

SUSE Linux Enterprise Desktop

11 SP1

www.novell.com

21 de abril de 2010

Guia de Administração



Guia de Administração

Todo o conteúdo é copyright © 2006- 2010 Novell, Inc.

Informações legais

Este manual é protegido pelos direitos de propriedade intelectual da Novell. Ao reproduzir, duplicar ou distribuir este manual, você concorda explicitamente com os termos e as condições deste contrato de licença.

Este manual pode ser livremente reproduzido, duplicado e distribuído da forma como está ou como parte de um pacote bundle em formato eletrônico e/ou impresso, desde que, entretanto, as seguintes condições sejam atendidas:

O aviso de copyright e os nomes dos autores e colaboradores devem aparecer de forma clara e evidente em todas as cópias reproduzidas, duplicadas e distribuídas. Este manual, especificamente no formato impresso, é reproduzido e/ou distribuído apenas para uso não comercial. A autorização expressa da Novell, Inc. deve ser obtida antes de qualquer outro uso de um manual ou de parte dele.

Para conhecer as marcas registradas da Novell, consulte a Lista de marcas registradas e de marcas de serviço da Novell <http://www.novell.com/company/legal/trademarks/tmlist.html>. *Linux é marca registrada de Linus Torvalds. Todas as outras marcas registradas de terceiros pertencem aos seus respectivos proprietários. Um símbolo de marca registrada (®, ™ etc.) indica uma marca registrada da Novell; um asterisco (*) indica uma marca registrada de terceiros.

Todas as informações deste manual foram compiladas com a maior atenção possível aos detalhes. Entretanto, isso não garante uma precisão absoluta. A Novell, Inc., o SUSE LINUX Products GmbH, os autores ou os tradutores não deverão ser responsabilizados por possíveis erros ou consequências decorrentes.

Sumário

Sobre este guia	ix
Parte I Suporte e tarefas comuns	1
1 Atualização Online do YaST	3
1.1 Instalando patches manualmente com a interface Qt	4
1.2 Instalando patches manualmente com a interface GTK	6
1.3 Atualização online automática	8
2 Reunindo informações do sistema para suporte	9
2.1 Visão geral do Link do Suporte Novell	9
2.2 Usando o supportconfig	10
2.3 Enviando informações à Novell	12
2.4 Para obter mais informações	14
3 YaST em modo de texto	15
3.1 Navegação em módulos	16
3.2 Restrição de combinações de tecla	18
3.3 Opções de linha de comando do YaST	18
4 Configuração do GNOME para administradores	21
4.1 O sistema GConf	21
4.2 Personalizado o menu principal, o painel e o browser de aplicativos	24
4.3 Iniciando aplicativos automaticamente	25
4.4 Montando automaticamente e gerenciando dispositivos de mídia	25
4.5 Mudando os aplicativos preferenciais	25

4.6	Gerenciando perfis com o Sabayon	26
4.7	Adicionando gabaritos de documentos	30
4.8	Recursos de bloqueio da área de trabalho	31
4.9	Para obter mais informações	31
5	Gerenciando software com ferramentas de linha de comando	33
5.1	Usando o zypper	33
5.2	RPM — o gerenciador de pacotes	43
6	Acessando áreas de trabalho remotas com o Nomad	55
6.1	Pré-requisitos do Nomad	56
6.2	Instalação e configuração	57
6.3	Usando o Nomad	59
6.4	Solução de problemas	60
6.5	Para obter mais informações	61
7	Bash e scripts Bash	63
7.1	O que é “o shell”?	63
7.2	Gravando scripts shell	70
7.3	Redirecionando eventos de comando	71
7.4	Usando aliases	72
7.5	Usando variáveis no Bash	72
7.6	Agrupando e combinando comandos	75
7.7	Trabalhando com construções de fluxo comuns	76
7.8	Para obter mais informações	77
Parte II	Sistema	79
8	Aplicativos de 32 bits e 64 bits em um ambiente de sistema de 64 bits	81
8.1	Suporte ao tempo de execução	82
8.2	Desenvolvimento de software	83
8.3	Compilação de software em plataformas biarch	83
8.4	Especificações do kernel	84
9	Inicializando e configurando um sistema Linux	87
9.1	Processo de boot do Linux	87
9.2	O processo init	91
9.3	Configuração do sistema via /etc/sysconfig	101

10	O carregador de boot GRUB	105
10.1	Inicializando com o GRUB	106
10.2	Configurando o carregador de boot com o YaST	117
10.3	Desinstalando a controladora de boot do Linux	124
10.4	Criando CDs de boot	124
10.5	A tela gráfica do SUSE	125
10.6	Solução de problemas	126
10.7	Para obter mais informações	128
11	Recursos especiais do sistema	129
11.1	Informações sobre pacotes de software especiais	129
11.2	Consoles virtuais	137
11.3	Mapeamento de teclado	137
11.4	Configurações de idioma e específicas de país	138
12	Operação da impressora	143
12.1	Fluxo de trabalho do sistema de impressão	145
12.2	Métodos e protocolos de conexão de impressoras	146
12.3	Instalando o software	146
12.4	Impressoras de rede	147
12.5	Imprimindo pela linha de comando	150
12.6	Recursos especiais do SUSE Linux Enterprise Desktop	150
12.7	Solução de problemas	153
13	Gerenciamento de dispositivo de kernel dinâmico com udev	163
13.1	O diretório /dev	163
13.2	udev e uevents de kernel	164
13.3	Drivers, módulos de kernel e dispositivos	164
13.4	Inicialização e configuração do dispositivo inicial	165
13.5	Monitorando o daemon do udev em execução	166
13.6	Influenciando o tratamento de evento de dispositivo de kernel com regras do udev	167
13.7	Nomeação de dispositivo persistente	175
13.8	Arquivos usados pelo udev	176
13.9	Para obter mais informações	177
14	O sistema X Window	179
14.1	Configurando manualmente o X Window System	179
14.2	Instalando e configurando fontes	186
14.3	Para obter mais informações	192

15	Acessando sistemas de arquivos com o FUSE	195
15.1	Configurando o FUSE	195
15.2	Plug-ins disponíveis do FUSE	195
15.3	Para obter mais informações	196
Parte III	Computadores móveis	197
16	Computação móvel com o Linux	199
16.1	Laptops	199
16.2	Hardware móvel	208
16.3	Telefones celulares e PDAs	209
16.4	Para obter mais informações	209
17	Rede local sem fio	211
17.1	Padrões de WLAN	211
17.2	Modos de funcionamento	212
17.3	Autenticação	213
17.4	Criptografia	215
17.5	Configuração com o YaST	216
17.6	Utilitários	221
17.7	Dicas sobre a configuração de uma WLAN	221
17.8	Solução de problemas	222
17.9	Para obter mais informações	224
18	Gerenciamento de energia	225
18.1	Funções de economia de energia	225
18.2	ACPI	226
18.3	Descanso do disco rígido	231
18.4	Solução de problemas	233
18.5	Para obter mais informações	234
19	Usando Tablet PCs	235
19.1	Instalando pacotes do Tablet PC	236
19.2	Configurando seu dispositivo tablet	237
19.3	Usando o teclado virtual	238
19.4	Girando a tela	239
19.5	Usando o reconhecimento de gestos	240
19.6	Fazendo anotações e criando esboços com a caneta	242
19.7	Solução de problemas	244
19.8	Para obter mais informações	246

Parte IV Serviços **247**

20 Rede básica **249**

20.1	Roteamento e endereços IP	252
20.2	IPv6 — a Internet de última geração	256
20.3	Resolução de nomes	265
20.4	Configurando uma conexão de rede com o YaST	267
20.5	NetworkManager	289
20.6	Configurando uma conexão de rede manualmente	291
20.7	smpppd como Assistente de Discagem	307

21 Serviços SLP na rede **311**

21.1	Instalação	311
21.2	Ativando o SLP	312
21.3	Front ends de SLP no SUSE Linux Enterprise Desktop	312
21.4	Fornecendo serviços por SLP	313
21.5	Para obter mais informações	314

22 Sincronização de horário com NTP **315**

22.1	Configurando um cliente NTP com o YaST	316
22.2	Configurando manualmente o ntp na rede	319
22.3	Sincronização de horário dinâmica em tempo de execução	320
22.4	Configurando um relógio de referência local	320

23 Usando o NetworkManager **323**

23.1	Casos de uso do NetworkManager	323
23.2	Habilitando o NetworkManager	324
23.3	Configurando conexões de rede	325
23.4	Usando o KNetworkManager	328
23.5	Usando o applet NetworkManager do GNOME	333
23.6	NetworkManager e VPN	336
23.7	NetworkManager e segurança	337
23.8	Perguntas mais frequentes	339
23.9	Solução de problemas	341
23.10	Para obter mais informações	342

24 Samba **343**

24.1	Terminologia	343
24.2	Configurando um servidor Samba	345
24.3	Configurando clientes	345

24.4	Samba como servidor de login	345
24.5	Para obter mais informações	347
25	Compartilhando sistemas de arquivos com o NFS	349
25.1	Instalando o software necessário	349
25.2	Importando sistemas de arquivos com o YaST	349
25.3	Importando sistemas de arquivos manualmente	351
25.4	NFS com Kerberos	352
25.5	Para obter mais informações	353
26	Sincronização de arquivos	355
26.1	Software de sincronização de dados disponível	355
26.2	Determinando fatores para selecionar um programa	357
26.3	Introdução ao CVS	360
26.4	Introdução ao rsync	363
26.5	Para obter mais informações	365
Parte V	Solução de problemas	367
27	Ajuda e documentação	369
27.1	Diretório da documentação	370
27.2	Páginas de manual	372
27.3	Páginas de informações	373
28	Problemas comuns e suas soluções	375
28.1	Localizando e reunindo informações	375
28.2	Problemas de instalação	379
28.3	Problemas de inicialização	390
28.4	Problemas de login	393
28.5	Problemas de rede	401
28.6	Problemas de dados	406

Sobre este guia

Este guia é destinado a administradores profissionais de rede e sistema durante a operação do SUSE® Linux Enterprise. Desta forma, ele se compromete exclusivamente em garantir que o SUSE Linux Enterprise esteja configurado adequadamente e que os serviços requisitados na rede estejam disponíveis para permitir que ele funcione como instalado inicialmente. Este guia não abrange o processo que garante que o SUSE Linux Enterprise ofereça compatibilidade adequada ao software aplicativo da empresa ou que sua funcionalidade principal atenda a esses requisitos. Ele assume que foi feita uma auditoria completa dos requisitos e que foi solicitada a instalação ou uma instalação de teste, visando tal auditoria.

Este guia contém o seguinte:

Administração

O SUSE Linux Enterprise oferece uma ampla variedade de ferramentas para personalizar diversos aspectos do sistema. Esta parte apresenta algumas delas.

Sistema

Aprenda mais sobre o sistema operacional subjacente estudando esta parte. O SUSE Linux Enterprise suporta várias arquiteturas de hardware e você pode usar isso para adaptar seus próprios aplicativos para serem executados no SUSE Linux Enterprise. As informações do carregador de boot e do procedimento de boot ajudam você a compreender como o sistema Linux funciona e como os seus próprios aplicativos e scripts personalizados podem se fundir a ele.

Computação móvel

Laptops e a comunicação entre dispositivos móveis como PDAs ou telefones celulares e o SUSE Linux Enterprise requerem atenção especial. Cuide da conservação da energia e da integração de diferentes dispositivos a um ambiente de rede que está sofrendo mudanças. Tenha contato também com tecnologias de segundo plano que fornecem a funcionalidade necessária.

Serviços

O SUSE Linux Enterprise foi projetado para ser um sistema operacional de rede. O SUSE® Linux Enterprise Desktop inclui suporte de cliente para muitos serviços de rede. Ele se integra bem em ambientes heterogêneos, inclusive clientes e servidores MS Windows.

Muitos capítulos neste manual contêm links para recursos adicionais de documentação. Isso inclui documentação adicional disponível no sistema assim como documentação disponível na Internet.

Para obter uma visão geral da documentação disponível para o seu produto e as atualizações mais recentes da documentação, consulte <http://www.novell.com/documentation>.

1 Documentação disponível

Fornecemos versões em HTML e PDF de nossos livros em idiomas diferentes. Os manuais a seguir para usuários e administradores estão disponíveis neste produto:

KDE User Guide (↑*KDE User Guide*)

Apresenta a área de trabalho KDE do SUSE Linux Enterprise Desktop. Fornece orientações a você durante o uso e a configuração da área de trabalho, além de ajudá-lo a executar tarefas principais. Ele se destina principalmente a usuários que desejam usar de forma eficiente a área de trabalho KDE como a área de trabalho padrão.

Guia do Usuário do GNOME (↑*Guia do Usuário do GNOME*)

Apresenta a área de trabalho GNOME do SUSE Linux Enterprise Desktop. Fornece orientações a você durante o uso e a configuração da área de trabalho, além de ajudá-lo a executar tarefas principais. Este manual é destinado principalmente a usuários finais que desejam usar de forma eficiente a área de trabalho GNOME como sua área de trabalho padrão.

Guia de Aplicativos (↑*Guia de Aplicativos*)

Saiba como usar e configurar os aplicativos principais da área de trabalho no SUSE Linux Enterprise Desktop. Este manual apresenta os browsers e os clientes de e-mail, bem como aplicativos de escritório e ferramentas de colaboração. Também aborda aplicativos gráficos e de multimídia.

Guia de Implantação (↑*Guia de Implantação*)

Mostra como instalar sistemas únicos ou múltiplos e como explorar os recursos inerentes ao produto para uma infra-estrutura de desenvolvimento. Escolha uma das várias abordagens que variam desde uma instalação local ou um servidor de instalação de rede até uma implantação em massa usando uma técnica de instalação remota controlada, automatizada e altamente personalizada.

Guia de Administração (p 1)

Abrange tarefas de administração do sistema, como manutenção, monitoramento e personalização de um sistema instalado inicialmente.

Security Guide (Guia de Segurança) (↑Security Guide (Guia de Segurança))

Introduz conceitos básicos de segurança do sistema, incluindo aspectos de segurança locais e de rede. Mostra como usar o software de segurança inerente do produto, como o Novell AppArmor (que permite que você especifique quais arquivos cada programa poderá ler, gravar e executar) ou o sistema de auditoria que coleta informações de forma confiável sobre qualquer evento relevante para a segurança.

System Analysis and Tuning Guide (Guia de Análise do Sistema e Ajuste) (↑System Analysis and Tuning Guide (Guia de Análise do Sistema e Ajuste))

Um guia do administrador para detecção de problema, resolução e otimização. Saiba como inspecionar e otimizar seu sistema através de ferramentas de monitoramento e como gerenciar recursos com eficiência. Também contém uma visão geral dos problemas comuns e soluções e da ajuda adicional e recursos de documentação.

Virtualization with Xen (Virtualização com Xen) (↑Virtualization with Xen (Virtualização com Xen))

Oferece uma introdução à tecnologia de virtualização de seu produto. Ele apresenta uma visão geral sobre os diversos campos dos tipos de aplicativo e de instalação de cada uma das plataformas suportadas pelo SUSE Linux Enterprise Server, assim como uma breve descrição do procedimento de instalação.

Além de manuais abrangentes, há vários guias de inicialização rápida disponíveis:

KDE Quick Start (↑KDE Quick Start)

Apresenta uma rápida introdução da área de trabalho KDE e de alguns dos principais aplicativos executados nela.

GNOME Quick Start (↑GNOME Quick Start)

Apresenta uma rápida introdução da área de trabalho GNOME e de alguns dos principais aplicativos executados nela.

OpenOffice.org Quick Start

Apresenta uma rápida introdução à suíte do OpenOffice.org e seus módulos para escrever textos, manipular planilhas ou criar gráficos e apresentações.

Inicialização rápida da instalação (↑Inicialização rápida da instalação)

Lista os requisitos de sistema e o orienta passo a passo através da instalação do SUSE Linux Enterprise Desktop de um DVD ou de uma imagem ISO.

Linux Audit Quick Start (Inicialização Rápida do Linux Audit)

Fornece uma breve visão geral de como habilitar e configurar o sistema de auditoria e como executar tarefas principais, como configurar regras de auditoria, gerar relatórios e analisar os arquivos de registro.

Novell AppArmor Quick Start (Inicialização Rápida do Novell AppArmor)

Ajuda você a compreender os principais conceitos do Novell® AppArmor.

Encontre as versões HTML de grande parte dos manuais dos produtos no sistema instalado em `/usr/share/doc/manual` ou nos centros de Ajuda do seu desktop. Obtenha as atualizações mais atuais da documentação em <http://www.novell.com/documentation> de onde você poderá fazer download das versões HTML ou PDF dos manuais referentes ao seu produto.

2 Comentários

Vários canais de comentário estão disponíveis:

Bugs e solicitações de aprimoramento

Para conhecer os serviços e as opções de suporte disponíveis para o seu produto, consulte <http://www.novell.com/services/>.

Para reportar bugs de um componente do produto, use <http://support.novell.com/additional/bugreport.html>.

Envie solicitações de aprimoramento em <https://secure-www.novell.com/rms/rmsTool?action=ReqActions.viewAddPage&return=www>.

Comentários do usuário

Gostaríamos de receber seus comentários e suas sugestões sobre este manual e sobre as outras documentações incluídas no produto. Use o recurso Comentários do Usuário, localizado na parte inferior de cada página da documentação online,

ou acesse <http://www.novell.com/documentation/feedback.html> e digite seus comentários.

3 Convenções da documentação

As seguintes convenções tipográficas são usadas neste manual:

- `/etc/passwd`: nomes de diretório e nomes de arquivo
- *marcador*: substitua *marcador* pelo valor real
- `PATH`: a variável do ambiente `PATH`
- `ls, --help`: comandos, opções e parâmetros
- `user`: usuários ou grupos
- `Alt, Alt + F1`: uma tecla ou uma combinação de teclas a serem pressionadas; as teclas são mostradas em letras maiúsculas como aparecem no teclado
- *Arquivo, Arquivo > Gravar Como*: itens de menu, botões
- *Pingüins Dançando* (Capítulo *Pingüins*, ↑Outro Manual): referência a outro capítulo em outro manual.

Parte I. Suporte e tarefas comuns

Atualização Online do YaST

A Novell oferece um fluxo contínuo de atualizações de segurança de software para o seu produto. Por padrão, o applet de atualização é usado para manter o seu sistema atualizado. Consulte a Seção “Keeping the System Up-to-date” (Capítulo 6, *Installing or Removing Software*, ↑ *Guia de Implantação*) para obter mais informações sobre o applet de atualização. Este capítulo trata da ferramenta alternativa para atualizar pacotes de software: Atualização Online do YaST.

Os patches atuais para o SUSE® Linux Enterprise Desktop estão disponíveis em um repositório de software de atualização. Se você registrou seu produto durante a instalação, já há um repositório de atualização configurado. Se você não registrou o SUSE Linux Enterprise Desktop, pode fazê-lo executando *Software > Configuração de Atualização Online* no YaST e iniciando *Avançado > Registrar-se para obter suporte e repositório de atualizações*. Alternativamente, você pode adicionar manualmente um repositório de atualização de uma fonte confiável. Para adicionar ou remover repositórios, inicie o Gerenciador de Repositórios com *Software > Repositórios de Software* no YaST. Saiba mais sobre o Gerenciador de Repositórios na Seção “Managing Software Repositories and Services” (Capítulo 6, *Installing or Removing Software*, ↑ *Guia de Implantação*).

NOTA: erro ao acessar o catálogo de atualização

Se você não conseguir acessar o catálogo de atualização, pode ser que a assinatura tenha expirado. Normalmente, o SUSE Linux Enterprise Desktop é fornecido com uma assinatura de um ou três anos, durante a qual você terá acesso ao catálogo de atualização. Esse acesso será negado quando a assinatura terminar.

No caso de uma negação de acesso ao catálogo de atualização, você verá uma mensagem de aviso com uma recomendação para visitar o Novell Customer Center e verificar sua assinatura. O Novell Customer Center está disponível em <http://www.novell.com/center/>.

fornece atualizações com diferentes níveis de relevância. As atualizações *Security* corrigem riscos graves à segurança e devem definitivamente ser instaladas. As atualizações *Recommended* corrigem problemas que poderiam comprometer seu computador, enquanto as atualizações *Optional* corrigem problemas relevantes não relacionados à segurança ou fornecem aprimoramentos.

Procedimento 1.1 *Instalando patches com a Atualização Online do YaST*

- 1 Execute *Software > Atualização Online* no YaST.
- 2 Todos os novos patches (exceto os opcionais) disponíveis atualmente para o seu sistema já estão marcados para instalação. Clique em *Aceitar* ou *Aplicar* para instalá-los automaticamente.
- 3 Confirme com *Concluir* após a conclusão da instalação. Seu sistema está atualizado.

DICA: desabilitando deltarpm

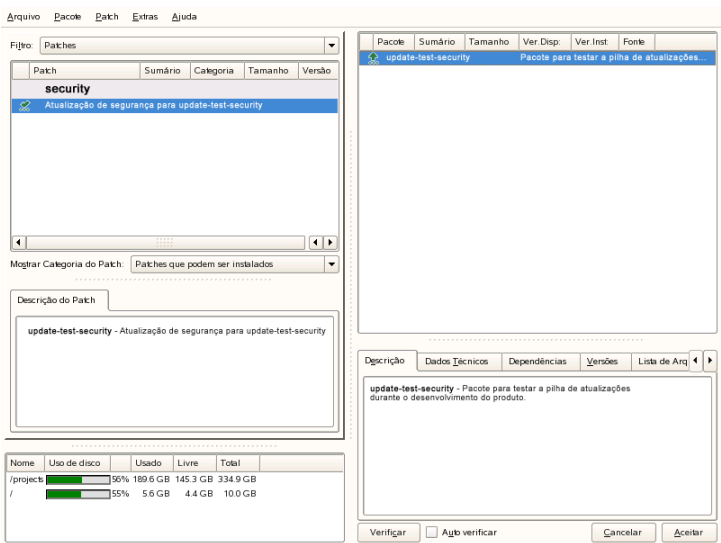
Por padrão, o download das atualizações é feito como deltarpm. Como a reconstrução dos pacotes rpm a partir de deltarpm é uma tarefa que consome muito tempo de uso da memória e da CPU, certas instalações ou configurações de hardware podem exigir que você desabilite o uso de deltarpm em benefício do desempenho. Para desabilitar o uso de deltarpm, edite o arquivo `/etc/zypp/zypp.conf` e defina `download.use_deltarpm` como `false`.

1.1 Instalando patches manualmente com a interface Qt

A janela *Atualização Online* é composta por quatro seções. A lista de todos os patches disponíveis está à esquerda. Encontre a descrição do patch selecionado exibida abaixo da lista de patches. A coluna à direita lista os pacotes incluídos no patch selecionado

(um patch pode ser composto por vários pacotes) e abaixo, há uma descrição detalhada do pacote selecionado.

Figura 1.1 Atualização Online do YaST



A tela de patches lista os patches disponíveis para o SUSE Linux Enterprise Desktop. Os patches são classificados por relevância de segurança (*security*, *recommended* e *optional*). Existem três telas diferentes dos patches. Use *Mostrar Categoria do Patch* para alterná-las:

Patches Necessários (tela padrão)

Patches não instalados que se aplicam aos pacotes instalados no seu sistema.

Patches Não Necessários

Os patches que se aplicam a pacotes não instalados no seu sistema, ou patches com requisitos que já foram atendidos (porque os pacotes relevantes já foram atualizados de outra fonte).

Todos os Patches

Todos os patches disponíveis para o SUSE Linux Enterprise Desktop.

Uma entrada da lista consiste em um símbolo e o nome do patch. Para obter uma lista dos símbolos possíveis, pressione Shift + F1. Ações exigidas pelos patches de

Security e *Recommended* são predefinidas automaticamente. Essas ações são *Instalar automaticamente*, *Atualizar automaticamente* e *Apagar automaticamente*. Ações para patches com relevância *Optional* não são predefinidas. Clique o botão direito do mouse em um patch e escolha uma ação da lista.

Se você instalar um pacote atualizado de um repositório que não seja o repositório de atualização, os requisitos de um patch para esse pacote poderão ser atendidos com essa instalação. Nesse caso, uma marca de seleção é exibida na frente do resumo do patch. O patch ficará visível na lista até você marcá-lo para instalação. Isso na verdade não instalará o patch (porque o pacote já está atualizado), mas marcará o patch como instalado.

A maioria dos patches inclui atualizações para diversos pacotes. Se desejar mudar as ações para pacotes individuais, clique o botão direito do mouse em um deles na janela de pacotes e escolha uma ação. Após ter marcado todos os patches e pacotes como desejado, prossiga com *Aceitar*.

1.2 Instalando patches manualmente com a interface GTK

A janela *Atualização Online* é composta por duas seções principais. O painel à esquerda lista todos os patches e fornece diferentes filtros para a lista. Veja no painel direito uma lista das mudanças que serão efetuadas após você clicar em *Aplicar*.

Figura 1.2 Atualização Online do YaST



Filtros da lista de patches

Disponível

Patches não instalados que se aplicam aos pacotes instalados no seu sistema.

Instalado

Patches que já estão instalados.

Todos

Patches que estão já instalados ou disponíveis.

Severidade

Mostrar apenas patches com relevância *Opcional*, *Recomendado* ou *Segurança*.
Por padrão, *Todos* os patches são mostrados.

Repositórios

Esse filtro permite exibir os patches por repositório.

Listagem de Pacotes

Aplique seu filtro personalizado aqui.

Clique em uma entrada de patch para abrir uma linha com informações detalhadas sobre o patch na área inferior da janela. Aqui você pode ver uma descrição detalhada de um patch, bem como as versões disponíveis. Você também pode escolher *Instalar* patches opcionais; os patches de segurança e os recomendados já estão pré-selecionados para instalação.

1.3 Atualização online automática

O YaST também oferece a possibilidade de configurar uma atualização automática.

Abra *Software > Configuração de Atualização Online*. Marque *Atualização Automática Online* e escolha se deseja atualizar *Diariamente*, *Semanalmente* ou *Mensalmente*.

Alguns patches, como atualizações de kernel, exigem interação do usuário, o que faria o procedimento de atualização automática parar. Portanto, você deve marcar *Ignorar Patches Interativos* se deseja que o procedimento de atualização prossiga de forma totalmente automática. Tendo feito isso, você deve executar uma *Atualização Online* manual ocasionalmente para instalar patches que exijam interação.

Reunindo informações do sistema para suporte

Quando surge um problema, use `supportconfig` para coletar informações do sistema. Tais informações podem ser, por exemplo, a versão atual em uso do kernel, o hardware, o banco de dados RPM, partições etc. O resultado é usado para ajudar o Centro de Suporte Novell a encontrar o seu problema.

2.1 Visão geral do Link do Suporte Novell

O Link do Suporte Novell (NSL) é novo no SUSE Linux Enterprise Desktop. Trata-se de uma ferramenta que reúne informações do sistema e permite enviá-las por upload a outro servidor para análise mais detalhada. O Centro de Suporte Novell usa o Link do Suporte Novell para reunir informações do sistema de servidores problemáticos e as envia ao servidor FTP público da Novell. As informações do sistema reunidas incluem: a versão atual em uso do kernel, o hardware, o banco de dados RPM, partições etc. O resultado é usado para ajudar o Centro de Suporte Novell a resolver sua solicitação de serviço em aberto.

Há duas maneiras de usar o Link do Suporte Novell:

1. Usar o módulo de Suporte do YaST.
2. Use o utilitário de linha de comando `supportconfig`.

O módulo de Suporte do YaST chama `supportconfig` para reunir as informações do sistema.

2.2 Usando o supportconfig

As seções a seguir descrevem como usar o `supportconfig` com o YaST, com a linha de comando e com as outras opções de que você dispõe.

2.2.1 Usando o YaST para coletar informações

Para usar o YaST para reunir as informações do seu sistema, proceda conforme a seguir:

- 1 Abra o URL <http://www.novell.com/center/eservice> e crie um número de solicitação de serviço.
- 2 Inicie o YaST.
- 3 Abra o módulo de *Suporte*.
- 4 Clique em *Criar relatório em arquivo tarball*.
- 5 Selecione uma opção na lista do botão de opção. Se desejar primeiro fazer um teste, use *Reunir apenas uma quantidade mínima de informações*. Continue com *Avançar*.
- 6 Digite suas informações de contato. Use seu número de solicitação de serviço da Passo 1 (p 10) e digite-o no campo de texto denominado *Número de solicitação de serviço Novell de 11 dígitos*. Continue com *Avançar*.
- 7 A coleta de informações é iniciada. Quando o processo for concluído, continue com *Avançar*.
- 8 Examine a coleta de dados e use *Remover dos Dados* se não precisar do respectivo nome de arquivo. Continue com *Avançar*.

- 9 Grave o tarball. Se desejar fazer upload para o Novell Customer Center, verifique se a opção *Fazer upload do tarball com arquivos de registro para o URL* está ativada. Conclua a operação com *Avançar*.

2.2.2 Usando o supportconfig diretamente para coletar informações

Para usar o `supportconfig` a partir da linha de comando, proceda da seguinte maneira:

- 1 Abra um shell e torne-se `root`.
- 2 Execute `supportconfig` sem qualquer opção. Isso reúne as informações padrão do sistema.
- 3 Aguarde a ferramenta concluir a operação.
- 4 O local padrão do arquivo é `/var/log`, com o formato de nome de arquivo `nts_HOST_DATA_HORÁRIO.tbz`

2.2.3 Opções comuns do supportconfig

O utilitário `supportconfig` possui várias opções de inicialização, as quais você pode ver com `supportconfig -h` ou usando a página de manual. Em geral, o `supportconfig` é executado sem o uso de opções. Veja a seguir um resumo das opções de inicialização mais comuns:

- Use a opção mínima (`-m`) para reduzir o tamanho das informações que serão reunidas:

```
supportconfig -m
```

- Inclua informações de contato adicionais na saída (em uma única linha):

```
supportconfig -E tux@example.org -N "Tux Penguin" -O "Penguin Inc." ...
```

- Durante a solução de um problema, talvez você queira reunir informações apenas sobre a área do problema em que está trabalhando no momento. Por exemplo, caso

you have problems with the LVM that you recently discovered in the standard output of supportconfig. After making changes, you want to gather the current information from the LVM. The command to follow gathers only the minimum information from supportconfig and the LVM.

```
supportconfig -i LVM
```

To view a complete list of resources, execute:

```
supportconfig -F
```

- Use the options `-u` and `-r` to make an upload of a tarball from supportconfig with the service request number. For example, in the case of you having opened a service request at Novell with the monitoring number 12345678901, execute the following:

```
supportconfig -ur 12345678901
```

2.3 Enviando informações à Novell

You can use the YaST Support module or the command-line utility supportconfig to send information from the system to Novell. If you have a problem with the server and want assistance from Novell, you must open a service request and send the information from the server to Novell. Both methods, from YaST and from the command-line, are described below.

Procedimento 2.1 *Enviando informações à Novell pelo YaST*

- 1 Abra o URL <http://www.novell.com/center/eservice> e crie um número de solicitação de serviço.
- 2 Anote o seu número de solicitação de serviço de 11 dígitos. Os exemplos a seguir usarão o número de solicitação de serviço fictício 12345678901.
- 3 Clique em *Criar relatório em arquivo tarball* na janela do módulo de Suporte do YaST.
- 4 Selecione o botão de opção *Usar personalizado*. Continue com *Avançar*.

5 Digite suas informações de contato, preencha o *Número de solicitação de serviço Novell de 11 dígitos* e inclua o URL de destino do upload da Novell.

- Para usar o destino de upload seguro, digite: `https://secure-www.novell.com/upload?appname=supportconfig&file={tarball}`.
- Para usar o destino de upload FTP normal, digite: `ftp://ftp.novell.com/incoming`.

Continue com *Avançar*. A coleta de informações é iniciada. Quando o processo for concluído, continue com *Avançar*.

6 Examine a coleta de dados e use *Remover dos Dados* para remover os arquivos que você deseja excluir do tarball que será enviado à Novell por upload. Continue com *Avançar*.

7 Por padrão, uma cópia do tarball será gravada em `/root`. Confirme se está usando um dos destinos de upload da Novell descritos acima e se a opção *Fazer upload do tarball com arquivos de registro para o URL* está ativada. Conclua com *Avançar*.

8 Clique em *Concluir*.

Procedimento 2.2 Enviando informações à Novell pelo supportconfig

1 Abra o URL `http://www.novell.com/center/eservice` e crie um número de solicitação de serviço.

2 Anote o seu número de solicitação de serviço de 11 dígitos. Os exemplos a seguir usarão o número de solicitação de serviço fictício 12345678901.

3 Servidores com conectividade à Internet:

3a Para usar o destino de upload padrão, execute:

```
supportconfig -ur 12345678901
```

3b Para usar o destino de upload seguro, digite o seguinte em uma única linha:

```
supportconfig -r 12345678901 -U  
'https://secure-www.novell.com/upload?appname=supportconfig&file={tarball}'
```

4 Servidores *sem* conectividade à Internet

4a Execute o seguinte:

```
supportconfig -r 12345678901
```

4b Faça o upload manual do tarball `/var/log/nts_SR12345678901*tbz` para o servidor FTP da Novell (<ftp://ftp.novell.com/incoming>).

4c Você também pode anexar o tarball à sua solicitação de serviço usando o URL da solicitação de serviço: <http://www.novell.com/center/eservice>.

5 Quando o tarball estiver no diretório <ftp://ftp.novell.com/incoming>, ele será anexado automaticamente à solicitação de serviço.

2.4 Para obter mais informações

Obtenha mais informações sobre a coleta de informações do sistema nos seguintes documentos:

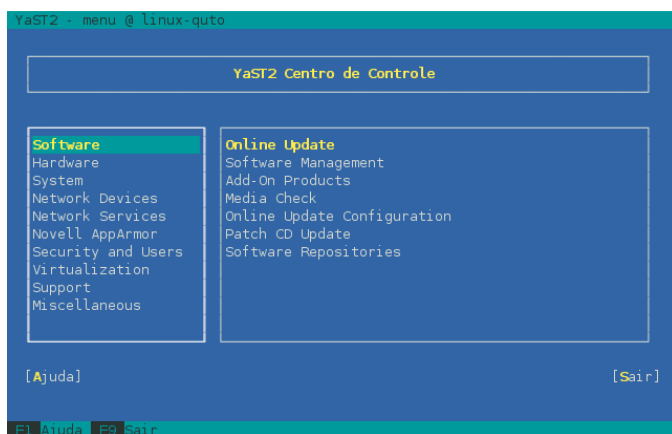
- `man supportconfig` — Página de manual do supportconfig
- `man supportconfig.conf` — Página de manual do arquivo de configuração do supportconfig
- <http://www.novell.com/communities/print/node/4097> — A Basic Server Health Check with Supportconfig (Verificação de integridade básica do servidor com o supportconfig)
- <http://www.novell.com/communities/print/node/4827> — Create Your Own Supportconfig Plugin (Crie seu próprio plug-in supportconfig)
- <http://www.novell.com/communities/print/node/4800> — Creating a Central Supportconfig Repository (Criando um repositório central do supportconfig)

YaST em modo de texto

Esta seção destina-se principalmente a administradores e especialistas do sistema que não executam um servidor X em seus sistemas e dependem da ferramenta de instalação baseada em texto. Ela contém informações básicas sobre como iniciar e operar o YaST em modo de texto.

O YaST em modo de texto usa a biblioteca ncurses para fornecer uma interface de usuário pseudográfica fácil de usar. A biblioteca ncurses está instalada por padrão. O tamanho mínimo suportado do emulador de terminal no qual se executará o YaST é de 80x25 caracteres.

Figura 3.1 Janela principal do YaST em modo de texto



Quando você inicia o YaST em modo de texto, o Centro de Controle do YaST é exibido (consulte a Figura 3.1). A janela principal contém três áreas: O quadro esquerdo apresenta as categorias às quais pertencem os vários módulos. Esse quadro fica ativo quando o YaST é iniciado e, portanto, é marcado por uma borda branca em negrito. A categoria ativa é realçada. O quadro direito apresenta uma visão geral dos módulos disponíveis na categoria ativa. O frame inferior contém os botões *Ajuda* e *Sair*.

Quando você inicia o Centro de Controle do YaST, a categoria *Software* é selecionada automaticamente. Use ↓ e ↑ para mudar a categoria. Para selecionar um módulo da categoria, ative o quadro direito com → e, em seguida, use ↓ e ↑ para selecionar o módulo. Mantenha as teclas de seta pressionadas para rolar pela lista de módulos disponíveis. O módulo selecionado é realçado. Pressione Enter para iniciar o módulo ativo.

Vários botões ou campos de seleção no módulo contêm uma letra realçada (amarelo por padrão). Use Alt + letra_realçada para selecionar um botão diretamente, em vez de navegar até ele com Tab. Saia do Centro de Controle do YaST pressionando Alt + Q ou selecionando *Sair* e pressionando Enter.

3.1 Navegação em módulos

A seguinte descrição dos elementos de controle nos módulos do YaST pressupõe que todas as teclas de função e combinações de teclas Alt funcionam e que não são atribuídas a funções globais diferentes. Leia a Seção 3.2, “Restrição de combinações de tecla” (p 18) para obter informações sobre possíveis exceções.

Navegação entre botões e listas de seleção

Use Tab para navegar entre os botões e frames contendo listas de seleção. Para navegar na ordem inversa, use Alt + Tab ou combinações de Shift + Tab.

Navegação em listas de seleção

Use as teclas de seta (↑ e ↓) para navegar entre os elementos individuais em um frame ativo que contenha uma lista de seleção. Se entradas individuais em um frame excederem a sua largura, use Shift + → ou Shift + ← para rolar horizontalmente para a direita e esquerda. Alternativamente, use Ctrl + E ou Ctrl + A. Essa combinação também pode ser usada se o uso de → ou ← resultar na mudança do frame ativo ou da lista de seleção atual, como no Centro de Controle.

Botões, botões de opção e caixas de seleção

Para selecionar botões com colchetes vazios (caixas de seleção) ou parênteses vazios (botões de opção), pressione Espaço ou Enter. Alternativamente, pode-se selecionar botões de opção e caixas de seleção diretamente com Alt + letra_realçada. Nesse caso, não é necessário confirmar com Enter. Se você navegar até um item com Tab, pressione Enter para executar a ação selecionada ou ativar o item de menu respectivo.

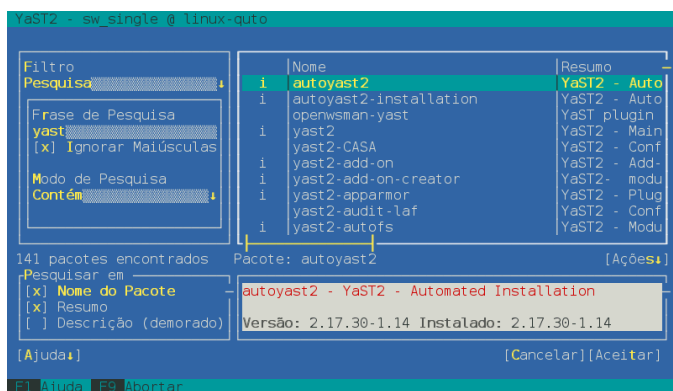
Teclas de função

As teclas F (F1 a F12) permitem acesso rápido aos vários botões. Os atalhos de teclas F disponíveis são mostrados na linha inferior da tela do YaST. As teclas de função que são realmente mapeadas para cada botão dependem do módulo YaST ativo, pois módulos diferentes oferecem botões diferentes (Detalhes, Informação, Adicionar, Apagar etc.). Use F10 para *Aceitar*, *OK*, *Avançar* e *Concluir*. Pressione F1 para acessar a ajuda do YaST.

Usando a árvore de navegação no modo ncurses

Alguns módulos do YaST usam uma árvore de navegação na parte esquerda da janela para seleção de caixas de diálogo de configuração. Use as teclas de seta (↑ e ↓) para navegar pelas três. Use Espaço para abrir ou fechar itens de árvore. No modo ncurses, você deve pressionar Enter após uma seleção na árvore de navegação, a fim de mostrar a caixa de diálogo selecionada. Esse é um comportamento intencional, para evitar atualizações demoradas da tela ao procurar na árvore de navegação.

Figura 3.2 Módulo de instalação de software



3.2 Restrição de combinações de tecla

Se o seu gerenciador de janelas usa combinações Alt globais, as combinações Alt no YaST talvez não funcionem. Teclas como Alt ou Shift também podem ser ocupadas pelas configurações do terminal.

Substituindo Alt por Esc

Os atalhos com Alt podem ser executados com Esc em vez de Alt. Por exemplo, Esc – H substitui Alt + H. (Primeiro pressione Esc, *depois* H.)

Navegação para trás e para frente com Ctrl + F e Ctrl + B

Se as combinações de Alt e Shift estiverem ocupadas pelo gerenciador de janelas ou pelo terminal, use as combinações Ctrl + F (para frente) e Ctrl + B (para trás).

Restrição de teclas de função

As teclas F também são usadas para funções. Certas teclas de função podem estar ocupadas pelo terminal e talvez não estejam disponíveis para o YaST. No entanto, as combinações de teclas Alt e teclas de função devem estar sempre disponíveis em um console de texto puro.

3.3 Opções de linha de comando do YaST

Além da interface de modo de texto, o YaST fornece uma interface de linha de comando pura. Para obter uma lista das opções de linha de comando do YaST, digite:

```
yast -h
```

3.3.1 Iniciando os módulos individuais

Para economizar tempo, os módulos do YaST individuais podem ser iniciados diretamente. Para iniciar um módulo, digite:

```
yast <module_name>
```

Exiba uma lista de todos os nomes de módulos disponíveis no seu sistema com `yast -l` ou `yast --list`. Inicie o módulo de rede, por exemplo, com `yast lan`.

3.3.2 Instalando pacotes a partir da linha de comando

Se você sabe o nome de um pacote e este é fornecido por qualquer um dos seus repositórios de instalação ativos, você pode usar a opção de linha de comando `-i` para instalar o pacote:

```
yast -i <package_name>
```

ou

```
yast --install <package_name>
```

package_name pode ser um único nome curto de pacote, por exemplo `gvim`, instalado com verificação de dependência, ou o caminho completo para um pacote rpm, instalado sem verificação de dependência.

Se precisar de um utilitário de gerenciamento de software baseado em linha de comando com funcionalidade adicional à fornecida pelo YaST, considere a possibilidade de usar o zypper. Esse novo utilitário usa a mesma biblioteca de gerenciamento de software que também é a base do gerenciador de pacotes do YaST. O uso básico do zypper é apresentado na Seção 5.1, “Usando o zypper” (p 33).

3.3.3 Parâmetros de linha de comando dos módulos do YaST

Para usar a funcionalidade do YaST em scripts, ele fornece suporte para linha de comando em módulos individuais. Nem todos os módulos têm suporte para linha de comando. Para exibir as opções disponíveis de um módulo, digite:

```
yast <module_name> help
```

Se um módulo não fornecer suporte para linha de comando, ele será iniciado no modo de texto e a seguinte mensagem aparecerá:

```
This YaST module does not support the command line interface.
```


Configuração do GNOME para administradores

Este capítulo introduz as opções de configuração do GNOME que os administradores podem usar para definir ajustes em todo o sistema, como personalização de menus, instalação de temas, configuração de fontes, mudança dos aplicativos preferidos e bloqueio de recursos.

Essas opções de configuração estão armazenadas no sistema GConf. Acesse o sistema GConf usando ferramentas como a interface de linha de comando `gconftool-2` ou a interface gráfica do usuário `gconf-editor`.

4.1 O sistema GConf

A área de trabalho GNOME gerencia sua própria configuração com o GConf. Trata-se de um banco de dados ou registro de estrutura hierárquica, no qual o usuário pode mudar suas próprias configurações e o administrador do sistema pode definir valores padrão ou obrigatórios para todos os usuários. As configurações do GConf são acessadas especificando-se caminhos de acesso como

`/desktop/gnome/background/nome_arquivo_imagem` — essa, por exemplo, é a chave que contém o nome do arquivo da imagem de segundo plano da área de trabalho.

Use o `gconf-editor` gráfico se quiser navegar por todas as opções de forma conveniente. Para obter uma descrição resumida sobre o uso do `gconf-editor`, consulte a Seção 4.1.1, “O `gconf-editor` gráfico” (p 22). Se você precisar de uma solução baseada em scripts, consulte a Seção 4.1.2, “Interface da linha de comando `gconftool-2`” (p 23).

ATENÇÃO: caixas de diálogo do Centro de Controle GNOME

O acesso direto ao Sistema Gconf, se feito de forma descuidada, pode fazer o sistema ficar inutilizável.

Para os usuários inexperientes que queiram ajustar apenas alguns recursos comuns da área de trabalho, recomenda-se usar as caixas de diálogo de configuração do Centro de Controle GNOME. Para iniciar o Centro de Controle GNOME, clique em *Computador > Centro de Controle*. Para obter mais informações, consulte a Seção “Centro de Controle” (Capítulo 3, *Personalizando suas configurações*, ↑*Guia do Usuário do GNOME*).

4.1.1 O gconf-editor gráfico

O gconf-editor permite navegar nas configurações do GConf e mudá-las de forma interativa. Para iniciar o gconf-editor na tela padrão da *janela Configurações*, clique em *Computador > Mais Aplicativos* e, no grupo *Sistema*, clique em *Editor de Configuração do GNOME*.

Por padrão, os usuários podem mudar as configurações de suas próprias áreas de trabalho, e o administrador pode preparar configurações para especificar valores padrão ou obrigatórios. Por exemplo, se você quiser habilitar o recurso de *interrupção de digitação* como obrigatório para todos os usuários, proceda da seguinte maneira:

- 1 Inicie o `gconf-editor` como `root` na linha de comando.
- 2 No painel de árvore à esquerda, expanda `/desktop/gnome/typing_break`.
- 3 Clique o botão direito do mouse em *habilitado* e selecione *Definir como Obrigatório*. Depois disso, você poderá gerenciar este recurso.
- 4 Abra a janela *Configurações obrigatórias* clicando em *Arquivo > Nova Janela Obrigatória*.
- 5 No painel de árvore da janela *Configurações obrigatórias*, expanda `/desktop/gnome/typing_break` e clique em *habilitado*.
- 6 Feche a janela para gravar as configurações clicando em *Arquivo > Fechar Janela*.

Para obter mais informações sobre o gconf-editor, consulte o Manual do Editor de Configurações em <http://library.gnome.org/users/gconf-editor/stable/>.

4.1.2 Interface da linha de comando gconftool-2

Para mudar as configurações a partir da linha de comando ou de dentro dos scripts, use `gconftool-2`. Veja alguns exemplos a seguir:

Como `root`, use o seguinte comando para listar os valores de todas as chaves:

```
gconftool-2 --recursive-list /
```

Se tiver interesse em apenas um subconjunto, especifique um caminho de acesso como `/desktop/gnome/typing_break`:

```
gconftool-2 --recursive-list /desktop/gnome/typing_break
```

Para listar as configurações obrigatórias:

```
gconftool-2 --recursive-list \  
  --config-source xml:readwrite:/etc/gconf/gconf.xml.mandatory /
```

Para definir uma configuração obrigatória, como `typing_break`:

```
gconftool-2 \  
  --config-source xml:readwrite:/etc/gconf/gconf.xml.mandatory \  
  --type bool \  
  --set /desktop/gnome/typing_break/enabled true
```

Para cancelar a definição de uma configuração obrigatória:

```
gconftool-2 \  
  --config-source xml:readwrite:/etc/gconf/gconf.xml.mandatory \  
  --unset /desktop/gnome/typing_break/enabled
```

Para acessar as configurações padrão, use `/etc/gconf/gconf.xml.default`.

Para obter mais informações sobre `gconftool-2`, consulte o Guia de Administração do Sistema do Ambiente de Trabalho GNOME, seção Ferramenta de Linha de Comando GConf em <http://library.gnome.org/admin/system-admin-guide/>

stable/gconf-6.html.en e a página de manual de `gconftool-2` (man `gconftool-2`).

4.2 Personalizado o menu principal, o painel e o browser de aplicativos

Controle os itens padrão mostrados em várias seções do menu principal (*Computador*) personalizado os seguintes arquivos:

- **`/usr/share/gnome-main-menu/applications.xbel`:** lista dos aplicativos padrão favoritos.
- **`/usr/share/gnome-main-menu/documents.xbel`:** lista dos documentos padrão favoritos.
- **`/usr/share/gnome-main-menu/system-items.xbel`:** itens mostrados na seção do sistema.

Com o `gconf-editor`, você pode personalizar o número de itens exibidos:

- **`/desktop/gnome/applications/main-menu/file-area/min_recent_items`:** número mínimo de itens recentes.
- **`/desktop/gnome/applications/main-menu/file-area/max_total_items`:** número máximo do total de itens.

Você pode personalizar o browser de aplicativos de várias maneiras, por exemplo, seu comportamento quando os usuários iniciam itens ou o número de itens exibidos na categoria *Novos Aplicativos*. Procure as chaves

`/desktop/gnome/applications/main-menu/ab_*` com o `gconf-editor`.

Para obter mais informações, consulte a seção Personalizar Menus no Guia de Administração do Sistema do Ambiente de Trabalho GNOME em <http://library.gnome.org/admin/system-admin-guide/stable/menustructure-0.html.en>.

4.3 Iniciando aplicativos automaticamente

Para iniciar aplicativos automaticamente no GNOME, use um dos seguintes métodos:

- **Para executar aplicativos para cada usuário:** coloque os arquivos `.desktop` em `/usr/share/gnome/autostart`.
- **Para executar aplicativos para um único usuário:** coloque os arquivos `.desktop` em `~/.config/autostart`.

Para desabilitar um aplicativo que é iniciado automaticamente, adicione `X-Autostart-enabled=false` ao arquivo `.desktop`.

4.4 Montando automaticamente e gerenciando dispositivos de mídia

O Nautilus (`nautilus`) monitora eventos relacionados a volume e responde com uma política especificada pelo usuário. Você pode usar o Nautilus para montar automaticamente as unidades de hot plug e a mídia removível inserida, executar programas automaticamente e reproduzir CDs de áudio ou DVDs de vídeo. O Nautilus também pode importar automaticamente fotos de uma câmera digital.

Os administradores do sistema podem definir padrões para todo o sistema. Para obter mais informações, consulte a Seção 4.5, “Mudando os aplicativos preferenciais” (p 25).

4.5 Mudando os aplicativos preferenciais

Para mudar os aplicativos preferenciais dos usuários, edite `/etc/gnome_defaults.conf`. Mais dicas são encontradas neste arquivo.

Após editar o arquivo, execute `SuSEconfig --module glib2`.

Para obter mais informações sobre tipos MIME, consulte <http://www.freedesktop.org/Standards/shared-mime-info-spec>.

4.6 Gerenciando perfis com o Sabayon

Sabayon é uma ferramenta de administração do sistema para criar e aplicar perfis do ambiente de área de trabalho. Perfil de área de trabalho é uma coleção de restrições e configurações padrão que podem ser aplicadas a usuários individuais ou a grupos de usuários. O Sabayon permite editar os padrões e chaves obrigatórias do GConf usando uma ferramenta gráfica.

A definição de perfil é feita por meio de uma sessão gráfica semelhante à sessão executada por um usuário, porém dentro de uma janela da área de trabalho. Você pode mudar as propriedades (como o segundo plano da área de trabalho, as barras de ferramentas e os applets disponíveis) normalmente. O Sabayon também detecta mudanças nas configurações padrão de quase todos os aplicativos.

Os arquivos ou documentos que ficam no diretório pessoal simulado ou na área de trabalho são incluídos no perfil concluído. Entre eles, muitos bancos de dados específicos de aplicativos, como as anotações do Tomboy. Com o uso desse mecanismo, é fácil fornecer anotações introdutórias ou gabaritos facilmente acessíveis aos novos usuários.

Um perfil de usuário pode herdar suas configurações de um perfil pai, anulando ou adicionando valores específicos. Isso habilita conjuntos de configurações hierárquicos. Por exemplo, você pode definir um perfil Empregado e derivar dele os perfis Artista e Garantia de Qualidade.

Além de fornecer padrões, o Sabayon também pode bloquear configurações. Esse recurso protege a configuração contra as mudanças de usuários. Por exemplo, você pode especificar que o segundo plano da área de trabalho não pode ser mudado para algo que não seja o padrão fornecido por você. Isso evita violações casuais das configurações, o que reduz o número de chamadas ao suporte técnico, além de habilitar ambientes tipo quiosque. Contudo, ele não fornece segurança absoluta e não deve ser usado para tal.

O Sabayon também fornece uma lista de configurações para aplicativos e elementos genéricos da interface do usuário que possuem suporte interno de bloqueio, incluindo

o OpenOffice.org e o painel do GNOME. Por exemplo, o painel pode ser configurado de modo a permitir a inclusão apenas de applets específicos e impedir a mudança de seu local ou tamanho na tela. Da mesma maneira, os itens do menu Gravar podem ser desabilitados para todos os aplicativos que o utilizam, impedindo que os usuários gravem documentos.

Os perfis podem ser transferidos para outros computadores. Eles ficam em `/etc/desktop-profiles/`, sendo que cada perfil é gravado em um arquivo ZIP separado.

4.6.1 Criando um perfil

Os perfis são gravados em arquivos ZIP localizados em `/etc/desktop-profiles`. Cada perfil que você grava é armazenado em um arquivo ZIP separado, como `nome-do-perfil.zip`. Você pode copiar ou mover os perfis para outros computadores.

- 1 Clique em *Computador > Mais Aplicativos > System > Editor de Perfil de Usuário*.
- 2 Se você não estiver conectado como `root`, digite a senha do `root` e clique em *Continuar*.

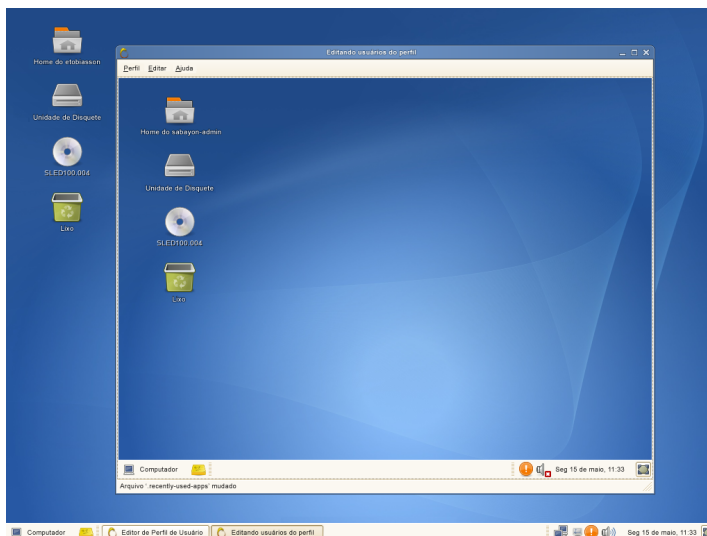
Figura 4.1 *Sabayon: Editor de Perfil de Usuário*



- 3 Clique em *Adicionar*.
- 4 Especifique um nome para o perfil e clique em *Adicionar*.
- 5 Selecione o perfil e clique em *Editar*.

Uma nova sessão da área de trabalho é aberta em uma janela do Xnest.

Figura 4.2 *Sabayon: nova janela do Xnest*



- 6 Na janela do Xnest, faça as mudanças nas configurações de sua escolha.

Cada configuração que você muda aparece na janela do Xnest.

Você pode optar por tornar obrigatórias todas as configurações (clcando em *Editar > Assegurar o Uso Obrigatório*), ignorar uma configuração (clcando em *Editar > Mudanças > Ignorar*) ou tornar uma configuração o padrão (não selecionando *Ignorar* nem *Obrigatório*).

- 7 Para bloquear as configurações para os usuários, clique em *Editar > Bloqueio* na janela do Xnest.

Você pode escolher uma destas opções:

Geral: permite desabilitar a linha de comando, a impressão, a configuração de impressão e o recurso de gravação em disco.

Painel: permite bloquear os painéis, desabilitar o fechamento forçado, desabilitar o bloqueio de tela, desabilitar o logout e desabilitar qualquer applet da lista *Desabilitar Applets*.

OpenOffice.org: permite definir o nível de segurança de macro para os documentos do OpenOffice.org, opções de carregamento e gravação, e opções da interface do usuário.

Browser da Web Epiphany: permite ocultar a barra de menus, fazer a janela ocupar a tela inteira, além de desabilitar a saída, URLs arbitrários, protocolos desprotegidos e a edição de favoritos e da barra de ferramentas.

- 8 Para gravar o perfil, clique em *Perfil > Gravar*.

O perfil é gravado em `/etc/desktop-profiles`.

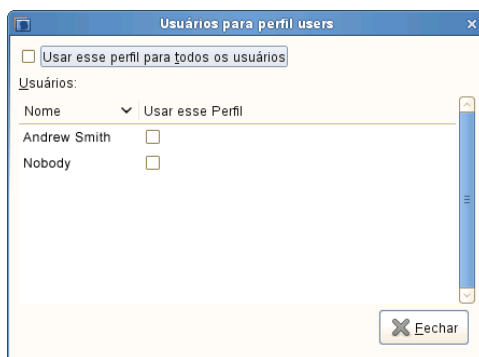
- 9 Clique em *Perfil > Sair* para fechar a janela do Xnest e clique em *Fechar* para sair do Sabayon.

4.6.2 Aplicando um perfil

Você pode aplicar um perfil a usuários individuais ou a todos os usuários em uma estação de trabalho.

- 1 Clique em *Computador > Mais Aplicativos > System > Editor de Perfil de Usuário*.
- 2 Se você não estiver conectado como `root`, digite a senha do `root` e clique em *Continuar*.
- 3 Selecione o perfil que deseja aplicar e clique em *Usuários*.

Figura 4.3 Sabayon: selecionando usuários



- 4 Selecione os usuários que usarão esse perfil.

Para aplicar o perfil a todos os usuários da estação de trabalho, clique em *Usar esse perfil para todos os usuários*.

- 5 Clique em *Fechar*.

4.7 Adicionando gabaritos de documentos

Para disponibilizar gabaritos de documentos aos usuários, insira-os no diretório `Templates` no diretório pessoal de um usuário. Isso pode ser feito manualmente para cada usuário, copiando-se os arquivos para `~/Templates`, ou para todo o sistema, adicionando-se um diretório `Templates` com documentos a `/etc/skel` antes que o usuário seja criado.

Um usuário cria um novo documento a partir de um gabarito clicando o botão direito do mouse na área de trabalho e selecionando *Criar Documento*.

4.8 Recursos de bloqueio da área de trabalho

Às vezes, convém remover ou desabilitar recursos da área de trabalho ou o acesso do usuário ao sistema operacional subjacente. O GNOME oferece recursos de bloqueio capazes de mudar a área de trabalho conforme a necessidade. Tecnicamente, você define chaves GConf para implementarem essas mudanças.

Por exemplo, se você abrir o gconf-editor, verá as chaves de bloqueio do menu principal em

`/desktop/gnome/applications/main-menu/lock-down/application_browser_link_visible`.
Esse local também contém as descrições de todas as chaves. Outras chaves de bloqueio:

`/desktop/gnome/lockdown/disable_command_line`

Se definida, os terminais não são mostrados no menu principal nem no Browser de Aplicativos.

`/apps/panel/global/disable_log_out`

`/apps/panel/global/disable_lock_screen`

Se definidas, o menu principal não mostra esses itens.

As chaves de bloqueio do Firefox estão em `/apps/firefox/lockdown`.

Para obter mais informações, consulte o “Desktop Administrators' Guide to GNOME Lockdown and Preconfiguration” (Guia do Administrador da Área de Trabalho para Bloqueio e Pré-configuração do GNOME), escrito por Sayamindu Dasgupta: <http://library.gnome.org/admin/deployment-guide/>.

4.9 Para obter mais informações

Para obter mais informações, consulte <http://library.gnome.org/admin/>.

Gerenciando software com ferramentas de linha de comando

Este capítulo descreve o Zypper e o RPM, duas ferramentas de linha de comando para gerenciar software.

5.1 Usando o zypper

O zypper é um gerenciador de pacotes de linha de comando para instalar, atualizar e remover pacotes, bem como para gerenciar repositórios. A sintaxe do zypper é semelhante à do `rug`. Ao contrário do `rug`, o zypper não requer que o daemon `zmd` seja executado nos bastidores. Para obter mais informações sobre compatibilidade com o `rug`, consulte `man zypper`, seção “COMPATIBILIDADE COM O RUG”. Ele é especialmente útil para realizar tarefas de gerenciamento remoto de software ou gerenciar software de scripts de shell.

Para obter mais informações sobre gerenciamento de software a partir da linha de comando, digite `zypper help` ou `zypper help comando` ou consulte a página de manual `zypper(8)`.

5.1.1 Uso geral

A sintaxe geral do zypper é:

```
zypper [global-options] command [command-options] [arguments] ...
```

Os componentes entre colchetes não são obrigatórios. A maneira mais simples de executar o zypper é digitar seu nome seguido de um comando. Por exemplo, para aplicar todos os patches necessários ao sistema, digite:

```
zypper patch
```

Além disso, você pode escolher dentre uma ou mais opções globais, digitando-as antes do comando. Por exemplo, `--non-interactive` significa executar o comando sem perguntar nada (aplicando as respostas padrão automaticamente):

```
zypper --non-interactive patch
```

Para usar as opções específicas de um comando em particular, digite-as logo após o comando. Por exemplo, `--auto-agree-with-licenses` significa aplicar todos os patches necessários ao sistema sem solicitar confirmação de nenhuma licença (eles serão aceitos automaticamente):

```
zypper patch --auto-agree-with-licenses
```

Alguns comandos requerem um ou mais argumentos. Ao usar o comando `install`, por exemplo, é preciso especificar o(s) pacote(s) a instalar:

```
zypper install mplayer
```

Algumas opções também requerem um argumento. O comando a seguir lista todos os padrões conhecidos:

```
zypper search -t pattern
```

Você pode combinar todos os anteriores. Por exemplo, o comando a seguir instalará os pacotes `mplayer` e `amarok` usando apenas o repositório `factory` e de modo verboso:

```
zypper -v install --repo factory mplayer amarok
```

Quase todos os comandos zypper possuem uma opção `dry-run` que simula o comando indicado. Ela pode ser usada para fins de teste.

```
zypper remove --dry-run MozillaFirefox
```

5.1.2 Instalando e removendo software com o zypper

Para instalar ou remover pacotes, use os seguintes comandos:

```
zypper install package
zypper remove package
```

O zypper conhece várias maneiras de tratar pacotes para os comandos install e remove:

pelo nome exato do pacote

```
zypper in MozillaFirefox
```

pelo alias do repositório e pelo nome do pacote

```
zypper in mozilla:MozillaFirefox
```

onde mozilla é o alias do repositório a partir do qual instalar.

pelo nome do pacote usando curingas

O comando a seguir instalará todos os pacotes cujos nomes começam com “Moz”. Use-o com cuidado, principalmente ao remover pacotes.

```
zypper in Moz*
```

por recurso

Se você, por exemplo, desejar instalar um módulo perl sem saber o nome do pacote, os recursos vêm a calhar:

```
zypper in 'perl(Time::ParseDate)'
```

por recurso e/ou arquitetura e/ou versão

Juntamente com um recurso, você pode especificar uma arquitetura (como i586 ou x86_64) e/ou uma versão. A versão deve ser precedida por um operador: < (menor que), <= (menor que ou igual a), = (igual a), >= (maior que ou igual a), > (maior que).

```
zypper in 'firefox.x86_64'
zypper in 'firefox>=3.5.3'
zypper in 'firefox.x86_64>=3.5.3'
```

pelo caminho

Você também pode especificar um local ou caminho remoto para um pacote:

```
zypper in /tmp/install/MozillaFirefox.rpm
zypper in
http://download.opensuse.org/repositories/mozilla/SUSE_Factory/x86_64/MozillaFirefox-3.5.3-1.3.x86_64.rpm
```

Para instalar e remover pacotes simultaneamente, use os modificadores +/-. Para instalar o emacs e remover o vim simultaneamente, use:

```
zypper install emacs -vim
```

Para remover o `emacs` e instalar o `vim` simultaneamente, use:

```
zypper remove emacs +vim
```

Para impedir que o nome do pacote iniciado por `-` seja interpretado como uma opção de comando, use-o sempre como segundo argumento. Se isso não for possível, preceda-o com `--`:

```
zypper install -emacs +vim      # Wrong
zypper install vim -emacs       # Correct
zypper install -- -emacs +vim   # same as above
zypper remove emacs +vim       # same as above
```

Por padrão, o `zypper` solicita uma confirmação antes de instalar ou remover um pacote selecionado, ou quando ocorre um problema. Você pode anular esse comportamento usando a opção `--non-interactive`. Essa opção deve ser fornecida antes do comando real (instalar, remover e `patch`), como em

```
zypper --non-interactive install package_name
```

Essa opção permite o uso do `zypper` em scripts e tarefas cron.

ATENÇÃO: não remova pacotes de sistema obrigatórios

Não remova pacotes como `glibc`, `zypper`, `kernel` ou similares. Esses pacotes são obrigatórios para o sistema e, se removidos, podem fazer o sistema ficar instável ou parar de funcionar de vez.

Instalando pacotes de fonte

Se desejar instalar o pacote de origem de um pacote, use:

```
zypper source-install package_name
```

Esse comando também instalará as dependências de compilação do pacote especificado. Se não quiser isso, adicione o switch `-D`. Para instalar apenas as dependências de compilação, use `-d`.

```
zypper source-install -d package_name # source package only
zypper source-install -D package_name # build dependencies only
```

Naturalmente isso só funcionará se o repositório com os pacotes de origem estiver habilitado na sua lista de repositórios (ele é adicionado por padrão, mas não habilitado). Consulte a Seção 5.1.4, “Gerenciando repositórios com o zypper” (p 40) para obter detalhes sobre o gerenciamento de repositórios.

Uma lista de todos os pacotes de origem disponíveis nos seus repositórios pode ser obtida com:

```
zypper search -t srcpackage
```

Utilitários

Para verificar se todas as dependências ainda são atendidas e para reparar dependências ausentes, use:

```
zypper verify
```

Além das dependências que precisam ser atendidas, alguns pacotes “recomendam” outros pacotes. Esses pacotes recomendados somente são instalados se estiverem disponíveis de fato. Caso os pacotes recomendados sejam disponibilizados após a instalação do pacote que fez a recomendação (pela adição de pacotes adicionais), use o seguinte comando:

```
zypper install-new-recommends
```

5.1.3 Atualizando software com o zypper

Existem três maneiras diferentes de atualizar o software usando o zypper: instalando patches, instalando uma versão nova de um pacote ou atualizando a distribuição inteira. Para executar a última maneira, usa-se o comando `zypper dist-upgrade`, abordado na Seção “Distribution Upgrade with zypper” (Capítulo 4, *Updating SUSE Linux Enterprise*, ↑ *Guia de Implantação*).

Instalando patches

Para instalar todos os patches lançados oficialmente que se aplicam ao seu sistema, execute:

```
zypper patch
```

Nesse caso, todos os patches disponíveis em seus repositórios são verificados quanto à sua relevância e instalados, se necessário. Após o registro de sua instalação do SUSE Linux Enterprise Desktop, um repositório de atualização oficial contendo tais patches será adicionado ao seu sistema. O comando acima é tudo o que você deve digitar para aplicá-los quando necessário.

O zypper conhece três comandos diferentes para consultar a disponibilidade dos patches:

```
zypper patch-check
```

Lista o número de patches necessários (patches que se aplicam ao seu sistema e ainda não estão instalados)

```
~ # zypper patch-check
Loading repository data...
Reading installed packages...
5 patches needed (1 security patch)
```

```
zypper list-patches
```

Lista todos os patches necessários (patches que se aplicam ao seu sistema e ainda não estão instalados)

```
~ # zypper list-updates
Loading repository data...
Reading installed packages...
S | Repository | Name | Current | Available | Arch
--+-+-----+-----+-----+-----+-----+
v | Updates   | update-test-interactive | 0-2.35 | 0-9999.1.2 | noarch
v | Updates   | update-test-optional    | 0-2.35 | 0-9999.1.2 | noarch
v | Updates   | update-test-reboot-needed | 0-2.35 | 0-9999.1.2 | noarch
v | Updates   | update-test-relogin-suggested | 0-2.35 | 0-9999.1.2 | noarch
v | Updates   | update-test-security     | 0-2.35 | 0-9999.1.2 | noarch
```

```
zypper patches
```

Lista todos os patches disponíveis para o SUSE Linux Enterprise Desktop, independentemente de já estarem instalados ou aplicarem-se à sua instalação.

Também é possível listar e instalar todos os patches relevantes a problemas específicos. Para listar patches específicos, use o comando `zypper list-patches` com as seguintes opções:

```
-b
```

Lista todos os patches necessários para problemas do Bugzilla.

```
--bugzilla [=número]
```

Lista os patches necessários para o problema do Bugzilla referente ao número especificado.

Para instalar um patch para um problema específico, use o comando:

```
zypper patch --bugzilla=number
```

Instalando atualizações

Se um repositório contém apenas pacotes novos, mas não fornece patches, `zypper patch` não surte nenhum efeito. Para atualizar todos os pacotes instalados com versões disponíveis mais novas, use:

```
zypper update
```

Para atualizar pacotes individuais, especifique o pacote com o comando `update` ou `install`:

```
zypper update package  
zypper install package
```

Uma lista de todos os novos pacotes disponíveis pode ser obtida com o comando:

```
zypper list-updates
```

NOTA: diferenças entre `zypper update` e `zypper dist-upgrade`

Escolha `zypper update` para atualizar os pacotes com as versões mais recentes disponíveis para a sua versão do produto e manter a integridade do sistema. `zypper update` obedecerá às seguintes regras:

- nenhuma mudança de fornecedor
- nenhuma mudança de arquitetura
- nenhum downgrade
- manter pacotes instalados

Para fazer upgrade da sua instalação para uma versão nova do produto, use `zypper dist-upgrade` com os repositórios obrigatórios (consulte a Seção 5.1.4, “Gerenciando repositórios com o zypper” (p 40) para obter detalhes). Esse comando garante que todos os pacotes serão instalados a partir

dos repositórios atualmente habilitados. Como essa regra tem uso obrigatório assegurado, os pacotes podem mudar de fornecedor ou arquitetura ou até sofrer downgrade. Todos os pacotes com dependências não atendidas após o upgrade serão desinstalados.

5.1.4 Gerenciando repositórios com o zypper

Todos os comandos de instalação ou patch do zipper dependem de uma lista de repositórios conhecidos. Para listar todos os repositórios conhecidos para o sistema, use o comando:

```
zypper repos
```

O resultado parecerá com o seguinte:

#	Alias	Enabled	Refresh	Name
1	SUSE-Linux-Enterprise-Server 11-0	Yes	No	SUSE-Linux-Enterprise-Server 11-0
2	SLES-11-Updates	Yes	Yes	SLES 11 Online Updates
3	broadcomdrv	Yes	No	Broadcom Drivers

Na especificação de repositórios em vários comandos, é possível usar um alias, URI ou número de repositório a partir da saída do comando `zypper repos`. Note, porém, que os números podem mudar após a modificação da lista de repositórios. O alias nunca mudará sozinho.

Por padrão, detalhes como o URI ou a prioridade do repositório não são exibidos. Use o seguinte comando para listar todos os detalhes:

Adicionando repositórios

Para adicionar um repositório, execute

```
zypper addrepo URI Alias
```

O *URI* pode ser um repositório da Internet, um recurso de rede, um diretório ou um CD ou DVD (consulte <http://en.opensuse.org/Libzypp/URI> para obter detalhes). O *Álias* é um identificador exclusivo e abreviado do repositório. Pode ser escolhido livremente, com a única condição de que seja exclusivo. O zypper emitirá um aviso se você especificar um alias que já está em uso. Para tornar o trabalho com repositórios mais conveniente, use alias curtos e fáceis de lembrar.

Removendo repositórios

Se você deseja remover um repositório da lista, use o comando `zypper removerepo` junto com o alias ou o número do repositório que você deseja apagar. Para remover a terceira entrada do exemplo, use o seguinte comando:

```
zypper removerepo 3
```

Modificando repositórios

Habilite ou desabilite os repositórios com `zypper modifyrepo`. Você também pode alterar as propriedades do repositório (por exemplo, atualizar o comportamento, o nome ou a prioridade) com esse comando. O comando a seguir habilitará o nome de repositório “atualizações”, ativar a atualização automática e definir sua prioridade como 20:

```
zypper mr -er -p 20 'updates'
```

A modificação de repositórios não se limita a um único repositório, você também pode operar em grupos:

- a: todos os repositórios
- l: repositórios locais
- t: repositórios remotos
- m *TIPO*: repositórios de determinado tipo (*TIPO* pode ser um dos seguintes: http, https, ftp, cd, dvd, dir, file, cifs, smb, nfs, hd, iso)

Para renomear o alias de um repositório, use o comando `renamerepo`. O exemplo a seguir muda o alias “Mozilla Firefox” para somente “firefox”:

```
zypper renamerepo 'Mozilla Firefox' firefox
```

5.1.5 Consultando repositórios e pacotes com o zypper

O zypper oferece vários métodos de consulta a repositórios ou pacotes. Para obter as listas de todos os produtos, padrões, pacotes ou patches disponíveis, use os seguintes comandos:

```
zypper products
zypper patterns
zypper packages
zypper patches
```

Para consultar todos os repositórios para determinados pacotes, use `search`. Ele funciona para nomes de pacotes, recursos ou, opcionalmente, para resumos e descrições de pacotes. O uso dos curingas `*` e `?` com o termo da pesquisa é permitido. Por padrão, a pesquisa não diferencia maiúsculas de minúsculas.

```
zypper se firefox          # simple search for "firefox"
zypper se *fire*           # using wildcards
zypper se -d fire          # also search in package descriptions and summaries
zypper se -u firefox       # only display packages not already installed
```

Para procurar pacotes que oferecem um recurso específico, use o comando `what-provides`. Se você, por exemplo, deseja saber qual pacote fornece o módulo `perl SVN::Core`, use o seguinte comando:

```
zypper what-provides 'perl(SVN::Core)'
```

Para consultar pacotes únicos, use `info` com um nome exato de pacote como argumento. Ele exibe informações detalhadas sobre um pacote. Use as opções `--requires` e `--recommends` para mostrar também o que é requerido/recomendado pelo pacote:

```
zypper info --requires MozillaFirefox
```

O `what-provides package` é semelhante ao `rpm -q --whatprovides package`, mas o `rpm` é capaz apenas de consultar o banco de dados RPM (que é o banco de dados de todos os pacotes instalados). O zypper, por outro lado, o informará sobre fornecedores do recurso a partir de qualquer repositório, não apenas aqueles que estão instalados.

5.2 RPM — o gerenciador de pacotes

O RPM (gerenciador de pacotes RPM) é usado para gerenciar pacotes de software. Seus principais comandos são `rpm` e `rpmbuild`. O banco de dados RPM avançado pode ser consultado pelos usuários, administradores de sistema e construtores de pacotes para obtenção de informações detalhadas sobre o software instalado.

Basicamente, o `rpm` possui cinco modos: instalação, desinstalação (ou atualização) de pacotes de software, reconstrução do banco de dados RPM, consulta de bancos RPM ou arquivos RPM individuais, verificação de integridade dos pacotes e assinatura de pacotes. O `rpmbuild` pode ser usado para construir pacotes instaláveis de fontes originais.

Os arquivos RPM instaláveis são compactados em um formato binário especial. Esses são arquivos de programa para instalação e determinadas metainformações usadas durante a instalação pelo comando `rpm` para configurar o pacote de softwares. Também são armazenados no banco de dados RPM com o objetivo de documentação. Os arquivos RPM normalmente têm a extensão `.rpm`.

DICA: pacotes de desenvolvimento de software

Para vários pacotes, os componentes necessários para o desenvolvimento de software (bibliotecas, cabeçalhos, arquivos de inclusão etc.) foram colocados em pacotes separados. Esses pacotes de desenvolvimento só são necessários quando você deseja compilar software por conta própria (por exemplo, os pacotes do GNOME mais recentes). Eles podem ser identificados pela extensão de nome `-devel`, como os pacotes `alsa-devel`, `gimp-devel` e `kdelibs3-devel`.

5.2.1 Verificando a autenticidade do pacote

Os pacotes RPM possuem uma assinatura GnuPG. O comando `rpm --checksig pacote-1.2.3.rpm` pode ser usado para verificar a assinatura de um pacote RPM e determinar se ele provém do SUSE ou de outro recurso confiável. Isso é especialmente recomendado para pacotes de atualização da Internet.

5.2.2 Gerenciando pacotes: instalar, atualizar e desinstalar

Normalmente, a instalação de um arquivo RPM é bem simples: `rpm -i pacote.rpm`. Com esse comando, o pacote será instalado, mas somente se as dependências forem atendidas e não houver conflitos com outros pacotes. Com uma mensagem de erro, o `rpm` solicita os pacotes que devem ser instalados para atender a requisitos de dependência. Em segundo plano, o banco de dados RPM garante que não haja conflitos, pois um arquivo específico pode pertencer a apenas um pacote. Ao escolher opções diferentes, você pode forçar o `rpm` a ignorar esses padrões, mas isso é somente para especialistas. Caso contrário, você se arrisca a comprometer a integridade do sistema e, possivelmente, ameaça a capacidade de atualização do sistema.

As opções `-U` ou `--upgrade` e `-F` ou `--freshen` podem ser usadas para atualizar um pacote (por exemplo, `rpm -F pacote.rpm`). Esse comando remove os arquivos da versão antiga e instala os novos arquivos imediatamente. A diferença entre as duas versões é que o `-U` instala pacotes que não existiam no sistema anteriormente, mas `-F` atualiza somente pacotes previamente instalados. Durante a atualização, o `rpm` atualiza arquivos de configuração cuidadosamente com a seguinte estratégia:

- Se um arquivo de configuração não tiver sido modificado pelo administrador de sistema, o `rpm` instalará a nova versão do arquivo apropriado. O administrador de sistema não precisa adotar nenhuma ação.
- Se um arquivo de configuração tiver sido mudado pelo administrador do sistema antes da atualização, o `rpm` gravará o arquivo mudado com a extensão `.rpmorig` ou `.rpmsave` (arquivo de backup) e instalará a versão do novo pacote (mas somente se o arquivo instalado originalmente e a versão mais nova forem diferentes). Nesse caso, compare o arquivo de backup (`.rpmorig` ou `.rpmsave`) com o arquivo recém-instalado e faça novamente as modificações no novo arquivo. Depois, verifique se apagou todos os arquivos `.rpmorig` e `.rpmsave` para evitar problemas em atualizações futuras.
- Arquivos `.rpmnew` são exibidos se o arquivo de configuração já existir e se o rótulo `noreplace` tiver sido especificado no arquivo `.spec`.

Após uma atualização, os arquivos `.rpmsave` e `.rpmnew` devem ser removidos depois de comparados, para que não impeçam atualizações futuras. A extensão

`.rpmorig` será atribuída se o arquivo não tiver sido previamente reconhecido pelo banco de dados RPM.

Caso contrário, o `.rpmsave` será usado. Em outras palavras, o `.rpmorig` resulta da atualização de um formato estranho ao RPM. O `.rpmsave` resulta da atualização de um RPM mais antigo para um RPM mais novo. O `.rpmnew` não revela se o administrador do sistema fez mudanças no arquivo de configuração. Uma lista destes arquivos está disponível em `/var/adm/rpmconfigcheck`. Alguns arquivos de configuração (como `/etc/httpd/httpd.conf`) não são sobregravados para permitir operação continuada.

O switch `-U` não é somente *um* equivalente para a desinstalação com a opção `-e` e a instalação com a opção `-i`. Use `-U` sempre que possível.

Para remover um pacote, digite `rpm -e pacote`. O `rpm`, que só apaga o pacote quando não há dependências não resolvidas. É teoricamente impossível apagar `Tcl/Tk`, por exemplo, enquanto outro aplicativo exigir sua existência. Mesmo nesse caso, o RPM pede ajuda do banco de dados. Se, por qualquer motivo, a exclusão for impossível (mesmo que não exista *nenhuma* dependência adicional), talvez seja útil reconstruir o banco de dados RPM usando a opção `--rebuilddb`.

5.2.3 RPM e patches

Para garantir a segurança operacional de um sistema, pacotes de atualização devem ser instalados no sistema periodicamente. Anteriormente, um erro em um pacote só poderia ser eliminado com a substituição de todo o pacote. Pacotes grandes com bugs em pequenos arquivos podem resultar facilmente nesse cenário. Porém, o RPM do SUSE oferece um recurso que permite a instalação de patches em pacotes.

Como exemplo, as considerações mais importantes são demonstradas com `pine`:

O RPM com patch é adequado para meu sistema?

Para verificar isso, consulte primeiro a versão instalada do pacote. No caso do `pine`, isso pode ser feito com

```
rpm -q pine
pine-4.44-188
```

Em seguida, verifique se o RPM com patch é adequado para essa versão do `pine`:

```
rpm -qp --basedon pine-4.44-224.i586.patch.rpm
pine = 4.44-188
pine = 4.44-195
pine = 4.44-207
```

Esse patch é adequado para três versões diferentes do pine. A versão instalada no exemplo também está listada para que o patch possa ser instalado.

Quais arquivos serão substituídos pelo patch?

Os arquivos afetados por um patch podem ser facilmente vistos no RPM com patch.

O parâmetro `rpm-P` permite a seleção de recursos de patch especiais. Exiba a lista de arquivos com o seguinte comando:

```
rpm -qpPl pine-4.44-224.i586.patch.rpm
/etc/pine.conf
/etc/pine.conf.fixed
/usr/bin/pine
```

ou, se o patch já estiver instalado, com o seguinte comando:

```
rpm -qPl pine
/etc/pine.conf
/etc/pine.conf.fixed
/usr/bin/pine
```

Como instalar um RPM com patch no sistema?

RPMs com patch são usados como RPMs comuns. A única diferença é que um RPM adequado já deve estar instalado.

Quais patches já estão instalados no sistema e para quais versões do pacote?

É possível exibir uma lista de todos os patches instalados no sistema com o comando

`rpm -qPa`. Se somente um patch for instalado em um novo sistema (como no exemplo), a lista será exibida como a seguir:

```
rpm -qPa
pine-4.44-224
```

Se posteriormente você desejar saber qual versão de pacote foi originalmente instalada, essas informações também estarão disponíveis no banco de dados RPM.

No caso do pine, é possível exibir essas informações com o seguinte comando:

```
rpm -q --basedon pine
pine = 4.44-188
```

Mais informações, incluindo informações sobre o recurso de patch do RPM, estão disponíveis nas páginas de manual de `rpm` e `rpmbuild`.

NOTA: atualizações oficiais do SUSE Linux Enterprise Desktop

Para que o tamanho de download das atualizações seja o menor possível, as atualizações oficiais do SUSE Linux Enterprise Desktop não são fornecidas como RPMs de patch, mas como pacotes Delta RPM (consulte a Seção 5.2.4, “Pacotes RPM Delta” (p 47) para obter detalhes).

5.2.4 Pacotes RPM Delta

Os pacotes RPM Delta possuem uma diferença entre uma versão nova e antiga de um pacote RPM. Aplicar um RPM delta a um RPM antigo resulta em um RPM completamente novo. Não é necessário ter uma cópia do RPM antigo, pois um RPM delta também pode funcionar com um RPM instalado. Os pacotes RPM delta têm tamanho ainda menor que os RPMs com patch, o que é uma vantagem durante a transferência de pacotes de atualização na Internet. A desvantagem é que operações de atualização que envolvem RPMs delta consomem consideravelmente mais ciclos de CPU do que as operações com RPMs com patch ou simples.

Os binários `prepdeltarpm`, `writedeltarpm` e `applydeltarpm` integram a suíte de RPM delta (pacote `deltarpm`) e ajudam na criação e aplicação de pacotes RPM delta. Com os seguintes comandos, crie um RPM delta chamado `new.delta.rpm`. O comando a seguir pressupõe que `old.rpm` e `new.rpm` estejam presentes:

```
prepdeltarpm -s seq -i info old.rpm > old.cpio
prepdeltarpm -f new.rpm > new.cpio
xdelta delta -0 old.cpio new.cpio delta
writedeltarpm new.rpm delta info new.delta.rpm
```

Por fim, remova os arquivos de trabalho temporários `old.cpio`, `new.cpio` e `delta`.

Usando `applydeltarpm`, você poderá reconstruir o novo RPM do arquivo de sistema, se o pacote antigo já estiver instalado:

```
applydeltarpm new.delta.rpm new.rpm
```

Para derivá-lo do RPM antigo sem acessar o sistema de arquivos, use a opção `-r`:

```
applydeltarpm -r old.rpm new.delta.rpm new.rpm
```

Consulte `/usr/share/doc/packages/deltarpm/README` para obter detalhes técnicos.

5.2.5 Consultas de RPM

Com a opção `-q`, o `rpm` inicia consultas, permitindo a inspeção de um arquivo RPM (adicionando-se a opção `-p`) e também a consulta ao banco de dados RPM de pacotes instalados. Vários switches estão disponíveis para especificar o tipo de informação necessária. Consulte a Tabela 5.1, “Opções mais importantes de consulta de RPM” (p 48).

Tabela 5.1 *Opções mais importantes de consulta de RPM*

<code>-i</code>	Informações de pacote
<code>-l</code>	Lista de arquivos
<code>-f ARQUIVO</code>	Consulte o pacote que contém o arquivo <i>ARQUIVO</i> (o caminho completo deve ser especificado com <i>ARQUIVO</i>)
<code>-s</code>	Lista de arquivos com informações de status (requer <code>-l</code>)
<code>-d</code>	Lista somente arquivos de documentação (requer <code>-l</code>)
<code>-c</code>	Lista somente arquivos de configuração (requer <code>-l</code>)
<code>--dump</code>	Lista de arquivos com detalhes completos (a ser usada com <code>-l</code> , <code>-c</code> ou <code>-d</code>)
<code>--provides</code>	Lista recursos do pacote que outro pacote pode solicitar com <code>--requires</code>
<code>--requires, -R</code>	Recursos exigidos pelo pacote
<code>--scripts</code>	Scripts de instalação (pré-instalação, pós-instalação, desinstalação)

Por exemplo, o comando `rpm -q -i wget` exibe as informações mostradas no Exemplo 5.1, “`rpm -q -i wget`” (p 49).

Exemplo 5.1 *rpm -q -i wget*

```
Name           : wget                               Relocations: (not relocatable)
Version        : 1.11.4                             Vendor: openSUSE
Release       : 1.70                                Build Date: Sat 01 Aug 2009
09:49:48 CEST
Install Date: Thu 06 Aug 2009 14:53:24 CEST      Build Host: build18
Group          : Productivity/Networking/Web/Utilities Source RPM:
wget-1.11.4-1.70.src.rpm
Size           : 1525431                             License: GPL v3 or later
Signature      : RSA/8, Sat 01 Aug 2009 09:50:04 CEST, Key ID b88b2fd43dbdc284
Packager       : http://bugs.opensuse.org
URL            : http://www.gnu.org/software/wget/
Summary        : A Tool for Mirroring FTP and HTTP Servers
Description    :
Wget enables you to retrieve WWW documents or FTP files from a server.
This can be done in script files or via the command line.
[...]
```

A opção `-f` funciona somente se você especificar o nome e o caminho completos do arquivo. Forneça quantos nomes de arquivo desejar. Por exemplo, o seguinte comando

```
rpm -q -f /bin/rpm /usr/bin/wget
```

resulta em:

```
rpm-4.4.2.3-45.5
wget-1.11.4-1.70
```

Se somente parte do nome de arquivo for conhecida, use um script de shell conforme mostrado no Exemplo 5.2, “Script para pesquisar pacotes” (p 49). Passe o nome de arquivo parcial para o script mostrado como um parâmetro ao executá-lo.

Exemplo 5.2 *Script para pesquisar pacotes*

```
#!/bin/sh
for i in $(rpm -q -a -l | grep $1); do
    echo "\"$i\" is in package:"
    rpm -q -f $i
    echo ""
done
```

O comando `rpm -q --changelog rpm` exibe uma lista detalhada de informações de mudança sobre um pacote específico, classificadas por data.

Com a ajuda do banco de dados RPM instalado, é possível realizar verificações. Inicie as verificações com `-V`, `-y` ou `--verify`. Com essa opção, o `rpm` mostra todos os

arquivos em um pacote que foram modificados desde a instalação. O `rpm` usa oito símbolos de caracteres para fornecer algumas dicas sobre as seguintes mudanças:

Tabela 5.2 *Opções de verificação do RPM*

5	Resumo de verificação MD5
S	Tamanho do arquivo
L	Link simbólico
T	Tempo de modificação
D	Números de dispositivo principais e auxiliares
U	Proprietário
C	Grupo
M	Modo (tipo de arquivo e permissões)

No caso de arquivos de configuração, a letra `c` é impressa. Por exemplo, para mudanças para `/etc/wgetrc` (`wget`):

```
rpm -V wget
S.5....T c /etc/wgetrc
```

Os arquivos do banco de dados RPM são colocados em `/var/lib/rpm`. Se a partição `/usr` tiver o tamanho de 1 GB, esse banco de dados poderá ocupar praticamente 30 MB, especialmente após uma atualização completa. Se o banco de dados for maior do que o esperado, será útil reconstruir o banco de dados com a opção `--rebuilddb`. Antes disso, faça um backup do banco de dados antigo. O script `cron cron.daily` faz cópias diárias do banco de dados (compactado com `gzip`) e as armazena em `/var/adm/backup/rpmdb`. O número de cópias é controlado pela variável `MAX_RPMDDB_BACKUPS` (padrão: 5) em `/etc/sysconfig/backup`. O tamanho de um único backup é de aproximadamente 1 MB para 1 GB em `/usr`.

5.2.6 Instalando e compilando pacotes de fonte

Todos os pacotes de fonte têm a extensão `.src.rpm` (RPM de fonte).

DICA

Pacotes de fonte podem ser copiados da mídia de instalação para o disco rígido e descompactados com o YaST. Porém, eles não são marcados como instalados (`[i]`) no gerenciador de pacotes. Isso ocorre porque os pacotes de fontes não são inseridos no banco de dados RPM. Somente o software do sistema operacional *instalado* está listado no banco de dados RPM. Quando você “instalar” um pacote de fontes, somente o código-fonte será adicionado ao sistema.

Os diretórios a seguir devem estar disponíveis para `rpm` e `rpmbuild` em `/usr/src/packages` (a menos que você tenha especificado configurações personalizadas em um arquivo como `/etc/rpmrc`):

SOURCES

para as fontes originais (arquivos `.tar.bz2` ou `.tar.gz` etc.) e para ajustes específicos de distribuição (geralmente arquivos `.diff` ou `.patch`)

SPECS

para os arquivos `.spec`, similares a um `metaMakefile`, que controla o processo de *construção*

BUILD

diretório em que todas as fontes são descompactadas, corrigidas e compiladas

RPMS

local em que os pacotes binários concluídos são armazenados

SRPMS

local em que estão os RPMs de fonte

Quando você instala um pacote de fonte com o YaST, todos os componentes necessários são instalados em `/usr/src/packages`; as fontes e os ajustes em `SOURCES` e o arquivo `.spec` relevante em `SPECS`.

ATENÇÃO

Não faça experiências com os componentes do sistema (`glibc`, `rpm`, `sysvinit` etc.), pois isso arrisca a estabilidade do sistema.

O exemplo a seguir usa o pacote `wget.src.rpm`. Após instalar o pacote de origem, você deverá ter arquivos semelhantes aos da seguinte lista:

```
/usr/src/packages/SOURCES/wget-1.11.4.tar.bz2
/usr/src/packages/SOURCES/wgetrc.patch
/usr/src/packages/SPECS/wget.spec
```

`rpmbuild -b X /usr/src/packages/SPECS/wget.spec` inicia a compilação. `X` é um curinga para vários estágios do processo de construção (consulte a saída de `--help` ou a documentação do RPM para obter detalhes). Veja a seguir uma breve explicação:

`-bp`

Preparar as fontes em `/usr/src/packages/BUILD`: descompactar e corrigir.

`-bc`

Faz o mesmo que `-bp`, mas com compilação adicional.

`-bi`

Faz o mesmo que `-bp`, mas com a instalação adicional do software criado. Cuidado: se o pacote não aceitar o recurso `BuildRoot`, talvez você sobregrave os arquivos de configuração.

`-bb`

Faz o mesmo que `-bi`, mas com a criação adicional do pacote binário. Se a compilação tiver sido bem-sucedida, o binário deverá estar em `/usr/src/packages/RPMS`.

`-ba`

Faz o mesmo que `-bb`, mas com a criação adicional do RPM de fonte. Se a compilação tiver sido bem-sucedida, o binário deverá estar em `/usr/src/packages/SRPMS`.

`--short-circuit`

Ignora algumas etapas.

O RPM binário criado agora pode ser instalado com `rpm -i` ou, de preferência, com `rpm -U`. A instalação com `rpm` faz com que ele apareça no banco de dados RPM.

5.2.7 Compilando pacotes RPM com build

O perigo de vários pacotes é que arquivos indesejados são adicionados ao sistema em execução durante o processo de construção. Para evitar isso, use `build`, que cria um ambiente definido para construção do pacote. Para estabelecer esse ambiente `chroot`, o script `build` deve ser fornecido com uma árvore de pacote completa. Essa árvore pode ser disponibilizada no disco rígido, por meio do NFS ou DVD. Defina a posição com `build --rpms diretório`. Ao contrário do comando `rpm`, o comando `build` procura o arquivo SPEC no diretório de origem. Para construir `wget` (como no exemplo acima) com o DVD montado no sistema em `/media/dvd`, use os comandos seguintes como `root`:

```
cd /usr/src/packages/SOURCES/  
mv ../SPECS/wget.spec .  
build --rpms /media/dvd/suse/ wget.spec
```

Depois disso, um ambiente mínimo é estabelecido em `/var/tmp/build-root`. O pacote é criado nesse ambiente. Após a conclusão, os pacotes resultantes estarão localizados em `/var/tmp/build-root/usr/src/packages/RPMS`.

O script `build` oferece várias opções adicionais. Por exemplo, fazer com que o script prefira seus próprios RPMs, omitir a inicialização do ambiente de construção ou limitar o comando `rpm` a um dos estágios mencionados acima. Acesse informações adicionais com `build --help` e a leitura da página de manual `build`.

5.2.8 Ferramentas para arquivos RPM e banco de dados RPM

O Midnight Commander (`mc`) pode exibir o conteúdo de arquivos RPM e copiar partes deles. Ele representa arquivos como sistemas de arquivos virtuais, oferecendo todas as opções de menu usuais do Midnight Commander. Exiba o `HEADER` com `F3`. Exiba a estrutura de arquivos com as teclas de cursor e `Enter`. Copie componentes de arquivos com `F5`.

O KDE oferece a ferramenta `kpackage` como front end para `rpm`. Um gerenciador de pacotes completo está disponível como um módulo do YaST (consulte o Capítulo 6, *Installing or Removing Software* (↑*Guia de Implantação*)).

Acessando áreas de trabalho remotas com o Nomad

O Nomad (Novell Open Mobile Agile Desktop) é fornecido com o SUSE® Linux Enterprise Desktop e permite que você execute sessões de área de trabalho separadamente de qualquer hardware gráfico. Ele consiste nos seguintes componentes básicos:

Servidor proxy X

Suporta as modernas extensões X, como Composição, XVideo e RANDR.

Gerenciador de Sessão

Responsável pela criação e pelo monitoramento de sessões de área de trabalho que podem ser acessadas remotamente.

Gerenciador de conexões

Usa o RDP (Remote Desktop Protocol) como transporte e camada de segurança. O RDP é um protocolo multicanal que permite ao usuário conectar-se a um computador com os Serviços de Terminal da Microsoft em execução. Entretanto, quando suportado pelo software cliente, o gerenciador de conexões usa um canal X11 virtual (rdpx11) que transfere o tráfego não filtrado do X11 ao servidor X local que exibe a área de trabalho. O gerenciador de conexões pode sempre reverter para os comandos RDP simples quando necessário, o que significa que as áreas de trabalho remotas podem ser acessadas por qualquer cliente RDP existente.

Programa cliente

Um cliente RDP especial é fornecido para o SUSE Linux Enterprise Desktop, o qual implementa extensões específicas do Nomad para o encaminhamento de protocolo X11 e a capacidade de composição de áreas de trabalho remotas

localmente quando os plug-ins apropriados do gerenciador de composições estão carregados.

Extensões do gerenciador de composições

A composição propicia efeitos visuais avançados nas janelas de aplicativos, como transparência, esmaecimento, dimensionamento, contorção, embaralhamento e redirecionamento.

O Nomad permite acessar remotamente as áreas de trabalho a partir de localizações físicas diferentes. Por exemplo, você pode acessar a mesma sessão de casa ou do trabalho. Após uma interrupção da sua sessão de trabalho, basta ir para outro terminal e continuar o trabalho de lá. Também é possível copiar o ambiente em execução atualmente para um dispositivo móvel, como um laptop. Com o Nomad, você também pode compartilhar áreas de trabalho para fins de colaboração ou treinamento, permitindo controlar e administrar remotamente.

Se você tiver efeitos da área de trabalho habilitados, ocorre aceleração gráfica no local do destinatário (máquina em frente à qual você está sentado), pois ele tem acesso direto ao hardware gráfico e de entrada. O remetente está onde a área de trabalho real e seus aplicativos residem (sistema remoto que você está acessando). Esse local pode ser um servidor em um data center, uma instância em uma nuvem ou uma máquina virtual.

6.1 Pré-requisitos do Nomad

Para usar o Nomad, é preciso instalar o pacote `rdesktop` na máquina local. Além disso, os seguintes pacotes podem ser instalados:

- `compiz`
- `compiz-plugins-dmx`
- `compiz-fusion-plugins-main`
- `libcompizconfig`
- `python-compizconfig`
- `compiz-manager`

- `simple-ccsm`
- `tsclient`

Na máquina remota de origem da área de trabalho, é preciso instalar o pacote `xrdp`, que contém um servidor RDP (remote desktop protocol) de código-fonte aberto.

Além disso, os seguintes pacotes podem ser instalados:

- `compiz`
- `compiz-plugins-dmx`
- `compiz-fusion-plugins-main`
- `libcompizconfig`
- `python-compizconfig`
- `compiz-manager`
- `simple-ccsm`

6.2 Instalação e configuração

NOTA: efeitos da área de trabalho

Se você pretende usar efeitos de área de trabalho na área de trabalho remota, verifique se o pacote `compiz-plugins-dmx` está instalado em ambos os sistemas: o sistema de origem da área de trabalho remota e o sistema local que acessa essa área de trabalho remota.

6.2.1 Máquina local

A máquina local que atua como host geralmente não precisa de nenhuma configuração especial. Logo após a instalação do pacote `rdesktop`, você pode usar a ferramenta de linha de comando `rdesktop` para conectar-se à máquina remota de origem da área de

trabalho. Se preferir uma interface gráfica de usuário, instale também o pacote `tsclient`. O `tsclient` (Cliente do Servidor de Terminal) é um front end do GNOME para o `rdesktop` e outras ferramentas de área de trabalho remota, que também suporta clientes Xnest e VNC (`vncviewer`). Para obter um melhor desempenho e efeitos de área de trabalho, instale os pacotes adicionais do `compiz`.

Entretanto, se você estiver usando o KDE, poderá precisar executar primeiro o seguinte comando enquanto `root`:

```
cp /etc/pam.d/xrdp-sesman /etc/pam.d/gdm
```

Caso contrário, o login falhará durante a tentativa de conectar-se à área de trabalho remota.

6.2.2 Máquina remota

No entanto, você deve preparar a máquina remota de origem da área de trabalho, conforme a seguir:

- 1** Instale o pacote `xrdp`. Isso adicionará o servidor `xrpd` automaticamente ao nível de execução 5. Para iniciar ou parar o serviço manualmente, execute `/etc/init.d/xrdp start` ou `/etc/init.d/xrdp stop` enquanto usuário `root`.
- 2** Configure o firewall de modo a permitir conexões na porta 3389, já que ela é usada para conexões RDP. Inicie o YaST e selecione *Segurança e Usuários > Firewall*. Clique em *Serviços Permitidos* e selecione a zona para a qual permitir o serviço. Clique em *Avançado* e digite 3389 como opção de *Porta TCP*. Confirme as configurações no YaST.
- 3** Se você quiser usar efeitos 3D da área de trabalho, instale os pacotes adicionais do `compiz`. Eles aprimoram o desempenho de maneira significativa quando se usa um cliente com suporte a canais virtuais. Quando se habilita efeitos de área de trabalho em ambas as áreas de trabalho (local e remota), o gerenciador de composições local adquire a capacidade de aplicar efeitos aos elementos provenientes da área de trabalho remota.

6.3 Usando o Nomad

Logo que o `xrdp` entrar em execução e a porta 3389 ser aberta na máquina remota, você já pode se conectar ao host remoto com o seu cliente RDP. Para conectar-se, use a ferramenta de linha de comando `rdesktop` ou o `tsclient` de origem de uma interface gráfica de usuário.

6.3.1 Conectando-se ao servidor com `rdesktop`

Para estabelecer uma conexão em modo compactado para o usuário `tux`, execute o seguinte comando de um shell:

```
rdesktop -u tux -z server
```

onde *servidor* é o nome de host ou endereço IP da máquina remota.

Esse comando inicia uma tela de login para o usuário especificado, na qual ele pode efetuar login na área de trabalho remota. As sessões de área de trabalho via `xrdp` são independentes e não entram em conflito com gerenciadores de exibição comuns, como o GDM ou o KDM. Para terminar a conexão, feche a janela de conexão.

Você pode definir algumas opções ao estabelecer a conexão. Por exemplo, você pode usar o modo de tela inteira, escolher um determinado layout de teclado ou ajustar a geometria. Saiba mais sobre as opções disponíveis de `rdesktop` em `rdesktop --help`.

6.3.2 Conectando-se ao servidor com `tsclient`

- 1 Pressione **Alt + F2** e digite `tsclient` para iniciar o front end gráfico de `rdesktop`.
- 2 Clique em *Adicionar Conexão* e selecione *Windows Terminal Service*.
- 3 Em *Host*, especifique o nome de host ou IP da máquina remota à qual você deseja conectar-se no *Host*.

- 4 Se desejar, digite também um *Nome de Usuário* e uma *Senha* com a qual conectar-se à máquina remota.
- 5 Defina as outras opções de acordo com o que você precisa e deseje ou deixe-as com os padrões e confirme as mudanças com *OK* para exibir uma entrada para a conexão recém-especificada.
- 6 Para editar ou remover a conexão, selecione a entrada de conexão e use o menu de contexto ou os respectivos ícones da barra de ferramentas.
- 7 Para iniciar a conexão, clique o botão direito do mouse na entrada da conexão e selecione a respectiva entrada do menu de contexto.

Esse comando inicia uma tela de login para o usuário especificado, na qual ele pode efetuar login na área de trabalho remota. As sessões de área de trabalho via `xrdp` são independentes e não entram em conflito com gerenciadores de exibição comuns, como o GDM ou o KDM.

- 8 Para terminar a conexão, feche a janela de conexão.

6.4 Solução de problemas

Se tiver dificuldades em estabelecer uma conexão, proceda de acordo com a lista a seguir.

O servidor `xrdp` está em funcionamento na máquina remota?

1. Verifique se o pacote `xrdp` está instalado na máquina remota de origem da área de trabalho.
2. Verifique se o serviço `xrdp` está em execução.
3. Se não estiver, inicie-o ou reinicie-o manualmente executando o seguinte comando enquanto usuário `root`: `/etc/init.d/xrdp start` ou `/etc/init.d/xrdp restart`.

Dois processos devem estar em execução após o início do serviço `xrdp`: `xrdp` e `xrdp-sesman`. Se um deles não for iniciado por qualquer motivo, iniciá-los manualmente no primeiro plano provavelmente acusará qual foi a falha.

4. Para iniciar os processos manualmente, torne-se `root` e execute
`/usr/sbin/xrdp-sesman -n e /usr/sbin/xrdp -nodaemon.`
5. Além disso, verifique a saída de `xrdp-sesman` output em `/var/log/xrdp-sesman.log` e a saída de `xrdp` em `/var/log/messages` para obter mais informações.

6.5 Para obter mais informações

Para obter mais informações sobre o Nomad, consulte <http://en.opensuse.org/Nomad>.

Bash e scripts Bash

Atualmente, muitas pessoas usam computadores com uma GUI (interface gráfica de usuário) como KDE ou GNOME. Embora ofereçam muitos recursos, elas ficam com uso limitado quando se trata da execução de tarefas automáticas. Shells são bons aliados das interfaces gráficas, por isso este capítulo apresenta uma visão geral de alguns aspectos dos shells, neste caso, o Bash.

7.1 O que é “o shell”?

Tradicionalmente, *o shell* é o Bash (Bourne again Shell). Quando este capítulo menciona “o shell”, ele se refere ao Bash. Na verdade, existem mais shells disponíveis além do Bash (ash, csh, ksh, zsh, ...), cada um deles empregando recursos e características diferentes. Se você precisar de mais informações sobre outros shells, procure por *shell* no YaST.

7.1.1 Conhecendo os arquivos de configuração do Bash

Um shell pode ser acionado como:

1. shell de login interativo. Esse tipo é usado para efetuar login em uma máquina, chamando o Bash com a opção `--login`, ou para efetuar login em uma máquina remota com SSH.

2. shell interativo “comum”. Normalmente esse é o caso quando se inicia o xterm, o konsole, o gnome-terminal ou ferramentas semelhantes.
3. shell não interativo. Esse tipo é usado para chamar um script shell na linha de comando.

Dependendo do tipo de shell usado, variam os arquivos de configuração lidos. As tabelas seguintes mostram os arquivos de configuração de shell de login e sem login.

Tabela 7.1 *Arquivos de configuração do Bash para shells de login*

Arquivo	Descrição
<code>/etc/profile</code>	Não modifique esse arquivo, senão as suas modificações poderão ser destruídas durante a próxima atualização!
<code>/etc/profile.local</code>	Use esse arquivos se for estender <code>/etc/profile</code>
<code>/etc/profile.d/</code>	Contém arquivos de configuração de programas específicos para todo o sistema
<code>~/.profile</code>	Insira aqui a configuração específica de usuário para os shells de login

Tabela 7.2 *Arquivos de configuração do Bash para shells sem login*

<code>/etc/bash.bashrc</code>	Não modifique esse arquivo, senão as suas modificações poderão ser destruídas durante a próxima atualização!
<code>/etc/bash.bashrc.local</code>	Use esse arquivo para inserir suas modificações apenas do Bash em todo o sistema
<code>~/bashrc</code>	Insira aqui a configuração específica de usuário

Além desses, o Bash usa mais outros arquivos:

Tabela 7.3 Arquivos especiais do Bash

Arquivo	Descrição
<code>~/.bash_history</code>	Contém uma lista de todos os comandos que você digitou
<code>~/.bash_logout</code>	Executado durante o logout

7.1.2 Estrutura de diretórios

A tabela a seguir fornece uma breve visão geral dos mais importantes diretórios de nível superior encontrados em um sistema Linux. Informações mais detalhadas sobre os diretórios e subdiretórios importantes são encontradas na lista a seguir.

Tabela 7.4 Visão geral de uma árvore de diretório padrão

Diretório	Conteúdo
<code>/</code>	Diretório raiz — o ponto de partida da árvore do diretório.
<code>/bin</code>	Arquivos binários essenciais, como comandos necessários pelo administrador do sistema e por usuários comuns. Geralmente contém os shells, como o Bash.
<code>/boot</code>	Arquivos estáticos do carregador de boot.
<code>/dev</code>	Arquivos necessários para acessar dispositivos específicos de host.
<code>/etc</code>	Arquivos de configuração do sistema específicos de host.
<code>/home</code>	Contém os diretórios pessoais de todos os usuários que possuem conta no sistema. Contudo, o diretório pessoal do <code>root</code> não está em <code>/home</code> , ele está em <code>/root</code> .
<code>/lib</code>	Bibliotecas compartilhadas e módulos de kernel essenciais.

Diretório	Conteúdo
<code>/media</code>	Pontos de montagem de mídia removível.
<code>/mnt</code>	Ponto de montagem para montar temporariamente um sistema de arquivos.
<code>/opt</code>	Pacotes de aplicativos complementares.
<code>/root</code>	Diretório pessoal do superusuário <code>root</code> .
<code>/sbin</code>	Binários essenciais do sistema.
<code>/srv</code>	Dados de serviços fornecidos pelo sistema.
<code>/tmp</code>	Arquivos temporários.
<code>/usr</code>	Hierarquia secundária com dados apenas leitura.
<code>/var</code>	Dados variáveis, como arquivos de registro.
<code>/windows</code>	Disponível apenas se você tiver o Microsoft Windows* e o Linux instalados no sistema. Contém os dados do Windows.

A lista a seguir fornece informações mais detalhadas e alguns exemplos de arquivos e subdiretórios encontrados nos diretórios:

`/bin`

Contém comandos básicos do shell que podem ser usados pelo `root` e por outros usuários. Esses comandos incluem `ls`, `mkdir`, `cp`, `mv`, `rm` e `rmdir`. `/bin` também contém o Bash, que é o shell padrão do SUSE Linux Enterprise Desktop.

`/boot`

Contém dados necessários para inicializar, como o carregador de boot, o kernel e outros dados usados para que o kernel possa executar programas em modo de usuário.

`/dev`

Contém arquivos de dispositivos que representam componentes de hardware.

`/etc`

Contém arquivos de configuração local que controlam a operação de programas como o X Window System. O subdiretório `/etc/init.d` contém scripts que são executados durante o processo de boot.

`/home/nome_do_usuario`

Contém os dados privados de todos os usuários que possuem uma conta no sistema. Os arquivos localizados aqui apenas podem ser modificados por seu proprietário ou pelo administrador do sistema. Por padrão, seu diretório de e-mail e sua configuração de área de trabalho pessoal estão localizados aqui, na forma de arquivos e diretórios ocultos. Usuários do KDE encontram os dados de configuração pessoal da área de trabalho em `.kde` ou `.kde4`. Os usuários do GNOME os encontram em `.gconf`.

NOTA: diretório pessoal em um ambiente de rede

Se você estiver trabalhando em um ambiente de rede, seu diretório pessoal poderá ser mapeado para um diretório no sistema de arquivos diferente de `/home`.

`/lib`

Contém as bibliotecas compartilhadas essenciais necessárias para inicializar o sistema e executar os comandos no sistema de arquivos raiz. O equivalente no Windows para as bibliotecas compartilhadas são os arquivos DLL.

`/media`

Contém pontos de montagem para mídia removível, como CD-ROMs, cartões USB e câmeras digitais (se usarem USB). `/media` geralmente mantém qualquer tipo de unidade, exceto o disco rígido do seu sistema. Assim que a mídia removível for inserida ou conectada no sistema e estiver montada, você poderá acessá-la a partir daqui.

`/mnt`

O diretório fornece um ponto de montagem para um sistema de arquivos montado temporariamente. O `root` pode montar os sistemas de arquivos aqui.

`/opt`

Reservado para a instalação de software adicional. Software opcional e pacotes de programas complementares maiores são encontrados aqui. O KDE3 fica localizado aqui, ao passo que o KDE4 e o GNOME agora ficam em `/usr`.

`/root`

Diretório pessoal do usuário `root`. Os dados pessoais do `root` estão localizados aqui.

`/sbin`

Como indicado pelo `s`, esse diretório contém utilitários do superusuário. `/sbin` contém os binários essenciais para boot, restauração e recuperação do sistema, além dos binários em `/bin`.

`/srv`

Contém dados de serviços fornecidos pelo sistema, como FTP e HTTP.

`/tmp`

Esse diretório é usado por programas que exigem o armazenamento temporário dos arquivos.

`/usr`

`/usr` não tem relação com os usuários, trata-se de um acrônimo de recursos de sistema do UNIX. Os dados em `/usr` são estáticos e apenas leitura, podendo ser compartilhados entre vários hosts em conformidade com o FHS (Filesystem Hierarchy Standard - Padrão da Hierarquia do Sistema de Arquivos). Esse diretório contém todos os programas aplicativos e estabelece uma segunda hierarquia no sistema de arquivos. O KDE4 e o GNOME também estão localizados aqui. `/usr` contém alguns subdiretórios como `/usr/bin`, `/usr/sbin`, `/usr/local` e `/usr/share/doc`.

`/usr/bin`

Contém programas geralmente acessíveis.

`/usr/bin`

Contém programas reservados ao administrador do sistema, como as funções de reparo.

`/usr/local`

Nesse diretório, o administrador do sistema pode instalar extensões locais e independentes de distribuição.

`/usr/share/doc`

Contém vários arquivos de documentação e as notas de versão do sistema. No subdiretório `manual`, você encontra uma versão online deste manual. Se houver mais de um idioma instalado, esse diretório poderá conter versões dos manuais em idiomas diferentes.

Em `packages`, você encontra a documentação incluída nos pacotes de software instalados no sistema. Para cada pacote, é criado um subdiretório `/usr/share/doc/packages/nome_do_pacote`, geralmente contendo arquivos `README` do pacote e, por vezes, exemplos, arquivos de configuração ou scripts adicionais.

Se houver `HOWTO`s instalados no sistema, `/usr/share/doc` também conterá o subdiretório `howto`, com documentação adicional sobre muitas tarefas relacionadas a configuração e operação do software Linux.

`/var`

Ao passo que `/usr` contém dados estáticos apenas leitura, `/var` destina-se aos dados gravados durante a operação do sistema, portanto variáveis, como arquivos de registro ou de spool. Para obter uma visão geral dos arquivos de registro mais importantes que estão em `/var/log/`, consulte a Tabela 28.1, “Arquivos de registro” (p 376).

`/windows`

Disponível apenas se você tiver o Microsoft Windows e o Linux instalados no sistema. Contém os dados do Windows disponíveis na partição Windows do sistema. A sua capacidade de editar dados nesse diretório depende do sistema de arquivos usado pelas partições Windows. No caso do FAT32, você pode abrir e editar os arquivos desse diretório. No caso de NTFS, o SUSE Linux Enterprise Desktop também inclui suporte ao acesso de gravação. Porém, o driver do sistema de arquivos NTFS-3g possui funcionalidade limitada.

7.2 Gravando scripts shell

Scripts shell são convenientes para todos os tipos de tarefas: coleta de dados, pesquisa por uma palavra ou frase em um texto e muitas outras coisas úteis. O exemplo seguinte mostra um pequeno script shell que imprime um texto:

Exemplo 7.1 *Um script shell que imprime um texto*

```
#!/bin/sh ❶  
# Output the following line: ❷  
echo "Hello World" ❸
```

- ❶ A primeira linha começa com os caracteres *Shebang* (`#!`), indicando que o arquivo é um script. O script é executado pelo interpretador especificado após o Shebang, neste caso, `/bin/sh`.
- ❷ A segunda linha é um comentário que começa com o sinal de hash. Ele é recomendado para inserir comentário em linhas cuja função é difícil de lembrar.
- ❸ A terceira linha usa o comando interno `echo` para imprimir o texto correspondente.

Antes de executar esse script, você precisa de alguns pré-requisitos:

1. Todo script deve conter uma linha Shebang (como foi o caso do nosso exemplo acima). Se um script não tiver essa linha, você deverá chamar o interpretador manualmente.
2. Grave o script no lugar desejado. Contudo, convém gravá-lo em um diretório onde o shell possa encontrá-lo. O caminho de pesquisa em um shell é determinado pela variável de ambiente `PATH`. Um usuário normal geralmente não tem acesso de gravação em `/usr/bin`. Por essa razão, recomenda-se gravar seus scripts no diretório `~/bin/` dos usuários. O exemplo acima leva o nome `hello.sh`.
3. O script requer permissões de executável. Defina as permissões com o seguinte comando:

```
chmod +x ~/bin/hello.sh
```

Se você atendeu a todos os pré-requisitos acima, poderá executar o script das seguintes maneiras:

1. **Como caminho absoluto** O script pode ser executado em um caminho absoluto. No nosso caso, ele é `~/bin/hello.sh`.
2. **Em todos os lugares** Se a variável de ambiente `PATH` contiver o diretório onde o script está localizado, você poderá executar o script apenas com `hello.sh`.

7.3 Redirecionando eventos de comando

Cada comando pode usar três canais, seja para entrada ou para saída:

- **Saída padrão** Esse é o canal de saída padrão. Sempre que um comando imprime algo, ele usa o canal de saída padrão.
- **Entrada padrão** Se um comando precisar da entrada dos usuários ou de outros comandos, ele usará esse canal.
- **Erro padrão** Os comandos usam esse canal para gerar relatórios de erros.

Para redirecionar os canais, as possibilidades são as seguintes:

Comando > Arquivo

Grava a saída do comando em um arquivo, apagando um arquivo existente. Por exemplo, o comando `ls` grava sua saída no arquivo `listing.txt`:

```
ls > listing.txt
```

Comando >> Arquivo

Anexa a saída do comando a um arquivo. Por exemplo, o comando `ls` anexa sua saída ao arquivo `listing.txt`:

```
ls >> listing.txt
```

Comando < Arquivo

Lê o arquivo como entrada do comando em questão. Por exemplo, o comando `read` extrai o conteúdo do arquivo para a variável:

```
read a < foo
```

Comando1 | Comando2

Redireciona a saída do comando à esquerda como entrada para o comando à direita.

Por exemplo, o comando `cat` gera a saída do conteúdo do arquivo `/proc/cpuinfo`. Essa saída é usada por `grep` para filtrar apenas as linhas que contêm `cpu`:

```
cat /proc/cpuinfo | grep cpu
```

Cada canal possui um *descriptor de arquivo*: 0 (zero) para entrada padrão, 1 para saída padrão e 2 para erro padrão. É permitido inserir esse descriptor de arquivo antes de um caractere `<` ou `>`. Por exemplo, a linha a seguir procura por um arquivo que começa com `foo`, mas suprime seus erros redirecionando-o para `/dev/null`:

```
find / -name "foo*" 2>/dev/null
```

7.4 Usando aliases

Um alias é uma definição de atalho de um ou mais comandos. A sintaxe de um alias é a seguinte:

```
alias NAME=DEFINITION
```

Por exemplo, a linha a seguir define um alias `lt` que gera uma listagem extensa (opção `-l`), classifica-a por horário de modificação (`-t`) e imprime-a em ordem inversa ao classificar (`-r`):

```
alias lt='ls -ltr'
```

Para ver todas as definições de alias, use `alias`. Remova o seu alias com `unalias` e o nome de alias correspondente.

7.5 Usando variáveis no Bash

Uma variável de shell pode ser global ou local. Variáveis globais, ou de ambiente, podem ser acessadas em todos os shells. As variáveis locais, ao contrário, são visíveis apenas no shell atual.

Para ver todas as variáveis de ambiente, use o comando `printenv`. Se for preciso saber o valor de uma variável, insira o nome da variável como argumento:

```
printenv PATH
```

Uma variável, seja ela global ou local, também pode ser visualizada com `echo`:

```
echo $PATH
```

Para definir uma variável local, use um nome de variável, seguido pelo sinal de igual, seguido pelo valor:

```
PROJECT="SLED"
```

Não insira espaços antes e depois do sinal de igual, senão você obterá um erro. Para definir uma variável de ambiente, use `export`:

```
export NAME="tux"
```

Para remover uma variável, use `unset`:

```
unset NAME
```

A tabela a seguir contém algumas variáveis de ambiente comuns que podem ser usadas nos seus scripts shell:

Tabela 7.5 *Variáveis de ambiente úteis*

HOME	diretório pessoal do usuário atual
HOST	nome do host atual
LANG	quando uma ferramenta é localizada, ela usa o idioma dessa variável de ambiente. Também é possível definir o idioma inglês como C
PATH	caminho de pesquisa do shell, uma lista de diretórios separados por dois-pontos
PS1	especifica o prompt normal impresso antes de cada comando
PS2	especifica o prompt secundário impresso quando você executa um comando em várias linhas
PWD	diretório de trabalho atual

7.5.1 Usando variáveis de argumento

Por exemplo, se você tiver o script `foo.sh`, poderá executá-lo desta maneira:

```
foo.sh "Tux Penguin" 2000
```

Para acessar todos os argumentos que são passados ao seu script, você precisa de parâmetros de posição. Isto é, `$1` para o primeiro argumento, `$2` para o segundo e assim sucessivamente. É possível usar até nove parâmetros. Para obter o nome do script, use `$0`.

O script `foo.sh` a seguir imprime todos os argumentos de 1 a 4:

```
#!/bin/sh
echo \"$1\" \"$2\" \"$3\" \"$4\"
```

Se você executar esse script com os argumentos acima, obterá:

```
"Tux Penguin" "2000" "" ""
```

7.5.2 Usando substituição de variável

As substituições de variáveis aplicam um padrão ao conteúdo de uma variável, seja da esquerda ou da esquerda. A lista a seguir contém as formas de sintaxe possíveis:

`${VAR#padrão}`

remove a correspondência mais curta possível da esquerda:

```
file=/home/tux/book/book.tar.bz2
echo ${file#*/}
home/tux/book/book.tar.bz2
```

`${VAR##padrão}`

remove a correspondência mais longa possível da esquerda:

```
file=/home/tux/book/book.tar.bz2
echo ${file##*/}
book.tar.bz2
```

```
${VAR%padrão}
```

remove a correspondência mais curta possível da direita:

```
file=/home/tux/book/book.tar.bz2
echo ${file%.*}
/home/tux/book/book.tar
```

```
${VAR%%padrão}
```

remove a correspondência mais longa possível da direita:

```
file=/home/tux/book/book.tar.bz2
echo ${file%%.*}
/home/tux/book/book
```

```
${VAR/padrão_1/padrão_2}
```

substitui o conteúdo de *VAR* do *padrão_1* pelo do *padrão_2*:

```
file=/home/tux/book/book.tar.bz2
echo ${file/tux/wilber}
/home/wilber/book/book.tar.bz2
```

7.6 Agrupando e combinando comandos

Os shells permitem concatenar e agrupar comandos para uma execução condicional. Cada comando retorna um código de saída que determina o sucesso ou a falha de sua operação. Se o código for 0 (zero), significa que o comando obteve sucesso. Todos os outros códigos significam erro específico do comando.

A lista a seguir mostra como os comandos podem ser agrupados:

`Comando1 ; Comando2`

executa os comandos em seqüência. O código de saída não é verificado. A linha a seguir exibe o conteúdo do arquivo com `cat` e depois imprime suas propriedades com `ls`, independentemente dos códigos de erro:

```
cat filelist.txt ; ls -l filelist.txt
```

`Comando1 && Comando2`

executa o comando à direita quando o comando à esquerda for bem-sucedido (E lógico). A linha a seguir exibe o conteúdo do arquivo e imprime suas propriedades

apenas quando o comando anterior obtiver sucesso (compare com a entrada anterior nesta lista):

```
cat filelist.txt && ls -l filelist.txt
```

Comando1 || Comando2

executa o comando à direita quando o comando da esquerda falhar (OU lógico). A linha a seguir cria um diretório em `/home/wilber/bar` apenas quando a criação do diretório em `/home/tux/foo` falhar:

```
mkdir /home/tux/foo || mkdir /home/wilber/bar
```

```
nome_da_função() { ... }
```

cria uma função shell. Você pode usar os parâmetros de posição para acessar seus argumentos. A linha a seguir define a função `hello` para imprimir uma mensagem curta:

```
hello() { echo "Hello $1"; }
```

Você pode chamar essa função assim:

```
hello Tux
```

que imprimirá:

```
Hello Tux
```

7.7 Trabalhando com construções de fluxo comuns

Para controlar o fluxo do seu script, um shell possui as construções `while`, `if`, `for` e `case`.

7.7.1 Comando de controle if

O comando `if` é usado para verificar expressões. Por exemplo, o código a seguir testa se o usuário atual é Tux:

```
if test $USER = "tux"; then
    echo "Hello Tux."
else
```

```
    echo "You are not Tux."
fi
```

A expressão de teste pode ser tão complexa ou simples quanto possível. a expressão a seguir verifica se o arquivo `foo.txt` existe:

```
if test -e /tmp/foo.txt ;
then
    echo "Found foo.txt"
fi
```

A expressão de teste também pode ser abreviada entre colchetes:

```
if [ -e /tmp/foo.txt ] ; then
    echo "Found foo.txt"
fi
```

Outras expressões úteis estão disponíveis em <http://www.cyberciti.biz/nixcraft/linux/docs/uniqlinuxfeatures/lsst/ch03sec02.html>.

7.7.2 Criando loops com o comando for

O loop `for` permite executar comandos para uma lista de entradas. Por exemplo, o código a seguir imprime algumas informações sobre arquivos PNG no diretório atual:

```
for i in *.png; do
    ls -l $i
done
```

7.8 Para obter mais informações

Informações importantes sobre o Bash são fornecidas nas páginas de manual de `man sh`. Mais informações sobre este tópico estão disponíveis na lista a seguir:

- <http://tldp.org/LDP/Bash-Beginners-Guide/html/index.html> — Bash Guide for Beginners (Guia do Bash para Iniciantes)
- <http://tldp.org/HOWTO/Bash-Prog-Intro-HOWTO.html> — BASH Programming - Introduction HOW-TO (Como Fazer Programação de Bash - Introdução)

- <http://tldp.org/LDP/abs/html/index.html> — Advanced Bash-Scripting Guide (Guia de Script Bash Avançado)
- <http://www.grymoire.com/Unix/Sh.html> — Sh - the Bourne Shell (Sh - o Bourne Shell)

Parte II. Sistema

Aplicativos de 32 bits e 64 bits em um ambiente de sistema de 64 bits

8

O SUSE® Linux Enterprise Desktop está disponível para plataformas de 64 bits. Isso não significa necessariamente que todos os aplicativos incluídos tenham sido transpostos para plataformas de 64 bits. O SUSE Linux Enterprise Desktop suporta o uso de aplicativos de 32 bits em um ambiente de 64 bits. Este capítulo oferece uma breve visão geral de como esse suporte é implementado em plataformas de 64 bits do SUSE Linux Enterprise Desktop. Ele explica como aplicativos de 32 bits são executados (suporte do tempo de execução) e como aplicativos de 32 bits devem ser compilados para que possam ser executados em ambientes de sistema de 32 bits e 64 bits. Além disso, você encontrará informações sobre a API do kernel e uma explicação sobre como os aplicativos de 32 bits podem ser executados em um kernel de 64 bits.

O SUSE Linux Enterprise Desktop para as plataformas de 64 bits amd64 e Intel 64 foi projetado para que os aplicativos existentes de 32 bits sejam executados no ambiente de 64 bits “imediatamente.” Este suporte significa que você pode continuar a usar os aplicativos de 32 bits de sua preferência sem esperar que uma porta de 64 bits correspondente se torne disponível.

8.1 Suporte ao tempo de execução

IMPORTANTE: conflitos entre versões de aplicativos

Se um aplicativo estiver disponível para ambientes de 32 bits e de 64 bits, a instalação paralela das duas versões provavelmente resultará em problemas. Em tais casos, opte pela instalação e pelo uso de uma das duas versões.

Uma exceção a essa regra é o PAM (módulo de autenticação conectável). O SUSE Linux Enterprise Desktop usa o PAM no processo de autenticação como uma camada que atua como mediador entre o usuário e o aplicativo. Em um sistema operacional de 64 bits que também executa aplicativos de 32 bits, é necessário sempre instalar as duas versões de um módulo PAM.

Para que os aplicativos sejam executados corretamente, cada um deles requer uma variedade de bibliotecas. Infelizmente, os nomes das versões de 32 bits e 64 bits das bibliotecas são idênticos. Eles devem ser diferenciados uns dos outros de outra forma.

Para obter compatibilidade com a versão de 32 bits, as bibliotecas são armazenadas no mesmo local no sistema e no ambiente de 32 bits. A versão de 32 bits de `libc.so.6` está localizada em `/lib/libc.so.6` nos ambientes de 32 bits e 64 bits.

Todos os arquivos de objetos e todas as bibliotecas de 64 bits estão localizados em diretórios denominados `lib64`. Os arquivos de objeto de 64 bits que normalmente são encontrados em `/lib` e em `/usr/lib`, agora estão em `/lib64` e em `/usr/lib64`. Isso significa que há espaço para as bibliotecas de 32 bits em `/lib` e em `/usr/lib`, permitindo que o nome de arquivo de ambas as versões permaneça sem mudanças.

Os subdiretórios dos diretórios `/lib` de 32 bits com conteúdo de dados que não depende do tamanho do texto não são movidos. Este esquema está em conformidade com a LSB (Linux Standards Base - Base de Padrões Linux) e com o FHS (File System Hierarchy Standard - Padrão de Hierarquia de Sistema de Arquivos).

8.2 Desenvolvimento de software

Uma cadeia de ferramentas de desenvolvimento biarch permite a geração de objetos de 32 bits e 64 bits. O padrão é compilar objetos de 64 bits. É possível gerar objetos de 32 bits usando sinalizadores especiais. Para GCC, o sinalizador especial é `-m32`.

Todos os arquivos de cabeçalho devem ser escritos em um formato independente de arquitetura. As bibliotecas de 32 bits e 64 bits instaladas devem ter uma API (application programming interface - interface de programação de aplicativo) que corresponda aos arquivos de cabeçalho instalados. O ambiente normal do SUSE Linux Enterprise Desktop foi projetado de acordo com esse princípio. No caso de bibliotecas atualizadas manualmente, solucione esses problemas por conta própria.

8.3 Compilação de software em plataformas biarch

Para desenvolver binários para outra arquitetura em uma arquitetura biarch, as respectivas bibliotecas da segunda arquitetura devem ser instaladas adicionalmente. Esses pacotes são chamados de `rpmname-32bit`. Você também precisará dos respectivos cabeçalhos e bibliotecas dos pacotes `rpmname-devel` e das bibliotecas de desenvolvimento para a segunda arquitetura de `rpmname-devel-32bit`.

A maioria dos programas de código-fonte aberto usa uma configuração de programa baseada em `autoconf`. Para usar o `autoconf` com o objetivo de configurar um programa para a segunda arquitetura, sobregrave as configurações do compilador normal e do linker de `autoconf` executando o script `configure` com variáveis de ambiente adicionais.

O exemplo a seguir refere-se a um sistema `x86_64`, cuja segunda arquitetura é `x86`.

- 1 Use o compilador de 32 bits:

```
CC="gcc -m32"
```

- 2 Instrua o linker a processar objetos de 32 bits (use sempre `gcc` como o front end do linker):

```
LD="gcc -m32"
```

3 Defina o assembler para gerar objetos de 32 bits:

```
AS="gcc -c -m32"
```

4 Especifique flags do linker, como o local das bibliotecas de 32 bits, por exemplo:

```
LD_FLAGS="-L/usr/lib"
```

5 Especifique o local das bibliotecas de código objeto de 32 bits:

```
--libdir=/usr/lib
```

6 Especifique o local das bibliotecas X de 32 bits:

```
--x-libraries=/usr/lib
```

Nem todas essas variáveis são necessárias para todos os programas. Adapte-as para o respectivo programa.

```
CC="gcc -m32"
LD_FLAGS="-L/usr/lib;"
./configure --prefix=/usr --libdir=/usr/lib --x-libraries=/usr/lib
make
make install
```

8.4 Especificações do kernel

Os kernels de 64 bits para o x86_64 oferecem uma ABI (interface binária de aplicativo) para kernel de 64 bits e de 32 bits. A de 64 bits é idêntica à ABI do kernel de 32 bits correspondente. Isso significa que o aplicativo de 32 bits pode se comunicar com o kernel de 64 bits da mesma forma que com o kernel de 32 bits.

A emulação de 32 bits de chamadas do sistema para um kernel de 64 bits não suporta todas as APIs usadas pelos programas do sistema. Isso depende da plataforma. Por isso, alguns poucos aplicativos, como o `lspci`, precisam ser compilados.

Um kernel de 64 bits só pode carregar módulos de kernel de 64 bits especificamente compilados para esse kernel. Não é possível usar módulos de kernel de 32 bits.

DICA

Alguns aplicativos requerem módulos separados carregáveis pelo kernel. Se você pretende usar um aplicativo de 32 bits desse tipo em um ambiente de sistema de 64 bits, contate o provedor do aplicativo e a Novell para verificar se a versão de 64 bits do módulo carregável pelo kernel e a versão compilada de 32 bits da API do kernel estão disponíveis para esse módulo.

Inicializando e configurando um sistema Linux

9

O boot de um sistema Linux envolve componentes diferentes. O próprio hardware é inicializado pelo BIOS, que inicia o kernel através de um carregador de boot. Depois disso, o processo de boot com init e os níveis de execução é totalmente controlado pelo sistema operacional. O conceito de nível de execução permite que você mantenha configurações para uso diário, e também execute tarefas de manutenção no sistema.

9.1 Processo de boot do Linux

O processo de boot do Linux consiste em vários estágios, cada um deles representado por um componente diferente. A lista a seguir resume o processo de boot e apresenta todos os principais componentes envolvidos.

1. **BIOS** Após ligar o computador, o BIOS inicializa a tela e o teclado e testa a memória principal. Até esse estágio, a máquina não acessa nenhuma mídia de armazenamento em massa. Em seguida, as informações sobre a data e o horário atuais e sobre os periféricos mais importantes são carregadas dos valores do CMOS. Quando o primeiro disco rígido e sua geometria são reconhecidos, o controle do sistema passa do BIOS para o carregador de boot.
2. **Carregador de boot** O primeiro setor de dados físico de 512 bytes do primeiro disco rígido é carregado na memória principal e o *carregador de boot* existente no início desse setor assume o controle. Os comandos executados pelo carregador de boot determinam a parte restante do processo de boot. Desse modo, os primeiros 512 bytes do primeiro disco rígido são chamados de MBR (*Master Boot Record*). O carregador de boot passa o controle para o sistema operacional real, nesse caso,

o kernel Linux. Mais informações sobre o GRUB, o carregador de boot do Linux, podem ser encontradas no Capítulo 10, *O carregador de boot GRUB* (p 105).

3. **Kernel e initramfs** Para passar o controle do sistema, o carregador de boot carrega na memória o kernel e um sistema de arquivos inicial baseado em RAM (initramfs). O conteúdo do initramfs pode ser usado diretamente pelo kernel. O initramfs contém um pequeno executável chamado init que trata a montagem do sistema de arquivos raiz real. Se forem necessários drivers de hardware especiais antes de o armazenamento em massa ser acessado, eles deverão estar em initramfs. Para obter mais informações sobre o initramfs, consulte a Seção 9.1.1, “initramfs” (p 88).
4. **init no initramfs** Este programa executa todas as ações necessárias para montar o sistema de arquivos raiz adequado, por exemplo, fornecer a funcionalidade de kernel para o sistema de arquivos e os drivers de dispositivo necessários aos controladores de armazenamento em massa com udev. Uma vez encontrado o sistema de arquivos raiz, ele é verificado quanto a erros e montado. Se esse procedimento for bem-sucedido, o initramfs será limpo e o programa init no sistema de arquivos raiz será executado. Para obter mais informações sobre o init, consulte a Seção 9.1.2, “init no initramfs” (p 89). Há mais informações a respeito do udev no Capítulo 13, *Gerenciamento de dispositivo de kernel dinâmico com udev* (p 163).
5. **init** O init realiza o boot do sistema através de diversos níveis, oferecendo funcionalidades diferentes. Ele é descrito na Seção 9.2, “O processo init” (p 91).

9.1.1 initramfs

initramfs é um pequeno arquivo cpio que pode ser carregado pelo kernel em um disco RAM. Ele fornece um ambiente Linux mínimo que permite a execução de programas antes da montagem do sistema de arquivos raiz. Esse ambiente é carregado na memória pelas rotinas de BIOS e não têm requisitos de hardware específicos, além de memória suficiente. O initramfs deve sempre fornecer um executável chamado init que deve executar o programa init no sistema de arquivos raiz para a continuação do processo de boot.

Antes da montagem do sistema de arquivos raiz e da inicialização do sistema operacional, o kernel precisa dos drivers correspondentes para acessar o dispositivo em que o sistema de arquivos raiz está localizado. Esses drivers podem incluir drivers especiais para determinados tipos de unidades de disco rígido ou até drivers de rede para acesso a um

sistema de arquivos de rede. Os módulos necessários para o sistema de arquivos raiz podem ser carregados pelo `init` no `initramfs`. Depois de carregados os módulos, o `udev` fornecerá os dispositivos necessários ao `initramfs`. Posteriormente no processo de boot, depois de mudar o sistema de arquivos raiz, será necessário gerar novamente os dispositivos. Isso é feito através de `boot .udev` com o comando `udevtrigger`.

Se você precisar mudar o hardware (por exemplo, discos rígidos) em um sistema instalado e esse hardware necessitar da existência de diversos drivers no kernel durante o boot, será necessário atualizar o `initramfs`. Para isso, basta chamar `mkinitrd`, o que também era feito no `initrd`, predecessor do `initramfs`. A chamada de `mkinitrd` sem argumentos cria um `initramfs`. A chamada de `mkinitrd` cria um `initrd`. No SUSE® Linux Enterprise Desktop, os módulos a serem carregados são especificados pela variável `INITRD_MODULES` em `/etc/sysconfig/kernel`. Após a instalação, essa variável é definida automaticamente para o valor correto. Os módulos são carregados na mesma ordem em que são exibidos em `INITRD_MODULES`. Isso só é importante quando você depende da configuração correta dos arquivos de dispositivo `/dev/sd ?`. No entanto, em sistemas atuais, também é possível usar os arquivos de dispositivo em `/dev/disk/` que são classificados em vários subdiretórios, chamados `by-id`, `by-path` e `by-uuid`, e que sempre representam o mesmo disco. Isso também é possível na hora da instalação, especificando a respectiva opção de montagem.

IMPORTANTE: atualizando o `initramfs` ou o `initrd`

O carregador de boot carrega o `initramfs` ou `initrd` da mesma maneira que o kernel. Não é necessário reinstalar o GRUB após a atualização do `initramfs` ou `initrd`, pois o GRUB procura o arquivo correto no diretório durante o boot.

9.1.2 `init` no `initramfs`

O principal objetivo do `init` no `initramfs` é preparar a montagem do sistema de arquivos raiz e o acesso a este. Dependendo da configuração do sistema, o `init` será responsável pelas tarefas a seguir.

Carregamento de módulos Kernel

Dependendo da configuração do seu hardware, drivers especiais podem ser necessários para acessar os componentes de hardware do computador (sendo que o componente mais importante é a unidade de disco rígido). Para acessar o sistema

de arquivos raiz final, o kernel precisa carregar os drivers adequados do sistema de arquivos.

Fornecendo arquivos especiais de bloco

Para cada módulo carregado, o kernel gera eventos de dispositivo. udev gerencia esses eventos e gera os arquivos especiais de bloco em um sistema de arquivos em RAM em `/dev`. Sem esses arquivos especiais, o sistema de arquivos e outros dispositivos não estariam acessíveis.

Gerenciamento de configurações RAID e LVM

Se você tiver configurado o sistema para armazenar o sistema de arquivos raiz no RAID ou no LVM, o init configurará o LVM ou o RAID para permitir acesso posterior ao sistema de arquivos raiz. Obtenha informações sobre RAID e LVM no Capítulo 12, *Advanced Disk Setup* (↑ *Guia de Implantação*).

Gerenciamento de conexões de rede

Se você tiver configurado o sistema para usar um sistema de arquivos raiz montado em rede (via NFS), o init deverá ter certeza de que os drivers de rede corretos foram carregados e de que estejam configurados para permitir acesso ao sistema de arquivos raiz.

Quando o init é chamado durante o boot inicial como parte do processo de instalação, as respectivas tarefas diferem das que foram mencionadas acima:

Localização da mídia de instalação

Quando o processo de instalação é iniciado, a máquina carrega um kernel de instalação e um initrd especial com o instalador do YaST localizado no meio de instalação. O instalador do YaST, executado em um sistema de arquivos em RAM, necessita das informações sobre a localização do meio de instalação para acessá-lo e instalar o sistema operacional.

Inicialização do reconhecimento de hardware e carregamento dos módulos kernel adequados

Como mencionado na Seção 9.1.1, “initramfs” (p 88), o processo de boot inicia com um conjunto mínimo de drivers que pode ser usado com a maioria das configurações de hardware. O init inicia um processo de exploração de hardware que determina o conjunto de drivers adequado para sua configuração de hardware. Os nomes dos módulos necessários ao processo de boot são gravados em `INITRD_MODULES`, localizado em `/etc/sysconfig/kernel`. Esses nomes

são usados para gerar um `initramfs` personalizado que é necessário para inicializar o sistema. Se os módulos não forem necessários para o boot, mas forem para `coldplug`, eles serão gravados em `/etc/sysconfig/hardware/hwconfig-*`. Todos os dispositivos descritos com arquivos de configuração nesse diretório são inicializados durante o processo de boot.

Carregamento do sistema de instalação ou do sistema de recuperação

Assim que o hardware for reconhecido corretamente, os drivers adequados serão carregados, o `udev` criará os arquivos de dispositivos especiais e o `init` iniciará o sistema de instalação com o instalador real do YaST ou o sistema de recuperação.

Iniciando o YaST

Por fim, `init` inicia o YaST, que, por sua vez, inicia a instalação do pacote e a configuração do sistema.

9.2 O processo `init`

O programa `init` tem ID de processo 1. Ele é responsável por inicializar o sistema da maneira necessária. O `init` é iniciado diretamente pelo kernel e resiste ao sinal 9, que normalmente elimina processos. Todos os outros programas são iniciados diretamente pelo `init` ou por um de seus processos-filho.

O `init` é configurado centralmente no arquivo `/etc/inittab` em que os *níveis de execução* são definidos (consulte a Seção 9.2.1, “Níveis de execução” (p 92)). O arquivo também especifica os serviços e os daemons disponíveis em cada um dos níveis de execução. Dependendo das entradas em `/etc/inittab`, vários scripts são executados pelo `init`. Por padrão, o primeiro script iniciado após o boot é o `/etc/init.d/boot`. Após concluída a fase de inicialização do sistema, o nível de execução do sistema muda para o padrão com o script `/etc/init.d/rc`. Para fins de clareza, esses scripts, chamados *scripts `init`*, residem no diretório `/etc/init.d` (consulte a Seção 9.2.2, “Scripts `Init`” (p 94)).

Todo o processo de inicialização e encerramento do sistema é mantido pelo `init`. Desse ponto de vista, o kernel pode ser considerado um processo em segundo plano para manter todos os outros processos e ajustar o horário da CPU e o acesso ao hardware de acordo com as solicitações de outros programas.

9.2.1 Níveis de execução

No Linux, os *níveis de execução* definem como o sistema é iniciado e quais serviços estão disponíveis no sistema em execução. Após o boot, o sistema é iniciado conforme definido em `/etc/inittab` na linha `initdefault`. Normalmente, é 3 ou 5. Consulte a Tabela 9.1, “Níveis de execução disponíveis” (p 92). Como alternativa, é possível especificar o nível de execução durante o boot (adicionando o número do nível de execução no prompt de boot, por exemplo). Os parâmetros que não forem avaliados diretamente pelo próprio kernel serão passados para o `init`. Para inicializar no nível de execução 3, basta adicionar o número 3 ao prompt de boot.

Tabela 9.1 *Níveis de execução disponíveis*

Nível de execução	Descrição
0	Desligamento do sistema
S ou 1	Modo de usuário único
2	Modo multiusuário local sem rede remota (NFS, etc.)
3	Modo multiusuário completo com rede
4	<i>Definido pelo Usuário</i> , não usado a menos que o administrador configure este nível de execução.
5	Modo multiusuário completo com rede e gerenciador de exibição X — KDM, GDM ou XDM
6	Reinicialização do sistema

IMPORTANTE: evite o Nível de execução 2 com uma partição montada via NFS

Você não deverá usar o nível de execução 2 se seu sistema montar uma partição como `/usr` através do NFS. O sistema pode comportar-se de forma inesperada se as bibliotecas ou arquivos de programa estiverem ausentes pois o serviço

NFS não está disponível no nível de execução 2 (modo multiusuário local sem rede remota).

Para mudar os níveis de execução durante a execução do sistema, digite `telinit` e o número correspondente como um argumento. Somente o administrador do sistema pode fazer isso. A lista a seguir resume os comandos mais importantes na área de nível de execução.

`telinit 1` ou `shutdown now`

O sistema muda para o *modo de usuário único*. Esse modo é usado para manutenção do sistema e tarefas de administração.

`telinit 3`

Todos os programas e serviços essenciais (incluindo a rede) são iniciados, e os usuários comuns podem efetuar login e trabalhar no sistema sem um ambiente gráfico.

`telinit 5`

O ambiente gráfico é habilitado. Geralmente um gerenciador de exibição como XDM, GDM ou KDM é iniciado. Se o login automático estiver habilitado, o usuário local será conectado ao gerenciador de janelas pré-selecionado (GNOME ou KDE ou qualquer outro gerenciador de janelas).

`telinit 0` ou `shutdown -h now`

O sistema é desligado.

`telinit 6` ou `shutdown -r now`

O sistema é desligado e, em seguida, reinicializado.

O nível de execução 5 é o nível de execução padrão em todas as instalações padrão do SUSE Linux Enterprise Desktop. É solicitado o login dos usuários com uma interface gráfica ou o usuário padrão está conectado automaticamente.

ATENÇÃO: os erros em `/etc/inittab` podem resultar em uma falha de boot do sistema

Se `/etc/inittab` for danificado, o sistema poderá não ser inicializado adequadamente. Portanto, seja extremamente cuidadoso ao editar `/etc/`

`inittab`. Sempre deixe que o `init` releia `/etc/inittab` com o comando `telinit q` antes de reinicializar a máquina.

Geralmente, há duas situações quando os níveis de execução são mudados. Primeiro, os scripts de parada do nível de execução atual são iniciados, fechando alguns programas essenciais ao nível de execução atual. Em seguida, os scripts do novo nível de execução são iniciados. Na maioria dos casos, vários programas são iniciados. Por exemplo, ocorre o seguinte quando o nível de execução 3 muda para 5:

1. O administrador (`root`) solicita que o `init` mude para um nível de execução diferente digitando `telinit 5`.
2. O `init` verifica o nível de execução atual (`runlevel`) e determina se ele deve iniciar `/etc/init.d/rc` com o novo nível de execução como parâmetro.
3. Agora, `rc` chama os scripts de parada do nível de execução atual para os quais não há script de início no novo nível de execução. Neste exemplo, todos os scripts residem em `/etc/init.d/rc3.d` (o nível de execução antigo era 3) e iniciam com `K`. O número após `K` especifica a ordem de execução dos scripts com o parâmetro `stop`, pois algumas dependências devem ser consideradas.
4. Os scripts do novo nível de execução são os últimos a serem iniciados. Neste exemplo, eles estão em `/etc/init.d/rc5.d` e começam com `S`. Mais uma vez, o número após `S` determina a seqüência de início dos scripts.

Ao mudar para o mesmo nível de execução que o atual, o `init` somente verifica as mudanças em `/etc/inittab` e inicia as etapas adequadas, por exemplo, para iniciar um `getty` em outra interface. A mesma funcionalidade pode ser obtida com o comando `telinit q`.

9.2.2 Scripts Init

Há dois tipos de scripts em `/etc/init.d`:

Scripts executados diretamente pelo `init`

Isso só ocorrerá durante o processo de boot ou se for iniciado um encerramento imediato do sistema (falha de energia ou pressionamento de `Ctrl + Alt + Del` pelo usuário). A execução desses scripts é definida em `/etc/inittab`.

Scripts executados indiretamente pelo `init`

São executados durante a mudança do nível de execução e sempre chamam o script `master /etc/init.d/rc`, que garante a ordem correta dos scripts relevantes.

Todos os scripts estão localizados em `/etc/init.d`. Scripts que são executados durante o boot são chamados através de links simbólicos de `/etc/init.d/boot.d`. Os scripts para mudança do nível de execução são chamados através de links simbólicos em um dos subdiretórios (`/etc/init.d/rc0.d` para `/etc/init.d/rc6.d`). Isso só serve para fins de clareza, além de evitar scripts duplicados se forem usados em vários níveis de execução. Como todos os scripts podem ser executados como de início ou de parada, eles devem entender os parâmetros `start` e `stop`. Os scripts também entendem as opções `restart`, `reload`, `force-reload` e `status`. Essas diversas opções são explicadas na Tabela 9.2, “Opções possíveis do script `init`” (p 95). Os scripts executados diretamente pelo `init` não têm esses links. Eles são executados independentemente do nível de execução, quando necessário.

Tabela 9.2 *Opções possíveis do script `init`*

Opção	Descrição
<code>iniciar</code>	Iniciar serviço.
<code>parar</code>	Interromper serviço.
<code>restart</code>	Se o serviço estiver sendo executado, o pára e o reinicia. Se não estiver, o inicia.
<code>reload</code>	Recarregar a configuração sem parar e reiniciar o serviço.
<code>force-reload</code>	Recarregar a configuração se o serviço suportá-la. Caso contrário, age como se <code>restart</code> tivesse sido ativado.
<code>status</code>	Mostrar o status atual do serviço.

Os links em cada subdiretório específico de nível de execução possibilitam a associação de scripts a diferentes níveis de execução. Durante a instalação ou desinstalação de pacotes, esses links são adicionados e removidos com a ajuda do programa `insserv` (ou

usando `/usr/lib/lsb/install_initd`, que é um script que chama esse programa). Consulte a página de manual `insserv(8)` para obter detalhes.

Todas essas configurações também podem ser mudadas com a ajuda do módulo do YaST. Se precisar verificar o status na linha de comando, use a ferramenta `chkconfig`, descrita na página de manual `chkconfig(8)`.

Veja a seguir uma pequena apresentação dos scripts de boot e de parada iniciados primeiro e por último, respectivamente, bem como uma explicação do script de manutenção.

`boot`

Executado na inicialização do sistema usando diretamente o `init`. É independente do nível de execução escolhido e só é executado uma vez. Nesse momento, os sistemas de arquivos `/proc` e `/dev/pts` são montados e `blogd` (boot logging daemon - daemon de registro de boot) é ativado. Se o sistema for inicializado pela primeira vez após uma atualização ou instalação, a configuração inicial do sistema será iniciada.

O daemon `blogd` é um serviço iniciado por `boot` e `rc` antes de qualquer outro. Ele pára após a conclusão do acionamento das ações por esses scripts (que executam vários subscripts, por exemplo, disponibilizando arquivos especiais de bloco). `blogd` grava qualquer saída de tela no arquivo de registro `/var/log/boot.msg`, mas somente se e quando `/var` for montado como leitura-gravação. Caso contrário, o `blogd` armazenará no buffer todos os dados de tela até que `/var` se torne disponível. Obtenha mais informações sobre o `blogd` na página de manual `blogd(8)`.

O script `boot` também é responsável pela inicialização de todos os scripts em `/etc/init.d/boot.d` cujos nomes começam com `S`. Nesse local, todos os sistemas de arquivos são verificados e os dispositivos de loop são configurados se necessário. O horário do sistema também é definido. Se ocorrer um erro durante a verificação e o reparo automáticos do sistema de arquivos, o administrador do sistema poderá intervir após digitar a senha raiz. O último script executado é `boot.local`.

`boot.local`

Digite aqui comandos adicionais a serem executados no boot antes de mudar para um nível de execução. Ele se assemelha ao `AUTOEXEC.BAT` nos sistemas DOS.

`halt`

Este script é executado somente durante a mudança para o nível de execução 0 ou 6. Aqui, ele é executado como `halt` ou `reboot`. O modo como `halt` é chamado determina se o sistema deve ser encerrado ou reinicializado. Se houver necessidade de comandos especiais durante o encerramento, adicione-os ao script `halt.local`.

`rc`

Este script chama os scripts de parada adequados do nível de execução atual e os scripts de início do nível de execução recém-selecionado. Assim como o script `/etc/init.d/boot`, esse script é chamado de `/etc/inittab` com o nível de execução desejado como parâmetro.

Você pode criar seus próprios scripts e integrá-los facilmente no esquema descrito acima. Para obter instruções sobre como formatar, nomear e organizar scripts personalizados, consulte as especificações do LSB e as páginas de manual de `init`, `init.d`, `chkconfig` e `insserv`. Além disso, consulte as páginas de manual do `startproc` e `killproc`.

ATENÇÃO: scripts init defeituosos podem desligar o seu sistema

Scripts `init` defeituosos podem travar sua máquina. Edite esses scripts com muito cuidado e, se possível, submeta-os a testes detalhados no ambiente multiusuário. Informações úteis sobre scripts `init` são encontradas na Seção 9.2.1, “Níveis de execução” (p 92).

Para criar um script `init` personalizado para determinado programa ou serviço, use o arquivo `/etc/init.d/skeleton` como gabarito. Grave uma cópia desse arquivo com o novo nome e edite o programa relevante e nomes de arquivos, caminhos e outros detalhes necessários. Você também pode precisar aprimorar o script com suas próprias partes, de modo que os acionamentos corretos sejam feitos pelo procedimento `init`.

O bloco `INIT INFO` na parte superior é uma parte necessária do script e deve ser editada. Consulte o Exemplo 9.1, “Um bloco `INIT INFO` mínimo” (p 98).

Exemplo 9.1 *Um bloco INIT INFO mínimo*

```
### BEGIN INIT INFO
# Provides:          FOO
# Required-Start:    $syslog $remote_fs
# Required-Stop:     $syslog $remote_fs
# Default-Start:     3 5
# Default-Stop:      0 1 2 6
# Description:       Start FOO to allow XY and provide YZ
### END INIT INFO
```

Na primeira linha do bloco `INFO`, após `Provides :`, especifique o nome do programa ou serviço controlado pelo script `init`. Nas linhas `Required-Start :` e `Required-Stop :`, especifique todos os serviços que precisam ser iniciados ou parados antes do próprio serviço ser iniciado ou parado. Essas informações são usadas posteriormente para gerar a numeração dos nomes de script, como encontrada nos diretórios de nível de execução. Depois de `Default-Start :` e `Default-Stop :`, especifique os níveis de execução em que o serviço deve ser iniciado ou parado automaticamente. Por fim, para `Description :`, forneça uma breve descrição do serviço em questão.

Para criar os links dos diretórios de nível de execução (`/etc/init.d/rc?.d/`) para os scripts correspondentes em `/etc/init.d/`, digite o comando `insserv new-script-name`. O programa `insserv` avalia o cabeçalho `INIT INFO` para criar os links necessários para os scripts de início e parada nos diretórios de nível de execução (`/etc/init.d/rc?.d/`). O programa também se encarrega da ordem correta de início e parada para cada nível de execução, incluindo os números necessários nos nomes desses links. Se você preferir uma ferramenta gráfica para criar esses links, use o editor de nível de execução fornecido pelo YaST, conforme descrito na Seção 9.2.3, “Configurando serviços do sistema (nível de execução) com o YaST” (p 99).

Se um script já presente em `/etc/init.d/` precisar ser integrado ao esquema de nível de execução existente, crie os links nos diretórios de nível de execução imediatamente com `insserv` ou habilitando o serviço correspondente no editor de nível de execução do YaST. As mudanças serão aplicadas durante a próxima reinicialização, e o novo serviço será iniciado automaticamente.

Não defina esses links manualmente. Se houver algum erro no bloco `INFO`, surgirão problemas quando `insserv` for executado posteriormente para algum outro serviço. O serviço adicionado manualmente será removido na próxima execução de `insserv` para esse script.

9.2.3 Configurando serviços do sistema (nível de execução) com o YaST

Depois que este módulo do YaST for iniciado com *YaST > Sistema > Serviços do Sistema (Nível de Execução)*, ele exibirá uma visão geral que lista todos os serviços disponíveis e o status atual de cada um deles (desabilitado ou habilitado). Decida se o módulo deve ser usado no *Modo Simples* ou no *Modo de Especialista*. O *Modo Simples* padrão deve ser suficiente na maior parte dos casos. A coluna à esquerda mostra o nome do serviço, a coluna ao centro indica seu status atual e a coluna à direita fornece uma descrição resumida. Para o serviço selecionado, uma descrição mais detalhada é fornecida na parte inferior da janela. Para habilitar um serviço, selecione-o na tabela e, em seguida, selecione *Habilitar*. As mesmas etapas se aplicam para desabilitar um serviço.

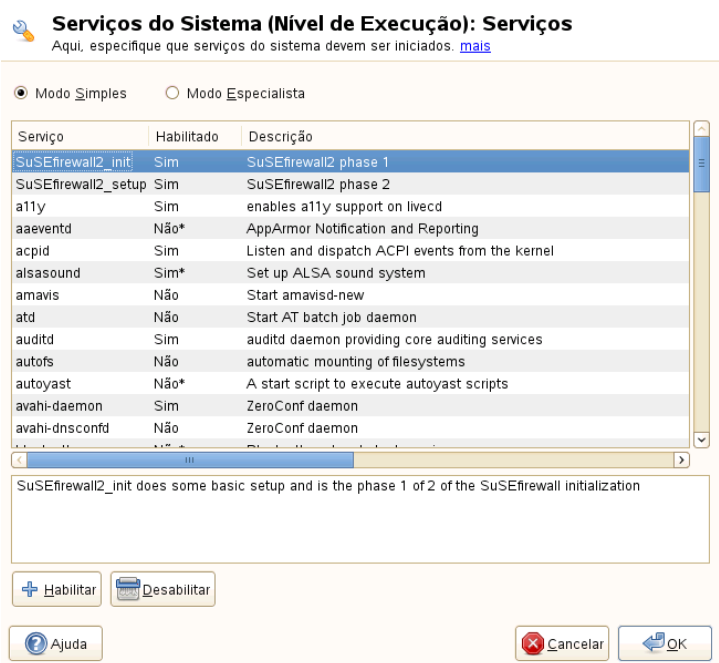
Para ter mais controle sobre os níveis de execução em que um serviço é iniciado ou parado ou para mudar o nível de execução padrão, selecione primeiro *Modo de Especialista*. O nível de execução padrão atual ou o “initdefault” (o nível de execução em que o sistema é inicializado por padrão) é exibido na parte superior. Normalmente, o nível de execução padrão de um sistema SUSE Linux Enterprise Desktop é o 5 (modo multiusuário completo com rede e X). Uma alternativa adequada poderia ser o nível de execução 3 (modo multiusuário completo com rede).

Esta caixa de diálogo do YaST permite a seleção de um dos níveis de execução (conforme listado na Tabela 9.1, “Níveis de execução disponíveis” (p 92)) como o novo padrão. Além disso, use a tabela mostrada nessa janela para habilitar ou desabilitar serviços e daemons individuais. A tabela lista os serviços e daemons disponíveis, mostra se eles estão habilitados no sistema e, se estiverem, para quais níveis de execução. Após selecionar uma das linhas com o mouse, clique nas caixas de seleção que representam os níveis de execução (*B*, *0*, *1*, *2*, *3*, *5*, *6* e *S*) para definir os níveis de execução em que o serviço ou daemon selecionado deve estar em execução. O nível de execução 4 é indefinido para permitir a criação de um nível de execução personalizado. Uma breve descrição do serviço ou daemon selecionado no momento é fornecida abaixo da visão geral da tabela.

ATENÇÃO: Configurações de nível de execução defeituosas podem danificar o sistema

Configurações de nível de execução defeituosas podem tornar o sistema inutilizável. Antes de aplicar as mudanças, tenha absoluta certeza sobre suas conseqüências.

Figura 9.1 *Serviços do Sistema (Nível de Execução)*



Com *Iniciar*, *Parar* ou *Atualizar*, decida se um serviço deve ser ativado. *Situação da Renovação* verifica o status atual. *Inicializar/Reinicializar* permite selecionar se você deseja aplicar as mudanças ao sistema ou restaurar as configurações existentes antes de inicializar o editor de nível de execução. A seleção de *Concluir* grava no disco as configurações mudadas.

9.3 Configuração do sistema via `/etc/sysconfig`

A configuração principal do SUSE Linux Enterprise Desktop é controlada pelos arquivos de configuração em `/etc/sysconfig`. Os arquivos individuais em `/etc/sysconfig` são lidos somente pelos scripts para os quais são relevantes. Isso garante que as configurações de rede, por exemplo, somente precisem ser analisadas pelos scripts relacionados à rede.

Há duas maneiras de editar a configuração do sistema. Use o Editor `sysconfig` do YaST ou edite os arquivos de configuração manualmente.

9.3.1 Mudando a configuração do sistema com o Editor `sysconfig` do YaST

O editor `sysconfig` do YaST fornece um front end fácil de usar para a configuração do sistema. Quando não souber a localização real da variável de configuração que precisa ser mudada, você pode apenas usar a função de pesquisa interna desse módulo, mudar o valor dessa variável conforme necessário e permitir que o YaST se encarregue de aplicar essas mudanças atualizando as configurações que dependem dos valores definidos no `sysconfig` e reiniciando os serviços.

ATENÇÃO: a modificação dos arquivos `/etc/sysconfig/*` pode danificar a instalação

Não modifique os arquivos `/etc/sysconfig` se você não tiver experiência e conhecimento prévios. Isso pode causar sérios danos ao sistema. Os arquivos em `/etc/sysconfig` contêm um pequeno comentário sobre cada variável para explicar seu efeito real.

Figura 9.2 Configuração do sistema usando o Editor sysconfig



A caixa de diálogo do sysconfig do YaST é dividida em três partes. A parte esquerda mostra uma tela de árvore de todas as variáveis configuráveis. Quando você seleciona uma variável, a parte direita exibe a seleção e a definição atuais dessa variável. Abaixo, uma terceira janela exibe uma descrição resumida da finalidade da variável, os valores possíveis, o valor padrão e o arquivo de configuração do qual essa variável se origina. A caixa de diálogo também fornece informações sobre qual script de configuração é executado após a mudança da variável e qual novo serviço é iniciado como resultado da mudança. O YaST solicita a confirmação das mudanças e informa quais scripts serão executados depois que você sair da caixa de diálogo selecionando *Concluir*. Além disso, selecione os serviços e scripts que devem ser ignorados agora e iniciados mais tarde. O YaST aplica todas as mudanças automaticamente e reinicia os serviços envolvidos para que as mudanças sejam efetivadas.

9.3.2 Mudando manualmente a configuração do sistema

Para mudar manualmente a configuração do sistema, faça o seguinte

- 1 Torne-se `root`.
- 2 Coloque o sistema no modo de usuário único (nível de execução 1) com `telinit 1`.
- 3 Mude os arquivos de configuração, conforme o necessário, com um editor de sua preferência.

Se você não usar o YaST para mudar os arquivos de configuração em `/etc/sysconfig`, verifique se os valores vazios das variáveis são representados por duas aspas (`KEYTABLE=""`) e se os valores com espaços em branco estão delimitados por aspas. Os valores constituídos de somente uma palavra não precisam ficar entre aspas.

- 4 Execute `SuSEconfig` para verificar se as mudanças foram efetivadas.
- 5 Coloque o sistema de volta no nível de execução anterior com o comando `telinit nível_de_execução_padrão`. Substitua `nível_de_execução_padrão` pelo nível de execução padrão do sistema. Escolha 5 para retornar ao modo multiusuário completo com rede e X ou escolha 3 se preferir trabalhar no modo multiusuário completo com rede.

Esse procedimento é relevante principalmente durante a mudança das configurações em todo o sistema, como a configuração da rede. Pequenas mudanças não devem requerer alternar para o modo de usuário único, mas você pode fazer isso para ter certeza de que todos os programas em questão foram reiniciados corretamente.

DICA: definindo a configuração automatizada do sistema

Para desabilitar a configuração automatizada do sistema pelo `SuSEconfig`, defina a variável `ENABLE_SUSECONFIG` em `/etc/sysconfig/suseconfig` como `no`. Não desabilite o `SuSEconfig` se quiser usar o suporte de instalação do SUSE. Também é possível desabilitar parcialmente a configuração automática.

O carregador de boot GRUB

Este capítulo descreve como configurar o GRUB, o carregador de boot usado no SUSE® Linux Enterprise Desktop. Há um módulo especial do YaST disponível para ajustar todas as configurações. Se você não estiver familiarizado com a idéia de entrar para o Linux, leia as seções a seguir para obter algumas informações de apoio. Este capítulo também descreve alguns dos problemas encontrados com frequência durante o boot com o GRUB, bem como suas soluções.

NOTA: ausência do GRUB em máquinas que usam UEFI

Como rotina, o GRUB será instalado nas máquinas equipadas com um BIOS tradicional e em máquinas com UEFI (Unified Extensible Firmware Interface) que usam um CSM (Compatibility Support Module - módulo de suporte a compatibilidade). Em máquinas com UEFI sem CSM habilitado, o `eLilo` será instalado automaticamente (desde que o DVD1 tenha sido inicializado com êxito). Consulte a documentação do `eLilo` em `/usr/share/doc/packages/elilo/` no seu sistema para obter detalhes.

Este capítulo trata do gerenciamento de boot e da configuração do carregador de boot GRUB. O procedimento de boot como um todo é detalhado em Capítulo 9, *Inicializando e configurando um sistema Linux* (p 87). Um carregador de boot representa a interface entre a máquina (BIOS) e o sistema operacional (SUSE Linux Enterprise Desktop). A configuração do carregador de boot influencia diretamente o boot do sistema operacional.

Os termos a seguir aparecem com frequência neste capítulo e talvez precisem de alguma explicação:

Master Boot Record

A estrutura do MBR é definida por uma convenção que não depende do sistema operacional. Os primeiros 446 bytes são reservados para o código do programa. Normalmente, eles contêm parte de um programa carregador de boot ou um seletor de sistema operacional. Os 64 bytes seguintes fornecem espaço para uma tabela de partição de até quatro entradas. A tabela de partição contém informações sobre o particionamento do disco rígido e sobre os tipos de sistema de arquivos. O sistema operacional precisa dessa tabela para lidar com o disco rígido. Com o código genérico convencional no MBR, exatamente uma partição deve ser marcada como *ativa*. Os dois últimos bytes do MBR devem conter um “número mágico” estático (AA55). Um MBR que contém um valor diferente é tido como inválido por alguns BIOS, não sendo considerado para o boot.

Setores de boot

Os setores de boot são os primeiros setores das partições do disco rígido, com a execução da partição estendida, que serve meramente como “container” para outras partições. Esses setores de boot têm 512 bytes de espaço para o código usado para inicializar um sistema operacional instalado na partição respectiva. Isso se aplica aos setores de boot das partições DOS, Windows e OS/2 formatadas, que também contêm alguns dados básicos importantes do sistema de arquivos. Os setores de boot das partições Linux, ao contrário, ficam inicialmente vazias após a configuração de um sistema de arquivos diferente do XFS. Portanto, uma partição Linux não é inicializável por si mesma, mesmo que contenha um kernel e um sistema válido de arquivos raiz. Um setor de boot com código válido para inicializar o sistema tem o mesmo número mágico que o MBR em seus dois últimos bytes (AA55).

10.1 Inicializando com o GRUB

O GRUB (Grand Unified Bootloader) tem dois estágios. O estágio 1 consiste em 512 bytes e sua única tarefa é carregar o segundo estágio do carregador de boot. Conseqüentemente, o estágio 2 é carregado. Este estágio contém a parte principal do carregador de boot.

Em algumas configurações, um estágio intermediário 1.5 pode ser usado, que localiza e carrega o estágio 2 de um sistema de arquivos apropriado. Se possível, este método é escolhido por padrão durante a instalação ou durante a configuração inicial do GRUB com o YaST.

O estágio 2 consegue acessar vários sistemas de arquivos. Atualmente, são suportados o Ext2, Ext3, ReiserFS, Minix e o sistema de arquivos FAT do DOS usado pelo Windows. Até certo ponto, XFS, e UFS e FFS usados pelos sistemas BSD também são suportados. Desde a versão 0.95, o GRUB também pode ser inicializado de um CD ou DVD que contenha um sistema de arquivos padrão ISO 9660 que está de acordo com a especificação “El Torito”. Mesmo antes de o sistema ser inicializado, o GRUB pode acessar os sistemas de arquivos dos dispositivos de disco BIOS suportados (disquetes ou discos rígidos, unidades de CD e unidades de DVD detectadas pelo BIOS). Portanto, as mudanças realizadas no arquivo de configuração do GRUB (`menu.lst`) não exigem a reinstalação do gerenciador de boot. Quando o sistema é inicializado, o GRUB recarrega o arquivo de menu com os caminhos e dados de partição válidos do kernel ou do disco RAM inicial (`initrd`) e localiza os arquivos.

A configuração real do GRUB se baseia em quatro arquivos, que são descritos a seguir:

`/boot/grub/menu.lst`

Esse arquivo contém todas as informações sobre partições ou sistemas operacionais que podem ser inicializados com o GRUB. Sem essas informações, a linha de comando do GRUB pergunta ao usuário como proceder (consulte a “Editando as entradas de menu durante o procedimento de boot” (p 112) para obter detalhes).

`/boot/grub/device.map`

Esse arquivo traduz os nomes dos dispositivos da notação do GRUB e do BIOS para os nomes de dispositivos Linux.

`/etc/grub.conf`

Esse arquivo contém os comandos, os parâmetros e as opções que o shell do GRUB precisa para instalar corretamente o carregador de boot.

`/etc/sysconfig/bootloader`

Esse arquivo é lido pela biblioteca `perl-bootloader` usada quando se configura o carregador de boot com o YaST e toda vez que um novo kernel é instalado. Ele contém opções de configuração (como parâmetros de kernel) que serão adicionadas por padrão ao arquivo de configuração do carregador de boot.

O GRUB pode ser controlado de várias maneiras. As entradas de boot de uma configuração existente podem ser selecionadas no menu gráfico (splash screen). A configuração é carregada a partir do arquivo `menu.lst`.

No GRUB, todos os parâmetros de boot podem ser mudados antes do boot. Por exemplo, os erros cometidos durante a edição do arquivo de menu podem ser corrigidos desta maneira. Os comandos de boot também podem ser inseridos de forma interativa através de um tipo de prompt de entrada (consulte “Editando as entradas de menu durante o procedimento de boot” (p 112)). O GRUB oferece a possibilidade de determinar a localização do kernel e do `initrd` antes do boot. Dessa maneira, você pode até inicializar um sistema operacional instalado para o qual não existe entrada na configuração do carregador de boot.

Na verdade, o GRUB existe em duas versões: como carregador de boot e como programa normal do Linux em `/usr/sbin/grub`. O segundo é conhecido como *shell do GRUB*. Ele fornece uma emulação do GRUB no sistema instalado e pode ser usado para instalar o GRUB ou testar novas configurações antes de aplicá-las. A funcionalidade para instalar o GRUB como carregador de boot em um disco rígido ou em um disquete é integrada ao GRUB na forma do comando `setup`. Ela fica disponível no shell do GRUB quando o Linux é carregado.

10.1.1 O menu de boot do GRUB

A splash screen gráfica no menu de boot baseia-se no arquivo de configuração do GRUB `/boot/grub/menu.lst`, que contém todas as informações sobre todas as partições ou sistemas operacionais que podem ser inicializados pelo menu.

Toda vez que o sistema é inicializado, o GRUB carrega o arquivo de menu a partir do sistema de arquivos. Por esse motivo, o GRUB não precisa ser reinstalado depois de todas as modificações no arquivo. Use o carregador de boot do YaST para modificar a configuração do GRUB conforme descrito na Seção 10.2, “Configurando o carregador de boot com o YaST” (p 117).

O arquivo de menu contém comandos. A sintaxe é muito simples. Cada linha contém um comando seguido de parâmetros opcionais separados por espaços, como ocorre no shell. Por razões históricas, alguns comandos admitem um `=` na frente do primeiro parâmetro. Os comentários são introduzidos por um hash (`#`).

Para identificar os itens do menu na visão geral do menu, defina um `título` para cada entrada. O texto (incluindo os espaços) que vem depois da palavra-chave `título` é exibido como opção selecionável no menu. Todos os comandos até o próximo `título` são executados quando se seleciona esse item de menu.

O caso mais simples é o redirecionamento para os carregadores de boot de outros sistemas operacionais. O comando é `chainloader` e o argumento é geralmente o bloco de boot de outra partição na notação de bloco do GRUB. Por exemplo:

```
chainloader (hd0,3)+1
```

Os nomes de dispositivos no GRUB são explicados na “Convenções de nomeação para discos rígidos e partições” (p 110). Este exemplo especifica o primeiro bloco da quarta partição do primeiro disco rígido.

Use o comando `kernel` para especificar uma imagem do kernel. O primeiro argumento é o caminho para a imagem do kernel em uma partição. Os outros argumentos são passados para o kernel na linha de comando.

Se o kernel não contiver drivers internos para acesso à partição raiz ou se for usado um sistema Linux recente com recursos de hotplug avançados, o `initrd` deve ser especificado com um comando separado do GRUB, cujo único argumento é o caminho para o arquivo `initrd`. Como o endereço de carregamento do `initrd` é gravado na imagem do kernel carregado, o comando `initrd` deve vir imediatamente após o comando `kernel`.

O comando `root` simplifica a especificação do kernel e dos arquivos `initrd`. O único argumento de `root` é um dispositivo ou uma partição. Esse dispositivo é usado para todos os kernels, `initrd`, ou para outros caminhos de arquivo para os quais não há dispositivos explicitamente especificados até o próximo comando `root`.

O comando `boot` está implícito no fim de cada entrada do menu, assim ele não precisa ser gravado no arquivo de menu. No entanto, ao usar o GRUB de forma interativa para o boot, você deve digitar o comando `boot` no final. O comando em si não tem argumentos. Ele meramente inicializa a imagem do kernel carregado ou do carregador de cadeia especificado.

Depois de gravar todas as entradas de menu, defina uma delas como entrada `default`. Do contrário, é utilizada a primeira (entrada 0). Você também pode especificar um tempo de espera em segundos depois do qual a entrada `default` deve ser inicializada. `timeout` e `default` geralmente precedem as entradas de menu. Um arquivo de exemplo é descrito em “Um exemplo de arquivo de menu” (p 111).

Convenções de nomeação para discos rígidos e partições

As convenções de nomeação que o GRUB utiliza para discos rígidos e partições diferem daquelas usadas para os dispositivos Linux normais. Elas são mais parecidas com a enumeração de disco simples feita pelo BIOS, além disso, a sintaxe é semelhante à usada em alguns derivativos do BSD. No GRUB, a numeração das partições começa por zero. Isso significa que `(hd0, 0)` é a primeira partição do primeiro disco rígido. Em uma máquina desktop comum, com um disco rígido conectado como master principal, o nome do dispositivo Linux correspondente é `/dev/sda1`.

As quatro partições principais possíveis são atribuídas aos números de partição de 0 a 3. As partições lógicas são numeradas a partir de 4:

```
(hd0,0)  first primary partition of the first hard disk
(hd0,1)  second primary partition
(hd0,2)  third primary partition
(hd0,3)  fourth primary partition (usually an extended partition)
(hd0,4)  first logical partition
(hd0,5)  second logical partition
```

Sendo dependente de dispositivos BIOS, o GRUB não faz distinção entre dispositivos IDE, SATA, SCSI e RAID de hardware. Todos os discos rígidos reconhecidos pelo BIOS ou por outras controladoras são numerados de acordo com a seqüência de boot predefinido no BIOS.

Infelizmente, geralmente não é possível mapear os nomes dos dispositivos Linux de forma exata para os nomes dos dispositivos BIOS. Ele gera esse mapeamento com a ajuda de um algoritmo e o grava no arquivo `device.map`, que pode ser editado se necessário. Na Seção 10.1.2, “O arquivo `device.map`” (p 114), há informações sobre o arquivo `device.map`.

O caminho completo do GRUB consiste em um nome de dispositivo escrito entre parênteses e o caminho para o arquivo no sistema de arquivos na partição especificada. O caminho começa com uma barra. Por exemplo, o kernel inicializável poderia ser especificado como segue em um sistema com um disco rígido único de IDE que contém o Linux em sua primeira partição:

```
(hd0,0)/boot/vmlinuz
```

Um exemplo de arquivo de menu

O exemplo a seguir mostra a estrutura de um arquivo de menu do GRUB. A instalação de exemplo compreende uma partição de boot do Linux em `/dev/sda5`, uma partição raiz em `/dev/sda7` e uma instalação do Windows em `/dev/sda1`.

```
gfxmenu (hd0,4)/boot/message
color white/blue black/light-gray
default 0
timeout 8

title linux
    root (hd0,4)
    kernel /boot/vmlinuz root=/dev/sda7 vga=791 resume=/dev/sda9
    initrd /boot/initrd

title windows
    rootnoverify (hd0,0)
    chainloader +1

title floppy
    rootnoverify (hd0,0)
    chainloader (fd0)+1

title failsafe
    root (hd0,4)
    kernel /boot/vmlinuz.shipped root=/dev/sda7 ide=nodma \
    apm=off acpi=off vga=normal nosmp maxcpus=0 3 noresume
    initrd /boot/initrd.shipped
```

O primeiro bloco define a configuração da splash screen:

`gfxmenu (hd0,4)/message`

A imagem de segundo plano `message` localiza-se no diretório de nível superior da partição `/dev/sda5`.

`color white/blue black/light-gray`

Esquema de cores: branco (primeiro plano), azul (segundo plano), preto (seleção) e cinza claro (segundo plano da seleção). O esquema de cores não tem efeito sobre a splash screen, apenas sobre o menu personalizável do GRUB que você pode acessar saindo da splash screen com `Esc`.

`default 0`

Por padrão, a primeira entrada do menu, `title linux`, é a utilizada para inicializar.

timeout 8

Após oito segundos sem nenhuma entrada do usuário, o GRUB inicializa automaticamente a entrada padrão. Para desativar o boot automático, apague a linha `timeout`. Se você definir `timeout 0`, o GRUB inicializará a entrada padrão imediatamente.

O segundo e maior bloco lista os vários sistemas operacionais inicializáveis. As seções para os sistemas operacionais individuais são introduzidas pelo `título`.

- A primeira entrada (`title linux`) é responsável por inicializar o SUSE Linux Enterprise Desktop. O kernel (`vmlinux`) localiza-se na primeira partição lógica (a partição de boot) do primeiro disco rígido. Os parâmetros do kernel, tais como a partição raiz e o modo VGA, são anexados aqui. A partição raiz é especificada de acordo com a convenção de nomeação do Linux (`/dev/sda7/`), pois essas informações são lidas pelo kernel e não têm nada a ver com o GRUB. O `initrd` também se localiza na primeira partição lógica do primeiro disco rígido.
- A segunda entrada é responsável por carregar o Windows. O Windows é inicializado a partir da primeira partição do primeiro disco rígido (`hd0, 0`). O comando `chainloader +1` faz com que o GRUB leia e execute o primeiro setor da partição especificada.
- A próxima entrada permite o boot a partir do disco rígido sem modificar as configurações do BIOS.
- A opção de boot `failsafe` inicia o Linux com uma seleção de parâmetros do kernel que permite que o Linux seja inicializado nos sistemas problemáticos.

O arquivo de menu pode ser mudado sempre que for necessário. O GRUB utiliza, então, as configurações modificadas durante o próximo boot. Edite o arquivo permanentemente usando o YaST ou um editor da sua escolha. Como alternativa, faça as mudanças temporárias de forma interativa usando a função de edição do GRUB. Consulte o “Editando as entradas de menu durante o procedimento de boot” (p 112).

Editando as entradas de menu durante o procedimento de boot

No menu gráfico de boot, selecione o sistema operacional a ser inicializado com as teclas de seta. Se selecionar um sistema Linux, você pode inserir parâmetros extras de

boot no prompt de boot. Para editar diretamente as entradas individuais do menu, pressione Esc para sair da splash screen e entrar no menu baseado em texto do GRUB, depois pressione E. As mudanças feitas desta maneira só se aplicam ao boot atual, não sendo adotadas permanentemente.

IMPORTANTE: layout do teclado durante o procedimento de boot

O layout do teclado norte-americano é o único disponível na hora de inicializar. Consulte a Figura 28.3, “Layout do teclado dos EUA” (p 385).

Editar entradas de menu facilita o reparo de um sistema com defeito que não pode mais ser inicializado, pois o arquivo de configuração defeituoso do carregador de boot pode ser evitado ao se inserir parâmetros manualmente. A inserção manual de parâmetros durante o procedimento de boot também é útil para testar novas configurações sem danificar o sistema nativo.

Depois de ativar o modo de edição, use as teclas de seta para selecionar a entrada de menu cuja configuração deve ser editada. Para tornar a configuração editável, pressione E novamente. Dessa maneira, edite as especificações incorretas das partições ou do caminho antes que tenham um efeito negativo sobre o processo de boot. Pressione Enter para sair do modo de edição e retornar ao menu. Depois pressione B para inicializar essa entrada. No texto de ajuda da parte inferior, são mostradas mais ações possíveis.

Para inserir permanentemente as opções de boot mudadas e passá-las para o kernel, abra o arquivo `menu.lst` como `raiz` do usuário e anexe os respectivos parâmetros do kernel à linha existente, separados por espaços:

```
title linux
    root(hd0,0)
    kernel /vmlinuz root=/dev/sda3 additional parameter
    initrd /initrd
```

O GRUB adota automaticamente os novos parâmetros na próxima vez em que o sistema é inicializado. Como alternativa, essa mudança também pode ser feita com o módulo carregador de boot do YaST. Anexe os novos parâmetros à linha existente, separados por espaços.

10.1.2 O arquivo `device.map`

O arquivo `device.map` mapeia os nomes de dispositivos GRUB e BIOS para os nomes de dispositivos Linux. Em um sistema misto que contém discos rígidos IDE e SCSI, o GRUB deve tentar determinar a sequência de boot através de um procedimento especial, pois o GRUB não tem acesso às informações do BIOS sobre a sequência de boot. O GRUB grava o resultado dessa análise no arquivo `/boot/grub/device.map`. Para um sistema no qual a sequência de boot no BIOS é configurada como IDE antes de SCSI, o arquivo `device.map` poderia aparecer da seguinte forma:

```
(fd0)  /dev/fd0
(hd0)  /dev/disk-by-id/DISK1 ID
(hd1)  /dev/disk-by-id/DISK2 ID
```

Como a ordem de discos rígidos IDE, SCSI e outros depende de vários fatores, e como o Linux não consegue identificar o mapeamento, a sequência no arquivo `device.map` pode ser definida manualmente. Se você encontrar problemas na hora do boot, verifique se a sequência nesse arquivo corresponde à sequência no BIOS e use o prompt do GRUB para modificá-la temporariamente, se necessário. Depois que o sistema Linux for inicializado, o arquivo `device.map` pode ser editado permanentemente com o módulo carregador de boot do YaST ou com um editor da sua preferência.

Depois de mudar manualmente o `device.map`, execute o seguinte comando para reinstalar o GRUB. Este comando faz com que o arquivo `device.map` seja recarregado e os comandos listados em `grub.conf` sejam executados:

```
grub --batch < /etc/grub.conf
```

10.1.3 O arquivo `/etc/grub.conf`

O terceiro arquivo de configuração importante do GRUB, depois do `menu.lst` e do `device.map`, é o `/etc/grub.conf`. Esse arquivo contém os comandos, os parâmetros e as opções que o shell do GRUB precisa para instalar corretamente o carregador de boot:

```
setup --stage2=/boot/grub/stage2 --force-lba (hd0,1) (hd0,1)
quit
```

Esse comando instrui o GRUB a instalar automaticamente o carregador de boot na segunda partição do primeiro disco rígido (`hd0,1`) usando as imagens de boot localizadas

na mesma partição. O parâmetro `--stage2=/boot/grub/stage2` é necessário para instalar a imagem `stage2` de um sistema de arquivos montado. Alguns BIOS possuem falha na implementação do suporte a LBA. `--force-lba` proporciona uma solução para ignorá-la.

10.1.4 O arquivo `/etc/sysconfig/bootloader`

Esse arquivo de configuração é usado apenas ao configurar o carregador de boot com o YaST e sempre que um novo kernel é instalado. Ele é avaliado pela biblioteca `perl-bootloader`, que modifica o arquivo de configuração do carregador de boot (por exemplo, `/boot/grub/menu.lst` para o GRUB) de forma apropriada. `/etc/sysconfig/bootloader` não é um arquivo de configuração específico do GRUB — os valores são aplicados a qualquer carregador de boot instalado no SUSE Linux Enterprise Desktop.

NOTA: configuração do carregador de boot após uma atualização de kernel

Toda vez que um novo kernel é instalado, o carregador de boot `perl` grava uma nova configuração de carregador de boot (por exemplo, `/boot/grub/menu.lst` para o GRUB) usando os padrões especificados em `/etc/sysconfig/bootloadert`. Se você estiver usando um conjunto personalizado de parâmetros de kernel, certifique-se de ajustar os padrões relevantes em `/etc/sysconfig/bootloader` de acordo com as suas necessidades.

`LOADER_TYPE`

Especifica o carregador de boot instalado no sistema (ex.: GRUB ou LILO). Não modifique, use o YaST para mudar o carregador de boot — consulte Procedimento 10.6, “Mudando o tipo de carregador de boot” (p 123) para obter detalhes.

`DEFAULT_VGA/FAILSAFE_VGA / XEN_VGA`

A resolução de tela e a profundidade de cores do buffer de quadros usadas durante o boot são configuradas com o parâmetro de kernel `vga`. Esses valores definem qual resolução e profundidade de cores usar para as entradas de boot `default`, `failsafe` e `XEN`. Os seguintes valores são válidos:

Tabela 10.1 Referência de resolução de tela e profundidade de cores

	640x480	800x600	1024 x 768	1280x1024	1600x1200
8bit	0x301	0x303	0x305	0x307	0x31C
15bit	0x310	0x313	0x316	0x319	0x31D
16bit	0x311	0x314	0x317	0x31A	0x31E
24bit	0x312	0x315	0x318	0x31B	0x31F

DEFAULT_APPEND/FAILSAFE_APPEND/XEN_KERNEL_APPEND

Parâmetros de kernel (diferentes de `vga`) automaticamente anexados às entradas de boot default, failsafe e XEN no arquivo de configuração do carregador de boot.

CYCLE_DETECTION/CYCLE_NEXT_ENTRY

Configure se desejar usar a detecção do ciclo de boot e, ao fazer isso, configure também qual entrada alternativa de `/boot/grub/menu.lst` (ex.: Failsafe) usar no boot em caso de um ciclo de reinicialização. Consulte `/usr/share/doc/packages/bootcycle/README` para obter informações detalhadas.

10.1.5 Configurando uma senha de boot

Mesmo antes de o sistema operacional ser inicializado, o GRUB permite acesso aos sistema de arquivos. Os usuários que não têm permissões raiz podem acessar os arquivos no seu sistema Linux aos quais não têm acesso depois que o sistema é inicializado. Para bloquear esse tipo de acesso ou impedir que os usuários inicializem certos sistemas operacionais, defina uma senha de boot.

IMPORTANTE: senha de boot e splash screen

Se você usar uma senha de boot para o GRUB, a splash screen normal não será exibida.

Como a raiz do usuário, proceda da seguinte forma para definir uma senha de boot:

- 1 No prompt do root, criptografe a senha usando `grub-md5-crypt`:

```
# grub-md5-crypt
Password: ****
Retype password: ****
Encrypted: $1$1S2dv/$JOYcdxIn7CJk9xShzzJVw/
```

2 Cole a string criptografada na seção global do arquivo menu.lst:

```
gfxmenu (hd0,4)/message
color white/blue black/light-gray
default 0
timeout 8
password --md5 $1$1S2dv/$JOYcdxIn7CJk9xShzzJVw/
```

Agora, só é possível executar os comandos do GRUB no prompt raiz depois de pressionar P e digitar a senha. No entanto, os usuários ainda podem inicializar todos os sistemas operacionais a partir do menu de boot.

3 Para impedir que um ou vários sistemas operacionais sejam inicializados a partir do menu de boot, acrescente a entrada lock em cada seção no menu.lst que não deveria ser inicializada sem se inserir uma senha. Por exemplo:

```
title linux
    kernel (hd0,4)/vmlinuz root=/dev/sda7 vga=791
    initrd (hd0,4)/initrd
    lock
```

Depois de reiniciar o sistema e selecionar a entrada no Linux no menu de boot, é exibida a seguinte mensagem de erro:

```
Error 32: Must be authenticated
```

Pressione Enter para inserir o menu. Depois pressione P para obter o prompt da senha. Depois de inserir a senha e pressionar Enter, o sistema operacional selecionado (o Linux, neste caso) não deve inicializar.

10.2 Configurando o carregador de boot com o YaST

A maneira mais fácil de configurar o carregador de boot no sistema SUSE Linux Enterprise Desktop é usando o módulo do YaST. No Centro de Controle do YaST, selecione *Sistema > Carregador de Boot*. Como na Figura 10.1, “Configurações do

carregador de boot” (p 118), isso mostra a configuração do carregador de boot atual do sistema e permite fazer mudanças.

Figura 10.1 Configurações do carregador de boot



Use a guia *Gerenciamento de Seções* para editar, mudar e apagar seções do carregador de boot referentes aos sistemas operacionais individuais. Para adicionar uma opção, clique em *Adicionar*. Para mudar o valor de uma opção existente, selecione-o com o mouse e clique em *Editar*. Para remover uma entrada existente, selecione-a e clique em *Apagar*. Se não estiver familiarizado com as opções do carregador de boot, leia primeiro a Seção 10.1, “Inicializando com o GRUB” (p 106).

Use a guia *Instalação do Carregador de Boot* para ver e mudar configurações relativas a tipo, local e opções avançadas do carregador.

Acesse opções de configuração avançadas no menu suspenso que aparece quando você clica em *Outros*. O editor interno permite mudar os arquivos de configuração do GRUB (consulte a Seção 10.1, “Inicializando com o GRUB” (p 106) para obter detalhes). Você também pode apagar a configuração existente e *Iniciar*, ou deixar o YaST *Propor Nova*

Configuração. Também é possível gravar a configuração em disco ou relê-la do disco. Para restaurar o MBR (Master Boot Record) original que foi gravado durante a instalação, escolha *Recuperar MBR do Disco Rígido*.

10.2.1 Ajustando a entrada de boot padrão

Para mudar o sistema que é inicializado por padrão, proceda da seguinte maneira:

Procedimento 10.1 *Definindo o sistema padrão*

- 1 Abra a guia *Gerenciamento de Seções*.
- 2 Selecione a entrada desejada na lista.
- 3 Clique em *Definir como Padrão*.
- 4 Clique em *Ok* para ativar essas mudanças.

10.2.2 Modificando a localização do carregador de boot

Para modificar o local do carregador de boot, siga estas etapas:

Procedimento 10.2 *Mudando a localização do carregador de boot*

- 1 Selecione a guia *Instalação do Carregador de Boot* e escolha uma das seguintes opções para a *Localização do Carregador de Boot*:

Boot do Master Boot Record

Instala o carregador de boot no MBR do primeiro disco (de acordo com a sequência de boot predefinida no BIOS).

Boot da partição raiz

Instala o carregador de boot no setor de boot da partição / (padrão).

Boot da partição de boot

Instala o carregador de boot no setor de boot da partição /boot.

Boot da partição estendida

Instala o carregador de boot no container da partição estendida.

Partição de boot personalizada

Use esta opção para especificar a localização do carregador de boot manualmente.

- 2 Clique em *OK* para aplicar as mudanças.

10.2.3 Mudando o tempo de espera do carregador de boot

O carregador de boot não inicializa o sistema padrão imediatamente. Durante o tempo de espera, você pode selecionar o sistema para inicializar ou gravar alguns parâmetros de kernel. Para definir o tempo de espera do carregador de boot, proceda da seguinte maneira:

Procedimento 10.3 *Mudando o tempo de espera do carregador de boot*

- 1 Abra a guia *Instalação do Carregador de Boot*.
- 2 Clique em *Opções do Carregador de Boot*.
- 3 Mude o valor de *Tempo de Espera em Segundos* digitando um novo valor e clicando na tecla de seta adequada com o mouse ou usando as teclas de seta do teclado.
- 4 Clique em *OK* duas vezes para gravar as mudanças.

10.2.4 Configurando uma senha de boot

Com esse módulo do YaST, também é possível definir uma senha para proteger o boot. Este procedimento aumenta o nível de segurança.

Procedimento 10.4 *Configurando uma senha do carregador de boot*

- 1 Abra a guia *Instalação do Carregador de Boot*.

- 2 Clique em *Opções do Carregador de Boot*.
- 3 Ative a opção *Proteger Carregador de Boot com Senha* com um clique e digite a sua *Senha* duas vezes.
- 4 Clique em *OK* duas vezes para gravar as mudanças.

10.2.5 Ajustando a ordem dos discos

Se o seu computador tiver mais de um disco rígido, é possível especificar a sequência de boot dos discos para corresponder à configuração do BIOS da máquina (consulte a Seção 10.1.2, “O arquivo device.map” (p 114)). Para fazer isso, proceda da seguinte maneira:

Procedimento 10.5 *Definindo a ordem dos discos*

- 1 Abra a guia *Instalação do Carregador de Boot*.
- 2 Clique em *Detalhes de Instalação do Carregador de Boot*.
- 3 Se mais de um disco for listado, selecione um disco e clique em *Para cima* ou *Para baixo* para reordenar os discos exibidos.
- 4 Clique em *OK* duas vezes para gravar as mudanças.

10.2.6 Configurando as opções avançadas

As opções avançadas de boot podem ser configuradas por meio de *Instalação do Carregador de Boot > Opções do Carregador de Boot*. Normalmente não há necessidade de mudar as configurações padrão.

Definir Flag Ativo na Tabela de Partição para a Partição de Boot

Ativa a partição que contém o carregador de boot. Alguns sistemas operacionais legados (como o Windows 98) podem ser inicializados apenas de uma partição ativa.

Gravar Código de Boot Genérico no MBR

Substitui o MBR atual por um código genérico independente de sistema operacional.

Flag de Depuração

Define o GRUB no modo de depuração, no qual são exibidas mensagens para mostrar a atividade do disco.

Ocultar Menu de Boot

Oculto o menu de boot e a entrada padrão.

Usar GRUB Confiável

Inicia o GRUB Confiável, que suporta a funcionalidade de computação confiável.

Arquivo de Menu Gráfico

Caminho do arquivo gráfico usado na exibição da tela de boot.

Parâmetros de Conexão Serial

Se a sua máquina é controlada por um console serial, você pode especificar a porta COM que será usada e em qual velocidade. Além disso, defina *Definição de Terminal* como “serial”. Consulte `info grub` ou <http://www.gnu.org/software/grub/manual/grub.html> para obter detalhes.

Definição de Terminal

Se for inicializar por meio de um console serial, digite “serial” aqui, caso contrário, deixe em branco. Você também deve especificar *Parâmetros de Conexão Serial* neste caso.

10.2.7 Mudando o tipo de carregador de boot

Defina o tipo de carregador de boot em *Instalação do Carregador de Boot*. O carregador de boot padrão do SUSE Linux Enterprise Desktop é o GRUB. Para usar o LILO ou o ELILO, proceda da seguinte maneira:

ATENÇÃO: o LILO não é suportado

O uso do LILO não é recomendado — ele não é suportado no SUSE Linux Enterprise Desktop. Use-o apenas em casos especiais.

Procedimento 10.6 *Mudando o tipo de carregador de boot*

- 1** Selecione a guia *Instalação do Carregador de Boot*.
- 2** Para *Carregador de Boot*, selecione *LILO*.
- 3** Na caixa de diálogo aberta, selecione uma das seguintes ações:

Propor Nova Configuração

Faça com que o YaST proponha uma nova configuração.

Converter Configuração Atual

Faça com que o YaST converta a configuração atual. Na conversão da configuração, algumas definições podem ser perdidas.

Iniciar Nova Configuração do Início

Grave uma configuração personalizada. Essa ação não está disponível durante a instalação do SUSE Linux Enterprise Desktop.

Ler Configuração Gravada em Disco

Carregue o `/etc/lilo.conf`. Essa ação não está disponível durante a instalação do SUSE Linux Enterprise Desktop.

- 4** Clique em *OK* duas vezes para gravar as mudanças.

Durante a conversão, a antiga configuração do GRUB é gravada no disco. Para utilizá-la, basta voltar o tipo de carregador de boot para GRUB e escolher *Recuperar Configuração Gravada Antes da Conversão*. Esta ação fica disponível somente em um sistema instalado.

NOTA: carregador de boot personalizado

Para usar um carregador de boot que não seja o GRUB nem o LILO, selecione *Não Instalar Nenhum Carregador de Boot*. Leia a documentação do seu carregador de boot cuidadosamente antes de escolher esta opção.

10.3 Desinstalando a controladora de boot do Linux

O YaST pode ser usado para desinstalar o carregador de boot do Linux e restaurar o estado do MBR anterior à instalação do Linux. Durante a instalação, o YaST cria automaticamente uma cópia de backup do MBR original e a restaura mediante solicitação.

Para desinstalar o GRUB, inicie o módulo carregador de boot do YaST (*Sistema > Carregador de Boot*). Selecione *Outro > Recuperar MBR do Disco Rígido* e confirme com *Sim, Regravar*.

10.4 Criando CDs de boot

Se o boot do sistema com um gerenciador de boot apresentar problemas ou se o gerenciador de boot não puder ser instalado no disco rígido, também será possível criar um CD inicializável com todos os arquivos de inicialização necessários para o Linux. Para isso, é necessário um gravador de CD instalado no sistema.

A criação de um CR-ROM inicializável com o GRUB requer simplesmente um formato especial de *stage2* chamado *stage2_eltorito* e, opcionalmente, um *menu.lst* personalizado. Os clássicos arquivos *stage1* e *stage2* não são necessários.

Procedimento 10.7 Criando CDs de boot

- 1 Passe para um diretório no qual será criada a imagem ISO, por exemplo: `cd /tmp`
- 2 Crie um subdiretório para o GRUB e passe para o diretório `iso` recém-criado:

```
mkdir -p iso/boot/grub && cd iso
```
- 3 Copie o kernel, os arquivos *stage2_eltorito*, *initrd*, *menu.lst* e *message* para `iso/boot/`:

```
cp /boot/vmlinuz boot/  
cp /boot/initrd boot/  
cp /boot/message boot/
```

```
cp /usr/lib/grub/stage2_eltorito boot/grub
cp /boot/grub/menu.lst boot/grub
```

- 4** Ajuste as entradas de caminho em `/boot/menu.lst` para que apontem para um dispositivo de CD-ROM. Faça isso substituindo o nome de dispositivo dos discos rígidos, listados no formato `(hdx, y)` nos nomes de caminho, por `(cd)`, o nome de dispositivo da unidade de CD-ROM. Você também pode precisar ajustar os caminhos do arquivo de mensagem, do kernel e do `initrd` — eles devem apontar para `/boot/message`, `/boot/vmlinuz` e `/boot/initrd`, respectivamente. Depois de fazer os ajustes, `menu.lst` deverá ter aparência semelhante ao exemplo a seguir:

```
timeout 8
default 0
gfxmenu (cd)/boot/message

title Linux
    root (cd)
    kernel /boot/vmlinuz root=/dev/sda5 vga=794 resume=/dev/sda1 \
    splash=verbose showopts
    initrd /boot/initrd
```

Use `splash=silent` em vez de `splash=verbose` para impedir que apareçam mensagens de boot durante o procedimento de boot.

- 5** Crie a imagem ISO com o seguinte comando:

```
genisoimage -R -b boot/grub/stage2_eltorito -no-emul-boot \
-boot-load-size 4 -boot-info-table -iso-level 2 -input-charset utf-8 \
-o grub.iso /tmp/iso
```

- 6** Grave o arquivo resultante `grub.iso` em um CD usando seu utilitário preferido. Não grave a imagem ISO como arquivo de dados, porém, use a opção para gravar uma imagem de CD no seu utilitário de gravação.

10.5 A tela gráfica do SUSE

A tela gráfica do SUSE será exibida no primeiro console se a opção `vga=valor` for usada como parâmetro de kernel. Se você fizer a instalação usando o YaST, essa opção é ativada automaticamente de acordo com a resolução e a placa de vídeo selecionadas. Há três maneiras de desabilitar a tela do SUSE, se desejado:

Desabilitando a tela do SUSE quando necessário

Insira o comando `echo 0 >/proc/splash` na linha de comando para desativar a tela gráfica. Para ativá-la novamente, insira `echo 1 >/proc/splash`.

Desabilitando a tela do SUSE por padrão

Acrescente o parâmetro de kernel `splash=0` à configuração do seu carregador de boot. O Capítulo 10, *O carregador de boot GRUB* (p 105) fornece mais informações sobre isso. No entanto, se você preferir o modo de texto (que foi o padrão nas versões anteriores), defina `vga=normal`.

Desativando completamente a tela do SUSE

Compile um novo kernel e desative a opção *Usar a splash screen em vez do logotipo de boot* no suporte a framebuffer.

DICA

A desabilitação do suporte a buffer de quadros no kernel também desabilita automaticamente a splash screen. O SUSE não pode fornecer suporte ao seu sistema se você o executar com um kernel personalizado.

10.6 Solução de problemas

Esta seção lista alguns dos problemas encontrados com frequência na hora de inicializar com o GRUB e uma descrição resumida das soluções possíveis. Alguns desses problemas são abordados em artigos da Base de Dados de Conhecimento, em <http://support.novell.com/>. Use a caixa de diálogo de pesquisa para procurar palavras-chave como *GRUB*, *boot* e *carregador de boot*.

GRUB e XFS

O XFS não deixa espaço para o `stage1` no bloco de boot da partição. Portanto, não especifique uma partição XFS como local do carregador de boot. Esse problema pode ser resolvido com a criação de uma partição separada de boot que não é formatada com o XFS.

O GRUB informa erro de geometria no GRUB

O GRUB verifica a geometria dos discos rígidos conectados quando o sistema é inicializado. Às vezes, o BIOS retorna informações inconsistentes e o GRUB cria um erro de geometria do GRUB. Quando isso ocorrer, atualize o BIOS.

O GRUB também retornará essa mensagem de erro se o Linux tiver sido instalado em um disco rígido adicional não registrado no BIOS. O *stage1* do carregador de boot foi encontrado e carregado corretamente, mas o *stage2* não foi encontrado. Esse problema pode ser remediado registrando-se o novo disco rígido no BIOS.

Sistema contendo vários discos rígidos não é inicializado

Durante a instalação, o YaST pode ter determinado incorretamente a seqüência de boot dos discos rígidos. Por exemplo, o GRUB pode considerar o disco IDE como *hd0* e o disco SCSI como *hd1*, embora a seqüência de boot no BIOS seja invertida (SCSI *antes* de IDE).

Nesse caso, corrija os discos rígidos durante o processo de boot com a ajuda da linha de comando do GRUB. Depois que o sistema for inicializado, edite *device.map* para aplicar o novo mapeamento permanentemente. Depois verifique os nomes de dispositivo do GRUB nos arquivos */boot/grub/menu.lst* e */boot/grub/device.map* e reinstale o carregador de boot com o seguinte comando:

```
grub --batch < /etc/grub.conf
```

Inicializando o Windows do segundo disco rígido

Alguns sistemas operacionais, como o Windows, podem ser inicializados apenas do primeiro disco rígido. Se um sistema operacional desse tipo for instalado em um disco rígido que não for o primeiro, você pode efetuar uma mudança lógica na respectiva entrada do menu.

```
...
title windows
    map (hd0) (hd1)
    map (hd1) (hd0)
    chainloader (hd1,0)+1
...
```

Nesse exemplo, o Windows é iniciado a partir do segundo disco rígido. Para essa finalidade, a ordem lógica dos discos rígidos é mudada com *map*. Essa mudança não afeta a lógica dentro do arquivo de menu do GRUB. Portanto, o segundo disco rígido deve ser especificado para *chainloader*.

10.7 Para obter mais informações

Em <http://www.gnu.org/software/grub/>, há informações abrangentes sobre o GRUB. Consulte também a página de informações [grub](#). Você também pode procurar a palavra-chave “GRUB” na Pesquisa de Informações Técnicas em <http://www.novell.com/support> para obter informações sobre problemas específicos.

Recursos especiais do sistema

Este capítulo começa com informações sobre vários pacotes de software, os consoles virtuais e o layout do teclado. Abordamos componentes de software como `bash`, `cron` e `logrotate`, porque eles foram mudados ou aperfeiçoados durante os últimos ciclos de lançamento. Mesmo que eles sejam pequenos ou considerados de menor importância, talvez os usuários desejem mudar o seu comportamento padrão, porque esses componentes muitas vezes estão intimamente ligados ao sistema. O capítulo termina com uma seção sobre configurações específicas de país e idioma (I18N e L10N).

11.1 Informações sobre pacotes de software especiais

Os programas `bash`, `cron`, `logrotate`, `locate`, `ulimit` e `free` são muito importantes para os administradores de sistema e para muitos usuários. Páginas do manual e de informações são duas fontes úteis de informações sobre comandos, mas nem sempre ambas estão disponíveis. O GNU Emacs é um editor de texto popular e muito configurável.

11.1.1 O pacote `bash` e `/etc/profile`

Bash é o shell de sistema padrão. Quando usado com um shell de login, ele lê vários arquivos de inicialização. O Bash os processa na ordem que são exibidos na lista:

1. `/etc/profile`
2. `~/.profile`
3. `/etc/bash.bashrc`
4. `~/.bashrc`

Faça configurações personalizadas em `~/.profile` ou `~/.bashrc`. Para assegurar o processamento correto desses arquivos, é necessário copiar as configurações básicas de `/etc/skel/.profile` ou `/etc/skel/.bashrc` no diretório pessoal do usuário. É recomendável copiar as configurações de `/etc/skel` após uma atualização. Execute os seguintes comandos de shell para evitar a perda de ajustes pessoais:

```
mv ~/.bashrc ~/.bashrc.old
cp /etc/skel/.bashrc ~/.bashrc
mv ~/.profile ~/.profile.old
cp /etc/skel/.profile ~/.profile
```

Em seguida, copie os ajustes pessoais novamente dos arquivos `*.old`.

11.1.2 O pacote cron

Se você deseja executar comandos de maneira regular e automática em segundo plano em horários predefinidos, cron é a ferramenta a ser usada. O cron é orientado por tabelas de horários especialmente formatadas. Algumas delas são fornecidas com o sistema e os usuários podem gravar as suas próprias tabelas, se necessário.

As tabelas cron estão localizadas em `/var/spool/cron/tabs`. `/etc/crontab` atua como uma tabela cron para todo o sistema. Digite o nome de usuário para executar o comando diretamente após a tabela de tempo e antes do comando. No Exemplo 11.1, “Entrada in `/etc/crontab`” (p 130), `root` é digitado. Tabelas específicas de pacote, localizadas em `/etc/cron.d`, possuem o mesmo formato. Consulte a página de manual `cron` (`man cron`).

Exemplo 11.1 *Entrada in `/etc/crontab`*

```
1-59/5 * * * * root test -x /usr/sbin/atrun && /usr/sbin/atrun
```

Você não pode editar `/etc/crontab` chamando o comando `crontab -e`. Esse arquivo deve ser carregado diretamente em um editor, modificado e gravado.

Alguns pacotes instalam scripts de shell nos diretórios `/etc/cron.hourly`, `/etc/cron.daily`, `/etc/cron.weekly` e `/etc/cron.monthly`, cuja execução é controlada por `/usr/lib/cron/run-crons`. `/usr/lib/cron/run-crons` é executado a cada 15 minutos da tabela principal (`/etc/crontab`). Isso garante que os processos que tenham sido negligenciados possam ser executados no momento adequado.

Para executar os scripts de manutenção por hora, diário ou outros scripts de manutenção periódica em horários personalizados, remova os arquivos de marcação de horário regularmente, utilizando as entradas `/etc/crontab` (consulte o Exemplo 11.2, “`/etc/crontab`: remova arquivos de marcação de horário” (p 131), que remove a opção por hora antes de cada hora cheia, a opção diário uma vez ao dia às 2h:14 etc.).

Exemplo 11.2 */etc/crontab: remova arquivos de marcação de horário*

```
59 * * * * root rm -f /var/spool/cron/lastrun/cron.hourly
14 2 * * * root rm -f /var/spool/cron/lastrun/cron.daily
29 2 * * 6 root rm -f /var/spool/cron/lastrun/cron.weekly
44 2 1 * * root rm -f /var/spool/cron/lastrun/cron.monthly
```

Ou você pode definir `DAILY_TIME` em `/etc/sysconfig/cron` com o horário de início de `cron.daily`. A configuração de `MAX_NOT_RUN` assegura que as tarefas diárias sejam acionadas para execução, mesmo se o usuário não ligou o computador no `DAILY_TIME` especificado por um período mais longo. O valor máximo de `MAX_NOT_RUN` é 14 dias.

Os trabalhos de manutenção diária de sistema são distribuídos a vários scripts por motivos de clareza. Eles estão contidos no pacote `aaa_base`. `/etc/cron.daily` contém, por exemplo, os componentes `suse.de-backup-rpmdb`, `suse.de-clean-tmp` ou `suse.de-cron-local`.

11.1.3 Arquivos de registro: pacote logrotate

Existem vários serviços de sistema (*daemons*) que, junto com o próprio kernel, gravam regularmente o status do sistema e eventos específicos em arquivos de registro. Dessa maneira, o administrador pode verificar regularmente o status do sistema em um determinado momento, reconhecer erros ou funções defeituosas e solucioná-los com

total precisão. Esses arquivos de registro são normalmente armazenados em `/var/log`, como especificado pelo FHS, e crescem diariamente. O pacote `logrotate` ajuda a controlar o crescimento desses arquivos.

Configure o `logrotate` com o arquivo `/etc/logrotate.conf`. Em particular, a especificação `include` configura principalmente os arquivos adicionais a serem lidos. Programas que produzem arquivos de registro instalam arquivos de configuração individuais em `/etc/logrotate.d`. Por exemplo, tais programas acompanham os pacotes, como `apache2` (`/etc/logrotate.d/apache2`) e `syslogd` (`/etc/logrotate.d/syslog`).

Exemplo 11.3 *Exemplo para `/etc/logrotate.conf`*

```
# see "man logrotate" for details
# rotate log files weekly
weekly

# keep 4 weeks worth of backlogs
rotate 4

# create new (empty) log files after rotating old ones
create

# uncomment this if you want your log files compressed
#compress

# RPM packages drop log rotation information into this directory
include /etc/logrotate.d

# no packages own lastlog or wtmp - we'll rotate them here
#/var/log/wtmp {
#   monthly
#   create 0664 root utmp
#   rotate 1
#}

# system-specific logs may be also be configured here.
```

`logrotate` é controlado pelo `cron` e é chamado diariamente por `/etc/cron.daily/logrotate`.

IMPORTANTE

A opção `create` lê todas as configurações feitas pelo administrador em `/etc/permissions*`. Certifique-se de que não haja conflitos devido a modificações pessoais.

11.1.4 O comando `locate`

`locate`, um comando para localização rápida de arquivos, não está incluído no escopo padrão do software instalado. Se desejado, instale o pacote `findutils-locate`. O processo `updatedb` é iniciado automaticamente a cada noite ou aproximadamente 15 minutos após a inicialização do sistema.

11.1.5 O comando `ulimit`

Com o comando `ulimit` (*limites do usuário*), é possível definir limites para o uso dos recursos do sistema e fazer com que sejam exibidos. O `ulimit` é especialmente útil para limitar a memória disponível para os aplicativos. Com isso, um aplicativo pode ser impedido de absorver recursos em demasia do sistema e deixar o sistema operacional lento ou até travá-lo.

O comando `ulimit` pode ser usado com várias opções. Para limitar o uso da memória, use as opções listadas na Tabela 11.1, “`ulimit`: definindo recursos para o usuário” (p 133).

Tabela 11.1 *ulimit: definindo recursos para o usuário*

<code>-m</code>	O tamanho máximo do conjunto residente
<code>-v</code>	A quantidade máxima de memória virtual disponível para o shell
<code>-s</code>	O tamanho máximo da pilha
<code>-c</code>	O tamanho máximo dos arquivos básicos criados

Entradas globais de sistema podem ser feitas em `/etc/profile`. Lá, habilite a criação de arquivos básicos (necessários aos programadores para *depuração*). Um usuário normal não pode aumentar os valores especificados em `/etc/profile` pelo administrador do sistema, mas pode fazer entradas especiais em `~/ .bashrc`.

Exemplo 11.4 *ulimit: configurações em `~/ .bashrc`*

```
# Limits maximum resident set size (physical memory):
ulimit -m 98304

# Limits of virtual memory:
ulimit -v 98304
```

As alocações de memória devem ser especificadas em KB. Para obter informações mais detalhadas, consulte `man bash`.

IMPORTANTE

Nem todos os shells suportam as diretivas `ulimit`. O PAM (por exemplo, `pam_limits`) oferece possibilidades abrangentes de ajustes se você depende de configurações abrangentes para essas restrições.

11.1.6 O comando `free`

O comando `free` é um pouco confuso se a sua meta é determinar a quantidade de memória RAM usada no momento. Essa informação pode ser encontrada em `/proc/meminfo`. Atualmente, os usuários com acesso a um sistema operacional moderno, como o Linux, não precisam se preocupar muito com memória. O conceito de *RAM disponível* surgiu antes da época do gerenciamento unificado de memória. O slogan *memória livre é memória ruim* se aplica bem ao Linux. Como resultado, o Linux sempre se esforçou para equilibrar caches externos sem realmente permitir memória livre ou sem uso.

Basicamente, o kernel não tem conhecimento direto de nenhum aplicativo ou dados de usuário. Em vez disso, ele gerencia aplicativos e dados de usuário em um *cache de página*. Se a memória diminuir, partes dele são gravadas na partição de troca ou em

arquivos, dos quais podem ser lidas inicialmente com a ajuda do comando `mmap` (consulte `man mmap`).

O kernel também contém outros caches, como o *cache slab*, onde os caches usados para acesso a rede são armazenados. Isso pode explicar as diferenças entre os contadores em `/proc/meminfo`. A maioria deles (mas não todos) pode ser acessada via `/proc/slabinfo`.

11.1.7 Páginas de manual e de informações

Para alguns aplicativos GNU (como o `tar`), as páginas de manuais não são mais mantidas. Para esses comandos, use a opção `--help` para obter uma breve visão geral das páginas de informações, que fornecem instruções mais detalhadas. O `info` é um sistema de hipertexto do GNU. Leia uma introdução sobre esse sistema digitando `info info`. As páginas de informações podem ser exibidas com Emacs digitando `emacs -f info` ou diretamente em um console, com `info`. Também é possível usar `tkinfo`, `xinfo` ou o sistema de ajuda do para exibir as páginas de informações.

11.1.8 Selecionando páginas de manual usando o comando man

Com `man página_de_manual`, normalmente você exibe uma página de manual para leitura instantânea. Mas se existir uma página de manual com o mesmo nome em seções diferentes, `man` perguntará ao usuário a seção cuja página deverá ficar visível. O usuário então deverá responder digitando a seção.

Se desejar retornar ao comportamento anterior, defina `MAN_POSIXLY_CORRECT=1` em um arquivo de inicialização de shell como `~/.bashrc`.

11.1.9 Configurações para GNU Emacs

O GNU Emacs é um complexo ambiente de trabalho. As seções a seguir descrevem os arquivos de configuração processados quando o GNU Emacs é iniciado. Há mais informações em <http://www.gnu.org/software/emacs/>.

Na inicialização, o Emacs lê vários arquivos que contêm as configurações do usuário, administrador do sistema e distribuidor para personalização ou pré-configuração. O arquivo de inicialização `~/ .emacs` é instalado nos diretórios pessoais dos usuários individuais por meio de `/etc/skel`. O `.emacs`, por sua vez, lê o arquivo `/etc/skel/.gnu-emacs`. Para personalizar o programa, copie o arquivo `.gnu-emacs` para o diretório pessoal (com `cp /etc/skel/.gnu-emacs ~/.gnu-emacs`) e faça as configurações desejadas nesse diretório.

O `.gnu-emacs` define o arquivo `~/ .gnu-emacs-custom` como arquivo personalizado. Se os usuários tiverem feito as configurações com as opções personalizar no Emacs, as configurações serão gravadas no arquivo `~/ .gnu-emacs-custom`.

Com o SUSE Linux Enterprise Desktop, o pacote do `emacs` instala o arquivo `site-start.el` no diretório `/usr/share/emacs/site-lisp`. O arquivo `site-start.el` é carregado antes do arquivo de inicialização `~/ .emacs`. Entre outras coisas, o arquivo `site-start.el` assegura que os arquivos de configuração especial distribuídos com os pacotes de expansão do Emacs, como o `psgml`, sejam carregados automaticamente. Os arquivos de configuração deste tipo também estão localizados em `/usr/share/emacs/site-lisp`, e sempre começam com o nome `suse-start-`. O administrador do sistema local pode especificar configurações globais do sistema no arquivo `default.el`.

Mais informações sobre esses arquivos estão disponíveis no arquivo de informações do Emacs em *Init File*: [info:/emacs/InitFile](http://info:emacs/InitFile). Informações sobre como desabilitar o carregamento desses arquivos, se necessário, também são fornecidas neste local.

Os componentes do Emacs são divididos em vários pacotes:

- O pacote base `emacs`.
- `emacs-x11` (geralmente instalado): o programa *com* suporte para X11.
- `emacs-nox`: o programa *sem* suporte para X11.
- `emacs-info`: documentação online em formato `info`.

- `emacs-el`: os arquivos de biblioteca não compilados em Emacs Lisp. Eles não são necessários em tempo de execução.
- Numerosos pacotes complementares podem ser instalados se necessário: `emacs-auctex` (LaTeX), `psgml` (SGML e XML), `gnuserv` (operação cliente e servidor) e outros.

11.2 Consoles virtuais

O Linux é um sistema multiusuário e multitarefa. As vantagens desses recursos podem ser apreciadas mesmo em um sistema de PC independente. No modo de texto, existem seis consoles virtuais disponíveis. Alterne entre eles utilizando a combinação de teclas de Alt + F1 até Alt + F6. O sétimo console é reservado para X e o décimo console mostra as mensagens do kernel. Podem ser atribuídos mais ou menos consoles com a modificação do arquivo `/etc/inittab`.

Para alternar para um console de X sem o fechar, use a combinação de teclas de Ctrl + Alt + F1 até Ctrl + Alt + F6. Para voltar para X, pressione Alt + F7.

11.3 Mapeamento de teclado

Para padronizar o mapeamento de teclado de programas, foram feitas mudanças nos seguintes arquivos:

```
/etc/inputrc
/etc/X11/Xmodmap
/etc/skel/.Xmodmap
/etc/skel/.exrc
/etc/skel/.less
/etc/skel/.lesskey
/etc/csh.cshrc
/etc/termcap
/usr/lib/terminfo/x/xterm
/usr/share/X11/app-defaults/XTerm
/usr/share/emacs/VERSION/site-lisp/term/*.el
```

Essas mudanças afetam apenas aplicativos que utilizam entradas `terminfo` ou cujos arquivos de configuração são mudados diretamente (`vi`, `less` etc.). Os aplicativos que não acompanham o sistema devem ser adaptados a esses padrões.

Em X, a chave de composição (multikey) pode ser acessada utilizando Ctrl + Shift (direita). Consulte também a entrada correspondente em `/etc/X11/Xmodmap`.

Outras configurações são possíveis utilizando-se a Extensão de Teclado X (XKB). Essa extensão também é usada pelos ambientes de área de trabalho GNOME (gswitchit) e KDE (kxkb).

DICA: para obter mais informações

Há informações sobre o XKB disponíveis nos documentos listados em `/usr/share/doc/packages/xkeyboard-config` (parte do pacote `xkeyboard-config`).

11.4 Configurações de idioma e específicas de país

O sistema está em grande parte internacionalizado e pode ser modificado flexivelmente de acordo com as necessidades locais. Em outras palavras, a internacionalização (*I18N*) permite localizações específicas (*L10N*). As abreviações I18N e L10N são derivadas das primeiras e últimas letras das palavras e, no meio, está o número de letras omitidas.

As configurações são feitas com variáveis `LC_` definidas no arquivo `/etc/sysconfig/language`. Elas referem-se não somente ao *suporte ao idioma nativo*, mas também às categorias *Mensagens* (Idioma), *Conjunto de Caracteres*, *Ordem de Classificação*, *Hora e Data*, *Números* e *Moeda*. Cada uma dessas categorias pode ser definida diretamente com sua própria variável ou indiretamente com uma variável master no arquivo `language` (consulte a página de manual `local`).

`RC_LC_MESSAGES`, `RC_LC_CTYPE`, `RC_LC_COLLATE`, `RC_LC_TIME`,
`RC_LC_NUMERIC`, `RC_LC_MONETARY`

Essas variáveis são passadas para o shell sem o prefixo `RC_` e representam as categorias listadas. Os perfis shell de referência estão listados abaixo. A configuração atual pode ser exibida com o comando `locale`.

`RC_LC_ALL`

Essa variável, se definida, sobregrava os valores das variáveis já mencionadas.

RC_LANG

Se nenhuma das variáveis anteriores for definida, esse é o fallback. Por padrão, apenas RC_LANG está definida. Isso facilita o processo para que os usuários informem seus próprios valores.

ROOT_USES_LANG

Uma variável `yes` ou `no`. Se for definida como `no`, `root` sempre funcionará no ambiente POSIX.

As variáveis podem ser definidas com o editor `sysconfig` do YaST (consulte a Seção 9.3.1, “Mudando a configuração do sistema com o Editor `sysconfig` do YaST” (p 101)). O valor dessa variável contém o código do idioma, código do país, codificação e modificador. Os componentes individuais são conectados por caracteres especiais:

```
LANG=<language>[_<COUNTRY>].<Encoding>[@<Modifier>]
```

11.4.1 Alguns exemplos

Você deve sempre definir os códigos do idioma e do país juntos. As configurações do idioma seguem o padrão ISO 639 disponível em <http://www.evertype.com/standards/iso639/iso639-en.html> e <http://www.loc.gov/standards/iso639-2/>. Os códigos de país estão listados na variável ISO 3166 disponível em http://www.din.de/gremien/nas/nabd/iso3166ma/codlstp1/en_listp1.html.

Só faz sentido definir valores para os quais os arquivos de descrição utilizáveis podem ser encontrados em `/usr/lib/locale`. Arquivos de descrição adicionais podem ser criados de arquivos em `/usr/share/i18n` utilizando o comando `localedef`. Os arquivos de descrição fazem parte do pacote `glibc-i18ndata`. Um arquivo de descrição para `en_US.UTF-8` (para inglês e Estados Unidos) pode ser criado com:

```
localedef -i en_US -f UTF-8 en_US.UTF-8
```

```
LANG=en_US.UTF-8
```

Essa é a configuração padrão se Inglês americano for selecionado durante a instalação. Se você tiver selecionado outro idioma, ele será habilitado, mas ainda terá o UTF-8 como codificação de caractere.

```
LANG=en_US.ISO-8859-1
```

Define o idioma como inglês, o país como Estados Unidos e o conjunto de caracteres como ISO-8859-1. Essa definição de caractere não suporta o sinal de Euro, mas às vezes pode ser útil para programas que não foram atualizados para suportar UTF-8. A string que define o conjunto de caracteres (ISO-8859-1 nesse caso) é então avaliada por programas como o Emacs.

```
LANG=en_IE@euro
```

O exemplo acima inclui explicitamente o sinal de Euro em uma configuração de idioma. Essa configuração está basicamente obsoleta agora, pois o UTF-8 também cobre o símbolo do Euro. Será útil apenas se um aplicativo suportar ISO-8859-15 e não UTF-8.

O SuSEconfig lê as variáveis em `/etc/sysconfig/language` e grava as mudanças necessárias em `/etc/SuSEconfig/profile` e `/etc/SuSEconfig/csh.cshrc`. `/etc/SuSEconfig/profile` é lido ou *originado* por `/etc/profile`. `/etc/SuSEconfig/csh.cshrc` é originado por `/etc/csh.cshrc`. Isso torna as configurações disponíveis em todo o sistema.

Os usuários anular os padrões do sistema editando o seu `~/ .bashrc` da maneira adequada. Por exemplo, se você não quiser usar o `en_US` para mensagens de programa em todo o sistema, inclua `LC_MESSAGES=es_ES` para que as mensagens sejam exibidas em espanhol.

11.4.2 Configurações locais em `~/ .i18n`

Se não estiver satisfeito com os padrões do sistema local, mude as configurações em `~/ .i18n` de acordo com a sintaxe de script Bash. As entradas em `~/ .i18n` substituem os padrões do sistema de `/etc/sysconfig/language`. Use os mesmos nomes de variáveis, mas sem os prefixos de namespace `RC_`. Por exemplo, use `LANG` em vez de `RC_LANG`:

```
LANG=cs_CZ.UTF-8
LC_COLLATE=C
```

11.4.3 Configurações de suporte de idioma

Arquivos na categoria *Mensagens* são, via de regra, armazenados somente no diretório do idioma correspondente (como `en`) para ter um fallback. Se você definir `LANG` para `en_US` e o arquivo de mensagem em `/usr/share/locale/en_US/LC_MESSAGES` não existir, ele voltará para `/usr/share/locale/en/LC_MESSAGES`.

Uma cadeia de fallback também pode ser definida, por exemplo, para bretão para francês ou galego para espanhol para português:

```
LANGUAGE="br_FR:fr_FR"
```

```
LANGUAGE="gl_ES:es_ES:pt_PT"
```

Se desejar, use as variantes norueguesas Nynorsk e Bokmål (com fallback adicional para não):

```
LANG="nn_NO"
```

```
LANGUAGE="nn_NO:nb_NO:no"
```

ou

```
LANG="nb_NO"
```

```
LANGUAGE="nb_NO:nn_NO:no"
```

Observe que em norueguês, `LC_TIME` também é tratado de maneira diferente.

Um problema que pode surgir é um separador usado para delimitar grupos de dígitos não ser reconhecido corretamente. Isso acontece se `LANG` for definido para um código de idioma com somente duas letras, como `de`, mas o arquivo de definição que o glibc utiliza estiver localizado em `/usr/share/lib/de_DE/LC_NUMERIC`. Por isso, `LC_NUMERIC` deve ser definido como `de_DE` para tornar a definição de separador visível para o sistema.

11.4.4 Para obter mais informações

- *The GNU C Library Reference Manual*, Capítulo “Locales and Internationalization”. Ele está incluído em `glibc-info`.
- Markus Kuhn, *UTF-8 and Unicode FAQ for Unix/Linux*, atualmente em <http://www.cl.cam.ac.uk/~mgk25/unicode.html>.
- *Unicode-Howto*, de Bruno Haible: `/usr/share/doc/howto/en/txt/Unicode-HOWTO.gz` (pacote `howto`).

Operação da impressora

O SUSE® Linux Enterprise Desktop suporta a impressão com muitos tipos de impressoras, incluindo impressoras de rede remotas. É possível configurar as impressoras manualmente ou com o YaST. Para obter instruções de configuração, consulte a Seção “Setting Up a Printer” (Capítulo 5, *Setting Up Hardware Components with YaST*, ↑ *Guia de Implantação*). Os utilitários gráficos e de linha de comando estão disponíveis para iniciar e gerenciar serviços de impressão. Se a sua impressora não funcionar como se esperava, consulte a Seção 12.7, “Solução de problemas” (p 153).

O CUPS é o sistema de impressão padrão do SUSE Linux Enterprise Desktop. Ele é altamente orientado ao usuário. Em muitos casos, é compatível com LPRng ou pode ser adaptado com relativamente pouco esforço. O LPRng é incluído no SUSE Linux Enterprise Desktop apenas por motivos de compatibilidade.

As impressoras podem ser distinguidas pela interface, como USB ou rede, e pela linguagem de impressão. Ao comprar uma impressora, verifique se há no seu hardware uma interface (como porta USB ou paralela) disponível para ela e uma linguagem de impressora adequada. As impressoras podem ser categorizadas com base em três classes de linguagem:

Impressoras PostScript

PostScript é a linguagem de impressora na qual a maior parte dos serviços de impressão em Linux e Unix são gerados e processados pelo sistema de impressão interno. Essa linguagem já existe há bastante tempo e é muito eficiente. Se documentos PostScript puderem ser diretamente processados pela impressora e não precisarem ser convertidos em estágios adicionais do sistema de impressão, o número de origens de erro potenciais será reduzido. Como as impressoras PostScript

estão sujeitas a custos de licenciamento substanciais, elas geralmente custam mais que as impressoras sem interpretador PostScript.

Impressora padrão (linguagens como PCL e ESC/P)

Embora essas linguagens de impressora tenham surgido há bastante tempo, ainda são usadas e sofrem constantes desenvolvimentos para se adaptarem aos novos recursos de impressoras. No caso de linguagens conhecidas, o sistema pode converter tarefas de impressão PostScript na respectiva linguagem de impressão com a ajuda do Ghostscript. Esse estágio de processamento é chamado de interpretação. As linguagens mais conhecidas são PCL (mais usada pelas impressoras HP e seus clones) e ESC/P (utilizada nas impressoras Epson). Geralmente, essas linguagens são suportadas no Linux e produzem um resultado de impressão adequado. Pode ocorrer de o Linux não conseguir lidar com algumas funções de impressoras muito recentes e de alta tecnologia, já que os desenvolvedores de código-fonte aberto talvez ainda estejam trabalhando nesses recursos. Além da HP, que desenvolve o HPLIP, nenhum outro fabricante de impressora desenvolve e disponibiliza drivers do Linux aos distribuidores do Linux como licença de código-fonte aberto. A maior parte dessas impressoras está na faixa de preços intermediária.

Impressoras proprietárias (também denominadas impressoras GDI)

Essas impressoras não suportam nenhuma das linguagens de impressora comuns. Elas usam suas próprias linguagens de impressora não documentadas, que ficam sujeitas a mudanças quando é lançada uma edição nova de um modelo. Geralmente, apenas os drivers do Windows estão disponíveis para essas impressoras. Consulte a Seção 12.7.1, “Impressoras sem suporte de linguagem de impressora padrão” (p 153) para obter mais informações.

Antes de comprar uma nova impressora, consulte as seguintes fontes para verificar a abrangência do suporte ao equipamento pretendido:

<http://www.linuxfoundation.org/OpenPrinting/>

A home page OpenPrinting com o banco de dados de impressão. O banco de dados sempre mostra o status de suporte Linux mais recente. No entanto, a distribuição do Linux só pode integrar os drivers disponíveis no momento da produção. Da mesma forma, uma impressora atualmente classificada como “perfeitamente suportada” talvez não apresentasse esse status quando a versão mais recente do SUSE Linux Enterprise Desktop foi lançada. Assim, os bancos de dados não indicarão necessariamente o status correto, mas apenas uma informação aproximada.

<http://www.cs.wisc.edu/~ghost/>

Página do Ghostscript na Web.

`/usr/share/doc/packages/ghostscript-library/catalog.devices`

Listas de drivers incluídos.

12.1 Fluxo de trabalho do sistema de impressão

O usuário cria um serviço de impressão. O serviço de impressão consiste nos dados a serem impressos mais as informações para o spooler, como nome da impressora ou nome da fila de impressão e, opcionalmente, informações para o filtro, como opções específicas da impressora.

Existe pelo menos uma fila de impressão dedicada para cada impressora. O spooler mantém o serviço de impressão em fila até que a impressora desejada esteja pronta para receber dados. Uma vez pronta, o spooler envia os dados pelo filtro, tendo a impressora como back end.

O filtro converte os dados gerados pelo aplicativo que está imprimindo (geralmente PostScript ou PDF, mas também ASCII, JPEG e outros) em dados específicos da impressora (PostScript, PCL, ESC/P etc.). Os recursos da impressora são descritos nos arquivos PPD. O arquivo PPD contém opções da impressora com os parâmetros necessários para habilitá-los. O sistema de filtros verifica se as opções selecionadas pelo usuário foram habilitadas.

Se você usa uma impressora PostScript, o sistema de filtros converte os dados em PostScript específico da impressora. Isso não exige um driver de impressora. Se você usa uma impressora não-PostScript, o sistema de filtros converte os dados em dados específicos da impressora. Isso exige um driver adequado à sua impressora. O back end recebe do filtro os dados específicos da impressora e os repassa a ela.

12.2 Métodos e protocolos de conexão de impressoras

Existem várias possibilidades para conectar uma impressora ao sistema. A configuração do sistema de impressão CUPS não faz distinção entre uma impressora local e uma impressora conectada ao sistema pela rede. No Linux, impressoras locais devem ser conectadas conforme descrito no manual do respectivo fabricante. O CUPS suporta conexões seriais, USB, paralelas e SCSI.

ATENÇÃO: mudando as conexões de cabo em um sistema em execução

Ao conectar a impressora à máquina, não esqueça de que apenas dispositivos USB podem ser conectados ou desconectados durante a operação. Para evitar danos ao sistema ou à impressora, encerre o sistema antes de mudar qualquer conexão que não seja USB.

12.3 Instalando o software

PPD (descrição de impressora PostScript) é a linguagem de computador que descreve as propriedades, como resolução, e as opções, como disponibilidade de uma unidade duplex. Essas descrições são necessárias para o uso de várias opções de impressora no CUPS. Sem um arquivo PPD, os dados de impressão seriam encaminhados à impressora em estado “bruto”, o que normalmente não é desejado. Durante a instalação do SUSE Linux Enterprise Desktop, muitos arquivos PPD são pré-instalados.

Para configurar uma impressora PostScript, a melhor opção é obter um arquivo PPD adequado. Há vários arquivos PPD disponíveis no pacote de PPDs do fabricante, que são automaticamente instalados no escopo da instalação padrão. Consulte a Seção 12.6.2, “Arquivos PPD em pacotes diferentes” (p 151) e a Seção 12.7.2, “Nenhum arquivo PPD adequado disponível para impressora PostScript” (p 154).

Novos arquivos PPD podem ser armazenados no diretório `/usr/share/cups/model/` ou adicionados ao sistema de impressão por meio do YaST (conforme descrito na “Adding Drivers with YaST” (Capítulo 5, *Setting Up Hardware Components with YaST*, ↑*Guia de Implantação*)). Posteriormente, é possível selecionar o arquivo PPD durante a instalação.

Tenha cuidado se o fabricante pedir que você instale pacotes de software inteiros para modificar arquivos de configuração. Em primeiro lugar, esse tipo de instalação pode resultar na perda do suporte oferecido pelo SUSE Linux Enterprise Desktop. Em segundo lugar, os comandos de impressão poderão funcionar de forma diferente, e talvez o sistema não consiga lidar com dispositivos de outros fabricantes. Por isso, não recomendamos instalar o software do fabricante.

12.4 Impressoras de rede

Uma impressora de rede pode suportar vários protocolos, alguns deles simultaneamente. Embora a maioria dos protocolos suportados sejam padronizados, alguns fabricantes expandem (modificam) o padrão porque eles testam sistemas que não implementaram o padrão corretamente ou porque querem fornecer certas funções que não estão disponíveis no padrão. Os fabricantes fornecem drivers apenas para alguns sistemas operacionais, eliminando dificuldades relativas a eles. Infelizmente, raros são os drivers para Linux. Na situação atual, não é possível agir como se todos os protocolos funcionassem perfeitamente no Linux. Portanto, talvez seja necessário testar várias opções para obter uma configuração funcional.

O CUPS suporta os protocolos `socket`, `LPD`, `IPP` e `smb`.

soquete

Soquete se refere a uma conexão na qual os dados são enviados a um soquete de Internet sem precedência de handshake de dados. Alguns dos números de portas de soquete normalmente usados são 9100 ou 35. A sintaxe do URI (uniform resource identifier) do dispositivo é `socket://IP.da.impressora:porta`, por exemplo: `socket://192.168.2.202:9100/`.

LPD (Line Printer Daemon)

O protocolo LPD comprovado é descrito em RFC 1179. Nesse protocolo, alguns dados relativos à tarefa, como ID da fila de impressão, são enviados antes dos dados de impressão propriamente ditos. Portanto, deve ser especificada uma fila de impressão durante a configuração do protocolo LPD para a transmissão de dados. As implementações de fabricantes de impressoras diferentes são flexíveis o suficiente para aceitar qualquer nome como fila de impressão. Se necessário, o manual da impressora indicará o nome a ser usado. Geralmente se usa LPT, LPT1, LP1 ou nomes semelhantes. Também é possível configurar uma fila LPD em um host Linux ou Unix diferente no sistema CUPS. O número de porta para o serviço

LPD é 515. Um exemplo de URI de dispositivo é

`lpd://192.168.2.202/LPT1.`

IPP (Internet Printing Protocol)

O IPP é um protocolo relativamente novo (1999) baseado no protocolo HTTP.

Com o IPP, mais dados referentes à tarefa são transmitidos. O CUPS usa o IPP em transmissões internas de dados. É o protocolo escolhido para a fila de encaminhamento entre dois servidores CUPS. É necessário indicar o nome da fila de impressão para que o IPP seja configurado corretamente. A porta padrão do IPP é 631. Exemplos de URIs de dispositivo: `ipp://192.168.2.202/ps` e `ipp://192.168.2.202/printers/ps.`

SMB (compartilhamento Windows)

O CUPS também suporta a impressão em impressoras conectadas a compartilhamentos Windows. O protocolo usado para essa finalidade é o SMB. O SMB usa os números de porta 137, 138 e 139. Exemplos de URIs de dispositivo: `smb://user:password@workgroup/smb.example.com/printer,` `smb://user:password@smb.example.com/printer` e `smb://smb.example.com/printer.`

O protocolo suportado pela impressora deve ser determinado antes da configuração. Se o fabricante não fornecer as informações necessárias, o comando `nmap` (que vem com o pacote `nmap`) pode ser usado para verificar o protocolo. O `nmap` verifica se há portas abertas em um host. Por exemplo:

```
nmap -p 35,137-139,515,631,9100-10000 printerIP
```

12.4.1 Configurando o CUPS com ferramentas da linha de comando

Além de configurar as opções do CUPS com o YaST durante a configuração de uma impressora de rede, o CUPS pode ser configurado com ferramentas de linha de comando como `lpadmin` e `lpoptions`. Você precisa de um URI de dispositivo composto por um back end, como uma porta paralela, e parâmetros. Para determinar os URIs de dispositivo válidos no sistema, use o comando `lpinfo -v | grep " :/ ":`

```
# lpinfo -v | grep " :/ ":
direct usb://ACME/FunPrinter%20XL
direct parallel:/dev/lp0
```

Com `lpadmin`, o administrador do servidor CUPS pode adicionar, remover ou gerenciar filas de classe e de impressão. Para adicionar uma fila de impressão, use a seguinte sintaxe:

```
lpadmin -p queue -v device-URI -P PPD-file -E
```

Em seguida, o dispositivo (`-v`) fica disponível como *fila* (`-p`), usando o arquivo PPD especificado (`-P`). Isso significa que você precisa saber qual é o arquivo PPD e o URI de dispositivo para configurar a impressora manualmente.

Não use `-E` como primeira opção. Em todos os comandos CUPS, `-E` como primeiro argumento define o uso de uma conexão criptografada. Para habilitar a impressora, `-E` deve ser usado como mostrado no seguinte exemplo:

```
lpadmin -p ps -v parallel:/dev/lp0 -P \
/usr/share/cups/model/Postscript.ppd.gz -E
```

O seguinte exemplo configura uma impressora de rede:

```
lpadmin -p ps -v socket://192.168.2.202:9100/ -P \
/usr/share/cups/model/Postscript-levell.ppd.gz -E
```

Para conhecer mais opções de `lpadmin`, consulte a página de manual de `lpadmin(8)`.

Durante a configuração da impressora, algumas opções são definidas como padrão. Essas opções podem ser modificadas para cada serviço de impressão (dependendo da ferramenta de impressão utilizada). Também é possível modificar essas opções padrão com o YaST. Usando ferramentas de linha de comando, defina opções padrão da seguinte forma:

1 Primeiro, liste todas as opções:

```
lpoptions -p queue -l
```

Exemplo:

```
Resolution/Output Resolution: 150dpi *300dpi 600dpi
```

A opção padrão ativada é identificada por um asterisco na frente (*).

2 Mude a opção com `lpadmin`:

```
lpadmin -p queue -o Resolution=600dpi
```

3 Verifique a nova configuração:

```
lpoptions -p queue -l
```

```
Resolution/Output Resolution: 150dpi 300dpi *600dpi
```

Quando um usuário comum executa `lpoptions`, as configurações são gravadas em `~/.cups/lpoptions`. Porém, as configurações de `root` são gravadas em `/etc/cups/lpoptions`.

12.5 Imprimindo pela linha de comando

Para imprimir pela linha de comando, digite `lp-d nome da fila nome do arquivo`, substituindo *nome da fila* e *nome do arquivo* pelos nomes correspondentes.

Alguns aplicativos dependem do comando `lp` para imprimir. Nesse caso, digite o comando correto na caixa de diálogo do aplicativo, geralmente sem especificar *nome do arquivo*, por exemplo `lp -d nome da fila`.

12.6 Recursos especiais do SUSE Linux Enterprise Desktop

Alguns recursos do CUPS foram adaptados para o SUSE Linux Enterprise Desktop. Algumas das mudanças mais importantes são abordadas aqui.

12.6.1 CUPS e firewall

Depois de uma instalação padrão do SUSE Linux Enterprise Desktop, o `SuSEfirewall2` fica ativo e as interfaces de rede são configuradas para estarem na `Zona Externa`, que bloqueia tráfego de entrada. Essas configurações padrão precisam ser ajustadas quando se usa o CUPS. Mais informações sobre a configuração do `SuSEfirewall2` estão disponíveis na Seção “`SuSEfirewall2`” (Capítulo 15, *Masquerading and Firewalls*, ↑*Security Guide (Guia de Segurança)*).

Cliente CUPS

Normalmente, um cliente CUPS é executado em uma estação de trabalho comum, localizada em um ambiente de rede confiável atrás de um firewall. Neste caso, é recomendável configurar a interface de rede para ficar na `Zona Interna`, de modo que a estação de trabalho possa ser alcançada de dentro da rede.

Servidor CUPS

Se o servidor CUPS fizer parte de um ambiente de rede confiável, protegido por um firewall, a interface de rede deverá ser configurada para ficar na `Zona Interna` do firewall. Não é recomendado configurar um servidor CUPS em um ambiente de rede não confiável, a menos que você tenha o cuidado de mantê-lo protegido por regras especiais de firewall e opções seguras na configuração do CUPS.

12.6.2 Arquivos PPD em pacotes diferentes

A configuração de impressora do YaST define as filas do CUPS usando apenas os arquivos PPD instalados em `/usr/share/cups/model/`. Para localizar os arquivos PPD adequados ao modelo da impressora, o YaST compara o fabricante e o modelo determinados durante a detecção de hardware com os fabricantes e modelos de todos os arquivos PPD disponíveis em `/usr/share/cups/model/` no sistema. Para isso, a configuração de impressora do YaST gera um banco de dados com as informações de fabricante e modelo extraídas dos arquivos PPD. Quando você seleciona uma impressora, recebe os arquivos PPD que correspondem ao fabricante e ao modelo da lista de modelos.

A configuração com apenas arquivos PPD e nenhuma outra fonte de informação tem a vantagem de permitir a livre modificação de arquivos PPD em `/usr/share/cups/model/`. A configuração de impressora do YaST reconhece as mudanças e gera novamente o banco de dados de fabricantes e modelos. Por exemplo, se você tem apenas impressoras PostScript, normalmente não precisa dos arquivos PPD Foomatic do pacote `cups-drivers` ou os arquivos PPD Gutenprint do pacote `gutenprint`. Em vez disso, os arquivos PPD das suas impressoras PostScript podem ser copiados diretamente para `/usr/share/cups/model` (se já não existem no pacote `manufacturer-PPDs`) para proporcionarem uma configuração ideal para suas impressoras.

Arquivos PPD do CUPS do pacote cups

Os arquivos PPD genéricos do pacote cups foram complementados com arquivos PPD Foomatic adaptados para impressoras PostScript nível 1 e 2:

- /usr/share/cups/model/Postscript-level1.ppd.gz
- /usr/share/cups/model/Postscript-level2.ppd.gz

Arquivos PPD do pacote cups-drivers

Normalmente, o filtro de impressora Foomatic `foomatic-rip` é usado junto com Ghostscript para impressoras não-PostScript. Os arquivos PPD Foomatic adequados possuem as entradas `*NickName: ... Foomatic/Ghostscript driver` e `*cupsFilter: ... foomatic-rip`. Esses arquivos PPD estão localizados no pacote cups-drivers.

O YaST geralmente prefere um arquivo `manufacturer-PPD`. Entretanto, quando não existe nenhum arquivo `manufacturer-PPD` adequado, um arquivo PPD Foomatic com a entrada `*NickName: ... Foomatic ... (recommended)` é selecionado.

Arquivos PPD Gutenprint do pacote gutenprint

Em vez de `foomatic-rip`, o filtro CUPS `rastertogutenprint` do Gutenprint (antes conhecido como GIMP-Print) pode ser usado em várias impressoras não-PostScript. Esse filtro e os arquivos PPD Gutenprint adequados estão disponíveis no pacote gutenprint. Os arquivos PPD Gutenprint estão localizados em `/usr/share/cups/model/gutenprint/` e possuem as entradas `*NickName: ... CUPS+Gutenprint` e `*cupsFilter: ... rastertogutenprint`.

Arquivos PPD de fabricantes de impressoras no pacote manufacturer-PPDs

O pacote `manufacturer-PPDs` contém arquivos PPD de fabricantes de impressoras que são liberados mediante uma licença suficientemente permissiva. Impressoras

PostScript devem ser configuradas com o arquivo PPD adequado do fabricante da impressora, já que esse arquivo permite o uso de todas as funções da impressora PostScript. O YaST prefere um arquivo PPD do `manufacturer-PPDs`. O YaST não poderá usar nenhum arquivo PPD do pacote `manufacturer-PPDs` se o nome do modelo não encontrar correspondência. Isso poderá ocorrer se o pacote `manufacturer-PPDs` contiver apenas um arquivo PPD para modelos semelhantes, como a série Funprinter 12xx. Nesse caso, selecione manualmente o arquivo PPD correspondente no YaST.

12.7 Solução de problemas

As seções a seguir abordam alguns dos problemas mais encontrados em relação a hardware e software de impressora, bem como formas de solucionar ou superar esses problemas. Os tópicos abordados incluem impressoras GDI, arquivos PPD e configuração de porta. Problemas comuns de impressoras de rede, impressões com defeito e gerenciamento de filas também são tratados.

12.7.1 Impressoras sem suporte de linguagem de impressora padrão

Essas impressoras não suportam nenhuma linguagem de impressora comum, podendo apenas ser tratadas com seqüências especiais de controle proprietário. Portanto, elas só funcionam com as versões de sistema operacional para as quais o fabricante fornece driver. GDI é uma interface de programação desenvolvida pela Microsoft* para dispositivos gráficos. Geralmente o fabricante fornece drivers apenas para Windows e, com o driver do Windows usa a interface GDI, essas impressoras também são chamadas de *impressoras GDI*. O verdadeiro problema não é a interface de programação, mas o fato de que tais impressoras só podem ser tratadas com a linguagem de impressora proprietária do respectivo modelo de impressora.

Algumas impressoras GDI podem ser ajustadas para funcionar no modo GDI ou em uma das linguagens de impressora padrão. Consulte o manual da impressora para saber se isso é possível. Alguns modelos exigem software especial do Windows para fazer o ajuste (observe que o driver de impressora do Windows pode sempre retornar a impressora para o modo GDI quando se imprime do Windows). Para outras impressoras

GDI, existem módulos de extensão disponíveis para uma linguagem de impressora padrão.

Alguns fabricantes oferecem drivers proprietários para suas impressoras. A desvantagem dos drivers de impressora proprietários é que não há garantia de que vão funcionar com o sistema de impressão instalado ou de que sejam adequados para as diferentes plataformas de hardware. Em contraste, impressoras que suportam uma linguagem de impressora padrão não dependem de uma versão do sistema de impressão especial ou de plataforma de hardware especial.

Em vez de desperdiçar tempo tentando fazer um driver Linux proprietário funcionar, pode ser mais eficaz comprar uma impressora suportada. Isso solucionaria o problema do driver de uma vez por todas, eliminando a necessidade de instalar e configurar software de driver especial e obter atualizações do driver eventualmente necessárias devido a novos avanços no sistema de impressão.

12.7.2 Nenhum arquivo PPD adequado disponível para impressora PostScript

Se o pacote `manufacturer-PPDs` não contiver qualquer arquivo PPD adequado para uma impressora PostScript, será possível usar o arquivo PPD do CD do driver do fabricante da impressora ou fazer download de um arquivo PPD adequado da página da Web do fabricante.

Se o arquivo PPD for fornecido como arquivo compactado (.zip) ou arquivo compactado de auto-extração (.exe), faça a descompactação com `unzip`. Primeiro, reveja os termos de licença do arquivo PPD. Em seguida, use o utilitário `cupstestppd` para verificar se o arquivo PPD atende à “Especificação de Formato de Arquivo PPD (PostScript Printer Description - Descrição de Impressora PostScript) da Adobe, versão 4.3”. Se o utilitário retornar “FAIL”, significa que os erros nos arquivos PPD são graves e provavelmente causam os principais problemas. Os problemas reportados pelo `cupstestppd` devem ser eliminados. Se necessário, peça o arquivo PPD adequado ao fabricante da impressora.

12.7.3 Portas paralelas

A abordagem mais segura é conectar a impressora diretamente à primeira porta paralela e selecionar as configurações de porta paralela no BIOS:

- Endereço de E/S: 378 (hexadecimal)
- Interrupção: irrelevante
- Modo: Normal, SPP ou Output Only
- DMA: desabilitado

Se a impressora não puder ser endereçada na porta paralela apesar dessas configurações, digite o endereço de E/S explicitamente de acordo com a configuração no BIOS no formato 0x378 em `/etc/modprobe.conf`. Se houver duas portas paralelas definidas para os endereços de E/S 378 e 278 (hexadecimal), digite-os no formato 0x378, 0x278.

Se a interrupção 7 estiver livre, poderá ser ativada com a entrada mostrada em Exemplo 12.1, “`/etc/modprobe.conf`: Modo de interrupção para a primeira porta paralela” (p 155). Antes de ativar o modo de interrupção, verifique o arquivo `/proc/interrupts` para ver quais interrupções já estão sendo usadas. Somente as interrupções usadas atualmente são exibidas. Isso pode mudar dependendo dos componentes de hardware ativos. A interrupção da porta paralela não deve ser usada por outro dispositivo. Se não tiver certeza, use o modo de polling com `irq=none`.

Exemplo 12.1 *`/etc/modprobe.conf`: Modo de interrupção para a primeira porta paralela*

```
alias parport_lowlevel parport_pc
options parport_pc io=0x378 irq=7
```

12.7.4 Conexões da impressora de rede

Identificação de problemas de rede

Conecte a impressora diretamente ao computador. Para fins de teste, configure-a como impressora local. Se isso funcionar, o problema está na rede.

Verificando a rede TCP/IP

A rede TCP/IP e a resolução de nomes devem ser funcionais.

Verificando um lpd remoto

Use o comando a seguir para testar o estabelecimento de uma conexão TCP com lpd (porta 515) no *host*.

```
netcat -z host 515 && echo ok || echo failed
```

Se a conexão com lpd não for estabelecida, o lpd pode não estar ativo ou pode haver problemas básicos de rede.

Como usuário *root*, use o seguinte comando para consultar um relatório de status (possivelmente muito longo) sobre a *fila* no *host* remoto, considerando que o respectivo lpd esteja ativo e o *host* aceite consultas:

```
echo -e "\004queue" \  
| netcat -w 2 -p 722 host 515
```

Se o lpd não responder, ele pode não estar ativo ou pode haver problemas básicos de rede. Se o lpd responder, a resposta deverá mostrar por que não é possível imprimir na fila do *host*. Se você receber uma resposta como esta, mostrada no Exemplo 12.2, “Mensagem de erro do lpd” (p 156), significa que o problema está sendo causado pelo lpd remoto.

Exemplo 12.2 *Mensagem de erro do lpd*

```
lpd: your host does not have line printer access  
lpd: queue does not exist  
printer: spooling disabled  
printer: printing disabled
```

Verificando um cupsd remoto

Por padrão, o servidor de rede CUPS deve transmitir suas filas a cada 30 segundos na porta UDP 631. Por isso, o seguinte comando pode ser usado para testar a existência de um servidor de rede CUPS na rede. Não deixe de parar seu daemon CUPS local antes de executar o comando.

```
netcat -u -l -p 631 & PID=$! ; sleep 40 ; kill $PID
```

Se existir um servidor de rede CUPS de transmissão, a saída aparecerá conforme mostrado no Exemplo 12.3, “Transmissão do servidor de rede CUPS” (p 157).

Exemplo 12.3 Transmissão do servidor de rede CUPS

```
ipp://192.168.2.202:631/printers/queue
```

Use o comando a seguir para testar o estabelecimento de uma conexão TCP com cupsd (porta 631) no *host*.

```
netcat -z host 631 && echo ok || echo failed
```

Se não for possível estabelecer a conexão com cupsd, pode ser que o cupsd não esteja ativo ou existam problemas básicos de rede. `lpstat -h host -l -t` retorna um relatório de status (possivelmente muito longo) de todas as filas do *host*, contanto que o respectivo cupsd esteja ativo e o *host* aceite consultas.

O próximo comando pode ser usado para testar se a *fila* do *host* aceita um serviço de impressão que consiste em um único caractere de retorno de carro. Nada será impresso. Possivelmente, será ejetada uma página em branco.

```
echo -en "\r" \  
| lp -d queue -h host
```

Solução de problemas da impressora de rede ou da caixa do servidor de impressão

Algumas vezes, spoolers executados na caixa do servidor de impressão causam problemas quando precisam lidar com vários serviços de impressão. Como isso é causado pelo spooler na caixa do servidor de impressão, não há como resolver essa questão. Como solução alternativa, desvie o spooler na caixa do servidor de impressão endereçando a impressora conectada à caixa diretamente com o soquete TCP. Consulte a Seção 12.4, “Impressoras de rede” (p 147).

Dessa forma, a caixa do servidor de impressão é reduzida a um conversor entre as várias formas de transferência de dados (conexão de rede TCP/IP e impressora local). Para usar esse método, você precisa conhecer a porta TCP da caixa do servidor de impressão. Se a impressora estiver conectada à caixa do servidor de impressão e ligada, a porta TCP poderá ser determinada normalmente com o utilitário `nmap` do pacote `nmap`, algum tempo depois que a caixa for ativada. Por exemplo, `nmap endereço_IP` pode resultar na seguinte saída para uma caixa do servidor de impressão:

Port	State	Service
23/tcp	open	telnet
80/tcp	open	http
515/tcp	open	printer
631/tcp	open	cups
9100/tcp	open	jetdirect

Essa saída indica que a impressora conectada à caixa do servidor de impressão pode ser endereçada via soquete TCP na porta 9100. Por padrão, `nmap` verifica somente algumas portas mais conhecidas listadas em `/usr/share/nmap/nmap-services`. Para verificar todas as portas possíveis, use o comando `nmap -p porta_de_origem-porta_de_destino endereço_IP`. O processo pode demorar. Para obter mais informações, consulte a página de manual de `nmap`.

Digite um comando como

```
echo -en "\rHello\r\f" | netcat -w 1 IP-address port
cat file | netcat -w 1 IP-address port
```

para enviar strings de caracteres ou arquivos diretamente à respectiva porta para testar se a impressora pode ser endereçada dessa porta.

12.7.5 Defeitos na impressão sem mensagem de erro

Para o sistema de impressão, o serviço de impressão é concluído quando o back end do CUPS conclui a transferência de dados ao destinatário (impressora). Se houver falha no processamento posterior no destinatário (por exemplo, se a impressora não imprimir seus próprios dados específicos), o sistema de impressão não notará. Se a impressora não imprimir seus próprios dados específicos, selecione um arquivo PPD mais adequado à impressora.

12.7.6 Filas desabilitadas

Se a transferência de dados para o destinatário falhar completamente após várias tentativas, o back end do CUPS, como `USB` ou `socket`, reportará um erro ao sistema de impressão (ao `cupsd`). O back end determina quantas tentativas malsucedidas são necessárias para que a transferência de dados seja considerada impossível. Visto que as tentativas posteriores serão inúteis, o `cupsd` desabilita a impressão da fila correspondente. Após eliminar a causa do problema, o administrador do sistema deve reabilitar a impressão com o comando `cupsenable`.

12.7.7 Navegação do CUPS: apagando serviços de impressão

Se um servidor de rede CUPS transmitir suas filas aos hosts de clientes via navegação e um `cupsd` local adequado estiver ativo nos hosts de clientes, o `cupsd` de cliente aceitará serviços de impressão de aplicativos e os encaminhará ao `cupsd` no servidor. Quando o `cupsd` aceita um serviço de impressão, atribui a ele um novo número. Portanto, o número da tarefa no host cliente é diferente do número da tarefa no servidor. Como geralmente um serviço de impressão é encaminhado de imediato, não é possível apagá-lo com o número de serviço do host cliente, porque o `cupsd` do cliente considera o serviço como concluído assim que ele é encaminhado ao `cupsd` do servidor.

Quando quiser apagar o serviço de impressão no servidor, use um comando como `lpstat -h cups.example.com -o` para determinar o número do serviço no servidor, contanto que o servidor ainda não tenha concluído o serviço de impressão (isto é, não o tenha enviado inteiramente para a impressora). Com esse número, o serviço de impressão pode ser apagado no servidor:

```
cancel -h cups.example.com queue-jobnumber
```

12.7.8 Serviços de impressão com defeito e erros de transferência de dados

Se você desligar a impressora ou o computador durante o processo de impressão, os serviços de impressão permanecerão na fila. A impressão continua quando o computador (ou a impressora) é ligado novamente. Os serviços de impressão com defeito devem ser removidos da fila com `cancel`.

Se o serviço de impressão apresentar defeito ou se ocorrer um erro na comunicação entre o host e a impressora, a impressora imprimirá várias folhas de papel com caracteres ininteligíveis, pois não consegue processar os dados corretamente. Para corrigir essa situação, siga as etapas a seguir:

- 1 Para interromper a impressão, remova todo o papel das bandejas da impressora jato de tinta ou laser. Impressoras de alta qualidade têm um botão de cancelamento da impressão.

- 2 O serviço de impressão pode ainda estar na fila, já que os serviços apenas são removidos depois de inteiramente enviados à impressora. Use `lpstat -o` ou `lpstat -h cups.example.com -o` para verificar a fila que está sendo impressa. Apague o serviço de impressão com `cancel`
fila-número_do_serviço ou `cancel -h cups.example.com`
fila-número_do_serviço.
- 3 Alguns dados podem ainda ser transferidos à impressora mesmo que o serviço tenha sido apagado da fila. Verifique se há um processo back end do CUPS em execução para a fila respectiva e termine-o. Por exemplo, para uma impressora conectada à porta paralela, o comando `fuser -k /dev/lp0` pode ser usado para terminar todos os processos que ainda estão acessando a impressora (mais precisamente, a porta paralela).
- 4 Reinicialize a impressora completamente deixando-a desligada por um tempo. Em seguida, insira o papel e ligue a impressora.

12.7.9 Depuração do sistema de impressão do CUPS

Use o seguinte procedimento genérico para localizar problemas no sistema de impressão do CUPS:

- 1 Defina `LogLevel debug` em `/etc/cups/cupsd.conf`.
- 2 Pare o `cupsd`.
- 3 Remova `/var/log/cups/error_log*` para não precisar procurar em arquivos de registro muito grandes.
- 4 Inicie o `cupsd`.
- 5 Repita a ação que causou o problema.
- 6 Verifique as mensagens em `/var/log/cups/error_log*` para identificar a causa do problema.

12.7.10 Para obter mais informações

Soluções para vários problemas específicos são apresentadas na Base de Dados de Conhecimento Novell (<http://support.novell.com/>). Localize os artigos relevantes com uma pesquisa pelo texto CUPS.

Gerenciamento de dispositivo de kernel dinâmico com udev

13

O kernel pode adicionar ou remover praticamente qualquer dispositivo em um sistema em execução. Mudanças no estado do dispositivo (se um dispositivo foi conectado ou removido) precisam ser estendidas ao espaço do usuário. Os dispositivos deverão ser configurados assim que forem conectados e reconhecidos. Os usuários de um determinado dispositivo precisam ser informados sobre qualquer mudança no estado reconhecido desse dispositivo. O udev fornece a infra-estrutura necessária para manter dinamicamente os arquivos dos nós de dispositivo e os links simbólicos no diretório `/dev`. As regras do udev fornecem uma maneira de conectar ferramentas externas ao processamento de evento do dispositivo de kernel. Isso permite que você personalize o tratamento do dispositivo do udev, por exemplo, adicionando determinados scripts a serem executados como parte do tratamento do dispositivo de kernel, ou solicite e importe dados adicionais para avaliação durante o tratamento do dispositivo.

13.1 O diretório `/dev`

Os nós de dispositivo no diretório `/dev` fornecem acesso aos dispositivos de kernel correspondentes. Com o udev, o diretório `/dev` reflete o estado atual do kernel. Cada dispositivo de kernel tem um arquivo de dispositivo correspondente. Se um dispositivo for desconectado do sistema, o nó de dispositivo será removido.

O conteúdo do diretório `/dev` será mantido em um sistema de arquivos temporário, e todos os arquivos serão renderizados a cada inicialização do sistema. Arquivos criados ou modificados manualmente por definição não resistem a uma reinicialização. Diretórios e arquivos estáticos que sempre devem estar presentes no diretório `/dev`, independentemente do estado do dispositivo de kernel correspondente, podem ser

colocados no diretório `/lib/udev/devices`. Na inicialização do sistema, o conteúdo do diretório é copiado para o diretório `/dev` com propriedade e permissões iguais às dos arquivos em `/lib/udev/devices`.

13.2 udev e uevents de kernel

As informações de dispositivo necessárias são exportadas pelo sistema de arquivos `sysfs`. Para cada dispositivo detectado e inicializado pelo kernel, um diretório com o nome do dispositivo é criado. Ele contém arquivos de atributos com propriedades específicas do dispositivo.

Sempre que um dispositivo é adicionado ou removido, o kernel envia um uevent para notificar o udev da mudança. O daemon udev lê e analisa todas as regras fornecidas dos arquivos `/etc/udev/rules.d/*.rules` uma vez na inicialização e mantém essas regras na memória. Se os arquivos de regras são mudados, adicionados ou removidos, o daemon pode recarregar a representação na memória de todas as regras com o comando `udevadm control reload_rules`. Isso também é feito ao executar `/etc/init.d/boot.udev reload`. Para obter mais detalhes sobre as regras do udev e sua sintaxe, consulte a Seção 13.6, “Influenciando o tratamento de evento de dispositivo de kernel com regras do udev” (p 167).

Cada evento recebido é comparado com o conjunto de regras fornecido. As regras podem adicionar ou modificar chaves de ambiente de eventos, solicitar um nome específico a ser criado pelo nó de dispositivo, adicionar symlinks apontando para o nó ou adicionar programas a serem executados após a criação do nó do dispositivo. Os uevents centrais do driver são recebidos de um soquete de netlink de kernel.

13.3 Drivers, módulos de kernel e dispositivos

Os drivers de barramento de kernel pesquisam dispositivos. Para cada dispositivo detectado, o kernel cria uma estrutura interna de dispositivo e o centro do driver envia um uevent para o daemon do udev. Dispositivos de barramento se identificam através de um ID formatado especialmente, que informa o tipo de dispositivo. Geralmente esses IDs consistem em IDs de produto e fornecedor, além de outros valores específicos do

subsistema. Cada barramento tem seu próprio esquema para esses IDs, chamados `MODALIAS`. O kernel toma as informações do dispositivo, compõe uma string de `MODALIAS` a partir dele e envia essa string junto com o evento. Para um mouse USB, a string tem a seguinte aparência:

```
MODALIAS=usb:v046DpC03Ed2000dc00dsc00dp00ic03isc01ip02
```

Cada driver de dispositivo carrega uma lista de aliases conhecidos para os dispositivos que pode tratar. A lista está contida no próprio arquivo de módulo de kernel. O programa `depmod` lê as listas de ID e cria o arquivo `modules.alias` no diretório `/lib/modules` do kernel para todos os módulos disponíveis atualmente. Com essa infraestrutura, carregar o módulo é fácil como chamar `modprobe` para cada evento com uma chave `MODALIAS`. Se `modprobe $MODALIAS` for chamado, ele corresponderá o alias do dispositivo composto para o dispositivo com os aliases fornecidos pelos módulos. Se uma entrada correspondente for encontrada, o módulo será carregado. Tudo isso é acionado automaticamente pelo `udev`.

13.4 Inicialização e configuração do dispositivo inicial

Todos os eventos de dispositivo que ocorrerem durante o processo de boot antes da execução do daemon do `udev` são perdidos, pois a infraestrutura para tratar esses eventos está no sistema de arquivos de raiz e não está disponível no momento. Para cobrir essa perda, o kernel fornece um arquivo `uevent` localizado no diretório de dispositivo de cada dispositivo no sistema de arquivos `sysfs`. Ao gravar `add` para esse arquivo, o kernel envia novamente o mesmo evento como o evento perdido durante a inicialização. Um loop simples em todos os arquivos `uevent` em `/sys` aciona todos os eventos novamente para criar os nós de dispositivo e executar a configuração do dispositivo.

Por exemplo, durante o boot, um mouse USB talvez não seja inicializado pela lógica de boot anterior, pois o driver não está disponível nesse momento. O evento para a descoberta do dispositivo foi perdido e não encontrou um módulo de kernel para o dispositivo. Em vez de você pesquisar manualmente por dispositivos possivelmente conectados, o `udev` solicita todos os eventos de dispositivo do kernel depois que o sistema de arquivos raiz está disponível. Assim, o evento do dispositivo do mouse USB

é executado novamente. Então ele encontra o módulo de kernel no sistema de arquivos raiz montado e o mouse USB pode ser inicializado.

No espaço do usuário, não há diferença visível entre uma sequência coldplug do dispositivo e uma detecção de dispositivo durante a execução. Em ambos os casos, as mesmas regras são usadas para correspondência e os mesmos programas configurados são executados.

13.5 Monitorando o daemon do udev em execução

O programa `udevadm monitor` pode ser usado para visualizar os eventos centrais do driver e a temporização dos processos de eventos do udev.

```
UEVENT[1185238505.276660] add    /devices/pci0000:00/0000:00:1d.2/usb3/3-1
(usb)
UDEV  [1185238505.279198] add    /devices/pci0000:00/0000:00:1d.2/usb3/3-1
(usb)
UEVENT[1185238505.279527] add
/devices/pci0000:00/0000:00:1d.2/usb3/3-1/3-1:1.0 (usb)
UDEV  [1185238505.285573] add
/devices/pci0000:00/0000:00:1d.2/usb3/3-1/3-1:1.0 (usb)
UEVENT[1185238505.298878] add
/devices/pci0000:00/0000:00:1d.2/usb3/3-1/3-1:1.0/input/input10 (input)
UDEV  [1185238505.305026] add
/devices/pci0000:00/0000:00:1d.2/usb3/3-1/3-1:1.0/input/input10 (input)
UEVENT[1185238505.305442] add
/devices/pci0000:00/0000:00:1d.2/usb3/3-1/3-1:1.0/input/input10/mouse2 (input)
UEVENT[1185238505.306440] add
/devices/pci0000:00/0000:00:1d.2/usb3/3-1/3-1:1.0/input/input10/event4 (input)
UDEV  [1185238505.325384] add
/devices/pci0000:00/0000:00:1d.2/usb3/3-1/3-1:1.0/input/input10/event4 (input)
UDEV  [1185238505.342257] add
/devices/pci0000:00/0000:00:1d.2/usb3/3-1/3-1:1.0/input/input10/mouse2 (input)
```

As linhas `UEVENT` mostram os eventos que o kernel enviou através de netlink. As linhas `UDEV` mostram os handlers de evento do udev concluídos. A temporização é impressa em microssegundos. O tempo entre `UEVENT` e `UDEV` é o tempo que udev levou para processar esse evento ou que o daemon udev atrasou sua execução para sincronizar esse evento com eventos relacionados e já em execução. Por exemplo, eventos para partições de disco rígido sempre esperam pela conclusão do evento do dispositivo de disco principal, pois os eventos de partição podem se basear nos dados que o evento de disco principal consultou do hardware.

`udevadm monitor --env` mostra o ambiente de evento completo:

```
ACTION=add
DEVPATH=/devices/pci0000:00/0000:00:1d.2/usb3/3-1/3-1:1.0/input/input10
SUBSYSTEM=input
SEQNUM=1181
NAME="Logitech USB-PS/2 Optical Mouse"
PHYS="usb-0000:00:1d.2-1/input0"
UNIQ=""
EV=7
KEY=70000 0 0 0 0
REL=103
MODALIAS=input:b0003v046DpC03Ee0110-e0,1,2,k110,111,112,r0,1,8,amlsfw
```

O `udev` também envia mensagens para o `syslog`. A prioridade padrão do `syslog` que controla quais mensagens são enviadas ao `syslog` é especificada no arquivo de configuração do `udev` `/etc/udev/udev.conf`. A prioridade de registro do daemon em execução pode ser modificada com `udevcontrol log_priority=level/number`.

13.6 Influenciando o tratamento de evento de dispositivo de kernel com regras do `udev`

Uma regra do `udev` pode corresponder a qualquer propriedade adicionada pelo kernel ao próprio evento ou a qualquer informação exportada pelo kernel para `sysfs`. A regra também pode solicitar informações adicionais de programas externos. Cada evento é correspondido com as regras fornecidas. Essas regras estão localizadas no diretório `/etc/udev/rules.d`.

Cada linha no arquivo de regras contém pelo menos um par de valores de chave. Há dois tipos de chaves, de atribuição e correspondência. Se todas as chaves de correspondência corresponderem aos valores, a regra será aplicada e as chaves de atribuição serão atribuídas ao valor especificado. Uma regra correspondente pode especificar o nome do nó de dispositivo, adicionar symlinks apontando para o nó ou executar um programa especificado como parte do tratamento de eventos. Se nenhuma regra de correspondência for encontrada, o nome do nó de dispositivo padrão será usado para criar o nó de dispositivo. Informações detalhadas sobre a sintaxe de regra e as chaves fornecidas para correspondência ou importação de dados são descritas na página

de manual do udev. As regras de exemplo a seguir fornecem uma introdução básica à sintaxe de regra do udev. As regras de exemplo são todas tiradas do conjunto de regras padrão do udev, localizado em `/etc/udev/rules.d/50-udev-default.rules`.

Exemplo 13.1 *Regras do udev de exemplo*

```
# console
KERNEL=="console", MODE="0600", OPTIONS="last_rule"

# serial devices
KERNEL=="ttyUSB*", ATTRS{product}=="[Pp]alm*Handheld*", SYMLINK+="pilot"

# printer
SUBSYSTEM=="usb", KERNEL=="lp*", NAME="usb/%k", SYMLINK+="usb%k", GROUP="lp"

# kernel firmware loader
SUBSYSTEM=="firmware", ACTION=="add", RUN+="firmware.sh"
```

A regra do `console` consiste em três chaves: uma chave de correspondência (`KERNEL`) e duas chaves de atribuição (`MODE`, `OPTIONS`). A regra de correspondência `KERNEL` pesquisa qualquer item do tipo `console` na lista de dispositivos. Apenas correspondências exatas são válidas e acionam essa regra para que seja executada. A chave `MODE` atribui permissões especiais ao nó de dispositivo, neste caso, permissões de leitura e gravação apenas ao proprietário desse dispositivo. A chave `OPTIONS` torna esta a última regra a ser aplicada a qualquer dispositivo desse tipo. Qualquer regra posterior que corresponda a esse tipo de dispositivo em particular não terá nenhum efeito.

A regra dos dispositivos `seriais` não está mais disponível em `50-udev-default.rules`, mas ainda vale a pena ser considerada. Consiste em duas chaves de correspondência (`KERNEL` e `ATTRS`) e uma de atribuição (`SYMLINK`). A chave `KERNEL` procura todos os dispositivos do tipo `ttyUSB`. Usando o curinga `*`, essa chave corresponde a diversos desses dispositivos. A segunda chave de correspondência, `ATTRS`, verifica se o arquivo de atribuição do produto em `sysfs` para qualquer dispositivo `ttyUSB` contém uma determinada string. A chave de atribuição (`SYMLINK`) aciona a adição de um link simbólico para esse dispositivo em `/dev/pilot`. O operador usado nessa chave (`+=`) diz ao udev para executar essa ação adicionalmente, mesmo se regras anteriores ou posteriores adicionarem outros links simbólicos. Como essa regra contém duas chaves de correspondência, ela é aplicada apenas se ambas as condições são cumpridas.

A regra da impressora lida com impressoras USB e contém duas chaves de correspondência que devem ser aplicadas para que a regra inteira seja aplicada (SUBSYSTEM e KERNEL). Três chaves de atribuição lidam com a nomeação desse tipo de dispositivo (NAME), a criação dos links de dispositivo simbólicos (SYMLINK) e a participação no grupo desse tipo de dispositivo (GROUP). O uso do curinga * na chave KERNEL faz com que ela corresponda a diversos dispositivos de impressora lp. Substituições são usadas pelo nome do dispositivo interno tanto na chave NAME quanto na SYMLINK para estender essas strings. Por exemplo, o symlink para a primeira impressora USB lp seria lido como /dev/usb/lp0.

A regra do carregador de firmware do kernel faz o udev carregar firmware adicional por um script de assistente externo durante o tempo de execução. A chave de correspondência SUBSYSTEM procura o subsistema de firmware. A chave ACTION verifica se algum dispositivo pertencente ao subsistema de firmware foi adicionado. A chave RUN+= aciona a execução do script firmware.sh para localizar o firmware a ser carregado.

Algumas características são comuns a todas as regras:

- Cada regra é composta por um ou mais pares de valores de chaves separados por vírgula.
- A operação de uma chave é determinada pelo operador. As regras do udev suportam diversos operadores diferentes.
- Cada valor dado deve estar entre aspas.
- Cada linha do arquivo de regras representa uma regra. Se uma regra for mais extensa e não couber em uma linha, use \ para juntar as linhas diferentes como se faria na sintaxe do shell.
- As regras do udev suportam um padrão no estilo do shell que corresponde aos padrões de *, ? e [].
- As regras do udev suportam substituições.

13.6.1 Usando operadores nas regras do udev

Ao criar chaves, você pode escolher dentre diversos operadores diferentes, dependendo do tipo de chave que quiser criar. As chaves de correspondência normalmente são usadas apenas para encontrar um valor que corresponda ou que explicitamente não corresponda ao valor de pesquisa. As chaves de correspondência contêm um dos seguintes operadores:

==

Comparar para igualdade. Se a chave contém um padrão de pesquisa, todos os resultados correspondentes a esse padrão são válidos.

!=

Comparar para não-igualdade. Se a chave contém um padrão de pesquisa, todos os resultados correspondentes a esse padrão são válidos.

Qualquer um dos operadores a seguir também pode ser usado com chaves de atribuição:

=

Atribuir um valor a uma chave. Se a chave consistia anteriormente em uma lista de valores, ela é redefinida e apenas o valor único é atribuído.

+=

Adicionar um valor a uma chave que contenha uma lista de entradas.

:=

Atribuir um valor final. Não permitir nenhuma mudança posterior por regras posteriores.

13.6.2 Usando substituições nas regras do udev

As regras do udev suportam o uso de marcadores e substituições. Use-as como faria em qualquer outro script. As substituições a seguir podem ser usadas com regras do udev:

`%r, $root`
O diretório do dispositivo, `/dev` por padrão.

`%p, $devpath`
O valor de `DEVPATH`.

`%k, $kernel`
O valor de `KERNEL` ou o nome do dispositivo interno.

`%n, $number`
O nome do dispositivo.

`%N, $tempnode`
O nome temporário do arquivo de dispositivo.

`%M, $major`
O número maior do dispositivo.

`%m, $minor`
O número menor do dispositivo.

`%s{attribute}, $attr{attribute}`
O valor de um atributo `sysfs` (especificado por *attribute*).

`%E{variable}, $attr{variable}`
O valor de uma variável do ambiente (especificado por *variable*).

`%c, $result`
A saída de `PROGRAM`.

`%%`
O caractere `%`.

`$$`
O caractere `$`.

13.6.3 Usando chaves de correspondência do udev

As chaves de correspondência descrevem condições que devem ser cumpridas antes da aplicação de uma regra do udev. As seguintes chaves de correspondência estão disponíveis:

ACTION

O nome da ação do evento, por exemplo, `add` ou `remove` na adição ou remoção de um dispositivo.

DEVPATH

O caminho do dispositivo do evento, por exemplo,
`DEVPATH=/bus/pci/drivers/ipw3945` para procurar todos os eventos relacionados ao driver `ipw3945`.

KERNEL

O nome interno (do kernel) do dispositivo do evento.

SUBSYSTEM

O subsistema do dispositivo do evento, por exemplo, `SUBSYSTEM=usb` para todos os eventos relacionados a dispositivos USB.

ATTR{*nome de arquivo*}

Atributos `sysfs` do dispositivo do evento. Para corresponder a uma string contida no nome de arquivo do atributo `fornecedor`, você poderia usar
`ATTR{fornecedor}=="On[sS]tream"`, por exemplo.

KERNELS

Permitir que o udev procure um nome de dispositivo correspondente no caminho de dispositivo em sentido ascendente.

SUBSYSTEMS

Permitir que o udev procure um nome de um subsistema de dispositivo correspondente no caminho de dispositivo em sentido ascendente.

DRIVERS

Permitir que o udev procure um nome de um driver de dispositivo correspondente no caminho de dispositivo em sentido ascendente.

ATTRS{*nome de arquivo*}

Permitir que o udev procure um dispositivo com valores de atributo sysfs correspondentes no caminho de dispositivo em sentido ascendente.

ENV{*chave*}

O valor de uma variável de ambiente, por exemplo, ENV{ID_BUS}="ieee1394 para procurar todos os eventos relacionados ao ID do barramento FireWire.

PROGRAM

Permitir que o udev execute um programa externo. Para ser bem-sucedido, o programa deve retornar com código de saída zero. A saída do programa, impressa em stdout, está disponível para a chave RESULT.

RESULT

Corresponder à string de saída da última chamada de PROGRAM. Incluir esta chave na mesma regra que a chave PROGRAM ou em uma posterior.

13.6.4 Usando chaves de atribuição do udev

Em contraste com as chaves de correspondência descritas anteriormente, as chaves de atribuição não descrevem condições que devem ser cumpridas. Elas atribuem valores, nomes e ações aos nós de dispositivo mantidos pelo udev.

NAME

O nome do nó de dispositivo a ser criado. Após uma regra definir um nome de nó, todas as demais regras com uma chave NAME para esse nó são ignoradas.

SYMLINK

O nome de um symlink relacionado a um nó a ser criado. Várias regras de correspondência podem adicionar symlinks a serem criados com o nó de dispositivo. Você também pode especificar vários symlinks para um nó em uma regra usando o caractere de espaço para separar os nomes dos symlinks.

OWNER, GROUP, MODE

As permissões do novo nó de dispositivo. Os valores especificados aqui sobregravam qualquer coisa que tenha sido compilada.

ATTR{*chave*}

Especificar um valor a ser gravado em um atributo sysfs do dispositivo de evento. Se o operador == é usado, essa chave também é usada para corresponder com o valor de um atributo sysfs.

ENV{*chave*}

Dizer ao udev para exportar uma variável para o ambiente. Se o operador == é usado, essa chave também é usada para corresponder com uma variável de ambiente.

RUN

Dizer ao udev para adicionar um programa à lista de programas a serem executados para esse dispositivo. Lembre-se de restringir isso a tarefas muito curtas, a fim de evitar o bloqueio de outros eventos para esse dispositivo.

LABEL

Adicionar um rótulo para onde um GOTO possa ir.

GOTO

Dizer ao udev para ignorar várias regras e continuar com aquela que tenha o rótulo mencionado pela chave GOTO.

IMPORT{*tipo*}

Carregar variáveis para o ambiente do evento, como a saída de um programa externo. O udev importa variáveis de vários tipos diferentes. Se nenhum tipo é especificado, o udev tenta determinar o tipo por conta própria, com base no bit executável das permissões de arquivo.

- `program` diz ao udev para executar um programa externo e importar sua saída.
- `file` diz ao udev para importar um arquivo texto.
- `parent` diz ao udev para importar as chaves armazenadas do dispositivo pai.

WAIT_FOR_SYSFS

Diz ao udev para aguardar que o arquivo sysfs especificado seja criado para um determinado dispositivo. Por exemplo, `WAIT_FOR_SYSFS="ioerr_cnt"` informa o udev para aguardar até que o arquivo `ioerr_cnt` seja criado.

OPTIONS

A chave `OPTION` pode ter diversos valores possíveis:

- `last_rule` diz ao udev para ignorar todas as regras posteriores.
- `ignore_device` diz ao udev para ignorar esse evento completamente.
- `ignore_remove` diz ao udev para ignorar todos os eventos de remoção posteriores para o dispositivo.
- `all_partitions` diz ao udev para criar nós de dispositivo para todas as partições disponíveis em um dispositivo de bloco.

13.7 Nomeação de dispositivo persistente

O diretório de dispositivo dinâmico e a infra-estrutura de regras do udev permitem fornecer nomes estáveis para todos os dispositivos de disco, independentemente da ordem de reconhecimento ou da conexão usada para o dispositivo. Cada dispositivo de bloco apropriado criado pelo kernel é examinado por ferramentas com conhecimento especial sobre determinados barramentos, tipos de unidade ou sistemas de arquivos. Junto com o nome do nó de dispositivo fornecido pelo kernel dinâmico, o udev mantém classes de links simbólicos apontando para o dispositivo:

```
/dev/disk
|-- by-id
|   |-- scsi-SATA_HTS726060M9AT00_MRH453M4HWHG7B -> ../../sda
|   |-- scsi-SATA_HTS726060M9AT00_MRH453M4HWHG7B-part1 -> ../../sda1
|   |-- scsi-SATA_HTS726060M9AT00_MRH453M4HWHG7B-part6 -> ../../sda6
|   |-- scsi-SATA_HTS726060M9AT00_MRH453M4HWHG7B-part7 -> ../../sda7
|   |-- usb-Generic_STORAGE_DEVICE_02773 -> ../../sdd
|   `-- usb-Generic_STORAGE_DEVICE_02773-part1 -> ../../sdd1
|-- by-label
|   |-- Photos -> ../../sdd1
|   |-- SUSE10 -> ../../sda7
|   `-- devel -> ../../sda6
```

```

|-- by-path
|   |-- pci-0000:00:1f.2-scsi-0:0:0:0 -> ../../sda
|   |-- pci-0000:00:1f.2-scsi-0:0:0:0-part1 -> ../../sda1
|   |-- pci-0000:00:1f.2-scsi-0:0:0:0-part6 -> ../../sda6
|   |-- pci-0000:00:1f.2-scsi-0:0:0:0-part7 -> ../../sda7
|   |-- pci-0000:00:1f.2-scsi-1:0:0:0 -> ../../sr0
|   |-- usb-02773:0:0:2 -> ../../sdd
|   |-- usb-02773:0:0:2-part1 -> ../../sdd1
`-- by-uuid
    |-- 159a47a4-e6e6-40be-a757-a629991479ae -> ../../sda7
    |-- 3e999973-00c9-4917-9442-b7633bd95b9e -> ../../sda6
    `-- 4210-8F8C -> ../../sdd1

```

13.8 Arquivos usados pelo udev

`/sys/*`

Sistema de arquivos virtual fornecido pelo kernel do Linux, exportando todos os dispositivos conhecidos atualmente. Essa informação é usada pelo udev para criar nós de dispositivo em `/dev`

`/dev/*`

Nós de dispositivo criados dinamicamente e conteúdo estático copiados no momento do boot de `/lib/udev/devices/*`

Os seguintes arquivos e diretórios contêm os elementos cruciais da infra-estrutura do udev:

`/etc/udev/udev.conf`

Arquivo de configuração principal do udev.

`/etc/udev/rules.d/*`

Regras de correspondência de evento do udev.

`/lib/udev/devices/*`

Conteúdo `/dev` estático.

`/lib/udev/*`

Programas auxiliares chamados de regras do udev.

13.9 Para obter mais informações

Para obter mais informações sobre a infra-estrutura do udev, consulte as seguintes páginas de manual:

udev

Informações gerais sobre o udev, chaves, regras e outras questões relevantes sobre configuração.

udevadm

O udevadm pode ser usado para controlar o comportamento em tempo de execução do udev, solicitar eventos de kernel, gerenciar a fila de eventos e fornecer mecanismos simples de depuração.

udev

Informações sobre o daemon de gerenciamento de eventos udev.

O sistema X Window

O sistema X Window (X11) é o padrão de fato para interfaces gráficas de usuário no UNIX. O X é baseado em rede, permitindo que aplicativos iniciados em um host sejam exibidos em outro host conectado em qualquer tipo de rede (LAN ou Internet). Este capítulo descreve a configuração e otimização do ambiente do X Window System, e fornece informações de fundo sobre o uso das fontes no SUSE® Linux Enterprise Desktop.

14.1 Configurando manualmente o X Window System

Por padrão, o X Window System é configurado com a interface do SaX2, descrita na Seção “Setting Up Graphics Card and Monitor” (Capítulo 5, *Setting Up Hardware Components with YaST*, ↑ *Guia de Implantação*). Alternativamente, pode ser configurado manualmente, editando seus arquivos de configuração.

ATENÇÃO: configurações defeituosas do X podem danificar seu hardware

Tenha cuidado ao configurar o sistema X Window. Nunca inicie o sistema X Window antes que a configuração esteja concluída. Um sistema mal configurado pode causar danos irreparáveis ao seu hardware (isso se aplica particularmente a monitores de frequência fixa). Os autores deste manual e do SUSE Linux Enterprise Desktop não podem ser responsabilizados por nenhum dano resultante. Essas informações foram pesquisadas cuidadosamente, mas isso não

garante que todos os métodos apresentados aqui estejam corretos e não danifiquem o seu hardware.

O comando `sax2` cria o arquivo `/etc/X11/xorg.conf`. Esse é o arquivo de configuração principal do X Window System. A seguir estão todas as configurações referentes ao monitor, ao mouse e à placa de vídeo.

IMPORTANTE: usando o X -configure

Use o `X -configure` para definir sua configuração do X se tentativas anteriores com o `SaX2` do SUSE Linux Enterprise Desktop tiverem falhado. Se sua configuração envolve drivers proprietários apenas binários, o `X -configure` não funcionará.

As seções a seguir descrevem a estrutura do arquivo de configuração `/etc/X11/xorg.conf`. Ela consiste em várias seções, cada uma delas referente a um determinado aspecto da configuração. Cada seção se inicia com a palavra-chave `Section` <designação> e termina com `EndSection`. A convenção a seguir se aplica a todas as seções:

```
Section "designation"
    entry 1
    entry 2
    entry n
EndSection
```

Os tipos de seção disponíveis estão listados na Tabela 14.1, “Seções em `/etc/X11/xorg.conf`” (p 180).

Tabela 14.1 Seções em `/etc/X11/xorg.conf`

Tipo	Significado
Arquivos	Os caminhos usados para as fontes e a tabela de cores RGB.
ServerFlags	Switches gerais para o comportamento do servidor.
Módulo	Uma lista de módulos que o servidor deve carregar

Tipo	Significado
InputDevice	Dispositivos de entrada, como teclados e dispositivos de entrada especiais (touchpads, joysticks, etc.), são configurados nessa seção. Parâmetros importantes nessa seção são <code>Driver</code> e as opções que definem o <code>Protocol</code> e o <code>Device</code> . Você normalmente tem uma seção <code>InputDevice</code> por dispositivo conectado ao computador.
Monitor	O monitor usado. Elementos importantes dessa seção são o <code>Identifier</code> , mencionado posteriormente na definição de <code>Screen</code> , a taxa de atualização <code>VertRefresh</code> e os limites da frequência de sincronização (<code>HorizSync</code> e <code>VertRefresh</code>). As configurações são fornecidas em MHz, kHz e Hz. Normalmente, o servidor recusa qualquer linha modelo que não corresponda à especificação do monitor. Isso evita que frequências muito altas sejam enviadas ao monitor por acidente.
Modes	Os parâmetros de modeline para as resoluções de tela específicas. Esses parâmetros podem ser calculados pelo <code>SaX2</code> com base nos valores fornecidos pelo usuário e, normalmente, não precisam ser mudados. Intervenha manualmente nesse ponto se, por exemplo, quiser conectar um monitor de frequência fixa. Há detalhes sobre o significado dos valores numéricos individuais nos arquivos <code>HOWTO</code> , em <code>/usr/share/doc/howto/en/html/XFree86-Video-Timings-HOWTO</code> (disponíveis no pacote <code>howtoenh</code>). Para calcular os modos VESA manualmente, você pode usar a ferramenta <code>cvt</code> . Por exemplo, para calcular uma modeline para um monitor de 1680x1050 a 60 Hz, use o comando <code>cvt 1680 1050 60</code> .
Device	Uma placa de vídeo específica. Ela é referenciada por seu nome descritivo. As opções disponíveis nessa seção dependem muito do driver usado. Por exemplo, se você usa o driver <code>i810</code> , encontre mais informações sobre as opções disponíveis na página de manual <code>man 4 i810</code> .

Tipo	Significado
Screen	<p>Combina um <code>Monitor</code> e um <code>Device</code> para compor todas as configurações necessárias para o <code>X.Org</code>. Na subseção <code>Display</code>, especifique o tamanho da tela virtual (<code>Virtual</code>), o <code>ViewPort</code> e os <code>Modes</code> usados com essa tela.</p> <p>Note que alguns drivers exigem que todas as configurações usadas estejam presentes na seção <code>Display</code> em algum lugar. Por exemplo, se você usa um laptop e deseja usar um monitor externo que seja maior do que o LCD interno, pode ser necessário adicionar uma resolução maior do que a suportada pelo LCD interno ao final da linha <code>Modes</code>.</p>
ServerLayout	<p>O layout de uma configuração <code>single-thread</code> ou <code>multithread</code>. Essa seção junta os dispositivos de entrada <code>InputDevice</code> e os dispositivos de exibição <code>Screen</code>.</p>
DRI	<p>Fornece informações para a Infra-estrutura de Renderização Direta (<code>DRI</code>).</p>

`Monitor`, `Device` e `Screen` são explicados em mais detalhes. Mais informações sobre as outras seções podem ser encontradas nas páginas de manual de `X.Org` e `xorg.conf`.

Há várias seções `Monitor` e `Device` diferentes em `xorg.conf`. Mesmo várias seções `Screen` são possíveis. A seção `ServerLayout` determina qual dessas seções é usada.

14.1.1 Seção de tela

A seção de tela combina um monitor com uma seção de dispositivo e determina a resolução e a intensidade de cor usadas. Uma seção de tela pode ter a aparência do Exemplo 14.1, “Seção de tela do arquivo `/etc/X11/xorg.conf`” (p 183).

Exemplo 14.1 Seção de tela do arquivo */etc/X11/xorg.conf*

```
Section "Screen"❶
    DefaultDepth 16❷
    SubSection "Display"❸
        Depth 16❹
        Modes "1152x864" "1024x768" "800x600"❺
        Virtual 1152x864❻
    EndSubSection
    SubSection "Display"
        Depth 24
        Modes "1280x1024"
    EndSubSection
    SubSection "Display"
        Depth 32
        Modes "640x480"
    EndSubSection
    SubSection "Display"
        Depth 8
        Modes "1280x1024"
    EndSubSection
    Device "Device[0]"
    Identifier "Screen[0]"❼
    Monitor "Monitor[0]"
EndSection
```

- ❶ Section determina o tipo de seção, neste caso, Screen.
- ❷ DefaultDepth determina a profundidade de cores a ser usada por padrão, a menos que outra seja especificada explicitamente.
- ❸ Para cada profundidade de cores, diferentes subseções Display são especificadas.
- ❹ Depth determina a profundidade de cores a ser usada com esse conjunto de configurações de Display. Os valores possíveis são 8, 15, 16, 24 e 32, embora nem todos sejam suportados por todos os módulos do servidor X ou resoluções.
- ❺ A seção Modes apresenta uma lista de possíveis resoluções de tela. O servidor X verifica essa lista da esquerda para a direita. Para cada resolução, o servidor X procura uma Modeline adequada na seção Modes. A Modeline depende da capacidade do monitor e da placa de vídeo. As configurações de Monitor determinam a Modeline resultante.

A primeira resolução encontrada é o Default mode. Com Ctrl + Alt + + (no teclado numérico), alterne para a resolução seguinte na lista à direita. Com Ctrl + Alt + - (no teclado numérico), alterne para a anterior. Isso permite a você variar a resolução enquanto o X está sendo executado.

- ⑥ A última linha da subseção `Display` com `Depth 16` refere-se ao tamanho da tela virtual. O tamanho máximo possível de uma tela virtual depende da quantidade de memória instalada na placa de vídeo e da intensidade de cor desejada, não da resolução máxima do monitor. Se essa linha é omitida, a resolução virtual é apenas a resolução física. Como placas de vídeo modernas têm uma grande quantidade de memória de vídeo, você pode criar áreas de trabalho virtuais bem grandes. Porém, você talvez não possa mais usar a funcionalidade de 3D se preencher a maior parte da memória de vídeo com uma área de trabalho virtual. Por exemplo, se a placa tiver 16 MB de memória RAM de vídeo, a tela virtual poderá ter até 4096x4096 pixels de tamanho, com profundidade de cores de 8 bits. Porém, principalmente para placas aceleradas, não é recomendável usar toda a memória para a tela virtual, pois a memória da placa também é usada para vários caches de vídeo e fontes.
- ⑦ A linha `Identifier` (aqui `Screen[0]`) fornece a essa seção um nome definido com o qual ela pode ser referenciada com exclusividade na seguinte seção `ServerLayout`. As linhas `Device` e `Monitor` especificam a placa de vídeo e o monitor que pertencem a essa definição. Esses são links para as seções `Device` e `Monitor` com seus nomes correspondentes ou *identificadores*. Essas seções são abordadas em detalhes abaixo.

14.1.2 Seção do dispositivo

Uma seção de dispositivo descreve uma placa de vídeo específica. Você pode ter quantas entradas de dispositivo desejar em `xorg.conf`, desde que os nomes sejam diferenciados pela palavra-chave `Identifier`. Se você tiver mais de uma placa de vídeo instalada, as seções serão simplesmente numeradas em ordem. A primeira é chamada `Device[0]`, a segunda `Device[1]` e assim por diante. O arquivo a seguir mostra um exemplo da seção `Device` de um computador com uma placa de vídeo PCI Matrox Millennium (conforme configurada pelo SaX2):

```
Section "Device"
    BoardName      "MGA2064W"
    BusID          "0:19:0"❶
    Driver         "mga"❷
    Identifier     "Device[0]"
    VendorName     "Matrox"
    Option         "sw_cursor"
EndSection
```

- ❶ O `BusID` refere-se ao slot PCI ou AGP no qual a placa de vídeo está instalada. Isso corresponde ao ID exibido pelo comando `lspci`. O servidor X precisa de detalhes no formato decimal, mas o `lspci` os exibe no formato hexadecimal. O valor de `BusID` é detectado automaticamente pelo SaX2.
- ❷ O valor de `Driver` é definido automaticamente pelo SaX2 e especifica qual o driver a ser usado para a sua placa de vídeo. Se a placa for Matrox Millennium, o módulo do driver será chamado `mga`. Em seguida, o servidor X pesquisa no `ModulePath` definido na seção `Files` no subdiretório `drivers`. Em uma instalação padrão, é o diretório `/usr/lib/xorg/modules/drivers` ou o `/usr/lib64/xorg/modules/drivers` para o diretório de sistemas operacionais de 64 bits. `_drv.o` será adicionado ao nome, por isso, no caso do driver `mga`, o arquivo de driver `mga_drv.o` será carregado.

O comportamento do servidor X ou do driver também pode ser influenciado por meio de opções adicionais. Um exemplo disso é a opção `sw_cursor`, definida na seção de dispositivo. Isso desativa o cursor do mouse do hardware e mostra o cursor do mouse usando o software. Dependendo do módulo do driver, há várias opções disponíveis (que podem ser encontradas nos arquivos de descrição dos módulos do driver no diretório `/usr/share/doc/packages/nome_do_pacote`). Opções geralmente válidas também podem ser encontradas nas páginas de manual (`man xorg.conf`, `man 4 <driver module>` e `man 4 chips`).

Se a placa de vídeo tem vários conectores de vídeo, é possível configurar os diferentes dispositivos dessa placa como uma única tela. Use o SaX2 para configurar sua interface de vídeo dessa maneira.

14.1.3 Seção Monitor e Modes

Como as seções `Device`, as seções `Monitor` e `Modes` descrevem um monitor cada. O arquivo de configuração `/etc/X11/xorg.conf` pode conter quantas seções `Monitor` você desejar. Cada seção `Monitor` faz referência a uma seção `Modes` com a linha `UseModes`, se houver. Se não houver nenhuma seção `Modes` disponível para a seção `Monitor`, o servidor X calculará valores apropriados a partir dos valores de sincronização gerais. A seção de layout do servidor especifica qual seção `Monitor` é relevante.

Definições de monitor devem ser configuradas por usuários experientes. As modelines constituem uma parte importante das seções `Monitor`. Linhas modelo definem temporizações verticais para a respectiva resolução. As propriedades do monitor, especialmente as frequências permitidas, estão armazenadas na seção `Monitor`. Modos VESA padrão podem ser gerados com o utilitário `cvt`. Para obter mais informações, leia a página de manual do `cvt` `man cvt`.

ATENÇÃO

A menos que você tenha conhecimento aprofundado sobre as funções do monitor e da placa de vídeo, não mude as modelines, pois isso pode danificar gravemente o monitor.

As pessoas que tentam desenvolver suas próprias descrições de monitor devem estar familiarizadas com a documentação em `/usr/share/X11/doc`. Instale o pacote `xorg-x11-doc` para encontrar PDFs e páginas em HTML.

A especificação manual de linhas modelo raramente é exigida atualmente. Se você está usando um monitor multisync moderno, as frequências permitidas e as resoluções ideais podem, como regra, ser lidas diretamente do monitor pelo servidor X via DDC, como descrito na seção de configuração do SaX2. Se isso não for possível por algum motivo, use um dos modos VESA incluídos no servidor X. Isso funcionará com a maioria das combinações de monitor e placa de vídeo.

14.2 Instalando e configurando fontes

A instalação de fontes adicionais no SUSE Linux Enterprise Desktop é muito fácil. Simplesmente copie as fontes para qualquer diretório localizado no caminho da fonte X11 (consulte a Seção 14.2.1, “Fontes centrais X11” (p 188)). Para habilitar o uso das fontes, o diretório de instalação deve ser um subdiretório dos diretórios configurados em `/etc/fonts/fonts.conf` (consulte a Seção 14.2.2, “Xft” (p 189)) ou incluso neste arquivo com `/etc/fonts/suse-font-dirs.conf`.

O arquivo a seguir é um exemplo de `/etc/fonts/fonts.conf`. Esse é o arquivo de configuração padrão que deve ser apropriado para a maioria das configurações. Define também o diretório incluso `/etc/fonts/conf.d`. Nesse diretório, todos os arquivos ou links simbólicos que começam com um número de dois dígitos são

carregados pelo fontconfig. Para obter uma explicação mais detalhada dessa funcionalidade, consulte `/etc/fonts/conf.d/README`.

```
<!-- Font directory list -->
<dir>/usr/share/fonts</dir>
<dir>/usr/X11R6/lib/X11/fonts</dir>
<dir>/opt/kde3/share/fonts</dir>
<dir>/usr/local/share/fonts</dir>
<dir>~/.fonts</dir>
```

`/etc/fonts/suse-font-dirs.conf` é gerado automaticamente para reunir fontes que acompanham aplicativos (em sua maioria de terceiros) como OpenOffice.org, Java ou Adobe Acrobat Reader. Uma entrada típica seria semelhante ao seguinte:

```
<dir>/usr/lib/Adobe/Reader9/Resource/Font</dir>
<dir>/usr/lib/Adobe/Reader9/Resource/Font/PPM</dir>
```

Para instalar fontes adicionais em todo o sistema, copie manualmente os arquivos de fonte em um diretório adequado (como o `raiz`), tal como `/usr/share/fonts/truetype`. Alternativamente, a tarefa pode ser realizada com o instalador de fontes do KDE no Centro de Controle do KDE. O resultado é o mesmo.

Em vez de copiar as fontes reais, você também pode criar links simbólicos. Por exemplo, é recomendável fazer isso se você tiver fontes licenciadas em uma partição do Windows montada e desejar usá-las. Em seguida, execute `SuSEconfig --module fonts`.

`SuSEconfig --module fonts` executa o script `/usr/sbin/fonts-config`, que lida com a configuração das fontes. Para obter mais informações sobre esse script, consulte sua página de manual (`man fonts-config`).

O procedimento é o mesmo para fontes de bitmap, fontes TrueType e OpenType, e fontes Type1 (PostScript). Todos esses tipos de fonte podem ser instalados em qualquer diretório.

O X.Org contém dois sistemas de fontes completamente diferentes: o antigo *sistema de fontes centrais X11* e o recém-criado sistema *Xft e fontconfig*. As seções a seguir descrevem brevemente esses dois sistemas.

14.2.1 Fontes centrais X11

Atualmente, o sistema de fontes centrais X11 suporta não apenas fontes de bitmap, mas também fontes escaláveis, como fontes Type1, TrueType e OpenType. Fontes escaláveis são suportadas somente sem a exibição de subpixel e antialiasing, e o carregamento de fontes escaláveis grandes com glifos para vários idiomas pode levar muito tempo. As fontes Unicode também são suportadas, mas seu uso pode ser lento e exigir mais memória.

O sistema de fontes centrais X11 tem algumas fraquezas inerentes. Ele está desatualizado e não pode mais ser estendido de forma significativa. Embora ele possa ser mantido por motivos de compatibilidade retroativa, o sistema Xft e fontconfig mais moderno deve ser usado se for possível.

Para sua operação, o servidor X precisa saber quais fontes estão disponíveis e onde ele pode encontrá-las no sistema. Isso é tratado por uma variável `FontPath`, que contém o caminho para todos os diretórios de fontes de sistemas válidos. Em cada um desses diretórios, um arquivo chamado `fonts.dir` lista as fontes disponíveis nesse diretório. O `FontPath` é gerado pelo servidor X na inicialização. Ele procura um arquivo `fonts.dir` válido em cada uma das entradas `FontPath` no arquivo de configuração `/etc/X11/xorg.conf`. Essas entradas são encontradas na seção `Files`. Exiba o `FontPath` real com `xset q`. Esse caminho também pode ser modificado no tempo de execução com `xset`. Para adicionar outro caminho, use `xset +fp <path>`. Para remover um caminho indesejado, use `xset -fp <path>`.

Se o servidor X já estiver ativo, fontes recém-instaladas em diretórios montados poderão ser disponibilizadas com o comando `xsetfp rehash`. Esse comando é executado por `SuSEconfig --module fonts`. Como o comando `xset` precisa de acesso ao servidor X em execução, isso funciona apenas se `SuSEconfig --module fonts` for iniciado de um shell com acesso ao servidor X em execução. A maneira mais fácil de conseguir isso é adquirir permissões de `root` digitando `su` e a senha do `root`. `su` transfere as permissões de acesso do usuário que iniciou o servidor X para o shell do `root`. Para verificar se as fontes foram instaladas corretamente e estão disponíveis por meio do sistema de fontes centrais X11, use o comando `xlsfonts` para listar todas as fontes disponíveis.

Por padrão, o SUSE Linux Enterprise Desktop usa idiomas UTF-8. Dessa forma, fontes Unicode devem ser preferidas (nomes de fontes terminados com `iso10646-1` na

saída `xlsfonts`). Todas as fontes Unicode disponíveis podem ser relacionadas com `xlsfonts | grep iso10646-1`. Praticamente todas as fontes Unicode disponíveis no SUSE Linux Enterprise Desktop contêm pelo menos os glifos necessários para os idiomas europeus (anteriormente codificados como `iso-8859-*`).

14.2.2 Xft

Desde o início, os programadores do Xft certificaram-se de que as fontes escaláveis, incluindo as de antialiasing, tivessem suporte adequado. Se o Xft for usado, as fontes serão exibidas pelo aplicativo usando as fontes, não pelo servidor X como no sistema de fontes central X11. Dessa forma, o respectivo aplicativo tem acesso aos arquivos de fontes reais e controle total sobre como os glifos são exibidos. Isso constitui a base para a exibição correta do texto em vários idiomas. Acesso direto aos arquivos de fontes é bastante útil para embutir fontes para impressão para garantir que a impressão tenha a mesma aparência da saída da tela.

No SUSE Linux Enterprise Desktop, os dois ambientes de área de trabalho (KDE e GNOME), o Mozilla e muitos outros aplicativos já usam o Xft por padrão. O Xft já é usado por mais aplicativos do que o sistema de fontes central X11 antigo.

O Xft usa a biblioteca `fontconfig` para localizar fontes e influenciar a maneira como elas são exibidas. As propriedades do `fontconfig` são controladas pelo arquivo de configuração global `/etc/fonts/fonts.conf`. Configurações especiais devem ser adicionadas a `/etc/fonts/local.conf` e ao arquivo de configuração específico do usuário `~/.fonts.conf`. Cada um desses arquivos de configuração `fontconfig` deve iniciar com

```
<?xml version="1.0"?>
<!DOCTYPE fontconfig SYSTEM "fonts.dtd">
<fontconfig>
```

e terminar com

```
</fontconfig>
```

Para adicionar diretórios para pesquisar fontes, acrescente linhas como as seguintes:

```
<dir>/usr/local/share/fonts/</dir>
```

Porém, isso geralmente não é necessário. Por padrão, o diretório específico do usuário `~/ .fonts` já está inserido em `/etc/fonts/fonts.conf`. Da mesma maneira, tudo o que você precisa fazer para instalar fontes adicionais é copiá-las para `~/ .fonts`.

Você também pode inserir regras que influenciam a aparência das fontes. Por exemplo, digite

```
<match target="font">
  <edit name="antialias" mode="assign">
    <bool>false</bool>
  </edit>
</match>
```

Para desabilitar o antialiasing para todas as fontes ou

```
<match target="font">
  <test name="family">
    <string>Luxi Mono</string>
    <string>Luxi Sans</string>
  </test>
  <edit name="antialias" mode="assign">
    <bool>false</bool>
  </edit>
</match>
```

para desabilitar o antialiasing para fontes específicas.

Por padrão, a maioria dos aplicativos usa os nomes de fontes `sans-serif` (ou o equivalente `sans`), `serif` ou `monospace`. Essas não são fontes reais, mas somente aliás que são resolvidos para uma fonte adequada, dependendo da configuração de idioma.

Usuários podem facilmente adicionar regras para `~/ .fonts.conf` a fim de resolver esses aliás para suas fontes favoritas:

```
<alias>
  <family>sans-serif</family>
  <prefer>
    <family>FreeSans</family>
  </prefer>
</alias>
<alias>
  <family>serif</family>
  <prefer>
    <family>FreeSerif</family>
  </prefer>
</alias>
```

```

<alias>
  <family>monospace</family>
  <prefer>
    <family>FreeMono</family>
  </prefer>
</alias>

```

Como quase todos os aplicativos usam esses aliás por padrão, isso afeta praticamente todo o sistema. Dessa forma, você pode facilmente usar suas fontes favoritas praticamente em qualquer local, sem precisar modificar as configurações de fontes nos aplicativos individuais.

Use o comando `fc-list` para encontrar as fontes instaladas e disponíveis para uso. Por exemplo, o comando `fc-list` retorna uma lista de todas as fontes. Para descobrir quais das fontes escaláveis disponíveis (`:scalable=true`) contêm todos os glifos exigidos para hebraico (`:lang=he`), os nomes de fontes (`family`), o estilo (`style`), o peso (`weight`) e o nome dos arquivos que contêm as fontes, digite o seguinte comando:

```
fc-list ":lang=he:scalable=true" family style weight
```

A saída do comando pode ter a seguinte aparência:

```

Lucida Sans:style=Demibold:weight=200
DejaVu Sans:style=Bold Oblique:weight=200
Lucida Sans Typewriter:style=Bold:weight=200
DejaVu Sans:style=Oblique:weight=80
Lucida Sans Typewriter:style=Regular:weight=80
DejaVu Sans:style=Book:weight=80
DejaVu Sans:style=Bold:weight=200
Lucida Sans:style=Regular:weight=80

```

Parâmetros importantes podem ser consultados com `fc-list`:

Tabela 14.2 *Parâmetros de `fc-list`*

Parâmetro	Significado e valores possíveis
<code>family</code>	Nome da família da fonte, por exemplo, <code>FreeSans</code> .
<code>foundry</code>	Nome do fabricante da fonte, por exemplo, <code>urw</code> .

Parâmetro	Significado e valores possíveis
<code>estilo</code>	O estilo da fonte, como Medium, Regular, Bold, Italic ou Heavy.
<code>lang</code>	O idioma que a fonte suporta, por exemplo, de para alemão, ja para japonês, zh-TW para chinês tradicional ou zh-CN para chinês simplificado.
<code>weight</code>	O peso da fonte, como 80 para normal ou 200 para negrito.
<code>slant</code>	A inclinação, geralmente 0 para nenhum e 100 para itálico.
<code>SETUP.ISS</code>	O nome do arquivo que contém a fonte.
<code>outline</code>	<code>true</code> para fontes de bordas ou <code>false</code> para outras fontes.
<code>scalable</code>	<code>true</code> para fontes escaláveis ou <code>false</code> para outras fontes.
<code>bitmap</code>	<code>true</code> para fontes de bitmap ou <code>false</code> para outras fontes.
<code>pixelsize</code>	Tamanho de fonte em pixels. Em conexão com a <code>fc-list</code> , essa opção só faz sentido para fontes de bitmap.

14.3 Para obter mais informações

Instale os pacotes `xorg-x11-doc` e `howtoenh` para obter informações mais aprofundadas sobre o X11. Mais informações sobre o desenvolvimento do X11 podem ser encontradas na home page do projeto, em <http://www.x.org>.

Muitos dos drivers fornecidos com o pacote `xorg-x11-driver-video` são descritos em detalhes em uma página de manual. Por exemplo, se você usar o driver `nv`, encontre mais informações sobre ele em `man 4 nv`.

Informações sobre drivers de terceiros devem estar disponíveis em `/usr/share/doc/packages/<package_name>`. Por exemplo, a documentação de `x11-video-nvidiaG01` está disponível em `/usr/share/doc/packages/x11-video-nvidiaG01` após a instalação do pacote.

Acessando sistemas de arquivos com o FUSE

15

FUSE é o acrônimo de *sistema de arquivos do espaço do usuário*. Isso significa que você pode configurar e montar um sistema de arquivos como um usuário sem privilégios. Normalmente, é necessário ser o `root` para executar essa tarefa. O FUSE, isoladamente, é um módulo de kernel. Combinado-o a plug-ins, você pode estender o FUSE para acessar quase todos os sistemas de arquivos, como conexões SSH remotas, imagens ISO e muito mais.

15.1 Configurando o FUSE

Antes de usar o FUSE, é necessário instalar o pacote `fuse`. Dependendo do sistema de arquivos que você deseja usar, serão necessários plug-ins adicionais, disponíveis em pacotes separados.

Em geral, não é necessário configurar o FUSE, basta usá-lo. Entretanto, convém criar um diretório no qual todos os seus pontos de montagem são combinados. Por exemplo, você pode criar um diretório `~/mounts` e inserir nele subdiretórios para os diferentes sistemas de arquivo.

15.2 Plug-ins disponíveis do FUSE

O FUSE depende de plug-ins. A tabela a seguir lista os plug-ins comuns.

Tabela 15.1 *Plug-ins disponíveis do FUSE*

<code>fuseiso</code>	monta imagens de CD-ROM contendo sistemas de arquivos ISO9660
<code>ntfs-3g</code>	monta volumes NTFS (com suporte de leitura e gravação)
<code>sshfs</code>	cliente de sistema de arquivos com base no protocolo de transferência de arquivo SSH
<code>wdfs</code>	monta sistemas de arquivos WebDAV

15.3 Para obter mais informações

Consulte a home page <http://fuse.sourceforge.net> do FUSE para obter mais informações.

Parte III. Computadores móveis

Computação móvel com o Linux

16

A computação móvel é geralmente associada a laptops, PDAs e telefones celulares (e ao intercâmbio de dados entre esses aparelhos). Componentes de hardware móveis, como discos rígidos externos, unidades flash ou câmeras digitais, podem ser conectados a laptops ou sistemas de desktop. Vários componentes de software estão envolvidos em cenários de computação e alguns aplicativos são desenvolvidos para uso móvel.

16.1 Laptops

O hardware de laptops difere do hardware de um sistema de desktop normal. Isso se deve a critérios como permutabilidade, requisitos de espaço e consumo de energia, que devem ser levados em conta. Os fabricantes de hardware móvel desenvolveram interfaces padrão, como PCMCIA (Personal Computer Memory Card International Association), Mini PCI e Mini PCIe, que podem ser usadas para estender o hardware de laptops. Os padrões abrangem cartões de memória, placas de interface de rede, ISDN (bem como placas de modem) e discos rígidos externos.

DICA: SUSE Linux Enterprise Desktop e Tablet PCs

O SUSE Linux Enterprise Desktop também suporta Tablet PCs. Os Tablet PCs incluem um touchpad/digitalizador que permite usar uma caneta digital, ou mesmo as pontas dos dedos, para editar dados diretamente na tela, em vez de usar mouse e teclado. Eles são instalados e configurados da mesma maneira que qualquer outros sistemas. Para obter uma introdução detalhada sobre a instalação e configuração de Tablet PCs, consulte o Capítulo 19, *Usando Tablet PCs* (p 235).

16.1.1 Conservação de energia

A inclusão de componentes de sistema com otimização de energia durante a fabricação de laptops contribui para a sua adequação ao uso sem acesso à rede elétrica. A contribuição desses componentes para a preservação de energia é, ao menos, tão importante quanto a do sistema operacional. O SUSE® Linux Enterprise Desktop oferece suporte a diversos métodos que influenciam o consumo de energia de um laptop e surtem efeitos variáveis sobre o tempo de operação com a carga da bateria. A lista a seguir está em ordem decrescente de contribuição para a conservação de energia:

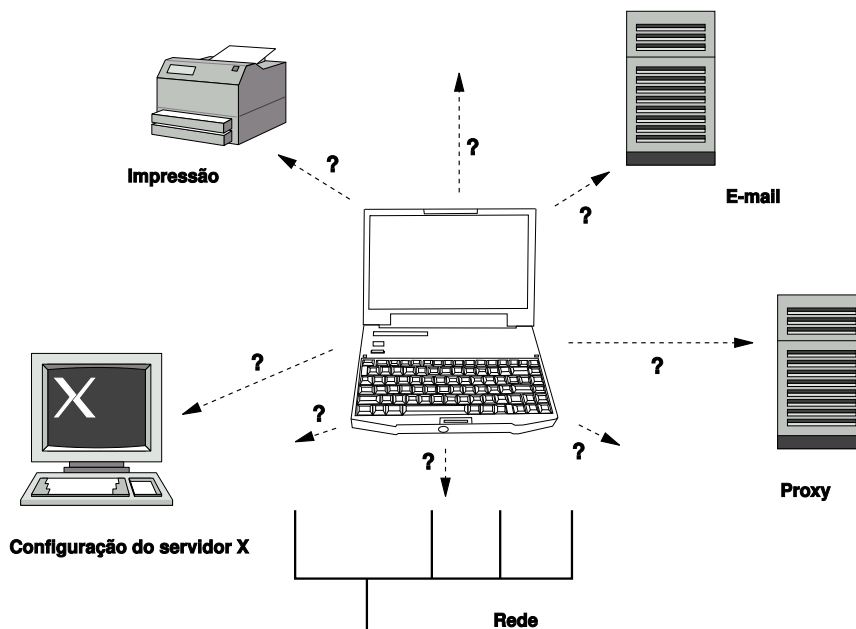
- Regulagem da velocidade da CPU.
- Desativação da iluminação da tela durante pausas.
- Ajuste manual da iluminação da tela.
- Desconexão de acessórios não utilizados e habilitados para hotplug (CD-ROM USB, mouse externo, placas PCMCIA sem uso, WLAN etc.).
- Colocação do disco rígido em modo de espera quando inativo.

Para obter mais informações sobre gerenciamento de energia específico de área de trabalho, consulte a Seção “Controlando o gerenciamento de energia da área de trabalho” (Capítulo 2, *Trabalhando com a área de trabalho*, ↑ *Guia do Usuário do GNOME*), que explica como usar o Gerenciador de Energia do GNOME. Mais informações sobre o applet de gerenciamento de energia do KDE estão disponíveis no Capítulo 9, *Controlling Your Desktop's Power Management* (↑ *KDE User Guide*).

16.1.2 Integração em ambientes operacionais variáveis

Seu sistema precisa se adaptar a ambientes operacionais variáveis quando for usado para a computação móvel. Vários serviços dependem do ambiente, e os clientes subjacentes precisam ser reconfigurados. O SUSE Linux Enterprise Desktop se encarrega dessa tarefa para você.

Figura 16.1 Integrando um computador móvel em um ambiente existente



Os serviços afetados no caso de um laptop que transita entre uma pequena rede doméstica e uma rede de escritório são:

Rede

Inclui a atribuição de endereço IP, a resolução do nome, a conectividade à Internet e a conectividade a outras redes.

Impressão

Precisam estar presentes um banco de dados atual de impressoras disponíveis e um servidor de impressão disponível, dependendo da rede.

E-mail e proxies

Assim como ocorre com a impressão, a lista dos servidores correspondentes precisa ser atual.

X (ambiente gráfico)

Se o seu laptop estiver temporariamente conectado a um projetor ou monitor externo, configurações de exibição diferentes precisam estar disponíveis.

O SUSE Linux Enterprise Desktop oferece várias opções de integração de laptops aos ambientes operacionais existentes:

NetworkManager

O NetworkManager é especialmente adaptado para rede móvel em laptops. Ele fornece uma maneira para alternar de forma fácil e automática entre ambientes de rede e tipos diferentes de redes, como rede local wireless e ethernet. O NetworkManager suporta criptografia WEP e WPA/WPA2-PSK em redes locais wireless. Ele também suporta conexões discadas (com smpppd), conexões DSL e a opção de configurar VPNs (virtual private networks). Ambos os ambientes de área de trabalho (GNOME e KDE) incluem um front end para o NetworkManager. Para obter mais informações sobre os applets de área de trabalho, consulte a Seção 23.4, “Usando o KNetworkManager” (p 328) e a Seção 23.5, “Usando o applet NetworkManager do GNOME” (p 333).

Tabela 16.1 Casos de uso do NetworkManager

Meu computador...	Uso do NetworkManager
é um laptop	Sim
algumas vezes está conectado a redes diferentes	Sim
fornece serviços de rede (como DNS ou DHCP)	Não
usa somente um endereço IP estático	Não

Use as ferramentas de rede do YaST para configurar a rede sempre que o NetworkManager não puder tratar a configuração de rede corretamente.

DICA: configuração DNS e vários tipos de conexões de rede

Se você está sempre viajando com seu laptop e usando tipos de conexões de rede diferentes, o NetworkManager funciona bem quando todos os endereços DNS estão atribuídos corretamente com o DHCP. Se alguma das suas conexões usar endereço(s) DNS estático(s), adicione-o(s) ao `NETCONFIG_DNS_STATIC_SERVERS` em `/etc/sysconfig/network/config`.

SCPM

O SCPM (system configuration profile management - gerenciamento de perfil de configuração do sistema) permite o armazenamento de estados de configuração arbitrários de um sistema em um tipo de “instantâneo” chamado de *perfil*. Os perfis podem ser criados para diferentes situações. Eles são úteis quando um sistema é operado em ambientes variáveis (rede doméstica, rede empresarial). Sempre é possível alternar entre perfis. Para que o SCPM funcione no seu sistema, instale o pacote `scpm`. Habilite o SCPM usando o módulo Gerenciamento de Perfis do YaST e configure os usuários que têm permissão de alternar perfis sem precisar digitar a senha do `root`. Determine se as mudanças de perfil devem sobreviver à reinicialização do sistema ou se devem ser descartadas no encerramento do sistema. Verifique se todos os grupos de recursos (por exemplo, serviços como rede e impressora) estão ativos. Proceda para a criação de perfis reais usando a ferramenta de linha de comando `scpm`. Consulte a página de manual de `scpm` para obter detalhes. Crie perfis para todas as configurações diferentes em que você deseja

usar o sistema. A alternância entre perfis pode ser feita com o sistema em execução, por meio do `switch scpm NOME_DO_PERFIL`, ou no momento do boot do sistema, por meio da tecla F3. Quando ocorre alternância de perfis, o SCPM ajusta automaticamente a configuração do sistema ao novo ambiente descrito no perfil escolhido.

SLP

O SLP (Service Location Protocol) simplifica a conexão do seu laptop para uma rede existente. Sem o SLP, o administrador do laptop normalmente necessita ter conhecimentos detalhados sobre os serviços disponíveis em uma rede. O SLP transmite a disponibilidade de um determinado tipo de serviço a todos os clientes de uma rede local. Os aplicativos que dão suporte ao SLP podem processar as informações despachadas pelo SLP e podem ser configurados automaticamente. O SLP também pode ser usado para instalar um sistema, minimizando o esforço de procurar uma fonte de instalação adequada. Encontre informações detalhadas sobre o SLP no Capítulo 21, *Serviços SLP na rede* (p 311).

16.1.3 Opções de software

Várias áreas de tarefas especiais no uso móvel ficam a cargo de software dedicado: monitoração do sistema (especialmente a carga da bateria), sincronização de dados e comunicação wireless com periféricos e com a Internet. As seções a seguir abordam os aplicativos mais importantes oferecidos pelo SUSE Linux Enterprise Desktop para cada tarefa.

Monitoração do sistema

Duas ferramentas de monitoração do sistema do KDE são oferecidas pelo SUSE Linux Enterprise Desktop:

PowerDevil

PowerDevil é um aplicativo, que pode ser aberto pelo *Disparador de Aplicativos Kickoff* (*Configurar Área de Trabalho > Avançado > Gerenciamento de Energia*) ou pelo ícone de bandeja do *Monitor de Bateria*. O ícone do applet se ajusta de modo a representar o tipo de fonte de alimentação. Ao trabalhar em corrente alternada, um pequeno ícone de raio é exibido. Ao trabalhar com bateria, o ícone se transforma em uma bateria.

Clique no ícone de bandeja do PowerDevil para acessar as opções para configurar seu comportamento. Você pode escolher um dos cinco perfis de energia exibidos, de acordo com as suas necessidades. Por exemplo, o esquema *Apresentação* desabilita a proteção de tela e o gerenciamento de energia em geral, de modo que a sua apresentação não seja interrompida pelos eventos do sistema. Clique em *Mais...* para abrir a tela de configuração do PowerDevil. Aqui você pode editar perfis individuais e definir opções avançadas de gerenciamento de energia, como o que fazer quando a tampa do laptop for fechada ou quando a bateria estiver fraca.

KSysguard

O KSysguard é um aplicativo independente que reúne todos os parâmetros mensuráveis do sistema em um único ambiente de monitoração. O KSysguard possui monitores de ACPI (status da bateria), carga da CPU, rede, particionamento, uso da memória e outros parâmetros do sistema. Ele também pode observar e exibir todos os processos do sistema. A apresentação e filtragem dos dados coletados podem ser personalizadas. É possível monitorar diferentes parâmetros do sistema em diversas páginas de dados ou coletar os dados de diversas máquinas em paralelo na rede. O KSysguard também pode ser executado como um daemon em máquinas desprovidas de um ambiente KDE. Há mais informações sobre esse programa na respectiva função de ajuda integrada ou nas páginas de ajuda do SUSE.

Na área de trabalho GNOME, use as Preferências de Energia e o Monitor do Sistema do GNOME.

Sincronizando dados

Ao alternar entre o trabalho em uma máquina móvel desconectada da rede e o trabalho em uma estação em rede em um escritório, é necessário manter a sincronização dos dados processados em todas as instâncias. Isso pode incluir pastas de e-mail, diretórios e arquivos individuais que precisam estar presentes tanto para o trabalho remoto como para o trabalho no escritório. A solução nos dois casos é a seguinte:

Sincronizando e-mail

Use uma conta IMAP para armazenar seus e-mails na rede empresarial. Em seguida, acesse os e-mails da estação de trabalho usando qualquer cliente de e-mail habilitado para IMAP que esteja desconectado, como o Mozilla Thunderbird Mail, o Evolution ou o KMail, conforme descrito no *Guia do Usuário do GNOME* (↑*Guia do Usuário do GNOME*) e no *KDE User Guide* (↑*KDE User Guide*). O cliente de e-mail precisa ser configurado de tal modo que as Mensagens enviadas sejam sempre

acessadas da mesma pasta. Isso assegura a disponibilidade de todas as mensagens com informações sobre seu status após a conclusão do processo de sincronização. Use um servidor SMTP implementado no cliente de e-mail para o envio de mensagens, em vez do postfix ou do sendmail do MTA em todo o sistema, para receber retorno confiável sobre e-mails não enviados.

Sincronizando arquivos e diretórios

Existem diversos utilitários adequados para a sincronização de dados entre um laptop e uma estação de trabalho. Um dos mais usados é uma ferramenta de área de trabalho chamada `rsync`. Para obter mais informações, consulte a respectiva página de manual (`man 1 rsync`).

Comunicação sem fio

Além da conexão a redes domésticas ou empresariais por cabo, também é possível fazer uma conexão wireless de um laptop para acessar outros computadores, periféricos, telefones celulares ou PDAs. O Linux oferece suporte a três tipos de comunicação wireless:

WLAN

Com o maior alcance dessas tecnologias wireless, a WLAN é a única adequada para a operação de redes de grande porte e, às vezes, até mesmo de redes virtualmente separadas. Máquinas individuais podem se conectar entre si para formar uma rede wireless independente ou para acessar a Internet. Dispositivos chamados de *pontos de acesso* atuam como estações de base para dispositivos habilitados para WLAN, além de servir como intermediários para o acesso à Internet. Um usuário móvel pode alternar entre pontos de acesso dependendo do local e de que ponto de acesso ofereça a melhor conexão. Assim como na telefonia celular, uma rede de grande porte está disponível aos usuários da WLAN sem restringi-los a um local específico para o acesso. Encontre informações sobre a WLAN no Capítulo 17, *Rede local sem fio* (p 211).

Bluetooth

Entre todas as tecnologias wireless, o Bluetooth é a que possui o mais amplo espectro de aplicação. Ele pode ser usado na comunicação entre computadores (laptops) e PDAs ou telefones celulares, assim como o IrDA. Também pode ser utilizado para conectar diversos computadores dentro de uma extensão. O bluetooth também é usado para conectar componentes wireless do sistema, como um teclado ou mouse. Entretanto, o alcance dessa tecnologia não é suficiente para conectar

sistemas remotos a uma rede. A WLAN é a melhor opção de tecnologia para comunicações em locais com obstáculos físicos, como paredes.

IrDA

O IrDA é a tecnologia wireless de menor alcance. As duas extremidades da comunicação precisam estar a uma distância visível uma da outra. Não é possível contornar obstáculos como paredes. Uma aplicação possível do IrDA é a transmissão de arquivos de um laptop para um telefone celular. O curto caminho do laptop para o telefone celular é coberto com o uso do IrDA. O transporte de longo alcance do arquivo ao seu destinatário é feito pela rede móvel. Outra aplicação do IrDA é a transmissão wireless de serviços de impressão no escritório.

16.1.4 Segurança de dados

Em termos ideais, os dados contidos no seu laptop são protegidos de diversas maneiras contra o acesso não autorizado. Possíveis medidas de segurança podem ser tomadas nas seguintes áreas:

Proteção contra roubo

Sempre que possível proteja a integridade física do seu sistema contra roubo. Diversas ferramentas de segurança (como correntes) podem ser adquiridas em lojas varejistas.

Autenticação avançada

Use a autenticação biométrica juntamente com a autenticação padrão por meio de login e senha. O SUSE Linux Enterprise Desktop suporta a autenticação por impressão digital. Para obter mais detalhes, consulte o Capítulo 7, *Using the Fingerprint Reader* (↑*Security Guide (Guia de Segurança)*).

Protegendo dados no sistema

Dados importantes devem ser criptografados não apenas durante a transmissão, mas também no disco rígido. Essa medida assegura sua segurança em caso de roubo. A criação de uma partição criptografada com o SUSE Linux Enterprise Desktop é descrita no Capítulo 11, *Encrypting Partitions and Files* (↑*Security Guide (Guia de Segurança)*). Outra possibilidade é criar diretórios pessoais criptografados ao adicionar o usuário com o YaST.

IMPORTANTE: segurança de dados e o evento Suspend para Disco

As partições criptografadas não são desmontadas durante um evento de suspend para disco. Assim, todos os dados contidos nessas partições ficarão disponíveis para qualquer pessoa que conseguir roubar o hardware e inicializar o disco rígido.

Segurança da rede

Qualquer transferência de dados deve ser protegida, independentemente de como seja feita. Para obter mais informações sobre problemas gerais de segurança referentes ao Linux e redes, consulte o Capítulo 1, *Security and Confidentiality* (↑*Security Guide (Guia de Segurança)*). Medidas de segurança referentes a redes wireless são fornecidas no Capítulo 17, *Rede local sem fio* (p 211).

16.2 Hardware móvel

O SUSE Linux Enterprise Desktop suporta a detecção automática de dispositivos de armazenamento móveis em FireWire (IEEE 1394) ou USB. O termo *dispositivo de armazenamento móvel* se aplica a qualquer tipo de disco rígido FireWire ou USB, unidade flash USB ou câmera digital. Esses dispositivos são automaticamente detectados e configurados logo após serem conectados ao sistema pela interface correspondente. Os gerenciadores de arquivos do GNOME e do KDE oferecem controle flexível de itens de hardware móveis. Para desmontar qualquer uma dessas mídias com segurança, use o recurso *Remover de Modo Seguro* (KDE) ou *Desmontar Volume* (GNOME) dos gerenciadores de arquivos. O gerenciamento de mídia removível pela área de trabalho é descrito em mais detalhes no *Guia do Usuário do GNOME* (↑*Guia do Usuário do GNOME*) e no *KDE User Guide* (↑*KDE User Guide*).

Discos rígidos externos (USB e FireWire)

Assim que o disco rígido externo for corretamente reconhecido pelo sistema, seu ícone aparecerá no gerenciador de arquivos. Clique no ícone para exibir o conteúdo da unidade. É possível criar pastas e arquivos aqui, além de editá-los ou apagá-los. Para mudar o nome que um disco rígido recebeu do sistema, clique o botão direito do mouse no ícone e selecione o item correspondente no menu. Essa mudança de nome é limitada à exibição no gerenciador de arquivos. O descritor através do qual o dispositivo é montado em `/media` permanece não afetado por isso.

Unidades flash USB

Esses dispositivos são tratados pelo sistema como discos rígidos externos. Também nesses dispositivos é possível renomear as entradas do gerenciador de arquivos.

Câmeras digitais (USB e FireWire)

As câmeras digitais reconhecidas pelo sistema também aparecem como unidades externas na visão geral do gerenciador de arquivos. O KDE permite a leitura e o acesso às imagens no URL `camera:/`. Essas imagens podem ser processadas com o digiKam ou o f-spot. Para o processamento avançado de fotos, use o GIMP. Para obter uma introdução resumida do digiKam, do f-spot e do GIMP, consulte o Capítulo 20, *DigiKam: gerenciando sua coleção de imagens digitais* (↑*Guia de Aplicativos*), o Capítulo 21, *F-Spot: gerenciando sua coleção de imagens digitais* (↑*Guia de Aplicativos*) e o Capítulo 19, *GIMP: manipulando gráficos* (↑*Guia de Aplicativos*).

16.3 Telefones celulares e PDAs

Tanto um sistema de desktop como um laptop podem se comunicar com um telefone celular via Bluetooth ou IrDA. Alguns modelos dão suporte aos dois protocolos; outros, somente a um dos dois. As áreas de uso dos dois protocolos e a extensa documentação correspondente já foram citadas na “Comunicação sem fio” (p 206). A configuração desses protocolos nos telefones celulares é descrita nos respectivos manuais.

O suporte à sincronização com dispositivos portáteis fabricados pela Palm, Inc. já vem incorporado ao Evolution e ao Kontact. A conexão inicial com o dispositivo é facilmente realizada com um assistente. Após a configuração do suporte para Palm Pilots, é necessário determinar que tipo de dados deve ser sincronizado (endereços, compromissos etc.). Para obter mais informações, consulte *Guia do Usuário do GNOME* (↑*Guia do Usuário do GNOME*) e *KDE User Guide* (↑*KDE User Guide*).

Uma solução de sincronização mais sofisticada está disponível com o programa `opensync` (consulte o pacote `libopensync` e respectivos plug-ins de cada dispositivo).

16.4 Para obter mais informações

O ponto central de referência para todas as dúvidas relativas a dispositivos móveis e o Linux é <http://tuxmobil.org/>. Diversas seções desse site da Web tratam de

aspectos de hardware e software de laptops, PDAs, telefones celulares e outros hardwares móveis.

Uma abordagem semelhante de <http://tuxmobil.org/> é feita por <http://www.linux-on-laptops.com/>. Informações sobre laptops e dispositivos portáteis podem ser encontradas nesse local.

O SUSE mantém uma lista de discussão em alemão dedicada a laptops. Consulte <http://lists.opensuse.org/opensuse-mobile-de/>. Nessa lista, usuários e desenvolvedores discutem todos os aspectos da computação móvel com o uso do SUSE Linux Enterprise Desktop. As mensagens em inglês são respondidas, mas a maioria das informações dos arquivos está disponível somente em alemão. Use <http://lists.opensuse.org/opensuse-mobile/> para ver postagens em inglês.

As informações sobre o OpenSync estão disponíveis em <http://en.opensuse.org/OpenSync>.

Rede local sem fio

As WLANs (Wireless Local Area Networks - redes locais wireless) passaram a ser um item indispensável na computação móvel. Atualmente, a maioria dos laptops tem placas WLAN embutidas. Este capítulo descreve como configurar uma placa de WLAN com o YaST, criptografar transmissões e usar dicas.

17.1 Padrões de WLAN

As placas de WLAN comunicam-se usando o padrão 802.11, preparado pela organização IEEE. Originalmente, esse padrão fornecia uma taxa de transmissão máxima de 2 MBit/s. Enquanto isso, vários suplementos foram adicionados para aumentar a taxa de dados. Esses suplementos definem detalhes como modulação, saída de transmissão e taxas de transmissão (consulte a Tabela 17.1, “Visão geral de vários padrões de WLAN” (p 212)). Além disso, muitas empresas implementam hardware com recursos proprietários ou preliminares.

Tabela 17.1 *Visão geral de vários padrões de WLAN*

Nome	Banda (GHz)	Taxa de transmissão máxima (MBit/s)	Nota
802.11 Legado	2.4	2	Desatualizado; praticamente nenhum dispositivo final disponível
802.11a	5	54	Menos sujeito a interferência
802.11b	2.4	11	Menos comum
802.11g	2.4	54	Disseminado, compatível retroativamente com 11b
802.11n (antigo 802.11n preliminar)	2.4 e/ou 5	300	Comum

As placas 802.11 Legado não são suportadas pelo SUSE® Linux Enterprise Desktop. A maioria das placas que usam 802.11a, 802.11b, 802.11g e 802.11n preliminar é suportada. Placas novas normalmente são compatíveis com o padrão 802.11n preliminar, mas placas que utilizam o 802.11g ainda estão disponíveis.

17.2 Modos de funcionamento

Nas redes sem fio, várias técnicas e configurações são usadas para assegurar conexões rápidas, seguras e com alta qualidade. Tipos operacionais diferentes adaptam-se a configurações diferentes. Pode ser difícil escolher o método de autenticação correto. Os métodos de criptografia disponíveis possuem diferentes vantagens e armadilhas.

Basicamente, as redes wireless podem ser classificadas em três modos de rede:

Gerenciado

As redes gerenciadas têm um elemento de gerenciamento: o ponto de acesso. Nesse modo (também conhecido como modo de infra-estrutura), todas as conexões das

estações WLAN na rede passam pelo ponto de acesso, que também pode servir como uma conexão para uma ethernet.

Ad-hoc

Redes ad-hoc não possuem um ponto de acesso. As estações se comunicam diretamente entre si, portanto, uma rede ad-hoc geralmente é mais rápida do que uma rede gerenciada. Entretanto, a faixa de transmissão e o número de estações participantes são muito limitados nas redes ad-hoc. Elas também não suportam autenticação WPA. Portanto, geralmente é usado um ponto de acesso. É até mesmo possível usar uma placa WLAN como um ponto de acesso. Algumas placas suportam essa funcionalidade.

Master

No modo master, a sua placa de rede é usada como ponto de acesso. Esse modo só funciona se a sua placa WLAN tiver suporte. Os detalhes sobre a sua placa WLAN encontram-se em <http://linux-wless.passys.nl>.

17.3 Autenticação

Como uma rede sem fio é muito mais fácil de interceptar e comprometer do que uma rede com fio, os vários padrões incluem métodos de autenticação e criptografia. Na versão original do padrão IEEE 802.11, esses métodos são descritos sob o termo WEP (Wired Equivalent Privacy - privacidade equivalente à das redes com fio). Porém, como o WEP se demonstrou inseguro (consulte a Seção 17.7.2, “Segurança” (p 222)), o setor de WLAN (unificado sob o nome *Wi-Fi Alliance*) definiu uma extensão denominada WPA, que supostamente elimina os pontos fracos do WEP. O padrão IEEE 802.11i posterior (também conhecido como WPA2, porque o WPA é baseado em uma versão preliminar do 802.11i) inclui o WPA e alguns outros métodos de autenticação e criptografia.

Para garantir que apenas as estações autorizadas possam se conectar, vários mecanismos de autenticação são usados em redes gerenciadas:

Nenhum (aberto)

Um sistema aberto é um sistema que não precisa de autenticação. Qualquer estação pode se juntar à rede. Contudo, a criptografia WEP (consulte a Seção 17.4, “Criptografia” (p 215)) pode ser usada.

Chave compartilhada (de acordo com o padrão IEEE 802.11)

Nesse procedimento, a chave WEP é usada para autenticação. Porém, esse procedimento não é recomendado, porque torna a chave WEP mais suscetível a ataques. Tudo o que um invasor precisa fazer é escutar durante tempo suficiente a comunicação entre a estação e o ponto de acesso. Durante o processo de autenticação, ambos os lados trocam as mesmas informações, uma vez de forma criptografada e outra de forma não criptografada. Isso possibilita a reconstrução da chave com as ferramentas adequadas. Como esse método utiliza a chave WEP para a autenticação e para a criptografia, ele não melhora a segurança da rede. Uma estação com a chave WEP correta pode ser autenticada, criptografada e descriptografada. Uma estação que não tem a chave não pode descriptografar os pacotes recebidos. Da mesma maneira, ela não pode se comunicar, mesmo que tenha que se autenticar.

WPA-PSK, às vezes WPA-Personal (de acordo com o IEEE 802.1x)

O WPA-PSK (PSK corresponde a preshared key - chave pré-compartilhada) funciona de maneira semelhante ao procedimento Chave compartilhada. Todas as estações participantes, assim como o ponto de acesso, precisam da mesma chave. A chave tem 256 bits de tamanho e normalmente é digitada como uma frase secreta. Esse sistema não precisa de um gerenciamento de chave complexo como o WPA-EAP e é mais adequado para uso privado. Portanto, o WPA-PSK é às vezes conhecido como WPA “Home”.

WPA-EAP, às vezes WPA-Enterprise (de acordo com o IEEE 802.1x)

Na verdade, o WPA-EAP (Extensible Authentication Protocol) não é um sistema de autenticação, e sim um protocolo para transporte de informações de autenticação. O WPA-EAP é usado para proteger redes sem fio em empresas. Em redes privadas, ele é raramente usado. Por esse motivo, o WPA-EAP é às vezes conhecido como WPA “Enterprise”.

O WPA-EAP precisa de um servidor Radius para autenticar os usuários. O EAP oferece três métodos diferentes para se conectar e autenticar no servidor: TLS (Transport Layer Security), TTLS (Tunneled Transport Layer Security) e PEAP (Protected Extensible Authentication Protocol). Em resumo, essas opções funcionam da seguinte maneira:

EAP-TLS

A autenticação TLS utiliza a troca mútua de certificados para servidor e cliente. Primeiro, o servidor apresenta o seu certificado para o cliente, onde ele é avaliado. Se o certificado for considerado válido, o cliente, por sua vez,

apresenta o seu certificado para o servidor. Embora o TLS seja seguro, ele exige uma infra-estrutura de gerenciamento de certificação que funcione em sua rede. Essa infra-estrutura é raramente encontrada em redes particulares.

EAP-TTLS e PEAP

Os protocolos TTLS e PEAP são protocolos de dois estágios. No primeiro estágio, uma conexão segura é estabelecida e, no segundo, os dados de autenticação do cliente são trocados. Eles exigem muito menos overhead de gerenciamento de certificação do que o TLS, se houver.

17.4 Criptografia

Existem vários métodos de criptografia para assegurar que pessoas não autorizadas não possam ler os pacotes de dados que são trocados em uma rede sem fio nem obter acesso à rede:

WEP (definido no padrão IEEE 802.11)

Esse padrão utiliza o algoritmo de criptografia RC4, originalmente com um tamanho de chave de 40 bits, posteriormente também com 104 bits. Muitas vezes, o tamanho é declarado como 64 bits ou 128 bits, dependendo da inclusão ou não dos 24 bits do vetor de inicialização. Porém, esse padrão tem algumas fraquezas. Os ataques contra as chaves geradas por esse sistema podem ser bem-sucedidos. Contudo, é melhor usar o WEP do que não criptografar a rede de maneira alguma.

Alguns fornecedores implementaram o “WEP Dinâmico” não-padrão. Ele funciona exatamente como o WEP e compartilha os mesmos pontos fracos, exceto pelo fato de que a chave é mudada periodicamente por um serviço de gerenciamento de chave.

TKIP (definido no padrão WPA/IEEE 802.11i)

Esse protocolo de gerenciamento de chave definido no padrão WPA utiliza o mesmo algoritmo de criptografia do WEP, mas elimina sua fraqueza. Como uma nova chave é gerada para cada pacote de dados, os ataques contra essas chaves são infrutíferos. O TKIP é usado junto com o WPA-PSK.

CCMP (definido no padrão IEEE 802.11i)

O CCMP descreve o gerenciamento de chave. Normalmente, ele é usado na conexão com o WPA-EAP, mas também pode ser usado com o WPA-PSK. A criptografia

acontece de acordo com o AES e é mais forte do que a criptografia RC4 do padrão WEP.

17.5 Configuração com o YaST

IMPORTANTE: segurança em redes sem fio

Certifique-se de usar um dos métodos de autenticação e criptografia suportados para proteger o tráfego da rede. As conexões de WLAN não criptografadas permitem que terceiros interceptem todos os dados da rede. Mesmo uma criptografia mais fraca (WEP) é melhor do que nenhuma. Consulte a Seção 17.4, “Criptografia” (p 215) e a Seção 17.7.2, “Segurança” (p 222) para obter mais informações.

Uma placa WLAN geralmente é detectada durante a instalação. Caso você precise configurá-la posteriormente, faça o seguinte:

- 1 Inicie o YaST como usuário `root`.
- 2 Selecione *Dispositivos de Rede > Configurações de Rede* no centro de controle do YaST. A caixa de diálogo Configurações de Rede é aberta. Se a sua rede for atualmente controlada pelo NetworkManager, ela não poderá ser editada pelo YaST e uma mensagem de aviso será exibida. Clique em *Ok* para exibir a guia *Opções Globais*. Selecione *Método Tradicional com ifup* para habilitar a edição com o YaST.
- 3 Passe para a guia *Visão Geral*, na qual são listadas todas as placas de rede que foram detectadas pelo sistema. Se você precisar de mais informações sobre a configuração geral da rede, consulte a Seção 20.4, “Configurando uma conexão de rede com o YaST” (p 267).
- 4 Escolha sua placa wireless na lista e clique em *Editar* para abrir a caixa de diálogo Configuração da Placa de Rede.
- 5 Configure o uso de um endereço IP estático ou dinâmico na guia *Endereço*. Geralmente a opção *Endereço Dinâmico* funciona bem.
- 6 Clique em *Avançar* para prosseguir para a caixa de diálogo *Configuração de Placa de Rede Wireless*.

Figura 17.1 YaST: configurando a placa de rede wireless

Configuração de Placa de Rede Wireless
Aqui, configure os dados mais importantes para rede wireless. [mais](#)

Configurações de dispositivo Wireless

Modo de Operação:
Gerenciado

Nome de rede (ESSID)
Verificar Rede

Modo de Autenticação:
WEP - Aberto

Tipo de Chave de Entrada
☒ Passphrase ☐ ASCII ☐ Hexadecimal

Chave de criptografia:

Configurações de especialista Chaves WEP

Ajuda Abacktar Voltar Avançar

7 Configure o modo de operação, o nome da rede (ESSID) e o modo de autenticação:

7a Escolha o *Modo de Operação*.

Uma estação pode ser integrada em uma WLAN de três modos diferentes. O modo adequado depende da rede na qual se dará a comunicação: *Ad-hoc* (rede ponto-a-ponto sem ponto de acesso), *Gerenciada* (a rede é gerenciada por um ponto de acesso) ou *Master* (sua placa de rede deve ser usada como ponto de acesso). Para usar qualquer um dos modos WPA-PSK ou WPA-EAP, o modo de funcionamento deve ser definido como *Gerenciada*.

7b Selecione um *Nome da Rede (ESSID)*.

Todas as estações em uma rede sem fio precisam do mesmo ESSID para se comunicar umas com as outras. Se nenhuma opção for especificada, a placa poderá selecionar automaticamente um ponto de acesso, que pode não ser o

desejado. Use *Explorar Rede* para obter uma lista das redes wireless disponíveis.

7c Selecione um *Modo de Autenticação*.

Selecione um método de autenticação adequado à sua rede: *Sem Criptografia* (não preferencial), *WEP - Aberto*, *WEP - Chave Compartilhada*, *WPA-EAP (WPA versão 1 ou 2)* ou *WPA-PSK (WPA versão 1 ou 2)*. Se você selecionar a autenticação WPA, um nome de rede (ESSID) deverá ser definido. Os métodos de autenticação WEP e WPA-PSK requerem a entrada de uma chave. A chave deve ser digitada como *Frase Secreta*, como uma string *ASCII* ou uma string *Hexadecimal*. Há as seguintes opções para o seu tipo de entrada de chave:

Chaves WEP

Digite a chave padrão aqui ou clique em *Chaves WEP* para entrar na caixa de diálogo de configuração avançada de chave. Defina o tamanho da chave como *128 bits* ou *64 bits*. A configuração padrão é *128 bits*. Na área de listas na parte inferior da caixa de diálogo, até quatro chaves diferentes podem ser especificadas para serem usadas pela sua estação para a criptografia. Pressione *Definir como Padrão* para definir uma delas como a chave padrão. A não ser que você mude a opção, o YaST utiliza a primeira chave informada como a chave padrão. Se a chave padrão for apagada, uma das outras chaves deverá ser marcada manualmente como a chave padrão. Clique em *Editar* para modificar as entradas de lista existentes ou criar novas chaves. Nesse caso, uma janela popup solicita que você selecione um tipo de entrada (*Frase Secreta*, *ASCII* ou *Hexadecimal*). Se você selecionar *Frase Secreta*, digite uma palavra ou string de caractere da qual uma chave é gerada de acordo com o tamanho especificado anteriormente. O ASCII exige uma entrada de 5 caracteres para uma chave de 64 bits e 13 caracteres para uma chave de 128 bits. Para a opção *Hexadecimal*, digite 10 caracteres para uma chave de 64 bits ou 26 caracteres para uma chave de 128 bits em notação hexadecimal.

WPA-PSK

Para digitar uma chave para WPA-PSK, selecione o método de entrada *Frase Secreta* ou *Hexadecimal*. No modo *Frase Secreta*, a entrada deve ser de 8 a 63 caracteres. No modo *Hexadecimal*, digite 64 caracteres.

- 7d** Se precisar configurar detalhadamente a sua conexão de WLAN, use o botão *Configurações de Especialista*. Em geral, não deve haver necessidade de mudar as configurações predefinidas. As opções disponíveis são:

Canal

A especificação de um canal no qual a estação WLAN deve funcionar é necessária somente nos modos *Ad-hoc* e *Master*. No modo *Gerenciado*, a placa pesquisa automaticamente os canais disponíveis para pontos de acesso. No modo *Ad-hoc*, selecione um dos canais oferecidos (11 a 14, dependendo do seu país) para a comunicação da sua estação com as outras estações. No modo *Master*, determine em qual canal a sua placa deve oferecer funcionalidade de ponto de acesso. A configuração padrão para esta opção é *Auto*.

Taxa de Bits

Dependendo do desempenho da sua rede, você pode definir uma determinada taxa de bits para a transmissão de um ponto para outro. Na configuração padrão *Automático*, o sistema tenta usar a taxa de transmissão de dados mais alta possível. Algumas placas WLAN não suportam a configuração da taxa de bits.

Access Point (Ponto de Acesso)

Em um ambiente com vários pontos de acesso, um deles pode ser pré-selecionado especificando-se o endereço MAC.

Utilizar o Gerenciamento de Energia

Quando você estiver em trânsito, use as tecnologias de gerenciamento de energia para maximizar o tempo de funcionamento da bateria. Mais informações sobre o gerenciamento de energia estão disponíveis no Capítulo 18, *Gerenciamento de energia* (p 225). O uso do gerenciamento de energia pode afetar a qualidade da conexão e aumentar a latência da rede.

- 8** Clique em *Avançar* e conclua com *Ok*.
- 9** Se você escolheu a autenticação WPA-EAP, será necessária mais uma etapa de configuração antes que sua estação esteja pronta para implantação na WLAN.
- 9a** Digite as credenciais fornecidas pelo seu administrador de rede. Para TLS, forneça *Identidade*, *Certificado de Cliente*, *Chave do Cliente* e *Certificado*

de Servidor. TTLS e PEAP exigem *Identidade e Senha*. As opções *Certificado de Servidor* *Identidade Anônima* são opcionais. O YaST procura qualquer certificado em `/etc/cert`. Portanto, grave os certificados concedidos a você nesse local e restrinja o acesso a esses arquivos para 0600 (leitura e gravação pelo proprietário).

- 9b** Clique em *Detalhes* para acessar a caixa de diálogo de autenticação avançada para a configuração do WPA-EAP.
- 9c** Selecione o método de autenticação para o segundo estágio da comunicação de EAP-TTLS ou EAP-PEAP. Se você selecionou TLS na caixa de diálogo anterior, escolha *any*, MD5, GTC, CHAP, PAP, MSCHAPv1 ou MSCHAPv2. Se você selecionou PEAP, escolha *any*, MD5, GTC ou MSCHAPv2. A versão PEAP pode ser usada para forçar o uso de uma determinada implementação de PEAP se a configuração determinada automaticamente não funcionar para você.

17.5.1 Estabelecendo uma rede ad-hoc

Em alguns casos, é útil conectar dois computadores equipados com uma placa WLAN. Para estabelecer uma rede ad-hoc usando o YaST, faça o seguinte:

- 1** Execute desde a Passo 1 (p 216) até a Passo 4 (p 216), conforme descrito na Seção 17.5, “Configuração com o YaST” (p 216).
- 2** Escolha *Endereço IP Atribuído Estaticamente* e digite os seguintes dados:
 - *Endereço IP*: 192.168.1.1. Mude esse endereço no segundo computador para 192.168.1.2, por exemplo.
 - *Máscara da Sub-rede*: /24
 - *Nome de Host*: escolha qualquer nome que desejar.
- 3** Continue com *Avançar*.
- 4** Configure o modo de operação, o nome da rede (ESSID) e o modo de autenticação:

- No menu popup *Modo de Operação*, escolha a entrada *Ad-hoc*.
- Escolha um *Nome da Rede (ESSID)*. Pode ser qualquer nome, mas ele precisa ser usado em todos os computadores.
- Em *Modo de Autenticação*, escolha a entrada *Sem Criptografia*.

5 Clique em *Avançar* e conclua com *Ok*.

6 Se você não tiver o `smpppd` instalado, o YaST o solicitará a fazê-lo.

17.6 Utilitários

O pacote `wireless-tools` contém utilitários que permitem definir parâmetros específicos para WLAN e obter estatísticas. Consulte http://www.hpl.hp.com/personal/Jean_Tourrilhes/Linux/Tools.html para obter mais informações.

17.7 Dicas sobre a configuração de uma WLAN

Essas dicas podem ajudar a ajustar a velocidade e a estabilidade, assim como os aspectos de segurança da sua WLAN.

17.7.1 Estabilidade e velocidade

O desempenho e a confiabilidade de uma rede wireless dependem principalmente do fato de as estações participantes receberem um sinal sem criptografia das outras estações. Obstruções como paredes podem enfraquecer grandemente o sinal. Quanto menor a força do sinal, mais lenta fica a transmissão. Durante a operação, verifique a intensidade do sinal usando o utilitário `iwconfig` na linha de comando (campo *Qualidade do Link*), o `NetworkManager` ou o `KNetworkManager`. Se tiver problemas com a qualidade do sinal, tente configurar os dispositivos em outro lugar ou ajuste a posição das antenas do seu ponto de acesso. Antenas auxiliares que melhoram substancialmente

a recepção estão disponíveis para várias placas PCMCIA WLAN. A taxa especificada pelo fabricante, como 54 MBit/s, é um valor nominal que representa o máximo teórico. Na prática, o throughput máximo de dados não passa da metade desse valor.

O prático comando `iwspy` é capaz de exibir as estatísticas da WLAN.

```
iwspy wlan0
wlan0      Statistics collected:
          00:AA:BB:CC:DD:EE : Quality:0   Signal level:0   Noise level:0
          Link/Cell/AP      : Quality:60/94 Signal level:-50 dBm  Noise level:-140
          dBm (updated)
          Typical/Reference : Quality:26/94 Signal level:-60 dBm  Noise level:-90
          dBm
```

17.7.2 Segurança

Se você desejar configurar uma rede sem fio, lembre-se de que qualquer pessoa dentro da faixa de transmissão poderá acessá-la facilmente se não forem implementadas medidas de segurança. Portanto, certifique-se de ativar o método de criptografia. Todas as placas WLAN e pontos de acesso suportam a criptografia WEP. Embora não seja completamente segura, ela representa um obstáculo para um invasor em potencial.

A criptografia WEP é normalmente adequada para uso particular. A WPA-PSK é ainda melhor, mas não é implementada em pontos de acesso ou roteadores antigos com funcionalidade WLAN. Em alguns dispositivos, o WPA pode ser implementado por meio de uma atualização de firmware. Além disso, embora o Linux suporte WPA na maioria dos componentes de hardware, alguns drivers não oferecem suporte para WPA. Se o WPA não estiver disponível, é melhor utilizar a criptografia WEP do que nenhum tipo de criptografia. Em empresas com requisitos de segurança avançados, as redes sem fio devem ser operadas somente com WPA.

Use senhas avançadas para o seu método de autenticação. Por exemplo, a página da Web <https://www.grc.com/passwords.htm> gera senhas aleatórias de 64 caracteres.

17.8 Solução de problemas

Se a sua placa WLAN não responder, verifique os seguintes pré-requisitos:

1. Você sabe o nome do dispositivo? Geralmente é wlan0. Verifique com a ferramenta ifconfig.
2. Você verificou o firmware necessário? Consulte /usr/share/doc/packages/wireless-tools/README.firmware para obter mais informações.
3. O ESSID do seu roteador é transmitido e fica visível (não oculto)?

17.8.1 Verificar seu status

O comando `iwconfig` pode fornecer informações importantes sobre a sua conexão wireless. Por exemplo, a linha a seguir exibe o ESSID, o modo wireless, a frequência, se o sinal está criptografado, a qualidade do link e muito mais:

```
iwconfig wlan0
wlan0 IEEE 802.11abg ESSID:"guest"
      Mode:Managed Frequency:5.22GHz Access Point: 00:11:22:33:44:55
      Bit Rate:54 Mb/s Tx-Power=13 dBm
      Retry min limit:7 RTS thr:off Fragment thr:off
      Encryption key:off
      Power Management:off
      Link Quality:62/92 Signal level:-48 dBm Noise level:-127 dBm
      Rx invalid nwid:0 Rx invalid crypt:0 Rx invalid frag:0
      Tx excessive retries:10 Invalid misc:0 Missed beacon:0
```

Você também pode obter as informações anteriores com o comando `iwlist`. Por exemplo, a linha a seguir exibe a taxa de bits atual:

```
iwlist wlan0 rate
wlan0      unknown bit-rate information.
          Current Bit Rate=54 Mb/s
```

Se desejar uma visão geral de quantos pontos de acesso estão disponíveis, use o comando `iwlist`. Ele mostra uma lista das “células” com a seguinte aparência:

```
iwlist wlan0 scanning
wlan0 Scan completed:
  Cell 01 - Address: 00:11:22:33:44:55
           Channel:40
           Frequency:5.2 GHz (Channel 40)
           Quality=67/70 Signal level=-43 dBm
           Encryption key: off
           ESSID:"Guest"
           Bit Rates: 6 Mb/s; 9 Mb/s; 12 Mb/s; 18 Mb/s;
                    24 Mb/s; 36 Mb/s; 48 Mb/s
           Mode: Master
```

```
Extra:tsf=0000111122223333
Extra: Last beacon: 179ms ago
IE: Unknown: ...
```

17.8.2 Vários dispositivos de rede

Laptops modernos geralmente têm uma placa de rede e uma placa WLAN. Se você configurar ambos os dispositivos com DHCP (atribuição de endereço automática), poderá encontrar problemas com a resolução de nome e o gateway padrão. Isso fica evidente quando você pode efetuar ping no roteador, mas não pode navegar na Internet. O Banco de Dados de Suporte no endereço http://en.opensuse.org/SDB:Name_Resolution_Does_Not_Work_with_Several_Concurrent_DHCP_Clients apresenta um artigo sobre o assunto.

17.8.3 Problemas com placas Prism2

Vários drivers estão disponíveis para dispositivos com chips Prism2. As várias placas funcionam mais ou menos adequadamente com os vários drivers. Com essas placas, a criptografia WPA somente pode ser usada com o driver hostap. Se tal placa não funcionar adequadamente ou não funcionar ou se você desejar usar a criptografia WPA, leia `/usr/share/doc/packages/wireless-tools/README.prism2`.

17.9 Para obter mais informações

Mais informações encontram-se nas seguintes páginas:

1. http://www.hpl.hp.com/personal/Jean_Tourrilhes/Linux/Wireless.html — As páginas da Internet de Jean Tourrilhes, que desenvolveu as *Ferramentas Wireless* para o Linux, apresentam uma variedade de informações úteis sobre redes wireless.
2. tuxmobil.org — Informações úteis e práticas sobre computadores móveis sob o Linux.
3. <http://www.linux-on-laptops.com> — Mais informações sobre o Linux em laptops.

Gerenciamento de energia

O gerenciamento de energia é especialmente importante em laptops, mas também é útil em outros sistemas. A ACPI (advanced configuration and power interface - interface de energia e configuração avançada) está disponível em todos os computadores modernos (laptops, desktops e servidores). As tecnologias de gerenciamento de energia exigem hardware adequado e rotinas BIOS. A maioria dos laptops e muitos desktops e servidores modernos atendem a esses requisitos. Também é possível controlar a escala de frequência de CPU para economizar energia ou reduzir o ruído.

18.1 Funções de economia de energia

As funções de economia de energia não são significativas apenas para o uso móvel de laptops, como também para sistemas desktop. As funções principais e respectivas utilizações na ACPI são:

Standby

não suportado.

Suspend (para memória)

Este modo grava todo o estado do sistema na memória RAM. Em seguida, todo o sistema é colocado em repouso, salvo a memória RAM. Neste estado, o computador consome pouquíssima energia. A vantagem desse estado é a possibilidade de reiniciar o trabalho no mesmo ponto em alguns segundos sem precisar inicializar e reiniciar os aplicativos. Esta função corresponde ao estado S3 de ACPI. O suporte desse estado ainda está em desenvolvimento e, portanto, depende muito do hardware.

Suspend (para o disco)

Neste modo operacional, o estado do sistema inteiro é gravado no disco rígido e o sistema é desligado. Deve existir uma partição de troca pelo menos tão grande quanto a RAM para gravar todos os dados ativos. A reativação desse estado leva de 30 a 90 segundos. O estado anterior ao suspenso é restaurado. Alguns fabricantes oferecem variantes híbridas desse modo, como RediSafe em Thinkpads da IBM. O estado correspondente da ACPI é S4. No Linux, a suspensão para disco é desempenhada pelas rotinas de kernel, que são independentes de ACPI.

Monitor de bateria

A ACPI verifica o status da carga da bateria e fornece informações correspondentes. Além disso, ela coordena as ações a serem desempenhadas quando um status de carga crítico é atingido.

Desligamento automático

Após um encerramento, o computador é desligado. Isto é especialmente importante quando um encerramento automático é realizado pouco antes da bateria esgotar-se.

Controle de velocidade do processador

Em conexão com a CPU, é possível economizar energia de três maneiras diferentes: escala de frequência e voltagem (também conhecida como PowerNow! ou Speedstep), throttling e colocação do processador em repouso (estados C). Dependendo do modo operacional do computador, esses métodos também podem ser combinados.

18.2 ACPI

A ACPI (Interface de Energia e Configuração Avançada) foi projetada para habilitar o sistema operacional a configurar e controlar os componentes individuais do hardware. A ACPI substitui PnP e APM. Ela envia informações sobre a bateria, o adaptador de CA, a temperatura, o ventilador e eventos do sistema, como “fechar tampa” ou “bateria fraca”.

O BIOS fornece tabelas que contém informações sobre os componentes individuais e métodos de acesso ao hardware. O sistema operacional usa essas informações para tarefas como atribuir interrupções ou ativar e desativar componentes. Como o sistema operacional executa comandos armazenados no BIOS, a funcionalidade depende da implementação do BIOS. As tabelas que a ACPI podem detectar e carregar são

reportadas em `/var/log/boot.msg`. Consulte a Seção 18.2.3, “Solução de problemas” (p 229) para obter mais informações sobre solução de problemas da ACPI.

18.2.1 Controlando o desempenho da CPU

A CPU pode economizar energia de três maneiras. Dependendo do modo operacional do computador, estes métodos também podem ser combinados. Economizar energia também significa que o sistema esquentará menos e os ventiladores são ativados com menos frequência.

Escala de frequência e voltagem

PowerNow! e Speedstep são as designações usadas pela AMD e pela Intel para esta tecnologia. No entanto, essa tecnologia também é aplicada em processadores de outros fabricantes. A frequência do relógio da CPU e sua voltagem básica são reduzidas ao mesmo tempo, resultando em economias de energia mais do que lineares. Isso significa que quando a frequência for reduzida pela metade (meio desempenho), muito menos que metade da energia é consumida. Essa tecnologia é independente de ACPI. Há dois métodos principais para desempenhar a escala de frequência da CPU: pelo próprio kernel ou por um aplicativo de espaço de usuário. Portanto, há diferentes reguladores de kernel que podem ser definidos abaixo de `/sys/devices/system/cpu/cpu*/cpufreq/`.

regulador de espaço de usuário

Se o regulador de espaço de usuário estiver definido, o kernel passa o controle da escala de frequência de CPU para um aplicativo de espaço de usuário, geralmente um daemon. Em distribuições do SUSE Linux Enterprise Desktop, esse daemon é o pacote `powersaved`. Quando essa implementação é usada, a frequência de CPU é ajustada em relação à carga do sistema atual. Por padrão, uma das implementações de kernel é usada. Porém, em alguns hardwares ou em relação a drivers ou processadores específicos, a implementação do espaço de usuário ainda é a única solução que funciona.

regulador em demanda

Esta é a implementação de kernel de uma política de frequência de CPU dinâmica e deve funcionar na maioria dos sistemas. Assim que houver uma carga alta de sistema, a frequência de CPU é imediatamente aumentada. Ela é reduzida em uma carga de sistema baixa.

regulador conservador

Esse regulador é semelhante à implementação em demanda, só que usa uma política mais conservadora. A carga do sistema deve ser alta por um tempo específico antes que a frequência do CPU seja aumentada.

regulador de economia de energia

A frequência de cpu é definida estaticamente para o mais baixo possível.

regulador de desempenho

A frequência de cpu é definida estaticamente para o mais alto possível.

Throttling da frequência do relógio

Esta tecnologia omite uma determinada porcentagem dos impulsos de sinal do relógio para a CPU. Com throttling a 25%, todo quarto impulso é omitido. A 87,5%, apenas cada oitavo impulso chega ao processador. No entanto, as economias de energia são pouco menos que lineares. Normalmente, o throttling só é usado se a escala da frequência não estiver disponível ou para maximizar as economias de energia. Essa tecnologia deve também ser controlada por um processo especial. A interface do sistema é `/proc/acpi/processor/*/throttling`.

Colocando o processador em repouso

O sistema operacional coloca o processador em repouso sempre que há inatividade. Nesse caso, o sistema operacional envia um comando `halt` à CPU. Existem três estados: C1, C2 e C3. No estado mais econômico, C3, até a sincronização do cache do processador com a memória principal é interrompida. Portanto, esse estado só pode ser aplicado se nenhum dispositivo modificar o conteúdo da memória principal por meio de atividade do barramento mestre. Alguns drivers impedem o uso de C3. O estado atual é exibido em `/proc/acpi/processor/*/power`.

A escala e o throttling da frequência só são relevantes se o processador estiver ocupado, porque o estado C mais econômico é aplicado sempre que o processador está inativo. Se a CPU estiver ocupada, a escala da frequência é o método recomendado para economia de energia. Em geral o processador só trabalha com carga parcial. Neste caso, pode ser executado com uma frequência inferior. Normalmente, a escala de frequência dinâmica controlada pelo regulador em demanda do kernel ou por um daemon, como `powersaved`, é o melhor método. Uma configuração estática em baixa frequência é útil para o funcionamento com bateria ou se você desejar que o computador permaneça frio ou silencioso.

Throttling deve ser usado como última alternativa, por exemplo, para ampliar o tempo de operação da bateria, apesar de uma alta carga do sistema. Contudo, alguns sistemas não são executados suavemente quando ocorrem throttlings em excesso. Ademais, o throttling da CPU não faz sentido se a CPU tem pouco a fazer.

18.2.2 Ferramentas da ACPI

A gama de utilitários mais ou menos abrangentes da ACPI inclui ferramentas que apenas exibem informações, como o nível de carga e a temperatura da bateria (`acpi`, `klaptopdaemon` etc.), ferramentas que facilitam o acesso às estruturas de `/proc/acpi` ou que auxiliam no monitoramento das mudanças (`akpi`, `acpiw`, `gtkacpiw`), e ferramentas para edição das tabelas da ACPI no BIOS (pacote `pmtools`).

18.2.3 Solução de problemas

Há dois tipos de problemas. De um lado, o código ACPI do kernel pode conter erros que não foram detectados em tempo útil. Neste caso, uma solução estará disponível para download. O mais comum é que os problemas sejam causados pelo BIOS. Às vezes, desvios da especificação da ACPI são propositalmente integrados ao BIOS para contornar erros na implementação da ACPI em outros sistemas operacionais amplamente utilizados. Componentes de hardware que têm erros sérios na implementação da ACPI são gravados em uma lista negra que impede que o kernel do Linux use a ACPI para esses componentes.

A primeira ação a ser tomada quando problemas forem detectados, é atualizar o BIOS. Se o computador não inicializar de jeito nenhum, um dos seguintes parâmetros de boot poderá ser útil:

`pci=noacpi`

Não use ACPI para configurar os dispositivos PCI.

`acpi=ht`

Realize apenas uma configuração com recursos simples. Não use a ACPI para outros fins.

`acpi=off`

Desabilitar a ACPI.

ATENÇÃO: problemas de boot sem ACPI

Algumas máquinas mais novas (especialmente os sistemas SMP e AMD64) precisam de ACPI para configurar o hardware corretamente. Nestas máquinas, desabilitar a ACPI pode causar problemas.

Às vezes a máquina é confundida pelo hardware conectado por USB ou FireWire. Se uma máquina se recusa a inicializar, desconecte todos os itens de hardware desnecessários e tente novamente.

Monitore as mensagens de boot do sistema com o comando `dmesg | grep -2i acpi` (ou todas as mensagens, porque o problema pode não ser causado pela ACPI) após o boot. Se ocorrer algum erro durante a análise de uma tabela ACPI, a tabela mais importante — a DSDT (*Differentiated System Description Table* - tabela de descrição diferenciada do sistema) — poderá ser substituída por uma versão aprimorada. Neste caso, a DSDT defeituosa do BIOS é ignorada. O procedimento está descrito em Seção 18.4, “Solução de problemas” (p 233).

Na configuração do kernel, há um switch para ativar as mensagens de depuração da ACPI. Se um kernel com depuração da ACPI for compilado e instalado, os técnicos que procuram o erro podem ser auxiliados com informações detalhadas.

Se você tiver problemas com BIOS ou hardware, é sempre recomendável entrar em contato com os fabricantes. Especialmente se eles nem sempre derem assistência ao Linux, devem ser indagados em caso de problemas. Os fabricantes só levarão a questão a sério se compreenderem que um número satisfatório de seus clientes usa Linux.

Para obter mais informações

- <http://tldp.org/HOWTO/ACPI-HOWTO/> (ACPI HOWTO detalhado, contém patches DSDT)
- <http://www.intel.com/technology/iapc/acpi/index.htm> (Advanced Configuration & Power Interface - Interface de Energia e Configuração Avançada)
- <http://www.lesswatts.org/projects/acpi/> (O projeto ACPI4Linux em Sourceforge)

- <http://acpi.sourceforge.net/dsdt/index.php> (patches DSDT por Bruno Ducrot)

18.3 Descanso do disco rígido

No Linux, o disco rígido pode colocado em repouso total se não estiver em uso e pode ser executado em modo mais econômico ou silencioso. Nos laptops modernos, não é necessário desativar o disco rígido manualmente, porque entram automaticamente em um modo operacional econômico sempre que não estão em uso. Contudo, se quiser maximizar a economia de energia, teste um dos seguintes métodos.

O comando `hdparm` pode ser usado para modificar várias configurações de disco rígido. A opção `-y` alterna instantaneamente o disco rígido para o modo standby. `-Y` coloca-o em repouso. `hdparm -S x` faz o disco rígido ser encerrado após um determinado período de inatividade. Substitua `x` conforme a seguir: 0 desabilita esse mecanismo, fazendo o disco rígido funcionar continuamente. Valores de 1 a 240 são multiplicados por 5 segundos. Valores de 241 a 251 correspondem de 1 a 11 vezes 30 minutos.

As opções de economia de energia interna do disco rígido podem ser controladas pela opção `-B`. Selecione um valor de 0 a 255 para obter de economia máxima a throughput máximo. O resultado depende do disco rígido usado e é difícil de avaliar. Para tornar um disco rígido mais silencioso, use a opção `-M`. Selecione um valor de 128 a 254 para obter de silencioso a rápido.

Muitas vezes não é fácil colocar o disco rígido em repouso. No Linux, vários processos gravam no disco rígido, ativando-o repetidamente. Portanto, é importante entender como o Linux trata os dados que necessitam ser gravados no disco rígido. Primeiro, todos os dados estão no buffer da memória RAM. Esse buffer é monitorado pelo daemon `pdflush`. Quando os dados atingem uma determinada idade limite ou quando o buffer está cheio até certo grau, o conteúdo do buffer é descarregado para o disco rígido. O tamanho do buffer é dinâmico e depende do tamanho da memória e da carga do sistema. Por padrão, `pdflush` é configurado em intervalos curtos para obter a integridade máxima de dados. Ele verifica o buffer a cada 5 segundos e grava os dados no disco rígido. As seguintes variáveis são interessantes:

`/proc/sys/vm/dirty_writeback_centisecs`

Contém o atraso até que um thread `pdflush` seja acionado (em centésimos de segundo).

`/proc/sys/vm/dirty_expire_centisecs`

Define o período após o qual uma página modificada deve ser gravada por último. O padrão é 3000, ou seja, 30 segundos.

`/proc/sys/vm/dirty_background_ratio`

Porcentagem máxima de páginas modificadas para `pdflush` começar a gravá-las. O padrão é 5%.

`/proc/sys/vm/dirty_ratio`

Quando a página modificada exceder essa porcentagem da memória total, os processos são forçados a gravar buffers modificados durante suas frações de tempo em vez de continuar gravando.

ATENÇÃO: deficiência da integridade de dados

Mudanças nas configurações do daemon `pdflush` arriscam a integridade dos dados.

Além desses processos, os sistemas de arquivo de registro em diário, como ReiserFS e Ext3, gravam seus metadados independentemente de `pdflush`, que também impede que o disco rígido seja encerrado. Para evitar isso, foi desenvolvida uma extensão especial de kernel para dispositivos móveis. Consulte `/usr/src/linux/Documentation/laptop-mode.txt` para obter detalhes.

Outro fator importante é o modo como se comportam os programas ativos. Por exemplo, os bons editores gravam regularmente backups ocultos do arquivo modificado no momento para o disco rígido, fazendo com que ele saia do modo de hibernação. Recursos como este podem ser desabilitados às custas da integridade dos dados.

Com relação a isso, o mail daemon postfix faz uso da variável `POSTFIX_LAPTOP`. Se essa variável for configurada para `sim`, postfix acessa o disco rígido com muito menos frequência.

No SUSE Linux Enterprise Desktop, essas tecnologias são controladas por `laptop-mode-tools`.

18.4 Solução de problemas

Todas as mensagens de erro e alertas são registradas no arquivo `/var/log/messages`. Se não conseguir encontrar as informações necessárias, aumente o detalhamento das mensagens de economia de energia usando `DEBUG` no arquivo `/etc/sysconfig/powersave/common`. Aumente o valor da variável para 7 ou mesmo 15 e reinicie o daemon. As mensagens de erro mais detalhadas em `/var/log/messages` devem ajudá-lo a localizar o erro. As seções a seguir explicam os problemas mais comuns do powersave e os diferentes tipos de modos adormecidos.

18.4.1 ACPI ativada com suporte de hardware, mas funções não funcionam

Se você tiver problemas com a ACPI, use o comando `dmesg|grep -i acpi` para pesquisar a saída de `dmesg` para mensagens específicas à ACPI. Poderá ser necessário atualizar o BIOS para solucionar o problema. Na home page do fabricante do seu laptop, procure uma versão atualizada do BIOS e instale-a. Peça ao fabricante para estar em conformidade com a última especificação da ACPI. Se os erros persistirem após a atualização do BIOS, faça o seguinte para substituir a tabela DSDT defeituosa no seu BIOS com um DSDT atualizado:

- 1 Faça o download do DSDT para o seu sistema em <http://acpi.sourceforge.net/dsdt/index.php>. Verifique se o arquivo está descompactado e compilado como mostra a extensão de arquivo `.aml` (linguagem computacional ACPI). Se for o caso, continue com a etapa 3.
- 2 Se a extensão de arquivo da tabela do download for `.asl` (linguagem fonte ACPI), compile-a com `iasl` (pacote `pmttools`). Digite o comando `iasl -sa file.asl`.
- 3 Copie o arquivo `DSDT.aml` para qualquer localização (`/etc/DSDT.aml` é recomendada). Edite `/etc/sysconfig/kernel` e adapte o caminho para o arquivo DSDT de forma compatível. Inicie `mkinitrd` (pacote `mkinitrd`).

Sempre que você instala o kernel e usar `mkinitrd` para criar um `initrd`, o DSDT modificado é integrado e carregado quando o sistema é inicializado.

18.4.2 A frequência da CPU não funciona

Consulte as fontes de kernel (`kernel-source`) para ver se o seu processador é suportado. Você poderá precisar de um módulo de kernel ou de opção especial para ativar o controle de frequência da CPU. Essas informações estão disponíveis em `/usr/src/linux/Documentation/cpu-freq/`.

18.4.3 Suspend e Standby não funcionam

Os sistemas ACPI podem ter problemas com `suspend` e `standby` devido a falha na implementação de DSDT (BIOS). Se esse for o seu caso, atualize o BIOS.

Quando o sistema tenta descarregar módulos defeituosos, o sistema é verificado ou o evento suspenso não é acionado. O mesmo também pode acontecer se você não descarregar módulos ou interromper serviços que impeçam uma suspensão bem-sucedida. Em ambos os casos, tente identificar o módulo defeituoso que impediu o modo adormecido. O arquivo de registro `/var/log/pm-suspend.log` contém informações detalhadas sobre o que está ocorrendo e onde estão os erros possíveis. Modifique a variável `SUSPEND_MODULES` em `/usr/lib/pm-utils/defaults` para descarregar os módulos com problema antes de efetuar suspensão ou `standby`.

Consulte <http://en.opensuse.org/Pm-utils> e <http://en.opensuse.org/S2ram> para obter informações mais detalhadas sobre como modificar o processo de suspensão e continuação.

18.5 Para obter mais informações

- <http://en.opensuse.org/S2ram> — Como colocar o recurso `suspend` para RAM funcionando
- <http://en.opensuse.org/Pm-utils> — Como modificar a metodologia geral de suspensão

Usando Tablet PCs

O SUSE® Linux Enterprise Desktop vem com suporte para Tablet PCs. A seguir, você aprenderá a instalar e configurar seu Tablet PC e descobrirá alguns aplicativos do Linux* úteis que aceitam entrada de canetas digitais.

Os seguintes Tablet PCs são suportados:

- Tablet PCs com dispositivos Wacom seriais, como ACER TM série C30x, Fujitsu Lifebook série T (T30xx/T40xx/T50xx), Gateway C-140X/E-295C, HP Compaq TC1100/TC4200/TC4400, 2710p/2730p, IBM/Lenovo X41t/X61t, LG LT20, Motion M1200/M1400, OQO 02, Panasonic Toughbook CF-18, Toshiba Portégé/Tecra série M e Satellite R15/R20.
- Tablet PCs com dispositivos Wacom USBP, como ASUS R1E/R1F, Gateway C-120X/E-155C e HP Pavilion série tx2000/tx2100/tx2500.
- Tablet PCs com dispositivos FinePoint, como Gateway C210X/M280E/CX2724 e HP Compaq TC1000.
- Tablet PCs com dispositivos de tela sensível ao toque, como Asus R2H, Clevo TN120R, Fujitsu Siemens Computers série P, LG C1 e Samsung Q1/Q1-Ultra.

Depois que você instalar os pacotes do Tablet PC e configurar seu digitalizador corretamente, a entrada com a caneta (também chamada de stylus) poderá ser usada para as seguintes ações e aplicativos:

- Efetuar login no KDM ou GDM
- Desbloquear sua tela nas áreas de trabalho KDE e GNOME
- Ações que também pode ser acionadas por outros dispositivos apontadores (como mouse ou touch pad), por exemplo, mover o cursor na tela, iniciar aplicativos, fechar, redimensionar e mover janelas, deslocar o foco da janela, e arrastar e soltar objetos
- Usar o reconhecimento de gestos nos aplicativos do X Window System
- Desenhar com o GIMP
- Fazer anotações ou criar esboços com aplicativos como o Jarnal ou o Xournal ou editar quantidades maiores de texto com o Dasher

NOTA: teclado ou mouse necessário para a instalação

Durante a instalação do SUSE Linux Enterprise Desktop, a caneta não pode ser usada como um dispositivo de entrada. Se o seu Tablet PC não possui um teclado ou touch pad embutido, conecte um teclado ou mouse externo ao Tablet PC para a instalação de seu sistema.

19.1 Instalando pacotes do Tablet PC

Os pacotes necessários para os Tablet PCs estão inclusos no padrão de instalação TabletPC. Se ele foi selecionado durante a instalação, os seguintes pacotes já deverão estar instalados no seu sistema:

- `cellwriter`: um painel de entrada de escrita à mão com base em caracteres
- `jarnal`: um aplicativo baseado em Java para anotações
- `wacom-kmp(-default)`: o driver do kernel para Tablet PCs com dispositivos Wacom USB

- `xournal`: um aplicativo para anotações e esboços
- `xstroke`: um programa de reconhecimento de gestos para o X Window System
- `xvkbd`: um teclado virtual para o X Window System
- `x11-input-fujitsu`: o módulo de entrada X para tablets Fujitsu série P
- `x11-input-evtouch`: o módulo de entrada X para alguns Tablet PCs com telas sensíveis ao toque
- `x11-input-wacom`: o módulo de entrada X para tablets Wacom
- `x11-input-wacom-tools`: configuração, diagnósticos e bibliotecas para tablets Wacom

Se esses pacotes não estiverem instalados, instale manualmente os pacotes necessários da linha de comando ou selecione o padrão `TabletPC` para instalação no YaST.

19.2 Configurando seu dispositivo tablet

Você pode configurar seu Tablet PC (não inclui Tablet PCs com telas sensíveis ao toque) durante o processo de instalação na tela *Configuração de Hardware*, mudando as opções de *Placa Gráfica*. Outra opção é configurar o dispositivo tablet (interno ou externo) a qualquer momento após a instalação.

1 Inicie o `SaX2` da linha de comando ou pressionando `Alt + F2` e digitando `sax2`.

2 Se você usa um dispositivo com Wacom ou Finepoint, clique em *Mesa Digitalizadora* para mostrar as *Propriedades da Mesa Digitalizadora*.

Se você usa um Tablet PC com tela sensível ao toque, clique em *Tela Sensível ao Toque*.

3 Na lista à direita, selecione *TABLET PCs* como fornecedor e o nome do seu tablet, e marque *Ativar esta Mesa Digitalizadora*.

Se sua máquina não estiver listada e você tiver certeza de que tem um dispositivo com Wacom, selecione *Tablet PC ISDV4 Wacom (SERIAL)* ou *Tablet PC ISDV4 Wacom (USB)*.

- 4 Alterne para a guia *Canetas Eletrônicas* e verifique se as seguintes opções estão ativadas: *Adicionar Caneta* e *Adicionar Borracha*. Se você tiver um Tablet PC com tela sensível ao toque, ative também *Adicionar Tela Sensível ao Toque*.
- 5 Clique em *OK* para gravar as mudanças.

Após concluir a configuração do X Window System, reinicie seu servidor X efetuando logout. Você pode também sair da interface de usuário e executar `init 3 && init 5` em um console virtual.

Após seu dispositivo tablet ser configurado, agora você usar a caneta (ou, dependendo do seu Tablet PC, o dedo) como dispositivo de entrada.

19.3 Usando o teclado virtual

Para efetuar login na área de trabalho KDE ou GNOME ou desbloquear a tela, você pode digitar seu nome de usuário e senha da maneira normal ou por meio do teclado virtual (xvkbd), exibido abaixo do campo de login. Para configurar o teclado ou acessar a ajuda integrada, clique no campo *xvkbd* no canto inferior esquerdo para abrir o menu principal do xvkbd.

Se sua entrada não estiver visível (ou não for transferida para a janela onde necessário), redirecione o foco clicando na tecla *Foco* no xvkbd e clicando na janela que deve receber os eventos do teclado.

Figura 19.1 Teclado virtual xvkbd

F1	F2	F3	F4	F5	F6	F7	F8	F9	F10	F11	F12	Backspace	xvkbd (v3.0)									
Esc	!	@	#	\$	%	^	&	*	()	-	+		~	Num Lock	/	*	Focus				
Tab	Q	W	E	R	T	Y	U	I	O	P	{	}	Del	7	Home	8	Up	9	PgUp	+		
Control	A	S	D	F	G	H	J	K	L	:	"	'	Return	4	Left	5	6	Right	-			
Shift	Z	X	C	V	B	N	M	<	>	?	,	.	/	Com pose	Shift	1	End	2	Down	3	PgDn	Enter
xvkbd	Caps Lock	Alt	Meta				Meta	Alt	←	→	↑	↓	Focus	0	Ins	.	Del					

Se você quiser usar o `xvkbd` após o login, inicie-o por meio do menu principal ou com `xvkbd` de um shell.

19.4 Girando a tela

Use o `KRandRTray` (KDE) ou o `gnome-display-properties` (GNOME) para girar ou redimensionar sua tela de forma manual e simultânea. Tanto o `KRandRTray` quanto o `gnome-display-properties` são applets para a extensão RANDR do servidor X.

Inicie o `KRandRTray` ou o `gnome-display-properties` do menu principal ou digite `krandrtray` ou `gnome-display-properties` para iniciar o applet de um shell. Após iniciar o applet, seu ícone geralmente é adicionado à sua bandeja do sistema. Se o ícone do `gnome-display-properties` não aparecer automaticamente na bandeja do sistema, verifique se *Mostrar Telas no Painel* está ativado na caixa de diálogo *Configurações de Resolução do Monitor*.

Para girar sua tela com o `KRandRTray`, clique o botão direito do mouse no ícone e selecione *Configurar Tela*. Selecione a orientação desejada na caixa de diálogo de configuração.

Para girar a tela com `gnome-display-properties`, clique o botão direito do mouse no ícone e selecione a orientação desejada. A tela é inclinada imediatamente na nova direção. A orientação do tablet de gráficos também muda, para que ainda possa interpretar o movimento da caneta corretamente.

Se tiver problemas ao mudar a orientação da sua área de trabalho, consulte a Seção 19.7, “Solução de problemas” (p 244) para obter mais informações.

Para obter mais informações sobre os applets específicos da área de trabalho da extensão RANDR, consulte a Seção “Monitor Settings” (Capítulo 3, *Customizing Your Settings*, ↑*KDE User Guide*) e a Seção “Configurando telas” (Capítulo 3, *Personalizando suas configurações*, ↑*Guia do Usuário do GNOME*).

19.5 Usando o reconhecimento de gestos

O SUSE Linux Enterprise Desktop inclui o CellWriter e o xstroke para reconhecimento de gestos. Ambos os aplicativos aceitam gestos executados com a caneta ou outros dispositivos apontadores como entrada para os aplicativos no X Window System.

19.5.1 Usando o CellWriter

Com o CellWriter, você pode escrever caracteres em uma grade de células. A escrita é reconhecida instantaneamente a cada caractere. Após terminar de escrever, você pode enviar a entrada para o aplicativo em foco no momento. Antes de se poder usar o CellWriter para reconhecimento de gestos, o aplicativo precisa ser treinado para reconhecer sua caligrafia: você precisa treinar cada caractere de um determinado mapa de teclas (caracteres não treinados não são ativados e, portanto, não podem ser usados).

Procedimento 19.1 *Treinando o CellWriter*

- 1 Inicie o CellWriter no menu principal ou com `cellwriter` na linha de comando. Na primeira inicialização, o CellWriter entra automaticamente em modo de treino. No modo de treino, mostra um conjunto de caracteres do mapa de teclas escolhido no momento.
- 2 Insira o gesto que gostaria de usar para um caractere em sua respectiva célula. Com a primeira entrada, o plano de fundo muda a cor para branco, enquanto o caractere em si é mostrado em cinza claro. Repita o gesto várias vezes até a cor do caractere mudar para preto. Caracteres não treinados são mostrados sobre fundo cinza claro ou marrom (dependendo do esquema de cores da área de trabalho).
- 3 Repita essa etapa até ter treinado o CellWriter para todos os caracteres de que você precisa.
- 4 Se desejar treinar o CellWriter para outro idioma, clique no botão *Configuração* e selecione um idioma da guia *Idiomas*. *Feche* a caixa de diálogo de configuração. Clique no botão *Treinar* e selecione o mapa de teclas na caixa suspensa no canto

inferior direito da janela do *CellWriter*. Agora repita seu treino para o novo mapa de teclas.

- 5 Após terminar o treino para o mapa de teclas, clique no botão *Treinar* para alternar para o modo normal.

No modo normal, a janela do *CellWriter* mostra algumas células vazias nas quais inserir os gestos. Os caracteres não são enviados a outro aplicativo até você clicar no botão *Inserir*, para que possa corrigir ou apagar caracteres antes de usá-los como entrada. Os caracteres que tiverem sido reconhecidos com baixo grau de confiança aparecerão realçados. Para corrigir sua entrada, use o menu de contexto que aparece ao se clicar com o botão direito do mouse em uma célula. Para apagar um caractere, use a borracha da sua caneta ou clique no meio com o mouse para limpar a célula. Após terminar sua entrada no *CellWriter*, defina qual aplicativo deve recebê-la clicando na janela desse aplicativo. Em seguida, envie a entrada para o aplicativo clicando em *Inserir*.

Figura 19.2 Reconhecimento de gestos com o *CellWriter*



Ao clicar no botão *Teclas* do *CellWriter*, você obtém um teclado virtual que pode ser usado em vez do reconhecimento de caligrafia.

Para ocultar o *CellWriter*, feche sua janela. O aplicativo agora aparece como um ícone na bandeja do sistema. Para mostrar a janela de entrada novamente, clique no ícone da bandeja do sistema.

19.5.2 Usando o Xstroke

Com o xstroke, você pode usar gestos com sua caneta ou outros dispositivos apontadores como entrada para aplicativos no X Window System. O alfabeto do xstroke é um alfabeto de traço único semelhante ao alfabeto Graffiti*. Quando ativado, o xstroke envia a entrada à janela atualmente focalizada.

- 1 Inicie o KRandRTray por meio do menu principal ou com `xstroke` em um shell. Isso adiciona um ícone de lápis à bandeja do sistema.
- 2 Inicie o aplicativo para o qual você deseja criar a entrada de texto com a caneta (por exemplo, uma janela de terminal, um editor de texto ou o Writer do OpenOffice.org).
- 3 Para ativar o modo de reconhecimento de gestos, clique no ícone de lápis uma vez.
- 4 Execute alguns gestos no tablet de gráficos com a caneta ou outro dispositivo apontador. O `xstroke` captura os gestos e transfere-os para o texto que é exibido na janela do aplicativo focalizado.
- 5 Para alternar o foco para uma janela diferente, clique na janela desejada com a caneta e mantenha o botão do mouse pressionado por um momento (ou use o atalho do teclado definido no centro de controle de sua área de trabalho).
- 6 Para desativar o modo de reconhecimento de gestos, clique no ícone de lápis novamente.

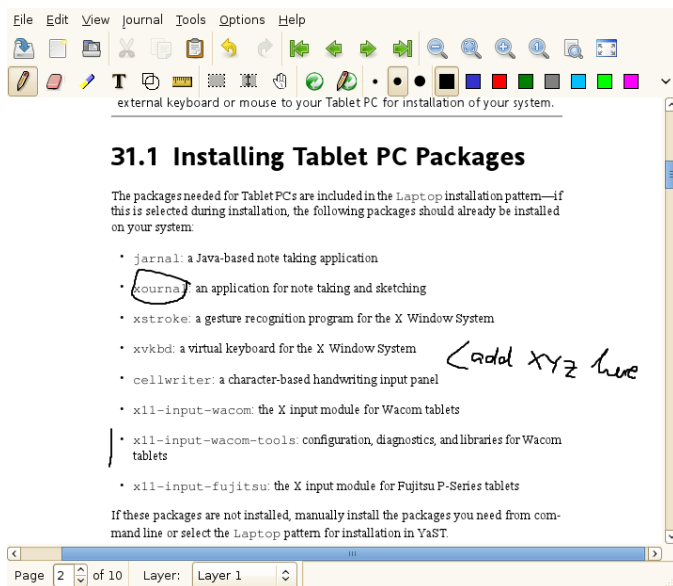
19.6 Fazendo anotações e criando esboços com a caneta

Para criar desenhos com a caneta, você pode usar um editor gráfico profissional como o GIMP ou experimentar um dos aplicativos para fazer anotações: Xournal ou Jarnal. Com o Xournal e o Jarnal, você pode fazer anotações, criar desenhos ou inserir comentários em arquivos PDF com a caneta. Como um aplicativo baseado em Java disponível para diversas plataformas, o Jarnal também oferece recursos básicos de colaboração. Para obter maiores informações, consulte <http://www.dklevine.com/general/software/tc1000/jarnal-net.htm>. Ao gravar seu conteúdo, o Jarnal armazena os dados em um formato de arquivo (*.jaj) que também contém um arquivo no formato SVG.

Inicie o Jarnal ou Xournal por meio do menu principal ou digitando `jarnal` ou `xournal` em um shell. Para inserir comentários em um arquivo PDF no Xournal, por exemplo, selecione *File (Arquivo) > Annotate PDF* (Anotar PDF) e abra o arquivo PDF

em seu sistema de arquivos. Use a caneta ou outro dispositivo apontador para fazer anotações no PDF e gravar suas mudanças com *Arquivo > Imprimir em PDF*.

Figura 19.3 Fazendo anotações em um PDF com o Xournal



O Dasher é outro aplicativo útil. Foi projetado para situações em que a entrada pelo teclado não é prática ou não está disponível. Com algum treinamento, você pode digitar rapidamente quantidades maiores de texto usando somente a caneta (ou outros dispositivos de entrada — é possível até usar um gerenciador de visão).

Inicie o Dasher por meio do menu principal ou com `dasher` em um shell. Mova sua caneta em uma direção e o aplicativo começará a ampliar as letras no lado direito. Com as letras que passam pelo meio do cursor de linha cruzada, o texto é criado ou previsto e é impresso na parte superior da janela. Para começar ou parar de escrever, clique na tela uma vez com a caneta. Modifique a velocidade de zoom na parte inferior da janela.

The screenshot shows the 'Hello World' application with a complex graphical representation of the text. The text 'Hello World' is displayed in large, bold, black letters. The letters are overlaid with a series of overlapping, semi-transparent colored rectangles (green, blue, yellow) that create a layered effect. A red line points to a specific area of the text. Below the main text, the phrase 'my name is' is visible in a smaller font, also overlaid with similar colored rectangles. The application's interface includes a menu bar at the top with 'Arquivo', 'Editar', and 'Ajuda'. A toolbar below the menu bar contains icons for file operations (new, open, save, print, delete, copy, paste, undo, redo) and a help icon. The status bar at the bottom shows 'Velocidade: 1.0' and 'Alfabeto:'. The text 'Hello World' is displayed in the main window area.

19.7 Solução de problemas

Ocasionalmente, o teclado virtual não é exibido na tela de login. Para resolver isso, reinicie o servidor X pressionando Ctrl + Alt + <— ou pressione a tecla apropriada em seu Tablet PC (se você usar um modelo plano sem teclado integrado). Se o teclado virtual ainda não for exibido, conecte um teclado externo a seu modelo plano e efetue logon usando o teclado do hardware.

A orientação dos tablets de gráficos com Wacom não muda

Com o comando `xrandr`, você pode mudar a orientação de sua tela por meio de um shell. Digite `xrandr --help` para ver as opções disponíveis. Para mudar simultaneamente a orientação de seu tablet de gráficos, o comando precisa ser modificado conforme descrito abaixo:

- Para a orientação normal (rotação de 0°):

```
xrandr --output LVDS ---rotate normal && xsetwacom set "Mouse[7]" Rotate NONE
```

- Para a rotação de 90° (no sentido horário, retrato):

```
xrandr --output LVDS ---rotate right && xsetwacom set "Mouse[7]" Rotate CW
```

- Para a rotação de 180° (paisagem):

```
xrandr --output LVDS --rotate inverted && xsetwacom set "Mouse[7]" Rotate HALF
```

- Para a rotação de 270° (no sentido anti-horário, retrato):

```
xrandr --output LVDS --rotate left && xsetwacom set "Mouse[7]" Rotate CCW
```

Observe que os comandos acima dependem do conteúdo de seu arquivo de configuração `/etc/X11/xorg.conf`. Se você configurou seu dispositivo com o SaX2 conforme descrito na Seção 19.2, “Configurando seu dispositivo tablet” (p 237), os comandos devem funcionar da forma como estão escritos. Se você tiver mudado o Identificador do dispositivo de entrada stylus do tablet em `xorg.conf` manualmente, substitua `"Mouse[7]"` pelo novo Identificador. Se você tiver um dispositivo com Wacom com suporte para tela sensível ao toque (você pode usar os dedos no tablet para mover o cursor), será necessário girar também o dispositivo de tela sensível ao toque.

19.8 Para obter mais informações

Alguns dos aplicativos mencionados aqui não oferecem ajuda on-line integrada, mas você pode encontrar informações úteis sobre o uso e a configuração em seu sistema instalado em `/usr/share/doc/package/packageName` ou na Web:

- Para obter o manual do Xournal, consulte <http://xournal.sourceforge.net/manual.html>
- A documentação do Jarnal está localizada em <http://www.dklevine.com/general/software/tc1000/jarnal.htm#documentation>
- Obtenha a página de manual do xstroke em <http://davesource.com/Projects/xstroke/xstroke.txt>
- Obtenha um documento HOWTO para configurar X no site na Web do Wacom sobre Linux: <http://linuxwacom.sourceforge.net/index.php/howto/x11>
- Obtenha um site na Web bastante informativo sobre o projeto do Dasher em <http://www.inference.phy.cam.ac.uk/dasher/>
- Obtenha mais informações e documentação sobre o CellWriter em <http://risujin.org/cellwriter/>
- Informações sobre o gnome-display-properties podem ser obtidas em <http://en.opensuse.org/GNOME/Multiscreen>

Parte IV. Serviços

Rede básica

O Linux oferece os recursos e as ferramentas de rede necessários para a integração em todos os tipos de estruturas de rede. O acesso à rede por meio de placa de rede, modem ou outro dispositivo pode ser configurado com o YaST. A configuração também pode ser feita manualmente. Neste capítulo são abordados apenas os mecanismos fundamentais e os arquivos de configuração de rede relevantes.

Linux e outros sistemas operacionais Unix usam o protocolo TCP/IP. Não é um protocolo de rede único, mas uma família de protocolos de rede que oferece vários serviços. Os protocolos listados na Tabela 20.1, “Vários protocolos na família de protocolos TCP/IP” (p 250) são fornecidos com a finalidade de trocar dados entre duas máquinas por meio do TCP/IP. As redes combinadas por TCP/IP compõem uma rede mundial também chamada de “Internet”.

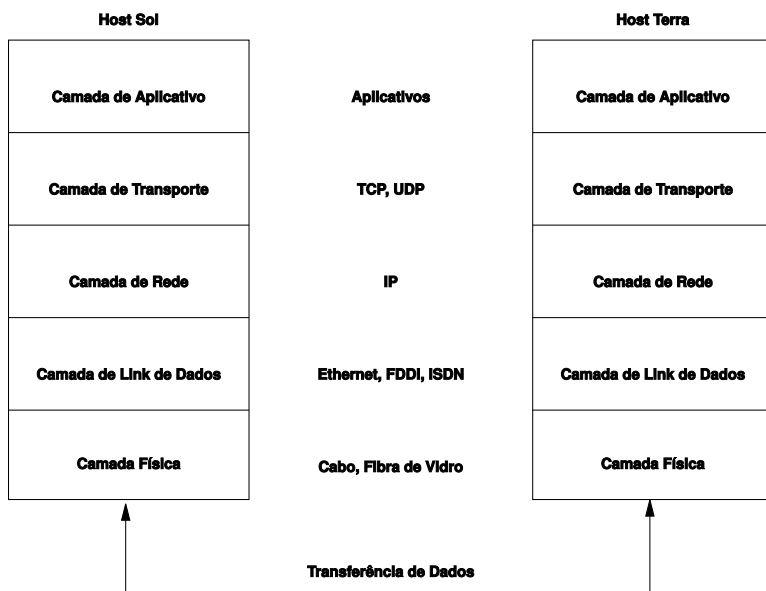
RFC significa *Request for Comments*. Os RFCs são documentos que descrevem vários procedimentos de implementação e protocolos da Internet para o sistema operacional e seus aplicativos. Os documentos RFC descrevem a configuração dos protocolos da Internet. Para ampliar seus conhecimentos sobre qualquer dos protocolos, consulte os documentos de RFC apropriados. Eles estão disponíveis em <http://www.ietf.org/rfc.html>.

Tabela 20.1 *Vários protocolos na família de protocolos TCP/IP*

Protocolo	Descrição
TCP	Transmission Control Protocol: um protocolo seguro orientado por conexão. Os dados a serem transmitidos são enviados primeiramente pelo aplicativo como fluxo de dados e convertidos no formato adequado ao sistema operacional. Os dados chegam ao respectivo aplicativo no host de destino com o formato original de fluxo de dados no qual foram inicialmente enviados. O TCP determina se algum dado foi perdido ou embaralhado durante a transmissão. O TCP é implementado onde a sequência de dados for necessária.
UDP	User Datagram Protocol: um protocolo inseguro, não baseado em conexão. Os dados a serem transmitidos são enviados na forma de pacotes gerados pelo aplicativo. A ordem em que os dados chegam ao destinatário não é garantida, havendo possibilidade de perda dos dados. O UDP é adequado para aplicativos orientados por registro. Ele possui um período de latência menor que o TCP.
ICMP	Internet Control Message Protocol: essencialmente, não se trata de um protocolo para o usuário final, mas um protocolo de controle especial que emite relatórios de erros e pode controlar o comportamento de máquinas que participam da transferência de dados TCP/IP. Além disso, ele fornece um modo de eco especial, que pode ser visualizado usando o programa ping.
IGMP	Internet Group Management Protocol: esse protocolo controla o comportamento da máquina na implementação de multicast IP.

Conforme mostrado na Figura 20.1, “Modelo de camadas simplificado para TCP/IP” (p 251), a troca de dados ocorre em camadas diferentes. A camada de rede real é a transferência de dados insegura por IP (Internet protocol). Acima do IP, o TCP garante, até certo ponto, a segurança na transferência de dados. A camada IP é suportada pelo protocolo dependente de hardware subjacente, como uma ethernet.

Figura 20.1 Modelo de camadas simplificado para TCP/IP



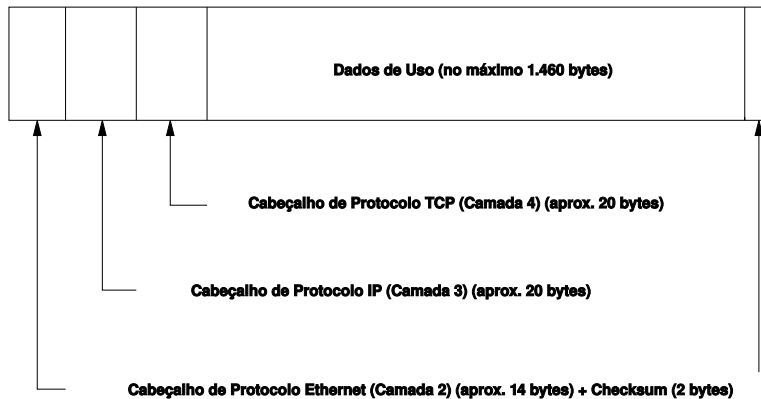
O diagrama fornece um ou dois exemplos para cada camada. As camadas são organizadas de acordo com os *níveis de abstração*. A camada mais baixa fica muito próxima do hardware. A camada mais alta é quase completamente abstraída do hardware. Todas as camadas possuem suas funções especiais próprias. As funções especiais de cada camada, na maioria das vezes, estão implícitas em suas descrições. O link de dados e as camadas físicas representam a rede física usada, como uma ethernet.

Quase todos os protocolos de hardware funcionam em uma base orientada por pacotes. Os dados a serem transmitidos são reunidos em *pacotes* (não podem ser enviados todos de uma vez). O tamanho máximo de um pacote TCP/IP é de, aproximadamente, 64 KB. Os pacotes são normalmente bem menores, já que o hardware da rede pode ser um fator de limitação. O tamanho máximo de um pacote de dados em uma ethernet é em torno de 1.500 bytes. O tamanho de um pacote TCP/IP limita-se a esse máximo quando os dados são enviados por uma ethernet. Se mais dados forem transferidos, mais pacotes de dados precisarão ser enviados pelo sistema operacional.

Para que as camadas executem suas respectivas funções, informações adicionais referentes a cada uma delas devem ser gravadas no pacote de dados. Isso ocorre no *cabeçalho* do pacote. Todas as camadas anexam um pequeno bloco de dados, chamado cabeçalho do protocolo, à frente de cada pacote emergente. Um exemplo de um pacote

de dados TCP/IP transmitido por um cabo ethernet é exibido na Figura 20.2, “Pacote Ethernet TCP/IP” (p 252). A soma de teste está localizada no final do pacote e não no início. Isso torna as coisas mais simples para o hardware de rede.

Figura 20.2 *Pacote Ethernet TCP/IP*



Quando um aplicativo envia dados por uma rede, eles passam por cada camada, todas implementadas no kernel do Linux, exceto a camada física. Cada camada é responsável pela preparação dos dados, para que eles possam passar para a camada seguinte. A camada mais baixa é a responsável pelo envio de dados. Todo o processo é invertido quando os dados são recebidos. Como camadas de uma cebola, em cada uma os cabeçalhos de protocolo são removidos dos dados transportados. Por fim, a camada de transporte é responsável por disponibilizar os dados para uso pelos aplicativos de destino. Dessa forma, cada camada se comunica somente com a camada diretamente acima ou abaixo dela. Para os aplicativos, é irrelevante o fato de os dados serem transmitidos por uma rede FDDI de 100 MBit/s ou por uma linha de modem de 56 kbit/s. Da mesma forma, é irrelevante para a linha de dados os tipos de dados transmitidos, contanto que os pacotes estejam no formato correto.

20.1 Roteamento e endereços IP

Esta seção limita-se à abordagem de redes IPv4. Para obter informações sobre o protocolo IPv6, sucessor do IPv4, consulte a Seção 20.2, “IPv6 — a Internet de última geração” (p 256).

20.1.1 Endereços IP

Todo computador na Internet possui um endereço de 32 bits exclusivo. Esses 32 bits (ou 4 bytes) são normalmente gravados conforme ilustrado na segunda linha no Exemplo 20.1, “Gravando endereços IP” (p 253).

Exemplo 20.1 *Gravando endereços IP*

```
IP Address (binary): 11000000 10101000 00000000 00010100
IP Address (decimal): 192.      168.      0.      20
```

Na forma decimal, os quatro bytes são gravados no sistema de números decimais, separados por pontos. O endereço IP é designado a um host ou a uma interface de rede. Ele pode ser usado apenas uma vez em todo o mundo. Há exceções a essa regra, mas não são relevantes para as passagens a seguir.

Os pontos nos endereços IP indicam o sistema hierárquico. Até os anos 90, os endereços IP eram estritamente categorizados em classes. Entretanto, esse sistema demonstrou ser excessivamente inflexível e foi desativado. Agora, o *CIDR* (Classless Interdomain Routing - Roteamento Interdomínio sem Classes) é usado.

20.1.2 Máscaras de rede e roteamento

As máscaras de rede são usadas para definir a faixa de endereços de uma sub-rede. Se dois hosts estiverem na mesma sub-rede, eles podem ter contato direto. Se não estiverem na mesma sub-rede, eles precisarão do endereço de um gateway que gerencie todo o tráfego da sub-rede. Para verificar se dois endereços IP estão em uma mesma sub-rede, basta “E” os dois endereços com a máscara de rede. Se o resultado for idêntico, os dois endereços IP estarão na mesma rede local. Se houver diferenças, o endereço IP remoto e, portanto, a interface remota, só poderão ser localizados através de um gateway.

Para compreender como as máscaras de rede funcionam, consulte o Exemplo 20.2, “Vinculando endereços IP à máscara de rede” (p 254). A máscara de rede consiste em 32 bits que identificam quanto de um endereço IP pertence à rede. Todos os bits 1 marcam o bit correspondente no endereço IP como pertencente à rede. Todos os bits 0 marcam os bits dentro da sub-rede. Isso significa que quanto maior a quantidade de bits 1, menor será o tamanho da sub-rede. Como a máscara de rede sempre consiste em vários bits 1 sucessivos, também é possível apenas contar o número de bits da máscara

de rede. No Exemplo 20.2, “Vinculando endereços IP à máscara de rede” (p 254) a primeira rede com 24 bits também poderia ser gravada como 192.168.0.0/24.

Exemplo 20.2 Vinculando endereços IP à máscara de rede

```
IP address (192.168.0.20):  11000000 10101000 00000000 00010100
Netmask   (255.255.255.0): 11111111 11111111 11111111 00000000
-----
Result of the link:         11000000 10101000 00000000 00000000
In the decimal system:      192.      168.      0.      0

IP address (213.95.15.200): 11010101 10111111 00001111 11001000
Netmask   (255.255.255.0): 11111111 11111111 11111111 00000000
-----
Result of the link:         11010101 10111111 00001111 00000000
In the decimal system:      213.      95.      15.      0
```

Um outro exemplo: todas as máquinas conectadas ao mesmo cabo ethernet, normalmente, estão localizadas na mesma sub-rede e são diretamente acessíveis. Mesmo quando a sub-rede é dividida fisicamente por switches ou pontes, esses hosts ainda assim podem ser diretamente localizados.

Endereços IP fora da sub-rede local só poderão ser localizados se um gateway for configurado para a rede de destino. Nos casos mais comuns, há somente um gateway que controla todo o tráfego externo. Entretanto, também é possível configurar vários gateways para sub-redes diferentes.

Se um gateway tiver sido configurado, todos os pacotes IP externos serão enviados para o gateway apropriado. Esse gateway tentará então encaminhar os pacotes da mesma forma (de host para host) até acessar o host de destino ou até o TTL (tempo de operação) do pacote expirar.

Tabela 20.2 Endereços específicos

Tipo de endereço	Descrição
Endereço de rede base	Essa é a máscara de rede E qualquer endereço na rede, conforme mostrado no Exemplo 20.2, “Vinculando endereços IP à máscara de rede” (p 254) em Resultado. Esse endereço não pode ser designado a nenhum host.

Tipo de endereço	Descrição
Endereço de broadcast	Isso significa, basicamente, “Acessar todos os hosts nesta sub-rede.” Para gerar isso, a máscara de rede é invertida no formato binário e vinculada ao endereço de rede base com um OU lógico. Portanto, o exemplo acima resulta em 192.168.0.255. Esse endereço não pode ser atribuído a nenhum host.
Host local	O endereço 127.0.0.1 é designado ao “dispositivo loopback” em cada host. Pode-se configurar uma conexão para a sua própria máquina com este endereço e com todos os endereços da rede de loopback completa 127.0.0.0/8, conforme definidos com o IPv4. Com o IPv6, existe apenas um endereço de loopback (:::1).

Como os endereços IP precisam ser exclusivos em qualquer parte do mundo, não é possível selecionar endereços aleatoriamente. Há três domínios de endereços a serem usados para configurar uma rede baseada em IP privado. Eles não conseguem se conectar ao restante da Internet, pois não podem ser transmitidos através dela. Esses domínios de endereço são especificados no RFC 1597 e listados na Tabela 20.3, “Domínios de endereços IP privados” (p 255).

Tabela 20.3 *Domínios de endereços IP privados*

Rede/máscara de rede	Domínio
10.0.0.0/255.0.0.0	10.x.x.x
172.16.0.0/255.240.0.0	172.16.x.x – 172.31.x.x
192.168.0.0/255.255.0.0	192.168.x.x

20.2 IPv6 — a Internet de última geração

Devido ao surgimento da WWW (World Wide Web), a Internet teve um crescimento acelerado com um número cada vez maior de computadores se comunicando por TCP/IP nos últimos quinze anos. Desde que Tim Berners-Lee da CERN (<http://public.web.cern.ch>) inventou a WWW em 1990, o número de hosts da Internet cresceu de poucos milhares para centenas de milhões deles.

Conforme mencionado, um endereço IPv4 consiste em apenas 32 bits. Além disso, poucos endereços IP são perdidos; eles não podem ser usados devido à forma como as redes são organizadas. O número de endereços disponíveis na sua sub-rede é dois elevado à potência do número de bits, menos dois. Uma sub-rede tem, por exemplo, 2, 6 ou 14 endereços disponíveis. Para conectar 128 hosts à Internet, por exemplo, você precisa de uma sub-rede com 256 endereços IP, dos quais apenas 254 são utilizáveis, visto que são necessários dois endereços IP para a estrutura da própria sub-rede: o endereço de broadcast e o endereço de rede base.

No protocolo IPv4 atual, DHCP ou NAT (Network Address Translation - Conversão de Endereços de Rede) são os mecanismos comuns usados para contornar a grande falta de endereços. Combinado à convenção de manter endereços públicos e privados separados por espaços, esses métodos podem certamente reduzir a falta de endereços. O problema deles está em suas configurações, trabalhosas para configurar e difíceis de manter. Para configurar um host em uma rede IPv4, é preciso que haja vários itens de endereços, como o próprio endereço IP do host, a máscara de sub-rede, o endereço de gateway e talvez um endereço de servidor de nomes. Todos esses itens precisam ser conhecidos e não podem ser derivados de outro lugar.

Com o IPv6, tanto a falta de endereços quanto as configurações complicadas passariam a ser problemas do passado. As seções a seguir oferecem mais informações sobre os aprimoramentos e benefícios trazidos pelo IPv6 e sobre a transição do protocolo antigo para o novo.

20.2.1 Vantagens

A melhoria mais importante e visível oferecida pelo novo protocolo é a expansão enorme do espaço disponível para endereços. Um endereço IPv6 é criado com valores de 128

bits em vez dos 32 bits tradicionais. Ele é capaz de fornecer 'quatrilhões' de endereços IP.

Entretanto, os endereços IPv6 não diferem de seus antecessores apenas em relação ao comprimento. Também possuem uma estrutura interna diferente, que pode conter mais informações específicas sobre os sistemas e as redes a que pertencem. Leia mais detalhes sobre eles na Seção 20.2.2, “Estrutura e tipos de endereços” (p 258).

A seguir, há uma lista de algumas outras vantagens do novo protocolo:

Configuração automática

O IPv6 torna apto o “plug and play” da rede, o que significa que um sistema recentemente configurado é integrado à rede (local) sem qualquer configuração manual. O novo host usa seu mecanismo de configuração automática para derivar seu próprio endereço a partir das informações disponibilizadas pelos roteadores vizinhos, com base em um protocolo chamado *ND* (Neighbor Discovery - descoberta de vizinho). Esse método não exige nenhuma intervenção por parte do administrador e não há necessidade de manter um servidor central para alocação de endereços: uma vantagem adicional em relação ao IPv4, cuja alocação automática de endereços exige um servidor DHCP.

Apesar disso, se houver um roteador conectado a um switch, ele deverá enviar anúncios periódicos com flags avisando os hosts de uma rede sobre como devem interagir entre si. Para obter mais informações, consulte o RFC 2462 e a página de manual de `radvd.conf(5)`, além do RFC 3315.

Mobilidade

O IPv6 torna possível a atribuição de vários endereços a uma interface de rede ao mesmo tempo. Isso permite que os usuários acessem várias redes com facilidade, algo comparável aos serviços de roaming internacional oferecidos por operadoras de telefonia celular: quando você leva seu telefone celular para o exterior, ele se registra automaticamente em um serviço estrangeiro logo que entra na área correspondente, de modo que você possa ser contatado pelo mesmo número em qualquer lugar e ligar para alguém do mesmo modo que faz em sua área de origem.

Comunicação segura

Com o IPv4, a segurança da rede é uma função adicional. O IPv6 inclui IPsec como um de seus recursos principais, permitindo que sistemas se comuniquem por um túnel seguro, para evitar a intromissão de estranhos na Internet.

Compatibilidade retroativa

De forma realista, seria impossível mudar toda a Internet de IPv4 para IPv6 de uma só vez. Portanto, é essencial que ambos os protocolos sejam capazes de coexistir na Internet, mas também em um sistema. Isso é garantido por endereços compatíveis (endereços IPv4 podem facilmente ser convertidos em endereços IPv6) e através do uso de vários túneis. Consulte a Seção 20.2.3, “Coexistência de IPv4 e IPv6” (p 263). Da mesma forma, os sistemas podem se basear em uma técnica *IP de pilha dupla* para suportar os dois protocolos ao mesmo tempo, significando que possuem duas pilhas de rede completamente separadas, de tal forma que não há interferência entre as duas versões de protocolos.

Serviços adaptados e personalizados através de Multicast

Com o IPv4, alguns serviços, como SMB, precisam transmitir seus pacotes para todos os hosts na rede local. O IPv6 oferece uma abordagem mais detalhada, permitindo que os servidores gerenciem os hosts por *multicast* — tratando um número de hosts como partes de um grupo (o que é diferente de gerenciar todos os hosts por *broadcast* ou cada host individualmente por *unicast*). Os hosts enviados como grupos talvez dependam do aplicativo concreto. É possível enviar todos os servidores de nomes para alguns grupos predefinidos (o *grupo multicast de servidores de nomes*), por exemplo ou todos os roteadores (o *grupo multicast de todos os roteadores*).

20.2.2 Estrutura e tipos de endereços

Conforme mencionado, o protocolo IP atual está em desvantagem em relação a dois aspectos importantes: os endereços IP estão cada vez mais escassos, e a configuração de rede com manutenção de tabelas de rotina vem se tornando cada vez mais uma tarefa complexa e onerosa. O IPv6 soluciona o primeiro problema, expandindo o espaço dos endereços para 128 bits. O segundo problema é contornado com a introdução de uma estrutura hierárquica de endereços, combinada com técnicas sofisticadas para alocar endereços de rede, assim como *multihoming* (a capacidade de designar vários endereços a um dispositivo, permitindo acesso a diversas redes).

Ao utilizar o IPv6, é útil saber que há três tipos diferentes de endereços:

Unicast

Endereços desse tipo são associados com exatamente uma interface de rede. Pacotes com esse tipo de endereço são entregues em apenas um destino. Da mesma forma, os endereços unicast são usados para transferir pacotes para hosts individuais na rede local ou na Internet.

Multicast

Endereços desse tipo estão relacionados a um grupo de interfaces de rede. Pacotes com esse tipo de endereço são entregues a todos os destinos pertencentes ao grupo. Endereços multicast são usados, principalmente, por certos tipos de serviços de rede para se comunicarem com determinados grupos de host de forma bem direcionada.

Anycast

Endereços desse tipo estão relacionados a um grupo de interfaces. Pacotes com esse tipo de endereço são entregues ao membro do grupo mais próximo do remetente, de acordo com os princípios do protocolo de roteamento subjacente. Endereços anycast são usados para que hosts possam descobrir mais facilmente servidores que oferecem certos serviços na área da rede determinada. Todos os servidores do mesmo tipo possuem o mesmo endereço anycast. Sempre que um host solicita um serviço, ele recebe uma resposta do servidor com o local mais próximo, conforme determinado pelo protocolo de roteamento. Caso ocorra alguma falha com esse servidor, o protocolo selecionará automaticamente o segundo servidor mais próximo ou então o terceiro e assim por diante.

Um endereço IPv6 é constituído de oito campos de quatro dígitos, cada um representando 16 bits, gravados em notação hexadecimal. Eles são separados por dois-pontos (:). Quaisquer zero bytes iniciais em um determinado campo podem ser descartados, mas zeros dentro ou no final do campo não podem ser descartados. Outra convenção é a de que mais de quatro zero bytes consecutivos podem retornar como dois-pontos duplos. Entretanto, apenas um separador do tipo :: é permitido por endereço. Esse tipo de notação reduzida é mostrado no Exemplo 20.3, “Amostra de endereço IPv6” (p 259), em que todas as três linhas representam o mesmo endereço.

Exemplo 20.3 *Amostra de endereço IPv6*

```
fe80 : 0000 : 0000 : 0000 : 0000 : 10 : 1000 : 1a4  
fe80 :    0 :    0 :    0 :    0 : 10 : 1000 : 1a4  
fe80 :                               : 10 : 1000 : 1a4
```

Cada parte de um endereço IPv6 possui uma função definida. Os primeiros bytes formam o prefixo e especificam o tipo de endereço. A parte central é a porção do endereço na rede, mas pode não ser utilizada. O final do endereço forma a parte do host. Com o IPv6, a máscara de rede é definida indicando o comprimento do prefixo depois de uma barra no final do endereço. Um endereço, como mostrado no Exemplo 20.4, “Endereço IPv6 especificando o comprimento do prefixo” (p 260), contém as informações de que os primeiros 64 bits formam a parte da rede do endereço e que os últimos 64 formam

a parte do host. Em outras palavras, 64 significa que a máscara de rede está preenchida com 64 valores de 1 bit a partir da esquerda. Da mesma forma que o IPv4, o endereço IP é combinado com E com os valores da máscara de rede, para determinar se o host está localizado na mesma sub-rede ou em outra.

Exemplo 20.4 *Endereço IPv6 especificando o comprimento do prefixo*

fe80::10:1000:1a4/64

O IPv6 conhece vários tipos de prefixos predefinidos. Alguns são mostrados na Tabela 20.4, “Vários prefixos IPv6” (p 260).

Tabela 20.4 *Vários prefixos IPv6*

Prefixo (hex)	Definição
00	Endereços IPv4 e endereços de compatibilidade de IPv4 sobre IPv6. Esses são usados para manter a compatibilidade com IPv4. O seu uso ainda exige um roteador capaz de converter pacotes IPv6 em pacotes IPv4. Vários endereços especiais, como o do dispositivo loopback, também possuem esse prefixo.
2 ou 3 como o primeiro dígito	Endereços unicast globais agregativos. Como no caso do IPv4, uma interface pode ser designada para fazer parte de uma determinada sub-rede. Atualmente, existem os seguintes espaços de endereço: 2001::/16 (espaço de endereço de qualidade de produção) e 2002::/16 (espaço de endereço 6to4).
fe80::/10	Endereços locais de links. Endereços com esse prefixo não devem ser roteados e, portanto, só devem ser encontrados na mesma sub-rede.
fe80::/10	Endereços locais de sites. Esses podem ser roteados, mas somente na rede da organização a que pertencem. Na verdade, eles são o equivalente IPv6 do espaço de endereço de rede privada atual, como 10.x.x.x.
ff	Esses são endereços multicast.

Um endereço unicast consiste em três componentes básicos:

Topologia pública

A primeira parte (que também contém um dos prefixos mencionados acima) é usada para rotear pacotes através da Internet pública. Ela inclui informações sobre a empresa ou instituição que fornece o acesso à Internet.

Topologia do site

A segunda parte contém informações de roteamento sobre a sub-rede à qual o pacote deve ser entregue.

ID de interface

A terceira parte identifica a interface à qual o pacote deve ser entregue. Isso também permite que o MAC faça parte do endereço. Como MAC é um identificador fixo globalmente exclusivo codificado no dispositivo pelo fabricante do hardware, o procedimento de configuração é bastante simplificado. Na verdade, os primeiros 64 bits de endereço são consolidados para formar o token $EUI-64$, com os últimos 48 bits obtidos no MAC e os 24 bits restantes contendo informações especiais sobre o tipo de token. Isso também possibilita designar um token $EUI-64$ a interfaces que não possuem MAC, como aquelas baseadas em PPP ou ISDN.

No topo dessa estrutura básica, o IPv6 faz distinção entre cinco tipos de endereços unicast:

: : (não especificado)

Esse endereço é usado pelo host como seu endereço de origem durante a primeira inicialização da interface, quando o endereço ainda não pode ser determinado por outros meios.

: : 1 (loopback)

O endereço do dispositivo loopback.

Endereços compatíveis com o IPv4

O endereço IPv6 é formado pelo endereço IPv4 e um prefixo consistindo em 96 zero bits. Esse tipo de endereço de compatibilidade é usado para um túnel (consulte a Seção 20.2.3, “Coexistência de IPv4 e IPv6” (p 263)) para permitir que os hosts IPv4 e IPv6 se comuniquem com outros que estejam operando em um ambiente IPv4 puro.

Endereços IPv4 mapeados para IPv6

Esse tipo de endereço especifica um endereço IPv4 puro em uma notação IPv6.

Endereços locais

Há dois tipos de endereços para uso local:

link-local

Esse tipo de endereço só pode ser usado na sub-rede local. Pacotes com endereço de origem ou de destino desse tipo não devem ser roteados para a Internet nem para outras sub-redes. Esses endereços contêm um prefixo especial ($f\epsilon 80 : : / 10$) e o ID da interface da placa de rede, com a parte do meio consistindo em zero bytes. Endereços desse tipo são usados durante a configuração automática para se comunicarem com outros hosts pertencentes à mesma sub-rede.

site-local

Pacotes com esse tipo de endereço podem ser roteados para outras sub-redes, mas não para a Internet mais ampla. Eles precisam permanecer dentro da própria rede da organização. Tais endereços são usados para intranets e equivalem ao espaço de endereço privado definido pelo IPv4. Eles contêm um prefixo especial ($f\epsilon c0 : : / 10$), o ID da interface e um campo de 16 bits especificando o ID da sub-rede. Novamente, o restante é preenchido com zero bytes.

Como um recurso completamente novo, introduzido com o IPv6, cada interface de rede normalmente obtém vários endereços IP, com a vantagem de que várias redes podem ser acessadas através da mesma interface. Uma dessas redes pode ser totalmente configurada automaticamente usando o MAC e um prefixo conhecido, resultando na possibilidade de todos os hosts na rede local serem encontrados assim que o IPv6 for habilitado (usando o endereço link-local). Com o MAC fazendo parte disso, qualquer endereço IP usado no mundo será exclusivo. As únicas partes variáveis do endereço são aquelas que indicam a *topologia do site* e a *topologia pública*, dependendo da rede real na qual o host estiver operando no momento.

Para que um host avance e retroceda entre duas redes diferentes ele precisa de, pelo menos, dois endereços. Um deles, o *endereço pessoal*, contém não só o ID de interface, como também um identificador da rede doméstica a que ele normalmente pertence (e o prefixo correspondente). O endereço pessoal é um endereço estático e, portanto, normalmente não se modifica. Mesmo assim, todos os pacotes destinados ao host móvel podem ser entregues a ele, independentemente de ele operar na rede doméstica ou em outro local externo. Isso é possível devido aos recursos totalmente novos introduzidos com o IPv6, como *configuração automática sem estado e descoberta de vizinho*. Além do endereço residencial, um host móvel obtém um ou mais endereços adicionais pertencentes às redes interurbanas com roaming. Eles são chamados endereços *care-*

of. A rede doméstica tem um recurso que encaminha qualquer pacote destinado ao host quando ele está em roaming. Em um ambiente IPv6, essa tarefa é executada pelo *agente local*, que retransmite todos os pacotes destinados ao endereço residencial através de um túnel. Por outro lado, esses pacotes destinados ao endereço care-of são diretamente transferidos para o host móvel sem qualquer desvio especial.

20.2.3 Coexistência de IPv4 e IPv6

A migração de todos os hosts conectados à Internet do IPv4 para o IPv6 é um processo gradual. Os dois protocolos coexistirão durante algum tempo. A coexistência deles em um sistema é garantida onde houver uma implementação de *pilha dupla* de ambos os protocolos. Ainda resta a dúvida de como um host habilitado do IPv6 deve se comunicar com um host IPv4 e como pacotes do IPv6 devem ser transportados pelas redes atuais, que são predominantemente baseadas no IPv4. As melhores soluções oferecem endereços de compatibilidade e túnel (consulte a Seção 20.2.2, “Estrutura e tipos de endereços” (p 258)).

Os hosts IPv6 que estiverem mais ou menos isolados na rede IPv4 (mundial) podem se comunicar por túneis: os pacotes IPv6 são encapsulados como pacotes IPv4 para que sejam transmitidos por uma rede IPv4. Tal conexão entre dois hosts IPv4 é chamada de *túnel*. Para que isso ocorra, os pacotes precisam incluir o endereço de destino do IPv6 (ou o prefixo correspondente), assim como o endereço IPv4 do host remoto no destino final do túnel. Um túnel básico pode ser configurado manualmente, de acordo com um contrato entre os administradores dos hosts. Também é chamado de *túnel estático*.

Entretanto, a configuração e manutenção de túneis estáticos é normalmente muito trabalhosa para ser usada diariamente em comunicações. Portanto, o IPv6 fornece três métodos de *túneis dinâmicos*:

6over4

Os pacotes IPv6 são automaticamente encapsulados como pacotes IPv4 e enviados por uma rede IPv4 com capacidade multicast. O IPv6 é induzido a considerar a rede inteira (Internet) como uma gigantesca rede local. Com isso, é possível determinar automaticamente o destino final do túnel IPv4. Entretanto, esse método não faz um dimensionamento muito bom e também é dificultado pelo fato de o multicast IP não ser tão difundido na Internet. Portanto, ele apenas fornece uma solução para redes corporativas ou institucionais menores, em que o multicast pode ser habilitado. As especificações para esse método estão descritas no RFC 2529.

6to4

Com esse método, os endereços IPv4 são automaticamente gerados a partir de endereços IPv6, habilitando a comunicação de hosts IPv6 isolados através de uma rede IPv4. Entretanto, alguns problemas foram relatados no que tange à comunicação entre esses hosts IPv6 isolados e a Internet. O método está descrito no RFC 3056.

Controlador do túnel IPv6

Esse método se baseia em servidores especiais que fornecem túneis dedicados para hosts IPv6. É descrito no RFC 3053.

20.2.4 Configurando o IPv6

Para configurar o IPv6, normalmente não é necessário fazer mudanças nas estações de trabalho individuais. O IPv6 é habilitado por padrão. Você pode desabilitá-lo durante a instalação na etapa de configuração da rede, descrita na “Network Configuration” (Capítulo 3, *Installation with YaST*, ↑ *Guia de Implantação*). Para desabilitar ou habilitar o IPv6 em um sistema instalado, use o módulo *Configurações de Rede* do YaST. Na guia *Opções Globais*, marque ou desmarque a opção *Habilitar IPv6* conforme for necessário. Se desejar habilitá-lo temporariamente até a próxima reinicialização, digite `modprobe -i ipv6` enquanto `root`. Basicamente, é impossível descarregar o módulo `ipv6` depois de carregado.

Devido ao conceito de configuração automática do IPv6, um endereço é designado à placa de rede na rede *link-local*. Normalmente, nenhum gerenciamento de tabela de roteamento é feito em uma estação de trabalho. Os roteadores de rede podem ser consultados pela estação de trabalho, usando o *protocolo de anúncios do roteador*, para o qual devem ser implementados um prefixo e gateways. O programa `radvd` pode ser usado para configurar um roteador IPv6. Esse programa informa às estações de trabalho o prefixo que deve ser usado para os endereços IPv6 e os roteadores. Outra opção é usar *zebra/quagga* para a configuração automática dos dois endereços e para roteamento.

Consulte a página de manual do `ifcfg-tunnel` (5) para obter informações sobre como configurar vários tipos de túneis usando os arquivos `/etc/sysconfig/network`.

20.2.5 Para obter mais informações

A visão geral acima não abrange totalmente o tópico do IPv6. Para obter informações mais detalhadas sobre o novo protocolo, consulte os livros e a documentação online a seguir:

<http://www.ipv6.org/>

O ponto de partida para tudo relativo ao IPv6.

<http://www.ipv6day.org>

Todas as informações necessárias para iniciar sua própria rede IPv6.

<http://www.ipv6-to-standard.org/>

A lista de produtos habilitados para IPv6.

<http://www.bieringer.de/linux/IPv6/>

Aqui, encontre o Linux IPv6-HOWTO e muitos links relacionados ao tópico.

RFC 2640

Informações fundamentais do RFC sobre o IPv6.

IPv6 Essentials

Um livro que descreve todos os aspectos importantes do tópico é o *IPv6 Essentials* de Silvia Hagen (ISBN 0-596-00125-8).

20.3 Resolução de nomes

O DNS ajuda na designação de um endereço IP a um ou mais nomes e na designação de um nome a um endereço IP. No Linux, essa conversão normalmente é executada por um tipo especial de software chamado bind. A máquina responsável por essa conversão é chamada de *servidor de nomes*. Os nomes criam um sistema hierárquico, no qual cada componente do nome é separado um ponto. A hierarquia de nomes é, entretanto, independente da hierarquia de endereços IP descrita acima.

Considere um nome completo, como `jupiter.example.com`, gravado no formato `nome_do_host.domínio`. Um nome completo, denominado *FQDN* (Fully Qualified Domain Name - Nome de Domínio Completo), consiste em um nome de host e um

nome de domínio (`example.com`). O último também inclui o *TLD* (Top Level Domain - Domínio de Nível Superior) (`com`).

A designação TLD tornou-se bastante confusa por razões históricas. Tradicionalmente, nomes de domínio com três letras são usados nos EUA. No resto do mundo, os códigos nacionais ISO de duas letras são o padrão. Além disso, TLDs mais longos foram introduzidos em 2000, representando certas esferas de atividades (por exemplo, `.info`, `.name`, `.museum`).

No início da Internet (antes de 1990), o arquivo `/etc/hosts` era usado para armazenar os nomes de todas as máquinas representadas na Internet. Isso rapidamente se tornou impraticável, devido ao crescente número de computadores conectados à Internet. Por essa razão, um banco de dados descentralizado foi desenvolvido para armazenar nomes de hosts de uma forma amplamente distribuída. Esse banco de dados, semelhante ao servidor de nomes, não possui os dados pertencentes a todos os hosts na Internet já disponíveis, mas pode encaminhar solicitações a outros servidores de nomes.

A parte superior da hierarquia é ocupada pelos *servidores de nomes raiz*. Esses servidores de nomes raiz gerenciam os domínios de nível superior e são executados pelo NIC (Network Information Center). Cada servidor de nomes raiz conhece os servidores de nomes responsáveis por um determinado domínio de nível superior. Para obter informações sobre NICs de domínio superior, vá para <http://www.internic.net>.

O DNS pode fazer mais do que apenas resolver nomes de hosts. O servidor de nomes também distingue qual host recebe e-mails de um domínio inteiro: o *servidor de correio* (*MX*).

Para sua máquina resolver um endereço IP, ela precisa pelo menos conhecer um servidor de nomes e seu respectivo endereço IP. É fácil especificar esse servidor de nomes com a ajuda do YaST. Se você tiver uma conexão de discagem por modem, talvez não precise nem mesmo configurar um servidor de nomes manualmente. O protocolo de discagem fornece o endereço do servidor de nomes enquanto a conexão é efetuada.

O protocolo `whois` está intimamente relacionado ao DNS. Com esse programa, é possível descobrir rapidamente o responsável por qualquer domínio especificado.

NOTA: MDNS e nomes do domínio .local

O domínio de nível superior `.local` é tratado como domínio link-local pelo resolver. As solicitações de DNS são enviadas como solicitações de DNS multicast, em vez de solicitações de DNS normal. Se você já utiliza o domínio `.local` na sua configuração de servidor de nomes, deverá desativar a opção `nameserver` em `/etc/host.conf`. Para obter mais informações, consulte a página de manual `host.conf`.

Se desejar desativar o MDNS durante a instalação, use `nomdns=1` como parâmetro de boot.

Para obter mais informações sobre DNS de multicast, consulte <http://www.multicastdns.org>.

20.4 Configurando uma conexão de rede com o YaST

Há muitos tipos de redes suportadas no Linux. A maioria delas usa nomes de dispositivos diferentes e os arquivos de configuração se espalham por vários locais no sistema de arquivos. Para obter uma visão geral detalhada dos aspectos da configuração manual de rede, consulte a Seção 20.6, “Configurando uma conexão de rede manualmente” (p 291).

No SUSE Linux Enterprise Desktop, onde o NetworkManager fica ativo por padrão, todas as placas de rede são configuradas. Se o NetworkManager não estiver ativo, apenas a primeira interface com link ativo (com cabo de rede conectado) será configurada automaticamente. Hardwares adicionais podem ser configurados a qualquer momento no sistema instalado. As seções a seguir descrevem a configuração de rede para todos os tipos de conexões de rede suportadas pelo SUSE Linux Enterprise Desktop.

20.4.1 Configurando a placa de rede com o YaST

Para configurar sua placa de rede wireless ou não no YaST, selecione *Dispositivos de Rede > Configurações de Rede*. Após iniciar o módulo, o YaST exibe a caixa de diálogo

Configurações de Rede com quatro guias: *Opções Globais*, *Visão Geral*, *Nome de Host/DNS* e *Roteamento*.

A guia *Opções Globais* permite definir opções gerais de rede, como o uso do NetworkManager, o IPv6 e opções gerais de DHCP. Para obter mais informações, consulte “Configurando opções globais de rede” (p 269).

A guia *Visão Geral* contém informações sobre interfaces de rede instaladas e configurações. Ela lista os nomes de todas as placas de rede detectadas corretamente. Nessa caixa de diálogo, você pode configurar manualmente novas placas, bem como remover ou mudar suas configurações. Se você quiser configurar manualmente uma placa que não foi detectada automaticamente, consulte “Configurando uma placa de rede não detectada” (p 276). Se você quiser mudar a configuração de uma placa que já está configurada, consulte “Mudando a configuração de uma placa de rede” (p 270).

A guia *Nome de Host/DNS* permite definir o nome de host da máquina e nomear os servidores que serão usados. Para obter mais informações, consulte “Configurando o nome do host e o DNS” (p 277).

A guia *Roteamento* é usada para a configuração do roteamento. Consulte “Configurando o roteamento” (p 279) para obter mais informações.

Figura 20.3 Definindo as configurações da rede



Configurando opções globais de rede

A guia *Opções Globais* do módulo *Configurações de Rede* do YaST permite definir opções globais de rede importantes, como o uso do NetworkManager, o IPv6 e opções de cliente DHCP. Essas configurações são aplicáveis a todas as interfaces de rede.

Em *Método de Configuração da Rede*, escolha o modo como as conexões de rede são gerenciadas. Se você quiser que um applet de área de trabalho NetworkManager gerencie as conexões de todas as interfaces, escolha *Controlado por Usuário com o NetworkManager*. Essa opção é ideal para fazer a alternância entre várias redes wireless ou não. Se você não tem um ambiente de área de trabalho (GNOME ou KDE) em execução, ou se o seu computador for um servidor Xen, um sistema virtual ou fornecer serviços de rede como DHCP ou DNS na rede em que se encontra, use o *Método Tradicional com ifup*. Se o NetworkManager for usado, `nm-applet` deverá ser usado para configurar as opções da rede, ficando desativadas as guias *Visão Geral*, *Nome de*

Host/DNS e Roteamento do módulo *Configurações de Rede*. Para obter mais informações sobre o NetworkManager, consulte o Capítulo 23, *Usando o NetworkManager* (p 323).

Nas *Configurações do Protocolo IPv6*, escolha entre usar ou não o protocolo IPv6. É possível usar o IPv6 juntamente com o IPv4. Por padrão, o IPv6 fica ativado. Contudo, nas redes que não usam o protocolo IPv6, os tempos de resposta podem ser acelerados com o protocolo IPv6 desabilitado. Para desabilitar o IPv6, desmarque a opção *Habilitar IPv6*. Isso desabilita o carregamento automático do módulo de kernel do IPv6. Essa ação será aplicada após a reinicialização.

Nas *Opções do Cliente DHCP*, configure as opções do cliente DHCP. Se você quiser que o cliente DHCP peça ao servidor para sempre transmitir suas respostas, marque *Requerer Resposta a Broadcast*. Isso pode ser necessário se houver o costume de mover a sua máquina entre redes diferentes. O *Identificador de Cliente DHCP* deve ser diferente para cada cliente DHCP na mesma rede. Se ficar vazio, assumirá como padrão o endereço de hardware da interface da rede. Entretanto, se você tiver várias máquinas virtuais em execução na mesma interface de rede e, portanto, com o mesmo endereço de hardware, especifique aqui um identificador exclusivo.

O *Nome do Host a Enviar* especifica uma string usada no campo da opção de nome de host quando o dhcpcd envia mensagens ao servidor DHCP. Alguns servidores DHCP atualizam as zonas do servidor de nomes (registros diretos e reversos) de acordo com esse nome de host (DNS Dinâmico). Além disso, alguns servidores DHCP exigem que o campo da opção *Nome do Host a Enviar* contenha uma string específica nas mensagens DHCP dos clientes. Mantenha *AUTO* para enviar o nome de host atual (ou seja, o que está definido em `/etc/HOSTNAME`). Deixe o campo da opção vazio para não enviar nenhum nome de host. Se você não quiser mudar a rota padrão de acordo com as informações do DHCP, desmarque *Mudar Rota Padrão via DHCP*.

Mudando a configuração de uma placa de rede

Para mudar a configuração de uma placa de rede, selecione uma placa na lista de placas detectadas em *Configurações de Rede > Visão Geral* no YaST e clique em *Editar*. A caixa de diálogo *Configuração da Placa de Rede* é exibida, na qual é possível ajustar a configuração da placa usando as guias *Geral*, *Endereço* e *Hardware*. Para obter informações sobre a configuração de placas wireless, consulte a Seção 17.5, “Configuração com o YaST” (p 216).

Configurando endereços IP

Você pode definir o endereço IP da placa de rede ou o modo como seu endereço IP é determinado na guia *Endereço* da caixa de diálogo *Configuração da Placa de Rede*. Há suporte para endereços IPv4 e IPv6. A placa de rede pode ser *Sem Endereço IP* (útil para dispositivos de vinculação), ter um *Endereço IP Atribuído Estaticamente* (IPv4 ou IPv6) ou um *Endereço Dinâmico* atribuído por *DHCP*, *Zeroconf* ou ambos.

Ao usar um *Endereço Dinâmico*, selecione se deseja usar *Apenas DHCP Versão 4* (para IPv4), *Apenas DHCP Versão 6* (para IPv6) ou *DHCP Versões 4 e 6*.

Se possível, a primeira placa de rede com link que estiver disponível durante a instalação será configurada automaticamente para usar a configuração automática de endereço via DHCP. No SUSE Linux Enterprise Desktop, no qual o NetworkManager fica ativo por padrão, todas as placas de rede são configuradas.

Também será necessário usar o DHCP se você estiver usando uma linha DSL sem nenhum IP estático atribuído pelo ISP (Internet Service Provider - Provedor de Serviços de Internet). Se você decidir usar o DHCP, configure os detalhes em *Opções do Cliente DHCP*, na guia *Opções Globais* da caixa de diálogo *Configurações de Rede* do módulo de configuração de placa de rede do YaST. Especifique se o cliente DHCP deve pedir que o servidor sempre transmita suas respostas em *Requerer Resposta a Broadcast*. Essa opção pode ser necessária se a sua máquina for um cliente móvel que costuma trocar de rede. Se você tiver uma configuração de host virtual, em que hosts diferentes se comunicam pela mesma interface, será necessário um *Identificador de Cliente DHCP* para diferenciá-las.

O DHCP é uma boa opção para a configuração de clientes, mas não é a ideal para a configuração de servidores. Para definir um endereço IP estático, faça o seguinte:

- 1 Selecione uma placa na lista de placas detectadas na guia *Visão Geral* do módulo de configuração de placa de rede do YaST e clique em *Editar*.
- 2 Na guia *Endereço*, escolha *Endereço IP Atribuído Estaticamente*.
- 3 Digite o *Endereço IP*. Podem ser usados endereços IPv4 e IPv6. Digite a máscara de rede em *Máscara de Sub-rede*. Se for usado o endereço IPv6, use *Máscara de Sub-rede* para um comprimento do prefixo no formato / 6 4.

Como opção, você pode digitar um *Nome de Host* completo para esse endereço, que será gravado no arquivo de configuração `/etc/hosts`.

- 4 Clique em *Avançar*.
- 5 Para ativar a configuração, clique em *OK*.

Se você usa o endereço estático, os servidores de nomes e o gateway padrão não são configurados automaticamente. Para configurar servidores de nomes, proceda conforme descrito em “Configurando o nome do host e o DNS” (p 277). Para configurar um gateway, proceda conforme descrito em “Configurando o roteamento” (p 279).

Configurando álias

Um dispositivo de rede pode ter vários endereços IP chamados álias.

NOTA: álias são um recurso de compatibilidade

Esses supostos álias ou rótulos funcionam apenas com IPv4. Com IPv6, eles serão ignorados. O uso das interfaces de rede `iproute2` pode ter um ou mais endereços.

Ao usar o YaST para definir um álias para a sua placa de rede, faça o seguinte:

- 1 Selecione uma placa na lista de placas detectadas na guia *Visão Geral* do módulo de configuração de placa de rede do YaST e clique em *Editar*.
- 2 Na guia *Endereço > Endereços Adicionais*, clique em *Adicionar*.
- 3 Insira o *Nome de Apelido*, o *Endereço IP* e a *Máscara de Rede*. Não inclua o nome da interface no nome do álias.
- 4 Clique em *OK*.
- 5 Clique em *Avançar*.
- 6 Para ativar a configuração, clique em *OK*.

Mudando o nome de dispositivo e as regras de udev

É possível mudar o nome de dispositivo da placa de rede quando ela for usada. Também é possível determinar se a placa de rede deve ser identificada pelo udev usando o endereço (MAC) de hardware ou o ID do barramento. A segunda opção é preferível em grandes servidores para facilitar o intercâmbio das placas. Para definir essas opções com o YaST, faça o seguinte:

- 1 Selecione uma placa na lista de placas detectadas na guia *Visão Geral* do módulo *Configurações de Rede* do YaST e clique em *Editar*.
- 2 Vá até a guia *Hardware*. O nome de dispositivo atual é mostrado em *Regras do Udev*. Clique em *Mudar*.
- 3 Selecione se o udev deve identificar a placa por seu *Endereço MAC* ou *ID do Bus*. O endereço MAC e o ID do barramento atuais da placa são mostrados na caixa de diálogo.
- 4 Para mudar o nome de dispositivo, marque a opção *Mudar Nome do Dispositivo* e edite o nome.
- 5 Clique em *OK* e em *Avançar*.
- 6 Para ativar a configuração, clique em *OK*.

Mudando o driver do kernel da placa de rede

Para algumas placas de rede, pode haver vários drivers de kernel disponíveis. Se a placa já estiver configurada, o YaST permitirá que você selecione um driver de kernel em uma lista de drivers adequados disponíveis. Também é possível especificar opções para o driver de kernel. Para definir essas opções com o YaST, faça o seguinte:

- 1 Selecione uma placa na lista de placas detectadas na guia *Visão Geral* do módulo *Configurações de Rede* do YaST e clique em *Editar*.
- 2 Vá até a guia *Hardware*.
- 3 Selecione o driver de kernel a ser usado em *Nome de Módulo*. Digite qualquer opção para o driver selecionado em *Opções*, usando o formato *opção=valor*. Se forem usadas mais opções, elas deverão ser separadas por espaços.

- 4 Clique em *OK* e em *Avançar*.
- 5 Para ativar a configuração, clique em *OK*.

Ativando o dispositivo de rede

Se você usa o método tradicional com ifup, poderá configurar seu dispositivo para ser iniciado em uma das seguintes situações: durante o boot, na conexão a cabo, ao detectar a placa, manualmente ou nunca. Para mudar a inicialização do dispositivo, faça o seguinte:

- 1 No YaST, selecione uma placa na lista de placas detectadas em *Dispositivos de Rede > Configurações de Rede* e clique em *Editar*.
- 2 Na guia *Geral*, selecione a entrada desejada em *Ativação de Dispositivo*.

Escolha *Em Tempo de Boot* para iniciar o dispositivo durante o boot do sistema. Com a opção *Em Conexão Cabo*, a interface é monitorada quanto a qualquer conexão física existente. Com a opção *Em Hotplug*, a interface é definida tão logo fique disponível. Ela se assemelha à opção *Em Tempo de Boot*, a única diferença é que não ocorre nenhum erro quando a interface não está presente no momento do boot. Escolha *Manualmente* para controlar a interface manualmente com ifup. Escolha *Nunca* para não iniciar o dispositivo. A opção *Em NFSroot* se assemelha a *Em Tempo de Boot*, porém, a interface não é encerrada com o comando `rcnetwork stop`. Use-a se você estiver usando um sistema de arquivos raiz nfs ou iscsi.

- 3 Clique em *Avançar*.
- 4 Para ativar a configuração, clique em *OK*.

Geralmente, apenas o administrador do sistema pode ativar e desativar as interfaces de rede. Se você quiser que algum usuário seja capaz de ativar essa interface por KInternet, selecione *Habilitar Controle de Dispositivo para Usuário Não-root Via KInternet*.

Configurando o tamanho da unidade máxima de transferência

Você pode definir uma unidade máxima de transferência (MTU) para a interface. A MTU refere-se ao maior tamanho de pacote permitido, em bytes. Uma MTU maior proporciona melhor eficiência da largura de banda. No entanto, pacotes grandes podem

bloquear uma interface lenta por algum tempo, aumentando a latência dos pacotes seguintes.

- 1 No YaST, selecione uma placa na lista de placas detectadas em *Dispositivos de Rede > Configurações de Rede* e clique em *Editar*.
- 2 Na guia *Geral*, selecione a entrada desejada na lista *Definir MTU*.
- 3 Clique em *Avançar*.
- 4 Para ativar a configuração, clique em *OK*.

Configurando o firewall

Sem precisar inserir a configuração de firewall detalhada como descrito na Seção “Configuring the Firewall with YaST” (Capítulo 15, *Masquerading and Firewalls*, ↑*Security Guide (Guia de Segurança)*), você pode determinar a configuração de firewall básica para seu dispositivo como parte da configuração dele. Proceda da seguinte maneira:

- 1 Abra o módulo *Dispositivos de Rede > Configurações de Rede* do YaST. Na guia *Visão Geral*, selecione uma placa na lista de placas detectadas e clique em *Editar*.
- 2 Acesse a guia *Geral* da caixa de diálogo *Configurações de Rede*.
- 3 Determine a zona de firewall à qual sua interface deve ser designada. As seguintes opções estão disponíveis:

Firewall Desabilitado

Essa opção fica disponível apenas quando o firewall está desabilitado, sem entrar em execução. Use esta opção apenas se a sua máquina pertencer a uma rede maior protegida por um firewall externo.

Zona Atribuída Automaticamente

Essa opção fica disponível apenas quando o firewall está habilitado. O firewall está em execução e a interface é atribuída automaticamente a uma zona de firewall. Para uma interface como essa, será usada a zona que contiver a palavra-chave *any* ou a zona externa.

Zona Interna (Desprotegida)

O firewall está em execução, mas não assegura o uso obrigatório de nenhuma regra para proteger a interface. Use esta opção se a sua máquina pertencer a uma rede maior protegida por um firewall externo. Ela também é útil para as interfaces conectadas à rede interna, quando a máquina possui mais interfaces de rede.

Zona Desmilitarizada

Zona desmilitarizada é uma linha de defesa adicional situada na frente de uma rede interna e da Internet (hostil). Os hosts designados a essa zona podem ser acessados a partir da rede interna e a Internet, mas não podem acessar a rede interna.

Zona Externa

O firewall está em execução nessa interface e a protege totalmente contra outros tráfegos de rede presumivelmente hostis. Ela é a opção padrão.

4 Clique em *Avançar*.

5 Ative a configuração clicando em *OK*.

Configurando uma placa de rede não detectada

Sua placa pode ser detectada incorretamente. Nesse caso, ela não será incluída na lista de placas detectadas. Se você tiver certeza de que o sistema contém um driver para sua placa, poderá configurá-la manualmente. Se for possível, configure também tipos especiais de dispositivos de rede, como ponte, ligação, TUN ou TAP. Para configurar uma placa de rede não detectada (ou um dispositivo especial), faça o seguinte:

- 1** Na caixa de diálogo *Dispositivos de Rede > Configurações de Rede > Visão Geral* no YaST, clique em *Adicionar*.
- 2** Na caixa de diálogo *Hardware*, defina o *Tipo de Dispositivo* da interface entre as opções disponíveis e o *Nome de Configuração*. Se a placa de rede for um dispositivo PCMCIA ou USB, ative a respectiva caixa de seleção e saia dessa caixa de diálogo com *Avançar*. Caso contrário, você pode definir o *Nome de Módulo* do kernel para ser usado para a placa e as respectivas *Opções*, se necessário.

Em *Opções do Ethtool*, você pode definir as opções de `ethtool` usadas pelo `ifup` para a interface. Consulte a página de manual de `ethtool` para conhecer as opções disponíveis. Se a string opcional iniciar com um `-` (por exemplo `-K nome_da_interface rx on`), a segunda palavra da string será substituída pelo nome da interface atual. Caso contrário (por exemplo `autoneg off speed 10`), `ifup` precederá `-s nome_da_interface`.

- 3 Clique em *Avançar*.
- 4 Configure quaisquer opções que forem necessárias, como o endereço IP, a ativação do dispositivo ou a zona de firewall da interface nas guias *Geral*, *Endereço* e *Hardware*. Para obter mais informações sobre as opções de configuração, consulte “Mudando a configuração de uma placa de rede” (p 270).
- 5 Se você selecionou *Wireless* como o tipo de dispositivo da interface, configure a conexão wireless na próxima caixa de diálogo. Informações detalhadas sobre a configuração do dispositivo wireless estão disponíveis no Capítulo 17, *Rede local sem fio* (p 211).
- 6 Clique em *Avançar*.
- 7 Para ativar a nova configuração de rede, clique em *OK*.

Configurando o nome do host e o DNS

Se você não mudou a configuração da rede durante a instalação e a placa com fio já estava disponível, um nome de host foi gerado automaticamente para o seu computador e o DHCP foi ativado. O mesmo se aplica às informações de serviço de nomes de que o host necessita para se integrar a um ambiente de rede. Se o DHCP for usado para a configuração de endereços de rede, a lista de servidores de nomes de domínio será preenchida automaticamente com os dados adequados. Se uma configuração estática for preferencial, defina esses valores manualmente.

Para mudar o nome do seu computador e ajustar a lista de pesquisa do servidor de nomes, faça o seguinte:

- 1 Vá até a guia *Configurações de Rede > Nome de Host/DNS* no módulo *Dispositivos de Rede* do YaST.

- 2 Digite o *Nome de Host* e, se necessário, o *Nome de Domínio*. O domínio é especialmente importante quando a máquina é um servidor de correio eletrônico. Observe que o nome de host é global e se aplica a todas as interfaces de rede definidas.

Se você estiver usando o DHCP para obter um endereço IP, o nome de host do seu computador será definido automaticamente pelo DHCP. Pode ser que você queira desabilitar esse comportamento ao conectar-se a outras redes, visto que elas podem atribuir nomes de host diferentes, e a mudança de nome de host em tempo de execução pode confundir a área de trabalho gráfica. Para desabilitar o uso do DHCP para obter um endereço IP, desmarque *Trocar Nome de Host via DHCP*.

Atribuir Nome de Host a IP de Loopback associa seu nome de host ao endereço IP 127.0.0.2 (loopback) em `/etc/hosts`. Trata-se de uma opção útil quando você deseja que o nome de host seja sempre resolvível, mesmo sem uma rede ativa.

- 3 Em *Modificar Configuração do DNS*, selecione o modo como a configuração do DNS (servidores de nomes, lista de pesquisa, o conteúdo do arquivo `/etc/resolv.conf`) é modificada.

Se a opção *Usar Política Padrão* for selecionada, a configuração será gerenciada pelo script `netconfig`, que funde os dados definidos estaticamente (com o YaST ou nos arquivos de configuração) com os dados obtidos dinamicamente (do cliente DHCP ou do NetworkManager). Essa política padrão é suficiente na maioria dos casos.

Se a opção *Apenas Manualmente* for selecionada, `netconfig` não terá permissão para modificar o arquivo `/etc/resolv.conf`. Entretanto, esse arquivo pode ser editado manualmente.

Se a opção *Política Personalizada* for selecionada, deverá ser especificada uma string de *Regra de Política Personalizada* definindo a política de fusão. A string consiste em uma lista de nomes de interface separados por vírgula, considerada como fonte válida de configurações. Além dos nomes completos de interface, também são permitidos curingas básicos para corresponder a várias interfaces. Por exemplo, `eth* ppp?` primeiramente encontrará todas as interfaces `eth`, depois, todas as interfaces de `ppp0` a `ppp9`. Existem dois valores de política

especiais que indicam como aplicar as configurações estáticas definidas no arquivo `/etc/sysconfig/network/config`:

STATIC

É preciso que haja a fusão das configurações estáticas com as configurações dinâmicas.

STATIC_FALLBACK

As configurações estáticas são usadas apenas quando não há nenhuma configuração dinâmica disponível.

Para obter mais informações, consulte `man 8 netconfig`.

- 4 Digite os *Servidores de Nome* e preencha a lista *Pesquisa de Domínio*. Servidores de nomes devem ser especificados por endereços IP, como 192.168.1.116, não por nomes de host. Os nomes especificados na guia *Pesquisa de Domínio* são nomes de domínio usados para resolver nomes de host sem um domínio especificado. Se for usada mais de uma *Pesquisa de Domínio*, separe os domínios por vírgulas ou espaços.
- 5 Para ativar a configuração, clique em *OK*.

Configurando o roteamento

Para que sua máquina se comunique com outras máquinas e redes, é necessário fornecer informações de roteamento para que o tráfego de rede siga o caminho correto. Se o DHCP for usado, essas informações serão fornecidas automaticamente. Se uma configuração estática for usada, esses dados deverão ser adicionados manualmente.

- 1 No YaST, vá até *Configurações de Rede > Roteamento*.
- 2 Digite o endereço IP do *Gateway Padrão* (IPv4 e IPv6, se necessário). O gateway padrão corresponde a todos os destinos possíveis, mas se houver qualquer outra entrada que corresponda ao endereço requerido, use-o em vez da rota padrão.
- 3 É possível digitar mais entradas na *Tabela de Roteamento*. Digite o endereço IP do *Destino*, o endereço IP do *Gateway* e a *Máscara de Rede*. Selecione o *Dispositivo* pelo qual será roteado o tráfego para a rede definida (o sinal de menos significa qualquer dispositivo). Para omitir qualquer um desses valores, use o

sinal de menos –. Para digitar um gateway padrão na tabela, use `padrão` no campo *Destino*.

NOTA

Se forem usadas mais rotas padrão, será possível especificar a opção métrica para determinar qual rota possui a prioridade mais alta. Para especificar a opção métrica, digite `metric número` em *Opções*. A rota com a métrica mais alta será usada como padrão. Se o dispositivo de rede for desconectado, sua rota será removida e o dispositivo seguinte será usado. Entretanto, o kernel atual não usa métrica no roteamento estático, apenas os daemons de roteamento, como `multipathd`, podem fazê-lo.

- 4 Se o sistema for um roteador, habilite a opção *Encaminhamento IP* nas *Configurações de Rede*.
- 5 Para ativar a configuração, clique em *OK*.

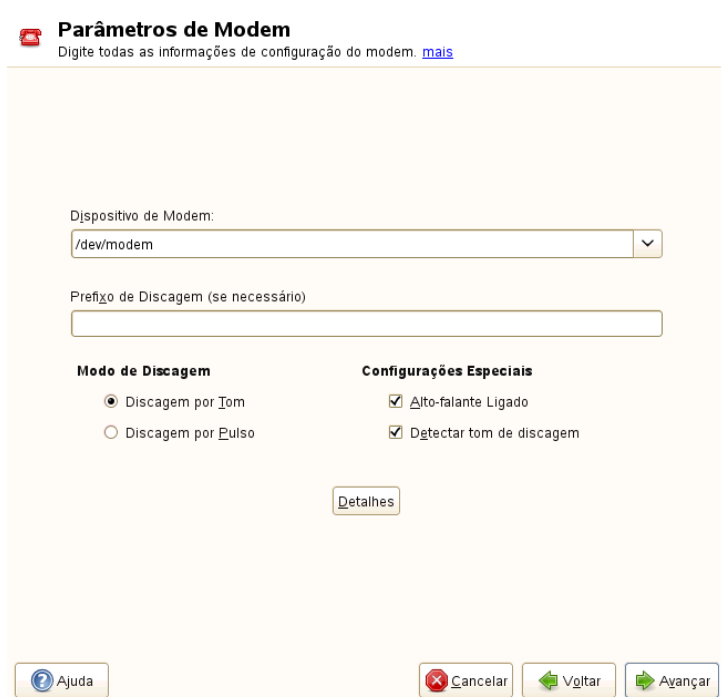
20.4.2 Modem

No Centro de Controle do YaST, acesse a configuração do modem em *Dispositivos de Rede > Modem*. Se o seu modem não foi detectado automaticamente, vá até a guia *Dispositivos de Modem* e abra a caixa de diálogo da configuração manual clicando em *Adicionar*. Digite a interface para a qual o modem está conectado em *Dispositivo de Modem*.

DICA: modems GPRS e CDMA

Configure os modems CDMA e GPRS suportados com o módulo *Modem* do YaST, do mesmo modo como são configurados os modems normais.

Figura 20.4 Configuração do modem



Parâmetros de Modem
Digite todas as informações de configuração do modem. [mais](#)

Dispositivo de Modem:

Prefixo de Discagem (se necessário)

Modo de Discagem

☒ Discagem por Tom
☐ Discagem por Pulso

Configurações Especiais

☒ Alto-falante Ligado
☒ Detectar tom de discagem

Se você estiver usando um PBX, talvez precise digitar um prefixo de discagem. Normalmente, é um zero. Consulte as instruções que acompanham o PBX para descobrir. Selecione também se usará a discagem por tom ou pulso, se o alto-falante estará ligado e se o modem aguardará até detectar um tom de discagem. A última opção não deve ser habilitada se o modem estiver conectado a um intercâmbio.

Em *Detalhes*, configure a taxa de transmissão e as strings de inicialização do modem. Somente mude essas configurações se seu modem não tiver sido detectado automaticamente ou se ele requerer configurações especiais para o funcionamento da transmissão de dados. Esse é basicamente o caso dos adaptadores do terminal ISDN. Saia dessa caixa de diálogo clicando em *OK*. Para delegar o controle do modem ao usuário comum, sem permissões de root, ative *Habilitar Controle de Dispositivo para Usuário Não-root Via KInternet*. Dessa forma, um usuário sem permissões de administrador poderá ativar ou desativar uma interface. Em *Dial Prefix Expressão Regular*, especifique uma expressão regular. O *Prefixo de Discagem* no KInternet, que pode ser modificado por um usuário normal, precisa corresponder a essa expressão

regular. Se esse campo for deixado vazio, o usuário não poderá configurar um *Prefixo de Discagem* diferente sem as permissões de administrador.

Na caixa de diálogo a seguir, selecione o ISP. Para escolher a partir de uma lista de ISPs predefinida operacional em seu país, selecione *País*. Ou então, clique em *Novo* para abrir uma caixa de diálogo em que você fornecerá os dados do seu ISP. Isso inclui um nome para a conexão de discagem e o ISP, assim como o login e a senha fornecidos pelo seu ISP. Habilite *Sempre Solicitar Senha* para que a senha seja solicitada sempre que você se conectar.

Na última caixa de diálogo, especifique as opções de conexão adicionais:

Discagem sob Demanda

Se você habilitar a *Discagem sob Demanda*, defina pelo menos um servidor de nomes. Use esse recurso apenas se a sua conexão de Internet for econômica, pois existem programas que solicitam dados da Internet periodicamente.

Modificar DNS Quando Conectado

Essa opção é habilitada por padrão, com o efeito de que o endereço do servidor de nomes é atualizado sempre que você se conectar à Internet.

Receber DNS Automaticamente

Se o provedor não transmitir seu servidor de nomes de domínio após a conexão, desabilite essa opção e digite os dados do DNS manualmente.

Reconectar Automaticamente

Se essa opção estiver habilitada, a conexão será restabelecida automaticamente após uma falha.

Ignorar Prompts

Essa opção desabilita a detecção de quaisquer prompts do servidor de discagem. Se a conexão for lenta ou não funcionar, tente essa opção.

Interface Externa do Firewall

Selecionar essa opção ativa o firewall e define a interface como externa. Desse modo, você fica protegido contra ataques externos enquanto durar a sua conexão de Internet.

Tempo Ocioso (segundos)

Com essa opção, especifique um período de inatividade da rede depois do qual o modem se desconectará automaticamente.

Detalhes IP

Essa opção abre a caixa de diálogo de configuração de endereço. Se o ISP não designar um endereço IP dinâmico ao host, desabilite *Endereço IP Dinâmico* e, depois, digite o endereço IP local do host e o endereço IP remoto. Peça essa informação ao ISP. Habilite *Rota Padrão* e feche a caixa de diálogo, selecionando *OK*.

Selecionando *Avançar*, você retorna à caixa de diálogo original, que exibirá um resumo da configuração do modem. Feche essa caixa de diálogo com *OK*.

20.4.3 ISDN

Use esse módulo para configurar uma ou várias placas ISDN para o seu sistema. Se o YaST não tiver detectado a sua placa ISDN, clique em *Adicionar* na guia *Dispositivos ISDN* e selecione a placa manualmente. É possível haver várias Interfaces, mas diversos ISPs podem ser configurados para uma única interface. Nas caixas de diálogo subseqüentes, configure as opções de ISDN necessárias para o funcionamento adequado da placa.

Figura 20.5 Configuração ISDN

Configuração de Nível Baixo RDSI (ISDN) para contrcontr0
Se você tem uma placa ISA antiga, você pode informar valores para a porta de IO ou endereço de memória e interrupç... [mais](#)

Informação de Placa ISDN
Fornecedor: Eicon Networks
Placa ISDN: Diva Piccola

Driver:
HISax driver

Protocolo ISDN
☒ Euro-ISDN (EDSS1)
☐ 1TR6
☐ Linha Dedicada
☐ NI1

País C: Alemanha
Código: +49
Código de Área:
Prefixo de Discagem:

☒ Iniciar Registro ISDN

Ativar dispositivo:
Em tempo de Boot

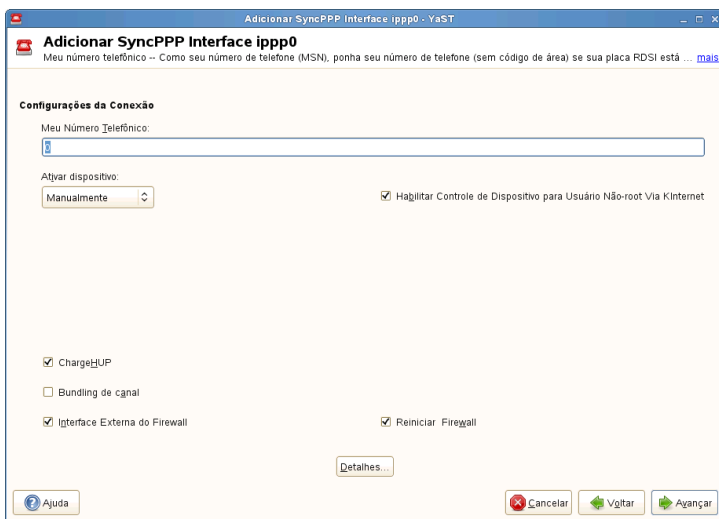
Ajuda Cancelar Voltar OK

Na caixa de diálogo a seguir, mostrada na Figura 20.5, “Configuração ISDN” (p 283), selecione o protocolo a ser usado. O padrão é *Euro-ISDN (EDSSI)*, mas para intercâmbios mais antigos ou maiores, selecione *1TR6*. Se você estiver nos E.U.A., selecione *NII*. Selecione seu país no campo relevante. O código de país correspondente aparecerá no campo próximo a ele. Por fim, forneça seu *Código de Área* e o *Prefixo de Discagem*, se necessário. Se você não quiser registrar todo o seu tráfego ISDN, desmarque a opção *Iniciar Registro ISDN*.

Ativar Dispositivo define como a interface ISDN deve ser iniciada: *Em tempo de Boot* faz o driver ISDN ser inicializado a cada boot do sistema. *Manualmente* exige que você carregue o driver ISDN como root com o comando `rcisdn start`. *Em Hotplug*, usado para dispositivos PCMCIA ou USB, carrega o driver depois que o dispositivo é conectado. Ao concluir essas configurações, selecione *OK*.

Na caixa de diálogo a seguir, especifique o tipo de interface para a placa ISDN e adicione ISPs a uma interface existente. As interfaces podem ser do tipo *SyncPPP* ou *RawIP*, mas a maioria dos ISPs opera no modo *SyncPPP*, descrito abaixo.

Figura 20.6 Configuração da interface ISDN



O número a ser digitado para *Meu Número Telefônico* dependerá da sua configuração específica:

Placa ISDN conectada diretamente à saída do fone

Uma linha ISDN padrão fornece três números telefônicos (chamados MSNs ou multiple subscriber numbers). Se o assinante pediu mais números, poderá ter até 10. Um desses MSNs precisa ser digitado aqui, mas sem o código de área. Se você digitar o número errado, o operador de fone retornará automaticamente ao primeiro MSN designado à sua linha ISDN.

Placa ISDN conectada a um PBX

Novamente, a configuração poderá variar de acordo com o equipamento instalado:

1. PBX menores, criados para fins domésticos, normalmente usam o protocolo Euro-ISDN (EDSS1) para chamadas internas. Esses intercâmbios possuem um barramento S0 interno e usam números internos para o equipamento conectado a eles.

Use um dos números internos como o seu MSN. Você deveria usar, pelo menos, um dos MSNs de intercâmbio habilitados para discagem direta para fora. Se não funcionar, tente um único zero. Para obter mais informações, consulte a documentação fornecida com a central telefônica.

2. Centrais telefônicas maiores, criadas para empresas, normalmente usam o protocolo 1TR6 para chamadas internas. Seus MSNs são chamados EAZ e, geralmente, correspondem ao número de discagem direta. Para a configuração no Linux, deverá ser suficiente digitar o último dígito de EAZ. Como última opção, tente cada um dos dígitos de 1 a 9.

Para que a conexão seja encerrada pouco antes de terminar a próxima unidade de carga, habilite *ChargeHUP*. Entretanto, lembre-se de que talvez não funcione com todos os ISPs. Você também pode habilitar o agrupamento de canais (multilink PPP) selecionando a opção correspondente. Por fim, você pode habilitar o firewall para o link selecionando *Interface Externa do Firewall* e *Reiniciar Firewall*. Para habilitar o usuário comum, sem permissões de administrador, a ativar ou desativar a interface, selecione *Habilitar Controle de Dispositivo para Usuário Não-root Via KInternet*.

Detalhes abre uma caixa de diálogo em que se implementa esquemas de conexão mais complexos, não relevantes para usuários domésticos comuns. Saia da caixa de diálogo *Detalhes* selecionando *OK*.

Na caixa de diálogo seguinte, ajuste as configurações de endereços IP. Se o provedor não tiver fornecido um IP estático, selecione *Endereço IP Dinâmico*. Caso contrário, use os campos fornecidos para digitar o endereço IP local e o remoto do seu host, de

acordo com as especificações do ISP. Se a interface for a rota padrão para a Internet, selecione *Rota Padrão*. Cada host só pode ter uma interface configurada como a rota padrão. Saia dessa caixa de diálogo selecionando *Avançar*.

A caixa de diálogo a seguir permite que você defina seu país e selecione um ISP. Os ISPs incluídos na lista são apenas provedores do tipo chamada-por-chamada. Se seu ISP não estiver na lista, selecione *Novo*. A caixa de diálogo *Parâmetros do Provedor* será aberta para que você digite todos os detalhes do seu ISP. Ao digitar o número telefônico, não inclua espaços vazios nem vírgulas entre os dígitos. Por fim, digite seu login e senha, conforme fornecido pelo ISP. Ao terminar, selecione *Avançar*.

Para usar *Discagem sob Demanda* em uma estação de trabalho independente, especifique também o servidor de nomes (servidor DNS). A maioria dos ISPs suporta DNS dinâmico, o que significa que o endereço IP de um servidor de nomes é enviado pelo ISP toda vez que você se conecta. Entretanto, para uma única estação de trabalho, é preciso fornecer um endereço marcador, como 192.168.22.99. Se o ISP não suportar um DNS dinâmico, especifique os endereços IP do servidor de nomes do ISP. Se desejar, especifique um tempo de espera para a conexão — o período de inatividade da rede (em segundos) após o qual a conexão deve ser automaticamente encerrada. Confirme as configurações com *Avançar*. O YaST exibe um resumo das interfaces configuradas. Para ativar essas configurações, selecione *OK*.

20.4.4 Modem a cabo

Em alguns países, é comum acessar a Internet por rede de TV a cabo. O assinante de TV a cabo normalmente recebe um modem, que é conectado à saída do cabo da TV em uma ponta e à placa de rede do computador na outra (usando um cabo de par trançado 10Base-TG). O modem a cabo então fornece uma conexão dedicada à Internet com um endereço IP fixo.

Dependendo as instruções fornecidas pelo seu ISP, ao configurar a placa de rede, selecione *Endereço Dinâmico* ou *Endereço IP Atribuído Estaticamente*. A maioria dos provedores usa atualmente o DHCP. Um endereço IP estático frequentemente vem como parte de uma conta comercial especial.

Para obter mais informações sobre a configuração de modems de cabo, leia o artigo Support Database (Banco de dados de suporte), disponível online em http://en.opensuse.org/SDB:Setting_Up_an_Internet_Connection_via_Cable_Modem_with_SuSE_Linux_8.0_or_Higher.

20.4.5 DSL

Para configurar o dispositivo DSL, selecione o módulo *DSL* na seção *Dispositivos de Rede* do YaST. Esse módulo do YaST consiste em várias caixas de diálogo nas quais são definidos os parâmetros de links DSL com base em um dos seguintes protocolos:

- PPPoE (PPP sobre Ethernet)
- PPPoATM (PPP sobre ATM)
- CAPI para ADSL (Placas Fritz)
- PPTP (Point-to-Point Tunneling Protocol) — Áustria

Na guia *Dispositivos DSL* da caixa de diálogo *Resumo de Configuração DSL*, há uma lista de dispositivos DSL instalados. Para mudar a configuração de um dispositivo DSL, selecione-o na lista e clique em *Editar*. Se você clicar em *Adicionar*, poderá configurar manualmente um novo dispositivo DSL.

A configuração de uma conexão DSL baseada em PPPoE ou PPTP exige que a placa de rede correspondente esteja configurada de forma correta. Se isso ainda não foi feito, primeiro configure a placa, selecionando *Configurar Placas de Rede* (consulte a Seção 20.4.1, “Configurando a placa de rede com o YaST” (p 267)). No caso de um link DSL, os endereços podem ser atribuídos automaticamente, mas não via DHCP, e é por isso que você não deve habilitar a opção *Endereço Dinâmico*. Em vez disso, digite um endereço estático simulado para a interface, como 192.168.22.1. Em *Máscara de Sub-rede*, digite 255.255.255.0. Se estiver configurando uma estação de trabalho independente, deixe a opção *Gateway Padrão* vazia.

DICA

Os valores em *Endereço IP* e *Máscara de Sub-rede* são apenas marcadores. Eles são necessários apenas para inicializar a placa de rede e não representam o link DSL.

Na primeira caixa de diálogo de configuração do DSL (consulte a Figura 20.7, “Configuração DSL” (p 288)), selecione o *Modo PPP* e a *Placa Ethernet* à qual se conecta o modem DSL (na maioria dos casos é `eth0`). Em seguida, use *Ativar Dispositivo* para especificar se o link DSL deve ser estabelecido durante o processo de boot. Clique em *Habilitar Controle de Dispositivo para Usuário Não-root Via KInternet*

para autorizar o usuário comum, sem permissões de root, a ativar ou desativar a interface com KInternet.

Na caixa de diálogo seguinte, selecione o seu país e escolha um dos ISPs que operam na região. Os detalhes de quaisquer caixas de diálogo subsequentes da configuração DSL dependem das opções configuradas até agora. É por essa razão que eles são apenas rapidamente mencionados nos parágrafos a seguir. Para obter detalhes sobre as opções disponíveis, leia a ajuda detalhada disponível nas caixas de diálogo.

Figura 20.7 Configuração DSL

Configuração DSL
Aqui, configure os dados mais importantes para conexão DSL. [mais](#)

Configurações da Conexão DSL

Modo PPP:
PPP sobre Ethernet

Configurações Dependentes de Modo PPP

VPI/VCI:

Placa Ethernet
79c970 [PCnet32 LANCE]
Placa de Rede - Endereço DHCP
Mudar Dispositivo
Configurar placa de rede

Nome ou Endereço IP do Servidor:
10.0.0.138

Ativar dispositivo:
Manualmente

☒ Habilitar Controle de Dispositivo para Usuário Não-root Via KInternet

Ajuda Cancelar Voltar Avançar

Para usar *Discagem sob Demanda* em uma estação de trabalho independente, especifique também o servidor de nomes (servidor DNS). A maioria dos ISPs suporta DNS dinâmico — o endereço IP de um servidor de nomes é enviado pelo ISP toda vez que você se conecta. Entretanto, para uma única estação de trabalho, é preciso fornecer um endereço marcador, como 192.168.22.99. Se o ISP não suportar um DNS dinâmico, especifique o endereço IP do servidor de nomes fornecido pelo ISP.

Tempo Ocioso (em segundos) define um período de inatividade da rede depois do qual a conexão é encerrada automaticamente. Um valor de tempo de espera razoável fica entre 60 e 300 segundos. Se a opção *Discagem sob Demanda* estiver desabilitada, talvez seja útil configurar o tempo de espera como zero para evitar um desligamento automático.

A configuração do T-DSL é muito parecida com a do DSL. Basta selecionar *T-Online* como seu provedor e o YaST abrirá a caixa de diálogo de configuração do T-DSL. Nessa caixa de diálogo, forneça algumas informações adicionais necessárias para T-DSL: o ID da linha, o T-Online number, o código do usuário e a sua senha. Tudo isso deve estar incluído nas informações que você recebeu após se inscrever no T-DSL.

20.5 NetworkManager

O NetworkManager é a solução ideal para laptops e outros computadores portáteis. Com o NetworkManager, não é necessário preocupar-se em configurar interfaces de rede e alternar entre redes quando você estiver em trânsito.

20.5.1 NetworkManager e ifup

Entretanto, como o NetworkManager não é uma solução adequada para todos os casos, você pode ainda escolher entre o método tradicional de gerenciamento de conexões de rede (ifup) e o NetworkManager. Se você quiser gerenciar a sua conexão de rede com o NetworkManager, habilite o NetworkManager no módulo Configurações de Rede do YaST, conforme descrito na Seção 23.2, “Habilitando o NetworkManager” (p 324) e configure suas conexões de rede com o NetworkManager. Para obter uma lista de casos de uso e uma descrição detalhada sobre como configurar e usar o NetworkManager, consulte o Capítulo 23, *Usando o NetworkManager* (p 323).

Algumas diferenças entre o ifup e o NetworkManager:

Privilégios do `root`

Se você usa o NetworkManager para configurar a rede, poderá alternar, parar ou iniciar com facilidade a conexão de rede, a qualquer momento, de dentro do ambiente de área de trabalho usando um applet. O NetworkManager também permite mudar e configurar conexões de placa wireless sem exigir privilégios de `root`.

Por esse motivo, o NetworkManager é a solução ideal para uma estação de trabalho móvel.

A configuração tradicional com o ifup também oferece algumas maneiras de alternar, parar ou iniciar a conexão com ou sem a intervenção do usuário, como em dispositivos gerenciados pelo usuário. No entanto, esses recursos sempre exigem privilégios do `root` para mudar ou configurar um dispositivo de rede. Isso normalmente é um problema para a computação móvel, na qual não é possível pré-configurar todas as possibilidades de conexão.

Tipos de conexões de rede

Tanto a configuração tradicional como o NetworkManager podem gerenciar conexões de rede com uma rede wireless (com acesso WEP, WPA-PSK e WPA-Enterprise), redes discada e redes com fio usando DHCP e configuração estática. Eles também oferecem suporte à conexão por meio de VPN.

O NetworkManager tenta manter o computador conectado o tempo todo usando a melhor conexão disponível. Se o cabo da rede for desconectado por acidente, ele tentará reconectar. Ele é capaz de localizar a rede que tiver a melhor intensidade de sinal na lista de conexões wireless e usá-la automaticamente para uma conexão. Para obter a mesma funcionalidade com o ifup, é necessário um grande esforço de configuração.

20.5.2 Funcionalidade e arquivos de configuração do NetworkManager

As configurações de conexão de rede individual criadas com o NetworkManager são armazenadas em perfis de configuração. As conexões de *system* configuradas com o NetworkManager ou o YaST encontram-se em `/etc/sysconfig/network/ifcfg-*`. Qualquer conexão definida pelo usuário é armazenada no GConf, para o GNOME, ou em `$HOME/.kde4/share/apps/networkmanagement/*`, para o KDE.

Caso não haja nenhum perfil configurado, o NetworkManager automaticamente cria um e o nomeia como `Auto $INTERFACE-NAME`. Isso é uma tentativa de fazer funcionar sem qualquer configuração para tantos casos quanto forem possíveis (com segurança). Se os perfis criados automaticamente não atenderem às suas necessidades, use as caixas de diálogo de configuração da conexão de rede, fornecidas pelo KDE ou

pelo GNOME, para modificá-los conforme desejado. Para obter maiores informações, consulte a Seção 23.3, “Configurando conexões de rede” (p 325).

20.5.3 Controlando e bloqueando os recursos do NetworkManager

Nas máquinas de administração central, determinados recursos do NetworkManager poderão ser controlados ou desabilitados com o PolicyKit, por exemplo, se um usuário tiver permissão para modificar as conexões definidas pelo administrador ou para definir suas próprias configurações de rede. Para ver ou mudar as respectivas políticas do NetworkManager, inicie a ferramenta gráfica *Autorizações* para o PolicyKit. Na árvore do lado esquerdo, elas se encontram abaixo da entrada *network-manager-settings*. Para obter uma introdução ao PolicyKit e detalhes sobre como usá-lo, consulte o Capítulo 9, *PolicyKit* (↑*Security Guide (Guia de Segurança)*).

20.6 Configurando uma conexão de rede manualmente

A configuração manual do software de rede deve ser sempre a última alternativa. É recomendável usar o YaST. Entretanto, essas informações de base sobre a configuração de rede também podem ajudar você na utilização do YaST.

Quando o kernel detecta uma placa de rede e cria uma interface de rede correspondente, ele atribui um nome de dispositivo de acordo com a ordem de descoberta de dispositivos ou a ordem de carregamento dos módulos de kernel. Os nomes de dispositivos padrão de kernel são previsíveis apenas em ambientes de hardware muito simples ou altamente controlados. Os sistemas que permitem adicionar ou remover hardware durante o tempo de execução ou que suportam a configuração automática de dispositivos não podem contar com nomes estáveis de dispositivos de rede atribuídos pelo kernel no decorrer das reinicializações.

Entretanto, todas as ferramentas de configuração do sistema contam com nomes de interface persistentes. O problema é solucionado por udev. O gerador de rede persistente udev (`/lib/udev/rules.d/75-persistent-net-generator.rules`) gera uma regra que corresponde ao hardware (usando seu endereço de hardware por padrão) e atribui uma interface exclusiva persistente ao hardware. O banco de dados

de interfaces de rede do udev fica armazenado no arquivo `/etc/udev/rules.d/70-persistent-net.rules`. Todas as linhas do arquivo descrevem uma interface de rede e especifique seu nome persistente. Os administradores de sistema podem mudar os nomes atribuídos editando as entradas `NAME=""`. As regras persistentes também podem ser modificadas por meio do YaST.

A Tabela 20.5, “Scripts de configuração de rede manual” (p 292) resume os scripts mais importantes envolvidos na configuração de rede.

Tabela 20.5 *Scripts de configuração de rede manual*

Comando	Função
<code>ifup</code> , <code>ifdown</code> , <code>ifstatus</code>	Os scripts <code>if</code> iniciam ou param interfaces de rede ou retornam o status da interface especificada. Para obter mais informações, consulte a página de manual <code>ifup</code> .
<code>rcnetwork</code>	O script <code>rcnetwork</code> pode ser usado para iniciar, parar ou reiniciar todas as interfaces de rede (ou apenas uma específica). Use <code>rcnetwork stop</code> para parar, <code>rcnetwork start</code> para iniciar e <code>rcnetwork restart</code> para reiniciar interfaces de rede. Se você quiser parar, iniciar ou reiniciar apenas uma interface, use o comando seguido pelo nome da interface, por exemplo, <code>rcnetwork restart eth0</code> . O comando <code>rcnetwork status</code> exibe o estado das interfaces, seus endereços IP e indica se há um cliente DHCP em execução. Com <code>rcnetwork stop-all-dhcp-clients</code> e <code>rcnetwork restart-all-dhcp-clients</code> , você pode parar ou reiniciar clientes DHCP em execução nas interfaces de rede.

Para obter mais informações sobre o udev e os nomes de dispositivo persistentes, consulte o Capítulo 13, *Gerenciamento de dispositivo de kernel dinâmico com udev* (p 163).

20.6.1 Arquivos de configuração

Esta seção fornece uma visão geral dos arquivos de configuração de rede e explica sua finalidade e formato usado.

/etc/sysconfig/network/ifcfg-*

Esses arquivos contêm as configurações de interfaces de rede. Eles incluem informações, como o modo de início e o endereço IP. Os parâmetros possíveis são descritos na página de manual de `ifup`. Além disso, quase todas as variáveis dos arquivos `dhcp`, `wireless` e `config` poderão ser usadas nos arquivos `ifcfg-*` se uma configuração geral for usada para apenas uma interface.

Para saber sobre o `ifcfg.template`, consulte “`/etc/sysconfig/network/config`, `/etc/sysconfig/network/dhcp` e `/etc/sysconfig/network/wireless`” (p 293).

/etc/sysconfig/network/config, /etc/sysconfig/network/dhcp e /etc/sysconfig/network/wireless

O arquivo `config` contém configurações gerais para o comportamento de `ifup`, `ifdown` e `ifstatus`. `dhcp` contém configurações para DHCP e `wireless` para placas de rede local wireless. Nos três arquivos de configuração, as variáveis estão em forma de comentário. Algumas das variáveis de `/etc/sysconfig/network/config` também podem ser usadas nos arquivos `ifcfg-*`, nos quais recebem prioridade mais alta. O arquivo `/etc/sysconfig/network/ifcfg.template` lista as variáveis que podem ser especificadas para cada interface. Entretanto, a maioria das variáveis de `/etc/sysconfig/network/config` são globais, não podendo ser anuladas em `ifcfg-files`. Por exemplo, as variáveis `NETWORKMANAGER` ou `NETCONFIG_*` são globais.

/etc/sysconfig/network/routes e /etc/sysconfig/network/ifroute-*

O roteamento estático dos pacotes TCP/IP é determinado aqui. Todas as rotas estáticas requeridas pelas várias tarefas do sistema podem ser digitadas no arquivo `/etc/sysconfig/network/routes` file: rotas para um host, rotas para um host via gateway e rotas para uma rede. Para cada interface que precisa de roteamento individual, defina um arquivo de configuração adicional: `/etc/sysconfig/network/ifroute-*`. Substitua `*` pelo nome da interface. As entradas nos arquivos de configuração de roteamento terão esta aparência:

# Destination	Dummy/Gateway	Netmask	Device
#			
127.0.0.0	0.0.0.0	255.255.255.0	lo
204.127.235.0	0.0.0.0	255.255.255.0	eth0
default	204.127.235.41	0.0.0.0	eth0
207.68.156.51	207.68.145.45	255.255.255.255	eth1
192.168.0.0	207.68.156.51	255.255.0.0	eth1

O destino da rota está na primeira coluna. Essa coluna pode conter o endereço IP de uma rede ou host ou, no caso de servidores de nomes *acessíveis*, a rede ou o nome completo do host.

A segunda coluna contém o gateway padrão ou um gateway por meio do qual um host ou uma rede podem ser acessados. A terceira coluna contém a máscara de rede para redes ou hosts atrás de um gateway. Por exemplo, a máscara em `255.255.255.255` para um host atrás de um gateway.

A quarta coluna só é relevante para redes conectadas ao host local, como loopback, Ethernet, ISDN, PPP e dispositivo simulado. O nome do dispositivo deve ser digitado aqui.

Uma quinta coluna (opcional) pode ser usada para especificar o tipo de uma rota. As colunas desnecessárias devem conter um sinal de subtração – para garantir que o analisador interpretará o comando corretamente. Para obter mais detalhes, consulte a página de manual `routes(5)`.

/etc/resolv.conf

O domínio ao qual o host pertence é especificado neste arquivo (palavra-chave `search`). Também está listado o status do endereço do servidor de nomes para acesso (palavra-

chave `nameserver`). Vários nomes de domínio podem ser especificados no arquivo. Durante a resolução de um nome incompleto, uma tentativa de gerar um nome será feita, anexando as entradas de pesquisa individuais. Vários servidores de nomes podem ser especificados em várias linhas, cada uma delas começando com `nameserver`. Comentários são precedidos pelo sinal `#`. O Exemplo 20.5, “`/etc/resolv.conf`” (p 295) exemplifica como pode ser a aparência do `/etc/resolv.conf`.

Entretanto, o `/etc/resolv.conf` não deve ser editado manualmente. Isso porque ele é gerado pelo script `netconfig`. Para definir a configuração do DNS estático sem usar o YaST, edite manualmente as variáveis apropriadas no arquivo `/etc/sysconfig/network/config: NETCONFIG_DNS_STATIC_SEARCHLIST` (lista de nomes de domínio DNS usados na pesquisa de nome de host), `NETCONFIG_DNS_STATIC_SERVERS` (lista de endereços IP do servidor de nomes a usar na pesquisa de nome de host), `NETCONFIG_DNS_FORWARDER` (define o nome do encaminhador de DNS que precisa ser configurado). Para desabilitar a configuração do DNS usando o `netconfig`, defina `NETCONFIG_DNS_POLICY= ''`. Para obter mais informações sobre o `netconfig`, consulte `man 8 netconfig`.

Exemplo 20.5 `/etc/resolv.conf`

```
# Our domain
search example.com
#
# We use dns.example.com (192.168.1.116) as nameserver
nameserver 192.168.1.116
```

/sbin/netconfig

O `netconfig` é uma ferramenta modular destinada a gerenciar configurações de rede adicionais. Ele funde as configurações definidas estaticamente com as configurações fornecidas pelos mecanismos de configuração automática, como `dhcp` ou `ppp`, de acordo com uma política predefinida. As mudanças necessárias são aplicadas ao sistema chamando-se os módulos do `netconfig` responsáveis pela modificação de um arquivo de configuração e pela reinicialização de um serviço ou uma ação semelhante.

O `netconfig` reconhece três ações principais. Os comandos `netconfig modify` e `netconfig remove` são usados por daemons, como `dhcp` ou `ppp`, para fornecer ou remover configurações do `netconfig`. Apenas o comando `netconfig update` está disponível para o usuário:

modify

O comando `netconfig modify` modifica as configurações dinâmicas específicas de interface e serviço, além de atualizar a configuração da rede. O `netconfig` lê as configurações da entrada padrão ou de um arquivo especificado pela opção `--lease-file nome_de_arquivo` e as armazena internamente até a próxima reinicialização do sistema (ou a próxima ação `modify` ou `remove`). As configurações que já existirem para a mesma combinação de interface e serviço serão sobregravadas. A interface é especificada pelo parâmetro `-i nome_da_interface`. O serviço é especificado pelo parâmetro `-s nome_do_serviço`.

remove

O comando `netconfig remove` remove as configurações dinâmicas fornecidas por uma ação modificadora para a combinação de interface e serviço especificada, além de atualizar a configuração da rede. A interface é especificada pelo parâmetro `-i nome_da_interface`. O serviço é especificado pelo parâmetro `-s nome_do_serviço`.

update

O comando `netconfig update` atualiza a configuração da rede usando as configurações atuais. Isso é útil quando a política ou a configuração estática é mudada. Use o parâmetro `-m tipo_de_módulo` se desejar atualizar apenas um serviço especificado (`dns`, `nis` ou `ntp`).

A política do `netconfig` e as configurações estáticas são definidas manualmente ou por meio do YaST no arquivo `/etc/sysconfig/network/config`. As configurações dinâmicas fornecidas pelas ferramentas de configuração automática, como `dhcp` ou `ppp`, são entregues diretamente por essas ferramentas com as ações `netconfig modify` e `netconfig remove`. O `NetworkManager` também usa as ações `netconfig modify` e `netconfig remove`. Quando o `NetworkManager` é habilitado, o `netconfig` (no modo de política `auto`) usa apenas as configurações do `NetworkManager`, ignorando as configurações de qualquer outra interface configurada pelo método tradicional com `ifup`. Se o `NetworkManager` não fornecer nenhuma configuração, as configurações estáticas serão usadas como fallback. Não há suporte para a utilização mista do `NetworkManager` nem para o método tradicional com `ifup`.

Para obter mais informações sobre o `netconfig`, consulte `man 8 netconfig`.

/etc/hosts

Nesse arquivo, mostrado no Exemplo 20.6, “/etc/hosts” (p 297), os endereços IP são designados a nomes de host. Se nenhum servidor de nomes for implementado, todos os hosts nos quais uma conexão IP for configurada precisarão ser listados aqui. Para cada host, digite uma linha no arquivo com o endereço IP, o nome completo do host e o nome de host. O endereço IP precisa estar no início da linha e as entradas separadas por espaços vazios e guias. Comentários são sempre precedidos pelo sinal #.

Exemplo 20.6 /etc/hosts

```
127.0.0.1 localhost
192.168.2.100 jupiter.example.com jupiter
192.168.2.101 venus.example.com venus
```

/etc/networks

Aqui, os nomes de rede são convertidos em endereços de rede. O formato é semelhante ao do arquivo `hosts`, exceto que os nomes de rede precedem os endereços. Consulte o Exemplo 20.7, “/etc/networks” (p 297).

Exemplo 20.7 /etc/networks

```
loopback      127.0.0.0
localnet      192.168.0.0
```

/etc/host.conf

A resolução de nomes (tradução de nomes de host e de rede pela biblioteca do *resolver*) é controlada por esse arquivo. Esse arquivo é usado somente para programas vinculados a `libc4` ou `libc5`. Para programas `glibc` atuais, consulte as configurações em `/etc/nsswitch.conf`. Um parâmetro precisa estar sempre independente em sua própria linha. Comentários são precedidos pelo sinal #. A Tabela 20.6, “Parâmetros para /etc/host.conf” (p 298) mostra os parâmetros disponíveis. Uma amostra de `/etc/host.conf` é mostrada no Exemplo 20.8, “/etc/host.conf” (p 298).

Tabela 20.6 *Parâmetros para /etc/host.conf*

<code>order hosts, bind</code>	<p>Especifica em que ordem os serviços são acessados para a resolução de nomes. Os argumentos disponíveis são (separados por espaços vazios ou vírgulas):</p> <p><i>hosts</i>: pesquisa o arquivo <code>/etc/hosts</code></p> <p><i>bind</i>: acessa um servidor de nomes</p> <p><i>nis</i>: usa o NIS</p>
<code>multi on/off</code>	<p>Define se um host digitado em <code>/etc/hosts</code> pode ter vários endereços IP.</p>
<code>nospoof on</code> <code>spoofalert on/off</code>	<p>Esses parâmetros influenciam o <i>spoof</i> do servidor de nomes, mas não exercem qualquer influência na configuração da rede.</p>
<code>trim domainname</code>	<p>O nome de domínio especificado é separado do nome de host depois da resolução do nome de host (desde que o nome de host inclua o nome de domínio). Essa opção é útil apenas quando os nomes do domínio local estão no arquivo <code>/etc/hosts</code>, mas ainda devem ser reconhecidos com os nomes de domínio anexados.</p>

Exemplo 20.8 */etc/host.conf*

```
# We have named running
order hosts bind
# Allow multiple address
multi on
```

/etc/nsswitch.conf

O lançamento do GNU C Library 2.0 foi acompanhado pelo lançamento do NSS (Name Service Switch). Consulte a página de manual do `nsswitch.conf(5)` e *The GNU C Library Reference Manual* (Manual de Referência da Biblioteca GNU C) para obter mais detalhes.

A ordem das consultas é definida no arquivo `/etc/nsswitch.conf`. Uma amostra do `nsswitch.conf` é exibida em Exemplo 20.9, “`/etc/nsswitch.conf`” (p 299). Comentários são precedidos pelo sinal `#`. Nesse exemplo, a entrada no banco de dados `hosts` significa que uma solicitação foi enviada para `/etc/hosts` (arquivos) através do DNS.

Exemplo 20.9 */etc/nsswitch.conf*

```
passwd:      compat
group:       compat

hosts:       files dns
networks:    files dns

services:    db files
protocols:   db files

netgroup:    files
automount:   files nis
```

Os “bancos de dados” disponíveis em NSS estão listados na Tabela 20.7, “Bancos de dados disponíveis por `/etc/nsswitch.conf`” (p 299). Além disso, `automount`, `bootparams`, `netmasks` e `publickey` são aguardados para breve. As opções de configuração para bancos de dados NSS estão listadas na Tabela 20.8, “Opções de configuração para bancos de dados “NSS”” (p 300).

Tabela 20.7 *Bancos de dados disponíveis por `/etc/nsswitch.conf`*

<code>aliases</code>	Álias de correio implementados por <code>sendmail</code> ; consulte <code>man 5 aliases</code> .
<code>ethers</code>	Endereços de Ethernet.
<code>group</code>	Para grupos de usuários usados por <code>getgrent</code> . Consulte também a página de manual para <code>group</code> .
<code>hosts</code>	Para nomes de <code>hosts</code> e endereços IP, usados por <code>gethostbyname</code> e funções similares.
<code>netgroup</code>	Listas de usuários e <code>hosts</code> válidos na rede com a finalidade de controlar permissões de acesso, consulte a página de manual do <code>netgroup(5)</code> .

<code>networks</code>	Nomes e endereços de redes, usados por <code>getnetent</code> .
<code>passwd</code>	Senhas de usuários, usadas por <code>getpwent</code> ; consulte a página de manual do <code>passwd(5)</code> .
<code>protocols</code>	Protocolos de rede, usados por <code>getprotoent</code> ; consulte a página de manual do <code>protocols(5)</code> .
<code>rpc</code>	Nomes e endereços de RPC (Remote Procedure Call) usados por <code>getrpcbyname</code> e funções similares.
<code>services</code>	Serviços de rede, usados por <code>getservent</code> .
<code>shadow</code>	Senhas transitórias de usuários, usadas por <code>getspnam</code> ; consulte a página de manual do <code>shadow(5)</code> .

Tabela 20.8 *Opções de configuração para bancos de dados “NSS”*

<code>files</code>	arquivos de acesso direto, por exemplo, <code>/etc/aliases</code>
<code>db</code>	acesso através de um banco de dados
<code>nis, nisplus</code>	NIS, consulte também o Capítulo 3, <i>Using NIS</i> (<i>↑Security Guide (Guia de Segurança)</i>)
<code>dns</code>	só pode ser usada como extensão de <code>hosts</code> e <code>networks</code>
<code>compat</code>	só pode ser usada como extensão de <code>passwd</code> , <code>shadow</code> e <code>group</code>

/etc/nscd.conf

Esse arquivo é usado para configurar o `nscd` (name service cache daemon). Consulte as páginas de manual de `nscd(8)` e `nscd.conf(5)`. Por padrão, as entradas do sistema de `passwd` e `groups` são armazenadas em cache pelo `nscd`. Isso é importante para o desempenho de serviços de diretório, como NIS e LDAP, pois, caso contrário, a conexão de rede precisaria ser usada para cada acesso a nomes ou grupos. `hosts`

não é armazenado em cache por padrão, porque o mecanismo no `nscd` para armazenar hosts em cache impede o sistema local de confiar em verificações de pesquisa `forward` e `reverse`. Em vez de solicitar ao `nscd` para armazenar nomes em cache, configure um servidor DNS para armazenamento em cache.

Se o armazenamento em cache de `passwd` estiver ativado, normalmente levará quinze segundos para que um usuário local recentemente adicionado seja reconhecido. Reduza esse tempo de espera reiniciando o `nscd` com o comando `rcnscd restart`.

/etc/HOSTNAME

Contém o nome de host sem o nome de domínio anexado. Esse arquivo é lido por vários scripts durante o boot da máquina. Ele deve conter apenas uma linha (na qual o nome de host é definido).

20.6.2 Testando a configuração

Antes de gravar sua configuração nos arquivos de configuração, você pode testá-la. Para definir uma configuração de teste, use o comando `ip`. Para testar a conexão, use o comando `ping`. As antigas ferramentas de configuração `ifconfig` e `route` também estão disponíveis.

Os comandos `ip`, `ifconfig` e `route` mudam a configuração da rede diretamente sem gravá-la no arquivo de configuração. A menos que você insira a configuração nos arquivos de configuração corretos, a configuração de rede mudada será perdida na reinicialização.

Configurando uma interface de rede com ip

O `ip` é uma ferramenta destinada a mostrar e configurar roteamentos, dispositivos de rede, roteamentos de políticas e túneis.

O `ip` é uma ferramenta muito complexa. Sua sintaxe comum é `ip opções objeto comando`. Você pode trabalhar com os seguintes objetos:

`link`

Este objeto representa um dispositivo de rede.

address

Este objeto representa o endereço IP do dispositivo.

neighbour

Este objeto representa uma entrada de cache ARP ou NDISC.

route

Este objeto representa a entrada da tabela de roteamento.

rule

Este objeto representa uma regra no banco de dados de políticas de roteamento.

maddress

Este objeto representa um endereço multicast.

mroute

Este objeto representa uma entrada de cache de roteamento multicast.

tunnel

Este objeto representa um túnel sobre IP.

Se nenhum comando for fornecido, será usado o comando padrão (normalmente `list`).

Mude o estado de um dispositivo com o comando `ip link set nome_do_dispositivo comando`. Por exemplo, para desativar o dispositivo `eth0`, digite `ip link set eth0 down`. Para ativá-lo novamente, use `ip link set eth0 up`.

Após ativar um dispositivo, você poderá configurá-lo. Para definir o endereço IP, use `ip addr add endereço_ip + dev nome_do_dispositivo`. Por exemplo, para definir o endereço da interface `eth0` como `192.168.12.154/30` com o broadcast padrão (opção `brd`), digite `ip addr add 192.168.12.154/30 brd + dev eth0`.

Para ter uma conexão ativa, você também precisa configurar o gateway padrão. Para definir um gateway para o sistema, digite `ip route add endereço_ip_do_gateway`. Para traduzir um endereço IP para outro, use `nat: ip route add nat endereço_ip via outro_endereço_ip`.

Para exibir todos os dispositivos, use `ip link ls`. Para exibir apenas as interfaces em execução, use `ip link ls up`. Para imprimir as estatísticas de interface de um dispositivo, digite `ip -s link ls nome_do_dispositivo`. Para ver os endereços dos dispositivos, digite `ip addr`. Na saída do comando `ip addr`, você também pode encontrar informações sobre os endereços MAC dos dispositivos. Para mostrar todas as rotas, use `ip route show`.

Para obter mais informações sobre como usar o `ip`, digite `ip help` ou consulte a página de manual de `ip(8)`. A opção `help` também está disponível para todos os objetos `ip`. Se, por exemplo, você quiser ler a ajuda de `ip addr`, digite `ip addr help`. Encontre o manual da `ip` em `/usr/share/doc/packages/iproute2/ip-cref.pdf`.

Testando uma conexão com o comando ping

O comando `ping` é a ferramenta padrão para testar o funcionamento de uma conexão TCP/IP. Ele usa o protocolo ICMP para enviar um pequeno pacote de dados, o datagrama `ECHO_REQUEST`, para o host de destino, solicitando uma resposta imediata. Se isso funcionar, o `ping` exibirá uma mensagem que indica que o link da rede está basicamente funcionando.

O `ping` vai além de simplesmente testar a função da conexão entre dois computadores; ele também fornece algumas informações básicas sobre a qualidade da conexão. No Exemplo 20.10, “Saída do comando `ping`” (p 304), você pode ver um exemplo da saída do `ping`. A penúltima linha contém informações sobre o número de pacotes transmitidos, o número de pacotes perdidos e o tempo total da execução do `ping`.

Como destino, você pode usar um nome de host ou endereço IP, por exemplo, `ping example.com` ou `ping 192.168.3.100`. O programa enviará pacotes até que você pressione `Ctrl + C`.

Se você só precisar verificar a funcionalidade da conexão, poderá limitar o número dos pacotes com a opção `-c`. Por exemplo, para limitar o `ping` a três pacotes, digite `ping -c 3 example.com`.

Exemplo 20.10 Saída do comando `ping`

```
ping -c 3 example.com
PING example.com (192.168.3.100) 56(84) bytes of data.
64 bytes from example.com (192.168.3.100): icmp_seq=1 ttl=49 time=188 ms
64 bytes from example.com (192.168.3.100): icmp_seq=2 ttl=49 time=184 ms
64 bytes from example.com (192.168.3.100): icmp_seq=3 ttl=49 time=183 ms
--- example.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2007ms
rtt min/avg/max/mdev = 183.417/185.447/188.259/2.052 ms
```

O intervalo padrão entre dois pacotes é um segundo. Para mudar o intervalo, o `ping` fornece a opção `-i`. Por exemplo, para aumentar o intervalo de ping para dez segundos, digite `ping -i 10 example.com`.

Em um sistema com vários dispositivos de rede, às vezes é útil enviar o ping através de um endereço de interface específico. Para isso, use a opção `-I` com o nome do dispositivo selecionado, por exemplo, `ping -I wlan1 example.com`.

Para obter mais opções e informações sobre como usar o `ping`, digite `ping -h` ou consulte a página de manual de `ping` (8).

Configurando a rede com o `ifconfig`

`ifconfig` é uma ferramenta de rede tradicional. Ao contrário da `ip`, você pode usá-la somente para a configuração de interfaces. Se você quiser configurar o roteamento, use o comando `route`.

NOTA: `ifconfig` e `ip`

O programa `ifconfig` está obsoleto. Em vez disso, use `ip`.

Sem argumentos, o `ifconfig` exibe o status das interfaces atualmente ativas. Como você pode ver no Exemplo 20.11, “Saída do comando `ifconfig`” (p 305), o `ifconfig` tem uma saída detalhada e bem organizada. A saída também contém informações sobre o endereço MAC do seu dispositivo (o valor de `HWaddr`) na primeira linha.

Exemplo 20.11 Saída do comando `ifconfig`

```
eth0      Link encap:Ethernet  HWaddr 00:08:74:98:ED:51
          inet6 addr: fe80::208:74ff:fe98:ed51/64 Scope:Link
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:634735 errors:0 dropped:0 overruns:4 frame:0
          TX packets:154779 errors:0 dropped:0 overruns:0 carrier:1
          collisions:0 txqueuelen:1000
          RX bytes:162531992 (155.0 Mb)  TX bytes:49575995 (47.2 Mb)
          Interrupt:11 Base address:0xec80

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:8559 errors:0 dropped:0 overruns:0 frame:0
          TX packets:8559 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:533234 (520.7 Kb)  TX bytes:533234 (520.7 Kb)

wlan1     Link encap:Ethernet  HWaddr 00:0E:2E:52:3B:1D
          inet addr:192.168.2.4  Bcast:192.168.2.255  Mask:255.255.255.0
          inet6 addr: fe80::20e:2eff:fe52:3b1d/64 Scope:Link
          UP BROADCAST NOTRAILERS RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:50828 errors:0 dropped:0 overruns:0 frame:0
          TX packets:43770 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:45978185 (43.8 Mb)  TX bytes:7526693 (7.1 MB)
```

Para obter mais opções e informações sobre como usar o `ifconfig`, digite `ifconfig -h` ou consulte a página de manual do `ifconfig` (8).

Configurando o roteamento com o comando `route`

`route` é um programa usado para manipular a tabela de roteamento IP. Você pode usá-lo para ver sua configuração de roteamento e adicionar ou remover rotas.

NOTA: `route` e `ip`

O programa `route` está obsoleto. Em vez disso, use `ip`.

O comando `route` será especialmente útil se você precisar de informações rápidas e compreensíveis sobre a configuração do roteamento para identificar problemas de roteamento. Para ver a configuração de roteamento atual, digite `route -n` enquanto usuário `root`.

Exemplo 20.12 Saída do comando `route -n`

```
route -n
Kernel IP routing table
Destination      Gateway          Genmask          Flags      MSS Window  irtt Iface
10.20.0.0        *               255.255.248.0   U          0  0           0 eth0
link-local       *               255.255.0.0     U          0  0           0 eth0
loopback         *               255.0.0.0       U          0  0           0 lo
default          styx.exam.com   0.0.0.0         UG         0  0           0 eth0
```

Para obter mais informações sobre como usar o `route`, digite `route -h` ou consulte a página de manual de `route` (8).

20.6.3 Scripts de inicialização

Além dos arquivos de configuração descritos acima, há também vários scripts que carregam os programas de rede durante o boot da máquina. Eles são iniciados assim que o sistema é alternado para um dos *níveis de execução multiusuário*. Alguns desses scripts são descritos na Tabela 20.9, “Alguns scripts de inicialização para programas de rede” (p 306).

Tabela 20.9 *Alguns scripts de inicialização para programas de rede*

<code>/etc/init.d/network</code>	Este script controla a configuração das interfaces de rede. Se o serviço <code>network</code> não tiver sido iniciado, nenhuma interface de rede será implementada.
<code>/etc/init.d/xinetd</code>	Inicia o <code>xinetd</code> . O <code>xinetd</code> pode ser usado para disponibilizar os serviços do servidor no sistema. Por exemplo, ele pode iniciar o <code>vsftpd</code> sempre que uma conexão FTP for inicializada.
<code>/etc/init.d/rpcbind</code>	Inicia o utilitário <code>rpcbind</code> , que converte os números de programa RPC em endereços universais. Necessário para os serviços RPC, como um servidor NFS.
<code>/etc/init.d/nfsserver</code>	Inicia o servidor NFS.

`/etc/init.d/postfix` Controla o processo de postfix.

`/etc/init.d/ypserv` Inicia o servidor NIS.

`/etc/init.d/ypbind` Inicia o cliente NIS.

20.7 smpppd como Assistente de Discagem

Alguns usuários domésticos não possuem uma linha dedicada de conexão à Internet. Em vez disso, usam conexões por discagem. Dependendo da forma de discagem (ISDN ou DSL), a conexão é controlada por `ippd` ou `pppd`. Basicamente, tudo o que precisa ser feito para estabelecer a conexão é iniciar esses programas corretamente.

Se você tiver uma conexão com tarifa fixa que não gere custos adicionais para a conexão por discagem, basta iniciar o respectivo daemon. Controle a conexão por discagem com um applet de área de trabalho ou uma interface de linha de comando. Se o portal de Internet não for o host que você estiver usando, você poderá controlar a conexão por discagem por intermédio de um host de rede.

É aí que entra o `smpppd`. Ele oferece uma interface uniforme para programas auxiliares e funciona nas duas direções. Primeiro, ele programa o `pppd` ou `ippd` necessário e controla suas propriedades de discagem. Em segundo lugar, disponibiliza diversos provedores aos programas do usuário e transmite informações sobre o atual status da conexão. Já que o `smpppd` também pode ser controlado por meio da rede, é adequado para controlar conexões por discagem à Internet de uma estação de trabalho de uma sub-rede privada.

20.7.1 Configurando o smpppd

As conexões fornecidas pelo `smpppd` são automaticamente configuradas pelo YaST. Os programas por discagem KInternet e cinternet propriamente ditos também são pré-configurados. Configurações manuais somente são necessárias para configurar recursos adicionais do `smpppd`, como o controle remoto.

O arquivo de configuração do `smpppd` é o `/etc/smpppd.conf`. Por padrão, ele não habilita o controle remoto. As opções mais importantes desse arquivo de configuração são:

`open-inet-socket = yes/no`

Para controlar o `smpppd` pela rede, defina essa opção como `yes`. O `smpppd` escuta na porta 3185. Se esse parâmetro for definido como `yes`, os parâmetros `bind-address`, `host-range` e `password` deverão ser definidos da mesma forma.

`bind-address = endereço ip`

Se um host tiver diversos endereços IP, use esse parâmetro para determinar o endereço IP em que o `smpppd` deve aceitar conexões. O padrão é escutar em todos os endereços.

`host-range = ip mín.ip máx.`

O parâmetro `host-range` define uma faixa de rede. Os hosts cujos endereços IP se situam dentro dessa faixa recebem acesso ao `smpppd`. O acesso é recusado a todos os hosts localizados fora dessa faixa.

`password = senha`

Ao atribuir uma senha, limite os clientes a hosts autorizados. Como se trata de uma senha de texto simples, não é recomendável superestimar a segurança oferecida. Se nenhuma senha for atribuída, todos os clientes terão permissão para acessar o `smpppd`.

`slp-register = yes/no`

Com esse parâmetro, o serviço `smpppd` pode ser anunciado na rede por meio do SLP.

Mais informações sobre o `smpppd` estão disponíveis nas páginas do manual `smpppd(8)` e `smpppd.conf(5)`.

20.7.2 Configurando KInternet e qinternet para uso remoto

O KInternet e o cinternet podem ser usados para controlar um `smpppd` local ou remoto. O cinternet é o equivalente da linha de comando ao KInternet gráfico. Para preparar

esses utilitários para uso com um smpppd remoto, edite o arquivo de configuração `/etc/smpppd-c.conf` manualmente ou com o KInternet. Esse arquivo usa apenas quatro opções:

`sites = lista de locais`

É a *lista de locais* onde os front ends procuram smpppd. Os front ends testam as opções na ordem especificada. A opção `local` solicita o estabelecimento de uma conexão com o smpppd local. A opção `gateway` aponta para um smpppd no gateway. O `config-file` indica que deve-se estabelecer a conexão com o smpppd especificado nas opções `server` e `port` em `/etc/smpppd-c.conf`. O `slp` ordena que os front ends se conectem com um smpppd encontrado por SLP.

`server = servidor`

O host em que o smpppd é executado.

`port = porta`

A porta em que o smpppd é executado.

`password = senha`

Senha selecionada para o smpppd.

Se o smpppd estiver ativo, tente acessá-lo. Por exemplo, com `cinternet --verbose --interface-list`. Em caso de dificuldade nesse ponto, consulte as páginas de manual de `smpppd-c.conf` (5) e de `cinternet` (8).

Serviços SLP na rede

O *SLP* foi criado para simplificar a configuração dos clientes em rede dentro de uma rede local. Para configurar um cliente em rede, inclusive todos os serviços necessários, o administrador normalmente precisa ter conhecimento detalhado dos servidores disponíveis na rede. O SLP divulga a disponibilidade de serviços selecionados a todos os clientes da rede local. Os aplicativos que dão suporte ao SLP podem usar as informações distribuídas e podem ser configurados automaticamente.

O SUSE® Linux Enterprise Desktop dá suporte à instalação com o uso de fontes de instalação fornecidas com o SLP e contém diversos serviços de sistema com suporte integrado ao SLP. O YaST e o Konqueror possuem front ends apropriados para SLP. Você pode usar o SLP para oferecer funções centrais aos clientes em rede, como servidor de instalação, servidor de arquivos ou servidor de impressão no sistema.

IMPORTANTE: suporte a SLP no SUSE Linux Enterprise Desktop

Serviços que oferecem suporte ao SLP: cupsd, rsyncd, ypserv, openldap2, ksysguardd, saned, kdm, vnc, login, smpppd, rpasswd, postfix e sshd (via fish).

21.1 Instalação

Todos os pacotes necessários são instalados por padrão. No entanto, se você quiser fornecer serviços via SLP, verifique se o pacote `openslp-server` está instalado.

21.2 Ativando o SLP

O `slpd` deve ser executado no sistema para oferecer serviços pelo SLP. Se a máquina pode operar apenas como cliente e não oferece serviços, não é necessário ter `slpd` em execução nela. Assim como a maioria dos serviços de sistema, no SUSE Linux Enterprise Desktop, o daemon `slpd` é controlado por intermédio de um script `init` separado. Após a instalação, o daemon fica inativo por padrão. Para ativá-lo temporariamente, execute `rcslpd start` enquanto usuário `root` ou `rcslpd stop` para pará-lo. Efetue uma verificação de reinicialização ou status com `restart` ou `status`. Se for necessário que o `slpd` fique sempre ativo após o boot, habilite o `slpd` no YaST *Sistema > Serviços do Sistema (Nível de Execução)* ou execute o comando `insserv slpd` enquanto usuário `root`. Isso inclui o `slpd` no conjunto de serviços a serem iniciados durante o boot.

21.3 Front ends de SLP no SUSE Linux Enterprise Desktop

Para encontrar os serviços fornecidos por SLP na sua rede, use um front end de SLP. O SUSE Linux Enterprise Desktop contém vários front ends:

`slptool`

O `slptool` é um programa de linha de comando simples que pode ser usado para anunciar consultas SLP na rede ou anunciar serviços proprietários. `slptool --help` lista todas as opções e funções disponíveis. O `slptool` também pode ser chamado a partir de scripts que processam informações do SLP. Por exemplo, para encontrar todos os servidores de horário da rede que se anunciam na rede atual, execute o comando:

```
slptool findsrvs service:ntp
```

YaST

No YaST, também há um browser SLP disponível. Entretanto, esse browser não está disponível por meio do Centro de Controle do YaST. Para iniciar esse módulo do YaST, execute `yast2 slp` enquanto usuário `root`. Clique nos diversos protocolos à esquerda da interface do usuário para obter mais informações sobre o serviço correspondente.

21.4 Fornecendo serviços por SLP

Vários aplicativos contidos no SUSE Linux Enterprise Desktop possuem suporte ao SLP integrado com o uso da biblioteca `libslp`. Se um serviço não tiver sido compilado com o suporte ao SLP, use um dos métodos a seguir para disponibilizá-lo por SLP:

Registro estático com `/etc/slp.reg.d`

Crie um arquivo de registro separado para cada novo serviço. A seguir há um exemplo de arquivo para o registro de serviço de scanner:

```
## Register a saned service on this system
## en means english language
## 65535 disables the timeout, so the service registration does
## not need refreshes
service:scanner.sane://$HOSTNAME:6566,en,65535
watch-port-tcp=6566
description=SANE scanner daemon
```

A linha mais importante desse arquivo é a linha *URL do serviço*, que começa com `service:.` Essa linha contém o tipo de serviço (`scanner.sane`) e o endereço em que o serviço está disponível no servidor. `$HOSTNAME` é automaticamente substituída pelo nome completo do host. Em seguida, vem o nome da porta TCP em que o serviço em questão pode ser encontrado, separado por dois-pontos. A seguir, especifique o idioma em que o serviço deve ser exibido e a duração do registro em segundos. Esses dados devem ser separados do URL do serviço por vírgulas. Defina o valor da duração do registro entre 0 e 65535. O valor 0 impede o registro. O valor 65535 elimina todas as restrições.

O arquivo de registro também contém as duas variáveis `watch-port-tcp` e `description`. `watch-port-tcp` vincula o anúncio do serviço SLP à atividade do serviço em questão fazendo com que o `slpd` verifique o status do serviço. A segunda variável contém uma descrição mais precisa do serviço que é exibido nos browsers apropriados.

Registro estático com `/etc/slp.reg`

A única diferença entre esse método e o procedimento de `/etc/slp.reg.d` é que todos os serviços são agrupados em um arquivo central.

Registro dinâmico com `slptool`

Se um serviço precisar ser registrado dinamicamente sem a necessidade de arquivos de configuração, use o utilitário de linha de comando `slptool`. O mesmo utilitário

também pode ser usado para cancelar o registro de uma oferta de serviço existente sem reiniciar o `slpd`.

21.5 Para obter mais informações

As fontes a seguir fornecem informações adicionais sobre o SLP:

RFC 2608, 2609, 2610

O RFC 2608 geralmente trata da definição de SLP. O RFC 2609 trata da sintaxe dos URLs de serviço usados em maior detalhe e o RFC 2610 trata do DHCP via SLP.

<http://www.openslp.org/>

A home page do projeto OpenSLP.

`/usr/share/doc/packages/openslp`

Esse diretório contém toda a documentação disponível do SLP, inclusive um arquivo `README.SuSE` contendo os detalhes sobre o SUSE Linux Enterprise Desktop, os RFCs e dois documentos HTML introdutórios. Os programadores que desejarem usar as funções do SLP podem obter mais informações no *Programmers Guide* (Guia do programador), incluído no pacote `openslp-devel`.

Sincronização de horário com NTP

22

O mecanismo NTP (network time protocol) é um protocolo para sincronizar o horário do sistema na rede. Primeiro, uma máquina pode obter o horário de um servidor, que é uma fonte de horário confiável. Segundo, a máquina pode agir como uma fonte de horário para outros computadores na rede. O objetivo é duplo: manter o tempo absoluto e a sincronização do horário do sistema de todas as máquinas na rede.

Manter um horário exato do sistema é importante em várias situações. O relógio do hardware interno (BIOS) não atende aos requisitos de aplicativos como bancos de dados. A correção manual do horário do sistema levaria a problemas severos pois, por exemplo, um pulo inverso pode causar o mau funcionamento de aplicativos críticos. Em uma rede, geralmente é necessário sincronizar o horário do sistema de todas as máquinas, porém, o ajuste manual do horário não é um bom método. O ntp oferece um mecanismo para resolver esses problemas. Ele ajusta continuamente o horário do sistema com a ajuda de servidores de horário confiáveis na rede. Ele habilita também o gerenciamento de relógios de referência local como relógios controlados pelo rádio.

NOTA

Para habilitar a sincronização de horário por meio do diretório ativo, siga as instruções em Procedimento “Joining an AD Domain” (↑*Security Guide (Guia de Segurança)*).

22.1 Configurando um cliente NTP com o YaST

O ntp é predefinido para usar o relógio do computador local como referência de horário. Usar o relógio (BIOS), porém, serve somente como uma alternativa caso não haja uma fonte de horário de precisão maior disponível. O YaST facilita a configuração de um cliente NTP. Para um sistema que não tenha um firewall em execução, use a configuração rápida ou a avançada. Para um sistema protegido por firewall, a configuração avançada pode abrir as portas necessárias no SuSEfirewall2.

22.1.1 Configuração avançada de cliente NTP

Você pode configurar o cliente NTP de forma manual ou automática para obter uma lista dos servidores NTP disponíveis na sua rede por DHCP. Se você escolher *Configurar o Daemon do NTP via DHCP*, as opções manuais explicadas abaixo não estarão disponíveis.

Os servidores e outras fontes de horário para a consulta do cliente estão listados na guia *Configurações Gerais*. Modifique esta lista conforme necessário com *Adicionar*, *Editar* e *Apagar*. *Exibir Registro* fornece a possibilidade de exibir os arquivos de registro do seu cliente.

Clique em *Adicionar* para adicionar uma nova fonte de informação de horário. Na caixa de diálogo seguinte, selecione o tipo de fonte com a qual a sincronização de horário deve ser realizada. As seguintes opções estão disponíveis:

Servidor

Outra caixa de diálogo lhe permite selecionar um servidor NTP. Ative *Usar para Sincronização Inicial* para acionar a sincronização da informação de horário entre o servidor e o cliente quando o sistema é inicializado. *Opções* permite que você especifique opções adicionais para o ntpd.

Com o uso de *Opções de Controle de Acesso*, você pode restringir as ações que o computador remoto pode desempenhar com o daemon em execução no seu computador. Esse campo só fica habilitado quando se marca a opção *Restringir Serviço NTP Apenas aos Servidores Configurados* na guia *Configurações de*

Segurança. As opções correspondem às cláusulas `restrict` em `/etc/ntp.conf`. Por exemplo, `nomodify notrap noquery` não permite que o servidor modifique as configurações de NTP do seu computador e use o recurso de detecção (um recurso de registro de eventos remotos) do seu daemon NTP. O uso dessas restrições é recomendado para os servidores fora de controle (por exemplo, na Internet).

Consulte `/usr/share/doc/packages/ntp-doc` (parte do pacote `ntp-doc`) para obter informações detalhadas.

Peer

Um peer é uma máquina com a qual é estabelecido um relacionamento simétrico: ele atua como servidor de horário e como cliente. Para usar um peer na mesma rede em vez de um servidor, digite o endereço do sistema. O restante da caixa de diálogo é igual à caixa de diálogo *Servidor*.

Relógio controlado pelo rádio

Para usar um relógio controlado pelo rádio no seu sistema para a sincronização de horário, insira o tipo de relógio, o número da unidade, o nome do dispositivo e outras opções nesta caixa de diálogo. Clique em *Calibração do Driver* para ajustar o driver. Informações detalhadas sobre a operação de um rádio relógio local estão disponíveis em `/usr/share/doc/packages/ntp-doc/html/refclock.htm`.

Transmissão de saída

Consultas e informações sobre horário também podem ser transmitidas na rede. Nesta caixa de diálogo, insira o endereço ao qual estas transmissões devem ser enviadas. Não ative a transmissão a menos que você tenha uma fonte de horário confiável como um relógio controlado por rádio.

Transmissão de entrada

Se você deseja que o seu cliente receba suas informações através de transmissão, insira o endereço do qual os respectivos pacotes devem ser aceitos nestes campos.

Figura 22.1 *Configuração NTP Avançada: Configurações de Segurança*



Na guia *Configurações de Segurança*, determine se o `ntpd` deve ser iniciado em `chroot jail`. Por padrão, a opção *Executar Daemon NTP em Chroot Jail* está ativada. Isso aumenta a segurança caso ocorra um ataque em `ntpd`, pois evita que o invasor comprometa todo o sistema.

Restringir Serviço NTP Apenas aos Servidores Configurados aumenta a segurança do seu sistema ao não permitir que os computadores remotos vejam e modifiquem as configurações de NTP do seu computador e que usem o recurso de detecção para o registro de eventos remotos. Uma vez habilitadas, essas restrições se aplicam a todos os computadores remotos, a menos que você anule as opções de controle de acesso para computadores individuais na lista de fontes de horário na guia *Configurações Gerais*. Para todos os outros computadores remotos, só é permitida a consulta de horário local.

Habilite *Abrir Porta no Firewall* se o `SuSEfirewall2` estiver ativo (ele fica ativo por padrão). Se você manter a porta fechada, não será possível estabelecer uma conexão com o servidor de horário.

22.2 Configurando manualmente o ntp na rede

A forma mais fácil de usar um servidor de horário na rede é definir parâmetros de servidor. Por exemplo, se um servidor de horário denominado `ntp.example.com` for alcançável a partir da rede, inclua seu nome no arquivo `/etc/ntp.conf` adicionando a seguinte linha:

```
server ntp.example.com
```

Para adicionar mais servidores de horário, insira linhas adicionais com a palavra-chave `server`. Após a inicialização do `ntpd` com o comando `rcntp start`, leva aproximadamente uma hora para que o horário fique estabilizado e o arquivo de descompasso para a correção do relógio do computador local seja criado. Com o arquivo de descompasso, o erro sistemático do relógio do hardware pode ser computado assim que o computador for ligado. A correção é usada imediatamente, resultando em uma estabilidade maior do horário do sistema.

Há duas maneiras possíveis de usar o mecanismo NTP como cliente: primeiro, o cliente pode consultar o horário a partir de um servidor conhecido em intervalos regulares. Com vários clientes, esta abordagem pode causar uma carga alta no servidor. Segundo, o cliente pode esperar por transmissões de NTP enviadas por servidores de horário de transmissão na rede. Esta abordagem tem a desvantagem de que a qualidade do servidor é desconhecida e um servidor transmitindo a informação errada pode causar problemas graves.

Se o horário for obtido através de uma transmissão, você não precisará do nome do servidor. Neste caso, insira a linha `broadcastclient` no arquivo de configuração `/etc/ntp.conf`. Para usar um ou mais servidores de horário conhecidos exclusivamente, insira seus nomes na linha iniciando com `servers`.

22.3 Sincronização de horário dinâmica em tempo de execução

Se o sistema for inicializado sem conexão de rede, o `ntpd` será iniciado, mas não poderá resolver os nomes DNS dos servidores de horário definidos no arquivo de configuração. Isso pode ocorrer se você usar o Gerenciador de Rede com uma WLAN criptografada.

Se desejar que o `ntpd` resolva os nomes DNS em tempo de execução, é preciso definir a opção `dynamic`. Em seguida, quando a rede é estabelecida algum tempo após o boot, o `ntpd` pesquisa os nomes novamente e consegue alcançar os servidores de horário para obter o horário.

Edite manualmente o `/etc/ntp.conf` e adicione `dynamic` a uma ou mais entradas `server`:

```
server ntp.example.com dynamic
```

Ou use o YaST e proceda da seguinte maneira:

- 1 No YaST, clique em *Serviços de Rede > Configuração NTP*.
- 2 Selecione o servidor que deseja configurar. Em seguida, clique em *Editar*.
- 3 Ative o campo *Opções* e adicione `dynamic`. Separe-o por um espaço, se já houver outras opções digitadas.
- 4 Clique em *OK* para fechar a caixa de diálogo de edição. Repita a etapa anterior para mudar todos os servidores conforme desejado.
- 5 Por fim, clique em *OK* para gravar as configurações.

22.4 Configurando um relógio de referência local

O pacote de software `ntp` contém drivers para conectar relógios de referência local. Uma lista de relógios suportados está disponível no pacote `ntp-doc` no arquivo `/usr/`

`share/doc/packages/ntp-doc/html/refclock.htm`. Cada driver está associado a um número. No `ntp`, a configuração real ocorre através de pseudo-endereços IP. Os relógios são inseridos no arquivo `/etc/ntp.conf` como se existissem na rede. Para este propósito, endereços IP especiais são atribuídos a eles no formato `127.127.t.u`. Aqui, *t* representa o tipo de relógio e determina o driver a ser usado e *u* representa a unidade, que determina a interface usada.

Normalmente, os drivers individuais têm parâmetros especiais que descrevem detalhes de configuração. O arquivo `/usr/share/doc/packages/ntp-doc/drivers/driverNN.html` (onde *NN* é o número do driver) fornece informações sobre o tipo específico de relógio. Por exemplo, o relógio “type 8” (relógio controlado por rádio na interface serial) exige um modo adicional que especifica o relógio de forma mais precisa. O módulo de recebimento Conrad DCF77, por exemplo, tem o modo 5. Para usar este relógio como referência preferida, especifique a palavra-chave `prefer`. A linha do servidor completa para um módulo de recebimento Conrad DCF77 seria:

```
server 127.127.8.0 mode 5 prefer
```

Outros relógios seguem o mesmo padrão. Seguindo a instalação do pacote `ntp-doc`, a documentação do `ntp` está disponível no diretório `/usr/share/doc/packages/ntp-doc`. O arquivo `/usr/share/doc/packages/ntp-doc/refclock.htm` fornece links para as páginas que descrevem os parâmetros do driver.

Usando o NetworkManager

O NetworkManager é a solução ideal para laptops e outros computadores portáteis. Ele suporta tipos de criptografia e padrões avançados para conexões de rede, incluindo conexões com redes protegidas por 802.1x. Com o NetworkManager, não é necessário preocupar-se em configurar interfaces de rede e alternar entre redes wireless ou não quando você estiver em trânsito. O NetworkManager pode conectar-se automaticamente a redes wireless conhecidas ou gerenciar várias conexões de rede paralelamente, caso em que a conexão mais rápida é usada como padrão. Além disso, você pode alternar manualmente entre as redes disponíveis e gerenciar sua conexão de rede usando um applet na bandeja do sistema.

Várias conexões podem estar ativas simultaneamente, em vez de apenas uma. Isso lhe permite desplugar o laptop de uma Ethernet e permanecer conectado por uma conexão wireless.

23.1 Casos de uso do NetworkManager

O NetworkManager oferece uma interface de usuário sofisticada e intuitiva, que permite aos usuários alternar facilmente seus ambientes de rede. Contudo, o NetworkManager não é uma solução adequada nos seguintes casos:

- O computador fornece serviços de rede para outros computadores de sua rede, por exemplo, se ele for um servidor DHCP ou DNS.

- Seu computador é um servidor Xen ou seu sistema é um sistema virtual dentro do Xen.
- Você quer usar o SCPM para o gerenciamento de configuração da rede. Para usar o SCPM e o NetworkManager ao mesmo tempo, desabilite o recurso de rede na configuração do SCPM.

23.2 Habilitando o NetworkManager

Em laptops, o NetworkManager fica habilitado por padrão. No entanto, ele pode ser habilitado ou desabilitado a qualquer momento no módulo Configurações de Rede do YaST.

- 1 Execute o YaST e vá até *Dispositivos de Rede > Configurações de Rede*.
- 2 A caixa de diálogo *Configurações de Rede* é aberta. Vá até a guia *Opções Globais*.
- 3 Para configurar e gerenciar suas conexões de rede com o NetworkManager, selecione *Controlado por Usuário com o NetworkManager*.
- 4 Clique em *OK*.
- 5 Após escolher o método para gerenciar as conexões de rede, configure sua placa de rede usando a configuração automática via DHCP ou um endereço IP estático, ou configure o seu modem (para conexões discadas, use *Dispositivos de Rede > Modem*). Para configurar um modem interno ou USB RDSI (ISDN), selecione *Dispositivos de Rede > ISDN*. Para configurar um modem USB DSL, selecione *Dispositivos de Rede > DSL*.

Uma descrição detalhada da configuração da rede com o YaST encontra-se na Seção 20.4, “Configurando uma conexão de rede com o YaST” (p 267) e na Capítulo 17, *Rede local sem fio* (p 211).

Após habilitar o NetworkManager, configure suas conexões de rede com o NetworkManager, conforme descrito na Seção 23.3, “Configurando conexões de rede” (p 325).

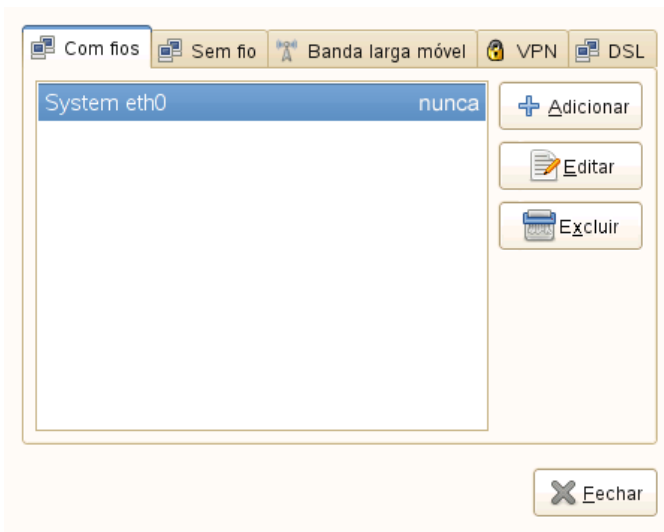
Se você quiser desativar o NetworkManager e controlar a rede do modo tradicional, escolha a opção *Método Tradicional com ifup* no campo *Método de Configuração da Rede*.

23.3 Configurando conexões de rede

Após habilitar o NetworkManager no YaST, configure suas conexões de rede com os front ends do NetworkManager disponíveis no KDE e no GNOME. As caixas de diálogo de configuração de rede para ambos os front ends são bem semelhantes. Elas apresentam guias para todos os tipos de conexões de rede, por exemplo, com fio, wireless, banda larga móvel, DSL e VPN. Em cada guia, você pode adicionar, editar ou apagar conexões do tipo em questão. Na caixa de diálogo de configuração do KDE, as guias apropriadas somente estarão ativas se o tipo de conexão estiver disponível no seu sistema (dependendo do hardware e do software). Por padrão, o KNetworkManager também exibe dicas de ferramentas abrangentes para os campos de entrada e as opções disponíveis em cada guia.

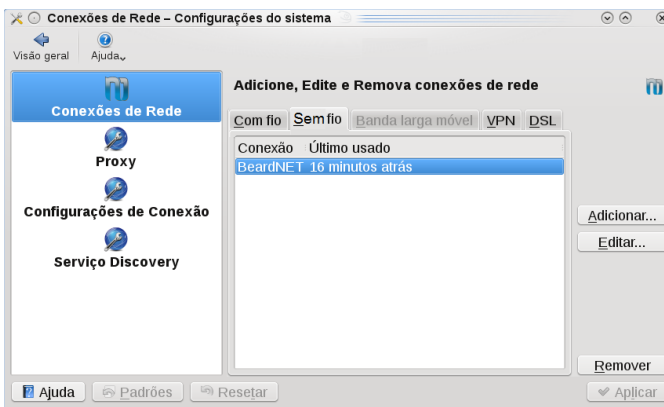
Para abrir a caixa de diálogo de configuração da rede no GNOME, abra o menu principal e clique na entrada *Rede* à direita. De outra forma, pressione **Alt + F2** e digite `nm-connection-editor` (ou, na Central de Controle GNOME, selecione *Sistema > Configurações de Rede*).

Figura 23.1 Caixa de diálogo de configuração de rede do GNOME



Se você usa o KDE, abra o menu principal e clique em *Configurar a Área de Trabalho*. Nas *Configurações Pessoais*, selecione *Configurações de Rede* na guia *Geral* para abrir a caixa de diálogo de configuração de rede.

Figura 23.2 Caixa de diálogo de configuração de rede do KDE



Por outro lado, você também pode iniciar as caixas de diálogo de configuração pelo applet do NetworkManager na bandeja do sistema. No KDE, clique o botão esquerdo

do mouse no ícone e selecione *Gerenciar Conexões*. No GNOME, clique o botão direito do mouse no ícone e selecione *Editar Conexões*.

NOTA: disponibilidade das opções

Dependendo da configuração do seu sistema, pode ser que você não tenha permissão para configurar conexões. Em um ambiente protegido, talvez algumas opções sejam bloqueadas ou exijam permissão do `root`. Consulte o administrador do sistema para obter detalhes.

Procedimento 23.1 *Adicionando ou editando conexões*

Ao configurar conexões de rede com o NetworkManager, você também pode definir conexões de sistema que podem ser compartilhadas por todos os usuários. Diferentemente das conexões de usuário, as conexões de sistema são disponibilizadas logo após o NetworkManager ser iniciado, antes que qualquer usuário efetue login. Para obter mais detalhes sobre ambos os tipos de conexões, consulte a Seção 23.7.1, “Conexões de usuário e sistema” (p 337).

No momento, a opção `system connection` não está disponível no KNetworkManager. Para configurar conexões do sistema, você precisa usar o YaST.

NOTA: redes ocultas

Para conectar-se a uma rede “oculta” (uma rede que não transmite seu serviço), você precisa saber o ESSID (Extended Service Set Identifier) da rede, já que ele não pode ser detectado automaticamente.

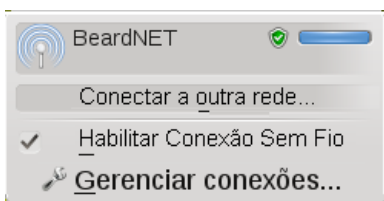
- 1 Para adicionar uma nova conexão, clique na guia referente ao tipo de conexão que você deseja usar e clique em *Adicionar*.
- 2 Digite um *Nome da Conexão* e os respectivos detalhes da conexão.
- 3 No caso de uma rede oculta, digite o ESSID e os parâmetros de criptografia.
- 4 Você pode vincular a conexão a um determinado dispositivo, caso haja mais de um dispositivo físico disponível por tipo de conexão (por exemplo, quando a máquina está equipada com duas placas ethernet ou duas placas wireless).

Ao usar o KDE, faça isso usando a opção *Restringir à Interface*. Ao usar o GNOME, digite o *endereço MAC* do dispositivo ao qual deseja vincular a conexão e confirme as configurações.

- 5 Se desejar que o NetworkManager automaticamente use uma determinada conexão, ative *Conectar Automaticamente* para essa conexão.
- 6 Para transformar uma conexão em conexão de sistema, ative *Disponível para todos os usuários* (GNOME). A criação e a edição de conexões do sistema exigem permissão de `root`.

Depois de confirmadas as mudanças, a conexão de rede recém-configurada é exibida na lista de redes disponíveis que aparece ao clicar-se o botão esquerdo do mouse no applet do NetworkManager.

Figura 23.3 *KNetworkManager — conexões configuradas e disponíveis*



23.4 Usando o KNetworkManager

O front end do KDE para o NetworkManager é o applet KNetworkManager. Se a rede tiver sido configurada para o controle do NetworkManager, o applet geralmente será iniciado automaticamente com o ambiente de área de trabalho e mostrado como um ícone na bandeja do sistema.

Se a bandeja do sistema não mostrar nenhum ícone de conexão de rede, provavelmente o applet não foi iniciado. Pressione `Alt + F2` e digite `knetworkmanager` para iniciá-lo manualmente.

O KNetworkManager mostra apenas as redes wireless para as quais você configurou uma conexão. Ele oculta as conexões quando você está fora do âmbito de uma rede wireless ou quando o cabo da rede está desconectado, de forma a apresentar-lhe sempre as conexões que podem ser usadas.

23.4.1 Conectando a redes com fio

Se o seu computador estiver conectado a uma rede por um cabo de rede, use o KNetworkManager para escolher a conexão de rede.

- 1 Clique o botão esquerdo do mouse no ícone do applet para mostrar um menu com as redes disponíveis. A conexão em uso no momento é selecionada no menu e marcada como *Ativa*.
- 2 Se desejar usar uma configuração diferente na rede com fio, clique em *Gerenciar Conexões* e adicione outra conexão com fio conforme descrito no Procedimento 23.1, “Adicionando ou editando conexões” (p 327).
- 3 Clique no ícone do KNetworkManager e selecione a conexão recém-configurada para ativá-la.

23.4.2 Conectando a redes wireless

Por padrão, o KNetworkManager mostra apenas as redes wireless para as quais você configurou uma conexão, desde que estejam disponíveis e visíveis. Para conectar-se a um rede wireless pela primeira vez, faça o seguinte:

- 1 Clique o botão esquerdo do mouse no ícone do applet e selecione *Criar Conexão de Rede*. O KNetworkManager mostra uma lista de redes wireless disponíveis visíveis, incluindo detalhes sobre força e segurança do sinal.
- 2 Para conectar-se a uma rede visível, selecione-a na lista e clique em *Conectar*. Se a rede estiver criptografada, uma caixa de diálogo será aberta. Escolha o tipo de *Segurança* que a rede usa e digite as credenciais apropriadas.
- 3 Para conectar-se a uma rede que não transmita seu ESSID (service set identifier - identificador de conjunto de serviços) e, assim, não possa ser detectada automaticamente, selecione *Conectar-se a Outra Rede*.
- 4 Na caixa de diálogo exibida, digite o ESSID e defina parâmetros de criptografia, se necessário.
- 5 Confirme as mudanças e clique em *OK*. O NetworkManager agora vai ativar a nova conexão.

- 6 Para terminar uma conexão e desabilitar a rede wireless, clique no ícone do applet e desmarque *Habilitar Conexão Sem Fio*. Isso poderá ser muito útil se você estiver em um avião ou em qualquer outro ambiente em que não é permitido usar rede wireless.

Uma rede wireless escolhida explicitamente permanecerá conectada o máximo de tempo possível. Se um cabo de rede estiver acoplado durante esse tempo, quaisquer conexões definidas com *Conectar Automaticamente* serão conectadas enquanto a conexão wireless permanecer ativa.

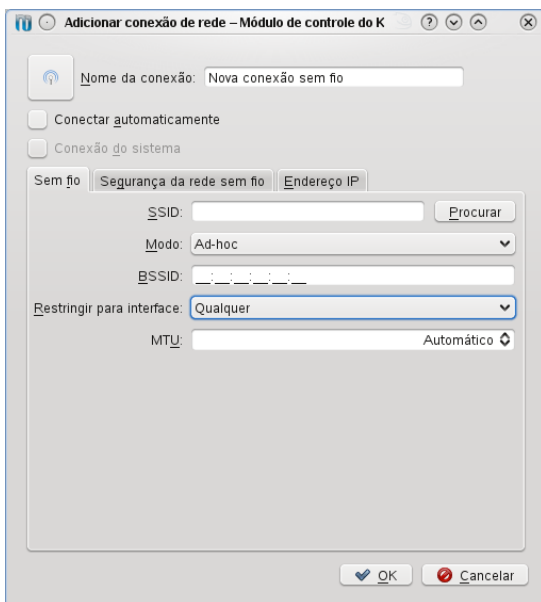
23.4.3 Configurando sua placa wireless como um ponto de acesso

Se a placa wireless suportar o modo de ponto de acesso, você poderá usar o NetworkManager para configuração.

NOTA: disponibilidade das opções

Dependendo da configuração do seu sistema, pode ser que você não tenha permissão para configurar conexões. Em um ambiente protegido, talvez algumas opções sejam bloqueadas ou exijam permissão do `root`. Consulte o administrador do sistema para obter detalhes.

- 1 Clique no applet do KNetworkManager e selecione *Criar Conexão de Rede > Nova Rede Ad-hoc*.
- 2 Na seguinte caixa de diálogo de configuração, digite um nome para a sua rede no campo *SSID*.



- 3 Defina a criptografia na guia *Segurança da Rede sem Fio*.

IMPORTANTE: redes wireless desprotegidas representam um risco de segurança

Se definir *Segurança* como *Nenhuma*, qualquer pessoa poderá se conectar à sua rede, reutilizar sua conectividade e interceptar sua conexão de rede. Use criptografia para restringir o acesso ao seu ponto de acesso e proteger sua conexão. Você pode escolher entre várias criptografias baseadas em WEP e WPA. Se não tiver certeza sobre qual tecnologia é mais apropriada para você, leia a Seção 17.3, “Autenticação” (p 213).

- 4 Na guia *Endereço IP*, verifique se a opção *Configurar* está definida como *Compartilhado* (opção padrão para redes ad-hoc).
- 5 Confirme sua configuração com *OK*.

23.4.4 Personalizando o KNetworkManager

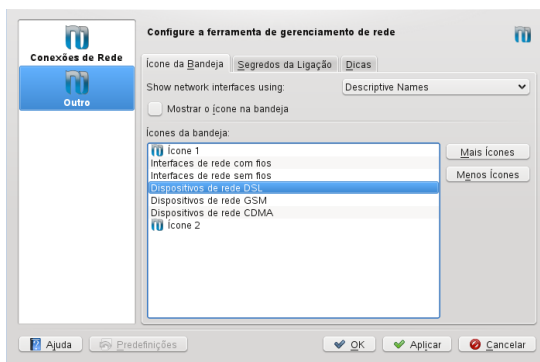
Você pode personalizar alguns aspectos do KNetworkManager: o número de ícones exibidos na bandeja do sistema, as dicas de ferramentas a mostrar e como armazenar sua senha e suas credenciais referentes às conexões de rede. Para obter mais informações sobre o último aspecto, consulte a Seção 23.7.2, “Armazenando senhas e credenciais” (p 338).

Para explorar as opções disponíveis, clique o botão direito do mouse no ícone do NetworkManager na bandeja do sistema e clique em *Outro* no lado esquerdo da caixa de diálogo de configuração.

Procedimento 23.2 *Configurando vários ícones de bandeja para o KNetworkManager*

Com a capacidade do KNetworkManager de manter várias conexões ativas ao mesmo tempo, talvez lhe convenha ser informado sobre o status de várias conexões em um único relance. Para fazer isso, use vários ícones do NetworkManager na sua bandeja do sistema, cada um deles representando um grupo diferente de tipos de conexão (por exemplo, um ícone para conexões com fio, outro ícone para conexões wireless).

- 1 Na caixa de diálogo de configuração, alterne para a guia *Ícone da Bandeja*.
- 2 Clique em *Mais Ícones*. Uma nova entrada de ícone é exibida na lista.
- 3 Selecione os tipos de conexão de rede que serão representados por esse ícone e agrupe-os sob ele.



4 Confirme as mudanças.

Agora a bandeja do sistema mostra vários ícones do NetworkManager, pelos quais você poderá acessar os tipos de conexão vinculados a cada um.

Ao configurar uma conexão de rede conforme descrito no Procedimento 23.1, “Adicionando ou editando conexões” (p 327), o KNetworkManager também lhe permite personalizar o ícone exibido para essa conexão. Para mudar o ícone, clique no botão do ícone ao lado de *Nome da Conexão* e, na caixa de diálogo a seguir, selecione o ícone da sua escolha. Após confirmadas as mudanças, o novo ícone é exibido na lista de conexões disponíveis que aparece quando se clica no ícone do KNetworkManager na bandeja do sistema.

23.5 Usando o applet NetworkManager do GNOME

No GNOME, o NetworkManager pode ser controlado com o applet NetworkManager do GNOME. Quando a rede está configurada para o controle do NetworkManager, o applet geralmente é iniciado automaticamente com o ambiente de área de trabalho e mostrado como um ícone na bandeja do sistema.

Se a bandeja do sistema não mostrar nenhum ícone de conexão de rede, provavelmente o applet não foi iniciado. Pressione Alt + F2 e digite `nm-applet` para iniciá-lo manualmente.

23.5.1 Conectando a redes com fio

Se o seu computador estiver conectado a uma rede com um cabo de rede, use o applet NetworkManager para escolher a conexão de rede.

- 1 Clique o botão esquerdo do mouse no ícone do applet para mostrar um menu com as redes disponíveis. A conexão usada no momento está selecionada no menu.
- 2 Para alternar para outra rede, escolha-a na lista.

- 3 Para desativar todas as conexões de rede, wireless ou não, clique o botão direito no ícone do applet e desmarque *Habilitar Rede*.

23.5.2 Conectando a redes wireless

As redes wireless visíveis que estiverem disponíveis são listadas no menu do applet NetworkManager do GNOME em *Redes sem Fio*. A força do sinal de cada rede também é mostrada no menu. Redes wireless criptografadas são marcadas com um ícone de escudo.

Procedimento 23.3 *Conectando a uma rede wireless*

- 1 Para se conectar a uma rede wireless, clique no ícone do applet e escolha uma entrada na lista de redes wireless disponíveis.
- 2 Se a rede estiver criptografada, uma caixa de diálogo será aberta. Ela mostra o tipo de criptografia usada pela rede (*Segurança da Rede sem Fio*) e contém uma série de campos de entrada de acordo com as respectivas configurações de criptografia e autenticação. Digite as credenciais apropriadas.
- 3 Para conectar-se a uma rede que não transmita seu ESSID (service set identifier - identificador de conjunto de serviços) e, com isso, não possa ser detectada automaticamente, clique o botão esquerdo do mouse no ícone do NetworkManager e escolha *Conectar-se a Rede sem Fio Oculta*.
- 4 Na caixa de diálogo exibida, digite o ESSID em *Nome da Rede* e defina parâmetros de criptografia, se necessário.
- 5 Para desabilitar a rede wireless, clique o botão direito do mouse no ícone do applet e desmarque *Habilitar Conexão sem Fio*. Isso poderá ser muito útil se você estiver em um avião ou em qualquer outro ambiente em que não é permitido usar rede wireless.

Uma rede wireless escolhida explicitamente permanecerá conectada o máximo de tempo possível. Se um cabo de rede estiver acoplado durante esse tempo, quaisquer conexões definidas com *Conectar Automaticamente* serão conectadas enquanto a conexão wireless permanecer ativa.

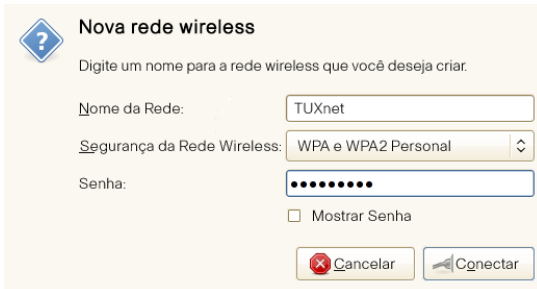
23.5.3 Configurando sua placa wireless como um ponto de acesso

Se a placa wireless suportar o modo de ponto de acesso, você poderá usar o NetworkManager para configuração.

NOTA: disponibilidade das opções

Dependendo da configuração do seu sistema, pode ser que você não tenha permissão para configurar conexões. Em um ambiente protegido, talvez algumas opções sejam bloqueadas ou exijam permissão do `root`. Consulte o administrador do sistema para obter detalhes.

- 1 Clique no applet do NetworkManager e selecione *Criar Nova Rede sem Fio*.



- 2 Digite um *Nome da Rede* e defina a criptografia a ser usada com a lista suspensa *Segurança da Rede sem Fio*.

IMPORTANTE: redes wireless desprotegidas representam um risco de segurança

Se você definir *Segurança da Rede sem Fio* como *Nenhuma*, qualquer pessoa poderá se conectar à sua rede, reutilizar sua conectividade e interceptar sua conexão de rede. Use criptografia para restringir o acesso ao seu ponto de acesso e proteger sua conexão. Você pode escolher entre várias criptografias baseadas em WEP e WPA. Se não tiver certeza

sobre qual tecnologia é mais apropriada para você, leia a Seção 17.3, “Autenticação” (p 213).

23.6 NetworkManager e VPN

O NetworkManager suporta algumas tecnologias VPN (Virtual Private Network). Para cada tecnologia, o SUSE Linux Enterprise Desktop possui um pacote básico que fornece o suporte genérico ao NetworkManager. Além disso, você também precisa instalar o respectivo pacote específico da área de trabalho para o seu applet.

NovellVPN

Para usar essa tecnologia VPN, instale o `NetworkManager-novellvpn` e o `NetworkManager-novellvpn-kde4` ou o `NetworkManager-novellvpn-gnome`.

No momento, o suporte do NovellVPN ao KDE ainda não está disponível, mas está sendo elaborado.

OpenVPN

Para usar essa tecnologia VPN, instale o `NetworkManager-openvpn` e o `NetworkManager-openvpn-kde4` ou o `NetworkManager-openvpn-gnome`.

vpnc (Cisco)

Para usar essa tecnologia VPN, instale o `NetworkManager-vpnc` e o `NetworkManager-vpnc-kde4` ou o `NetworkManager-vpnc-gnome`.

PPTP (Point-to-Point Tunneling Protocol)

Para usar essa tecnologia VPN, instale o `NetworkManager-pptp` e o `NetworkManager-pptp-kde4` ou o `NetworkManager-pptp-gnome`.

Após instalar os pacotes, configure sua conexão VPN conforme descrito na Seção 23.3, “Configurando conexões de rede” (p 325).

23.7 NetworkManager e segurança

O NetworkManager distingue dois tipos de conexões wireless: confiáveis e não confiáveis. Uma conexão confiável é qualquer rede selecionada explicitamente no passado. Todas as outras são não confiáveis. As conexões confiáveis são identificadas pelo nome e pelo endereço MAC do ponto de acesso. O uso do endereço MAC garante que você não possa usar um ponto de acesso diferente com o nome da conexão confiável.

O NetworkManager faz uma busca periódica de redes wireless. Se forem encontradas várias redes confiáveis, a usada mais recentemente será selecionada automaticamente. O NetworkManager aguarda a sua seleção caso nenhuma das redes seja confiável.

Se a configuração de criptografia mudar, mas o nome e o endereço MAC continuarem os mesmos, o NetworkManager tentará se conectar, mas primeiro você será solicitado a confirmar as novas configurações de criptografia e fornecer atualizações, como uma nova chave.

Se você alternar entre o uso de uma conexão wireless e o modo offline, o NetworkManager deixará o ESSID em branco. Isso garante que a placa seja desconectada.

23.7.1 Conexões de usuário e sistema

O NetworkManager conhece dois tipos de conexões: conexões do usuário e do sistema. As conexões do usuário são aquelas que ficam disponíveis ao NetworkManager quando o primeiro usuário efetua login. Quaisquer credenciais requeridas são solicitadas do usuário e, quando ele efetua logout, as conexões são desconectadas e removidas do NetworkManager. AS conexões definidas como sendo do sistema podem ser compartilhadas por todos os usuários e disponibilizadas logo após o NetworkManager ser iniciado — antes que qualquer usuário efetue login. No caso das conexões do sistema, todas as credenciais devem ser fornecidas no momento em que a conexão é criada. Tais conexões do sistema podem ser usadas para conectar-se automaticamente a redes que exigem autorização. Para obter informações sobre como configurar as conexões de usuário ou sistema com o NetworkManager, consulte a Seção 23.3, “Configurando conexões de rede” (p 325).

No KDE, no momento não há suporte para as conexões do sistema com o NetworkManager (use o YaST para isso).

23.7.2 Armazenando senhas e credenciais

Se você não quiser digitar novamente suas credenciais toda vez que se conectar a uma rede criptografada, use as ferramentas específicas de área de trabalho Gerenciador de Chaves do GNOME ou KWalletManager para armazenar suas credenciais criptografadas no disco, protegidas por uma senha master.

Com o KNetworkManager, você pode configurar se e como armazenar suas credenciais no KDE. Para fazer isso, clique o botão esquerdo do mouse no ícone do KNetworkManager e selecione *Gerenciar Conexões*. Clique em *Outro > Segredos da Conexão* e selecione uma das seguintes opções:

Não Armazenar (Perguntar Sempre)

Isso é útil quando você está trabalhando em um ambiente onde o armazenamento de credenciais é considerado um risco de segurança.

No Arquivo (Sem Encriptação)

ATENÇÃO: risco de segurança

Armazenar suas credenciais de rede sem criptografia é um risco de segurança. Todos que acessam o seu computador podem reutilizar a sua conectividade e interceptar sua conexão de rede.

Se você escolher essa opção, suas senhas serão armazenadas sem criptografia no respectivo arquivo de conexão criado para cada conexão. Eles se encontram em `$HOME/.kde4/share/apps/networkmanagement/connections`.

Em Armazenamento Seguro (Criptografado)

Se você escolher essas opções, suas credenciais serão armazenadas no KWalletManager. Para obter mais informações sobre o KWalletManager, consulte o Capítulo 8, *Managing Passwords with KWallet Manager* (↑*KDE User Guide*).

O NetworkManager também pode recuperar seus certificados para conexões seguras (por exemplo, conexões com fio, wireless ou VPN criptografadas) do armazenamento de certificado. Para obter mais informações, consulte o Capítulo 12, *Certificate Store* (↑*Security Guide (Guia de Segurança)*).

Outra opção é usar o Single Sign-on com o Novell CASA. Single Sign-on é um método de controle de acesso que permite que usuários se autenticuem uma vez e, desse modo,

obtenham acesso aos recursos de vários sistemas de software. Se o Novell CASA estiver configurado para seu sistema, o NetworkManager não solicitará uma senha adicional para desbloquear o Gerenciador de Chaves do GNOME. Em vez disso, a chave será desbloqueada automaticamente quando os usuários fizerem login na área de trabalho. Para obter mais informações sobre o Novell CASA, consulte a <http://developer.novell.com/wiki/index.php/Special:Downloads/casa>.

23.8 Perguntas mais freqüentes

A seguir, são apresentadas algumas perguntas mais freqüentes sobre a configuração de opções de rede especiais com o NetworkManager.

Como vincular uma conexão a um dispositivo específico?

Por padrão, as conexões no NetworkManager são específicas ao tipo de dispositivo: elas se aplicam a todos os dispositivos físicos do mesmo tipo. Se houver mais de um dispositivo físico disponível por tipo de conexão (por exemplo, quando a máquina está equipada com duas placas ethernet), você poderá vincular uma conexão a um determinado dispositivo.

Para fazer isso no GNOME, primeiro procure o endereço MAC do seu dispositivo (use as *Informações da Conexão* disponíveis no applet ou use a saída das ferramentas de linha de comando, como `nm-tool` ou `ifconfig`). Em seguida, inicie a caixa de diálogo para configurar conexões de rede e escolher a conexão que você deseja modificar. Na guia *Com fio* ou *Wireless*, digite o *Endereço MAC* do dispositivo e confirme suas mudanças.

Se você usa o KDE, inicie a caixa de diálogo para configurar conexões de rede e escolher a conexão que deseja modificar. Na guia *Ethernet* ou *Wireless*, use a opção *Restringir à Interface* para selecionar a interface de rede à qual vincular a conexão.

Como especificar um determinado ponto de acesso caso sejam detectados vários pontos de acesso com o mesmo ESSID?

Quando há vários pontos de acesso disponíveis com bandas wireless diferentes (a/b/g/n), o ponto de acesso com o sinal mais forte é automaticamente escolhido por padrão. Para anular isso, use o campo *BSSID* ao configurar conexões wireless.

O BSSID (Basic Service Set Identifier) identifica de forma exclusiva cada Conjunto de Serviços Básicos. Em um Conjunto de Serviços Básicos de infra-estrutura, o BSSID é o endereço MAC do ponto de acesso wireless. Em um Conjunto de

Serviços Básicos independente (ad-hoc), o BSSID é um endereço MAC administrado localmente, gerado de um número aleatório de 46 bits.

Inicie a caixa de diálogo de configuração de conexões de rede pelo Centro de Controle GNOME, em *Sistema > Configuração da Rede*, ou pelas *Configurações Pessoais* do KDE 4, em *Configurações de Rede*. Escolha a conexão wireless que você deseja modificar e clique em *Editar*. Na guia *Wireless*, digite o BSSID.

Como compartilhar conexões de rede com outros computadores?

O dispositivo principal (que está conectado à Internet) não precisa de nenhuma configuração especial. Entretanto, você deve configurar o dispositivo que está conectado ao barramento local ou à máquina, conforme a seguir:

1. Inicie a caixa de diálogo de configuração de conexões de rede pelo Centro de Controle GNOME, em *Sistema > Configuração da Rede*, ou pelas *Configurações Pessoais* do KDE 4, em *Avançado > Configurações de Rede*. Escolha a conexão que você deseja modificar e clique em *Editar*. Se você estiver usando o GNOME, alterne para a guia *Configurações IPv4* e, na lista suspensa *Método*, escolha *Compartilhado com outros computadores*. Se estiver usando o KDE, alterne para a guia *Endereço IP* e, na lista suspensa *Configurar*, escolha *Compartilhado*. Isso habilitará o encaminhamento de tráfego IP e executar um servidor DHCP no dispositivo. Confirme suas mudanças no NetworkManager.
2. Visto que o servidor DHCP usa a porta 67, verifique se ela não está bloqueada pelo firewall: na máquina que compartilha as conexões, inicie o YaST e selecione *Segurança e Usuários > Firewall*. Alterne para a categoria *Serviços Permitidos*. Se o *Servidor DHCP* ainda não for exibido como *Serviço Permitido*, selecione *Servidor DHCP* em *Serviços a Permitir* e clique em *Adicionar*. Confirme as mudanças no YaST.

Como fornecer informações de DNS estático com endereços automáticos (DHCP, PPP, VPN)?

Caso um servidor DHCP forneça informações (e/ou rotas) inválidas de DNS, você pode anulá-las. Inicie a caixa de diálogo de configuração de conexões de rede pelo Centro de Controle GNOME, em *Sistema > Configuração da Rede*, ou pelas *Configurações Pessoais* do KDE 4, em *Avançado > Configurações de Rede*. Escolha a conexão que você deseja modificar e clique em *Editar*. Se você estiver usando o GNOME, alterne para a guia *Configurações IPv4* e, na lista suspensa *Método*, escolha *Somente endereços (DHCP) automáticos*. Se você estiver usando o KDE, passe para a guia *Endereço IP* e, na lista suspensa *Configurar*, escolha *Somente*

endereços (DHCP) automáticos. Digite as informações de DNS nos campos Servidores DNS e Domínios de Pesquisa. Na lista suspensa no fim da guia, selecione Rotas se desejar Ignorar automaticamente rotas obtidas. Confirme as mudanças.

Como fazer o NetworkManager conectar-se a redes protegidas por senha antes que um usuário efetue login?

Defina uma conexão do sistema que possa ser usada para esse fim. Para obter maiores informações, consulte a Seção 23.7, “NetworkManager e segurança” (p 337).

23.9 Solução de problemas

Podem ocorrer problemas de conexão. Alguns problemas comuns relacionados ao NetworkManager incluem o applet não ser iniciado, a opção VPN estar ausente e problemas com o SCPM. Métodos para resolver e evitar esses problemas dependem da ferramenta usada.

O applet da área de trabalho do NetworkManager não é iniciado

Os applets GNOME e KDE para NetworkManager serão iniciados automaticamente se a rede for configurada para o controle do NetworkManager. Se o applet não for iniciado, verifique se o NetworkManager está habilitado no YaST, conforme descrito na Seção 23.2, “Habilitando o NetworkManager” (p 324). Em seguida, verifique se o pacote apropriado para o seu ambiente de área de trabalho também está instalado. Se você estiver usando o KDE 4, o pacote é `NetworkManager-kde4`. Para usuários do GNOME, o pacote é `NetworkManager-gnome`.

Se o applet de área de trabalho estiver instalado, mas não estiver em execução por algum motivo, inicie-o manualmente com o comando `nm-applet` (GNOME) ou `knetworkmanager` (KDE).

O applet do NetworkManager não inclui a opção VPN

O suporte ao NetworkManager, a applets e ao VPN para NetworkManager é distribuído em pacotes separados. Se o applet do NetworkManager não incluir a opção VPN, verifique se os pacotes do NetworkManager com suporte à sua tecnologia VPN estão instalados. Para obter mais informações, consulte a Seção 23.6, “NetworkManager e VPN” (p 336).

O SCPM não troca a configuração de rede

Provavelmente você está usando o SCPM junto com o NetworkManager. No momento, o NetworkManager não funciona com os perfis SCPM. Não use o NetworkManager junto com o SCPM quando perfis SCPM também mudarem configurações de rede. Para usar o SCPM e o NetworkManager ao mesmo tempo, desabilite o recurso de rede na configuração do SCPM.

Nenhuma conexão de rede disponível

Se você configurou sua conexão de rede corretamente e todos os outros componentes para a conexão de rede (roteador etc.) também estiverem em funcionamento, pode ser útil reiniciar as interfaces de rede no seu computador. Para isso, efetue login em uma linha de comando como usuário `root` e execute `rcnetwork restart`.

23.10 Para obter mais informações

Mais informações sobre o NetworkManager podem ser encontradas nos seguintes sites na Web e diretórios:

Página do projeto do NetworkManager

<http://projects.gnome.org/NetworkManager/>

Front end KDE do NetworkManager

<http://userbase.kde.org/NetworkManagement>

Documentação do pacote

Verifique também o conteúdo dos seguintes diretórios para obter as informações mais recentes sobre o NetworkManager e os applets GNOME e KDE para NetworkManager:

- `/usr/share/doc/packages/NetworkManager/`,
- `/usr/share/doc/packages/NetworkManager-kde4/` e
- `/usr/share/doc/packages/NetworkManager-gnome/`.

Samba

Com o Samba, uma máquina Unix pode ser configurada como um servidor de arquivos e de impressão para máquinas Mac OS X, Windows e OS/2. O Samba se tornou um produto completo e bastante complexo. Configure o Samba com o YaST, o SWAT (uma interface da Web) ou editando manualmente o arquivo de configuração.

24.1 Terminologia

A seguir são apresentados alguns termos usados na documentação do Samba e no módulo do YaST.

Protocolo SMB

O Samba usa o protocolo SMB (bloco de mensagens do servidor), que é baseado nos serviços NetBIOS. A Microsoft lançou o protocolo para que outros fabricantes de software pudessem estabelecer conexões com uma rede de domínio Microsoft. Com o Samba, o protocolo SMB opera acima do protocolo TCP/IP, de modo que este último precisa estar instalado em todos os clientes.

Protocolo CIFS

O protocolo CIFS (sistema de arquivos da Internet comuns) é outro protocolo que possui suporte no Samba. O CIFS é um protocolo de acesso padrão a sistemas de arquivos remotos para utilização pela rede, permitindo que grupos de usuários trabalhem juntos e compartilhem documentos pela rede.

NetBIOS

NetBIOS é uma interface de software (API) projetada para a comunicação entre máquinas que fornecem serviço de nomes. Ele permite que máquinas conectadas à rede reservem nomes para si. Após a reserva, essas máquinas podem ser tratadas pelo nome. Não há um processo central para a verificação de nomes. Qualquer máquina da rede pode reservar quantos nomes quiser, contanto que os nomes não estejam em uso ainda. A interface NetBIOS pode ser implementada para diferentes arquiteturas de rede. Uma implementação que funciona com relativa proximidade com o hardware da rede é chamada de NetBEUI, mas ela muitas vezes é chamada de NetBIOS. Os protocolos de rede implementados com o NetBIOS são o IPX da Novell (NetBIOS via TCP/IP) e TCP/IP.

Os nomes de NetBIOS enviados por TCP/IP não possuem nada em comum com os nomes usados em `/etc/hosts` ou com os nomes definidos pelo DNS. O NetBIOS usa sua própria convenção de nomes independente. Contudo, é recomendável usar nomes que correspondam aos nomes de hosts DNS para facilitar a administração ou usar o DNS nativamente. Esse é o padrão usado pelo Samba.

servidor Samba

O servidor Samba fornece serviços SMB/CIFS e serviços de nomeação NetBIOS por IP aos clientes. Para o Linux, existem três daemons para um servidor Samba: `smnd` para serviços SMB/CIFS, `nmbd` para serviços de nomeação e `winbind` para autenticação.

cliente Samba

O cliente Samba é um sistema que usa serviços Samba de um servidor Samba pelo protocolo SMB. Todos os sistemas operacionais comuns, como Mac OS X, Windows e OS/2, prestam suporte ao protocolo SMB. O protocolo TCP/IP precisa estar instalado em todos os computadores. O Samba fornece um cliente para as diferentes versões do UNIX. No caso do Linux, há um módulo de kernel para SMB que permite a integração de recursos SMB no nível de sistema Linux. Não é necessário executar nenhum daemon para o cliente Samba.

Compartilhamentos

Os servidores SMB oferecem recursos aos clientes por meio de compartilhamentos. Compartilhamentos são impressoras e diretórios com seus subdiretórios no servidor. Ele é exportado por meio de um nome e pode ser acessado pelo nome. O nome do compartilhamento pode ser definido por qualquer nome; não precisa ser o nome do diretório de exportação. Uma impressora também recebe um nome. Os clientes podem acessar a impressora pelo nome.

DC

Um controlador de domínio (DC) é um servidor que gerencia contas em domínios. Para a replicação de dados, os controladores de domínio adicionais estão disponíveis em um domínio.

24.2 Configurando um servidor Samba

Para configurar um servidor Samba, consulte a documentação do SUSE Linux Enterprise Server.

24.3 Configurando clientes

Os clientes somente podem acessar o servidor Samba via TCP/IP. O NetBEUI e o NetBIOS via IPX não podem ser usados com o Samba.

24.3.1 Configurando um cliente Samba com o YaST

Configure um cliente Samba para acessar recursos (arquivos ou impressoras) no servidor Samba. Digite o domínio ou o grupo de trabalho na caixa de diálogo *Serviços de Rede > Participação no Domínio do Windows*. Se você ativar *Usar também informações SMB para a Autenticação de Linux*, a autenticação do usuário será executada no servidor Samba. Após concluir todas as configurações, clique em *Concluir* para finalizar a configuração.

24.4 Samba como servidor de login

Em redes onde se encontram predominantemente clientes Windows, muitas vezes é preferível que os usuários somente possam se registrar com uma conta e senha válidos. Em uma rede baseada no Windows, essa tarefa é gerenciada por um PDC (primary domain controller - controlador de domínio primário). Você pode usar um servidor Windows NT configurado como PDC, mas essa tarefa também pode ser executada com

um servidor Samba. As entradas a serem feitas na seção `[global]` de `smb.conf` aparecem em Exemplo 24.1, “Seção global em `smb.conf`” (p 346).

Exemplo 24.1 *Seção global em `smb.conf`*

```
[global]
    workgroup = TUX-NET
    domain logons = Yes
    domain master = Yes
```

Se forem usadas senhas criptografadas para fins de verificação, os servidores Samba devem ser capazes de gerenciá-las. A entrada `encrypt passwords = yes` na seção `[global]` permite isso (com a versão 3 do Samba, esse passa a ser o padrão). Além disso, é necessário preparar contas e senhas de usuários em formato de criptografia compatível com o Windows. Para isso, use o comando `smbpasswd -a name`. Crie a conta de domínio dos computadores, exigida pelo conceito de domínio do Windows, com os seguintes comandos:

```
useradd hostname\$
smbpasswd -a -m hostname
```

Com o comando `useradd`, um símbolo de cifrão é adicionado. O comando `smbpasswd` insere esse símbolo automaticamente quando o parâmetro `-m` é usado. O exemplo de configuração comentado (`/usr/share/doc/packages/samba/examples/smb.conf.SUSE`) contém configurações que automatizam essa tarefa.

```
add machine script = /usr/sbin/useradd -g nogroup -c "NT Machine Account" \
-s /bin/false %m\$
```

Para certificar-se de que o Samba possa executar esse script corretamente, escolha um usuário do Samba com as permissões de administrador necessárias e adicione-o ao grupo `ntadmin`. Em seguida, será possível atribuir a todos os usuários pertencentes a esse grupo Linux o status de Domain Admin com o comando:

```
net groupmap add ntgroup="Domain Admins" unixgroup=ntadmin
```

Para obter mais informações sobre este tópico, consulte o Capítulo 12 do HOWTO do Samba 3, encontrado em `/usr/share/doc/packages/samba/Samba3-HOWTO.pdf`.

24.5 Para obter mais informações

Informações detalhadas sobre o Samba estão disponíveis na documentação digital. Para obter mais documentação e exemplos online, digite `apropos samba` na linha de comando para exibir algumas páginas de manual ou simplesmente pesquise no diretório `/usr/share/doc/packages/samba`, se a documentação do Samba estiver instalada. Um exemplo de configuração comentado (`smb.conf.SUSE`) encontra-se no subdiretório `examples`.

O HOWTO do Samba 3, fornecido pela equipe Samba, inclui uma seção sobre a solução de problemas. Além disso, a Parte V do documento oferece um guia passo a passo para a verificação da configuração. O HOWTO do Samba 3 poderá ser encontrado em `/usr/share/doc/packages/samba/Samba3-HOWTO.pdf` após a instalação do pacote `samba-doc`.

Compartilhando sistemas de arquivos com o NFS

25

Distribuir e compartilhar sistemas de arquivos em uma rede é uma tarefa comum em ambientes corporativos. O sistema NFS comprovado funciona junto com o NIS, o protocolo de yellow pages. Para saber sobre um protocolo mais seguro que funcione junto com o LDAP e também possa usar Kerberos, confira o NFSv4.

O NFS com o NIS torna uma rede transparente para o usuário. Com o NFS, é possível distribuir sistemas de arquivos arbitrários pela rede. Com a configuração adequada, os usuários sempre ficam no mesmo ambiente, independentemente do terminal que estejam usando.

25.1 Instalando o software necessário

Para configurar seu host como cliente NFS, você não precisa instalar software adicional. Todos os pacotes necessários para configurar um cliente NFS são instalados por padrão.

25.2 Importando sistemas de arquivos com o YaST

Usuários autorizados podem montar diretórios NFS de um servidor NFS na árvore de arquivos local usando o módulo de cliente NFS do YaST. Clique em *Adicionar* e digite o nome de host do servidor NFS, o diretório a ser importado e o ponto de montagem

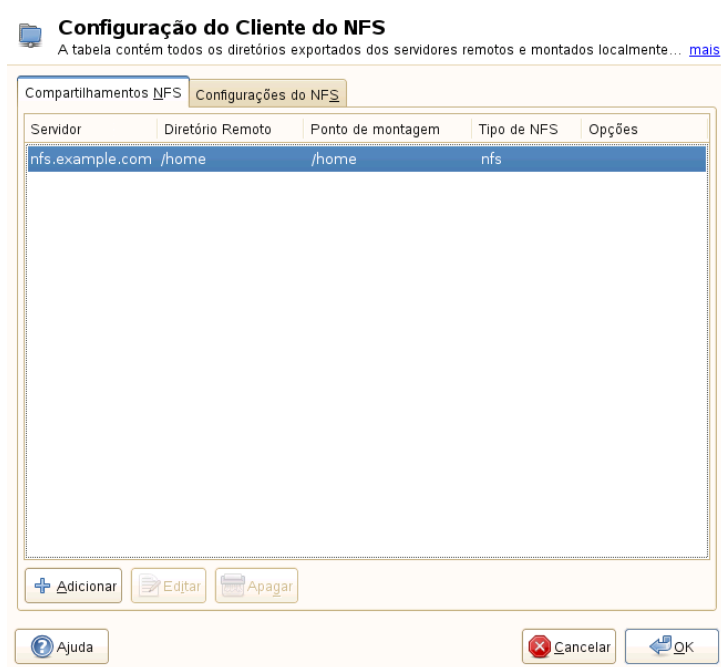
no qual esse diretório deve ser montado localmente. As mudanças terão efeito depois que *Concluir* for clicado na primeira caixa de diálogo.

Na guia *Configurações do NFS*, habilite *Abrir Porta no Firewall* para permitir que computadores remotos acessem o serviço. O status do firewall é mostrado próximo à caixa de seleção. Ao usar o NFSv4, verifique se a caixa de seleção *Habilitar NFSv4* está habilitada e se *Nome de Domínio NFSv4* contém o mesmo valor usado pelo servidor NFSv4. O domínio padrão é *localdomain*.

Clique em *OK* para gravar as mudanças. Consulte a Figura 25.1, “Configuração do cliente NFS no YaST” (p 350).

A configuração é gravada em */etc/fstab* e os sistemas de arquivos especificados são montados. Quando você iniciar o cliente de configuração do YaST posteriormente, ele também lerá a configuração existente desse arquivo.

Figura 25.1 *Configuração do cliente NFS no YaST*



25.3 Importando sistemas de arquivos manualmente

O pré-requisito para importar os sistemas de arquivos manualmente de um servidor NFS é um mapeador de portas RPC em execução. Comece digitando `rcrepcbind start` enquanto usuário `root`. Em seguida, os sistemas de arquivos exportados remotamente podem ser montados no sistema de arquivos como as partições locais usando `mount` da seguinte maneira:

```
mount host:remote-path local-path
```

Para importar os diretórios de usuário da máquina do `nfs.example.com`, por exemplo, use:

```
mount nfs.example.com:/home /home
```

25.3.1 Usando o serviço de montagem automática

O daemon `autofs` pode ser usado para montar sistemas de arquivos remotos automaticamente. Adicione a seguinte entrada ao seu arquivo `/etc/auto.master`:

```
/nfsmounts /etc/auto.nfs
```

Agora, o diretório `/nfsmounts` atuará como raiz para todas as montagens NFS no cliente se o arquivo `auto.nfs` for preenchido adequadamente. O nome `auto.nfs` foi escolhido por mera conveniência; você pode escolher qualquer nome. Adicione entradas ao `auto.nfs` para todas as montagens NFS da seguinte maneira:

```
localdata -fstype=nfs server1:/data  
nfs4mount -fstype=nfs4 server2:/
```

Ative as configurações com `rcautofs start` enquanto `root`. Neste exemplo, `/nfsmounts/localdata`, o diretório `/data` do `server1`, é montado com NFS e `/nfsmounts/nfs4mount`, do `server2`, é montado com NFSv4.

Se o arquivo `/etc/auto.master` for editado enquanto o serviço `autofs` estiver em execução, o automontador deverá ser reiniciado com `rcautofs restart` para que as mudanças tenham efeito.

25.3.2 Editando /etc/fstab manualmente

Uma entrada de montagem típica do NFSv3 em `/etc/fstab` tem aparência semelhante a esta:

```
nfs.example.com:/data /local/path nfs rw,noauto 0 0
```

As montagens NFSv4 também podem ser adicionadas ao arquivo `/etc/fstab`. Para essas montagens, use `nfs4` em vez de `nfs` na terceira coluna e verifique se o sistema de arquivos remoto aparece como `/` após o `nfs.example.com`: na primeira coluna. Uma linha de amostra de uma montagem NFSv4 em `/etc/fstab` tem aparência semelhante a esta:

```
nfs.example.com:/ /local/pathv4 nfs4 rw,noauto 0 0
```

A opção `noauto` impede que o sistema de arquivos seja montado automaticamente na inicialização. Se desejar montar o respectivo sistema de arquivos manualmente, é possível abreviar o comando de montagem especificando apenas o ponto de montagem:

```
mount /local/path
```

Observe que, se você não digitar a opção `noauto`, os scripts de inicialização do sistema gerenciarão a montagem dos sistemas de arquivos na inicialização.

25.4 NFS com Kerberos

Para usar a autenticação Kerberos para o NFS, é preciso que a segurança GSS esteja habilitada. Para fazer isso, selecione *Habilitar Segurança GSS* na caixa de diálogo inicial do YaST. É preciso ter um servidor Kerberos ativo para usar esse recurso. O YaST não configura o servidor, ele apenas usa a funcionalidade em questão. Se você quiser usar a autenticação Kerberos além da configuração do YaST, conclua pelo menos as etapas seguintes antes de executar a configuração do NFS:

- 1 Verifique se o servidor e o cliente estão no mesmo domínio Kerberos. Eles precisam acessar o mesmo servidor KDC (Key Distribution Center - Centro de Distribuição de Chaves) e compartilhar o arquivo `krb5.keytab` (o local padrão em qualquer máquina é `/etc/krb5.keytab`).
- 2 Inicie o serviço `gssd` no cliente com `rcgssd start`.

Para obter mais informações sobre como configurar o NFS que usa Kerberos, consulte os links na Seção 25.5, “Para obter mais informações” (p 353).

25.5 Para obter mais informações

Além das páginas de manual de `exports`, `nfs` e `mount`, há informações disponíveis sobre como configurar servidores e clientes NFS em `/usr/share/doc/packages/nfsidmap/README`. A documentação online encontra-se nos seguintes documentos da Web:

- A documentação técnica online encontra-se no SourceForge [<http://nfs.sourceforge.net/>].
- Para obter instruções sobre como configurar o NFS que usa Kerberos, consulte o documento NFS Version 4 Open Source Reference Implementation [<http://www.citi.umich.edu/projects/nfsv4/linux/krb5-setup.html>] (Implementação da referência de código-fonte aberto do NFSv4).
- Se você tiver dúvidas sobre o NFSv4, consulte as Perguntas frequentes do Linux NFSv4 [<http://www.citi.umich.edu/projects/nfsv4/linux/faq/>].

Sincronização de arquivos

Atualmente, muitas pessoas usam vários computadores; um computador em casa, um ou mais no trabalho e, possivelmente, um laptop ou PDA quando viajam. Vários arquivos são necessários em todos esses computadores. Talvez você queira trabalhar com todos os computadores e modificar os arquivos, de modo que a versão mais recente dos dados fique disponível em todos os computadores.

26.1 Software de sincronização de dados disponível

A sincronização de dados não é um problema para computadores permanentemente conectados por uma rede rápida. Nesse caso, use um sistema de arquivos de rede, como o NFS, e armazene os arquivos em um servidor para que todos os hosts acessem os mesmos dados via rede. Essa abordagem será impossível se a conexão de rede for instável ou não permanente. Quando você viaja com um laptop, precisa ter cópias de todos os arquivos necessários no disco rígido local. Entretanto, é necessário sincronizar os arquivos modificados. Quando você modificar um arquivo em um computador, verifique se uma cópia dele foi atualizada em todos os outros computadores. No caso de cópias ocasionais, elas podem ser feitas manualmente com o scp ou o rsync. Entretanto, se vários arquivos forem envolvidos, o procedimento poderá ser complicado e demandar muito cuidado para evitar erros, como a sobregravação de um arquivo novo por um antigo.

ATENÇÃO: risco de perda de dados

Antes de começar a gerenciar seus dados com um sistema de sincronização, você deve se informar sobre o programa usado e testar sua funcionalidade. É indispensável ter um backup de arquivos importantes.

A tarefa prolongada e sujeita a erros de sincronizar dados manualmente pode ser evitada se você usar um dos programas que utilizam vários métodos para automatizá-la. Os resumos a seguir têm o simples objetivo de dar uma visão geral sobre como esses programas funcionam e como podem ser usados. Se você planeja usá-los, leia a documentação do programa.

26.1.1 CSV

O CVS, que é mais usado para gerenciar versões de origem de programas, oferece a possibilidade de manter cópias dos arquivos em vários computadores. Dessa forma, ele também é adequado para sincronização de dados. O CVS mantém um repositório central no servidor, no qual os arquivos e as mudanças feitas neles são gravados. As mudanças realizadas localmente são enviadas para o repositório e podem ser recuperadas de outros computadores por meio de uma atualização. Todos os procedimentos devem ser iniciados pelo usuário.

O CVS é muito suscetível a erros quando ocorrem mudanças em vários computadores. As mudanças são fundidas e, se ocorrerem nas mesmas linhas, um conflito será reportado. Quando ocorre um conflito, o banco de dados permanece em estado consistente. O conflito só fica visível para resolução no host cliente.

26.1.2 rsync

Quando o controle de versão não é necessário, mas grandes estruturas de diretório precisam ser sincronizadas em conexões de rede lentas, a ferramenta rsync oferece mecanismos avançados para a transmissão apenas de mudanças entre arquivos. Isso não diz se aplica apenas a arquivos de texto, mas também a arquivos binários. Para detectar as diferenças entre os arquivos, o rsync os subdivide em blocos e realiza checksums neles.

O esforço dedicado à detecção das mudanças tem um preço. Os sistemas a serem sincronizados devem ser dimensionados generosamente para uso do rsync. A RAM é especialmente importante.

26.2 Determinando fatores para selecionar um programa

Há alguns fatores importantes a serem considerados ao decidir que programa será usado.

26.2.1 Cliente-servidor versus ponto a ponto

Dois modelos diferentes são comumente usados para distribuir dados. No primeiro modelo, todos os clientes sincronizam seus arquivos com um servidor central. O servidor deve ser acessível a todos os clientes pelo menos ocasionalmente. Esse modelo é usado pelo CVS.

A outra possibilidade é deixar todos os hosts ligados em rede sincronizarem seus dados entre os pontos uns dos outros. O rsync funciona de fato no modo cliente, mas qualquer cliente também pode atuar como servidor.

26.2.2 Portabilidade

O CVS e o rsync também estão disponíveis para muitos outros sistemas operacionais, incluindo vários sistemas Unix e Windows.

26.2.3 Interativo versus automático

No CVS, a sincronização de dados começa manualmente pelo usuário. Isso permite um controle fino dos dados a serem sincronizados e um fácil gerenciamento de conflitos. No entanto, se os intervalos de sincronização forem muito longos, será mais provável que ocorram conflitos.

26.2.4 Conflitos: incidência e solução

Conflitos só ocorrem raramente no CVS, mesmo quando há muitas pessoas trabalhando em um grande projeto de programa. Isso ocorre porque os documentos são fundidos na base de linhas individuais. Quando ocorre um conflito, somente um cliente é afetado. Normalmente, os conflitos no CVS podem ser facilmente resolvidos.

Não há gerenciamento de conflitos no `rsync`. O usuário é responsável por não sobregravar acidentalmente arquivos e resolver manualmente todos os possíveis conflitos. Por segurança, é possível empregar também um sistema de controle de versão.

26.2.5 Selecionando e adicionando arquivos

No CVS, diretórios e arquivos novos devem ser adicionados explicitamente com o comando `cvcs add`. Esse procedimento resulta em um maior controle do usuário sobre os arquivos a serem sincronizados. Por outro lado, novos arquivos são sempre ignorados, especialmente quando os pontos de interrogação na saída de `cvcs update` são ignorados devido ao grande número de arquivos.

26.2.6 Histórico

Um recurso adicional do CVS é a possibilidade de reconstrução de versões antigas de arquivos. Um breve comentário de edição pode ser inserido em cada mudança, e o desenvolvimento dos arquivos pode ser facilmente rastreado posteriormente com base no conteúdo dos comentários. Essa é uma ajuda valiosa para textos de teses e de programas.

26.2.7 Volume de dados e requisitos do disco rígido

Os discos rígidos de todos os hosts envolvidos devem ter espaço em disco suficiente para todos os dados distribuídos. O CVS requer espaço adicional para o banco de dados de repositório no servidor. O histórico do arquivo também é armazenado no servidor, requerendo ainda mais espaço. Quando arquivos em formato de texto são mudados,

somente as linhas modificadas são gravadas. Arquivos binários requerem espaço em disco adicional relativo ao tamanho do arquivo sempre que ele for mudado.

26.2.8 GUI

Usuários experientes normalmente executam o CVS a partir da linha de comando. Entretanto, há interfaces gráficas do usuário disponíveis para Linux (como a cervisia) e para outros sistemas operacionais (como a wincvs). Muitas ferramentas de desenvolvimento (como a kdevelop) e editores de texto (como o Emacs) fornecem suporte ao CVS. É sempre mais fácil realizar a resolução de conflitos com esses front ends.

26.2.9 Facilidade de uso

O rsync é bastante fácil de usar, sendo também adequado para principiantes. O CVS é um pouco mais difícil de operar. Os usuários devem entender a interação entre o repositório e os dados locais. As mudanças dos dados devem ser primeiro fundidas localmente no repositório. Esse procedimento é feito com o comando `cvs update`. Em seguida, as mudanças devem ser retornadas ao repositório com o comando `cvs commit`. Depois de compreender esse procedimento, os usuários principiantes também serão capazes de usar o CVS com facilidade.

26.2.10 Segurança contra ataques

Durante a transmissão, o ideal é proteger os dados contra interceptação e manipulação. O CVS e o rsync podem ser facilmente usados via ssh (secure shell), fornecendo segurança contra ataques deste tipo. A execução do CVS via rsh (remote shell) deve ser evitada. O acesso ao CVS com o mecanismo *pserver* em redes desprotegidas também não é recomendável.

26.2.11 Proteção contra perda de dados

O CVS tem sido usado por desenvolvedores por um longo tempo para gerenciar projetos de programas e é extremamente estável. Como o histórico do desenvolvimento é gravado,

o CVS fornece proteção até mesmo contra certos erros do usuário, como uma exclusão não intencional de um arquivo.

Tabela 26.1 *Recursos das Ferramentas de Sincronização de Arquivos: -- = muito ruim, - = ruim ou indisponível, o = médio, + = bom, ++ = excelente, x = disponível*

	CSV	rsync
Cliente/Servidor	C-S	C-S
Portabilidade	Lin,Un*x,Win	Lin,Un*x,Win
Interatividade	x	x
Velocidade	o	+
Conflitos	++	o
Sel. de arquivos	Sel./arq., dir.	Dir.
Histórico	x	-
Espaço em disco rígido	--	o
Interface gráfica do usuário (GUI)	o	-
Dificuldade	o	+
Ataques	+(ssh)	+(ssh)
Perda de dados	++	+

26.3 Introdução ao CVS

O CVS é adequado para fins de sincronização, caso arquivos específicos sejam editados com frequência e sejam armazenados em um formato de arquivo, como texto ASCII, ou como texto de origem de programa. O uso do CVS para sincronizar dados em outros

formatos (como arquivos JPEG) é possível, mas gera grandes volumes de dados, pois todas as variantes de um arquivo ficam armazenadas permanentemente no servidor CVS. Nesses casos, não é possível usar a maioria dos recursos do CVS. O uso do CVS para sincronizar arquivos só será possível se todas as estações de trabalho puderem acessar o mesmo servidor.

26.3.1 Configurando um servidor CVS

O *servidor* é o host em que todos os arquivos válidos se localizam, incluindo as versões mais recentes de todos os arquivos. Qualquer estação de trabalho estacionária pode ser usada como um servidor. Se possível, os dados do repositório do CVS devem ser incluídos em backups regulares.

Durante a configuração de um servidor CVS, é uma boa idéia conceder aos usuários o acesso ao servidor via SSH. Se o usuário for conhecido pelo servidor como `tux` e o software do CVS estiver instalado tanto no servidor quanto no cliente, as variáveis de ambiente a seguir deverão ser definidas no lado do cliente:

```
CVS_RSH=ssh CVSROOT=tux@server:/serverdir
```

O comando `cvs init` pode ser usado para inicializar o servidor CVS no lado cliente. Esse procedimento deve ser executado apenas uma vez.

Finalmente, é necessário designar um nome à sincronização. Selecione ou crie um diretório no cliente para conter arquivos a serem gerenciados com o CVS (o diretório também pode ficar vazio). O nome do diretório também será o nome da sincronização. Neste exemplo, o diretório é chamado de `synchome`. Vá para esse diretório e digite o comando a seguir para definir o nome de sincronização como `synchome`:

```
cvs import synchome tux wilber
```

Vários comandos do CVS requerem um comentário. Para essa finalidade, o CVS inicia um editor (o editor definido na variável do ambiente `$EDITOR` ou `vi`, se nenhum editor tiver sido definido). A chamada do editor pode ser evitada se você inserir o comentário antes na linha de comando, como no exemplo a seguir:

```
cvs import -m 'this is a test' synchome tux wilber
```

26.3.2 Usando o CVS

O repositório de sincronização agora pode ter a saída registrada de todos os hosts com `cvs co synchome`. Esse procedimento cria um novo subdiretório `synchome` no cliente. Para confirmar suas mudanças ao servidor, vá para o diretório `synchome` (ou um de seus subdiretórios) e digite `cvs commit`.

Por padrão, todos os arquivos (incluindo subdiretórios) são confirmados no servidor. Para confirmar apenas determinados arquivos ou diretórios individuais, especifique-os como em `cvs commit arquivo1 diretório1`. É necessário adicionar novos arquivos e diretórios ao repositório com um comando como `cvs add arquivo1 diretório1` antes de confirmá-los no servidor. Depois disso, confirme os arquivos e diretórios recém-adicionados com `cvs commit arquivo1 diretório1`.

Se você for para outra estação de trabalho, registre a saída do repositório de sincronização, caso isso não tenha sido feito em uma sessão anterior na mesma estação de trabalho.

Inicie a sincronização com o servidor com `cvs update`. Atualize arquivos ou diretórios individuais como em `cvs update arquivo1 diretório1`. Para ver a diferença entre os arquivos atuais e versões armazenadas no servidor, use o comando `cvs diff` ou `cvs diff arquivo1 diretório1`. Use `cvs -nq update` para ver quais arquivos podem ser afetados por uma atualização.

Estes são alguns símbolos de status exibidos durante uma atualização:

U

A versão local foi atualizada. Isso afeta todos os arquivos fornecidos pelo servidor e ausentes no sistema local.

M

A versão local foi modificada. Se havia mudanças no servidor, foi possível fundir as diferenças na cópia local.

P

A versão local foi corrigida com a versão do servidor.

C

O arquivo local está em conflito com a versão atual do repositório.

?

Este arquivo não existe no CVS.

O status M indica um arquivo modificado localmente. Envie a cópia local para o servidor ou remova o arquivo local e execute a atualização novamente. Nesse caso, o arquivo ausente será recuperado do servidor. Se você enviar um arquivo modificado localmente e ele tiver sido mudado na mesma linha de comando e enviado, poderá haver um conflito, indicado por C.

Nesse caso, observe as marcas de conflito (“>” e “<”) no arquivo e decida-se entre as duas versões. Como essa tarefa pode ser desagradável, você pode abandonar as mudanças, apagar o arquivo local e digitar `cvsv up` para recuperar a versão atual do servidor.

26.4 Introdução ao rsync

O rsync será útil quando for necessário transmitir grandes quantidades de dados regularmente, sem que haja muitas mudanças. Esse é, por exemplo, sempre o caso da criação de backups. Uma outra aplicação diz respeito a servidores para teste. Esses servidores armazenam árvores completas de diretório de servidores Web regularmente espelhadas em um servidor Web em um DMZ.

26.4.1 Configuração e operação

O rsync pode ser operado em dois modos diferentes. Ele pode ser usado para arquivar ou copiar dados. Para isso, somente um shell remoto, como o ssh, é necessário no sistema de destino. Entretanto, o rsync também pode ser usado como um daemon para fornecer diretórios à rede.

O modo de operação básica do rsync não requer qualquer configuração especial. O rsync permite diretamente o espelhamento de diretórios inteiros em outro sistema. Como

exemplo, o comando a seguir cria um backup do diretório pessoal do tux em um servidor de backup denominado sun:

```
rsync -baz -e ssh /home/tux/ tux@sun:backup
```

O comando a seguir é usado para reproduzir o diretório de volta:

```
rsync -az -e ssh tux@sun:backup /home/tux/
```

Até esse ponto, o gerenciamento não é muito diferente do de uma ferramenta de cópia comum, como o scp.

O rsync deve ser operado no modo “rsync” para que todos os recursos fiquem totalmente disponíveis. Isso é feito ao se iniciar o daemon rsyncd em mais de um sistema.

Configure-o no arquivo `/etc/rsyncd.conf`. Por exemplo, para tornar o diretório `/srv/ftp` disponível com o rsync, use a seguinte configuração:

```
gid = nobody
uid = nobody
read only = true
use chroot = no
transfer logging = true
log format = %h %o %f %l %b
log file = /var/log/rsyncd.log
```

```
[FTP]
```

```
path = /srv/ftp
comment = An Example
```

Em seguida, inicie o rsyncd com `rcrsyncd start`. O rsyncd também pode ser iniciado automaticamente durante o processo de boot. Configure esse recurso ativando o serviço no editor de nível de execução fornecido pelo YaST ou digitando manualmente o comando `insserv rsyncd`. O rsyncd também pode ser iniciado com `xinetd`. Entretanto, isso só é recomendável para servidores que raramente usam o rsyncd.

O exemplo também cria um arquivo de registro listando todas as conexões. Esse arquivo é armazenado em `/var/log/rsyncd.log`.

Então será possível testar a transferência de um sistema cliente. Faça isso com o seguinte comando:

```
rsync -avz sun::FTP
```

Esse comando lista todos os arquivos presentes no diretório `/srv/ftp` do servidor. Essa solicitação também é registrada no arquivo de registro `/var/log/rsyncd`

`.log`. Para iniciar uma transferência real, forneça um diretório de destino. Use `.` para o diretório atual. Por exemplo:

```
rsync -avz sun::FTP .
```

Por padrão, nenhum arquivo será apagado durante a sincronização com o `rsync`. Se esse procedimento for forçado, a opção adicional `--delete` deverá ser expressa. Para garantir que nenhum arquivo novo seja apagado, use a opção `--update` como alternativa. Qualquer conflito ocorrido deve ser resolvido manualmente.

26.5 Para obter mais informações

CSV

Informações importantes sobre o CVS encontram-se na home page <http://www.cvshome.org>.

rsync

Informações importantes sobre o `rsync` são fornecidas nas páginas de manual `man rsync` e `man rsyncd.conf`. Uma referência técnica sobre os princípios de operação do `rsync` pode ser encontrada em `/usr/share/doc/packages/rsync/tech_report.ps`. As notícias mais recentes sobre o `rsync` encontram-se no site do projeto na Web, em <http://rsync.samba.org/>.

Parte V. Solução de problemas

Ajuda e documentação

O SUSE® Linux Enterprise Desktop é fornecido com várias fontes de informações e documentação, muitas das quais já integradas no sistema instalado:

Documentação em `/usr/share/doc`

Esse diretório de ajuda tradicional contém vários arquivos de documentação e notas de versão do seu sistema. Mais informações podem ser encontradas na Seção 27.1, “Diretório da documentação” (p 370).

Páginas de manual e páginas de informações para comandos do shell

Ao trabalhar com o shell, você não precisa saber de cor as opções de comandos. Tradicionalmente, o shell oferece ajuda integrada por meio das páginas de manual e de informações. Leia mais na Seção 27.2, “Páginas de manual” (p 372) e na Seção 27.3, “Páginas de informações” (p 373).

Centros de ajuda da área de trabalho

Os centros de ajuda da área de trabalho KDE (KDE help center) e da área de trabalho GNOME (Yelp) oferecem acesso centralizado aos recursos de documentação mais importantes no sistema na forma pesquisável. Esses recursos incluem ajuda online para os aplicativos instalados, páginas de manual, páginas de informações e os manuais do Novell/SUSE fornecidos com o produto.

Pacotes de Ajuda separados para alguns aplicativos

Quando você instala o novo software com o YaST, a documentação do software é instalada automaticamente (na maioria dos casos) e normalmente aparece no centro de ajuda da área de trabalho. Contudo, alguns aplicativos, como o GIMP, podem ter diversos pacotes de ajuda online a serem instalados separadamente com o YaST e que não se integram aos centros de ajuda.

27.1 Diretório da documentação

O diretório tradicional para encontrar a documentação do sistema Linux instalado é `/usr/share/doc`. Geralmente, o diretório contém informações sobre os pacotes instalados no sistema, bem como notas de versão, manuais e muito mais.

NOTA: o conteúdo depende dos pacotes instalados

No mundo do Linux, muitos manuais e outros tipos de documentação estão disponíveis na forma de pacotes, assim como um software. As informações encontradas em `/usr/share/docs` também dependem dos pacotes (de documentação) instalados. Se você não encontrar os subdiretórios mencionados aqui, verifique se os respectivos pacotes estão instalados no seu sistema e adicione-os com o YaST, se necessário.

27.1.1 Manuais Novell/SUSE

Fornecemos versões em HTML e PDF dos nossos manuais em idiomas diferentes. No subdiretório `manual`, você encontra as versões em HTML de quase todos os manuais Novell/SUSE disponíveis para o seu produto. Para obter uma visão geral de toda a documentação disponível para o seu produto, consulte o prefácio dos manuais.

Se houver mais de um idioma instalado, `/usr/share/doc/manual` poderá conter versões em idiomas diferentes dos manuais. As versões em HTML dos manuais Novell/SUSE também estão disponíveis no centro de ajuda de ambas as áreas de trabalho. Para obter informações sobre onde encontrar as versões em PDF e HTML dos manuais na mídia de instalação, consulte as Notas de Versão do SUSE Linux Enterprise Desktop. Elas estão disponíveis no sistema instalado, no diretório `/usr/share/doc/release-notes/`, ou online, na página da Web específica do produto em <http://www.novell.com/documentation/>.

27.1.2 HOWTOs

Se o pacote `howto` estiver instalado no sistema, `/usr/share/doc` também conterá o subdiretório `howto`, no qual você encontra documentação adicional de muitas tarefas relacionadas a configuração e operação do software Linux.

27.1.3 Documentação do pacote

Em `packages`, você encontra a documentação incluída nos pacotes de software instalados no seu sistema. Para qualquer pacote, é criado um subdiretório `/usr/share/doc/packages/nome_do_pacote`. Ele geralmente contém arquivos `README` do pacote e às vezes exemplos, arquivos de configuração ou scripts adicionais. A lista a seguir apresenta arquivos típicos encontrados em `/usr/share/doc/packages`. Nenhuma dessas entradas é obrigatória e muitos pacotes podem incluir apenas alguns deles.

AUTHORS

Lista dos principais desenvolvedores.

BUGS

Bugs ou falhas conhecidos. Pode conter também um link para uma página do Bugzilla na Web, onde é possível pesquisar todos os bugs.

CHANGES , ChangeLog

Resumo de mudanças de versão para versão. Geralmente interessante para desenvolvedores, pois é bastante detalhado.

COPYING , LICENSE

Informações sobre licenciamento.

FAQ

Perguntas e respostas coletadas em listas de endereçamento ou grupos de notícias.

INSTALL

Como instalar esse pacotes no seu sistema. Visto que o pacote já estará instalado no momento em que você ler este arquivo, você poderá ignorar o conteúdo do arquivo com segurança.

README, README.*

Informações gerais sobre o software. Por exemplo, a finalidade e o modo de usá-lo.

TODO

Itens ainda não implementados, mas que provavelmente serão no futuro.

MANIFEST

Lista de arquivos com um breve resumo.

NEWS

Descrição do que há de novo nesta versão.

27.2 Páginas de manual

Páginas de manual são uma parte essencial de qualquer sistema Linux. Elas explicam o uso de um comando e todos os parâmetros e opções disponíveis. As páginas de manual podem ser acessadas com `man` seguido do nome do comando, por exemplo, `man ls`.

As páginas de manual são exibidas diretamente no shell. Para navegar nelas, mova-se para cima e para baixo com **Page ↑** e **Page ↓**. Desloque-se entre o início e o fim do documento com **Home** e **End**. Conclua esta exibição pressionando **Q**. Aprenda mais sobre o próprio comando `man` com `man man`. Páginas de manual são classificadas em categorias, como mostrado na Tabela 27.1, “Páginas de manual — categorias e descrições” (p 372) (extraída da página de manual do próprio comando `man`).

Tabela 27.1 *Páginas de manual — categorias e descrições*

Número	Descrição
1	Programas executáveis ou comandos de shell
2	Chamadas do sistema (funções fornecidas pelo kernel)
3	Chamadas de biblioteca (funções em bibliotecas de programas)
4	Arquivos especiais (geralmente encontrados em <code>/dev</code>)
5	Convenções e formatos de arquivos (<code>/etc/fstab</code>)
6	Jogos
7	Diversos (incluindo convenções e pacotes de macro); por exemplo, <code>man(7)</code> , <code>groff(7)</code>

Número	Descrição
8	Comandos de administração do sistema (geralmente apenas para o <code>root</code>)
9	Rotinas de kernel (não padrão)

Cada página de manual consiste em várias partes rotuladas *NAME*, *SYNOPSIS*, *DESCRIPTION*, *SEE ALSO*, *LICENSING* e *AUTHOR*. Pode haver seções adicionais disponíveis, dependendo do tipo de comando.

27.3 Páginas de informações

Páginas de informações são outra fonte importante de informações no sistema. Geralmente, elas são mais detalhadas do que as páginas de manual. Para ver a página de informações de um determinado comando, digite `info` seguido pelo nome do comando, por exemplo, `info ls`. Você pode procurar uma página de informações com um viewer diretamente no shell e exibir as seções diferentes, denominadas “nós.” Use `Space` para avançar e `<—` para voltar. Em um nó, você também pode procurar com `Page ↑` e `Page ↓`, mas apenas `Space` e `<—` o levarão também para o nó anterior ou subsequente. Pressione `Q` para sair do modo de visualização. Nem todas as páginas de manual contêm uma página de informações e vice-versa.

Problemas comuns e suas soluções

28

Este capítulo descreve uma gama de problemas em potencial e suas soluções. Mesmo se a sua situação não esteja listada aqui com precisão, poderá haver alguma semelhante que ofereça dicas para a solução do seu problema.

28.1 Localizando e reunindo informações

O Linux reporta os dados de forma bastante detalhada. Há vários lugares a recorrer quando você tem problemas com o seu sistema, a maioria dos quais é padrão para sistemas Linux em geral e alguns são relevantes para os sistemas SUSE Linux Enterprise Desktop. É possível ver a maioria dos arquivos de registro com o YaST (*Miscelânea > Registro de Inicialização*).

O YaST oferece a possibilidade de coletar todas as informações do sistema necessárias à equipe de suporte. Use *Miscelânea > Consulta ao Suporte* e selecione a categoria do problema. Quando todas as informações forem reunidas, anexe-as à sua solicitação de suporte.

Veja a seguir uma lista dos arquivos de registro verificados com mais frequência com a descrição de seus objetivos principais. Os caminhos contendo ~ referem-se ao diretório pessoal do usuário atual.

Tabela 28.1 Arquivos de registro

Arquivo de registro	Descrição
<code>~/.xsession-errors</code>	Mensagens de aplicativos de área de trabalho atualmente em execução.
<code>/var/log/apparmor/</code>	Arquivos de registro do AppArmor, consulte a Parte “Confining Privileges with Novell AppArmor” (↑ <i>Security Guide (Guia de Segurança)</i>) para obter informações detalhadas.
<code>/var/log/audit/audit.log</code>	Arquivo de registro do Audit para monitorar qualquer acesso a arquivos, diretórios ou recursos do seu sistema, bem como rastrear as chamadas do sistema.
<code>/var/log/boot.msg</code>	Mensagens do kernel reportadas durante o processo de boot.
<code>/var/log/mail.*</code>	Mensagens do sistema de correio.
<code>/var/log/messages</code>	Mensagens ininterruptas do kernel e do daemon de registro do sistema (durante a execução).
<code>/var/log/NetworkManager</code>	Arquivo de registro do NetworkManager para a coleta de problemas de conectividade da rede.
<code>/var/log/samba/</code>	Diretório contendo mensagens do registro de cliente e servidor do Samba.
<code>/var/log/SaX.log</code>	Mensagens de hardware do sistema KVM e da tela do SaX.
<code>/var/log/warn</code>	Todas as mensagens do kernel e do daemon do registro do sistema com o nível “warning” ou superior.

Arquivo de registro	Descrição
<code>/var/log/wtmp</code>	Arquivo binário contendo registros de login de usuário para a sessão da máquina atual. Exiba-o com <code>last</code> .
<code>/var/log/Xorg.*.log</code>	Vários registros de inicialização e tempo de execução do sistema X Window. São úteis para depurar inicializações malsucedidas do X.
<code>/var/log/YaST2/</code>	Diretório contendo as ações do YaST e respectivos resultados.
<code>/var/log/zypper.log</code>	Arquivo de registro do zypper.

Além dos arquivos de registro, a sua máquina também lhe fornece informações sobre o sistema em execução. Consulte a Tabela 28.2: Informações do sistema no sistema de arquivos `/proc`.

Tabela 28.2 *Informações do sistema no sistema de arquivos `/proc`*

Arquivo	Descrição
<code>/proc/cpuinfo</code>	Contém informações do processador, incluindo o seu tipo, marca, modelo e desempenho.
<code>/proc/dma</code>	Mostra quais canais DMA estão sendo usados no momento.
<code>/proc/interrupts</code>	Mostra quais interrupções estão em uso e quantas de cada foram usadas.
<code>/proc/iomem</code>	Exibe o status da memória de E/S (entrada/saída).
<code>/proc/ioports</code>	Mostra quais portas de E/S estão em uso no momento.
<code>/proc/meminfo</code>	Exibe o status da memória.

Arquivo	Descrição
/proc/modules	Exibe os módulos individuais.
/proc/mounts	Exibe os dispositivos montados no momento.
/proc/partitions	Mostra o particionamento de todos os discos rígidos.
/proc/version	Exibe a versão atual do Linux.

Além do sistema de arquivos `/proc`, o kernel do Linux exporta informações com o módulo `sysfs`, um sistema de arquivos na memória. Esse módulo representa objetos Kernel, seus atributos e relacionamentos. Para obter mais informações sobre o `sysfs`, consulte o contexto de `udev` no Capítulo 13, *Gerenciamento de dispositivo de kernel dinâmico com udev* (p 163). A Tabela 28.3 contém uma visão geral dos diretórios mais comuns em `/sys`.

Tabela 28.3 Informações do sistema no sistema de arquivos `/sys`

Arquivo	Descrição
/sys/block	Contém subdiretórios para cada dispositivo de bloco descoberto no sistema. Geralmente, esses dispositivos são de tipo de disco.
/sys/bus	Contém subdiretórios para cada tipo de barramento físico.
/sys/class	Contém subdiretórios agrupados como tipos funcionais de dispositivos (como gráficos, de rede, de impressora etc.)
/sys/device	Contém a hierarquia global de dispositivos.

O Linux vem com várias ferramentas para monitoramento e análise do sistema. Consulte o Capítulo 1, *System Monitoring Utilities* (↑*System Analysis and Tuning Guide (Guia de Análise do Sistema e Ajuste)*) para obter uma seleção das mais importantes usadas em diagnósticos de sistema.

Cada um dos seguintes cenários começa com um cabeçalho que descreve o problema, seguido de um ou dois parágrafos apresentando sugestões para solução, referências disponíveis para consultar soluções mais detalhadas e referências cruzadas para outros cenários relacionados.

28.2 Problemas de instalação

Problemas de instalação são situações que ocorrem quando a máquina falha na instalação. Ela pode falhar inteiramente ou talvez não consiga iniciar o instalador gráfico. Esta seção destaca alguns dos problemas típicos que você pode encontrar e oferece soluções ou alternativas possíveis para esses tipos de situações.

28.2.1 Verificação de mídia

Se você tiver qualquer problema ao usar a mídia de instalação do SUSE Linux Enterprise Desktop, verifique a integridade da sua mídia de instalação com *Software > Verificação de Mídia*. Problemas de mídia são mais prováveis com a mídia que você mesmo gravou. Para verificar o meio do SUSE Linux Enterprise Desktop, insira-o na unidade e clique em *Iniciar Verificação* na tela *Verificação de Mídia* do YaST. Isso pode levar alguns minutos. Se forem detectados erros, não use esta mídia para instalação.

Figura 28.1 Verificação de mídia

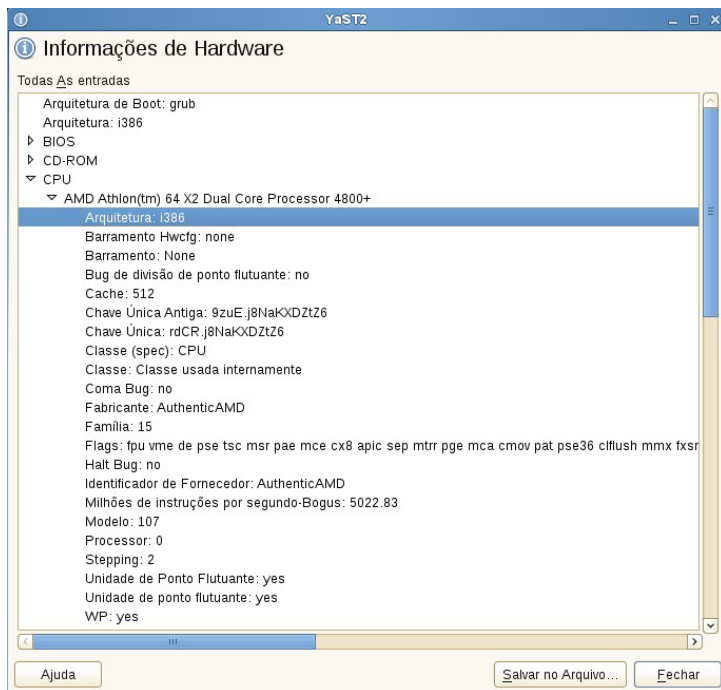


28.2.2 Informações sobre hardware

Exiba hardware detectado e dados técnicos usando *Hardware > Informações de Hardware*. Clique em qualquer nó da árvore para obter mais informações sobre um dispositivo. Este módulo é especialmente útil quando você deseja enviar uma solicitação de suporte para a qual precisa de informações sobre o hardware.

Grave as informações de hardware exibidas em um arquivo clicando em *Salvar no Arquivo*. Selecione o nome de arquivo e diretório desejados e clique em *Salvar* para criar o arquivo.

Figura 28.2 *Exibindo informações sobre hardware*



28.2.3 Nenhuma unidade de DVD inicializável disponível

Se o seu computador não contém uma unidade de DVD-ROM inicializável ou se a que você tem não é suportada pelo Linux, há várias opções para instalar sua máquina sem uma unidade de DVD interna:

Inicializando de um disquete

Crie um disquete de boot e inicialize por ele em vez de inicializar pelo DVD.

Usando um dispositivo de inicialização externo

Se for suportado pelo BIOS e pelo kernel de instalação, inicialize pelas unidades de DVD externas.

Inicialização de rede via PXE

Se uma máquina não tiver uma unidade de DVD, mas oferecer uma conexão de ethernet funcional, execute uma instalação completamente baseada em rede. Consulte a Seção “Remote Installation via VNC—PXE Boot and Wake on LAN” (Capítulo 11, *Remote Installation*, ↑ *Guia de Implantação*) e a Seção “Remote Installation via SSH—PXE Boot and Wake on LAN” (Capítulo 11, *Remote Installation*, ↑ *Guia de Implantação*) para obter detalhes.

Inicializando de um disquete (SYSLINUX)

Em alguns computadores mais antigos, não há unidade de DVD inicializável disponível, mas há uma unidade de disquete. Para instalar em tal sistema, crie discos de inicialização e inicialize seu sistema com eles.

Os discos de boot incluem o carregador denominado SYSLINUX e o programa linuxrc. O SYSLINUX permite a seleção de um kernel durante o procedimento de inicialização e a especificação de quaisquer parâmetros necessários para o hardware usado. O programa linuxrc suporta o carregamento de módulos de kernel para o seu hardware e inicia subsequentemente a instalação.

Quando a inicialização é feita de um disquete de inicialização, o procedimento é iniciado pelo carregador de boot do SYSLINUX (pacote `syslinux`). Quando o sistema é inicializado, o SYSLINUX executa uma detecção mínima de hardware que consiste principalmente nas seguintes etapas:

1. O programa verifica se o BIOS fornece suporte de framebuffer compatível com VESA 2.0 e se inicializa o kernel de forma correspondente.
2. Os dados do monitor (informações de DDC) são lidos.
3. O primeiro bloco do primeiro disco rígido (MBR) é lido para mapear IDs de BIOS para nomes de dispositivos do Linux durante a configuração do carregador de boot.

O programa tenta ler o bloco através das funções lba32 do BIOS para determinar se o BIOS suporta essas funções.

Se você mantiver Shift pressionado quando o SYSLINUX iniciar, todas essas etapas podem ser ignoradas. Para fins de solução de problemas, insira a linha

```
verbose 1
```

em `syslinux.cfg` para o carregador de boot exibir qual ação está sendo executada atualmente.

Se a máquina não inicializar do disquete, você talvez precise mudar a seqüência de inicialização no BIOS para A, C, CDROM.

Dispositivos de inicialização externos

O Linux suporta a maioria das unidades de DVD existentes. Mesmo se o sistema não tiver uma unidade de DVD nem de disquete, ainda será possível usar uma unidade de DVD externa (conectada por USB, FireWire ou SCSI) para inicializar o sistema. Isso depende principalmente da interação entre o BIOS e o hardware usado. Algumas vezes uma atualização do BIOS pode ajudar se você tiver problemas.

28.2.4 Falha na inicialização da mídia de instalação

Um motivo possível para a máquina não inicializar a mídia de instalação é uma configuração incorreta de seqüência de boot no BIOS. A seqüência de boot do BIOS deve ter uma unidade de DVD definida como a primeira entrada de boot. De outra forma, a máquina tentaria inicializar de outro meio, normalmente o disco rígido. Diretrizes para mudar a seqüência de boot do BIOS encontram-se na documentação fornecida com a placa-mãe ou nos parágrafos seguintes.

O BIOS é o software que habilita as funções mais básicas de um computador. Fabricantes de placas-mãe fornecem um BIOS especificamente fabricado para o hardware. Normalmente, a configuração do BIOS só pode ser acessada em um momento específico: durante a inicialização da máquina. Durante a fase de inicialização, a máquina executa vários testes de diagnóstico de hardware. Um deles é uma verificação de memória, indicado por um contador de memória. Quando o contador aparecer, procure uma linha, geralmente abaixo dele ou em algum local na parte inferior, mencionando a tecla a ser

pressionada para acessar a configuração do BIOS. Geralmente, a tecla a ser pressionada é Del, F1 ou Esc. Pressione esta tecla até que a tela de configuração do BIOS seja exibida.

Procedimento 28.1 *Mudando a sequência de inicialização do BIOS*

- 1 Digite o BIOS usando a tecla apropriada conforme anunciada pelas rotinas de inicialização e espere até que a tela do BIOS seja exibida.
- 2 Para mudar a sequência de inicialização em um AWARD BIOS, procure a entrada *BIOS FEATURES SETUP*. Outros fabricantes talvez tenham um nome diferente para isso, como *ADVANCED CMOS SETUP*. Quando encontrar a entrada, selecione-a e confirme com Enter.
- 3 Na tela exibida, procure uma subentrada denominada *BOOT SEQUENCE* ou *BOOT ORDER*. A sequência de boot é algo do tipo C, A ou A, C. Nesse caso, a máquina primeiro pesquisa o disco rígido (C) e, em seguida, o disquete (A) para encontrar um meio inicializável. Modifique as configurações pressionando PgUp ou PgDown até que a sequência seja A, CDROM, C.
- 4 Saia da tela de configuração do BIOS pressionando Esc. Para gravar as mudanças, selecione *SAVE & EXIT SETUP* ou pressione F10. Para confirmar que as configurações devem ser gravadas, pressione Y.

Procedimento 28.2 *Mudando a sequência de inicialização em um SCSI BIOS (Adaptador de Host Adaptec)*

- 1 Abra a configuração pressionando Ctrl + A.
- 2 Selecione *Utilitários de Disco*. Os componentes de hardware conectados agora são exibidos.

Anote o ID do SCSI da sua unidade de DVD.
- 3 Saia do menu com Esc.
- 4 Abra *Definir Configurações do Adaptador*. Em *Opções Adicionais*, selecione *Opções do Dispositivo de Inicialização* e pressione Enter.
- 5 Digite o ID da unidade de DVD e pressione Enter novamente.
- 6 Pressione Esc duas vezes para retornar à tela de inicialização do BIOS do SCSI.

7 Saia dessa tela e confirme com *Sim* para inicializar o computador.

Independentemente do idioma e do layout do teclado que a instalação final usará, a maioria das configurações de BIOS usa o layout de teclado dos EUA, conforme mostrado na figura a seguir:

Figura 28.3 Layout do teclado dos EUA



28.2.5 Falha na inicialização

Alguns tipos de hardware, principalmente os muito antigos ou muito recentes, falham na instalação. Em muitos casos, isso pode ocorrer devido à ausência de suporte para esse tipo de hardware no kernel de instalação ou devido a alguma funcionalidade incluída nesse kernel, como a ACPI, que ainda causa problemas em alguns hardwares.

Se o seu sistema falhar na instalação usando o modo de *instalação* padrão da primeira tela de boot da instalação, tente o seguinte:

- 1** Com o DVD ainda na unidade, reinicialize a máquina com Ctrl + Alt + Del ou usando o botão de reinicialização do hardware.
- 2** Quando a tela de boot for exibida, pressione F5, use as teclas de seta do teclado para navegar até *Sem ACPI* e pressione Enter para iniciar o processo de boot e instalação. Essa opção desabilita o suporte para as técnicas de gerenciamento de energia da ACPI.
- 3** prossiga com a instalação conforme descrito no Capítulo 3, *Installation with YaST* (↑ *Guia de Implantação*).

Se isso falhar, proceda como acima, mas escolha *Configurações Seguras*. Essa opção desabilita o suporte de ACPI e DMA. A maioria dos hardwares inicializará com essa opção.

Se ambas as opções falharem, use o prompt das opções de inicialização para transmitir quaisquer parâmetros adicionais necessários para suportar esse tipo de hardware no kernel de instalação. Para obter mais informações sobre os parâmetros disponíveis como opções de inicialização, consulte a documentação do kernel localizada em `/usr/src/linux/Documentation/kernel-parameters.txt`.

DICA: obtendo documentação do kernel

Instale o pacote `kernel-source` para exibir a documentação do kernel.

Há vários outros parâmetros de kernel relacionados à ACPI que podem ser digitados no prompt de inicialização antes da inicialização para a instalação:

`acpi=off`

Esse parâmetro desabilita o subsistema completo da ACPI no seu computador. Isso poderá ser útil se o computador não puder lidar com a ACPI de modo algum ou se você achar que a ACPI no computador causa problemas.

`acpi=force`

Sempre habilite a ACPI mesmo que o computador tenha um BIOS antigo anterior ao ano 2000. Esse parâmetro também habilitará a ACPI se ele estiver definido além de `acpi=off`.

`acpi=noirq`

Não use a ACPI para roteamento de IRQ.

`acpi=ht`

Execute somente ACPI o suficiente para habilitar hyper-threading.

`acpi=strict`

Tenha menos tolerância com plataformas que não sejam estritamente compatíveis com a especificação ACPI.

`pci=noacpi`

Desabilita o roteamento de IRQ de PCI do novo sistema da ACPI.

`pnpacpi=off`

Essa opção serve para problemas de porta serial ou paralela quando a configuração do BIOS contiver interrupções ou portas incorretas.

`notsc`

Desabilita o contador da marcação de horário. Essa opção pode ser usada para solucionar problemas de tempo nos seus sistemas. Trata-se de um recurso recente, por isso, se você perceber regressões na sua máquina, especialmente relativas a horário ou mesmo um travamento total, vale a pena tentar essa opção.

`nohz=off`

Desabilita o recurso nohz. Se a sua máquina trava, essa opção pode ajudar. Caso contrário, ela não tem utilidade.

Após determinada a combinação correta de parâmetros, o YaST os grava automaticamente na configuração do carregador de boot para certificar-se de que o sistema inicie de forma correta na próxima vez.

Se erros inexplicáveis ocorrerem quando o kernel estiver carregado ou durante a instalação, selecione *Teste de Memória* no menu de inicialização para verificar a memória. Se *Teste de Memória* retornar um erro, geralmente será um erro de hardware.

28.2.6 Falha na inicialização do instalador gráfico

Depois que você insere o meio na unidade e reinicializa a máquina, a tela de instalação é exibida, mas depois que a opção *Instalação* é selecionada, o instalador gráfico não inicializa.

Há várias maneiras de lidar com essa situação:

- Tente selecionar outra resolução de tela para as caixas de diálogo de instalação.
- Selecione *Modo de Texto* para a instalação.
- Faça uma instalação remota através de VNC usando o instalador gráfico.

Procedimento 28.3 *Mudar a resolução de tela para instalação*

- 1 Inicialize para a instalação.
- 2 Pressione F3 para abrir um menu do qual selecionar uma resolução mais baixa para fins de instalação.
- 3 Selecione *Instalação* e prossiga com a instalação conforme descrito no Capítulo 3, *Installation with YaST* (↑ *Guia de Implantação*).

Procedimento 28.4 *Instalação em modo de texto*

- 1 Inicialize para a instalação.
- 2 Pressione F3 e selecione *Modo de Texto*.
- 3 Selecione *Instalação* e prossiga com a instalação conforme descrito no Capítulo 3, *Installation with YaST* (↑ *Guia de Implantação*).

Procedimento 28.5 *Instalação VNC*

- 1 Inicialize para a instalação.
- 2 Insira o texto a seguir no prompt de opções de inicialização:

```
vnc=1 vncpassword=some_password
```

Substitua *senha* pela senha a ser usada para a instalação do VNC.

- 3 Selecione *Instalação* e pressione Enter para iniciar a instalação.

Em vez de iniciar com a rotina de instalação gráfica, o sistema continua em execução no modo de texto, depois trava, exibindo uma mensagem que contém o endereço IP e o número de porta com que o instalador pode ser acessado por uma interface de browser ou um aplicativo viewer do VNC.

- 4 Se estiver usando um browser para acessar o instalador, inicie o browser e digite as informações de endereço fornecidas pelas rotinas de instalação na futura máquina do SUSE Linux Enterprise Desktop e pressione Enter:

```
http://ip_address_of_machine:5801
```

Uma caixa de diálogo é aberta na janela do browser solicitando a senha VNC. Insira-a e continue com a instalação conforme descrito no Capítulo 3, *Installation with YaST* (↑ *Guia de Implantação*).

IMPORTANTE

A instalação através de VNC funciona com qualquer navegador em qualquer sistema operacional, desde que o suporte Java esteja habilitado.

Forneça o endereço IP e a senha do seu viewer do VNC quando solicitado. Uma janela é aberta, exibindo as caixas de diálogo de instalação. Prossiga com a instalação como de costume.

28.2.7 Apenas a tela de boot simples é aberta

Você inseriu o meio na unidade, as rotinas do BIOS foram encerradas, mas o sistema não inicia com a tela de boot gráfica. Em vez disso, ele inicia uma interface baseada em texto bastante simples. Isso pode acontecer em qualquer máquina que não forneça memória gráfica suficiente para renderizar uma tela de boot gráfica.

Embora a tela de boot de texto tenha aparência simples, ela fornece praticamente a mesma funcionalidade que a gráfica:

Opções de inicialização

Diferentemente da interface gráfica, as diversas opções de inicialização não podem ser selecionadas usando as teclas de cursor do teclado. O menu de inicialização da tela de boot em modo de texto oferece algumas palavras-chave no prompt de inicialização. Essas palavras-chave são mapeadas para as opções oferecidas na versão gráfica. Insira sua escolha e pressione Enter para iniciar o processo de boot.

Opções de inicialização personalizadas

Após selecionar uma opção de inicialização, insira a palavra-chave apropriada no prompt de inicialização ou insira algumas opções de inicialização personalizadas conforme descrito na Seção 28.2.5, “Falha na inicialização” (p 385). Para iniciar o processo de instalação, pressione Enter.

Resoluções de tela

Use as teclas F para determinar a resolução de tela para a instalação. Se você precisa inicializar no modo de texto, escolha F3.

28.3 Problemas de inicialização

Problemas de inicialização são situações em que o sistema não inicializa de forma adequada (não inicializa no nível de execução e na tela de login esperados).

28.3.1 Falha ao carregar o carregador de boot do GRUB

Se o hardware estiver funcionando de forma adequada, é possível que o carregador de boot esteja corrompido e que o Linux não possa ser iniciado na máquina. Nesse caso, é necessário reinstalar o carregador de boot. Para reinstalar o carregador de boot, proceda da seguinte maneira:

- 1 Insira a mídia de instalação na unidade.
- 2 Reinicialize a máquina.
- 3 Selecione *Instalação* no menu de inicialização.
- 4 Selecione um idioma.
- 5 Aceite o contrato de licença.
- 6 Na tela *Modo de Instalação*, selecione *Outro* e defina o modo de instalação como *Reparar o Sistema Instalado*.
- 7 Quando estiver no módulo Reparo do Sistema do YaST, selecione *Ferramentas Especialista* e selecione *Instalar Novo Bootloader*.
- 8 Restaure as configurações originais e reinstale o carregador de boot.
- 9 Saia do Reparo do Sistema do YaST e reinicialize o sistema.

Outros motivos para a máquina não inicializar podem estar relacionadas ao BIOS:

Configurações do BIOS

Verifique o BIOS para obter referências para o disco rígido. O GRUB talvez não seja iniciado se o próprio disco rígido não puder se encontrado com as configurações atuais do BIOS.

Ordem de inicialização do BIOS

Verifique se a ordem de inicialização do sistema inclui o disco rígido. Se a opção do disco rígido não tiver sido habilitada, o sistema talvez seja instalado de forma adequada, mas não seja inicializado quando o acesso ao disco rígido for necessário.

28.3.2 Não é exibido nenhum prompt nem tela de login

Isso costuma ocorrer após uma falha de atualização do kernel e é conhecido como *pânico do kernel* devido ao tipo de erro do console do sistema que às vezes se verifica no estágio final do processo. Se a máquina realmente tiver sido reinicializada após uma atualização de software, o objetivo imediato é reinicializá-la usando a versão antiga e segura do kernel do Linux e os arquivos associados. Isso pode ser feito na tela do carregador de boot GRUB durante o processo de inicialização da seguinte forma:

- 1 Reinicialize o computador usando o botão de reinicialização ou desligue-o e ligue-o novamente.
- 2 Quando a tela de boot do GRUB for exibida, selecione *Linux--Failsafe* e pressione Enter. A máquina será inicializada com a versão anterior do kernel e seus arquivos associados.
- 3 Após a conclusão do processo de boot, remova o kernel recém-instalado e, se necessário, modifique manualmente `/boot/grub/menu.lst` para tornar o kernel mais antigo a opção padrão. Para obter informações detalhadas sobre a sintaxe usada nesse arquivo de configuração, consulte o Capítulo 10, *O carregador de boot GRUB* (p 105).

A atualização desse arquivo pode não ser necessária porque as ferramentas automatizadas de atualização geralmente o modificam durante o processo de rollback.

4 Reinicializar.

Se isso não resolver o problema porque a opção *Linux--Failsafe* não inicia o computador como deveria, inicialize-o usando a mídia de instalação. Após a inicialização da máquina, prossiga com o Passo 3 (p 391).

28.3.3 Não há login gráfico

Se a máquina ligar, mas não inicializar no gerenciador de login gráfico, evite problemas com a escolha do nível de execução padrão ou a configuração do sistema X Window. Para verificar a configuração do nível de execução, efetue login como o usuário `root` e verifique se a máquina está configurada para inicializar no nível de execução 5 (área de trabalho gráfica). Uma maneira rápida de verificar isso é examinar o conteúdo de `/etc/inittab`, da seguinte maneira:

```
tux@mercury:~> grep "id:" /etc/inittab
id:5:initdefault:
```

A linha retornada indica que o nível de execução padrão da máquina (`initdefault`) está definido como 5 e que ela deve inicializar na área de trabalho gráfica. Se o nível de execução estiver definido como qualquer outro número, use o módulo Editor de Níveis de Execução do YaST para defini-lo como 5.

IMPORTANTE

Não edite a configuração do nível de execução manualmente. Caso contrário, o SuSEconfig (executado pelo YaST) sobregravará essas mudanças na próxima execução. Se você precisa fazer mudanças manuais aqui, desabilite mudanças futuras do SuSEconfig definindo `CHECK_INITTAB` em `/etc/sysconfig/suseconfig` como `no`.

Se o nível de execução estiver definido como 5, provavelmente a sua área de trabalho ou o software X Window está mal configurado ou corrompido. Examine os arquivos de registro em `/var/log/Xorg.*.log` para obter mensagens detalhadas do servidor X enquanto ele tenta iniciar. Se a área de trabalho falhar durante a inicialização, talvez ela registre mensagens de erro em `/var/log/messages`. Se essas mensagens de erro sugerirem um problema de configuração no servidor X, tente corrigi-lo. Se o sistema gráfico ainda não aparecer, reinstale a área de trabalho gráfica.

DICA: iniciando o sistema X Window manualmente

Um teste rápido: o comando `startx` deverá forçar o sistema X Window a iniciar com os padrões configurados se o usuário estiver logado no console. Se isso não funcionar, ele deve registrar erros no console.

28.4 Problemas de login

Problemas de login são aqueles em que sua máquina, de fato, inicializa na tela de boas-vindas ou no prompt de login, como esperado, mas recusa-se a aceitar o nome de usuário e a senha ou aceita-os mas não se comporta de forma adequada (não inicia a área de trabalho gráfica, produz erros, passa para uma linha de comando, entre outros).

28.4.1 Falha nas combinações de nome de usuário e senha válidas

Isso geralmente ocorre quando o sistema está configurado para usar autenticação de rede ou serviços de diretório e, por alguma razão, não é capaz de recuperar resultados de seus servidores configurados. O usuário `root`, como o único usuário local, é o único que ainda pode efetuar login nessas máquinas. A seguir estão alguns motivos comuns para uma máquina parecer funcional, mas não conseguir processar logins corretamente:

- A rede não está funcionando. Para obter mais instruções sobre isso, consulte a Seção 28.5, “Problemas de rede” (p 401).
- O DNS não está funcionando no momento (o que impede o GNOME ou o KDE de trabalhar e o sistema de efetuar solicitações válidas a servidores seguros). Uma indicação de que esse é o caso é que a máquina leva muito tempo para responder a qualquer ação. Há mais informações a respeito desse tópico na Seção 28.5, “Problemas de rede” (p 401).
- Se o sistema estiver configurado para usar Kerberos, o horário local do sistema poderá ter ultrapassado a variação aceita com o horário do servidor Kerberos (geralmente 300 segundos). Se o NTP (protocolo de horário de rede) não estiver funcionando de forma adequada ou os servidores NTP locais não estiverem

funcionando, a autenticação do Kerberos não funcionará pois depende da sincronização comum do relógio na rede.

- A configuração de autenticação do sistema está definida incorretamente. Verifique se há erros de digitação ou ordem incorreta de diretivas nos arquivos de configuração PAM envolvidos. Para obter informações adicionais sobre o PAM e a sintaxe dos arquivos de configuração envolvidos, consulte o Capítulo 2, *Authentication with PAM* (↑*Security Guide (Guia de Segurança)*).
- A partição pessoal está criptografada. Há mais informações a respeito desse tópico na Seção 28.4.3, “Falha de login na partição pessoal criptografada” (p 398).

Em todos os casos que não envolvem problemas de rede externos, a solução é reinicializar o sistema em um modo de usuário único e reparar a configuração antes de inicializar novamente no modo de operação e tentar efetuar login novamente. Para inicializar no modo de usuário único:

- 1 Reinicialize o sistema. A tela de boot é exibida e apresenta um prompt.
- 2 Insira 1 no prompt de inicialização para fazer o sistema inicializar no modo de usuário único.
- 3 Insira o nome de usuário e a senha para `root`.
- 4 Faça as mudanças necessárias.
- 5 Inicialize no modo de rede e multiusuário total digitando `telinit 5` na linha de comando.

28.4.2 Nome de usuário e senha válidos não foram aceitos

Esse é o um dos problemas mais comuns que os usuários podem encontrar, pois há vários motivos pelos quais isso pode ocorrer. Dependendo de você usar gerenciamento e autenticação de usuário local ou autenticação em rede, as falhas de login ocorrem por motivos diferentes.

O gerenciamento de usuário local pode falhar pelos seguintes motivos:

- O usuário pode ter digitado a senha errada.
- O diretório pessoal do usuário que contém arquivos de configuração da área de trabalho está corrompido ou protegido contra gravação.
- Talvez haja problemas com o sistema X Window ao autenticar esse usuário específico, especialmente se o diretório pessoal do usuário tiver sido usado com outra distribuição do Linux antes da instalação da atual.

Para encontrar o motivo de uma falha de login local, proceda da seguinte maneira:

- 1** Verifique se o usuário memorizou a senha corretamente antes de começar a depurar todo o mecanismo de autenticação. Se o usuário não se lembrar da senha correta, use o módulo Gerenciamento de Usuário do YaST para mudar a senha do usuário. Fique atento à tecla Caps Lock e libere-a, se necessário.
- 2** Efetue login como `root` e, em `/var/log/messages`, verifique se há mensagens de erro do processo de login e do PAM.
- 3** Tente efetuar login de um console (usando Ctrl + Alt + F1). Se esse procedimento for bem-sucedido, não será responsabilidade do PAM, pois é possível autenticar o usuário nessa máquina. Tente localizar quaisquer problemas com o sistema X Window ou a área de trabalho (GNOME ou KDE). Para obter mais informações, consulte a Seção 28.4.4, “Login bem-sucedido mas há falha na área de trabalho GNOME” (p 398) e a Seção 28.4.5, “Login bem-sucedido mas há falha na área de trabalho KDE” (p 399).
- 4** Se o diretório pessoal do usuário foi usado com outra distribuição Linux, remova o arquivo `Xauthority` no diretório do usuário. Use um login de console por meio de Ctrl + Alt + F1 e execute o comando `rm .Xauthority` como esse usuário. Isso deve eliminar problemas de autenticação X para o usuário. Tente o login gráfico novamente.
- 5** Se o login gráfico ainda falhar, efetue um login de console com Ctrl + Alt + F1. Tente iniciar uma sessão X em outra tela, a primeira (: 0) já está em uso:

```
startx -- :1
```

Isso deve exibir uma tela gráfica e a sua área de trabalho. Se não, verifique os arquivos de registro do sistema X Window (`/var/log/Xorg. número_de_exibição.log`) ou o arquivo de registro para seus aplicativos de área de

trabalho (`.xsession-errors` no diretório pessoal do usuário) em busca de quaisquer irregularidades.

- 6 Se a área de trabalho não puder iniciar devido a arquivos de configuração corromptos, continue com a Seção 28.4.4, “Login bem-sucedido mas há falha na área de trabalho GNOME” (p 398) ou a Seção 28.4.5, “Login bem-sucedido mas há falha na área de trabalho KDE” (p 399).

Veja a seguir alguns motivos comuns pelos quais a autenticação em rede de um usuário específico pode falhar em uma máquina específica:

- O usuário pode ter digitado a senha errada.
- O nome de usuário existe nos arquivos de autenticação local da máquina e também é fornecido por um sistema de autenticação de rede, causando conflitos.
- O diretório pessoal existe mas está corrompido ou não disponível. Talvez ele esteja protegido contra gravação ou está em um servidor inacessível no momento.
- O usuário não tem permissão para efetuar login neste host específico no sistema de autenticação.
- A máquina mudou de nomes de host, por qualquer motivo, e o usuário não tem permissão para efetuar login no host.
- A máquina não pode acessar o servidor de diretório ou o servidor de autenticação que contém as informações do usuário.
- Talvez haja problemas com o sistema X Window ao autenticar esse usuário específico, especialmente se o diretório pessoal do usuário tiver sido usado com outra distribuição do Linux antes da instalação da atual.

Para localizar a causa das falhas de login com a autenticação de rede, proceda da seguinte maneira:

- 1 Verifique se o usuário memorizou a senha corretamente antes de começar a depurar todo o mecanismo de autenticação.
- 2 Determine o servidor de diretórios usado pela máquina para autenticação e verifique se ele está funcionando e se comunicando corretamente com as outras máquinas.

- 3 Determine se o nome e a senha do usuário funcionam em outras máquinas para verificar se os dados de autenticação existem e são distribuídos corretamente.
- 4 Verifique se outro usuário pode efetuar login na máquina com comportamento incorreto. Se outro usuário ou o usuário `root` puder efetuar login sem dificuldade, conecte-se e examine o arquivo `/var/log/messages`. Localize as marcações de horário que correspondem às tentativas de login e determine se o PAM produziu alguma mensagem de erro.
- 5 Tente efetuar login de um console (usando `Ctrl + Alt + F1`). Se der certo, o problema não é do PAM ou do servidor de diretórios no qual o diretório pessoal do usuário está hospedado, pois é possível autenticar o usuário nessa máquina. Tente localizar quaisquer problemas com o sistema X Window ou a área de trabalho (GNOME ou KDE). Para obter mais informações, consulte a Seção 28.4.4, “Login bem-sucedido mas há falha na área de trabalho GNOME” (p 398) e a Seção 28.4.5, “Login bem-sucedido mas há falha na área de trabalho KDE” (p 399).
- 6 Se o diretório pessoal do usuário foi usado com outra distribuição Linux, remova o arquivo `Xauthority` no diretório do usuário. Use um login de console por meio de `Ctrl + Alt + F1` e execute o comando `rm .Xauthority` como esse usuário. Isso deve eliminar problemas de autenticação X para o usuário. Tente o login gráfico novamente.
- 7 Se o login gráfico ainda falhar, efetue um login de console com `Ctrl + Alt + F1`. Tente iniciar uma sessão X em outra tela, a primeira (`:0`) já está em uso:

```
startx -- :1
```

Isso deve exibir uma tela gráfica e a sua área de trabalho. Se não, verifique os arquivos de registro do sistema X Window (`/var/log/Xorg. número_de_exibição.log`) ou o arquivo de registro para seus aplicativos de área de trabalho (`.xsession-errors` no diretório pessoal do usuário) em busca de quaisquer irregularidades.

- 8 Se a área de trabalho não puder iniciar devido a arquivos de configuração corromptos, continue com a Seção 28.4.4, “Login bem-sucedido mas há falha na área de trabalho GNOME” (p 398) ou a Seção 28.4.5, “Login bem-sucedido mas há falha na área de trabalho KDE” (p 399).

28.4.3 Falha de login na partição pessoal criptografada

Recomenda-se o uso de uma partição pessoal criptografada para laptops. Se você não puder efetuar login no seu laptop, o motivo geralmente é simples: a sua partição pode não estar desbloqueada.

No momento da inicialização, você precisa digitar a frase secreta para desbloquear a sua partição criptografada. Se você não a digitar, o processo de boot continuará, deixando a partição bloqueada.

Para desbloquear a partição criptografada, faça o seguinte:

- 1 Passe para o console de texto com Ctrl + Alt + F1.
- 2 Torne-se `root`.
- 3 Reinicie o processo de desbloqueio novamente com:

```
/etc/init.d/boot.crypto restart
```
- 4 Digite sua frase secreta para desbloquear a partição criptografada.
- 5 Saia do console de texto e volte para a tela de login com Alt + F7.
- 6 Efetue login como de costume.

28.4.4 Login bem-sucedido mas há falha na área de trabalho GNOME

Se esse for o caso, provavelmente os seus arquivos de configuração do GNOME se corromperam. Alguns sintomas podem incluir falha de funcionamento do teclado, a geometria da tela distorcida ou até mesmo a tela exibida como um campo cinza vazio. A distinção importante é que se outro usuário efetuar login, a máquina funcionará normalmente. Provavelmente o problema possa ser corrigido rapidamente com a transferência do diretório de configuração do GNOME do usuário para um novo local,

o que faz a área de trabalho GNOME inicializar um novo. Embora o usuário seja forçado a reconfigurar o GNOME, nenhum dado é perdido.

- 1 Alterne para um console de texto pressionando Ctrl + Alt + F1.
- 2 Efetue login com o seu nome de usuário.
- 3 Mova os diretórios de configuração do GNOME do usuário para um local temporário:

```
mv .gconf .gconf-ORIG-RECOVER
mv .gnome2 .gnome2-ORIG-RECOVER
```

- 4 Efetue logout.
- 5 Efetue login novamente, mas não execute nenhum aplicativo.
- 6 Recupere seus dados individuais de configuração de aplicativo (inclusive os dados de cliente de e-mail do Evolution) copiando o diretório ~/gconf-ORIG-RECOVER/apps/ de volta para o novo diretório ~/.gconf da seguinte maneira:

```
cp -a .gconf-ORIG-RECOVER/apps .gconf/
```

Se isso causar os problemas de login, tente recuperar somente os dados de aplicativo críticos e reconfigure o restante dos aplicativos.

28.4.5 Login bem-sucedido mas há falha na área de trabalho KDE

Há vários motivos pelos quais uma área de trabalho KDE não permitiria que usuários efetuassem login. Dados de cache corrompidos podem causar problemas de login e arquivos de configuração de área de trabalho KDE corrompidos.

Dados de cache são usados na inicialização da área de trabalho para aumentar o desempenho. Se os dados estiverem corrompidos, a inicialização será mais lenta ou falhará inteiramente. Removê-los força as rotinas de inicialização da área de trabalho a iniciarem desde o começo. Isso leva mais tempo do que uma inicialização normal, mas os dados estarão intactos depois disso e o usuário poderá efetuar login.

Para remover os arquivos de cache da área de trabalho KDE, emita o seguinte comando como `root`:

```
rm -rf /tmp/kde-user /tmp/ksocket-user
```

Substitua *usuário* pelo seu nome de usuário. A remoção desses dois diretórios remove somente os arquivos de cache corrompidos. Nenhum dado real é danificado por esse procedimento.

Arquivos de configuração de área de trabalho corrompidos sempre podem ser substituídos pelos arquivos de configuração inicial. Se você deseja recuperar os ajustes do usuário, copie-os cuidadosamente de volta do local temporário após a configuração ter sido restaurada usando os valores de configuração padrão.

Para substituir uma configuração de área de trabalho corrompida pelos valores de configuração inicial, proceda da seguinte maneira:

- 1 Alterne para um console de texto pressionando `Ctrl + Alt + F1`.
- 2 Efetue login com o seu nome de usuário.
- 3 Mova o diretório de configuração do KDE e os arquivos `.skel` para um local temporário:

- Para o KDE3, use estes comandos:

```
mv .kde .kde-ORIG-RECOVER
mv .skel .skel-ORIG-RECOVER
```

- Para o KDE4, use estes comandos:

```
mv .kde4 .kde4-ORIG-RECOVER
mv .skel .skel-ORIG-RECOVER
```

- 4 Efetue logout.
- 5 Efetue login novamente.
- 6 Após a inicialização bem-sucedida da área de trabalho, copie a configuração do usuário de volta no local:

```
cp -a KDEDIR/share .kde/share
```

Substitua *KDEDIR* pelo diretório do Passo 3 (p 400).

IMPORTANTE

Se os ajustes do usuário causaram a falha no login e continuam a fazer isso, repita o procedimento como descrito acima, mas não copie o diretório `.kde/share`.

28.5 Problemas de rede

Quaisquer problemas do seu sistema podem estar relacionados à rede, mesmo que inicialmente não transmitam essa impressão. Por exemplo, o motivo para um sistema não permitir o login de usuários pode ser algum tipo de problema de rede. Esta seção apresenta uma lista de verificação simples que você pode aplicar para identificar a causa de qualquer problema de rede encontrado.

Procedimento 28.6 *Como identificar problemas de rede*

Ao verificar a conexão de rede da sua máquina, proceda da seguinte maneira:

- 1 Se você estiver usando uma conexão ethernet, verifique o hardware primeiro. Verifique se o cabo de rede está acoplado corretamente no computador e no roteador (ou hub etc.). As luzes de controle próximas ao seu conector ethernet devem estar ativas.

Se a conexão falhar, verifique se o cabo de rede funciona com outra máquina. Se funcionar, a placa de rede será a causa da falha. Se houver hubs ou switches incluídos na configuração da sua rede, eles também podem estar com defeito.

- 2 Se estiver usando uma conexão sem fio, verifique se o link sem fio pode ser estabelecido por outras máquinas. Caso contrário, contate o administrador da rede wireless.
- 3 Após verificar sua conectividade de rede básica, tente descobrir qual serviço não está respondendo. Reúna as informações de endereço de todos os servidores de rede necessários na configuração. Procure-os no módulo apropriado do YaST ou peça ao administrador do sistema. A lista a seguir fornece alguns dos servidores de rede típicos envolvidos em uma configuração junto com os sintomas de uma falha.

DNS (Serviço de Nomes)

Um serviço de nomes inoperante ou defeituoso afeta a funcionalidade da rede de várias maneiras. Se a máquina local depender de quaisquer servidores de rede para autenticação e esses servidores não puderem ser encontrados devido a problemas de resolução de nomes, os usuários não serão capazes nem de efetuar login. As máquinas da rede gerenciadas por um servidor de nomes inoperante não seriam capazes de “ver” umas às outras e de se comunicarem.

NTP (Serviço de Horário)

Um serviço NTP defeituoso ou totalmente inoperante pode afetar a funcionalidade do servidor X e a autenticação Kerberos.

NFS (Serviço de Arquivos)

Se qualquer aplicativo precisar de dados armazenados em um diretório NFS montado, ele não conseguirá iniciar nem funcionar corretamente se esse serviço estiver inoperante ou mal configurado. No pior cenário possível, a configuração da área de trabalho pessoal de um usuário não será exibida se o seu diretório pessoal que contém os subdiretórios `.gconf` ou `.kde` não forem encontrados devido a falha do servidor NFS.

Samba (Serviço de Arquivos)

Se qualquer aplicativo precisar de dados armazenados em um diretório de um servidor Samba defeituoso, ele não conseguirá iniciar ou funcionar corretamente.

NIS (Gerenciamento de Usuário)

Se o seu sistema SUSE Linux Enterprise Desktop usa um servidor NIS defeituoso para fornecer os dados de usuários, os usuários não conseguirão efetuar login nessa máquina.

LDAP (Gerenciamento de Usuário)

Se o seu sistema SUSE Linux Enterprise Desktop usa um servidor LDAP defeituoso para fornecer os dados de usuários, os usuários não conseguirão efetuar login nessa máquina.

Kerberos (Autenticação)

A autenticação não funcionará e o login em qualquer máquina falhará.

CUPS (Impressão de Rede)

Os usuários não conseguem imprimir.

- 4 Verifique se os servidores de rede estão em execução e se a configuração de rede permite estabelecer uma conexão:

IMPORTANTE

O procedimento de depuração descrito abaixo aplica-se somente a uma configuração simples de servidor/cliente de rede que não envolva roteamento interno. Supõe-se que o servidor e o cliente integrem a mesma sub-rede sem necessidade de roteamento adicional.

- 4a** Use `ping endereço IP` ou `nome_do_host` (substitua `nome_do_host` pelo nome do host do servidor) para verificar se cada um deles está funcionando e respondendo à rede. Se esse comando for bem-sucedido, ele informará que o host que você estava procurando está em execução e o serviço de nomes da rede está configurado corretamente.

Se o ping falhar com `destination host unreachable`, o seu sistema ou o servidor desejado não está configurado de forma adequada ou está inoperante. Verifique se o sistema pode ser alcançado com `ping endereço IP` ou `seu_nome_de_host` em outra máquina. Se você obtiver êxito em acessar sua máquina de outra máquina, significará que o servidor não está sendo executado ou não está configurado corretamente.

Se o ping falhar com `unknown host`, significará que o serviço de nomes não está configurado corretamente ou o nome do host usado estava incorreto. Para obter mais verificações sobre esse assunto, consulte o Passo 4b (p 403). Se o ping ainda falhar, significará que a placa de rede não está configurada de forma correta ou o hardware de rede está defeituoso.

- 4b** Use `host nome_do_host` para verificar se o nome do host do servidor ao qual você está tentando se conectar está convertido de forma adequada em um endereço IP e vice-versa. Se esse comando retornar o endereço IP do host, significará que o serviço de nomes está funcionando. Se houver falha nesse comando `host`, verifique todos os arquivos de configuração de rede relacionados à resolução de nomes e de endereços no seu host:

/etc/resolv.conf

Este arquivo é usado para controlar o domínio e o servidor de nomes que você está usando no momento. Ele pode ser modificado manualmente ou ajustado automaticamente pelo YaST ou DHCP. O ajuste automático é preferencial. Porém, verifique se o arquivo tem a estrutura a seguir e se todos os endereços de rede e nomes de domínio estão corretos:

```
search fully_qualified_domain_name
nameserver ipaddress_of_nameserver
```

Este arquivo pode conter mais de um endereço de servidor de nomes, mas pelo menos um deles deve estar correto para fornecer a resolução de nomes para o seu host. Se necessário, ajuste esse arquivo usando o módulo Configurações de Rede do YaST (guia Nome de host/DNS).

Se a conexão de rede for gerenciada por DHCP, habilite o DHCP para mudar as informações de serviço de nomes e nome de host selecionando *Trocar Nome de Host via DHCP* e *Atualizar Servidor de Nomes e Lista de Pesquisa via DHCP* no módulo DNS e Nome de Host do YaST.

/etc/nsswitch.conf

Este arquivo informa ao Linux onde procurar informações de serviço de nomes. Ele deve ter a seguinte aparência:

```
...
hosts: files dns
networks: files dns
...
```

A entrada `dns` é essencial. Ela informa ao Linux para usar um servidor de nomes externo. Geralmente essas entradas são gerenciadas automaticamente pelo YaST, mas é prudente verificar.

Se todas as entradas relevantes no host estiverem corretas, deixe o seu administrador de sistema verificar a configuração do servidor DNS para obter as informações de zona corretas. Se você verificou se a configuração DNS do seu host e o servidor DNS estão corretos, continue verificando a configuração da rede e do dispositivo de rede.

- 4c** Se o sistema não puder estabelecer uma conexão a um servidor de redes e você excluiu problemas de serviço de nomes da lista de possíveis responsáveis, verifique a configuração da placa de rede.

Use o comando `ifconfig dispositivo_de_rede` (executado como `root`) para verificar se este dispositivo foi configurado de forma adequada. Verifique se `inet address` e `Mask` estão configurados corretamente. Um erro no endereço IP ou um bit ausente na máscara de rede inutilizam a configuração de rede. Se necessário, execute essa verificação no servidor também.

- 4d** Se o hardware de rede e o serviço de nomes estiverem configurados de forma adequada e em execução, mas algumas conexões de rede externas ainda tiverem longos tempos de espera ou falharem inteiramente, use `traceroute nome_completo_do_domínio` (executado como `root`) para controlar a rota de rede tomada pelas solicitações. Esse comando lista qualquer gateway (hop) que uma solicitação da sua máquina transmitir no caminho ao seu destino. Ele lista o tempo de resposta de cada hop e se esse hop é acessível. Use uma combinação de `traceroute` e `ping` para identificar o responsável e informar aos administradores.

Após identificar a causa do problema de rede, você poderá resolvê-lo (se o problema estiver na sua máquina) ou informar os administradores de sistema da rede sobre suas descobertas para que eles possam reconfigurar os serviços ou reparar os sistemas necessários.

28.5.1 Problemas do NetworkManager

Se você tiver problema com a conectividade da rede, restrinja-a conforme descrito no Procedimento 28.6, “Como identificar problemas de rede” (p 401). Se tudo indicar que a culpa é do NetworkManager, faça o seguinte para obter os registros com dicas sobre a causa da falha do NetworkManager:

- 1 Abra um shell e efetue login como `root`.

- 2 Reinicie o NetworkManager:

```
rcnetwork restart -o nm
```

- 3 Abra uma página Web, por exemplo, <http://www.opensuse.org>, como um usuário normal para ver se você consegue se conectar.

- 4 Colete as informações sobre o estado do NetworkManager em `/var/log/NetworkManager`.

Para obter maiores informações sobre o NetworkManager, consulte o Capítulo 23, *Usando o NetworkManager* (p 323).

28.6 Problemas de dados

Problemas de dados ocorrem quando a máquina pode ou não inicializar corretamente, mas em ambos os casos, está claro que há dados corrompidos no sistema e que o sistema precisa ser recuperado. Essas situações exigem um backup dos seus dados críticos, permitindo que você recupere o estado anterior à falha do sistema. O SUSE Linux Enterprise Desktop oferece módulos do YaST dedicados para backup e restauração do sistema, bem como um sistema de recuperação que pode ser usado para recuperar um sistema corrompido externamente.

28.6.1 Gerenciando imagens de partição

Às vezes é necessário fazer um backup de uma partição inteira ou até do disco rígido. O Linux possui a ferramenta `dd`, capaz de criar uma cópia exata do seu disco. Combinada ao `gzip`, faz você economizar espaço.

Procedimento 28.7 *Fazendo backup e restauração de discos rígidos*

- 1 Inicie um shell como usuário `root`.
- 2 Selecione o seu dispositivo de origem. Normalmente, ele assemelha-se a `/dev/sda` (com a etiqueta `SOURCE`).
- 3 Indique onde deseja armazenar sua imagem (com a etiqueta `BACKUP_PATH`). Esse local deverá ser diferente do dispositivo de origem. Em outras palavras: se você fizer um backup de `/dev/sda`, o seu arquivo de imagem não precisará ser armazenado em `/dev/sda`.
- 4 Execute os comandos para criar um arquivo de imagem compactado:

```
dd if=/dev/SOURCE | gzip > /BACKUP_PATH/image.gz
```

5 Recupere o disco rígido usando os seguintes comandos:

```
gzip -dc /BACKUP_PATH/image.gz | dd of=/dev/SOURCE
```

Se você precisar de apenas uma partição para o backup, substitua o marcador *SOURCE* pela sua respectiva partição. Nesse caso, o seu arquivo de imagem pode usar o mesmo disco rígido, só que em outra partição.

28.6.2 Fazendo backup de dados críticos

Backups de sistema podem ser facilmente gerenciados usando-se o módulo Backup do Sistema do YaST:

- 1** Como `root`, inicie o YaST e selecione *Sistema > Backup do Sistema*.
- 2** Crie um perfil de backup com todos os detalhes necessários para o backup, o nome do arquivo, o escopo e o tipo de backup:
 - 2a** Selecione *Gerenciamento de Perfil > Adicionar*.
 - 2b** Especifique um nome para o arquivo.
 - 2c** Insira o caminho no local do backup se desejar manter um backup local. Para que seu backup seja arquivado em um servidor de rede (via NFS), insira o endereço IP ou o nome do servidor e o diretório que deve armazenar seu arquivo.
 - 2d** Determine o tipo de arquivo e clique em *Avançar*.
 - 2e** Determine as opções de backup a serem usadas, se os arquivos não pertencentes a algum pacote devem sofrer backup e se uma lista de arquivos deve ser exibida antes da criação do arquivo. Determine também se os arquivos mudados devem ser identificados usando o mecanismo MD5 demorado.

Use *Especialista* para inserir uma caixa de diálogo para o backup de áreas inteiras de disco rígido. Atualmente, essa opção aplica-se somente ao sistema de arquivos Ext2.

2f Por fim, defina as restrições de pesquisa para excluir da área de backup determinadas áreas do sistema que não precisam de backup, como arquivos de bloqueio e de cache. Adicione, edite ou apague itens até que suas necessidades sejam atendidas e saia com *OK*.

3 Após terminar as configurações de perfil, você pode começar o backup imediatamente com *Criar Backup* ou configurar o backup automático. Também é possível criar outros perfis adaptados para várias outras finalidades.

Para configurar o backup automático de um determinado perfil, proceda da seguinte maneira:

- 1** Selecione *Backup Automático* no menu *Gerenciamento de Perfil*.
- 2** Selecione *Iniciar Backup Automaticamente*.
- 3** Determine a frequência de backup. Escolha *diariamente*, *semanalmente* ou *mensalmente*.
- 4** Determine o horário de início do backup. Essas configurações dependem da frequência de backup selecionada.
- 5** Decida se manterá backups antigos e quantos devem ser mantidos. Para receber uma mensagem de status gerada automaticamente do processo de backup, marque *Enviar Mensagem de Resumo ao Usuário root*.
- 6** Clique em *OK* para aplicar suas configurações e fazer com que o primeiro backup seja iniciado no horário especificado.

28.6.3 Restaurando um backup de sistema

Use o módulo Restauração do Sistema do YaST para restaurar a configuração do sistema a partir de um backup. Restaure todo o backup ou selecione componentes específicos que estavam corrompidos e precisam ser redefinidos ao estado antigo.

1 Inicie *YaST* > *Sistema* > *Restauração do Sistema*.

2 Insira o local do arquivo de backup. Pode ser um arquivo local, um arquivo de rede montado ou um arquivo em um dispositivo removível, como disquete ou DVD. Depois, clique em *Avançar*.

A caixa de diálogo a seguir exibe um resumo das propriedades do arquivo, como nome de arquivo, data de criação, tipo de backup e comentários opcionais.

3 Revise o conteúdo do arquivo clicando em *Conteúdo do Arquivo*. Se você clicar em *OK*, retornará à caixa de diálogo *Propriedades do Arquivo*.

4 *Opções de Especialista* abre uma caixa de diálogo na qual é possível ajustar o processo de restauração. Retorne à caixa de diálogo *Propriedades do Arquivo* clicando em *OK*.

5 Clique em *Avançar* para abrir a exibição dos pacotes a serem restaurados. Pressione *Aceitar* para restaurar todos os arquivos do pacote, ou use os vários botões *Selecionar Tudo*, *Anular Seleção* e *Selecionar Arquivos* para fazer a sintonia fina da sua seleção. Somente use a opção *Restaurar Banco de Dados RPM* se o banco de dados RPM estiver corrompido ou tiver sido apagado e se esse arquivo estiver incluído no backup.

6 Depois que você clicar em *Aceitar*, o backup será restaurado. Clique em *Concluir* para sair do módulo após a conclusão do processo de restauração.

28.6.4 Recuperando um sistema corrompido

Há vários motivos pelos quais um sistema pode não ser inicializado ou executado adequadamente. Um sistema de arquivos corrompido após uma falha do sistema, arquivos de configuração corrompidos ou uma configuração de carregador de boot corrompida são os mais comuns.

O SUSE Linux Enterprise Desktop oferece dois métodos diferentes para resolver essas situações. Você pode usar a funcionalidade Reparo do Sistema do YaST ou inicializar o sistema de recuperação. As seções a seguir abordam os dois tipos de reparo do sistema.

Usando o Reparo do Sistema do YaST

NOTA: configurações de teclado e idioma

Se você mudar as configurações de idioma depois de inicializar, o teclado também será adaptado.

Antes de iniciar o módulo Reparo do Sistema do YaST, determine em que modo ele será executado para melhor atender às suas necessidades. Dependendo da gravidade e da causa da falha do sistema (bem como da sua experiência), existem três modos diferentes a escolher:

Reparo Automático

Se o sistema falhou devido a uma causa desconhecida e você basicamente não sabe que parte do sistema é responsável pela falha, use *Reparo Automático*. Uma ampla verificação automatizada será executada em todos os componentes do sistema instalado. Para obter uma descrição detalhada deste procedimento, consulte “Reparo Automático” (p 411).

Reparo Personalizado

Se o sistema falhou e você sabe qual é o componente responsável, poderá reduzir a extensa verificação do sistema com *Reparo Automático*, e limitar o escopo da análise do sistema a esses componentes. Por exemplo, se as mensagens do sistema antes da falha sugerirem a existência de um erro no banco de dados de pacotes, você poderá limitar o procedimento de análise e reparo para que apenas verifique e restaure esse aspecto do sistema. Para obter uma descrição detalhada deste procedimento, consulte “Reparo Personalizado” (p 413).

Ferramentas Especialista

Se você já tem uma idéia clara do componente que falhou e como isso deve ser corrigido, pode ignorar as execuções de análise e aplicar diretamente as ferramentas necessárias para o reparo do componente relevante. Para obter informações detalhadas, consulte “Ferramentas Especialista” (p 414).

Escolha um dos modos de reparo descritos acima e prossiga com o reparo do sistema conforme explicado nas seções a seguir:

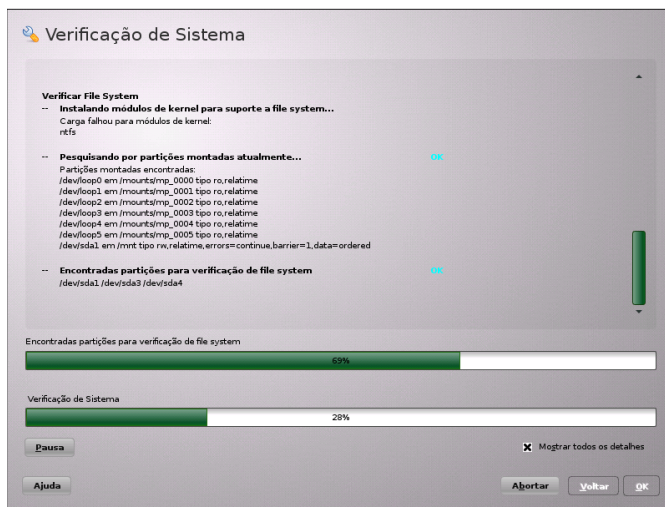
Reparo Automático

Para iniciar o modo de reparo automático do Reparo do Sistema do YaST, faça o seguinte:

- 1 Insira a mídia de instalação do SUSE Linux Enterprise Desktop na unidade de DVD.
- 2 Reinicialize o sistema.
- 3 Na tela de boot, selecione *Reparar o Sistema Instalado*.
- 4 Confirme o contrato de licença e clique em *Avançar*.
- 5 Selecione *Reparo Automático*.

O YaST inicia uma ampla análise do sistema instalado. O progresso do procedimento é exibido na parte inferior da tela com duas barras. A barra superior mostra o progresso do teste atualmente em execução. A barra inferior mostra o progresso geral da análise. A janela de registro na seção superior controla o teste atualmente em execução e o seu resultado. Consulte a Figura 28.4, “Modo de Reparo Automático” (p 411).

Figura 28.4 Modo de Reparo Automático



As execuções de testes principais a seguir são feitas com cada execução e contém, por sua vez, vários subtestes individuais:

Verificar Tabela de Partições

Verifica a validade e coerência das tabelas de partição de todos os discos rígidos detectados.

Verificar Área de Swap

As partições de troca do sistema instalado são detectadas, testadas e oferecidas para ativação, onde aplicável. Essa oferta deve ser aceita para que a velocidade de reparo do sistema aumente.

Verificar File System

Todos os sistemas de arquivos detectados estão sujeitos a uma verificação específica de sistema de arquivos.

Verificar Entradas fstab

As entradas no arquivo são verificadas quanto à totalidade e consistência. Todas as partições válidas são montadas.

Verificar Banco de Dados de Pacotes

Verifica se todos os pacotes necessários para a operação de uma instalação mínima estão presentes. Embora seja opcionalmente possível analisar também os pacotes básicos, isso leva muito tempo, devido a seu grande número.

Verificar Configuração do Bootloader

A configuração do carregador de boot do sistema instalado (GRUB ou LILO) é verificada quanto à totalidade e coerência. Dispositivos de boot e root são examinados e a disponibilidade dos módulos initrd é verificada.

- 6** Sempre que um erro é encontrado, o procedimento pára e uma caixa de diálogo com os detalhes e possíveis soluções é aberta.

Leia as mensagens da tela com cuidado antes de aceitar a correção proposta. Se você decidir recusar uma solução proposta, seu sistema permanecerá inalterado.

- 7** Depois que o processo de reparo tiver terminado com sucesso, clique em *OK* e *Concluir* e remova a mídia de instalação. O sistema é reinicializado automaticamente.

Reparo Personalizado

Para iniciar o modo *Reparo Personalizado* e verificar seletivamente certos componentes do sistema instalado, proceda da seguinte maneira:

- 1 Insira a mídia de instalação do SUSE Linux Enterprise Desktop na unidade de DVD.
- 2 Reinicialize o sistema.
- 3 Na tela de boot, selecione *Reparar o Sistema Instalado*.
- 4 Confirme o contrato de licença e clique em *Avançar*.
- 5 Selecione *Reparo Personalizado*.

A escolha de *Reparo Personalizado* mostra uma lista de execuções de testes que são todas marcadas inicialmente para execução. A faixa total de testes corresponde à faixa de reparo automático. Se você já sabe onde não há danos, desmarque os testes correspondentes. Clique em *Próximo* para iniciar um procedimento de teste mais restrito, que provavelmente tem um tempo de execução bem menor.

Nem todos os grupos de testes podem ser aplicados individualmente. A análise das entradas fstab está sempre atrelada a uma verificação dos sistemas de arquivo, incluindo partições de troca existentes. O YaST resolve automaticamente essas dependências selecionando o menor número de execuções de teste necessárias.

- 6 Sempre que um erro é encontrado, o procedimento pára e uma caixa de diálogo com os detalhes e possíveis soluções é aberta.

Leia as mensagens da tela com cuidado antes de aceitar a correção proposta. Se você decidir recusar uma solução proposta, seu sistema permanecerá inalterado.

- 7 Depois que o processo de reparo tiver terminado com sucesso, clique em *OK* e *Concluir* e remova a mídia de instalação. O sistema é reinicializado automaticamente.

Ferramentas Especialista

Se você tem conhecimento do SUSE Linux Enterprise Desktop e já tem uma idéia bem clara do que precisa ser reparado em seu sistema, aplique diretamente as ferramentas, ignorando a análise do sistema.

Para usar o recurso *Ferramentas Especialista* do módulo Reparo do Sistema do YaST, faça o seguinte:

- 1 Insira a mídia de instalação do SUSE Linux Enterprise Desktop na unidade de DVD.
- 2 Reinicialize o sistema.
- 3 Na tela de boot, selecione *Reparar o Sistema Instalado*.
- 4 Confirme o contrato de licença e clique em *Avançar*.
- 5 Selecione *Ferramentas Especialista* e escolha uma opção de reparo.
- 6 Depois que o processo de reparo tiver terminado com sucesso, clique em *OK* e *Concluir* e remova a mídia de instalação. O sistema é reinicializado automaticamente.

As *Ferramentas Especialista* oferecem as seguintes opções para reparar a falha do sistema:

Instalar Novo Bootloader

Isso inicia o módulo de configuração do carregador de boot do YaST. Encontre detalhes na Seção 10.2, “Configurando o carregador de boot com o YaST” (p 117).

Inicializar Sistema Instalado

Tente inicializar um sistema Linux já instalado.

Iniciar Ferramenta de Particionamento

Essa opção inicia a ferramenta técnica de particionamento no YaST.

Reparar Sistema de Arquivos

Essa opção verifica os sistemas de arquivos do sistema instalado. Na seleção de todas as partições detectadas apresentada primeiro, escolha aquelas que deseja verificar.

Recuperar Partições Perdidas

É possível tentar reconstruir tabelas de partição danificadas. Uma lista de discos rígidos detectados é apresentada primeiro para seleção. Clicar em *OK* inicia a verificação. Isso pode demorar um pouco, dependendo da velocidade do seu computador e do tamanho e da velocidade do disco rígido.

IMPORTANTE: *reconstruindo uma tabela de partição*

A reconstrução de uma tabela de partição é complicada. O YaST tenta reconhecer partições perdidas analisando os setores de dados do disco rígido. As partições perdidas são adicionadas à tabela de partição de reconstrução quando reconhecidas. Isso, no entanto, não é bem-sucedido em todos os casos imagináveis.

Gravar Configurações do Sistema em Disquete

Essa opção grava arquivos de sistemas importantes em um disquete. Se um desses arquivos ficar danificado, ele poderá ser restaurado a partir do disco.

Verificar Software Instalado

Isso verifica a consistência do banco de dados de pacotes e a disponibilidade dos pacotes mais importantes. Quaisquer pacotes instalados podem ser reinstalados com essa ferramenta.

Usando o sistema de recuperação

O SUSE Linux Enterprise Desktop contém um sistema de recuperação, que consiste em um pequeno sistema Linux que pode ser carregado em um disco de RAM e montado como um sistema de arquivos raiz, permitindo acesso externo às partições Linux. Com o sistema de recuperação, você pode recuperar ou modificar qualquer aspecto importante do sistema:

- Manipule qualquer tipo de arquivo de configuração.
- Verifique se há defeitos no sistema de arquivos e inicie processos de reparo automáticos.
- Acesse o sistema instalado em um ambiente de “mudança de raiz.”
- Verifique, modifique e reinstale a configuração do carregador de boot.

- Redimensione as partições usando o comando `parted`. Encontre mais informações sobre essa ferramenta no site GNU Parted na Web <http://www.gnu.org/software/parted/parted.html>.

É possível carregar o sistema de recuperação a partir de várias origens e locais. A opção mais simples é inicializar o sistema de recuperação a partir do meio original de instalação:

- 1 Insira o meio de instalação na unidade de DVD.
- 2 Reinicialize o sistema.
- 3 Na tela de boot, pressione F4 e escolha *DVD-ROM*. Em seguida, escolha *Sistema de Recuperação* no menu principal.
- 4 Digite `root` no prompt `Rescue :`. Não é necessário inserir uma senha.

Se a sua configuração de hardware não inclui uma unidade de DVD, você poderá inicializar o sistema de recuperação a partir de uma fonte na rede. O exemplo a seguir aplica-se a um cenário de boot remoto. Se você estiver usando outro meio de boot, como um DVD, modifique o arquivo `info` adequadamente e inicialize como faria em uma instalação normal.

- 1 Digite a configuração do seu boot PXE e adicione as linhas `install=protocolo://fonte_de_instalação` e `rescue=1`. Se precisar iniciar o sistema de recuperação, prefira `repair=1`. Como em uma instalação normal, `protocolo` significa qualquer um dos protocolos de rede suportados (NFS, HTTP, FTP, etc.) e `origem_inst` é o caminho da origem de instalação da rede.
- 2 Inicialize o sistema usando “Wake on LAN”, conforme descrito na Seção “Wake on LAN” (Capítulo 11, *Remote Installation*, ↑ *Guia de Implantação*).
- 3 Digite `root` no prompt `Rescue :`. Não é necessário inserir uma senha.

Depois de acessar o sistema de recuperação, você poderá utilizar os consoles virtuais por meio das teclas `Alt + F1` a `Alt + F6`.

Um shell e muitos outros eficientes utilitários, como o programa de montagem, estão disponíveis no diretório `/bin`. O diretório `sbin` contém importantes utilitários de

arquivo e de rede para a análise e o reparo do sistema de arquivos. Esse diretório também contém os binários mais importantes para a manutenção do sistema, por exemplo, fdisk, mkfs, mkswap, mount, init e shutdown, assim como ifconfig, ip, route e netstat para a manutenção da rede. O diretório `/usr/bin` contém o editor vi, find, less e ssh.

Para ver as mensagens do sistema, use o comando `dmesg` ou exiba o arquivo `/var/log/messages`.

Verificando e manipulando arquivos de configuração

Como exemplo de uma configuração que possa ser corrigida por meio do sistema de recuperação, suponha que você tenha um arquivo de configuração defeituoso que impeça a inicialização adequada do sistema. Você pode corrigir isso usando o sistema de recuperação.

Para manipular um arquivo de configuração, faça o seguinte:

- 1 Inicie o sistema de recuperação usando um dos métodos descritos acima.
- 2 Para montar uma sistema de arquivos raiz localizado em `/dev/sda6` para o sistema de recuperação, use o seguinte comando:

```
mount /dev/sda6 /mnt
```

Agora, todos os diretórios do sistema estão localizados em `/mnt`

- 3 Mude o diretório para o sistema de arquivos raiz montado:

```
cd /mnt
```

- 4 Abra o arquivo de configuração problemático no editor vi. Ajuste e grave a configuração.
- 5 Desmonte o sistema de arquivos raiz no sistema de recuperação:

```
umount /mnt
```

- 6 Reinicialize a máquina.

Reparando e verificando os sistemas de arquivos

Geralmente, não é possível reparar sistemas de arquivos em um sistema em execução. Se você tiver sérios problemas, talvez não consiga montar seu sistema de arquivos raiz e a inicialização do sistema poderá ser encerrada com “kernel panic”. Nesse caso, a única maneira será reparar o sistema externamente. É recomendável usar o Reparo do Sistema do YaST para essa tarefa (consulte “Usando o Reparo do Sistema do YaST” (p 410) para obter detalhes). Contudo, se você precisar fazer uma verificação ou um reparo manual no sistema de arquivos, inicialize o sistema de recuperação. Ele contém os utilitários para verificar e reparar os sistemas de arquivos `ext2`, `ext3`, `ext4`, `reiserfs`, `xfs`, `dosfs` e `vfat`.

Acessando o sistema instalado

Se precisar acessar o sistema instalado a partir do sistema de recuperação, faça isso em um ambiente de *mudança de raiz*. Por exemplo, para modificar a configuração do carregador de boot ou executar um utilitário de configuração de hardware.

Para configurar um ambiente de mudança de raiz com base no sistema instalado, faça o seguinte:

- 1 Primeiro monte a partição raiz do sistema instalado e do sistema de arquivos do dispositivo (mude o nome do dispositivo de acordo com as suas configurações atuais):

```
mount /dev/sda6 /mnt
mount --bind /dev /mnt/dev
```

- 2 Agora, você pode “mudar a raiz” no novo ambiente:

```
chroot /mnt
```

- 3 Em seguida, monte `/proc` e `/sys`:

```
mount /proc
mount /sys
```

- 4 Por fim, monte as partições restantes no sistema instalado:

```
mount -a
```

- 5 Agora, você tem acesso ao sistema instalado. Antes de reinicializar o sistema, desmonte as partições com `umount -a` e saia do ambiente de “mudança de raiz” com `exit`.

ATENÇÃO: limitações

Embora você tenha acesso total aos arquivos e aplicativos do sistema instalado, há algumas limitações. O kernel em execução é o que foi inicializado com o sistema de recuperação, e não com o ambiente de mudança de raiz. Ele suporta somente o hardware essencial e não é possível adicionar módulos de kernel do sistema instalado, a menos que as versões de kernel sejam iguais (o que é improvável). Portanto, você não conseguirá acessar uma placa de som, por exemplo. Também não será possível iniciar uma interface gráfica de usuário.

Observe também que você sai do ambiente de “mudança de raiz” ao percorrer o console com as teclas `Alt + F1` a `Alt + F6`.

Modificando e reinstalando o carregador de boot

Às vezes, não é possível reinicializar um sistema porque a configuração do carregador de boot está corrompida. As rotinas de inicialização não podem, por exemplo, converter unidades físicas em locais reais no sistema de arquivos Linux sem um carregador de boot ativo.

Para verificar a configuração do carregador de boot e reinstalá-lo, faça o seguinte:

- 1 Execute as etapas necessárias para acessar o sistema instalado como descrito em “Acessando o sistema instalado” (p 418).
- 2 Verifique se os arquivos a seguir estão configurados corretamente de acordo com os princípios de configuração do GRUB, descritos no Capítulo 10, *O carregador de boot GRUB* (p 105) e aplique as correções, se necessário.

- `/etc/grub.conf`
- `/boot/grub/device.map`
- `/boot/grub/menu.lst`
- `/etc/sysconfig/bootloader`

3 Reinstale o carregador de boot usando a seguinte sequência de comandos:

```
grub --batch < /etc/grub.conf
```

4 Desmonte as partições, efetue logout do ambiente de “mudança de raiz” e reinicialize o sistema:

```
umount -a  
exit  
reboot
```