的备用配置管理邮件传送”

更改 sendmail 配置

第 261 页中的“如何生成新的 sendmail.cf 文件”说明了如何生成该配置文件。尽管您仍可使用旧版本的 sendmail.cf 文件，但最佳做法是使用新格式。

有关更多详细信息，请参阅以下内容。

- /etc/mail/cf/README 完整说明了配置过程。
- http://www.sendmail.org 概述了有关 sendmail 配置的信息。
- 第 14 章，邮件服务（参考）中的第 296 页中的“配置文件的版本”和第 314 页中的“sendmail 配置文件”提供了一些指南。
- 第 338 页中的“sendmail 版本 8.12 中新增和修订的 m4 配置宏”也很有帮助。

▼ 如何生成新的 sendmail.cf 文件

以下过程说明了如何生成新的配置文件。

注 – /usr/lib/mail/cf/main-v7sun.mc 现在是 /etc/mail/cf/cf/main.mc。

---

1 **成为超级用户或承担等效角色。**

角色包含授权和具有特权的命令。有关角色的更多信息，请参见《系统管理指南：安全性服务》中的“配置 RBAC（任务列表）”。

2 **停止 sendmail。**

```
# svcadm disable -t network/smtp:sendmail
```

3 **复制要更改的配置文件。**

```
# cd /etc/mail/cf/cf
# cp sendmail.mc myhost.mc
```

myhost 选择 .mc 文件的新名称。

4 **根据需要，编辑新配置文件（如 *myhost*.mc）。**

例如，添加以下命令行以启用域伪装。

```
# cat myhost.mc
..
MASQUERADE_AS(‘host.domain’)
```

host.domain 使用所需的主机名和域名。

在此示例中，MASQUERADE_AS 将已发送邮件标记为来自 *host.domain*，而不是 $j。

5 **使用 m4 生成配置文件。**

```
# /usr/ccs/bin/make myhost.cf
```

6 **使用 --C 选项指定新文件，以测试新配置文件。**

```
# /usr/lib/sendmail -C myhost.cf -v testaddr </dev/null
```

当此命令显示消息时，将会向 testaddr 发送一条消息。如果不重新启动系统中的 sendmail 服务，则只能对外发邮件进行测试。对于尚未处理邮件的系统，请使用第 286 页中的“如何测试邮件配置”所介绍的完整测试过程。

7 **复制原始配置文件后，安装新配置文件。**

```
# cp /etc/mail/sendmail.cf /etc/mail/sendmail.cf.save
# cp myhost.cf /etc/mail/sendmail.cf
```

8 **重新启动 sendmail 服务。**

```
# svcadm enable network/smtp:sendmail
```

设置虚拟主机

如果需要为主机指定多个 IP 地址，请参见以下 Web 站点：http://www.sendmail.org/tips/virtualHosting。此站点完整介绍了如何使用 sendmail 设置虚拟主机。但是，在“Sendmail 配置”部分中，不会执行步骤 3b，如以下所示。

```
# cd sendmail-VERSION/cf/cf
# ./Build mailserver.cf
# cp mailserver.cf /etc/mail/sendmail.cf
```

相反，对于 Solaris 操作系统，会执行以下步骤。

```
# cd /etc/mail/cf/cf
# /usr/ccs/bin/make mailserver.cf
# cp mailserver.cf /etc/mail/sendmail.cf
```

mailserver　使用 .cf 文件的名称。

第 261 页中的“更改 sendmail 配置”中将这相同的三个步骤作为生成过程的一部分进行了概述。

生成 /etc/mail/sendmail.cf 文件后，可以继续执行以下步骤创建虚拟用户表。

▼ 如何自动重新生成配置文件

如果已生成自己的 sendmail.cf 或 submit.cf 副本，则升级过程中不替换该配置文件。以下过程显示如何配置 sendmail 服务属性以便为您自动重新生成 sendmail.cf 文件。有关如何自动生成 submit.cf 配置文件的说明，请参见示例 13–1。如果需要生成这两个文件，则可以结合执行这两个过程。

1. **成为超级用户或承担等效角色。**

   角色包含授权和具有特权的命令。有关角色的更多信息，请参见《系统管理指南：安全性服务》中的“配置 RBAC（任务列表）”。

2. **设置 sendmail 属性。**

```
# svccfg -s sendmail
svc:/network/smtp:sendmail> setprop config/path_to_sendmail_mc=/etc/mail/cf/cf/myhost.mc
svc:/network/smtp:sendmail> quit
```

3. **刷新和重新启动 sendmail 服务。**

   第一个命令会将更改推送到正在运行的快照。第二个命令使用新选项重新启动 sendmail 服务。

```
# svcadm refresh svc:/network/smtp:sendmail
# svcadm restart svc:/network/smtp:sendmail
```

示例 13–1 建立 submit.cf 的自动重新生成

此过程配置 sendmail 服务，以便自动重新生成 submit.mc 配置文件。

```
# svccfg -s sendmail-client:default
svc:/network/smtp:sendmail> setprop config/path_to_submit_mc=/etc/mail/cf/cf/submit-myhost.mc
svc:/network/smtp:sendmail> exit
# svcadm refresh svc:/network/sendmail-client
# svcadm restart svc:/network/sendmail-client
```

▼ 如何在打开模式下使用 sendmail

在 Solaris 10 发行版中，更改了 sendmail 服务，以便该服务缺省情况下在仅本地模式下运行。仅本地模式意味着仅接受本地主机的邮件。将拒绝来自任何其他系统的邮件。早期的发行版配置为接受所有远程系统的传入邮件，这称为打开模式。要使用打开模式，请执行以下过程。

注意 – 在仅本地模式下运行 sendmail 比在打开模式下运行更安全。如果遵循以下过程，请确保您能够识别出潜在安全风险。

1. **成为超级用户或承担等效角色。**

   角色包含授权和具有特权的命令。有关角色的更多信息，请参见《系统管理指南：安全性服务》中的“配置 RBAC（任务列表）”。

2. **设置 sendmail 属性。**

```
# svccfg -s sendmail
svc:/network/smtp:sendmail> setprop config/local_only = false
svc:/network/smtp:sendmail> quit
```

3. **刷新和重新启动 sendmail 服务。**

```
# svcadm refresh svc:/network/smtp:sendmail
# svcadm restart svc:/network/smtp:sendmail
```

▼ 设置 SMTP 以使用 TLS

从 Solaris 10 1/06 发行版开始，SMTP 可在 sendmail 8.13 版中使用传输层安全性 (Transport Layer Security, TLS)。此服务面向 SMTP 服务器和客户机，通过 Internet 提供专用的、认证的通信，并且可保护系统免受窃听者和攻击者的侵害。请注意，缺省情况下不会启用此服务。

以下过程使用样例数据说明如何设置证书，以便 sendmail 使用 TLS。有关更多信息，请参见第 325 页中的 “sendmail 版本 8.13 支持运行 SMTP 时使用 TLS”。

1. **成为超级用户或承担等效角色。**

   角色包含授权和具有特权的命令。有关角色的更多信息，请参见《系统管理指南：安全性服务》中的“配置 RBAC（任务列表）”。

2. **停止 sendmail。**

```
# svcadm disable -t network/smtp:sendmail
```

3. **设置相应证书，以便 sendmail 使用 TLS。**

   a. **完成以下命令：**

```
# cd /etc/mail
# mkdir -p certs/CA
# cd certs/CA
# mkdir certs crl newcerts private
# echo "01" > serial
# cp /dev/null index.txt
# cp /etc/sfw/openssl/openssl.cnf .
```

   b. **使用您选择的文本编辑器，将 openssl.cnf 文件中的 dir 值从 /etc/sfw/openssl 更改为 /etc/mail/certs/CA。**

c. 使用 openssl 命令行工具实现 TLS。

请注意，以下命令行会生成交互式文本。

```
# openssl req -new -x509 -keyout private/cakey.pem -out cacert.pem -days 365 \
-config openssl.cnf
Generating a 1024 bit RSA private key
.....................................++++++
.....................................++++++
writing new private key to 'private/cakey.pem'
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) []:US
State or Province Name (full name) []:California
Locality Name (eg, city) []:Menlo Park
Organization Name (eg, company) [Unconfigured OpenSSL Installation]:Sun Microsystems
Organizational Unit Name (eg, section) []:Solaris
Common Name (eg, YOUR name) []:somehost.somedomain.example.com
Email Address []:someuser@example.com
```

req	此命令用于创建和处理证书请求。
-new	此 req 选项用于生成一个新的证书请求。
-x509	此 req 选项用于创建一个自签名证书。
-keyout private/cakey.pem	此 req 选项允许将 private/cakey.pem 指定为新建的私钥的文件名。
-out cacert.pem	此 req 选项允许将 cacert.pem 指定为输出文件。
-days 365	此 req 选项允许确保证书有效期为 365 天。缺省值为 30。
-config openssl.cnf	此 req 选项允许将 openssl.cnf 指定为配置文件。

请注意，此命令要求您提供以下信息：

- Country Name，如 US。
- State or Province Name，如 California。
- Locality Name，如 Menlo Park。
- Organization Name，如 Oracle Corporation。
- Organizational Unit Name，如 Solaris。
- Common Name，该名称是计算机的全限定主机名。有关更多信息，请参见 check-hostname(1M) 手册页。

- Email Address，如 someuser@example.com。

4 可选如果需要新的安全连接，请创建新证书并使用证书颁发机构签名。

a. 创建新证书。

```
# cd /etc/mail/certs/CA
# openssl req -nodes -new -x509 -keyout newreq.pem -out newreq.pem -days 365 \
-config openssl.cnf
Generating a 1024 bit RSA private key
..............++++++
..............++++++
writing new private key to 'newreq.pem'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) []:US
State or Province Name (full name) []:California
Locality Name (eg, city) []:Menlo Park
Organization Name (eg, company) [Unconfigured OpenSSL Installation]:Sun Microsystems
Organizational Unit Name (eg, section) []:Solaris
Common Name (eg, YOUR name) []:somehost.somedomain.example.com
Email Address []:someuser@example.com
```

此命令要求您提供的信息与步骤 3c 中提供的信息相同。

请注意，在此示例中，证书和私钥位于文件 newreq.pem 中。

b. 使用证书颁发机构对新证书进行签名。

```
# cd /etc/mail/certs/CA
# openssl x509 -x509toreq -in newreq.pem -signkey newreq.pem -out tmp.pem
Getting request Private Key
Generating certificate request
# openssl ca -config openssl.cnf -policy policy_anything -out newcert.pem -infiles tmp.pem
Using configuration from openssl.cnf
Enter pass phrase for /etc/mail/certs/CA/private/cakey.pem:
Check that the request matches the signature
Signature ok
Certificate Details:
        Serial Number: 1 (0x1)
        Validity
            Not Before: Jun 23 18:44:38 2005 GMT
            Not After : Jun 23 18:44:38 2006 GMT
        Subject:
            countryName               = US
            stateOrProvinceName       = California
            localityName              = Menlo Park
            organizationName          = Sun Microsystems
            organizationalUnitName    = Solaris
            commonName                = somehost.somedomain.example.com
            emailAddress              = someuser@example.com
```

```
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            Netscape Comment:
                OpenSSL Generated Certificate
            X509v3 Subject Key Identifier:
                93:D4:1F:C3:36:50:C5:97:D7:5E:01:E4:E3:4B:5D:0B:1F:96:9C:E2
            X509v3 Authority Key Identifier:
                keyid:99:47:F7:17:CF:52:2A:74:A2:C0:13:38:20:6B:F1:B3:89:84:CC:68
                DirName:/C=US/ST=California/L=Menlo Park/O=Sun Microsystems/OU=Solaris/\
                CN=someuser@example.com/emailAddress=someuser@example.com
                serial:00

Certificate is to be certified until Jun 23 18:44:38 2006 GMT (365 days)
Sign the certificate? [y/n]:y


1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
# rm -f tmp.pem
```

在此示例中，文件 newreq.pem 包含未签名证书和私钥。文件 newcert.pem 包含已签名证书。

x509 实用程序	显示证书信息、将证书转换为各种格式以及对证书请求进行签名
ca 应用程序	用于对各种格式的证书请求进行签名以及生成 CRL（certificate revocation list，证书撤销列表）

5 在 .mc 文件中添加以下行，以便 sendmail 使用证书。

```
define('confCACERT_PATH', '/etc/mail/certs')dnl
define('confCACERT', '/etc/mail/certs/CAcert.pem')dnl
define('confSERVER_CERT', '/etc/mail/certs/MYcert.pem')dnl
define('confSERVER_KEY', '/etc/mail/certs/MYkey.pem')dnl
define('confCLIENT_CERT', '/etc/mail/certs/MYcert.pem')dnl
define('confCLIENT_KEY', '/etc/mail/certs/MYkey.pem')dnl
```

有关更多信息，请参见第 326 页中的 "用于在运行 SMTP 时使用 TLS 的配置文件选项"。

6 在 /etc/mail 目录中重新生成并安装 sendmail.cf 文件。

有关详细说明，请参见第 261 页中的 "更改 sendmail 配置"。

7 创建从使用 openssl 创建的文件到 .mc 文件中定义的文件的符号链接。

```
# cd /etc/mail/certs
# ln -s CA/cacert.pem CAcert.pem
# ln -s CA/newcert.pem MYcert.pem
# ln -s CA/newreq.pem MYkey.pem
```

8 为提高安全性，拒绝对 MYkey.pem 的组和其他项目的读取权限。

```
# chmod go-r MYkey.pem
```

9 **使用符号链接将 CA 证书安装在指定给 confCACERT_PATH 的目录中。**

```
# C=CAcert.pem
# ln -s $C ‘openssl x509 -noout -hash < $C‘.0
```

10 **为确保其他主机的邮件安全，安装相应的主机证书。**

a. **将通过其他主机的 confCACERT 选项定义的文件复制到 /etc/mail/certs/*host.domain*.cert.pem。**

将 *host.domain* 替换为其他主机的全限定主机名。

b. **使用符号链接将 CA 证书安装在指定给 confCACERT_PATH 的目录中。**

```
# C=host.domain.cert.pem
# ln -s $C ‘openssl x509 -noout -hash < $C‘.0
```

将 *host.domain* 替换为其他主机的全限定主机名。

11 **重新启动 sendmail。**

```
# svcadm enable network/smtp:sendmail
```

示例 13–2 Received: 邮件头

以下是使用 TLS 的安全邮件的 Received: 头示例。

```
Received: from his.example.com ([IPv6:2001:db8:3c4d:15::1a2f:1a2b])
        by her.example.com (8.13.4+Sun/8.13.4) with ESMTP id j2TNUB8i242496
        (version=TLSv1/SSLv3 cipher=DHE-RSA-AES256-SHA bits=256 verify=OK)
        for <janepc@her.example.com>; Tue, 29 Mar 2005 15:30:11 -0800 (PST)
Received: from her.example.com (her.city.example.com [192.168.0.0])
        by his.example.com (8.13.4+Sun/8.13.4) with ESMTP id j2TNU7cl571102
        version=TLSv1/SSLv3 cipher=DHE-RSA-AES256-SHA bits=256 verify=OK)
        for <janepc@her.example.com>; Tue, 29 Mar 2005 15:30:07 -0800 (PST)
```

请注意，verify 的值为 OK，这表明验证成功。有关更多信息，请参见第 328 页中的 “用于在运行 SMTP 时使用 TLS 的宏”。

另请参见 以下 OpenSSL 手册页：

- openssl(1) (http://www.openssl.org/docs/apps/openssl.html)。
- req(1) (http://www.openssl.org/docs/apps/req.html)。
- x509(1) (http://www.openssl.org/docs/apps/x509.html)。
- ca(1) (http://www.openssl.org/docs/apps/ca.html)。

▼ 如何使用 sendmail.cf 的备用配置管理邮件传送

为便于传入邮件和外发邮件的传输，sendmail 的新缺省配置使用了守护进程和客户机队列运行器。客户机队列运行器必须能够将邮件提交至本地 SMTP 端口上的守护进程。如果该守护进程没有侦听 SMTP 端口，邮件将保留在队列中。要避免此问题，请执行以下任务。有关守护进程和客户机队列运行器的更多信息，以及要了解可能必须使用此备用配置的原因，请参阅第 333 页中的 “sendmail 版本 8.12 中的配置文件 submit.cf”。

此过程可确保守护进程的运行仅用于接受来自本地主机的连接。

1. **成为超级用户或承担等效角色。**

   角色包含授权和具有特权的命令。有关角色的更多信息，请参见《系统管理指南：安全性服务》中的“配置 RBAC（任务列表）”。

2. **停止 sendmail 客户机服务。**

   ```
   # svcadm disable -t sendmail-client
   ```

3. **复制要更改的配置文件。**

   ```
   # cd /etc/mail/cf/cf
   # cp submit.mc submit-myhost.mc
   ```

   myhost　选择 .mc 文件的新名称。

4. **编辑新配置文件（例如，submit- *myhost*.mc）。**

   将侦听主机 IP 地址更改为 msp 定义。

   ```
   # grep msp submit-myhost.mc
   FEATURE('msp', '[#.#.#.#]')dnl
   ```

5. **使用 m4 生成配置文件。**

   ```
   # /usr/ccs/bin/make submit-myhost.cf
   ```

6. **复制原始配置文件后，安装新配置文件。**

   ```
   # cp /etc/mail/submit.cf /etc/mail/submit.cf.save
   # cp submit-myhost.cf /etc/mail/submit.cf
   ```

7. **重新启动 sendmail 客户机服务。**

   ```
   # svcadm enable sendmail-client
   ```

管理邮件别名文件（任务列表）

下表介绍了管理邮件别名文件的过程。有关本主题的更多信息，请参阅第 14 章，邮件服务（参考）中的第 315 页中的 “邮件别名文件”。

任务	说明	参考
管理 NIS+ `mail_aliases` 表中的别名项	如果名称服务是 NIS+，请使用这些过程管理 `mail_aliases` 表中的内容。 启动 NIS+ `mail_aliases` 表。	第 271 页中的 “如何启动 NIS+ `mail_aliases` 表”
	列出 NIS+ `mail_aliases` 表中的内容。 此过程包含有关如何列出单项以及如何列出部分匹配项的示例。	第 271 页中的 “如何列出 NIS+ `mail_aliases` 表中的内容”
	通过命令行向 NIS+ `mail_aliases` 表添加别名。	第 272 页中的 “如何通过命令行向 NIS+ `mail_aliases` 表添加别名”
	通过编辑 NIS+ `mail_aliases` 表添加项。	第 273 页中的 “如何通过编辑 NIS+ `mail_aliases` 表添加项”
	编辑 NIS+ `mail_aliases` 表中的项。 此过程包含有关如何删除项的示例。	第 274 页中的 “如何编辑 NIS+ `mail_aliases` 表中的项”
设置 NIS `mail.aliases` 映射	如果名称服务是 NIS，请按照以下说明简化 `mail.aliases` 映射的别名设置。	第 274 页中的 “如何设置 NIS `mail.aliases` 映射”
设置本地邮件别名文件	如果未使用名称服务（如 NIS 或 NIS+），请按照以下说明简化 `/etc/mail/aliases` 文件的别名设置。	第 275 页中的 “如何设置本地邮件别名文件”
创建加密映射文件	使用以下步骤可简化加密映射文件的别名设置。	第 277 页中的 “如何创建加密映射文件”
设置 `postmaster` 别名	使用本节中的过程可管理 `postmaster` 别名。您必须使用此别名。	第 277 页中的 “管理 `postmaster` 别名”

管理邮件别名文件

邮件别名在域中必须唯一。本节介绍管理邮件别名文件的过程。或者，您可以使用 Solaris Management Console 的邮递列表功能，在别名数据库上执行这些任务。

另外，您还可以使用 `makemap` 为本地邮件主机创建数据库文件。请参阅 `makemap(1M)` 手册页。使用这些数据库文件不会提供使用 NIS 或 NIS+ 等名称服务的所有优点。但是，由于不涉及网络查找，因此可以更快地从这些本地数据库文件检索数据。有关更多信息，请参阅第 14 章，邮件服务（参考）中的第 321 页中的 “`sendmail` 与名称服务的交互”和第 315 页中的 “邮件别名文件”。

请从以下过程中进行选择：

▼ 如何启动 NIS+ mail_aliases 表

您可以使用 aliasadm 命令来管理 NIS+ 表中的项。要创建表，请按照以下说明操作。有关更多信息，请参阅 aliasadm(1M) 手册页。

1 **成为拥有该表的 NIS+ 组的成员或邮件服务器的 root，或者承担等效角色。**

角色包含授权和具有特权的命令。有关角色的更多信息，请参见《系统管理指南：安全性服务》中的“配置 RBAC（任务列表）”。

2 **启动 NIS+ 表。**

```
# aliasadm -I
```

3 **将项添加到该表中。**

- 要添加两个或三个别名，请参阅第 272 页中的 “如何通过命令行向 NIS+ mail_aliases 表添加别名”。
- 要添加两个或三个以上的别名，请参阅第 273 页中的 “如何通过编辑 NIS+ mail_aliases 表添加项”。

▼ 如何列出 NIS+ mail_aliases 表中的内容

要查看该表中的完整内容列表，请按照以下说明操作。

1 **成为拥有该表的 NIS+ 组的成员或邮件服务器的 root，或者承担等效角色。**

角色包含授权和具有特权的命令。有关角色的更多信息，请参见《系统管理指南：安全性服务》中的“配置 RBAC（任务列表）”。

2 **按别名字母顺序列出所有项。**

```
# aliasadm -l
```

有关更多信息，请参阅 aliasadm(1M) 手册页。

示例 13–3 列出 NIS+ mail_aliases 表中的单项

或者，可以使用 aliasadm 命令列出单项。完成此过程的第一步后，请键入以下内容：

```
# aliasadm -m ignatz
ignatz: ignatz@saturn # Alias for Iggy Ignatz
```

该命令仅会匹配完整的别名，而不会匹配部分字符串。不能将 * 和 ? 等元字符与 aliasadm -m 一起使用。

示例 13–4 列出 NIS+ mail_aliases 表中的部分匹配项

另外，还可以使用 aliasadm 命令列出部分匹配项。完成此过程的第一步后，请键入以下内容：

```
# aliasadm -l | grep partial-string
```

将 *partial_string* 替换为搜索所需的字符串。

▼ 如何通过命令行向 NIS+ mail_aliases 表添加别名

要将两个或三个别名添加到该表中，请按照以下说明操作。如果要添加两个或三个以上的别名，请参见第 273 页中的 “如何通过编辑 NIS+ mail_aliases 表添加项”。

1. **编辑各个邮件客户机、邮箱位置和邮件服务器系统名称的列表。**
2. **成为拥有该表的 NIS+ 组的成员或邮件服务器的 root，或者承担等效角色。**

   角色包含授权和具有特权的命令。有关角色的更多信息，请参见《系统管理指南：安全性服务》中的“配置 RBAC（任务列表）”。
3. **可选如有必要，请启动 NIS+ 表。**

   如果创建的是一个全新的 NIS+ mail_aliases 表，则必须首先启动该表。要完成此任务，请参阅第 271 页中的 “如何启动 NIS+ mail_aliases 表”。
4. **将别名添加到该表中。**

   请参见以下典型项示例。

   ```
   # aliasadm -a iggy iggy.ignatz@saturn "Iggy Ignatz"
   ```

   以下列表说明了上面示例的输入。

-a	用于添加别名的选项
iggy	别名的缩写
iggy.ignatz@saturn	扩展的别名

`"Iggy Ignatz"` 使用引号的别名

5 **显示创建的项并确保其正确。**

```
# aliasadm -m alias
```

alias 创建的项

有关更多信息，请参阅 `aliasadm(1M)` 手册页。

▼ 如何通过编辑 NIS+ mail_aliases 表添加项

您可以使用 `aliasadm` 命令来管理 NIS+ 表中的项。要将两个或三个以上的别名添加到该表中，请按照以下说明操作。

1 **编辑各个邮件客户机、邮箱位置和邮件服务器系统名称的列表。**

2 **成为拥有该表的 NIS+ 组的成员或邮件服务器的 `root`，或者承担等效角色。**

角色包含授权和具有特权的命令。有关角色的更多信息，请参见《系统管理指南：安全性服务》中的“配置 RBAC（任务列表）”。

3 **显示并编辑该别名表。**

```
# aliasadm -e
```

此命令将显示该表，并允许您对其进行编辑。所用的编辑器已使用 `$EDITOR` 环境变量进行了设置。如果未设置此变量，则 `vi` 为缺省编辑器。

4 **使用以下格式在单独一行中键入每个别名。**

alias: *expanded-alias* `#` [`"`*option*`"` `#` `"`*comments*`"`]

alias 此列用于别名的缩写。

expanded-alias 此列用于扩展的别名。

option 此列保留供将来使用。

comments 此列用于有关单个别名的注释，如别名的名称。

如果将选项列保留为空，请键入一对空引号 (`""`) 并添加注释。

项的顺序对 NIS+ `mail_aliases` 表并不重要。`aliasadm -l` 命令按字母顺序对列表进行排序并显示项。

有关更多信息，请参阅第 315 页中的 “邮件别名文件”和 `aliasadm(1M)` 手册页。

▼ 如何编辑 NIS+ mail_aliases 表中的项

要编辑该表中的项，请按照以下说明操作。

1. **成为拥有该表的 NIS+ 组的成员或邮件服务器的 root，或者承担等效角色。**
   角色包含授权和具有特权的命令。有关角色的更多信息，请参见《系统管理指南：安全性服务》中的“配置 RBAC（任务列表）”。

2. **显示别名项。**
   ```
   # aliasadm -m alias
   ```
   将 *alias* 替换为指定的别名。

3. **根据需要编辑别名项。**
   ```
   # aliasadm -c alias expanded-alias [options comments]
   ```
   alias 如有必要，编辑别名。
   expanded-alias 如有必要，编辑扩展的别名。
   options 如有必要，编辑选项。
   comments 如有必要，编辑此项的注释。
   有关更多信息，请参阅 aliasadm(1M) 手册页以及第 315 页中的 “邮件别名文件”。

4. **显示编辑的项并确保其正确。**
   ```
   # aliasadm -m alias
   ```
   有关更多信息，请参阅 aliasadm(1M) 手册页。

示例 13–5 删除 NIS+ mail_aliases 表中的项

要删除该表中的项，请在完成此过程的第一步后使用以下语法：

```
# aliasadm -d alias
```

将 *alias* 替换为要删除的项的别名。

▼ 如何设置 NIS mail.aliases 映射

使用以下过程可简化 NIS mail.aliases 映射的别名设置。

1. **编辑各个邮件客户机、邮箱位置和邮件服务器系统名称的列表。**

2. **成为 NIS 主服务器的 root 或承担等效角色。**

   角色包含授权和具有特权的命令。有关角色的更多信息，请参见《系统管理指南：安全性服务》中的“配置 RBAC（任务列表）”。

3. **编辑 /etc/mail/aliases 文件，并创建以下项。**

   a. **为每台邮件客户机添加项。**

   ```
   # cat /etc/mail/aliases
   ..
   alias:expanded-alias
   ```

   alias 使用缩写的别名。

   expanded-alias 使用扩展的别名 (user@host.domain.com)。

   b. **确保具有 Postmaster: root 项。**

   ```
   # cat /etc/mail/aliases
   ..
   Postmaster: root
   ```

   c. **为 root 添加别名。使用指定为邮件管理员的人员的邮件地址。**

   ```
   # cat /etc/mail/aliases
   ..
   root: user@host.domain.com
   ```

   user@host.domain.com 使用指定的邮件管理员的指定地址。

4. **确保 NIS 主服务器正在运行名称服务，以解析每台邮件服务器上的主机名。**

5. **转至 /var/yp 目录。**

   ```
   # cd /var/yp
   ```

6. **应用 make 命令。**

   ```
   # make
   ```

   /etc/hosts 和 /etc/mail/aliases 文件的更改将传播到 NIS 从属系统。这些更改至多仅在几分钟后便会生效。

▼ 如何设置本地邮件别名文件

使用以下过程可解析本地邮件别名文件的别名。

1. **编辑各个用户及其邮箱位置的列表。**

2 **成为邮件服务器的 root 或承担等效角色。**

角色包含授权和具有特权的命令。有关角色的更多信息，请参见《系统管理指南：安全性服务》中的“配置 RBAC（任务列表）”。

3 **编辑 /etc/mail/aliases 文件，并创建以下项。**

a. **为每个用户添加项。**

user1: *user2@host.domain*

user1	使用新别名。
user2@host.domain	使用新别名的实际地址。

b. **确保具有 Postmaster: root 项。**

```
# cat /etc/mail/aliases
..
Postmaster: root
```

c. **为 root 添加别名。使用指定为邮件管理员的人员的邮件地址。**

```
# cat /etc/mail/aliases
..
root: user@host.domain.com
```

user@host.domain.com	使用指定的邮件管理员的指定地址。

4 **重新生成别名数据库。**

```
# newaliases
```

/etc/mail/sendmail.cf 中 AliasFile 选项的配置可确定此命令是以二进制格式生成单个文件 /etc/mail/aliases.db，还是生成文件对 /etc/mail/aliases.dir 和 /etc/mail/aliases.pag。

5 **执行以下步骤之一，复制生成的文件。**

a. **可选将 /etc/mail/aliases、/etc/mail/aliases.dir 和 /etc/mail/aliases.pag 文件复制到其他各个系统中。**

您可以使用 rcp 或 rdist 命令复制这三个文件。有关更多信息，请参阅 rcp(1) 手册页或 rdist(1) 手册页。或者，可以为此创建脚本。

复制这些文件时，无需在其他各个系统上都运行 newaliases 命令。但是请记住，每次添加或删除邮件客户机时，必须更新所有 /etc/mail/aliases 文件。

b. **可选将 /etc/mail/aliases 和 /etc/mail/aliases.db 文件复制到其他各个系统中。**

您可以使用 rcp 或 rdist 命令复制这些文件。有关更多信息，请参阅 rcp(1) 手册页或 rdist(1) 手册页。或者，可以为此创建脚本。

复制这些文件时，无需在其他各个系统上都运行 newaliases 命令。但是请记住，每次添加或删除邮件客户机时，必须更新所有 /etc/mail/aliases 文件。

▼ 如何创建加密映射文件

要创建加密映射文件，请按照以下说明操作。

1 **成为超级用户或承担等效角色。**

角色包含授权和具有特权的命令。有关角色的更多信息，请参见《系统管理指南：安全性服务》中的"配置 RBAC（任务列表）"。

2 **创建输入文件。**

项可以使用以下语法。

```
old-name@newdomain.com     new-name@newdomain.com
old-name@olddomain.com     error:nouser No such user here
@olddomain.com             %l@newdomain.com
```

old_name@newdomain.com 使用以前指定的用户名以及新指定的域。

new_name@newdomain.com 使用新指定的地址。

old_name@olddomain.com 使用以前指定的用户名及域。

olddomain.com 使用以前指定的域。

newdomain.com 使用新指定的域。

第一项将邮件重定向到新别名。下一项在使用的别名错误时创建一条消息。最后一项将所有传入邮件从 olddomain 重定向到 newdomain。

3 **创建数据库文件。**

```
# /usr/sbin/makemap maptype newmap < newmap
```

maptype 选择数据库类型，如 dbm、btree 或 hash。

newmap 使用输入文件名称以及数据库文件名称的第一部分。如果选择 dbm 数据库类型，则会使用 .pag 和 .dir 后缀创建数据库文件。对于其他两种数据库类型，文件名后跟 .db。

管理 postmaster 别名

每个系统都必须能够将邮件发送到 postmaster 邮箱。您可以为 postmaster 创建 NIS 或 NIS+ 别名，也可在每个本地 /etc/mail/aliases 文件中创建该别名。请参阅以下过程。

- 第 278 页中的 "如何在每个本地 /etc/mail/aliases 文件中创建 postmaster 别名"

- 第 278 页中的 “如何为 postmaster 创建单独的邮箱”
- 第 279 页中的 “如何为 /etc/mail/aliases 文件中的别名添加 postmaster 邮箱”

▼ 如何在每个本地 /etc/mail/aliases 文件中创建 postmaster 别名

如果要在每个本地 /etc/mail/aliases 文件中创建 postmaster 别名，请按照以下说明操作。

1 成为超级用户或承担等效角色。

角色包含授权和具有特权的命令。有关角色的更多信息，请参见《系统管理指南：安全性服务》中的“配置 RBAC（任务列表）”。

2 查看 /etc/mail/aliases 项。

```
# cat /etc/mail/aliases
# Following alias is required by the mail protocol, RFC 2821
# Set it to the address of a HUMAN who deals with this system's
# mail problems.
Postmaster: root
```

3 编辑每个系统的 /etc/mail/aliases 文件。

将 root 更改成指定为邮件管理员的人员的邮件地址。

Postmaster: *mail-address*

mail-address 使用指定为邮件管理员的人员的指定地址。

4 可选为邮件管理员创建单独的邮箱。

可以为邮件管理员创建单独的邮箱，以便将邮件管理员邮件与个人邮件分开。如果创建单独的邮箱，请在编辑 /etc/mail/aliases 文件时使用该邮箱地址，而不要使用邮件管理员的个人邮件地址。有关详细信息，请参阅第 278 页中的 “如何为 postmaster 创建单独的邮箱”。

▼ 如何为 postmaster 创建单独的邮箱

如果要为 postmaster 创建单独的邮箱，请按照以下说明操作。

1 成为超级用户或承担等效角色。

角色包含授权和具有特权的命令。有关角色的更多信息，请参见《系统管理指南：安全性服务》中的“配置 RBAC（任务列表）”。

2 为指定为 postmaster 的人员创建用户帐户。在口令字段中放置一个星号 (*)。

有关添加用户帐户的详细信息，请参阅《系统管理指南：基本管理》中的“设置用户帐户（任务列表）”。

3 **完成邮件传送后，启用 `mail` 程序读取和写入邮箱名称。**

```
# mail -f postmaster
```

postmaster 使用指定的地址。

▼ 如何为 /etc/mail/aliases 文件中的别名添加 postmaster 邮箱

如果要为 `/etc/mail/aliases` 文件中的别名添加 `postmaster` 邮箱，请按照以下说明操作。

1 **成为超级用户或承担等效角色。**

角色包含授权和具有特权的命令。有关角色的更多信息，请参见《系统管理指南：安全性服务》中的“配置 RBAC（任务列表）”。

2 **为 `root` 添加别名。使用指定为邮件管理员的人员的邮件地址。**

```
# cat /etc/mail/aliases
..
root: user@host.domain.com
```

user@host.domain.com 使用指定为邮件管理员的人员的指定地址。

3 **在邮件管理员本地系统的 `/etc/mail/aliases` 文件中，创建一个定义别名名称的项。以 `sysadmin` 为例。另外，还在其中包含指向本地邮箱的路径。**

```
# cat /etc/mail/aliases
..
sysadmin: /usr/somewhere/somefile
```

sysadmin 为新别名创建名称。

/usr/somewhere/somefile 使用指向本地邮箱的路径。

4 **重新生成别名数据库。**

```
# newaliases
```

管理队列目录（任务列表）

下表介绍了管理邮件队列的过程。

任务	说明	参考
显示邮件队列 `/var/spool/mqueue` 的内容	使用此过程可查看队列中的消息数，以及从队列中清除消息的速度。	第 280 页中的“如何显示邮件队列 `/var/spool/mqueue` 的内容”

任务	说明	参考
强制对邮件队列 /var/spool/mqueue 进行邮件队列处理	使用此过程可处理向以前无法接收消息的系统发送的消息。	第 281 页中的 “如何在邮件队列 /var/spool/mqueue 中强制进行邮件队列处理”
运行邮件队列 /var/spool/mqueue 的子集	使用此过程可强制处理地址子串（如主机名）。另外，使用此过程还可强制处理队列中的特定消息。	第 281 页中的 “如何运行邮件队列 /var/spool/mqueue 的子集”
移动邮件队列 /var/spool/mqueue	使用此过程可移动该邮件队列。	第 281 页中的 “如何移动邮件队列 /var/spool/mqueue”
运行旧邮件队列 /var/spool/omqueue	使用此过程可运行旧邮件队列。	第 282 页中的 “如何运行旧邮件队列 /var/spool/omqueue”

管理队列目录

本节介绍了一些有助于队列管理的任务。有关仅客户机适用的队列的信息，请参阅第 333 页中的 “sendmail 版本 8.12 中的配置文件 submit.cf”。有关其他相关信息，可以参阅第 343 页中的 “sendmail 版本 8.12 中新增的队列功能”。

请参阅以下内容：

- 第 280 页中的 “如何显示邮件队列 /var/spool/mqueue 的内容”
- 第 281 页中的 “如何在邮件队列 /var/spool/mqueue 中强制进行邮件队列处理”
- 第 281 页中的 “如何运行邮件队列 /var/spool/mqueue 的子集”
- 第 281 页中的 “如何移动邮件队列 /var/spool/mqueue”
- 第 282 页中的 “如何运行旧邮件队列 /var/spool/omqueue”

▼ 如何显示邮件队列 /var/spool/mqueue 的内容

- **显示队列中的消息数以及从队列中清除消息的速度。**

  键入以下命令：

  ```
  # /usr/bin/mailq | more
  ```

  此命令将提供以下信息。

  - 队列 ID
  - 消息大小
  - 消息进入队列的日期
  - 消息状态
  - 发件人和收件人

  另外，此命令还会立即检查授权属性 solaris.admin.mail.mailq。如果检查成功，将执行与使用 sendmail 指定 --bp 标志等效的操作。如果检查失败，则会输出一条错误消

息。缺省情况下，对所有用户均会启用此授权属性。通过修改 prof_attr 中的用户项，可以禁用该授权属性。有关更多信息，请参阅 prof_attr(4) 和 mailq(1) 手册页。

▼ 如何在邮件队列 /var/spool/mqueue 中强制进行邮件队列处理

例如，使用此过程可处理向以前无法接收消息的系统发送的消息。

1 **成为超级用户或承担等效角色。**

角色包含授权和具有特权的命令。有关角色的更多信息，请参见《系统管理指南：安全性服务》中的“配置 RBAC（任务列表）”。

2 **强制进行队列处理，并在清空队列时显示作业进度。**

```
# /usr/lib/sendmail -q -v
```

▼ 如何运行邮件队列 /var/spool/mqueue 的子集

例如，使用此过程可强制处理地址子串（如主机名）。另外，使用此过程还可强制处理队列中的特定消息。

1 **成为超级用户或承担等效角色。**

角色包含授权和具有特权的命令。有关角色的更多信息，请参见《系统管理指南：安全性服务》中的“配置 RBAC（任务列表）”。

2 **使用 --qR*string* 随时运行该邮件队列的子集。**

```
# /usr/lib/sendmail -qRstring
```

string　使用收件人别名或 *user@host.domain* 的子串（如主机名）。

或者，可使用 --qI*nnnnn* 运行该邮件队列的子集。

```
# /usr/lib/sendmail -qInnnnn
```

nnnnn　使用队列 ID。

▼ 如何移动邮件队列 /var/spool/mqueue

如果要移动该邮件队列，请按照以下说明操作。

1 **成为邮件主机的 root 或承担等效角色。**

角色包含授权和具有特权的命令。有关角色的更多信息，请参见《系统管理指南：安全性服务》中的“配置 RBAC（任务列表）”。

2 **中止 sendmail 守护进程。**

```
# svcadm disable network/smtp:sendmail
```

现在， sendmail 将不再处理该队列目录。

3 **转至 /var/spool 目录。**

```
# cd /var/spool
```

4 **将目录 mqueue 及其所有内容移动到 omqueue 目录中。然后，创建一个名为 mqueue 的新的空目录。**

```
# mv mqueue omqueue; mkdir mqueue
```

5 **将该目录权限按所有者设置为读取/写入/执行，按组设置为读取/执行。另外，将所有者和组设置为 daemon。**

```
# chmod 750 mqueue; chown root:bin mqueue
```

6 **启动 sendmail。**

```
# svcadm enable network/smtp:sendmail
```

▼ 如何运行旧邮件队列 /var/spool/omqueue

要运行旧邮件队列，请按照以下说明操作。

1 **成为超级用户或承担等效角色。**

角色包含授权和具有特权的命令。有关角色的更多信息，请参见《系统管理指南：安全性服务》中的“配置 RBAC（任务列表）”。

2 **运行该旧邮件队列。**

```
# /usr/lib/sendmail -oQ/var/spool/omqueue -q
```

-oQ 标志用于指定备用队列目录。-q 标志用于指示运行该队列中的所有作业。如果要在屏幕中显示详细输出，请使用 -v 标志。

3 **删除该空目录。**

```
# rmdir /var/spool/omqueue
```

管理 .forward 文件（ 任务列表 ）

下表介绍了管理 .forward 文件的过程。有关更多信息，请参阅第 14 章，邮件服务（参考）中的第 318 页中的 “.forward 文件”。

任务	说明	参考
禁用 .forward 文件	例如，如果要阻止自动转发，请使用此过程。	第 283 页中的“如何禁用 .forward 文件”
更改 .forward 文件搜索路径	例如，如果要将所有 .forward 文件移动到公用目录中，请使用此过程。	第 284 页中的“如何更改 .forward－文件搜索路径”
创建和填充 /etc/shells	通过此过程，用户可使用 .forward 文件将邮件转发到程序或文件。	第 284 页中的“如何创建和填充 /etc/shells”

管理 .forward 文件

本节介绍了与 .forward 文件管理相关的若干过程。由于用户可以编辑这些文件，因此可能导致出现问题。有关更多信息，请参阅第 14 章，邮件服务（参考）中的第 318 页中的“.forward 文件”。

请参阅以下内容：

- 第 283 页中的“如何禁用 .forward 文件”
- 第 284 页中的“如何更改 .forward－文件搜索路径”
- 第 284 页中的“如何创建和填充 /etc/shells”

▼ 如何禁用 .forward 文件

此过程用于阻止自动转发，可禁用特定主机的 .forward 文件。

1. **成为超级用户或承担等效角色。**

   角色包含授权和具有特权的命令。有关角色的更多信息，请参见《系统管理指南：安全性服务》中的“配置 RBAC（任务列表）”。

2. **复制 /etc/mail/cf/domain/solaris-generic.m4 或站点特定的域 m4 文件。**

   ```
   # cd /etc/mail/cf/domain
   # cp solaris-generic.m4 mydomain.m4
   ```

   mydomain　使用选择的文件名。

3. **在刚创建的文件中添加以下行。**

   ```
   define('confFORWARD_PATH','')dnl
   ```

   如果 m4 文件中已存在 confFORWARD_PATH 的值，请将该值替换为空值。

4. **生成并安装新的配置文件。**

   如果需要有关此步骤的帮助信息，请参阅第 261 页中的“如何生成新的 sendmail.cf 文件”。

注 – 编辑 .mc 文件时，请记住将 DOMAIN(‘solaris-generic’) 更改为 DOMAIN(‘*mydomain*’)。

▼ 如何更改 .forward 一文件搜索路径

例如，如果要将所有 .forward 文件放置在公用目录中，请按照以下说明操作。

1. **成为超级用户或承担等效角色。**

   角色包含授权和具有特权的命令。有关角色的更多信息，请参见《系统管理指南：安全性服务》中的“配置 RBAC（任务列表）”。

2. **复制 /etc/mail/cf/domain/solaris-generic.m4 或站点特定的域 m4 文件。**

   ```
   # cd /etc/mail/cf/domain
   # cp solaris-generic.m4 mydomain.m4
   ```

   mydomain 使用选择的文件名。

3. **在刚创建的文件中添加以下行。**

   ```
   define(‘confFORWARD_PATH’,‘$z/.forward:/var/forward/$u’)dnl
   ```

   如果 m4 文件中已存在 confFORWARD_PATH 的值，请将其替换为该新值。

4. **生成并安装新的配置文件。**

   如果需要有关此步骤的帮助信息，请参阅第 261 页中的 “如何生成新的 sendmail.cf 文件”。

注 – 编辑 .mc 文件时，请记住将 DOMAIN(‘solaris-generic’) 更改为 DOMAIN(‘*mydomain*’)。

▼ 如何创建和填充 /etc/shells

此文件未包含在标准发行版中。如果要允许用户使用 .forward 文件将邮件转发到程序或文件，则必须添加该文件。您可以通过使用 grep 标识口令文件中列出的所有 shell，手动创建该文件。然后，可将这些 shell 键入到文件中。但是，使用可下载脚本的以下过程更易于使用。

1. **下载脚本。**

   http://www.sendmail.org/vendor/sun/gen-etc-shells.html

2 **成为超级用户或承担等效角色。**

角色包含授权和具有特权的命令。有关角色的更多信息，请参见《系统管理指南：安全性服务》中的“配置 RBAC（任务列表）”。

3 **要生成 shell 列表，请运行 `gen-etc-shells` 脚本。**

```
# ./gen-etc-shells.sh > /tmp/shells
```

此脚本使用 `getent` 命令收集 `/etc/nsswitch.conf` 中列出的口令文件源所包含的 shell 名称。

4 **检查并编辑 `/tmp/shells` 中的 shell 列表。**

使用您选择的编辑器，删除不包含的所有 shell。

5 **将文件移动到 `/etc/shells`。**

```
# mv /tmp/shells /etc/shells
```

邮件服务故障排除过程和技巧（任务列表）

下表介绍了邮件服务故障排除过程和技巧。

任务	说明	参考
测试邮件配置	用于测试对 `sendmail` 配置文件的更改的步骤	第 286 页中的“如何测试邮件配置”
检查邮件别名	用于确认是否能将邮件传送到指定收件人的步骤	第 286 页中的“如何检查邮件别名”
测试规则集	用于检查 `sendmail` 规则集的输入和返回的步骤	第 287 页中的“如何测试 `sendmail` 规则集”
验证与其他系统的连接	用于验证与其他系统的连接的技巧	第 288 页中的“如何验证与其他系统的连接”
使用 `syslogd` 程序记录消息	用于收集错误消息信息的技巧	第 288 页中的“记录错误消息”
检查其他源的诊断信息	用于从其他源获取诊断信息的技巧	第 289 页中的“邮件诊断信息的其他源”

邮件服务故障排除过程和技巧

本节介绍了一些可用于解决邮件服务问题的过程和技巧。

▼ 如何测试邮件配置

要测试对配置文件所做的更改，请按照以下说明操作。

1. **在包含已修订的配置文件的任何系统上重新启动 sendmail。**

   ```
   # svcadm refresh network/smtp:sendmail
   ```

2. **从各个系统发送测试消息。**

   ```
   # /usr/lib/sendmail -v names </dev/null
   ```

   names 指定收件人的电子邮件地址。

   此命令会向指定的收件人发送一条空消息，并在监视器上显示该消息的活动。

3. **通过将该消息发送至一般用户名，向您自己或本地系统中的其他人发送邮件。**

4. **可选如果已连接到网络，请按三个方向将邮件发送到其他系统中的某个用户。**

   - 从主系统到客户机系统
   - 从客户机系统到主系统
   - 从一台客户机系统到另一台客户机系统

5. **可选如果具有邮件网关，请将邮件从邮件主机发送到其他域，以确保中继邮件程序和主机的配置正确。**

6. **可选如果通过电话线设置了与另一台主机的 UUCP 连接，请将邮件发送到该主机的某个用户，并要求该用户回复邮件或在收到消息时与您联系。**

7. **要求某用户通过 UUCP 连接向您发送邮件。**

   由于 sendmail 程序会将消息传递给 UUCP 进行传送，因此该程序无法检测消息是否已传送。

8. **通过不同系统将消息发送到 postmaster，并确保消息传送到邮件管理员的邮箱。**

如何检查邮件别名

以下示例说明了如何验证别名。

```
% mconnect
connecting to host localhost (127.0.0.1), port 25
connection open
220 your.domain.com ESMTP Sendmail 8.13.6+Sun/8.13.6; Tue, 12 Sep 2004 13:34:13 -0800 (PST)
expn sandy
250 2.1.5 <sandy@phoenix.example.com>
quit
```

```
221 2.0.0 your.domain.com closing connection
%
```

在此示例中，mconnect 程序打开了一个与本地主机上的邮件服务器的连接，并允许您测试该连接。该程序以交互方式运行，因此可以发出各种诊断命令。有关完整说明，请参见 mconnect(1) 手册页。项 expn sandy 提供了扩展地址 sandy@phoenix.example.com。因此，您已验证了使用别名 sandy 时可以传送邮件。

使用本地范围和域范围的别名时，请记住避免产生循环和不一致的数据库。尤其要注意，在系统之间移动用户时应避免创建别名循环。

▼ 如何测试 sendmail 规则集

要检查 sendmail 规则集的输入和返回，请按照以下说明操作。

1. **更改为地址测试模式。**

   ```
   # /usr/lib/sendmail -bt
   ```

2. **测试邮件地址。**

   在最后一个提示符 (>) 下提供以下数字和地址。

   ```
   > 3,0 mail-sraddress
   ```

   mail-address　　使用要测试的邮件地址。

3. **结束会话。**

   按 Ctrl-D 组合键。

示例 13–6 地址测试模式输出

以下是地址测试模式的输出示例。

```
% /usr/lib/sendmail -bt
ADDRESS TEST MODE (ruleset 3 NOT automatically invoked)
Enter <ruleset> <address>
> 3,0 sandy@phoenix
canonify           input: sandy @ phoenix
Canonify2          input: sandy < @ phoenix >
Canonify2        returns: sandy < @ phoenix . example . com . >
canonify         returns: sandy < @ phoenix . example . com . >
parse              input: sandy < @ phoenix . example . com . >
Parse0             input: sandy < @ phoenix . example . com . >
Parse0           returns: sandy < @ phoenix . example . com . >
ParseLocal         input: sandy < @ phoenix . example . com . >
ParseLocal       returns: sandy < @ phoenix . example . com . >
Parse1             input: sandy < @ phoenix . example . com . >
MailerToTriple     input: < mailhost . phoenix . example . com >
     sandy < @ phoenix . example . com . >
```

```
MailerToTriple   returns: $# relay $@ mailhost . phoenix . example . com
     $: sandy < @ phoenix . example . com . >
Parse1           returns: $# relay $@ mailhost . phoenix . example . com
     $: sandy < @ phoenix . example . com . >
parse            returns: $# relay $@ mailhost . phoenix . example . com
     $: sandy < @ phoenix . example . com . >
```

如何验证与其他系统的连接

mconnect 程序打开一个与指定主机上邮件服务器的连接，并允许您测试该连接。该程序以交互方式运行，因此可以发出各种诊断命令。有关完整说明，请参见 mconnect(1) 手册页。以下示例确认发送到用户名 sandy 的邮件是可传送的。

```
% mconnect phoenix

connecting to host phoenix (172.31.255.255), port 25
connection open
220 phoenix.example.com ESMTP Sendmail 8.13.1+Sun/8.13.1; Sat, 4 Sep 2004 3:52:56 -0700
expn sandy
250 2.1.5 <sandy@phoenix.example.com>
quit
```

如果无法使用 mconnect 连接到某个 SMTP 端口，请检查以下情况。

- 系统负载是否太高?
- sendmail 守护进程是否正在运行?
- 系统是否具有相应的 /etc/mail/sendmail.cf 文件?
- sendmail 使用的端口 25 是否处于活动状态?

记录错误消息

邮件服务使用 syslogd 程序记录大多数错误消息。缺省情况下，syslogd 程序会将这些消息发送到一个称为 loghost 的系统，该系统可在 /etc/hosts 文件中指定。可以将 loghost 定义为保存整个 NIS 域的所有日志。如果未指定 loghost，则不会报告 syslogd 中的错误消息。

/etc/syslog.conf 文件用于控制 syslogd 程序转发消息的位置。可以通过编辑 /etc/syslog.conf 文件来更改缺省配置。为使所有更改生效，必须重新启动 syslog 守护进程。要收集有关邮件的信息，可在该文件中添加以下选项。

- mail.alert－有关应立即修复的情况的消息
- mail.crit－关键消息
- mail.warning－警告消息
- mail.notice－并非错误，但可能需要注意的消息
- mail.info－提示性消息
- mail.debug－调试消息

/etc/syslog.conf 文件中的以下项会将所有关键消息、提示性消息和调试消息的副本发送到 /var/log/syslog。

```
mail.crit;mail.info;mail.debug              /var/log/syslog
```

在系统日志中，每一行都包含时间标记、生成该行的系统名称以及消息。syslog 文件可以记录大量信息。

该日志按级别顺序进行排列。在最低级别，仅记录异常情况。在最高级别，即使最普通和最不受关注的事件也会被记录。根据约定，10 以下的日志级别被视为“有用”级别。10 以上的日志级别通常用于调试。有关 loghost 和 syslogd 程序的信息，请参见《系统管理指南：高级管理》中的“定制系统消息日志”。

邮件诊断信息的其他源

对于其他诊断信息，请检查以下源。

- 查看消息头中的 Received 行。这些行跟踪中继消息时消息所采用的路由。请记住考虑时区差异。
- 查看 MAILER-DAEMON 中的消息。这些消息通常会报告传送问题。
- 检查记录系统组传送问题的系统日志。sendmail 程序始终在系统日志中记录其活动。您可能需要修改 crontab 文件，以便在夜间运行 shell 脚本。该脚本在日志中搜索 SYSERR 消息，并将找到的任何消息发送到邮件管理员。
- 使用 mailstats 程序测试邮件类型，并确定传入消息和外发消息的数量。

解决错误消息

本节介绍了如何解析一些与 sendmail 相关的错误消息。此外，还可参阅 http://www.sendmail.org/faq。

以下错误消息包含两种或多种以下类型的信息。

- **原因**：何种情况可能会导致出现该消息
- **说明**：出现错误消息时用户正在执行哪些操作
- **解决方案**：采取何种措施可解决问题或继续工作

451 timeout waiting for input during *source*

原因: 当 sendmail 从可能超时的任何源（如 SMTP 连接）进行读取时，该程序会在开始读取之前将计时器设置为各种 Timeout 选项的值。如果在计时器到期之前没有完成读取，则会出现此消息并且停止读取。通常，这种情况发生在 RCPT 过程中。然后，该邮件在队列中排队以便以后传送。

解决方法: 如果经常显示此消息，请增大 `/etc/mail/sendmail.cf` 文件中各种 `Timeout` 选项的值。如果已将计时器设置为一个较大的数字，请查找硬件问题（如网络线路较差或连接不正确）。

`550` *hostname*`... Host unknown`
原因: 此 `sendmail` 消息表明，在域名系统 (Domain Name System, DNS) 查找过程中，找不到通过 at 符号 (@) 后面的地址部分指定的目标主机计算机。

解决方法: 使用 `nslookup` 命令验证在该域或其他域中是否存在此目标主机，可能是由于拼写有所不同。否则，请与预定收件人联系并请求正确的地址。

`550` *username*`... User unknown`
原因: 此 `sendmail` 消息表明，在目标主机计算机上，找不到通过 at 符号 (@) 前面的地址部分指定的预定收件人。

解决方法: 检查该电子邮件地址并重试，可能是由于拼写有所不同。如果此修正方法无效，请与预定收件人联系并请求正确的地址。

`554` *hostname*`... Local configuration error`
原因: 此 `sendmail` 消息通常表明，本地主机正尝试向其本身发送邮件。

解决方法: 检查 `/etc/mail/sendmail.cf` 文件中的 `$j` 宏的值，确保该值为全限定域名。

描述: 当发送系统在 SMTP `HELO` 命令中将其主机名提供给接收系统时，接收系统会将其名称与发件人名称进行比较。如果这些名称相同，接收系统将发出此错误消息并关闭连接。`HELO` 命令中提供的名称即 `$j` 宏的值。

有关其他信息，请参阅 `http://www.sendmail.org/faq/section4#4.5`。

`config error: mail loops back to myself.`
原因: 如果设置了 MX 记录并使主机 *bar* 成为域 *foo* 的邮件交换器，则会出现此错误消息。但是，配置主机 *bar* 失败，无法了解它即是域 *foo* 的邮件交换器。

此外，另一种可能是发送系统和接收系统都识别为同一个域。

解决方法: 有关说明，请参阅 `http://www.sendmail.org/faq/section4#4.5`。

`host name configuration error`
描述: 这是一条旧的 `sendmail` 消息，该消息替换了 `I refuse to talk to myself`，现在则替换为 `Local configuration error` 消息。

解决方法: 按照为解析错误消息 `554` *hostname*`... Local configuration error` 提供的说明进行操作。

user unknown

原因: 尝试向某用户发送邮件时，显示了 `Username... user unknown` 错误。该用户位于同一系统中。

解决方法: 检查所输入的电子邮件地址是否存在拼写错误。或者，可将该用户的别名设置为 `/etc/mail/aliases` 或该用户的 `.mailrc` 文件中不存在的电子邮件地址。另外，检查用户名的大写字符。电子邮件地址最好不要区分大小写。

有关其他信息，请参阅 `http://www.sendmail.org/faq/section4#4.17`。

◆ ◆ ◆ 第 14 章

14 邮件服务（参考）

sendmail 程序是一个邮件传输代理。该程序使用配置文件来提供别名和转发、到网络网关的自动路由以及灵活的配置。Solaris OS 提供了大多数站点都可以使用的标准配置文件。第 12 章，邮件服务（概述）介绍了邮件服务的组件，并对典型邮件服务配置进行了说明。第 13 章，邮件服务（任务）说明了如何设置和管理电子邮件系统。本章介绍了有关以下主题的信息。

有关这些章节中未介绍的详细信息，请参见以下手册页：

- sendmail(1M)
- mail.local(1M)
- mailstats(1)
- makemap(1M)
- editmap(1M)

Solaris 版本的 sendmail

本节包括以下主题，其中介绍了 Solaris 版本的 sendmail 与普通 Berkeley 版本之间的一些差异。

编译 sendmail 时使用和未使用的标志

从 Solaris 10 发行版开始，可使用以下标志来编译 sendmail。如果您的配置需要使用其他标志，则需下载源代码并重新编译此二进制命令。可在 http://www.sendmail.org 中找到有关此过程的信息。

表 14–1 常规 sendmail 标志

标志	说明
SOLARIS=21000	支持 Solaris 10 发行版。
MILTER	支持邮件过滤器 API。缺省情况下，在 sendmail 版本 8.13 中会启用此标志。请参见第 295 页中的 “MILTER（用于 sendmail 的邮件过滤器 API）”。
NETINET6	支持 IPv6。此标志已从 conf.h 移至 Makefile。

表 14–2 映射和数据库类型

标志	说明
NDBM	支持 ndbm 数据库
NEWDB	支持 Berkeley DB 数据库
USERDB	支持用户数据库
NIS	支持 nis 数据库
NISPLUS	支持 nisplus 数据库
LDAPMAP	支持 LDAP 映射
MAP_REGEX	支持正则表达式映射

表 14–3 操作系统标志

标志	说明
SUN_EXTENSIONS	支持 sun_compat.o 中包括的扩展。
SUN_INIT_DOMAIN	为了实现向下兼容，支持使用 NIS 域名来完全限定本地主机名。有关更多信息，请参阅 http://www.sendmail.org 中的供应商特定信息。
SUN_SIMPLIFIED_LDAP	支持特定于 Sun 的简化的 LDAP API。有关更多信息，请参阅 http://www.sendmail.org 中的供应商特定信息。
VENDOR_DEFAULT=VENDOR_SUN	选择 Sun 作为缺省供应商。

下表列出了编译 Solaris 10 发行版附带的 sendmail 版本时未使用的普通标志。

表 14–4 此版本的 sendmail 中未使用的普通标志

标志	说明
SASL	简单身份验证和安全层 (RFC 2554)
STARTTLS	事务处理级安全 (RFC 2487)

要查看用于编译 sendmail 的标志的列表，请使用以下命令。

```
% /usr/lib/sendmail -bt -d0.10 < /dev/null
```

注 – 上一命令不会列出特定于 Sun 的标志。

MILTER（用于 sendmail 的邮件过滤器 API）

MILTER 是 sendmail 的邮件过滤器 API，通过它第三方程序可在处理邮件以过滤元信息和内容时访问邮件。无需构建过滤器并配置 sendmail 即可使用它。缺省情况下，sendmail 版本 8.13 中会启用该 API。

有关更多详细信息，请访问以下站点：

- http://www.sendmail.org
- https://www.milter.org/

替代 sendmail 命令

Solaris 发行版中不包括 sendmail.org 所提供的普通发行版中的所有命令同义词。下表提供了命令别名的完整列表。该表还列出了 Solaris 发行版中是否包括这些命令以及如何使用 sendmail 来生成相同行为。

表 14–5 替代 sendmail 命令

替代名称	是否在此发行版中？	用于 sendmail 的选项
hoststat	否	sendmail -bh
mailq	是	sendmail -bp
newaliases	是	sendmail -bi
purgestat	否	sendmail -bH
smtpd	否	sendmail -bd

配置文件的版本

从 Solaris 10 发行版开始，sendmail 提供了一个配置选项，用于定义 sendmail.cf 文件的版本。通过此选项，可将较旧的配置文件用于当前版本的 sendmail。可将版本级别设置为 0 和 10 之间的值。另外，还可以定义供应商。Berkeley 和 Sun 都是有效的供应商选项。如果指定了版本级别而未定义供应商，则将使用 Sun 作为缺省供应商设置。下表列出了一些有效选项。

表 14–6 配置文件的版本值

字段	说明
V7/Sun	用于 sendmail 版本 8.8 的设置。
V8/Sun	用于 sendmail 版本 8.9 的设置。此设置包括在 Solaris 8 发行版中。
V9/Sun	用于 sendmail 版本 8.10 和 8.11 的设置。
V10/Sun	用于 sendmail 版本 8.12 和 8.13 的设置。版本 8.12 是 Solaris 9 发行版的缺省版本。从 Solaris 10 发行版开始，版本 8.13 为缺省版本。

注 – 建议您不要使用 V1/Sun。有关更多信息，请参阅 http://www.sendmail.org/vendor/sun/differences.html#4。

有关任务信息，请参阅第 13 章，邮件服务（任务）中的第 261 页中的 “更改 sendmail 配置”。

邮件服务的软件和硬件组件

本节介绍了邮件系统的软件和硬件组件。

- 第 296 页中的 “软件组件”
- 第 303 页中的 “硬件组件”

软件组件

每种邮件服务都至少包括以下软件组件之一。

- 第 297 页中的 “邮件用户代理”
- 第 297 页中的 “邮件传输代理”
- 第 297 页中的 “本地传送代理”

本节还介绍了以下软件组件。

- 第 297 页中的 “邮件程序与 sendmail”
- 第 298 页中的 “邮件地址”
- 第 300 页中的 “邮箱文件”
- 第 302 页中的 “邮件别名”

邮件用户代理

邮件用户代理是用户与邮件传输代理之间用作接口的程序。sendmail 程序是一个邮件传输代理。Solaris 操作系统提供了以下邮件用户代理。

- /usr/bin/mail
- /usr/bin/mailx
- /usr/dt/bin/dtmail

邮件传输代理

邮件传输代理负责邮件的路由以及邮件地址的解析。此代理也称为邮件**传输**代理。用于 Solaris 操作系统的传输代理是 sendmail。该传输代理可执行以下功能。

- 接受来自邮件用户代理的邮件
- 解析目标地址
- 选择正确的传送代理来传送邮件
- 接收从其他邮件传输代理传入的邮件

本地传送代理

本地传送代理是实现邮件传送协议的程序。Solaris 操作系统附带了以下本地传送代理。

- UUCP 本地传送代理，它使用 uux 传送邮件
- 本地传送代理，它是标准 Solaris 发行版中的 mail.local

第 332 页中的 “sendmail 版本 8.12 中的更改”提供了有关以下相关主题的信息。

- 第 341 页中的 “sendmail 版本 8.12 中新增的传送代理标志”
- 第 342 页中的 “sendmail 版本 8.12 中新增的用于传送代理的等式”

邮件程序与 sendmail

邮件程序是特定于 sendmail 的术语。sendmail 使用**邮件程序**来识别定制的本地传送代理或定制的邮件传输代理的特定实例。至少需要在 sendmail.cf 文件中指定一个邮件程序。有关任务信息，请参阅第 13 章，邮件服务（任务）中的第 261 页中的 “更改 sendmail 配置”。本节对以下两种类型的邮件程序进行了简短说明。

- 第 298 页中的 “简单邮件传输协议 (Simple Mail Transfer Protocol, SMTP) 邮件程序”
- 第 298 页中的 “UNIX 对 UNIX 复制程序 (UNIX-to-UNIX Copy Program, UUCP) 邮件程序”

有关邮件程序的其他信息，请参见 http://www.sendmail.org/m4/readme.html或 /etc/mail/cf/README。

简单邮件传输协议 (Simple Mail Transfer Protocol, SMTP) 邮件程序

SMTP 是在 Internet 中使用的标准邮件协议。此协议定义了以下邮件程序。

- smtp，用于向其他服务器提供常规 SMTP 传输。
- esmtp，用于向其他服务器提供扩展 SMTP 传输。
- smtp8，用于向其他服务器提供 SMTP 传输，而不会将 8 位数据转换为 MIME。
- dsmtp，用于通过使用 F=% 邮件程序标志来提供即时传送。请参阅第 341 页中的 “sendmail 版本 8.12 中对 MAILER() 声明的更改”和第 341 页中的 “sendmail 版本 8.12 中新增的传送代理标志”。

UNIX 对 UNIX 复制程序 (UNIX-to-UNIX Copy Program, UUCP) 邮件程序

应尽可能避免使用 UUCP。有关说明，请参阅 http://www.sendmail.org/m4/uucp_mailers.html或在 /etc/mail/cf/README 中搜索以下字符串：USING UUCP MAILERS。

UUCP 定义了以下邮件程序。

uucp-old　属于 $=U 类的名称将发送至 uucp-old。uucp 是此邮件程序的废弃名称。uucp-old 邮件程序在头中使用叹号地址。

uucp-new　属于 $=Y 类的名称将发送至 uucp-new。如果知道接收 UUCP 邮件程序可在一次传输中管理多个收件人，请使用此邮件程序。suucp 是此邮件程序的废弃名称。uucp-new 邮件程序在头中也使用叹号地址。

如果配置中还指定了 MAILER(smtp)，则还需定义另外两个邮件程序。

uucp-dom　此邮件程序使用域样式地址，并且基本上应用 SMTP 重写规则。

uucp-uudom　属于 $=Z 类的名称将发送至 uucp-uudom。uucp-uudom 和 uucp-dom 使用相同的头地址格式，即域样式地址。

注 – 由于 smtp 邮件程序会修改 UUCP 邮件程序，因此在 .mc 文件中应始终将 MAILER(smtp) 放在 MAILER(uucp) 的前面。

邮件地址

邮件地址包含邮件传送到的收件人和系统的名称。管理不使用名称服务的小型邮件系统时，对邮件进行寻址很容易。登录名可以唯一标识用户。如果管理的邮件系统中存在多个具有邮箱的系统，或者该邮件系统有一个或多个域，则情况会变得很复杂。如果与网络之外的服务器之间建立了 UUCP（或其他）邮件连接，则会进一步增加复杂性。以下各节中的信息有助于理解邮件地址的各个部分及其复杂性。

域和子域

电子邮件地址会使用域。**域**是用于网络地址命名的目录结构。一个域可以包含一个或多个**子域**。地址的域和子域与文件系统的分层结构类似。正如我们认为子目录位于其上面的目录之内，同样可以认为邮件地址中的每个子域位于其右侧的位置之内。

下表显示了一些顶层域。

表 14–7 顶层域

域	说明
com	商业站点
edu	教育站点
gov	美国政府机构
mil	美国军事机构
net	联网组织
org	其他非赢利组织

域不区分大小写。在地址的域部分中，可以使用大写、小写或大小写混合的字母，而不会产生任何错误。

名称服务域名和邮件域名

使用名称服务域名和邮件域名时，请记住以下几点。

- 缺省情况下，`sendmail` 程序会从 NIS 或 NIS+ 域名中去除第一个组成部分，以形成邮件域名。例如，如果 NIS+ 域名为 `bldg5.example.com`，则其邮件域名将为 `example.com`。
- 尽管邮件域地址不区分大小写，但 NIS 或 NIS+ 域名会区分大小写。为了获得最佳结果，在设置邮件以及 NIS 或 NIS+ 域名时请使用小写字符。
- DNS 域名和邮件域名必须相同。

有关更多信息，请参阅第 321 页中的 “`sendmail` 与名称服务的交互”。

邮件地址的典型格式

通常，邮件地址具有以下格式。有关详细信息，请参阅第 300 页中的 “与路由无关的邮件地址”。

user@subdomain. subdomain2.subdomain1.top-level-domain

@ 符号左侧的地址部分是本地地址。本地地址可以包含以下内容。

- 有关其他邮件传输的路由信息（例如 `bob::vmsvax@gateway` 或 `smallberries%mill.uucp@gateway`）
- 别名（例如 `iggy.ignatz`）

注 – 接收邮件程序负责确定地址的本地部分的含义。有关邮件程序的信息，请参阅第 297 页中的 “邮件程序与 sendmail”。

@ 符号右侧的地址部分显示域的级别，它是本地地址驻留的位置。每个子域之间用点分隔。地址的域部分可以是一个组织、物理地区或地理区域。此外，域信息的顺序是分层的，即子域的本地性越明显，该子域距离 @ 符号越近。

与路由无关的邮件地址

邮件地址可以与路由无关。与路由无关的寻址要求电子邮件的发件人指定收件人的名称以及最终目标。高速网络（如 Internet）可使用与路由无关的地址。与路由无关的地址可以具有以下格式。

user@*host*.*domain*

用于 UUCP 连接的与路由无关的地址可以具有以下地址格式。

host.*domain*!*user*

随着计算机的域分层命名方案越来越受欢迎，与路由无关的地址也越来越普遍。实际上，最常见的与路由无关的地址会省略主机名，并依赖域名服务来正确识别电子邮件的最终目标。

user@*domain*

通过搜索 @ 符号可首先读取与路由无关的地址。然后，从右（最高层）向左（@ 符号右侧的地址中最具体的部分）读取域分层结构。

邮箱文件

邮箱是指作为电子邮件的最终目标的文件。邮箱的名称可以是用户名或特定功能的标识，如邮件管理员。邮箱位于 `/var/mail/` *username* 文件中，该文件可以存在于用户的本地系统或远程邮件服务器上。在任一情况中，邮箱都位于邮件传送到的系统中。

应始终将邮件传送到本地文件系统，以便用户代理可从邮件缓冲池中提取邮件，并轻松将其存储在本地邮箱中。请勿使用已挂载 NFS 的文件系统作为用户邮箱的目标。具体来说，请勿将邮件定向至要从远程服务器挂载 /var/mail 文件系统的邮件客户机。在此情况下，应将用户的邮件发往邮件服务器而非客户机主机名。已挂载 NFS 的文件系统会导致在邮件传送和处理中出现问题。

/etc/mail/aliases 文件和名称服务（如 NIS 和 NIS+）提供了为电子邮件地址创建别名的机制。因此，用户无需知道用户邮箱的准确本地名称。

下表显示了一些针对专用邮箱的常见命名约定。

表 14–8 针对邮箱名称格式的约定

格式	说明
username	用户名通常与邮箱名称相同。
Firstname. *Lastname* *Firstname*_ *Lastname* *Firstinitial*. *Lastname* *Firstinitial*_ *Lastname*	可将用户名标识为用点（或下划线）分隔名和姓的全名。或者，也可以通过用点（或下划线）分隔首字母和姓来标识用户名。
postmaster	用户可以向 postmaster 邮箱发送并报告邮件系统的问题。每个站点和域都应该有一个 postmaster 邮箱。
MAILER-DAEMON	sendmail 会自动将发往 MAILER-DAEMON 的所有邮件路由至邮件管理员。
aliasname-request	以 -request 结尾的名称是分发列表的管理地址。此地址应将邮件重定向至维护分发列表的人员。
owner-*aliasname*	以 owner- 开头的名称是分发列表的管理地址。此地址应将邮件重定向至处理邮件错误的人员。
owner-owner	当不存在错误返回到的 owner-*aliasname* 别名时，可使用此别名。此地址应将邮件重定向至处理邮件错误的人员。在维护大量别名的所有系统中，也都应定义此地址。
local%*domain*	百分比符号 (%) 用来标记邮件到达其目标时扩展的本地地址。大多数邮件系统都会将带有 % 符号的邮箱名称解释为完整邮件地址。% 将用 @ 替换，并相应地重定向邮件。尽管许多人都使用 % 约定，但此约定并不是正式标准。此约定称为 "percent hack"。通常可以使用此功能来帮助调试邮件问题。

从 sendmail 版本 8 开始，如果存在所有者别名，则发送至组别名的邮件的信封发件人地址将更改为由所有者别名扩展所得的地址。通过此更改，可将所有邮件错误都发送至别名所有者，而不是返回给发件人。进行此更改后，用户会注意到，在传送发送至别名的邮件时，邮件看似来自别名所有者。以下别名格式有助于解决与此更改关联的一些问题。

```
mygroup: :include:/pathname/mygroup.list
owner-mygroup: mygroup-request
mygroup-request: sandys, ignatz
```

在本示例中，mygroup 别名是组的实际邮件别名。owner-mygroup 别名用来接收错误消息。应将 mygroup-request 别名用于管理请求。此结构意味着，在发送至 mygroup 别名的邮件中，信封发件人地址会更改为 mygroup-request。

邮件别名

别名是替代名称。对于电子邮件，可以使用别名来指定邮箱位置或定义邮件列表。有关任务列表，请参阅第 13 章，邮件服务（任务）中的第 270 页中的“管理邮件别名文件（任务列表）”。另外，还可以参阅本章中的第 315 页中的“邮件别名文件”。

对于大型站点，邮件别名通常用来定义邮箱的位置。提供邮件别名类似于在有多个房间的大公司内为个人提供房间号作为地址的一部分。如果不提供房间号，邮件将传送至中心地址。如果没有房间号，则需要花费额外的精力来确定邮件传送到该建筑内的地址。因此，更容易出现错误。例如，在同一建筑内有两个人名为 Kevin Smith，则仅有其中一个人可获取该邮件。为改正此问题，每个 Kevin Smith 都应在其地址中添加一个房间号。

创建邮件列表时，请尽可能使用与域和位置无关的地址。要提高别名文件的可移植性和灵活性，请尽可能使邮件列表中的别名项可以通用并与系统无关。例如，如果域 example.com 中的系统 mars 上有一个名为 ignatz 的用户，则应创建别名 ignatz@example 而非 ignatz@mars。如果用户 ignatz 更改了其系统名称但仍处于 example 域中，则无需更新别名文件即可反映系统名称的更改。

创建别名项时，请在每一行中键入一个别名。应该仅有一项包含用户的系统名称。例如，可为用户 ignatz 创建以下各项。

```
ignatz: iggy.ignatz
iggyi: iggy.ignatz
iggy.ignatz: ignatz@mars
```

可为本地名称或域创建别名。例如，如果用户 fred 在系统 mars 中具有一个邮箱并且该用户位于域 planets 中，则 NIS+ 别名表中可包含该用户的别名项。

```
fred: fred@planets
```

如果创建的邮件列表中包括域外面的用户，请使用用户名和域名来创建别名。例如，如果域 example.com 中的系统 privet 上有一个名为 smallberries 的用户，可创建别名为 smallberries@example.com。现在，向用户域之外发送邮件时，发件人的电子邮件地址会自动转换为全限定域名。

以下列表介绍了创建和管理邮件别名文件的方法。

- 可以创建在 NIS+ mail_aliases 表、NIS aliases 映射或本地 /etc/mail/aliases 文件中全局使用的邮件别名。另外，还可以创建和管理使用相同别名文件的邮件列表。
- 根据邮件服务的配置，可以通过使用 NIS 或 NIS+ 名称服务来管理别名，以维护全局 aliases 数据库。或者，也可以更新所有本地 /etc/mail/aliases 文件，以使别名保持同步。

- 用户也可以创建和使用别名。用户可以在其本地 `~/.mailrc` 文件（仅供该用户使用）或在本地 `/etc/mail/aliases` 文件（可供任何用户使用）中创建别名。用户通常不能创建或管理 NIS 或 NIS+ 别名文件。

硬件组件

可在同一系统中提供三种必需的邮件配置元素，也可通过单独的系统来提供这些元素。

- 第 303 页中的 “邮件主机”
- 第 303 页中的 “邮件服务器”
- 第 304 页中的 “邮件客户机”

当用户要与域之外的网络通信时，还必须添加第四个元素，即邮件网关。有关更多信息，请参阅第 304 页中的 “邮件网关”。以下各节介绍了每个硬件组件。

邮件主机

邮件主机是在网络中指定作为主邮件计算机的计算机。站点中的其他系统会将无法传送的邮件转发给邮件主机。通过在本地 `/etc/hosts` 文件中的 IP 地址右侧添加 `mailhost` 一词，可在 `hosts` 数据库中将某个系统指定为邮件主机。或者，也可以用类似的方法向名称服务的主机文件中添加 `mailhost` 一词。有关详细的任务信息，请参阅第 13 章，邮件服务（任务）中的第 257 页中的 “如何设置邮件主机”。

合适的候选邮件主机是配置作为您的网络和 Internet 全局网络之间的路由器的系统。有关更多信息，请参阅第 15 章，Solaris PPP 4.0（概述）、第 24 章，UUCP（概述）以及《系统管理指南：IP 服务》中的“配置 IPv4 路由器”。如果本地网络中没有系统具有调制解调器，请指定一个系统作为邮件主机。

有些站点在分时配置中会使用未联网的独立计算机。特别需要指出的是，独立计算机将为连接到其串行端口的终端提供服务。通过将独立系统指定为单系统网络的邮件主机，可为此配置设置电子邮件。第 12 章，邮件服务（概述）的第 246 页中的 “硬件组件概述”提供的图中显示了典型的电子邮件配置。

邮件服务器

邮箱是包含特定用户的电子邮件的单个文件。邮件会传送到用户邮箱驻留的系统，这可以是本地计算机或远程服务器。**邮件服务器**是可在其 `/var/mail` 目录中维护用户邮箱的任何系统。有关任务信息，请参阅第 13 章，邮件服务（任务）中的第 253 页中的 “如何设置邮件服务器”。

邮件服务器会路由来自客户机的所有邮件。客户机发送邮件时，邮件服务器会将该邮件放入队列进行传送。邮件进入队列后，用户可以重新引导或关闭客户机，而不会丢失这些邮件。收件人从客户机获取邮件时，邮件的 `From` 行中的路径包含了邮件服务器的名称。如果收件人做出响应，该响应将转到用户的邮箱。合适的候选邮件服务器是为用户提供起始目录的系统或定期备份的系统。

如果邮件服务器不是用户的本地系统，则使用 NFS 软件的配置中的用户可以使用 `/etc/vfstab` 文件来挂载 `/var/mail` 目录，前提是用户具有 `root` 访问权限。或者，用户也可以使用自动挂载程序。如果未提供 NFS 支持，用户可以登录到服务器来阅读其邮件。

如果网络中的用户发送其他类型的邮件（如音频文件或来自桌面发布系统的文件），则需要在邮件服务器中为邮箱分配更多空间。

通过为所有邮箱建立一个邮件服务器，可以简化进行备份的过程。如果邮件分散在多个系统中，则很难进行备份。在一台服务器中存储许多邮箱的缺点是该服务器会成为许多用户的单点故障。但是，可提供良好备份的优点则通常值得冒这个风险。

邮件客户机

邮件客户机是一个在邮件服务器上具有邮箱的邮件服务用户。此外，邮件客户机在指向邮箱位置的 `/etc/mail/aliases` 文件中还具有邮件别名。有关任务信息，请参阅第 13 章，邮件服务（任务）中的第 255 页中的 “如何设置邮件客户机”。

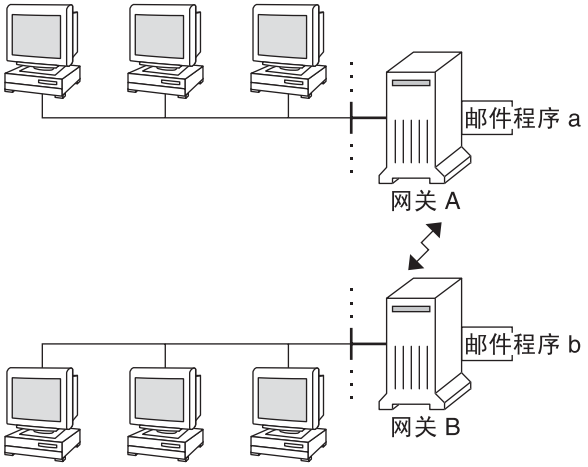
邮件网关

邮件网关是一台计算机，用于处理运行不同通信协议的网络之间的连接或在使用相同协议的不同网络之间进行通信。例如，邮件网关可能会将 TCP/IP 网络连接到运行系统网络体系结构 (Systems Network Architecture, SNA) 协议集的网络。

要设置的最简单的邮件网关是连接使用相同协议或邮件程序的两个网络的网关。此系统可以处理 `sendmail` 在域中无法根据其地址找到收件人的邮件。如果存在邮件网关，`sendmail` 将使用网关来发送和接收域外面的邮件。

可在使用不匹配邮件程序的两个网络之间设置邮件网关，如下图所示。要支持此配置，必须在邮件网关系统中定制 `sendmail.cf` 文件，这可能是一个很困难并且耗时的过程。

图 14–1 不同通信协议之间的网关



如果有一台计算机与 Internet 建立连接，则可将该计算机配置为邮件网关。配置邮件网关之前，请仔细考虑站点的安全需求。您可能需要在公司网络与其他网络之间创建防火墙网关，并将该网关设置为邮件网关。有关任务信息，请参阅第 13 章，邮件服务（任务）中的第 258 页中的 “如何设置邮件网关”。

邮件服务的程序和文件

邮件服务包括许多彼此交互的程序和守护进程。本节介绍了与管理电子邮件相关的文件、程序、术语和概念。

vacation 实用程序的增强功能

从 Solaris 10 发行版开始，vacation 实用程序进行了增强，允许用户指定哪些传入邮件可以接收自动生成的回复。使用此增强功能，用户可以避免与不认识的人共享机密信息或联系人信息。来自垃圾邮件发件人或不认识的人的邮件将不会收到回复。

此项增强功能将收到的发件人电子邮件地址与 .vacation.filter 文件中的域列表或电子邮件地址列表进行比较。该文件由用户创建，并保存在用户的起始目录中。如果找到了匹配的域或电子邮件地址，则会发送回复。如果没有找到，则不发送回复。

.vacation.filter 可能包含以下类似项：

```
company.com
mydomain.com
onefriend@hisisp.com
anotherfriend@herisp.com
```

请注意，每一行包含一个域或一个电子邮件地址。每项必须位于单独的一行中。要使发件人的电子邮件地址与某个电子邮件地址项匹配，除大小写之外，该匹配必须是精确匹配。发件人地址中的字母是大写还是小写将会忽略。要使发件人的电子邮件地址与某个域项匹配，该发件人的地址必须包含列出的域。例如，somebody@dept.company.com 和 someone@company.com 都可与域项 company.com 匹配。

有关更多信息，请参见 vacation(1) 手册页。

/usr/bin 目录的内容

下表显示了用于邮件服务的 /usr/bin 目录的内容。

名称	类型	说明
aliasadm	文件	用于处理 NIS+ 别名映射的程序。
mail	文件	用户代理。
mailcompat	文件	用于以 SunOS 4.1 邮箱格式存储邮件的过滤器。
mailq	文件	用于列出邮件队列内容的程序。
mailstats	文件	用于读取 /etc/mail/statistics 文件（如果存在）中存储的邮件统计信息的程序。
mailx	文件	用户代理。
mconnect	文件	用于连接至邮件程序以进行地址验证和调试的程序。
praliases	文件	用于“取消编译”别名数据库的命令。请参阅 praliases(1) 手册页中提供的取消编译信息。
rmail	符号链接	指向 /usr/bin/mail 的符号链接。通常用于仅允许发送邮件的命令。
vacation	文件	用于设置自动回复邮件的命令。

/etc/mail 目录的内容

下表显示了 /etc/mail 目录的内容。

名称	类型	说明
Mail.rc	文件	mailx 用户代理的缺省设置。
aliases	文件	邮件转发信息。
aliases.db	文件	通过运行 newaliases 创建的缺省二进制形式的邮件转发信息。
aliases.dir	文件	通过运行 newaliases 创建的二进制形式的邮件转发信息。仍然可以使用，但从 Solaris 9 发行版开始，缺省情况下不会再使用该文件。
aliases.pag	文件	通过运行 newaliases 创建的二进制形式的邮件转发信息。仍然可以使用，但从 Solaris 9 发行版开始，缺省情况下不会再使用该文件。
mailx.rc	文件	mailx 用户代理的缺省设置。
main.cf	符号链接	提供从主系统的此样例配置文件到 sendmail.cf 的符号链接是为了实现向下兼容。在 sendmail 版本 8.13 中，无需此文件。
relay-domains	文件	允许进行中继的所有域的列表。缺省情况下，仅本地域允许进行中继。
sendmail.cf	文件	用于邮件路由的配置文件。
submit.cf	文件	用于邮件提交程序 (mail submission program, MSP) 的新配置文件。有关更多信息，请参阅第 333 页中的 “sendmail 版本 8.12 中的配置文件 submit.cf”。
local-host-names	文件	在邮件主机的别名数太长时可以创建的可选文件。
helpfile	文件	SMTP HELP 命令使用的帮助文件。
sendmail.pid	文件	用于列出侦听守护进程的 PID 并且现在位于 /var/run 中的文件。
statistics	文件	sendmail 统计文件。如果存在此文件，sendmail 会记录通过每个邮件程序的流量。以前，此文件名为 sendmail.st。
subsidiary.cf	符号链接	提供从辅助系统的此样例配置文件到 sendmail.cf 的符号链接是为了实现向下兼容。在 sendmail 版本 8.13 中，无需此文件。

名称	类型	说明
trusted-users	文件	用于列出执行某些邮件操作时可信任的用户（每行一个用户）的文件。缺省情况下，此文件中仅包含 root。不可信用户执行某些邮件操作时，将产生以下警告：X-Authentication-Warning: header being added to a message。

/etc/mail/cf 目录的内容

/etc/mail 目录中有一个子目录 cf，其中包含生成 sendmail.cf 文件所需的全部文件。表 14–9 中显示了 cf 的内容。

从 Solaris 10 发行版开始，为支持只读的 /usr 文件系统，/usr/lib/mail 目录的内容已移至 /etc/mail/cf 目录。但是，请注意以下例外情况。Shell 脚本 /usr/lib/mail/sh/check-hostname 和 /usr/lib/mail/sh/check-permissions 现在位于 /usr/sbin 目录中。请参见第 310 页中的 “用于邮件服务的其他文件”。为了实现向下兼容，符号链接指向每个文件的新位置。

表 14–9 用于邮件服务的 /etc/mail/cf 目录的内容

名称	类型	说明
README	文件	介绍配置文件。
cf/main.cf	符号链接	从 Solaris 10 发行版起，此文件名链接至 cf/sendmail.cf。它是主配置文件。
cf/main.mc	符号链接	从 Solaris 10 发行版起，此文件名链接至 cf/sendmail.mc。它是用于创建主配置文件的文件。
cf/Makefile	文件	提供生成新配置文件的规则。
cf/submit.cf	文件	邮件提交程序 (mail submission program, MSP) 的配置文件，用于提交邮件。
cf/submit.mc	文件	它是用于生成 submit.cf 文件的文件。此文件定义邮件提交程序 (mail submission program, MSP) 的 m4 宏。
cf/sendmail.cf	文件	它是 sendmail 的主配置文件。
cf/sendmail.mc	文件	包含用于生成 sendmail.cf 文件的 m4 宏。
cf/subsidiary.cf	符号链接	从 Solaris 10 发行版起，此文件名链接至 cf/sendmail.cf。它是 NFS 挂载了其他主机中的 /var/mail 的主机的配置文件。

表 14–9 用于邮件服务的 /etc/mail/cf 目录的内容 （续）

名称	类型	说明
cf/subsidiary.mc	符号链接	从 Solaris 10 发行版起，此文件名链接至 cf/sendmail.mc。它包含用于生成 subsidiary.cf 文件的 m4 宏。
domain	目录	提供与站点相关的子域的说明。
domain/generic.m4	文件	来自 Berkeley 软件分发机构的普通域文件。
domain/solaris-antispam.m4	文件	域文件，可将 sendmail 的功能更改为类似于以前的 版本的 sendmail。但是完全禁用了中继，因此将拒绝没有主机名的发件人地址和无法解析的域。
domain/solaris-generic.m4	文件	缺省的域文件，可将 sendmail 的功能更改为类似于以前版本的 sendmail。
feature	目录	包含对特定主机的特定功能的定义。有关这些功能的完整说明，请参见 README。
m4	目录	包含与站点无关的头文件。
mailer	目录	包含邮件程序的定义，包括 local、smtp 和 uucp 的定义。
main-v7sun.mc	文件	过时：从 Solaris 10 发行版起，此文件名重命名为 cf/sendmail.mc。
ostype	目录	介绍各种操作系统环境。
ostype/solaris2.m4	文件	用于将缺省的本地邮件程序定义为 mail.local。
ostype/solaris2.ml.m4	文件	用于将缺省的本地邮件程序定义为 mail.local。
ostype/solaris2.pre5.m4	文件	用于将本地邮件程序定义为 mail。
ostype/solaris8.m4	文件	用于将本地邮件程序定义为 mail.local（在 LMTP 模式下），启用 IPv6，将 /var/run 指定为 sendmail.pid 文件的目录。
subsidiary-v7sun.mc	文件	过时：从 Solaris 10 发行版起，此文件名重命名为 cf/sendmail.mc。

/usr/lib 目录的内容

下表显示了用于邮件服务的 /usr/lib 目录的内容。

表 14–10 /usr/lib 目录的内容

名称	类型	说明
mail.local	文件	用于将邮件传送到邮箱的邮件程序。
sendmail	文件	路由程序，也称为邮件传输代理。
smrsh	文件	Shell 程序（限制 sendmail 的 shell），该程序使用 sendmail 的 "|program" 语法将 sendmail 可以运行的程序限制为 /var/adm/sm.bin 目录中列出的程序。有关对 /var/adm/sm.bin 中所包括内容的建议，请参阅 smrsh(1M) 手册页。要启用该程序，请在 mc 文件中包括以下 m4 命令：FEATURE('smrsh')。
mail	符号链接	指向 /etc/mail/cf 目录的符号链接。有关更多信息，请参阅第 308 页中的 "/etc/mail/cf 目录的内容"。

用于邮件服务的其他文件

如表 14–11 所示，还有几个其他文件和目录可用于邮件服务。

表 14–11 用于邮件服务的其他文件

名称	类型	说明
/etc/default/sendmail	文件	用于列出 sendmail 的启动脚本的环境变量。
/etc/shells	文件	用于列出有效的登录 shell。
/etc/mail/cf/sh	目录	包含 m4 生成过程和迁移帮助使用的 shell 脚本。
/usr/sbin/check-permissions	文件	用于检查 :include: 别名的权限以及 .forward 文件及其父目录路径是否具有正确权限。
/usr/sbin/check-hostname	文件	用于验证 sendmail 是否可确定全限定主机名。
/usr/sbin/editmap	文件	在数据库映射中查询和编辑用于 sendmail 的单个记录。
/usr/sbin/in.comsat	文件	邮件通知守护进程。
/usr/sbin/makemap	文件	生成二进制形式的加密映射。
/usr/sbin/newaliases	符号链接	指向 /usr/lib/sendmail 的符号链接。用于创建二进制形式的别名数据库。以前位于 /usr/bin 中。
/usr/sbin/syslogd	文件	sendmail 使用的错误消息记录程序。

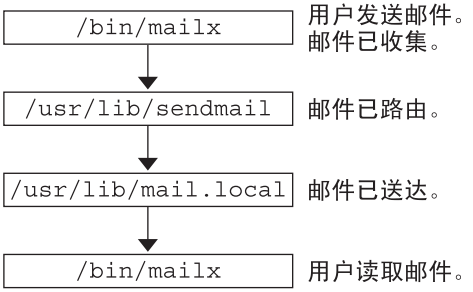
表 14–11 用于邮件服务的其他文件 （续）

名称	类型	说明
/usr/sbin/etrn	文件	用于启动客户端远程邮件队列的 Perl 脚本。
/usr/dt/bin/dtmail	文件	CDE（公用桌面环境）邮件用户代理
/var/mail/*mailbox1*, /var/mail/*mailbox2*	文件	用于已传送邮件的邮箱。
/var/spool/clientmqueue	目录	客户机守护进程传送的邮件的存储器。
/var/spool/mqueue	目录	主服务器守护进程传送的邮件的存储器。
/var/run/sendmail.pid	文件	用于列出侦听守护进程的 PID 的文件。

邮件程序的交互

邮件服务由以下程序的组合提供，这些程序按图 14–2 的简图中所示进行交互。

图 14–2 邮件程序的交互



下面对邮件程序的交互进行了说明。

1. 用户使用程序（如 mailx）发送邮件。有关更多信息，请参见 mailx(1) 手册页。
2. 邮件由生成它的程序收集，然后传递给 sendmail 守护进程。
3. sendmail 守护进程**解析**邮件中的地址（将其划分为可识别的段）。该守护进程使用配置文件 /etc/mail/sendmail.cf 中的信息来确定网络名的语法、别名、转发信息和网络拓扑。通过使用此信息，sendmail 可以确定邮件要到达收件人所必须采用的路由。
4. sendmail 守护进程将邮件传递给相应系统。
5. 本地系统中的 /usr/lib/mail.local 程序将邮件传送至邮件收件人在 /var/mail/*username* 目录中的邮箱。
6. 通知收件人邮件已到达，收件人使用 mail、mailx 或类似程序检索邮件。

sendmail 程序

以下列表介绍了 sendmail 程序的一些功能。

- sendmail 可以使用不同类型的通信协议，如 TCP/IP 和 UUCP。
- sendmail 可以实现 SMTP 服务器、邮件排队和邮件列表。
- sendmail 可以通过使用符合以下命名约定的模式匹配系统来控制名称解释。
  - 基于域的命名约定。通过域技术可以区分物理命名和逻辑命名问题。有关域的更多信息，请参阅第 298 页中的 “邮件地址”。
  - 临时技术，如提供对于其他网络中的主机而言看似位于本地的网络名。
  - 任意（早期）命名语法。
  - 完全不同的命名方案。

Solaris 操作系统使用 sendmail 程序作为邮件路由器。以下列表介绍了该程序的一些功能。

- sendmail 负责接收电子邮件并将其传送给本地传送代理，如 mail.local 或 procmail。
- sendmail 是一个邮件传输代理，用于接受来自用户代理（如 mailx 和 Mozilla 邮件）的邮件并通过 Internet 将其路由至目标。
- sendmail 控制用户以下列方式发送的电子邮件。
  - 确定收件人的地址
  - 选择合适的传送程序
  - 以传送代理可以处理的格式重写地址
  - 根据需要重新格式化邮件头
  - 最后将已转换的邮件传递给邮件程序以进行传送

有关 sendmail 程序的更多信息，请参阅以下主题。

- 第 312 页中的 “sendmail 及其重新路由机制”
- 第 314 页中的 “sendmail 功能”
- 第 314 页中的 “sendmail 配置文件”

sendmail 及其重新路由机制

sendmail 程序支持三种邮件重新路由机制。您选择的机制取决于涉及的更改类型。

- 服务器更改
- 域范围的更改
- 面向一个用户的更改

此外，您选择的重新路由机制还会影响所需要的管理级别。请考虑以下选项。

1. 一种重新路由机制是**别名**。

根据使用的文件类型，别名可在服务器范围内或名称服务范围内将名称映射到地址。

请考虑名称服务别名的以下优点和缺点。

- 使用名称服务别名文件允许从单个源中管理邮件重新路由更改。但是传播重新路由更改时，名称服务别名会产生延迟时间。
- 名称服务管理通常限制为一组选定的系统管理员。普通用户将不能管理此文件。

请考虑使用服务器别名文件的以下优点和缺点。

- 通过使用服务器别名文件，指定的服务器上能够成为 root 的任何用户都可管理重新路由。
- 传播重新路由更改时，服务器别名会产生很短的延迟时间或消除延迟时间。
- 更改仅会影响本地服务器，这在大多数邮件都发送至一台服务器时可以接受。但是，如果需要将此更改传播至许多邮件服务器，请使用名称服务。
- 普通用户将不能管理此更改。

有关更多信息，请参阅本章中的第 315 页中的 “邮件别名文件”。有关任务列表，请参阅第 13 章，邮件服务（任务）中的第 270 页中的 “管理邮件别名文件（任务列表）”。

2. 第二种机制是**转发**。

   通过此机制，用户可以管理邮件重新路由。本地用户可将其传入邮件重新路由至以下位置。

   - 其他邮箱
   - 不同的邮件程序
   - 其他邮件主机

   通过使用 .forward 文件可支持此机制。有关这些文件的更多信息，请参阅本章中的第 318 页中的 “.forward 文件”。有关任务列表，请参阅第 13 章，邮件服务（任务）中的第 282 页中的 “管理 .forward 文件（任务列表）”。

3. 最后一种重新路由机制是**包含**。

   通过此机制，用户可维护别名列表而不会要求 root 访问。要提供此功能，root 用户必须在服务器上的别名文件中创建相应的项。创建该项之后，用户即可根据需要重新路由邮件。有关包含的更多信息，请参阅本章中的第 315 页中的 “/etc/mail/aliases 文件”。有关任务列表，请参阅第 13 章，邮件服务（任务）中的第 270 页中的 “管理邮件别名文件（任务列表）”。

注 – 读取邮件的程序（如 /usr/bin/mailx）可以有自己的别名，该别名在邮件到达 sendmail 之前会进行扩展。sendmail 的别名可以来自许多名称服务源，如本地文件、NIS 或 NIS+。查找的顺序由 nsswitch.conf 文件确定。请参阅 nsswitch.conf(4)手册页。

---

sendmail 功能

sendmail 程序提供了以下功能。

- sendmail 很可靠。该程序旨在正确传送每封邮件。任何邮件都不会完全丢失。
- sendmail 会尽可能使用现有软件进行传送。例如，用户会与邮件生成程序和邮件发送程序进行交互。提交邮件时，邮件生成程序会调用 sendmail，后者将邮件路由至正确的邮件程序。由于有些发送器可能是网络服务器，有些邮件程序可能是网络客户机，因此可将 sendmail 用作 Internet 邮件网关。有关该过程的更详细说明，请参见第 311 页中的 “邮件程序的交互”。
- 可将 sendmail 配置为用于包括多个网络的复杂环境。sendmail 会检查地址的内容及其语法，以确定要使用的邮件程序。
- sendmail 使用配置文件来控制邮件配置，而不要求将该配置信息编译成代码。
- 用户可以维护各自的邮件列表。此外，各用户还可以指定各自的转发机制，而无需修改域范围的别名文件，该文件通常位于 NIS 或 NIS+ 维护的域范围别名中。
- 每个用户可以指定定制邮件程序，以处理传入邮件。定制邮件程序可以提供返回内容为 "I am on vacation." 等类似邮件的功能。有关更多信息，请参见 vacation(1) 手册页。
- sendmail 可将地址批处理至单独一台主机，以减少网络通信流量。

sendmail 配置文件

配置文件控制 sendmail 执行其功能的方法。配置文件可确定要选择的传送代理、地址重写规则以及邮件头格式。sendmail 程序使用 /etc/mail/sendmail.cf 文件中的信息来执行其功能。

Solaris 操作系统在 /etc/mail 目录中提供了两个缺省配置文件。

1. sendmail.cf，用于在守护进程模式下运行 sendmail 的配置文件。
2. submit.cf，用于在邮件提交程序模式而非守护进程模式下运行 sendmail 的配置文件。有关更多信息，请参阅第 333 页中的 “sendmail 版本 8.12 中的配置文件 submit.cf”。

设置邮件客户机、邮件服务器、邮件主机或邮件网关时，请考虑以下情况：

- 对于邮件客户机或邮件服务器，无需执行任何操作即可设置或编辑缺省配置文件。
- 要设置邮件主机或邮件网关，需要设置邮件配置所需的中继邮件程序和中继主机参数。有关任务信息，请参阅第 13 章，邮件服务（任务）中的第 253 页中的 “设置邮件服务（任务列表）”或第 261 页中的 “更改 sendmail 配置”。请注意，在 sendmail 版本 8.13 中，不再需要 main.cf 文件。

以下列表介绍了可以根据站点的要求来更改的一些配置参数。

- 时间值，用于指定以下信息。
  - 读取超时。

  - 将邮件返回给发件人之前，该邮件在队列中保持未传送状态的时间长度。请参阅第 343 页中的 “sendmail 版本 8.12 中新增的队列功能”。有关任务列表，请参阅第 279 页中的 “管理队列目录（任务列表）”。
- 传送模式，用于指定传送邮件的快速程度。
- 负荷限制，可在繁忙期间提高效率。这些参数可防止 sendmail 尝试传送大型邮件、向许多收件人传送邮件以及向已长时间关闭的站点传送邮件。
- 日志级别，用于指定记录的问题的种类。

邮件别名文件

可以使用以下任何文件、映射或表来维护别名。

- 第 315 页中的 “.mailrc 别名”
- 第 315 页中的 “/etc/mail/aliases 文件”
- 第 317 页中的 “NIS aliases 映射”
- 第 317 页中的 “NIS+ mail_aliases 表”

维护别名的方法取决于使用别名的用户以及需要可更改别名的用户。每种别名类型都具有唯一的格式要求。

如果要查找任务信息，请参阅第 13 章，邮件服务（任务）中的第 270 页中的 “管理邮件别名文件（任务列表）”。

.mailrc 别名

.mailrc 文件中列出的别名仅能由拥有该文件的用户进行访问。借助此限制，用户可以建立由其控制并且仅能由所有者使用的别名文件。.mailrc 文件中的别名遵循以下格式。

alias *aliasname value value value* ...

aliasname 是用户发送邮件时使用的名称，*value* 是有效的电子邮件地址。

如果用户为 scott 建立的个人别名在名称服务中与 scott 的电子邮件地址不匹配，则会出现错误。他人尝试回复此用户生成的邮件时，邮件会路由至错误的人员。唯一的解决方法是使用其他任一别名机制。

/etc/mail/aliases 文件

知道别名名称和包含该文件的系统的主机名的任何用户都可以使用 /etc/mail/aliases 文件中建立的任何别名。本地 /etc/mail/aliases 文件中的分发列表格式遵循以下格式。

aliasname: *value,value,value* ...

aliasname 是用户向此别名发送邮件时使用的名称，*value* 是有效的电子邮件地址。

如果网络未运行名称服务，则每个系统的 `/etc/mail/aliases` 文件都应包含用于所有邮件客户机的项。可以在每个系统中编辑该文件，也可在一个系统中编辑该文件，然后再将其复制到其他所有系统中。

`/etc/mail/aliases` 文件中的别名以文本形式存储。编辑 `/etc/mail/aliases` 文件时，需要运行 `newaliases` 程序。此程序将重新编译数据库并使别名可以二进制形式供 `sendmail` 程序使用。有关任务信息，请参阅第 13 章，邮件服务（任务）中的第 275 页中的 “如何设置本地邮件别名文件”。或者，也可以使用 Solaris Management Console 中的邮件列表功能来管理本地 `/etc` 文件中存储的邮件别名。

可以仅为本地名称（当前主机名或无主机名）创建别名。例如，如果用户 `ignatz` 在系统 `saturn` 中有一个邮箱，则 `/etc/mail/aliases` 文件中可包含该用户的以下别名项。

```
ignatz: ignatz@saturn
```

应为每台邮件服务器创建一个管理帐户。创建此类帐户的方法是在邮件服务器上为 `root` 指定一个邮箱并在 `/etc/mail/aliases` 文件中为 `root` 添加一项。例如，如果系统 `saturn` 是邮箱服务器，则可向 `/etc/mail/aliases` 文件中添加项 `root: sysadmin@saturn`。

通常，仅有 `root` 用户才能编辑此文件。但是，使用 Solaris Management Console 时，组 14（sysadmin 组）中的所有用户都可以更改该本地文件。另外，还可选择创建以下项。

aliasname`: :include:`*/path/aliasfile*

aliasname 是用户在发送邮件时使用的名称，*/path/aliasfile* 是包含别名列表的文件的全路径。该别名文件应包括电子邮件项（每行一项），并且不包括任何其他符号。

user1@host1
user2@host2

可在 `/etc/mail/aliases` 中定义附加的邮件文件，以保留日志或备份副本。以下项会将发送给 *aliasname* 的所有邮件都存储在 *filename* 中。

aliasname`: /home/backup/`*filename*

另外，还可以将邮件路由至其他进程。以下示例将邮件副本存储在 *filename* 中并列出副本。

aliasname`: "|tee -a /home/backup/`*filename*` |lp"`

有关任务列表，请参阅第 13 章，邮件服务（任务）中的第 270 页中的 “管理邮件别名文件（任务列表）”。

NIS aliases 映射

本地域中的所有用户都可以使用 NIS aliases 映射中的各项。原因是 sendmail 程序可以使用 NIS aliases 映射而非本地 /etc/mail/aliases 文件来确定邮件地址。有关更多信息，请参阅 nsswitch.conf(4)手册页。

NIS aliases 映射中的别名遵循以下格式。

aliasname: *value,value,value* ...

aliasname 是用户发送邮件时使用的名称，*value* 是有效的电子邮件地址。

NIS aliases 映射应包含用于所有邮件客户机的各项。通常，只有 NIS 主服务器中的 root 用户才能更改这些项。对于经常更改的别名，最好不要选择此类型。但是，如果这些别名指向其他别名文件，则这类别名将很有用，如以下语法示例所示。

aliasname: *aliasname@host*

aliasname 是用户发送邮件时使用的名称，*host* 是包含 /etc/mail/alias 文件的服务器的主机名。

有关任务信息，请参阅第 13 章，邮件服务（任务）中的第 274 页中的 “如何设置 NIS mail.aliases 映射”。

NIS+ mail_aliases 表

NIS+ mail_aliases 表包含在本地域中用于标识系统或个人的名称。sendmail 程序可以使用 NIS+ mail_aliases 表而非本地 /etc/mail/aliases 文件来确定邮件地址。有关更多信息，请参阅 aliasadm(1M) 和 nsswitch.conf(4) 手册页。

NIS+ mail_aliases 表中的别名遵循以下格式：

alias: *expansion* # ["*options*" # "*comments*"]

表 14–12 介绍了 NIS+ mail_aliases 表中的四列。

表 14–12 NIS+ mail_aliases 表中的各列

列	说明
alias	别名的名称
expansion	别名或别名列表的值，与 sendmail /etc/mail/aliases 文件中显示的值一样
options	保留供将来使用的列
comments	有关单个别名的注释列

NIS+ mail_aliases 表应包含用于所有邮件客户机的项。可以使用 aliasadm 命令列出、创建、修改和删除 NIS+ aliases 表中的各项。要使用 aliasadm 命令，您必须是拥有 aliases 表的 NIS+ 组的成员。有关任务信息，请参阅第 13 章，邮件服务（任务）中的第 270 页中的 “管理邮件别名文件（任务列表）”。或者，也可以使用 Solaris Management Console 来管理 NIS+ 邮件别名。

注 – 如果要创建新的 NIS+ aliases 表，必须在创建项之前先初始化该表。如果该表已存在，则无需进行初始化。

.forward 文件

用户可在其起始目录中创建一个 .forward 文件，以供 sendmail 以及其他程序用于重定向邮件或发送邮件。请参阅以下主题。

- 第 318 页中的 “应避免的情况”
- 第 318 页中的 “对 .forward 文件的控制”
- 第 319 页中的 “.forward.*hostname* 文件”
- 第 319 页中的 “.forward+*detail* 文件”

有关任务列表，请参阅第 13 章，邮件服务（任务）中的第 282 页中的 “管理 .forward 文件（任务列表）”。

应避免的情况

以下列表介绍了可以避免或轻松解决问题的一些情况。

- 如果邮件未传送至预期的地址，请检查该用户的 .forward 文件。用户可能已将 .forward 文件放入了 host1 的起始目录，该文件会将邮件转发至 user@host2。邮件到达 host2 时，sendmail 会在 NIS 或 NIS+ 别名中检查 user 并将邮件发回至 user@host1。此路由将产生循环以及更多退回的邮件。
- 要避免安全问题，请勿将 .forward 文件放在 root 和 bin 帐户中。如有必要，请改用 aliases 文件转发邮件。

对 .forward 文件的控制

要使 .forward 文件成为邮件传送中的有效部分，请确保正确应用以下控制（主要是权限设置）。

- .forward 文件必须只能由文件所有者写入。此限制可以防止其他用户破坏安全性。
- 至起始目录的路径必须只能由 root 拥有和写入。例如，如果 .forward 文件位于 /export/home/terry 中，则 /export 和 /export/home 必须只能由 root 拥有和写入。
- 实际起始目录应只能由用户写入。
- .forward 文件不能是符号链接，并且此文件不能包含多个硬链接。

.forward.hostname 文件

可以创建 .forward. *hostname* 文件以重定向发送给特定主机的邮件。例如，如果用户的别名已从 sandy@phoenix.example.com 更改为 sandy@example.com，请在 sandy 的起始目录中放入一个 .forward.phoenix 文件。

```
% cat .forward.phoenix
sandy@example.com
"|/usr/bin/vacation sandy"
% cat .vacation.msg
From: sandy@example.com (via the vacation program)
Subject: my alias has changed

My alias has changed to sandy@example.com.
Please use this alias in the future.
The mail that I just received from you
has been forwarded to my new address.

Sandy
```

在本示例中，在通知发件人发生别名更改后，可将邮件转发至正确地址。由于 vacation 程序仅允许一个邮件文件，因此每次仅能转发一封邮件。但是，如果邮件不是特定于主机，则 .forward 文件可将一个休假邮件文件用于多台主机。

.forward+detail 文件

对转发机制的另一种扩展是 .forward+*detail* 文件。*detail* 字符串可以是除运算符字符之外的任意字符序列。运算符字符包括 .:%&!^[]+。通过使用此类型的文件，可以确定是否有其他人在您不知情的情况下使用您的电子邮件地址。例如，如果某个用户告诉其他人使用电子邮件地址 sandy+test1@example.com，该用户将能够识别将来传送给此别名的任何邮件。缺省情况下，将根据别名和 .forward+*detail* 文件对发送至 sandy+test1@example.com 别名的所有邮件进行检查。如果未找到任何匹配项，邮件将转而传送至 sandy@example.com，但用户可以看到 To: 邮件头中的更改。

/etc/default/sendmail 文件

此文件用于存储 sendmail 的启动选项，以免在升级主机时删除这些选项。可以使用以下变量。

CLIENTOPTIONS="*string*"
: 选择要用于客户机守护进程的其他选项，该守护进程会查看仅客户机队列 (/var/spool/clientmqueue) 并可用作客户机队列运行程序。不会进行任何语法检查，因此在更改此变量时请务必小心。

CLIENTQUEUEINTERVAL=#
: 与 QUEUEINTERVAL 选项类似，CLIENTQUEUEINTERVAL 用于设置邮件队列运行的时间间隔。但是，CLIENTQUEUEINTERVAL 选项将控制客户机守护进程的功能而非主服务器守护进程的功能。通常，主服务器守护进程可将所有邮件都传送至 SMTP 端口。但

是，如果邮件负荷过高或主服务器守护进程未运行，则邮件会进入仅客户机队列 `/var/spool/clientmqueue`。然后，检查仅客户机队列的客户机守护进程将用作客户机队列处理器。

ETRN_HOSTS="*string*"
可使 SMTP 客户机和服务器立即交互，而无需等待达到队列运行间隔，该间隔是周期性的。服务器可以立即传送队列中转至指定主机的部分。有关更多信息，请参阅 `etrn(1M)` 手册页。

MODE=-bd
选择用于启动 `sendmail` 的模式。使用 `-bd` 选项或不予以定义。

OPTIONS=*string*
选择要用于主服务器守护进程的其他选项。不会进行任何语法检查，因此在更改此变量时请务必小心。

QUEUEINTERVAL=#
设置邮件队列在主服务器守护进程中的运行间隔。`#` 可以是一个正整数，后跟 `s`（秒）、`m`（分钟）、`h`（小时）、`d`（天）或 `w`（星期）。在启动 `sendmail` 之前会先检查语法。如果间隔为负或者该项不是以合适字母结尾，则会忽略该间隔，`sendmail` 将以 15 分钟的队列间隔启动。

QUEUEOPTIONS=p
启用一个在队列运行间隔之间休眠的持久性队列运行程序，而不是为每个队列运行间隔启用一个新队列运行程序。可将此选项设置为 `p`，这是唯一可用的设置。否则，将不设置此选项。

邮件地址和邮件路由

邮件在传送过程中所遵循的路径取决于客户机系统的设置以及邮件域的拓扑。邮件主机或邮件域每增加一个级别，便需要多进行一次别名解析，但路由过程在大多数主机上基本相同。

可将客户机系统设置为在本地接收邮件。在本地接收邮件即是在本地模式下运行 `sendmail`。本地模式是所有邮件服务器和一些客户机的缺省模式。在本地模式下的邮件服务器或邮件客户机上，邮件通过以下方式进行路由。

注 – 以下示例假定您使用的是 `sendmail.cf` 文件中设置的缺省规则。

---

1. 如果可能，请扩展邮件别名，并重新启动本地路由进程。

   邮件地址是通过检查名称服务中的邮件别名并替换新值（如果找到新值）来扩展的。随后会再次检查此新别名。

2. 如果邮件是本地的，则将其传送至 `/usr/lib/mail.local`。

   邮件将传送至本地邮箱。

3. 如果邮件地址中包括此邮件域内的一台主机，则将邮件传送至该主机。

4. 如果地址中不包括此域内的主机，则将邮件转发至邮件主机。

   邮件主机使用与邮件服务器相同的路由进程。但是，邮件主机可以接收发往域名以及主机名的邮件。

sendmail 与名称服务的交互

本节介绍应用于 sendmail 和名称服务的域名。此外，本节还介绍了有效使用名称服务的规则以及 sendmail 与名称服务的特定交互。有关详细信息，请参阅以下主题。

- 第 321 页中的 “sendmail.cf 和邮件域”
- 第 321 页中的 “sendmail 和名称服务”
- 第 322 页中的 “NIS 与 sendmail 的交互”
- 第 323 页中的 “sendmail 与 NIS 和 DNS 的交互”
- 第 324 页中的 “NIS+ 与 sendmail 的交互”
- 第 324 页中的 “sendmail 与 NIS+ 和 DNS 的交互”

如果要查找相关的任务信息，请参阅第 13 章，邮件服务（任务）中的第 260 页中的 “如何使用 DNS 和 sendmail”或第 270 页中的 “管理邮件别名文件（任务列表）”。

sendmail.cf 和邮件域

标准的 sendmail.cf 文件使用邮件域来确定是直接传送邮件还是通过邮件主机传送邮件。域内邮件通过直接的 SMTP 连接传送，而域间邮件则会转发至邮件主机。

在安全网络中，仅会对少数选定的主机进行授权，允许其生成向外部目标发送的包。即使主机具有邮件域外部的远程主机的 IP 地址，也不能保证可以建立 SMTP 连接。标准的 sendmail.cf 假定以下情况成立。

- 未授权当前主机直接向邮件域外部的主机发送包。
- 邮件主机能够将邮件转发给授权主机，该主机可以直接将包传输给外部主机。实际上，邮件主机可以是授权主机。

通过这些假设，邮件主机将负责传送或转发域间邮件。

sendmail 和名称服务

sendmail 可对名称服务强加各种要求。为增强您对这些要求的理解，本节将首先介绍邮件域与名称服务域之间的关系。然后，本节会介绍各种要求。请参阅以下主题。

- 第 322 页中的 “邮件域和名称服务域”
- 第 322 页中的 “名称服务的要求”
- NIS+(1)、nisaddent(1M) 和 nsswitch.conf(4) 的手册页

邮件域和名称服务域

邮件域名必须是名称服务域名的后缀。例如，如果名称服务的域名为 A.B.C.D，则邮件域名可能是以下各项之一。

- A.B.C.D
- B.C.D
- C.D
- D

最初建立时，邮件域名通常与名称服务域名相同。随着网络规模的变大，名称服务域可以划分为几个较小的部分，以使名称服务更易于管理。但是，为提供一致的别名，邮件域通常保持不划分状态。

名称服务的要求

本节介绍 sendmail 对名称服务强加的要求。

必须在名称服务中设置主机表或映射，才能支持三种类型的 gethostbyname() 查询。

- mailhost－部分名称服务配置会自动满足此要求。
- 完整主机名（例如，smith.admin.acme.com）－许多名称服务配置都满足此要求。
- 短主机名（例如 smith）－sendmail 必须连接至邮件主机，才能转发外部邮件。要确定邮件地址是否位于当前邮件域内，可使用完整主机名调用 gethostbyname()。如果找到该项，则将地址视为内部地址。

  NIS、NIS+ 和 DNS 都支持 gethostbyname() 以短主机名作为参数，因此会自动满足这一要求。

还需要遵循有关主机名服务的其他两条规则，才能在名称服务内建立有效的 sendmail 服务。

- gethostbyname() 在使用完整主机名参数和短主机名参数时应产生一致的结果。例如，如果从邮件域 admin.acme.com 中调用 gethostbyname(smith.admin.acme.com) 和 gethostbyname(smith)，则这两个函数应返回相同结果。
- 对于通用邮件域下的所有名称服务域，使用短主机名的 gethostbyname() 应产生相同结果。例如，如果给定邮件域 smith.admin.acme.com，则当调用来自 ebb.admin.acme.com 域或 esg.admin.acme.com 域时，gethostbyname(smith) 应返回相同结果。邮件域名通常比名称服务域名短，这样此要求针对各种名称服务可具有特殊含义。

有关 gethostbyname() 函数的更多信息，请参阅 gethostbyname(3NSL) 手册页。

NIS 与 sendmail 的交互

以下列表介绍了 sendmail 与 NIS 的交互并提供了一些指导。

- **邮件域名** – 如果要将 NIS 设置为主名称服务，则 sendmail 会自动去除 NIS 域名的第一个组成部分并使用剩下的部分作为邮件域名。例如，ebs.admin.acme.com 将成为 admin.acme.com。
- **邮件主机名** – 必须在 NIS 主机映射中具有一个 mailhost 项。
- **完整主机名** – 标准的 NIS 设置不能“识别”完整主机名。此设置不会尝试使 NIS 识别完整主机名，而是通过编辑 sendmail.cf 文件并使用 %y 替换出现的所有 %l，从 sendmail 端取消此要求。此更改将关闭 sendmail 的域间邮件检测。如果目标主机可以解析为一个 IP 地址，则会尝试直接进行 SMTP 传送。请确保 NIS 主机映射不包含在当前邮件域之外的任何主机项。否则，需要进一步定制 sendmail.cf 文件。
- **匹配完整主机名和短主机名** – 请遵循前面有关如何为完整主机名禁用 gethostbyname() 的说明。
- **多个 NIS 域在一个邮件域中** – 一个通用邮件域下的所有 NIS 主机映射应具有同一组主机项。例如，ebs.admin.acme.com 域中的主机映射应该与 esg.admin.acme.com 中的主机映射相同。否则，一个地址可能可在一个 NIS 域中正常使用，但是无法用于其他 NIS 域。

有关任务信息，请参阅第 13 章，邮件服务（任务）中的第 270 页中的 “管理邮件别名文件（任务列表）”。

sendmail 与 NIS 和 DNS 的交互

以下列表介绍了 sendmail 与 NIS 和 DNS 的交互并提供了一些指导。

- **邮件域名** – 如果要将 NIS 设置为主名称服务，则 sendmail 会自动去除 NIS 域名的第一个组成部分并使用剩下的部分作为邮件域名。例如，ebs.admin.acme.com 将成为 admin.acme.com。
- **邮件主机名** – 启用 DNS 转发功能时，对 NIS 无法解析的查询将转发至 DNS，因此在 NIS 主机映射中无需 mailhost 项。
- **完整主机名** – 尽管 NIS 不能“识别”完整主机名，但 DNS 可以识别。如果遵循设置 NIS 和 DNS 的常规过程，则会满足此要求。
- **匹配完整主机名和短主机名** – 对于 NIS 主机表中的每个主机项，必须在 DNS 中具有对应的主机项。
- **多个 NIS 域在一个邮件域中** – 一个通用邮件域下的所有 NIS 主机映射应具有同一组主机项。例如，ebs.admin.acme.com 域中的主机映射应该与 esg.admin.acme.com 域中的主机映射相同。否则，一个地址可能可在一个 NIS 域中正常使用，但是无法用于其他 NIS 域。

有关任务信息，请参阅第 13 章，邮件服务（任务）中的第 260 页中的 “如何使用 DNS 和 sendmail”和第 270 页中的 “管理邮件别名文件（任务列表）”。

NIS+ 与 sendmail 的交互

以下列表介绍了 sendmail 与 NIS+ 的交互并提供了一些指导。

- **邮件域名** – 如果要将 NIS+ 设置为主名称服务，sendmail 可检查 NIS+ sendmailvars 表中的邮件域。此 NIS+ 表包含一个关键字列和一个值列。要设置邮件域，必须向该表中添加一项。此项应将关键字列设置为字符串 maildomain，将值列设置为邮件域名。例如 admin.acme.com。尽管 NIS+ 允许 sendmailvars 表中包含任何字符串，但要使邮件系统正常工作，仍需应用后缀规则。可以使用 nistbladm 将 maildomain 项添加到 sendmailvars 表中。请注意，在以下示例中，邮件域是 NIS+ 域的后缀。

  ```
  nistbladm -A key="maildomain" value=<mail domain> sendmailvars.org_dir.<NIS+ domain>
  ```

- **Mailhost 主机名** – 必须在 NIS+ 主机表中具有一个 mailhost 项。
- **完整主机名** – NIS+ 可以“识别”完整主机名。遵循常规的 NIS+ 设置过程即可满足此要求。
- **匹配完整主机名和短主机名** – 要满足此要求，可以复制主机表中的项。或者，也可以将用户名称服务域中的所有主机项都输入到邮件域级别的主主机表中。
- **多个 NIS 域在一个邮件域中** – 要满足此要求，可复制所有主机表中的项。或者，也可以将用户名称服务域中的所有主机项都输入到邮件域级别的主主机表中。比较有效的方法是，将多个逻辑或物理主机表合并为一个主机表。因此，在共享一个通用邮件域的多个名称服务域中，不能重用相同的主机名。

有关任务信息，请参阅第 13 章，邮件服务（任务）中的第 270 页中的 “管理邮件别名文件（任务列表）”。

sendmail 与 NIS+ 和 DNS 的交互

以下列表介绍了 sendmail 与 NIS+ 和 DNS 的交互并提供了一些指导。

- **邮件域名** – 如果要将 NIS+ 设置为主名称服务，sendmail 可检查 NIS+ sendmailvars 表中的邮件域。此 NIS+ 表包含一个关键字列和一个值列。要设置邮件域，必须向该表中添加一项。此项应将关键字列设置为字符串 maildomain，将值列设置为邮件域名。例如 admin.acme.com。尽管 NIS+ 允许 sendmailvars 表中包含任何字符串，但要使邮件系统正常工作，仍需应用后缀规则。可以使用 nistbladm 将 maildomain 项添加到 sendmailvars 表中。请注意，在以下示例中，邮件域是 NIS+ 域的后缀。

  ```
  nistbladm -A key="maildomain" value=<mail domain> sendmailvars.org_dir.<NIS+ domain>
  ```

- **Mailhost 主机名** – 如果网络同时使用 NIS+ 和 DNS 作为主机数据库源，则可将 mailhost 项放入 NIS+ 或 DNS 主机表中。请确保用户在 /etc/nsswitch.conf 文件中同时包括 NIS+ 和 DNS 作为主机数据库源。
- **完整主机名** – NIS+ 和 DNS 都可以“识别”完整主机名。遵循常规 NIS+ 和 DNS 设置过程即可满足此要求。

- **匹配完整主机名和短主机名** – 对于 NIS+ 主机表中的每个主机项，必须在 DNS 中具有对应的主机项。
- **多个 NIS 域在一个邮件域中** – 要满足此要求，可复制所有主机表中的项。或者，也可以将用户名称服务域中的所有主机项都输入到邮件域级别的主主机表中。

有关任务信息，请参阅第 13 章，邮件服务（任务）中的第 270 页中的 “管理邮件别名文件（任务列表）”和第 260 页中的 “如何使用 DNS 和 sendmail”。

sendmail 版本 8.13 中的更改

虽然此新版 sendmail 提供了许多新增功能，但最重要的还是其中的 FallBackSmartHost 选项。由于此选项，您无需再使用 main.cf 和 subsidiary.cf。main.cf 文件用于支持 MX 记录的环境。subsidiary.cf 文件用于不具备完全功能的 DNS 的环境。上述环境使用智能主机，不使用 MX 记录。FallBackSmartHost 选项可提供统一的配置。此选项的作用与所有环境最不可能首选的 MX 记录类似。要确保邮件传送到客户机，此选项（如果启用）需提供一台正确连接的（或智能）主机，此主机将用作出现故障的 MX 记录的备份（或故障转移）。

有关版本 8.13 的更多信息，请参见以下各节：

- 第 330 页中的 “sendmail 版本 8.13 中新增的命令行选项”
- 第 330 页中的 “sendmail 版本 8.13 中新增和修订的配置文件选项”
- 第 332 页中的 “sendmail 版本 8.13 中新增和修订的 FEATURE() 声明”

此外，从 Solaris 10 1/06 发行版开始，SMTP 运行时可以使用传输层安全性 (Transport Layer Security, TLS)。请参见以下说明。

sendmail 版本 8.13 支持运行 SMTP 时使用 TLS

SMTP 服务器和客户机之间的通信通常不受任何一端的控制或信任。由于缺少安全性，第三方可能会监视甚至修改服务器与客户机之间的通信。要解决此问题，在 sendmail 版本 8.13 中，SMTP 可以使用传输层安全性 (Transport Layer Security, TLS)。SMTP 服务器和客户机的这种扩展服务可提供以下功能：

- Internet 中专用的、经过验证的通信
- 保护不受窃听者和攻击者的攻击

注 – TLS 的实现基于安全套接字层 (Secure Sockets Layer, SSL) 协议。

STARTTLS 是使用 TLS 启动安全 SMTP 的 SMTP 关键字。此安全连接可能建立在两台服务器之间或一台服务器与一台客户机之间。安全连接定义如下：

- 源电子邮件地址和目标电子邮件地址都已加密。
- 电子邮件的内容已加密。

当客户机发出 STARTTLS 命令时，服务器将使用以下各项之一来响应：

- `220 Ready to start TLS`
- `501 Syntax error (no parameters allowed)`
- `454 TLS not available due to temporary reason`

220 响应要求客户机启动 TLS 协商。501 响应指明客户机未正确发出 STARTTLS 命令。发出 STARTTLS 时未使用任何参数。454 响应需要客户机应用规则集值来确定是接受还是维护连接。

请注意，要维护 Internet 的 SMTP 基础结构，公共使用的服务器决不能要求 TLS 协商。但是，专用服务器可能会要求客户机执行 TLS 协商。在这类情况下，服务器会返回以下响应：

```
530 Must issue a STARTTLS command first
```

530 响应会指示客户机发出 STARTTLS 命令，以建立连接。

如果不满足身份验证和保密性的级别，服务器或客户机可以拒绝连接。同样，由于大多数 SMTP 连接都不安全，因此服务器和客户机可能会保留不安全的连接。保留还是拒绝连接由服务器和客户机的配置来确定。

缺省情况下，不支持在运行 SMTP 时使用 TLS。SMTP 客户机发出 STARTTLS 命令时，将启用 TLS。必须先设置允许 sendmail 使用 TLS 的证书，然后 SMTP 客户机才能发出此命令。请参见第 264 页中的 “设置 SMTP 以使用 TLS”。请注意，此过程包括定义新的配置文件选项和重新生成 sendmail.cf 文件。

用于在运行 SMTP 时使用 TLS 的配置文件选项

下表介绍了用于在运行 SMTP 时使用 TLS 的配置文件选项。如果要声明其中的任何选项，请使用以下语法之一：

- `O` *OptionName*`=` *argument* `# for the configuration file`
- `-O` *OptionName*`=` *argument* `# for the command line`
- `define(`‘*m4Name*', *argument*`) # for m4 configuration`

表 14–13 用于在运行 SMTP 时使用 TLS 的配置文件选项

选项	说明
CACertFile	m4 名称：confCACERT 参数：*filename* 缺省值：未定义 用于标识包含一个 CA 证书的文件。
CACertPath	m4 名称：confCACERT_PATH 参数：*path* 缺省值：未定义 用于标识包含 CA 证书的目录的路径。
ClientCertFile	m4 名称：confCLIENT_CERT 参数：*filename* 缺省值：未定义 用于标识包含客户机证书的文件。请注意，此证书在 sendmail 用作客户机时使用。
ClientKeyFile	m4 名称：confCLIENT_KEY 参数：*filename* 缺省值：未定义 用于标识包含属于客户机证书的私钥的文件。
CRLFile	m4 名称：confCRL 参数：*filename* 缺省值：未定义 用于标识包含证书撤销状态的文件，该文件用于 X.509v3 身份验证。
DHParameters	m4 名称：confDH_PARAMETERS 参数：*filename* 缺省值：未定义 用于标识包含 Diffie-Hellman (DH) 参数的文件。

表 14–13 用于在运行 SMTP 时使用 TLS 的配置文件选项 （续）

选项	说明
RandFile	m4 名称：confRAND_FILE 参数：file:*filename* 或 egd:*UNIX socket* 缺省值：未定义 使用 file: 前缀标识包含随机数据的文件，或使用 egd: 前缀标识 UNIX 套接字。请注意，由于 Solaris OS 支持**随机**数生成器设备，因此无需指定此选项。请参见 random(7D) 手册页。
ServerCertFile	m4 名称：confSERVER_CERT 参数：*filename* 缺省值：未定义 用于标识包含服务器证书的文件。此证书在 sendmail 用作服务器时使用。
Timeout.starttls	m4 名称：confTO_STARTTLS 参数：*amount of time* 缺省值：1h 设置 SMTP 客户机等待 STARTTLS 命令的响应的时间。
TLSSrvOptions	m4 名称：confTLS_SRV_OPTIONS 参数：V 缺省值：未定义 用于确定服务器是否向客户机请求证书。如果此选项设置为 V，则不执行客户机验证。

要使 sendmail 支持 SMTP 使用 TLS，必须定义以下选项：

- CACertPath
- CACertFile
- ServerCertFile
- ClientKeyFile

不需要定义其他选项。

用于在运行 SMTP 时使用 TLS 的宏

下表介绍了 STARTTLS 命令使用的宏。

表 14–14 用于在运行 SMTP 时使用 TLS 的宏

宏	说明
`${cert_issuer}`	保存证书颁发机构 (certification authority, CA)（证书签发者）的标识名 (distinguished name, DN)。
`${cert_subject}`	保存名为**证书主题**的证书 DN。
`${cn_issuer}`	保存 CA 的公用名称 (common name, CN)，即**证书签发者**。
`${cn_subject}`	保存名为**证书主题**的证书 CN。
`${tls_version}`	保存用于连接的 TLS 的版本。
`${cipher}`	保存用于连接的一组加密算法（名为**加密套件**）。
`${cipher_bits}`	以位为单位保存用于连接的对称加密算法的密钥长度。
`${verify}`	保存所提供证书的验证结果。可能值如下所示： ■ `OK`－验证成功。 ■ `NO`－未提供证书。 ■ `NOT`－未请求证书。 ■ `FAIL`－无法验证提供的证书。 ■ `NONE`－尚未执行 `STARTTLS`。 ■ `TEMP`－出现临时错误。 ■ `PROTOCOL`－出现 SMTP 错误。 ■ `SOFTWARE`－`STARTTLS` 握手失败。
`${server_name}`	保存当前具有外出 SMTP 连接的服务器的名称。
`${server_addr}`	保存当前具有外出 SMTP 连接的服务器的地址。

用于在运行 SMTP 时使用 TLS 的规则集

下表介绍了一些规则集，用于确定应接受、继续还是拒绝使用 TLS 的 SMTP 连接。

表 14–15 用于在运行 SMTP 时使用 TLS 的规则集

规则集	说明
`tls_server`	用作客户机时，`sendmail` 使用此规则集来确定 TLS 当前是否支持该服务器。
`tls_client`	用作服务器时，`sendmail` 使用此规则集来确定 TLS 当前是否支持该客户机。
`tls_rcpt`	此规则集要求验证收件人的 MTA。此收件人限制可完全避免 DNS 电子欺骗等攻击。
`TLS_connection`	此规则集针对当前 TLS 连接的实际参数检查由访问映射的 RHS 指定的要求。
`try_tls`	`sendmail` 使用此规则集来确定连接到其他 MTA 时使用 `STARTTLS` 的可行性。如果 MTA 不能正确实现 `STARTTLS`，则不使用 `STARTTLS`。

有关更多信息，请参见 http://www.sendmail.org/m4/starttls.html。

与运行 SMTP 时使用 TLS 相关的安全注意事项

作为用于定义在 Internet 中运行的邮件程序的标准邮件协议，SMTP 不是一种端对端机制。由于此协议限制，通过 SMTP 的 TLS 安全性不包括邮件用户代理。邮件用户代理用作用户与邮件传输代理（如 sendmail）之间的接口。

另外，邮件也可以在多台服务器之间路由。为了实现完整的 SMTP 安全性，整个 SMTP 连接链必须具有 TLS 支持。

最后，还必须考虑在每对服务器之间或客户机和服务器对之间的协商身份验证和保密性的级别。有关更多信息，请参见《系统管理指南：安全性服务》中的“验证服务”。

sendmail 版本 8.13 中新增的命令行选项

下表介绍了在 sendmail 版本 8.13 中新增的可用命令行选项。sendmail(1M) 手册页介绍了其他命令行选项。

表 14–16 sendmail 版本 8.13 中可用的命令行选项

选项	说明
-D *logfile*	将调试输出发送至指明的 *logfile*，而不是将此信息包括在标准输出中。
-q[!]Q*substr*	指定对包含此 *substr* 的隔离作业的处理，前者是隔离 *reason* 的子字符串。请参见 -Q*reason* 选项的说明。 如果添加了 !，此选项将处理不包含此 *substr* 的隔离作业。
-Q*reason*	以此 *reason* 隔离标准队列项。如果未给定 *reason*，则隔离的队列项将取消隔离。此选项可与 -q[!]Q*substr* 选项结合使用。*substr* 是 *reason* 的一部分（或子字符串）。

sendmail 版本 8.13 中新增和修订的配置文件选项

下表介绍了添加和修订的配置文件选项。如果要声明其中的任何选项，请使用以下语法之一。

```
O OptionName=argument            # for the configuration file
-O OptionName=argument           # for the command line
define(‘m4Name’,argument)       # for m4 configuration
```

表 14–17 sendmail 版本 8.13 中可用的配置文件选项

选项	说明
ConnectionRateWindowSize	m4 名称：confCONNECTION_RATE_WINDOW_SIZE 参数：*number* 缺省值：60 用于设置传入连接保持的秒数。
FallBackSmartHost	m4 名称：confFALLBACK_SMARTHOST 参数：*hostname* 要确保邮件传送到客户机，此选项需提供正确连接的主机，此主机将用作出现故障的 MX 记录的备份（或故障转移）。
InputMailFilters	m4 名称：confINPUT_MAIL_FILTERS 参数：*filename* 用于列出 sendmail 守护进程的输入邮件过滤器。
PidFile	m4 名称：confPID_FILE 参数：*filename* 缺省值：/var/run/sendmail.pid 与以前的发行版相同，在打开文件之前会对文件名进行宏扩展。此外，在版本 8.13 中，sendmail 退出时还将断开文件的链接。
QueueSortOrder	m4 名称：confQUEUE_SORT_ORDER 添加的参数：none 在版本 8.13 中，none 用于指定无排序顺序。
RejectLogInterval	m4 名称：confREJECT_LOG_INTERVAL 参数：*period_of_time* 缺省值：3h，表示 3 个小时。 对于指定的 *period_of_time* 拒绝守护进程连接时，将记录此信息。
SuperSafe	m4 名称：confSAFE_QUEUE 短名称：s 添加的参数：postmilter 缺省值：true 如果设置 postmilter，sendmail 将推迟同步队列文件，直到所有 milters 都已发出接受邮件的信号为止。要使此参数可用，sendmail 必须作为 SMTP 服务器运行。否则，postmilter 的运行将类似于使用 true 参数。

sendmail 版本 8.13 中新增和修订的 FEATURE() 声明

下表介绍了添加和修订的 FEATURE() 声明。此 m4 宏使用以下语法。

```
FEATURE(‘name’, ‘argument’)
```

表 14–18 sendmail 版本 8.13 中可用的 FEATURE() 声明

FEATURE() 的名称	说明
conncontrol	与 access_db 规则集结合使用，用于检查传入的 SMTP 连接的数量。有关详细信息，请参见 /etc/mail/cf/README。
greet_pause	添加 greet_pause 规则集，它将启用开放的代理和 SMTP 攻击保护。有关详细信息，请参见 /etc/mail/cf/README。
local_lmtp	缺省参数仍为 mail.local，该参数在此 Solaris 发行版中是具有 LMTP 功能的邮件程序。但是，在版本 8.13 中，如果使用其他具有 LMTP 功能的邮件程序，则可将其路径名指定为第二个参数，并且可在第三个参数中指定传递给第二个参数的参数。例如： FEATURE(‘local_lmtp’, ‘/usr/local/bin/lmtp’, ‘lmtp’)
mtamark	对“在带有 TXT RR 的反向 DNS 中标记邮件传输代理”(MTAMark) 提供实验支持。有关详细信息，请参见 /etc/mail/cf/README。
ratecontrol	与 access_db 规则集结合使用，用于控制主机的连接速率。有关详细信息，请参见 /etc/mail/cf/README。
use_client_ptr	如果启用此 FEATURE()，规则集 check_relay 将使用参数 $&{client_ptr} 覆盖其第一个参数。

sendmail 版本 8.12 中的更改

本节介绍了有关以下主题的信息。

sendmail 版本 8.12 支持 TCP 包装

TCP 包装提供了一种实现访问权控制的方法，即根据访问控制列表 (access control list, ACL) 检查请求特定网络服务的主机的地址。请求将相应地被授权或拒绝。除了提供此项访问控制机制外，TCP 包装还会记录对网络服务的主机请求，这是一项有用的监视功能。可能受到访问控制的网络服务包括 `rlogind`、`telnetd` 和 `ftpd`。

从版本 8.12 开始，`sendmail` 将允许使用 TCP 包装。此项检查不会忽略其他安全标准。通过在 `sendmail` 中启用 TCP 包装，可以在授权请求前进行检查以验证网络请求的来源。请参见 `hosts_access`(4) 手册页。

注 – 从 Solaris 9 发行版开始，`inetd`(1M) 和 `sshd`(1M) 中将支持 TCP 包装。

有关 ACL 的信息，请参见《系统管理指南：安全性服务》中的“使用访问控制列表保护 UFS 文件”。

sendmail 版本 8.12 中的配置文件 submit.cf

从版本 8.12 开始，`sendmail` 包括一个附加配置文件 `/etc/mail/submit.cf`。此 `submit.cf` 文件用于在邮件提交程序模式而非守护进程模式下运行 `sendmail`。与守护进程模式不同，邮件提交程序模式不要求 `root` 特权，因此这一新模式可以提供更好的安全性。

请参见以下列出的 `submit.cf` 功能：

- `sendmail` 使用 `submit.cf` 在邮件提交程序 (mail-submission program, MSP) 模式下运行，该模式可提交电子邮件并可由程序（如 `mailx`）以及用户启动。请参阅 `sendmail`(1M) 手册页中有关 `-Ac` 选项和 `-Am` 选项的说明。
- `submit.cf` 可用于以下操作模式中：
  - `-bm`，此为缺省操作模式
  - `-bs`，它使用标准输入来运行 SMTP
  - `-bt`，此为用于解析地址的测试模式
- `sendmail` 在使用 `submit.cf` 时不会作为 SMTP 守护进程运行。
- `sendmail`，它使用 `submit.cf` 时将使用仅客户机邮件队列 `/var/spool/clientmqueue`，该队列中保存未传送至 `sendmail` 守护进程的邮件。仅客户机队列中的邮件由客户机“守护进程”来传送，该守护进程实际用作客户机队列运行程序。

- 缺省情况下，sendmail 会定期使用 submit.cf 来运行 MSP 队列（也称为仅客户机队列）/var/spool/clientmqueue。

```
/usr/lib/sendmail -Ac -q15m
```

请注意以下事项：

- 从 Solaris 9 发行版开始，将自动提供 submit.cf。
- 安装 Solaris 9 发行版或更新发行版之前，submit.cf 不要求执行任何规划或预备过程。
- 除非指定配置文件，否则 sendmail 将根据需要自动使用 submit.cf。基本上，sendmail 知道哪些任务适合 submit.cf，哪些任务适合 sendmail.cf。

可区分 sendmail.cf 与 submit.cf 的功能

sendmail.cf 配置文件用于守护进程模式。使用此文件时，sendmail 用作邮件传输代理 (mail transfer agent, MTA)，该代理由 root 启动。

```
/usr/lib/sendmail -L sm-mta -bd -q1h
```

请参见以下列出的 sendmail.cf 的其他特性：

- 缺省情况下，sendmail.cf 在端口 25 和 587 上接受 SMTP 连接。
- 缺省情况下，sendmail.cf 会运行主队列 /var/spool/mqueue。

sendmail 版本 8.12 中功能的更改

除添加 submit.cf 之外，在功能方面还有以下更改：

- 从 sendmail 版本 8.12 开始，仅有 root 可以运行邮件队列。有关更多详细信息，请参阅 mailq(1) 手册页中介绍的更改。有关新任务的信息，请参阅第 279 页中的 “管理队列目录（任务列表）”。
- 邮件提交程序模式运行时无需 root 特权，这可能会导致 sendmail 无法访问某些文件（例如 .forward 文件）。因此，sendmail 的 -bv 选项为用户提供的输出可能具有误导性。没有切实可行的解决方法。
- 在 sendmail 版本 8.12 之前，如果不在守护进程模式下运行 sendmail，则只会阻止传入邮件的传送。从 sendmail 版本 8.12 开始，如果不使用缺省配置运行 sendmail 守护进程，则还会阻止外发邮件的传送。客户机队列运行程序（又称为邮件提交程序）必须能够将邮件提交至本地 SMTP 端口上的守护进程。如果客户机队列运行程序尝试打开与本地主机的 SMTP 会话，并且守护进程未侦听 SMTP 端口，则邮件将保留在队列中。缺省配置确实会运行守护进程，因此使用缺省配置时不会出现此问题。但是，如果已禁用守护进程，请参阅第 269 页中的 “如何使用 sendmail.cf 的备用配置管理邮件传送”以寻找解决此问题的方法。

sendmail 版本 8.12 中新增或过时的命令行选项

下表介绍了 sendmail 的新增或过时的命令行选项。sendmail(1M) 手册页介绍了其他命令行选项。

表 14–19 sendmail 版本 8.12 中新增或过时的命令行选项

选项	说明
-Ac	表示即使操作模式未指明初始邮件提交，仍希望使用配置文件 submit.cf。有关 submit.cf 的更多信息，请参阅第 333 页中的 “sendmail 版本 8.12 中的配置文件 submit.cf”。
-Am	表示即使操作模式指明初始邮件提交，仍希望使用配置文件 sendmail.cf。有关更多信息，请参阅第 333 页中的 “sendmail 版本 8.12 中的配置文件 submit.cf”。
-bP	表示要输出每个队列中的项数。
-G	表示通过命令行提交的邮件将用于中继，而不用于初始提交。如果地址不是全限定地址，则会拒绝该邮件。不会进行标准化。如 ftp://ftp.sendmail.org 上的 sendmail 分发部分所包含的发行说明所述，将来的发行版中可能会拒绝形式不正确的邮件。
-L *tag*	将用于系统日志消息的标识符设置为所提供的 *tag*。
-q[!]I *substring*	仅处理其中一个收件人包含此 *substring* 的作业。添加 ! 之后，该选项仅处理其中一个收件人不包含此 *substring* 的作业。
-q[!]R *substring*	仅处理队列 ID 包含此 *substring* 的作业。添加 ! 之后，该选项仅处理队列 ID 不包含此 *substring* 的作业。
-q[!]S *substring*	仅处理发件人包含此 *substring* 的作业。添加 ! 之后，该选项仅处理发件人不包含此 *substring* 的作业。
-qf	一次处理队列中保存的邮件而不使用 fork 系统调用，并在前台运行该进程。请参阅 fork(2) 手册页。
-qG*name*	仅处理 *name* 队列组中的邮件。
-qp*time*	使用为每个队列派生的单个子项并以特定时间间隔来处理队列中保存的邮件。该子项在队列的每两次运行之间处于休眠状态。这一新选项与 -q*time* 类似，后者会定期派生一个子项来处理队列。
-U	如 ftp://ftp.sendmail.org 上的 sendmail 分发所包含的发行说明所述，在版本 8.12 之前不提供此选项。邮件用户代理应使用 -G 参数。

sendmail 版本 8.12 中新增的用于 PidFile 和 ProcessTitlePrefix 选项的参数

下表介绍了新增的用于 PidFile 和 ProcessTitlePrefix 选项的宏处理参数。有关这些选项的更多信息，请参见 sendmail(1M) 手册页。

表 14–20 PidFile 和 ProcessTitlePrefix 选项的参数

宏	说明
${daemon_addr}	用于提供守护进程地址（例如 0.0.0.0）
${daemon_family}	用于提供守护进程系列（例如 inet 和 inet6）
${daemon_info}	用于提供守护进程信息（例如 SMTP+queueing@00:30:00）
${daemon_name}	用于提供守护进程名称（例如 MSA）
${daemon_port}	用于提供守护进程端口（例如 25）
${queue_interval}	用于提供队列运行间隔（例如 00:30:00）

sendmail 版本 8.12 中新增的已定义宏

下表介绍了新增的、保留以供 sendmail 程序使用的宏。这些宏的值在内部指定。有关更多信息，请参阅sendmail(1M) 手册页。

表 14–21 sendmail 新增的已定义宏

宏	说明
${addr_type}	用于将当前地址标识为信封发件人地址或收件人地址。
${client_resolve}	用于保存 ${client_name} 的解析调用结果：OK、FAIL、FORGED 或 TEMP。
${deliveryMode}	用于指定 sendmail 正在使用的当前传送模式，而不是 DeliveryMode 选项的值。
${dsn_notify}、${dsn_envid}、${dsn_ret}	用于保存对应的 DSN 参数值。
${if_addr}	用于为传入连接提供接口的地址，前提是该接口不属于回送网络。此宏对于虚拟主机特别有用。
${if_addr_out}、${if_name_out}、${if_family_out}	用于避免重用 ${if_addr}。可分别保存以下值。 用于传出连接的接口地址。 用于传出连接的接口主机名。 用于传出连接的接口系列。
${if_name}	用于为传入连接提供接口的主机名，对于虚拟主机特别有用。
${load_avg}	用于检查并报告运行队列中当前的平均作业数。

表 14–21 sendmail 新增的已定义宏 （续）

宏	说明
${msg_size}	用于在收集邮件之前，在 ESMTP 对话框中保存邮件大小 (SIZE=parameter) 的值。此后，此宏将保存 sendmail 计算的邮件大小并将其用于 check_compat 中。有关 check_compat 的信息，请参阅表 14–25。
${nrcpts}	用于保存经过验证的收件人数。
${ntries}	用于保存尝试传送的次数。
${rcpt_mailer}、${rcpt_host}、${rcpt_addr}、${mail_mailer}、${mail_host}、${mail_addr}	用于保存 RCPT 和 MAIL 参数的分析结果，这是从邮件传送代理 ($#*mailer*)、主机 ($@*host*) 和用户 ($:*addr*) 中解析出的右侧 (right-hand side, RHS) 三重参数。

sendmail 版本 8.12 中新增的宏

本节中的表介绍了新增的用于生成 sendmail 配置文件的宏。

表 14–22 新增的用于生成 sendmail 配置文件的宏

宏	说明
LOCAL_MAILER_EOL	用于覆盖本地邮件程序缺省的行结束字符串。
LOCAL_MAILER_FLAGS	用于在缺省情况下添加 Return-Path: 头。
MAIL_SETTINGS_DIR	用于包含邮件设置目录的路径（包括结尾斜杠）。
MODIFY_MAILER_FLAGS	用于改进 *_MAILER_FLAGS。此宏可以设置、添加或删除标志。
RELAY_MAILER_FLAGS	用于为中继邮件程序定义新增标志。

sendmail 版本 8.12 中新增的 MAX 宏

使用以下宏可以配置在 sendmail 降低传送速度之前可以接收的命令的最大数目。可在编译时设置这些 MAX 宏。下表中的最大值也表示当前的缺省值。

表 14–23 新增的 MAX 宏

宏	最大值	每个宏检查的命令
MAXBADCOMMANDS	25	未知命令

表 14–23 新增的 MAX 宏 （续）

宏	最大值	每个宏检查的命令
MAXNOOPCOMMANDS	20	NOOP、VERB、ONEX、 XUSR
MAXHELOCOMMANDS	3	HELO、EHLO
MAXVRFYCOMMANDS	6	VRFY、EXPN
MAXETRNCOMMANDS	8	ETRN

注 – 通过将宏的值设置为零可以禁用宏检查。

sendmail 版本 8.12 中新增和修订的 m4 配置宏

本节中的表介绍了 sendmail 中新增和修订的 m4 配置宏。可使用以下语法来声明这些宏。

symbolic-name(‘*value*’)

如果需要生成新的 sendmail.cf 文件，请参阅第 13 章，邮件服务（任务）中的第 261 页中的 “更改 sendmail 配置”。

表 14–24 sendmail 中新增和修订的 m4 配置宏

m4 宏	说明
FEATURE()	有关详细信息，请参阅第 338 页中的 “sendmail 版本 8.12 中对 FEATURE() 声明的更改”。
LOCAL_DOMAIN()	此宏可向类 w ($=w) 中添加项。
MASQUERADE_EXCEPTION()	用于定义不能伪装的主机或子域的新宏。
SMART_HOST()	现在，此宏可用于用括号括起来的地址，如 user@[**主机**]。
VIRTUSER_DOMAIN() 或 VIRTUSER_DOMAIN_FILE()	使用这些宏时，请在 $=R 中包括 ${VirtHost}。请记住，$=R 是可以中继的主机名的集合。

sendmail 版本 8.12 中对 FEATURE() 声明的更改

有关对 FEATURE() 声明的特定更改信息，请参阅下表。

要使用新增和修订的 FEATURE 名称，请使用以下语法。

FEATURE(‘*name*’, ‘*argument*’)

如果需要生成新的 sendmail.cf 文件，请参阅第 13 章，邮件服务（任务）中的第 261 页中的 “更改 sendmail 配置”。

表 14–25 新增和修订的 FEATURE() 声明

FEATURE() 的名称	说明
compat_check	参数：请参阅以下段落中的示例。 使用此新增的 FEATURE()，可以在由发件人地址和收件人地址组成的访问映射中查找关键字。此 FEATURE() 由字符串 <@> 来分隔。例如 *sender*@*sdomain*<@>*recipient* @*rdomain*。
delay_checks	参数：friend（用于启用垃圾邮件-朋友测试）或 hater（用于启用垃圾邮件-攻击者测试）。 可延迟所有检查的新增 FEATURE()。通过使用 FEATURE('delay_checks')，在客户机分别连接或发出 MAIL 命令时，将不调用规则集 check_mail 和 check_relay，而是由 check_rcpt 规则集调用上述规则集。有关详细信息，请参阅 /etc/mail/cf/README 文件。
dnsbl	参数：此 FEATURE() 最多可以接受两个参数： ■ DNS 服务器名 ■ 拒绝邮件 新增的 FEATURE()，可以多次使用以检查 DNS 查找的返回值。请注意，通过此 FEATURE() 可以指定临时查找失败时的行为。
enhdnsbl	参数：域名。 新增的 FEATURE()，它是 dnsbl 的增强版本，可用于检查 DNS 查找的返回值。有关更多信息，请参阅 /etc/mail/cf/README。
generics_entire_domain	参数：无。 新增的 FEATURE()，使用它还可以将 genericstable 应用于 $=G 的子域。
ldap_routing	参数：有关详细信息，请参阅 http://www.sendmail.org 中的 "Release Notes"。 可实现 LDAP 地址路由的新增 FEATURE()。
local_lmtp	参数：具有 LMTP 功能的邮件程序的路径名。缺省为 mail.local，它在此 Solaris 发行版中具有 LMTP 功能。 该 FEATURE() 现在可将本地邮件程序的传送状态通知 (delivery status notification, DSN) 诊断代码类型设置为正确的 SMTP 值。
local_no_masquerade	参数：无。 可用于避免伪装本地邮件程序的新增 FEATURE()。
lookupdotdomain	参数：无。 也可用于在访问映射中查找 *.domain* 的新增 FEATURE()。

表 14–25 新增和修订的 FEATURE() 声明 （续）

FEATURE() 的名称	说明
nocanonify	参数：canonify_hosts 或无参数。 该 FEATURE() 现在包括以下功能。 将 CANONIFY_DOMAIN 或 CANONIFY_DOMAIN_FILE 指定的一系列域传递给 $[和 $] 运算符进行标准化。 如果将 canonify_hosts 指定为其参数，则可以对仅包含主机名的地址（如 <user@host>）进行标准化。 向包含多个组成部分的地址添加尾随句点。
no_default_msa	参数：无。 这一新增的 FEATURE() 可禁用 m4 生成的配置文件中 sendmail 的缺省设置，以“侦听”多个不同端口，这是 RFC 2476 的实现。
nouucp	参数：reject（不允许使用 ! 标记）或 nospecial（允许使用 ! 标记）。 该 FEATURE() 可确定是否允许在地址的本地部分中使用 ! 标记。
nullclient	参数：无。 该 FEATURE() 现在可提供标准配置的完整规则集，从而允许执行防垃圾邮件检查。
preserve_local_plus_detail	参数：无。 通过这一新增的 FEATURE()，可在 sendmail 将地址传递给本地传送代理时保留地址中的 +detail 部分。
preserve_luser_host	参数：无。 如果使用 LUSER_RELAY，则通过这一新增的 FEATURE() 可以保留收件人主机的名称。
queuegroup	参数：无。 通过这一新增的 FEATURE()，可以选择基于完整电子邮件地址或基于收件人的域的队列组。
relay_mail_from	参数：**域**是一个可选参数。 如果邮件发件人在访问映射中列为 RELAY 并使用 From: 头行来标记，则通过这一新增的 FEATURE() 可进行中继。如果给定可选的**域**参数，则还会检查邮件发件人的域部分。
virtuser_entire_domain	参数：无。 现在，可以使用该 FEATURE() 来应用 $={VirtHost}，这是一个新类，用于匹配可由 VIRTUSER_DOMAIN 或 VIRTUSER_DOMAIN_FILE 填充的 virtusertable 项。 FEATURE(‘virtuser_entire_domain’) 还可以将类 $={VirtHost} 应用于整个子域。

不再支持以下 FEATURE() 声明。

表 14–26 不支持的 FEATURE() 声明

FEATURE() 的名称	替代函数
rbl	FEATURE(‘dnsbl’) 和 FEATURE(‘enhdnsbl’) 替代已删除的 FEATURE()。
remote_mode	MASQUERADE_AS(‘$S’) 将替代 /etc/mail/cf/subsidiary.mc 中的 FEATURE(‘remote_mode’)。$S 是 sendmail.cf 中的 SMART_HOST 值。
sun_reverse_alias_files	FEATURE(‘genericstable’).
sun_reverse_alias_nis	FEATURE(‘genericstable’)。
sun_reverse_alias_nisplus	FEATURE(‘genericstable’)。

sendmail 版本 8.12 中对 MAILER() 声明的更改

MAILER() 声明可指定对传送代理的支持。要声明传送代理，请使用以下语法。

MAILER(‘*symbolic-name*’)

请注意以下更改。

- 在此新版本的 sendmail 中，MAILER(‘smtp’) 声明现在包括一个附加邮件程序 dsmtp，该邮件程序通过使用 F=% 邮件程序标志可提供即时传送。dsmtp 邮件程序定义使用新增的 DSMTP_MAILER_ARGS，后者缺省为 IPC $h。
- MAILER 使用的规则集的数量已删除。现在无需按顺序列出 MAILER，但 MAILER(‘uucp’) 除外。如果使用了 uucp-dom 和 uucp-uudom，则它必须在 MAILER(‘smtp’) 之后。

有关邮件程序的更多信息，请参阅第 297 页中的 “邮件程序与 sendmail”。如果需要生成新的 sendmail.cf 文件，请参阅第 13 章，邮件服务（任务）中的第 261 页中的 “更改 sendmail 配置”。

sendmail 版本 8.12 中新增的传送代理标志

下表介绍了新增的传送代理标志，缺省情况下不会设置这些标志。这些单字符标志是布尔型的。通过在配置文件的 F= 语句中包括或排除标志，可以设置或取消设置标志，如以下示例所示。

```
Mlocal,    P=/usr/lib/mail.local, F=lsDFMAw5:/|@qSXfmnz9, S=10/30, R=20/40,
Mprog,     P=/bin/sh, F=lsDFMoqeu9, S=10/30, R=20/40, D=$z:/,
Msmtp,     P=[IPC], F=mDFMuX, S=11/31, R=21, E=\r\n, L=990,
Mesmtp,    P=[IPC], F=mDFMuXa, S=11/31, R=21, E=\r\n, L=990,
Msmtp8,    P=[IPC], F=mDFMuX8, S=11/31, R=21, E=\r\n, L=990,
Mrelay,    P=[IPC], F=mDFMuXa8, S=11/31, R=61, E=\r\n, L=2040,
```

表 14–27 新增的邮件程序标志

标志	说明
%	除非使用 ETRN 请求或以下队列选项之一选择排队的邮件，否则使用此标志的邮件程序不会尝试向邮件的初始收件人或队列运行中传送邮件：-qI、-qR 或 -qS。
1	此标志可禁用邮件程序发送空字符的功能（例如 \0）。
2	此标志可禁用 ESMTP 并要求改用 SMTP。
6	此标志可使邮件程序将头缩减至 7 位。

sendmail 版本 8.12 中新增的用于传送代理的等式

下表介绍了新增的可用于 M 传送代理定义命令的等式。以下语法说明如何在配置文件中已存在的等式后附加新的等式或参数。

M*agent-name*, *equate*, *equate*, ...

以下示例中包括新的 W= 等式。此等式可指定在发送所有数据后等待邮件程序返回的最长时间。

```
Msmtp, P=[IPC], F=mDFMuX, S=11/31, R=21, E=\r\n, L=990, W=2m
```

在为 m4 配置修改值的定义时，请使用以下示例中提供的语法。

```
define('SMTP_MAILER_MAXMSGS', '1000')
```

上一示例将 smtp 邮件程序每次连接时传送的邮件数量限制为 1000。

如果需要生成新的 sendmail.cf 文件，请参阅第 13 章，邮件服务（任务）中的第 261 页中的 “更改 sendmail 配置”。

注 – 通常，仅当进行微调时，才会修改 mailer 目录中的等式定义。

表 14–28 用于传送代理的新增等式

等式	说明
/=	参数：目录的路径。 用于指定执行邮件程序之前要应用 chroot() 的目录。

表 14–28 用于传送代理的新增等式 （续）

等式	说明
m=	参数：以前使用 define() 例程定义的以下任意 m4 值 SMTP_MAILER_MAXMSGS，用于 smtp 邮件程序 LOCAL_MAILER_MAXMSGS，用于 local 邮件程序 RELAY_MAILER_MAXMSGS，用于 relay 邮件程序 用于限制 smtp、local 或 relay 邮件程序每次连接时传送的邮件数量
W=	参数：时间增量 用于指定在发送所有数据后等待邮件程序返回的最长时间

sendmail 版本 8.12 中新增的队列功能

以下列表提供了有关新增队列功能的详细信息。

- 此发行版可支持多个队列目录。要使用多个队列，请在配置文件中提供以星号 (*) 结尾的 QueueDirectory 选项值，如以下示例所示。

  ```
  O QueueDirectory=/var/spool/mqueue/q*
  ```

  选项值 /var/spool/mqueue/q* 使用以 "q" 开头的所有目录（或指向这些目录的符号链接）作为队列目录。请勿在 sendmail 运行时更改队列目录结构。除非在非守护进程队列运行中使用冗余标志 (-v)，否则队列运行会创建一个单独进程来运行每个队列。新项将随机指定给队列。
- 新增的队列文件命名系统使用的文件名保证在 60 年内唯一。使用此系统，可在不使用复杂的文件系统锁定的情况下指定队列 ID，并简化排队的项在队列之间的移动。
- 从版本 8.12 开始，仅有 root 才能运行邮件队列。有关更多详细信息，请参阅 mailq(1) 手册页中介绍的更改。有关新任务的信息，请参阅第 279 页中的 “管理队列目录（任务列表）”。
- 为适应信封拆分，现在队列文件名长度为 15 个字符，而不是 14 个字符。将不再支持名称限制为 14 个字符的文件系统。

有关任务信息，请参阅第 279 页中的 “管理队列目录（任务列表）”。

sendmail 版本 8.12 中对 LDAP 的更改

以下列表介绍了在将轻量目录访问协议 (Lightweight Directory Access Protocol, LDAP) 用于 sendmail 时的一些更改。

- LDAPROUTE_EQUIVALENT() 和 LDAPROUTE_EQUIVALENT_FILE() 允许指定等效的主机名，这些主机名将替换为用于 LDAP 路由查找的伪装域名。有关更多信息，请参阅 /etc/mail/cf/README。

- 如 ftp://ftp.sendmail.org 上的 sendmail 分发部分所包含的发行说明所述，LDAPX 映射已重命名为 LDAP。请针对 LDAP 使用以下语法。

  ```
  Kldap ldap options
  ```

- 此发行版支持一次 LDAP 查找返回多个值。请使用 -v 选项将要返回的值放入用逗号分隔的字符串中，如下所示。

  ```
  Kldap ldap -v"mail,more-mail"
  ```

- 如果 LDAP 映射声明中未指定任何 LDAP 属性，则会返回找到的所有匹配属性。
- 此版本的 sendmail 可防止使用 LDAP 别名文件规范中带引号的关键字和值字符串内的逗号来将单个项划分为多个项。
- 此版本的 sendmail 为 LDAP 映射提供了一个新选项。使用选项 -V*separator*，可指定一个分隔符，这样查找便可返回由相关的 *separator* 分隔的属性和值。
- 除了使用 %s 标记分析 LDAP 过滤器规范外，还可以使用新标记 %0 对关键字缓冲区进行编码。%0 标记会对 LDAP 特殊字符应用字面含义。

以下示例显示了这些标记在用于 "*" 查找时的差异。

表 14–29 标记的比较

LDAP 映射规范	规范等效形式	结果
-k"uid=%s"	-k"uid=*"	匹配具有用户属性的任何记录
-k"uid=%0"	-k"uid=\2A"	匹配具有名称 "*" 的用户

下表介绍了新增的 LDAP 映射标志。

表 14–30 新增的 LDAP 映射标志

标志	说明
-1	要求返回单个匹配项。如果返回多个匹配项，则结果与未找到任何记录等效。
-r never|always|search|find	设置 LDAP 别名取消引用选项。
-Z size	限制要返回的匹配项数。

sendmail 版本 8.12 中对内置邮件程序的更改

原有的 [TCP] 内置邮件程序不可用。请改用 P=[IPC] 内置邮件程序。进程间通信 ([IPC]) 内置邮件程序现在可向支持它的系统中的 UNIX 域套接字进行传送。可将此邮件程序与侦听指定套接字的 LMTP 传送代理结合使用。示例邮件程序可能如下所示。

```
Mexecmail, P=[IPC], F=lsDFMmnqSXzA5@/:|, E=\r\n,
S=10, R=20/40, T=DNS/RFC822/X-Unix, A=FILE /var/run/lmtpd
```

现在，系统将检查 [IPC] 邮件程序中的第一个邮件程序参数是否具有合法值。下表提供了第一个邮件程序参数的可能值。

表 14–31 第一个邮件程序参数的可能值

值	说明
A=FILE	用于 UNIX 域套接字传送
A=TCP	用于 TCP/IP 连接
A=IPC	不再用作第一个邮件程序参数

sendmail 版本 8.12 中新增的规则集

下表列出了新增规则集并介绍了这些规则集的功能。

表 14–32 新规则集

集	说明
check_eoh	将在头之间收集的信息关联并检查是否缺少头。此规则集用于宏存储映射，并在收集所有头后调用。
check_etrn	使用 ETRN 命令（与 check_rcpt 使用 RCPT 类似）。
check_expn	使用 EXPN 命令（与 check_rcpt 使用 RCPT 类似）。
check_vrfy	使用 VRFY 命令（与 check_rcpt 使用 RCPT 类似）。

以下列表介绍了新增的规则集功能。

- 编号的规则集也已命名，但仍然可以按编号访问相应的规则集。
- H 头配置文件命令允许为头检查指定缺省的规则集。仅当未对个别头指定各自的规则集时，才会调用此规则集。
- 如果配置文件的版本为 9 或更高版本，则不删除规则集中的注释（即括号内的文本）。例如，以下规则可匹配输入 token (1)，但不匹配输入 token。

```
R$+ (1)         $@ 1
```

- sendmail 即使由于 TCP 包装或 check_relay 规则集而拒绝命令，也会接受 SMTP RSET 命令。
- 如果多次设置 OperatorChars 选项，则会收到警告。另外，请勿在定义规则集之后设置 OperatorChars。
- 如果声明的规则集无效，则会忽略该规则集的名称以及其中的各行。该规则集行不会添加至 S0。

sendmail 版本 8.12 中对文件的更改

请注意以下更改。

- 从 Solaris 10 发行版开始，为了支持只读的 /usr 文件系统，/usr/lib/mail 目录的内容已移至 /etc/mail/cf 目录。有关详细信息，请参阅第 308 页中的 “/etc/mail/cf 目录的内容”。但请注意，shell 脚本 /usr/lib/mail/sh/check-hostname 和 /usr/lib/mail/sh/check-permissions 现在位于 /usr/sbin 目录中。请参见第 310 页中的 “用于邮件服务的其他文件”。为了实现向下兼容，符号链接指向每个文件的新位置。
- /usr/lib/mail/cf/main-v7sun.mc 的新名称是 /etc/mail/cf/cf/main.mc。
- /usr/lib/mail/cf/subsidiary-v7sun.mc 的新名称是 /etc/mail/cf/cf/subsidiary.mc。
- helpfile 现在位于 /etc/mail/helpfile 中。旧名称 (/etc/mail/sendmail.hf) 具有指向新名称的符号链接。
- trusted-users 文件现在位于 /etc/mail/trusted-users 中。在升级过程中，如果检测到旧名称 (/etc/mail/sendmail.ct) 而未检测到新名称，则会创建从旧名称到新名称的硬链接。否则，不会进行任何更改。缺省内容为 root。
- local-host-names 文件现在位于 /etc/mail/local-host-names 中。在升级过程中，如果检测到旧名称 (/etc/mail/sendmail.cw) 而未检测到新名称，则会创建从旧名称到新名称的硬链接。否则，不会进行任何更改。缺省内容的长度为零。

sendmail 版本 8.12 和配置中的 IPv6 地址

从 8.12 版本的 sendmail 开始，在配置中使用的 IPv6 地址应以 IPv6: 标记作为前缀，以正确标识地址。如果不标识 IPv6 地址，则不会使用前缀标记。

第 5 部 分

串行网络主题

本节主要讲述串行网络，其中提供了有关 PPP 和 UUCP 的概述、任务和参考信息。

◆ ◆ ◆ 第 15 章

15 Solaris PPP 4.0（概述）

本节介绍串行联网主题。串行联网是指使用串行接口（如 RS-232 或 V.35 端口）连接两台或更多计算机，以便进行数据传送。与 LAN 接口（如以太网）不同，这些串行接口用于连接相距很远的系统。PPP（Point-to-Point Protocol，点对点协议）和 UUCP（UNIX-to-UNIX CoPy，UNIX 对 UNIX 复制）是可用于实现串行联网的独特技术。为联网配置串行接口之后，多个用户可以按照几乎与使用任何其他网络接口（如以太网）相同的方法使用该接口。

本章介绍 Solaris PPP 4.0。利用此版本的 PPP，可以使位于不同物理位置的两台计算机能够在多种介质上使用 PPP 来相互通信。从 Solaris 9 发行版开始，Solaris PPP 4.0 将作为基本安装的一部分。

本章包含以下主题：

Solaris PPP 4.0 基础知识

Solaris PPP 4.0 实现点对点协议 (Point-to-Point Protocol, PPP)，此协议为数据链路协议，是 TCP/IP 协议集的成员之一。PPP 说明通过通信介质（如电话线路）在两台端点计算机之间传输数据的方式。

自 20 世纪 90 年代初以来，PPP 已广泛用作通过通信链路发送数据报的 Internet 标准。PPP 标准由 Internet 工程任务组 (Internet Engineering Task Force, IETF) 的点对点工作组在 RFC 1661 中说明。当远程计算机呼叫配置用于接收传入呼叫的 Internet 服务提供商 (Internet service provider, ISP) 或公司服务器时，通常使用 PPP。

Solaris PPP 4.0 基于公开的澳大利亚国立大学 (Australian National University, ANU) PPP–2.4 并实现 PPP 标准。支持异步和同步 PPP 链路。

Solaris PPP 4.0 兼容性

在整个 Internet 社区中可以获取各种版本的标准 PPP，并且正在广泛使用这些版本。ANU PPP-2.4 广泛用于 Linux、Tru64 UNIX 以及 BSD 的三种最主要变体：

- FreeBSD
- OpenBSD
- NetBSD

Solaris PPP 4.0 为运行 Solaris 操作系统的计算机带来了 ANU PPP-2.4 的高可配置特性。在运行 Solaris PPP 4.0 的计算机上可以轻易地设置连接到任何运行标准 PPP 实现的计算机的 PPP 链路。

不基于 ANU 但却能成功地与 Solaris PPP 4.0 进行交互操作的 PPP 实现包括：

- Solaris PPP，也称为 `asppp`，在 Solaris 2.4 到 Solaris 8 发行版中提供
- Solstice PPP 3.0.1
- Microsoft Windows 98 DUN
- Cisco IOS 12.0（同步）

使用哪个版本的 Solaris PPP

Solaris PPP 4.0 是支持的 PPP 实现。Solaris 9 发行版和之后的发行版不包含早期的异步 Solaris PPP (`asppp`) 软件。有关更多信息，请参阅以下内容：

- 第 23 章，从异步 Solaris PPP 迁移至 Solaris PPP 4.0（任务）
- http://docs.sun.com 上的 Solaris System Administrator Collection

为什么使用 Solaris PPP 4.0？

如果当前使用的是 `asppp`，请考虑迁移到 Solaris PPP 4.0。请注意这两种 Solaris PPP 技术之间的以下差别：

- **传送模式**

  `asppp` 仅支持异步通信。Solaris PPP 4.0 支持异步通信和同步通信。

- **配置过程**

  设置 `asppp` 需要对 `asppp.cf` 配置文件、三个 UUCP 文件和 `ifconfig` 命令进行配置。此外，必须为可能登录到计算机的所有用户预先配置接口。

  设置 Solaris PPP 4.0 需要为 PPP 配置文件定义选项，或发出带选项的 `pppd` 命令。您也可以将配置文件和命令行方法结合使用。Solaris PPP 动态创建和删除接口。不需要为每个用户直接配置 PPP 接口。

- **asppp 中不提供的 Solaris PPP 4.0 功能**
  - MS-CHAPv1 和 MS-CHAPv2 验证
  - 基于以太网的 PPP (PPP over Ethernet, PPPoE)，用于支持 ADSL 网桥

- PAM 验证
- 插件模块
- IPv6 寻址
- 使用 Deflate 或 BSD 压缩方法进行的数据压缩
- Microsoft 客户端回调支持

Solaris PPP 4.0 升级途径

如果要将现有 asppp 配置转换为 Solaris PPP 4.0，可以使用此发行版附带的转换脚本。有关完整说明，请参阅第 472 页中的 “如何从 asppp 转换为 Solaris PPP 4.0”。

其他可获取更多 PPP 信息的渠道

可利用印刷材料和联机文档等多种资源获取更多有关 PPP 的信息。以下几个小节给出了一些建议。

有关 PPP 的专业参考书籍

有关广泛使用的 PPP 实现（包括 ANU PPP）的更多信息，请参阅以下书籍：

- 由 Carlson, James 编著的 《PPP Design, Implementation, and Debugging》，第 2 版。Addison-Wesley 出版，2000。
- 由 Sun, Andrew 编著的《Using and Managing PPP》。O'Reilly & Associates 出版，1999。

有关 PPP 的 Web 站点

要获取有关 PPP 的常规信息，请访问以下 Web 站点：

- 有关 Solaris 系统管理和 PPP 早期版本的技术信息、常见问题解答和讨论，请访问系统管理员资源，网址为 http://www.sun.com/bigadmin/home/index.html。
- 有关许多不同 PPP 实现的调制解调器配置和建议，请参阅 Stokely Consulting 的 Web 项目管理与软件开发 Web 站点：http://www.stokely.com/unix.serial.port.resources/ppp.slip.html。

有关 PPP 的请求注解文档 (Requests for Comments, RFC)

有关 PPP 的一些有用的 Internet RFC 包括：

- 1661 和 1662，说明 PPP 的主要功能
- 1334，说明验证协议（如口令验证协议 (Password Authentication Protocol, PAP) 和质询握手身份验证协议 (Challenge-Handshake Authentication Protocol, CHAP)）
- 1332，说明基于以太网的 PPP (PPP over Ethernet, PPPoE) 的信息性 RFC

要获取 PPP RFC 的副本，请在 http://www.ietf.org/rfc.html 的 IETF RFC Web 页上指定 RFC 的编号。

有关 PPP 的手册页

有关 Solaris PPP 4.0 实现的详细技术信息，请参阅以下手册页：

- pppd(1M)
- chat(1M)
- pppstats(1M)
- pppoec(1M)
- pppoed(1M)
- sppptun(1M)
- snoop(1M)

此外，还可以参见 pppdump(1M) 的手册页。可使用 man 命令找到与 PPP 有关的手册页。

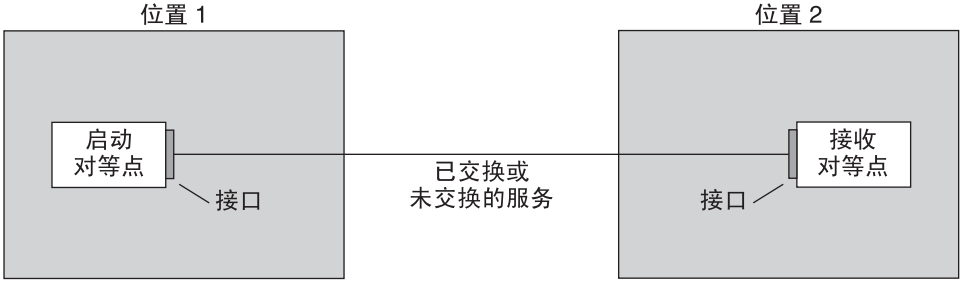
PPP 配置和术语

本节介绍 PPP 配置，还将介绍本指南中使用的术语。

Solaris PPP 4.0 支持许多配置。

- 交换式访问（或称为**拨号**）配置
- 硬连线（或称为**租用线路**）配置

图 15–1 PPP 链路的各部分



上图显示了基本 PPP 链路。该链路包含以下部分：

- 两台计算机，通常位于独立物理位置，称为**对等点**。对等点可以是个人计算机、工程工作站、大型服务器，甚至商业路由器，具体取决于网站的要求。
- 每个对等点上的串行接口。在 Solaris 计算机上，此接口可以是 cua、hihp 或其他接口，具体取决于配置的是异步还是同步 PPP。
- 物理链路，如串行电缆、调制解调器连接或来自网络提供商的租用线路（如 T1 或 T3 线路）。

拨号 PPP 概述

最常用的 PPP 配置是**拨号链路**。在拨号链路中，本地对等点向远程对等点**拨号**以建立连接并运行 PPP。在拨号过程中，本地对等点呼叫远程对等点的电话号码以启动该链路。

常见拨号情况包括呼叫 ISP 的对等点（配置用于接收传入呼叫）的家庭计算机。另外一种情况是公司站点，此站点中的本地计算机基于 PPP 链路向另一建筑内的对等点传输数据。

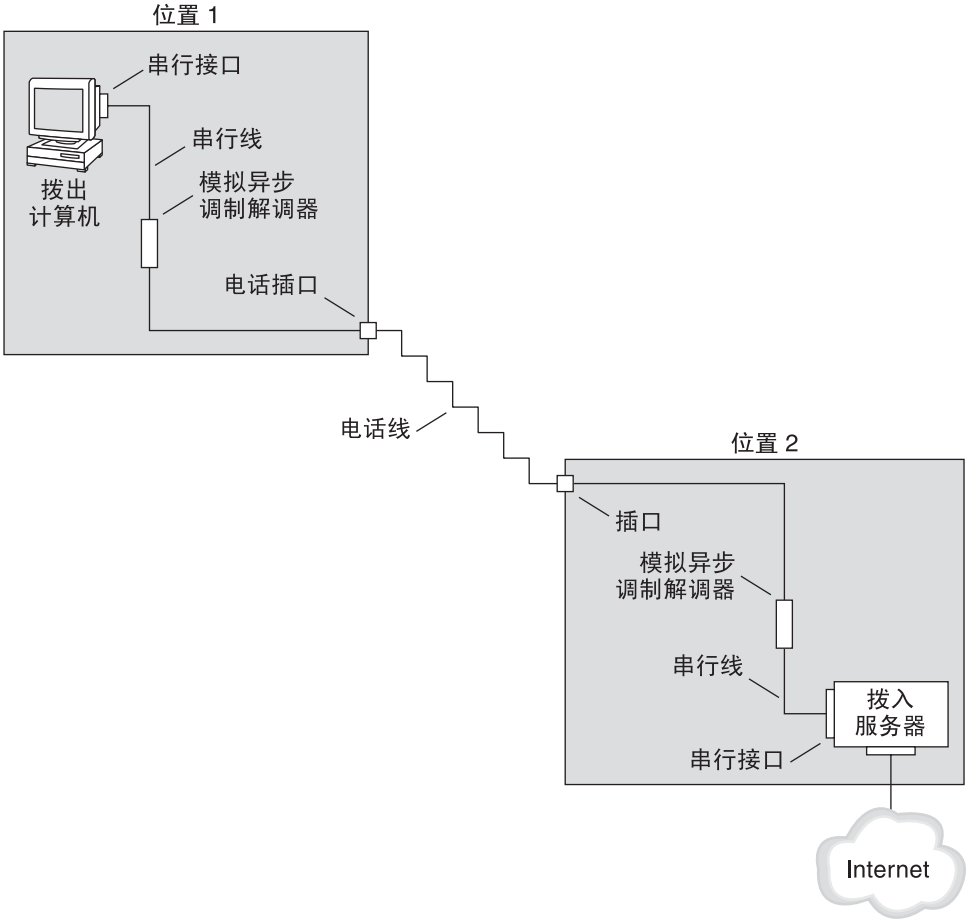
在本指南中，启动拨号连接的本地对等点称为**拨出计算机**。接收传入呼叫的对等点称为**拨入服务器**。此计算机实际上是拨出计算机的目标对等点，它可能是一台真实服务器也可能不是。

PPP 不是客户机/服务器协议。一些 PPP 文档使用术语“客户机”和“服务器”表示电话呼叫的建立。拨入服务器与文件服务器或名称服务器类似，不是一台真实的服务器。拨入服务器成为广泛使用的 PPP 术语是因为拨入计算机通常为多台拨出计算机提供网络访问“服务”。不过，拨入服务器是拨出计算机的目标对等点。

拨号 PPP 链路的各部分

请参见下图。

图 15–2 基本模拟拨号 PPP 链路



位置 1（链路的拨出端）的配置由以下元素组成：

- 拨出计算机，通常为个人计算机或个人家庭中的工作站。
- 拨出计算机上的串行接口。`/dev/cua/a` 或 `/dev/cua/b` 是运行 Solaris 软件的计算机上传出呼叫的标准串行接口。
- 连接到电话插口的异步调制解调器或 ISDN 终端适配器 (terminal adapter, TA)。
- 电话线和电话公司的服务。

位置 2（链路的拨入端）的配置由以下元素组成：

- 连接到电话网络的电话插口或类似连接器
- 异步调制解调器或 ISDN TA
- 拨入服务器上的串行接口，它是传入呼叫的 `ttya` 或 `ttyb`

- 连接到网络（如公司内联网，对于 ISP 则为全球 Internet）的拨入服务器

使用拨出计算机上的 ISDN 终端适配器

外部 ISDN TA 具有比调制解调器更快的速度，但可以按照基本相同的方法配置 TA。配置 ISDN TA 的主要差别在于聊天脚本，该脚本需要使用特定于 TA 制造商的命令。有关 ISDN TA 的聊天脚本的信息，请参阅第 449 页中的 “外部 ISDN TA 的聊天脚本”。

拨号通信期间发生的操作

拨出和拨入对等点上的 PPP 配置文件包含用于设置链路的指令。启动拨号链路时将发生以下过程。

1. 拨出计算机上的用户或进程运行 `pppd` 命令以启动链路。
2. 拨出计算机读取其 PPP 配置文件。然后，拨出计算机基于串行线路将指令（包括拨入服务器的电话号码）发送到其调制解调器。
3. 调制解调器拨打电话号码，以与拨入服务器上的调制解调器建立电话连接。

   拨出计算机发送到调制解调器和拨入服务器的一系列文本字符串包含在称为**聊天脚本**的文件中。如有必要，拨出计算机可发送命令到拨入服务器以呼叫该服务器上的 PPP。
4. 连接到拨入服务器的调制解调器开始与拨出计算机上的调制解调器进行链路协商。
5. 完成调制解调器对调制解调器协商后，拨出计算机上的调制解调器将报告 "CONNECT"。
6. 两个对等点上的 PPP 都将进入**建立**阶段，此阶段中链路控制协议 (Link Control Protocol, LCP) 协商基本链路参数和验证的使用。
7. 如有必要，对等点相互验证。
8. PPP 的网络控制协议 (Network Control Protocol, NCP) 会协商网络协议（如 IPv4 或 IPv6）的使用。

然后，拨出计算机对通过拨入服务器可访问的主机运行 `telnet` 或类似命令。

租用线路 PPP 概述

硬连线的**租用线路** PPP 配置包括通过链路连接的两个对等点。该链路由从提供商处租用的交换式或非交换式数字服务组成。Solaris PPP 4.0 基于任何全双工、点对点租用线路介质工作。通常，公司从网络提供商租用硬连线的链路以连接到 ISP 或其他远程站点。

拨号链路与租用线路链路的比较

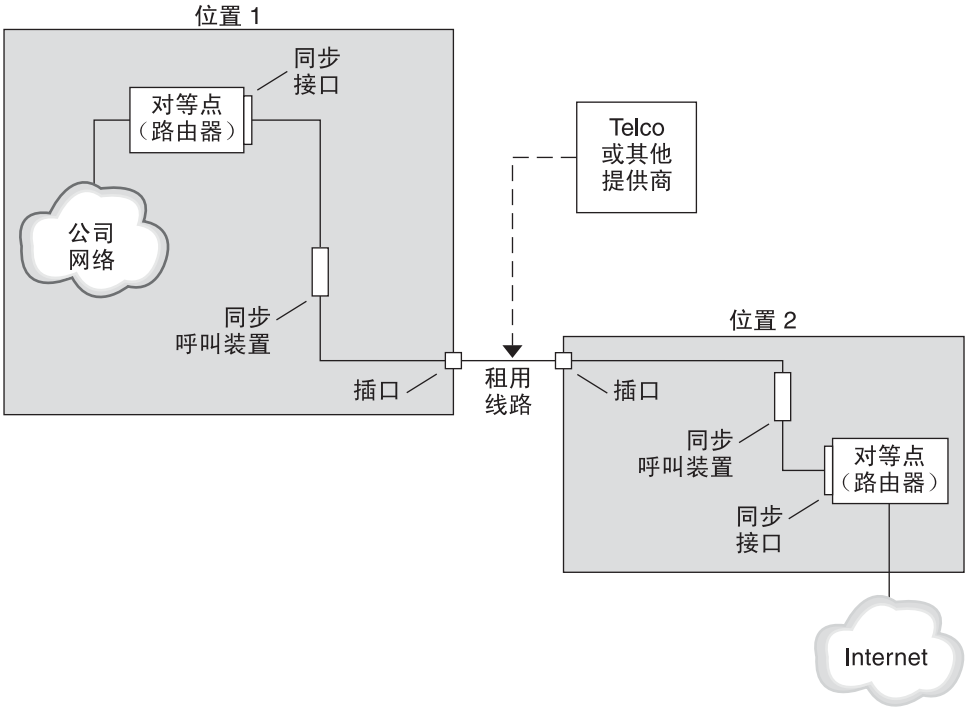
拨号链路和租用线路链路都包括通过通信介质连接的两个对等点。下表概述了两种链路类型之间的差别。

租用线路	拨号线路
始终处于连接状态，除非系统管理员断开租用线路的连接或由于停电而断开连接。	根据需要在用户尝试呼叫远程对等点时启动。
使用同步和异步通信。对于异步通信，通常使用长通信距离调制解调器。	使用异步通信。
从提供商处租用。	使用现有电话线路。
需要同步设备。	使用低成本的调制解调器。
需要大多数 SPARC 系统中常见的同步端口。但是，同步端口在 x86 系统和较新的 SPARC 系统中不常见。	使用大多数计算机中附带的标准串行接口。

租用线路 PPP 链路的各部分

请参见下图。

图 15–3 基本租用线路配置



租用线路链路包含以下部分：

- **两个对等点**，每个对等点位于链路的一端。每个对等点可以是工作站或服务器。通常，一个对等点充当其网络或 Internet 与另外一个对等点之间的路由器。
- **每个对等点上的同步接口**。一些运行 Solaris 软件的计算机需要购买同步接口卡（如 HSI/P）才能连接到租用线路。其他计算机（如 UltraSPARC 工作站）具有内置同步接口。
- **每个对等点上的 CSU/DSU 同步数字单元**，用于将同步端口连接到租用线路。

  根据所在地区，CSU 可能内置在 DSU 中、由个人拥有或从提供商处租用。DSU 为 Solaris 计算机提供了标准的同步串行接口。通过帧中继，帧中继访问设备 (Frame Relay Access Device, FRAD) 可执行串行接口适配。
- **租用线路**，用于提供交换式或非交换式数字服务。例如 SONET/SDH、帧中继 PVC 和 T1。

租用线路通信期间发生的操作

在大多数类型的租用线路中，对等点实际上不相互拨号。相反，公司购买租用线路服务在两个固定位置之间显式建立连接。有时，位于租用线路两端的两个对等点处于同一公司的不同物理位置。另外一种情况是公司在租用线路上设置用于连接到 ISP 的路由器。

尽管硬连线的链路更容易设置，但租用线路通常没有拨号链路使用广泛。硬连线的链路不需要聊天脚本。租用线路时，由于两个对等点可相互识别，通常不使用验证。两个对等点启动基于链路的 PPP 之后，该链路将保持活动状态。如果线路未失败，或任何一个对等点未显式终止租用线路链路，该链路将会一直保持活动状态。

租用线路上运行 Solaris PPP 4.0 的对等点使用的配置文件大部分与定义拨号链路的配置文件相同。

启动基于租用线路的通信时，将发生以下过程：

1. 每台对等计算机都在引导过程中或在其他管理脚本中运行 `pppd` 命令。
2. 对等点读取其 PPP 配置文件。
3. 对等点协商通信参数。
4. IP 链路建立。

PPP 验证

验证是检验用户是否是其声明的身份的过程。UNIX 登录序列是一种简单形式的验证：

1. `login` 命令提示用户键入名称和口令。
2. 然后，`login` 尝试在口令数据库中查找所键入的用户名和口令以验证该用户。
3. 如果数据库中包含该用户名和口令，则用户将通过**验证**并得到访问系统的权限。如果数据库中不包含该用户名和口令，则将拒绝用户访问系统。

缺省情况下，Solaris PPP 4.0 在未指定缺省路由的计算机上不要求验证。因此，不包含缺省路由的本地计算机不会验证远程呼叫者。相反，如果计算机定义了缺省路由，则计算机会始终验证远程呼叫者。

对于设置连接到您计算机的 PPP 链路的呼叫者，可以使用 PPP 验证协议来检验其身份。相反，如果本地计算机必须呼叫会验证呼叫者的对等点，则必须配置 PPP 验证信息。

验证者和被验证者

由于呼叫者必须向远程对等点证明其身份，所以 PPP 链路上的呼叫计算机被视为**被验证者**。对等点被视为**验证者**。验证者将在安全协议的相应 PPP 文件中查找呼叫者的身份，然后确定是否对呼叫者进行验证。

通常为拨号链路配置 PPP 验证。开始呼叫时，拨出计算机是被验证者。拨入服务器是验证者。服务器中包含一个**机密**文件形式的数据库。此文件列出了被授予可设置连接到服务器的 PPP 链路权限的用户。这些用户被视为**可信呼叫者**。

一些拨出计算机要求远程对等点在响应拨出计算机的呼叫时提供验证信息。然后，它们的角色将互换：远程对等点成为被验证者，而拨出计算机成为验证者。

注 – PPP 4.0 不阻止租用线路对等点的验证，但租用线路链路中通常不使用验证。租用线路合同的性质通常表示，线路两端的参与者可相互识别。两端的参与者通常是可信赖的。但是，由于 PPP 验证并不难于管理，所以应认真考虑实现租用线路的验证。

PPP 验证协议

PPP 验证协议包括口令验证协议 (Password Authentication Protocol, PAP) 和质询握手验证协议 (Challenge-Handshake Authentication Protocol, CHAP)。对于允许链接到本地计算机的每个呼叫者，每一种协议都使用包含呼叫者标识信息（或称为**安全凭证**）的**机密**数据库。有关 PAP 的详细说明，请参见第 452 页中的 “口令验证协议 (Password Authentication Protocol, PAP)”。有关 CHAP 说明，请参见第 455 页中的 “质询握手身份验证协议 (Challenge-Handshake Authentication Protocol, CHAP)”。

为什么使用 PPP 验证？

在 PPP 链路上提供验证是可选的操作。此外，尽管验证会检验对等点是否可信赖，但 PPP 验证不提供数据的机密性。为了保密，可使用加密软件，如 IPsec、PGP、SSL、Kerberos 和 Solaris 安全 Shell。

注 – Solaris PPP 4.0 未实现 RFC 1968 中说明的 PPP 加密控制协议 (Encryption Control Protocol, ECP)。

请考虑在下列情况下实现 PPP 验证。

- 您的公司接受来自基于公共交换式电话网络的用户的传入呼叫。
- 您的公司安全策略要求远程用户在通过公司防火墙访问网络或从事安全事务时提供验证凭证。
- 您需要根据标准 UNIX 口令数据库（如 `/etc/passwd`、NIS、NIS+、LDAP 或 PAM）对呼叫者进行验证。对于此情况使用 PAP 验证。
- 公司的拨入服务器还提供网络的 Internet 连接。对于此情况使用 PAP 验证。
- 串行线路没有位于链路任何一端的计算机或网络上的口令数据库安全。对于此情况使用 CHAP 验证。

通过 PPPoE 支持 DSL 用户

许多网络提供商和在家工作的个人使用数字用户线路 (Digital Subscriber Line, DSL) 技术提供快速的网络访问。为了支持 DSL 用户，Solaris PPP 4.0 包括了基于以太网的 PPP (PPP over Ethernet, PPPoE) 功能。借助 PPPoE 技术，多个主机可以通过一个指向一个或多个目标的以太网链路来运行 PPP 会话。

如果您的情况符合下列之一，则应使用 PPPoE :

- 支持 DSL 用户（可能包括您自己）。您的 DSL 服务提供商要求用户配置 PPPoE 通道来接收基于 DSL 线路的服务。
- 您的站点是计划用于向用户提供 PPPoE 的 ISP。

本节介绍与 PPPoE 关联的术语和基本 PPPoE 拓扑的概述。

PPPoE 概述

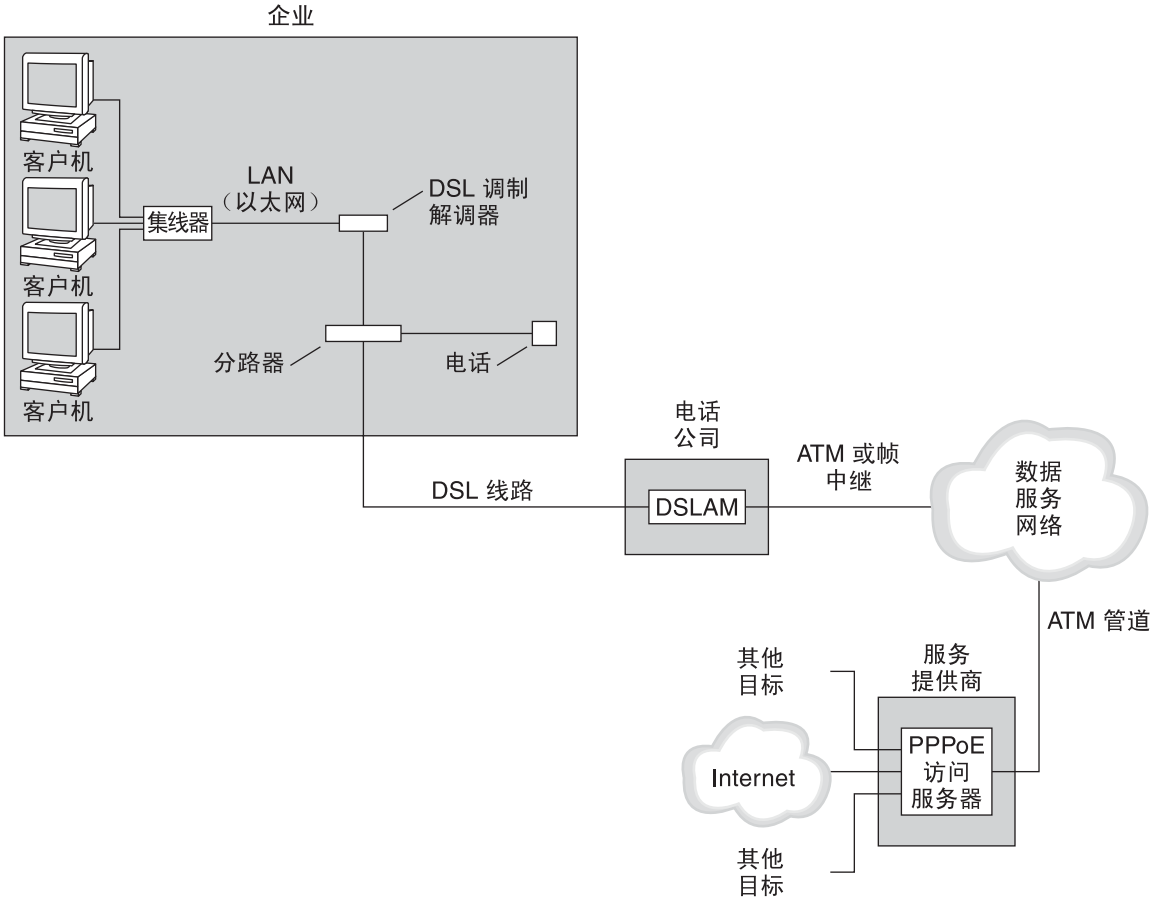
PPPoE 是 RedBack Networks 的专有协议。PPPoE 为搜索协议，而不是标准 PPP 的另一个版本。在 PPPoE 情况中，启动 PPP 通信的计算机必须首先查找（或称为**搜索**）运行 PPPoE 的对等点。PPPoE 协议使用以太网广播包来查找对等点。

在搜索过程之后，PPPoE 通过启动主机（或称为 *PPPoE* **客户机**）设置连接到对等点（*PPPoE* **访问服务器**）的基于以太网的通道。**建立通道**是在一种协议顶端运行另一种协议的做法。使用 PPPoE，Solaris PPP 4.0 可建立基于以太网 IEEE 802.2 的 PPP 通道，这两种协议都是数据链路协议。产生的 PPP 连接就像是 PPPoE 客户机和访问服务器之间的专用连接。有关 PPPoE 的详细信息，请参见第 460 页中的 “创建用于支持 DSL 的 PPPoE 通道”。

PPPoE 配置的各部分

PPPoE 配置中包括三个参与者：使用者、电话公司和服务提供商，如下图所示。

图 15–4 PPPoE 通道中的参与者



PPPoE 使用者

作为系统管理员，您可以帮助使用者配置其 PPPoE。一种常见类型的 PPPoE 使用者是需要基于 DSL 线路运行 PPPoE 的个人。另外一种 PPPoE 使用者是购买 DSL 线路的公司，员工可以通过该线路运行 PPPoE 通道，如上图所示。

公司使用者使用 PPPoE 的主要原因是通过高速的 DSL 设备向大量的主机提供 PPP 通信。通常，单独一台 PPPoE 客户机具有一个 *DSL* **调制解调器**。或者，集线器上的一组客户机可以共享一个 DSL 调制解调器，该调制解调器也通过以太网线路连接到集线器。

注 – 从技术上讲，DSL 设备是网桥而不是调制解调器。但是，由于常见做法将这些设备称为调制解调器，所以本指南使用术语“DSL 调制解调器”。

PPPoE 通过连接到 DSL 调制解调器的以太网线路上的通道运行 PPP。该线路连接到分路器，而分路器又连接到电话线。

电话公司的 PPPoE

电话公司是 PPPoE 方案的中间层。电话公司使用称为**数字用户线路访问多路复用器** *(Digital Subscriber Line Access Multiplexer, DSLAM)* 的设备，对通过电话线路接收的信号进行分路。DSLAM 将信号分离到独立的线路，模拟线路用于电话服务，数字线路用于 PPPoE。通过 DSLAM，数字线路将基于 ATM 数据网络的通道扩展到 ISP。

服务器提供商的 PPPoE

ISP 通过基于网桥的ATM 数据网络接收 PPPoE 传输。在 ISP 位置，运行 PPPoE 的访问服务器充当 PPP 链路的对等点。访问服务器在功能上与图 15–2 中介绍的拨入服务器非常类似，但访问服务器不使用调制解调器。访问服务器将单个 PPPoE 会话转换为常规 IP 流量，如 Internet 访问。

如果您是 ISP 的系统管理员，可能负责配置和维护访问服务器。

PPPoE 通道的安全性

PPPoE 通道实际上并不安全。您可以使用 PAP 或 CHAP 为基于通道运行的 PPP 链路提供用户验证。

◆ ◆ ◆ 第 16 章

16 规划 PPP 链路（任务）

设置 PPP 链路涉及一组独立的任务，其中包括规划任务以及与 PPP 无关的其他活动。本章介绍如何规划最常见的 PPP 链路、如何规划验证以及如何规划 PPPoE。

第 16 章，规划 PPP 链路（任务）后面的任务章节使用配置样例说明如何设置特定链路。本章中介绍了这些配置样例。

具体包含以下主题：

整体 PPP 规划（任务列表）

在实际设置链路之前，PPP 需要对任务进行规划。此外，如果要使用 PPPoE 通道，还必须首先设置 PPP 链路，然后提供通道。以下任务列表列出了本章中讨论的大型规划任务。您可能只需使用针对要配置的链路类型的常规任务。或者，可能需要执行针对链路、验证或 PPPoE 的任务。

表 16–1 PPP 规划的任务列表

任务	说明	参考
规划拨号 PPP 链路	收集设置拨出计算机或拨入服务器需要的信息	第 364 页中的 “规划拨号 PPP 链路”
规划租用线路链路	收集设置租用线路上的客户机需要的信息	第 367 页中的 “规划租用线路链路”
规划 PPP 链路上的验证	收集在 PPP 链路上配置 PAP 或 CHAP 验证需要的信息	第 369 页中的 “规划链路上的验证”

表 16–1 PPP 规划的任务列表 （续）

任务	说明	参考
规划 PPPoE 通道	收集设置可以运行 PPP 链路的 PPPoE 通道需要的信息	第 373 页中的 “规划 PPPoE 通道上的 DSL 支持”

规划拨号 PPP 链路

拨号链路是最常用的 PPP 链路。本节包含以下信息：

- 拨号链路的规划信息
- 第 17 章，设置拨号 PPP 链路（任务）中使用的链路样例说明

通常，只需配置拨号 PPP 链路一端的计算机：拨出计算机或拨入服务器。有关拨号 PPP 的介绍，请参阅第 353 页中的 “拨号 PPP 概述”。

设置拨出计算机之前

配置拨出计算机之前，请收集下表中列出的信息。

注 – 本节中的规划信息不包括要收集的有关验证或 PPPoE 的信息。有关验证规划的详细信息，请参阅第 369 页中的 “规划链路上的验证”。有关 PPPoE 规划的信息，请参阅第 373 页中的 “规划 PPPoE 通道上的 DSL 支持”。

表 16–2 拨出计算机的信息

信息	操作
调制解调器最大速度	请参阅调制解调器制造商提供的文档。
调制解调器连接命令（AT 命令）	请参阅调制解调器制造商提供的文档。
用于链路另一端的拨入服务器的名称	创建有助于标识拨入服务器的任何名称。
拨入服务器所需的登录序列	与拨入服务器的管理员联系或参阅 ISP 文档（如果拨入服务器属于 ISP）。

设置拨入服务器之前

配置拨入服务器之前，请收集下表中列出的信息。

注 – 本节中的规划信息不包括要收集的有关验证或 PPPoE 的信息。有关验证规划的详细信息，请参阅第 369 页中的 “规划链路上的验证”。有关 PPPoE 规划的信息，请参阅第 373 页中的 “规划 PPPoE 通道上的 DSL 支持”。

表 16–3 拨入服务器的信息

信息	操作
调制解调器最大速度	请参阅调制解调器制造商提供的文档。
允许呼叫拨入服务器的人员的用户名	在设置预期用户的起始目录之前，获取这些用户的名称，如第 386 页中的 “如何配置拨入服务器的用户”中所述。
用于 PPP 通信的专用 IP 地址	从贵公司中负责分派 IP 地址的个人获取地址。

拨号 PPP 配置示例

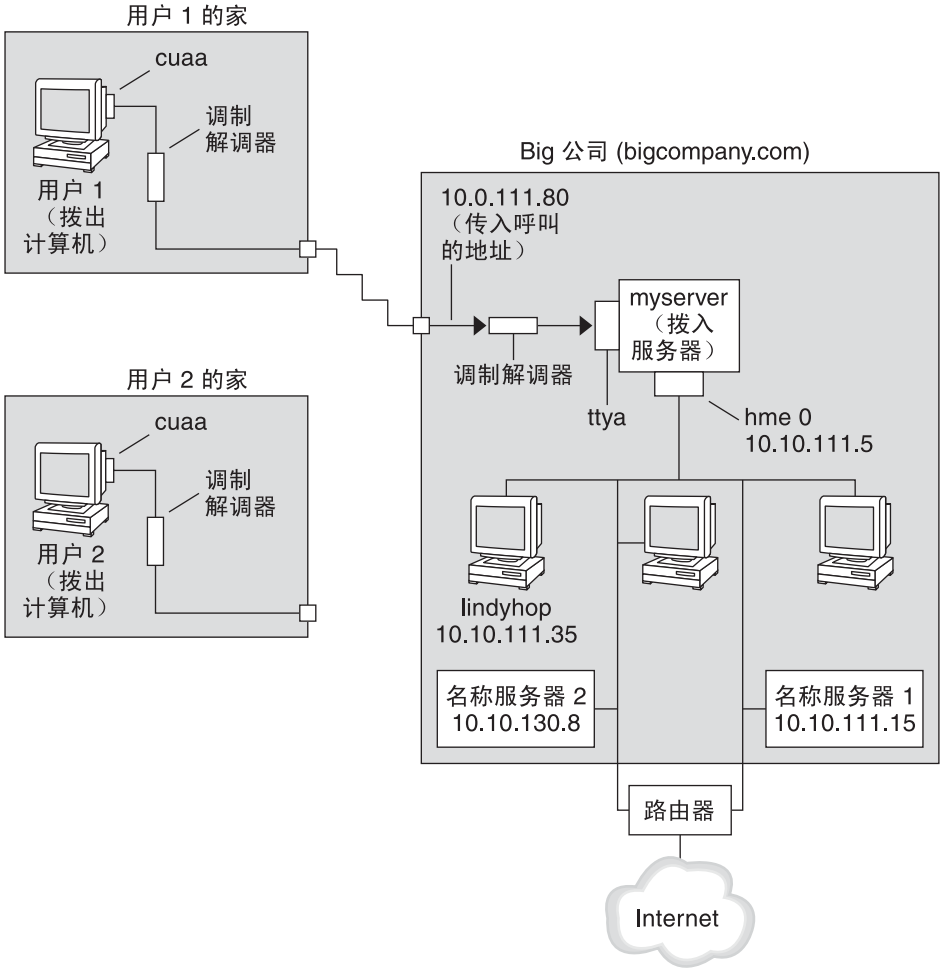
第 17 章，设置拨号 PPP 链路（任务）中将介绍的任务可满足一家小型公司的需求，即允许员工在一周内有几天在家工作。某些员工需要在其家庭计算机上安装 Solaris OS。这些员工还需要远程登录到公司内联网中的工作计算机。

这些任务可设置具有以下特性的基本拨号链路：

- **拨出**计算机位于需要呼叫公司内联网的员工家中。
- **拨入**服务器是公司内联网中配置为接收员工传入呼叫的计算机。
- 使用 UNIX 样式登录验证拨出计算机。公司的安全策略不需要功能更强大的 Solaris PPP 4.0 验证方法。

下图显示了第 17 章，设置拨号 PPP 链路（任务）中设置的链路。

图 16–1 拨号链路样例



在此图中，某台远程主机使用电话线通过调制解调器拨叫 Big Company 的内联网。另一台主机已配置为拨叫 Big Company，但当前处于不活动状态。远程用户的呼叫按与 Big Company 中的拨入服务器相连的调制解调器的接收顺序进行应答。对等点之间建立了 PPP 连接。这样，拨出计算机就可以远程登录到内联网中的主机。

有关拨号 PPP 的更多参考信息

请参阅以下内容：

- 要设置拨出计算机，请参见表 17–2。
- 要设置拨入计算机，请参见表 17–3。

- 要获取拨号链路的概述，请参见第 353 页中的 “拨号 PPP 概述”。
- 要获取 PPP 文件和命令的详细信息，请参见第 433 页中的 “在文件中和命令行上使用 PPP 选项”。

规划租用线路链路

设置租用线路链路涉及配置从提供商处租用的交换式或非交换式服务的一端中的对等点。

本节包含以下信息：

- 租用线路链路的规划信息
- 图 16–2 中所示的链路样例说明

有关租用线路链路的介绍，请参阅第 355 页中的 “租用线路 PPP 概述”。有关设置租用线路的任务，请参见第 18 章，设置租用线路 PPP 链路（任务）。

设置租用线路链路之前

如果您的公司租用网络提供商的租用线路链路，则通常只需配置您所在链路端的系统。链路另一端的对等点由其他管理员维护。此管理员可以是公司远程位置的某个系统管理员，也可以是 ISP 的系统管理员。

租用线路链路需要的硬件

除链路介质外，您所在链路端还需要以下硬件：

- 系统同步接口
- 同步单元 (CSU/DSU)
- 您的系统

某些网络提供商的用户驻地设备 (customer premises equipment, CPE) 中包括路由器、同步接口和 CSU/DSU。但是，必需设备随提供商和您所在地区的政府限制的不同而变化。如果所需设备未随租用线路一起提供，则网络提供商可以提供此设备的相关信息。

要收集的租用线路链路信息

配置本地对等点之前，可能需要收集下表中列出的各项。

表 16–4 规划租用线路链路

信息	操作
接口的设备名称	请参阅接口卡文档。

表 16–4 规划租用线路链路 （续）

信息	操作
同步接口卡的配置说明	请参阅接口卡文档。配置 HSI/P 接口时需要此信息。可能不需要配置其他类型的接口卡。
（可选的）远程对等点的 IP 地址	请参阅服务提供商文档。或者，与远程对等点的系统管理员联系。仅当 IP 地址未在两个对等点之间协商时，才需要此信息。
（可选的）远程对等点的名称	请参阅服务提供商文档。或者，可与远程对等点的系统管理员联系。
（可选的）链路的速度	请参阅服务提供商文档。或者，可与远程对等点的系统管理员联系。
（可选的）远程对等点使用的压缩	请参阅服务提供商文档。或者，可与远程对等点的系统管理员联系。

租用线路链路配置示例

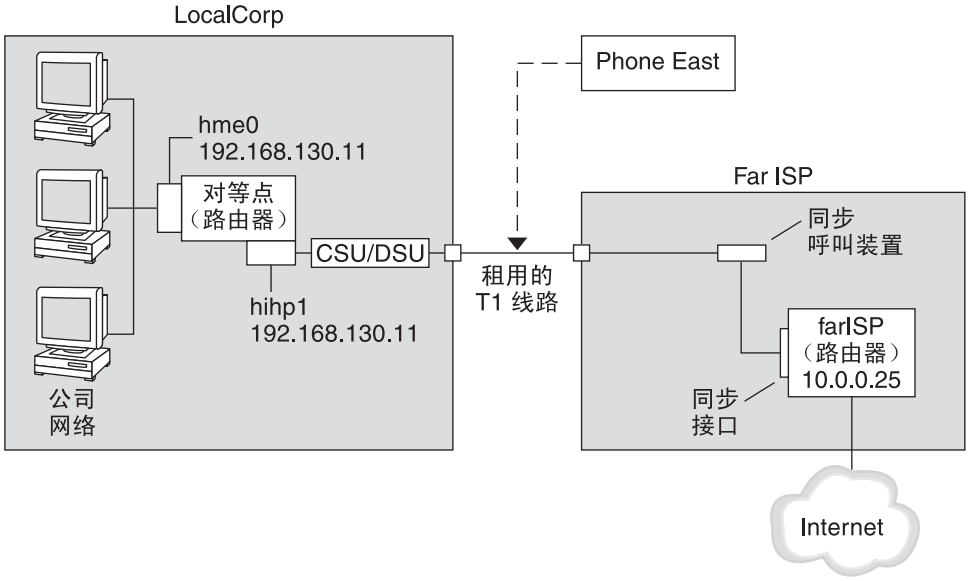
第 18 章，设置租用线路 PPP 链路（任务）中的任务说明如何实现一个中型组织 (LocalCorp) 为其员工提供 Internet 访问的目标。当前，员工的计算机连接到公司的专用内联网。

LocalCorp 需要快速处理和访问 Internet 上的许多资源。该组织与服务提供商 Far ISP 签订合同，以允许 LocalCorp 设置其自己的连接到 Far ISP 的租用线路。然后，LocalCorp 从一家电话公司 Phone East 租用 T1 线路。Phone East 使用租用线路连接 LocalCorp 与 Far ISP。然后，Phone East 为 LocalCorp 提供已配置的 CSU/DSU。

这些任务可设置具有下列特征的租用线路链路。

- LocalCorp 将一个系统设置为网关路由器，用于通过租用线路将包转发至 Internet 上的主机。
- Far ISP 也将一个对等点设置为路由器，用于连接客户的租用线路。

图 16–2 租用线路配置示例



在上图中，在 LocalCorp 中设置了一台路由器以实现 PPP。该路由器通过其 `hme0` 接口与公司内联网相连。第二个连接是通过计算机的 HSI/P 接口 (hihp1) 连接至 CSU/DSU 数字单元。然后，CSU/DSU 连接至已安装的租用线路。LocalCorp 管理员配置 HSI/P 接口和 PPP 文件。然后，该管理员键入 `/etc/init.d/pppd` 以启动 LocalCorp 与 Far ISP 之间的链路。

有关租用线路的更多参考信息

请参阅以下内容：

- 第 18 章，设置租用线路 PPP 链路（任务）
- 第 355 页中的 “租用线路 PPP 概述”

规划链路上的验证

本节包含有关在 PPP 链路上提供验证的规划信息。第 19 章，设置 PPP 验证（任务）包含在您的站点中实现 PPP 验证的任务。

PPP 提供两种类型的验证：PAP（详见第 452 页中的 “口令验证协议 (Password Authentication Protocol, PAP)”）和 CHAP（详见第 455 页中的 “质询握手身份验证协议 (Challenge-Handshake Authentication Protocol, CHAP)”）。

在链路上设置验证之前，必须选择最符合您站点的安全策略的验证协议。然后，为拨入计算机或呼叫者的拨出计算机（或者两种类型的计算机）设置机密文件和 PPP 配置文件。有关为您的站点选择合适的验证协议的信息，请参见第 358 页中的 “为什么使用 PPP 验证？ ”。

本节包含以下信息：

- PAP 和 CHAP 验证的规划信息
- 图 16–3 和图 16–4 中所示的验证方案样例说明

有关设置验证的任务，请参见第 19 章，设置 PPP 验证（任务）。

设置 PPP 验证之前

在您的站点设置验证应该作为 PPP 整体策略一个不可或缺的部分。实现验证之前，应组装硬件、配置软件并测试链路。

表 16–5 配置验证之前的先决条件

信息	参考
配置拨号链路的任务	第 17 章，设置拨号 PPP 链路（任务）。
测试链路的任务	第 21 章，修复常见的 PPP 问题（任务）。
您站点的安全要求	您公司的安全策略。如果没有安全策略，则可通过设置 PPP 验证来创建安全策略。
有关在您的站点中使用 PAP 还是使用 CHAP 的建议	第 358 页中的 “为什么使用 PPP 验证？ ”。有关这些协议的更多详细信息，请参阅第 452 页中的 “验证链路上的呼叫者”。

PPP 验证配置示例

本节介绍要在第 19 章，设置 PPP 验证（任务）的过程中使用的验证方案示例。

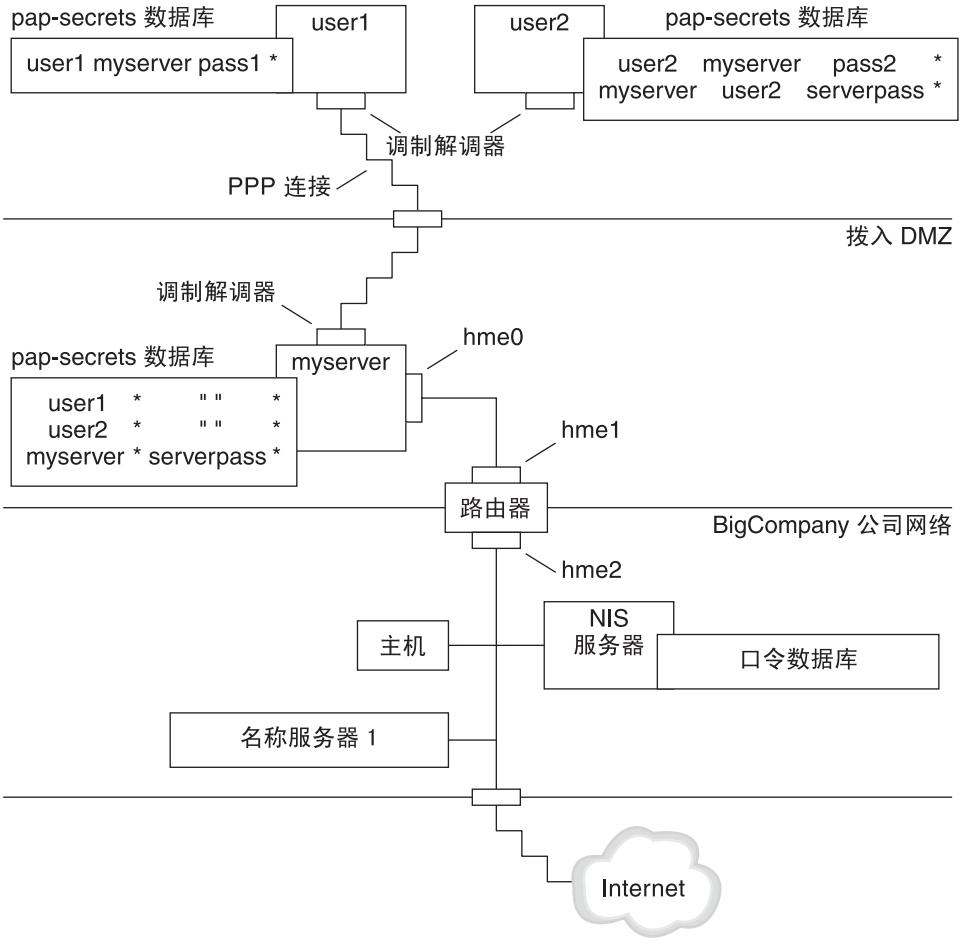
- 第 370 页中的 “使用 PAP 验证的配置示例”
- 第 372 页中的 “使用 CHAP 验证的配置示例”

使用 PAP 验证的配置示例

第 398 页中的 “配置 PAP 验证”中的任务说明如何在 PPP 链路上设置 PAP 验证。这些过程使用为第 365 页中的 “拨号 PPP 配置示例”中虚构的 "Big Company" 创建的 PAP 方案作为示例。

Big Company 希望其用户能够在家工作。系统管理员则希望为连接到拨入服务器的串行线路提供一种安全解决方案。使用 NIS 口令数据库的 UNIX 样式登录已在过去为 Big Company 的网络提供了良好的服务。系统管理员希望对通过 PPP 链路进入网络的呼叫使用类似于 UNIX 的验证方案。因此，管理员可实现使用 PAP 验证的以下方案。

图 16–3 PAP 验证方案示例（在家工作）



系统管理员可创建一个专用的拨入 DMZ，它通过路由器与公司网络的其余部分隔开。术语 DMZ 来自军事术语“非军事化区”。DMZ 是为了安全而设置的一个隔离网络。DMZ 通常包含公司为公众提供的资源，如 Web 服务器、匿名 FTP 服务器、数据库和调制解调器服务器。一般情况下，网络设计者会将 DMZ 放置在防火墙与公司的 Internet 连接之间。

在图 16–3 中，唯一的 DMZ 占用者是拨入服务器 `myserver` 和路由器。设置链路时，拨入服务器要求呼叫者提供 PAP 凭证，包括用户名和口令。此外，拨入服务器还会使用 PAP 的 `login` 选项。因此，呼叫者的 PAP 用户名和口令必须与其在拨入服务器口令数据库中的 UNIX 用户名和口令完全相符。

建立 PPP 链路之后，呼叫者的包将转发到路由器。然后，路由器将传输内容转发到其在公司网络或 Internet 上的目标。

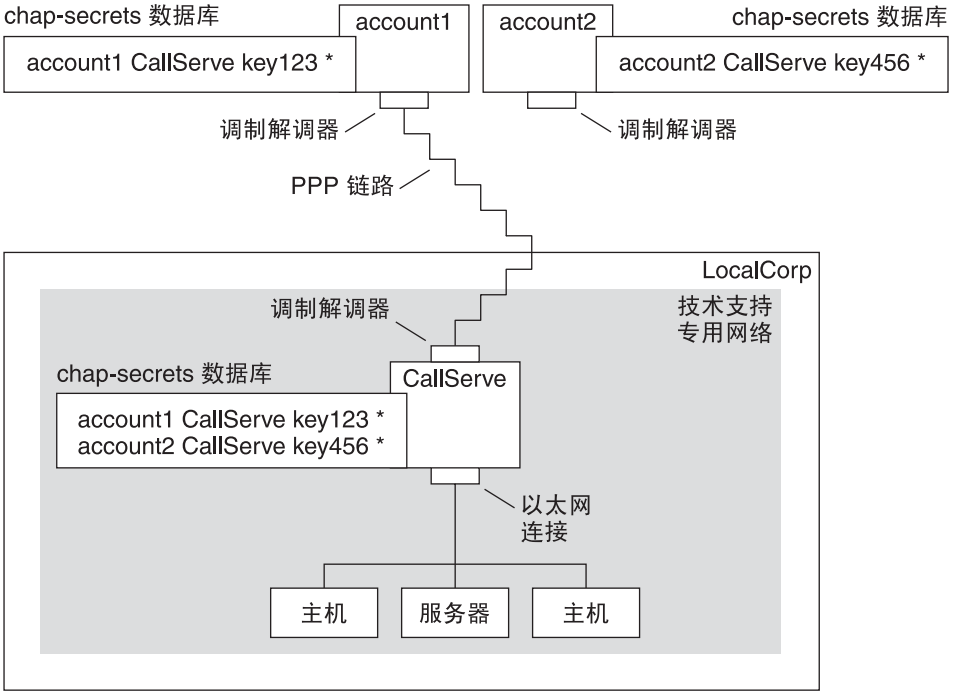
使用 CHAP 验证的配置示例

第 404 页中的 “配置 CHAP 验证”中的任务说明如何设置 CHAP 验证。这些过程使用要为第 368 页中的 “租用线路链路配置示例”中介绍的虚构 LocalCorp 创建的 CHAP 方案作为示例。

LocalCorp 通过连接到 ISP 的租用线路提供与 Internet 的连接。LocalCorp 中的技术支持部门会产生巨大的网络通信流量。因此，技术支持部门需要拥有自己的隔离专用网络。该部门的现场技术人员经常到处出差，他们需要从远程位置访问技术支持部门的网络以获取解决问题的信息。为了保护专用网络数据库中的敏感信息，必须对远程呼叫者进行验证方可授予登录权限。

因此，系统管理员可对拨号 PPP 配置实现以下 CHAP 验证方案。

图 16–4 CHAP 验证方案示例（呼叫专用网络）



技术支持部门网络与外界的唯一链路是连接到拨入服务器所在链路端的串行线路。系统管理员可配置每位现场服务代表的手提电脑，以实现具有 CHAP 安全性（包括 CHAP 机密）的 PPP。在拨入服务器的 chap-secrets 数据库中，包含允许呼入技术支持部门网络的所有计算机的 CHAP 凭证。

有关验证的更多参考信息

请选择以下内容：

- 请参见第 398 页中的 “配置 PAP 验证”。
- 请参见第 404 页中的 “配置 CHAP 验证”。
- 请参见第 452 页中的 “验证链路上的呼叫者”和 pppd(1M) 手册页。

规划 PPPoE 通道上的 DSL 支持

某些 DSL 提供商要求您为站点设置 PPPoE 通道，以便通过提供商的 DSL 线路和高速数字网络运行 PPP。有关 PPPoE 的概述，请参见第 359 页中的 “通过 PPPoE 支持 DSL 用户”。

PPPoE 通道包括三个参与者：使用者、电话公司和 ISP。您可以为您公司的 PPPoE 客户机使用者、家中的使用者或 ISP 服务器的使用者配置 PPPoE。

本节包含有关在客户机和访问服务器上运行 PPPoE 的规划信息。本章包含以下主题：

- PPPoE 主机和访问服务器的规划信息
- 第 374 页中的 “PPPoE 通道配置示例”中介绍的 PPPoE 方案说明

有关设置 PPPoE 通道的任务，请参见第 20 章，设置 PPPoE 通道（任务）。

设置 PPPoE 通道之前

预配置活动取决于您是配置通道的客户端还是服务器端。无论哪种情况，您或您的组织都必须与电话公司签订合同。电话公司为客户机提供 DSL 线路，以及为访问服务器提供某种形式的桥接并可能提供 ATM 管道。在大多数合同中，电话公司都会在您的站点组装其设备。

配置 PPPoE 客户机之前

PPPoE 客户机实现通常包含以下设备：

- 个体使用的个人计算机或其他系统
- DSL 调制解调器，通常由电话公司或 Internet 访问提供商安装
- （可选的）集线器（涉及多台客户机时），适用于公司的 DSL 使用者

- （可选的）分路器，通常由提供商安装

根据用户或公司的需求以及提供商提供的服务，可以使用许多不同的 DSL 配置。

表 16–6 规划 PPPoE 客户机

信息	操作
如果为个人或您自己设置家庭 PPPoE 客户机，请获取 PPPoE 范围之外的任何设置信息。	请求电话公司或 ISP 提供所需的任何设置过程。
如果在公司站点中设置 PPPoE 客户机，请收集被指定 PPPoE 客户机系统的用户的名称。如果配置远程 PPPoE 客户机，则您可能要负责提供有关添加家庭 DSL 设备的用户信息。	请求公司中的管理人员提供已授权用户的列表。
查找 PPPoE 客户机上的可用接口。	在每台计算机上运行 `ifconfig -a` 命令，以列出接口名称。
（可选的）获取 PPPoE 客户机的口令。	请求用户提供其首选口令。或者，为用户指定口令。请注意，此口令用于链路验证，而不用于 UNIX 登录。

配置 PPPoE 服务器之前

规划 PPPoE 访问服务器涉及与电话公司合作，用于提供与其数据服务网络的连接。电话公司将在您的站点上安装其线路（通常为 ATM 管道），并为访问服务器提供某种形式的桥接。您需要配置以太网接口以访问公司提供的服务。例如，您需要配置用于访问 Internet 的接口，以及电话公司网桥的以太网接口。

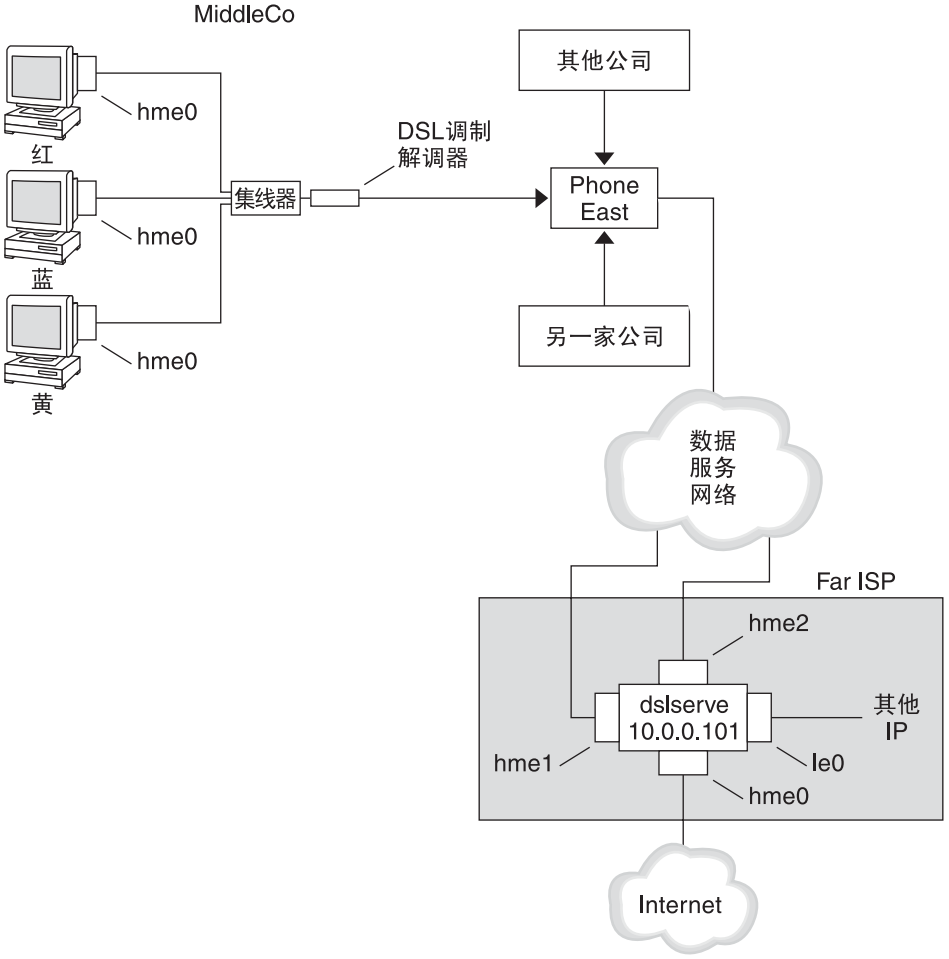
表 16–7 规划 PPPoE 访问服务器

信息	操作
用于数据服务网络中的线路的接口	运行 `ifconfig -a` 命令以标识接口。
PPPoE 服务器提供的服务类型	请求管理人员和网络规划者提出要求和建议。
（可选的）为使用者提供的服务类型	请求管理人员和网络规划者提出要求和建议。
（可选的）远程客户机的主机名和口令	询问网络规划者和您站点中负责合同协商的其他人。主机名和口令用于 PAP 或 CHAP 验证，而不用于 UNIX 登录。

PPPoE 通道配置示例

本节包含 PPPoE 通道示例，用于说明第 20 章，设置 PPPoE 通道（任务）中的任务。虽然下图中显示了通道的所有参与者，但您只管理其中一端：客户端或服务器端。

图 16–5 PPPoE 通道示例



在该样例中，MiddleCo 希望为其员工提供高速 Internet 访问。MiddleCo 从 Phone East 处购买 DSL 包，而 Phone East 又与服务提供商 Far ISP 签订合同。Far ISP 为从 Phone East 处购买 DSL 的客户提供 Internet 和其他 IP 服务。

PPPoE 客户机配置示例

MiddleCo 从为站点提供一条 DSL 线路的 Phone East 处购买包。该包包含一条连接到 MiddleCo 的 PPPoE 客户机 ISP 的已验证专用连接。系统管理员用电缆将预期的 PPPoE 客户机与集线器相连。然后，Phone East 的技术人员用电缆将集线器连接到其 DSL 设备。

PPPoE 服务器配置示例

为了实现 FarISP 与 Phone East 之间的业务安排，FarISP 的系统管理员需要配置访问服务器 `dslserve`。此服务器具有以下四个接口：

- `eri0` — 与本地网络连接的主网络接口
- `hme0` — FarISP 用于为其客户提供 Internet 服务的接口
- `hme1` — MiddleCo 约定用于已验证的 PPPoE 通道的接口
- `hme2` — 其他客户约定用于其 PPPoE 通道的接口

有关 PPPoE 的更多参考信息

请选择以下内容：

- 请参见第 410 页中的 “设置 PPPoE 客户机”。
- 请参见第 412 页中的 “设置 PPPoE 访问服务器”。
- 请参见第 460 页中的 “创建用于支持 DSL 的 PPPoE 通道”以及 `pppoed(1M)`、`pppoec(1M)` 和 `sppptun(1M)` 手册页。

◆ ◆ ◆ 第 17 章

17 设置拨号 PPP 链路（任务）

本章介绍配置最常见的 PPP 链路（即拨号链路）的任务。主要主题如下：

设置拨号 PPP 链路的主要任务（任务列表）

您可通过配置调制解调器、修改网络数据库文件以及修改表 22–1 中描述的 PPP 配置文件来设置拨号 PPP 链路。

下表列出了配置拨号 PPP 链路两端的主要任务。通常，您只需配置该链路的一端，拨出计算机或拨入服务器。

表 17–1 设置拨号 PPP 链路的任务列表

任务	说明	参考
1. 收集预配置信息	设置链路之前，收集所需数据，例如对等主机名、目标电话号码和调制解调器速度。	第 364 页中的 “规划拨号 PPP 链路”
2. 配置拨出计算机	在通过该链路进行呼叫的计算机上设置 PPP。	表 17–2
3. 配置拨入服务器	在接收传入呼叫的计算机上设置 PPP。	表 17–3
4. 呼叫拨入服务器	键入 pppd 命令以启动通信。	第 389 页中的 “如何呼叫拨入服务器”

配置拨出计算机

本节中的任务说明如何配置拨出计算机。这些任务以图 16–1 中介绍的从家中拨入方案为例。您可以在将计算机提供给预期用户之前，在公司执行这些任务。或者，可以指导有经验的用户设置其家庭计算机。设置拨出计算机的任何用户都必须对该计算机具有 root 权限。

配置拨出计算机的任务（任务列表）

表 17–2 设置拨出计算机的任务列表

任务	说明	参考
1. 收集预配置信息	设置链路之前，收集所需数据，例如对等主机名、目标电话号码和调制解调器速度。	第 364 页中的 “规划拨号 PPP 链路”
2. 配置调制解调器和串行端口	设置调制解调器和串行端口。	第 379 页中的 “如何配置调制解调器和串行端口（拨出计算机）”
3. 配置串行线路通信	配置串行线路的传输特性。	第 380 页中的 “如何定义串行线路上的通信”
4. 定义拨出计算机与对等点之间的会话	收集创建聊天脚本时使用的通信数据。	第 381 页中的 “如何创建用于呼叫对等点的指令”
5. 配置有关特定对等点的信息	配置用于呼叫单个拨入服务器的 PPP 选项。	第 382 页中的 “如何定义与单个对等点的连接”
6. 呼叫对等点	键入 `pppd` 命令以启动通信。	第 389 页中的 “如何呼叫拨入服务器”

拨号 PPP 模板文件

Solaris PPP 4.0 提供了模板文件。每个模板都包含特定 PPP 配置文件的公用选项。下表列出了可用于设置拨号链路的样例模板以及与其等效的 Solaris PPP 4.0 文件。

模板文件	PPP 配置文件	参考
`/etc/ppp/options.tmpl`	`/etc/ppp/options`	第 437 页中的 “`/etc/ppp/options.tmpl` 模板”
`/etc/ppp/options.ttya.tmpl`	`/etc/ppp/options.`*ttyname*	第 439 页中的 “`options.ttya.tmpl` 模板文件”
`/etc/ppp/myisp-chat.tmpl`	采用所选名称且用以包含聊天脚本的文件	第 445 页中的 “`/etc/ppp/myisp-chat.tmpl` 聊天脚本模板”

模板文件	PPP 配置文件	参考
/etc/ppp/peers/myisp.tmpl	/etc/ppp/peers/*peer-name*	第 442 页中的 “/etc/ppp/peers/myisp.tmpl 模板文件”

如果您决定使用其中一个模板文件，请务必将该模板重命名为与其等效的 PPP 配置文件。但聊天文件模板 /etc/ppp/myisp-chat.tmpl 例外。您可以为聊天脚本选择任何名称。

配置拨出计算机上的设备

设置拨出 PPP 计算机的第一个任务是配置串行线路中的设备：调制解调器和串行端口。

注 – 适用于调制解调器的任务通常适用于 ISDN TA。

执行下一过程之前，必须完成下列操作。

- 在拨出计算机上安装 Solaris 发行版
- 确定调制解调器的最佳速度
- 确定所要使用的拨出计算机串行端口
- 获取拨出计算机的超级用户口令

有关规划信息，请参见表 16–2。

▼ 如何配置调制解调器和串行端口（拨出计算机）

1 对调制解调器进行编程。

虽然存在多种类型的调制解调器，但大多数调制解调器出厂时都具有适合 Solaris PPP 4.0 的正确设置。以下列出了使用 Solaris PPP 4.0 的调制解调器的基本参数设置。

- **DCD** – 遵照载体说明
- **DTR** – 设置得较低，以便调制解调器挂起，并使调制解调器处于挂机状态
- **流控制** – 设置为 RTS/CTS，以便进行全双工硬件流控制
- **注意序列** – 禁用

如果在设置链路时遇到问题，并且怀疑调制解调器出现故障，请首先参阅调制解调器制造商所提供的文档。此外，许多 Web 站点都提供了有关调制解调器编程方面的帮助。最后，您可以从第 425 页中的 “如何诊断调制解调器问题”中获得一些解决调制解调器问题的建议。

2 将调制解调器电缆与拨出计算机的串行端口以及电话插口相连。

3 **成为拨出计算机的超级用户或承担等效角色。**

角色包含授权和具有特权的命令。有关角色的更多信息，请参见《系统管理指南：安全性服务》中的“配置 RBAC（任务列表）”。

4 **如《 系统管理指南：高级管理 》中的“使用串行端口工具设置终端和调制解调器（ 概述 ）”中所述，运行 `/usr/sadm/bin/smc` 命令。此命令用于打开 Solaris Management Console。**

使用 Solaris Management Console 可执行以下操作。

a. **选择与调制解调器相连的端口。**

b. **将调制解调器方向指定为仅拨出。**

您可以将调制解调器设置为双向。但是，选择仅拨出更安全，这样可以阻止可能的侵入者。

注 – 您可以通过 `/usr/sadm/bin/smc` 设置波特率和超时。但是，`pppd` 守护进程将忽略这些设置。

---

5 **单击“确定”应用更改。**

配置拨出计算机的通信

本节中的各个过程说明如何配置拨出计算机串行线路上的通信。使用这些过程之前，必须首先对调制解调器和串行端口进行配置，如第 379 页中的 “如何配置调制解调器和串行端口（拨出计算机）”中所述。

以下任务说明如何启用拨出计算机，以成功启动与拨入服务器的通信。通信是按照 PPP 配置文件中的选项所定义的方式启动的。需要创建以下文件：

- `/etc/ppp/options`
- `/etc/ppp/options.`*ttyname*
- 聊天脚本
- `/etc/ppp/peers/`*peer-name*

Solaris PPP 4.0 提供了 PPP 配置文件模板，您可以根据需要定制这些模板。有关这些文件的详细信息，请参阅第 378 页中的 “拨号 PPP 模板文件”。

▼ 如何定义串行线路上的通信

1 **成为拨出计算机的超级用户或承担等效角色。**

角色包含授权和具有特权的命令。有关角色的更多信息，请参见《系统管理指南：安全性服务》中的“配置 RBAC（任务列表）”。

2 **使用以下项创建名为 /etc/ppp/options 的文件：**

```
lock
```

/etc/ppp/options 文件由本地计算机用来定义适用于所有通信的全局参数。lock 选项启用 UUCP 样式锁定，格式为 /var/spool/locks/LK.xxx.yyy.zzz。

注 – 如果拨出计算机没有 /etc/ppp/options 文件，则只有超级用户才能运行 pppd 命令。但是，/etc/ppp/options 可以为空。

有关 /etc/ppp/options 的完整说明，请参阅第 437 页中的 “/etc/ppp/options 配置文件”。

3 **可选创建名为 /etc/ppp/options.*ttyname* 的文件，用于定义从特定串行端口启动通信的方式。**

以下示例显示了设备名称为 /dev/cua/a 的端口的 /etc/ppp/options. *ttyname* 文件。

```
# cat /etc/ppp/options.cua.a
crtscts
```

PPP 选项 crtscts 指示 pppd 守护进程针对串行端口 a 打开硬件流控制。

有关 /etc/ppp/options.ttyname 文件的更多信息，请转至第 438 页中的 “/etc/ppp/options.*ttyname* 配置文件”。

4 **按照第 385 页中的 “如何设置调制解调器速度”中所述，设置调制解调器速度。**

▼ 如何创建用于呼叫对等点的指令

在拨出计算机启动 PPP 链路之前，必须收集有关将成为对等点的拨入服务器的信息。然后，使用此信息创建聊天脚本，用于描述拨出计算机与对等点之间的实际会话。

1 **确定拨出计算机的调制解调器所需的运行速度。**

有关更多信息，请参见第 443 页中的 “配置拨号链路的调制解调器速度”。

2 **从拨入服务器的站点获取以下信息：**

- 服务器的电话号码
- 使用的验证协议（如果适用）
- 对于聊天脚本对等点所需的登录序列

3 **获取拨入服务器站点中的名称服务器的名称和 IP 地址。**

4 **在聊天脚本中，提供用于启动呼叫特定对等点的指令。**

例如，可以创建以下聊天脚本 /etc/ppp/mychat，以呼叫拨入服务器 myserver。

```
SAY "Calling the peer\n"
        TIMEOUT 10
        ABORT BUSY
        ABORT 'NO CARRIER'
        ABORT ERROR
        REPORT CONNECT
        "" AT&F1&M5S2=255
        TIMEOUT 60
        OK ATDT1-123-555-1234
        CONNECT \c
        SAY "Connected; logging in.\n"
        TIMEOUT 5
        ogin:--ogin: pppuser
        TIMEOUT 20
        ABORT 'ogin incorrect'
        ssword: \qmypassword
        "% " \c
        SAY "Logged in.  Starting PPP on peer system.\n"
        ABORT 'not found'
        "" "exec pppd"
        ~ \c
```

该脚本包含用于呼叫需要登录序列的 Solaris 拨入服务器的指令。有关每条指令的说明，请参阅第 447 页中的 “用于 UNIX 样式登录的增强型基本聊天脚本”。有关创建聊天脚本的完整详细信息，请阅读第 443 页中的 “定义拨号链路上的会话”一节。

注 – 不要直接调用该聊天脚本，而应将聊天脚本的文件名用作 chat 命令的参数来调用该脚本。

如果对等点运行 Solaris 或类似操作系统，请考虑将上述聊天脚本用作拨出计算机的模板。

▼ 如何定义与单个对等点的连接

1 **成为拨出计算机的超级用户或承担等效角色。**

角色包含授权和具有特权的命令。有关角色的更多信息，请参见《系统管理指南：安全性服务》中的“配置 RBAC（任务列表）”。

2 **通过创建以下 /etc/resolv.conf 文件来更新 DNS 数据库：**

```
domain bigcompany.com
nameserver 10.10.111.15
nameserver 10.10.130.8
```

domain bigcompany.com

指定对等点的 DNS 域为 bigcompany.com。

nameserver 10.10.111.15 和 **nameserver 10.10.130.8**
列出 bigcompany.com 中的名称服务器的 IP 地址。

3 **编辑 /etc/nsswitch.conf 文件，指示首先在 DNS 数据库中搜索主机信息。**

```
hosts:      dns [NOTFOUND=return] files
```

4 **为对等点创建文件。**

例如，可以创建以下文件来定义拨入服务器 myserver：

```
# cat /etc/ppp/peers/myserver
/dev/cua/a
57600
noipdefault
defaultroute
idle 120
noauth
connect "chat -U 'mypassword' -T 1-123-555-1213 -f /etc/ppp/mychat"
```

/dev/cua/a
指定应将设备 /dev/cua/a 用作呼叫 myserver 的串行接口。

57600
定义链路的速度。

noipdefault
指定对于使用对等点 myserver 的事务，拨出计算机的初始 IP 地址为 0.0.0.0。myserver 会为每个拨号会话的拨出计算机分配一个 IP 地址。

idle 120
指示链路在空闲 120 秒之后必须超时。

noauth
指定对等点 myserver 在与拨出计算机协商连接时，无需提供验证凭证。

connect "chat -U 'mypassword' -T 1-123-555-1213 -f /etc/ppp/mychat"
指定 connect 选项及其参数，包括对等点的电话号码以及带有呼叫指令的聊天脚本 /etc/ppp/mychat。

另请参见 以下列出了相关的参考信息。

- 要配置其他拨出计算机，请参见第 379 页中的 “如何配置调制解调器和串行端口（拨出计算机）”。
- 要通过拨叫其他计算机来测试调制解调器的连通性，请参见 cu(1C) 和 tip(1) 手册页。这些实用程序有助于您测试调制解调器的配置是否正确。此外，这些实用程序还可用于测试是否可与另一台计算机建立连接。
- 要了解有关配置文件和选项的更多信息，请参见第 433 页中的 “在文件中和命令行上使用 PPP 选项”。
- 要配置拨入服务器，请参见第 384 页中的 “配置拨入服务器上的设备”。

配置拨入服务器

本节中的任务用于配置拨入服务器。拨入服务器是一台通过 PPP 链路接收拨出计算机的呼叫的对等计算机。这些任务说明如何配置图 16–1 中介绍的拨入服务器 `myserver`。

配置拨入服务器的任务（任务列表）

表 17–3 设置拨入服务器的任务列表

任务	说明	参考
1. 收集预配置信息	设置链路之前，收集所需数据，例如对等主机名、目标电话号码和调制解调器速度。	第 364 页中的 “规划拨号 PPP 链路”
2. 配置调制解调器和串行端口	设置调制解调器和串行端口。	第 384 页中的 “如何配置调制解调器和串行端口（拨入服务器）”
3. 配置呼叫对等点信息	为允许呼叫拨入服务器的每台拨出计算机设置用户环境和 PPP 选项。	第 386 页中的 “如何配置拨入服务器的用户”
4. 配置串行线路通信	配置串行线路的传输特性。	第 387 页中的 “如何定义串行线路上的通信（拨入服务器）”

配置拨入服务器上的设备

以下过程说明如何配置拨入服务器的调制解调器和串行端口。

执行下一过程之前，必须在对等拨入服务器上完成下列活动：

- 安装 Solaris 发行版
- 确定调制解调器的最佳速度
- 决定要使用的串行端口

▼ 如何配置调制解调器和串行端口（拨入服务器）

1 **按照调制解调器制造商所提供的文档中的说明，对调制解调器进行编程。**

有关其他建议，请参阅第 379 页中的 “如何配置调制解调器和串行端口（拨出计算机）”。

2 **连接调制解调器和拨入服务器上的串行端口。**

3. **成为拨入服务器的超级用户或承担等效角色。**

   角色包含授权和具有特权的命令。有关角色的更多信息，请参见《系统管理指南：安全性服务》中的“配置 RBAC（任务列表）”。

4. **使用 Solaris Management Console 的 `/usr/sadm/bin/smc` 命令配置串行端口，如《系统管理指南：高级管理》中的“使用串行端口工具设置终端和调制解调器（概述）”中所述。**

   使用 Solaris Management Console 可执行以下操作：

   a. **选择与调制解调器相连的串行端口。**

   b. **将调制解调器方向指定为仅拨入。**

      注 – Solaris PPP 4.0 支持调制解调器进行双向通信。

   c. **单击“确定”应用更改。**

▼ 如何设置调制解调器速度

下一过程说明如何设置拨入服务器的调制解调器速度。有关 Oracle Corporation 计算机使用的速度的建议，请参见第 443 页中的 “配置拨号链路的调制解调器速度”。

1. **登录到拨入服务器。**

2. **使用 `tip` 命令访问调制解调器。**

   有关使用 `tip` 设置调制解调器速度的说明，请参阅 `tip`(1) 手册页。

3. **将调制解调器配置为固定 DTE 速率。**

4. **使用 `ttymon` 或 `/usr/sadm/bin/smc` 将串行端口锁定为该速率，如《系统管理指南：高级管理》中的“使用串行端口工具设置终端和调制解调器（概述）”中所述。**

另请参见 以下列出了相关的参考信息。

- 第 384 页中的 “如何配置调制解调器和串行端口（拨入服务器）”
- 第 386 页中的 “如何配置拨入服务器的用户”

设置拨入服务器的用户

设置拨入服务器的过程中涉及配置有关每个已知远程呼叫者的信息。

开始本节中的过程之前，必须完成以下操作：

- 获取允许从远程拨出计算机登录的所有用户的 UNIX 用户名。
- 按照第 384 页中的 “如何配置调制解调器和串行端口（拨入服务器）”中的说明，设置调制解调器和串行线路。
- 确定指定给远程用户传入呼叫的专用 IP 地址。如果潜在呼叫者数超出拨入服务器上调制解调器和串行端口数，则可考虑创建一个专用的传入 IP 地址。有关创建专用 IP 地址的完整信息，请转至第 458 页中的 “为呼叫者创建 IP 寻址方案”。

▼ 如何配置拨入服务器的用户

1. **成为拨入服务器的超级用户或承担等效角色。**

   角色包含授权和具有特权的命令。有关角色的更多信息，请参见《系统管理指南：安全性服务》中的“配置 RBAC（任务列表）”。

2. **在拨入服务器上为每个远程 PPP 用户创建一个新帐户。**

   可以使用 Solaris Management Console 来新建用户。`/usr/sadm/bin/smc` 命令用于打开 Solaris Management Console。有关通过 Solaris Management Console 创建新用户的说明，请参见《系统管理指南：基本管理》中的“设置用户帐户（任务列表）”。

3. **使用 Solaris Management Console 为新用户指定参数。**

   例如，下表显示了拨出计算机 `myhome` 上 `user1` 的 `pppuser` 帐户的参数。

参数	值	定义
用户名	`pppuser`	远程用户的用户帐户名。此帐户名应与聊天脚本登录序列中指定的帐户名相符。例如，`pppuser` 是第 381 页中的 “如何创建用于呼叫对等点的指令”的聊天脚本中的帐户名。
登录 Shell	`/usr/bin/pppd`	远程用户的缺省登录 Shell。登录 Shell `/usr/bin/pppd` 最初会将呼叫者限制到专用 PPP 环境。
创建起始目录路径	`/export/home/pppuser`	当呼叫者成功登录到拨入服务器时，将设置起始目录 `/export/home/pppuser`。

4 **为每个呼叫者创建一个 $HOME/.ppprc 文件，用于包含各种特定于用户 PPP 会话的选项。**

例如，可为 pppuser 创建以下 .ppprc 文件。

```
# cat /export/home/pppuser/.ppprc
noccp
```

noccp 用于禁用链路上的压缩控制。

另请参见 以下列出了相关的参考信息。

- 第 386 页中的 “如何配置拨入服务器的用户”。
- 第 387 页中的 “如何定义串行线路上的通信（拨入服务器）”。

配置拨入服务器的通信

以下任务说明如何启用拨入服务器以打开与任何拨出计算机的通信。以下 PPP 配置文件中定义的选项可确定如何建立通信。

- /etc/ppp/options
- /etc/ppp/options.*ttyname*

有关这些文件的详细信息，请参阅第 433 页中的 “在文件中和命令行上使用 PPP 选项”。

继续之前，应完成以下操作：

- 配置拨入服务器的串行端口和调制解调器，如第 384 页中的 “如何配置调制解调器和串行端口（拨入服务器）”中所述。
- 配置有关拨入服务器的预期用户的信息，如第 386 页中的 “如何配置拨入服务器的用户”中所述。

▼ 如何定义串行线路上的通信（拨入服务器）

1 **成为拨入服务器的超级用户或承担等效角色。**

角色包含授权和具有特权的命令。有关角色的更多信息，请参见《系统管理指南：安全性服务》中的“配置 RBAC（任务列表）”。

2 **使用以下项创建 /etc/ppp/options 文件。**

nodefaultroute

nodefaultroute 表明如果没有 root 特权，则本地系统上的任何 pppd 会话都无法建立缺省路由。

注 – 如果拨入服务器没有 `/etc/ppp/options` 文件，则只有超级用户才能运行 `pppd` 命令。但是，`/etc/ppp/options` 文件可以为空。

3 **创建文件 `/etc/options.`*ttyname*，以定义如何处理通过串行端口 *ttyname* 接收的呼叫。**

以下 `/etc/options.ttya` 文件定义了拨入服务器的串行端口 `/dev/ttya` 处理传入呼叫的方式。

```
:10.0.0.80
xonxoff
```

`:10.0.0.80` 为通过串行端口 `ttya` 呼入的所有对等点指定 IP 地址 10.0.0.80

`xonxoff` 允许串行线路在启用了软件流控制的情况下处理来自调制解调器的通信

另请参见 如果按照本章中的所有过程进行操作，则至此已完成拨号链路配置。以下列出了相关的参考信息。

- 要通过拨叫其他计算机来测试调制解调器的连通性，请参见 cu(1C) 和 tip(1) 手册页。这些实用程序有助于您测试调制解调器的配置是否正确。此外，这些实用程序还可用于测试是否可与另一台计算机建立连接。
- 要为拨入服务器配置更多选项，请参见第 384 页中的 “配置拨入服务器”。
- 要配置更多拨出计算机，请参见第 378 页中的 “配置拨出计算机”。
- 要指示远程计算机呼叫拨入服务器，请参见第 388 页中的 “呼叫拨入服务器”。

呼叫拨入服务器

通过指示拨出计算机呼叫拨入服务器，可建立拨号 PPP 链路。您可通过在本地 PPP 配置文件中指定 `demand` 选项，指示拨出计算机呼叫服务器。但是，建立该链路的最常用方法是让用户在拨出计算机上运行 `pppd` 命令。

继续执行下面的任务之前，应完成下面的一个或两个操作：

- 按照第 378 页中的 “配置拨出计算机”中所述，设置拨出计算机
- 按照第 384 页中的 “配置拨入服务器”中所述，设置拨入服务器

▼ 如何呼叫拨入服务器

1 **使用一般用户帐户而不是 root 登录到拨出计算机。**

2 **通过运行 pppd 命令来呼叫拨入服务器。**

例如，以下命令将启动拨出计算机与拨入服务器 myserver 之间的链路：

```
% pppd 57600 call myserver
```

pppd	通过调用 pppd 守护进程来启动呼叫
57600	设置主机与调制解调器之间的线路速度
call myserver	调用 pppd 的 call 选项。pppd，然后读取在第 382 页中的 “如何定义与单个对等点的连接”中创建的 /etc/ppp/peers/myserver 文件中的选项。

3 **与服务器网络中的某台主机联系，例如，图 16–1 中所示的主机 lindyhop：**

```
ping lindyhop
```

如果链路未正常工作，请参阅第 21 章，修复常见的 PPP 问题（任务）。

4 **终止 PPP 会话：**

```
% pkill -x pppd
```

另请参见 如果按照本章中的所有过程进行操作，则至此已完成拨号链路配置。以下列出了相关的参考信息。

- 要指示用户开始在其拨出计算机上工作，请参见第 389 页中的 “如何呼叫拨入服务器”。
- 要解决链路上的问题，请参见第 21 章，修复常见的 PPP 问题（任务）。
- 要了解有关本章中使用的文件和选项的更多信息，请参见第 433 页中的 “在文件中和命令行上使用 PPP 选项”。

◆ ◆ ◆ 第 18 章

18 设置租用线路 PPP 链路（任务）

本章介绍如何配置在对等点之间使用租用线路的 PPP 链路。主要章节包括：

设置租用线路（任务列表）

与设置拨号链路相比，设置租用线路链路相对比较容易。在大多数情况下，您都无需配置 CSU/DSU、拨号服务或验证。如果您确实需要配置 CSU/DSU，请参阅制造商所提供的文档以获取有关此复杂任务的帮助。

下面的任务列表中介绍了与基本租用线路链路设置有关的所有任务。

注 – 某些类型的租用线路确实需要 CSU/DSU，才能对另外一个对等点的地址进行“拨号”。例如，帧中继使用交换式虚拟电路 (Switched Virtual Circuit, SVC) 或交换式 56 服务。

表 18–1 设置租用线路链路的任务列表

任务	说明	参考
1. 收集预配置信息	设置链路之前，收集所需数据。	表 16–4
2. 设置租用线路硬件	组装 CSU/DSU 和同步接口卡。	第 392 页中的 “如何配置同步设备”
3. 如果需要，配置接口卡	配置启动租用线路时要使用的接口脚本。	第 392 页中的 “如何配置同步设备”
4. 配置有关远程对等点的信息	定义本地机器和远程对等点之间的通信的工作方式。	第 393 页中的 “如何配置租用线路上的计算机”
5. 启动租用线路	作为引导过程的一部分，将计算机配置为在租用线路上启动 PPP。	第 393 页中的 “如何配置租用线路上的计算机”

配置租用线路上的同步设备

本节中的任务涉及配置第 368 页中的 “租用线路链路配置示例”中介绍的租用线路拓扑所需的设备。连接租用线路需要的同步设备包括接口和调制解调器。

设置同步设备的先决条件

执行下一过程之前，必须具有下列各项：

- 由提供商安装在您站点中的工作租用线路
- 同步单元 (CSU/DSU)
- 在系统上安装的 Solaris 发行版
- 您的系统所需类型的同步接口卡

▼ 如何配置同步设备

1 **如有必要，将接口卡物理安装在本地机器中。**

按照制造商所提供的文档说明进行操作。

2 **将 CSU/DSU 电缆连接到接口。**

如有必要，将 CSU/DSU 电缆连接到租用线路插口或类似连接器。

3 **根据制造商或网络提供商所提供的文档说明配置 CSU/DSU。**

注 – 提供租用线路的提供商可能会为您的链路提供和配置 CSU/DSU。

---

4 **如有必要，按照接口文档的说明配置接口卡。**

配置接口卡涉及为接口创建启动脚本。在图 16–2所示的租用线路配置中，位于 LocalCorp 的路由器使用 HSI/P 接口卡。

以下脚本 `hsi-conf` 用于启动 HSI/P 接口。

```
#!/bin/ksh
/opt/SUNWconn/bin/hsip_init hihp1 speed=1536000 mode=fdx loopback=no \
nrzi=no txc=txc rxc=rxc txd=txd rxd=rxd signal=no 2>&1 > /dev/null
```

`hihp1`	指示使用的同步端口为 HSI/P
`speed=1536000`	设置该项以指示 CSU/DSU 的速度

另请参见 要配置租用线路上的本地机器，请参阅第 393 页中的 “如何配置租用线路上的计算机”。

配置租用线路上的计算机

本节中的任务说明如何设置路由器，以使其在租用线路的末端（您所在的一端）充当本地对等点。该任务以第 368 页中的 “租用线路链路配置示例”中介绍的租用线路为例。

配置租用线路上的本地机器的先决条件

执行下一过程之前，必须完成下列操作：

- 按照第 392 页中的 “配置租用线路上的同步设备”中介绍的方法，安装并配置链路的同步设备
- 获取租用线路上本地机器的超级用户口令
- 将本地机器设置为在网络上作为路由器来运行，以使用租用线路提供商提供的服务

▼ 如何配置租用线路上的计算机

1 成为本地计算机（路由器）的超级用户或承担等效角色。

角色包含授权和具有特权的命令。有关角色的更多信息，请参见《系统管理指南：安全性服务》中的“配置 RBAC（任务列表）”。

2 在路由器的 `/etc/hosts` 文件中，为远程对等点添加项。

```
# cat /etc/hosts
#
# Internet host table
#
127.0.0.1       localhost
192.168.130.10  local2-peer        loghost
192.168.130.11  local1-net
10.0.0.25       farISP
```

`/etc/hosts` 文件示例适用于虚构的 LocalCorp 中的本地路由器。请注意服务提供商的远程对等点 `farISP` 的 IP 地址和主机名。

3 创建文件 `/etc/ppp/peers/`*peer-name* 以保留有关提供商对等点的信息。

在以下租用线路链路示例中，将创建文件 `/etc/ppp/peers/farISP`。

```
# cat /etc/ppp/peers/farISP
init '/etc/ppp/conf_hsi'
local
/dev/hihp1
sync
noauth
192.168.130.10:10.0.0.25
passive
persist
noccp
```

```
nopcomp
novj
noaccomp
```

下表对 /etc/ppp/peers/farISP 中使用的各个选项和参数进行了说明。

选项	定义
init '/etc/ppp/conf_hsi'	启动链路。然后，init 使用脚本 /etc/ppp/conf_hsi 中的参数配置 HSI 接口。
local	指示 pppd 守护进程不要更改数据终端就绪 (Data Terminal Ready, DTR) 信号的状态。此外，还指示 pppd 忽略数据载波检测 (Data Carrier Detect, DCD) 输入信号。
/dev/hihp1	指定同步接口的设备名称。
sync	为链路建立同步编码。
noauth	确定本地系统不需要求从其对等点进行验证。但是，对等点仍会要求验证。
192.168.130.10:10.0.0.25	定义本地对等点和远程对等点的 IP 地址，并用冒号分隔。
passive	指示本地计算机上的 pppd 守护进程在发出最大数目的 LCP 配置请求后保持静默，并等待对等点启动。
persist	指示 pppd 守护进程在连接终止后尝试重新启动链路。
noccp, nopcomp, novj, noaccomp	分别禁用压缩控制协议 (Compression Control Protocol, CCP)、协议字段压缩、Van Jacobson 压缩以及地址和控制字段压缩。这些形式的压缩可加快拨号链路上的传输，但可能会降低租用线路的速度。

4 创建名为 demand 的初始化脚本，以作为引导过程的一部分创建 PPP 链路。

```
# cat /etc/ppp/demand
#!/bin/sh
if [ -f /var/run/ppp-demand.pid ] &&
   /usr/bin/kill -s 0 `/bin/cat /var/run/ppp-demand.pid`
then
        :
else
        /usr/bin/pppd call farISP
fi
```

demand 脚本包含用于建立租用线路链路的 pppd 命令。下表对 $PPPDIR/demand 的内容进行了说明。

代码样例	说明
if [-f /var/run/ppp-demand.pid] && /usr/bin/kill -s 0 `/bin/cat /var/run/ppp-demand.pid`	这些行用于检查 pppd 是否正在运行。如果 pppd 正在运行，则无需启动它。

代码样例	说明
`/usr/bin/pppd call farISP`	此行用于启动 `pppd`。 `pppd` 从 `/etc/ppp/options` 读取选项。此外，命令行中的 `call farISP` 选项也会使其读取 `/etc/ppp/peers/farISP`。

作为引导过程的一部分，Solaris PPP 4.0 启动脚本 `/etc/rc2.d/S47pppd` 会调用 `demand` 脚本。`/etc/rc2.d/S47pppd` 中的以下行用于搜索是否存在名为 `$PPPDIR/demand` 的文件。

```
if [ -f $PPPDIR/demand ]; then
            . $PPPDIR/demand
    fi
```

如果找到该文件，则执行 `$PPPDIR/demand`。在执行 `$PPPDIR/demand` 过程中，将建立链路。

注 – 要访问本地网络以外的计算机，请指示用户运行 `telnet`、`ftp`、`rsh` 或类似命令。

另请参见 如果您已按照本章中的所有过程进行操作，则至此已完成租用线路链路的配置。以下列出了相关的参考信息。

- 要查找故障排除信息，请参见第 431 页中的 “修复租用线路问题”。
- 要了解有关本章中使用的文件和选项的更多信息，请参见第 433 页中的 “在文件中和命令行上使用 PPP 选项”。

◆ ◆ ◆ 第 19 章

19 设置 PPP 验证（任务）

本章介绍设置 PPP 验证的任务，具体包含以下主题：

- 第 398 页中的 “配置 PAP 验证”
- 第 404 页中的 “配置 CHAP 验证”

这些过程说明如何基于拨号链路实现验证，因为与租用线路链路相比，配置拨号链路进行验证的可能性更大。如果公司的安全策略要求基于租用线路进行验证，则可以配置该验证。可使用本章中的任务来指导租用线路验证。

如果要使用 PPP 验证，但又不能确定应使用的协议，请查看第 358 页中的 “为什么使用 PPP 验证？ ”一节。有关 PPP 验证的更多详细信息，请参阅 pppd(1M) 手册页和第 452 页中的 “验证链路上的呼叫者”。

配置 PPP 验证（任务列表）

本节包含有助于您快速访问 PPP 验证过程的任务列表。

表 19–1 常规 PPP 验证的任务列表

任务	说明	参考
配置 PAP 验证	使用这些过程在拨入服务器和拨出计算机上启用 PAP 验证。	第 398 页中的 “设置 PAP 验证（任务列表）”
配置 CHAP 验证	使用这些过程在拨入服务器和拨出计算机上启用 CHAP 验证。	第 404 页中的 “设置 CHAP 验证（任务列表）”

配置 PAP 验证

本节中的任务说明如何使用口令验证协议 (Password Authentication Protocol, PAP) 在 PPP 链路上实现验证。这些任务使用第 370 页中的 “PPP 验证配置示例”中的示例来说明拨号链路的 PAP 工作方案。请根据这些说明在您的站点上实现 PAP 验证。

执行后续过程之前，必须完成下列操作：

- 设置并测试拨入服务器与属于可信呼叫者的拨出计算机之间的拨号链路
- 理论上，对于拨入服务器验证，必须获取管理网络口令数据库（例如，在 LDAP、NIS 或本地文件中）的计算机的超级用户权限
- 获取本地计算机（拨入服务器或拨出计算机）的超级用户权限

设置 PAP 验证（任务列表）

借助下面的任务列表，可快速访问针对拨入服务器和针对拨出计算机上的可信呼叫者的 PAP 相关任务。

表 19–2 PAP 验证的任务列表（拨入服务器）

任务	说明	参考
1. 收集预配置信息	收集验证所需的用户名和其他数据。	第 369 页中的 “规划链路上的验证”
2. 如有必要，更新口令数据库	确保所有可能的呼叫者均位于服务器的口令数据库中。	第 399 页中的 “如何创建 PAP 凭证数据库（拨入服务器）”
3. 创建 PAP 数据库	在 `/etc/ppp/pap-secrets` 中为所有预期呼叫者创建安全凭证。	第 399 页中的 “如何创建 PAP 凭证数据库（拨入服务器）”
4. 修改 PPP 配置文件	将特定于 PAP 的选项添加到 `/etc/ppp/options` 和 `/etc/ppp/peers/`*peer-name* 文件中。	第 400 页中的 “如何将 PAP 支持添加到 PPP 配置文件（拨入服务器）”

表 19–3 PAP 验证的任务列表（拨出计算机）

任务	说明	参考
1. 收集预配置信息	收集验证所需的用户名和其他数据。	第 369 页中的 “规划链路上的验证”
2. 为可信呼叫者的计算机创建 PAP 数据库	在 `/etc/ppp/pap-secrets` 中为可信呼叫者创建安全凭证，如有必要，还为呼叫拨出计算机的其他用户创建安全凭证。	第 401 页中的 “如何为可信呼叫者配置 PAP 验证凭证”
3. 修改 PPP 配置文件	将特定于 PAP 的选项添加到 `/etc/ppp/options` 和 `/etc/ppp/peers/`*peer-name* 文件中。	第 403 页中的 “如何将 PAP 支持添加到 PPP 配置文件（拨出计算机）”

在拨入服务器上配置 PAP 验证

要设置 PAP 验证，必须执行以下操作：

- 创建 PAP 凭证数据库
- 修改 PPP 配置文件以支持 PAP

▼ 如何创建 PAP 凭证数据库（拨入服务器）

此过程修改 `/etc/ppp/pap-secrets` 文件，该文件包含用于对链路上的呼叫者进行验证的 PAP 安全凭证。PPP 链路上的两台计算机中必须都存在 `/etc/ppp/pap-secrets`。

图 16–3 中介绍的 PAP 配置样例使用了 PAP 的 `login` 选项。如果计划使用此选项，则可能还需要更新网络的口令数据库。有关 `login` 选项的更多信息，请参阅第 455 页中的“使用带有 `login` 选项的 `/etc/ppp/pap-secrets`”。

1. **汇编包含所有可能的可信呼叫者的列表。可信呼叫者是将被授予从其远程计算机呼叫拨入服务器的权限的人员。**

2. **检验每个可信呼叫者在拨入服务器的口令数据库中是否已具有 UNIX 用户名和口令。**

   注 – 对于使用 PAP 的 `login` 选项对呼叫者进行验证的 PAP 配置样例，这种检验尤其重要。如果选择不实现 PAP 的 `login` 选项，则呼叫者的 PAP 用户名不必与其 UNIX 用户名相符。有关标准 `/etc/ppp/pap-secrets` 的信息，请参阅第 452 页中的“`/etc/ppp/pap-secrets` 文件”。

   如果某个可能的可信呼叫者没有 UNIX 用户名和口令，请执行以下操作：

   a. **向您不认识的呼叫者的管理者确认其是否具有访问拨入服务器的权限。**

   b. **在公司安全策略的指导下，为这些呼叫者创建 UNIX 用户名和口令。**

3. **成为拨入服务器的超级用户或承担等效角色。**

   角色包含授权和具有特权的命令。有关角色的更多信息，请参见《系统管理指南：安全性服务》中的“配置 RBAC（任务列表）”。

4. **编辑 `/etc/ppp/pap-secrets` 文件。**

   此发行版在 `/etc/ppp` 中提供了一个 `pap-secrets` 文件，该文件包含有关如何使用 PAP 验证的注释，但不包含任何选项。可以在注释末尾添加以下选项。

```
user1      myserver        ""          *
user2      myserver        ""          *
myserver   user2           serverpass  *
```

要使用 /etc/ppp/pap-secrets 的 login 选项，必须键入每个可信呼叫者的 UNIX 用户名。只要第三个字段中出现一组双引号 ("")，就会在服务器的口令数据库中查找该呼叫者的口令。

myserver * serverpass * 项包含拨入服务器的 PAP 用户名和口令。在图 16–3 中，可信呼叫者 user2 需要从远程对等点进行验证。因此，myserver 的 /etc/ppp/pap-secrets 文件包含与 user2 建立链路时要使用的 PAP 凭证。

另请参见 以下列出了相关的参考信息。

- 第 400 页中的“修改 PPP 配置文件以进行 PAP 验证（拨入服务器）”
- 第 401 页中的“为可信呼叫者配置 PAP 验证（拨出计算机）”

修改 PPP 配置文件以进行 PAP 验证（拨入服务器）

本节中的任务说明如何更新任何现有 PPP 配置文件，以支持在拨入服务器上进行 PAP 验证。

▼ 如何将 PAP 支持添加到 PPP 配置文件（拨入服务器）

此过程以第 387 页中的“如何定义串行线路上的通信（拨入服务器）”中介绍的 PPP 配置文件为例。

1. **以超级用户身份登录到拨入服务器或承担等效角色。**

   角色包含授权和具有特权的命令。有关角色的更多信息，请参见《系统管理指南：安全性服务》中的“配置 RBAC（任务列表）”。

2. **将验证选项添加到 /etc/ppp/options 文件中。**

   例如，将以粗体显示的选项添加到现有 /etc/ppp/options 文件中，以实现 PAP 验证：

   ```
   lock
   auth
   login
   nodefaultroute
   proxyarp
   ms-dns 10.0.0.1
   idle 120
   ```

auth	指定服务器必须在建立链路之前对呼叫者进行验证。
login	指定应使用标准 UNIX 用户验证服务对远程呼叫者进行验证。
nodefaultroute	表明如果没有 root 特权，则本地系统上的任何 pppd 会话都无法建立缺省路由。

`proxyarp`	在系统的地址解析协议 (Address Resolution Protocol, ARP) 表中添加项，用于指定对等点的 IP 地址和系统的以太网地址。使用此选项，对等点看起来位于其他系统的本地以太网中。
`ms-dns 10.0.0.1`	启用 `pppd` 以便为客户机提供域名服务器 (Domain Name Server, DNS) 地址 `10.0.0.1`。
`idle 120`	指定将在两分钟后断开空闲用户的连接。

3 **在 `/etc/ppp/options.cua.a` 文件中，为 `cua/a` 用户添加以下地址。**

```
:10.0.0.2
```

4 **在 `/etc/ppp/options.cua.b` 文件中，为 `cua/b` 用户添加以下地址。**

```
:10.0.0.3
```

5 **在 `/etc/ppp/pap-secrets` 文件中，添加以下项。**

```
*     *          ""      *
```

注 – 如前所述，`login` 选项提供必需的用户验证。`/etc/ppp/pap-secrets` 文件中的此项是使用 `login` 选项启用 PAP 的标准方法。

另请参见 有关如何为拨入服务器的可信呼叫者配置 PAP 验证凭证，请参阅第 401 页中的 “为可信呼叫者配置 PAP 验证（拨出计算机）”。

为可信呼叫者配置 PAP 验证（拨出计算机）

本节包含在可信呼叫者的拨出计算机上设置 PAP 验证的任务。作为系统管理员，在将 PAP 凭证分发给预期呼叫者之前，可在系统上设置 PAP 验证。或者，如果远程呼叫者已经有自己的计算机，则可以指导这些呼叫者完成本节中的任务。

为可信呼叫者配置 PAP 涉及两个任务：

- 配置呼叫者的 PAP 安全凭证
- 配置呼叫者的拨出计算机以支持 PAP 验证

▼ 如何为可信呼叫者配置 PAP 验证凭证

此过程说明如何为两个可信呼叫者设置 PAP 凭证，其中一个可信呼叫者需要来自远程对等点的验证凭证。此过程中的步骤假定，作为系统管理员的您要在可信呼叫者的拨出计算机上创建 PAP 凭证。

1. **成为拨出计算机的超级用户或承担等效角色。**

   角色包含授权和具有特权的命令。有关角色的更多信息，请参见《系统管理指南：安全性服务》中的“配置 RBAC（任务列表）”。

   使用图 16–3 中介绍的 PAP 配置样例，并假定拨出计算机属于 `user1`。

2. **修改呼叫者的 pap-secrets 数据库。**

   此发行版提供了一个包含有用注释但不包含任何选项的 `/etc/ppp/pap-secrets` 文件。可以将以下选项添加到此 `/etc/ppp/pap-secrets` 文件中。

   ```
   user1    myserver  pass1    *
   ```

   请注意，`user1` 的口令 `pass1` 以可读的 ASCII 格式在链路中传递。`myserver` 是呼叫者 `user1` 的对等点名称。

3. **成为另一台拨出计算机的超级用户或承担等效角色。**

   角色包含授权和具有特权的命令。有关角色的更多信息，请参见《系统管理指南：安全性服务》中的“配置 RBAC（任务列表）”。

   使用 PAP 验证示例，并假定此拨出计算机属于呼叫者 `user2`。

4. **修改呼叫者的 pap-secrets 数据库。**

   可以将以下选项添加到现有 `/etc/ppp/pap-secrets` 文件的末尾。

   ```
   user2     myserver   pass2       *
   myserver  user2      serverpass  *
   ```

   在此示例中，`/etc/ppp/pap-secrets` 有两个项。第一个项包含 `user2` 传递给拨入服务器 `myserver` 以进行验证的 PAP 安全凭证。

   作为链路协商的一部分，`user2` 需要拨入服务器的 PAP 凭证。因此，`/etc/ppp/pap-secrets` 的第二行中还包含期望来自 `myserver` 的 PAP 凭证。

注 – 由于大多数 ISP 不提供验证凭证，因此要与 ISP 进行通信，上述方案可能不切实际。

另请参见 以下列出了相关的参考信息。

- 第 399 页中的“如何创建 PAP 凭证数据库（拨入服务器）”
- 第 401 页中的“如何为可信呼叫者配置 PAP 验证凭证”

修改 PPP 配置文件以进行 PAP 验证（拨出计算机）

以下任务说明如何更新现有 PPP 配置文件，以支持在可信呼叫者的拨出计算机上进行 PAP 验证。

此过程使用以下参数在属于图 16–3 中介绍的 user2 的拨出计算机上配置 PAP 验证。user2 要求传入呼叫者对呼叫（包括来自拨入服务器 myserver 的呼叫）进行验证。

▼ 如何将 PAP 支持添加到 PPP 配置文件（拨出计算机）

此过程以第 380 页中的“如何定义串行线路上的通信”中介绍的 PPP 配置文件为例。此过程将配置属于 user2 的拨出计算机，如图 16–3 中所示。

1 **以超级用户身份登录到拨出计算机。**

2 **修改 /etc/ppp/options 文件。**

以下 /etc/ppp/options 文件包含 PAP 支持选项，如粗体所示。

```
# cat /etc/ppp/options
lock
name user2
auth
require-pap
```

name user2　将 user2 设置为本地计算机上用户的 PAP 名称。如果使用 login 选项，则 PAP 名称必须与口令数据库中该用户的 UNIX 用户名相同。

auth　说明拨出计算机在建立链路之前必须对呼叫者进行验证。

注 – 虽然大多数拨出计算机不要求从其对等点进行验证，但此拨出计算机要求这样做。可使用任意一种方法。

---

require-pap　要求来自对等点的 PAP 凭证。

3 **为远程计算机 myserver 创建 /etc/ppp/peers/*peer-name* 文件。**

以下示例说明如何将 PAP 支持添加到第 382 页中的“如何定义与单个对等点的连接”中创建的现有 /etc/ppp/peers/myserver 文件。

```
# cat /etc/ppp/peers/myserver
/dev/cua/a
57600
noipdefault
defaultroute
idle 120
user user2
remotename myserver
connect "chat -U 'mypassword' -f /etc/ppp/mychat"
```

以粗体显示的新选项用于添加对等点 myserver 的 PAP 要求。

user user2　将 user2 定义为本地计算机的用户名

remotename myserver　　将 myserver 定义为要求来自本地计算机的验证凭证的对等点

另请参见　以下列出了相关的参考信息。

- 要通过呼叫拨入服务器来测试 PAP 验证设置，请参见第 389 页中的 “如何呼叫拨入服务器”。
- 有关 PAP 验证的更多信息，请参见第 452 页中的 “口令验证协议 (Password Authentication Protocol, PAP)”。

配置 CHAP 验证

本节中的任务说明如何使用质询握手身份验证协议 (Challenge-Handshake Authentication Protocol, CHAP) 在 PPP 链路上实现验证。这些任务使用图 16–4 中的示例来说明进行专用网络拨号的 CHAP 工作方案。请根据这些说明在您的站点上实现 CHAP 验证。

执行后续过程之前，必须完成下列操作：

- 设置并测试拨入服务器与属于可信呼叫者的拨出计算机之间的拨号链路
- 获取本地计算机（拨入服务器或拨出计算机）的超级用户权限

设置 CHAP 验证（任务列表）

表 19–4　CHAP 验证的任务列表（拨入服务器）

任务	说明	参考
1. 将 CHAP 机密指定给所有可信呼叫者	创建呼叫者的 CHAP 机密，或指示呼叫者创建自己的 CHAP 机密。	第 405 页中的 “如何创建 CHAP 凭证数据库（拨入服务器）”
2. 创建 chap-secrets 数据库	将所有可信呼叫者的安全凭证添加到 /etc/ppp/chap-secrets 文件中。	第 405 页中的 “如何创建 CHAP 凭证数据库（拨入服务器）”
3. 修改 PPP 配置文件	将特定于 CHAP 的选项添加到 /etc/ppp/options 和 /etc/ppp/peers/*peer-name* 文件中。	第 406 页中的 “如何将 CHAP 支持添加到 PPP 配置文件（拨入服务器）”

表 19–5　CHAP 验证的任务列表（拨出计算机）

任务	说明	参考
1. 为可信呼叫者的计算机创建 CHAP 数据库	在 /etc/ppp/chap-secrets 中为可信呼叫者创建安全凭证，如有必要，还为呼叫拨出计算机的其他用户创建安全凭证。	第 405 页中的 “如何创建 CHAP 凭证数据库（拨入服务器）”

表 19–5 CHAP 验证的任务列表（拨出计算机） （续）

任务	说明	参考
2. 修改 PPP 配置文件	将特定于 CHAP 的选项添加到 /etc/ppp/options 文件中。	第 408 页中的“如何将 CHAP 支持添加到 PPP 配置文件（拨出计算机）”

在拨入服务器上配置 CHAP 验证

设置 CHAP 验证的第一个任务是修改 /etc/ppp/chap-secrets 文件。此文件包含用于对链路上的呼叫者进行验证的 CHAP 安全凭证（包括 CHAP 机密）。

注 – UNIX 或 PAM 验证机制对 CHAP 无效。例如，不能按第 399 页中的“如何创建 PAP 凭证数据库（拨入服务器）”中所述的内容使用 PPP login 选项。如果验证方案需要 PAM 或 UNIX 样式的验证，请改为选择 PAP。

以下过程为专用网络中的拨入服务器实现 CHAP 验证。PPP 链路是与外界的唯一连接。网络管理员（可能包括系统管理员）已对可访问网络的那些呼叫者授予权限。

▼ 如何创建 CHAP 凭证数据库（拨入服务器）

1 **汇编包含所有可信呼叫者的用户名的列表。**

可信呼叫者包括所有已授予呼叫专用网络权限的人员。

2 **为每个用户指定 CHAP 机密。**

注 – 务必选择不易猜出的可靠 CHAP 机密。CHAP 机密的内容无任何其他限制。

指定 CHAP 机密的方法取决于站点的安全策略。或者由您负责创建机密，或者呼叫者必须创建自己的机密。如果您不负责指定 CHAP 机密，则务必获取由每个可信呼叫者创建的、或为每个可信呼叫者创建的 CHAP 机密。

3 **成为拨入服务器的超级用户或承担等效角色。**

角色包含授权和具有特权的命令。有关角色的更多信息，请参见《系统管理指南：安全性服务》中的“配置 RBAC（任务列表）”。

4 **修改 /etc/ppp/chap-secrets 文件。**

此发行版提供了一个包含有用注释但不包含任何选项的 /etc/ppp/chap-secrets 文件。可以在现有 /etc/ppp/chap-secrets 文件的末尾为服务器 CallServe 添加以下选项。

```
account1  CallServe   key123   *
account2  CallServe   key456   *
```

key123 是可信呼叫者 account1 的 CHAP 机密。

key456 是可信呼叫者 account2 的 CHAP 机密。

另请参见 以下列出了相关的参考信息。

- 第 405 页中的 “如何创建 CHAP 凭证数据库（拨入服务器）”
- 第 406 页中的 “如何将 CHAP 支持添加到 PPP 配置文件（拨入服务器）”
- 第 407 页中的 “为可信呼叫者配置 CHAP 验证（拨出计算机）”

修改 PPP 配置文件以进行 CHAP 验证（拨入服务器）

本节中的任务说明如何更新现有 PPP 配置文件，以支持在拨入服务器上进行 CHAP 验证。

▼ 如何将 CHAP 支持添加到 PPP 配置文件（拨入服务器）

1. **以超级用户身份登录到拨入服务器。**

2. **修改 /etc/ppp/options 文件。**

   添加以粗体显示的 CHAP 支持选项。

   ```
   # cat /etc/ppp/options
   lock
   nodefaultroute
   name CallServe
   auth
   ```

name *CallServe*	将 *CallServe* 定义为本地计算机（在此实例中为拨入服务器）上用户的 CHAP 名称
auth	使本地计算机在建立链路之前对呼叫者进行验证

3. **创建其他 PPP 配置文件以支持可信呼叫者。**

   请参见第 386 页中的 “如何配置拨入服务器的用户”和第 387 页中的 “如何定义串行线路上的通信（拨入服务器）”。

另请参见 要为可信呼叫者配置 CHAP 验证凭证，请参阅第 405 页中的 “如何创建 CHAP 凭证数据库（拨入服务器）”。

为可信呼叫者配置 CHAP 验证（拨出计算机）

本节包含在可信呼叫者的拨出计算机上设置 CHAP 验证的任务。根据站点的安全策略，可以由您或可信呼叫者负责设置 CHAP 验证。

在远程呼叫者配置 CHAP 的情况下，应确保该呼叫者的本地 CHAP 机密与拨入服务器的 /etc/ppp/chap-secrets 文件中该呼叫者的等效 CHAP 机密匹配。然后，指示这些呼叫者执行本节中的任务以配置 CHAP。

为可信呼叫者配置 CHAP 涉及两个任务：

- 创建呼叫者的 CHAP 安全凭证
- 配置呼叫者的拨出计算机以支持 CHAP 验证

▼ 如何为可信呼叫者配置 CHAP 验证凭证

此过程说明如何为两个可信呼叫者设置 CHAP 凭证。此过程中的步骤假定，作为系统管理员的您要在可信呼叫者的拨出计算机上创建 CHAP 凭证。

1 **成为拨出计算机的超级用户或承担等效角色。**

角色包含授权和具有特权的命令。有关角色的更多信息，请参见《系统管理指南：安全性服务》中的“配置 RBAC（任务列表）”。

使用第 372 页中的 “使用 CHAP 验证的配置示例”中的 CHAP 配置样例，并假定拨出计算机属于可信呼叫者 account1。

2 **修改呼叫者 account1 的 chap-secrets 数据库。**

此发行版提供了一个包含有用注释但不包含任何选项的 /etc/ppp/chap-secrets 文件。可以将以下选项添加到现有 /etc/ppp/chap-secrets 文件中。

```
account1   CallServe    key123    *
```

CallServe 是 account1 要尝试访问的对等点的名称。key123 是将用于 account1 与 CallServer 之间的链路的 CHAP 机密。

3 **成为另一台拨出计算机的超级用户或承担等效角色。**

角色包含授权和具有特权的命令。有关角色的更多信息，请参见《系统管理指南：安全性服务》中的“配置 RBAC（任务列表）”。

假定此计算机属于呼叫者 account2。

4 **修改呼叫者 account2 的 /etc/ppp/chap-secrets 数据库。**

```
account2   CallServe    key456    *
```

现在，account2 将机密 key456 作为在指向对等点 CallServe 的链路上使用的 CHAP 凭证。

另请参见 以下列出了相关的参考信息。

- 第 405 页中的 “如何创建 CHAP 凭证数据库（拨入服务器）”
- 第 407 页中的 “如何为可信呼叫者配置 CHAP 验证凭证”

将 CHAP 添加到配置文件（拨出计算机）

要了解有关 CHAP 验证的更多信息，请参阅第 455 页中的 “质询握手身份验证协议 (Challenge-Handshake Authentication Protocol, CHAP)”。下一任务将配置拨出计算机，该拨出计算机属于在第 372 页中的 “使用 CHAP 验证的配置示例”中介绍的呼叫者 `account1`。

▼ 如何将 CHAP 支持添加到 PPP 配置文件（拨出计算机）

1. **以超级用户身份登录到拨出计算机。**

2. **确保 `/etc/ppp/options` 文件包含以下选项。**

```
# cat /etc/ppp/options
lock
nodefaultroute
```

3. **为远程计算机 `CallServe` 创建 `/etc/ppp/peers/`*peer-name* 文件。**

```
# cat /etc/ppp/peers/CallServe
/dev/cua/a
57600
noipdefault
defaultroute
idle 120
user account1
connect "chat -U 'mypassword' -f /etc/ppp/mychat"
```

选项 `user account1` 将 `account1` 设置为指定给 `CallServe` 的 CHAP 用户名。有关以上文件中其他选项的说明，请参见第 382 页中的 “如何定义与单个对等点的连接”中类似的 `/etc/ppp/peers/myserver` 文件。

另请参见 要通过呼叫拨入服务器来测试 CHAP 验证，请参阅第 389 页中的 “如何呼叫拨入服务器”。

◆ ◆ ◆ 第 20 章

20 设置 PPPoE 通道（任务）

本章介绍在 PPPoE 通道的任何一端设置参与者（PPPoE 客户机和 PPPoE 访问服务器）的任务。包含以下特定主题：

- 第 409 页中的“设置 PPPoE 通道的主要任务（任务列表）”
- 第 410 页中的“设置 PPPoE 客户机”
- 第 412 页中的“设置 PPPoE 访问服务器”

这些任务以第 373 页中的“规划 PPPoE 通道上的 DSL 支持”中介绍的方案为例。有关 PPPoE 概述，请参阅第 359 页中的“通过 PPPoE 支持 DSL 用户”。

设置 PPPoE 通道的主要任务（任务列表）

下表列出了配置 PPPoE 客户机和 PPPoE 访问服务器的主要任务。要在您的站点实现 PPPoE，只需设置您所在的 PPPoE 通道的一端（客户端或访问服务器端）。

表 20–1 设置 PPPoE 客户机的任务列表

任务	说明	参考
1. 配置 PPPoE 接口	定义要用于 PPPoE 通道的以太网接口。	第 410 页中的“如何配置 PPPoE 客户机接口”
2. 配置有关 PPPoE 访问服务器的信息	为 PPPoE 通道的服务提供商端的访问服务器定义参数。	第 411 页中的“如何定义 PPPoE 访问服务器对等点”
3. 设置 PPP 配置文件	定义客户机的 PPP 配置文件（如果尚未定义）。	第 380 页中的“如何定义串行线路上的通信”
4. 创建通道	呼叫访问服务器。	第 411 页中的“如何定义 PPPoE 访问服务器对等点”

表 20–2 设置 PPPoE 访问服务器的任务列表

任务	说明	参考
1. 设置 PPPoE 访问服务器	定义要用于 PPPoE 通道的以太网接口以及访问服务器提供的服务。	第 412 页中的 “如何设置 PPPoE 访问服务器”
2. 设置 PPP 配置文件	定义客户机的 PPP 配置文件（如果尚未定义）。	第 387 页中的 “配置拨入服务器的通信”
3. （可选的）限制接口的使用	使用 PPPoE 选项和 PAP 验证，将特定的以太网接口限制为仅某些客户机可使用。	第 414 页中的 “如何将接口限制为仅特定客户机可使用”

设置 PPPoE 客户机

要通过 DSL 为客户机系统提供 PPP，必须首先在与相应调制解调器或集线器相连的接口上配置 PPPoE。然后，需要更改 PPP 配置文件，以便在 PPPoE 的另外一端定义访问服务器。

设置 PPPoE 客户机的先决条件

设置 PPPoE 客户机之前，必须完成下列操作：

- 在要使用 PPPoE 通道的客户机上，安装 Solaris 发行版。
- 联系服务提供商，了解有关其 PPPoE 访问服务器的信息。
- 指示电话公司或服务提供商组装客户机使用的设备。这些设备包括 DSL 调制解调器和分路器等，最好由电话公司而非您来组装这些设备。

▼ 如何配置 PPPoE 客户机接口

使用此过程可定义要用于 PPPoE 通道的以太网接口。

1 **成为 PPPoE 客户机的超级用户或承担等效角色。**

角色包含授权和具有特权的命令。有关角色的更多信息，请参见《系统管理指南：安全性服务》中的“配置 RBAC（任务列表）”。

2 **将连接到 DSL 的以太网接口名称添加到 `/etc/ppp/pppoe.if` 文件中。**

例如，对于将 `hme0` 用作连接到 DSL 调制解调器的网络接口的 PPPoE 客户机，将以下项添加到 `/etc/ppp/pppoe.if` 中。

```
hme0
```

有关 `/etc/ppp/pppoe.if` 的更多信息，请转至第 460 页中的 “`/etc/ppp/pppoe.if` 文件”。

3 **为使用 PPPoE 配置接口。**

```
# /etc/init.d/pppd start
```

4 **可选检验是否现在已对 PPPoE 接口进行检测。**

```
# /usr/sbin/sppptun query
hme0:pppoe
hme0:pppoed
```

此外，也可以使用 `/usr/sbin/sppptun` 命令，手动检测 PPPoE 接口。有关说明，请参阅第 461 页中的 “`/usr/sbin/sppptun` 命令”。

▼ 如何定义 PPPoE 访问服务器对等点

您可以在 `/etc/ppp/peers/` *peer-name* 文件中定义访问服务器。用于访问服务器的许多选项也可用于定义拨号方案中的拨入服务器。有关 `/etc/ppp/peers.`*peer-name* 的详细说明，请参阅第 441 页中的 “`/etc/ppp/peers/`*peer-name* 文件”。

1 **成为 PPPoE 客户机的超级用户或承担等效角色。**

角色包含授权和具有特权的命令。有关角色的更多信息，请参见《系统管理指南：安全性服务》中的“配置 RBAC（任务列表）”。

2 **在 `/etc/ppp/peers/`*peer-name* 文件中，定义服务提供商的 PPPoE 访问服务器。**

例如，以下文件 `/etc/ppp/peers/dslserve` 定义第 374 页中的 “PPPoE 通道配置示例”中介绍的 Far ISP 的访问服务器 `dslserve`。

```
# cat /etc/ppp/peers/dslserve
sppptun
plugin pppoe.so
connect "/usr/lib/inet/pppoec hme0"
noccp
noauth
user Red
password redsecret
noipdefault
defaultroute
```

有关此文件中的选项定义，请转至第 467 页中的 “用于定义访问服务器对等点的 `/etc/ppp/peers/`*peer-name* 文件”。

3 **修改 PPPoE 客户机的其他 PPP 配置文件。**

a. **按照第 378 页中的“配置拨出计算机”中配置拨出计算机的说明中所述，配置 `/etc/ppp/options`。**

b. 创建 /etc/ppp/options.sppptun 文件。/etc/ppp/options.sppptun 可为检测的 PPPoE 接口所连接到的串行端口定义 PPP 选项。

可以使用任何可用于 /etc/ppp/options. *ttyname* 文件的选项，如第 438 页中的 “/etc/ppp/options.*ttyname* 配置文件”中所述。由于 sppptun 是 pppd 配置中的指定设备名称，因此必须为文件 /etc/ppp/options.sppptun 命名。

4 确保所有用户都可以在客户机上启动 PPP。

```
# touch /etc/ppp/options
```

5 测试 PPP 是否可在 DSL 线路上运行。

```
% pppd debug updetach call dslserve
```

dslserve 是指定给第 374 页中的 “PPPoE 通道配置示例”中所示的 ISP 访问服务器的名称。debug updetach 选项则使调试信息显示在终端窗口中。

如果 PPP 正常运行，终端输出将显示处于活动状态的链路。如果 PPP 仍未运行，请尝试以下命令以查看服务器是否正常运行：

```
# /usr/lib/inet/pppoec -i hme0
```

注 – 已配置的 PPPoE 客户机的用户可以通过键入以下命令，在 DSL 线路上开始运行 PPP：

```
% pppd call ISP-server-name
```

然后，用户便可以运行应用程序或服务。

另请参见 以下列出了相关的参考信息。

- 请参见第 410 页中的 “设置 PPPoE 客户机”。
- 请参见第 460 页中的 “创建用于支持 DSL 的 PPPoE 通道”。
- 请参见第 21 章，修复常见的 PPP 问题（任务）。
- 请参见第 412 页中的 “设置 PPPoE 访问服务器”。

设置 PPPoE 访问服务器

如果您的公司是服务提供商，则可以为通过 DSL 连接访问您站点的客户机提供 Internet 服务和其他服务。该过程包括确定服务器中哪些接口与 PPPoE 通道有关，以及定义哪些服务可供用户使用。

▼ 如何设置 PPPoE 访问服务器

使用此过程可定义要用于 PPPoE 通道的以太网接口，以及配置访问服务器提供的服务。

1. **成为访问服务器的超级用户或承担等效角色。**

   角色包含授权和具有特权的命令。有关角色的更多信息，请参见《系统管理指南：安全性服务》中的“配置 RBAC（任务列表）”。

2. **将 PPPoE 通道专用的以太网接口名称添加到 /etc/ppp/pppoe.if 文件。**

   例如，对于第 374 页中的 “PPPoE 通道配置示例”中所示的访问服务器 dslserve，可以使用以下 /etc/ppp/pppoe.if 文件。

   ```
   # cat /etc/ppp/pppoe.if
   hme1
   hme2
   ```

3. **在 /etc/ppp/pppoe 文件中定义访问服务器提供的全局服务。**

   在以下 /etc/ppp/pppoe 文件中，列出了图 16–5 中所示的访问服务器 dslserve 提供的服务。

   ```
   device hme1,hme2
   service internet
       pppd "proxyarp 192.168.1.1:"
   service debugging
       pppd "debug proxyarp 192.168.1.1:"
   ```

   在该文件示例中，对于 dslserve 的以太网接口 hme1 和 hme2，宣布支持 Internet 服务。在这些以太网接口上，对 PPP 链路启用了调试功能。

4. **采用与设置拨入服务器相同的方法设置 PPP 配置文件。**

   有关更多信息，请参阅第 458 页中的 “为呼叫者创建 IP 寻址方案”。

5. **启动 pppoed 守护进程。**

   ```
   # /etc/init.d/pppd start
   ```

   pppd 还会检测 /etc/ppp/pppoe.if 中列出的接口。

6. **可选检验是否已检测服务器上的 PPPoE 接口。**

   ```
   # /usr/sbin/sppptun query
   hme1:pppoe
   hme1:pppoed
   hme2:pppoe
   hme2:pppoed
   ```

   以上样例表明，当前正在检测 PPPoE 接口 hme1 和 hme2。此外，也可以使用 /usr/sbin/sppptun 命令，手动检测 PPPoE 接口。有关说明，请参阅第 461 页中的 “/usr/sbin/sppptun 命令”。

▼ 如何修改现有 /etc/ppp/pppoe 文件

1 **成为访问服务器的超级用户或承担等效角色。**

角色包含授权和具有特权的命令。有关角色的更多信息，请参见《系统管理指南：安全性服务》中的“配置 RBAC（任务列表）”。

2 **根据需要修改 /etc/ppp/pppoe。**

3 **使 pppoed 守护进程识别新服务。**

```
# pkill -HUP pppoed
```

▼ 如何将接口限制为仅特定客户机可使用

以下过程说明如何将接口限制为仅一组 PPPoE 客户机可使用。执行此任务之前，需要获取指定给该接口的客户机的实际以太网 MAC 地址。

注 – 某些系统允许您更改以太网接口的 MAC 地址。您应将此功能视为一种便利因素，而非一种安全措施。

使用第 374 页中的 “PPPoE 通道配置示例”中所示的示例，这些步骤说明如何为 MiddleCo 中的客户机保留 `dslserve` 的接口之一 `hme1`。

1 **配置访问服务器接口并定义服务，如第 412 页中的“如何设置 PPPoE 访问服务器”中所示。**

2 **在服务器的 /etc/ethers 数据库中创建客户机项。**

以下是客户机 Red、Blue 和 Yellow 的项样例。

```
8:0:20:1:40:30 redether
8:0:20:1:40:10 yellowether
8:0:20:1:40:25 blueether
```

该样例将符号名称 `redether`、`yellowether` 和 `blueether` 指定给客户机 Red、Yellow 和 Blue 的以太网地址。为 MAC 地址指定符号名称为可选的操作。

3 **通过在 /etc/ppp/pppoe.*device* 文件中定义以下信息，限制特定接口上提供的服务。**

在此文件中，*device* 为要定义的设备的名称。

```
# cat /etc/ppp/pppoe.hme1
service internet
     pppd "name dslserve-hme1"
     clients redether,yellowether,blueether
```

dslserve-hme1 是访问服务器的名称，该名称用于匹配 pap-secrets 文件中的项。clients 选项将接口 hme1 限制为以太网符号名称为 redether、yellowether 和 blueether 的客户机可使用。

如果未在 /etc/ethers 中为客户机的 MAC 地址定义符号名称，则可将数字地址用作 clients 选项的参数。允许使用通配符。

例如，可以指定数字地址 clients 8:0:20:*:*:*。通过使用通配符，可接受 /etc/ethers 中的所有匹配地址。

4 **为访问服务器创建 /etc/ppp/pap-secrets 文件：**

```
Red         dslserve-hme1   redpasswd     *
Blue        dslserve-hme1   bluepasswd    *
Yellow      dslserve-hme1   yellowpassd   *
```

这些项为允许在 dslserve 的 hme1 接口上运行 PPP 的客户机的 PAP 名称和口令。

有关 PAP 验证的更多信息，请参见第 398 页中的 “配置 PAP 验证”。

另请参见 以下列出了相关的参考信息。

- 有关 PPPoE 的更多信息，请参见第 460 页中的 “创建用于支持 DSL 的 PPPoE 通道”。
- 有关 PPPoE 和 PPP 问题故障排除的信息，请参见第 421 页中的 “解决与 PPP 及 PPPoE 相关的问题”。
- 有关配置 PPPoE 客户机的信息，请参见第 410 页中的 “设置 PPPoE 客户机”。
- 有关为客户机配置 PAP 验证的信息，请参见第 401 页中的 “为可信呼叫者配置 PAP 验证（拨出计算机）”。
- 有关在服务器上配置 PAP 验证的信息，请参见第 399 页中的 “在拨入服务器上配置 PAP 验证”。

◆ ◆ ◆ 第 21 章

21 修复常见的 PPP 问题（任务）

本章包含解决 Solaris PPP 4.0 常见问题的相关信息，本章包含以下主题：

- 第 418 页中的 “PPP 故障排除工具”
- 第 421 页中的 “解决与 PPP 及 PPPoE 相关的问题”
- 第 431 页中的 “修复租用线路问题”
- 第 432 页中的 “诊断和修复验证问题”

此外，在 James Carlson 编著的 *PPP Design, Implementation, and Debugging* 以及澳大利亚国立大学的网站中，也提供了有关 PPP 故障排除的详细建议。有关更多信息，请参见第 351 页中的 “有关 PPP 的专业参考书籍”和第 351 页中的 “有关 PPP 的 Web 站点”。

解决 PPP 问题（任务列表）

使用以下任务列表可快速访问有关常见 PPP 问题的建议和解决方案。

表 21–1 PPP 故障排除任务列表

任务	定义	参考
获取有关 PPP 链路的诊断信息	使用 PPP 诊断工具获取用于故障排除的输出。	第 418 页中的 “如何从 pppd 获取诊断信息”
获取 PPP 链路的调试信息	使用 pppd debug 命令可生成用于故障排除的输出。	第 420 页中的 “如何启用 PPP 调试”
网络层一般问题的故障排除	通过使用一系列检查，确定并修复与网络相关的 PPP 问题。	第 421 页中的 “如何诊断网络问题”
一般通信问题的故障排除	确定并修复影响 PPP 链路的通信问题。	第 423 页中的 “如何诊断和修复通信问题”
配置问题的故障排除	确定并修复 PPP 配置文件中的问题。	第 424 页中的 “如何诊断 PPP 配置问题”

表 21–1 PPP 故障排除任务列表 （续）

任务	定义	参考
调制解调器相关问题的故障排除	确定并修复调制解调器问题。	第 425 页中的 “如何诊断调制解调器问题”
聊天脚本相关问题的故障排除	确定并修复拨出计算机的聊天脚本问题。	第 426 页中的 “如何获取聊天脚本的调试信息”
串行线路速度问题的故障排除	确定并修复拨入服务器的线路速度问题。	第 428 页中的 “如何诊断和修复串行线路速度问题”
租用线路常见问题的故障排除	确定并修复租用线路的性能问题。	第 431 页中的 “修复租用线路问题”
验证相关问题的故障排除	确定并修复与验证数据库相关的问题。	第 432 页中的 “诊断和修复验证问题”
PPPoE 范围问题的故障排除	使用 PPP 诊断工具获取用于确定并修复 PPPoE 问题的输出。	第 429 页中的 “如何获取 PPPoE 的诊断信息”

PPP 故障排除工具

PPP 链路一般有以下三种主要的故障范围：

- 要建立的链路的故障
- 链路在常规使用期间性能不佳
- 在链路任一端出现的可追溯到网络的问题

确定 PPP 是否正常的最简单方法是在链路上运行命令。对对等点网络上的主机运行 `ping` 或 `traceroute` 之类的命令，然后观察结果。但是，应使用 PPP 和 UNIX 调试工具来监视已建立的链路的性能，或者为有问题的链路排除故障。

本节说明如何从 `pppd` 及其关联的日志文件获取诊断信息。本章的其余各节将介绍借助 PPP 故障排除工具可以发现和修复的 PPP 常见问题。

▼ 如何从 pppd 获取诊断信息

下一个过程展示如何在本地计算机上查看链路的当前操作。

1 **成为本地计算机的超级用户或承担等效角色。**

角色包含授权和具有特权的命令。有关角色的更多信息，请参见《系统管理指南：安全性服务》中的“配置 RBAC（任务列表）”。

2 **使用为 PPP 配置的串行设备作为参数，运行 `pppd`：**

```
# pppd cua/b debug updetach
```

下一个示例将展示 `pppd` 在前台运行时产生的拨号链路和租用线路链路的显示内容。如果在后台运行 `pppd debug`，生成的输出将发送到 `/etc/ppp/connect-errors` 文件。

示例 21–1 正常运行的拨号链路的输出

```
# pppd /dev/cua/b debug updetach
have route to 0.0.0.0/0.0.0.0 via 172.21.0.4
serial speed set to 230400 bps
Using interface sppp0
Connect: sppp0 <--> /dev/cua/b
sent [LCP ConfReq id=0x7b <asyncmap 0x0> <magic 0x73e981c8> <pcomp> <accomp>]
rcvd [LCP Ident id=0x79 magic=0x0 "ppp-2.4.0b1 (Sun Microsystems, Inc., Oct  6
    2004 09:36:22)"]
Peer Identification: ppp-2.4.0b1 (Sun Microsystems, Inc., Oct  6 2004 09:36:22)
    rcvd [LCP ConfRej id=0x7b <asyncmap 0x0>]
sent [LCP Ident id=0x7c magic=0x0 "ppp-2.4.0b1 (Sun Microsystems, Inc., Sep 15
    2004 09:38:33)"
sent [LCP ConfReq id=0x7d <magic 0x73e981c8> <pcomp> <accomp>]
rcvd [LCP ConfAck id=0x7d <magic 0x73e981c8> <pcomp> <accomp>]
rcvd [LCP ConfAck id=0x78 <magic 0xdd4ad820> <pcomp> <accomp>]
sent [LCP ConfAck id=0x78 <magic 0xdd4ad820> <pcomp> <accomp>]
sent [LCP Ident id=0x7e magic=0x73e981c8 "ppp-2.4.0b1 (Sun Microsystems, Inc.,
    Sep 15 2004 09:38:33)"]
sent [IPCP ConfReq id=0x3d <addr 0.0.0.0> <compress VJ 0f 01>]
rcvd [LCP Ident id=0x7a magic=0xdd4ad820 "ppp-2.4.0b1 (Sun Microsystems, Inc.,
    Oct  6 2004 09:36:22)"]
Peer Identification: ppp-2.4.0b1 (Sun Microsystems, Inc., Oct  6 2004 09:36:22)
rcvd [IPCP ConfReq id=0x92 <addr 10.0.0.1> <compress VJ 0f 01>
sent [IPCP ConfAck id=0x92 <addr 10.0.0.1> <compress VJ 0f 01>
rcvd [IPCP ConfNak id=0x3d <addr 10.0.0.2>]]
sent [IPCP ConfReq id=0x3e <addr 10.0.0.2> <compress VJ 0f 01>]
rcvd [IPCP ConfAck id=0x3e <addr 10.0.0.2> <compress VJ 0f 01>]
local  IP address 10.0.0.2
remote IP address 10.0.0.1
```

示例 21–2 正常运行的租用线路链路的输出

```
# pppd /dev/se_hdlc1 default-asyncmap debug updetach
pppd 2.4.0b1 (Sun Microsystems, Inc., Oct 24 2004 07:13:18) started by root, uid 0
synchronous speed appears to be 0 bps
init option: '/etc/ppp/peers/syncinit.sh' started (pid 105122)
Serial port initialized.
synchronous speed appears to be 64000 bps
Using interface sppp0
Connect: sppp0 <--> /dev/se_hdlc1
sent [LCP ConfReq id=0xe9 <magic 0x474283c6><pcomp> <accomp>]
rcvd [LCP ConfAck id=0xe9 <magic 0x474283c6><pcomp> <accomp>]
rcvd [LCP ConfReq id=0x22 <magic 0x8e3a53ff><pcomp> <accomp>]
sent [LCP ConfReq id=0x22 <magic 0x8e3a53ff><pcomp> <accomp>]
sent [LCP Ident id=0xea magic=0x474283c6 "ppp-2.4.0b1 (Sun Microsystems, Inc., Oct
    22 2004 14:31:44)"]
sent [IPCP ConfReq id=0xf7 <addr 0.0.0.0> <compress VJ 0f o1>]]
sent [CCP ConfReq id=0x3f <deflate 15> <deflate(old#) 15> <bsd v1 15>]
rcvd [LCP Ident id=0x23 magic=0x8e3a53ff "ppp-2.4.0b1 (Sun Microsystems, Inc., Oct
    22 2004 14:31:44)"]
Peer Identification: ppp-2.4.0b1 (Sun Microsystems, Inc., Oct 22 2004 14:31:44)
rcvd [IPCP ConfReq id=0x25 <addr 10.0.0.1> <compress VJ 0f 01>]
sent [IPCP ConfAck id=0x25 <addr 10.0.0.1> <compress VJ 0f 01>]
rcvd [CCP ConfReq id=0x3 <deflate 15> <deflate(old#) 15 <bsd v1 15>]
sent [CCP ConfAck id=0x3 <deflate 15> <deflate(old#) 15 <bsd v1 15>]
```

```
rcvd [IPCP ConfNak id=0xf8 <addr 10.0.0.2>]
rcvd [IPCP ConfReq id=0xf7 <addr 10.0.0.2> <compress VJ 0f 01>]
rcvd [CCP ConfAck id=0x3f <deflate 15> <deflate(old#) 15 <bsd v1 15>]
Deflate (15) compression enabled
rcvd [IPCP ConfAck id=0xf8 <addr 10.0.0.2> <compress VJ 0f 01>]
local  IP address 10.0.0.2
remote IP address 10.0.0.1
```

▼ 如何启用 PPP 调试

下一个任务将展示如何使用 pppd 命令获取调试信息。

注 – 对于每台主机，只需执行一次步骤 1 到步骤 3。此后，可以继续执行步骤 4 为主机启用调试功能。

---

1. **成为超级用户或承担等效角色。**

   角色包含授权和具有特权的命令。有关角色的更多信息，请参见《系统管理指南：安全性服务》中的“配置 RBAC（任务列表）”。

2. **创建日志文件以保存 pppd 的输出。**

   ```
   # touch /var/log/pppdebug
   ```

3. **在 /etc/syslog.conf 中为 pppd 添加以下 syslog 工具。**

   ```
   daemon.debug;local2.debug       /var/log/pppdebug
   ```

4. **重新启动 syslogd。**

   ```
   # pkill -HUP -x syslogd
   ```

5. **使用以下 pppd 语法，为对特定对等点的呼叫启用调试功能。**

   ```
   # pppd debug call peer-name
   ```

   peer-name 必须是 /etc/ppp/peers 目录中的某个文件的名称。

6. **查看日志文件的内容。**

   ```
   # tail -f /var/log/pppdebug
   ```

   有关日志文件的示例，请参见步骤 3。

解决与 PPP 及 PPPoE 相关的问题

有关如何解决 PPP 及 PPPoE 相关问题的信息，请参阅以下各节。

▼ 如何诊断网络问题

如果 PPP 链路处于活动状态，但远程网络上可以访问的主机很少，则可能表明存在网络问题。以下过程展示了如何隔离并修复影响 PPP 链路的网络问题。

1. **成为本地计算机的超级用户或承担等效角色。**

   角色包含授权和具有特权的命令。有关角色的更多信息，请参见《系统管理指南：安全性服务》中的“配置 RBAC（任务列表）”。

2. **关闭有问题的链路。**

3. **通过为 PPP 配置添加以下选项，在配置文件中禁用所有可选协议：**

   ```
   noccp novj nopcomp noaccomp default-asyncmap
   ```

   这些选项可提供最简单且未压缩的可用 PPP。尝试在命令行上将这些选项作为 `pppd` 的参数进行调用。如果可以访问先前无法访问的主机，则可在以下任一位置添加这些选项。

   - `/etc/ppp/peers/`*peer-name*，在 `call` 选项之后
   - `/etc/ppp/options`，确保这些选项全局适用

4. **呼叫远程对等点。然后，启用调试功能。**

   ```
   % pppd debug call peer-name
   ```

5. **使用 `chat` 的 `-v` 选项，获取聊天程序的详细日志。**

   例如，在任一 PPP 配置文件中使用以下格式：

   ```
   connect 'chat -v -f /etc/ppp/chatfile'
   ```

   /etc/ppp/chatfile 代表聊天文件的名称。

6 **通过使用 Telnet 或其他应用程序访问远程主机，尝试重新生成该问题。**

观察调试日志。如果仍然无法访问远程主机，则 PPP 问题可能与网络相关。

7 **验证远程主机的 IP 地址是否为已注册的 Internet 地址。**

某些组织会指定在本地网络内可识别但无法路由至 Internet 的内部 IP 地址。如果远程主机位于公司内，则必须设置名称到地址转换 (name-to-address translation, NAT) 服务器或代理服务器才能访问 Internet。如果远程主机不在公司内，则应向远程组织报告该问题。

8 **检查路由表。**

a. **检查本地计算机和对等点上的路由表。**

b. **检查位于从对等点到远程系统的路径中的所有路由器的路由表。另外，检查返回对等点的路径中的所有路由器的路由表。**

确保中间路由器的配置正确。通常，在返回对等点的路径中，可能会发现问题。

9 **可选如果计算机为路由器，需检查可选功能。**

```
# ndd -set /dev/ip ip_forwarding 1
```

有关 ndd 的更多信息，请参阅 ndd(1M) 手册页。

在 Solaris 10 发行版中，可以使用 routeadm(1M) 来代替 ndd(1M)。

```
# routeadm -e ipv4-forwarding -u
```

注 – ndd 命令没有持久性。使用该命令设置的值将在重新引导系统时丢失。routeadm 命令具有持久性。使用该命令设置的值将在重新引导系统后保留。

---

10 **检查通过 netstat -s 和类似工具获取的统计信息。**

有关 netstat 的完整详细信息，请参阅 netstat(1M) 手册页。

a. **在本地计算机上运行统计信息。**

b. **呼叫对等点。**

c. **观察 netstat -s 生成的新统计信息。有关更多信息，请参阅第 423 页中的“影响 PPP 的常见网络问题”。**

11 **检查 DNS 配置。**

错误的名称服务配置会因无法解析 IP 地址而使应用程序无法运行。

影响 PPP 的常见网络问题

可以使用 `netstat -s` 生成的消息修复下表中所示的网络问题。相关的过程信息，请参阅第 421 页中的 “如何诊断网络问题”。

表 21–2 影响 PPP 的常见网络问题

消息	问题	解决方案
`IP packets not forwardable`	本地主机缺少路由。	在本地主机的路由表中添加缺失的路由。
`ICMP input destination unreachable`	本地主机缺少路由。	在本地主机的路由表中添加缺失的路由。
`ICMP time exceeded`	两个路由器正在互相转发同一个目标地址，导致包来回传递，直到超出生存时间 (time-to-live, TTL) 值。	使用 `traceroute` 查找路由循环的原因，然后与出现错误的路由器的管理员联系。有关 `traceroute` 的信息，请参阅 `traceroute(1M)` 手册页。
`IP packets not forwardable`	本地主机缺少路由。	在本地主机的路由表中添加缺失的路由。
`ICMP input destination unreachable`	本地主机缺少路由。	在本地主机的路由表中添加缺失的路由。

▼ 如何诊断和修复通信问题

两个对等点无法成功建立链路，则表明出现了通信问题。有时，这些问题实际上是由于聊天脚本配置错误而导致的协商问题。以下过程说明如何清除通信问题。有关清除由于聊天脚本错误而导致的协商问题，请参见表 21–5。

1. **成为本地计算机的超级用户或承担等效角色。**

   角色包含授权和具有特权的命令。有关角色的更多信息，请参见《系统管理指南：安全性服务》中的“配置 RBAC（任务列表）”。

2. **呼叫对等点。**

3. **呼叫远程对等点。然后，启用调试功能。**

   ```
   % pppd debug call peer-name
   ```

   为修复某些通信问题，可能需要从对等点获取调试信息。

4. **检查生成的日志以查找通信问题。有关更多信息，请参阅第 424 页中的“影响 PPP 的一般通信问题”。**

影响 PPP 的一般通信问题

下表描述了与第 423 页中的“如何诊断和修复通信问题”过程的日志输出相关的症状。

表 21–3 影响 PPP 的一般通信问题

症状	问题	解决方案
`too many Configure-Requests`	一个对等点无法接收另一个对等点的信息。	检查以下问题： ■ 计算机或调制解调器的布线可能出错。 ■ 调制解调器配置的位设置可能不正确。或者，配置可能中断了流量控制。 ■ 聊天脚本可能出现故障。在这种情况下，请参见表 21–5。
`pppd debug` 输出显示 LCP 已启动，但更高级别的协议失败或显示出现 CRC 错误。	异步控制字符映射 (asynchronous control character map, ACCM) 的设置不正确。	使用 `default-async` 选项将 ACCM 设置为标准缺省值 FFFFFFFF。首先，尝试在命令行上使用 `default-async` 作为 `pppd` 的选项。如果问题已解决，则将 `default-async` 添加到 `/etc/ppp/options`，或添加到 call 选项之后的 `/etc/ppp/peers/`*peer-name*。
`pppd debug` 输出显示，IPCP 在启动后立即终止。	IP 地址配置可能不正确。	1. 检查聊天脚本以验证脚本的 IP 地址是否正确。 2. 如果聊天脚本正确，则请求对等点的调试日志，然后检查对等点日志中的 IP 地址。
链路显示性能很差。	调制解调器的配置不正确，并出现流量控制配置错误、调制解调器设置错误以及 DTE 日志配置错误。	检查调制解调器配置。如有必要，调整该配置。

▼ 如何诊断 PPP 配置问题

某些 PPP 问题可以追溯到 PPP 配置文件的问题。以下过程说明如何确定并修复常见的配置问题。

1. **成为本地计算机的超级用户或承担等效角色。**

   角色包含授权和具有特权的命令。有关角色的更多信息，请参见《系统管理指南：安全性服务》中的“配置 RBAC（任务列表）”。

2. **呼叫远程对等点。然后，启用调试功能。**

   ```
   % pppd debug call peer-name
   ```

3. **在生成的日志中检查配置问题。有关更多信息，请参阅第 425 页中的“常见的 PPP 配置问题”。**

常见的 PPP 配置问题

下表介绍了与第 424 页中的 “如何诊断 PPP 配置问题”过程的日志输出相关的症状。

表 21–4 常见的 PPP 配置问题

症状	问题	解决方案
pppd debug 输出包含错误消息 `Could not determine remote IP address`。	`/etc/ppp/peers/`*peer-name* 文件未包含对等点的 IP 地址。对等点在链路协商期间没有提供 IP 地址。	在 pppd 命令行或 `/etc/ppp/peers/`*peer-name* 中，使用以下格式为对等点提供 IP 地址： :10.0.0.10
pppd debug 输出显示 CCP 数据压缩失败。该输出还指示链路被丢弃。	对等点的 PPP 压缩配置可能出现冲突。	通过在 `/etc/ppp/options` 中添加 `noccp` 选项，对其中一个对等点禁用 CCP 压缩。

▼ 如何诊断调制解调器问题

调制解调器问题可能是拨号链路的主要问题。调制解调器配置问题的最常见指示是对等点没有响应。但是，要确定链路问题是否确实为调制解调器配置问题所致，可能会有些困难。

有关调制解调器故障排除的基本建议，请参阅《系统管理指南：高级管理》中的“解决终端和调制解调器问题”。此外，调制解调器制造商所提供的文档和网站也提供了有关其特定设备问题的解决方案。以下过程有助于确定调制解调器配置错误是否会导致链路问题。

1. **按照第 420 页中的 “如何启用 PPP 调试”中的说明，呼叫已启用调试功能的对等点。**

2. **显示生成的 `/var/log/pppdebug` 日志，以检查调制解调器配置是否错误。**

3. **使用 `ping` 在链路上发送各种大小的包。**

   有关 `ping` 的完整详细信息，请参阅 `ping(1M)` 手册页。

   如果收到较小的包，而较大的包被丢弃，则表明调制解调器存在问题。

4. **检查接口 `sppp0` 上的错误：**

```
% netstat -ni
Name  Mtu  Net/Dest   Address      Ipkts    Ierrs Opkts    Oerrs Collis Queue
lo0   8232 127.0.0.0  127.0.0.1    826808   0     826808   0     0      0
hme0  1500 172.21.0.0 172.21.3.228 13800032 0     1648464  0     0      0
sppp0 1500 10.0.0.2   10.0.0.1     210      0     128      0     0      0
```

   如果接口错误随时间而增加，则调制解调器配置可能存在问题。

故障排除 显示生成的 /var/log/pppdebug 日志时，输出中出现以下症状可以表明调制解调器配置出现错误。本地计算机可以接收对等点的信息，而对等点却无法接收本地计算机的信息。

- 对等点未发送任何 "recvd" 消息。
- 输出包含来自对等点的 LCP 消息，但链路失败，并显示本地计算机发送的 too many LCP Configure Requests 消息。
- 链路终止，并显示 SIGHUP 信号。

▼ 如何获取聊天脚本的调试信息

以下过程用于从 chat 获取调试信息和常见问题的清除建议。有关更多信息，请参阅第 426 页中的 “常见的聊天脚本问题”。

1. **成为拨出计算机的超级用户或承担等效角色。**

   角色包含授权和具有特权的命令。有关角色的更多信息，请参见《系统管理指南：安全性服务》中的“配置 RBAC（任务列表）”。

2. **编辑要呼叫的对等点的 /etc/ppp/peers/*peer-name* 文件。**

3. **添加 -v 作为 connect 选项中指定的 chat 命令的参数。**

   ```
   connect "/usr/bin/chat -v -f /etc/ppp/chat-script-name"
   ```

4. **查看 /etc/ppp/connect-errors 文件中的聊天脚本错误。**

   以下是使用 chat 出现的主要错误。

   ```
   Oct 31 08:57:13 deino chat[107294]: [ID 702911 local2.info] expect (CONNECT)
   Oct 31 08:57:58 deino chat[107294]: [ID 702911 local2.info] alarm
   Oct 31 08:57:58 deino chat[107294]: [ID 702911 local2.info] Failed
   ```

   该示例展示了在等待 (CONNECT) 字符串时出现的超时。如果 chat 失败，将从 pppd 获取以下消息：

   ```
   Connect script failed
   ```

常见的聊天脚本问题

聊天脚本是拨号链路中容易出现问题的地方。下表列出了常见的聊天脚本错误，并提供了用于修复这些错误的建议。有关过程信息，请参阅第 426 页中的 “如何获取聊天脚本的调试信息”。

表 21–5 常见的聊天脚本问题

症状	问题	解决方案
pppd debug 输出包含 Connect script failed	聊天脚本提供了用户名和口令。 ogin: *user-name* ssword: *password* 但是，计划与之连接的对等点却没有提示此信息。	1. 从聊天脚本中删除登录名和口令。 2. 再次尝试呼叫对等点。 3. 如果仍然出现该消息，请致电 ISP，要求 ISP 提供正确的登录顺序。
/usr/bin/chat -v 日志包含 "expect (login:)" alarm read timed out	聊天脚本提供了用户名和口令。 ogin: pppuser ssword: \q\U 但是，计划与之连接的对等点却没有提示此信息。	1. 从聊天脚本中删除登录名和口令。 2. 再次尝试呼叫对等点。 3. 如果仍然出现该消息，请致电 ISP，要求 ISP 提供正确的登录顺序。
pppd debug 输出包含 possibly looped-back	本地计算机或其对等点正在命令行上挂起，并且未运行 PPP。聊天脚本中包含未正确配置的登录名和口令。	1. 从聊天脚本中删除登录名和口令。 2. 再次尝试呼叫对等点。 3. 如果仍然出现该消息，请致电 ISP，要求提供正确的登录顺序。
pppd debug 输出显示 LCP 已激活，但之后链路很快终止。	聊天脚本中的口令可能不正确。	1. 确保您拥有正确的本地计算机口令。 2. 检查聊天脚本中的口令。修复不正确的口令。 3. 再次尝试呼叫对等点。 4. 如果仍然出现该消息，请致电 ISP，要求 ISP 提供正确的登录顺序。
对等点的文本以波浪号 (~) 开头。	聊天脚本提供了用户名和口令。 ogin: pppuser ssword: \q\U 但是，计划与之连接的对等点却没有提示此信息。	1. 从聊天脚本中删除登录名和口令。 2. 再次尝试呼叫对等点。 3. 如果仍然出现该消息，请致电 ISP，请求正确的登录顺序。
调制解调器挂起。	聊天脚本使用以下行来强制本地计算机等待来自对等点的 CONNECT 消息： CONNECT ”	如果希望聊天脚本等待来自对等点的 CONNECT 消息，可使用以下行： CONNECT \c 聊天脚本以 ~ \c 结尾。
pppd debug 输出包含 LCP: timeout sending Config-Requests	聊天脚本使用以下行来强制本地计算机等待来自对等点的 CONNECT 消息： CONNECT ”	如果希望聊天脚本等待来自对等点的 CONNECT 消息，可使用以下行： CONNECT \c 聊天脚本以 ~ \c 结尾。

表 21–5 常见的聊天脚本问题 （续）

症状	问题	解决方案
pppd debug 输出包含 Serial link is not 8-bit clean	聊天脚本使用以下行来强制本地计算机等待来自对等点的 CONNECT 消息： CONNECT ”	如果希望聊天脚本等待来自对等点的 CONNECT 消息，可使用以下行： CONNECT \c 聊天脚本以 ~ \c 结尾。
pppd debug 输出包含 Loopback detected	聊天脚本使用以下行来强制本地计算机等待来自对等点的 CONNECT 消息： CONNECT ”	如果希望聊天脚本等待来自对等点的 CONNECT 消息，可使用以下行： CONNECT \c 聊天脚本以 ~ \c 结尾。
pppd debug 输出包含 SIGHUP	聊天脚本使用以下行来强制本地计算机等待来自对等点的 CONNECT 消息： CONNECT ”	如果希望聊天脚本等待来自对等点的 CONNECT 消息，可使用以下行： CONNECT \c 聊天脚本以 ~ \c 结尾。

▼ 如何诊断和修复串行线路速度问题

拨入服务器可能会因速度设置冲突而出现问题。以下过程有助于您确定引起串行线路速度产生冲突的链路问题。

下列行为可导致速度问题：

- 通过 /bin/login 等程序调用了 PPP 并指定了线路速度。
- 通过 mgetty 启动了 PPP 并无意中提供了位速率。

由于 pppd 将初始设置的线路速度更改为通过 /bin/login 或 mgetty 设置的速度，因此线路出现故障。

1 **登录到拨入服务器。呼叫启用了调试功能的对等点。**

如果需要说明，请参见第 420 页中的 “如何启用 PPP 调试”。

2 **显示生成的 /var/log/pppdebug 日志。**

在输出中检查有无以下消息：

```
LCP too many configure requests
```

此消息表明，为 PPP 配置的串行线路速度可能会出现冲突。

3 **检查是否已通过 /bin/login 等程序调用 PPP，并检查设置的线路速度。**

在这种情况下，pppd 会将初始配置的线路速度更改为 /bin/login 中指定的速度。

4. **检查用户是否已通过 `mgetty` 命令启动 PPP 并无意中指定了位速率。**
   该操作还会导致串行线路速度冲突。

5. **按如下所示，修复串行线路速度冲突问题：**

   a. **锁定调制解调器的 DTE 速率。**

   b. **不使用自动波特。**

   c. **配置后不更改线路速度。**

▼ 如何获取 PPPoE 的诊断信息

可以使用 PPP 和标准的 UNIX 实用程序来确定 PPPoE 问题。如果怀疑链路问题是由 PPPoE 所致，可使用以下诊断工具获取故障排除信息。

1. **成为运行 PPPoE 通道的计算机（PPPoE 客户机或 PPPoE 访问服务器）的超级用户。**

2. **按照第 420 页中的“如何启用 PPP 调试”过程中的说明，启用调试功能。**

3. **查看日志文件 `/var/log/pppdebug` 的内容。**
   以下示例展示了使用 PPPoE 通道生成的部分链路日志文件。

```
Sep  6 16:28:45 enyo pppd[100563]: [ID 702911 daemon.info] Plugin
  pppoe.so loaded.
Sep  6 16:28:45 enyo pppd[100563]: [ID 860527 daemon.notice] pppd
  2.4.0b1 (Sun Microsystems, Inc.,
Sep  5 2001 10:42:05) started by troot, uid 0
Sep  6 16:28:46 enyo pppd[100563]: [ID 702911 daemon.debug] connect option:
   '/usr/lib/inet/pppoec
-v hme0' started (pid 100564)
Sep  6 16:28:46 enyo pppd[100563]: [ID 702911 daemon.info] Serial connection established.
Sep  6 16:28:46 enyo pppd[100563]: [ID 702911 daemon.info] Using interface sppp0
Sep  6 16:28:46 enyo pppd[100563]: [ID 702911 daemon.notice] Connect: sppp0
   <--> /dev/sppptun
Sep  6 16:28:46 enyo pppd[100563]: [ID 702911 daemon.debug] /etc/ppp/pap-secrets
  is apparently empty
Sep  6 16:28:46 enyo pppd[100563]: [ID 702911 daemon.debug] /etc/ppp/chap-secrets
  is apparently empty
Sep  6 16:28:46 enyo pppd[100563]: [ID 702911 daemon.debug] sent
  [LCP ConfReq id=0xef <mru 1492>
asyncmap 0x0 <magic 0x77d3e953><pcomp><acomp>
Sep  6 16:28:46 enyo pppd[100563]: [ID 702911 daemon.debug] rcvd
  [LCP ConfReq id=0x2a <mru 1402>
asyncmap 0x0 <magic 0x9985f048><pcomp><acomp
```

   如果通过该调试输出无法确定问题，请继续执行此过程。

4. **获取 PPPoE 的诊断消息。**

```
# pppd connect "/usr/lib/inet/pppoec -v interface-name"
```

pppoec 将诊断信息发送到 stderr。如果在前台运行 pppd，输出将显示在屏幕上。如果在后台运行 pppd，输出将发送到 /etc/ppp/connect-errors。

以下示例展示了协商 PPPoE 通道时生成的消息。

```
Connect option: '/usr/lib/inet/pppoec -v hme0' started (pid 100564)
/usr/lib/inet/pppoec: PPPoE Event Open (1) in state Dead (0): action SendPADI (2)
/usr/lib/inet/pppoec: Sending PADI to ff:ff:ff:ff:ff:ff: 18 bytes
/usr/lib/inet/pppoec: PPPoE State change Dead (0) -> InitSent (1)
/usr/lib/inet/pppoec: Received Active Discovery Offer from 8:0:20:cd:c1:2/hme0:pppoed
/usr/lib/inet/pppoec: PPPoE Event rPADO+ (5) in state InitSent (1): action SendPADR+ (5)
/usr/lib/inet/pppoec: Sending PADR to 8:0:20:cd:c1:2: 22 bytes
/usr/lib/inet/pppoec: PPPoE State change InitSent (1) -> ReqSent (3)
/usr/lib/inet/pppoec: Received Active Discovery Session-confirmation from
   8:0:20:cd:c1:2/hme0:pppoed
/usr/lib/inet/pppoec: PPPoE Event rPADS (7) in state ReqSent (3): action Open (7)
/usr/lib/inet/pppoec: Connection open; session 0002 on hme0:pppoe
/usr/lib/inet/pppoec: PPPoE State change ReqSent (3) -> Convers (4)
/usr/lib/inet/pppoec: connected
```

如果通过该诊断消息无法确定问题，请继续执行此过程。

5 运行 snoop。然后将跟踪保存到文件。

有关 snoop 的信息，请参阅 snoop(1M) 手册页。

```
# snoop -o pppoe-trace-file
```

6 查看 snoop 跟踪文件。

```
# snoop -i pppoe-trace-file -v pppoe

ETHER: ----- Ether Header -----
ETHER:
ETHER: Packet 1 arrived at 6:35:2.77
ETHER: Packet size = 32 bytes
ETHER: Destination = ff:ff:ff:ff:ff:ff, (broadcast)
ETHER: Source      = 8:0:20:78:f3:7c, Sun
ETHER: Ethertype = 8863 (PPPoE Discovery)
ETHER:
PPPoE: ----- PPP Over Ethernet -----
PPPoE:
PPPoE: Version = 1
PPPoE: Type = 1
PPPoE: Code = 9 (Active Discovery Initiation)
PPPoE: Session Id = 0
PPPoE: Length = 12 bytes
PPPoE:
PPPoE: ----- Service-Name -----
PPPoE: Tag Type = 257
PPPoE: Tag Length = 0 bytes
PPPoE:
PPPoE: ----- Host-Uniq -----
PPPoE: Tag Type = 259
PPPoE: Tag Length = 4 bytes
PPPoE: Data = Ox00000002
PPPoE:
.
```

```
.
.
ETHER: ----- Ether Header -----
ETHER:
ETHER: Packet 5 arrived at 6:35:2.87
ETHER: Packet size = 60 bytes
ETHER: Destination = 8:0:20:78:f3:7c, Sun)
ETHER: Source      = 0:2:fd:39:7f:7,
ETHER: Ethertype = 8864 (PPPoE Session)
ETHER:
PPPoE: ----- PPP Over Ethernet -----
PPPoE:
PPPoE: Version = 1
PPPoE: Type = 1
PPPoE: Code = 0 (PPPoE Session)
PPPoE: Session Id = 24383
PPPoE: Length = 20 bytes
PPPoE:
PPP: ----- Point-to-Point Protocol -----
PPP:
PPP-LCP: ----- Link Control Protocol -----
PPP-LCP:
PPP-LCP: Code = 1 (Configure Request)
PPP-LCP: Identifier = 80
PPP-LCP: Length = 18
```

修复租用线路问题

租用线路的最常见问题是性能差。在大多数情况下，需要与电话公司共同修复该问题。

表 21–6 常见的租用线路问题

症状	问题	解决方案
链路未启动。	可能是因为 CSU 双极违规 (CSU biopolar violation, CSU BPV)。链路一端被设置为用于 AMI 线路。而另一端被设置为用于 ESF 位–8 零替换 (bit–8 zero substitute, B8Z)。	如果您在美国或加拿大境内，则可直接通过 CSU/DSU 的菜单修复此问题。有关详细信息，请查看 CSU/DSU 制造商所提供的文档。 如果位于其他地区，则提供商可能会负责修复 CSU BPV。
链路性能差。	链路中有持续通信流时，`pppd debug` 输出显示发生了 CRC 错误。您的线路可能存在计时问题，这是由于电话公司和您的网络之间的配置错误所致。	联系电话公司以确保正在使用“循环计时”(loop clocking)。 在某些非结构化的租用线路上，可能必须提供计时。北美用户应使用循环计时。

诊断和修复验证问题

下表介绍了一般验证问题的解决方案。

表 21–7 一般验证问题

症状	问题	解决方案
`pppd debug` 输出显示消息 `Peer is not authorized to use remote address` *address*。	您正在使用 PAP 验证，但远程对等点的 IP 地址不在 `/etc/ppp/pap-secrets` 文件中。	在 `/etc/ppp/pap-secrets` 文件中，在对等点的项后添加一个星号 (*)。
`pppd debug` 输出显示，LCP 启动，但在启动后很快终止。	对于特定的安全协议，数据库中的口令可能不正确。	在 `/etc/ppp/pap-secrets` 或 `/etc/ppp/chap-secrets` 文件中检查对等点的口令。

◆ ◆ ◆ 第 22 章

22 Solaris PPP 4.0（参考）

本章介绍有关 Solaris PPP 4.0 的详细概念信息。具体包括以下主题：

在文件中和命令行上使用 PPP 选项

Solaris PPP 4.0 包含大量选项，可将其用于定义 PPP 配置。可以在 PPP 配置文件中或在命令行上使用这些选项，也可以组合使用文件选项和命令行选项。本节包含有关在配置文件中使用 PPP 选项以及将这些选项用作 PPP 命令参数的详细信息。

定义 PPP 选项的位置

Solaris PPP 4.0 的配置非常灵活。可以在以下位置定义 PPP 选项：

- PPP 配置文件
- 在命令行上发出的 PPP 命令
- 以上两种位置的组合

下表列出了 PPP 配置文件和命令。

表 22–1 PPP 配置文件和命令汇总

文件或命令	定义	参考
/etc/ppp/options	包含缺省应用于系统中所有 PPP 链路的特征（例如，计算机是否要求对等点对其本身进行验证）的文件。如果不存在此文件，将禁止非超级用户使用 PPP。	第 437 页中的 “/etc/ppp/options 配置文件”
/etc/ppp/options.*ttyname*	描述通过串行端口 *ttyname* 进行的所有通信的特征的文件。	第 438 页中的 “/etc/ppp/options.*ttyname* 配置文件”
/etc/ppp/peers	通常包含有关拨出计算机连接到的对等点信息的目录。此目录中的文件与 pppd 命令的 call 选项一起使用。	第 441 页中的 “指定用于与拨入服务器通信的信息”
/etc/ppp/peers/*peer-name*	包含远程对等点 *peer-name* 的特征的文件。典型的特征包括远程对等点的电话号码，以及用于与对等点协商链路的聊天脚本。	第 441 页中的 “/etc/ppp/peers/*peer-name* 文件”
/etc/ppp/pap-secrets	包含进行口令验证协议 (Password Authentication Protocol, PAP) 验证所必需的安全凭证的文件。	第 452 页中的 “/etc/ppp/pap-secrets 文件”
/etc/ppp/chap-secrets	包含进行质询握手身份验证协议 (Challenge-Handshake Authentication Protocol, CHAP) 验证所必需的安全凭证的文件。	第 455 页中的 “/etc/ppp/chap-secrets 文件”
~/.ppprc	PPP 用户的起始目录中的文件，通常与拨入服务器一起使用。此文件包含有关每个用户的配置的特定信息。	第 440 页中的 “在拨入服务器上配置 $HOME/.ppprc”
pppd 选项	用于启动 PPP 链路并说明其特征的命令和选项。	第 434 页中的 “如何处理 PPP 选项”

有关 PPP 文件的详细信息，请参阅 pppd(1M) 手册页。pppd (1M) 还包含 pppd 命令可用的所有选项的全面说明。/etc/ppp 中提供了所有 PPP 配置文件的样例模板。

如何处理 PPP 选项

1. pppd 守护进程解析以下项目：

   所有 Solaris PPP 4.0 操作都由 pppd 守护进程处理，它在用户运行 pppd 命令时启动。用户呼叫远程对等点时，将发生以下操作：

   - /etc/ppp/options
   - $HOME/.ppprc
   - 由 /etc/ppp/options 和 $HOME/.ppprc 中的 file 或 call 选项打开的任何文件

2. pppd 扫描命令行以确定正在使用的设备。守护进程此时不会解释遇到的任何选项。

3. pppd 尝试使用以下条件搜索要使用的串行设备：
   - 如果在命令行或先前处理的配置文件中指定了串行设备，则 pppd 将使用该设备的名称。
   - 如果未命名任何串行设备，则 pppd 将在命令行上搜索 notty、pty 或 socket 选项。如果指定了其中某个选项，则 pppd 将假定不存在任何设备名称。
   - 或者，如果 pppd 发现标准输入连接到某个 tty，则将使用该 tty 的名称。
   - 如果 pppd 仍然找不到串行设备，则 pppd 将终止连接并发出错误。
4. 然后，pppd 会检查是否存在 /etc/ppp/options.*ttyname* 文件。如果找到该文件，pppd 将对其进行解析。
5. pppd 处理命令行上的任何选项。
6. pppd 协商链路控制协议 (Link Control Protocol, LCP) 以设置链路。
7. （可选的）如果需要验证，pppd 将读取 /etc/ppp/pap-secrets 或 /etc/ppp/chap-secrets，对另外一个对等点进行验证。

pppd 守护进程在命令行上或在其他配置文件中遇到选项 call *peer-name* 时，将读取文件 /etc/ppp/peers/*peer-name*。

PPP 配置文件特权工作原理

Solaris PPP 4.0 配置中使用**特权**概念。特权确定配置选项的优先级，尤其是在多个位置调用同一个选项的情况下。从特权源调用的选项优先于从非特权源调用的相同选项。

用户特权

唯一的特权用户是 UID 为零的超级用户 (root)。其他所有用户没有特权。

文件特权

以下配置文件拥有特权，无论其归谁所有：

- /etc/ppp/options
- /etc/ppp/options.*ttyname*
- /etc/ppp/peers/*peer-name*

文件 $HOME/.ppprc 由用户拥有。仅当调用 pppd 的用户是 root 时，从 $HOME/.ppprc 和命令行上读取的选项才拥有特权。

file 选项后面的参数拥有特权。

选项特权的影响

有些选项要求发起调用的用户或源要拥有特权才会有效。在命令行上调用的选项将拥有正在运行 pppd 命令的用户的特权。只有调用 pppd 的用户为 root 时，这些选项才拥有特权。

选项	状态	说明
`domain`	拥有特权	要求拥有特权才能使用。
`linkname`	拥有特权	要求拥有特权才能使用。
`noauth`	拥有特权	要求拥有特权才能使用。
`nopam`	拥有特权	要求拥有特权才能使用。
`pam`	拥有特权	要求拥有特权才能使用。
`plugin`	拥有特权	要求拥有特权才能使用。
`privgroup`	拥有特权	要求拥有特权才能使用。
`allow-ip` *addresses*	拥有特权	要求拥有特权才能使用。
`name` *hostname*	拥有特权	要求拥有特权才能使用。
`plink`	拥有特权	要求拥有特权才能使用。
`noplink`	拥有特权	要求拥有特权才能使用。
`plumbed`	拥有特权	要求拥有特权才能使用。
`proxyarp`	如果指定了 `noproxyarp`，则将拥有特权	无法由非特权用户忽略。
`defaultroute`	如果 `nodefaultroute` 在特权文件中设置，或由特权用户设置，则该选项将拥有特权	无法由非特权用户忽略。
`disconnect`	如果该选项在特权文件中设置或由特权用户设置，则将拥有特权	无法由非特权用户忽略。
`bsdcomp`	如果该选项在特权文件中设置或由特权用户设置，则将拥有特权	非特权用户指定的代码大小不能大于特权用户已指定的大小。
`deflate`	如果该选项在特权文件中设置或由特权用户设置，则将拥有特权	非特权用户指定的代码大小不能大于特权用户已指定的大小。
`connect`	如果该选项在特权文件中设置或由特权用户设置，则将拥有特权	无法由非特权用户忽略。
`init`	如果该选项在特权文件中设置或由特权用户设置，则将拥有特权	无法由非特权用户忽略。
`pty`	如果该选项在特权文件中设置或由特权用户设置，则将拥有特权	无法由非特权用户忽略。
`welcome`	如果该选项在特权文件中设置或由特权用户设置，则将拥有特权	无法由非特权用户忽略。

选项	状态	说明
ttyname	如果该选项在特权文件中设置，则将拥有特权 如果在非特权文件中设置，则没有特权	无论谁调用 pppd，都将使用 root 权限打开。 使用调用 pppd 的用户的特权打开。

/etc/ppp/options 配置文件

使用 /etc/ppp/options 文件可为本地计算机上的所有 PPP 通信定义全局选项。/etc/ppp/options 是特权文件。/etc/ppp/options 应由 root 拥有，但 pppd 不会强制执行此规则。/etc/ppp/options 中定义的选项优先于在其他所有文件中和命令行上相同选项的定义。

可能会在 /etc/ppp/options 中使用的典型选项包括：

- **lock**－启用 UUCP 样式的文件锁定
- **noauth**－指示计算机将不验证呼叫者

注 – Solaris PPP 4.0 软件不包括缺省的 /etc/ppp/options 文件。pppd 不需要 /etc/ppp/options 文件也可正常工作。如果某个计算机上没有 /etc/ppp/options 文件，则只有 root 可以在该计算机上运行 pppd。

必须使用文本编辑器创建 /etc/ppp/options，如第 380 页中的 “如何定义串行线路上的通信”中所示。如果计算机不需要全局选项，可以创建空的 /etc/ppp/options 文件。然后，root 和一般用户都可以在本地计算机上运行 pppd。

/etc/ppp/options.tmpl 模板

/etc/ppp/options.tmpl 包含有关 /etc/ppp/options 文件的有用注释，以及全局 /etc/ppp/options 文件的三个常用选项。

```
lock
nodefaultroute
noproxyarp
```

选项	定义
lock	启用 UUCP 样式的文件锁定
nodefaultroute	指定未定义任何缺省路由
noproxyarp	禁止 proxyarp

要将 /etc/ppp/options.tmpl 用作全局选项文件，可将 /etc/ppp/options.tmpl 重命名为 /etc/ppp/options。然后，根据站点的需要修改文件内容。

/etc/ppp/options 文件示例的位置

要查找 /etc/ppp/options 文件的示例，请参阅以下内容：

- 对于拨出计算机，请参见第 380 页中的 “如何定义串行线路上的通信”。
- 对于拨入服务器，请参见第 387 页中的 “如何定义串行线路上的通信（拨入服务器）”。
- 对于拨入服务器上的 PAP 支持，请参见第 400 页中的 “如何将 PAP 支持添加到 PPP 配置文件（拨入服务器）”。
- 对于拨出计算机上的 PAP 支持，请参见第 403 页中的 “如何将 PAP 支持添加到 PPP 配置文件（拨出计算机）”。
- 对于拨入服务器上的 CHAP 支持，请参见第 406 页中的 “如何将 CHAP 支持添加到 PPP 配置文件（拨入服务器）”。

/etc/ppp/options.ttyname 配置文件

可以在 /etc/ppp/options.*ttyname* 文件中配置串行线路上的通信特征。/etc/ppp/options.*ttyname* 是特权文件，由 pppd 在解析了任何现有 /etc/ppp/options 和 $HOME/.pppрc 文件之后读取。否则，pppd 将在解析了 /etc/ppp/options 之后读取 /etc/ppp/options. *ttyname*。

ttyname 既可用于拨号链路，也可用于租用线路链路。*ttyname* 代表计算机上的某个特定串行端口（如 cua/a 或 cua/b），在该端口上可能连接了调制解调器或 ISDN TA。

命名 /etc/ppp/options.*ttyname* 文件时，将设备名称中的斜杠 (/) 替换为点 (.)。例如，设备 cua/b 的 options 文件应命名为 /etc/ppp/options.cua.b。

注 – Solaris PPP 4.0 不需要 /etc/ppp/options.*ttyname* 文件也可以正常工作。您的服务器可能只有一条用于 PPP 的串行线路。而且，服务器需要的选项很少。在这种情况下，可以在另外一个配置文件中或在命令行上指定所需要的任何选项。

在拨入服务器上使用 etc/ppp/options. ttyname

对于拨号链路，可以选择为连接了调制解调器的拨入服务器上的每个串行端口创建单个 /etc/ppp/options.*ttyname* 文件。以下是一些典型选项：

- 拨入服务器所需的 IP 地址

  如果要求串行端口 *ttyname* 上的传入呼叫者使用特定 IP 地址，需设置此选项。与可能的呼叫者数量相比，您的地址空间中可能只有数量有限的 IP 地址可供 PPP 使用。在这种情况下，可考虑为拨入服务器上用于 PPP 的每个串行接口指定一个 IP 地址。此指定操作可实现 PPP 的动态寻址。

- `asyncmap` *map-value*

  `asyncmap` 选项映射特定调制解调器或 ISDN TA 无法通过串行线路接收的控制字符。使用 `xonxoff` 选项时，`pppd` 会自动将 asyncmap 设置为 0xa0000。

  map_value 以十六进制格式描述有问题的控制字符。

- `init "chat -U -f /etc/ppp/mychat"`

  `init` 选项指示调制解调器使用 `chat -U` 命令中的信息初始化串行线路上的通信。调制解调器使用 `/etc/ppp/mychat` 文件中的聊天字符串。

- `pppd`(1m) 手册页中列出的安全参数

在拨出计算机上使用 etc/ppp/options. ttyname

对于拨出系统，可以为连接到调制解调器的串行端口创建 `/etc/ppp/options.` *ttyname* 文件，或者选择不使用 `/etc/ppp/options.`*ttyname*。

注 – Solaris PPP 4.0 不需要 `/etc/ppp/options.`*ttyname* 文件也可以正常工作。拨出计算机可能只有一条用于 PPP 的串行线路。此外，拨出计算机需要的选项可能很少。可以在另外一个配置文件中或在命令行上指定所需要的任何选项。

---

options.ttya.tmpl 模板文件

`/etc/ppp/options.ttya.tmpl` 文件包含有关 `/etc/ppp/options.`*tty-name* 文件的有用注释。该模板包含 `/etc/ppp/options.`*tty-name* 文件的三个常用选项。

```
38400
asyncmap 0xa0000
:192.168.1.1
```

选项	定义
`38400`	将此波特率用于端口 ttya。
`asyncmap 0xa0000`	指定 asyncmap 值 0xa0000，从而使本地计算机可以与中断的对等点通信。
`:192.168.1.1`	将 IP 地址 192.168.1.1 指定给通过链路呼入的所有对等点。

要在您的站点上使用 `/etc/ppp/options.ttya.tmpl`，需将 `/etc/ppp/options.tmpl` 重命名为 `/etc/ppp/options.` *ttya-name*。将 *ttya-name* 替换为调制解调器的串行端口的名称。然后，根据您的站点的需要修改文件内容。

/etc/ppp/options.ttyname 文件示例的位置

要查找 /etc/ppp/options.*ttyname* 文件的示例，请参阅以下内容：

- 对于拨出计算机，请参见第 380 页中的 “如何定义串行线路上的通信”。
- 对于拨入服务器，请参见第 387 页中的 “如何定义串行线路上的通信（拨入服务器）”。

配置特定于用户的选项

本节包含有关在拨入服务器上设置用户的详细信息。

在拨入服务器上配置 $HOME/.ppprc

$HOME/.ppprc 文件适用于要配置首选 PPP 选项的用户。作为管理员，您也可以为用户配置 $HOME/.ppprc。

$HOME/.ppprc 中的选项只有在调用该文件的用户拥有特权时才拥有特权。

呼叫者使用 pppd 命令启动呼叫时，.ppprc 文件是由 pppd 守护进程检查的第二个文件。

有关在拨入服务器上设置 $HOME/.ppprc 的说明，请参见第 386 页中的 “设置拨入服务器的用户”。

在拨出计算机上配置 $HOME/.ppprc

在拨出计算机上，Solaris PPP 4.0 不需要 $HOME/.ppprc 文件也可以正常工作。此外，除了特殊情况，拨出计算机上无需具有 $HOME/.ppprc 文件。如果要执行以下操作，请创建一个或多个 .ppprc 文件：

- 允许多个通信需求不同的用户从同一台计算机呼叫远程对等点。在这种情况下，需在必须拨出的每个用户的起始目录中创建单个 .ppprc 文件。
- 需要指定用于控制特定于链路的问题的选项（如禁用 Van Jacobson 压缩）。有关链路问题故障排除的帮助，请参见 James Carlson 编著的 *PPP Design, Implementation, and Debugging* 和 pppd(1M) 手册页。

由于 .ppprc 文件通常在配置拨入服务器时使用，因此如需有关 .ppprc 的配置说明，可参阅第 386 页中的 “如何配置拨入服务器的用户”。

指定用于与拨入服务器通信的信息

要与拨入服务器通信，需要收集有关该服务器的信息，然后编辑几个文件。最重要的是，必须配置拨出计算机需要呼叫的所有拨入服务器的通信要求。可以在 `/etc/ppp/options.`*ttyname* 文件中指定有关拨入服务器的选项（如 ISP 电话号码）。但是，配置对等点信息的最佳位置是在 `/etc/ppp/peers/`*peer-name* 文件中。

/etc/ppp/peers/peer-name 文件

注 – 在拨出计算机上，Solaris PPP 4.0 不需要 `/etc/ppp/peers/`*peer-name* 文件也可以正常工作。

使用 `/etc/ppp/peers/`*peer-name* 文件可提供用于与特定对等点通信的信息。`/etc/ppp/peers/`*peer-name* 允许普通用户调用不允许用户设置的预选择的特权选项。

例如，如果在 `/etc/ppp/peers/`*peer-name* 文件中指定了 `noauth`，非特权用户将无法忽略 `noauth` 选项。假定用户要设置指向 `peerB` 的链路，而该对等点不提供验证凭证。作为超级用户，您可以创建一个包括 `noauth` 选项的 `/etc/ppp/peers/peerB` 文件。`noauth` 指示本地计算机不验证来自 `peerB` 的呼叫。

`pppd` 遇到以下选项时，`pppd` 守护进程将读取 `/etc/ppp/peers/`*peer-name*：

`call` *peer-name*

可以为拨出计算机需要与其通信的每个目标对等点创建一个 `/etc/ppp/peers/`*peer-name* 文件。此做法对于允许普通用户调用特殊拨出链路特别方便，无需使用 root 特权。

可以在 `/etc/ppp/peers/`*peer-name* 中指定的典型选项包括：

- `user` *user-name*

  使用 PAP 或 CHAP 进行验证时，为拨入服务器提供 *user_name* 作为拨出计算机的登录名。

- `remotename` *peer-name*

  使用 *peer-name* 作为拨入计算机的名称。扫描 `/etc/ppp/pap-secrets` 或 `/etc/ppp/chap-secrets` 文件时，`remotename` 将与 PAP 或 CHAP 验证配合使用。

- `connect "chat` *chat_script* `..."`

  使用聊天脚本中的指令打开到拨入服务器的通信。

- `noauth`

  启动通信时，不要验证对等点 *peer-name*。

- `noipdefault`

将与对等点协商时使用的初始 IP 地址设置为 0.0.0.0。在设置指向大多数 ISP 的链路以方便对等点之间进行 IPCP 协商时，可使用 `noipdefault`。

- `defaultroute`

  在链路上建立 IP 时安装缺省 IPv4 路由。

有关可能适用于特定目标对等点的更多选项，请参见 `pppd(1M)` 手册页。

/etc/ppp/peers/myisp.tmpl 模板文件

`/etc/ppp/peers/myisp.tmpl` 文件包含有关 `/etc/ppp/peers/`*peer-name* 文件的有用注释。该模板总结了可用于 `/etc/ppp/peers/`*peer-name* 文件的常用选项：

```
connect "/usr/bin/chat -f /etc/ppp/myisp-chat"
user myname
remotename myisp
noauth
noipdefault
defaultroute
updetach
noccp
```

选项	定义
`connect "/usr/bin/chat -f /etc/ppp/myisp-chat"`	使用聊天脚本 `/etc/ppp/myisp-chat` 呼叫对等点。
`user myname`	将此帐户名用于本地计算机。`myname` 是此计算机在对等点的 `/etc/ppp/pap-secrets` 文件中的名称。
`remotename myisp`	将 `myisp` 识别为对等点在本地计算机的 `/etc/ppp/pap-secrets` 文件中的名称。
`noauth`	不要求发起呼叫的对等点提供验证凭证。
`noipdefault`	不使用本地计算机的缺省 IP 地址。
`defaultroute`	使用为本地计算机指定的缺省路由。
`updetach`	在 PPP 日志文件（而不是标准输出）中记录错误。
`noccp`	不使用 CCP 压缩。

要在您的站点上使用 `/etc/ppp/peers/myisp.tmpl`，需将 `/etc/ppp/peers/myisp.tmpl` 重命名为 `/etc/ppp/peers/.`*peer-name*。将 *peer-name* 替换为要呼叫的对等点的名称。然后，根据您的站点的需要修改文件内容。

/etc/ppp/peers/peer-name 文件示例的位置

要查找 /etc/ppp/peers/*peer-name* 文件的示例，请参阅以下内容：

- 对于拨出计算机，请参见第 382 页中的 “如何定义与单个对等点的连接”。
- 对于租用线路上的本地计算机，请参见第 393 页中的 “如何配置租用线路上的计算机”。
- 对于拨出计算机上的 PAP 验证支持，请参见第 403 页中的 “如何将 PAP 支持添加到 PPP 配置文件（拨出计算机）”。
- 对于拨出计算机上的 CHAP 验证支持，请参见第 408 页中的 “如何将 CHAP 支持添加到 PPP 配置文件（拨出计算机）”。
- 对于客户机系统上的 PPPoE 支持，请参见第 410 页中的 “设置 PPPoE 客户机”。

配置拨号链路的调制解调器速度

调制解调器配置的主要问题是指定调制解调器运行的速度。以下指导适用于与 Oracle Corporation 计算机配合使用的调制解调器：

- 早期的 SPARC 系统－查看系统附带的硬件文档。许多 SPARCstation 计算机要求调制解调器速度不超过 38400 bps。
- UltraSPARC 计算机－将调制解调器速度设置为 115200 bps，此速度适用于新式调制解调器，其速度足以用于拨号链路。如果计划使用带压缩功能的双通道 ISDN TA，则需要提高调制解调器速度。对于异步链路，对 UltraSPARC 的限制为 460800 bps。

对于**拨出计算机**，调制解调器的速度可在 PPP 配置文件（如 /etc/ppp/peers/*peer-name*）中设置，或者通过将速度指定为 pppd 的选项进行设置。

对于**拨入服务器**，需要使用 ttymon 工具或 Solaris Management Console 设置速度，如第 384 页中的 “配置拨入服务器上的设备”中所述。

定义拨号链路上的会话

拨出计算机及其远程对等点通过协商和交换各种指令在 PPP 链路中通信。配置拨出计算机时，需要确定本地和远程调制解调器所需的指令。然后，创建一个名为聊天脚本的文件，其中包含这些指令。本节将讨论有关配置调制解调器和创建聊天脚本的信息。

聊天脚本的内容

拨出计算机需要连接到的每个远程对等点可能要求使用其自身的聊天脚本。

注 – 聊天脚本通常仅在拨号链路上使用。租用线路链路不使用聊天脚本，除非链路中包含了需要启动配置的异步接口。

聊天脚本的内容由调制解调器型号或 ISDN TA 以及远程对等点的要求确定。这些内容显示为一组 Expect-send（期待发送）字符串。拨出计算机及其远程对等点会在其通信启动过程中交换这些字符串。

expect 字符串包含拨出主机期望从远程对等点接收以启动会话的字符。*send* 字符串包含拨出计算机在接收了 expect 字符串之后发送到远程对等点的字符。

聊天脚本中的信息通常包括以下内容：

- 调制解调器命令，通常称为 *AT* **命令**，这些命令使调制解调器可以通过电话线路传输数据
- 目标对等点的电话号码

  此电话号码可能是 ISP、公司站点的拨入服务器或单个计算机要求提供的号码。
- 超时值（如果需要）
- 期望从远程对等点获取的登录序列
- 由拨出计算机发送的登录序列

聊天脚本示例

本节包含一些聊天脚本，可供在创建聊天脚本时用于参考。调制解调器制造商的指南和来自 ISP 及其他目标主机的信息包含调制解调器和目标对等点的聊天要求。此外，许多 PPP Web 站点都有聊天脚本样例。

基本调制解调器聊天脚本

以下是一个基本聊天脚本，创建自己的聊天脚本时可以此为模板。

```
ABORT   BUSY
ABORT   'NO CARRIER'
REPORT  CONNECT
TIMEOUT 10
"" AT&F1M0&M5S2=255
SAY     "Calling myserver\n"
TIMEOUT 60
OK      "ATDT1-123-555-1212"
ogin: pppuser
ssword: \q\U
% pppd
```

下一个表描述了聊天脚本的内容。

脚本内容	说明
ABORT BUSY	如果调制解调器从对应对等点收到此消息，则中止传输。
ABORT 'NO CARRIER'	如果调制解调器在拨号时报告 ABORT 'NO CARRIER'，则中止传输。出现此消息通常是因为拨号或调制解调器协商故障。
REPORT CONNECT	从调制解调器收集 CONNECT 字符串。输出字符串。
TIMEOUT 10	将初始超时设置为 10 秒。调制解调器会立即做出响应。
"" AT&F1M0&M5S2=255	M0－连接过程中关闭扬声器。
	&M5－使调制解调器要求进行错误控制。
	S2=255－禁用 TIES "+++" 中断序列。
SAY "Calling myserver\n"	在本地计算机上显示消息 Calling myserver。
TIMEOUT 60	将超时重置为 60 秒，为链路协商留出更多时间。
OK "ATDT1-123-555-1212"	使用电话号码 123-555-1212 呼叫远程对等点。
ogin: pppuser	使用 UNIX 样式的登录来登录到对等点。提供用户名 pppuser。
ssword: \q\U	\q－如果使用 -v 选项调试，则不进行日志记录。
	\U－在此位置插入命令行上指定的 -U 之后的字符串内容。通常，该字符串包含口令。
% pppd	等待 % shell 提示，并运行 pppd 命令。

/etc/ppp/myisp-chat.tmpl 聊天脚本模板

此发行版包括 /etc/ppp/myisp-chat.tmpl 模板，可以修改该模板供您的站点使用。/etc/ppp/myisp-chat.tmpl 与基本调制解调器聊天脚本类似，不同的是该模板不包括登录序列。

```
ABORT   BUSY
ABORT   'NO CARRIER'
REPORT  CONNECT
TIMEOUT 10
""      "AT&F1"
OK      "AT&C1&D2"
SAY     "Calling myisp\n"
TIMEOUT 60
OK      "ATDT1-123-555-1212"
CONNECT \c
```

脚本内容	说明
ABORT BUSY	如果调制解调器从对应对等点收到此消息，则中止传输。

脚本内容	说明
ABORT 'NO CARRIER	如果调制解调器在拨号时报告 ABORT 'NO CARRIER'，则中止传输。出现此消息通常是因为拨号或调制解调器协商故障。
REPORT CONNECT	从调制解调器收集 CONNECT 字符串。输出字符串。
TIMEOUT 10	将初始超时设置为 10 秒。调制解调器会立即做出响应。
"" "AT&F1"	将调制解调器重置为出厂缺省值。
OK "AT&C1&D2"	重置调制解调器，以便对于 &C1，来自调制解调器的 DCD 位于载波之后。如果远程端由于某种原因而挂起，DCD 将被丢弃。 对于 &D2，DTR 高到低转换会导致调制解调器"挂起"。
SAY "Calling myisp\n"	在本地计算机上显示消息 "Calling myisp"。
TIMEOUT 60	将超时重置为 60 秒，为链路协商留出更多时间。
OK "ATDT1-123-555-1212"	使用电话号码 123-555-1212 呼叫远程对等点。
CONNECT \c	等待来自对应对等点的调制解调器的 CONNECT 消息。

用于呼叫 ISP 的调制解调器聊天脚本

使用以下聊天脚本作为模板，用于从带有 U.S. Robotics Courier 调制解调器的拨出计算机呼叫 ISP。

```
ABORT   BUSY
ABORT   'NO CARRIER'
REPORT  CONNECT
TIMEOUT 10
"" AT&F1M0&M5S2=255
SAY     "Calling myisp\n"
TIMEOUT 60
OK      "ATDT1-123-555-1212"
CONNECT \c
\r \d\c
SAY "Connected; running PPP\n"
```

下表描述了聊天脚本的内容。

脚本内容	说明
ABORT BUSY	如果调制解调器从对应对等点收到此消息，则中止传输。
ABORT 'NO CARRIER'	如果调制解调器从对应对等点收到此消息，则中止传输。
REPORT CONNECT	从调制解调器收集 CONNECT 字符串。输出字符串。
TIMEOUT 10	将初始超时设置为 10 秒。调制解调器会立即做出响应。

脚本内容	说明
"" AT&F1M0M0M0M0&M5S2=255	M0－连接过程中关闭扬声器。 &M5－使调制解调器要求进行错误控制。 S2=255－禁用 TIES "+++" 中断序列。
SAY "Calling myisp\n"	在本地计算机上显示消息 Calling myisp。
TIMEOUT 60	将超时重置为 60 秒，为链路协商留出更多时间。
OK "ATDT1-123-555-1212"	使用电话号码 123-555-1212 呼叫远程对等点。
CONNECT \c	等待来自对应对等点的调制解调器的 CONNECT 消息。
\r \d\c	一直等到 CONNECT 消息结束。
SAY “Connected; running PPP\n”	在本地计算机上显示提示性消息 Connected; running PPP。

用于 UNIX 样式登录的增强型基本聊天脚本

以下聊天脚本是为呼叫远程 Solaris 对等点或其他 UNIX 类型的对等点而进行了增强的基本脚本。此聊天脚本在第 381 页中的 “如何创建用于呼叫对等点的指令”中使用。

```
SAY "Calling the peer\n"
TIMEOUT 10
ABORT BUSY
ABORT ’NO CARRIER’
ABORT ERROR
REPORT CONNECT
"" AT&F1&M5S2=255
TIMEOUT 60
OK ATDT1-123-555-1234
CONNECT \c
SAY "Connected; logging in.\n"
TIMEOUT 5
ogin:--ogin: pppuser
TIMEOUT 20
ABORT ’ogin incorrect’
ssword: \qmypassword
"% " \c
SAY "Logged in.  Starting PPP on peer system.\n"
ABORT ’not found’
"" "exec pppd"
~ \c
```

下表说明了该聊天脚本的参数。

脚本内容	说明
TIMEOUT 10	将初始超时设置为 10 秒。调制解调器会立即做出响应。
ABORT BUSY	如果调制解调器从对应对等点收到此消息，则中止传输。

脚本内容	说明
ABORT 'NO CARRIER'	如果调制解调器从对应对等点收到此消息，则中止传输。
ABORT ERROR	如果调制解调器从对应对等点收到此消息，则中止传输。
REPORT CONNECT	从调制解调器收集 CONNECT 字符串。输出字符串。
"" AT&F1&M5S2=255	&M5－使调制解调器要求进行错误控制。 S2=255－禁用 TIES "+++" 中断序列。
TIMEOUT 60	将超时重置为 60 秒，为链路协商留出更多时间。
OK ATDT1-123-555-1234	使用电话号码 123-555-1212 呼叫远程对等点。
CONNECT \c	等待来自对应对等点的调制解调器的 CONNECT 消息。
SAY "Connected; logging in.\n"	显示提示性消息 Connected; logging in 以指出用户状态。
TIMEOUT 5	更改超时以便快速显示登录提示。
ogin:--ogin: pppuser	等待登录提示。如果未收到提示，则发送 RETURN 并等待。然后，将用户名 pppuser 发送到对等点。大多数 ISP 将随后的序列称为 PAP 登录。但是，PAP 登录与 PAP 验证毫不相关。
TIMEOUT 20	将超时更改为 20 秒，以便进行慢速口令验证。
ssword: \qmysecrethere	等待来自对等点的口令提示。收到提示时，发送口令 \qmysecrethere。\q 阻止将口令写入系统日志文件。
"% " \c	等待来自对等点的 shell 提示。聊天脚本使用 C shell。如果用户喜欢使用其他 shell 登录，可以更改此值。
SAY "Logged in. Starting PPP on peer system.\n"	显示提示性消息 Logged in. Starting PPP on peer system 以指出用户状态。
ABORT 'not found'	如果 shell 遇到错误，则中止传输。
"" "exec pppd"	在对等点上启动 pppd。
~ \c	等待在对等点上启动 PPP。

紧接 CONNECT \c 之后启动 PPP 通常被 ISP 称为 *PAP* **登录**，但 PAP 登录实际上不属于 PAP 验证。

短语 ogin:--ogin: pppuser 指示调制解调器发送用户名 pppuser 以响应来自拨入服务器的登录提示。pppuser 是为拨入服务器上的远程 user1 创建的特殊 PPP 用户帐户名。有关在拨入服务器上创建 PPP 用户帐户的说明，请参阅第 386 页中的 "如何配置拨入服务器的用户"。

外部 ISDN TA 的聊天脚本

以下聊天脚本用于从使用 ZyXEL omni.net.ISDN TA 的拨出计算机进行呼叫。ISDN TA。

```
SAY "Calling the peer\n"
TIMEOUT 10
ABORT BUSY
ABORT 'NO CARRIER'
ABORT ERROR
REPORT CONNECT
"" AT&FB40S83.7=1&K44&J3X7S61.3=1S0=0S2=255
OK ATDI18882638234
CONNECT \c
\r \d\c
SAY "Connected; running PPP\n"
```

下表说明了该聊天脚本的参数。

脚本内容	说明
`SAY "Calling the peer"`	在拨出计算机的屏幕上显示此消息。
`TIMEOUT 10`	将初始超时设置为 10 秒。
`ABORT BUSY`	如果调制解调器从对应对等点收到此消息，则中止传输。
`ABORT 'NO CARRIER'`	如果调制解调器从对应对等点收到此消息，则中止传输。
`ABORT ERROR`	如果调制解调器从对应对等点收到此消息，则中止传输。
`REPORT CONNECT`	从调制解调器收集 `CONNECT` 字符串。输出字符串。
`"" AT&FB40S83.7=1&K44&J3X7S61.3=1S0=0S2=255`	此行中的字母具有以下含义： ■ `&F`－使用出厂缺省值 ■ `B40`－执行异步 PPP 转换 ■ `S83.7=1`－使用“通过语音承载传输数据” ■ `&K44`－启用 CCP 压缩 ■ `&J3`－启用 MP ■ `X7`－报告 DCE 端速率 ■ `S61.3=1`－使用包分段 ■ `S0=0`－无自动应答 ■ `S2=255`－禁用 TIES 转义
`OK ATDI18882638234`	进行 ISDN 呼叫。对于多链路，会对同一电话号码进行二次呼叫，通常大多数 ISP 要求这样做。如果远程对等点要求另一个不同的电话号码，可附加 "+ *nnnn*"。*nnnn* 表示第二个电话号码。
`CONNECT \c`	等待来自对应对等点的调制解调器的 `CONNECT` 消息。

脚本内容	说明
\r \d\c	一直等到 CONNECT 消息结束。
SAY "Connected; running PPP\n"	在拨出计算机的屏幕上显示此消息。

有关聊天脚本的选项说明和其他详细信息，请参阅 chat(1M) 手册页。有关 expect-send（期待发送）字符串的说明，请参阅第 494 页中的 “/etc/uucp/Systems 文件中的聊天脚本字段”。

更多聊天脚本示例

很多网站提供用于创建聊天脚本的聊天脚本样例和帮助。有关示例，请参见 http://ppp.samba.org/ppp/index.html。

调用聊天脚本

可以使用 connect 选项调用聊天脚本。可以在任何 PPP 配置文件中或在命令行上使用 connect "chat ..."。

聊天脚本不可执行，但 connect 调用的程序必须可执行。可以使用聊天实用程序作为 connect 要调用的程序。在这种情况下，如果通过 -f 选项将聊天脚本存储在外部文件中，则聊天脚本文件将不可执行。

chat(1m) 中介绍的 chat 程序执行实际的聊天脚本。只要 pppd 遇到 connect "chat ..." 选项，pppd 守护进程就会调用 chat 程序。

注 – 可以使用任何外部程序（如 Perl 或 Tcl）来创建高级聊天脚本。为了方便使用，提供了 chat 实用程序。

▼ 如何调用聊天脚本（任务）

1. **以 ASCII 文件形式创建聊天脚本。**
2. **使用以下语法调用任何 PPP 配置文件中的聊天脚本：**

   ```
   connect 'chat  -f /etc/ppp/chatfile'
   ```

   -f 标志指示后面将跟一个文件名。*/etc/ppp/chatfile* 表示聊天文件的名称。
3. **将外部聊天文件的读取权限授予运行 pppd 命令的用户。**

注意 – 聊天程序始终使用用户的特权运行，即使从特权源调用 `connect 'chat ...'` 选项也是如此。因此，使用 `-f` 选项读取的独立聊天文件必须可被调用用户读取。如果该聊天脚本包含口令或其他敏感信息，则此特权可能会引起安全问题。

示例 22–1 内置聊天脚本

可将整个聊天脚本会话放置在一行中，类似如下内容：

```
connect 'chat "" "AT&F1" OK ATDT5551212 CONNECT "\c"'
```

完整的聊天脚本接在 `chat` 关键字之后。脚本以 `"\c"'` 终止。可以在任何 PPP 配置文件或命令行上使用此格式作为 `pppd` 的参数。

更多信息 外部文件中的聊天脚本

如果特定对等点需要的聊天脚本比较长或很复杂，可以考虑将该脚本作为一个独立文件创建。外部聊天文件易于维护和记录。可以通过在注释前加上井 (#) 号添加对聊天文件的注释。

第 381 页中的 “如何创建用于呼叫对等点的指令”过程展示了如何使用外部文件中包含的聊天脚本。

创建可执行的聊天文件

可以创建一个聊天文件，该脚本是一个可执行脚本，可在启动拨号链路时自动运行。因此，在链路启动过程中，除了可运行包含在传统聊天脚本中的命令之外，还可以运行其他命令（如用于奇偶校验设置的 `stty`）。

此可执行聊天脚本登录到旧式 UNIX 系统（要求 7 位，包含偶校验）。运行 PPP 时，系统将更改为不包含奇偶校验的 8 位。

```
#!/bin/sh
chat "" "AT&F1" OK "ATDT555-1212" CONNECT "\c"
stty evenp
chat ogin: pppuser ssword: "\q\U" % "exec pppd"
stty -evenp
```

▼ 如何创建可执行聊天程序

1. **使用文本编辑器创建可执行聊天程序（如前面的示例）。**
2. **使聊天程序可执行。**

   ```
   # chmod +x /etc/ppp/chatprogram
   ```

3 **调用聊天程序。**

```
connect /etc/ppp/chatprogram
```

聊天程序无需位于 /etc/ppp 文件系统中。可以将聊天程序存储在任何位置。

验证链路上的呼叫者

本节将介绍 PPP 验证协议的工作原理，并介绍与验证协议关联的数据库。

口令验证协议 (Password Authentication Protocol, PAP)

PAP 验证在操作方面与 UNIX login 程序有些类似，但 PAP 不向用户授予 shell 访问权限。PAP 使用 /etc/ppp/pap-secrets 文件格式的 PPP 配置文件和 PAP 数据库进行验证设置。PAP 还使用 /etc/ppp/pap-secrets 定义 PAP 安全凭证。这些凭证包括对等点名称、PAP 用语中的“用户名”以及口令。PAP 凭证还包含允许链接到本地计算机的每个呼叫者的相关信息。PAP 用户名和口令可以与口令数据库中的 UNIX 用户名和口令相同，也可以不同。

/etc/ppp/pap-secrets 文件

PAP 数据库在 /etc/ppp/pap-secrets 文件中实现。要成功地验证，PPP 链路两端的计算机必须在其 /etc/ppp/pap-secrets 文件中正确配置 PAP 凭证。呼叫者（被验证者）在 /etc/ppp/pap-secrets 文件的 user 和 password 列中或 +ua 文件（已过时）中提供凭证。服务器（验证者）通过 UNIX passwd 数据库或在 PAM 工具中，对照 /etc/ppp/pap-secrets 中的信息来验证这些凭证。

/etc/ppp/pap-secrets 文件具有以下语法。

```
myclient ISP-server mypassword *
```

这些参数具有以下含义：

myclient	呼叫者的 PAP 用户名。通常，此名称与呼叫者的 UNIX 用户名相同，拨入服务器使用 PAP 的 login 选项时尤其如此。
ISP-server	远程计算机（通常为拨入服务器）的名称。
mypassword	呼叫者的 PAP 口令。
*	与呼叫者关联的 IP 地址。使用星号 (*) 表示任何 IP 地址。

创建 PAP 口令

PAP 口令在链路中以**明文**（即可读的 ASCII 码）形式发送。对于呼叫者（被验证者），PAP 口令必须以明文形式存储在以下任何位置中：

- 存储在 `/etc/ppp/pap-secrets` 中
- 存储在另外一个外部文件中
- 通过 `pap-secrets @` 功能存储在命名管道中
- 在命令行或 PPP 配置文件中作为 `pppd` 的选项存储
- 通过 `+ua` 文件中存储

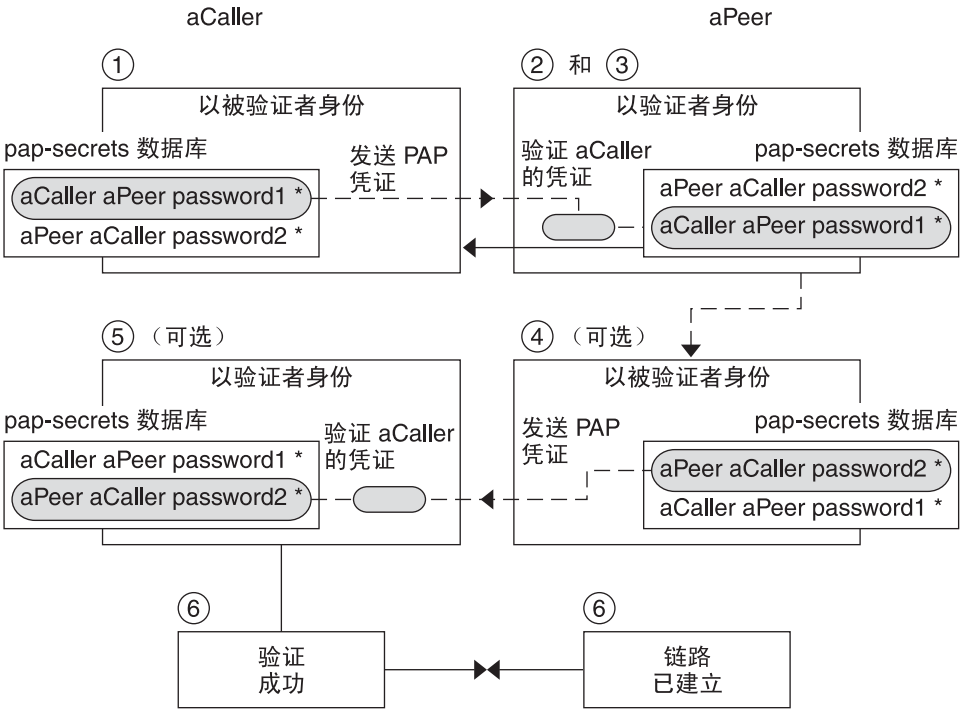
在服务器（验证者）中，可以通过执行以下某个操作隐藏 PAP 口令：

- 指定 `papcrypt` 并使用由 `pap-secrets` 文件中的 `crypt`(3C) 进行了散列处理的口令。
- 为 `pppd` 指定选项 `login` 并通过在口令列中放置双引号 ("") 来省略 `pap-secrets` 文件中的口令。在这种情况下，将通过 UNIX 口令数据库或 `pam`(3pam) 机制执行验证。

PAP 验证期间发生的操作

PAP 验证按以下顺序发生。

图 22–1 PAP 验证流程



1. 呼叫者（被验证者）呼叫远程对等点（验证者），并在链路协商过程中提供其 PAP 用户名和口令。
2. 对等点通过其 `/etc/ppp/pap-secrets` 文件验证呼叫者的身份。如果对等点使用 PAP 的 `login` 选项，则对等点通过其口令数据库验证呼叫者的用户名和口令。
3. 如果验证成功，则对等点将继续与呼叫者进行链路协商。如果验证失败，则链路将被丢弃。
4. （可选的）如果呼叫者验证来自远程对等点的响应，则远程对等点必须将自己的 PAP 凭证发送给呼叫者。因此，远程对等点成为被验证者，而呼叫者成为验证者。
5. （可选的）原始呼叫者读取其自己的 `/etc/ppp/pap-secrets` 以验证远程对等点的身份。

注 – 如果原始呼叫者确实要求远程对等点的验证凭证，则步骤 1 和步骤 4 将同时发生。

如果对等点通过验证，协商将继续。否则，将丢弃链路。

6. 呼叫者和对等点之间的协商会一直继续，直到成功建立链路。

使用带有 login 选项的 /etc/ppp/pap-secrets

可以将用于验证 PAP 凭证的 login 选项添加到任何 PPP 配置文件中。例如，在 /etc/ppp/options 中指定 login 时，pppd 将验证呼叫者的 PAP 凭证在口令数据库中是否存在。下面展示了包含 login 选项的 /etc/ppp/pap-secrets 文件的格式。

```
joe    *  ""  *
sally  *  ""  *
sue    *  ""  *
```

这些参数具有以下含义：

Caller（呼叫者）	joe、sally 和 sue 为授权的呼叫者的名称。
Server（服务器）	星号 (*)，指示任何服务器名称都有效。PPP 配置文件中不需要 name 选项。
Password（口令）	双引号，指示任何口令都有效。 如果此列中有口令，则来自对等点的口令必须与 PAP 口令和 UNIX passwd 数据库匹配。
IP Addresses（IP 地址）	星号 (*)，指示允许使用任何 IP 地址。

质询握手身份验证协议 (Challenge-Handshake Authentication Protocol, CHAP)

CHAP 验证使用**质询**和**响应**的概念，此概念表示对等点（验证者）会质询呼叫者（被验证者）以证明其身份。质询包括一个随机数和一个由验证者生成的唯一 ID。呼叫者必须使用 ID、随机数及其 CHAP 安全凭证来生成要发送到对等点的正确响应（握手）。

CHAP 安全凭证包括 CHAP 用户名和 CHAP“密钥”。CHAP 密钥是呼叫者和对等点在进行 PPP 链路协商之前可识别的任意字符串。可在 CHAP 数据库 /etc/ppp/chap-secrets 中配置 CHAP 安全凭证。

/etc/ppp/chap-secrets 文件

CHAP 数据库在 /etc/ppp/chap-secrets 文件中实现。要成功进行验证，PPP 链路两端的计算机必须在其 /etc/ppp/chap-secrets 文件中包含另一方的 CHAP 凭证。

注 – 与 PAP 不同，共享密钥必须以明文形式保存在两个对等点中。不能将 crypt、PAM 或 PPP 登录选项与 CHAP 一起使用。

/etc/ppp/chap-secrets 文件具有以下语法。

```
myclient myserver secret5748 *
```

这些参数具有以下含义：

`myclient` 呼叫者的 CHAP 用户名。此名称可以与呼叫者的 UNIX 用户名相同，也可以不同。

`myserver` 远程计算机（通常为拨入服务器）的名称。

`secret5748` 呼叫者的 CHAP 密钥。

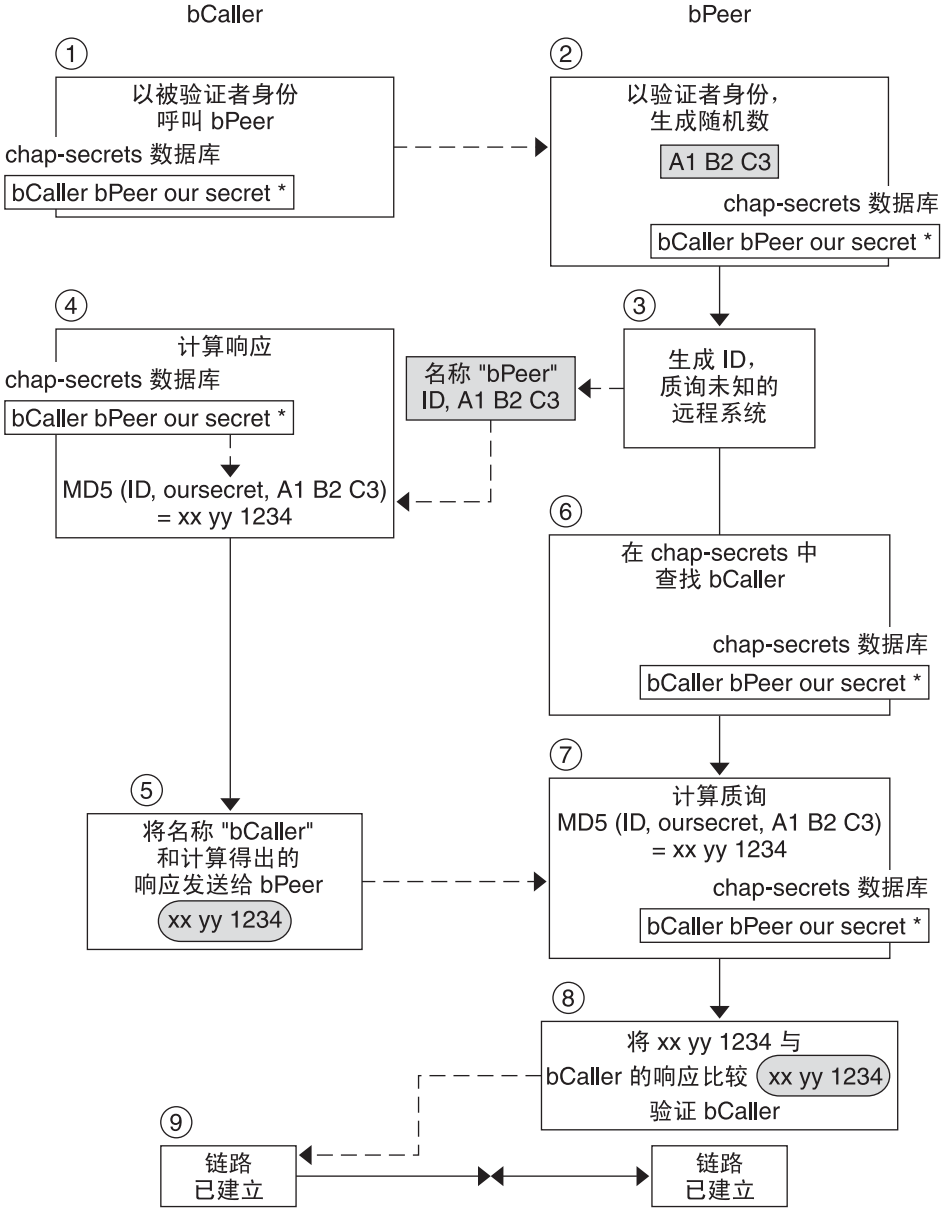
注 – 与 PAP 口令不同，CHAP 密钥不通过链路发送，CHAP 密钥在本地计算机计算响应时使用。

`*` 与呼叫者关联的 IP 地址。使用星号 (*) 表示任何 IP 地址。

CHAP 验证期间发生的操作

CHAP 验证按以下顺序发生。

图 22–2 CHAP 验证顺序



1. 将要启动通信的两个对等点针对在 PPP 链路协商期间用于验证的密钥达成一致。
2. 两台计算机的管理员将密钥、CHAP 用户名和其他 CHAP 凭证添加到各自计算机的 `/etc/ppp/chap-secrets` 数据库中。

3. 呼叫者（被验证者）呼叫远程对等点（验证者）。
4. 验证者生成随机数和 ID，并将这些数据作为质询发送给被验证者。
5. 被验证者在其 /etc/ppp/chap-secrets 数据库中查找对等点的名称和密钥。
6. 被验证者通过对密钥和对等点的随机数质询应用 MD5 计算算法来计算响应。然后，被验证者将结果作为响应发送给验证者。
7. 验证者在其 /etc/ppp/chap-secrets 数据库中查找被验证者的名称和密钥。
8. 验证者通过将 MD5 应用于作为 /etc/ppp/chap-secrets 中被验证者的质询和密钥生成的数字，来计算其自己的数字。
9. 验证者将其结果与呼叫者的响应进行比较。如果两个数字相同，则表示对等点成功验证了呼叫者，链路协商将继续。否则，将丢弃链路。

为呼叫者创建 IP 寻址方案

考虑为所有传入呼叫创建一个或多个 IP 地址，而不要为每个远程用户指定一个唯一的 IP 地址。如果可能的呼叫者数超出拨入服务器上的串行端口和调制解调器数，则使用专用的 IP 地址特别重要。可以根据站点的需要实现许多不同的方案。此外，多种方案不会相互排斥。

为呼叫者指定动态 IP 地址

动态寻址涉及为每个呼叫者指定在 /etc/ppp/options. *ttyname* 中定义的 IP 地址。动态寻址按串行端口进行。呼叫通过串行线路到达时，呼叫者将会收到所呼叫的串行接口的 /etc/ppp/options. *ttyname* 文件中的 IP 地址。

例如，假定拨入服务器具有为传入呼叫提供拨号服务的四个串行接口：

- 对于串行端口 term/a，创建包含以下项的 /etc/ppp/options.term.a 文件：

  ```
  :10.1.1.1
  ```
- 对于串行端口 term/b，创建包含以下项的 /etc/ppp/options.term.b 文件：

  ```
  :10.1.1.2
  ```
- 对于串行端口 term/c，创建包含以下项的 /etc/ppp/options.term.c 文件：

  ```
  :10.1.1.3
  ```
- 对于串行端口 term/d，创建包含以下项的 /etc/ppp/options.term.d 文件：

  ```
  :10.1.1.4
  ```

使用上面的寻址方案，串行接口 /dev/term/c 上的传入呼叫在呼叫期间将得到 IP 地址 10.1.1.3。第一个呼叫者挂起之后，通过串行接口 /dev/term/c 传入的后续呼叫也将得到 IP 地址 10.1.1.3。

动态寻址具有以下优势：

- 可以跟踪 PPP 网络使用情况到串行端口。
- 可以为 PPP 使用指定最少数量的 IP 地址。
- 可以通过更简化的方式管理 IP 过滤。

为呼叫者指定静态 IP 地址

如果您的站点实现 PPP 验证，则可以为单个呼叫者指定特定的**静态** IP 地址。在此情况下，每次拨出计算机呼叫拨入服务器时，呼叫者都将会收到相同的 IP 地址。

可以在 pap-secrets 或 chap-secrets 数据库中实现静态地址。以下是定义静态 IP 地址的 `/etc/ppp/pap-secrets` 文件的示例。

```
joe    myserver  joepasswd   10.10.111.240
sally  myserver  sallypasswd 10.10.111.241
sue    myserver  suepasswd   10.10.111.242
```

Caller（呼叫者）	`joe`、`sally` 和 `sue` 为授权的呼叫者的名称。
Server（服务器）	`myserver` 表示服务器的名称。
Password（口令）	`joepasswd`、`sallypasswd` 和 `suepasswd` 表示每个呼叫者的口令。
IP Addresses（IP 地址）	`10.10.111.240`、`10.10.111.241` 和 `10.10.111.242` 是为每个呼叫者指定的 IP 地址。

以下是定义静态 IP 地址的 `/etc/ppp/chap-secrets` 文件的示例。

```
account1 myserver secret5748  10.10.111.244
account2 myserver secret91011 10.10.111.245
```

Caller（呼叫者）	`account1` 和 `account2` 表示呼叫者的名称。
Server（服务器）	`myserver` 表示每个呼叫者的服务器的名称。
Password（口令）	`secret5748` 和 `secret91011` 表示每个呼叫者的 CHAP 密钥。
IP Addresses（IP 地址）	`10.10.111.244` 和 `10.10.111.245` 是每个呼叫者的 IP 地址。

通过 sppp 单元编号指定 IP 地址

如果使用 PAP 或 CHAP 验证，则可以通过 `sppp` 单元编号为呼叫者指定 IP 地址。下面展示了此用法的一个示例。

```
myclient ISP-server mypassword 10.10.111.240/28+
```

加号 (+) 表示已将单元编号添加到 IP 地址。请注意以下事项：

- 为远程用户指定 `10.10.111.240` 到 `10.10.111.255` 之间的地址。
- `sppp0` 得到 IP 地址 `10.10.111.240`。
- `sppp1` 得到 IP 地址 `10.10.111.241`，依此类推。

创建用于支持 DSL 的 PPPoE 通道

使用 PPPoE，可以为使用一个或多个 DSL 调制解调器的多台客户机提供基于高速数字服务的 PPP。PPPoE 通过在以下三个参与者之间创建以太网通道来实现这些服务：企业、电话公司和服务提供商。

- 有关 PPPoE 工作原理的概述和说明，请参见 第 359 页中的 “PPPoE 概述”。
- 有关设置 PPPoE 通道的任务，请参见第 20 章，设置 PPPoE 通道（任务）。

本节包含有关 PPPoE 命令和文件的详细信息，下一个表中对这些信息进行了汇总。

表 22–2 PPPoE 命令和配置文件

文件或命令	说明	参考
`/etc/ppp/pppoe`	包含缺省情况下应用于所有通道的特征的文件，这些通道由系统中的 PPPoE 设置	第 462 页中的 “`/etc/ppp/pppoe` 文件”
`/etc/ppp/pppoe.`*device*	包含特定接口的特征的文件，PPPoE 将该接口用于某个通道	第 464 页中的 “`/etc/ppp/pppoe.`*device* 文件”
`/etc/ppp/pppoe.if`	列出以太网接口的文件，PPPoE 设置的通道在这些接口上运行	第 460 页中的 “`/etc/ppp/pppoe.if` 文件”
`/usr/sbin/sppptun`	用于配置 PPPoE 通道中涉及的以太网接口的命令	第 461 页中的 “`/usr/sbin/sppptun` 命令”
`/usr/lib/inet/pppoed`	使用 PPPoE 设置通道的命令和选项	第 462 页中的 “`/usr/lib/inet/pppoed` 守护进程”

用于配置 PPPoE 的接口的文件

只有首先对 PPPoE 通道任何一端使用的接口进行配置，该通道才能支持 PPP 通信。可使用 `/usr/sbin/sppptun` 和 `/etc/ppp/pppoe.if` 文件进行此操作。必须使用这些工具在所有 Solaris PPPoE 客户机和 PPPoE 访问服务器上配置以太网接口。

/etc/ppp/pppoe.if 文件

`/etc/ppp/pppoe.if` 文件列出了主机上要用于 PPPoE 通道的所有以太网接口的名称。系统引导期间，当检测要用于 PPPoE 通道的所列出接口时，将会对此文件进行处理。

您需要显式创建 /etc/ppp/pppoe.if。在每一行上键入要为 PPPoE 配置的某个接口的名称。

以下示例展示了为 PPPoE 通道提供三个接口的服务器的 /etc/ppp/pppoe.if 文件。

```
# cat /etc/ppp/pppoe.if
hme1
hme2
hme3
```

PPPoE 客户机通常仅有一个在 /etc/ppp/pppoe.if 中列出的接口。

/usr/sbin/sppptun 命令

可以使用 /usr/sbin/sppptun 命令手动检测和取消检测要用于 PPPoE 通道的以太网接口。与此相反，系统引导期间 /etc/ppp/pppoe.if 仅被读取。这些接口应与 /etc/ppp/pppoe.if 中列出的接口相对应。

sppptun 以与 ifconfig 命令类似的方式检测 PPPoE 通道中使用的以太网接口。与 ifconfig 不同，因为涉及两个以太网协议编号，所以必须检测接口两次才能支持 PPPoE。

sppptun 的基本语法如下所示：

```
# /usr/sbin/sppptun plumb pppoed device-name
     device-name:pppoed
# /usr/sbin/sppptun plumb pppoe device-name
     device-name:pppoe
```

在此语法中，*device-name* 是要为 PPPoE 检测的设备的名称。

首次发出 sppptun 命令时，将会在接口上检测搜索协议 pppoed。第二次运行 sppptun 时，将会检测会话协议 pppoe。sppptun 可输出已检测的接口的名称。如果需要，可以使用此名称取消检测接口。

有关更多信息，请参阅 sppptun(1M) 手册页。

用于管理接口的 sppptun 命令的示例

以下示例展示了如何使用 /usr/sbin/sppptun 手动检测用于 PPPoE 的接口。

```
# /usr/sbin/sppptun plumb pppoed hme0
hme0:pppoed
# /dev/sppptun plumb pppoe hme0
 hme0:pppoe
```

以下示例展示了如何列出访问服务器上为 PPPoE 检测的接口。

```
# /usr/sbin/sppptun query
hme0:pppoe
hme0:pppoed
```

```
hme1:pppoe
hme1:pppoed
hme2:pppoe
hme2:pppoed
```

以下示例展示了如何取消检测接口。

```
# sppptun unplumb hme0:pppoed
# sppptun unplumb hme0:pppoe
```

PPPoE 访问服务器命令和文件

为客户提供 DSL 服务或支持的服务提供商可以使用正在运行 PPPoE 的访问服务器。PPPoE 访问服务器和客户机采用传统客户机/服务器关系进行工作。此关系与拨号链路上拨出计算机和拨入服务器的关系类似。一个 PPPoE 系统启动通信，一个 PPPoE 系统应答。与此相反，PPP 协议没有客户机/服务器关系的概念。PPP 将两个系统视为相等的对等点。

可用于设置 PPPoE 访问服务器的命令和文件包括：

- 第 461 页中的 “/usr/sbin/sppptun 命令”
- 第 462 页中的 “/usr/lib/inet/pppoed 守护进程”
- 第 462 页中的 “/etc/ppp/pppoe 文件”
- 第 464 页中的 “/etc/ppp/pppoe.*device* 文件”
- 第 467 页中的 “pppoe.so 共享对象”

/usr/lib/inet/pppoed 守护进程

pppoed 守护进程接受来自预期的 PPPoE 客户机的服务广播。此外，pppoed 将协商 PPPoE 通道的服务器端，然后基于该通道运行 pppd（PPP 守护进程）。

可以在 /etc/ppp/pppoe 和 /etc/ppp/pppoe.*device* 文件中配置 pppoed 服务。引导系统时，如果 /etc/ppp/pppoe 存在，将自动运行 pppoed。也可以通过键入 /usr/lib/inet/pppoed，在命令行上显式运行 pppoed 守护进程。

/etc/ppp/pppoe 文件

/etc/ppp/pppoe 文件说明访问服务器提供的服务，以及定义 PPP 如何通过 PPPoE 通道运行的选项。可以为单个接口定义服务，也可以全局定义服务（即为访问服务器上的所有接口定义服务）。访问服务器发送 /etc/ppp/pppoe 文件中的信息以响应来自可能的 PPPoE 客户机的广播。

以下是 /etc/ppp/pppoe 的基本语法：

global-options
service service-name
    service-specific-options
    device interface-name

这些参数具有以下含义：

global-options
设置 /etc/ppp/pppoe 文件的缺省选项。这些选项可以是通过 pppoed 或 pppd 使用的任何选项。有关这些选项的完整列表，请参见手册页 pppoed(1M) 和 pppd(1M)。

例如，必须在 *global options* 中列出 PPPoE 通道可以使用的以太网接口。如果未在 /etc/ppp/pppoe 中定义设备，则不会在任何接口上提供服务。

要将 devices 定义为全局选项，请使用以下格式：

device interface <,interface>

interface 指定服务将侦听可能的 PPPoE 客户机的接口。如果多个接口与服务关联，请使用逗号分隔每个名称。

service service-name
启动对服务 *service-name* 的定义。*service-name* 是一个字符串，它可以是适用于所提供服务的任何短语。

service-specific-options
列出特定于此服务的 PPPoE 和 PPP 选项。

device *interface-name*
指定以使用前面列出的服务的接口。

有关 /etc/ppp/pppoe 的其他选项，请参阅 pppoed(1M) 和 pppd(1M) 手册页。

典型的 /etc/ppp/pppoe 文件可能类似如下内容：

示例 22–2 基本 /etc/ppp/pppoe 文件

```
device hme1,hme2,hme3
service internet
   pppd "name internet-server"
service intranet
   pppd "192.168.1.1:"
service debug
   device hme1
   pppd "debug name internet-server"
```

在此文件中，以下值适用：

hme1,hme2,hme3
访问服务器上将要用于 PPPoE 通道的三个接口。

service internet
向预期的客户机通告名为 internet 的服务。提供该服务的提供商还会决定 internet 的定义方式。例如，提供商可以将 internet 解释为表示各种 IP 服务以及对 Internet 的访问。

`pppd`	设置呼叫者调用 `pppd` 时将使用的命令行选项。选项 "`name internet-server`" 将本地计算机（访问服务器）的名称指定为 `internet-server`。
`service intranet`	向预期的客户机通知名为 `intranet` 的另一个服务。
`pppd "192.168.1.1:"`	设置呼叫者调用 `pppd` 时将使用的命令行选项。呼叫者调用 `pppd` 时，将 192.168.1.1 设置为本地计算机（访问服务器）的 IP 地址。
`service debug`	在为 PPPoE 定义的接口上通告第三种服务（调试）。
`device hme1`	将对 PPPoE 通道的调试限制为 `hme1`。
`pppd "debug name internet-server"`	设置呼叫者调用 `pppd` 时将使用的命令行选项。在本例中，是对 `internet-server` （本地计算机）进行的 PPP 调试。

/etc/ppp/pppoe.device 文件

`/etc/ppp/pppoe.`*device* 文件描述了在 PPPoE 访问服务器的一个接口上提供的服务。`/etc/ppp/pppoe.`*device* 还包括定义 PPP 在 PPPoE 通道上运行的方式的选项。`/etc/ppp/pppoe.`*device* 是一个可选文件，其运行方式与全局 `/etc/ppp/pppoe` 的运行方式完全相同。但是，如果为接口定义了 `/etc/ppp/pppoe.`*device*，则该接口的参数优先于 `/etc/ppp/pppoe` 中定义的全局参数。

以下是 `/etc/ppp/pppoe.`*device* 的基本语法：

service *service-name*
service-specific-options
service *another-service-name*
service-specific-options

此语法与 `/etc/ppp/pppoe` 的语法的唯一差别是，不能使用第 462 页中的 “`/etc/ppp/pppoe` 文件” 中所示的 `device` 选项。

pppoe.so 插件

`pppoe.so` 是必须由 PPPoE 访问服务器和客户机调用的 PPPoE 共享对象文件。此文件将 MTU 和 MRU 限制为 1492，过滤驱动程序中的包，并与 `pppoed` 一起协商 PPPoE 通道。在访问服务器端，`pppoe.so` 由 `pppd` 守护进程自动调用。

使用 PPPoE 和 PPP 文件配置访问服务器

本节包含用于配置访问服务器的所有文件样例。访问服务器为多宿主服务器。该服务器连接到三个子网：green、orange 和 purple。pppoed 在服务器上以 root 身份运行，这是缺省设置。

PPPoE 客户机可以通过接口 hme0 和 hme1 访问 orange 和 purple 网络。客户机使用标准 UNIX 登录来登录到服务器。服务器使用 PAP 验证客户机。

green 网络没有通告给客户机。客户机可以访问 green 的唯一方法是直接指定 "green-net" 并提供 CHAP 验证凭证。此外，仅允许客户机 joe 和 mary 使用静态 IP 地址访问 green 网络。

示例 22–3 访问服务器的 /etc/ppp/pppoe 文件

```
service orange-net
     device hme0,hme1
     pppd "require-pap login name orange-server orange-server:"
service purple-net
     device hme0,hme1
     pppd "require-pap login name purple-server purple-server:"
service green-net
     device hme1
     pppd "require-chap name green-server green-server:"
     nowildcard
```

此样例说明访问服务器提供的服务。第一个服务部分说明 orange 网络的服务。

```
service orange-net
     device hme0,hme1
     pppd "require-pap login name orange-server orange-server:"
```

客户机通过接口 hme0 和 hme1 访问 orange 网络。指定给 pppd 命令的选项将强制服务器要求潜在的客户机提供 PAP 凭证。pppd 选项还将服务器的名称设置为 orange-server，与 pap-secrets 文件中所使用的相同。

purple 网络的服务部分与 orange 网络的服务部分相同，唯一不同的是网络和服务器名称。

接下来的部分说明了 green 网络的服务：

```
service green-net
     device hme1
     pppd "require-chap name green-server green-server:"
     nowildcard
```

此部分限制客户机访问接口 hme1。指定给 pppd 命令的选项将强制服务器要求预期的客户机提供 CHAP 凭证。pppd 选项还将服务器名称设置为 green-server，此名称将在 chap-secrets 文件中使用。nowildcard 选项指定不向客户机通告 green 网络的存在。

对于上面讨论的访问服务器方案，可以设置以下 /etc/ppp/options 文件。

示例 22–4 访问服务器的 /etc/ppp/options 文件

```
auth
proxyarp
nodefaultroute
name no-service    # don't authenticate otherwise
```

选项 name no-service 会忽略通常在 PAP 和 CHAP 验证期间搜索的服务器名称。服务器的缺省名称是由 /usr/bin/hostname 命令搜索到的名称。上一示例中的 name 选项将服务器的名称更改为 no-service。名称 no-service 可能不会出现在 pap 和 chap-secrets 文件中。此操作禁止随机用户运行 pppd 以及忽略在 /etc/ppp/options 中设置的 auth 和 name 选项。这样，由于找不到服务器名称为 no-service 的客户机的密钥，pppd 将失败。

访问服务器方案使用以下 /etc/hosts 文件。

示例 22–5 访问服务器的 /etc/hosts 文件

```
172.16.0.1    orange-server
172.17.0.1    purple-server
172.18.0.1    green-server
172.18.0.2    joes-pc
172.18.0.3    marys-pc
```

以下是用于对尝试访问 orange 和 purple 网络的客户机进行 PAP 验证的 /etc/ppp/pap-secrets 文件。

示例 22–6 访问服务器的 /etc/ppp/pap-secrets 文件

```
* orange-server "" 172.16.0.2/16+
* purple-server "" 172.17.0.2/16+
```

以下是用于 CHAP 验证的 /etc/ppp/chap-secrets 文件。请注意，该文件中只列出了 joe 和 mary 客户机。

示例 22–7 访问服务器的 /etc/ppp/chap-secrets 文件

```
 joe green-server "joe's secret" joes-pc
mary green-server "mary's secret" marys-pc
```

PPPoE 客户机命令和文件

要通过 DSL 调制解调器运行 PPP，计算机必须成为 PPPoE 客户机。必须检测用于运行 PPPoE 的接口，然后使用 pppoec 实用程序“发现”是否存在访问服务器。此后，客户机可以创建通过 DSL 调制解调器的 PPPoE 通道，并运行 PPP。

PPPoE 客户机与传统客户机/服务器模型中的访问服务器相关。PPPoE 通道不是拨号链路，但配置和操作该通道的方式几乎相同。

可用于设置 PPPoE 客户机的命令和文件包括：

- 第 461 页中的 “/usr/sbin/sppptun 命令”
- 第 467 页中的 “/usr/lib/inet/pppoec 实用程序”
- 第 467 页中的 “pppoe.so 共享对象”
- 第 441 页中的 “/etc/ppp/peers/*peer-name* 文件”
- 第 437 页中的 “/etc/ppp/options 配置文件”

/usr/lib/inet/pppoec 实用程序

/usr/lib/inet/pppoec 实用程序负责协商 PPPoE 通道的客户机端。pppoec 与 chat 实用程序类似。不直接调用 pppoec，而是将 /usr/lib/inet/pppoec 作为 pppd 的 connect 选项的参数启动。

pppoe.so 共享对象

pppoe.so 是 PPPoE 共享对象，它必须通过 PPPoE 装入，从而为访问服务器和客户机提供 PPPoE 功能。pppoe.so 共享对象将 MTU 和 MRU 限制为 1492，过滤驱动程序中的包，以及处理运行时 PPPoE 消息。

在客户机端，pppd 将在用户指定 plugin pppoe.so 选项时装入 pppoe.so。

用于定义访问服务器对等点的 /etc/ppp/peers/peer-name 文件

定义要由 pppoec 发现的访问服务器时，可以使用应用于 pppoec 和 pppd 守护进程的选项。访问服务器的 /etc/ppp/peers/*peer-name* 文件需要以下参数：

- sppptun－PPPoE 通道使用的串行设备的名称。
- plugin pppoe.so－指示 pppd 装入 pppoe.so 共享对象。
- connect "/usr/lib/inet/pppoec *device* "－启动连接。然后，connect 通过 *device*（为 PPPoE 检测的接口）调用 pppoec 实用程序。

/etc/ppp/peers/*peer-name* 文件中的其余参数应该应用于服务器上的 PPP 链路。使用将用于拨出计算机上的 /etc/ppp/peers/*peer-name* 的相同选项。尝试将 PPP 链路需要的选项数量限制为最小。

第 411 页中的“如何定义 PPPoE 访问服务器对等点”中介绍了以下示例。

示例 22–8 用于定义远程访问服务器的 /etc/ppp/peers/peer-name

```
# cat /etc/ppp/peers/dslserve
sppptun
plugin pppoe.so
connect "/usr/lib/inet/pppoec hme0"
noccp
noauth
user Red
password redsecret
noipdefault
defaultroute
```

此文件定义在设置 PPPoE 通道和指向访问服务器 `dslserve` 的 PPP 链路时要使用的参数。包括的选项如下所示。

选项	说明
`sppptun`	将 `sppptun` 定义为串行设备的名称。
`plugin pppoe.so`	指示 `pppd` 装入 `pppoe.so` 共享对象。
`connect "/usr/lib/inet/pppoec hme0"`	运行 `pppoec` 并将 `hme0` 指定为 PPPoE 通道和 PPP 链路的接口。
`noccp`	关闭链路上的 CCP 压缩。 **注 –** 许多 ISP 仅使用专有压缩算法。关闭公开提供的 CCP 算法可节省协商时间，并避免极其少见的互操作性问题。
`noauth`	禁止 `pppd` 要求访问服务器提供验证凭证。大多数 ISP 不向用户提供验证凭证。
`user Red`	将名称 `Red` 设置为客户机的用户名，访问服务器要求提供该名称以进行 PAP 验证。
`password redsecret`	将 `redsecret` 定义为要提供给访问服务器以进行 PAP 验证的口令。
`noipdefault`	将 0.0.0.0 指定为初始 IP 地址。
`defaultroute`	指示 `pppd` 在 IPCP 协商之后安装缺省 IPv4 路由。如果链路是指向 Internet 的系统链路，则应在 `/etc/ppp/peers/`*peer-name* 中包括 `defaultroute`；这也适用于 PPPoE 客户机。

◆ ◆ ◆ 第 23 章

从异步 Solaris PPP 迁移至 Solaris PPP 4.0（任务）

早期版本的 Solaris OS 实现另外一种 PPP，即异步 Solaris PPP (asppp)。如果要将运行 asppp 的对等点转换为较新的 PPP 4.0，则需要运行转换脚本。本章介绍 PPP 转换的以下主题：

- 第 469 页中的 “转换 asppp 文件之前”
- 第 472 页中的 “运行 asppp2pppd 转换脚本（任务）”

本章使用一个 asppp 配置样例来说明如何完成 PPP 转换。有关 Solaris PPP 4.0 和 asppp 之间的差别的说明，请转至第 350 页中的 “使用哪个版本的 Solaris PPP”。

转换 asppp 文件之前

您可以使用转换脚本 /usr/sbin/asppp2pppd 来转换组成标准 asppp 配置的文件：

- /etc/asppp.cf－异步 PPP 配置文件
- /etc/uucp/Systems－说明远程对等点的特征的 UUCP 文件
- /etc/uucp/Devices－说明本地计算机上的调制解调器的 UUCP 文件
- /etc/uucp/Dialers－包含调制解调器所用登录序列的 UUCP 文件，该调制解调器在 /etc/uucp/Devices 文件中说明

有关 asppp 的更多信息，请参见 *Solaris 8 System Administration Collection, Volume 3*（网址为 http://docs.sun.com）。

/etc/asppp.cf 配置文件示例

第 472 页中的 “如何从 asppp 转换为 Solaris PPP 4.0” 中所示的过程使用以下 /etc/asppp.cf 文件。

```
#
ifconfig ipdptp0 plumb mojave gobi up
```

```
path
 inactivity_timeout 120     # Approx. 2 minutes
    interface ipdptp0
    peer_system_name Pgobi    # The name we log in with (also in
                                      # /etc/uucp/Systems
```

该文件包含以下参数。

`ifconfig ipdptp0 plumb mojave gobi up`	运行 `ifconfig` 命令，以配置从本地计算机 `mojave` 的 PPP 接口 `ipdptp0` 到远程对等点 `gobi` 的链路
`inactivity_timeout 120`	若不活动时间达到两分钟，则终止该线路
`interface ipdptp0`	在拨出计算机上为异步 PPP 配置接口 `ipdptp0`
`peer_system_name Pgobi`	指定远程对等点 `Pgobi` 的名称

/etc/uucp/Systems 文件示例

第 472 页中的 “如何从 asppp 转换为 Solaris PPP 4.0” 中所示的过程使用以下 `/etc/uucp/Systems` 文件。

```
#ident  "@(#)Systems    1.5  92/07/14 SMI"  /* from SVR4 bnu:Systems 2.4 */
#

# .
# .
Pgobi Any ACU 38400 15551212 in:--in: mojave word: sand
```

该文件包含以下参数：

`Pgobi`	使用 `Pgobi` 作为远程对等点的主机名。
`Any ACU`	通知拨出计算机 `mojave` 上的调制解调器，可在一天内的任何时间与 `Pgobi` 上的调制解调器建立链路。Any ACU 表示“在 `/etc/uucp/Devices` 文件中查找 ACU”。
`38400`	将链路的最大速度设置为 38400。
`15551212`	指定 `Pgobi` 的电话号码。
`in:–in: mojave word: sand`	定义 `Pgobi` 需要用来对拨出计算机 `mojave` 进行验证的登录脚本。

/etc/uucp/Devices 文件示例

第 472 页中的 “如何从 asppp 转换为 Solaris PPP 4.0” 中所示的过程使用以下 /etc/uucp/Devices 文件。

```
#ident  "@(#)Devices  1.6  92/07/14 SMI"  /* from SVR4 bnu:Devices 2.7 */

.
.
#

TCP,et - - Any TCP -
.
.
#
ACU cua/b - Any hayes
# 0-7 are on a Magma 8 port card
Direct cua/0 - Any direct
Direct cua/1 - Any direct
Direct cua/2 - Any direct
Direct cua/3 - Any direct
Direct cua/4 - Any direct
Direct cua/5 - Any direct
Direct cua/6 - Any direct
Direct cua/7 - Any direct
# a is the console port (aka "tip" line)
Direct cua/a - Any direct
# b is the aux port on the motherboard
Direct cua/b - Any direct
# c and d are high speed sync/async ports
Direct cua/c - Any direct
Direct cua/d - Any direct
```

此文件支持连接到串行端口 cua/b 的任何 Hayes 调制解调器。

/etc/uucp/Dialers 文件示例

第 472 页中的 “如何从 asppp 转换为 Solaris PPP 4.0” 中所示的过程使用以下 /etc/uucp/Dialers 文件。

```
#
#       <Much information about modems supported by Oracle Solaris UUCP>


penril    =W-P    "" \d > Q\c : \d- > s\p9\c )-W\p\r\ds\p9\c-) y\c : \E\TP > 9\c OK
ventel    =&-%    "" \r\p\r\c $ k\c ONLINE!
vadic    =K-K    "" \005\p *-\005\p-*\005\p-* D\p BER? \E\T\e \r\c LINE
develcon ""    "" \pr\ps\c est:\007 \E\D\e \n\007
micom    ""    "" \s\c NAME? \D\r\c GO
direct
```

```
#
#
#
#   Hayes Smartmodem -- modem should be set with the configuration
#   switches as follows:
#
#       S1 - UP         S2 - UP         S3 - DOWN     S4 - UP
#       S5 - UP         S6 - DOWN     S7 - ?        S8 - DOWN
#
hayes    =,-,    "" \dA\pTE1V1X1Q0S2=255S12=255\r\c OK\r \EATDT\T\r\c CONNECT
```

<much more information about modems supported by Oraccle Solaris UUCP>

此文件包含所有类型调制解调器的聊天脚本，包括 `/etc/uucp/Dialers` 文件中支持的 Hayes 调制解调器。

运行 asppp2pppd 转换脚本（ 任务 ）

`/usr/sbin/asppp2pppd` 脚本将 `/etc/asppp.cf` 和与 PPP 相关的 UUCP 文件中的 PPP 信息复制到 Solaris PPP 4.0 文件中的相应位置。

任务先决条件

在执行下一任务之前，必须完成以下操作：

- 在同时包含 `asppp` 和 UUCP 配置文件的计算机上安装 Solaris 发行版
- 成为包含 PPP 文件的计算机（例如，计算机 `mojave`）上的超级用户

▼ 如何从 asppp 转换为 Solaris PPP 4.0

1 启动转换脚本。

```
# /usr/sbin/asppp2pppd
```

将启动转换过程，并显示以下屏幕输出。

```
This script provides only a suggested translation for your existing aspppd
configuration.  You will need to evaluate for yourself whether the translation
is appropriate for your operating environment.
Continue [Yn]?
```

2 键入 "Y" 以继续。

将显示以下输出。

```
Chat cannot do echo checking; requests for this removed.
Adding 'noauth' to /etc/ppp/options

Preparing to write out translated configuration:
    1 chat file:
        1.  /etc/ppp/chat.Pgobi.hayes
    2 option files:
        2.  /etc/ppp/peers/Pgobi
        3.  /etc/ppp/options
    1 script file:
        4.  /etc/ppp/demand
```

新的 Solaris PPP 4.0 文件已生成。

▼ 如何查看转换结果

您可以在转换过程结束时查看由 `/usr/sbin/asppp2pppd` 转换脚本创建的 Solaris PPP 4.0 文件。该脚本显示以下选项列表。

```
Enter option number:
        1 - view contents of file on standard output
        2 - view contents of file using /usr/bin/less
        3 - edit contents of file using /usr/bin/vi
        4 - delete/undelete file from list
        5 - rename file in list
        6 - show file list again
        7 - escape to shell (or "!")
        8 - abort without saving anything
        9 - save all files and exit (default)
Option:
```

1 键入 1 以查看屏幕上文件的内容。

脚本会要求提供所要查看的文件的编号。

```
File number (1 .. 4):
```

这些编号表示转换过程中列出的已转换文件，如前面的步骤 2 中所示。

2 键入 1 以查看聊天文件 `/etc/ppp/chat.Pgobi.hayes`。

```
File number (1 .. 4):  1
"" \d\dA\p\pTE1V1X1Q0S2=255S12=255\r\c
OK\r ATDT\T\r\c
CONNECT \c
in:--in: mojave
word: sand
```

聊天脚本包含 `/etc/uucp/Dialers` 文件样例的 hayes 行中显示的调制解调器“聊天”信息。`/etc/ppp/chat.Pgobi.hayes` 还包含 `/etc/uucp/Systems` 文件样例中显示的 `Pgobi` 的登录序列。聊天脚本现在已位于 `/etc/ppp/chat.Pgobi.hayes` 文件中。

3 **键入 2 以查看对等点文件 /etc/ppp/peers/Pgobi。**

```
File number (1 .. 4):  2
/dev/cua/b
38400
demand
idle 120
connect "/usr/bin/chat -f /etc/ppp/chat.Pgobi.hayes -T ’15551212’"
user NeverAuthenticate
mojave:gobi
```

串行端口信息 (/dev/cua/b) 来自 /etc/uucp/Devices 文件。链路速度、空闲时间、验证信息和对等点名称来自 /etc/asppp.cf 文件。"demand" 表示 "demand" 脚本，将在拨出计算机尝试连接到对等点 Pgobi 时调用。

4 **键入 3 以查看为拨出计算机 mojave 创建的 /etc/ppp/options 文件。**

```
File number (1 .. 4):  3
#lock
noauth
```

/etc/ppp/options 中的信息来自 /etc/asppp.cf 文件。

5 **键入 4 以查看 demand 脚本的内容。**

```
File number (1 .. 4):  4
/usr/bin/pppd file /etc/ppp/peers/Pgobi
```

调用此脚本时将运行 pppd 命令，接着此命令将读取 /etc/ppp/peers/Pgobi 以启动 mojave 和 Pgobi 之间的链路。

6 **键入 9 以保存已创建的文件。然后退出转换脚本。**

◆ ◆ ◆ 第 24 章

24 UUCP（概述）

本章介绍 UNIX 对 UNIX 复制程序 (UNIX-to-UNIX Copy Program, UUCP) 及其守护进程。本章包含以下主题：

计算机可以通过 UUCP 来传输文件和彼此交换邮件，还可以通过该程序参与大型网络，如 Usenet。

Solaris OS 提供基本网络实用程序 (Basic Network Utilities, BNU) 版本的 UUCP，该版本 UUCP 也称为 HoneyDanBer UUCP。*UUCP* 一词可以表示组成系统的所有文件和实用程序，而程序 `uucp` 只是其中的一部分。从用于在计算机之间复制文件的那些实用程序（`uucp` 和 `uuto`）到用于远程登录和执行命令的那些实用程序（`cu` 和 `uux`），都属于 UUCP 实用程序。

UUCP 硬件配置

UUCP 支持以下硬件配置：

直接链路　通过在两台计算机上的串行端口之间连接 RS-232 电缆，可以在彼此之间创建直接链路。当两台计算机定期通信且彼此之间的实际距离在 50 英尺以内时，直接链路非常有用。可以使用有限距离调制解调器来略微增大此距离。

电话线　计算机可使用高速调制解调器等自动呼叫装置 (Automatic Call Unit, ACU)，通过标准电话线与其他计算机进行通信。调制解调器将拨打 UUCP 请求的电话号码。接收端计算机具有的调制解调器必须能够应答传入的呼叫。

网络　UUCP 还可以通过运行 TCP/IP 或其他协议系列的网络进行通信。将计算机设立为网络上的主机后，该计算机即可与连接至网络的任何其他主机进

行联络。

本章假设已组装并配置了 UUCP 硬件。如果需要设置调制解调器，请参阅《系统管理指南：基本管理》和调制解调器附带的手册以获取帮助。

UUCP 软件

运行 Solaris 安装程序并选择完整分发时，将自动引入 UUCP 软件。或者，可以使用 `pkgadd` 命令来添加 UUCP 软件。可以将 UUCP 程序分成三个类别：守护进程、管理程序和用户程序。

UUCP 守护进程

UUCP 系统具有四个守护进程：`uucico`、`uuxqt`、`uusched` 和 `in.uucpd`。这些守护进程可以处理 UUCP 文件传输和命令执行。如果必要，您还可以从 shell 手动运行这些守护进程。

`uucico` 选择用于链路的设备，建立通往远程计算机的链路，并执行所需的登录步骤和权限检查。另外，`uucico` 还可以传输数据文件、执行文件以及日志结果，并通过邮件通知用户传输完成。`uucico` 作为 UUCP 登录帐户的“登录 shell”。当本地 `uucico` 守护进程调用远程计算机时，它将在会话期间与远程 `uucico` 守护进程直接进行通信。

创建所有必需的文件后，`uucp`、`uuto` 和 `uux` 程序将执行 `uucico` 守护进程，以便与远程计算机联络。`uusched` 和 `Uutry` 都执行 `uucico`。有关详细信息，请参见 `uucico(1M)` 手册页。

`uuxqt` 执行远程执行请求。此守护进程将搜索假脱机目录以找到从远程计算机发送的执行文件（始终命名为 `X.`*file*）。找到 `X.`*file* 文件后，`uuxqt` 会将其打开，以获取执行所需的数据文件列表。随后 `uuxqt` 将检查以了解所需的数据文件是否可用以及是否可访问。如果文件可用，`uuxqt` 将检查 `Permissions` 文件以确认该文件有权执行所请求的命令。`uuxqt` 守护进程由 `uudemon.hour` shell 脚本执行，该脚本由 `cron` 启动。有关详细信息，请参见 `uuxqt(1M)` 手册页。

`uusched` 调度假脱机目录中排队的工作。`uusched` 最初是在引导时通过 `uudemon.hour` shell 脚本运行的，该脚本由 `cron` 启动。有关详细信息，请参见 `uusched(1M)` 手册页。启动 `uucico` 守护进程之前，`uusched` 会对调用远程计算机的顺序进行随机化处理。

`in.uucpd` 支持通过网络的 UUCP 连接。只要建立了 UUCP 连接，远程主机上的 `inetd` 就会调用 `in.uucpd`。随后 `uucpd` 将提示您输入登录名。调用主机上的 `uucico` 必须使用登录名来做出响应。随后 `in.uucpd` 将提示您输入口令（除非不需要口令）。有关详细信息，请参见 `in.uucpd(1M)` 手册页。

UUCP 管理程序

大多数 UUCP 管理程序都位于 /usr/lib/uucp 中。大多数基础数据库文件都位于 /etc/uucp 中。唯一的例外是 uulog，它位于 /usr/bin 中。uucp 登录 ID 的起始目录为 /usr/lib/uucp。通过 su 或 login 运行管理程序时，请使用 uucp 用户 ID。该用户 ID 拥有程序和假脱机数据文件。

uulog	显示指定计算机的日志文件的内容。系统将为与您的计算机进行通信的每台远程计算机创建日志文件。日志文件记录 uucp、uuto 和 uux 的每一次使用。有关详细信息，请参见 uucp(1C) 手册页。
uucleanup	清除假脱机目录。uucleanup 通常是通过 uudemon.cleanup shell 脚本执行的，该脚本由 cron 启动。有关详细信息，请参见 uucleanup(1M) 手册页。
Uutry	测试调用处理功能并执行适度调试。Uutry 将调用 uucico 守护进程以便在您的计算机与指定的远程计算机之间建立通信链路。有关详细信息，请参见 Uutry(1M) 手册页。
uucheck	检查 UUCP 目录、程序和支持文件是否存在。uucheck 还可以检查 /etc/uucp/Permissions 文件的某些部分是否存在明显的语法错误。有关详细信息，请参见 uucheck(1M) 手册页。

UUCP 用户程序

UUCP 用户程序位于 /usr/bin 中。使用这些程序不需要特殊权限。

cu	将您的计算机连接到远程计算机，以便您可以同时登录这两台计算机。使用 cu，可以在其中任意一台计算机上传输文件或执行命令，而不失去初始链路。有关详细信息，请参见 cu(1C) 手册页。
uucp	用于将文件从一台计算机复制到另一台计算机。uucp 创建工作文件和数据文件，对要传输的作业进行排队，并调用 uucico 守护进程，随即该守护进程将尝试与远程计算机进行联络。有关详细信息，请参见 uucp(1C) 手册页。
uuto	将文件从本地计算机复制到远程计算机上的公共假脱机目录 /var/spool/uucppublic/receive。uucp 用于将文件复制到远程计算机上的任何可访问目录中，与之不同的是，uuto 将文件置于适当的假脱机目录中，并指示远程用户使用 uupick 来选取该文件。有关详细信息，请参见 uuto(1C) 手册页。
uupick	使用 uuto 将文件传输到计算机时在 /var/spool/uucppublic/receive 中检索文件。请参见 uuto(1C) 手册页。
uux	创建在远程计算机上执行命令所需的工作、数据和执行文件。有关详细信息，请参见 uux(1C) 手册页。

uustat	显示所请求的传输（uucp、uuto 或 uux）的状态。uustat 还提供控制排队传输的方式。有关详细信息，请参见 uustat(1C) 手册页。

UUCP 数据库文件

UUCP 设置的主要部分是配置组成 UUCP 数据库的文件。这些文件位于 /etc/uucp 目录中。需要编辑这些文件，才能在您的计算机上设置 UUCP 或 asppp。这些文件包括：

Config	包含变量参数的列表。可以手动设置这些参数以配置网络。
Devconfig	用于配置网络通信。
Devices	用于配置网络通信。
Dialcodes	包含 Systems 文件项的电话号码字段中可以使用的拨号代码缩写。尽管不要求，但 Dialcodes 仍可由 asppp 和 UUCP 使用。
Dialers	包含与调制解调器协商以便与远程计算机建立连接所需的字符串。Dialers 由 asppp 和 UUCP 使用。
Grades	定义作业等级以及与每个作业等级关联的权限，用户可以指定这些权限以便对远程计算机的作业进行排队。
Limits	定义允许在计算机上同时执行的 uucico、uuxqt 和 uusched 的最大数量。
Permissions	定义为试图在您的计算机上传输文件或执行命令的远程主机授予的访问权限级别。
Poll	定义系统将要轮询的计算机以及轮询时间。
Sysfiles	将 uucico 和 cu 使用的不同文件或多个文件指定为 Systems、Devices 和 Dialers 文件。
Sysname	用于为计算机定义唯一的 UUCP 名称（除了其 TCP/IP 主机名以外）。
Systems	包含 uucico 守护进程、cu 和 asppp 建立通往远程计算机的链路所需的信息。此信息包括： ■ 远程主机的名称 ■ 与远程主机关联的连接设备的名称 ■ 可访问主机的时间 ■ 电话号码 ■ 登录 ID ■ 口令

可以将多个其他文件作为支持数据库的一部分，但这些文件并不直接参与建立链路和传输文件。

配置 UUCP 数据库文件

UUCP 数据库包含第 478 页中的 “UUCP 数据库文件”中显示的文件。但是，基本 UUCP 配置仅包含以下关键文件：

- /etc/uucp/Systems
- /etc/uucp/Devices
- /etc/uucp/Dialers

由于 asppp 会使用某些 UUCP 数据库，因此，如果您计划配置 asppp，应至少了解这些关键数据库文件。配置这些数据库之后，UUCP 管理会变得非常简单。一般应先编辑 Systems 文件，然后编辑 Devices 文件。通常，可以使用缺省的 /etc/uucp/Dialers 文件（除非您计划添加缺省文件中不包含的拨号程序）。此外，您可能还需要使用以下文件来执行基本的 UUCP 和 asppp 配置：

- /etc/uucp/Sysfiles
- /etc/uucp/Dialcodes
- /etc/uucp/Sysname

由于这些文件彼此联系紧密，因此在进行任何更改之前，您应该先了解其全部内容。对某个文件中的一项进行更改可能要求对其他文件中的相关项也进行更改。第 478 页中的 “UUCP 数据库文件”中列出的其他文件之间没有密切关系。

注 – asppp 仅使用本节中介绍的文件。asppp 不使用其他 UUCP 数据库文件。

◆ ◆ ◆ 第 25 章

管理 UUCP（任务）

本章介绍在修改与计算机相关的数据库文件之后如何启动 UUCP 操作。本章包含有关在运行 Solaris OS 的计算机上设置和维护 UUCP 的过程和故障排除的信息，如下所示：

UUCP 管理（任务列表）

下表除了提供本章中包含的每个过程的简短说明外，还提供了指向这些过程的链接。

表 25–1 UUCP 管理的任务列表

任务	说明	参考
允许远程计算机访问您的系统	编辑 `/etc/passwd` 文件以添加用于标识计算机的项，将允许这些计算机访问您的系统。	第 482 页中的 “如何添加 UUCP 登录”
启动 UUCP	使用所提供的 shell 脚本启动 UUCP。	第 483 页中的 “如何启动 UUCP”
启用 UUCP 以使用 TCP/IP	编辑 `/etc/inetd.conf` 和 `/etc/uucp/Systems` 文件以激活 UUCP 的 TCP/IP 功能。	第 484 页中的 “如何激活 UUCP 的 TCP/IP 功能”
解决一些常见的 UUCP 问题	使用诊断步骤检查有故障的调制解调器或 ACU。	第 487 页中的 “如何检查有故障的调制解调器或 ACU”
	使用诊断步骤调试传输。	第 487 页中的 “如何调试传输”

添加 UUCP 登录

要正确处理来自远程计算机的传入 UUCP (uucico) 请求，每台计算机都必须在您的系统上有登录帐户。

▼ 如何添加 UUCP 登录

要允许远程计算机访问您的系统，需要按照以下步骤向 /etc/passwd 文件中添加项：

1. **成为超级用户或承担等效角色。**

   角色包含授权和具有特权的命令。有关角色的更多信息，请参见《系统管理指南：安全性服务》中的“配置 RBAC（任务列表）”。

2. **编辑 /etc/passwd 文件并添加用于标识计算机的项，以允许该计算机访问您的系统。**

   对于被允许使用 UUCP 连接访问您的系统的远程计算机，放入 /etc/passwd 文件中的项通常为：

   ```
   Ugobi:*:5:5:gobi:/var/spool/uucppublic:/usr/lib/uucp/uucico
   ```

   根据约定，远程计算机的登录名是前面带有大写字母 U 的计算机名。请注意，名称不应超过八个字符。否则，可能需要截断或缩写该名称。

   上面的项说明，Ugobi 请求的登录由 /usr/lib/uucp/uucico 回答。起始目录为 /var/spool/uucppublic。口令从 /etc/shadow 文件中获取。您必须与远程计算机的 UUCP 管理员协调口令和登录名。然后，远程管理员必须将包含登录名和未加密的口令的相应项添加到远程计算机的 Systems 文件中。

3. **与其他系统的 UUCP 管理员协调您的计算机名。**

   同样，也必须与您希望通过 UUCP 访问的所有计算机的 UUCP 管理员协调您的计算机名和口令。

启动 UUCP

UUCP 包含执行以下操作的四种 shell 脚本：轮询远程计算机、重新安排传输以及清除旧的日志文件和不成功的传输。这些脚本如下所示：

- uudemon.poll
- uudemon.hour
- uudemon.admin
- uudemon.cleanup

这些 shell 脚本应定期执行以确保 UUCP 运行正常。如果选择完全安装，则在 Solaris 安装期间，会自动在 /usr/lib/uucp/uudemon.crontab 中创建用于运行这些脚本的 crontab 文件。否则，该文件将在您安装 UUCP 软件包时创建。

您也可以手动运行 UUCP shell 脚本。以下是可以针对特定计算机进行调整的原型 uudemon.crontab 文件：

```
#
#ident  "@(#)uudemon.crontab    1.5     97/12/09 SMI"
#
# This crontab is provided as a sample. For systems
# running UUCP edit the time schedule to suit, uncomment
# the following lines, and use crontab(1) to activate the
# new schedule.
#
#48 8,12,16 * * * /usr/lib/uucp/uudemon.admin
#20 3 * * * /usr/lib/uucp/uudemon.cleanup
#0 * * * * /usr/lib/uucp/uudemon.poll
#11,41 * * * * /usr/lib/uucp/uudemon.hour
```

注 – 缺省情况下，UUCP 操作被禁用。要启用 UUCP，请在 uudemon.crontab 文件中编辑时间安排并取消对相应行的注释。

▼ 如何启动 UUCP

要激活 uudemon.crontab 文件，请执行以下操作：

1. **成为超级用户或承担等效角色。**

   角色包含授权和具有特权的命令。有关角色的更多信息，请参见《系统管理指南：安全性服务》中的“配置 RBAC（任务列表）”。

2. **根据需要，编辑 /usr/lib/uucp/uudemon.crontab 文件并更改相应项。**

3. **通过发出以下命令激活 uudemon.crontab 文件：**

   ```
   crontab < /usr/lib/uucp/uudemon.crontab
   ```

uudemon.poll Shell 脚本

缺省 uudemon.poll shell 脚本每小时读取一次 /etc/uucp/Poll 文件。如果安排轮询 Poll 文件中的所有计算机，则会将工作文件 (C.*sysnxxxx*) 放在 /var/spool/uucp/*nodename* 目录中。*nodename* 表示计算机的 UUCP 节点名称。

安排 shell 脚本在 uudemon.hour 之前每小时运行一次，以便在调用 uudemon.hour 时工作文件处于正确位置。

uudemon.hour Shell 脚本

缺省 uudemon.hour shell 脚本执行以下操作：

- 调用 uusched 程序以便在假脱机目录中搜索尚未处理的工作文件 (C.)。然后，脚本会安排将这些文件传输到远程计算机。
- 调用 uuxqt 守护进程以便在假脱机目录中搜索执行文件 (X.)，这些文件已传送到您的计算机，但在传送时未进行处理。

缺省情况下，uudemon.hour 每小时运行两次。如果预计远程计算机调用失败率比较高，则可能需要更频繁地运行 uudemon.hour。

uudemon.admin Shell 脚本

缺省 uudemon.admin shell 脚本执行以下操作：

- 运行带有 p 和 q 选项的 uustat 命令。q 报告已排队的工作文件 (C.)、数据文件 (D.) 和执行文件 (X.) 的状态。p 输出锁定文件 (/var/spool/locks) 中列出的联网进程的进程信息。
- 使用 mail 将产生的状态信息发送到 uucp 管理登录。

uudemon.cleanup Shell 脚本

缺省 uudemon.cleanup shell 脚本执行以下操作：

- 从 /var/uucp/.Log 目录中收集各台计算机的日志文件，合并这些文件，并将这些文件放入包含其他旧日志信息的 /var/uucp/.Old 目录中。
- 删除假脱机文件中保存了七天或七天以上的工作文件 (C.) 和数据文件 (D.)，以及保存了两天或两天以上的执行文件 (X.)。
- 将无法送达的邮件返回给发件人。
- 将当日收集的状态信息摘要通过邮件发送给 UUCP 管理登录 (uucp)。

在 TCP/IP 上运行 UUCP

要在 TCP/IP 网络上运行 UUCP，需要按照本节中的说明进行一些修改。

▼ 如何激活 UUCP 的 TCP/IP 功能

1 **成为超级用户或承担等效角色。**

角色包含授权和具有特权的命令。有关角色的更多信息，请参见《系统管理指南：安全性服务》中的“配置 RBAC（任务列表）”。

2 **编辑 /etc/uucp/Systems 文件以确保项中具有以下字段：**

System-Name Time TCP Port networkname Standard-Login-Chat

典型项与以下内容类似：

```
rochester Any TCP - ur-seneca login: Umachine password: xxx
```

请注意，*networkname* 字段允许您显式指定 TCP/IP 主机名。此功能对于一些站点很重要。在上面的示例中，该站点具有 UUCP 节点名称 rochester，该名称与 TCP/IP 主机名 ur-seneca 不同。此外，完全不同的计算机可以轻易运行 UUCP 并具有 TCP/IP 主机名 rochester。

Systems 文件中的 Port 字段应具有项 -。此语法等效于将该项列为 uucp。几乎在所有情况下，*networkname* 都与系统名相同，并且 Port 字段为 -，这表示将使用 services 数据库中的标准 uucp 端口。in.uucpd 守护进程期望远程计算机发送其登录名和口令进行验证，并且 in.uucpd 会提示输入登录名和口令，这与 getty 和 login 很相似。

3 **编辑 /etc/inet/services 文件以设置 UUCP 端口：**

```
uucp    540/tcp    uucpd        # uucp daemon
```

您不需要更改项。但是，如果计算机运行的是 NIS 或 NIS+ 名称服务，则应更改 /etc/services 的 /etc/nsswitch.conf 项，以便先检查 files，然后检查 nis 或 nisplus。

4 **验证是否已启用 UUCP。**

```
# svcs network/uucp
```

UUCP 服务由服务管理工具管理。要查询此服务的状态，可以使用 svcs 命令。有关服务管理工具的概述，请参阅《系统管理指南：基本管理》中的第 18 章 “管理服务（概述）”。

5 **可选如果需要，请通过键入以下内容来启用 UUCP：**

```
# inetadm -e network/uucp
```

UUCP 安全和维护

设置 UUCP 之后，维护很简单。本节介绍与安全、维护和故障排除有关的持续性 UUCP 任务。

设置 UUCP 安全

缺省 /etc/uucp/Permissions 文件可最大程度地确保 UUCP 链路的安全。缺省 Permissions 文件不包含任何项。

可以为每台远程计算机设置其他参数以定义以下内容：

- 远程计算机从您的计算机接收文件的方法
- 远程计算机具有读写权限的目录
- 远程计算机可用于远程执行的命令

典型 Permissions 项如下所示：

```
MACHINE=datsun LOGNAME=Udatsun VALIDATE=datsun
COMMANDS=rmail REQUEST=yes SENDFILES=yes
```

此项允许向“标准”UUCP 目录（而非系统中的任何位置）发送文件，或从该目录接收文件。此项还将使 UUCP 用户名在登录时得到验证。

定期 UUCP 维护

UUCP 不需要很多维护工作。但是，必须确保 crontab 文件位于第 483 页中的 “如何启动 UUCP”一节中所述的位置。您应关注邮件文件和公共目录大小的增长。

UUCP 电子邮件

UUCP 程序和脚本生成的所有电子邮件都将发送到用户 ID uucp。如果不经常以该用户身份登录，您可能不会意识到邮件不断地增加并占用了磁盘空间。要解决此问题，请在 /etc/mail/aliases 中创建一个别名，并将此类电子邮件重定向到 root 或您自己以及负责维护 UUCP 的其他人员。修改 aliases 文件之后，请记住运行 newaliases 命令。

UUCP 公共目录

目录 /var/spool/uucppublic 是每个系统中缺省情况下 UUCP 可以复制文件的位置。每个用户都具有转至 /var/spool/uucppublic 并读写该目录中的文件的权限。但是，该目录的 sticky 位已设置，目录的模式为 01777。因此，用户不能删除已复制到该目录中的文件和属于 uucp 的文件。只有您（以 root 或 uucp 身份登录的 UUCP 管理员）可以删除该目录中的文件。要防止该目录中的文件毫无控制地增加，应确保定期删除其中的文件。

如果用户不方便进行此维护，应建议他们使用 uuto 和 uupick，而不要删除出于安全原因而设置的 sticky 位。有关使用 uuto 和 uupick 的说明，请参见 uuto(1C) 手册页。也可以将目录的模式限定为仅适用于某组用户。如果不希望出现某用户将磁盘填满的情况，甚至可以拒绝其 UUCP 访问权限。

UUCP 故障排除

这些过程介绍如何解决常见 UUCP 问题。

▼ 如何检查有故障的调制解调器或 ACU

可以使用多种方法检查调制解调器或其他 ACU 是否工作正常。

1. **成为超级用户或承担等效角色。**

   角色包含授权和具有特权的命令。有关角色的更多信息，请参见《系统管理指南：安全性服务》中的“配置 RBAC（任务列表）”。

2. **通过运行以下命令获取联系失败的次数和原因：**

   ```
   # uustat -q
   ```

3. **通过特定线路呼叫并尝试输出调试信息。**

   必须在 `/etc/uucp/Devices` 文件中将该线路定义为 `direct`。如果要将该线路连接至自动拨号器，必须在命令行的结尾添加电话号码，否则必须将该设备设置为 `direct`。键入：

   ```
   # cu -d -lline
   ```

   line 为 `/dev/cua/a`。

▼ 如何调试传输

如果无法联系特定计算机，可以使用 `Uutry` 和 `uucp` 检查与该计算机的通信。

1. **成为超级用户或承担等效角色。**

   角色包含授权和具有特权的命令。有关角色的更多信息，请参见《系统管理指南：安全性服务》中的“配置 RBAC（任务列表）”。

2. **尝试联系：**

   ```
   # /usr/lib/uucp/Uutry -r machine
   ```

   将 *machine* 替换为无法联系的计算机的主机名。此命令执行以下操作：

   - 启动包含调试的传送守护进程 (`uucico`)。如果您是 `root`，则可以获取更多调试信息。
   - 将调试输出定向到 `/tmp/`*machine*。
   - 通过发出以下命令将调试输出列出到终端：

     ```
     # tail -f
     ```

按 Ctrl-C 组合键终止输出。如果要保存输出，可以从 /tmp/*machine* 中复制输出。

3 **如果 Uutry 未排查出问题，请尝试将作业排队：**

```
# uucp -r file machine\!/dir/file
```

file 使用要传送的文件的名称。

machine 使用要复制到的计算机的名称。

/dir/file 指定其他计算机的文件的位置。

4 **执行以下命令：**

```
# Uutry
```

如果仍然无法解决问题，可能需要联系当地的支持代表。请保存可以帮助诊断问题的调试输出。

注 – 也可以通过 -x *n* 选项来降低或升高 Uutry 提供的调试级别。*n* 表示调试级别。Uutry 的缺省调试级别为 5。

调试级别 3 提供有关建立连接的时间和方式的基本信息，而不提供很多关于传输的信息。但是，调试级别 9 会提供有关传输过程的详细信息。请注意，调试在传送开始和结束时都会发生。如果要对中等大小的文本使用高于 5 的级别，可以联系其他站点的管理员以决定更改该级别的时间。

检查 UUCP /etc/uucp/Systems 文件

如果在联系特定计算机时出现问题，请验证 Systems 文件中是否具有最新的信息。对于某个计算机而言，可能过期的信息包括：

- 电话号码
- 登录 ID
- 口令

检查 UUCP 错误消息

UUCP 有两种类型的错误消息：ASSERT 和 STATUS。

- 异常中止进程时，会在 /var/uucp/.Admin/errors 中记录 ASSERT 错误消息。这些消息包括文件名、sccsid、行号和文本。这些消息通常由于系统问题而产生。
- STATUS 错误消息存储在 /var/uucp/.Status 目录中。该目录包含您的计算机尝试与其通信的每台远程计算机的独立文件。这些文件包含所尝试通信的状态信息以及通信是否成功的状态信息。

检查基本信息

可以使用多个命令检查基本联网信息：

- 使用 `uuname` 命令列出您的计算机可以联系的那些计算机。
- 使用 `uulog` 命令显示特定主机的日志目录的内容。
- 使用 `uucheck -v` 命令检查 `uucp` 需要的文件和目录是否存在。此命令还将检查 `Permissions` 文件，并显示有关已设置的权限的信息。

◆ ◆ ◆ 第 26 章

26 UUCP（参考）

本章提供有关使用 UUCP 的参考信息。本章包含以下主题：

UUCP /etc/uucp/Systems 文件

/etc/uucp/Systems 文件包含 uucico 守护进程与远程计算机建立通信链路所需的信息。/etc/uucp/Systems 是配置 UUCP 时需要编辑的第一个文件。

Systems 文件中的每个项都代表一台与您的主机进行通信的远程计算机。某台特定主机可以对应多个项。附加的项代表按顺序尝试的备用通信路径。此外，缺省情况下，UUCP 将阻止 /etc/uucp/Systems 中未包含的任何计算机登录您的主机。

通过使用 Sysfiles 文件，您可以定义几个文件以用作 Systems 文件。有关 Sysfiles 的说明，请参见第 508 页中的 “UUCP /etc/uucp/Sysfiles 文件”。

以下是 Systems 文件中项的语法：

```
System-Name    Time    Type    Speed    Phone    Chat Script
```

以下是 Systems 文件中的项的示例。

示例 26–1 /etc/uucp/Systems 中的项

```
Arabian     Any  ACUEC 38400 111222  ogin: Puucp ssword:beledi
```

`Arabian`	对应系统名称字段的项。有关更多信息，请参见第 492 页中的 “/etc/uucp/Systems 文件中的系统名称字段”。
`Any`	对应时间字段的项。有关更多信息，请参见第 492 页中的 “/etc/uucp/Systems 文件中的时间字段”。
`ACUEC`	对应类型字段的项。有关更多信息，请参见第 493 页中的 “/etc/uucp/Systems 文件中的类型字段”。
`38400`	对应速度字段的项。有关更多信息，请参见第 494 页中的 “/etc/uucp/Systems 文件中的速度字段”。
`111222`	对应电话字段的项。有关更多信息，请参见第 494 页中的 “/etc/uucp/Systems 文件中的电话字段”。
`ogin: Puucp ssword:beledi`	对应聊天脚本字段的项。有关更多信息，请参见第 494 页中的 “/etc/uucp/Systems 文件中的聊天脚本字段”。

/etc/uucp/Systems 文件中的系统名称字段

此字段包含远程计算机的节点名。在 TCP/IP 网络上，此名称可以是计算机的主机名，也可以是通过 `/etc/uucp/Sysname` 文件特别为 UUCP 通信创建的名称。请参见第 491 页中的 “UUCP /etc/uucp/Systems 文件”。在示例 26–1 中，系统名称字段包含代表远程主机 `Arabian` 的项。

/etc/uucp/Systems 文件中的时间字段

此字段指定可调用远程计算机的周日期和时间。时间字段的格式如下：

```
daytime[;retry]
```

时间字段的 day 部分

day 部分可以是包含以下某些项的列表。

`Su Mo Tu We Th Fr Sa`	对应于各个周日期。
`Wk`	对应于任意工作日。
`Any`	对应于任意一天。

`Never`	您的主机永远不会启动对远程计算机的调用。调用必须由远程计算机启动。随后，您的主机在**被动模式**下工作。

时间字段的 time 部分

示例 26–1 中的时间字段为 `Any`，表示可以随时调用主机 `Arabian`。

time 部分应该是以 24 小时表示法指定的时间范围，例如 `0800-1230` 表示从 8:30 a.m. 到 12:30 p.m.。如果未指定 *time* 部分，则认为允许在一天的任何时间执行呼叫。

允许跨 0000 的时间范围。例如，`0800-0600` 表示允许在 6 a.m. 到 8 a.m. 之外的任何时间执行调用。

时间字段的 *retry* 部分

可以在 *retry* 子字段中指定尝试失败后重试之前的最短时间（以分钟为单位）。缺省等待时间为 60 分钟。该子字段分隔符为分号 (;)。例如，`Any;9` 解释为可随时执行调用，但出现故障后至少要等待 9 分钟才可重试。

如果未指定 *retry* 项，则会使用指数补偿算法。这意味着 UUCP 将以缺省等待时间开始，并且该等待时间会随尝试失败次数的增加而不断增加。例如，假设初始重试时间为 5 分钟。如果没有任何响应，则下一次重试将在 10 分钟后进行。接下来的重试将在 20 分钟后进行，依此类推，直至达到最长重试时间 23 小时为止。如果指定了 *retry*，则指定的值始终为重试时间。否则，将使用补偿算法。

/etc/uucp/Systems 文件中的类型字段

此字段包含与远程计算机建立通信链路所应使用的设备类型。此字段中使用的关键字应与 `Devices` 文件项的第一个字段匹配。

示例 26–2 类型字段中的关键字

```
Arabian     Any     ACUEC, g     38400     1112222     ogin: Puucp ssword:beledi
```

通过在类型字段中添加协议，可以定义与系统联系时采用的协议。以上示例显示如何将协议 `g` 附加到设备类型 `ACUEC` 中。有关协议的信息，请参见第 502 页中的“/etc/uucp/Devices 文件中的协议定义”。

/etc/uucp/Systems 文件中的速度字段

此字段（也称为类字段）指定建立通信链路时所使用的设备的传输速度。UUCP 速度字段可以包含字母和速度（如 C1200 或 D1200）以区分拨号器的类。请参见第 500 页中的 “/etc/uucp/Devices 文件中的类字段”。

某些设备可以在任何速度下使用，因此可以使用关键字 Any。此字段必须与关联的 Devices 文件项中的类字段匹配。

示例 26–3 速度字段中的项

```
eagle    Any    ACU, g    D1200    NY3251    ogin: nuucp ssword:Oakgrass
```

如果不需要为此字段指定信息，请使用短横线 (-) 作为此字段的占位符。

/etc/uucp/Systems 文件中的电话字段

使用此字段，可以指定供自动拨号器（称为**端口选定器**）使用的远程计算机的电话号码（称为**令牌**）。电话号码包含可选的字母缩写和数字部分。如果使用缩写，则必须在 Dialcodes 文件中列出缩写。

示例 26–4 电话字段中的项

```
nubian    Any    ACU       2400    NY555-1212    ogin: Puucp ssword:Passuan
eagle     Any    ACU, g    D1200   NY=3251       ogin: nuucp ssword:Oakgrass
```

在 Phone 字段中，等号 (=) 指示 ACU 等待二次拨号音响起后再拨打其余的数字。字符串中的短横线 (-) 指示 ACU 暂停四秒后再拨打下一个数字。

如果您的计算机与端口选定器相连，您便可以访问与该选定器连接的其他计算机。这些远程计算机的 Systems 文件项不应在 Phone 字段中包含电话号码。此字段应包含要传递给交换机的令牌。这样，端口选定器即可了解主机要与其进行通信的远程计算机，通常只需了解系统名称。关联的 Devices 文件项的结尾应该有 \D，从而确保不使用 Dialcodes 文件来转换此字段。

/etc/uucp/Systems 文件中的聊天脚本字段

此字段（也称为登录字段）包含称为**聊天脚本**的字符串。聊天脚本包含本地和远程计算机必须在其初始会话中传递给对方的字符。聊天脚本具有以下格式：

expect send [expect send] ....

expect 表示本地主机为启动会话而期待从远程主机接收的字符串。*send* 是本地主机在从远程主机接收 *expect* 字符串后发送的字符串。聊天脚本可以具有多个 expect-send（期待发送）序列。

基本聊天脚本可能包含以下内容：

- 本地主机期待从远程计算机接收的登录提示
- 本地主机为进行登录而向远程计算机发送的登录名
- 本地主机期待从远程计算机接收的口令提示
- 本地主机向远程计算机发送的口令

expect 字段可以包含的子字段形式如下：

expect[-send-expect]...

如果未成功读取前一个 *expect*，则会发送 *-send*。*-send* 后的 *- expect* 是下一个期待字符串。

例如，如果字符串为 `login--login`，则本地主机上的 UUCP 将期待 `login`。如果 UUCP 从远程计算机接收到 `login`，则 UUCP 将转至下一个字段。如果 UUCP 未收到 `login`，UUCP 将发送回车，然后再次查找 `login`。如果本地计算机最初不期待任何字符，请在 *expect* 字段中使用字符 `""`（代表 NULL 字符串）。除非 *send* 字符串以 `\c` 结束，否则所有 *send* 字段发送时都将附加一个回车。

以下是使用 *expect-send* 字符串的 `Systems` 文件项的示例：

```
sonora Any ACUEC 9600 2223333 "" \r \r ogin:-BREAK-ogin: Puucpx ssword:xyzzy
```

本示例指示本地主机上的 UUCP 发送两个回车并等待 `ogin:`（对应于 `Login:`）。如果未收到 `ogin:`，则发送 `BREAK`。收到 `ogin:` 时，将发送登录名 `Puucpx`。收到 `ssword:`（对应于 `Password:`）时，将发送口令 `xyzzy`。

下表列出了一些有用的转义符。

表 26–1 Systems 文件的聊天脚本字段中使用的转义符

转义符	含义
`\b`	发送或期待退格字符。
`\c`	如果位于字符串结尾，则取消通常发送的回车。否则应忽略。
`\d`	延迟 1 至 3 秒，然后再发送更多字符。
`\E`	启动回显检查。从此刻开始，无论何时传输字符，UUCP 都会等待接收到字符后才继续执行检查。
`\e`	关闭回显检查。

表 26–1 Systems 文件的聊天脚本字段中使用的转义符 （续）

转义符	含义
\H	忽略某一挂起。对回拨调制解调器使用此选项。
\K	发送 BREAK 字符。
\M	启用 CLOCAL 标志。
\m	禁用 CLOCAL 标志。
\n	发送或期待换行符。
\N	发送 NULL 字符 (ASCII NUL)。
\p	暂停大约 1/4 至 1/2 秒。
\r	发送或期待回车。
\s	发送或期待空格字符。
\t	发送或期待制表符。
EOT	发送 EOT，随后带有两次换行。
BREAK	发送 BREAK 字符。
ddd	发送或期待八进制数字 (*ddd*) 表示的字符。

通过聊天脚本启用回拨

某些公司设置了拨入服务器以处理来自远程计算机的调用。例如，您的公司可能已具有配备了回拨调制解调器的拨入服务器，员工可以从其家用计算机对该服务器进行呼叫。拨入服务器识别远程计算机后，便会断开与远程计算机的链路，然后再回调远程计算机。随后将重新建立通信链路。

在 Systems 文件聊天脚本中应进行回拨的位置使用 \H 选项可以简化回拨。在希望拨入服务器挂起的位置包含 \H 作为期待字符串的一部分。

例如，假设调用拨入服务器的聊天脚本包含以下字符串：

```
INITIATED\Hogin:
```

本地计算机上的 UUCP 拨号设备期待从拨入服务器接收字符 INITIATED。与字符 INITIATED 匹配后，拨号设备就会刷新它所接收的所有后续字符，直到拨入服务器挂起为止。随后，本地拨号设备将等待，直到从拨入服务器接收到期待字符串的下一部分（即字符 ogin:）为止。接收到 ogin: 后，拨号设备随后会继续处理聊天脚本。

字符串不需要直接放在 \H 之前或之后，如前面的样例字符串所示。

/etc/uucp/Systems 文件中的硬件流控制

也可以使用伪发送 STTY=*value* 字符串设置调制解调器特性。例如，STTY=crtscts 可启用硬件流控制。STTY 接受所有的 stty 模式。有关完整的详细信息，请参见 stty(1) 和 termio(7I) 手册页。

以下示例在 Systems 文件项中启用了硬件流控制：

```
unix Any ACU 2400 12015551212 "" \r ogin: Puucp ssword:Passuan "" \ STTY=crtscts
```

也可以在 Dialers 文件的项中使用此伪发送字符串。

在 /etc/uucp/Systems 文件中设置奇偶校验

在某些情况下，由于您正在呼叫的系统会检查端口奇偶校验并删除错误的行，因此您必须重置奇偶校验。expect-send（期待发送）对句 "" P_ZERO 将高序位（奇偶校验位）设置为 0。请参见以下示例中的 expect-send（期待发送）对句：

```
unix Any ACU 2400 12015551212 "" P_ZERO "" \r ogin: Puucp ssword:Passuan
```

以下是可跟在 expect-send（期待发送）对句 "" P_ZERO 后的奇偶校验对句：

"" P_EVEN　将奇偶校验设置为偶校验（缺省设置）

"" P_ODD　将奇偶校验设置为奇校验

"" P_ONE　将奇偶校验位设置为 1

可以将这些奇偶校验对句插入聊天脚本中的任何位置。奇偶校验对句适用于 expect-send（期待发送）对句 "" P_ZERO 后的聊天脚本中的所有信息。奇偶校验对句还可以用在 Dialers 文件的项中。以下示例包括奇偶校验对句 "" P_ONE：

```
unix Any ACU 2400 12015551212 "" P_ZERO "" P_ONE "" \r ogin: Puucp ssword:Passuan
```

UUCP /etc/uucp/Devices 文件

/etc/uucp/Devices 文件包含可用于与远程计算机建立链路的所有设备的信息。这些设备包括 ACU（包括高速调制解调器）、直接链路和网络连接。

/etc/uucp/Devices 文件中的项具有以下语法：

```
Type   Line   Line2   Class   Dialer-Token-Pairs
```

以下是 Devices 文件中的项，该项对应于与端口 A 连接且以 38,400 bps 速度运行的 U.S. Robotics V.32bis 调制解调器。

```
ACUEC   cua/a   -   38400   usrv32bis-ec
```

ACUEC	对应类型字段的项。有关更多信息，请参见第 498 页中的“/etc/uucp/Devices 文件中的类型字段”。
cua/a	对应线路字段的项。有关更多信息，请参见第 499 页中的“/etc/uucp/Devices 文件中的线路字段”。
-	对应线路 2 字段的项。有关更多信息，请参见第 499 页中的“/etc/uucp/Devices 文件中的线路 2 字段”。
38400	对应类字段的项。有关更多信息，请参见第 500 页中的“/etc/uucp/Devices 文件中的类字段”。
usrv32bis-ec	对应拨号器-令牌对字段的项。有关更多信息，请参见第 500 页中的“/etc/uucp/Devices 文件中的拨号器-令牌对字段”。

下一节将对每个字段加以介绍。

/etc/uucp/Devices 文件中的类型字段

此字段说明设备建立的链路的类型。UUCP 类型字段可以包含下面各节中介绍的某个关键字。

Direct 关键字

Direct 关键字主要出现在 cu 连接的项中。此关键字指明链路是连接其他计算机或端口选定器的直接链路。请为通过 cu 的 -l 选项引用的每一行单独创建一项。

ACU 关键字

ACU 关键字指明连接远程计算机的链路（无论通过 cu、UUCP、asppp 还是 Solaris PPP 4.0）是通过调制解调器建立的。可以将此调制解调器直接连接到您的计算机，也可以通过端口选定器间接连接到您的计算机。

端口选定器

端口选定器是类型字段中的变量，由端口选定器的名称替换。端口选定器是连接到网络的设备，用于提示输入呼叫调制解调器的名称，随后授予访问权限。文件 /etc/uucp/Dialers 包含仅用于 micom 和 develcon 端口选定器的调用程序脚本。可以将您自己的端口选定器项添加到 Dialers 文件中。有关更多信息，请参见第 503 页中的“UUCP /etc/uucp/Dialers 文件”。

系统名称变量

此变量由类型字段中的计算机名称替换，指明链路是连接此特定计算机的直接链路。可使用此命名方案将 Devices 项中的行与 /etc/uucp/Systems 中用于计算机 *System-Name* 的项进行关联。

Devices 文件和 Systems 文件中的类型字段

示例 26–5 对 /etc/uucp/Devices 中的字段和 /etc/uucp/Systems 中的字段进行了比较。Devices 文件的类型字段中使用的关键字要与 Systems 文件项的第三个字段匹配。在 Devices 文件中，类型字段具有 ACUEC 项，指明本例中的自动呼叫装置为 V.32bis 调制解调器。此值与 Systems 文件中的类型字段（也包含 ACUEC 项）匹配。有关更多信息，请参见第 491 页中的 “UUCP /etc/uucp/Systems 文件”。

示例 26–5 Devices 文件与 Systems 文件中类型字段的比较

以下是 Devices 文件中的项的示例。

```
ACUEC cua/a - 38400 usrv32bis-ec
```

以下是 Systems 文件中的项的示例。

```
Arabian Any ACUEC 38400 111222 ogin: Puucp ssword:beledi
```

/etc/uucp/Devices 文件中的线路字段

此字段包含与 Devices 项关联的线路（称为端口）的设备名称。如果与特定项关联的调制解调器已连接到 /dev/cua/a 设备（串行端口 A），则在此字段中输入的名称将为 cua/a。在线路字段中可以使用可选调制解调器控制标志 M 来指明设备应该处于打开状态，而无需等待载体。例如：

```
cua/a,M
```

/etc/uucp/Devices 文件中的线路 2 字段

此字段是一个占位符。请始终使用连字符 (-)。801 型拨号器（在 Solaris OS 中不受支持）使用线路 2 字段。非 801 拨号器通常不使用此配置，但仍要求在此字段中使用连字符。

/etc/uucp/Devices 文件中的类字段

如果在类型字段中使用关键字 ACU 或 Direct，则类字段包含设备的速度。不过，类字段可以包含字母和速度（如 C1200 或 D1200）以区分拨号器的类，如 Centrex 或 Dimension PBX。

由于许多大型办公室具有多种类型的电话网络，因此这种区分是必要的。一个网络可能专用于内部办公室通信，而另一个网络用于处理外部通信。在这种情况下，必须区分内部通信应该使用的线路和外部通信应该使用的线路。

Devices 文件的类字段中使用的关键字应与 Systems 文件的速度字段匹配。

示例 26–6 Devices 文件中的类字段

```
ACU   cua/a   -   D2400  hayes
```

某些设备可以在任何速度下使用，因此可以在类字段中使用关键字 Any。如果使用 Any，则线路可以满足 Systems 文件的速度字段中请求的任何速度。如果此字段为 Any 且 Systems 文件速度字段也为 Any，则缺省速度为 2400 bps。

/etc/uucp/Devices 文件中的拨号器-令牌对字段

拨号器-令牌对 (Dialer-Token-Pairs, DTP) 字段包含拨号器的名称及传递该名称的令牌。DTP 字段具有以下语法：

dialer token [dialer token]

dialer 部分可以是调制解调器和端口监视器的名称，也可以是直接链路设备的 direct 或 uudirect。您可以具有任意数目的拨号器-令牌对。如果 *dialer* 部分不存在，则可以从 Systems 文件的相关项中获取它。*token* 部分可以紧接在 dialer 部分之后提供。

最后一个拨号器-令牌对可能不存在，具体取决于关联的拨号器。在大多数情况下，最后一对仅包含 *dialer* 部分。*token* 部分可以从关联的 Systems 文件项的电话字段中获取。

dialer 部分中的有效项可以在 Dialers 文件中定义，也可以是几个特殊拨号器类型之一。这些特殊的拨号器类型被编译为软件，因此即使 Dialers 文件中不包含相应的项，也可以使用这些特殊的拨号器类型。以下列出了特殊的拨号器类型。

TCP	TCP/IP 网络
TLI	传输级别接口网络（不含 STREAMS）
TLIS	传输级别接口网络（含 STREAMS）

有关更多信息，请参见第 502 页中的“/etc/uucp/Devices 文件中的协议定义”。

/etc/uucp/Devices 文件中的拨号器-令牌对字段的结构

可以采用四种不同的方式构建 DTP 字段，具体取决于与项关联的设备。

以下是构建 DTP 字段的第一种方式：

直接连接的调制解调器－如果调制解调器直接连接至计算机上的端口，则关联的 Devices 文件项的 DTP 字段只有一对。通常是调制解调器的名称。此名称用于将特定的 Devices 文件项与 Dialers 文件中的项进行匹配。因此，拨号器字段必须与 Dialers 文件项的第一个字段匹配。

示例 26–7 直接连接的调制解调器的拨号器字段

```
Dialers    hayes =,-,   ""          \\dA\pTE1V1X1Q0S2=255S12=255\r\c
                                    \EATDT\T\r\c CONNECT
```

请注意，Devices 文件项的 DTP 字段中仅存在拨号器部分 (hayes)。这意味着将被传递给拨号器的 *token*（在本例中为电话号码）来自 Systems 文件项的电话字段。（\T 被隐含了，如示例 26–9 所示。）

以下是构建 DTP 字段的第二和第三种方式：

- **直接链路**－对于到特定计算机的直接链路，关联项的 DTP 字段包含关键字 direct。这种情况对于两类直接链路项 Direct 和 *System-Name* 都适用。请参见第 498 页中的 “/etc/uucp/Devices 文件中的类型字段”。
- **同一端口选定器上的计算机**－如果要与之通信的计算机与您的计算机位于同一个端口选定器交换机上，则您的计算机必须首先访问该交换机。然后，该交换机将与其他计算机进行连接。这类项只具有一对。*dialer* 部分用于匹配 Dialers 文件项。

示例 26–8 同一端口选定器上的计算机的 UUCP 拨号器字段

```
Dialers    develcon ,""   ""            \pr\ps\c est:\007 \E\D\e \007
```

如上所示，*token* 部分被保留为空。这指示从 Systems 文件中检索令牌。此计算机的 Systems 文件项的电话字段中包含令牌，电话字段通常是为计算机的电话号码而保留的。有关详细信息，请参见第 491 页中的 “UUCP /etc/uucp/Systems 文件”。此类 DTP 包含转义符 (\D)，可确保电话字段的内容不被解释为 Dialcodes 文件中的有效项。

以下是构建 DTP 字段的第四种方式：

连接至端口选定器的调制解调器－如果高速调制解调器连接至端口选定器，则计算机必须首先访问端口选定器交换机。该交换机将与调制解调器进行连接。此类项需要两个拨号器-令牌对。每一对的 *dialer* 部分（项的第五个和第七个字段）用于匹配 Dialers 文件中的项，如下所示。

示例 26–9 与端口选定器连接的调制解调器的 UUCP 拨号器字段

```
develcon ""     ""    \pr\ps\c  est:\007    \E\D\e      \007
ventel   =&-%   t""   \r\p\r\c  $           <K\T%\r>\c  ONLINE!
```

在第一对中，develcon 是拨号器，vent 是传递给 Develcon 交换机的令牌，用于告知该交换机与您的计算机连接的设备，如 Ventel 调制解调器。由于可以采用不同的方式来设置每个交换机，因此该令牌对于每个端口选定器都是唯一的。连接 Ventel 调制解调器后，即可访问第二对。Ventel 是拨号器，令牌来自 Systems 文件。

DTP 字段中可以出现两个转义符：

- \T－指示应使用 /etc/uucp/Dialcodes 文件来转换电话 (*token*) 字段。此转义符通常位于与调制解调器（如 Hayes 和 U.S. Robotics）关联的每个呼叫者脚本的 /etc/uucp/Dialers 文件中。因此，访问呼叫者脚本之前不会进行转换。
- \D－指示不应使用 /etc/uucp/Dialcodes 文件来转换电话 (*token*) 字段。如果未在 Devices 项的结尾指定转义符，则假设具有 \D（缺省值）。\D 还可以在 /etc/uucp/Dialers 文件中使用，该文件中应包含与网络交换机 develcon 和 micom 关联的项。

/etc/uucp/Devices 文件中的协议定义

可以定义 /etc/uucp/Devices 中的每个设备使用的协议。由于可以使用缺省协议，也可以与正在呼叫的特定系统定义协议，因此该规范通常是不必要的。有关详细信息，请参见第 491 页中的 “UUCP /etc/uucp/Systems 文件”。如果确实要指定协议，则必须使用以下格式：

Type,*Protocol [parameters]*

例如，可以使用 TCP,te 来指定 TCP/IP 协议。

下表显示了 Devices 文件的可用协议。

表 26–2 /etc/uucp/Devices 中使用的协议

协议	说明
t	此协议通常用于通过 TCP/IP 和其他可靠连接的传输。t 采用无错传输。
g	此协议是 UUCP 的固有协议。g 速度较慢，但非常可靠且适用于通过噪音较大的电话线的传输。
e	此协议采用通过面向消息的无错通道进行的传输，面向消息的通道与面向字节流的通道（如 TCP/IP）相反。

表 26–2 /etc/uucp/Devices 中使用的协议 （续）

协议	说明
f	此协议用于通过 X.25 连接的传输。f 依赖于数据流的流控制，且对于通过（几乎）可保证无错的链路（特别是 X.25/PAD 链路）进行传输非常有意义。只能针对整个文件执行校验和。如果传输失败，接收方可以请求重新传输。

以下示例显示了设备项的协议名称：

```
TCP,te - - Any TCP -
```

此示例指明，对于设备 TCP，应尝试使用 t 协议。如果传输的另一端拒绝，则使用 e 协议。

e 和 t 都不适合在调制解调器上使用。即使调制解调器能保证无错传输，数据仍可能会在调制解调器与 CPU 之间丢失。

UUCP /etc/uucp/Dialers 文件

/etc/uucp/Dialers 文件包含常用调制解调器的拨号说明。您可能不需要在此文件中更改或添加项，除非计划使用非标准调制解调器或计划定制您的 UUCP 环境。不过，您应该了解该文件的内容以及它与 Systems 和 Devices 文件之间的关系。

该文件中的内容指定在使用某条线路进行数据传输之前，必须先在该线路上进行的初始会话。此会话（称为聊天脚本）通常是传输和期待的 ASCII 字符串序列。聊天脚本通常用于拨打电话号码。

如第 497 页中的 “UUCP /etc/uucp/Devices 文件”中的示例所示，Devices 文件项中的第五个字段是 Dialers 文件或特殊拨号器类型（如 TCP、TLI 或 TLIS）的索引。uucico 守护进程尝试将 Devices 文件中的第五个字段与每个 Dialers 文件项的第一个字段进行匹配。此外，从第七个位置开始，每个奇数编号的 Devices 字段都会用作 Dialers 文件的索引。如果匹配成功，系统会解释 Dialers 项以执行拨号器会话。

Dialers 文件中的每个项都具有以下语法：

```
dialer   substitutions   expect-send
```

以下示例显示 U.S. Robotics V.32bis 调制解调器的项。

示例 26–10 /etc/uucp/Dialers 文件中的项

```
usrv32bis-e    =,-,  ""    dA\pT&FE1V1X1Q0S2=255S12=255&A1&H1&M5&B2&W\r\c OK\r
                           \EATDT\T\r\c CONNECT\s14400/ARQ STTY=crtscts
```

usrv32bis-e
: 对应 Dialer 字段的项。拨号器字段与 Devices 文件中的第五个以及其他奇数编号的字段匹配。

`=,-, ""`
对应 Substitutions 字段的项。Substitutions 字段是转换字符串。每一对字符中的第一个字符都被映射为该对的第二个字符。此映射通常用于将 = 和 - 转换为拨号器“等待拨号音”和“暂停”所需的内容。

`dA\pT&FE1V1X1Q0S2=255S12=255&A1&H1&M5&B2&W\r\c OK\r`
对应 Expect-Send 字段中的项。Expect-Send 字段是字符串。

`\EATDT\T\r\c CONNECT\s14400/ARQ STTY=crtscts`
对应 Expect-Send 字段的更多内容。

以下示例显示在运行 Solaris 安装程序期间，安装 UUCP 时分发的 `Dialers` 文件项的样例。

示例 26–11 /etc/uucp/Dialers 摘录

```
penril    =W-P "" \d > Q\c : \d- > s\p9\c )-W\p\r\ds\p9\c-) y\c : \E\TP > 9\c OK

ventel    =&-%    "" \r\p\r\c $ <K\T%%\r>\c ONLINE!

vadic    =K-K    "" \005\p *-\005\p-*\005\p-* D\p BER? \E\T\e \r\c LINE

develcon    ""    "" \pr\ps\c est:\007

\E\D\e \n\007 micom    ""    "" \s\c NAME? \D\r\c GO

hayes    =,-,    "" \dA\pTE1V1X1Q0S2=255S12=255\r\c OK\r \EATDT\T\r\c CONNECT

#   Telebit TrailBlazer
tb1200    =W-,    "" \dA\pA\pA\pTE1V1X1Q0S2=255S12=255S50=2\r\c OK\r
\EATDT\T\r\c CONNECT\s1200
tb2400    =W-,    "" \dA\pA\pA\pTE1V1X1Q0S2=255S12=255S50=3\r\c OK\r
\EATDT\T\r\c CONNECT\s2400
tbfast    =W-,    "" \dA\pA\pA\pTE1V1X1Q0S2=255S12=255S50=255\r\c OK\r
\EATDT\T\r\c CONNECT\sFAST

# USrobotics, Codes, and DSI modems

dsi-ec  =,-,    "" \dA\pTE1V1X5Q0S2=255S12=255*E1*F3*M1*S1\r\c OK\r \EATDT\T\r\c
CONNECT\sEC STTY=crtscts,crtsxoff

dsi-nec =,-,    "" \dA\pTE1V1X5Q0S2=255S12=255*E0*F3*M1*S1\r\c OK\r \EATDT\T\r\c CONNECT
STTY=crtscts,crtsxoff

usrv32bis-ec =,-,  "" \dA\pT&FE1V1X1Q0S2=255S12=255&A1&H1&M5&B2&W\r\c OK\r \EATDT\T\r\c
CONNECT\s14400/ARQ STTY=crtscts,crtsxoff

usrv32-nec =,-, "" \dA\pT&FE1V1X1Q0S2=255S12=255&A0&H1&M0&B0&W\r\c OK\r \EATDT\T\r\c
CONNECT STTY=crtscts,crtsxoff

codex-fast =,-, "" \dA\pT&C1&D2*MF0*AA1&R1&S1*DE15*FL3S2=255S7=40S10=40*TT5&W\r\c OK\r
\EATDT\T\r\c CONNECT\s38400 STTY=crtscts,crtsxoff

tb9600-ec =W-,  "" \dA\pA\pA\pTE1V1X1Q0S2=255S12=255S50=6\r\c OK\r
\EATDT\T\r\cCONNECT\s9600 STTY=crtscts,crtsxoff
```

示例 26–11 /etc/uucp/Dialers 摘录 （续）

```
tb9600-nec =W-, "" \dA\pA\pA\pTE1V1X1Q0S2=255S12=255S50=6S180=0\r\c OK\r \EATDT\T\r\c
CONNECT\s9600 STTY=crtscts,crtsxoff
```

下表列出了 Dialers 文件的发送字符串中常用的转义符。

表 26–3 /etc/uucp/Dialers 的反斜杠字符

字符	说明
\b	发送或期待退格字符。
\c	无换行符或回车。
\d	延迟大约 2 秒。
\D	未使用 Dialcodes 进行转换的电话号码或令牌。
\e	禁用回显检查。
\E	对速度较慢的设备启用回显检查。
\K	插入 Break 字符。
\n	发送换行符。
\nnn	发送八进制数字。第 491 页中的 “UUCP /etc/uucp/Systems 文件”一节中列出了可以使用的其他转义符。
\N	发送或期待 NULL 字符 (ASCII NUL)。
\p	暂停大约 12–14 秒。
\r	返回。
\s	发送或期待空格字符。
\T	使用 Dialcodes 进行转换的电话号码或令牌。

这是 Dialers 文件中的 penril 项：

```
penril =W-P "" \d > Q\c : \d- > s\p9\c )-W\p\r\ds\p9\c-) y\c : \E\TP > 9\c OK
```

首先，建立了电话号码参数的替换机制，以便将任何 = 替换为 W（等待拨号音），将任何 - 替换为 P（暂停）。

下面是该行的其余部分提供的握手情况：

- ""－不等待，表示继续执行下一步。
- \d－延迟 2 秒，然后发送回车。
- >－等待 >。

- Q\c－发送 Q（不带回车）。
- :－期待 :。
- \d-－延迟 2 秒，发送 - 和回车。
- >－等待 >。
- s\p9\c－发送 s，暂停，发送 9（不带回车）。
-)-W\p\r\ds\p9\c-)－等待)。如果未收到)，则会按照以下方式处理 - 字符之间的字符串。发送 W，暂停，发送回车，延迟，发送 s，暂停，发送 9（不带回车），然后等待)。
- y\c－发送 y（不带回车）。
- :－等待 :。
- \E\TP－\E 启用回显检查。从此刻开始，无论何时传输字符，UUCP 都会等待接收到字符后才继续操作。随后，UUCP 将发送电话号码。\T 旨在获取作为参数传递的电话号码。\T 将应用 Dialcodes 转换和此项的字段 2 指定的调制解调器功能转换。随后，\T 将发送 P 和回车。
- >－等待 >。
- 9\c－发送 9（不带换行符）。
- OK－等待字符串 OK。

启用 /etc/uucp/Dialers 文件中的硬件流控制

也可以使用伪发送 STTY=*value* 字符串设置调制解调器特性。例如，STTY=crtscts 可启用外发硬件流控制。STTY=crtsxoff 可启用传入硬件流控制。STTY=crtscts,crtsxoff 可同时启用外发和传入硬件流控制。

STTY 接受所有的 stty 模式。请参见 stty(1) 和 termio(7I) 手册页。

以下示例在 Dialers 项中启用了硬件流控制：

```
dsi =,–, "" \dA\pTE1V1X5Q0S2=255S12=255*E1*F3*M1*S1\r\c OK\r \EATDT\T\r\c
CONNECT\sEC STTY=crtscts
```

也可以在 Systems 文件的项中使用此伪发送字符串。

在 /etc/uucp/Dialers 文件中设置奇偶校验

在某些情况下，由于您正在呼叫的系统会检查端口奇偶校验并删除错误的行，因此您必须重置奇偶校验。expect-send（期待发送）对句 P_ZERO 将奇偶校验设置为零：

```
foo =,-, "" P_ZERO "" \dA\pTE1V1X1Q0S2=255S12=255\r\c OK\r\EATDT\T\r\c CONNECT
```

以下是可跟在 expect-send（期待发送）对句后的奇偶校验对句：

"" P_EVEN　将奇偶校验设置为偶校验（缺省设置）

"" P_ODD　将奇偶校验设置为奇校验

"" P_ONE　将奇偶校验设置为 1

也可以在 Systems 文件项中使用此伪发送字符串。

其他基本 UUCP 配置文件

执行基本的 UUCP 配置时，除了 Systems、Devices 和 Dialers 文件，还可以使用本节中介绍的文件。

UUCP /etc/uucp/Dialcodes 文件

使用 /etc/uucp/Dialcodes 文件，可以定义在 /etc/uucp/Systems 文件的电话字段中使用的拨号代码缩写。可以使用 Dialcodes 文件提供有关由同一站点中的多个系统使用的基本电话号码的附加信息。

每个项都具有以下语法：

```
Abbreviation    Dial-Sequence
```

Abbreviation　此字段提供 Systems 文件的电话字段中使用的缩写。

Dial-Sequence　此字段提供访问特定的 Systems 文件项时传递给拨号器的拨号序列。

下面对这两个文件中的字段进行了比较。以下是 Dialcodes 文件中的字段。

```
Abbreviation    Dial-Sequence
```

以下是 Systems 文件中的字段。

```
System-Name    Time    Type    Speed    Phone    Chat Script
```

下表包含 Dialcodes 文件中字段内容的样例。

表 26–4　Dialcodes 文件中的项

缩写	拨号序列
NY	1=212
jt	9+847

在第一行中，NY 是出现在 Systems 文件的电话字段中的缩写。例如，Systems 文件可能具有以下项：

```
NY5551212
```

当 uucico 读取 Systems 文件中的 NY 时，uucico 在 Dialcodes 文件中搜索 NY 并获取拨号序列 1=212。1=212 是呼叫纽约市任何电话所需的拨号序列。此序列包括数字 1、表示暂停和等待二次拨号音的“等号” (=)，以及区号 212。uucico 会将此信息发送给拨号器，然后返回 Systems 文件获取电话号码的其余部分：5551212。

jt 9=847- 项将与 Systems 文件中的电话字段（如 jt7867）协同使用。当 uucico 读取 Systems 文件中包含 jt7867 的项时，uucico 会将序列 9=847-7867 发送给拨号器（如果拨号器-令牌对中的令牌为 \T）。

UUCP /etc/uucp/Sysfiles 文件

通过 /etc/uucp/Sysfiles 文件，可以将 uucp 和 cu 使用的不同文件指定为 Systems、Devices 和 Dialers 文件。有关 cu 的更多信息，请参见 cu(1C) 手册页。您可以针对以下文件使用 Sysfiles：

- 不同的 Systems 文件，以便可以向 uucp 服务以外的其他地址请求登录服务。
- 不同的 Dialers 文件，以便可以为 cu 和 uucp 指定不同的握手方式。
- 多个 Systems、Dialers 和 Devices 文件。需要特别指出的是，Systems 文件可能会变得非常大，因而可以将该文件分成多个较小的文件，使其更便于处理。

Sysfiles 文件的语法如下：

```
service=w systems=x:x dialers=y:y devices=z:z
```

w 表示 uucico、cu 或这两个命令（以冒号分隔）

x 表示一个或多个要用作 Systems 文件的文件，每个文件名以冒号分隔且按照其出现的顺序读取

y 表示一个或多个要用作 Dialers 文件的文件

z 表示一个或多个要用作 Devices 文件的文件

假设每个文件名都相对于 /etc/uucp 目录（除非指定了全路径）。

以下样例 /etc/uucp/Sysfiles，除了定义标准的 /etc/uucp/Systems 文件以外，还定义了本地 Systems 文件 (Local_Systems)。

```
service=uucico:cu systems=Systems :Local_Systems
```

当 /etc/uucp/Sysfiles 包含此项时，uucico 和 cu 将首先检查标准的 /etc/uucp/Systems。如果该文件中没有对应于被调用系统的项，或者该文件中的项出现问题，这两个命令将检查 /etc/uucp/Local_Systems。

正如在前一项中指定的那样，cu 和 uucico 将共享 Dialers 和 Devices 文件。

当为 uucico 和 cu 服务定义了不同的 Systems 文件时，计算机会存储两个不同的 Systems 列表。可以使用 uuname 命令输出 uucico 列表，或者使用 uuname - C 命令输出 cu 列表。以下是该文件的另一个示例，说明了先检查备用文件，然后再检查缺省文件（如果必要）的情况：

```
service=uucico systems=Systems.cico:Systems
  dialers=Dialers.cico:Dialers \
devices=Devices.cico:Devices
  service=cu systems=Systems.cu:Systems \
dialers=Dialers.cu:Dialers \
  devices=Devices.cu:Devices
```

UUCP /etc/uucp/Sysname 文件

使用 UUCP 的每一台计算机都必须具有标识名称，通常称为**节点名**。节点名随聊天脚本和其他标识信息一同包含在远程计算机的 /etc/uucp/Systems 文件中。通常，UUCP 使用的节点名与 uname -n 命令返回的节点名相同，TCP/IP 也使用该名称。

通过创建 /etc/uucp/Sysname 文件，可以指定与 TCP/IP 主机名完全无关的 UUCP 节点名。该文件有一个占据一行的项，其中包含系统的 UUCP 节点名。

UUCP /etc/uucp/Permissions 文件

/etc/uucp/Permissions 文件指定远程计算机在登录、访问文件和执行命令方面具有的权限。某些选项可限制远程计算机请求文件的能力及其接收本地计算机放入队列中的文件的能力。其他选项可用于指定远程计算机能够在本地计算机上执行的命令。

UUCP 结构化项

每项都是一个逻辑行，物理行以反斜杠 (\) 结尾以指示连续性。以空格分隔的选项组成了项。每个选项都是采用以下格式的名称-值对：

name=value

Values 可以是以冒号分隔的列表。指定的选项中不允许包含空格。

注释行以井号 (#) 开头，且占用整行，直到换行符。空白行将被忽略，即使是在多行项中。

Permissions 文件项的类型如下所示：

- LOGNAME－指定远程计算机登录（调用）您的计算机时生效的权限。

  注 – 远程计算机呼叫您的计算机时，其标识是可疑的，除非远程计算机具有唯一的登录名和可验证的口令。

- MACHINE－指定您的计算机登录（呼叫）远程计算机时生效的权限。

LOGNAME 项包含一个 LOGNAME 选项。MACHINE 项包含一个 MACHINE 选项。一个项可以同时包含这两个选项。

UUCP 注意事项

使用 Permissions 文件限制授予远程计算机的访问权限级别时，应该考虑以下几点：

- 远程计算机登录以进行 UUCP 通信时使用的所有登录 ID 都必须出现在一个且仅一个 LOGNAME 项中。
- 使用 MACHINE 项中未包含的名称呼叫的任何站点都具有以下缺省权限或限制：
  - 执行本地发送和接收请求。
  - 远程计算机可以将文件发送到您的计算机的 /var/spool/uucppublic 目录。
  - 远程计算机发出的、在您的计算机上执行的命令必须为缺省命令之一，通常为 rmail。

UUCP REQUEST 选项

远程计算机呼叫您的计算机并请求接收文件时，该请求可能会被授权，也可能会被拒绝。REQUEST 选项指定远程计算机是否可以请求从您的计算机建立文件传输。字符串 REQUEST=yes 指定远程计算机可以请求从您的计算机传输文件。字符串 REQUEST=no 指定远程计算机不能请求从您的计算机接收文件。如果未指定 REQUEST 选项，则将使用缺省值 REQUEST=no。REQUEST 选项可以出现在 LOGNAME 项中（这样远程计算机就能呼叫您的计算机），也可以出现在 MACHINE 项中（这样您的计算机就可以呼叫远程计算机）。

UUCP SENDFILES 选项

远程计算机调用您的计算机并完成其工作后，即会尝试检索您的计算机针对远程计算机排入队列的工作。SENDFILES 选项指定您的计算机是否可以发送针对远程计算机排入队列的工作。

如果远程计算机使用 LOGNAME 选项中的一个名称进行登录，字符串 SENDFILES=yes 将指定您的计算机可以发送针对远程计算机排入队列的工作。如果在 /etc/uucp/Systems 的时间字段中输入了 Never，则此字符串是**必需的**。Never 项将本地计算机设置为被动模式，但是不允许启动对此特定远程计算机的呼叫。有关更多信息，请参见第 491 页中的 “UUCP /etc/uucp/Systems 文件”。

字符串 SENDFILES=call 指定仅当您的计算机呼叫远程计算机时才发送在您的计算机中排入队列的文件。call 值是 SENDFILES 选项的缺省值。此选项仅在 LOGNAME 项中有意义，因为将呼叫发送到远程计算机时将应用 MACHINE 项。如果该选项与 MACHINE 项结合使用，则会忽略该选项。

UUCP MYNAME 选项

使用此选项，除您的计算机的 TCP/IP 主机名（通过 hostname 命令返回）外，还可以指定其唯一的 UUCP 节点名。例如，如果您无意中为您的主机指定的名称与某个其他系统的名称相同，则可以设置 Permissions 文件的 MYNAME 选项。假设您希望将您的组织称为 widget。如果您的所有调制解调器都与主机名为 gadget 的计算机相连，则 gadget 的 Permissions 文件中的项如下：

```
service=uucico systems=Systems.cico:Systems
  dialers=Dialers.cico:Dialers \
  devices=Devices.cico:Devices
service=cu systems=Systems.cu:Systems \
  dialers=Dialers.cu:Dialers \
  devices=Devices.cu:Devices
```

现在，系统 world 可以登录计算机 gadget，就像登录 widget 一样。为了在您呼叫计算机 world 时，也能使其通过别名 widget 识别您的计算机，可以定义如下项：

```
MACHINE=world MYNAME=widget
```

也可以使用 MYNAME 选项进行测试，因为此选项允许计算机呼叫其本身。但是，由于可能会使用此选项屏蔽计算机的实际标识，因此应使用第 514 页中的 “UUCP VALIDATE 选项”中介绍的 VALIDATE 选项。

UUCP READ 和 WRITE 选项

这些选项指定 uucico 可以读取或写入的文件系统的各个部分。可以在 MACHINE 或 LOGNAME 项中指定 READ 和 WRITE 选项。

READ 和 WRITE 选项的缺省值都为 uucppublic 目录，如以下字符串所示：

```
READ=/var/spool/uucppublic WRITE=/var/spool/uucppublic
```

字符串 READ=/ 和 WRITE=/ 指定具有对“其他”权限的本地用户可访问的任何文件的访问权限。

这些项的值是以冒号分隔的路径名称的列表。READ 选项用于请求文件，而 WRITE 选项用于存储文件。其中的一个值必须是要进入或退出的文件的全路径名的前缀。要授予在 /usr/news 和公共目录中存储文件的权限，请对 WRITE 选项使用以下值：

```
WRITE=/var/spool/uucppublic:/usr/news
```

如果使用 READ 和 WRITE 选项，则必须指定所有的路径名，因为系统不会将这些路径名添加到缺省列表中。例如，如果 /usr/news 路径名是 WRITE 选项中指定的唯一路径，则系统将拒绝在公共目录中存储文件的权限。

在设置可供远程系统进行读写访问的目录时需格外小心。例如，/etc 目录包含许多关键的系统文件。远程用户不应拥有在此目录中存储文件的权限。

UUCP NOREAD 和 NOWRITE 选项

NOREAD 和 NOWRITE 选项指定除 READ 和 WRITE 选项或缺省值之外的其他情况。以下项允许读取除 /etc 目录（及其子目录，请记住，这些选项是前缀）中的文件以外的任何文件。

```
READ=/ NOREAD=/etc WRITE=/var/spool/uucppublic
```

此项只允许向缺省目录 /var/spool/uucppublic 中写入内容。NOWRITE 与 NOREAD 选项的工作方式相同。可以在 LOGNAME 和 MACHINE 项中使用 NOREAD 和 NOWRITE 选项。

UUCP CALLBACK 选项

可以在 LOGNAME 项中使用 CALLBACK 选项指定在回调调用系统之前不执行任何事务。以下是设置 CALLBACK 的原因：

- 出于安全目的－如果回调计算机成功，则可以确认它是正确的计算机。
- 出于记帐目的－如果要执行长时间的数据传输，则可以选择针对较长时间调用进行计费的计算机。

字符串 CALLBACK=yes 指定您的计算机必须回叫远程计算机，然后才能进行文件传输。

CALLBACK 选项的缺省值为 CALLBACK=no。如果将 CALLBACK 设置为 yes，则必须在对应于呼叫者的 MACHINE 项中指定影响其余会话的权限。请勿在 LOGNAME 或远程计算机针对您的主机设置的 LOGNAME 项中指定这些权限。

注 – 如果两个站点为彼此都设置了 CALLBACK 选项，则永远不会启动会话。

UUCP COMMANDS 选项

注意 – COMMANDS 选项可能会危及系统的安全性。使用此选项时应格外小心。

可以在 MACHINE 项中使用 COMMANDS 选项指定远程计算机可在您的计算机上执行的命令。uux 程序生成远程执行请求，并对要传输到远程计算机的请求进行排队。文件和命令将被发送到目标计算机进行远程执行，这对于仅在您的系统发出呼叫时才会应用 MACHINE 项而言，是一个例外。

请注意，不能在 LOGNAME 项中使用 COMMANDS。MACHINE 项中的 COMMANDS 定义命令权限，无论是您呼叫远程系统还是远程系统呼叫您。

字符串 COMMANDS=rmail 指定远程计算机可在您的计算机上执行的缺省命令。如果在 MACHINE 项中使用命令字符串，则将忽略缺省命令。例如，以下项将忽略 COMMAND 缺省值，以使名为 owl、raven、hawk 和 dove 的计算机可在您的计算机上执行 rmail、rnews 和 lp。

```
MACHINE=owl:raven:hawk:dove COMMANDS=rmail:rnews:lp
```

除以上指定的名称外，还可以指定命令的全路径名。例如，以下项指定命令 rmail 使用缺省搜索路径。

```
COMMANDS=rmail:/usr/local/rnews:/usr/local/lp
```

UUCP 的缺省搜索路径为 /bin 和 /usr/bin。远程计算机为要执行的命令指定 rnews 或 /usr/local/rnews 时，则无论缺省路径是什么，始终执行 /usr/local/rnews。同样，/usr/local/lp 是要执行的 lp 命令。

在列表中包含 ALL 值意味着，系统将执行该项中指定的远程计算机的任何命令。如果使用此值，则将授予远程计算机对您的计算机的完全访问权限。

注意 – 此值允许的访问权限远远多于普通用户拥有的访问权限。仅当两台计算机都位于同一个站点、紧密连接，且用户可信时，才应使用此值。

以下是添加了 ALL 值的字符串：

```
COMMANDS=/usr/local/rnews:ALL:/usr/local/lp
```

此字符串说明了两点：

- ALL 值可以出现在字符串中的任何位置。
- 如果请求的命令不包含 rnews 或 lp 的全路径名，则将使用为 rnews 和 lp 指定的路径名（而不是缺省路径名）。

只要指定了存在潜在危险的命令（如带有 COMMANDS 选项的 cat 和 uucp），就应使用 VALIDATE 选项。通过 UUCP 远程执行守护进程 (uuxqt) 执行命令时，读写文件的任何命令都会对本地安全性造成潜在危险。

UUCP VALIDATE 选项

只要指定的命令对您的计算机的安全造成潜在危险，就应同时使用 VALIDATE 选项和 COMMANDS 选项。尽管 VALIDATE 提供的命令访问权限比 ALL 更安全，但它也不过是在 COMMANDS 选项之上提高了安全性级别。

VALIDATE 通过交叉检查呼叫计算机的主机名与它使用的登录名，提供一定程度的呼叫者身份验证。以下字符串可确保除 widget 或 gadget 之外的任何计算机尝试以 Uwidget 身份进行登录时会拒绝连接。

```
LOGNAME=Uwidget VALIDATE=widget:gadget
```

VALIDATE 选项要求拥有特权的计算机具有处理 UUCP 事务的唯一登录名和口令。此验证的重要特征是使与此项关联的登录名和口令受到保护。如果外界人员获取了该信息，便不能再将特定的 VALIDATE 选项视为安全选项。

请认真考虑要对哪些远程计算机授予能够处理 UUCP 事务的拥有特权的登录名和口令。为远程计算机提供具有文件访问和远程执行功能的特殊登录名和口令等同于为该计算机上的任何人提供访问您计算机的普通登录名和口令。因此，如果您不信任远程计算机上的某个人，请勿为该计算机提供拥有特权的登录名和口令。

以下 LOGNAME 项指定：如果声明为 eagle、owl 或 hawk 的某个远程计算机登录了您的计算机，则它一定使用了登录名 uucpfriend：

```
LOGNAME=uucpfriend VALIDATE=eagle:owl:hawk
```

如果外界人员获取了 uucpfriend 登录名和口令，便很容易进行伪装。

但是，此项与仅在 MACHINE 项中显示的 COMMANDS 选项有什么关系呢？此项会将 MACHINE 项（和 COMMANDS 选项）与 LOGNAME 项（该项与拥有特权的登录名关联）相链接。由于登录远程计算机时不会运行执行守护进程，因此需要此链接。实际上，该链接是不知道哪个计算机发送执行请求的异步进程。因此，真正的问题是：您的计算机如何识别执行文件的来源？

每个远程计算机在您的本地计算机上都有其自己的假脱机目录。这些假脱机目录具有仅为 UUCP 程序提供的写入权限。远程计算机中的执行文件在传输到您的计算机后将被置于其假脱机目录中。uuxqt 守护进程运行时，即可使用假脱机目录名称在 Permissions 文件中查找 MACHINE 项，并获取 COMMANDS 列表。或者，如果该计算机名称未出现在 Permissions 文件中，则将使用缺省列表。

以下示例显示 MACHINE 项与 LOGNAME 项之间的关系：

```
MACHINE=eagle:owl:hawk REQUEST=yes \
COMMANDS=rmail:/usr/local/rnews \
READ=/ WRITE=/
LOGNAME=uucpz VALIDATE=eagle:owl:hawk \
REQUEST=yes SENDFILES=yes \
READ=/ WRITE=/
```

COMMANDS 选项中的值表示，远程用户可以执行 rmail 和 /usr/local/rnews。

在第一项中，必须假定在想要呼叫列出的某一台计算机时，实际呼叫的是 eagle、owl 或 hawk。因此，eagle、owl 或 hawk 假脱机目录中的所有文件都是由这些计算机中的某一台放入的。如果远程计算机登录并声明它是这三台计算机中的某一台，则其执行文件也将被置于拥有特权的假脱机目录中。因此，必须确认该计算机具有拥有特权的登录名 uucpz。

OTHER 的 UUCP MACHINE 项

可以为特定的 MACHINE 项中未提到的远程计算机指定不同的选项值。当许多计算机呼叫您的主机，且命令集不断发生变化时，可能会产生这种需要。可将 OTHER 作为计算机名称用于此项，如以下示例所示：

```
MACHINE=OTHER \
COMMANDS=rmail:rnews:/usr/local/Photo:/usr/local/xp
```

也可以针对其他 MACHINE 项中未提到的计算机设置 MACHINE 项可用的所有其他选项。

合并 UUCP 的 MACHINE 项和 LOGNAME 项

当常用选项相同时，可以将 MACHINE 和 LOGNAME 项合并为一个项。例如，以下两组项具有相同的 REQUEST、READ 和 WRITE 选项：

```
MACHINE=eagle:owl:hawk REQUEST=yes \
READ=/ WRITE=/
```

和

```
LOGNAME=uupz REQUEST=yes SENDFILES=yes \
READ=/ WRITE=/
```

可以合并这些项，如下所示：

```
MACHINE=eagle:owl:hawk REQUEST=yes \
logname=uucpz SENDFILES-yes \
READ=/ WRITE=/
```

通过合并 MACHINE 和 LOGNAME 项，提高了 Permissions 文件的可管理性和有效性。

UUCP 转发

通过一系列计算机发送文件时，中间计算机在其 COMMANDS 选项中必须具有命令 uucp。如果键入以下命令，则仅在计算机 willow 允许计算机 oak 执行 uucp 程序时才执行转发操作。

```
% uucp sample.txt oak\!willow\!pine\!/usr/spool/uucppublic
```

计算机 oak 还必须允许您的计算机执行 uucp 程序。计算机 pine（指定的最后一个计算机）不必允许执行 uucp 命令，因为该计算机不会执行任何转发操作。通常情况下，不会以该方式设置计算机。

UUCP /etc/uucp/Poll 文件

/etc/uucp/Poll 文件包含轮询远程计算机所需的信息。Poll 文件中的每个项依次包含要呼叫的远程计算机的名称、制表符或空格以及应呼叫该计算机的时间点（小时）。Poll 文件中项的格式如下所示：

sys-name hour ...

例如，项 **eagle 0 4 8 12 16 20** 指示系统每四小时对计算机 eagle 轮询一次。

uudemon.poll 脚本负责处理 Poll 文件，但并不实际执行轮询。该脚本仅在假脱机目录中设置轮询工作文件（名称始终为 C.*file*）。uudemon.poll 脚本将启动调度程序，且调度程序将检查假脱机目录中的所有工作文件。

UUCP /etc/uucp/Config 文件

使用 /etc/uucp/Config 文件，可以手动覆盖某些参数。Config 文件中的每个项都具有以下格式：

parameter=value

有关可配置参数名称的完整列表，请参见随同系统提供的 Config 文件。

以下 Config 项将缺省协议排序设置为 Gge，并将 G 协议缺省值更改为 7 个窗口和 512 字节的包。

```
Protocol=G(7,512)ge
```

UUCP /etc/uucp/Grades 文件

/etc/uucp/Grades 文件包含作业等级的定义，将发送到远程计算机的作业排入队列时会使用作业等级定义。此文件还包含每个作业等级的权限。此文件中的每一项都代表由管理员定义的作业等级的定义，用户将使用该定义将作业排入队列。

Grades 文件中的每一项都具有以下格式：

User-job-grade System-job-grade Job-size Permit-type ID-list

每一项包含的各字段间以空格分隔。项中最后一个字段所包含的子字段也以空格分隔。如果某项占用多个物理行，则可以使用反斜杠以继续在下一行中输入内容。注释行以井号 (#) 开头，且占用整行。将始终忽略空行。

UUCP 用户作业等级字段

此字段包含管理员定义的用户作业等级名称，最多可含 64 个字符。

UUCP 系统作业等级字段

此字段包含**用户作业等级**映射到的单字符作业等级。有效的字符列表为 A–Z、a–z，A 的优先级最高，z 的优先级最低。

用户作业等级与系统作业等级之间的关系

可以将一个用户作业等级绑定到多个系统作业等级。请注意，系统将在 Grades 文件中按顺序查找用户作业等级。因此，应列出系统作业等级的多次出现情况，以符合对最大作业大小的限制。

虽然未限制用户作业等级的最大数目，但是系统作业等级允许的最大数目为 52。原因是可以将多个**用户作业等级**映射到一个**系统作业等级**，但是每个**用户作业等级**在文件中必须占用单独的一行。以下是一个示例：

```
mail N Any User Any netnews N Any User Any
```

如果 Grades 文件中包含此配置，则这两个**用户作业等级**字段将共享同一个**系统作业等级**。由于**作业等级**的权限与**用户作业等级**关联，而不是与**系统作业等级**关联，因此两个**用户作业等级**可以共享同一个**系统作业等级**并具有两组不同的权限。

缺省等级

可以定义缺省**用户作业等级**到系统作业等级的绑定。必须将关键字 default 用作 Grades 文件的**用户作业等级**字段中的用户作业等级及其要绑定到的系统作业等级。应该将限制字段和 ID 字段定义为 Any，以便可以将任何用户和任何大小的作业排入此等级。以下是一个示例：

```
default a Any User Any
```

如果未定义缺省用户作业等级，则将使用内置的缺省等级 Z。由于限制字段的缺省值为 Any，因此不会检查多次出现的缺省等级。

UUCP 作业大小字段

此字段指定可进入队列的最大作业大小。**作业大小**以字节为单位，且可以是下述选项的列表。

nnnn	指定此作业等级的最大作业大小的整数
n K	表示多少 KB 的十进制数（K 是千字节的缩写）
n M	表示多少 MB 的十进制数（M 是兆字节的缩写）
Any	指定不存在最大作业大小的关键字

以下是一些示例：

- 5000 表示 5000 字节
- 10K 表示 10 KB
- 2M 表示 2 MB

UUCP 允许类型字段

此字段包含表示如何解释 ID 列表的关键字。下表列出了这些关键字及其含义。

表 26–5 允许类型字段

关键字	ID 列表内容
User	允许其使用此作业等级的用户的登录名
Non-user	不允许其使用此作业等级的用户的登录名

表 26–5 允许类型字段 （续）

关键字	ID 列表内容
Group	允许其成员使用该作业等级的组名
Non-group	不允许其成员使用该作业等级的组名

UUCP ID 列表字段

此字段包含允许或拒绝排入此作业等级的登录名或组名的列表。名称列表以空格分隔，且以换行符终止。关键字 Any 用于表示允许任何人排入此作业等级。

其他 UUCP 配置文件

本节介绍三个影响 UUCP 设备使用但很少修改的文件。

UUCP /etc/uucp/Devconfig 文件

使用 /etc/uucp/Devconfig 文件，可以按服务（如 uucp 或 cu）来配置设备。Devconfig 项定义用于特定设备的 STREAMS 模块。这些项具有以下格式：

service=*x* device=*y* push=*z*[:*z*...]

x 可以是 cu、uucico，或这两种服务（以冒号分隔）。*y* 是网络名称，而且必须与 Devices 文件中的项匹配。*z* 由 STREAMS 模块的名称替换（按这些模块推入流的顺序）。可以为 cu 和 uucp 服务定义不同的模块和设备。

以下是适用于 STARLAN 网络且在该文件中最常使用的项：

```
service=cu       device=STARLAN     push=ntty:tirdwr
service=uucico   device=STARLAN     push=ntty:tirdwr
```

此示例将推送 ntty，然后推送 tirdwr。

UUCP /etc/uucp/Limits 文件

/etc/uucp/Limits 文件控制在 uucp 网络中同时运行的 uucico、uuxqt 和 uusched 的最大数目。在大多数情况下，缺省值是可接受的，且不需要进行更改。但是，如果要更改缺省值，请使用任意文本编辑器。

Limits 文件的格式如下：

service=*x* max=*y*：

x 可以是 uucico、uuxqt 或 uusched，而 *y* 是该服务所允许的限制。这些字段可以采用任何顺序且为小写形式。

以下项是 Limits 文件中最常用的项：

```
service=uucico max=5
service=uuxqt max=5
service=uusched max=2
```

该示例允许在计算机上运行五个 uucico、五个 uuxqt 和两个 uusched。

UUCP remote.unknown 文件

影响通信设备使用的另一文件是 remote.unknown 文件。此文件是在任何 Systems 文件启动会话的情况下找不到计算机时执行的二进制程序。此程序记录会话尝试并丢弃连接。

注意 – 如果更改 remote.unknown 文件的权限使得该文件不能执行，则系统将接受来自任何系统的连接。

不存在于任何 Systems 中的计算机启动会话时，将执行此程序。该程序会记录会话尝试，但无法建立连接。如果更改此文件的权限使得该文件不能执行 (chmod 000 remote.unknown)，则系统将接受任何会话请求。这种更改非常严肃。必须有充分理由才应进行此更改。

UUCP 管理文件

接下来介绍 UUCP 管理文件。这些文件是在假脱机目录中创建的，用于锁定设备、保存临时数据或保留有关远程传输或执行的信息。

- **临时数据文件** (TM) – 从其他计算机收到文件时，UUCP 进程将在假脱机目录 /var/spool/uucp/*x* 下创建这些数据文件。目录 *x* 的名称与发送文件的远程计算机的名称相同。临时数据文件的名称具有以下格式：

  TM. *pid.ddd*

  pid 是进程 ID，*ddd* 是从 0 开始的连续的三位数字。

  收到整个文件后，TM. *pid.ddd* 文件将被移至导致传输的 C.*sysnxxxx* 文件（在后文中论述）中指定的路径名下。如果处理被异常终止，TM.*pid.ddd* 文件可以保留在 *x* 目录中。uucleanup 应自动删除这些文件。

- **锁定文件** (LCK) – 锁定文件是在每个正在使用的设备的 /var/spool/locks 目录中创建的。锁定文件可防止重复的会话和多次尝试使用同一个呼叫设备。下表显示了不同类型的 UUCP 锁定文件。

表 26–6 UUCP 锁定文件

文件名	说明
LCK.*sys*	*sys* 表示正在使用该文件的计算机的名称
LCK.*dev*	*dev* 表示正在使用该文件的设备的名称
LCK.*LOG*	*LOG* 表示锁定的 UUCP 日志文件

如果意外丢弃了通信链路（如在计算机崩溃时），这些文件可以保留在假脱机目录中。父进程不再处于活动状态后，锁定文件即被忽略（删除）。锁定文件包含创建锁定的进程的进程 ID。

- **工作文件**（C.）– 工作文件是在已针对远程计算机排队工作（如文件传输或远程命令执行）后在假脱机目录中创建的。工作文件的名称具有以下格式：

  C.*sysnxxxx*

  sys 是远程计算机的名称，*n* 是表示工作等级（优先级）的 ASCII 字符，*xxxx* 是由 UUCP 指定的四位作业序列号。工作文件包含以下信息：

  - 要发送或请求的文件的全路径名。
  - 目标或用户的全路径名或文件名。
  - 用户登录名。
  - 选项列表。
  - 假脱机目录中的关联数据文件的名称。如果已指定 uucp -C 或 uuto -p 选项，则将使用伪名称 (D.0)。
  - 源文件的模式位。
  - 完成传输时通知的远程用户的登录名。
- **数据文件**(D.) – 数据文件是在命令行上指定将源文件复制到假脱机目录时创建的。数据文件的名称具有以下格式：

  D.*systmxxxxyyy* – *systm* 是远程计算机名称中的前五个字符。*xxxx* 是由 uucp 指定的四位作业序列号。该四位作业序列号的后面可以跟有后续数字。在为一个工作文件 (C.) 创建多个 D. 文件时将使用 *yyy*。
- X.（**执行文件**）– 执行文件是在执行远程命令之前在假脱机目录中创建的。执行文件的名称具有以下格式：

  X.*sysnxxxx*

  sys 是远程计算机的名称。*n* 是表示工作等级（优先级）的字符。*xxxx* 是由 UUCP 指定的四位序列号。执行文件包含以下信息：

  - 请求者的登录名和计算机名称
  - 执行命令所需的文件的名称
  - 作为命令字符串的标准输入的输入

- 接收执行命令后的标准输出的计算机和文件的名称
- 命令字符串
- 状态返回请求的选项行

UUCP 错误消息

本节列出了与 UUCP 关联的错误消息。

UUCP ASSERT 错误消息

下表列出了 ASSERT 错误消息。

表 26–7 ASSERT 错误消息

错误消息	说明或操作
CAN'T OPEN	open() 或 fopen() 失败。
CAN'T WRITE	write()、fwrite()、fprint() 或类似命令失败。
CAN'T READ	read()、fgets() 或类似命令失败。
CAN'T CREATE	creat() 调用失败。
CAN'T ALLOCATE	动态分配失败。
CAN'T LOCK	尝试创建 LCK（锁定）文件失败。在某些情况下，该错误是致命的。
CAN'T STAT	stat() 调用失败。
CAN'T CHMOD	chmod() 调用失败。
CAN'T LINK	link() 调用失败。
CAN'T CHDIR	chdir() 调用失败。
CAN'T UNLINK	unlink() 调用失败。
WRONG ROLE	这是内部逻辑问题。
CAN'T MOVE TO CORRUPTDIR	尝试将某些错误的 C. 或 X. 文件移至 /var/spool/uucp/.Corrupt 目录失败。可能缺少该目录，或者模式或所有者不正确。
CAN'T CLOSE	close() 或 fclose() 调用失败。
FILE EXISTS	尝试创建 C. 或 D. 文件，但该文件已存在。当序列文件访问发生问题时就会出现此错误，通常说明软件出现错误。
NO uucp SERVICE NUMBER	尝试 TCP/IP 调用，但是 /etc/services 文件中没有任何对应 UUCP 的项。
BAD UID	用户 ID 不在口令数据库中。请检查名称服务配置。

表 26–7 ASSERT 错误消息 （续）

错误消息	说明或操作
BAD LOGIN_UID	与上一个说明相同。
BAD LINE	Devices 文件中有错误的行。一行或多行中的参数不足。
SYSLST OVERFLOW	gename.c 中的内部表溢出。单个作业尝试与 30 多个系统对话。
TOO MANY SAVED C FILES	与上一个说明相同。
RETURN FROM fixline ioctl	ioctl(2) 应该永远不会失败，但却失败了。系统驱动程序出现问题。
BAD SPEED	Devices 或 Systems 文件（类或速度字段）中出现错误的行速度。
BAD OPTION	Permissions 文件中有错误的行或选项。必须立即纠正此错误。
PKCGET READ	远程计算机可能已挂起。无需执行任何操作。
PKXSTART	远程计算机以无法恢复的方式异常中止。通常可以忽略此错误。
TOO MANY LOCKS	出现内部问题。请与系统供应商联系。
XMV ERROR	某个文件或目录出现了问题。可能是假脱机目录造成的，因为尝试此进程之前假设已检查目标的模式。
CAN'T FORK	尝试进行 fork 和 exec 失败。不应丢失当前作业，稍后将尝试该操作 (uuxqt)。无需执行任何操作。

UUCP STATUS 错误消息

下表列出了最常见的 STATUS 错误消息。

表 26–8 UUCP STATUS 消息

错误消息	说明/操作
OK	状态是可接受的。
NO DEVICES AVAILABLE	当前没有可调用的设备。请检查特定系统的 Devices 文件中是否包含有效设备。请在 Systems 文件中检查用于调用系统的设备。
WRONG TIME TO CALL	在 Systems 文件中指定的时间以外的其他时间对系统进行了调用。
TALKING	自解释。
LOGIN FAILED	登录特定计算机失败。原因可能是登录名或口令错误、编号错误、计算机速度较慢，或执行拨号器-令牌对脚本时发生故障。
CONVERSATION FAILED	会话在成功启动后失败。此错误通常意味着：一端已关闭、程序异常中止或线路（链路）断开。
DIAL FAILED	远程计算机始终无应答。原因可能是拨号器错误或电话号码错误。

表 26–8 UUCP STATUS 消息 （续）

错误消息	说明/操作
BAD LOGIN/MACHINE COMBINATION	调用计算机时使用的登录名/计算机名与 Permissions 文件中指定的不一致。此错误可能是由于有人试图通过伪装身份进行呼叫而造成的。
DEVICE LOCKED	要使用的调用设备当前已锁定且正在被其他进程使用。
ASSERT ERROR	出现 ASSERT 错误。请检查 /var/uucp/.Admin/errors 文件中的错误消息，并参阅第 522 页中的 “UUCP ASSERT 错误消息”一节。
SYSTEM NOT IN Systems FILE	该系统不在 Systems 文件中。
CAN’T ACCESS DEVICE	尝试使用的设备不存在或模式错误。请检查 Systems 和 Devices 文件中的相应项。
DEVICE FAILED	无法打开设备。
WRONG MACHINE NAME	被调用的计算机报告的名称与期待的名称不同。
CALLBACK REQUIRED	被调用的计算机要求回调您的计算机。
REMOTE HAS A LCK FILE FOR ME	远程计算机具有针对您的计算机的 LCK 文件。远程计算机可能正在尝试呼叫您的计算机。如果远程计算机具有旧版本的 UUCP，则与您的计算机对话的进程可能已失败，但保留了 LCK 文件。如果远程计算机具有新版本的 UUCP 且未与您的计算机进行通信，则具有 LCK 文件的进程被挂起。
REMOTE DOES NOT KNOW ME	远程计算机的 Systems 文件中没有您的计算机的节点名。
REMOTE REJECT AFTER LOGIN	您的计算机登录时使用的登录名与远程计算机期待的登录名不一致。
REMOTE REJECT, UNKNOWN MESSAGE	远程计算机因未知原因拒绝与您的计算机进行通信。远程计算机运行的可能不是标准版本的 UUCP。
STARTUP FAILED	登录成功，但是初始握手失败。
CALLER SCRIPT FAILED	此错误通常与 DIAL FAILED 相同。但是，如果经常出现此错误，则可能是 Dialers 文件中的呼叫者脚本存在问题。请使用 Uutry 进行检查。

UUCP 数字错误消息

下表列出了 /usr/include/sysexits.h 文件产生的错误状态消息的退出代码编号。uucp 当前仅使用了部分代码编号。

表 26–9 按编号排列的 UUCP 错误消息

消息编号	说明	含义
64	错误消息的基准值	错误消息从该值开始。
64	命令行用法错误	命令使用不正确，例如参数数目错误、标志错误或语法错误。
65	数据格式错误	输入数据在某方面不正确。此数据格式只能应用于用户数据，不能用于系统文件。

表 26–9 按编号排列的 UUCP 错误消息 （续）

消息编号	说明	含义
66	无法打开输入	输入文件（不是系统文件）不存在或不可读。此问题可能还包括诸如邮件程序“找不到邮件”等错误。
67	地址未知	指定的用户不存在。此错误可用于邮件地址或远程登录。
68	主机名未知	主机不存在。此错误用于邮件地址或网络请求。
69	服务不可用	服务不可用。如果支持程序或文件不存在，就会出现此错误。此消息也可能只是简单地指明出现了某些问题，但当前无法确定原因。
70	内部软件错误	检测到内部软件错误。此错误应限于与非操作系统相关的错误（如果可能）。
71	系统错误	检测到操作系统错误。发生诸如“不能派生”、“不能创建管道”等情况时可能出现此错误。例如，此错误包括 getuid 返回 passwd 文件中不存在的用户。
72	缺少关键的 OS 文件	系统文件（如 /etc/passwd 或 /var/admin/utmpx）不存在、无法打开，或包含错误（如语法错误）。
73	无法创建输出文件	无法创建用户指定的输出文件。
74	输入/输出错误	对某个文件执行 I/O 操作时出现错误。
75	临时故障。邀请用户重试	临时故障并非是真正的错误。例如，在 sendmail 中，这可能表示邮件程序无法创建连接，应在稍后重试请求。
76	协议中的远程错误	远程系统在协议交换期间返回了“不可能”出现的内容。
77	权限被拒绝	您没有足够的权限执行此操作。此消息不适用于文件系统问题（文件系统问题应使用 NOINPUT 或 CANTCREAT），而适用于较高级别的权限。例如，kre 使用此消息限制可发送邮件的学生。
78	配置错误	系统检测到配置中有错误。
79	找不到项	找不到项。
79	列出的最大值	错误消息的最高值。

第 6 部 分

使用远程系统主题

本节提供了在 Solaris 环境中管理 FTP 服务器和访问远程系统的说明。

◆ ◆ ◆ 第 27 章

27 使用远程系统（概述）

本节包括有关使用远程文件的信息。

什么是 FTP 服务器？

FTP 服务器基于 wu-ftpd。wu-ftpd 最初由位于圣路易斯的华盛顿大学开发，广泛用于互联网上批量数据的分发，它是大型 FTP 站点的首选标准。有关许可条款的信息，请参阅以下位置的相关资料：`/var/sadm/pkg/SUNWftpu/install/copyright`。

什么是远程系统？

在本章中，**远程系统**是指通过任何类型的物理网络连接到本地系统并且配置为进行 TCP/IP 通信的工作站或服务器。

在运行 Solaris 发行版的系统上，TCP/IP 配置在启动时自动建立。有关更多信息，请参见《系统管理指南：IP 服务》。

对 FTP 服务的最新更改

以前的发行版包括对 FTP 服务的多个更改。这些更改包括对 FTP 服务器的增强以及对 `ftpcount`、`ftpwho` 和 `ftp` 命令的更改。

FTP 服务器的增强功能提高可伸缩性，并改进传送日志记录功能。这些选项在第 554 页中的 “繁忙站点的配置帮助”和 ftpaccess(4) 手册页中介绍。具体而言：

- sendfile() 函数用于二进制数据下载
- ftpaccess 文件中支持的新功能
  - flush-wait 控制下载或目录列表结束时的行为
  - ipcos 为控制或数据连接设置 IP 服务类
  - 可以对 passive ports 进行配置，这样内核便可选择要侦听的 TCP 端口
  - quota-info 启用了配额信息检索功能
  - recvbuf 设置用于二进制传送的接收（上载）缓冲区大小
  - rhostlookup 允许或禁止远程主机名的查找
  - sendbuf 设置用于二进制传送的发送（下载）缓冲区大小
  - xferlog 格式定制传送日志项的格式
- -4 选项使得 FTP 服务器以单机模式运行时仅侦听 IPv4 套接字上的连接

此外，ftpcount 和 ftpwho 现在支持 -v 选项，此选项将显示虚拟主机 ftpaccess 文件中定义的 FTP 服务器类的用户计数和进程信息。有关更多信息，请参见 ftpcount(1) 和 ftpwho(1) 手册页。

FTP 客户机和服务器现在支持 Kerberos。有关更多信息，请参阅 ftp(4) 手册页和《系统管理指南：安全性服务》中的“Kerberos 用户命令”。

ftp 命令已更改。缺省情况下，在对连接到 Solaris FTP 服务器的 Solaris FTP 客户机发出 ls 命令时，该客户机将列出目录和纯文本文件。如果 FTP 服务器未在 Solaris OS 中运行，则可能不会列出目录。要在连接到非 Solaris FTP 服务器时执行缺省 Solaris 行为，可在每台 Solaris 客户机上相应地编辑 /etc/default/ftp 文件。要对单个用户进行更改，可将 FTP_LS_SENDS_NLST 环境变量设置为 yes。有关更多信息，请参见 ftp(4) 手册页。

ftpd 守护进程由服务管理工具管理。可使用 svcadm 命令对此服务执行管理操作，如启用、禁用或重新启动。可使用 svcs 命令来查询此服务对应所有守护进程的状态。有关服务管理工具的概述，请参阅《系统管理指南：基本管理》中的第 18 章 “管理服务（概述）”。

◆ ◆ ◆ 第 28 章

管理 FTP 服务器（任务）

本章包括下表中介绍的设置和管理 FTP 服务器的任务。

管理 FTP 服务器（任务列表）

表 28–1 任务列表：管理 FTP 服务器

任务	说明	参考
配置对 FTP 服务器的访问	使用 `/etc/ftpd` 目录中的 `ftpaccess`、`ftpusers` 和 `ftphosts` 文件可建立或限制对 FTP 服务器的访问。	第 534 页中的 “如何设置用户登录限制” 第 535 页中的 “如何控制无效登录尝试的次数” 第 535 页中的 “如何禁止特定用户访问 FTP 服务器” 第 536 页中的 “如何限制对缺省 FTP 服务器的访问” 第 533 页中的 “如何定义 FTP 服务器类”

表 28–1 任务列表：管理 FTP 服务器 （续）

任务	说明	参考
设置 FTP 服务器登录	为实际用户、临时用户和匿名用户建立登录帐户。	第 538 页中的“如何设置实际 FTP 用户” 第 538 页中的“如何设置临时 FTP 用户” 第 539 页中的“如何设置匿名 FTP 用户” 第 540 页中的“如何创建 /etc/shells 文件”
定制消息文件	编辑 /etc/ftpd/ftpaccess 文件以配置 FTP 服务器，使其将消息返回到与特定事件相关的 FTP 客户机。	第 541 页中的“如何定制消息文件” 第 541 页中的“如何创建要发送到用户的消息” 第 542 页中的“如何配置 README 选项”
配置对 FTP 服务器上文件的访问	使用 /etc/ftpd/ftpaccess 文件可指定用户类，允许该类用户执行某些命令或者从 FTP 服务器下载文件以及将文件上载到该服务器。	第 211 页中的“如何为拨号网络配置 DA 搜索” 第 544 页中的“控制 FTP 服务器上的上载和下载”
启用有限或完整虚拟主机	使用 /etc/ftpd/ftpaccess 文件可配置 FTP 服务器，使其支持同一计算机上的多个域。	第 547 页中的“如何启用有限虚拟主机” 第 549 页中的“如何启用完整虚拟主机”
启动 FTP 服务器	更改服务属性以在 nowait 模式、单机模式或前台模式下启动 FTP 服务器。	第 550 页中的“如何使用 SMF 启动 FTP 服务器” 第 551 页中的“如何在后台启动独立 FTP 服务器” 第 551 页中的“如何在前台启动独立 FTP 服务器”
关闭 FTP 服务器	使用 /etc/ftpd/ftpaccess 文件并运行 ftpshut 可关闭 FTP 服务器。	第 552 页中的“关闭 FTP 服务器”
常见 FTP 服务器问题故障排除	选中 syslogd 并使用 greeting text 和 log commands 可调试 FTP 服务器上的问题。	第 553 页中的“如何在 syslogd 中检查 FTP 服务器消息” 第 553 页中的“如何使用 greeting text 验证 ftpaccess” 第 554 页中的“如何检查由 FTP 用户执行的命令”

控制 FTP 服务器访问

可以使用 /etc/ftpd 目录中的以下配置文件控制对 FTP 服务器的访问。

- ftpusers 用于列出被拒绝访问 FTP 服务器的用户。
- ftphosts 用于允许或拒绝从各种主机登录到 FTP 服务器上的各种帐户。
- ftpaccess 是主 FTP 配置文件。只有使用 -a 选项调用 /etc/ftpd/ftpaccess，FTP 服务器才会读取该文件。使用 ftpaccess 文件时，所有用户必须为被允许访问 FTP 服务器的某类的成员。您可以指定仅应用于特定类的许多 ftpaccess 指令。

  有关详细信息，请参见 ftpusers(4)、ftphosts(4) 和 ftpaccess(4)。

注 – 在所有 FTP 服务器配置文件中，以 # 号开头的行被认为是注释。

▼ 如何定义 FTP 服务器类

要登录到 FTP 服务器，用户在使用 `ftpaccess` 文件时必须是某类的成员。要将 `class` 指令添加到 `ftpaccess` 文件中，应指定允许通过特定主机进行访问的用户的 *class* 名称和 *typelist*。

1 成为超级用户或承担等效角色。

角色包含授权和具有特权的命令。有关角色的更多信息，请参见《系统管理指南：安全性服务》中的“配置 RBAC（任务列表）”。

2 在 `ftpaccess` 文件中为匿名用户、临时用户和实际用户添加项。

`class` *class typelist addrglob*[*addrglob...*]

`class` 用于定义 FTP 用户的关键字。

class 由 `class` 关键字定义的名称。每次登录会与所定义类的列表进行比较。已登录的用户被视为匹配的第一个类的成员。

typelist 与三类用户（`anonymous`、`guest` 和 `real`）匹配的、用逗号分隔的关键字列表。

addrglob 域名簇或数字地址簇。*addrglob* 也可以是包含其他地址簇、以斜杠 (‘/‘) 开头的文件名：`address:netmask` 或 `address/cidr`。

以下是一些地址簇示例：

- 数字 IPv4 地址：**`10.1.2.3`**
- 域名簇 **`*.provider.com`**
- 数字 IPv4 地址簇 **`10.1.2.*`**
- 数字 IPv4 地址：网络掩码 **`10.1.2.0:255.255.255.0`**
- 数字 IPv4 地址/CIDR **`10.1.2.0/24`**
- 数字 IPv6 地址：**`2000::56:789:21ff:fe8f:ba98`**
- 数字 IPv6 地址/CIDR：**`2000::56:789:21ff:fe8f:ba98/120`**

示例 28–1 定义 FTP 服务器类

```
class  local  real,guest,anonymous *.provider.com
class  remote real,guest,anonymous *
```

上一示例将 `local` 类定义为从 `*.provider.com` 登录的 `real`、`guest` 或 `anonymous` 类型的任何用户。最后一行将 `remote` 定义为从 `*.provider.com` 之外的任何位置登录的任何用户。

▼ 如何设置用户登录限制

您可以使用 ftpaccess 文件中设置的指令限制同时登录的某类用户的数量。每个登录限制包含类名、UUCP 样式的周日期列表和超出限制时将显示的消息文件。

要设置用户登录限制，请使用以下过程中的步骤。

1 **成为超级用户或承担等效角色。**

角色包含授权和具有特权的命令。有关角色的更多信息，请参见《系统管理指南：安全性服务》中的“配置 RBAC（任务列表）”。

2 **将以下项添加到 ftpaccess 文件中：**

`limit` *class n times* [*message-file*]

`limit`	用于限制同时登录的关键字，即对属于某个已定义类的指定数目的用户在特定连接时段的同时登录进行限制。
class	由 `class` 关键字定义的名称。每次登录会与所定义类的列表进行比较。已登录的用户被视为匹配的第一个类的成员。
n	用户数。
times	可以连接相应类的周日期和时间。用 `Any` 表示任何日期。
message-file	如果用户被拒绝访问将显示的消息文件。

示例 28–2 设置用户登录限制

```
limit   anon     50  Wk0800-1800        /etc/ftpd/ftpmsg.deny
limit   anon    100  Any                 /etc/ftpd/ftpmsg.deny
limit   guest   100  Any                 /etc/ftpd/ftpmsg.deny
```

上面示例中的第一行显示，在每周的工作时间内，允许同时登录的 anon 类用户不能超过 50 个。第二行将工作时间之外可同时登录的 anon 用户限制为 100 个。最后一行显示，在任何时间，允许同时登录的 guest 用户不能超过 100 个。有关如何指定日期和时间参数的信息，请参见 `ftpaccess(4)`。

该示例还说明，达到指定的登录限制时，将返回 `/etc/ftpd/ftpmsg.deny` 文件的内容（假设 `ftpmsg.deny` 存在）。有关使用 `/usr/sbin/ftpcount` 命令查看在特定时间登录的每类用户的数量和登录限制的信息，请参见 `ftpcount(1)`。

除非达到了指定的限制，否则将允许用户登录到 FTP 服务器。匿名用户以用户 `ftp` 的身份登录。实际用户以真实身份登录；临时用户以实际用户身份登录，但其访问特权受 `chroot` 环境限制。

有关使用 `/usr/sbin/ftpwho` 命令检查登录到 FTP 服务器的用户身份信息，请参见 `ftpwho(1)`。

▼ 如何控制无效登录尝试的次数

如果因为出现问题（如需要的信息拼写错误）导致登录到 FTP 服务器失败，则通常会重复登录。在将消息记录到 `syslog` 文件之前，允许用户连续尝试登录特定的次数。然后，将断开用户的连接。通过执行以下过程中的步骤，可对登录尝试失败的次数设置限制。

1. **成为超级用户或承担等效角色。**

   角色包含授权和具有特权的命令。有关角色的更多信息，请参见《系统管理指南：安全性服务》中的“配置 RBAC（任务列表）”。

2. **将以下项添加到 `ftpaccess` 文件中。**

   ```
   loginfails n
   ```

   loginfails　用于指定在终止 FTP 连接之前，允许登录失败的次数的关键字

   n　登录可以失败的次数

示例 28–3　控制无效登录尝试的次数

```
loginfails 10
```

上面的示例说明，在尝试登录失败 10 次后，将会断开用户与 FTP 服务器的连接。

▼ 如何禁止特定用户访问 FTP 服务器

`/etc/ftpd/ftpusers` 文件列出了不允许登录到 FTP 服务器的用户名。尝试登录时，FTP 服务器将会检查 `/etc/ftpd/ftpusers` 文件，以确定是否拒绝该用户访问。如果在该文件中未找到该用户名，服务器将会在 `/etc/ftpusers` 文件中搜索。

如果 `/etc/ftpusers` 中存在匹配的用户名，则会写入一条 `syslogd` 消息，声明在过时的文件中找到匹配项。该消息还建议使用 `/etc/ftpd/ftpusers`，而不要使用 `/etc/ftpusers`。

注 – 此发行版不再支持 `/etc/ftpusers` 文件。如果安装 FTP 服务器时存在 `/etc/ftpusers` 文件，则会将该文件移到 `/etc/ftpd/ftpusers` 中。

有关其他信息，请参见 `syslogd(1M)`、`in.ftpd(1M)` 和 `ftpusers(4)`。

1. **成为超级用户或承担等效角色。**

   角色包含授权和具有特权的命令。有关角色的更多信息，请参见《系统管理指南：安全性服务》中的“配置 RBAC（任务列表）”。

2 **将不允许登录到 FTP 服务器的用户的项添加到 /etc/ftpd/ftpusers 文件中。**

示例 28–4 禁止 FTP 服务器访问

```
root
daemon
bin
sys
adm
lp
uccp
nuucp
listen
nobody
noaccess
nobody4
```

上面的示例列出了 ftpusers 文件中的典型项。用户名与 /etc/passwd 中的项匹配。该列表通常包括 root 及其他管理和系统应用程序标识。

作为安全措施，根项包括在 ftpusers 文件中。缺省安全策略是禁止 root 的远程登录。对于 /etc/default/loginfile 中设置为 CONSOLE 项的缺省值，也遵守该策略。请参见 login(1)。

▼ 如何限制对缺省 FTP 服务器的访问

除了上面提到的控制方法，还可以向 ftpaccess 文件中添加显式声明来限制对 FTP 服务器的访问。

1 **成为超级用户或承担等效角色。**

角色包含授权和具有特权的命令。有关角色的更多信息，请参见《系统管理指南：安全性服务》中的“配置 RBAC（任务列表）”。

2 **将以下项添加到 ftpaccess 文件中。**

a. **缺省情况下，允许所有用户访问缺省（非虚拟）FTP 服务器。要拒绝特定用户（anonymous 用户之外的用户）的访问，请添加以下项：**

```
defaultserver deny username [username...]
```

defaultserver	用于标识拒绝或允许对其进行访问的非虚拟服务器的关键字
username	拥有对 defaultserver 的受限访问权限的用户的登录名

b. **要允许 deny 行中未列出的用户访问，请添加以下行：**

```
defaultserver allow username [username...]
```

c. **要阻止匿名用户访问，请添加以下项：**

```
defaultserver private
```

示例 28–5 限制对缺省 FTP 服务器的访问

```
defaultserver deny *
defaultserver allow username
```

上面的示例说明，FTP 服务器拒绝除 anon 用户和 allow 行中列出的那些用户之外的所有用户访问。

也可以使用 ftphosts 文件拒绝特定登录帐户从各种主机访问。有关其他信息，请参见 ftphosts(4)。

设置 FTP 服务器登录

要访问 FTP 服务器，必须先登录。FTP 服务器支持三种类型的用户登录帐户，分别是**实际**用户、**临时**用户和**匿名**用户。

- **实际**用户具有允许他们在运行 FTP 服务器的系统上建立终端会话的帐户。整个磁盘结构对实际用户是否可见取决于目录和文件访问权限。
- **临时**用户也需要帐户来登录到 FTP 服务器。可以使用用户名和口令设置每个临时用户帐户。为了防止临时用户建立终端会话，将不会为该类用户指定功能登录 shell。登录时，FTP 服务器执行 chroot(2) 操作以限制临时用户查看到的服务器磁盘结构。

  注 – 要允许实际用户和临时用户访问 FTP 服务器，必须在 /etc/shells 文件中列出他们的登录 shell。

- **匿名**用户通过使用 ftp 或 anonymous 作为用户名来登录到 FTP 服务器。根据约定，在系统提示输入口令时，匿名用户提供电子邮件地址。

  登录时，FTP 服务器执行 chroot(2) 操作以限制匿名用户查看到的服务器磁盘结构。与可以为每个临时用户创建独立的区域不同，所有匿名用户共享一个文件区域。

  实际用户和临时用户使用包含口令（仅一个人知道）的各个帐户登录。匿名用户登录到可能对所有用户可用的已知帐户。大多数大规模文件分发是通过使用匿名帐户创建的。

▼ 如何设置实际 FTP 用户

要使实际用户可以访问 FTP 服务器，请按照以下说明操作：

1. **验证用户是否具有使用用户名和口令设置的可用于建立终端会话的帐户。**
   有关更多信息，请参见《系统管理指南：基本管理》中的第 4 章 “管理用户帐户和组（概述）”。

2. **确认该实际用户是否是 `ftpaccess` 文件中某类的成员。**
   有关 `ftpaccess` 文件中定义的用户类的信息，请参见第 533 页中的 “如何定义 FTP 服务器类”。

3. **验证 `/etc/shells` 文件中是否列出了用户的登录 shell。**

▼ 如何设置临时 FTP 用户

`ftpconfig` 脚本用于将所有需要的系统文件复制到起始目录中。如果临时用户和临时用户的起始目录已存在，则 `ftpconfig` 脚本将会使用当前的系统文件更新该区域。

有关更多信息，请参见 `ftpconfig(1M)`。

注 – 与为匿名用户设置的用户名（`anonymous` 或 `ftp`）不同，FTP 临时用户的用户名不是固定的。可以选择将任何名称作为实际用户名。

要使临时用户可以访问 FTP 服务器，请执行以下操作：

1. **使用 `useradd` 脚本创建包含登录 shell `/bin/true` 和起始目录 *`/root-dir/./home-dir`* 的临时用户帐户。**
   有关更多信息，请参见 `useradd(1M)` 和《系统管理指南：基本管理》中的第 4 章 “管理用户帐户和组（概述）”。

注 – 在此过程中，**`/home/guests/./guest1`** 用作 `guest1` 用户的起始目录名称。

```
# /usr/sbin/useradd -m -c "Guest FTP" -d \
  /home/guests/./guest1 -s /bin/true guest1
```

2. **为临时帐户指定口令。**

3. **将 `guestuser` 项添加到 `ftpaccess` 文件中。**

```
guestuser guest1
```

注 – 也可以使用 ftpaccess 文件中的 guestgroup 功能指定临时用户。使用 ftpaccess 中的 guest-root 功能，临时用户的起始目录路径中就不需要 /./。

4 **确认该临时用户是否是 ftpaccess 文件中某个 class 的成员。有关详细信息，请参见** **第 533 页中的“如何定义 FTP 服务器类”**。

5 **使用 ftpconfig 脚本在 chroot 区域中创建需要的文件。**

```
/usr/sbin/ftpconfig -d /home/guests
```

6 **确认 /bin/true 是否列在 /etc/shells 文件中。请参见** **第 540 页中的“如何创建 /etc/shells 文件”**。

示例 28–6 设置临时 FTP 服务器

在此示例中，将在 /home/guests 目录中设置 FTP 区域。

```
# /usr/sbin/ftpconfig -d /home/guests
Updating directory /home/guests
```

▼ 如何设置匿名 FTP 用户

ftpconfig 脚本创建 anonymous 用户帐户并使用需要的文件填充起始目录。

有关更多信息，请参见 ftpconfig(1M)。

要使匿名用户可以访问 FTP 服务器，请按照以下说明操作：

1 **使用 ftpconfig 脚本创建匿名用户帐户。**

```
/usr/sbin/ftpconfig anonymous-ftp-directory
```

2 **确认是否在 ftpaccess 文件的某个 class 中指定了该匿名用户。**
有关详细信息，请参见第 533 页中的“如何定义 FTP 服务器类”。

示例 28–7 设置匿名 FTP 用户

在此示例中，将在 /home/ftp 目录中设置 FTP 区域。

```
# /usr/sbin/ftpconfig /home/ftp
Creating user ftp
Updating directory /home/ftp
```

▼ 如何创建 /etc/shells 文件

1 **成为超级用户或承担等效角色。**

角色包含授权和具有特权的命令。有关角色的更多信息，请参见《系统管理指南：安全性服务》中的“配置 RBAC（任务列表）”。

2 **创建 `/etc/shells` 文件。**

3 **编辑 `/etc/shells`。添加每个 shell 的全路径，一个路径占一行。**

示例 28–8 创建 /etc/shells 文件

以下是 `/etc/shells` 文件的一个示例，其中列出了 FTP 临时用户的 `/bin/true`：

```
/sbin/sh
/bin/csh
/bin/jsh
/bin/ksh
/bin/remsh
/bin/rksh
/bin/rsh
/bin/sh
/usr/bin/csh
/usr/bin/ksh
/usr/bin/bash
/usr/bin/tcsh
/usr/bin/zsh
/bin/true
```

定制消息文件

可以配置 FTP 服务器，使其将与特定事件有关的消息返回到 FTP 客户机。可以设置当用户登录到 FTP 服务器时显示欢迎消息。可以在用户更改目录时显示另外一条消息。

除了纯文本外，消息文件还可以包含一个或多个**魔饼** (magic cookie)。魔饼由 `%`（百分号）后接单个字符构成。如果在消息文本中嵌入 cookie，则当调用该消息文件时，将会在屏幕上显示与该 cookie 关联的信息。

例如，消息文本可能包含 cookie `%L`：

```
Welcome to %L!
```

显示消息时，魔饼 `%L` 将替换为由 `ftpaccess` 文件中的 `hostname` 语句定义的服务器的名称。有关支持的消息 cookie 的完整列表，请参见 `ftpaccess(4)`。

注 – 如果 ftpaccess 文件中未定义主机名，则将使用本地计算机的缺省主机名。

▼ 如何定制消息文件

1. **成为超级用户或承担等效角色。**
   角色包含授权和具有特权的命令。有关角色的更多信息，请参见《系统管理指南：安全性服务》中的“配置 RBAC（任务列表）”。

2. **根据需要，编辑消息文件以包括魔饼。**
   有关可以使用的 cookie 的列表，请参见 ftpaccess(4)。

示例 28–9 定制消息文件

以下是包括魔饼的消息文件的示例：

```
Welcome to %L -- local time is %T.

You are number %N out of a maximum of %M.
All transfers are logged.

If your FTP client crashes or hangs shortly after login
please try
using a dash (-) as the first character of your password.
This will
turn off the informational messages that may be confusing
your FTP
client.

Please send any comments to %E.
```

▼ 如何创建要发送到用户的消息

用户登录后，屏幕上将显示与系统相关或与应用程序相关的消息。ftpaccess 文件列出了触发关联的 message 语句的事件。

1. **成为超级用户或承担等效角色。**
   角色包含授权和具有特权的命令。有关角色的更多信息，请参见《系统管理指南：安全性服务》中的“配置 RBAC（任务列表）”。

2. **将以下项添加到 ftpaccess 文件中：**

```
message message-file [when [class ...]]
```

`message`	该关键字用于指定当用户登录或执行命令以更改工作目录时，将显示的消息文件。
message-file	要显示的消息文件的名称。
when	设置为 `login` 或 `cwd=`*dir* 的参数。请参见以下示例。
class	`class` 规范允许仅向特定类的成员显示消息。

示例 28–10 创建要发送到用户的消息

```
message    /etc/ftpd/Welcome    login    anon guest
message    .message    cwd=*
```

上面的示例说明，`anon` 或 `guest` 类的用户登录时将显示 `/etc/ftpd/Welcome` 文件。第二行说明，将对所有用户显示当前工作目录中的 `.message` 文件。

对于临时用户和匿名用户，将创建相对于 `chroot` 目录的消息文件。

▼ 如何配置 README 选项

首次访问目录时，可能会列出 `README` 文件。要配置 README 选项，请将以下项添加到 `ftpaccess` 文件中。

1 成为超级用户或承担等效角色。

角色包含授权和具有特权的命令。有关角色的更多信息，请参见《系统管理指南：安全性服务》中的“配置 RBAC（任务列表）”。

2 将以下项添加到 `ftpaccess` 文件中。

`readme` *message-file* `[when [`*class*`...]]`

`readme`	该关键字用于指定当用户登录或更改工作目录时，将检查的消息文件。如果该消息文件存在，则将通知用户，并指出文件被修改的日期。
message-file	要检查的消息文件的名称。
when	设置为 `login` 或 `cwd=`*dir* 的参数。请参见以下示例。
class	`class` 规范允许仅向特定类的成员显示消息。

注 – `greeting` 和 `banner` 关键字也可用于向用户发送消息。请参见 `ftpaccess(4)`。

示例 28–11 配置 README 选项

```
readme  README*     login
readme  README*     cwd=*
```

上面的示例说明，登录或更改目录时将列出与 README* 匹配的所有文件。以下是基于上面示例中使用的设置的登录样例。

```
% ftp earth
Connected to earth.
220 earth FTP server ready.
Name (earth:rimmer): ftp
331 Guest login ok, send your complete e-mail address as password.
Password:
230-
230-Welcome to earth -- local time is Thu Jul 15 16:13:24
1999.
230-
230-You are number 1 out of a maximum of 10.
230-All transfers are logged.
230-
230-If your FTP client crashes or hangs shortly after login
please try
230-using a dash (-) as the first character of your
password.  This will
230-turn off the informational messages that may be
confusing your FTP
230-client.
230-
230-Please send any comments to ftpadmin@earth.
230-
230 Guest login ok, access restrictions apply.
ftp> cd pub
250-Please read the file README
250-  it was last modified on Thu Jul 15 16:12:25 1999 - 0
days ago
250 CWD command successful.
ftp> get README /tmp/README
200 PORT command successful.
150 Opening ASCII mode data connection for README (0
bytes).
226 ASCII Transfer complete.
ftp> quit
221 Goodbye.
```

控制对 FTP 服务器上文件的访问

本节中的 FTP 服务器访问控制是发行版提供的标准文件和目录访问控制的补充。使用标准命令可限制能够访问、更改或上载文件的用户。请参见 chmod(1)、chown(1) 和 chgrp(1)。

▼ 如何控制文件访问命令

要使用 ftpaccess 中的权限功能指定哪种类型的用户允许执行哪些命令，请执行以下操作：

1 **成为超级用户或承担等效角色。**

角色包含授权和具有特权的命令。有关角色的更多信息，请参见《系统管理指南：安全性服务》中的“配置 RBAC（任务列表）”。

2 **将以下项添加到 ftpaccess 中：**

command yes|no *typelist*

command chmod、delete、overwrite、rename 或 umask 等命令

yes|no 允许或禁止用户发出命令

typelist 用逗号分隔的任何关键字（anonymous、guest 和 real）的列表

示例 28–12 控制文件访问命令

以下是对 FTP 服务器上的文件访问功能设置的权限示例。

```
chmod no anonymous, guest
delete    no anonymous
overwrite no anonymous
rename    no anonymous
umask     no guest, anonymous
```

上面的示例说明了以下内容：

- 不允许匿名用户删除、覆写或重命名文件。
- 禁止临时用户和匿名用户更改访问模式和重置 umask。

控制 FTP 服务器上的上载和下载

通过对 FTP 服务器上的目录设置权限，可以控制对 FTP 服务器执行的已启动的上载和下载操作。缺省情况下，不允许匿名用户上载。启用匿名上载时请务必小心。

▼ 如何控制对 FTP 服务器执行的上载操作

向 ftpaccess 文件中添加指令以指定上载权限和上载失败的错误消息。

1 成为超级用户或承担等效角色。

角色包含授权和具有特权的命令。有关角色的更多信息，请参见《系统管理指南：安全性服务》中的“配置 RBAC（任务列表）”。

2 将以下项添加到 ftpaccess 文件中。

要使用户可以上载文件，请添加以下项：

```
upload [absolute|relative] [class=<classname>]... [-] root-dir \
dirglob yes|no owner group mode [dirs|nodirs] [<d_mode>]

path-filter typelist mesg allowed-charset {disallowed regexp...}
```

`upload`	该关键字应用于起始目录（`chroot()` 的参数）为 *root-dir* 的用户。可以将 *root-dir* 指定为 "*" 以便与任何起始目录匹配。
`absolute|relative`	该参数指定将 *root-dir* 目录路径解释为绝对路径还是相对于当前 `chroot` 目录的路径。
`class`	该关键字用于指定任何数量的 `class=<classname>` 限制。如果指定该限制，则仅在当前用户为指定的某个类的成员时，上载子句才有效。
root-dir	匿名用户的用户根目录和起始目录。
dirglob	与目录名称匹配的模式。可以在任何位置或单独使用星号来表示任何目录。
`yes|no`	允许或禁止上载到 FTP 服务器的变量。
owner	上载到 `dirnames` 中的文件的属主。
group	与上载到 `dirnames` 中的文件关联的组。
mode	用于对已上载的文件指定访问权限的参数。缺省模式 `0440` 禁止匿名帐户读取已上载的文件。
`dirs|nodirs`	该关键字允许或禁止用户在 `dirnames` 中列出的目录中创建子目录。
`d_mode`	确定新创建目录的权限的可选模式。
`path-filter`	控制已上载文件的名称的关键字。
typelist	用逗号分隔的任何关键字（`anonymous`、`guest` 和 `real`）的列表。
mesg	与 `regexp` 条件匹配失败时将显示的消息文件。

allowed-charset {disallowed regexp...} 文件名称中允许或禁止使用的字母或数字。

示例 28–13 控制到 FTP 服务器的上载

```
upload /export/home/ftp /incoming yes ftpadm ftpadmin 0440 nodirs
path-filter anonymous /etc/ftpd/filename.msg ^[-A-Za-z0-9._]*$ ^[.-]
```

上面的示例说明了以下内容：

- 对 `/export/home/ftp` 使用 `chroot` 的 FTP 用户帐户可以上载到 `/incoming` 目录。已上载的文件为用户 `ftpadm` 和组 `ftpadmin` 拥有。使用 `nodirs` 关键字将模式设置为 `0440` 以阻止匿名用户创建子目录。
- 对于匿名用户，文件名可以是 A-Z、a-z、0-9、.（点）、-（破折号）或 _（下划线）组成的任意序列。文件名不能以 .（点）或 -（破折号）开始。如果文件名不能通过此过滤，则会显示消息 `/etc/ftpd/filename.msg`（如果 FTP 管理员已创建该消息文件）。此消息后接 FTP 服务器错误消息。

应对允许匿名上载到的目录的拥有权和权限进行严格控制。FTP 管理员应该是上载到 FTP 服务器的所有文件的属主。允许匿名用户上载文件时，需要创建 FTP 管理员。该目录应为权限设置为 `3773` 的用户 `ftpadm` 和组 `ftpadm` 拥有。

上载到 FTP 服务器的文件的访问模式应为 `0440`。`0440` 模式禁止匿名帐户读取已上载的文件。此限制可以防止服务器成为第三方文件分发的临时区域。

要使已上载的文件可以进行分发，FTP 管理员可以将这些文件移到公共目录中。

▼ 如何控制对 FTP 服务器执行的下载操作

1 成为超级用户或承担等效角色。

角色包含授权和具有特权的命令。有关角色的更多信息，请参见《系统管理指南：安全性服务》中的“配置 RBAC（任务列表）”。

2 将以下项添加到 `ftpaccess` 文件中以禁止用户检索文件。

`noretrieve [absolute|relative] [class=`*classname*`]... [-]` *filename ...*

`noretrieve`	用于拒绝检索特定文件的关键字
`absolute|relative`	该参数指定将 *root-dir* 目录路径解释为绝对路径还是相对于当前 `chroot` 目录的路径
`class`	该关键字用于指定要应用 `noretrieve` 限制的用户的 `class=<classname>`
filename	不允许用户检索的文件的名称

示例 28–14 控制对 FTP 服务器执行的下载操作

```
noretrieve /etc/passwd
```

上面的示例说明，将禁止所有用户检索 /etc/passwd 文件。

虚拟主机

虚拟主机允许 FTP 服务器支持同一计算机上的多个域。每个虚拟主机需要单独的逻辑接口和 IP 地址。

FTP 服务器支持两种类型的虚拟主机：**有限**和**完整**。使用有限虚拟主机时，将对所有虚拟主机使用相同的配置文件。使用完整虚拟主机时，将对每个虚拟主机使用单独的配置文件。

注 – 缺省情况下，不允许实际用户和临时用户登录到虚拟主机。您可以设置以下 ftpaccess 指令来忽略缺省值。

```
To allow access to specific users:
virtual address allow username
To deny access to anonymous users:
virtual address private username
```

有关详细信息，请参见 ftpaccess(4)。

▼ 如何启用有限虚拟主机

有限虚拟主机提供对虚拟 FTP 服务器的部分支持。可以通过指定虚拟根目录来启用对有限虚拟主机的支持。如果需要，也可以在 ftpaccess 文件中设置虚拟主机的以下参数：

- banner
- logfile
- email
- hostname

ftpaccess 文件中的所有指令在所有虚拟服务器中全局共享。

1 **成为超级用户或承担等效角色。**

角色包含授权和具有特权的命令。有关角色的更多信息，请参见《系统管理指南：安全性服务》中的“配置 RBAC（任务列表）”。

2 **将以下项添加到 ftpaccess 文件中。**

```
virtual address root|banner|logfile path
virtual address hostname|email string
```

`virtual`	用于启用虚拟服务器功能的关键字
address	虚拟服务器的 IP 地址
`root`	虚拟服务器的根目录
`banner`	连接到虚拟服务器时将显示的标题文件
`logfile`	虚拟服务器上的文件传送记录
path	用于指定虚拟服务器上的目录和文件位置的变量
`email`	消息文件和 HELP 命令中使用的电子邮件地址
`hostname`	问候消息或状态命令中显示的主机的名称
string	用于指定 `email` 或 `hostname` 参数的变量

注 – 虽然可以使用 `hostname` 作为虚拟服务器的 *address*，但强烈建议您使用 IPv4 地址。为了匹配 `hostname`，接收 FTP 连接时 DNS 必须可用。对于 IPv6 主机，请使用主机名而不要使用 IPv6 地址。

示例 28–15 在 ftpaccess 文件中启用有限虚拟主机

```
virtual 10.1.2.3 root    /var/ftp/virtual/ftp-serv
virtual 10.1.2.3 banner  /var/ftp/virtual/ftp-serv/banner.msg
virtual 10.1.2.3 logfile /var/log/ftp/virtual/ftp-serv/xferlog
```

上面的示例设置 `root` 目录、`banner` 和 `logfile` 在虚拟 FTP 服务器上的位置。

示例 28–16 在命令行中启用有限虚拟主机

带有 `-l` 选项的 ftpaddhost(1M) 脚本可用于配置有限虚拟主机。

在以下示例中，运行带有 `-l -b -x` 选项的 `ftpaddhost`，可以使用虚拟根 `/var/ftp/virtual/10.1.2.3` 下的测试标题和日志文件 `/var/ftp/virtual/10.1.2.3/xferlog` 配置有限虚拟主机。

```
# ftpaddhost -l -b -x /var/ftp/virtual/10.1.2.3/xferlog \
/var/ftp/virtual/10.1.2.3
```

▼ 如何启用完整虚拟主机

完整虚拟主机允许每个虚拟域使用单独的配置文件。要在 FTP 服务器上启用对虚拟主机的完整支持，可以创建或修改特定域的以下 FTP 配置文件：

- ftpaccess
- ftpusers
- ftpgroups
- ftphosts
- ftpconversions

有关详细信息，请参见 ftpaccess(4)、ftpusers(4)、ftpgroups(4)、ftphosts(4) 和 ftpconversions(4)。

注 – 如果单独版本的配置文件不可用，则可以使用 /etc/ftpd 目录中的主版本的文件。

---

1. **成为超级用户或承担等效角色。**

   角色包含授权和具有特权的命令。有关角色的更多信息，请参见《系统管理指南：安全性服务》中的“配置 RBAC（任务列表）”。

2. **将以下项添加到 /etc/ftpd/ftpservers 文件中。**

   address */config-file-dir*

address	虚拟服务器的 IP 地址
config-file-dir	包含对虚拟主机定制的配置文件的目录

   注 – 虽然可以使用 hostname 作为虚拟服务器的 *address*，但强烈建议您使用 IPv4 地址。为了匹配 hostname，接收 FTP 连接时 DNS 必须可用。对于 IPv6 主机，请使用主机名而不要使用 IPv6 地址。

   ---

3. **要为虚拟主机创建定制版本的 FTP 服务器配置文件，请将主版本的文件从 /etc/ftpd 复制到 /config-file-dir 目录中。**

   有关详细信息，请参见 ftpservers(4)。

示例 28–17 在 ftpservers 文件中启用完整虚拟主机

```
#
# FTP Server virtual hosting configuration file
#

10.1.2.3 /net/inet/virtual/somedomain/
10.1.2.4 /net/inet/virtual/anotherdomain/
```

上面的示例为虚拟服务器上的两个不同域指定 IP 地址。

示例 28–18 在命令行中启用完整虚拟主机

带有 -c 选项的 ftpaddhost(1M) 脚本可用于配置完整虚拟主机。

在以下示例中，运行带有 - c -b -x 选项的 ftpaddhost，可以使用虚拟根 /var/ftp/virtual/10.1.2.3 下的测试标题和日志文件 /var/ftp/virtual/10.1.2.3/xferlog 配置完整虚拟主机。

```
# ftpaddhost -c -b -x /var/ftp/virtual/10.1.2.3/xferlog \
/var/ftp/virtual/10.1.2.3
```

自动启动 FTP 服务器

可以通过以下三种方式之一启动 FTP 服务器：

- 作为由 inetd 启动的 nowait 服务器
- 作为在后台运行的独立服务器
- 通过 inittab 文件作为在前台运行的独立服务器

独立服务器始终具有可能最快的响应时间，适用于专门提供 FTP 服务的大型服务器。由于独立系统无需重新启动，所以独立服务器可以为专用服务器提供较低的连接延迟。即使在非高峰时间，独立服务器也始终处于运行状态以无限等待连接。

▼ 如何使用 SMF 启动 FTP 服务器

缺省情况下，SMF 服务配置为使用 nowait 模式启动 FTP 服务器。如果站点处理许多连接，还可以在单机模式下运行 FTP 服务器。有关其他命令行选项的信息，请参见 in.ftpd(1M) 手册页。

1 成为超级用户或承担等效角色。

角色包含授权和具有特权的命令。有关角色的更多信息，请参见《系统管理指南：安全性服务》中的“配置 RBAC（任务列表）”。

2 验证 FTP 服务器的 wait 属性。

报告 wait=FALSE 的行指示服务器在 nowait 模式下启动。

```
# inetadm -l network/ftp
SCOPE    NAME=VALUE
         name="ftp"
         endpoint_type="stream"
         proto="tcp6"
         isrpc=FALSE
         wait=FALSE
         exec="/usr/sbin/in.ftpd -a"
         user="root"
```

```
default  bind_addr=""
default  bind_fail_max=-1
default  bind_fail_interval=-1
default  max_con_rate=-1
default  max_copies=-1
default  con_rate_offline=-1
default  failrate_cnt=40
default  failrate_interval=60
default  inherit_env=TRUE
default  tcp_trace=FALSE
default  tcp_wrappers=FALSE
```

3 **启动 FTP 服务器。**

```
# svcadm enable network/ftp
```

▼ 如何在后台启动独立 FTP 服务器

1 **成为超级用户或承担等效角色。**

角色包含授权和具有特权的命令。有关角色的更多信息，请参见《系统管理指南：安全性服务》中的“配置 RBAC（任务列表）”。

2 **禁用 FTP 服务器。**

```
# svcadm disable network/ftp
```

3 **启动独立 FTP 服务器。**

```
# /usr/sbin/in.ftpd -a -S
```

将该行添加到 FTP 服务器启动脚本中。有关创建系统启动脚本的信息，请参见《系统管理指南：基本管理》中的“使用运行控制脚本”。

▼ 如何在前台启动独立 FTP 服务器

1 **成为超级用户或承担等效角色。**

角色包含授权和具有特权的命令。有关角色的更多信息，请参见《系统管理指南：安全性服务》中的“配置 RBAC（任务列表）”。

2 **禁用 FTP 服务器。**

```
# svcadm disable network/ftp
```

3 **向 inittab 文件中添加项以启动该服务。**

/etc/inittab 中的新项应与以下类似：

```
ftpd:3:respawn:/usr/sbin/in.ftpd -a -s
```

4 **通知 init 重新检查 /etc/inittab。**

此命令应启动 FTP 服务。

```
# init q
```

关闭 FTP 服务器

ftpshut(1M) 命令在特定时间关闭 FTP 服务器。

运行 ftpshut 时，将通过用于指定发生关闭的时间、拒绝新连接的时间和放弃现有连接的时间的命令行选项，生成一个文件。将基于此信息向用户发出服务器关闭通知。由 ftpshut 创建的文件的位置由 ftpaccess 文件中的 shutdown 指令指定。

▼ 如何关闭 FTP 服务器

按照以下过程中的步骤运行 ftpshut 并将 shutdown 指令添加到 ftpaccess 文件中。

1 **成为超级用户或承担等效角色。**

角色包含授权和具有特权的命令。有关角色的更多信息，请参见《系统管理指南：安全性服务》中的“配置 RBAC（任务列表）”。

2 **将以下项添加到 ftpaccess 文件中。**

```
shutdown path
```

shutdown	该关键字用于指定一个文件的 *path*，将定期检查该文件来查看 FTP 服务器是否已按预定关闭
path	由 ftpshut 命令创建的文件的位置

3 **运行 ftpshut 命令。**

```
ftpshut [ -V ] [ -l min] [ -d min] time [warning-message...]
```

ftpshut	该命令提供用于通知用户 FTP 服务器正在关闭的过程。
-V	一个选项，指定显示版权和版本信息，然后终止
-l	该标志用于调整拒绝 FTP 服务器的新连接的时间
-d	该标志用于调整断开 FTP 服务器的现有连接的时间。
time	由单词 now 指定的立即关机的关机时间，或使用两种格式之一（+ *number* 或 *HHMM*）指定的将来关机的关机时间
[warning-message...]	关机通知消息

4. **使用 ftprestart 命令可在关机之后重新启动 FTP 服务器。**
   有关详细信息，请参见 ftpshut(1M)、ftpaccess(4) 和 ftprestart(1M)。

调试 FTP 服务器

本节介绍调试 FTP 服务器的问题的一些方法。

▼ 如何在 syslogd 中检查 FTP 服务器消息

FTP 服务器将用于调试的消息写入为 /etc/syslog.conf 文件中的守护进程消息指定的位置。如果使用 FTP 服务器出现问题，请首先检查此文件中的这类消息。

FTP 服务器消息由工具守护进程和级别信息控制。要将来自 FTP 服务器的消息发送到 /var/adm/message 并让 syslogd 重新读取其配置文件，请按照以下说明操作：

1. **将如下所示的项添加到 /etc/syslog.conf 文件中。**

   ```
   daemon.info /var/adm/message
   ```

2. **向 syslogd 发出重新读取其配置的信号。**

   ```
   # svcadm refresh system/system-log
   ```

   此操作将导致来自 FTP 服务器的提示性消息被写入 /var/adm/messages 中。

▼ 如何使用 greeting text 验证 ftpaccess

要使用 greeting text 功能检查是否正确使用了 ftpaccess 文件，请执行以下操作：

1. **将以下指令添加到 ftpaccess 文件中。**

   ```
   greeting text message
   ```

2. **连接到 FTP 服务器。**

3. **如果显示消息失败，请执行以下操作：**

   a. **确认 ftpaccess 文件的位置是否正确。使用 strings(1) 命令获取 FTP 服务器二进制程序的文件位置。**

      ```
      # strings /usr/sbin/in.ftpd | grep "^/.*ftpaccess"
      ```

b. **检查 ftpservers 文件以查看是否已配置虚拟主机。**
有关详细信息，请参见 ftpaccess(4)、ftpservers(4)、strings(1)、syslog.conf(4) 和 pgrep(1)。

▼ 如何检查由 FTP 用户执行的命令

要查看由 FTP 用户执行的命令，请使用 ftpaccess 中的 log commands 日志记录功能。

1 **将以下指令添加到 ftpaccess 文件中以记录由 *typelist* 中指定的用户执行的各个命令。**

```
log commands typelist
```

2 **检查写入 /etc/syslog.conf 中指定的位置的消息。**

繁忙站点的配置帮助

以下列出了有关提高繁忙 FTP 站点性能的一些建议。

1. 通常支持许多同时连接的站点应在单机模式下运行 FTP 服务器，请参见第 550 页中的 “自动启动 FTP 服务器”。
2. 使用 vmstat 和其他系统实用程序监视 FTP 服务器的主机系统。如果系统资源不足，请对同时连接的数量设置限制，请参见第 534 页中的 “如何设置用户登录限制”。有关系统监视的更多信息，请参见《系统管理指南：高级管理》中的第 13 章 “监视系统性能（任务）”。
3. 如果强加连接限制，请考虑使用 ftpaccess 文件中的 limit-time 和 timeout idle 功能阻止用户过多占用连接。如果不强加连接限制，请针对 in.ftpd 指定 -Q 选项。
4. 如果不需要 /var/adm/wtmpx 中的 ftp 登录和注销记录，请针对 in.ftpd 指定 -W 选项。
5. 要降低 FTP 服务器的主机系统的负载，请使用 ftpaccess 文件中的 recvbuf 和 sendbuf 功能增加传送缓冲区大小。如果选择比较大的缓冲区大小，则可能需要使用 ftpaccess 文件中的 timeout data 功能延长数据活动的超时时间。
6. FTP 服务器将读取各种数据库中的内容，包括主机、口令、组和服务。较慢的查找可能会导致登录到 FTP 服务器出现严重延迟，首先在 nsswitch.conf 中配置 files 源可将查找时间降至最低。有关更多信息，请参见 nsswitch.conf(4) 手册页。
7. 缺省情况下，FTP 服务器尝试查找远程主机的名称，此过程可能很慢，导致登录出现显著延迟。ftpaccess 文件中的 rhostlookup 功能可用于停止此查找。但是，请注意，如果不查找远程主机的名称，使用 ftpaccess 文件中的其他功能和匹配 ftphosts 文件中的项时，将仅匹配远程主机的 IP 地址。远程主机的 IP 地址还将用在消息中及取代 %R 魔饼。有关更多详细信息，请参见 ftpaccess(4) 手册页中 rhostlookup 功能的说明。

8. 检索配额信息也可能导致登录到 FTP 服务器时出现显著延迟，因此如果利用配额魔饼，请仅使用 `ftpaccess` 文件中的 `quota-info` 功能。有关配额魔饼的列表，请参见 `ftpaccess(4)` 手册页。

◆ ◆ ◆ 第 29 章

29 访问远程系统（任务）

本章介绍登录到远程系统并管理其文件所需的全部任务。以下是本章中逐步说明的列表。

访问远程系统（任务列表）

本章介绍了用于登录远程系统并从中复制文件的任务，如下表中所述。

表 29–1 任务列表：访问远程系统

任务	说明	参考
登录到远程系统 (rlogin)	■ 删除 .rhosts 文件。 ■ 使用 rlogin 命令访问远程系统。	第 561 页中的“如何搜索并删除 .rhosts 文件” 第 562 页中的“如何查明远程系统是否在运行” 第 562 页中的“如何查找已登录到远程系统的用户” 第 563 页中的“如何登录到远程系统 (rlogin)” 第 564 页中的“如何从远程系统注销 (exit)”
登录到远程系统 (ftp)	■ 打开和关闭 ftp 连接。 ■ 将文件复制到远程系统，以及从远程系统复制文件。	第 565 页中的“如何打开与远程系统的 ftp 连接” 第 566 页中的“如何关闭与远程系统的 ftp 连接” 第 566 页中的“如何从远程系统复制文件 (ftp)” 第 568 页中的“如何将文件复制到远程系统 (ftp)”
使用 rcp 复制远程文件	使用 rcp 命令将文件复制到远程系统，以及从远程系统复制文件。	第 572 页中的“如何在本地系统和远程系统间复制文件 (rcp)”

登录到远程系统 (rlogin)

通过 rlogin 命令，可以登录到远程系统。登录之后，可以浏览远程文件系统并处理其内容（受授权限制）、复制文件或执行远程命令。

如果要登录到的系统位于远程域中，请务必在系统名称后附加域名。在以下示例中，SOLAR 是远程域的名称：

```
rlogin pluto.SOLAR
```

此外，也可以通过键入 Ctrl-D 组合键随时中断远程登录操作。

远程登录验证 (rlogin)

通过远程系统或网络环境，可以执行 rlogin 操作的验证（确定身份）。

这些验证形式的主要差别在于它们要求与您进行的交互类型以及建立验证的方式。如果远程系统尝试对您进行验证，则除非您设置 /etc/hosts.equiv 或 .rhosts 文件，否则将提示您输入口令。如果网络尝试对您进行验证，则不会要求您输入口令，因为网络已经知道您的身份。

当远程系统尝试对您进行验证时，将会依据其本地文件中的信息，尤其是在满足下列其中一个条件时：

- 您的系统名和用户名出现在远程系统的 /etc/hosts.equiv 文件中。
- 您的系统名和用户名出现在远程用户起始目录下的 .rhosts 文件中。

网络验证依据下列两种方法之一：

- 使用本地网络信息服务和自动挂载程序设置的“信任网络环境”。
- 远程系统的 /etc/nsswitch.conf 文件所指向的网络信息服务之一包含有关您的信息。

注 – 网络验证通常会取代系统验证。

/etc/hosts.equiv 文件

/etc/hosts.equiv 文件包含远程系统的可信主机列表，每行显示一台主机。如果用户尝试从此文件中列出的主机之一远程登录（使用 rlogin 命令），并且如果远程系统可以访问用户的口令项，则远程系统允许用户在不使用口令的情况下登录。

典型的 hosts.equiv 文件具有以下结构：

```
host1
host2 user_a
+@group1
-@group2
```

如果在 hosts.equiv 中创建一个简单的主机项（如上述 host1 项），则表示该主机是可信的，该计算机中的任何用户也是可信的。

如果还包含用户名（如示例中的第二项），则该主机只有在指定用户尝试访问时才可信。

前面带有加号 (+) 的组名表示，该网络组中的所有计算机均被视为可信。

前面带有减号 (-) 的组名表示，该网络组中的所有计算机均被视为不可信。

使用 /etc/hosts.equiv 文件时的安全风险

/etc/hosts.equiv 文件存在安全风险。如果将 /etc/hosts.equiv 文件保存在系统上，则应仅包含网络中的可信主机。该文件不应包含属于不同网络的任何主机或公共区域中的所有计算机。例如，不应包含终端室内的主机。

使用不受信任的主机可能产生严重的安全问题。请将 /etc/hosts.equiv 文件替换为正确配置的文件，或者完全删除该文件。

/etc/hosts.equiv 文件中的一个 + 行表示信任所有已知主机。

.rhosts 文件

.rhosts 文件是 /etc/hosts.equiv 文件的用户等效文件。此文件包含主机-用户组合列表，而不包含一般意义的主机。如果此文件中列出了主机-用户组合，则指定用户将被授予从指定主机登录而不必提供口令的权限。

请注意，.rhosts 文件必须驻留在用户起始目录的顶层。如果 .rhost 文件位于子目录中，则不会访问这些文件。

用户可在其起始目录中创建 .rhosts 文件。使用 .rhosts 文件是另外一种允许在不使用 /etc/hosts.equiv 文件的情况下，在不同系统的用户自己帐户之间进行可信访问的方法。

使用 .rhosts 文件时的安全风险

遗憾的是，.rhosts 文件存在严重的安全问题。虽然 /etc/hosts.equiv 文件受系统管理员的控制并且可以有效地管理，但任何用户都可以创建 .rhosts 文件，从而可以在系统管理员不知情时对其选择的任何人授予访问权限。

如果所有用户起始目录都在一台服务器上，并且只有某些人员才在该服务器上具有超级用户权限，则防止用户使用 .rhosts 文件的一种好方法就是以超级用户身份在用户起始目录中创建一个空文件。然后，将此文件的权限更改为 000，这样即使作为超级用户也很难更改它。此更改可有效地防止用户因不负责任地使用 .rhosts 文件而导致的系统安全风险。但是，如果用户能够更改指向其起始目录的有效路径，则此更改将不能解决任何问题。

管理 .rhosts 文件的唯一安全方法是完全禁用它们。有关详细说明，请参见第 561 页中的 “如何搜索并删除 .rhosts 文件”。作为系统管理员，可以经常检查系统以了解此策略的违规情况。此策略可能存在一种例外情况，即超级用户帐户可能需要使用 .rhosts 文件来执行网络备份和其他远程服务。

链接远程登录

如果系统配置正确，则可链接远程登录。例如，earth 中的用户可登录到 jupiter，并从该处决定登录到 pluto。

该用户也可以从 jupiter 注销然后直接登录到 pluto，但此类型的链接更加方便。

要链接远程登录而不必提供口令，必须正确设置 /etc/hosts.equiv 或 .rhosts 文件。

直接或间接远程登录

通过 rlogin 命令，可以直接或间接地登录到远程系统。

使用缺省用户名（即当前登录到本地系统的个人用户名）尝试直接远程登录。这是最常见的远程登录形式。

在远程登录操作时，可以通过提供不同的用户名来尝试间接远程登录。这是在从临时借用的工作站尝试登录的情况下采用的远程登录方式。例如，如果您在同事的办公室并且需要检查您的起始目录中的文件，则可以从同事的系统远程登录到您的系统。但是，在执行间接远程登录时应提供您自己的用户名。

下表概述了直接和间接登录与验证方法之间的相关性。

表 29–2 登录方法与验证方法 (rlogin) 之间的相关性

登录类型	用户名提供者	验证	口令
直接	系统	网络	无
		系统	必需
间接	用户	网络	无
		系统	必需

远程登录后发生的情况

登录到远程系统时，rlogin 命令将尝试查找您的起始目录。如果 rlogin 命令找不到您的起始目录，它会将您指定给远程系统的根 (/) 目录。例如：

```
Unable to find home directory, logging in with /
```

但是，如果 rlogin 命令找到您的起始目录，它将获取 .cshrc 和 .login 文件。因此，在远程登录后，提示符即成为标准登录提示符，并且当前目录与本地登录时的目录相同。

例如，如果常规提示符显示系统名和工作目录，并且在登录时工作目录是您的起始目录，则登录提示符与以下类似：

```
earth(/home/smith):
```

随后，当您登录到远程系统时，则不管您从哪个目录输入 rlogin 命令，都会显示类似的提示符并且工作目录是您的起始目录：

```
earth(/home/smith): rlogin pluto
.
.
.
pluto(/home/smith):
```

唯一的差别在于远程系统名称将替代提示符开头的本地系统名称。远程文件系统相当于您的起始目录。

实际上，如果将目录更改为 /home 然后运行 ls，则会显示以下内容：

```
earth(home/smith): cd ..
earth(/home): ls
smith  jones
```

▼ 如何搜索并删除 .rhosts 文件

1 **成为超级用户或承担等效角色。**

角色包含授权和具有特权的命令。有关角色的更多信息，请参见《系统管理指南：安全性服务》中的“配置 RBAC（任务列表）”。

2 **使用 find(1) 命令搜索并删除 .rhosts 文件。**

```
# find home-directories -name .rhosts -print -exec rm {} \;
```

home-directories 标识指向用户起始目录所在目录的路径。请注意，一次可输入多个路径来搜索多个起始目录。

`-name .rhosts` 标识文件名。

`-print` 输出当前路径名。

`-exec rm {} \;` 指示 find 命令将 rm 命令应用于通过匹配文件名标识的所有文件。

find 命令将从指定目录开始搜索名为 .rhosts 的所有文件。如果找到此类文件，find 将在屏幕上输出相应路径并删除该文件。

示例 29–1 搜索并删除 .rhosts 文件

以下示例搜索并删除 /export/home 目录的所有用户起始目录中的 .rhosts 文件。

```
# find /export/home -name .rhosts -print | xargs -i -t rm {} \;
```

如何查明远程系统是否在运行

使用 ping 命令查明远程系统是否在运行。

$ **ping** *system-name* | *ip-address*

system-name 远程系统的名称

ip-address 远程系统的 IP 地址

ping 命令将返回以下三条消息之一：

状态消息	说明
system-name is alive	可通过网络访问系统。
ping: unknown host *system-name*	系统名未知。
ping: no answer from *system-name*	系统已知，但当前未运行。

如果您对其执行 "ping" 操作的系统位于其他域中，则返回消息还可包含路由信息，不过您可以忽略该信息。

ping 命令的超时时间为 20 秒。实际上，如果该命令在 20 秒内未接收到响应，则会返回第三条消息。您可以通过键入 *time-out* 值（以秒为单位），强制 ping 等待更长（或更短）的时间：

$ **ping** *system-name* | *ip-address time-out*

有关更多信息，请参见 ping(1M)。

如何查找已登录到远程系统的用户

使用 rusers(1) 命令查找已登录到远程系统的用户。

$ **rusers** [**-l**] *remote-system-name*

rusers （无选项）显示系统名称，后跟当前已登录到系统的用户的名称，包括超级用户

`-l` 显示有关每个用户的其他信息：用户的登录窗口、登录时间和日期、已登录时间以及用户从中登录的远程系统的名称

示例 29–2 查找已登录到远程系统的用户

以下示例显示 `rusers` 的简短输出。

```
$ rusers pluto
pluto    smith  jones
```

在以下示例中，较长版本的 `rusers` 显示两个用户已登录到远程系统 `starbug`。第一个用户在 9 月 10 日从系统控制台登录并且已登录 137 小时 15 分钟。第二个用户在 9 月 14 日从远程系统 `mars` 登录。

```
$rusers -l starbug
root         starbug:console           Sep 10 16:13  137:15
rimmer       starbug:pts/0             Sep 14 14:37         (mars)
```

如何登录到远程系统 (rlogin)

使用 `rlogin(1)` 命令登录到远程系统。

`$ rlogin [-l` *user-name*`] system-name`

`rlogin` （无选项）使用当前用户名有效地**直接**登录到远程系统

`-l` *user-name* 使用您提供的用户名有效地**间接**登录到远程系统

如果网络尝试对您进行验证，将不会提示您输入口令。如果远程系统尝试对您进行验证，则会要求您提供口令。

如果操作成功，则 `rlogin` 命令会显示有关您最近登录该系统的简要信息、远程系统上运行的操作系统版本以及您的起始目录中是否有邮件等待查阅。

示例 29–3 登录到远程系统 (rlogin)

以下示例显示直接远程登录 `pluto` 的输出。网络已对用户进行了验证。

```
$ rlogin starbug
Last login: Mon Jul 12 09:28:39 from venus
Sun Microsystems Inc.   SunOS 5.8       February 2000
starbug:
```

以下示例显示间接远程登录 `pluto` 的输出，并且用户由远程系统进行验证。

```
$ rlogin -l smith pluto
password: user-password
Last login: Mon Jul 12 11:51:58 from venus
Sun Microsystems Inc.   SunOS 5.8       February 2000
```

示例 29–3 登录到远程系统 (rlogin) （续）

```
starbug:
```

如何从远程系统注销 (exit)

使用 exit(1) 命令从远程系统注销。

```
$ exit
```

示例 29–4 从远程系统注销 (exit)

此示例说明用户 smith 如何从系统 pluto 注销。

```
$ exit
pluto% logout
Connection closed.
earth%
```

登录到远程系统 (ftp)

ftp 命令打开 Internet 文件传输协议的用户接口。此用户接口又称为命令解释程序，它允许您登录到远程系统并对其文件系统执行各种操作。下表概述了主要操作。

与 rlogin 和 rcp 相比， ftp 的主要优点在于 ftp 不要求远程系统运行 UNIX。不过，远程系统却需要进行 TCP/IP 通信配置。但是，与 ftp 相比， rlogin 提供使用的文件处理命令更丰富。

远程登录验证 (ftp)

通过以下方法之一，可以建立 ftp 远程登录操作验证：

- 在远程系统的 /etc/passwd 文件或等效网络信息服务图或表中加入口令项
- 在远程系统上建立匿名 ftp 帐户

基本 ftp 命令

表 29–3 基本 ftp 命令

命令	说明
`ftp`	访问 `ftp` 命令解释程序。
`ftp` *remote-system*	建立与远程系统的 `ftp` 连接。有关说明，请参见第 565 页中的 “如何打开与远程系统的 ftp 连接”。
`open`	从命令解释程序登录到远程系统。
`close`	从远程系统注销并返回到命令解释程序。
`bye`	退出 `ftp` 命令解释程序。
`help`	列出所有 `ftp` 命令；或者如果提供了命令名称，则简要说明该命令所执行的操作。
`reset`	使命令-回复序列与远程 `ftp` 服务器再次同步。
`ls`	列出远程工作目录的内容。
`pwd`	显示远程工作目录的名称。
`cd`	更改远程工作目录。
`lcd`	更改本地工作目录。
`mkdir`	在远程系统上创建目录。
`rmdir`	删除远程系统上的目录。
`get, mget`	将远程工作目录中的某个文件（或多个文件）复制到本地工作目录。
`put, mput`	将本地工作目录中的某个文件（或多个文件）复制到远程工作目录。
`delete, mdelete`	删除远程工作目录中的某个文件（或多个文件）。

有关更多信息，请参见 `ftp(1)`。

▼ 如何打开与远程系统的 ftp 连接

1 **确保您具有 `ftp` 验证。**

您必须具有 `ftp` 验证，如第 564 页中的 “远程登录验证 (ftp)”中所述。

2 **使用 `ftp` 命令打开与远程系统的连接。**

```
$ ftp remote-system
```

如果连接成功，则会显示确认消息和提示。

3 **键入用户名。**

```
Name (remote-system:user-name): user-name
```

4 **如有提示，请键入口令。**

```
331 Password required for user-name:
Password: password
```

如果要访问的系统已建立了匿名 ftp 帐户，将会提示您输入电子邮件地址作为口令。如果 ftp 接口接受您的口令，则它会显示确认消息和 (ftp>) 提示符。

您现在可使用 ftp 接口提供的任何命令，包括 help。表 29–3 概述了主要命令。

示例 29–5 打开与远程系统的 ftp 连接

此 ftp 会话由远程系统 pluto 中的用户 smith 建立：

```
$ ftp pluto
Connected to pluto.
220 pluto FTP server ready.
Name (pluto:smith): smith
331 Password required for smith:
Password: password
230 User smith logged in.
ftp>
```

如何关闭与远程系统的 ftp 连接

使用 bye 命令关闭与远程系统的 ftp 连接。

```
ftp> bye
221-You have  transferred 0 bytes in 0 files.
221-Total traffic for this sessions was 172 bytes in 0 transfers.
221-Thanks you for using the FTP service on spdev.
221 Goodbye.
```

此时将显示再见消息，随后会出现常规 shell 提示符。

▼ 如何从远程系统复制文件 (ftp)

1 **转至要将远程系统中的文件复制到其中的本地系统目录。**

```
$ cd target-directory
```

2 **建立 ftp 连接。**

请参见第 565 页中的 “如何打开与远程系统的 ftp 连接”。

3 **转至源目录。**

```
ftp> cd source-directory
```

如果系统正在使用自动挂载程序，则远程系统用户的起始目录可能与 /home 中您的起始目录并行。

4 **确保您对源文件具有读取权限。**

```
ftp> ls -l
```

5 **将传送类型设置为 binary。**

```
ftp> binary
```

6 **要复制单个文件，请使用 get 命令。**

```
ftp> get filename
```

7 **要一次复制多个文件，请使用 mget 命令。**

```
ftp> mget filename [filename ...]
```

您可提供一系列单个文件名，也可使用通配字符。mget 命令会分别复制每个文件，并且每次都要求您进行确认。

8 **关闭 ftp 连接。**

```
ftp> bye
```

示例 29–6 从远程系统复制文件 (ftp)

在此示例中，用户 kryten 将打开与系统 pluto 的 ftp 连接，并使用 get 命令来复制 /tmp 目录中的单个文件。

```
$ cd $HOME
ftp pluto
Connected to pluto.
220 pluto FTP server (SunOS 5.8) ready.
Name (pluto:kryten): kryten
331 Password required for kryten.
Password: xxx
230 User kryten logged in.
ftp> cd /tmp
250 CWD command successful.
ftp> ls
200 PORT command successful.
150 ASCII data connection for /bin/ls (129.152.221.238,34344)
(0 bytes).
filea
files
ps_data
226 ASCII Transfer complete.
53 bytes received in 0.022 seconds (2.39 Kbytes/s)
ftp> get filea
200 PORT command successful.
150 ASCII data connection for filea (129.152.221.238,34331)
(0 bytes).
221 Goodbye.
```

在此示例中，同一用户 kryten 使用 mget 命令将 /tmp 目录中的一组文件复制到其起始目录。请注意，kryten 可以接受或拒绝该文件组中的个别文件。

```
$ ftp> cd /tmp
250 CWD command successful.
ftp> ls files
200 PORT command successful.
150 ASCII data connection for /bin/ls (129.152.221.238,34345)
(0 bytes).
fileb
filec
filed
remote: files
21 bytes received in 0.015 seconds (1.36 Kbytes/s)
ftp> cd files
250 CWD command successful.
ftp> mget file*
mget fileb? y
200 PORT command successful.
150 ASCII data connection for fileb (129.152.221.238,34347)
(0 bytes).
226 ASCII Transfer complete.
mget filec? y
200 PORT command successful.
150 ASCII data connection for filec (129.152.221.238,34348)
(0 bytes).
226 ASCII Transfer complete.
mget filed? y
200 PORT command successful.
150 ASCII data connection for filed (129.152.221.238,34351)
(0 bytes).
226 ASCII Transfer complete.200 PORT command successful.
ftp> bye
221 Goodbye.
```

▼ 如何将文件复制到远程系统 (ftp)

1. **转至本地系统上的源目录。**

   您键入 ftp 命令的目录是本地工作目录，也即此操作的源目录。

2. **建立 ftp 连接。**

   请参见第 565 页中的 “如何打开与远程系统的 ftp 连接”。

3. **转至目标目录。**

   ftp> **cd** *target-directory*

   请记住，如果系统正在使用自动挂载程序，则远程系统用户的起始目录可能与 /home 中您的起始目录并行。

4. **确保您对目标目录具有写入权限。**

   ftp> **ls -l** *target-directory*

5 **将传送类型设置为 binary。**

```
ftp> binary
```

6 **要复制单个文件，请使用 put 命令。**

```
ftp> put filename
```

7 **要一次复制多个文件，请使用 mput 命令。**

```
ftp> mput filename [filename ...]
```

您可提供一系列单个文件名，也可使用通配字符。mput 命令会分别复制每个文件，并且每次都要求您进行确认。

8 **要关闭 ftp 连接，请键入 bye。**

```
ftp> bye
```

示例 29–7 将文件复制到远程系统 (ftp)

在此示例中，用户 kryten 将打开与系统 pluto 的 ftp 连接，并使用 put 命令将其系统中的文件复制到系统 pluto 上的 /tmp 目录。

```
$ cd /tmp
ftp pluto
Connected to pluto.
220 pluto FTP server (SunOS 5.8) ready.
Name (pluto:kryten): kryten
331 Password required for kryten.
Password: xxx
230 User kryten logged in.
ftp> cd /tmp
250 CWD command successful.
ftp> put filef
200 PORT command successful.
150 ASCII data connection for filef (129.152.221.238,34356).
226 Transfer complete.
ftp> ls
200 PORT command successful.
150 ASCII data connection for /bin/ls (129.152.221.238,34357) (0 bytes).
filea
filef
files
ps_data
226 ASCII Transfer complete.
60 bytes received in 0.058 seconds (1.01 Kbytes/s)
ftp> bye
221 Goodbye.
```

在此示例中，同一用户 kryten 使用 mput 命令将其起始目录中的一组文件复制到 pluto 的 /tmp 目录。请注意，kryten 可以接受或拒绝该文件组中的个别文件。

```
$ cd $HOME/testdir
$ ls
test1   test2   test3
```

```
$ ftp pluto
Connected to pluto.
220 pluto FTP server (SunOS 5.8) ready.
Name (pluto:kryten): kryten
331 Password required for kryten.
Password: xxx
230 User kryten logged in.
ftp> cd /tmp
250 CWD command successful.
ftp> mput test*
mput test1? y
200 PORT command successful.
150 ASCII data connection for test1 (129.152.221.238,34365).
226 Transfer complete.
mput test2? y
200 PORT command successful.
150 ASCII data connection for test2 (129.152.221.238,34366).
226 Transfer complete.
mput test3? y
200 PORT command successful.
150 ASCII data connection for filef (129.152.221.238,34356).
226 Transfer complete.
ftp> bye
221 Goodbye.
```

使用 rcp 进行远程复制

rcp 命令可在本地系统与远程系统或两个远程系统之间复制文件或目录。您可从远程系统使用此命令（使用 rlogin 命令登录后），也可从本地系统（在未登录到远程系统的情况下）使用此命令。

使用 rcp，可执行以下远程复制操作：

- 将您系统中的文件或目录复制到远程系统
- 将远程系统中的文件或目录复制到本地系统
- 从本地系统在远程系统间复制文件或目录

如果正在运行自动挂载程序，则可以使用 cp 命令来执行这些远程操作。但是，cp 只能应用于自动挂载程序创建的虚拟文件系统以及与用户起始目录有关的操作。由于 rcp 可以执行同样的操作而没有这些约束，因此本节仅介绍如何使用 rcp 来完成这些任务。

复制操作的安全注意事项

要在系统间复制文件或目录，必须具有登录和复制文件的权限。

注意 – cp 和 rcp 命令都可以覆写文件而不发出任何警告。执行该命令之前，请确保文件名正确。

指定源和目标

借助 C shell 中的rcp 命令，可使用绝对或缩写路径名指定源（要复制的文件或目录）和目标（将文件或目录复制到的位置）。

	绝对路径名	缩写路径名
从本地系统	mars:/home/jones/myfile.txt	~jones/myfile.txt
在远程登录后	/home/jones/myfile.txt	~jones/myfile.txt

绝对路径名可标识特定系统上挂载的文件或目录。在前面的示例中，第一个绝对路径名标识 mars 系统上的文件 (MyFile.txt)。缩写路径名标识相对于用户起始目录的文件或目录，而不管起始目录的驻留位置如何。在前面的第一个示例中，缩写路径名标识的是同一个 MyFile.txt 文件，只不过使用 "~" 符号来表示 jones 起始目录：

```
~ = mars:/home/jones
```

第二行中的示例向用户演示远程登录后的绝对路径名和缩写路径名。缩写路径名的差别并不明显。不过，由于远程登录操作将 jones 起始目录挂载到本地系统上（相当于本地用户的起始目录），因此绝对路径名不再需要指明系统名 mars。有关远程登录操作如何挂载其他用户的起始目录的更多信息，请参见第 560 页中的 “远程登录后发生的情况”。

下表提供了 C shell 识别的绝对路径名和缩写路径名的样例。该样例使用的术语如下：

- 工作目录－从中输入 rcp 命令的目录。可以是远程目录，也可以是本地目录。
- 当前用户－用来输入 rcp 命令的用户名。

表 29–4 允许使用的目录和文件名语法

登录到	语法	说明
本地系统	.	本地工作目录
	path/filename	本地工作目录中的 *path* 和 *filename*
	~	当前用户的起始目录
	~/path/filename	当前用户起始目录下的 *path* 和 *filename*
	~user	*user* 的起始目录
	~user/path/filename	*user* 起始目录下的 *path* 和 *filename*

表 29–4 允许使用的目录和文件名语法 （续）

登录到	语法	说明
	remote-system:path/filename	远程工作目录中的 *path* 和 *filename*
远程系统	.	远程工作目录
	filename	远程工作目录中的 *filename*
	path/filename	远程工作目录中的 *path* 和 *filename*
	~	当前用户的起始目录
	~/path/filename	当前用户起始目录中的 *path* 和 *filename*
	~user	*user* 的起始目录
	~/user/path/filename	*user* 起始目录下的 *path* 和 *filename*
	local-system:path/filename	本地工作目录中的 *path* 和 *filename*

▼ 如何在本地系统和远程系统间复制文件 (rcp)

1 **确保您具有复制权限。**

您至少应在源系统上具有读取权限，在目标系统上具有写入权限。

2 **确定源和目标的位置。**

如果不知道源或目标的路径，可以先按第 563 页中的 “如何登录到远程系统 (rlogin)”中所述使用 `rlogin` 命令登录到远程系统。然后，浏览远程系统直到找到该位置。从而，可在未注销的情况下执行下一步。

3 **复制文件或目录。**

```
$ rcp [-r] source-file|directory  target-file|directory
```

`rcp` （无选项）将源中的单个文件复制到目标。

`-r` 将源中的目录复制到目标。

无论您登录到远程系统还是登录到本地系统，此语法都适用。只是文件或目录的路径名要进行相应更改，如表 29–4 及以下样例所示。

您可使用 "~" 和 "." 字符来指定本地文件或目录名称的路径部分。但是请注意，"~" 适用于当前用户而不适用于远程系统，"." 适用于所登录到的系统。有关这些符号的说明，请参见表 29–4。

示例 29–8 使用 rcp 将远程文件复制到本地系统

在此示例中，rcp 用于将远程系统 pluto 的 /home/jones 目录中的文件 letter.doc 复制到本地系统 earth 上的工作目录 (/home/smith)：

```
earth(/home/smith): rcp pluto:/home/jones/letter.doc .
```

在此情况下，rcp 操作是在未远程登录的情况下执行的。此处，命令行结尾的 "." 符号表示本地系统而非远程系统。

目标目录也是本地用户的起始目录，因此还可使用 "~" 符号来指定它。

示例 29–9 使用 rlogin 和 rcp 将远程文件复制到本地系统

在此示例中，rcp 操作在执行 rlogin 命令之后运行，以将远程系统中的文件复制到本地系统。尽管该操作的流程与前一示例的流程相同，但已针对远程登录更改了路径：

```
earth(/home/smith): rlogin pluto
.
.
.
pluto(/home/jones): rcp letter.doc ~
```

在此情况下，不适合在命令行结尾使用 "." 符号。由于远程登录，因此该符号仅表示远程系统－实质上指示 rcp 创建重复文件。但是，"~" 符号表示当前用户的起始目录，即使登录远程系统也是如此。

示例 29–10 使用 rcp 将本地文件复制到远程系统

在此示例中，rcp 用于将本地系统 earth 的起始目录 (/home/smith) 中的文件 notice.doc 复制到远程系统 pluto 的 /home/jones 目录：

```
earth(/home/smith): rcp notice.doc pluto:/home/jones
```

由于未提供远程文件名，因此文件 notice.doc 将以相同名称复制到 /home/jones 目录。

在此情况下，将重复执行前面示例中的 rcp 操作，但 rcp 是从本地系统上的另一工作目录 (/tmp) 输入的。请注意，"~" 符号用于表示当前用户的起始目录：

```
earth(/tmp): rcp ~/notice.doc pluto:/home/jones
```

示例 29–11 使用 rlogin 和 rcp 将本地文件复制到远程系统

在此示例中，rcp 操作在执行 rlogin 命令之后运行，以将本地文件复制到远程目录。尽管该操作的流程与先前示例的流程相同，但路径已经针对远程登录进行了更改。

```
earth(/home/smith): rlogin pluto
.
.
.
pluto(/home/jones): rcp ~/notice.doc .
```

在此情况下，"~" 符号可用来指示当前用户的起始目录，即使该目录位于本地系统上。由于用户已登录到远程系统，因此 "." 符号表示远程系统上的工作目录。以下是可执行相同操作的替换语法：

```
pluto(/home/jones): rcp earth:/home/smith/notice.doc /home/jones
```

第 7 部分

监视网络服务主题

本部分提供有关监视网络服务的逐步说明。

◆ ◆ ◆ 第 30 章

30 监视网络性能（任务）

本章介绍如何监视网络性能。以下是本章中的逐步说明列表。

监视网络性能

表 30–1 中介绍了可用于监视网络性能的命令。

表 30–1 网络监视命令

命令	说明
`ping`	查看网络中主机的响应。
`spray`	测试包大小的可靠性。此命令可指出网络将延迟包还是删除包。
`snoop`	从网络中捕获包，并跟踪每台客户机对每台服务器的调用。
`netstat`	显示网络状态，包括用于 TCP/IP 流量的接口的状态、IP 路由表以及用于 `UDP`、`TCP`、`ICMP` 和 `IGMP` 的按协议的统计信息。
`nfsstat`	显示可用于确定 NFS 问题的服务器和客户机统计信息的汇总。

如何检查网络中主机的响应

使用 `ping` 命令可检查网络中主机的响应。

```
$ ping hostname
```

如果您怀疑存在物理问题，可以使用 ping 确定网络中若干个主机的响应时间。如果某一主机的响应不是您期望的，则可对该主机进行研究。物理问题可能由以下原因引起：

- 电缆或连接器松动
- 接地错误
- 无终止
- 信号反射

有关此命令的更多信息，请参见 ping(1M)。

示例 30–1 检查网络中主机的响应

最简单版本 ping 可将单个包发送至网络中的主机。如果 ping 接收到正确的响应，该命令将输出消息 *host* is alive。

```
$ ping elvis
elvis is alive
```

使用 -s 选项时，ping 可以每秒向主机发送一个数据报。然后，该命令将输出每个响应以及往返所需的时间。以下是一个示例。

```
$ ping -s pluto
64 bytes from pluto (123.456.78.90): icmp_seq=0. time=3.82 ms
64 bytes from pluto (123.456.78.90): icmp_seq=5. time=0.947 ms
64 bytes from pluto (123.456.78.90): icmp_seq=6. time=0.855 ms
^C
----pluto PING Statistics----
3 packets transmitted, 3 packets received, 0% packet loss

round-trip (ms) min/avg/max/sttdev = 0.855/1.87/3.82/1.7
```

如何向网络中的主机发送包

用 spray 命令可以测试包大小的可靠性。

$ spray [-c *count* -d *interval* -l *packet-size*] *hostname*

-i *count* 要发送的包的数目。

-d *interval* 在两次发送包之间暂停的微秒数。如果不使用延迟，则可能耗尽缓冲区。

-l *packet-size* 包的大小。

hostname 要发送包的系统。

有关此命令的更多信息，请参见 spray(1M)。

示例 30–2 向网络中的主机发送包

以下示例将向主机 (`-c 100`) 发送 100 个包，包大小为 2048 字节 (`-l 2048`)。发送包时，每次成组传输之间的延迟时间为 20 微秒 (`-d 20`)。

```
$ spray -c 100 -d 20 -l 2048 pluto
sending 100 packets of length 2048 to pluto ...
no packets dropped by pluto
279 packets/sec, 573043 bytes/sec
```

如何从网络中捕获包

要从网络中捕获包并跟踪每台客户机对每台服务器的调用，请使用 `snoop`。此命令提供了精确的时间标记，因此可以快速隔离一些网络性能问题。有关更多信息，请参见 snoop(1M)。

```
# snoop
```

删除包可能是由缓冲区空间不足或 CPU 过载引起的。

如何检查网络状态

要显示网络状态信息，例如有关网络接口状态、路由表和各种协议的统计信息，请使用 `netstat` 命令。

```
$ netstat [-i] [-r] [-s]
```

`-i` 显示 TCP/IP 接口的状态

`-r` 显示 IP 路由表

`-s` 显示 `UDP`、`TCP`、`ICMP` 和 `IGMP` 协议的统计信息

有关更多信息，请参见 netstat(1M)。

示例－检查网络状态

以下示例显示 `netstat -i` 命令的输出，其中显示了用于 TCP/IP 流量的接口的状态。

```
$ netstat -i
Name  Mtu  Net/Dest    Address      Ipkts  Ierrs Opkts  Oerrs Collis Queue
lo0   8232 software    localhost     1280   0     1280     0       0    0
eri0   1500 loopback    venus      1628480   0   347070    16   39354    0
```

此输出显示了计算机在每个接口中传输和接收的包数。对于具有活动网络通信流量的机器而言，`Ipkts` 和 `Opkts` 都应持续增加。

将冲突计数 (Collis) 除以传出的包数 (Opkts)，以计算网络冲突率。在上一示例中，冲突率为 11%。如果网络范围内的冲突率大于 5% 至 10 %，则表示可能存在问题。

将输入错误数除以输入包的总数 (Ierrs/Ipkts)，以计算输入包的错误率。输出包的错误率等于输出错误数除以输出包的总数 (Oerrs/Opkts)。如果输入错误率较高（高于 0.25%），则主机可能在删除包。

以下示例显示 `netstat -s` 命令的输出，其中显示了 UDP、TCP、ICMP 和 IGMP 协议的按协议的统计信息。

```
UDP
    udpInDatagrams      =196543    udpInErrors         =     0
    udpOutDatagrams     =187820

TCP
    tcpRtoAlgorithm     =     4    tcpRtoMin           =   200
    tcpRtoMax           = 60000    tcpMaxConn          =    -1
    tcpActiveOpens      = 26952    tcpPassiveOpens     =   420
    tcpAttemptFails     =  1133    tcpEstabResets      =     9
    tcpCurrEstab        =    31    tcpOutSegs          =3957636
    tcpOutDataSegs      =2731494   tcpOutDataBytes     =1865269594
    tcpRetransSegs      = 36186    tcpRetransBytes     =3762520
    tcpOutAck           =1225849   tcpOutAckDelayed    =165044
    tcpOutUrg           =     7    tcpOutWinUpdate     =   315
    tcpOutWinProbe      =     0    tcpOutControl       = 56588
    tcpOutRsts          =   803    tcpOutFastRetrans   =   741
    tcpInSegs           =4587678
    tcpInAckSegs        =2087448   tcpInAckBytes       =1865292802
    tcpInDupAck         =109461    tcpInAckUnsent      =     0
    tcpInInorderSegs    =3877639   tcpInInorderBytes   =-598404107
    tcpInUnorderSegs    = 14756    tcpInUnorderBytes   =17985602
    tcpInDupSegs        =    34    tcpInDupBytes       = 32759
    tcpInPartDupSegs    =   212    tcpInPartDupBytes   =134800
    tcpInPastWinSegs    =     0    tcpInPastWinBytes   =     0
    tcpInWinProbe       =   456    tcpInWinUpdate      =     0
    tcpInClosed         =    99    tcpRttNoUpdate      =  6862
    tcpRttUpdate        =435097    tcpTimRetrans       = 15065
    tcpTimRetransDrop   =    67    tcpTimKeepalive     =   763
    tcpTimKeepaliveProbe=     1    tcpTimKeepaliveDrop =     0

IP
    ipForwarding        =     2    ipDefaultTTL        =   255
    ipInReceives        =11757234  ipInHdrErrors       =     0
    ipInAddrErrors      =     0    ipInCksumErrs       =     0
    ipForwDatagrams     =     0    ipForwProhibits     =     0
    ipInUnknownProtos   =     0    ipInDiscards        =     0
    ipInDelivers        =4784901   ipOutRequests       =4195180
    ipOutDiscards       =     0    ipOutNoRoutes       =     0
    ipReasmTimeout      =    60    ipReasmReqds        =  8723
    ipReasmOKs          =  7565    ipReasmFails        =  1158
    ipReasmDuplicates   =     7    ipReasmPartDups     =     0
    ipFragOKs           = 19938    ipFragFails         =     0
    ipFragCreates       =116953    ipRoutingDiscards   =     0
    tcpInErrs           =     0    udpNoPorts          =6426577
    udpInCksumErrs      =     0    udpInOverflows      =   473
```

```
    rawipInOverflows    =     0

ICMP
    icmpInMsgs          =490338    icmpInErrors        =     0
    icmpInCksumErrs     =     0    icmpInUnknowns      =     0
    icmpInDestUnreachs  =   618    icmpInTimeExcds     =   314
    icmpInParmProbs     =     0    icmpInSrcQuenchs    =     0
    icmpInRedirects     =   313    icmpInBadRedirects  =     5
    icmpInEchos         =   477    icmpInEchoReps      =    20
    icmpInTimestamps    =     0    icmpInTimestampReps =     0
    icmpInAddrMasks     =     0    icmpInAddrMaskReps  =     0
    icmpInFragNeeded    =     0    icmpOutMsgs         =   827
    icmpOutDrops        =   103    icmpOutErrors       =     0
    icmpOutDestUnreachs =    94    icmpOutTimeExcds    =   256
    icmpOutParmProbs    =     0    icmpOutSrcQuenchs   =     0
    icmpOutRedirects    =     0    icmpOutEchos        =     0
    icmpOutEchoReps     =   477    icmpOutTimestamps   =     0
    icmpOutTimestampReps=     0    icmpOutAddrMasks    =     0
    icmpOutAddrMaskReps =     0    icmpOutFragNeeded   =     0
    icmpInOverflows     =     0

IGMP:
        0 messages received
        0 messages received with too few bytes
        0 messages received with bad checksum
        0 membership queries received
        0 membership queries received with invalid field(s)
        0 membership reports received
        0 membership reports received with invalid field(s)
        0 membership reports received for groups to which we belong
        0 membership reports sent
```

以下示例显示 `netstat - r` 命令的输出，其中显示了 IP 路由表。

```
Routing Table:
  Destination        Gateway           Flags  Ref   Use    Interface
------------------- -------------------- ----- ----- ------ ---------
localhost           localhost             UH       0   2817  lo0
earth-bb            pluto                 U        3  14293  eri0
224.0.0.0           pluto                 U        3      0  eri0
default             mars-gate             UG       0  14142
```

下表介绍了 `netstat - r` 报告中的字段。

表 30–2 netstat - r 命令的输出

字段名		说明
Flags	U	路由向上。
	G	路由通过网关。
	H	路由到主机。
	D	路由是使用重定向动态创建的。

表 30–2 netstat - r 命令的输出 （续）

字段名	说明
Ref	显示共享相同链路层的当前路由数。
Use	表示发出的包的数目。
Interface	列出用于路由的网络接口。

如何显示 NFS 服务器和客户机统计信息

NFS 分布式文件服务使用远程过程调用 (remote procedure call, RPC) 工具来将本地命令转换为对远程主机的请求。远程过程调用是同步的。在服务器完成调用并返回结果之前，客户机应用程序将被阻塞或暂停。影响 NFS 性能的一个主要因素是重新传输率。

如果文件服务器不能对客户机的请求做出响应，则客户机在退出之前将按指定次数重新传输该请求。每次重新传输都会产生系统开销并增加网络通信流量。过多的重新传输会引起网络性能问题。如果重新传输率很高，可检查是否存在以下问题：

- 服务器过载导致完成请求过慢
- 某个以太网接口正在删除包
- 网络拥塞减慢了包传输

下表介绍了用于显示客户机和服务器统计信息的 nfsstat 选项。

表 30–3 用于显示客户机/服务器统计信息的命令

命令	显示
nfsstat -c	客户机统计信息
nfsstat -s	服务器统计信息
netstat -m	每个文件系统的网络统计信息

使用 nfsstat -c 可以显示客户机统计信息，使用 nfsstat -s 可以显示服务器统计信息。使用 netstat -m 可以显示每个文件系统的网络统计信息。有关更多信息，请参见 nfsstat(1M)。

示例－显示 NFS 服务器和客户机统计信息

以下示例显示客户机 pluto 的 RPC 和 NFS 数据。

```
$ nfsstat -c

Client rpc:
Connection oriented:
calls    badcalls  badxids  timeouts newcreds  badverfs   timers
```

```
1595799  1511      59       297      0         0          0
cantconn nomem     interrupts
1198      0         7
Connectionless:
calls    badcalls  retrans  badxids  timeouts  newcreds   badverfs
80785    3135      25029    193      9543      0          0
timers   nomem     cantsend
17399    0         0

Client nfs:
calls    badcalls  clgets   cltoomany
1640097  3112      1640097  0
Version 2: (46366 calls)
null     getattr   setattr  root     lookup     readlink  read
0 0%     6589 14%  2202 4%  0 0%     11506 24%  0 0%      7654 16%
wrcache  write     create   remove   rename     link      symlink
0 0%     13297 28% 1081 2%  0 0%     0 0%       0 0%      0 0%
mkdir    rmdir     readdir  statfs
24 0%    0 0%      906 1%   3107 6%
Version 3: (1585571 calls)
null    getattr    setattr  lookup     access     readlink  read
0 0%    508406 32% 10209 0% 263441 16% 400845 25% 3065 0%  117959 7%
write    create     mkdir    symlink    mknod    remove   rmdir
69201 4% 7615 0%    42 0%    16 0%      0 0%     7875 0%  51 0%
rename   link       readdir  readdir+   fsstat   fsinfo   pathconf
929 0%   597 0%     3986 0%  185145 11% 942 0%   300 0%   583 0%
commit
4364 0%

Client nfs_acl:
Version 2: (3105 calls)
null       getacl     setacl     getattr    access
0 0%       0 0%       0 0%       3105 100%  0 0%
Version 3: (5055 calls)
null       getacl     setacl
0 0%       5055 100%  0 0%
```

下表介绍了 `nfsstat -c` 命令的输出。

表 30–4 nfsstat -c命令的输出

字段	说明
`calls`	发送的调用总数。
`badcalls`	RPC 拒绝的调用总数。
`retrans`	重新传输的总数。对于此客户机，重新传输率小于 1%，或者 6888 次调用中有 10 次超时。这些重新传输可能是由临时故障引起的。更高的比率表明可能存在问题。
`badxid`	对一个 NFS 请求收到重复确认的次数。
`timeout`	超时的调用数。
`wait`	因没有可用的客户机句柄，调用必须等待的次数。
`newcred`	必须刷新验证信息的次数。

表 30–4 nfsstat -c 命令的输出 （续）

字段	说明
timers	超时值大于或等于为调用指定的超时值的次数。
readlink	使 read 成为符号链接的次数。如果此值很高（超过 10 %），则可能存在过多符号链接。

以下示例显示 nfsstat -m 命令的输出。

```
pluto$ nfsstat -m
/usr/man from pluto:/export/svr4/man
Flags: vers=2,proto=udp,auth=unix,hard,intr,dynamic,
        rsize=8192, wsize=8192,retrans=5
 Lookups: srtt=13 (32ms), dev=10 (50ms), cur=6 (120ms)
 All:     srtt=13 (32ms), dev=10 (50ms), cur=6 (120ms)
```

nfsstat -m 命令的此输出以毫秒显示，下表对其进行了介绍。

表 30–5 nfsstat -m 命令的输出

字段	说明
srtt	往返时间的平滑平均值
dev	平均偏差
cur	当前的“预期”响应时间

如果怀疑网络的硬件组件存在问题，则需要仔细检查电缆和连接器。

词汇表

asppp 随操作系统（从 Solaris 2.4 到 Solaris 8 发行版）提供的 PPP 版本。asppp 仅支持异步 PPP 通信。

asynchronous PPP（异步 PPP） 一种在异步串行线路上运行的 PPP 形式，异步串行线路一次只能传送一个字符数据。拨号链路是 PPP 最常见的配置形式，它采用异步 PPP 通信。

authentication（验证） 检验由远程用户或实体（如程序）通过网络提供的身份的动作。某些验证协议使您能生成由潜在用户的验证凭证组成的数据库。其他验证协议使用证书颁发机构针对验证目的生成的信任证书链。这些凭证可以在用户尝试与您通信或使用您站点的服务时对该用户进行验证。

broadcast（广播） 数据链路层过程，用于将包传输至子网上的每一台计算机。广播包通常不会路由至子网之外。

Callback Control Protocol, CBCP（回叫控制协议） 专有 Microsoft PPP 扩展，用于协商回叫会话。Solaris PPP 4.0 仅支持此协议的客户机（初始呼叫者）端。

channel service unit, CSU（通道服务单元） 一种同步电信设备，它为租用的电信线路提供本地接口并且充当该线路的终端。在美国，CSU 充当 T1 线路的终端并且提供 DS1 接口或 DSX 接口。在国际上，CSU 通常归电话公司提供商所有。

另请参见 CSU/DSU 和 data service unit, DSU（数据服务单元）。

CHAP 质询握手身份验证协议 (Challenge-Handshake Authentication Protocol, CHAP) 是一种验证协议，用于检验 PPP 链路上呼叫者的身份。CHAP 验证使用**质询**和**响应**的概念，其中接收呼叫的计算机会质询呼叫者以证明其身份。

另请参见 password authentication protocol, PAP（口令验证协议）。

CHAP Secret（CHAP 机密） ASCII 或二进制字符串，用于标识目的。PPP 链路上的两个对等点都可识别这两种字符串。CHAP 机密以明文格式存储在系统的 /etc/ppp/chap-secrets 文件中，但从不会通过 PPP 链路发送，即便使用加密格式也是如此。CHAP 协议检验呼叫者使用的 CHAP 机密散列，确定它是否与接收者的 /etc/ppp/chap-secrets 文件中呼叫者的 CHAP 机密散列项相匹配。

chat script（聊天脚本） 指示调制解调器如何在其自身与远程对等点之间建立通信链路的一些指令。PPP 和 UUCP 协议都使用聊天脚本来建立拨号链路和回拨呼叫。

Compression Control Protocol, CCP（压缩控制协议） PPP 的子协议，协商链路上数据压缩的使用。与头压缩不同，CCP 会压缩在链路上发送的包中的所有数据。

CSU/DSU 一个组合了 CSU 和 DSU 设备的同步电信设备，用于租用线路 PPP 链路中。CSU/DSU 将信号从一个对等点转换到租用线路上。大多数 CSU/DSU 不需要使用聊天脚本来建立链路。CSU/DSU 通常由租用线路提供商配置。

另请参见 channel service unit, CSU（通道服务单元）和 data service unit, DSU（数据服务单元）。

data service unit, DSU（数据服务单元） 在租用线路 PPP 链路上使用的同步电信设备。DSU 在电信线路上使用的数据帧格式之间进行转换，并且提供标准数据通信接口。

另请参见 channel service unit, CSU（通道服务单元）和 CSU/DSU。

dial-in server（拨入服务器） 一种对等点，它在接收来自拨出计算机的呼叫后，协商并建立拨号 PPP 链路的接收端。尽管“拨入服务器”是常用术语，但拨入服务器的作用与客户机/服务器模型并不一致。更确切地说，拨入服务器只是响应对设置拨号链路的请求的对等点。拨入服务器配置后，可接收来自任意数量的拨出计算机的呼叫。

dial-out machine（拨出计算机） 发出呼叫，要求建立拨号 PPP 链路的对等点。配置拨出计算机后，可呼叫任意数量的拨入服务器。通常，拨出计算机会先提供验证凭证，然后才能建立拨号链路。

dial-up PPP link（拨号 PPP 链路） 一种 PPP 连接，在电话线路（或类似通信介质，如 ISDN 提供的介质）的一端有一个对等点和一个调制解调器。术语“拨号”指的是本地调制解调器使用远程对等点的电话号码向该对等点拨号时，所使用的链路协商顺序。拨号链路是最常见最经济的 PPP 配置。

Directory Agent, DA（目录代理） 可选的 SLP 代理，用于存储和维护由服务代理 (service agent, SA) 发送的服务通告的高速缓存。DA 经过部署后可解析用户代理 (user agent, UA) 服务请求。DA 响应来自 SA 和 UA 的有关目录通告的活动请求。因此，SA 和 UA 会搜索关联的 DA 和**范围**。DA 会定期发送未经请求的通告，UA 和 SA 借助这些通告来搜索共享范围内的 DA。

expect-send（期待发送） 在 PPP 和 UUCP 聊天脚本中使用的一种脚本格式。此聊天脚本以**期待**来自远程对等点的文本或指令开头。接下来的一行包含从对等点接收到正确的 expect 字符串后，要从本地主机**发送**的响应。后续行会重复本地主机和对等点之间的 expect-send（期待发送）指令，直到建立通信所需的所有指令协商成功。

extended accounting（扩展记帐） 以任务或进程为单位记录资源占用情况的灵活方法。

Internet Protocol Control Protocol, IPCP（Internet 协议控制协议） PPP 的子协议，用于协商链路上对等点的 IP 地址。IPCP 还会协商链路的头压缩，并允许使用网络层协议。

Internet Protocol Version 6 Control Protocol, IPV6CP（Internet 协议版本 6 控制协议） 请参见 Internet Protocol Control Protocol, IPCP（Internet 协议控制协议）。

ISDN terminal adaptor, TA（ISDN 终端适配器）
一种信号适配设备，为基于 ISDN 网络的拨号 PPP 链路提供类似调制解调器的接口。可使用配置标准调制解调器时使用的相同 Solaris PPP 4.0 配置文件来配置 ISDN TA。

leased-line PPP link（租用线路 PPP 链路）
一种 PPP 连接，包括连接到从提供商处租用的同步网络介质的主机和 CSU/DSU。常见的租用线路介质有 OC3 和 T1。尽管租用线路链路易于管理，但它的成本要比拨号 PPP 链路高得多，所以使用得比较少。

legacy services（传统服务）
未启用 SLP 的联网服务。可创建代理注册以向 SLP 注册传统服务。然后，基于 SLP 的客户机便可搜索传统服务（请参见第 10 章，引入传统服务）。

link control protocol, LCP（链路控制协议）
PPP 的子协议，用于协商对等点之间的一组初始链路参数。LCP 的一部分功能是测试链路完整性，所以许多与链路有关的问题会显示为 LCP 故障。

link（链路）
在 PPP 中两个对等点之间协商并建立的通信连接。Solaris PPP 4.0 支持两种类型的链路：拨号链路和租用线路链路。

Microsoft CHAP (MS-CHAP)
用于 PPP 的 Microsoft 专有验证协议。Solaris PPP 4.0 支持在客户机和服务器模式下使用此协议的版本 1 和版本 2。

multicast（多播）
一个网络层过程，用于将数据报包发送到 IP 网络上的多台计算机。与广播路由一样，这些包不会被每台计算机处理。多播要求使用特殊路由协议来配置路由器。

password authentication protocol, PAP（口令验证协议）
一种验证协议，用于检验 PPP 链路上呼叫者的身份。PAP 使用通过链路传送的明文口令，这样就可以将口令存储在其中一台端点计算机上。例如，PAP 可使用接收呼叫的计算机上 UNIX `passwd` 数据库中的登录和口令项来检验呼叫者的身份。

另请参见 CHAP。

peer（对等点）
PPP 中位于 PPP 通信链路一端的单台计算机。PPP 通信链路由通过通信介质连接的两个对等点组成。可将多种类型的计算设备配置为对等点，如工作站、个人计算机、路由器或巨型机。

point-to-point protocol, PPP（点对点协议）
一种数据链路层协议，提供通过点对点介质传送数据报的标准方法。PPP 配置由称为**对等点**的两个端点计算机，以及对等点用于通信的电话线路或另一双向链路组成。两个对等点之间的硬件和软件连接将视为 *PPP* **链路**。

PPP 由许多子协议（包括 PAP、CHAP、LCP 和 CCP）组成。有大量 PPP 实现可用。

PPP over Ethernet, PPPoE（基于以太网的 PPP）
来自 RedBack Networks 的专有协议，它允许主机通过以太网链路运行 PPP 会话。PPPoE 通常与数字用户线路 (Digital Subscriber Line, DSL) 服务配合使用。

scope（范围）
按管理方式、拓扑方式或其他某种方式整理的 UA 和 SA 分组。可使用范围来修改对企业中各种服务的访问进行置备的方式。

service advertisements（服务通告）
由 SA 分发的用于说明服务的信息。服务通告由一个 URL 和一组用于说明服务的属性/值列表对组成。所有服务通告都具有生命周期。生命周期到期后，除非重新注册，否则服务通告不再有效。

Service Agent, SA（服务代理） 用于维护联网服务的服务通告的 SLP 代理。如果未提供任何 DA，则 SA 会答复来自 UA 的多播服务请求。如果提供了 DA，则 SA 会向支持其范围的 DA 注册服务和（可选的）注销服务。

service URL（服务 URL） 用于通告服务的网络位置的 URL。此 URL 包含服务类型、主机名或服务主机的网络地址。此 URL 还可能包含端口号和使用该服务所需的其他信息。

SLP daemon, slpd（SLP 守护进程） 在 SLP 的 Oracle Solaris 实现中充当 DA 或 SA 服务器的守护进程。主机上的服务进程会向 `slpd` 注册服务通告，而不是分别维护这些通告。每个进程都包含一个 SA 客户机库，当将守护进程配置为 SA 服务器时该客户机库将与 `slpd` 通信。SLP 守护进程会将所有注册和注销转发到 DA。此守护进程会将过期服务通告标记为超时，并通过执行主动和被动 DA 搜索来维护可用 DA 表。DA 信息将通过这样的机制提供给 UA 客户机。UA 客户机仅将主机上的 `slpd` 用于 DA 信息。可以选择将 `slpd` 配置为 DA。

synchronous PPP（同步 PPP） 一种在同步数字线路上运行的 PPP，同步数字线路以连续的原始位流的形式传送数据。租用线路 PPP 链路使用同步 PPP。

trusted callers（可信呼叫者） PPP 中拨入服务器对其授予访问权（通过在此服务器的 PAP 或 CHAP 机密数据库中加入对等点的安全凭证）的远程对等点。

User Agent, UA（用户代理） 代表用户应用程序运行的 SLP 代理。此代理会查询对应范围、目录代理和服务通告的身份。

索引

D

E

F

G

H

N

O

P

S

T

U

V

W

X

安

澳

八

版

包

关

管

广

规

和

后

换

回

生

实

时

使

示

守

输

数

有

与

域

只

指

质

中

主

注

转

状

桌

自

租