RWTUV
ISO 9001: 2000 Certificated
In Publication & Cover Design

Vol. 2

Mastering
Red Hat Linux

Translated by: Ali Nasseh

مؤسسه فرهنگی هنری دیباگران تهران
سعادت آباد - میدان کاج - سرو شرقی
روبه روی خیابان علامه - پلاک ۹۷
تلفن ۷-۲۲۰۹۸۴۳۶ دورنگار ۲۲۰۹۸۴۴۸
فروش اینترنتی www.mftshop.com
E-mail : publishing@mftmail.com
URL : www.mftsite.com

ISBN 964-354-709-0
ISBN 964-354-701-9(2VOL.SET)
9 789643 547004

به نام خدا

مؤسسه فرهنگی هنری
دیباگران تهران

مرجع کامل
Red Hat Linux

(جلد دوم)

مترجم

مهندس علی ناصح

دارنده گواهینامه ISO 9001/2000
در زمینه نشر کتاب و طراحی جلد

Mastering Red Hat Linux 9

مرجع کامل Red Hat Linux (جلد دوم)

مترجم : مهندس علی ناصح

ناشر : مؤسسه فرهنگی هنری دیباگران تهران

حروفچینی و صفحه‌آرایی : مجتمع فنی تهران

طرح روی جلد : مجتمع فنی تهران

چاپ : کبریا

نوبت چاپ : اول

تاریخ نشر : خرداد ماه ۱۳۸۵

تیراژ : ۳۰۰۰ نسخه

قیمت : ۶۷۰۰۰ ریال

شابک : ۰- ۷۰۰-۳۵۴-۹۶۴

ISBN: 964-354-700-0

شابک دوره :۹-۷۰۱- ۳۵۴ -۹۶۴

ISBN: 964-354-701-9(Vol. SET)

جانگ، مایکل Jang, Michael.

مرجع کامل Red Hat Linux [رد هت لینوکس] / مایکل جانگ؛ مترجم علی ناصح.—تهران: مؤسسه فرهنگی هنری دیباگران تهران، ۱۳۸۵.

ج.: مصور، جدول.

ISBN 964-354-705-1 (ج.۱)

ISBN 964-354-700-0 (ج.۲)

ISBN 964-354-701-9 (دوره)

فهرست‌نویسی بر اساس اطلاعات فیپا.

عنوان اصلی: Mastering Red Hat Linux 9, 2003.

۱.سیستم عامل لینوکس.۲.سیستم‌های عامل (کامپیوتر).الف.ناصح، علی، ۱۳۵۲- ، مترجم.ب.عنوان.

QA۷۶/۷۶/س۹۴ج۲۲ ۰۰۵/۲۶۸

۱۳۸۵

کتابخانه ملی ایران ۸۵-۳۵۸۲م

آدرس: سعادت آباد، میدان کاج . خ سرو شرقی. روبه‌روی خ علامه . ساختمان شماره ۹۷

تلفن : ۷- ۲۲۰۹۸۴۴۶ صندوق پستی: ۹۴۳/ ۱۴۳۳۵

فهرست مطالب

بخش ششم: سرویس‌های شبکه در سیستم‌عامل Linux

فصل بیست‌وسوم: سرویس دسترسی از راه دور و شبح xinetd

فصل بیست‌وچهارم: سرویس‌های DNS و DHCP

فصل بیست‌وپنجم: بهره‌برداری از سرویس‌های چاپ CUPS و LPD در سیستم‌عامل Linux

فصل بیست‌وششم: استفاده از سرویس پست الکترونیکی

بخش هفتم: سرویس‌های اشتراک فایل در سیستم‌عامل Linux

فصل بیست‌وهفتم: استفاده از سرویس FTP

مقدمه ناشر

حمد و سپاس ایزد منان را که با الطاف بیکران خود این توفیق را به ما ارزانی داشت تا بتوانیم در راه ارتقای دانش عمومی و فرهنگ این مرز و بوم در زمینه چاپ و نشر کتب علمی دانشگاهی، علوم پایه و به ویژه علوم کامپیوتر و انفورماتیک گام‌هایی هر چند کوچک برداشته و در انجام رسالتی که بر عهده داریم، مؤثر واقع شویم. گستردگی علوم و توسعه روزافزون آن، شرایطی را به وجود آورده که هر روز شاهد تحولات اساسی چشمگیری در سطح جهان هستیم. این گسترش و توسعه نیاز به منابع مختلف از جمله کتاب را به عنوان قدیمی‌ترین و راحت‌ترین راه دستیابی به اطلاعات و اطلاع‌رسانی، بیش از پیش روشن می‌نماید. در این راستا، واحد انتشارات مؤسسه فرهنگی هنری دیباگران تهران با همکاری جمعی از اساتید، مؤلفان، مترجمان، متخصصان، پژوهشگران، محققان و نیز پرسنل ورزیده و ماهر در زمینه امور نشر درصدد هستند تا با تلاش‌های مستمر خود برای رفع کمبودها و نیازهای موجود، منابعی پربار، معتبر و با کیفیت مناسب در اختیار علاقه‌مندان قرار دهند.

کتابی که در دست دارید با همت "**مهندس علی ناصح**" و تلاش جمعی از همکاران انتشارات میسر گشته که شایسته است از یکایک این گرامیان تشکر و قدردانی کنیم.

ویراستاری: بهنوش قیاسوند

ویرایش و صفحه‌آرایی کامپیوتری: تهمینه کاشانیان

طرح جلد: محبوبه توکلی

امور چاپ و نشر: حیدر شفیعی

ناظر چاپ: کریم براغ

در خاتمه از خوانندگان عزیز و دانش‌پژوهان گرامی خواهشمندیم ما را با ارایه پیشنهادها و انتقادهای خود در بهبود کمی و کیفی کارهای انجام شده راهنمایی کنند تا بتوانیم در آینده کتاب‌هایی با کیفیت بهتر تقدیم حضورشان کنیم.

مدیر انتشارات

مؤسسه فرهنگی هنری دیباگران تهران

publishing@mftmail.com

مقدمه مترجم

ظهور سیستم‌عامل Linux بدون شک یکی از وقایعی است که تحولات قابل توجهی را در دنیای کامپیوترها به دنبال داشت، چنان‌که سیاست‌گذاری بسیاری از سازمان‌ها و شرکت‌های دولتی و غیردولتی را در خصوص تهیه نرم‌افزار، آموزش و استفاده از کامپیوترها تحت تأثیر قرار داد. این سیستم‌عامل خیلی زود تبدیل به عرصه جدیدی برای رقابت شرکت‌های فعال در زمینه تولید نرم‌افزار و خدمات اینترنتی شد.

این سیستم‌عامل شبه UNIX فرصت بسیار خوبی را نیز برای کاربران کامپیوترهای شخصی که قبلاً تنها از سیستم‌عامل Windows استفاده می‌کردند فراهم کرد، چراکه پیش از این سیستم‌عامل UNIX تنها روی کامپیوترهای خاصی قابل اجرا بود که دسترسی به آن‌ها اغلب از طریق ترمینال‌های ویژه‌ای که برای همین منظور تدارک دیده شده بودند، انجام می‌شد. این قبیل کامپیوترها بسیار گران قیمت بودند به طوری که تنها مراکز تحقیقاتی، سازمان‌های بزرگ دولتی و برخی از دانشگاه‌ها توان خرید آن‌ها را داشتند. امروزه کاربران علاقه‌مند به UNIX می‌توانند نسخه‌ای از سیستم عامل Linux را روی کامپیوتر شخصی خود نصب کرده و از کار با آن لذت ببرند.

کتاب حاضر به بررسی نسخه‌ای از این سیستم‌عامل می‌پردازد که توسط شرکت Red Hat تهیه و توزیع می‌شود. کلیه جزییات مربوط به نصب، پیکربندی و راه‌اندازی در این کتاب توضیح داده شده است. به طور مشخص، مسایل مربوط به نصب و پیکربندی در جلد اول و استفاده از قابلیت‌های تحت شبکه و سرویس‌های اینترنتی در جلد دوم مورد بررسی قرار گرفته‌اند. هیچ فصلی از کتاب به موضوع برنامه‌نویسی تحت Linux نمی‌پردازد. علاقه‌مندان به برنامه‌نویسی باید کتاب دیگر را در این زمینه تهیه کنند. با این وجود، کتاب حاضر برای مدیران سیستم‌ها که در امور روزمره خود با مسایل مختلفی در زمینه نگهداری سیستم کامپیوتری مواجه هستند بسیار مناسب است.

در ارتباط با ترجمه تنها ذکر چند نکته ضروری است. منظور از "سیستم‌عامل Linux" هسته سیستم عامل Linux و در مواردی تمام نسخه‌هایی از این سیستم‌عامل است که توسط شرکت‌های مختلف تهیه و توزیع می‌شود. در نتیجه، "سیستم‌عامل Red Hat Linux" به نسخه‌ای از این سیستم‌عامل که توسط شرکت Red Hat تهیه و توزیع می‌شود اشاره دارد. واژه daemon با عنوان "شبح" ترجمه شده و منظور از آن برنامه‌ای است که به طور نامحسوس (یا اصطلاحاً در پشت صحنه) اجرا شده و خدمات لازم را در اختیار سایر برنامه‌ها قرار می‌دهد. در این زمینه می‌توان به مواردی چون شبح NFS و شبح LPD اشاره کرد. واژه "پوسته" و در مواردی "مفسر فرمان" برای اشاره به shell و shell interpreter در نظر گرفته شده است. از نظر فنی هر دو ترجمه صحیح است. پوسته محل تماس کاربر با سیستم‌عامل است و می‌تواند یک فرمان ساده یا مجموعه‌ای از فرامین را که در قالب فایلی نگهداری می‌شود، تفسیر کرده و به اجرا درآورد.

لازم می‌دانم از همکاری مدیریت محترم و پرسنل "انتشارات دیباگران تهران" که امور مربوط به ویرایش ادبی، حروفچینی و در نهایت چاپ و نشر کتاب را به عهده داشته‌اند، تشکر کنم.

علی ناصح

بخش چهارم

مدیریت زیرسیستم
X Window

اهداف:

- پیکربندی زیرسیستم X Window
- بهره‌برداری از محیط گرافیکی GNOME
- بهره‌برداری از محیط گرافیکی KDE
- بهره‌برداری از برنامه‌های کاربردی گرافیکی
- بهره‌برداری از برنامه‌های گرافیکی توسعه یافته توسط شرکت Red Hat

فصل پانزدهم

پیکربندی زیرسیستم X Window

کاربران مبتدی سیستم‌عامل Linux اغلب ترجیح می‌دهند تا از نوعی رابط گرافیکی (اصطلاحاً Graphical User Interface یا به اختصار GUI) به منظور بهره‌برداری از آن استفاده کنند. در واقع برای کاربرانی که مسئولیت مدیریت سیستم Linux را به عهده ندارند، نیازی نیست از قابلیت‌های سطر فرمان سیستم‌عامل استفاده کنند. این گونه کاربران اغلب به برنامه‌های کاربردی مختلفی برای امور روزمره خود، از جمله طراحی هواپیما، فیلم‌سازی، ترسیم نمودارهای آماری و مانند آن نیاز دارند. برخی از آن‌ها نیز قبلاً تجربه کار با یک سیستم‌عامل دیگر را داشته و اکنون مایلند تا به راحتی بتوانند با سیستم‌عامل Linux ارتباط برقرار کنند. دو رابط گرافیکی GNOME و KDE متداول‌ترین رابط‌های گرافیکی موجود برای سیستم‌عامل Linux محسوب می‌شوند که به ترتیب در فصل شانزدهم و هفدهم آن‌ها را مورد بررسی قرار خواهیم داد.

با وجودی که بیشتر مدیران سیستم‌های Linux استفاده از قابلیت‌های سطر فرمان را ترجیح می‌دهند، اغلب کاربران برای انجام امور روزانه خود نیازمند رابط‌های گرافیکی هستند. در همین راستا، سیستم‌عامل Red Hat Linux امکان بهره‌برداری از زیرسیستم گرافیکی X Window را که در قالب پروژه‌ای با عنوان Xfree86 در حال توسعه است، در اختیار قرار داده است. (برای اطلاع بیشتر در این زمینه به وب سایت رسمی پروژه مذکور در آدرس اینترنتی http://www.xfree86.org مراجعه کنید.) ساختار زیرسیستم گرافیکی X Window متشکل از دو بخش کلاینت و سرور با اسامی X Client و X Server بوده و تمام رابط‌های گرافیکی سیستم‌عامل Linux از این ساختار جهت سرویس‌دهی به کاربران استفاده می‌کنند.

چنان‌چه هنگام نصب سیستم‌عامل Red Hat Linux رابط گرافیکی GNOME یا KDE را نصب کرده و زیرسیستم گرافیکی X Window را نیز پیکربندی کرده باشید، اکنون می‌توانید کار با آن‌را شروع کنید. در غیر این صورت، اگر بسته‌های نرم‌افزاری اصلی مرتبط با زیرسیستم گرافیکی X Window را نصب کرده باشید، با بهره‌گیری از ابزار پیکربندی xf86config یا redhat-config-xfree86 می‌توانید آن‌را روی کامپیوتر خود پیکربندی کرده و مورد استفاده قرار دهید.

فایل اصلی پیکربندی زیرسیستم گرافیکی X Window فایلی است با عنوان XF86Config که در فهرست /etc/X11 مستقر است. این فایل از بخش‌های مختلفی تشکیل شده که در این فصل به بررسی جزییات هریک از آن‌ها خواهیم پرداخت. چندین فایل پیکربندی دیگر نیز در ارتباط با زیرسیستم گرافیکی X Window موجود است که از طریق آن‌ها می‌توان قابلیت‌های گرافیکی کامپیوتر میزبان را به نحو مطلوب پیکربندی کرد. در فصل حاضر این موضوعات را مورد بررسی قرار می‌دهیم:

- استفاده از ابزارهای پیکربندی زیرسیستم گرافیکی X Window
- بررسی فایل‌های پیکربندی زیرسیستم گرافیکی X Window
- اشکال‌زدایی زیرسیستم گرافیکی X Window

استفاده از ابزارهای پیکربندی زیرسیستم گرافیکی X Window

فرآیند پیکربندی زیرسیستم گرافیکی X Window تجهیزات سخت‌افزاری مختلفی را نیز شامل می‌شود. این تجهیزات سخت‌افزاری علاوه بر مانیتور شامل هرگونه تجهیزات ورودی است که به نوعی با آن در تعامل است. تجهیزات سخت‌افزاری موردنیاز برای پیکربندی زیرسیستم گرافیکی X Window را می‌توان به این صورت دسته‌بندی کرد:

- مانیتور با قابلیت تنظیم فرکانس جاروب افقی و عمودی، وضوح نمایش و نرخ نوسازی
- کارت گرافیکی با ظرفیت مشخص حافظه
- ماوس یا هر نوع ابزار اشاره‌گر دیگر جهت استفاده از رابط گرافیکی برنامه‌ها
- صفحه کلید برای استفاده از رابط گرافیکی برنامه‌ها

مشخصات پیکربندی تجهیزات سخت‌افزاری فوق در فایل /etc/X11/XF86Config به ثبت رسیده است. در صورت لزوم می‌توان محتوای این فایل را مستقیماً مورد ویرایش قرار داد. در قسمت‌های مختلف این فصل تمام محتوای فایل مزبور را بررسی خواهیم کرد. با وجود این، باید به این نکته اشاره کنیم که متأسفانه فهم محتوای این فایل تا اندازه‌ای مشکل است. از این‌رو، اغلب کاربران ترجیح می‌دهند تا از یک ابزار پیکربندی برای ویرایش محتوای این فایل استفاده کنند.

برنامه redhat-config-xfree86، ابزار مورد استفاده در سیستم‌عامل Red Hat Linux برای پیکربندی زیرسیستم گرافیکی X Window است. شرکت Red Hat مدتی‌است که سه‌ابزارپیکربندی xf86config، Xconfigator و XF86Setup را که پیش از این ابزارهای متداول برای پیکربندی زیرسیستم نامبرده محسوب می‌شدند، مورد پشتیبانی قرار نمی‌دهد. با وجود این، از آن‌جا که ابزار xf86config اغلب به عنوان ابزار پیکربندی استاندارد زیرسیستم گرافیکی X Window قلمداد شده و در قالب بسته

نرم‌افزاری این زیرسیستم توزیع می‌شود، در این فصل ابزار پیکربندی xf86config را نیز مورد بررسی قرار خواهیم داد.

چنان‌چه سیستم‌عامل Linux تجهیزات سخت‌افزاری کامپیوتر میزبان را شناسایی کرده باشد، با اجرای فرمان X -configure نیز می‌توان فایل پیکربندی زیرسیستم گرافیکی X Window را ایجاد کرد.

بسته‌های نرم‌افزاری RPM حاوی زیرسیستم گرافیکی X Window

پیش از پرداختن به ابزارهای پیکربندی زیرسیستم گرافیکی X Window اجازه دهید به طور خلاصه در مورد بسته‌های نرم‌افزاری حاوی این زیرسیستم صحبت کنیم. چنان‌چه پس از نصب سیستم‌عامل Red Hat Linux مایل به نصب بسته‌های نرم‌افزاری بیشتری باشید، می‌توانید برنامه‌ای با عنوان redhat-config-packages را که در فصل نوزدهم مورد بررسی قرار خواهیم داد، اجرا کنید. به واسطه اجرای این برنامه، صفحه‌ای با عنوان Package Group Selection شامل امکانات لازم به منظور انتخاب گروه‌های نرم‌افزاری موردنظر به نمایش درمی‌آید. (برای اطلاع بیشتر در این زمینه به فصل سوم مراجعه کنید.) با وجود این، در صورتی که زیرسیستم گرافیکی X Window و دست کم یکی از رابط‌های گرافیکی را نصب نکرده باشید، نمی‌توانید از این برنامه استفاده کنید.

در صورت عدم دسترسی به رابط گرافیکی، برای نصب بسته‌های نرم‌افزاری RPM حاوی زیرسیستم گرافیکی X Window (واقع در گروه نرم‌افزاری base-x) می‌توانید از فرمان rpm استفاده کنید. (برای اطلاع بیشتر درباره این فرمان به فصل دهم مراجعه کنید.) برای مشاهده لیست بسته‌های نرم‌افزاری گروه base-x، کافی است محتوای فایل comps.xml موجود در فهرست RedHat/base/ از نخستین CD نصب سیستم‌عامل Red Hat Linux را مورد بازبینی قرار دهید. برای راحتی بیشتر، لیست بسته‌های نرم‌افزاری گروه base-x در فصل پنجم از سری فصل‌های اینترنتی کتاب حاضر تکرار شده است. از این‌رو، جهت مشاهده لیست مزبور می‌توانید به وب سایت انتشارات Sybex در آدرس اینترنتی http://www.sybex.com نیز مراجعه کنید.

پس از نصب بسته‌های نرم‌افزاری حاوی زیرسیستم گرافیکی X Window می‌توانید برای نصب یک یا چند رابط گرافیکی نیز اقدام کنید. همان گونه که در فصل‌های سوم و چهارم توضیح داده شد، دستیابی به رابط‌های گرافیکی GNOME و KDE مستلزم نصب بسته‌های نرم‌افزاری جداگانه‌ای است. لیست بسته‌های نرم‌افزاری مربوطه را به ترتیب می‌توانید با مراجعه به گروه‌های gnome-desktop و kde-desktop از فایل comps.xml مشاهده کنید.

ابزار پیکربندی xf86config

ابزار xf86config ابزار استاندارد مورد استفاده برای پیکربندی زیرسیستم گرافیکی X Window است. دسترسی به امکانات این ابزار تنها از طریق سطر فرمان امکان‌پذیر است. به این ترتیب، برای دستیابی به آن نیازی به رابط گرافیکی نیست. به کمک این ابزار می‌توان تجهیزات سخت‌افزاری موردنیاز برای برخورداری از زیرسیستم گرافیکی X Window، یعنی ماوس، صفحه کلید، مانیتور و کارت گرافیکی را پیکربندی کرد.

با وجودی که ابزار پیکربندی xf86config به همراه سیستم‌عامل Red Hat Linux 9 توزیع نمی‌شود، هم‌چنان یک ابزار استاندارد برای پیکربندی زیرسیستم گرافیکی X Window محسوب شده و به همراه بسته‌های نرم‌افزاری XFree86 از طریق وب سایت http://www.xfree86.org توزیع می‌شود.

برای دستیابی به امکاناتی که ابزار پیکربندی xf86confog در اختیار می‌گذارد، کافی است فرمانی با همین عنوان یعنی xf86config را اجرا کنید. استفاده از این ابزار نسبتاً ساده است. ابزار مورد بحث لیست کاملی از کارت‌های گرافیکی را جهت انتخاب کاربر در اختیار وی قرار می‌دهد. برای پیکربندی تجهیزات سخت‌افزاری موردنظر این مراحل را دنبال کنید:

۱- پیش از هر چیز از فایل /etc/X11/XF86Config یک نسخه پشتیبان تهیه کنید. با این اقدام، چنان‌چه ضمن پیکربندی، مرتکب اشتباه شوید، می‌توانید پیکربندی اصلی را از روی نسخه پشتیبان فایل مزبور مجدداً بازیابی کنید.

۲- فرمان xf86config را به منظور دسترسی به امکانات ابزار پیکربندی xf86config اجرا کنید. با این اقدام صفحه‌ای مشابه شکل ۱-۱۵ به نمایش درمی‌آید. چنان‌که مشاهده می‌کنید، در انتهای این صفحه به برنامه‌ای با عنوان SuperProbe اشاره شده است. این برنامه در سیستم‌عامل Red Hat Linux با برنامه دیگری به نام ddcprobe جایگزین شده است. برای ادامه عملیات کلید Enter را فشار دهید.

۳- با اقدام فوق صفحه دیگری مشابه شکل ۲-۱۵ به نمایش درآمده و امکانات لازم به منظور تعیین نوع ماوس، شبیه‌سازی دکمه سوم ماوس برای ماوس‌های دوکلیدی و تجهیزات سخت‌افزاری مربوطه در اختیار قرار می‌گیرد. پیش از تعیین مورد آخر، فرمان ls -l /dev/mouse را در کنسول مجازی دیگری اجرا کنید. (برای اطلاع بیشتر درباره کنسول‌های مجازی به فصل یازدهم مراجعه کنید.) چنان‌چه تجهیزات سخت‌افزاری /dev/mouse به پورت ماوس متصل باشد نیازی نیست که آن‌را تغییر دهید. برای ادامه عملیات کلید Enter را فشار دهید.

```
This program will create a basic XF86Config file, based on menu selections you
make.

The XF86Config file usually resides in /usr/X11R6/etc/X11 or /etc/X11.  A sample
XF86Config file is supplied with XFree86; it is configured for a standard
VGA card and monitor with 640x480 resolution.  This program will ask for a
pathname when it is ready to write the file.

You can either take the sample XF86Config as a base and edit it for your
configuration, or let this program produce a base XF86Config file for your
configuration and fine-tune it.

Before continuing with this program, make sure you know what video card
you have, and preferably also the chipset it uses and the amount of video
memory on your video card.  SuperProbe may be able to help with this.

Press enter to continue, or ctrl-c to abort.
```

شکل ۱-۱۵ نخستین صفحه‌ای که پس از اجرای فرمان xf86config به نمایش درمی‌آید.

```
1.  Microsoft compatible (2-button protocol)
2.  Mouse Systems (3-button protocol)
3.  Bus Mouse
4.  PS/2 Mouse
5.  Logitech Mouse (serial, old type, Logitech protocol)
6.  Logitech MouseMan (Microsoft compatible)
7.  MM Series
8.  MM HitTablet
9.  Microsoft IntelliMouse

If you have a two-button mouse, it is most likely of type 1, and if you have
a three-button mouse, it can probably support both protocol 1 and 2. There are
two main varieties of the latter type.  Mice with a switch to select the
protocol, and mice that default to 1 and require a button to be held at
boot-time to select protocol 2. Some mice can be convinced to do 2 by sending
a special sequence to the serial port (see the ClearDTR/ClearRTS options).

Enter a protocol number: 4

If your mouse has only two buttons, it is recommended that you enable
Emulate3Buttons

Please answer the following question with either 'y' or 'n'.
Do you want to enable Emulate3Buttons? y

Now give the full device name that the mouse is connected to, for example
/dev/ttyO0. Just pressing enter will use the default, /dev/mouse.

Mouse device.
```

شکل ۲-۱۵ پیکربندی ماوس

بسته به نوع ماوس انتخاب شده، ممکن است تنظیمات دیگری نیز موردنیاز باشد. برای مثال، در مورد ماوس‌های Logitech ممکن است لازم باشد تا قابلیت ChordMiddle را فعال کنید. هم‌چنین می‌توانید ترتیبی دهید تا حالت عملیاتی پیش‌فرض ماوس‌های Mouse Systems که دارای سه دکمه هستند، با

ماوس‌های ساخت شرکت مایکروسافت یا سازگار با آن (ماوس‌های دو دکمه‌ای) مشابه نباشد. برای اطلاع بیشتر در این زمینه به مستندات مربوطه در آدرس اینترنتی http://www.xfree86.org مراجعه کنید.

۴- در این مرحله می‌توانید صفحه کلید موردنظر خود را از میان بیش از ۲۵ نوع صفحه کلید موجود انتخاب کنید. برای ادامه عملیات کلید Enter را فشار دهید.

۵- اکنون وقت آن است تا زبان موردنظر خود را به منظور تعیین کاراکترهای قابل دستیابی از طریق‌صفحه‌کلید انتخاب کنید. تنوع این زبان‌ها قابل توجه است به طوری که حتی زبان‌هایی مانند آلبانیایی و ویتنامی را نیز شامل می‌شود. پس از انتخاب زبان موردنظر کلید Enter را فشار دهید. به این ترتیب می‌توانید عنوانی را برای پیکربندی خود وارد کنید. پس از وارد کردن عنوان مورد نظر، برای ادامه عملیات مجدداً کلید Enter را فشار دهید. با اقدام فوق این پیغام را مشاهده خواهید کرد:

```
Please answer the following question with either 'y' or 'n'.
Do you want to select additional XKB options (group switcher,
group indicator, etc)?
```

۶- مجموعه گزینه‌های XKB برای کاربران غیر انگلیسی زبانی که به ویژه از صفحه کلیدهایی با چندین نوع الفبا استفاده می‌کنند، جالب توجه است. به استثنای تجربیات آقای ایوان پاسکال در این زمینه که با مراجعه به آدرس اینترنتی htt://www.tsu.ru/~pascal/en/xkb قابل دستیابی است، مستندات قابل توجهی در ارتباط با گزینه‌های XKB در دسترس نیست. چنان‌چه از صفحه کلیدی شامل یک نوع الفبا استفاده می‌کنید، کافی است در مقابل پرسش فوق پاسخ n را وارد کرده و برای ادامه عملیات کلید Enter را فشار دهید.

۷- در این مرحله می‌توانید مانیتور مورد استفاده خود را پیکربندی کنید. با مراجعه به دفترچه راهنمای مانیتور، محدوده قابل قبول فرکانس جاروب افقی و عمودی را وارد کنید. در صورتی که از محدوده قابل قبول مانیتور خود اطلاع ندارید، به منظور اجتناب از آسیب‌دیدگی آن کمترین محدوده ممکن را انتخاب کنید. پس از تعیین شناسه‌ای برای این تنظیمات کلید Enter را به منظور ادامه عملیات فشار دهید.

۸- با اقدام فوق گزینه‌های مربوط به پیکربندی کارت گرافیکی به نمایش درمی‌آید. پیش از هر اقدامی دفترچه راهنمای کارت گرافیکی خود را مورد مطالعه قرار داده و از نوع کارت گرافیکی مورد استفاده اطلاع حاصل کنید. چنان‌که شکل ۳-۱۵ نیز نشان می‌دهد، برای تعیین نوع کارت گرافیکی می‌توانید به بانک اطلاعاتی مربوطه مراجعه کنید. برای این منظور کافی است در مقابل

پرسش مربوطه پاسخ y را وارد کرده و کارت گرافیکی موردنظر را از لیست حاصل انتخاب کنید. در این صورت ابزار پیکربندی xf86config، گزینه‌هایی را نیز به منظور پیکربندی سایر جزییات در اختیار قرار خواهد داد.

```
Now we must configure video card specific settings  At this point you can
choose to make a selection out of a database of video card definitions
Because there can be variation in Randacs and clock generators even
between cards of the same model, it is not sensible to blindly copy
the settings (e g. a Device section)  For this reason, after you make a
selection, you will still be asked about the conponents of the card, with
the settings from the chosen database entry presented as a strong hint

The database entries include information about the chipset, what driver to
run, the Ramdac and ClockChip, and comments that will be included in the
Device section  However, a lot of definitions only hint about what driver
to run (based on the chipset the card uses) and are untested.

If you can't find your card in the database, there's nothing to worry about.
You should only choose a database entry that is exactly the same model as
your card; choosing one that looks similar is just a bad idea (e g  a
GemStone Snail 64 may be as different from a GemStone Snail 64+ in terms of
hardware as can be)

Do you want to look at the card database? ▌
```

شکل ۳-۱۵ پیکربندی کارت گرافیکی

۹- بانک اطلاعاتی فوق حاوی مشخصات بیش از ۷۰۰ نوع کارت گرافیکی است. از این میان کارت گرافیکی مورد استفاده خود را پیدا کرده و شماره مربوط به آن‌را وارد کنید. در غیر این صورت حرف q را (به نشانه quit) برای خروج از بانک اطلاعاتی وارد کرده و پس از تأیید مشخصات کارت گرافیکی موردنظر کلید Enter را جهت ادامه عملیات فشار دهید.

۱۰- اندازه حافظه کارت گرافیکی را پس از نمایش پرسش مربوطه تعیین کنید. سپس شناسه‌ای را برای این تنظیمات وارد کنید.

۱۱- در این مرحله می‌توانید چند وضوح تصویر مختلف را برای کارت گرافیکی و مانیتور خود مشخص کنید. همان گونه که شکل ۴-۱۵ نشان می‌دهد، با انتخاب یکی از سه گزینه 1، 2 یا 3 در این مرحله می‌توانید وضوح تصویر پیش‌فرض را برای سه عمق رنگ ۸ بیتی، ۱۶ بیتی و ۲۴ بیتی تعیین کنید. انتخاب گزینه 4 مستقیماً تنظیمات مرحله ۱۳ را در اختیار قرار می‌دهد.

```
For each depth, a list of modes (resolutions) is defined. The default
resolution that the server will start-up with will be the first listed
mode that can be supported by the monitor and card
Currently it is set to:

"640x400" for 8-bit
"640x480" for 16-bit
"640x480" for 24-bit

Modes that cannot be supported due to monitor or clock constraints will
be automatically skipped by the server.

 1  Change the modes for 8-bit (256 colors)
 2  Change the modes for 16-bit (32K/64K colors)
 3  Change the modes for 24-bit (24-bit color)
 4  The modes are OK, continue.

Enter your choice  3

Select modes from the following list:

 1  "640x400"
 2  "640x480"
 3  "800x600"
 4  "1024x768"
 5  "1280x1024"
 6  "320x200"
 7  "320x240"
 8  "400x300"
 9  "1152x864"
```

شکل ۴-۱۵ تنظیم وضوح تصویر کارت گرافیکی و مانیتور

۱۲- وضوح تصویر پیش‌فرض را برای عمق رنگ موردنظر انتخاب کنید. در صورت تمایل می‌توانید گزینه virtual screen را به منظور دستیابی به وضوح تصویری که بیش از حوزه مانیتور است (مانند ۱۴۰۰ × ۱۸۰۰) انتخاب کنید. اقدام مرحله ۱۱ را مجدداً تکرار کنید.

۱۳- عمق رنگ پیش‌فرض را از میان گزینه‌های موجود، شامل عمق ۱ بیتی، ۴ بیتی، ۸ بیتی، ۱۶ بیتی، ۲۴ بیتی و در صورت امکان ۳۲ بیتی انتخاب کنید.

۱۴- چنان‌چه با تنظیمات انجام شده موافق هستید، اجازه دهید تا ابزار xf86config آن‌ها را در فایل پیکربندی /etc/X11/XF86Config منعکس کند.

همان‌گونه که شکل ۵-۱۵ نیز نشان می‌دهد، در صورت تمایل می‌توانید تنظیمات دیگری را نیز انجام دهید.

```
I am going to write the XF86Config file now  Make sure you don't accidently
overwrite a previously configured one.

Shall I write it to /etc/X11/XF86Config? n

Please answer the following question with either 'y' or 'n'.
Shall I write it to the default location. /usr/X11R6/etc/X11/XF86Config? n

Do you want it written to the current directory as 'XF86Config'? y

File has been written. Take a look at it before running 'startx'  Note that
the XF86Config file must be in one of the directories searched by the server
(e g  /etc/X11) in order to be used  Within the server press
ctrl, alt and '+' simultaneously to cycle video resolutions  Pressing ctrl,
alt and backspace simultaneously immediately exits the server (use if
the monitor doesn't sync for a particular mode).

For further configuration, refer to the XF86Config(5) manual page

[root@RH9Test root]#
```

شکل ۵-۱۵ ثبت مشخصات پیکربندی در فایل /etc/X11/XF86Config

فراموش نکنید که سیستم‌عامل Linux بین حروف بزرگ و کوچک الفبا تفاوت قایل می‌شود. از این‌رو، نام ابزار مورد استفاده برای پیکربندی زیرسیستم گرافیکی X Window، یعنی xf86config با نام فایلی که این پیکربندی نهایتاً در آن درج می‌شود، یعنی /etc/X11/XF86Config متفاوت است.

ابزار پیکربندی redhat-config-xfree86

در سیستم‌عامل Red Hat Linux ابزار دیگری با عنوان redhat-config-xfree86 به منظور پیکربندی زیرسیستم گرافیکی X Window مورد استفاده قرار می‌گیرد. در بیشتر موارد دسترسی به این ابزار از طریق سطر فرمان سیستم‌عامل مزبور امکان‌پذیر است. این ابزار کلیه امکانات موردنیاز برای پیکربندی مانیتور و کارت گرافیکی را در اختیار می‌گذارد. ابزار مذکور امکاناتی را نیز جهت پیکربندی کارت‌های گرافیکی ساخته شده بر اساس استاندارد VESA در اختیار قرار می‌دهد.

استاندارد VESA توسط سازمانی به همین نام، یعنی Video Electronics Standards Association توسعه یافته است. اصطلاح Super VGA به کارت‌های گرافیکی ساخته شده بر اساس همین استاندارد اطلاق می‌شود.

ابزار redhat-config-xfree86 تمام اقدامات لازم برای شناسایی تجهیزات گرافیکی کامپیوتر میزبان، شامل مانیتور و کارت گرافیکی و تعیین قابلیت‌های نمایشی را انجام می‌دهد.

شناسایی تجهیزات گرافیکی

پیش از آن‌که ابزار redhat-config-xfree86 کادر محاوره‌ای Display Settings را نمایش دهد، برنامه‌ای با عنوان ddcprobe را اجرا می‌کند. در صورت لزوم می‌توانید این برنامه را به طور دستی از طریق سطر فرمان سیستم‌عامل Red Hat Linux به اجرا درآورید. شکل ۶-۱۵ خروجی حاصل از اجرای دستی این برنامه را روی یک کامپیوتر نمونه نشان می‌دهد.

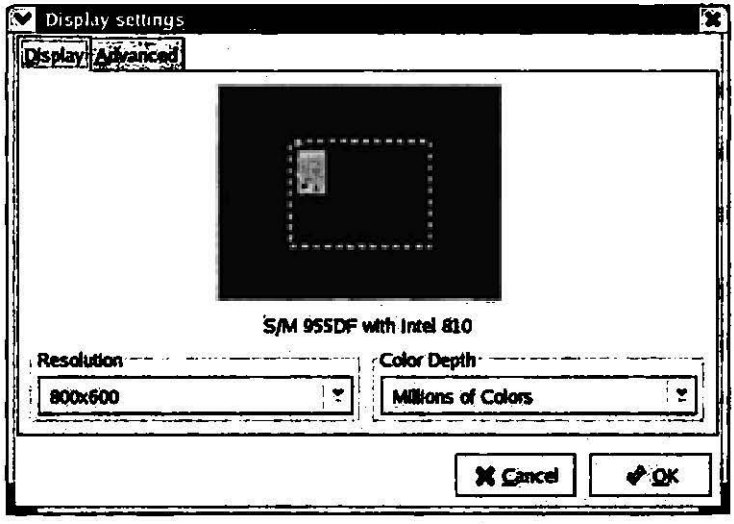
```
[root@RH9Test root]# ddcprobe

Videocard DDC probe results
Description.  Intel Corporation i810 Graphics Controller
Memory (MB)·  1

Monitor DDC probe results
ID  SAM413b
Name· S/N 95SDF
Horizontal Sync (kHZ)· 30-85
Vertical Sync (HZ)  · 50-160
Width (mm)  360
Height(mm)  270
[root@RH9Test root]#
```

شکل ۶-۱۵ شناسایی تجهیزات گرافیکی کامپیوتر میزبان توسط برنامه ddcprobe

تنظیمات صفحه نمایش

با اجرای فرمان redhat-config-xfree86 یک کادر محاوره‌ای با عنوان Display Settings مشابه شکل ۷-۱۵ به نمایش درمی‌آید. بخش Display از کادر محاوره‌ای فوق شامل امکانات لازم برای تنظیم وضوح تصویر و عمق رنگ است. این تنظیمات با توجه به قابلیت‌های کارت گرافیکی و محدودیت‌های مانیتور قابل پیکربندی است.

نیمه بالایی بخش Display از کادر محاوره‌ای Display Settings نشان‌دهنده برنامه‌های کاربردی با رابط گرافیکی است که در حال حاضر باز شده‌اند. به این ترتیب می‌توان ایده‌ای از نحوه نمایش پنجره برنامه‌های کاربردی روی مانیتور موردنظر به دست آورد. اندازه محدوده‌ای که با نقطه‌چین مشخص شده است، متناسب با انتخاب وضوح تصویر از منوی Resolution تغییر خواهد کرد.



شکل ۷-۱۵ امکانات بخش Display از کادر محاوره‌ای Display Settings

وضوح تصویر (اصطلاحاً resolution) بیانگر تعداد نقاطی است که کارت گرافیکی جهت نمایش برای مانیتور ارسال می‌کند. این عدد به صورت یک حاصلضرب بیان می‌شود. به عنوان نمونه، وضوح تصویر ۶۰۰ × ۸۰۰ بیانگر وجود ۸۰۰ نقطه در راستای افقی و ۶۰۰ نقطه در راستای عمودی است. وضوح تصویر از طریق منوی Resolution قابل تنظیم است.

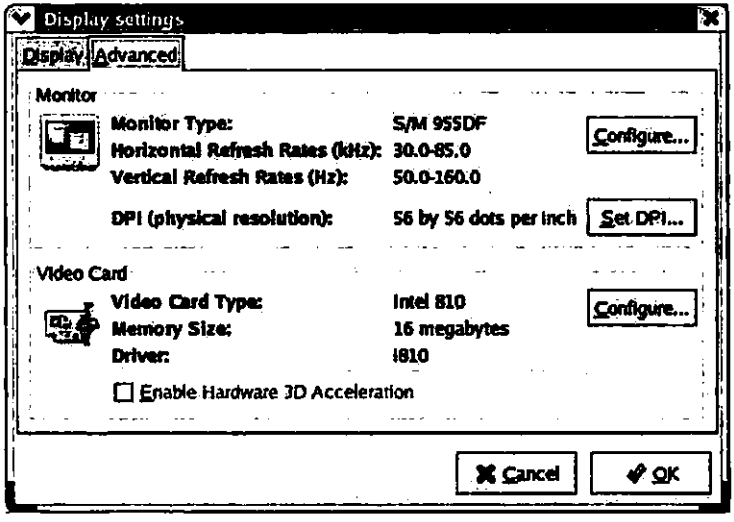
ویژگی عمق رنگ (اصطلاحاً color depth) بیانگر تعداد رنگ‌هایی است که برای نمایش هر یک از نقاط مورد استفاده قرار می‌گیرد. برای مثال، عمق رنگ ۱۶ بیتی به‌معنی استفاده از ۲ به توان ۱۶ یا ۶۵،۵۳۶ رنگ برای نمایش هر یک از نقاط است. ویژگی عمق رنگ از طریق منوی Color Depth قابل تنظیم است.

تنظیمات کارت گرافیکی

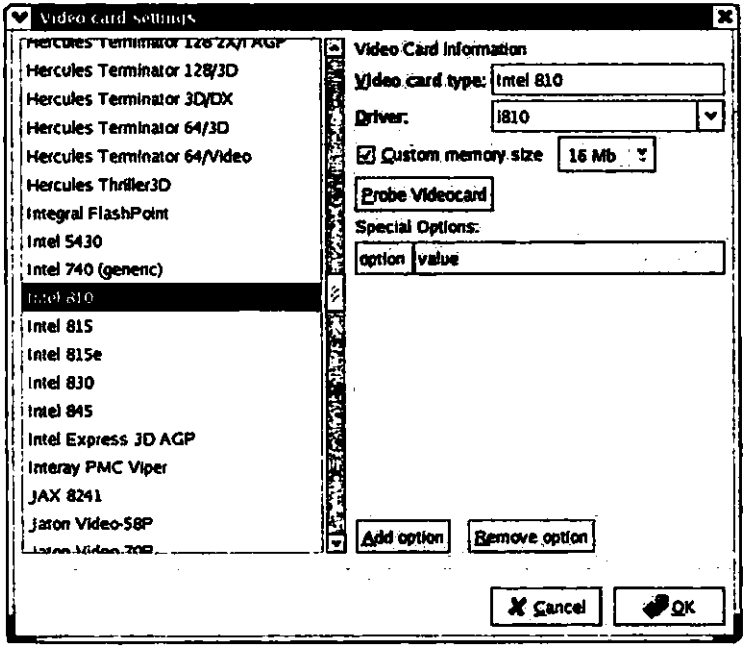
همان‌گونه که شکل ۸-۱۵ نیز نشان می‌دهد، نیمه پایینی بخش Advanced از کادر محاوره‌ای Display Settings شامل امکانات موردنیاز برای پیکربندی کارت گرافیکی است. دقت کنید که چگونه نوع مشخصات گرافیکی کامپیوتر میزبان توسط ابزار پیکربندی redhat-config-xfree86 به درستی تشخیص داده شده است.

برای پیکربندی کارت گرافیکی می‌توانید دکمه Configure از قسمت Video Card بخش Advanced از کادر محاوره‌ای Display Settings را کلیک کنید. با این اقدام، کادر محاوره‌ای دیگری با عنوان

Video Card Settings شامل امکانات موردنیاز به نمایش درمی‌آید. شکل ۹-۱۵ این کادر محاوره‌ای را نشان می‌دهد.



شکل ۸-۱۵ امکانات بخش Advanced از پنجره Display Settings



شکل ۹-۱۵ کادر محاوره‌ای Video Card Settings

کارت گرافیکی موردنظر خود را می‌توانید از لیستی شامل بیش از ۶۰۰ نوع کارت گرافیکی موجود انتخاب کنید. با انجام این کار نوع کارت گرافیکی و درایور مربوطه به ترتیب در فیلدهای Video Card Type و Driver درج می‌شود. بسته به نوع کارت گرافیکی ممکن است بتوان گزینه‌های دیگری را نیز در قسمت Special Options مقداردهی کرد.

چنان‌چه کارت گرافیکی موردنظر خود را در این لیست مشاهده نمی‌کنید، می‌توانید شانس خود را با کلیک دکمه Probe Video Card امتحان کنید. در برخی موارد، برنامه redhat-config-xfree86 با این اقدام، موفق به شناسایی کارت گرافیکی شده و درایورهای مناسب آن‌را نیز انتخاب خواهد کرد. در غیر این صورت، می‌توانید یکی از این اقدامات را انجام دهید:

- گزینه VESA Driver (Generic) را به عنوان کارت گرافیکی انتخاب کنید. با این اقدام تنظیمات استاندارد مربوط به کارت‌های گرافیکی Super VGA فعال شده و از درایور vesa به منظور راه‌اندازی آن استفاده خواهد شد. درایور مزبور برای راه‌اندازی اغلب کارت‌های گرافیکی ساخته شده در چند سال گذشته مناسب است.
- گزینه Unsupported VGA Compatible را به عنوان کارت گرافیکی انتخاب کنید. با این اقدام از درایور vga برای راه‌اندازی آن استفاده خواهد شد.
- گزینه Custom واقع در بالای لیست عناوین کارت‌های گرافیکی را انتخاب کرده و درایور موردنظر خود را جهت راه‌اندازی آن به فهرست /usr/X11R6/lib/modules/drivers که شامل ماجول‌های نرم‌افزاری موردنیاز برای راه‌اندازی تجهیزات گرافیکی است، کپی کنید.

در هر صورت، دقت کنید که باید کادر Custom Memory Size را علامت زده و اندازه حافظه کارت گرافیکی را از منوی مربوطه انتخاب کنید.

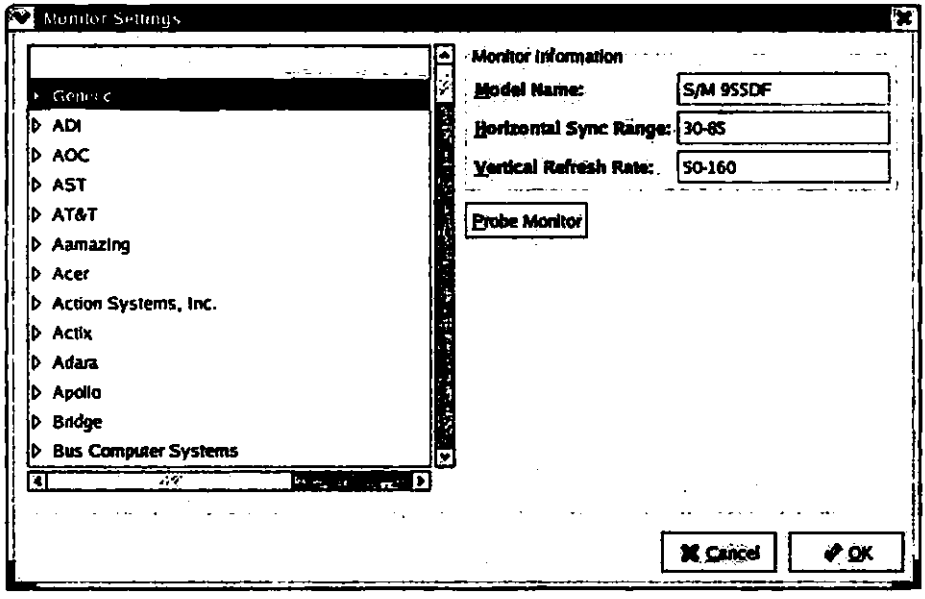
برخی از کارت‌های گرافیکی امکان تنظیمات دیگری را نیز در اختیار قرار می‌دهند. برای این منظور می‌توانید با کلیک دکمه Add Options گزینه موردنظر را مقداردهی کنید. پس از انجام این کار دکمه OK را جهت ادامه عملیات کلیک کنید.

جهت اطلاع از قابلیت تنظیمات اضافی باید نام شرکت سازنده و مدل کارت گرافیکی خود را دقیقاً بشناسید. برای مشاهده این مشخصات و هم‌چنین گزینه‌های مختلفی که می‌توان در فایل پیکربندی XF86Config برای هریک از این کارت‌های گرافیکی تنظیم کرد، به آدرس اینترنتی http://www.xfree86.org/4.3.0/RELNOTES.html مراجعه کرده و بخش Video Drivers را مورد بازبینی قرار دهید.

با این اقدام بخش Advanced از کادر محاوره‌ای Display Settings مجدداً در دسترس قرار می‌گیرد. اکنون به کادر Enable Hardware 3D Acceleration از بخش مزبور توجه کنید. چنان‌چه کارت گرافیکی مورد نظردارای قابلیت مربوطه باشد، جهت برخورداری از آن می‌توانید این کادر را علامت بزنید.

پیکربندی مانیتور

ابزار پیکربندی redhat-config-xfree86 امکانات لازم برای تنظیمات مانیتور را نیز در اختیار قرار می‌دهد. بار دیگر، در نیمه بالایی بخش Advanced از کادر محاوره‌ای Display Settings دکمه Configure را به منظور نمایش کادر محاوره‌ای Monitor Settings کلیک کنید. شکل ۱۰-۱۵ این کادر محاوره‌ای را نشان می‌دهد.

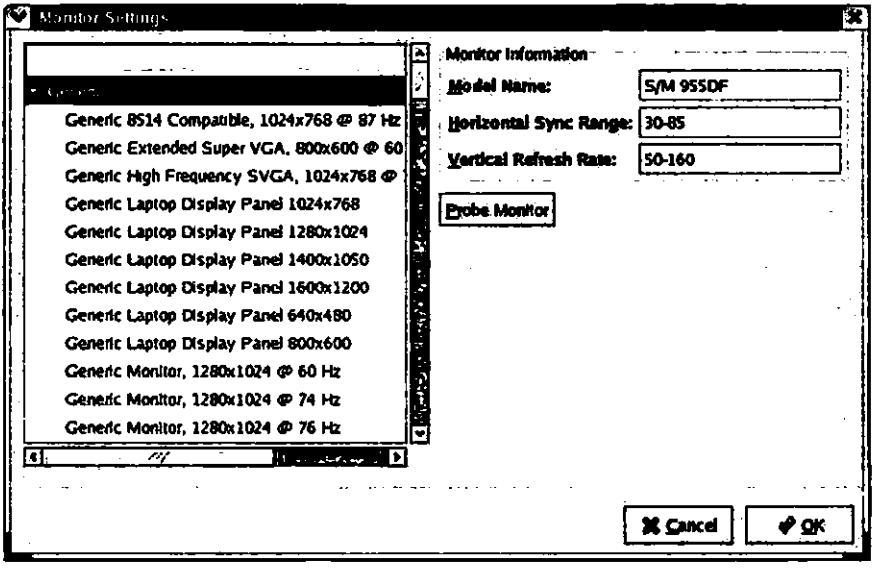


شکل ۱۰-۱۵ کادر محاوره‌ای Monitor Settings

ابزار پیکربندی redhat-config-xfree86 امکان تنظیمات مانیتورهای ساخته شده توسط بیش از ۱۰۰ شرکت سازنده را در اختیار می‌گذارد. پس از یافتن نام شرکت سازنده مانیتور، علامت فلش کنار آن‌را کلیک کنید. با این اقدام لیستی از مدل‌های مختلف مانیتورهای ساخت آن شرکت را مشاهده خواهید کرد.

علاوه بر این، با کلیک دکمه Probe Monitor ممکن است برنامه redhat-config-xfree86 موفق به تشخیص دقیق مانیتور شود.

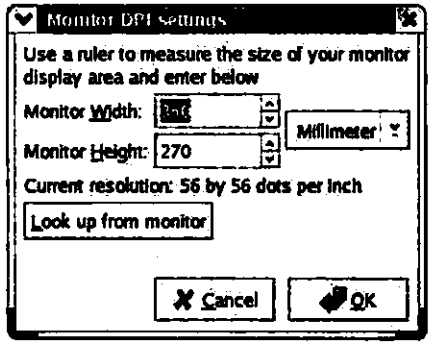
در صورتی که عنوان دقیق مانیتور خود را در لیست مانیتورهای شرکت سازنده مربوطه مشاهده نمی‌کنید می‌توانید یکی از مانیتورهای‌عمومی را انتخاب کنید. شکل ۱۱-۱۵ تعدادی از این مانیتورهای عمومی را نشان می‌دهد. این لیست حتی مانیتورهای عمومی کامپیوترهای کیفی (یا اصطلاحاً laptop) را نیز شامل می‌شود.



شکل ۱۱-۱۵ کادر محاوره‌ای Monitor Settings

تنظیمات Horizontal Sync Range و Vertical Refresh Rate را با دقت زیادی انجام دهید. برای این منظور حتماً به دفترچه راهنمای مانیتور مراجعه کنید. در صورتی که فرکانس‌های جاروب افقی یا عمودی از محدوده مجاز تعیین شده برای مانیتور موردنظر متجاوز شود، ممکن است آسیب جدی به آن برسد. با وجود مدارهای الکتریکی محافظ در اغلب مانیتورهای امروزی، بهتر است فرکانس‌های مزبور را در محدوده‌های مجاز تنظیم کنید.

پس از انجام تنظیمات جهت دستیابی مجدد به بخش Advanced از کادر محاوره‌ای Display Settings دکمه OK را کلیک کنید. با کلیک دکمه Set DPI از این بخش، کادر محاوره‌ای دیگری با عنوان Monitor DPI Settings باز می‌شود. شکل ۱۲-۱۵ این کادر محاوره‌ای را نشان می‌دهد.



شکل ۱۲-۱۵ کادر محاوره‌ای Monitor DPI Settings

به کمک امکانات این کادر محاوره‌ای می‌توانید اندازه تصاویری را که روی مانیتور به نمایش درمی‌آید، تعیین کنید. طول و عرض صفحه نمایش مانیتور به ترتیب از طریق گزینه‌های Monitor Width و Monitor Height قابل تنظیم است. به عنوان واحد اندازه‌گیری می‌توان یکی از دو گزینه میلی‌متر یا اینچ را از منوی مربوطه انتخاب کرد. برای مشاهده تنظیمات فعلی کافی است دکمه Look Up From Monitor را کلیک کنید. پس از انجام تغییرات موردنظر دکمه OK را به نشانه تأیید تنظیمات کلیک کنید. به این ترتیب کادر محاوره‌ای Display Settings بار دیگر قابل دستیابی خواهد بود.

با کلیک دکمه OK از کادر محاوره‌ای Display Settings برنامه redhat-config-xfree86 کلیه تنظیمات را درفایل /etc/X11/XF86Config ذخیره‌خواهدکرد. تأثیر این تنظیمات را می‌توانید طی راه‌اندازی‌های بعدی زیرسیستم گرافیکی X Window مشاهده کنید.

پیکربندی خودکار زیرسیستم گرافیکی X Window

در صورتی که هیچ کدام از ابزارهای پیکربندی xf86config و redhat-config-xfree86 رضایت خاطرتان را جلب نمی‌کند، می‌توانید از روش دیگری برای پیکربندی زیرسیستم گرافیکی X Window استفاده کنید. چنان‌چه مشکلی در ارتباط با شناسایی کارت گرافیکی و مانیتور وجود نداشته باشد، شانس خود را با اجرای این فرمان آزمایش کنید:

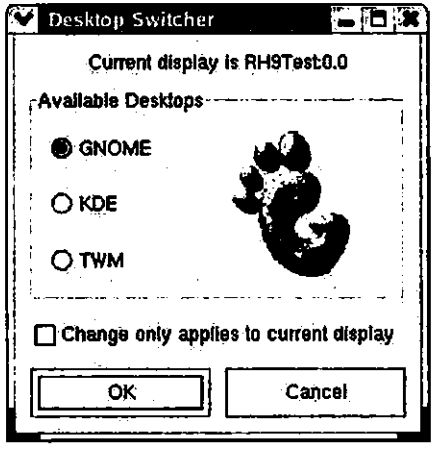
```
# X -configure
```

اجرای موفقیت آمیز فرمان فوق منجر به ایجاد فایل جدیدی با عنوان XF86Config.new در فهرست جاری خواهد شد. پیش از هر اقدام دیگری از فایل /etc/X11/XF86Config نسخه پشتیبان کنید. در صورت لزوم می‌توانید تغییراتی را در محتوای فایل جدید ایجاد کنید. (درباره چگونگی انجام این کار به زودی صحبت خواهیم کرد.) اکنون فایل جدید را به XF86Config تغییر نام داده و پس از جایگزین

کردن آن با فایل /etc/X11/XF86Config فرمان startx را جهت مشاهده نتیجه عملیات اجرا کنید.

برنامه switchdesk

درصورتی‌که رابط‌های گرافیکی متعددی را نصب کرده باشید، با استفاده از برنامه‌ای با نام switchdesk، به سادگی می‌توانید رابط گرافیکی دلخواه خود را جهت استفاده انتخاب کنید. چنان‌چه کاربر پیش از این یک محیط گرافیکی (مثلاً محیط GNOME) را راه‌اندازی کرده باشد، با اجرای فرمان switchdesk پنجره‌ای با عنوان Desktop Switcher به نمایش درمی‌آید. شکل ۱۳-۱۵ پنجره حاصل از این اقدام را نشان می‌دهد.



شکل ۱۳-۱۵ پنجره Desktop Switcher

پنجره Desktop Switcher، گزینه‌هایی را برای انتخاب رابط‌های گرافیکی نصب شده روی کامپیوتر میزبان در اختیار قرار می‌دهد. با استفاده از این گزینه‌ها به سادگی می‌توان از یک محیط گرافیکی به محیط دیگر (مثلاً از محیط GNOME به KDE) سوییچ کرد.

چنان‌چه قبلاً هیچ‌کدام از رابط‌های گرافیکی راه‌اندازی نشده باشد، باز هم می‌توان فرمان switchdesk را از طریق سطر فرمان سیستم‌عامل Linux اجرا کرد. برای این منظور کافی است عنوان محیط گرافیکی پیش‌فرض خود را در مقابل این فرمان مشخص کنید. به عنوان مثال، با این فرمان محیط گرافیکی KDE به عنوان محیط گرافیکی پیش‌فرض در نظر گرفته خواهد شد:

```
# switchdesk KDE
```

محیط‌های گرافیکی سیستم‌عامل Linux

محیط‌های گرافیکی متعددی را می‌توان در سیستم‌عامل Linux مورد استفاده قرار داد. برخی از مداول‌ترین محیط‌های گرافیکی که برای برنامه switchdesk نیز قابل شناسایی است به این شرح است:

- **GNOME**: این محیط در واقع محیط گرافیکی پیش‌فرض سیستم‌عامل Red Hat Linux است. اصطلاح GNOME کوتاه شده عبارت GNU Network Object Model Environment است.
- **KDE**: این محیط یکی از متداول‌ترین محیط‌های گرافیکی است. اصطلاح KDE کوتاه شده K Desktop Environment است.
- **fvwm و fvwm95**: پیش از ظهور محیط‌های گرافیکی GNOME و KDE، دو محیط fvwm و fvwm95 محیط‌های گرافیکی‌استاندارد در سیستم‌عامل Red Hat Linux به شمار می‌آمدند. از آن‌جا که بهره‌برداری از این دو محیط گرافیکی نیازمند حافظه بسیار کمی است، استفاده از آن‌ها در دوران گرانی حافظه کامپیوترهای شخصی بسیار متداول بود.
- **Enlightenment**: این‌محیط از بیشترین قابلیت‌پیکربندی درمیان‌محیط‌های‌گرافیکی سیستم‌عامل Linux برخوردار است.
- **twm**: این محیط شامل ابتدایی‌ترین امکانات گرافیکی است. در سیستم‌عامل Red Hat Linux محیط twm تنها یک کنسول ساده بوده و کمترین ابزارها و برنامه‌های گرافیکی را در اختیار می‌گذارد. با این وجود، از کارآیی خوبی برخوردار است.
- **WindowMaker**: کاربری آسان و سادگی در برقراری ارتباط، باآن، از ویژگی‌های محیط گرافیکی WindowMaker به‌شمار می‌رود. این‌محیط بی‌شباهت به‌محیط‌گرافیکی سیستم‌عامل NeXTStep نیست.

تغییر برنامه Display Manager

برنامه Display Manager امکانات لازم برای ورود به سیستم را در قالب یک محیط گرافیکی در اختیار کاربر می‌گذارد. در سیستم‌عامل Red Hat Linux سه نسخه متفاوت از این برنامه را می‌توان مورد استفاده قرار داد. دو نسخه از آن در قالب محیط‌های گرافیکی GNOME و KDE و دیگری در قالب زیرسیستم گرافیکی X Window روی کامپیوتر میزبان نصب می‌شود.

با ویرایش فایل /etc/X11/prefdm و مقداردهی مناسب متغیری با عنوان preferred می‌توان برنامه Display Manager پیش‌فرض را مشخص کرد. تقریباً در خط دهم از این فایل متغیر نامبرده را می‌توان

به این صورت مشاهده کرد:

```
preferred=
```

برای تعیین برنامه Display Manager پیش‌فرض کافی است متغیر فوق را به یکی از این روش‌ها مقداردهی کنید:

```
preferred=gdm
preferred=kdm
preferred=xdm
```

مقداردهی اول برنامه GNOME Display Manager، مقداردهی دوم برنامه KDE Display Manager و مقداردهی سوم برنامه X Display Manager را به عنوان برنامه Display Manager پیش‌فرض پیکربندی می‌کند. در قسمت‌های بعد به بررسی هریک از این برنامه‌ها می‌پردازیم.

برنامه GNOME Display Manager

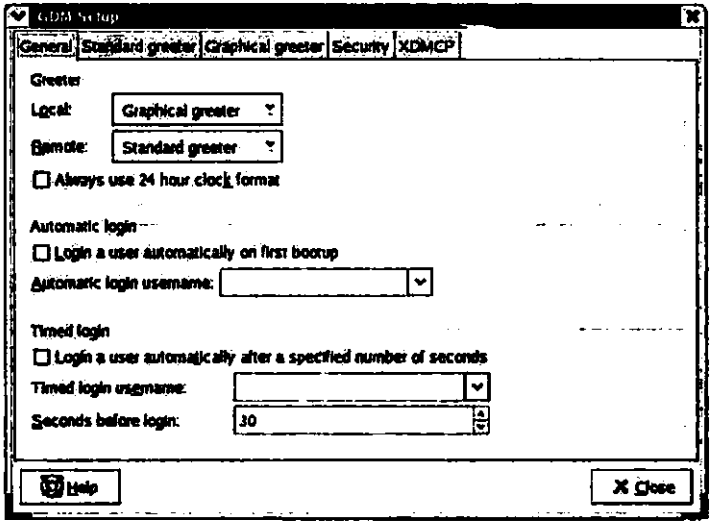
شکل ۱۴-۱۵ صفحه برنامه GNOME Display Manager را نشان می‌دهد.

شکل ۱۴-۱۵ رابط گرافیکی برنامه GNOME Display Manager

در پایین این صفحه که شامل یک کادر متنی برای دریافت نام کاربری است، چهار گزینه مختلف به این شرح وجود دارد:

- **منوی Language**: چنان‌چه قبلاً بسته‌های نرم‌افزاری حاوی زبان‌های مختلفی را نصب کرده باشید، با کلیک روی این گزینه می‌توانید زبان موردنظر خود را جهت کار با سیستم‌عامل Red Hat Linux انتخاب کنید.
- **منوی Session**: با کلیک روی این گزینه می‌توانید محیط گرافیکی موردنظر خود را جهت کار با سیستم‌عامل Red Hat Linux انتخاب کنید.
- **منوی Reboot**: کلیک روی این گزینه، پس از تأیید عملیات منجر به راه‌اندازی مجدد کامپیوتر خواهد شد.
- **منوی Shutdown**: کلیک روی این گزینه، پس از تأیید عملیات منجر به خاموش شدن کامپیوتر خواهد شد.

در صورت تمایل می‌توانید برنامه GNOME Display Manager را پیکربندی کنید. برای این منظور، فرمان gdmsetup را در یک محیط گرافیکی اجرا کنید تا به این ترتیب کادر محاوره‌ای GDM Setup باز شود. شکل ۱۵-۱۵ این کادر محاوره‌ای را نشان می‌دهد.



شکل ۱۵-۱۵ کادر محاوره‌ای GDM Setup

بخش‌های مختلف کادر محاوره‌ای فوق به این شرح است:

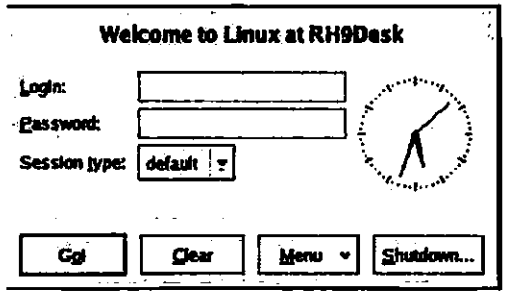
- **بخش General**: این بخش حاوی امکانات لازم برای تعیین مقادیر پارامترهای ورود به سیستم چه به صورت محلی و چه از راه دور است.

- **بخش Standard Greeter**: این بخش حاوی امکانات لازم برای تعیین نحوه نمایش (یا اصطلاحاً look and feel) رابطی است که معمولاً برای ورود به سیستم از راه دور مورد استفاده قرار می‌گیرد.
- **بخش Graphical Greeter**: این بخش حاوی چند ماسک (اصطلاحاً theme) است که با انتخاب هریک می‌توان رابط گرافیکی برنامه Display Manager را تغییر داد. شرکت Red Hat به طور پیوسته ماسک‌های جدیدی را توسعه داده و در اختیار کاربران قرار می‌دهد. ماسک‌های متعددی نیز در قالب پروژه GNOME و هم‌چنین توسط شرکت‌های مختلف از جمله Ximian توسعه یافته است.
- **بخش Security**: این بخش امکاناتی را جهت کنترل ورود کاربر اصلی به سیستم و کاربرانی که از راه دور برای ورود به سیستم اقدام می‌کنند، در اختیار قرار می‌دهد.
- **بخش XDMCP**: این بخش حاوی امکاناتی برای تعیین نحوه ارتباط برنامه Display Manager با کاربرانی است که از راه دور برای ورود به سیستم اقدام می‌کنند. اصطلاح XDCMP کوتاه شده عبارت X Display Manager Control Panel است.

همان گونه که در فصل هفدهم توضیح خواهیم داد، پیکربندی برنامه KDE Display Manager را می‌توان از طریق تنظیماتی با عنوان KDE Control Center Login Manager انجام داد. این در حالی است که برنامه X Display Manager فاقد امکانات گرافیکی لازم برای پیکربندی است. با وجود این، برنامه مزبور را می‌توان با ویرایش فایل /etc/X11/xdm/ پیکربندی کرد.

برنامه KDE Display Manager

شکل ۱۶-۱۵ رابط گرافیکی برنامه KDE Display Manager را نشان می‌دهد.



شکل ۱۶-۱۵ رابط گرافیکی برنامه KDE Display Manager

در ادامه به شرح امکانات این برنامه توجه کنید.

- **منوی Session Type**: این منو حاوی گزینه‌هایی برای انتخاب رابط گرافیکی موردنظر جهت کار با سیستم‌عامل Red Hat Linux است.
- **دکمه Go!**: با کلیک این دکمه نام کاربری و کلمه عبور تایپ شده در فیلدهای متنی مربوطه مورد ارزیابی قرار می‌گیرد.
- **دکمه Clear**: با کلیک این دکمه مقادیر فیلدهای متنی Username و Password پاک می‌شود.
- **منوی Menu**: این منو امکانات لازم برای راه‌اندازی مجدد بخش X Server از زیرسیستم گرافیکی X Window را در اختیار قرار می‌دهد.
- **دکمه Shutdown**: با کلیک این دکمه یک کادر محاوره‌ای جدید باز شده و گزینه‌هایی با عناوین Turn Off Computer و Restart Computer را به منظور خاموش کردن کامپیوتر و راه‌اندازی مجدد آن در اختیار می‌گذارد.

برنامه X Display Manager

شکل ۱۷-۱۵ رابط گرافیکی برنامه X Display Manager را نشان می‌دهد. چنان‌که مشاهده می‌کنید، این رابط بسیار ساده بوده و تنها شامل امکانات موردنیاز برای ورود به سیستم است.

شکل ۱۷-۱۵ رابط گرافیکی برنامه X Display Manager

تعریف چند اصطلاح مهم

در ارتباط با زیرسیستم گرافیکی X Window لازم است با تعریف چند اصطلاح مهم آشنا شوید. شباهت میان مفاهیم برخی از این اصطلاحات، چنان است که گاهی می‌توان آن‌ها را به جای یکدیگر مورد استفاده قرار داد. اکنون به شرح این اصطلاحات توجه کنید:

- **برنامه Display Manager**: این برنامه یک رابط گرافیکی است که امکانات موردنیاز برای ورود به سیستم را در اختیار کاربر قرار می‌دهد. برنامه‌های متداول در این زمینه عبارتند از GNOME

Display Manager، KDE Display Manager و X Display Manager یا به اختصار gdm، kdm و xdm.

- **محیط گرافیکی:** اصطلاح محیط گرافیکی یا دسک‌تاپ برای اشاره به یک برنامه Window Manager و مجموعه‌ای از ابزارها و برنامه‌ها مورد استفاده قرار می‌گیرد. دو محیط گرافیکی متداول در سیستم‌عامل Linux عبارتند از GNOME و KDE که در این میان برای دستیابی به محیط گرافیکی GNOME نیازی به استفاده از برنامه Window Manager خاص آن نیست. برای مثال، در نسخه‌های قدیمی‌تر سیستم‌عامل Red Hat Linux از برنامه‌ای با عنوان Enlightenment جهت دستیابی به محیط گرافیکی GNOME استفاده می‌شد.
- **رابط گرافیکی کاربر:** اصطلاح رابط گرافیکی کاربر یا Graphical User Interface (به اختصار GUI) برای اشاره به رابط گرافیکی مورد استفاده کاربر جهت تعامل با کامپیوتر مورد استفاده قرار می‌گیرد. هر رابط گرافیکی کاربر در حقیقت مجموعه‌ای از دو برنامه X Client و X Server است.
- **برنامه Window Manager:** این اصطلاح به یک برنامه X Client به‌خصوص اشاره دارد که وظیفه آن کنترل نحوه نمایش رابط گرافیکی کاربر و چگونگی تعامل کاربر با آن است.
- **برنامه X Client:** این اصطلاح به برنامه خاصی اشاره دارد که درون یک رابط گرافیکی کاربر به اجرا درمی‌آید. اجرای این برنامه به صورت محلی یا از راه دور امکان‌پذیر است.
- **برنامه X Server:** این اصطلاح به مجموعه‌ای از برنامه‌ها اطلاق می‌شود که وظیفه ایجاد رابط گرافیکی کاربر را روی کامپیوتر محلی به عهده دارند.

بررسی فایل‌های پیکربندی زیرسیستم گرافیکی X Window

در راه‌اندازی زیرسیستم گرافیکی X Window سهم فایل‌های پیکربندی و برنامه‌های مختلف را نباید نادیده گرفت. اغلب کاربران سیستم‌عامل Linux با فرمان راه‌اندازی این زیرسیستم با عنوان startx آشنایی دارند. فرمان فوق را می‌توان به این صورت اجرا کرد:

```
# startx
```

این برنامه مجموعه‌ای از فایل‌های پیکربندی و سایر برنامه‌های موجود در دو فهرست /etc/X11/xinit و /usr/X11R6/bin را مورد استفاده قرار می‌دهد. فایل‌های موجود در فهرست /etc را می‌توان برای هریک از کاربران به طور مستقل پیکربندی کرد.

مهم‌ترین فایل پیکربندی زیرسیستم گرافیکی X Window فایل /etc/X11/XF86Config است که در قسمت‌های بعدی همین فصل جزییات آن‌را بررسی خواهیم کرد.

برنامه startx

برای دستیابی به محیط گرافیکی سیستم‌عامل Linux سه روش وجود دارد. روش نخست این است که متغیر id موجود در فایل پیکربندی /etc/inittab را به نحوی ویرایش کنید که پس از بوت شدن کامپیوتر سیستم‌عامل مزبور در پنجمین سطح اجرایی راه‌اندازی شود. روش دوم این است که برای دستیابی به پنجمین سطح اجرایی فرمان init 5 را اجرا کنید. (جهت اطلاع بیشتر درباره فایل پیکربندی /etc/inittab و فرمان init به فصل یازدهم مراجعه کنید.) هر دو روش فوق یکی از رابط‌های گرافیکی برنامه Display Manager را که در قسمت‌های قبل توضیح داده شد، در اختیار قرار می‌دهد. روش سوم این است که فرمان startx را اجرا کنید. فایل اجرایی startx در فهرست /usr/X11R6/bin مستقر است. در صورت تمایل می‌توانید محتوای آن‌را با استفاده از یک ویرایشگر متنی تغییر دهید. شکل ۱۸-۱۵ بخشی از محتوای این فایل را نشان می‌دهد.

```
# This is just a sample implementation of a slightly less primitive
# interface than xinit  It looks for user  xinitrc and .xserverrc
# files, then system xinitrc and xserverrc files, else lets xinit choose
# its default.  The system xinitrc should probably do things like check
# for  Xresources files and merge them in, startup up a window manager,
# and pop a clock and serveral xterms
#
# Site administrators are STRONGLY urged to write nicer versions
#
# $XFree86  xc/programs/xinit/startx.cpp,v 3.14 2002/01/28 18 19:50 tsi Exp $

userclientrc=$HOME/.xinitrc
userserverrc=$HOME/ xserverrc
sysclientrc=/etc/X11/xinit/xinitrc
sysserverrc=/etc/X11/xinit/xserverrc
defaultclient=/usr/X11R6/bin/xterm
defaultserver=/usr/X11R6/bin/X
defaultclientargs=""
defaultserverargs=""
clientargs=""
serverargs=""
```

شکل ۱۸-۱۵ بخشی از محتوای فایل startx

همان‌گونه که مشاهده می‌کنید، این فایل شامل چندین متغیر است. با اجرای فرمان startx پیش از هر چیز، موقعیت دو فایل xinitrc. و xserverrc. در فهرست خانگی کاربر موردنظر شناسایی می‌شود. چنان‌چه فایلی با این اسامی در موقعیت مزبور موجود نباشد، به طور پیش‌فرض از فایل‌هایی با همین اسامی که در فهرست /etc/X11/xinit موجود هستند، استفاده خواهد شد.

در سیستم‌عامل Red Hat Linux فایل /etc/X11/xinit/xserverrc به طور پیش‌فرض موجود نیست. به این دلیل، فرمان startx برنامه X Server را از طریق نخستین کنسول گرافیکی ممکن و به واسطه اجرای فرمان X :0 راه‌اندازی می‌کند.

متغیرهای defaultclient و defaultserver حاوی موقعیت برنامه‌های X Client و X Server پیش‌فرض هستند. چنان‌چه در برنامه switchdesk محیط twm به عنوان محیط گرافیکی پیش‌فرض تعیین شده باشد، متغیر xterm نیز در فایل startx مقداردهی خواهد شد. سایر متغیرها به طور پیش‌فرض فاقد مقدار هستند. در صورت آشنایی با برنامه‌نویسی ممکن است به نحوه مقداردهی این متغیرها علاقه‌مند شوید.

دستیابی هم‌زمان به چند زیرسیستم گرافیکی X Window

درصورت تمایل می‌توان بیش از یک زیرسیستم گرافیکی را به صورت محلی یا از راه دور راه‌اندازی کرد. چنان‌چه در فصل سوم نیز اشاره شد، زیرسیستم گرافیکی X Window در قالب یک کنسول مجازی راه‌اندازی می‌شود. به شرطی که محیط گرافیکی قبلاً راه‌اندازی شده باشد، همواره با فشار کلید ترکیبی Ctrl+Alt+F7 می‌توان آن‌را از یک محیط صرفاً متنی (اصطلاحاً text screen) مورد دستیابی قرار داد. اگر کامپیوتر میزبان دارای حافظه کافی باشد، با اجرای فرمان startx -- :1 می‌توانید دومین زیرسیستم گرافیکی X Window را نیز به صورت محلی راه‌اندازی کرده و با فشار کلید ترکیبی Ctrl+Alt+F8 آن‌را مورد دستیابی قرار دهید.

در صورت تمایل می‌توان برنامه‌های کاربردی با رابط گرافیکی را از راه دور نیز روی کامپیوتر میزبان به اجرا درآورد. البته این کار مستلزم آن است که ابتدا کامپیوتر میزبان را جهت دریافت و اجرای فرامین ارسال شده از یک کامپیوتر راه دور پیکربندی کنید. پیش از هر چیز باید مکانیزم‌های دفاعی موجود هم‌چون دیوار آتش را غیرفعال کرده و سپس با اجرای فرمان ساده xhost +*computername* یا xhost +*remoteipaddr* زمینه لازم برای دستیابی کامپیوتر موردنظر به کامپیوتر میزبان را فراهم کنید. (در فرامین مذکور متغیرهای *computername* و *remoteipaddr* به ترتیب بیانگر نام و آدرس IP کامپیوتر راه دور هستند.) به این ترتیب، کامپیوتر راه دور می‌تواند با اجرای فرامین مناسب مانند gimp -- display *youraddr*:0.0 یا xclock -display *youripaddr*:0.0 برنامه‌های کاربردی با رابط گرافیکی را روی کامپیوتر میزبان به اجرا درآورد.

استفاده از سوییچ display در فرامین ارسالی از کامپیوتر راه دور پیرو قاعده مشخصی نیست. در مورد برخی از فرامین مانند xclock وجود تنها یک علامت خط فاصله و در مورد برخی دیگر مانند gimp

وجود دو خط فاصله قبل از آن ضروری است. برای اطلاع بیشتر در این زمینه کافی است فرمان موردنظر خود را به همراه سوییچ h- (مانند xclock -h یا gimp -h) اجرا کنید.

فهرست /etc/X11

فهرست /etc/X11 حاوی زیرفهرست‌ها و فایل‌های پیکربندی مهمی است. شرح این زیرفهرست‌ها و فایل‌های پیکربندی در جدول ۱-۱۵ آمده است.

جدول ۱-۱۵ شرح زیرفهرست‌ها و فایل‌های پیکربندی موجود در فهرست /etc/X11

عنوان فایل یا فهرست	توضیح
applink	این فهرست حاوی پیوندهای مرتبط با برنامه‌های کاربردی موجود در منوی start است.
desktop-menus	این فهرست حاوی پیکربندی‌های مربوط به منوهای مختلف مورد استفاده در محیط گرافیکی است.
fs	این فهرست حاوی پیکربندی‌های مربوط به برنامه Font Server است.
gdm	این فهرست حاوی پیکربندی‌های مربوط به برنامه GNOME Display Manager است.
lbxproxy	این فهرست حاوی پیکربندی‌های لازم برای تعامل با برنامه X Server از طریق اتصالی با پهنای باند پایین است.
prefdm	این فایل پیکربندی تعیین کننده برنامه Display Manager پیش‌فرض است
proxymngr	این فهرست حاوی فایلی از مشخصات سرویس‌های پروکسی موجود است.
rstart	این فهرست حاوی برنامه‌ای برای راه‌اندازی زیرسیستم گرافیکی X Window از راه دور است که بر اساس برنامه دیگری با عنوان rsh توسعه یافته است.
serverconfig	این فهرست حاوی پیکربندی‌های مربوط به برنامه X Server است.
starthere	این‌فهرست حاوی‌پیکربندی‌های‌لازم برای تنظیمات‌ابتدایی محیط گرافیکی است.
sysconfig	این فهرست حاوی فایل پیکربندی gnome-lokkit است.
twm	این‌فهرست حاوی فایل پیکربندی محیط گرافیکی twm با عنوان system.twmrc است.
X	این فایل، پیوندی به برنامه X Server است.

عنوان فایل یا فهرست	توضیح
xdm	این فهرست حاوی پیکربندی‌های مربوط به برنامه X Display Manager است.
XF86Config	این فایل پیکربندی، حاوی مشخصات برنامه X Server است.
xinit	این فهرست حاوی فایل‌های پیکربندی پیش‌فرض برای راه‌اندازی زیرسیستم گرافیکی X Window است. چنان‌چه فهرست خانگی کاربری که اقدام به اجرای فرمان startx کرده است فاقد فایل‌های پیکربندی مشابه باشد، با اجرای فرمان مذکور فایل‌های موجود در این فهرست جهت پیکربندی زیرسیستم گرافیکی X Window مورد استفاده قرار می‌گیرند.
xkb	این فهرست حاوی پیکربندی‌های مربوط به صفحه کلید است.
Xmodmap	این فایل پیکربندی، حاوی مشخصات صفحه کلید پیش‌فرض است.
Xresources	این فایل پیکربندی تعیین کننده فونت‌های به کار رفته در صفحه مورد استفاده کاربر (اصطلاحاً login screen) برای ورود به سیستم است.
xserver	این فهرست حاوی فایل پیکربندی SecurityPolicy است.
xsm	این فهرست حاوی پیکربندی‌های مربوط به‌مدیریت جلسات‌کاربران با زیرسیستم گرافیکی X Window است.

فایل‌های پیکربندی محلی

با استفاده از فایل‌های پیکربندی موجود در فهرست خانگی کاربران، می‌توان زیرسیستم گرافیکی X Window را برای هریک از کاربران به طور جداگانه پیکربندی کرد. چنان‌که قبلاً نیز اشاره شد، برنامه startx از مجموع این فایل‌ها دو فایل پیکربندی ~/.xinitrc و ~/.xserverrc را جهت تنظیمات زیرسیستم گرافیکی X Window مورد توجه قرار می‌دهد. علامت نقطه در ابتدای اسامی این فایل‌ها دلیل بر مخفی بودن آن‌هاست، به طوری که با اجرای فرمان ls نمی‌توان آن‌ها را مشاهده کرد.

همان‌گونه که از فصل ششم به خاطر دارید، با اجرای فرمان ls -a می‌توان فایل‌های مخفی موجود در یک فهرست را مشاهده کرد.

همان‌گونه که قبلاً توضیح داده شد، سیستم‌عامل Red Hat Linux از فایل پیکربندی xserverrc استفاده نمی‌کند. از این‌رو، فایل پیکربندی اصلی همان ~/.xinitrc است که البته به نوبه خود چندین فایل پیکربندی دیگر از فهرست خانگی کاربر را مورد استفاده قرار می‌دهد.

به خاطر داشته باشید که علامت ~ (اصطلاحاً tilde) نماینده فهرست خانگی کاربر است.

سایر فایل‌های پیکربندی مهم در این رابطه عبارتند از ~/.Xclients و ~/.Xclients-default که برنامه switchdesk امکان تغییر محتوای آن‌ها را از طریق یک رابط گرافیکی در اختیار کاربر قرار داده و به این ترتیب برنامه startx همواره از محیط گرافیکی پیش‌فرض مطلع می‌شود. چنان‌چه در مورد نحوه عملکرد این فایل‌ها کنجکاو هستید می‌توانید محتوای آن‌ها را مورد مطالعه قرار دهید. برای این منظور، پس از اجرای فرمان switchdesk محیط گرافیکی پیش‌فرض را از طریق رابط گرافیکی حاصل تغییر داده و تأثیر را روی محتوای فایل ~/.Xclients-default بررسی کنید.

برنامه xinitrc

با اجرای فرمان startx برنامه X Server اجرا شده و از طریق فایل‌های پیکربندی مربوطه تنظیماتی را در ارتباط با فونت‌ها، صفحه کلید و برنامه‌های X Client پیش‌فرض انجام می‌دهد.

فایل xinitrc یک فایل اجرایی بوده و در فهرست /etc/X11/xinit مستقر است. با وجود این، کاربران می‌توانند این فایل را به دلخواه پیکربندی کرده و آن‌را با نام xinitrc. یعنی به عنوان یک فایل مخفی در فهرست خانگی خود ذخیره کنند. در این قسمت به شرح جزییات فایل پیکربندی پیش‌فرض یعنی xinitrc می‌پردازیم. برای شروع به چند خط نخست از این فایل توجه کنید:

```
#!/bin/sh
        -2003 Red Hat, Inc.
userresources=$HOME/.Xresources
usermodmap=$HOME/.Xmodmap
userxkbmap=$HOME/.Xkbmap

sysresources=/etc/X11/Xresources
sysmodmap=/etc/X11/Xmodmap
sysxkbmap=/etc/X11/Xkbmap
```

تنظیمات فوق بیان کننده موقعیت سایر فایل‌های پیکربندی موردنیاز است. چنان‌که به زودی خواهید دید، در صورت عدم دسترسی به فایل‌های *user، برنامه xinitrc از فایل‌های *sys استفاده خواهد کرد.

```
# merge in defaults
if [ -f "$sysresources" ]; then
      xrdb -merge "$sysresources"
fi
```

```
if [ -f "$userresources" ]; then
      xrdb -merge "$userresources"
fi
```

دستورالعمل‌های فوق در صورت وجود منابع $sysresources و $userresources (یعنی دو فایل /etc/X11/Xresources و ~/.Xresources) آن‌ها را با یکدیگر تلفیق می‌کند.

```
# merge in keymaps
if [ -f "$sysxkbmap" ]; then
      setxkbmao `cat "$sysxkbmap"`
      XKB_INUSE=yes
fi

if [ -f "$userxkbmap" ]; then
      setxkbmao `cat "$userxkbmap"`
      XKB_INUSE=yes
fi
```

دستورالعمل‌های فوق در صورت وجود منابع $sysxkbmap و $userxkbmap (یعنی دو فایل /etc/X11/Xkbmap و ~/.Xkbmap)، آن‌ها را با یکدیگر تلفیق می‌کند. با این حال، عدم وجود این منابع در سیستم‌عامل Red Hat Linux موجب صرف نظر از آن‌ها می‌شود. ادامه فایل xinitrc حاوی خطوطی است که به برنامه X Server توسعه یافته توسط شرکت Sun Microsystems مربوط می‌شود و از این‌رو سیستم‌عامل Red Hat Linux، آن‌ها را نیز نادیده می‌گیرد.

```
# xkb and xmodmap don't play nice together
if [ -z "$XKB_IN_USE" ]; then
      if [ -f "$sysmodmap" ]; then
            xmodmap "$sysmodmap"
      fi

      if [ -f "$usermodmap" ]; then
            xmodmep "$usermodmap"
      fi
fi

unset XKB_IN_USE
```

دستورالعمل‌های فوق بررسی لازم را در مورد فایل Xmodmap از فهرست /etc/X11/xinit (یا نسخه پنهان آن که در فهرست خانگی کاربر موجود است) انجام داده و در صورت وجود ترتیبی می‌دهد تا این

فایل به جای فایل Xkbdmap مورد استفاده قرار بگیرد. اما به خاطر داشته باشید که فایل مورد بحث در سیستم‌عامل Red Hat Linux موجود نیست.

```
# run all system xinitrc shell scripts.
for i in /etc/X11/xinit/xinitrc.d/* ; do
      if [ -x "$I" ]; then
            . "$i"
      fi
done
```

دستورالعمل‌های فوق فایل‌های اسکریپت‌های موجود در فهرست /etc/X11/xinit/xinitrc.d از جمله xinput و xmbind را که به زودی شرح خواهیم داد، به اجرا درمی‌آید.

```
if [ -f $HOME/.Xclients ]; then
      [ -x /usr/bin/ssh-agent -a -z "$SSH_AGENT_PID" ] && \
            exec ssh-agent $HOME/.Xclients || \
            exec $HOME/.Xclients
elif [ -f /exec/X11/xinit/Xclients ]; then
      [ -x /usr/bin/ssh-agent -a -z "$SSH_AGENT_PID" ] && \
            exec ssh-agent /etc/X11/xinit/Xclients || \
            exec /etc/X11/xinit/Xclients
else
```

دستورالعمل‌های فوق بررسی لازم در مورد برنامه‌های کلاینت پیش‌فرض موجود در فایل Xclient را انجام می‌دهد. این خطوط ضمناً تنظیماتی را نیز در ارتباط با سرویس SSH انجام می‌دهد. (برای اطلاع بیشتر در این زمینه به فصل بیست و سوم مراجعه کنید).

```
      xclock -geometry 100x100-5+5 &
      xterm -geometry 80x50-50+150 &
      if [ -x /usr/bin/netscape
           -a -f /usr/share/doc/HTML/index.html ]; then
                 netscape /usr/share/doc/HTML/index.html &
      fi
      if [ -x /usr/X11R6/bin/fvwm2 ]; then
            exec fvwm2
      else
            exec twm
      fi
fi
```

دستورالعمل‌های فوق برنامه‌های کلاینت پیش‌فرض را در صورت عدم وجود فایل Xclients مشخص می‌کند. دقت کنید که این موضوع شامل برنامه Netscape نیز می‌شود. (برنامه مزبور به همراه نسخه‌های اخیر سیستم‌عامل Red Hat Linux منتشر نمی‌شود.) علاوه بر این، از برنامه xclock (یک نمایشگر ساعت با رابط گرافیکی) و xterm (یک رابط سطر فرمان در سیستم‌عامل Linux) نیز استفاده شده است.

در صورت تمایل می‌توانید فایلی با عنوان xinitrc. را نیز در فهرست خانگی خود ایجاد کنید. در صورت انجام این کار فراموش نکنید که باید با استفاده از فرمان chmod امکان اجرای این فایل را فراهم کنید. برای مثال، ممکن است مایل باشید که این خطوط را در فایل xinitrc. درج کنید:

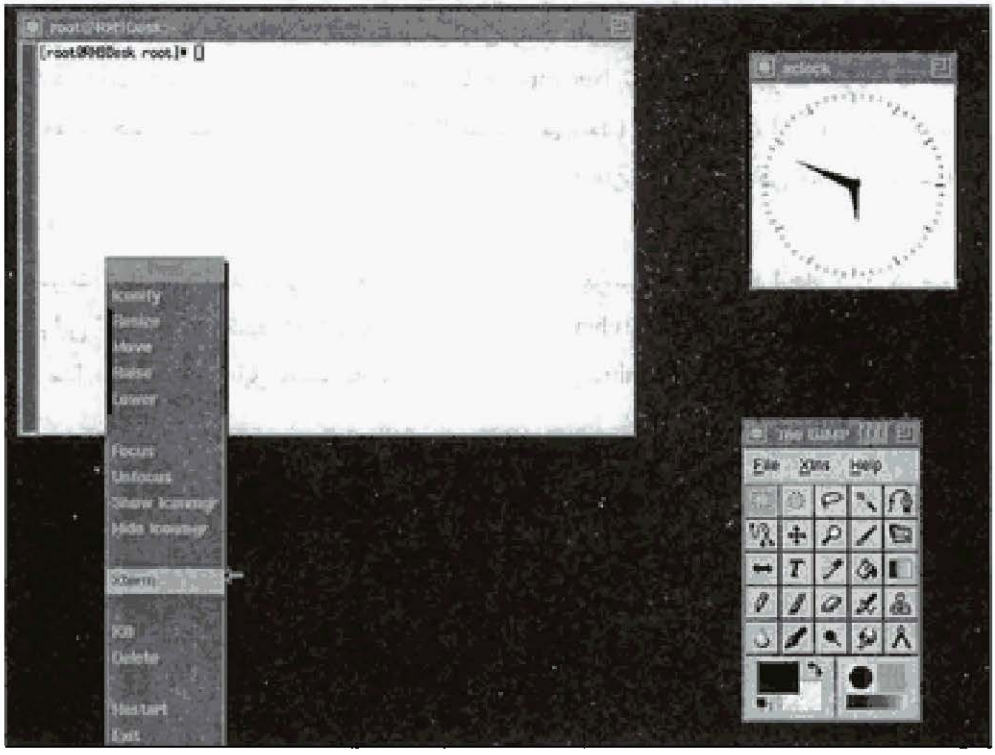
```
#!/bin/bash
xclock &
xterm &
gimp &
exec twm
```

دستورالعمل #!/bin/bash بیانگر آن است که دستورالعمل‌های بعدی، یعنی نمایش ساعت گرافیکی محیط X، نمایش ترمینال محیط X با عنوان xterm، اجرای برنامه GNU Image Manipulation Program یا به اختصار GIMP و فعال‌سازی محیط گرافیکی twm برای اجرا در پوسته bash تهیه شده‌اند. شکل ۱۹-۱۵ نتیجه حاصل از اجرای این دستورالعمل‌ها را نشان می‌دهد.

برنامه Xresources

در حالت عادی فایلی با عنوان Xresources. در فهرست خانگی هریک از کاربران و یک فایل پیش‌فرض با عنوان Xresources در فهرست etc/X11/ موجود است. اقدامات لازم به منظور تشخیص محیط گرافیکی موردنظر در قالب همین فایل پیش‌فرض گنجانده شده است. چنان‌چه به دلایلی هیچ یک از دو محیط گرافیکی GNOME یا KDE قابل راه‌اندازی نباشد، فایلی با عنوان wm_style. در فهرست خانگی کاربر مورد جستجو قرار می‌گیرد تا به این ترتیب دست کم یک محیط گرافیکی قدیمی‌تر راه‌اندازی شده و در اختیار وی قرار بگیرد.

رنگ‌های به کار رفته در برنامه‌هایی که از رابط گرافیکی برخوردارند، در قالب فایل Xresources. مشخص می‌شود. سایر جزییات خارج از حوزه این کتاب است.



شکل ۱۹-۱۵ نتیجه حاصل از اجرای یک فایل xinitrc، نمونه

فایل XF86Config

فایل XF86Config /etc/X11/ شامل مشخصات اصلی پیکربندی برنامه X Server است. به محض اجرای برنامه‌ای با رابط گرافیکی، تنظیمات مربوط به وضوح تصویر، درایورهای گرافیکی، صفحه نمایش، صفحه کلید، ماوس و سایر ابزارهای اشاره‌گر از طریق مشخصات مندرج در این فایل تعیین می‌شود. فایل مزبور از بخش‌های مختلفی تشکیل شده که در ادامه به بررسی آن‌ها می‌پردازیم.

فایل XF86Config ممکن است توسط یکی از دو برنامه Anaconda یا redhat-config-xfree86 تولید شده باشد. در صورت تولید این فایل توسط برنامه Anaconda نخستین خط آن به این صورت خواهد بود:

```
# Xfree86 4 configuration created by pyxf86config
```

اما در صورتی که فایل مزبور توسط برنامه redhat-config-xfree86 تولید شده باشد، محتوای نخستین خط آن چنین خواهد بود:

```
# Xfree86 4 configuration created by redhat-config-xfree86
```

پیش از عرضه نسخه Red Hat Linux 8.0 فایل پیکربندی پیش‌فرض برنامه X Server عبارت از /etc/X11/XF86Config-4 بود. پسوند *4-* در عنوان فایل نامبرده به این دلیل بود که نسخه‌های مزبور از سیستم‌عامل Red Hat Linux به همراه دو نسخه از برنامه XFree86 Server (یا به اختصار برنامه X Server) یکی با شاخص *3.a.b* و دیگری *4.x.y* عرضه می‌شدند. به دلیل آن‌که نسخه قدیمی‌تر برنامه XFree86 Server (یعنی نسخه *3.a.b*) به همراه نسخه‌های جدید سیستم‌عامل Red Hat Linux عرضه نمی‌شود، پسوند *4-* نیز از انتهای عنوان فایل مورد بحث حذف شده است. نسخه *4.x.y* از برنامه XFree86 Server شامل اطلاعات مربوط به کلیه کارت‌های گرافیکی جدید است.

جدول ۲-۱۵ اغلب خصوصیات مورد استفاده در فایل پیکربندی XF86Config را شرح می‌دهد. در قسمت‌های بعد به بررسی بخش‌های مختلف این فایل می‌پردازیم.

جدول ۲-۱۵ شرح خصوصیات مورد استفاده در فایل پیکربندی XFree86Config

عنوان خصوصیت	توضیح
BoardName	این خصوصیت عنوان تجهیزات سخت‌افزاری موردنظر مانند کارت گرافیکی را مشخص می‌کند.
BusID	چنان‌چه سیستم‌عامل Linux قادر به تشخیص کارت گرافیکی PCI یا AGP نصب شده روی کامپیوتر میزبان نباشد، این خصوصیت موقعیت آن‌را مشخص می‌کند.
DefaultDepth	این خصوصیت تعداد پیش‌فرض بیت‌هایی را مشخص می‌کند که برای تشخیص هر پیکسل مورد استفاده قرار می‌گیرند. این تعداد معمولاً برابر با ۱، ۴، ۸، ۱۶، ۲۴ یا ۳۲ است.
DisplaySize	این خصوصیت طول و عرض صفحه نمایش را بر حسب میلی‌متر مشخص می‌کند.
Driver	این خصوصیت درایور مربوط به تجهیزات سخت‌افزاری موردنظر را مشخص می‌کند.
EndSection	این خصوصیت بیانگر نقطه پایان گروهی از فرامین است.
EndSubSection	این خصوصیت بیانگر نقطه پایان گروهی از فرامین است که ابتدای آن توسط خصوصیت SubSection مشخص شده است.
FontPath	این خصوصیت بیانگر موقعیت فونت‌های قابل استفاده در رابط گرافیکی سیستم‌عامل Linux (اصطلاحاً X) است. خصوصیت مزبور معمولاً به یک فایل به خصوص یا یکی از پورت‌های TCP/IP ماشین Font Server محلی (اغلب unix/:7100) اشاره دارد.
HorizSync	این خصوصیت بیانگر محدوده مجاز نرخ جاروب افقی مانیتور است.

عنوان خصوصیت	توضیح
Identifier	این خصوصیت تعامل میان گروه‌های مختلفی از فرامین را امکان‌پذیر می‌سازد.
InputDevice	این خصوصیت به صفحه کلید یا ابزارهای اشاره‌گری هم‌چون ماوس یا touchpad اشاره دارد.
Load	این خصوصیت امکان بارگذاری ماجول‌های موردنظر را در اختیار قرار می‌دهد.
ModelName	این خصوصیت بیانگر عنوان یک مدل به‌خصوص بوده و به همراه خصوصیت VendorName به کار می‌رود.
Modes	این خصوصیت بیانگر محدوده‌های مجازی است که می‌توان وضوح مانیتور را بر اساس آن تنظیم کرد.
Module	این خصوصیت بیانگر اسامی ماجول‌های مورد استفاده جهت پشتیبانی از فونت‌هایی است که توسط برنامه X Server بارگذاری شده‌اند.
Monitor	این خصوصیت بیانگر شناسه مانیتوری است که اطلاعات یک صفحه نمایش به خصوص (که توسط خصوصیت Screen مشخص شده است) روی آن ارسال می‌شود.
Option	این‌خصوصیت بیانگر یکی از چند گزینه موجود در مورد تجهیزات سخت‌افزاری مختلف است.
RgbPath	این خصوصیت بیانگر یک بانک اطلاعاتی (در قالب متنی) است که شدت سه رنگ قرمز، سبز و آبی را برای رنگ‌های مختلف مشخص می‌کند.
Section	این خصوصیت بیانگر نقطه آغاز گروهی از فرامین است. هر گروه از فرامین باید توسط یک برچسب علامت‌گذاری شده و انتهای آن با استفاده از خصوصیت EndSection مشخص شود.
SubSection	این خصوصیت بیانگر نقطه آغاز یک گروه فرعی از فرامین است که در قالب یک گروه اصلی (که توسط خصوصیت Section مشخص شده است) تعریف می‌شود.
VendorName	این خصوصیت بیانگر عنوان شرکت سازنده تجهیزات سخت‌افزاری موردنظر است.
VertRefresh	این خصوصیت بیانگر نرخ نوسازی عمودی مجاز مانیتور است.
VideoRam	این خصوصیت بیانگر میزان حافظه کارت گرافیکی موجود (اصطلاحاً Video RAM) است.

بخش ServerLayout

این بخش از فایل پیکربندی XF86Config شامل مجموعه‌ای از خصوصیات InputDevice و خصوصیت Screen بوده و به این ترتیب ترکیبی از پیکربندی مانیتور و کارت گرافیکی است. به محتوای نمونه‌ای از این بخش توجه کنید:

```
Section "ServerLayout"
      Identifier  "Default Layout"
      Screen  0   "Screen0" 0 0
      IputDevice  "Mouse0" "CorePointer"
      InputDevice "Keyboard0" "CoreKeyboard"
      InputDevice "DevInputMice" "AlwaysCore"
EndSection
```

چنان‌که در نمونه فوق مشاهده می‌کنید، تنظیمات مربوط به تجهیزات سخت‌افزاری مختلفی شامل Screen0، Mouse0، DevInputMice و Keyboard که توسط برنامه نصب سیستم‌عامل Red Hat Linux (موسوم به Anaconda) انجام شده، با یکدیگر ترکیب شده است.

بخش Files

این بخش از فایل پیکربندی XF86Config، حاوی اطلاعات موردنیاز برنامه X Server درباره رنگ‌ها و فونت‌های مورد استفاده است. به محتوای نمونه‌ای از این بخش توجه کنید:

```
Section "Files"
      RgbPath     "/usr/X11R6/lib/X11/rgb"
      FontPath    "unix/:7100"
EndSection
```

چنان‌که در نمونه فوق مشاهده می‌کنید، موقعیت فایل حاوی مشخصات موردنیاز جهت رنگ‌آمیزی به سبک Red Green Blue (به اختصار RGB) و هم‌چنین مشخصات پورت TCP/IP موردنیاز برای دستیابی به X Font Server (به اختصار xfs) توسط خصوصیات RgbPath و FontPath مشخص شده است. (اصطلاح RGB به یک تکنیک استاندارد برای ترکیب طیف‌های مختلف سه رنگ قرمز، سبز و آبی جهت دستیابی به سایر رنگ‌ها اشاره دارد.)

تکنیک RGB تنها روش استاندارد موجود برای دستیابی به رنگ‌های متنوع نیست، به طوری که بسیاری از هنرمندان و گرافیست‌ها از تکنیک‌های دیگری هم‌چون Cyan Magnet Yellow Black یا به اختصار CMYK برای این منظور استفاده می‌کنند. در برخی از برنامه‌های کاربردی سیستم‌عامل

Linux از جمله Houdini و Maya از تکنیک استاندارد CMYK پشتیبانی به عمل آمده است. (جهت اطلاع بیشتر درباره این برنامه‌ها به دو آدرس اینترنتی http://www.sidefx.com و http://www.aliaswavefront.com مراجعه کنید.) تکنیک CMYK تاکنون انتظارات بسیاری از استودیوهای فیلم‌سازی از جمله DreamWorks و Disney را برآورده کرده است.

بخش Module

بخش Module از فایل پیکربندی XF86Config وظیفه بارگذاری کلیه ماجول‌های موردنیاز برای پشتیبانی از فونت‌های مورد استفاده و سایر ماجول‌های موردنیاز سرور را به عهده دارد. به محتوای نمونه‌ای از این بخش توجه کنید:

```
Section "Module"
      Load "dbe"
      Load "extmod"
      Load "fbdevhw"
      Load "dri"
      Load "glx"
      Load "record"
      Load "freetype"
      Load "type1"
EndSection
```

چنان‌که در نمونه فوق مشاهده می‌کنید، فونت‌های مختلفی از جمله Freetype (یکی از فونت‌های موجود در مجموعه True Type) و Type بارگذاری شده‌اند. برای اطلاع از سایر ماجول‌ها به فهرست /usr/X11R6/lib/modules مراجعه کنید.

بخش InputDevice

بخش InputDevice از فایل پیکربندی XF86Config، شامل مشخصات تجهیزات سخت‌افزاری مورد استفاده کاربر جهت ارسال اطلاعات به کامپیوتر است. (به‌چنین‌تجهیزاتی در اصطلاح Human Interface Device یا به اختصار HID گفته می‌شود.) با وجودی که تجهیزات مزبور در اصل شامل صفحه کلید و ماوس است، می‌تواند موارد دیگری از جمله trackball، touchpad و مانند آن‌ها را نیز شامل شود. هر بخش InputDevice تنها شامل مشخصات یک نوع از تجهیزات سخت‌افزاری مورد بحث است. به محتوای نمونه‌ای از این بخش توجه کنید:

```
Section "InputDevice"
      Identifier  "keyboard0"
      Driver      "keyboard"
      Option      "XkbRules" "xfree86"
      Option      "XkbModel" "pc105"
      Option      "XkbLayout" "us"
EndSection
```

چنان‌که مشاهده می‌کنید، بخش فوق شامل مشخصات صفحه کلیدی با شناسه keyboard0 و درایوری با همین عنوان است. هم‌چنین نقش کلیدها بیانگر الگویی است که با برنامه XFree86 Server مطابقت دارد و بالاخره مدل موردنظر بیانگر صفحه کلید استاندارد ۱۰۵ کلیدی متداول در ایالات متحده است. به نمونه دیگری از یک بخش InputDevice توجه کنید:

```
Section "InputDevice"
      Identifier  "Mouse0"
      Driver      "mouse"
      Option      "Protocol" "IMPS/2"
      Option      "Device" "/dev/psaux"
      Option      "ZaxisMapping" "4 5"
      Option      "Emulate3Buttons" "no"
EndSection
```

به گونه‌ای که ملاحظه می‌کنید، بخش فوق شامل مشخصات ماوسی از نوع PS/2 است. درایور این ماوس در قالب فایل /dev/psaux که اغلب به فایل/dev/mouse متصل است، قابل دستیابی است. گزینه ZAxisMapping بیانگر حرکت یکی از محورهای ماوس در جهت بالا و پایین بوده و در این مورد به دکمه‌های چهارم و پنجم از یک ماوس استاندارد اشاره دارد. لازم به ذکر است که این دکمه‌ها در تمام ماوس‌ها تعبیه نشده‌اند. دکمه چهارم در ماوس‌های سه دکمه‌ای به منظور اسکرول صفحات تعبیه شده است. دکمه پنجم نیز اغلب در یکی از دو سمت کناری ماوس تعبیه می‌شود. چنان‌چه بیش از یک ماوس یا ابزار اشاره‌گر به کامپیوتر میزبان متصل باشد، مشخصات هریک از آن‌ها را می‌توان در قالب یک بخش InputDevice جداگانه تعریف کرد.

بخش Monitor

بخش Monitor از فایل پیکربندی XF86Config حاوی تنظیمات مربوط به مانیتور است. به محتوای نمونه‌ای از این بخش توجه کنید:

```
Section "Monitor"
      Identifier  "Monitor0"
```

```
    VendorName  "Monitor Vendor"
    ModelName   "S/M 955DF"
    DisplaySize 360    270
    HorizSync   30.0 - 85.0
    VertRefresh 50.0 - 160.0
    Option      "dpms"
EndSection
```

چنان‌که در نمونه فوق مشاهده می‌کنید، این مشخصات بیانگر مدل مانیتور، اندازه صفحه نمایش برحسب میلی‌متر، نرخ جاروب افقی و نرخ نوسازی عمودی مانیتور است. گزینه dpms بیانگر تنظیمات مربوط به صرفه‌جویی توان مصرفی مانیتور است. در صورت استفاده بیش از یک مانیتور می‌توان مشخصات آن‌ها را به طور جداگانه در قالب چند بخش Monitor تعریف کرد. چنان‌که به زودی خواهید دید، در بخش Screen از فایل پیکربندی XF86Config شناسه مانیتور و کارت گرافیکی به طور مشخص درج می‌شود.

بخش Device

کارت گرافیکی اصلی‌ترین تجهیزات سخت‌افزاری موردنیاز برای پشتیبانی از هر رابط گرافیکی محسوب می‌شود. به محتوای نمونه‌ای از بخش Device که بیانگر مشخصات یک کارت گرافیکی، شامل درایور مربوطه و میزان حافظه تعبیه شده در آن است، توجه کنید:

```
Section "Device"
    Identifier  "Videocard0"
    Driver      "i810"
    VendorName  "Videocard vendor"
    BoardName   "Intel 810"
    VideoRam    16384
EndSection
```

در صورت وجود بیش از یک کارت گرافیکی می‌توان مشخصات آن‌ها را به طور جداگانه در قالب چند بخش Device تعریف کرد.

بخش Screen

بخش Screen از فایل پیکربندی XF86Config شامل مجموعه‌ای مرکب از تنظیمات کارت گرافیکی و مانیتور است. بدیهی است عناوین Device و Monitor برگرفته از دو بخش هم‌نام در فایل پیکربندی XF86Config هستند. به محتوای نمونه‌ای از این بخش توجه کنید:

```
Section "Screen"
      Identifier "Screen0"
      Device      "Videocard0"
      Monitor     "Monitor0"
      DefaultDepth      24
      SubSection  "Display"
            Depth 16
            Modes "1024x768" "800x600" "640x480"
      EndSubsection
      Subsection  "Display"
            Depth 24
            Modes "800x600" "640x480"
      EndSubsection
EndSection
```

دو خصوصیت Depth و Modes که به ترتیب بیانگر تعداد نقاط در یک اینچ مربع و وضوح تصویر هستند به واسطه ترکیب تنظیمات کارت گرافیکی و مانیتور مشخص می‌شود. چنان‌که مشاهده می‌کنید، در نمونه اخیر دو بخش فرعی با عناوین "SubSection "Display تعریف شده است. با وجود تفاوت مقادیر خصوصیت Depth در این دو بخش فرعی، برخی مقادیر خصوصیت Modes مشابه یکدیگر هستند.

بخش DRI

تنظیمات بخش DRI یا Direct Rendering Interface از فایل پیکربندی XF86Config تنها در مورد آن دسته از کارت‌های گرافیکی سودمند است که قادر هستند تا پردازش سه بعدی را با سرعت بسیار بالا انجام دهند. (این گونه کارت‌های گرافیکی از یک تراشه شتاب‌دهنده جهت پردازش سه بعدی استفاده می‌کنند.) چنین کارت‌هایی مناسب کاربردهایی چون بازی‌های کامپیوتری، فیلم‌سازی و مدل‌سازی کامپیوتری هستند. به محتوای نمونه‌ای از این بخش توجه کنید:

```
Section "DRI"
      Mode  0666
EndSection
```

مقدار خصوصیت Mode در نمونه فوق، یعنی عدد 0666 بیانگر آن است که تمام کاربران از مجوز خواندن و نوشتن فایل‌های مربوط به استفاده از قابلیت پردازش سه بعدی با سرعت بالا برخوردارند. با تعریف گروهی از کاربران در فهرست /etc/group می‌توان استفاده این قابلیت را به اعضای آن گروه

محدود کرد. برای مثال، چنان‌چه گروهی از کاربران تحت عنوان gallery در فهرست etc/group/ تعریف شده باشند، به این صورت می‌توان قابلیت مورد بحث را به اعضای آن گروه محدود کرد:

```
Section "DRI"
      Group "gallery"
      Mode  0666
EndSection
```

اشکال‌زدایی زیرسیستم X Window

هنگام بروز اشکال در عملکرد زیرسیستم X Window موارد بسیاری را می‌توان مورد بازبینی قرار داد. در این فصل بیشتر به بررسی ابزارهای پیکربندی زیرسیستم مزبور پرداختیم. استفاده از این ابزارها را همواره می‌توانید در رأس اقداماتی قرار دهید که برای اشکال‌زدایی زیرسیستم X Window انجام می‌دهید.

مشابه سایر برنامه‌های سرور، بسیاری از اشکالات را می‌توان با مراجعه به فایل‌های ثبت وقایع موجود در فهرست var/log/ تشخیص داد. یکی از مشکلات متداول درراه‌اندازی زیرسیستم X Window، به فونت‌ها مربوط می‌شود، به این ترتیب که اگر برنامه سرور مربوطه یعنیX Font Server به درستی راه‌اندازی نشده باشد، زیرسیستم X Window نیز راه‌اندازی نخواهد شد.

بررسی فایل‌های ثبت وقایع

در ارتباط با زیرسیستم X Window دو فایل ثبت وقایع موجود است. هر دو فایل مزبور در فهرست var/log/ مستقر هستند. فایل نخست با عنوان var/log/XFree86.0.log/ حاوی کلیه وقایعی است که هنگام اجرای برنامه startx و نیز فرامینی که با فایل‌های پیکربندی به ویژه XF86Config در تعامل هستند، رخ می‌دهند. فایل دیگر با عنوان var/log/messages/ حاوی راهنمایی‌های مفیدی برای رفع اشکالات مربوط به برنامه X Font Server است.

حتی در صورتی که کوچک‌ترین اشکالی در راه‌اندازی زیرسیستم X Window وجود نداشته باشد، مطالعه محتوای این فایل‌ها می‌تواند مفید واقع شود. خطاهای به ثبت رسیده در این فایل‌ها ممکن است همواره شما را به تعجب وادارد. با این حال، به واسطه درس‌هایی که از مطالعه محتوای این فایل‌ها فرامی‌گیرید، می‌توانید سرعت عملیاتی زیرسیستم X Window را افزایش داده و به طور مؤثرتری از آن بهره‌برداری کنید.

فایل ثبت وقایع XFree86.0.log

شکل ۲۰-۱۵ بخشی از محتوای یک نمونه فایل ثبت وقایع XFree86.0.log را نشان می‌دهد. با کمی دقت می‌توانید خصوصیاتی را که در قسمت‌های قبل هنگام مطالعه بخش‌های مختلف فایل پیکربندی XF86Config با آن‌ها برخورد کردید، تشخیص دهید.

```
Markers: (--) probed, (**) from config file, (==) default setting,
        (++) from command line, (!!) notice, (II) informational,
        (WW) warning, (EE) error, (NI) not implemented, (??) unknown.
(==) Log file: "/var/log/XFree86.0.log", Time: Sun Dec 22 09:47:01 2002
(==) Using config file: "/etc/X11/XF86Config"
(==) ServerLayout "Default Layout"
(**) |-->Screen "Screen0" (0)
(**) |   |-->Monitor "Monitor0"
(**) |   |-->Device "Videocard0"
(**) |-->Input Device "Mouse0"
(**) |-->Input Device "Keyboard0"
(**) Option "XkbRules" "xfree86"
(**) XKB: rules: "xfree86"
(**) Option "XkbModel" "pc105"
(**) XKB: model: "pc105"
(**) Option "XkbLayout" "us"
(**) XKB: layout: "us"
(==) Keyboard: CustomKeycode disabled
(**) |-->Input Device "DevInputMice"
(**) FontPath set to "unix/:7100"
(**) RgbPath set to "/usr/X11R6/lib/X11/rgb"
(==) ModulePath set to "/usr/X11R6/lib/modules"
(--) using VT number 7
"XFree86.0.log" 625L, 32662C                                  31,10         2%
```

شکل ۲۰-۱۵ بخشی از محتوای فایل ثبت وقایع XFree86.0.log

به خطوطی از این فایل که ابتدای آن‌ها با علامت ** مشخص شده است، توجه کنید. این خطوط تنظیمات‌خصوصیاتی را نشان می‌دهدکه پیش از این دربخش‌های‌مختلف فایل پیکربندی XF86Config در مورد آن‌ها صحبت کردیم. چنان‌چه اشکالی در این تنظیمات وجود داشته باشد، می‌توانید مقدار خصوصیات مربوطه را در فایل نامبرده تغییر دهید. هم‌چنین ابتدای برخی از خطوط در فایل ثبت وقایع XFree86.0.log ممکن است با علامت II، WW یا EE مشخص شده باشد. این سه علامت به ترتیب بیانگر پیغام ساده، هشدار و پیغام خطا هستند. به نمونه‌ای از یک پیغام ساده توجه کنید:

```
(II) I810(0): Not using default mode "320X175" (bad mode
clock/interlace/doublescan)
```

مهارت در اشکال‌زدایی

فرآیند اشکال‌زدایی در مواقعی ممکن است دشوار باشد. یکی از رویکردهای موجود در اشکال‌زدایی این است که تا زمان وقوع اشکال صبر کرده و سپس برای رفع آن دست به کار شوید. رویکرد دیگر این است که دست به تجربه بزنید. از آن‌جا که عملکرد زیرسیستم X Window بستگی زیادی به تنظیمات فایل پیکربندی XF86Config دارد، با تغییراتی که در مقادیر خصوصیات مندرج در این فایل می‌دهید، می‌توانید تأثیر آن‌را در عملکرد زیرسیستم مزبور مشاهده کنید. اگر با حالت Linux rescue که در فصل یازدهم به بررسی آن پرداختیم آشنایی داشته و به نظم در امور پایبند هستید، این رویکرد را به طرز مؤثری مفید خواهید یافت.

اما پیش از آن‌که به تجربه با فایل پیکربندی XF86Config بپردازید، از آن یک نسخه پشتیبان تهیه کنید. علاوه بر این مقدار متغیر id در فایل /etc/inittab را به سومین سطح اجرایی تغییر دهید. به این ترتیب هنگام بروز اشکال در عملکرد زیرسیستم X Window می‌توانید سیستم‌عامل Linux را مجدداً راه‌اندازی کرده و رابط سطر فرمان آن‌را در اختیار بگیرید.

پس از انجام این اقدامات، با درج علامت # در ابتدای خطوط موردنظر از فایل پیکربندی XF86Config موقتاً آن‌ها را بی‌تأثیر کرده و برنامه startx را اجرا کنید. به تجربه درمی‌یابید که برخی از این تغییرات تأثیر چندانی بر عملکرد زیرسیستم X Window ندارد. با وجود این، گاهی نیز تغییرات چنان است که زیرسیستم مزبور از عملکرد خود بازمی‌ماند. در هر صورت، همواره به ارتباط میان پیغام‌های خطا (با شاخص EE) و تغییراتی که در فایل پیکربندی XF86Config می‌دهید توجه خاص داشته باشید.

پس از اتمام کار، فراموش نکنید که فایل پیکربندی را مجدداً از روی نسخه پشتیبانی که قبلاً آن‌را تهیه کرده‌اید، بارگذاری کنید.

فایل ثبت وقایع /var/log/messages

زیرسیستم X Window بدون اجرای موفقیت‌آمیز برنامه X Font Server راه‌اندازی نمی‌شود. مشابه سایر برنامه‌های سرور، این برنامه نیز از طریق فهرست /etc/rc.d/init.d قابل کنترل است.

فایل اصلی پیکربندی فونت‌ها در سیستم‌عامل Linux عبارت از /etc/font/font.conf است.

محتوای فایل ثبت وقایع /var/log/messages طولانی است. به طور پیش‌فرض، در این فایل پیغام‌های مربوط به راه‌اندازی و توقف سیستم‌عامل Linux برای حداکثر یک هفته اخیر نگهداری می‌شود. به این ترتیب، چنان‌چه به تازگی اشکالی در این موارد پیش آمده باشد، باید به پیغام‌هایی که در انتهای این

فایل ثبت شده‌اند، توجه کنید. نخستین پیغامی که ضمن فرآیند راه‌اندازی سیستم‌عامل Linux در فایل مزبور به ثبت می‌رسد، باید شبیه به این باشد:

```
Dec 22 10:25:09 RH9Server kernel: linux version 2.4.20-3
```

و به دنبال آن پیغامی نظیر این در مورد راه‌اندازی برنامه X Font Server به ثبت می‌رسد:

```
Dec 22 10:25:09 RH9Server xfs: xfs startup succeeded
```

بدیهی است در صورت عدم مشاهده پیغام فوق، ممکن است اشکالی در ارتباط با فونت وجود داشته باشد. تحت چنین شرایطی لازم است این اقدامات را انجام دهید:

- وضعیت سرویس xfs را مورد بازبینی قرار دهید. در صورت متوقف بودن این سرویس با اجرای فرمان service xfs start برای راه‌اندازی آن اقدام کنید. هم‌چنین با استفاده از فرمان chkconfig که پیش از این در فصل سیزدهم به بررسی آن پرداختیم، مطمئن شوید که سرویس xfs هنگام راه‌اندازی سیستم به طور خودکار راه‌اندازی می‌شود.
- مطمئن شوید که مقدار متغیر FontPath از فایل پیکربندی XF86Config به موقعیت واقعی فونت‌ها یا به پورت TCP/IP شماره ۷۱۰۰ اشاره دارد.
- مطمئن شوید که فایل‌هایی که موقعیت آن‌ها توسط مقدار متغیر FontPath از فایل پیکربندی XF86Config مشخص شده است، وجود دارند. در غیر این صورت باید برای نصب آن‌ها از طریق بسته‌های نرم‌افزاری RPM اقدام کنید. بسته‌های نرم‌افزاری‌مربوطه به صورت XFree86-*-fonts-* نام‌گذاری شده‌اند.
- قوانین مکانیزم بازدارنده دیوار آتش را مورد بازبینی قرار دهید. چنان‌چه امکان دسترسی محلی به پورت TCP/IP شماره ۷۱۰۰ محدود شده باشد، برنامه X Font Server نمی‌تواند اطلاعات لازم درباره فونت‌ها را در اختیار زیرسیستم X Window قرار دهد.

شکل کوتاه شده عنوان برنامه X Font Server یعنی xfs با عنوان سیستم فایل ابداعی شرکت Silicon Graphics یعنی xfs یکی است.

جمع‌بندی

در این فصل اصول پیکربندی زیرسیستم گرافیکی X Window یا به اختصار X را فراگرفتید. با وجودی که اغلب کاربران حرفه‌ای سیستم‌عامل Linux تمایل و نیازی به استفاده از رابط گرافیکی ندارند، این زیرسیستم هم‌چنان به عنوان ابزار مهمی برای استفاده بسیاری از کاربران مطرح است. زیرسیستم X

Window برای کاربران سیستم‌هایی چون Microsoft Windows که به استفاده از رابط‌های گرافیکی خو گرفته‌اند جاذبه‌های بسیاری دارد.

پیکربندی زیرسیستم X Window ضمن نصب سیستم‌عامل Linux نیز امکان‌پذیر است. چنان‌چه تاکنون این کار را انجام نداده‌اید یا اکنون مایل هستید تا در پیکربندی این زیرسیستم تغییراتی بدهید، می‌توانید یکی از دو ابزار xf86config یا redhat-config-xfree86 را که به همین منظور پیش‌بینی شده‌اند، مورد بهره‌برداری قرار دهید. در حالی که ابزار redhat-config-xfree86 تنها در سیستم‌عامل Red Hat Linux قابل دستیابی است، ابزار xf86config به همراه تمام نسخه‌های سیستم‌عامل Linux توزیع می‌شود. هم‌چنان امکان دستیابی به آن از طریق وب سایت http://www.xfree86.org نیز وجود دارد.

زیرسیستم گرافیکی X Window دارای فایل‌های پیکربندی متعددی است، که توسط برنامه startx مورد استفاده قرار می‌گیرند. با وجود این، در صورت تمایل می‌توانید تنظیمات موردنظر خود در مورد این زیرسیستم را در قالب یک فایل پیکربندی در فهرست خانگی خود ذخیره کنید. در غیر این صورت، برنامه startx تنظیمات عمومی مندرج در فایل‌های پیکربندی مستقر در فهرست /etc/X11 را مورد توجه قرار خواهد داد.

کلیدی‌ترین فایل پیکربندی زیرسیستم X Window فایلی با عنوان /etc/X11/XF86Config است. اطلاع از تنظیمات مندرج در این فایل بسیار مفید بوده و در فرآیند اشکال‌زدایی عملکرد زیرسیستم مزبور بسیار مؤثر است. بهره‌برداری از زیرسیستم X Window بدون اجرای موفقیت‌آمیز برنامه X Font Server یا به اختصار xfs غیرممکن است. با وجود این، بسیاری از سایر مشکلات مربوط به این زیرسیستم در فایل /var/log/XFree86.0.log به ثبت می‌رسد.

در فصل آینده به بررسی محیط گرافیکی پیش‌فرض سیستم‌عامل Red Hat Linux با عنوان GENOME می‌پردازیم. چنان‌که خواهید دید، این محیط گرافیکی کلیه امکانات محیط گرافیکی سیستم‌عامل Microsoft Windows را در اختیار کاربران قرار می‌دهد. حتی در صورتی که از زیرسیستم X Window استفاده نمی‌کنید، باید از مزایای محیط گرافیکی GENOME به منظور راهنمایی کاربران خود آگاه باشید.

فصل شانزدهم

محیط گرافیکی GNOME

با وجودی که ممکن است مدیران سیستم‌های Linux در انجام امور روزمره خود به استفاده از محیط گرافیکی (اصطلاحاً Graphical User Interface یا به اختصار GUI) نیاز نداشته باشند، تقریباً برای تمام کاربرانی که تا به حال از سیستم‌عامل Microsoft Windows استفاده می‌کردند، دسترسی به چنین محیطی یک ضرورت محسوب می‌شود. یکی از اهداف جامعه کاربران نرم‌افزارهای GNU همواره این بوده که سیستم‌عامل Linux در حوزه کاربردهای عامیانه (کاربردهایی که عموم کاربران به آن علاقه‌مند هستند) با سیستم‌عامل‌های مشابه قابل‌رقابت باشد. از این‌رو، سیستم‌عامل Linux به یک رابط گرافیکی نیاز داشت که کاربران سایر سیستم‌ها، به ویژه کاربران سیستم‌عامل Microsoft Windows با آن احساس راحتی کنند.

برای دستیابی به این هدف مهم، شرکت Red Hat نرم‌افزاری با عنوان GNU Network Object Model Environment یا به اختصار GNOME را به همراه سیستم‌عامل خود منتشر می‌کند. این نرم‌افزار علاوه بر یک محیط گرافیکی کارآمد شامل برنامه‌های کاربردی متعددی است، که تنها یکی از آن‌ها قابلیت‌هایی مشابه نرم‌افزار اداری چند صد دلاری Microsoft Office را به رایگان در اختیار کاربران قرار می‌دهد. گذشته از این، استفاده از سیستم‌عامل Linux نیز هزینه‌ای ندارد. چنان‌که در فصل اول اشاره شد، این موضوع باعث شده تا بسیاری از شرکت‌ها و سازمان‌های دولتی سیستم‌عامل Microsoft Windows را با Linux جایگزین کنند.

نرم‌افزار GNOME شامل یک رابط گرافیکی رومیزی (اصطلاحاً GUI desktop)، مجموعه‌ای از برنامه‌های سیستمی و چندین برنامه کاربردی مهم است. برخی از این برنامه‌ها را می‌توان جایگزین برنامه‌های کاربردی تحت ویندوز دانست که برای استفاده از آن‌ها باید بهایی معادل چند صد دلار پرداخت کرد. در این فصل محیط گرافیکی GNOME، برنامه Control Center و برخی از برنامه‌های کاربردی توزیع شده به همراه سیستم‌عامل Red Hat Linux را مورد بررسی قرار می‌دهیم.

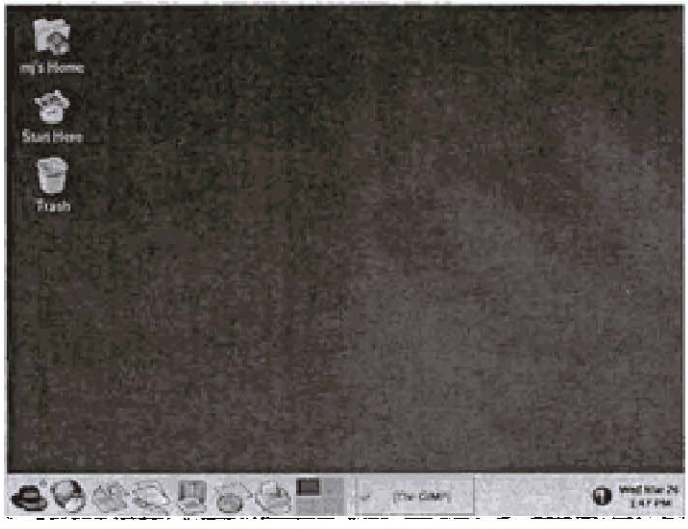
با وجود این، فصل حاضر فاقد معرفی جامع نرم‌افزار GNOME است، به طوری که بررسی برنامه‌های کاربردی متداولی از این نرم‌افزار، هم‌چون OpenOffice تا فصل هجدهم به تعویق افتاده است. ضمناً بررسی مجموعه ابزارهای *-redhat-config نیز به فصل نوزدهم موکول شده است.

قابلیت‌های نرم‌افزار GNOME تحت سیستم‌عامل Red Hat Linux به نحوی است که می‌توان برخی از ابزارها و برنامه‌های کاربردی نرم‌افزار KDE را (که در فصل هفدهم مورد بررسی قرار خواهد گرفت) به اجرا درآورد. برخی از ابزارها را مستقیماً می‌توان از طریق منوی Main Menu مورد دستیابی قرار داد. موضوعات مورد بررسی در فصل حاضر به این قرار است:

- محیط گرافیکی GNOME
- ابزارها و برنامه‌های کاربردی توزیع شده برای استفاده در محیط گرافیکی GNOME

رابط محیط گرافیکی GNOME

محیط‌گرافیکی GNOME دارای کلیه‌مشخصات استانداردمحیط‌های‌گرافیکی است که سیستم‌عامل‌های امروزی از آن برخوردارند. این محیط گرافیکی متشکل از یک پانل، یک منوی اصلی با عنوان Main Menu و مجموعه‌ای از آیکن‌هاست. در صورت تمایل می‌توان تنظیمات مربوط به هریک از اجزای تشکیل دهنده محیط گرافیکی GNOME را به دلخواه تغییر داده و حتی یک رابط استاندارد برای کامپیوترهایی که محیط گرافیکی مزبور روی آن‌ها مورد استفاده قرار می‌گیرد، پیکربندی کرد. امکانات موجود در مرکز کنترل محیط گرافیکی GNOME (اصطلاحاً GNOME Control Center) امکانات لازم برای تغییر در ظاهر و شیوه ارتباط با آن‌را در اختیار قرار می‌دهد. پس از راه‌اندازی محیط گرافیکی سیستم‌عامل Red Hat Linux برای نخستین مرتبه، احتمالاً با فضایی کم‌وبیش مشابه شکل ۱-۱۶ مواجه می‌شوید.



شکل ۱-۱۶ دسک‌تاپ محیط گرافیکی GNOME

پانل سیستم‌عامل Red Hat Linux جایی است که نوار وظایف یا اصطلاحاً taskbar سیستم‌عامل Microsoft Windows در آن‌جا واقع شده است. هم‌چنین دکمه Main Menu (که با آیکنی شبیه به یک کلاه قرمز مشخص شده) جایی است که دکمه Start در سیستم‌عامل Microsoft Windows قرار دارد.

مروری بر محیط گرافیکی GNOME

دسک‌تاپ محیط گرافیکی GNOME بسیار ساده است و چنان‌که در شکل ۱-۱۶ نیز مشاهده می‌کنید، شامل آیکنی برای مشاهده محتوای فهرست خانگی، آیکنی با عنوان Start Here برای دستیابی به ابزارها و برنامه‌های کاربردی و آیکنی با عنوان Trash است. با کلیک روی هر یک از این آیکن‌ها برنامه‌ای با عنوان Nautilus به اجرا درمی‌آید. برنامه مزبور دارای یک رابط گرافیکی است که به منظور مدیریت فایل‌ها، پیکربندی محیط گرافیکی GNOME و هر برنامه دیگری که از یک رابط گرافیکی برخوردار است، پیش‌بینی شده است. برنامه Nautilus را در قسمت‌های بعدی همین فصل مورد بررسی قرارخواهیم داد. در این قسمت به بررسی کاربرد دکمه‌های موجود روی پانل محیط گرافیکی GNOME و مرکز کنترل آن (اصطلاحاً GNOME Control Center) می‌پردازیم.

پانل محیط گرافیکی GNOME

به کمک امکانات موجود روی پانل محیط گرافیکی GNOME، می‌توانید برنامه‌های کاربردی را به اجرا درآورید. به کمک همین امکانات می‌توانید مابین برنامه‌های کاربردی مختلف و حتی بین چند محیط کاری (اصطلاحاً workspace) سوییچ کنید. شکل ۲-۱۶ نمونه‌ای از یک پانل را نشان می‌دهد. چنان‌که مشاهده می‌کنید، بخش سمت چپ این پانل نمونه دارای هفت آیکن است. شرح این آیکن‌ها در جدول ۱-۱۶ آمده است.

محیط کاری شبیه به یک دسک‌تاپ استاندارد بوده و اغلب شامل تعدادی آیکن و چندین برنامه باز است. به طور پیش فرض، محیط گرافیکی GNOME دارای چهار محیط کاری است.

شکل ۲-۱۶ نمونه‌ای از پانل محیط گرافیکی GNOME

جدول ۱-۱۶ شرح آیکن‌های موجود روی پانل محیط گرافیکی GNOME

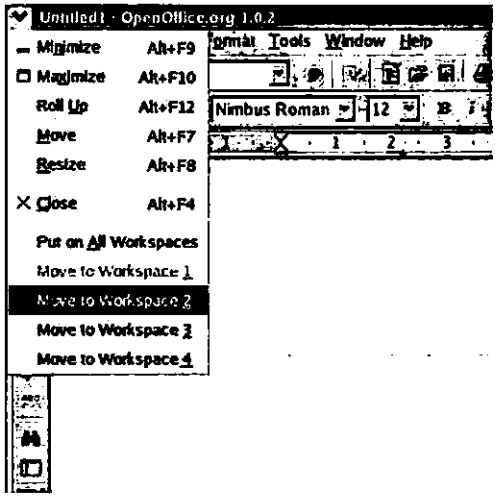
آیکن	توضیح
	با کلیک روی این آیکن منوی اصلی محیط گرافیکی GNOME باز شده و امکان دسترسی به برنامه‌ها و ابزارهای مختلف در اختیار قرار می‌گیرد. عملکرد این آیکن شبیه به دکمه Start در سیستم‌عامل Microsoft Windows است.
	با کلیک روی این آیکن پنجره اصلی مرورگر وب Mozilla باز می‌شود.
	با کلیک روی این آیکن پنجره اصلی برنامه مدیریت اطلاعات شخصی Evolution باز می‌شود.
	با کلیک روی این آیکن پنجره اصلی برنامه واژه‌پرداز OpenOffice Writer باز می‌شود کاربرد این برنامه مشابه برنامه Microsoft Word است.
	با کلیک روی این آیکن پنجره اصلی برنامه مدیریت نمایش OpenOffice Impress باز می‌شود. کاربرد این برنامه مشابه برنامه Microsoft PowerPoint است.
	با کلیک روی این آیکن پنجره اصلی برنامه صفحه گسترده OpenOffice Calc باز می‌شود. کاربرد این برنامه مشابه برنامه Microsoft Excel است.
	با کلیک روی این آیکن پنجره اصلی برنامه GNOME Print Manager باز می‌شود. این برنامه به منظور مدیریت چاپ اسناد طراحی شده است.

محیط‌های کاری

محیط گرافیکی GNOME بسیار منعطف است به نحوی که می‌توان پنجره‌های مربوط به برنامه‌های کاربردی را در محیط‌های کاری مختلف باز کرد. از این‌رو، به جای باز و بسته کردن پنجره‌ها کافی است بین محیط‌های کاری سوییچ کرده و پنجره مربوط به برنامه کاربردی موردنظر را در اختیار گرفت. برای مثال، می‌توان واژه‌پرداز OpenOffice Writer را در محیط کاری اول، صفحه گسترده OpenOffice Impress را در محیط کاری دوم، برنامه پردازش تصویر GIMP را در محیط کاری سوم و پنجره مربوط به ترمینال ورودی (جهت صدور فرامین) را در محیط کاری چهارم باز کرد. شکل ۳-۱۶ وضعیت این چهار محیط کاری را در قالب بخش کوچکی از پانل محیط گرافیکی GNOME نشان می‌دهد.

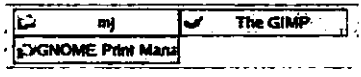
شکل ۳-۱۶ وضعیت فعلی چهار محیط کاری موجود که در قالب بخشی از پانل محیط گرافیکی GNOME به نمایش درآمده است.

برای سوییچ از یک محیط کاری به دیگری، کافی است روی بخشی از شکل قبل که نماینده محیط کاری موردنظر است، کلیک کنید. هم‌چنین برای انتقال یک برنامه کاربردی از یک محیط کاری به دیگری، ابتدا گوشه بالای سمت چپ پنجره مربوط به آن برنامه کاربردی را کلیک کنید تا منویی مشابه منوی شکل ۴-۱۶ باز شود. سپس گزینه مربوط به انتقال آن برنامه کاربردی به محیط کاری موردنظر را انتخاب کنید.



شکل ۴-۱۶ منویی که با کلیک گوشه بالای سمت چپ پنجره اصلی برنامه کاربردی باز می‌شود.

علاوه بر این می‌توانید مابین برنامه‌های کاربردی باز که نماد آن‌ها در بخشی از پانل محیط گرافیکی GNOME به نمایش درآمده است، سوییچ کنید. برای مثال، مطابق شکل ۵-۱۶ می‌توانید مابین سه برنامه کاربری باز سوییچ کنید.



شکل ۵-۱۶ بخشی از پانل محیط گرافیکی GNOME که نماد مربوط به برنامه‌ها را نشان می‌دهد.

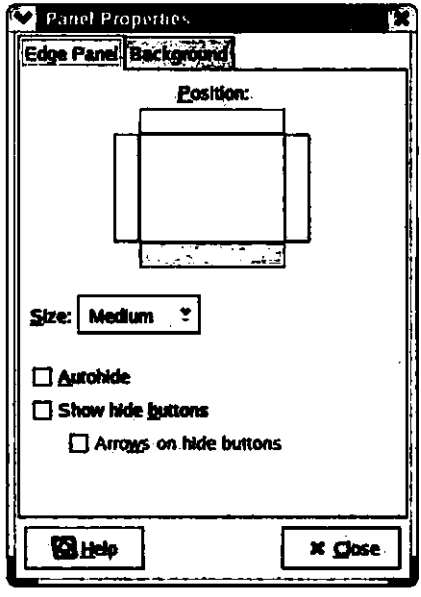
سایر امکانات پانل محیط گرافیکی GNOME

در منتهی‌الیه سمت راست از پانل محیط گرافیکی GNOME دو آیکن بزرگ وجود دارد. در این میان آیکن قرمز به شکل علامت تعجب و با عنوان Red Hat Network Alert Icon امکان بهره‌گیری از برنامه up2date را جهت اتصال به شبکه شرکت Red Hat و ارتقای بسته‌های نرم‌افزاری به نسخه‌های جدید را

در اختیار می‌گذارد. (چنان‌چه این آیکن به رنگ آبی باشد، نیازی به ارتقای بسته‌های نرم‌افزاری نیست. این بدان معنی است که سیستم موردنظر از آخرین نسخه برنامه‌های کاربردی برخوردار است.) برای اطلاع بیشتر درباره برنامه up2date به فصل دهم مراجعه کنید.

آیکن دوم بیانگر تاریخ و ساعت است. با کلیک روی این آیکن امکان تقویم ماه جاری به نمایش درمی‌آید. هم‌چنین با کلیک راست روی آیکن مزبور و انتخاب گزینه Adjust Date & Time از منوی حاصل، برنامه redhat-config-date در اختیار قرار می‌گیرد. این برنامه که درفصل نوزدهم به بررسی آن خواهیم پرداخت، امکانات لازم برای تنظیم تاریخ و ساعت را در اختیار قرار می‌دهد.

پیکربندی پانل محیط گرافیکی GNOME نیز بسیار ساده است. برای این منظور روی یک بخش خالی از این پانل کلیک راست کرده و گزینه Properties را از منوی حاصل انتخاب کنید تا به این ترتیب کادر محاوره‌ای Panel Properties باز شود. شکل ۶-۱۶ این کادر محاوره‌ای را نشان می‌دهد.



شکل ۶-۱۶ کادر محاوره‌ای Panel Properties

کادر محاوره‌ای Panel Properties امکانات متنوعی را به منظور پیکربندی پانل محیط گرافیکی GNOME در اختیار می‌گذارد. به کمک این امکانات می‌توانید اندازه و موقعیت پانل را تغییر داده و ترتیبی دهید که پانل مزبور تا زمانی که اشاره‌گر ماوس به حریم آن نزدیک نشده است، هم‌چنان پنهان

باقی بماند. علاوه بر این، با استفاده از امکانات بخش Background این کادر محاوره‌ای می‌توانید پشت صحنه یا اصطلاحاً background پانل را دستخوش تغییرات کنید.

برخی از مدیران سیستم‌های Linux استفاده از رابط سطر فرمان را بر ابزارهای گرافیکی ترجیح می‌دهند. برای دستیابی به رابط سطر فرمان در محیط گرافیکی GNOME روی محل دلخواهی از دسک‌تاپ کلیک راست کرده و گزینه New Terminal را از منوی حاصل انتخاب تا به این ترتیب پنجره مربوطه با عنوان gnome-terminal باز شود. برای دستیابی به این پنجره هم‌چنین می‌توانید گزینه Terminal را از منوی System Tools واقع در منوی اصلی محیط گرافیکی GNOME یعنی Main Menu انتخاب کنید.

منوی اصلی محیط گرافیکی GNOME

در این قسمت اجازه دهید تا به منوی اصلی محیط گرافیکی GNOME با عنوان Main Menu نگاهی بیندازیم. برای‌دستیابی به این منو کافی است روی آیکنی به شکل یک کلاه قرمز منتهی‌الیه سمت چپ از پانل محیط‌گرافیکی GNOME کلیک‌کنید. شکل ۷-۱۶ گزینه‌های‌موجود دراین منو را نشان می‌دهد.

شکل ۷-۱۶ منوی اصلی محیط گرافیکی GNOME

چنان‌که در این شکل مشاهده می‌کنید، منوی اصلی محیط گرافیکی GNOME حاوی مجموعه‌ای از فرامین و منوهای فرعی است که شرح مختصری از آن‌ها در جدول ۲-۱۶ آمده است. جزییات بیشتر درباره این منوها را در این فصل و فصول بعدی بررسی خواهیم کرد. البته برخی از برنامه‌های کاربردی که از طریق این منوها قابل دستیابی هستند به طور خاص برای محیط گرافیکی KDE طراحی شده‌اند. محیط گرافیکی KDE یا K Desktop Environment را در فصل هفدهم مورد بررسی قرار می‌دهیم. بسیاری از برنامه‌های کاربردی قابل دستیابی از طریق منوهای فرعی مستقر در منوی اصلی محیط گرافیکی GNOME، از جمله نرم‌افزارهای اداری و گرافیکی را در فصل هجدهم بررسی خواهیم کرد. در فصل نوزدهم نیز به بررسی ابزارهای مدیریتی خاص سیستم‌عامل Red Hat Linux خواهیم پرداخت.

جدول ۲-۱۶ شرح مختصری درباره فرامین و منوهای فرعی موجود در منوی اصلی محیط گرافیکی GNOME

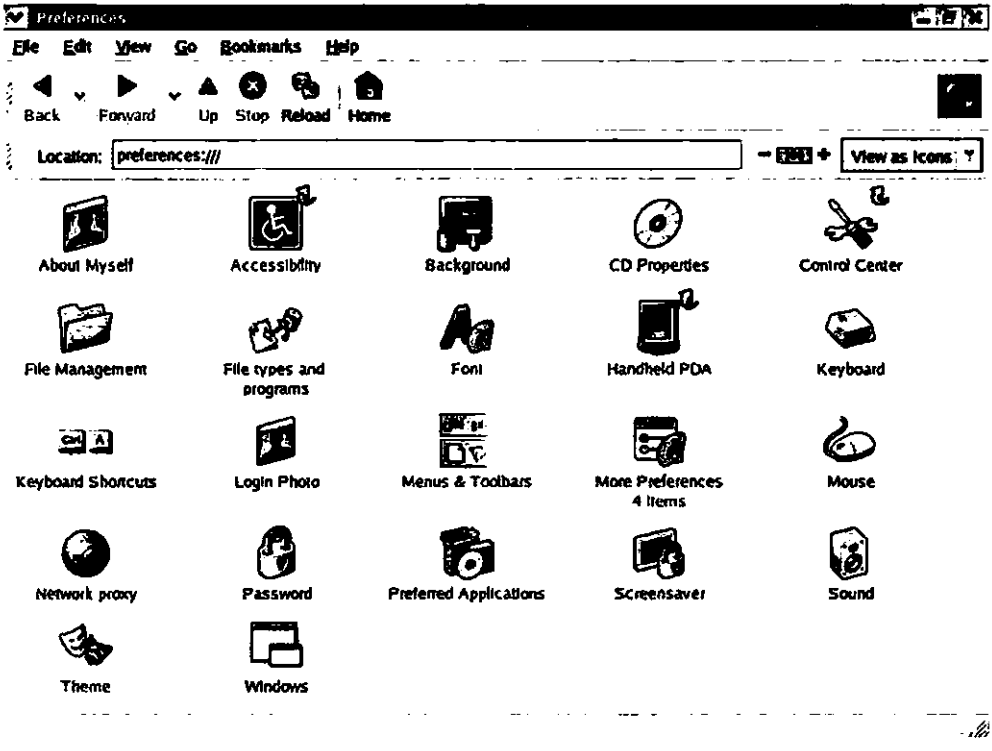
عنوان فرمان یا منوی فرعی	توضیح
Accessories	این منوی فرعی امکان دسترسی به مجموعه‌ای از برنامه‌های کوچک از جمله ویرایشگرهای متنی و ماشین حساب را در اختیار می‌گذارد.
Documentation	این منوی فرعی اسنادی را که ممکن است از روی CD حاوی مستندات سیستم‌عامل Red Hat Linux بارگذاری کرده باشید، در اختیار می‌گذارد.
Games	این منوی فرعی امکان دسترسی به بازی‌های کامپیوتری نصب شده روی ماشین میزبان را در اختیار می‌گذارد.
Graphics	این منوی فرعی امکان دسترسی به برنامه‌هایی جهت ویرایش تصویر، تهیه عکس از صفحه نمایش، بازخوانی اسناد PDF و سایر برنامه‌های مشابه را در اختیار قرار می‌دهد.
Internet	این منوی فرعی امکان دسترسی به برنامه‌هایی جهت برقراری ارتباط از طریق شبکه‌هایی از نوع TCP/IP مانند شبکه جهانی اینترنت را در اختیار قرار می‌دهد.
Office	این منوی فرعی امکان دسترسی به برنامه‌هایی را در اختیار می‌گذارد که در قالب نرم‌افزار اداری OpenOffice روی ماشین میزبان نصب شده‌اند. سایر نرم‌افزارهای اداری مشابه نیز از طریق همین منوی فرعی قابل دستیابی هستند.
Preferences	این منوی فرعی امکاناتی را به منظور انجام تنظیمات مختلف به ویژه در مورد دسک‌تاپ فراهم می‌کند.

عنوان فرمان یا منوی فرعی	توضیح
Programming	این منوی فرعی امکان دسترسی به ابزارهای برنامه‌نویسی را در اختیار می‌گذارد. نکته عجیب آن‌که برنامه Emacs نیز از طریق همین منوی فرعی قابل دستیابی است.
Sound & Video	این منوی فرعی امکان دسترسی به برنامه‌های کاربردی چند رسانه‌ای، شامل برنامه‌ای برای نوشتن روی CD را در اختیار می‌گذارد.
System Settings	این منوی فرعی دسترسی به مجموعه ابزارهای *-redhat-config را فراهم می‌کند. تنها کاربر اصلی (اصطلاحاً root) قادر است تمام این ابزارها را مورد استفاده قرار دهد.
System Tools	این منوی فرعی امکان دسترسی به مجموعه‌ای از ابزارهای مدیریتی را در اختیار می‌گذارد.
Help	این فرمان راهنمای مربوط به محیط گرافیکی GNOME را در قالب یک برنامه مرورگر به نمایش می‌گذارد.
Home Folder	این فرمان محتوای فهرست خانگی (اصطلاحاً home directory) را در قالب برنامه Nautilus به نمایش می‌گذارد.
Network Servers	این فرمان امکان دسترسی به فهرست‌های مشترک بین ماشین میزبان و سایر ماشین‌ها را فراهم می‌کند. (دسترسی به‌ماشین‌هایی که از سیستم‌عامل Microsoft Windows استفاده می‌کنند از طریق همین فرمان و به واسطه سرویس Samba امکان‌پذیر است.)
Run Program	این فرمان موجب نمایش کادر محاوره‌ای Run Program شده و به این ترتیب امکان اجرای برنامه کاربردی موردنظر را در اختیار می‌گذارد.
Search For Files	این فرمان امکانات لازم برای جستجوی فایل‌ها در یک فهرست مشخص را فراهم می‌کند.
Open Recent	این منوی فرعی امکان دسترسی به اسنادی را فراهم می‌کند که اخیراً مورد دستیابی قرار گرفته‌اند.
Lock Screen	این فرمان موجب نمایش صفحه screensaver می‌شود. برای دستیابی مجدد به دسک‌تاپ کاربر باید شناسه و کلمه‌عبور خود را در کادر محاوره‌ای مربوطه وارد کند.
Log Out	این فرمان موجب خروج از محیط گرافیکی GNOME می‌شود.

اگر منوی فرعی به خصوصی را در منوی اصلی Main Menu مشاهده نمی‌کنید، به احتمال قوی بسته نرم‌افزاری مربوطه را نصب نکرده‌اید. برای مثال، چنان‌چه بسته نرم‌افزاری gnome-games-* یا kdegames-* را نصب نکنید، منوی فرعی Games را مشاهده نخواهید کرد.

مرکز کنترل محیط گرافیکی GNOME

در این قسمت به بررسی جزییات بیشتری درباره پیکربندی محیط گرافیکی GNOME می‌پردازیم. ابزارهای موردنیاز برای انجام این کار از طریق مرکز کنترل این محیط گرافیکی موسوم به GNOME Control Center قابل دستیابی هستند. برای مشاهده این گزینه‌ها کافی است گزینه Control Center از منوی فرعی Preferences واقع در منوی اصلی Main Menu را انتخاب کنید. با اقدام فوق آیکن‌های مربوط به این ابزارها را در قالب پنجره برنامه Nautilus مشاهده خواهید کرد. شکل ۸-۱۶ پنجره مزبور را در حال نمایش ابزارهای مرکز کنترل محیط گرافیکی GNOME نشان می‌دهد.

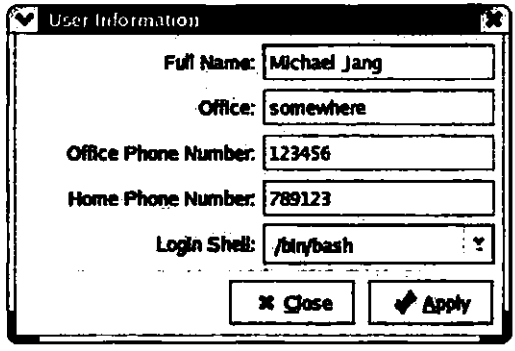


شکل ۸-۱۶ مرکز کنترل محیط گرافیکی GNOME

تمام ابزارهای موجود در مرکز کنترل محیط گرافیکی GNOME از طریق منوی فرعی Preferences واقع در منوی اصلی Main Menu قابل دستیابی هستند.

ابزار About Myself

با کلیک روی آیکن مربوط به ابزار About Myself پنجره‌ای مشابه شکل ۹-۱۶ با عنوان User Information باز می‌شود. به کمک تنظیمات موجود در این پنجره می‌توانید اطلاعات بیشتری از جمله تلفن تماس و آدرس پستی را در مورد حساب کاربری خود در اختیار سیستم قرار دهید. این ابزار در واقع رابط گرافیکی برنامه chfn است. اطلاعات وارد شده توسط فرمان finger قابل بازیابی است.



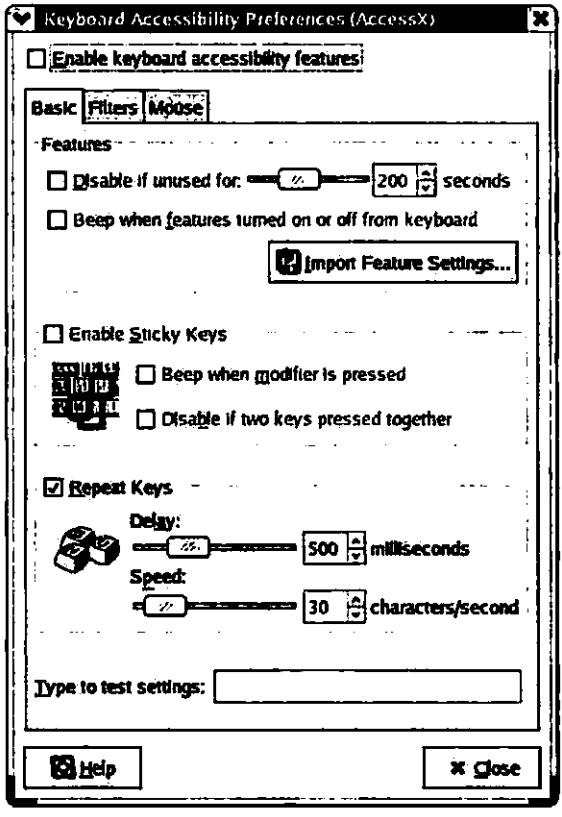
شکل ۹-۱۶ پنجره User Information

ابزار Accessibility

با کلیک روی آیکن مربوط به ابزار Accessibility پنجره‌ای مشابه شکل ۱۰-۱۶ با عنوان Keyboard Accessibility Preferences باز می‌شود. چنان‌چه مایل به تغییر ویژگی خاصی هستید، ابتدا باید گزینه Enable Keyboard Accessibility Features را فعال کنید.

امکانات موجود در این پنجره در سه بخش مختلف با عناوین Basic، Filters و Mouse قالب‌بندی شده است. بخش Basic امکانات موردنیاز برای تغییر تنظیمات استاندارد صفحه کلید را در اختیار می‌گذارد. بخش Filter تنظیمات مربوط به پیشگیری از خطای ورودی را در اختیار قرار می‌دهد. برای مثال، چنان‌چه انگشتان شما ضمن لمس کلیدها دچار لرزش شده به نحوی که کاراکتر مربوطه دو بار تایپ شود، با فعال کردن گزینه Enable Bounce Keys از این بخش می‌توانید ترتیبی دهید که تأثیر فشار کلیدها در فاصله زمانی چند میلی ثانیه نادیده گرفته شده و به این ترتیب از تایپ مضاعف کاراکترهای

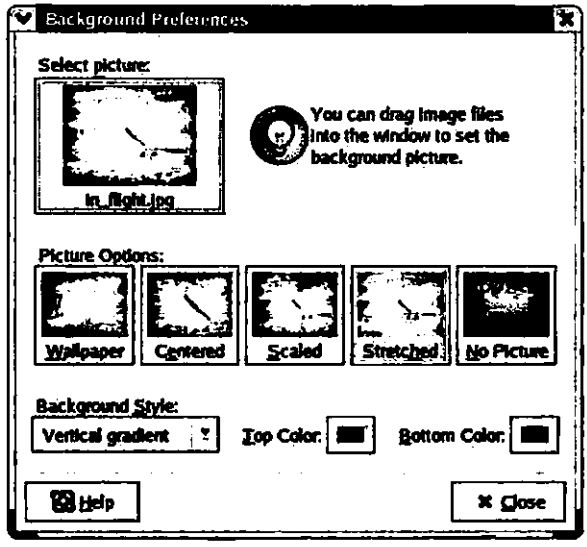
مربوطه به واسطه خطای انگشتان جلوگیری به عمل آید. بخش Mouse نیز امکاناتی را در ارتباط با تنظیم سرعت انتقال اشاره‌گر ماوس روی صفحه نمایش در اختیار می‌گذارد.



شکل ۱۰-۱۶ پنجره Keyboard Accessibility Preferences

ابزار Background

با کلیک روی آیکن مربوط به ابزار Background پنجره‌ای مشابه شکل ۱۱-۱۶ با عنوان Background Properties باز می‌شود. به کمک امکانات موجود در این پنجره می‌توان تنظیمات مربوط به صفحه نمایش و تصویر مورد استفاده به عنوان پس‌زمینه آن‌را انجام داد. برای تعویض تصویر پس‌زمینه صفحه نمایش کافی است روی صفحه تصویر موردنظر در قسمت Select Picture از پنجره مذکور کلیک کنید.

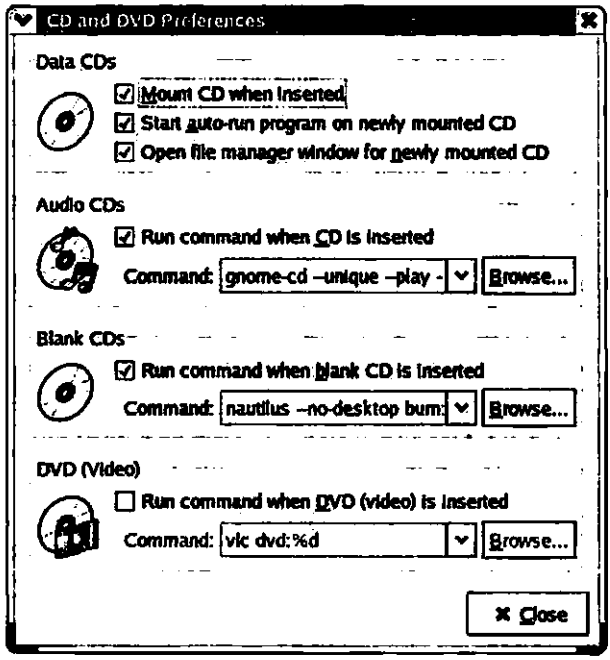


شکل ۱۱-۱۶ پنجره Background Preferences

ابزار CD Properties

با کلیک روی آیکن مربوط به ابزار CD Properties، مشابه شکل ۱۲-۱۶ پنجره‌ای با عنوان CD And DVD Preferences باز می‌شود. به کمک امکانات موجود در این پنجره می‌توان خط مشی سیستم را هنگام ورود یک CD یا DVD به درایو مربوطه مشخص کرد. به طور پیش‌فرض، چنان‌چه CD موردنظر حاوی اطلاعات باشد به طور خودکار روی سیستم فایل سوار می‌شود. هم‌چنین اگر CD از نوع صوتی باشد، توسط برنامه gnome-cd به اجرا درآمده و بالاخره اگر CD خالی باشد، امکان نوشتن روی آن از طریق برنامه Nautilus CD Burner فراهم می‌شود. در دو مورد اخیر یعنی CD صوتی و CD خالی و هم‌چنین DVD می‌توان فرمان مشخصی را در کادر متنی Command وارد کرد.

با کلیک روی آیکن مربوط به این برنامه در مرکز کنترل محیط گرافیکی GNOME پنجره دیگری نیز باز می‌شود.

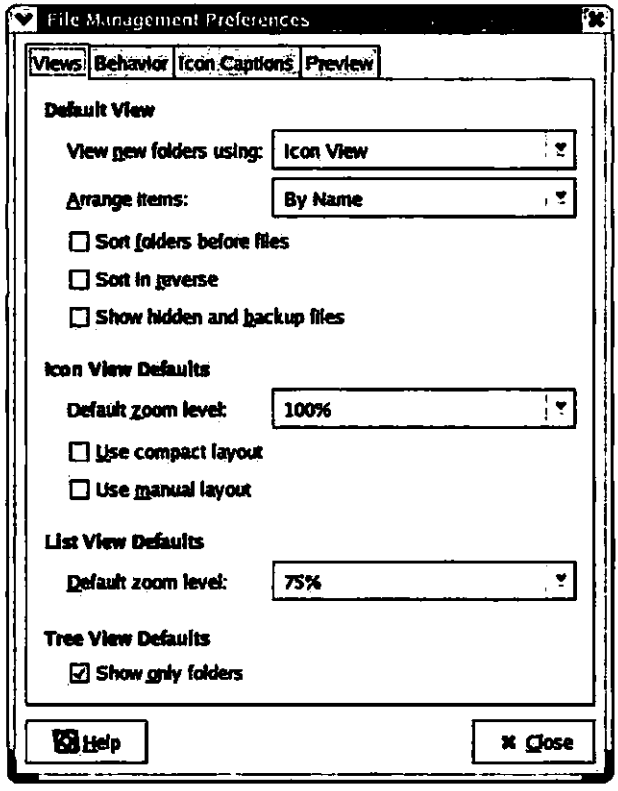


شکل ۱۲-۱۶ پنجره CD and DVD Preferences

ابزار File Management

با کلیک روی آیکن مربوط به ابزار File Management، پنجره‌ای مشابه شکل ۱۳-۱۶ با عنوان File Management Preferences باز می‌شود. به کمک امکانات موجود در این پنجره می‌توان تنظیمات مربوط به نحوه نمایش آیکن فایل‌ها و تعامل با آن‌ها در برنامه Nautilus را انجام داد. پنجره مذکور از چهار بخش مختلف به این شرح تشکیل شده است:

- بخش Views شامل امکاناتی برای تنظیم نحوه نمایش آیکن فایل‌ها در برنامه Nautilus است. مقدار پیش‌فرض گزینه View name folders using برابر با Icon View است، به این معنی که در برنامه Nautilus محتوای فایل‌های گرافیکی در نمای thumbnail به نمایش درمی‌آید.
- در بخش Behavior می‌توان عکس‌العملی را که در ازای کلیک روی آیکن فایل‌ها رخ می‌دهد، مشخص کرد. برای مثال، به کمک این تنظیمات می‌توان ترتیبی داد تا کلیک روی آیکن فایل‌های اجرای موجب اجرای این گونه فایل‌ها شود.
- به کمک امکانات موجود در بخش Icon Caption می‌توان اطلاعاتی از یک فایل را که در کنار آیکن مربوط به آن فایل نمایش داده می‌شود، مشخص کرد.

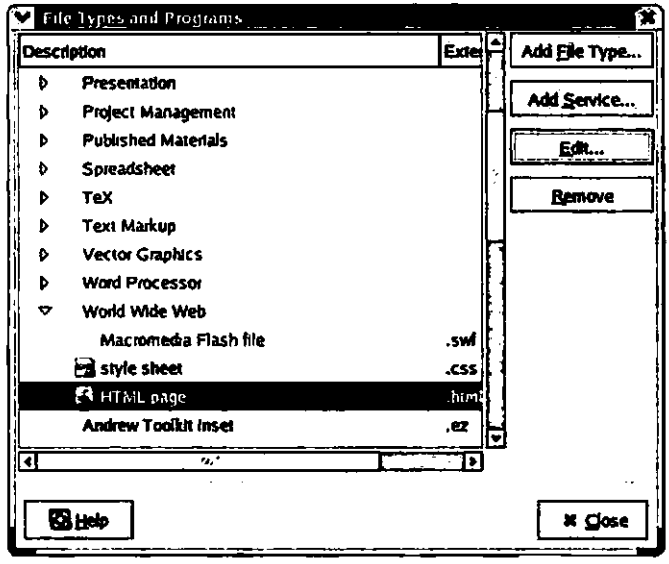


شکل ۱۳-۱۶ پنجره File Management Preferences

- بخش Preview تنظیمات‌مربوط به تعیین نحوه رفتار فایل‌های متنی، تصویری، صوتی و فهرست‌ها را در برنامه Nautilus در اختیار می‌گذارد.

ابزار File Types And Programs

با کلیک روی آیکن مربوط به ابزار File Types And Programs پنجره‌ای مشابه شکل ۱۴-۱۶ با عنوان File Types And Programs باز می‌شود. به کمک امکانات موجود در این پنجره می‌توان ارتباط لازم میان انواع فایل‌ها با برنامه‌های کاربردی را برقرار کرد، به نحوی که با کلیک روی آیکن مربوط به فایل، برنامه کاربردی مربوطه باز شود. شناسایی نوع فایل‌ها از طریق پسوند آن‌ها (هم‌چون doc. یا tif.) صورت می‌گیرد. برای ویرایش یک ارتباط از پیش تعیین شده میان نوعی فایل و یک برنامه کاربردی، کافی است نوع فایل موردنظر را از لیست موجود در این پنجره انتخاب کرده و دکمه Edit را کلیک کنید.



شکل ۱۳-۱۶ پنجره File Types And Programs

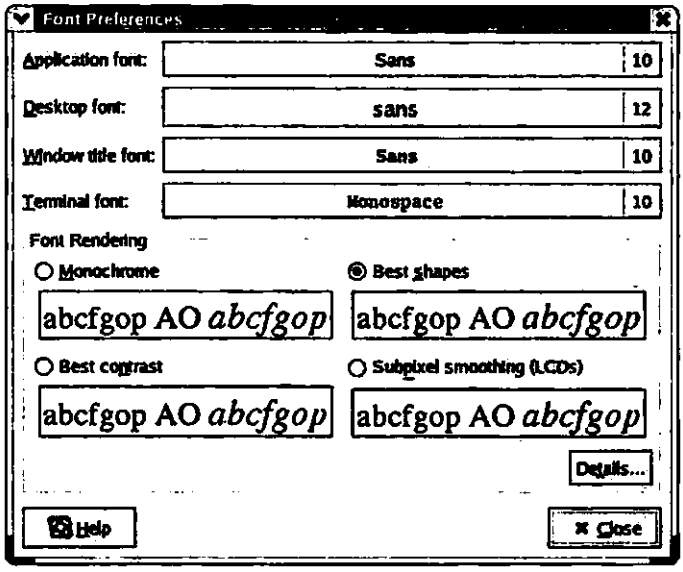
نوع فایل مربوط به صفحات HTML تحت زیر مجموعه World Wide Web از مجموعه Documents دسته‌بندی شده است.

ابزار Font

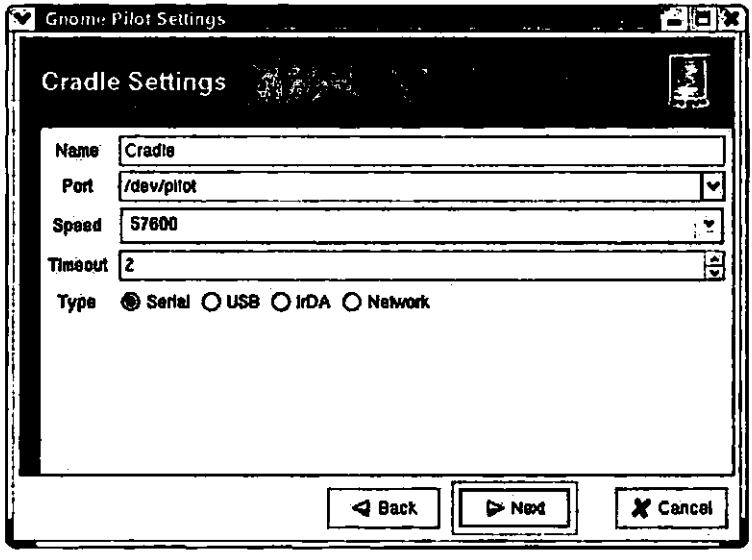
با کلیک روی آیکن مربوط به ابزار Font پنجره‌ای مشابه شکل ۱۵-۱۶ با عنوان Font Properties باز می‌شود. به کمک امکانات موجود در این پنجره می‌توان فونت پیش‌فرض عناصر مختلف موجود روی دسک‌تاپ را مشخص کرد. تعیین فونت‌های مورد استفاده در برنامه‌های کاربردی و ابزارهای مختلف، از جمله فونت مورد استفاده در ترمینال نیز از طریق همین تنظیمات امکان‌پذیر است.

ابزار Handheld PDA

با کلیک روی آیکن مربوط به ابزار Handheld PDA پنجره‌ای مشابه شکل ۱۶-۱۶ با عنوان GNOME Pilot Settings باز می‌شود. این ابزار، که در واقع رابط گرافیکی برنامه gnome-pilot است، به منظور هماهنگی داده‌ها میان محیط گرافیکی GNOME و تجهیزات ساخته شده براساس استانداردهای PalmPilot و PalmOS پیش‌بینی شده است. اگر برای نخستین بار روی آیکن مربوط به این ابزار کلیک می‌کنید، تنظیمات موردنیاز را می‌توانید با استفاده از ویزاردی که به همین منظور پیش‌بینی شده است، به راحتی انجام دهید.



شکل ۱۵-۱۶ پنجره Font Properties

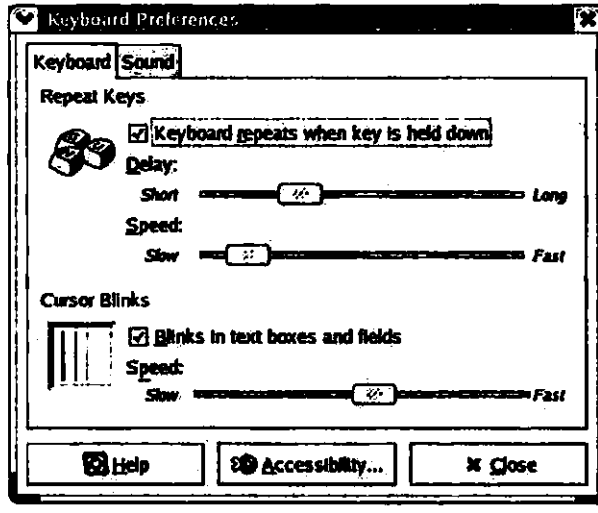


شکل ۱۶-۱۶ پنجره GNOME Pilot Settings

ابزار Keyboard

با کلیک روی آیکن مربوط به ابزار Keyboard، پنجره‌ای مشابه شکل ۱۷-۱۶ با عنوان Keyboard Preferences باز می‌شود. به کمک امکانات موجود در این پنجره می‌توان تنظیماتی را در مورد صفحه

کلید، از جمله نحوه پاسخ به فشار یک کلید، کیفیت چشمک‌زدن مکان‌نما و استفاده از صدا هنگام وقوع رخدادهای مربوط به صفحه کلید انجام داد.



شکل ۱۷-۱۶ پنجره Keyboard Preferences

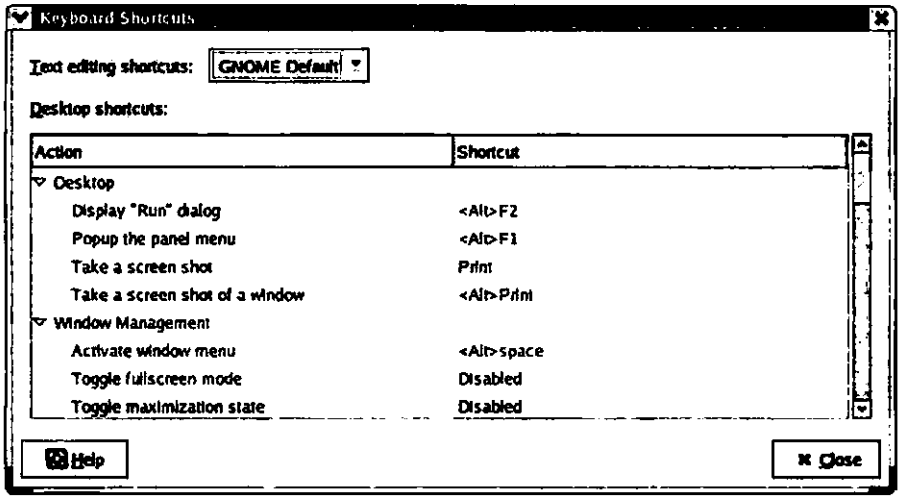
ابزار Keyboard Shortcuts

با کلیک‌روی آیکن مربوط به ابزار Keyboard Shortcuts، پنجره‌ای با همین عنوان مشابه شکل ۱۸-۱۶ باز می‌شود. محتوای این پنجره حاوی شرح قابلیت‌های کلیدهای کنترلی شامل Shift، Ctrl، Alt، Tab و Esc است. تنظیمات پیش‌فرض محیط گرافیکی GNOME و برنامه Emacs با انتخاب گزینه مربوطه از لیست Text Editing Shortcuts در این پنجره به نمایش درمی‌آید.

برای تغییر یک کلید میانبر، ابتدا آن‌را از لیست موجود انتخاب کرده و کلید Backspace را فشار دهید. سپس کلیدهای موردنظر خود را فشار دهید.

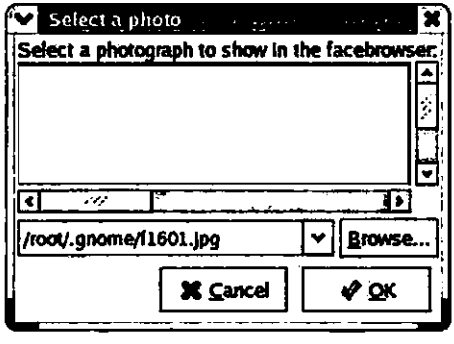
ابزار Login Photo

پنجره Login Photo بخشی از امکانات برنامه GNOME Display Manager یا به اختصار GDM است که پیشتر در فصل پانزدهم به بررسی آن پرداختیم. تنظیمات موجود در این پنجره امکان تعیین تصویری را به منظور نمایش در صفحه خوش‌آمدگویی استاندارد یا اصطلاحاً GDM Standard Greeter در اختیار قرار می‌دهد. این عکس تنها در صورت استفاده از برنامه GDM به نمایش درمی‌آید.



شکل ۱۸-۱۶ پنجره Keyboard Shortcuts

برای تعیین تصویر موردنظر گزینه Show Choosable User Images از بخش Standard Greeter واقع در پنجره GDM Setup را فعال کنید. (برای اطلاع بیشتر به فصل پانزدهم مراجعه کنید.) در این صورت، به کمک تنظیمات کادر محاوره‌ای Select A Photo می‌توانید تصویر موردنظر را انتخاب کنید. شکل ۱۹-۱۶ این کادر محاوره‌ای را نشان می‌دهد.

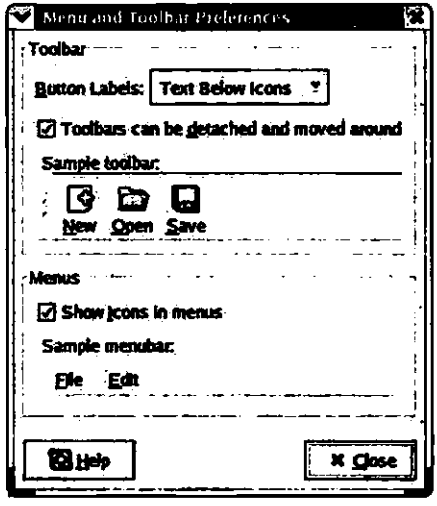


شکل ۱۹-۱۶ کادر محاوره‌ای Select A Photo

اندازه تصویر منتخب در کادر محاوره‌ای Select A Photo حداکثر باید ۶۴ کیلو بایت باشد.

ابزار Menus And Toolbars

با کلیک روی آیکن مربوط به ابزار Menus And Toolbars پنجره‌ای مشابه شکل ۲۰-۱۶ با عنوان Menu And Toolbar Preferences باز می‌شود. به کمک امکانات موجود در این پنجره می‌توان ظاهر آیکن‌ها و متون به کار رفته در منوها را تغییر داد.



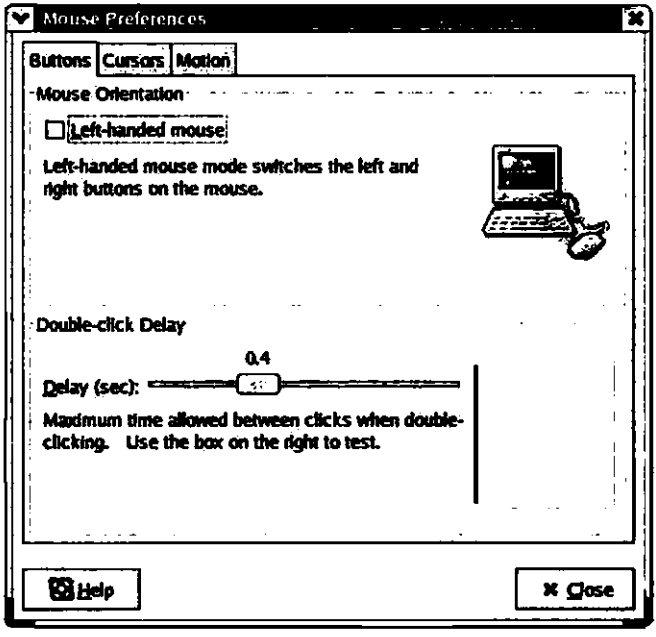
شکل ۲۰-۱۶ پنجره Menu And Toolbar Preferences

ابزار Mouse

با کلیک روی ابزار Mouse پنجره‌ای مشابه شکل ۲۱-۱۶ با عنوان Mouse Preferences باز می‌شود. به کمک امکانات موجود در این پنجره می‌توان مشخصات ماوس را تغییر داد.

چنان‌که مشاهده می‌کنید، پنجره فوق از سه بخش مختلف به این شرح تشکیل شده است:

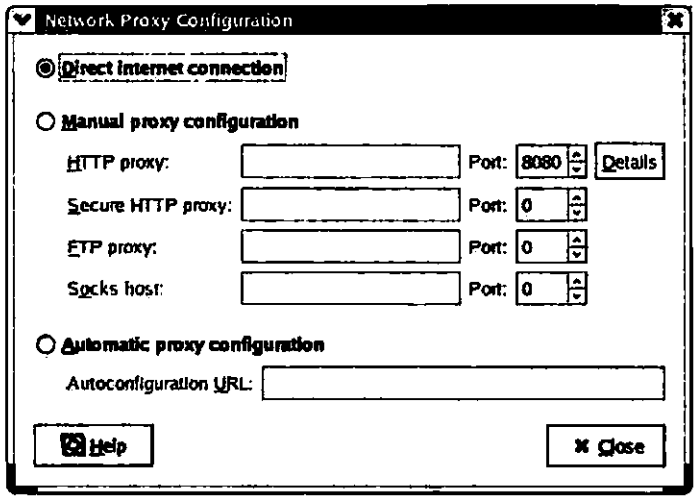
- **بخش Buttons**: تنظیمات موجود در این بخش امکان تعویض عملکرد دکمه‌های چپ و راست ماوس و میزان تأخیر دو کلیک پیاپی در دابل کلیک را در اختیار می‌گذارد.
- **بخش Cursors**: تنظیمات موجود در این بخش امکان انتخاب علایم مختلف را به عنوان اشاره‌گر ماوس فراهم می‌کند.
- **بخش Motion**: تنظیمات موجود در این بخش امکان تعیین سرعت حرکت اشاره‌گر ماوس روی صفحه و نحوه درگ کردن را در اختیار قرار می‌دهد.



شکل ۲۱-۱۶ پنجره Mouse Preferences

ابزار Network Proxy

با کلیک روی آیکن مربوط به ابزار Network Proxy، پنجره‌ای مشابه شکل ۲۲-۱۶ با عنوان Network Proxy Configuration باز می‌شود. به کمک امکانات موجود در این پنجره، می‌توان نحوه دسترسی به شبکه خارجی را که عموماً اینترنت است، تعیین کرد. گزینه نخست با عنوان Direct internet connection برای دسترسی‌مستقیم به اینترنت و دو گزینه دیگر برای دسترسی غیرمستقیم به اینترنت از طریق سرور پروکسی پیش‌بینی شده‌اند. در صورت انتخاب گزینه دوم با عنوان Manual proxy configuration لازم است تنظیمات دیگری را نیز انجام دهید. برخی از مدیران سیستم‌ها تسهیلاتی را به منظور پیکربندی خودکار سرور پروکسی مستقر در شبکه مهیا می‌کنند. در این صورت بهتر است گزینه سوم با عنوان Automatic proxy configuration را انتخاب‌کرده و آدرس فایل پیکربندی مربوطه را در فیلد متنی مربوطه وارد کنید.



شکل ۲۲-۱۶ پنجره Network Proxy Configuration

ابزار Password

کاربرد ابزار Password بسیار ساده و مشخص است. به کمک تنظیماتی که این ابزار در اختیار می‌گذارد می‌توان کلمه عبور حساب کاربران را تغییر داد. این ابزار در واقع رابطی برای اجرای فرمان passwd است. (برای تغییر کلمه عبور با استفاده از این فرمان، کافی است آن‌را اجرا کرده و پس از وارد کردن کلمه عبور فعلی، کلمه عبور جدید را یک بار وارد کرده و بار دیگر آن‌را تأیید کنید.)

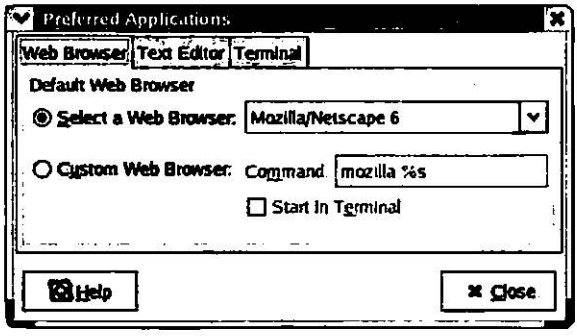
ابزار Preferred Applications

با کلیک روی آیکن مربوط به ابزار Preferred Applications پنجره‌ای مشابه شکل ۲۳-۱۶ با همین عنوان باز می‌شود. به کمک امکانات موجود در این پنجره می‌توان برنامه‌های کاربردی پیش‌فرض شامل مرورگر وب، ویرایشگر متن و ترمینال موردنظر برای اجرای فرامین را مشخص کرد. مرورگر وب پیش‌فرض Mozilla و ترمینال پیش‌فرض gnome-terminal است. با وجود این، هیچ پیش‌فرضی برای ویرایشگر متن در نظر گرفته نشده است.

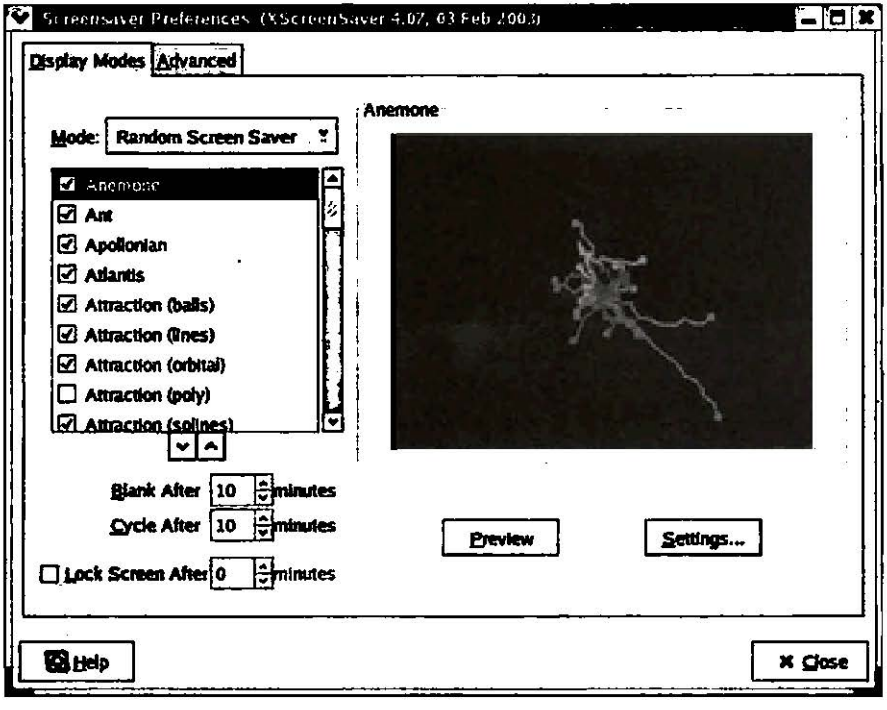
ابزار Screensaver

با کلیک روی آیکن مربوط به ابزار Screensaver پنجره‌ای مشابه شکل ۲۴-۱۲ با عنوان Screensaver Preferences باز می‌شود. به کمک تنظیمات موجود در این پنجره می‌توان برنامه یا برنامه‌های screensaver موردنظر را از لیست موجود انتخاب کرد. هم‌چنین می‌توان ترتیبی داد تا پس از سپری

شدن مدت زمان معلوم که توسط مقدار گزینه Cycle After بر حسب دقیقه مشخص می‌شود، به شرطی که طی این مدت کاربر ماوس را حرکت نداده یا کلیدی را فشار نداده باشد، یکی از این برنامه‌ها به طور تصادفی اجرا شود. علاوه بر این، در صورت تمایل می‌توان تنظیمات دیگری را نیز انجام داد.



شکل ۱۶-۲۳ پنجره Preferred Applications

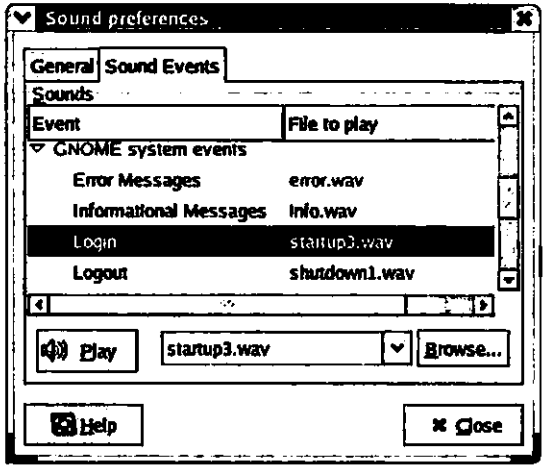


شکل ۱۶-۲۴ پنجره Screensaver Preferences

کاربر اصلی (اصطلاحاً root) در محیط گرافیکی GNOME امکان دسترسی به برنامه‌های screensaver را ندارد، مگر آن‌که فرمان xhost +localhost را قبلاً اجرا کرده باشد. فرمان xhost که در فصل سیزدهم به توضیح آن پرداختیم، امکان دسترسی به کامپیوتر موردنظر را از طریق شبکه فراهم می‌کند. در واقع محیط گرافیکی GNOME کاربر اصلی را از دسترسی به رابط گرافیکی (اصطلاحاً GUI) منع می‌کند.

ابزار Sound

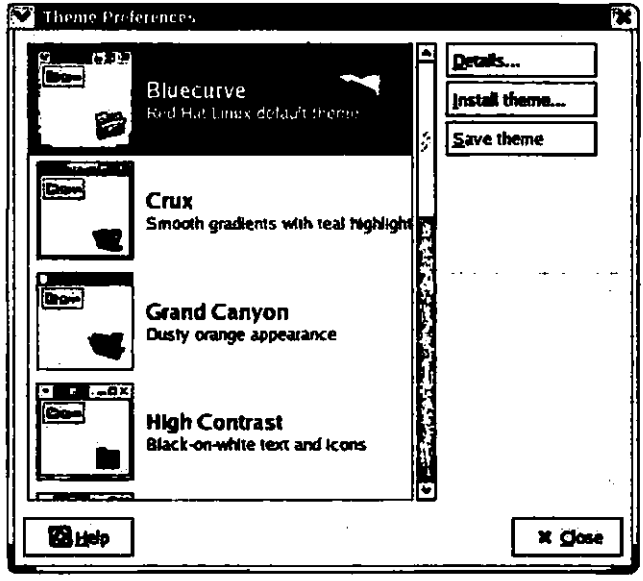
با کلیک روی آیکن مربوط به ابزار Sound پنجره‌ای مشابه شکل ۲۵-۱۶ با عنوان Sound Preferences باز می‌شود. چنان‌چه قبلاً کارت صوتی متصل به کامپیوتر به درستی پیکربندی شده باشد، با استفاده از امکانات موجود در این پنجره می‌توان صداهای مختلفی را برای مواردی چون دریافت پیغام‌های الکترونیکی، ورود به سیستم، وقوع خطاها و سایر موارد پیکربندی کرد.



شکل ۲۵-۱۶ پنجره Sound Preferences

ابزار Theme

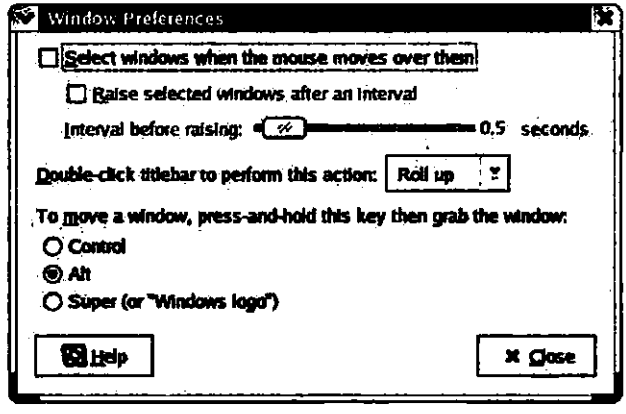
با کلیک روی آیکن مربوط به ابزار Theme پنجره‌ای مشابه شکل ۲۵-۱۶ با عنوان Theme Preferences باز می‌شود. تنظیمات موجود در این پنجره بسیار ساده هستند. چنان‌که در این شکل مشاهده می‌کنید، گزینه Bluecurve در این مورد به عنوان گزینه پیش‌فرض مورد استفاده در سیستم‌عامل Red Hat Linux انتخاب شده است. برای اطلاع از جزییات مربوطه، شامل نحوه نمایش کنترل‌های مختلف، حاشیه پنجره‌ها و آیکن‌ها، ابتدا گزینه موردنظر را انتخاب کرده و سپس دکمه Defaults را کلیک کنید.



شکل ۱۶-۲۶ پنجره Theme Preferences

ابزار Windows

با کلیک روی آیکن مربوط به ابزار Windows پنجره‌ای مشابه شکل ۱۶-۲۷ با عنوان Window Preferences باز می‌شود. به کمک تنظیمات موجود در این پنجره می‌توان رفتار پنجره‌ها در محیط گرافیکی GNOME، از جمله عکس‌العمل آن‌ها در ازای دابل کلیک روی نوار عنوان و ترکیب کلیدهای مورد استفاده جهت انتقال آن‌ها را مشخص کرد.



شکل ۱۶-۲۷ پنجره Window Preferences

ابزار More Preferences

با کلیک روی آیکن مربوط به این ابزار پنجره دیگری شامل سه گزینه CD Database، Panel و Session باز می‌شود. با کلیک روی هر یک از این گزینه‌ها تنظیمات مربوط به آن‌ها در اختیار قرار می‌گیرد. در قسمت‌های بعد این موضوع را بررسی خواهیم کرد.

ابزارها و برنامه‌های کاربردی توزیع شده برای استفاده در محیط گرافیکی GNOME

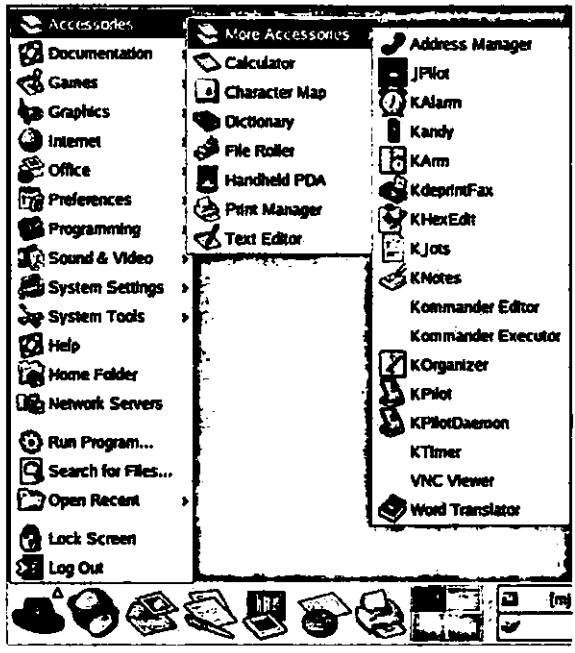
محیط گرافیکی GNOME خود حاوی برنامه‌های کاربردی متعددی است. این برنامه‌ها را می‌توان از طریق منوی اصلی مورد دستیابی قرار داد. برنامه‌های کاربردی مورد بحث به خوبی در قالب گروه‌های مختلفی با عنوان Accessories، Internet، Preferences، Multimedia و System Tools دسته بندی شده‌اند. البته برنامه‌های کاربردی بیشتری از طریق منوی اصلی قابل دستیابی است. در این فصل تنها به بررسی آن دسته از برنامه‌های کاربردی می‌پردازیم که در قالب پروژه GNOME توسعه یافته و در واقع بخشی از آن محسوب می‌شوند. ضمن این بررسی، به برخی از برنامه‌های متفرقه نیز اشاره خواهیم کرد. بررسی سایر برنامه‌ها را به سه فصل بعدی موکول می‌کنیم.

گروه برنامه‌های Accessories

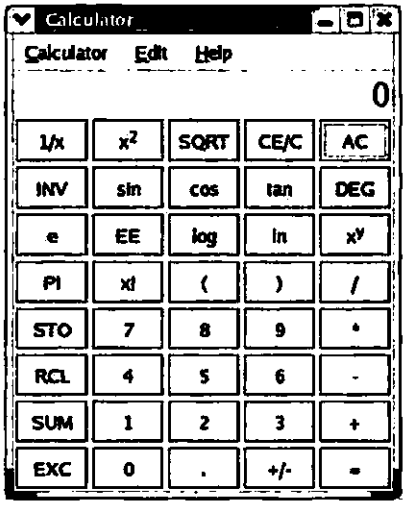
این گروه شامل برنامه‌هایی است که به منظور ساده‌تر کردن وظایف متداول طراحی شده‌اند. دسترسی به این برنامه‌ها از طریق منوی فرعی Accessories واقع در منوی اصلی محیط گرافیکی GNOME امکان‌پذیر است. شکل ۲۸-۱۶ محتوای این منو را نشان می‌دهد. چنان‌که مشاهده می‌کنید، منوی فرعی More Accessories خود حاوی برنامه‌های دیگری است. از آن‌جا که توسعه اغلب این برنامه‌ها در قالب پروژه KDE انجام شده است، بررسی آن‌ها را به فصل بعد موکول می‌کنیم. در این قسمت به بررسی محتوای منوی Accessories می‌پردازیم.

برنامه Calculator

برنامه Calculator یک ماشین حساب علمی ساده است که با فشار کلیدهای عددی موجود در صفحه کلید نیز قابل بهره‌برداری است. در صورت تمایل می‌توان نتیجه حاصل از محاسبات را در برنامه کاربردی دیگری مورد استفاده قرار داد. شکل ۲۹-۱۶ پنجره این برنامه را نشان می‌دهد.



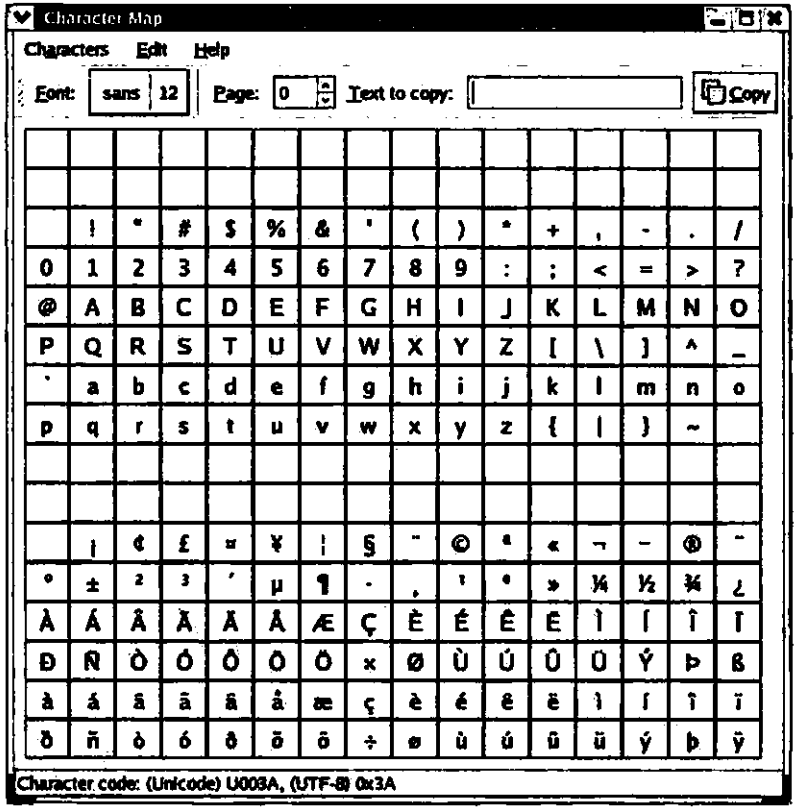
شکل ۲۸-۱۶ محتوای منوی Accessories



شکل ۲۹-۱۶ پنجره برنامه Calculator

برنامه Character Map

برنامه Character Map امکانات لازم برای کار با برخی زبان‌های غیرانگلیسی را که ساختاری متشکل از الفبای لاتین دارند، در اختیار می‌گذارد. با کلیک روی کاراکترهای موجود در پنجره این برنامه می‌توان آن‌ها را در اسناد موردنظر درج کرد. شکل ۳۰-۱۶ پنجره مذکور را نشان می‌دهد.

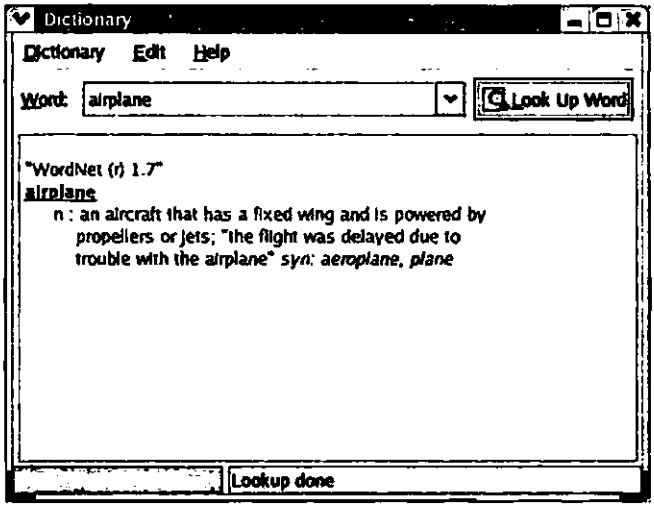


شکل ۳۰-۱۶ پنجره برنامه Character Map

برنامه Dictionary

برنامه Dictionary در واقع رابطی برای دسترسی به یک فرهنگ لغات جامع مستقر در شبکه اینترنت به آدرس dict.org است. ارتباط این برنامه برای ارتباط با دیکشنری مذکور از طریق پورت TCP/IP شماره ۲۶۲۸ برقرار می‌شود. از این‌رو، در آدرس فوق اثری از پروتکل http یا www به چشم نمی‌خورد. برای استفاده از این برنامه بدیهی است که باید ارتباط کامپیوتر میزبان با شبکه اینترنت برقرار باشد.

شکل ۳۱-۱۶ پنجره برنامه Dictionary را پس از بازیابی توضیح مربوط به واژه airplane از دیکشنری مورد بحث نشان می‌دهد.



شکل ۳۱-۱۶ پنجره برنامه Dictionary

برنامه File Roller

برنامه File Roller قابلیتی شبیه به برنامه Zip را که به منظور استفاده در سیستم‌عامل ویندوز توسعه یافته است، در اختیار قرار می‌دهد. به کمک امکانات این برنامه می‌توان محتوای فایل‌های فشرده را مورد مشاهده قرار داده و در صورت لزوم آن‌ها را بازیابی کرد. شکل ۳۲-۱۶ پنجره این برنامه را در حال بازیابی محتوای فایل فشرده‌ای از نوع tar.gz. نشان می‌دهد.

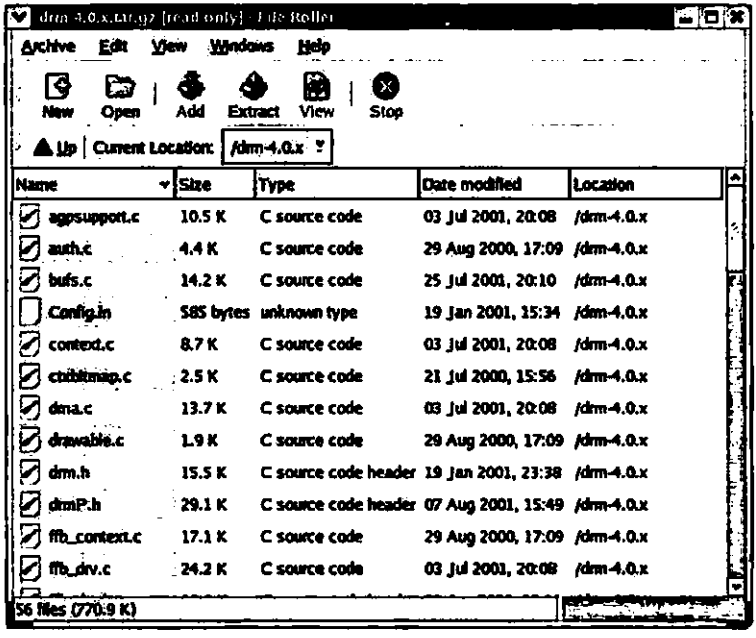
برنامه Handheld PDA

با انتخاب گزینه Handheld PDA از منوی فرعی Accessories واقع در منوی اصلی، پنجره مربوط به ابزار Pilot Link باز می‌شود. به دلیل آن‌که در قسمت‌های قبل به شرح امکانات این ابزار پرداختیم، از بررسی برنامه Handheld PDA در این‌جا صرف نظر می‌کنیم.

برنامه Print Manager

با انتخاب گزینه Print Manager از منوی فرعی Accessories واقع در منوی اصلی، پنجره مربوط به این برنامه باز شده و امکانات لازم جهت بازبینی اسناد موجود در سبد چاپ را در اختیار می‌گذارد. برای

دسترسی به اطلاعات بیشتر در این زمینه گزینه Preferences واقع در منوی Edit از پنجره این برنامه را انتخاب کنید. چنان‌چه قبلاً برای پیکربندی چاپگر اقدام کرده باشید، برنامه Print Manager امکان دسترسی به ابزار پیکربندی redhat-config-printer را در اختیار قرار خواهد داد. (برای اطلاع بیشتر درباره این ابزار به فصل بیست و پنجم مراجعه کنید.)



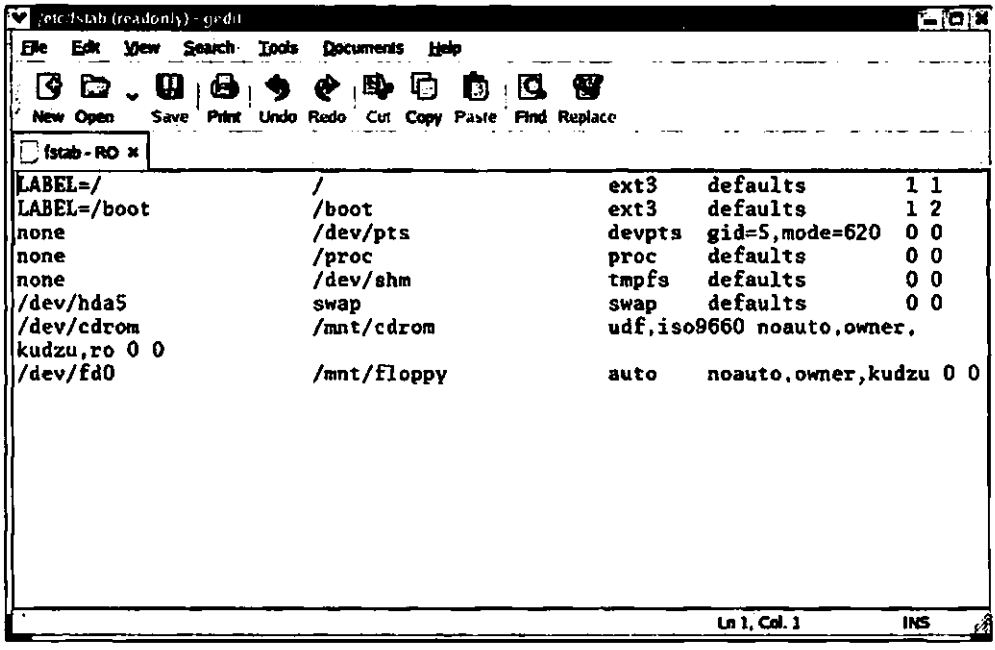
شکل ۳۲-۱۶ پنجره برنامه File Roller

برنامه Text Editor

با انتخاب گزینه Text Editor از منوی فرعی Accessories واقع در منوی اصلی، پنجره مربوط به برنامه ویرایشگر استاندارد محیط GNOME یعنی gedit باز می‌شود. این برنامه، به ویژه در مقایسه با ویرایشگر متنی vi دارای امکانات چشمگیری است. شکل ۳۳-۱۶ پنجره این برنامه را در حالی که فایل پیکربندی /etc/fstab در آن باز شده است، نشان می‌دهد.

برنامه gedit کاملاً قابل پیکربندی است. انتخاب گزینه Preferences از منوی Edit در این برنامه امکانات لازم برای پیکربندی آن‌را در اختیار قرار می‌دهد. به کمک این امکانات، علاوه بر تغییر فونت و رنگ مورد استفاده برای نمایش متون، می‌توان ترتیبی داد تا شماره هر خط در ابتدای آن درج شود.

تنظیمات دیگری نیز جهت تعیین نحوه چاپ اسناد و افزودن قابلیت‌های جدید از طریق نصب قطعه برنامه‌های کوچک (اصطلاحاً plug-ins) پیش‌بینی شده است.

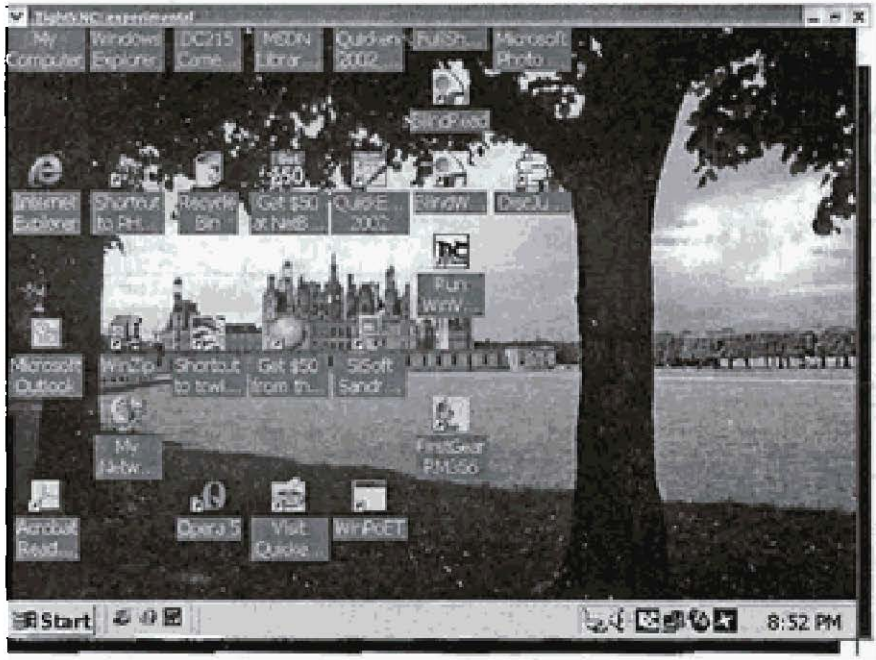


شکل ۳۳-۱۶ پنجره برنامه gedit

برنامه VNC Viewer

برنامه Virtual Network Computing یا به اختصار VNC یک برنامه client/server است که توسط شرکت AT&T طراحی شده است. برنامه مذکور امکان دسترسی از راه دور به سیستم‌عامل‌های دارای رابط گرافیکی را فراهم می‌کند. برنامه VNC Viewer که گزینه مربوط به آن در منوی فرعی More Accessories واقع شده، در حقیقت یک برنامه کلاینت است که به منظور استفاده از این قابلیت توسعه یافته است.

با کلیک روی گزینه مزبور پنجره کوچکی باز می‌شود. برای دسترسی به سرور VNC، کافی است آدرس IP و کلمه عبور معتبری را در این پنجره وارد کنید. شکل ۳۴-۱۶ نتیجه این اقدام را که جهت دسترسی به دسک‌تاپ کامپیوتری از نوع ویندوز 2000 انجام شده است، نشان می‌دهد.



شکل ۳۴-۱۶ برنامه VNC Viewer امکان دسترسی از راه دور به سایر سیستم‌عامل‌ها را فراهم می‌کند.

دسترسی به مستندات

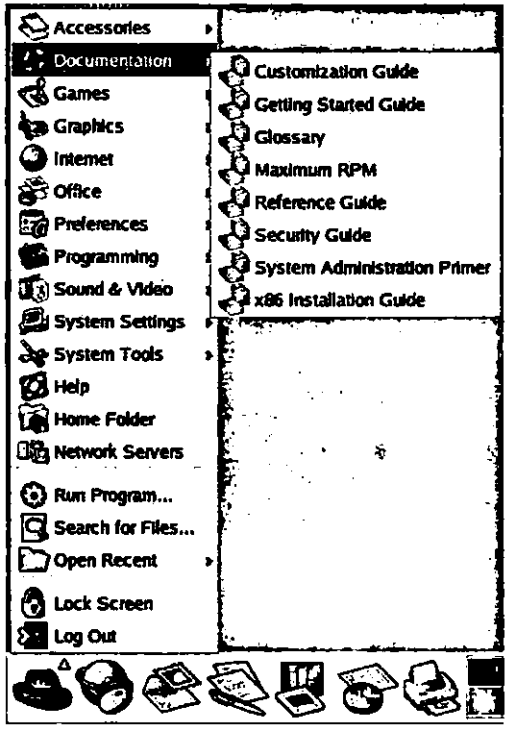
در صورتی که قبلاً بسته‌های نرم‌افزاری حاوی مستندات سیستم‌عامل Red Hat Linux را نصب کرده باشید، با انتخاب گزینه Documentation از منوی اصلی می‌توانید آن‌ها را مورد دستیابی قرار دهید. شکل ۳۵-۱۶ محتوای منوی Documentations را نشان می‌دهد.

با انتخاب یکی از گزینه‌های موجود در این منو مستندات مربوطه، در پنجره برنامه مرورگر پیش‌فرض باز می‌شود.

گروه Games

چنان‌چه قبلاً بسته‌های نرم‌افزاری حاوی بازی‌های استاندارد محیط گرافیکی GNOME یا KDE را نصب کرده باشید، از طریق منوی فرعی Games واقع در منوی اصلی می‌توانید آن‌ها را مورد دستیابی قرار دهید. عده‌ای بر این باور هستند که با این وجود بازی‌های کامپیوتری، رویکرد کاربران ویندوز به

Linux با اطمینان خاطر بیشتری همراه خواهد بود. با وجود این، در کتاب حاضر از پرداختن به مبحث بازی‌ها صرف‌نظر می‌کنیم.



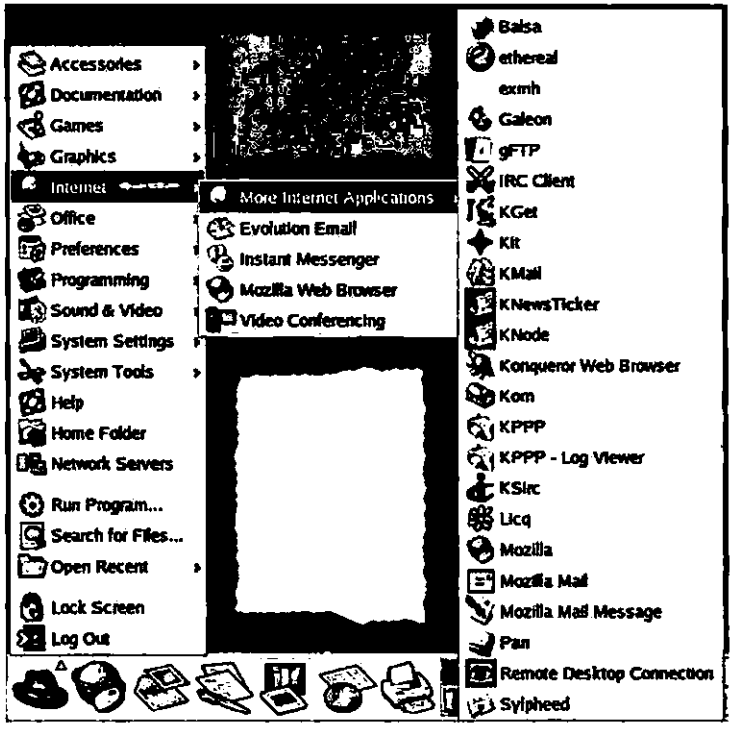
شکل ۳۵-۱۶ محتوای منوی Documentation

گروه Internet

محیط گرافیکی GNOME شامل ابزارها و برنامه‌های کاربردی متعددی در ارتباط با اینترنت است. در این مورد، تفاوت میان ابزارها و برنامه‌های کاربردی چندان مهم نیست. در قسمت "برنامه‌های کاربردی اینترنت" از این فصل به بررسی سه برنامه کاربردی مختلف از این گروه، شامل مرورگر Mozilla، برنامه مدیریت اطلاعات شخصی Evolution و یک برنامه ارسال سریع پیغام با عنوان Gaim را مورد بررسی قرار خواهیم داد.

در این قسمت به بررسی برنامه‌های کاربردی ساده‌تری مانند برنامه مورد استفاده جهت گپ‌زنی و چند ابزار مفید برای برقراری ارتباط با اینترنت می‌پردازیم. چنان‌که شکل ۳۶-۱۶ نیز نشان می‌دهد، دسترسی به برخی از این برنامه‌ها با انتخاب گزینه Internet از منوی اصلی و دسترسی به برخی دیگر با

انتخاب گزینه More Internet Applications از منوی فرعی Internet واقع در منوی اصلی امکان‌پذیر است. بررسی آن دسته از برنامه‌های کاربردی را که به طور خاص برای محیط گرافیکی KDE توسعه داده شده‌اند، در فصل بعد انجام خواهیم داد.



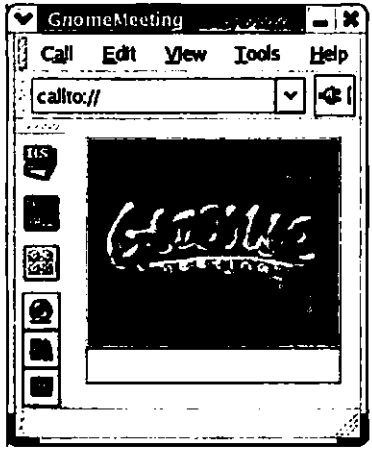
شکل ۳۶-۱۶ محتوای منوی Internet

برخی از این برنامه‌های کاربردی، از جمله Balsa و Ethereal کاملاً مستقل از پروژه GNOME و KDE هستند. از این‌رو، بررسی آن‌ها را در سایر فصل‌ها انجام خواهیم داد.

کنفرانس ویدیویی

برنامه کنفرانس ویدیویی GnomeMeeting با انتخاب گزینه Video Conferencing از منوی فرعی Internet واقع در منوی اصلی به اجرا درمی‌آید. این برنامه دارای تمام قابلیت‌های یک برنامه کنفرانس ویدیویی بوده و کاملاً مطابق با استاندارد H.323 است، به طوری که می‌توان آن‌را به سایر برنامه‌های مشابه‌ازجمله Microsoft NetMeeting متصل‌کرد. به‌منظوراستفاده‌ازقابلیت‌های‌برنامه GnomeMeeting

لازم است یک کارت صوتی و یک دوربین webcam روی کامپیوتر نصب کنید. شکل ۳۷-۱۶ پنجره این برنامه را نشان می‌دهد.

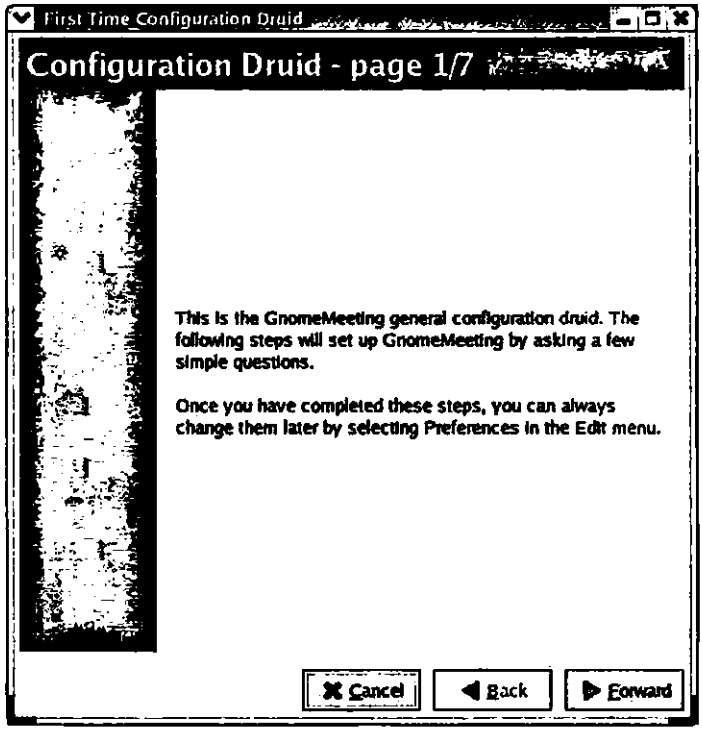


شکل ۳۷-۱۶ پنجره برنامه GnomeMetting

برای اطلاع از دوربین‌های webcam قابل استفاده در سیستم‌عامل Linux مستندات مربوطه در آدرس http://www.tldp.org/HOWTO/Hardware-HOWTO/other.html را مورد مطالعه قرار دهید. ضمناً مستندات http://www.dkfz.de/Macromol/wedemann/mini-HOWTO-cqcam.html نیز حاوی اطلاعات مفیدی در این زمینه است.

با اجرای برنامه GnomeMeeting برای نخستین بار، پنجره مربوط به ابزار پیکربندی آن با عنوان First Time Configuration Druid باز می‌شود. عموماً برای دستیابی به این ابزار، کافی است گزینه Configuration Druid را از منوی Edit برنامه مذکور انتخاب کنید. شکل ۳۸-۱۶ پنجره موردنظر را نشان می‌دهد.

به کمک ویزاردی که این پنجره در اختیار می‌گذارد، می‌توانید اطلاعات شناسایی خود، نحوه اتصال به اینترنت (مودم، ISDN یا DSL) و درایور تجهیزات صوتی و ویدیویی (کارت صوتی و دوربین webcam) را مشخص کنید. هم‌چنین پس از باز کردن یک حساب کاربری معتبر در وب سایت MicroTelco به آدرس اینترنتی http://www.microtelco.com، به کمک برنامه GnomeMeeting می‌توانید کامپیوتر خود را به شبکه تلفن متصل کنید. سایر تنظیمات را می‌توان با انتخاب گزینه Preferences از منوی Edit این برنامه انجام داد.

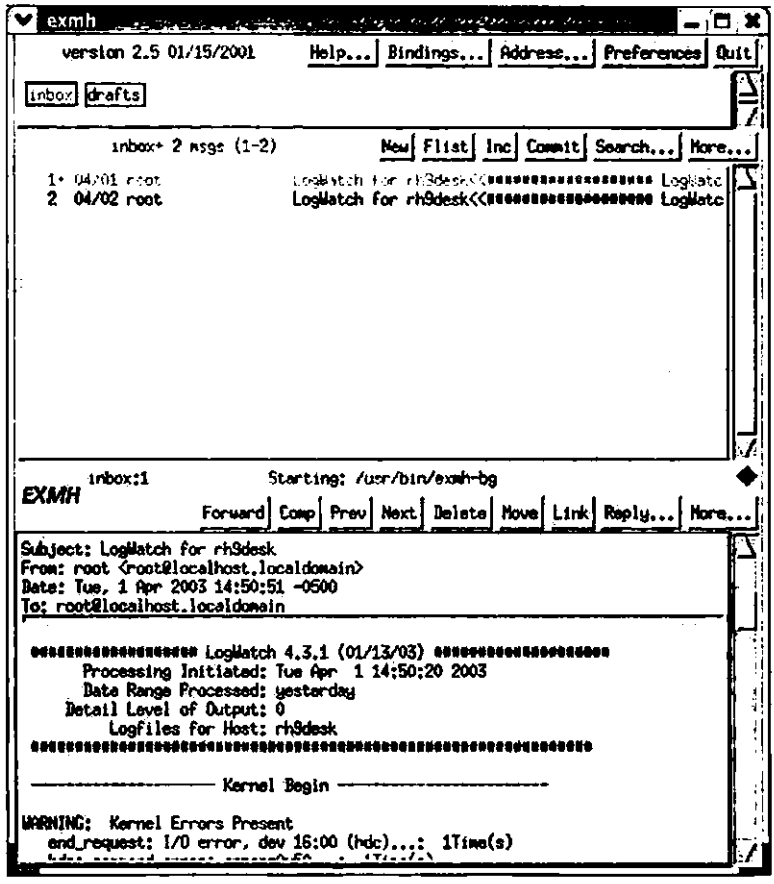


شکل ۳۸-۱۶ پنجره ابزار پیکربندی برنامه GnomeMeeting با عنوان Configuration Druid

برنامه exmh

برنامه exhm که از طریق منوی فرعی More Internet Applications قابل دستیابی است، به منظور مدیریت پیغام‌های الکترونیکی به سبک متداول در سیستم‌عامل UNIX طراحی شده است. چنان‌که در شکل ۳۹-۱۶ مشاهده می‌کنید، این برنامه دارای رابط گرافیکی بوده و تسهیلاتی را به منظور جستجوی پیغام موردنظر در میان پیغام‌های موجود در اختیار می‌گذارد. در صورت نصب و پیکربندی برنامه sendmail می‌توان پیغام‌های دریافتی را برای سایرین ارسال کرده یا به آن‌ها پاسخ داد. (برای اطلاع بیشتر درباره برنامه sendmail به فصل بیست و پنجم مراجعه کنید.)

با اجرای برنامه exhm برای نخستین بار، این برنامه وجود حساب کاربری معتبر را مورد بررسی قرار می‌دهد. در صورتی که چنین حسابی موجود نباشد، برنامه مذکور امکان ایجاد آن‌را از طریق ویزاردی که به همین منظور پیش‌بینی شده است، در اختیار کاربر قرار می‌دهد. حساب کاربری موردنظر در قالب فایلی با عنوان mh_profile. در فهرست خانگی کاربر ایجاد می‌شود.



شکل ۱۶-۳۹ پنجره برنامه exhm

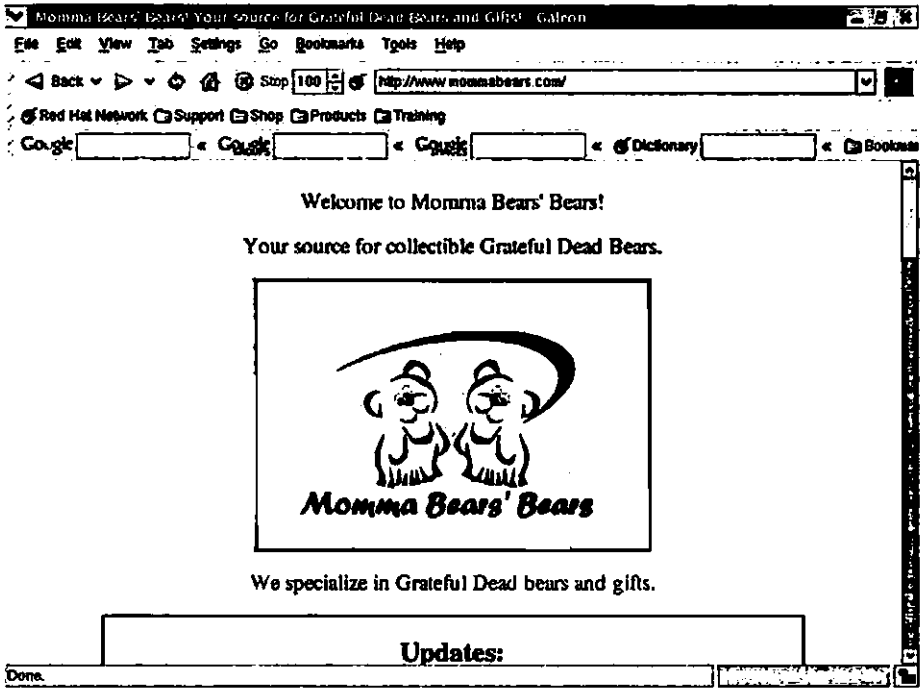
برنامه Galeon

برنامه Mozilla به عنوان مرورگر پیش‌فرض در سیستم‌عامل Red Hat Linux پیکربندی می‌شود. با وجود این، در صورت تمایل می‌توان مرورگر دیگری با عنوان Galeon را نیز که توسعه آن در قالب پروژه GNOME انجام شده است، مورد استفاده قرار داد. با اجرای برنامه Galeon برای نخستین بار، تنظیمات مربوط به نوار ابزارها، پروکسی و دروازه شبکه (در صورت وجود) به نمایش درآمده و امکان درج آدرس‌های bookmark مرورگر Netscape یا Mozilla در این مرورگر از طریق تنظیمات مربوطه فراهم می‌شود.

در صورت تمایل می‌توان این برنامه را به عنوان مرورگر پیش‌فرض جهت دسترسی به صفحات وب عادی و محافظت شده، سایت‌های FTP، مستندات محیط گرافیکی و برنامه‌های کاربردی GNOME و

بالاخره ابزار دسترسی به فایل‌های موجود در فهرست‌های محلی پیکربندی کرد. (دسترسی به صفحات عادی وب از طریق پروتکل HTTP و دسترسی به صفحات محافظت شده از طریق پروتکل HTTPS انجام می‌شود.)

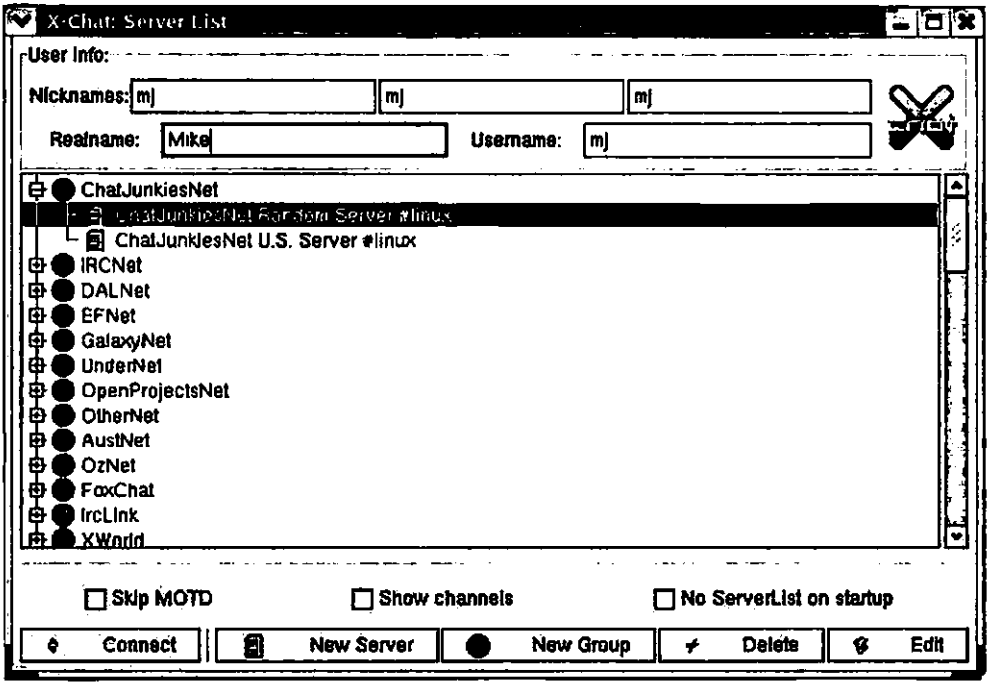
چنان‌که شکل ۴۰-۱۶ نشان می‌دهد، برنامه Galeon فاقد تسهیلات موجود در قاب سمت چپ مرورگر Mozilla است. با وجود این، عده‌ای از کاربران بر این باور هستند که رابط این برنامه نسبت به مرورگر Mozilla از کارآیی بیشتری برخوردار است. با انتخاب گزینه Preferences از منوی Edit تنظیمات دیگری برای پیکربندی در اختیار قرار می‌گیرد.



شکل ۴۰-۱۶ پنجره برنامه Galeon

برنامه X-Chat

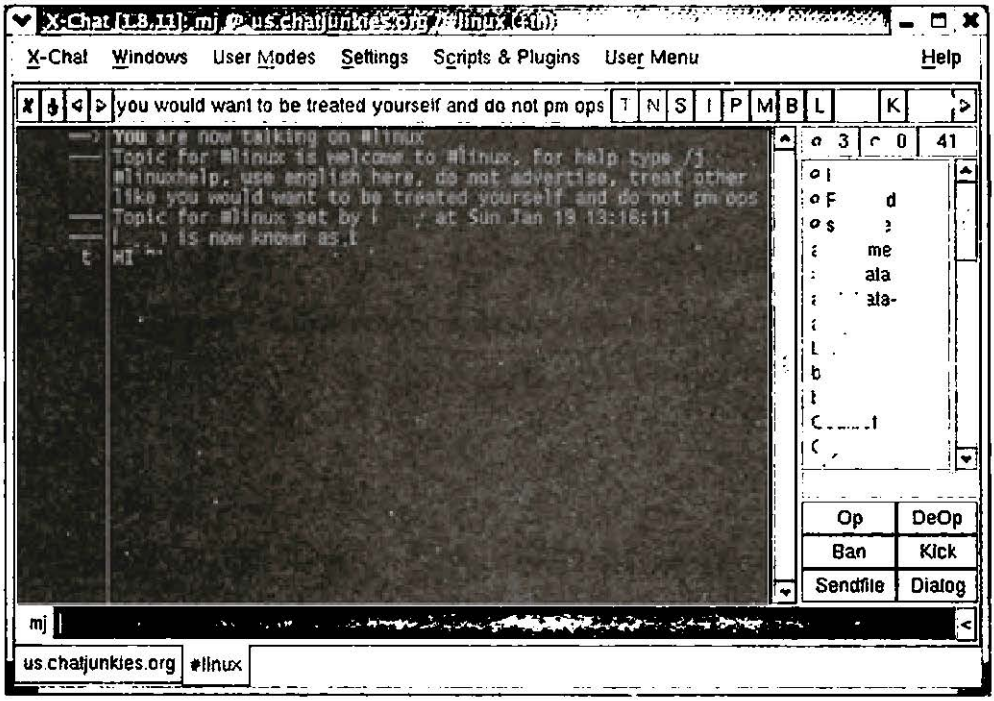
برنامه X-Chat نمونه‌ای از یک برنامه IRC یا اصطلاحاً Internet Relay Chat است که امکان دسترسی به انواع سرورهای گپ‌زنی را در اختیار می‌گذارد. برای اجرای این برنامه کافی است گزینه IRC Client از منوی فرعی More Internet Applications را انتخاب کنید. شکل ۴۱-۱۶ پنجره این برنامه را نشان می‌دهد.



شکل ۴۱-۱۶ پنجره برنامه X-Chat

برای پیکربندی یک سرور گپ‌زنی جدید روی دکمه New Server کلیک کنید. (برنامه‌های گپ‌زنی یا اصطلاحاً chat نمونه‌ای از برنامه‌های client/server هستند. برای استفاده از این قبیل برنامه‌ها ابتدا باید بخش سرور راه‌اندازی شود. بخش کلاینت درخواست‌هایی را به سرور ارسال کرده و سرور پاسخ‌های موردنظر را در اختیار آن‌ها قرار می‌دهد. منظور از سرور گپ‌زنی بخشی از یک برنامه client/server است که به درخواست‌های ارسالی از جانب برنامه‌های کلاینت پاسخ می‌دهد. برنامه X-Chat نمونه‌ای از این گونه برنامه‌های کلاینت است. ـ مترجم)

پس از پیکربندی برنامه X-Chat سرور موردنظر را انتخاب کرده و روی دکمه Connect کلیک کنید تا ارتباط لازم برقرار شود. چنان‌چه سرور موردنظر قبلاً راه‌اندازی شده و قابل دسترس باشد، پنجره گپ‌زنی مشابه شکل ۴۲-۱۶ باز می‌شود.

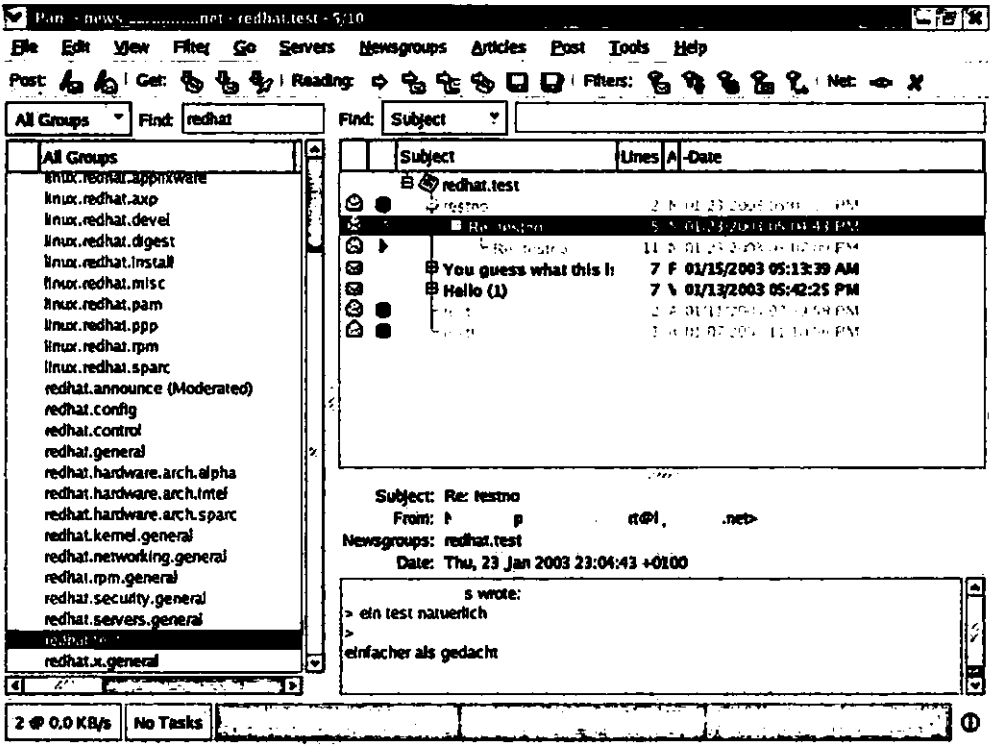


شکل ۴۲-۱۶ پنجره گپزنی برنامه X-Chat

برنامه Pan

برنامه Pan نمونه‌ای از یک برنامه newsreader است. این گونه برنامه‌ها امکانات لازم برای خواندن اخبار منتشر شده از جانب گروه‌های خبری (اصطلاحاً newsgroups) را در اختیار کاربران قرار می‌دهند. چنان‌که شکل ۴۳-۱۶ نشان می‌دهد، به کمک رابط گرافیکی این برنامه به راحتی می‌توان چنین پیغام‌هایی را خواند و در صورت تمایل به آن‌ها پاسخ داد.

هنگام اجرای برنامه Pan برای نخستین بار، اعلانی برای دریافت اطلاعات موردنیاز این برنامه شامل آدرس پست الکترونیکی، آدرس کامپیوتر میزبان سرور SMTP و نام کامپیوتر میزبان سرور خبری یا اصطلاحاً news server به نمایش درمی‌آید. چنان‌چه قبلاً برنامه sendmail را روی کامپیوتر میزبان نصب و پیکربندی کرده باشید، به عنوان آدرس کامپیوتر میزبان سرورSMTP می‌توانید شاخص localhost را در مقابل اعلان مربوطه وارد کنید. در غیر این صورت، باید از آدرس کامپیوتری که وظیفه ارسال پیغام‌های الکترونیکی را به عهده دارد، مطلع باشید. (برای اطلاع از این موضوع با تأمین کننده خدمات اینترنت طرف قرارداد خود مشورت کنید.)



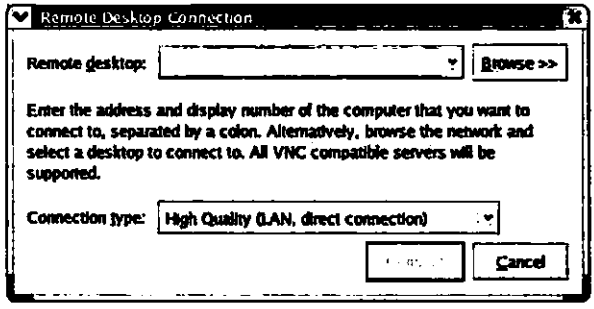
شکل ۴۳-۱۶ پنجره برنامه Pan

برای تغییر پروفایل ضمیمه شده به پاسخ‌های ارسالی گزینه Posting Profiles و برای اضافه کردن یک سرور خبری جدید به لیست سرورهای خبری موجود گزینه News Servers را از منوی Tools انتخاب کنید.

برنامه Remote Desktop Connection

در صورت دسترسی به یک سرور VNC، با استفاده از برنامه Remote Desktop Connection می‌توانید برای ارتباط با آن اقدام کنید. دسترسی به این برنامه از طریق منوی فرعی More Internet Applications امکان‌پذیر است. شکل ۴۴-۱۶ امکانات برنامه مذکور را نشان می‌دهد.

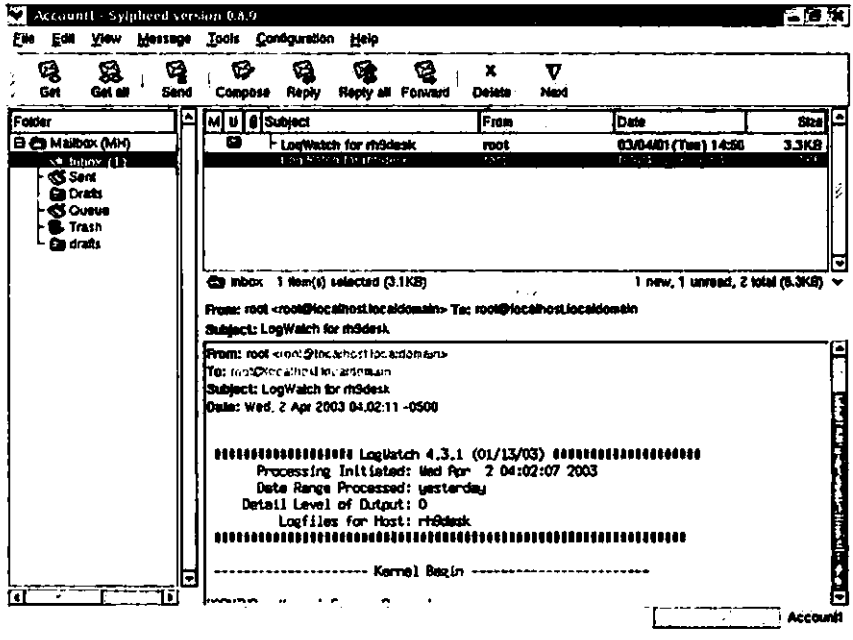
مزیت استفاده از این برنامه، قابلیت نمایش آن به صورت تمام صفحه (اصطلاحاً full-screen) است. صرف نظر از برچسب کوچک موجود در بالای صفحه، نتیجه حاصل کاملاً مشابه دسک‌تاپ کامپیوتر مورد نظر، یعنی کامپیوتر میزبان سرور VNC خواهد بود.



شکل ۴۴-۱۶ پنجره برنامه Remote Desktop Connection

برنامه Sylpheed

برنامه Sylpheed نمونه‌ای از یک برنامه کلاینت است که جهت بهره‌برداری از سرویس پست الکترونیکی توسعه یافته است. این برنامه با استفاده از ابزار توسعه برنامه‌های کاربردی GNOME (یعنی GTK+) و در کشور ژاپن توسعه یافته است. از این‌رو، می‌توان انتظار داشت که پشتیبانی خوبی از زبان ژاپنی به عمل آورد. برنامه Sylpheed در نوع خود بسیار کارآمد است و بدون مصرف بی‌رویه منابع سیستمی به خوبی از عهده مدیریت پیغام‌های الکترونیکی برمی‌آید. شکل ۴۵-۱۶ پنجره این برنامه را نشان می‌دهد.



شکل ۴۵-۱۶ پنجره برنامه Sylpheed

پیکربندی این برنامه نیز بسیار ساده است. مجموعه‌ای از گزینه‌های موردنیاز برای این منظور در منوی Configuration پیش‌بینی شده است. جدول ۳-۱۶ عملکرد این گزینه‌ها را شرح می‌دهد.

جدول ۳-۱۶ شرح عملکرد گزینه‌های موجود در منوی Configuration

عنوان گزینه	توضیح
Common Preferences	این گزینه امکان انجام تنظیمات‌عمومی برنامه، از جمله تعیین موقعیت فهرست‌ها، پیکربندی رابط گرافیکی برنامه، تعیین موارد پیش‌فرض در پاسخ‌های ارسالی، تعیین دوره زمانی سرکشی به صندوق پستی جهت بازیابی پیغام‌های دریافتی و موارد دیگری از این قبیل را در اختیار می‌گذارد.
Filter Setting	این گزینه امکان تعیین مشخصات پیغام‌های ناخواسته و پیغام‌هایی‌را که پس از دریافت باید برای سایرین ارسال شوند، در اختیار قرار می‌دهد.
Templates	این گزینه امکان پیکربندی الگوهای عمومی مورد استفاده برای ارسال پاسخ پیغام‌های دریافتی را در اختیار قرار می‌دهد.
Actions	این گزینه امکان اجرای فرامین خاصی را در مورد پیغام‌هایی با ویژگی مشخص در اختیار می‌گذارد. (برای مثال، با استفاده از این امکانات می‌توان پیغام‌هایی را که دارای ویژگی خاصی هستند، رمزگشایی کرد.)
Preferences For Current Account	این گزینه امکان پیکربندی برنامه را برای کاربر پیش‌فرض در اختیار می‌گذارد.
Create New Account	این گزینه امکانات لازم برای تعریف حساب کاربری جدید را در اختیار می‌گذارد.
Edit Accounts	این گزینه امکان ویرایش حساب کاربری موردنظر را در اختیار می‌گذارد.
Change Current Account	این گزینه امکان تغییر حساب کاربری پیش‌فرض را در اختیار قرار می‌دهد.

برنامه‌های کاربردی اینترنت

در این قسمت سه برنامه کاربردی متداول در زمینه اینترنت، شامل یک مرورگر وب با عنوان Mozilla، یک برنامه مدیریت اطلاعات شخصی با عنوان Evolutions و یک برنامه ارسال سریع پیغام با عنوان Gaim را که درنوع خود از برنامه‌های پیش‌فرض سیستم‌عامل Red Hat Linux محسوب می‌شوند، مورد بررسی قرارمی‌دهیم. دسترسی به این برنامه‌ها به ترتیب با انتخاب گزینه‌های Mozilla Web Browser، Evolution Email و Instant Messenger از منوی فرعی Internet امکان‌پذیر است.

برنامه Mozilla

برنامه Mozilla مرورگر وب پیش‌فرض در سیستم‌عامل Red Hat Linux است. این برنامه شامل انبوهی از ویژگی‌ها و قابلیت‌های چشمگیر بوده و بر اساس کد منبع مرورگر Netscape که در سال ۱۹۹۸ از جانب شرکت مربوطه منتشر شد توسعه یافته و پیاده‌سازی شده است. به کمک آیکن‌های موجود در قسمت پایین سمت چپ از پنجره این برنامه می‌توان از قابلیت‌های مختلف آن استفاده کرد. شکل ۴۶-۱۶ این آیکن‌ها را نشان می‌دهد.

شکل ۴۶-۱۶ آیکن‌های مرورگر Mozilla

این آیکن‌ها از چپ به راست جهت دسترسی به نمونه جدیدی از پنجره مرورگر وب، ابزار مدیریت پیغام‌های الکترونیکی و دسترسی به گروه‌های خبری، ابزار ایجاد اسناد وب، کتاب آدرس (اصطلاحاً address book) و برنامه گپ‌زنی پیش‌بینی شده‌اند.

روش دیگر انتخاب هریک از این گزینه‌ها و ترکیب کلید کنترلی Ctrl با کلیدهای عددی 1 تا 5 است. جدول ۴-۱۶ این موضوع را شرح می‌دهد.

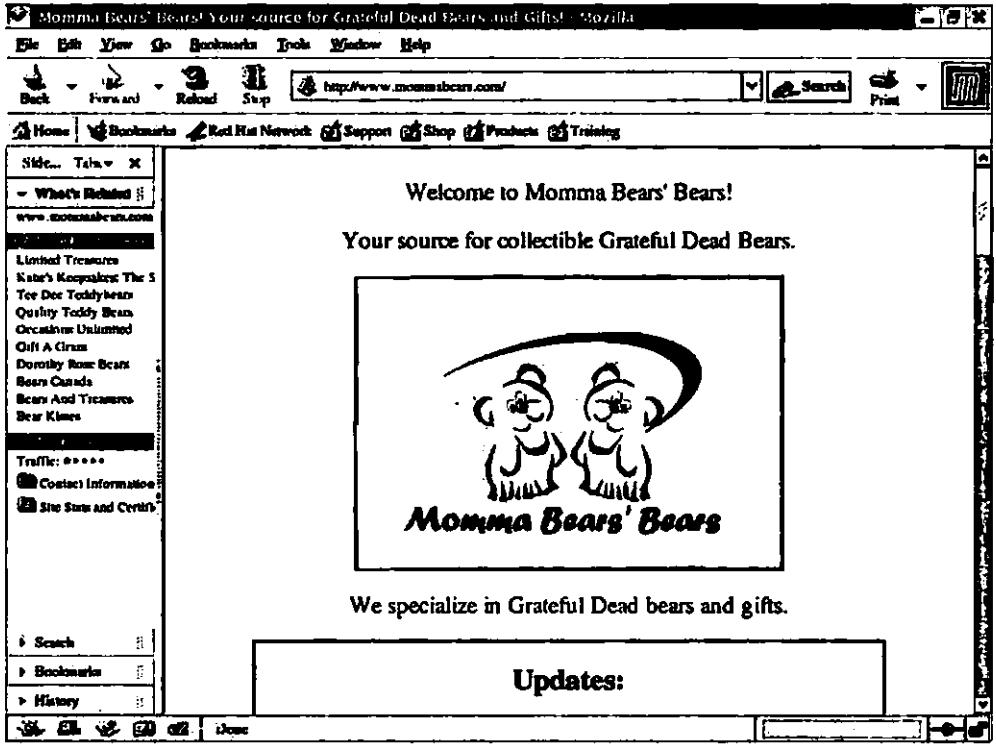
جدول ۴-۱۶ ترکیب کلید کنترلی Ctrl معادل با آیکن‌های مرورگر Mozilla

ترکیب کلیدها	توضیح
Ctrl+1	این ترکیب، نمونه جدیدی از پنجره مرورگر Mozilla را باز می‌کند.
Ctrl+2	این ترکیب، امکانات لازم برای مدیریت پیغام‌های الکترونیکی و دسترسی به گروه‌های خبری را از طریق برنامه Mozilla Mail And Newsgroup Reader در اختیار می‌گذارد.
Ctrl+3	این ترکیب، امکان گپ‌زنی با سایر کاربران را از طریق برنامه ChatZilla! مهیا می‌کند.
Ctrl+4	این ترکیب، امکان ایجاد اسناد وب را از طریق برنامه Mozilla Composer در اختیار می‌گذارد.
Ctrl+5	این ترکیب، امکان دسترسی به کتاب آدرس را از طریق برنامه Mozilla Address Book فراهم می‌کند.

هنگامی که مارک اندرسن مشغول توسعه مرورگر Netscape بود، مرورگر Mozaic در عرصه وب رقیب نداشت. وی اغلب برای اشاره به این مرورگر از اصطلاح "Mozaic Godzilla" استفاده می‌کرد. ترکیب دو واژه Mozaic و Godzilla به صورت Mozilla بعدها عنوان پروژه‌ای شد که نتیجه آن مرورگر Mozilla است.

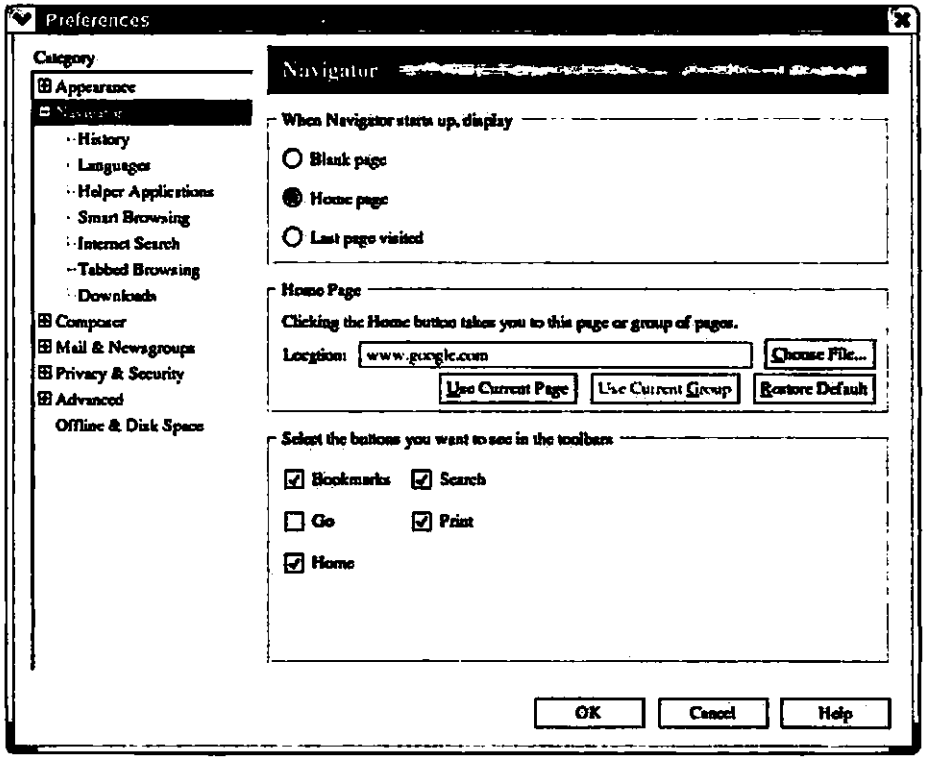
مرورگر Mozilla

چنان‌که در شکل ۴۷-۱۶ مشاهده می‌کنید، مرورگر Mozilla بسیار شبیه به مرورگر Netscape است. به ویژه نوار کناری با عنوان What's Related به همین شکل در مرورگر Netscape نیز وجود دارد.



شکل ۴۷-۱۶ پنجره مرورگر Mozilla

با انتخاب گزینه Preferences از منوی Edit امکانات پیکربندی مرورگر Mozilla از طریق پنجره‌ای با عنوان Preferences در اختیار قرار می‌گیرد. شکل ۴۸-۱۶ این پنجره را نشان می‌دهد. حتی تنظیمات مرورگر Mozilla نیز شبیه به تنظیمات مرورگر Netscape است.



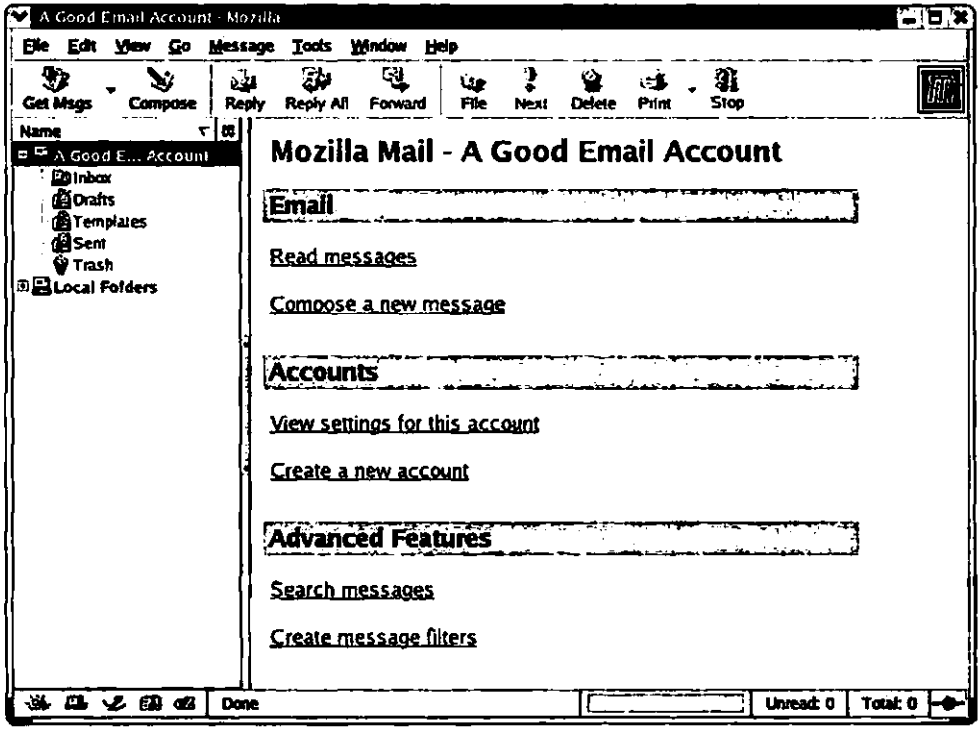
شکل ۴۸-۱۶ پنجره حاوی امکانات پیکربندی مرورگر Mozilla

برنامه Mozilla Mail And Newsgroup Reader

با دسترسی به برنامه Mozilla Mail And Newsgroup Reader برای نخستین بار، امکانات مربوط به تعریف حساب کاربری برای استفاده از سرویس پست الکترونیکی و دسترسی به گروه‌های خبری در اختیار قرار می‌گیرد. در صورت لزوم، با انتخاب گزینه Mail And Newsgroup Account Settings از منوی Edit و کلیک روی دکمه Add Account، می‌توانید برای تعریف حساب‌های کاربری متعدد اقدام کنید.

هنگام تعریف حساب کاربری موردنظر برای استفاده از سرویس پست الکترونیکی لازم است نام، آدرس پست الکترونیکی، آدرس سرور POP یا IMP (جهت دریافت پیغام‌ها) و آدرس سرور SMTP (به منظور ارسال پیغام‌ها) را مشخص کنید. برای اطلاع از این مشخصات با تأمین کننده خدمات اینترنت طرف قرارداد خود مشورت کنید. هم‌چنین برای اطلاع بیشتر درباره پروتکل‌های نامبرده به فصل بیست و ششم مراجعه کنید.

شکل ۴۹-۱۶ پنجره این برنامه را که شامل امکاناتی برای بازخوانی پیغام‌های دریافتی، نگارش پیغام جدید و سایر موارد است، نشان می‌دهد.

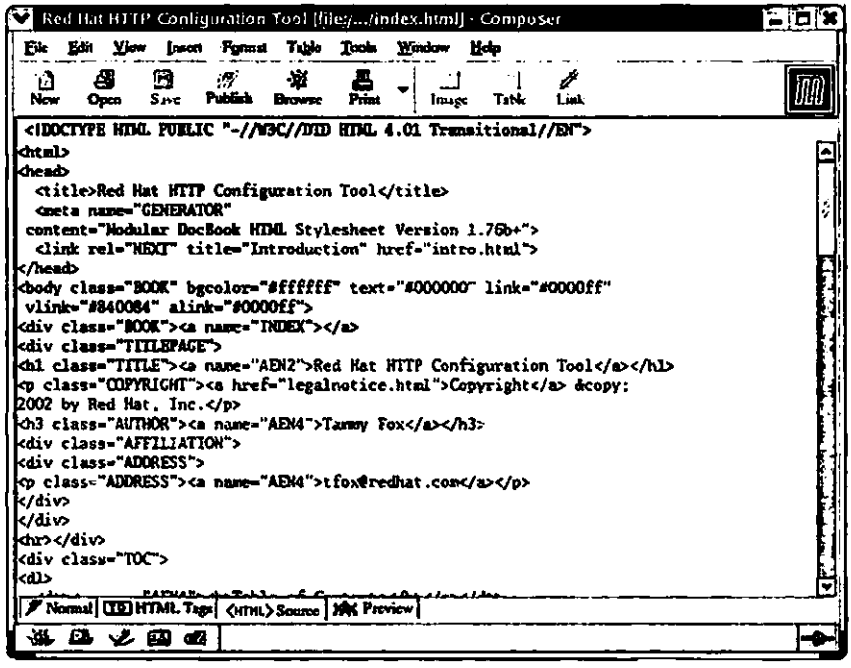


شکل ۴۹-۱۶ پنجره برنامه Mozilla Mail And Newsgroup Reader

برنامه Mozilla Composer

برنامه Mozilla Composer ابزاری برای ایجاد و ویرایش اسناد وب است. شکل ۵۰-۱۶ پنجره این برنامه را در حال نمایش کد منبع یکی از فایل‌های ابزار پیکربندی redhat-config-utility نشان می‌دهد.

در صورت لزوم، با انتخاب گزینه مناسب می‌توان اسناد وب را در نمای عادی، به همراه برچسب‌های HTML و آن‌گونه که در مرورگرهای وب به نمایش درمی‌آید، مشاهده کرد. هم‌چنین با انتخاب گزینه مربوطه می‌توان کد منبع اسناد وب را مشاهده کرد.



شکل ۱۶-۵۰ پنجره برنامه Mozilla Composer

برنامه Mozilla Address Book

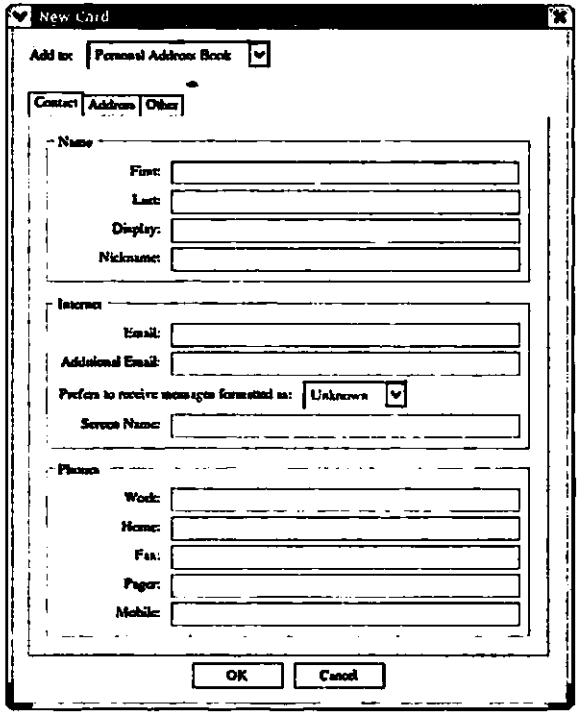
برنامه Mozilla Address Book حاوی امکاناتی به منظور مدیریت اطلاعات اشخاص موردنظر است. شکل ۱۶-۵۱ پنجره مربوط به درج این اطلاعات را نشان می‌دهد.

برنامه ChatZilla!

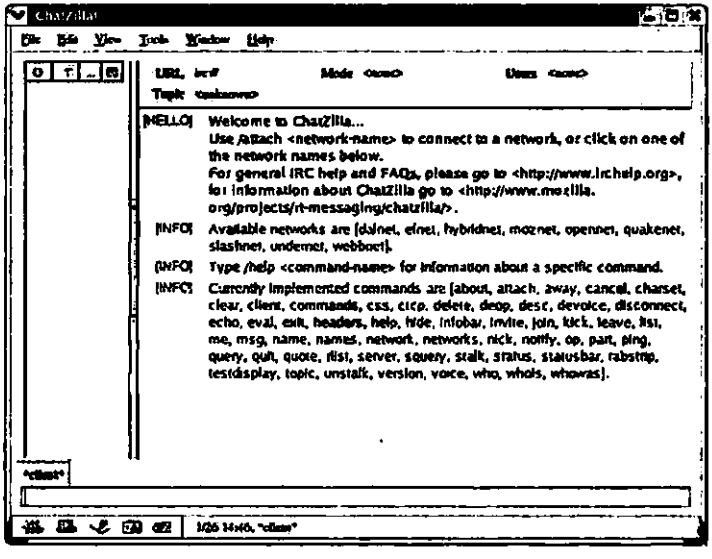
برنامه ChatZilla! نمونه‌ای از یک برنامه کلاینت است که به منظور گپ‌زنی با سایر کاربران طراحی شده است. شکل ۱۶-۵۲ پنجره این برنامه را نشان می‌دهد.

برای دسترسی به سرور IRC موردنظر (هم‌چون undernet) کافی است، روی پیوند مربوطه کلیک کنید. (کلیه پیوندها در پنجره این برنامه با رنگ آبی مشخص شده‌اند.) پس از برقراری ارتباط لازم با سرور می‌توانید به اتاق گپ‌زنی دلخواه خود وارد شوید. برای مثال، جهت ورود به اتاق گپ‌زنی phoenix کافی است این فرمان را تایپ کنید:

```
/join #phoenix
```

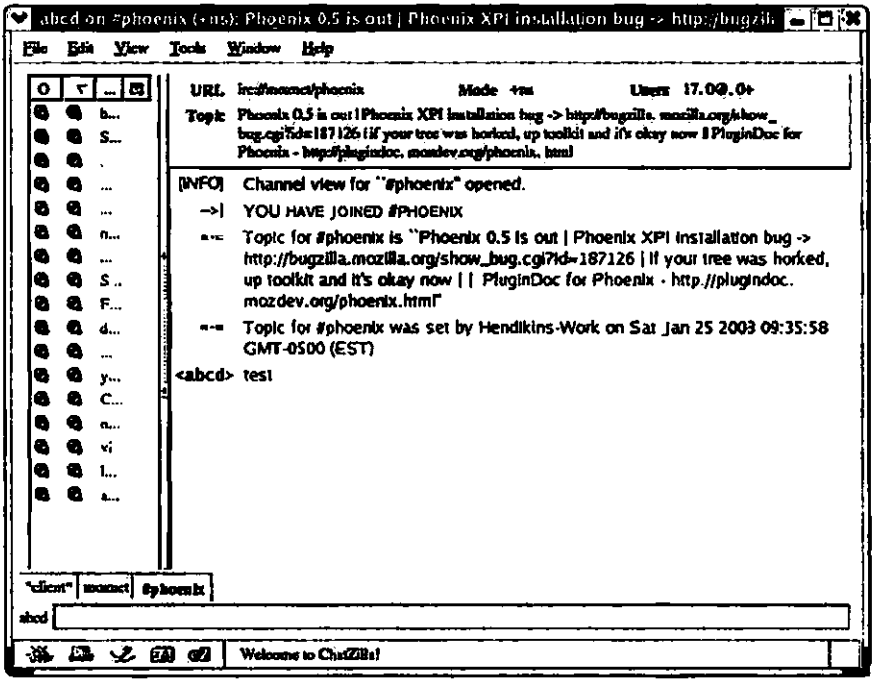


شکل ۱۶-۵۱ درج اطلاعات اشخاص موردنظر در برنامه Mozilla Address Book از طریق پنجره New Card انجام می‌شود.



شکل ۱۶-۵۲ پنجره برنامه ChatZilla!

چنان‌چه این اقدام موفقیت‌آمیز باشد، پنجره‌ای مشابه شکل ۵۳-۱۶ را مشاهده خواهید کرد. در این صورت می‌توانید با اشخاص موجود در آن اتاق گپ بزنید.



شکل ۵۳-۱۶ گپ‌زنی در اتاق موردنظر با استفاده از برنامه ChatZilla!

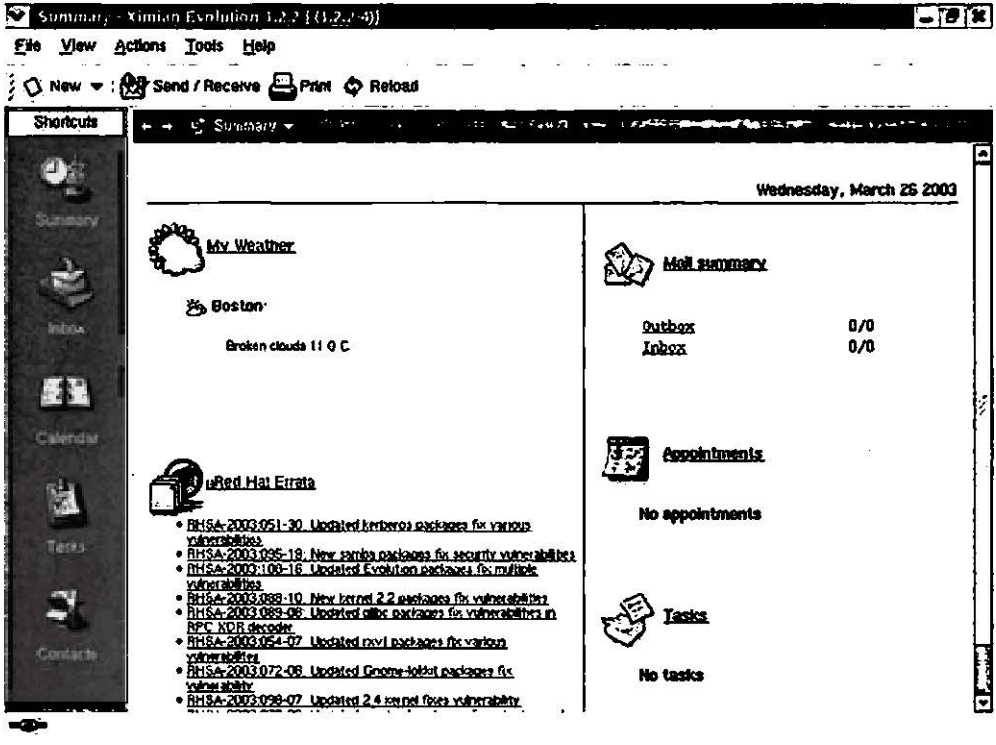
چنان‌چه دسترسی به سرور IRC موفقیت‌آمیز نباشد، ممکن است کانال ارتباطی میان برنامه کلاینت و سرور که همان پورت شماره ۶۶۶۷ است، به واسطه تنظیمات مکانیزم بازدارنده دیوار آتش مسدود شده باشد. در این صورت با در اختیار داشتن مجوزهای لازم و استفاده از فرمان iptables می‌توانید این کانال ارتباطی را به منظور برقراری ارتباط، مجدداً مهیا کنید. (برای اطلاع بیشتر درباره نحوه تنظیمات مکانیزم مذکور و قابلیت‌های فرمان iptables به فصل بیست و دوم مراجعه کنید.)

برنامه Evolution

این‌برنامه باانتخاب‌گزینه Evolution Email از منوی‌فرعی Internet قابل دستیابی است. علیرغم عنوان گزینه مذکور، قابلیت‌های این برنامه فراتر از مدیریت پیغام‌های الکترونیکی است، به طوری که می‌توان آن‌را مانند برنامه Microsoft Outlook جهت مدیریت اطلاعات شخصی نیز مورد استفاده قرار داد.

با اجرای این برنامه برای نخستین بار، امکانات لازم برای پیکربندی به نمایش درمی‌آید. برنامه Evolution به خوبی قادر است با سرویس‌های استانداردی مانند POP و IMAP ارتباط برقرار کند. برنامه Evolution هم‌چنین اعلانی را جهت تعیین ناحیه زمانی کامپیوتر میزبان در اختیار می‌گذارد. علاوه بر این، اعلان دیگری را نیز جهت ورود اطلاعات کتاب آدرس از سایر برنامه‌ها به این برنامه نمایش می‌دهد.

شکل ۵۴-۱۶ پنجره برنامه Evolution را در حال نمایش وضعیت هوای محلی، جعبه پستی، قرارهای ملاقات و لیست وظایف نشان می‌دهد. یکی از قابلیت‌های ارزشمند این برنامه (به ویژه برای مدیران سیستم‌ها) نمایش لیستی تحت عنوان Red Hat Errata است. با کلیک روی پیوندهای موجود در این لیست می‌توان نقاط ضعف شناخته شده سیستم‌عامل و برنامه‌های کاربردی را اصلاح کرد.



شکل ۵۴-۱۶ پنجره برنامه Evolution

برنامه Evolution محصول شرکت Ximian است. در دنیای سیستم‌عامل Linux این شرکت نقش مهمی در توسعه برنامه‌های کاربردی با رابط گرافیکی ایفا می‌کند. یکی از پروژه‌های شرکت Ximian

پیاده‌سازی نسخه کد باز نرم‌افزار .NET Microsoft برای محیط Linux است. جهت اطلاع از فعالیت‌های این شرکت به وب سایت مربوطه در آدرس http://www.ximian.com مراجعه کنید.

برنامه Gaim

برنامه Gaim جهت ارسال سریع پیغام به سایر کاربران طراحی شده است. (به چنین برنامه‌هایی اصطلاحاً instant messenger گفته می‌شود.) این برنامه کلاینت به خوبی قادر است با سرورهای America Online (به اختصار AOL)، Yahoo! و Microsoft Network (به اختصار MSN) ارتباط برقرار کند. عنوان این برنامه یعنی Gaim از عبارت a GNU version of some popular IM program برگرفته شده است. در واقع عنوان مذکور حق مطلب را چنان که باید در مورد این برنامه ادا نمی‌کند، چرا که برخلاف برنامه‌های مشابه، برنامه Gaim به واسطه ماجول‌های خاصی که در حقیقت نقش تطبیق دهنده را ایفا می‌کنند، می‌تواند با انواع مختلفی از سرورها ارتباط برقرار کرده و به این ترتیب امکان ارسال سریع پیغام از طریق آن سرورها را در اختیار کاربران قرار دهد. شکل ۵۵-۱۶ پنجره Gaim - Login را از این برنامه نشان می‌دهد.

شکل ۵۵-۱۶ پنجره Gaim - Login

جهت دسترسی به سرور موردنظر باید ماجول مربوطه را بارگذاری کنید. برای این منظور، روی دکمه Plugins کلیک کنید تا پنجره‌ای با عنوان Gaim - Plugins باز شود. روی دکمه Load از پنجره مذکور کلیک کنید تا لیست ماجول‌های موجود در فهرست /usr/lib/gaim به نمایش درآید. جدول ۵-۱۶ برخی از متداول‌ترین ماجول‌ها را شرح می‌دهد.

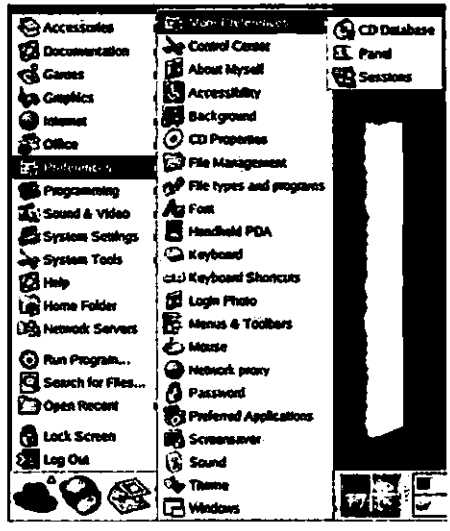
جدول ۵-۱۶ شرح برخی از ماجول‌های برنامه Gaim

عنوان ماجول	توضیح
libicq.so	این ماجول جهت دسترسی به شبکه ICQ طراحی شده است.
libirc.so	این ماجول جهت دسترسی به شبکه IRC طراحی شده است.
libmsn.so	این ماجول جهت دسترسی به شبکه MSN طراحی شده است.
libyahoo.so	این ماجول جهت دسترسی به شبکه Yahoo! طراحی شده است.

برای اطلاع درباره نحوه ثبت نام در این شبکه‌ها به وب سایت مربوطه مراجعه کنید. مقدار فیلد متنی Screen Name با توجه به حساب کاربری تعیین می‌شود. نام مستعار یا اصطلاحاً alias شناسه کاربر در محیط گپ‌زنی است.

گروه Preferences

بیشتر ابزارهایی را که از طریق منوی فرعی Preferences قابل دستیابی هستند، قبلاً در قسمت "مرکز کنترل محیط گرافیکی GNOME" از این فصل مورد بررسی قرار دادیم. در این قسمت به بررسی ابزارهایی می‌پردازیم که گزینه مربوط به آن‌ها از طریق منوی فرعی More Preferences واقع در منوی فرعی Preferences از منوی اصلی قابل‌دستیابی است. شکل ۵۶-۱۶ محتوای منوی فرعی Preferences را نشان می‌دهد.



شکل ۵۶-۱۶ محتوای منوی فرعی Preferences

ابزار CD Database

یکی از روش‌های متداول برای اطلاع از CDهای موسیقی، دسترسی به سرورهایی است که امکان جستجو در بانک‌های اطلاعاتی خاصی تحت عنوان CD Database (به اختصار CDDB) را در اختیار قرار می‌دهند. با انتخاب گزینه CD Database از منوی فرعی More Preferences پنجره حاوی تنظیمات لازم، جهت دسترسی به این سرورها با عنوان CD Database Preferences باز می‌شود. دسترسی به برخی از این سرورها از طریق مراجعه به وب سایت http://www.freedb.org امکان‌پذیر است. برای اطلاع بیشتر درباره ابزار CD Database به وب سایت مربوطه در آدرس اینترنتی http://www.gracenote.com مراجعه کنید.

ابزار Panel

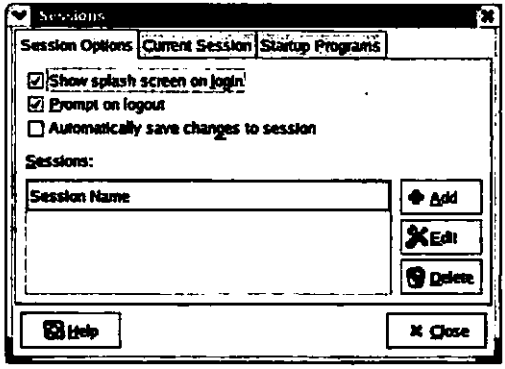
پنجره ابزار Panel با عنوان Panel Preferences، حاوی تنظیماتی برای تعیین نحوه عملکرد پانل محیط گرافیکی GNOME و مؤلفه‌های موجود در آن است. دکمه منوی اصلی، نمونه‌ای از این مؤلفه‌هاست که امکان دسترسی به برنامه‌های کاربردی و گزینه‌های مختلف را در اختیار قرار می‌دهد.

ابزار Sessions

پنجره ابزار Sessions حاوی تنظیماتی است که امکان راه‌اندازی برنامه‌های کاربردی موردنظر را ضمن ورود به محیط گرافیکی GNOME در اختیار می‌گذارد. به کمک این تنظیمات هم‌چنین می‌توان برخی از رفتارها (از جمله نمایش صفحه خوش‌آمدگویی یا اصطلاحاً splash screen) را ضمن ورود به محیط گرافیکی مذکور و خروج از آن پیکربندی کرد. علاوه بر این، پنجره مزبور لیست برنامه‌های در حال اجرا در محیط گرافیکی GNOME را نشان می‌دهد.چنان‌که در شکل ۵۷-۱۶ مشاهده می‌کنید، این پنجره از سه بخش مختلف تشکیل شده است. جدول ۶-۱۶ به طور خلاصه امکانات موجود در هر بخش را توضیح می‌دهد.

جدول ۶-۱۶ شرح بخش‌های مختلف پنجره ابزار Sessions

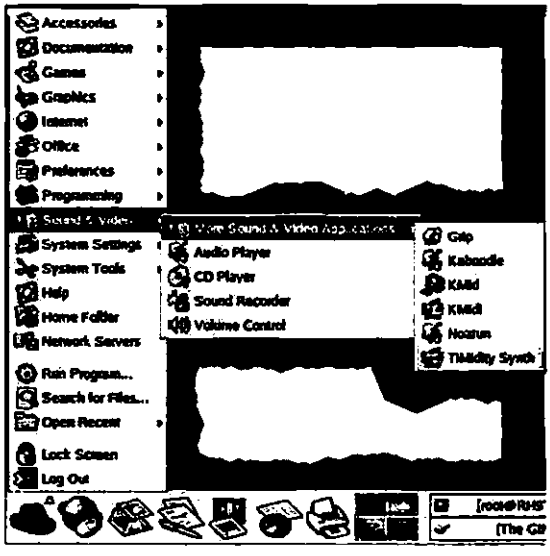
عنوان بخش	توضیح
Session Options	تنظیمات موجود در این بخش امکان پیکربندی رفتارهای خاصی را ضمن ورود به محیط گرافیکی GNOME و خروج از آن در اختیار می‌گذارد.
Current Sessions	این بخش حاوی لیست برنامه‌های در حال اجرا در محیط گرافیکی GNOME است.
Startup Programs	این بخش حاوی اسامی برنامه‌هایی است که ضمن ورود به محیط گرافیکی GNOME به اجرا درمی‌آیند.



شکل ۵۷-۱۶ پنجره ابزار Sessions

برنامه‌های کاربردی چندرسانه‌ای

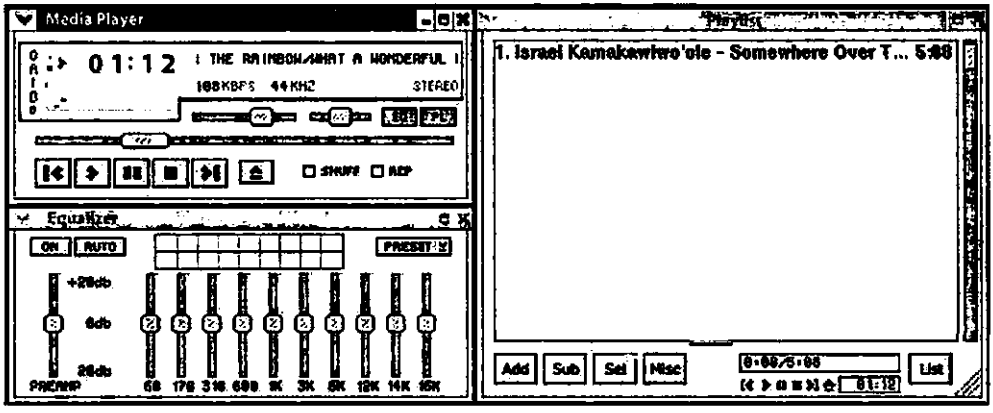
محیط گرافیکی GNOME حاوی تعدادی برنامه کاربردی چندرسانه‌ای شامل برنامه‌هایی برای پخش CD صوتی و تصویری و ابزارهای کنترل صداست. امکان دسترسی به این برنامه‌ها از طریق منوی فرعی Sound & Video واقع در منوی اصلی فراهم شده است. چنان‌که در شکل ۵۸-۱۶ مشاهده می‌کنید، منوی فرعی More Sound & Video Applications نیز حاوی تعدادی برنامه کاربردی چندرسانی است که در اصل برای محیط گرافیکی KDE طراحی شده‌اند. بررسی این برنامه‌ها را به فصل هفدهم موکول می‌کنیم.



شکل ۵۸-۱۶ محتوای منوی فرعی Sound & Video

برنامه Audio Player

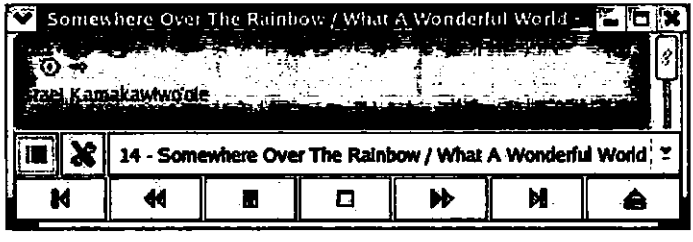
برنامه Audio Player نوعی سیستم چندرسانه‌ای است که به منظور اجرا در محیط‌های گرافیکی طراحی شده است. (به چنین برنامه‌هایی اصطلاحاً X Multimedia System یا به اختصار XMMS گفته می‌شود.) علیرغم ظاهر ساده برنامه مذکور، این برنامه امکاناتی را به منظور ترکیب صداهای مختلف با یکدیگر در اختیار می‌گذارد. از این‌رو می‌توان آن‌را یک استودیوی صوتی مجازی ساده محسوب کرد. شکل ۵۹-۱۶ پنجره این برنامه را با عنوان Media Player نشان می‌دهد.



شکل ۵۹-۱۶ پنجره برنامه Audio Player

برنامه CD Player

برنامه CD Player ابزار ساده‌ای برای پخش CDهای صوتی است. چنان‌که در شکل ۶۰-۱۶ مشاهده می‌کنید، پنجره این برنامه شامل دکمه‌های استاندارد موردنیاز برای پخش موزیک ضبط شده روی شیار جاری و شیارهای قبلی و بعدی است.



شکل ۶۰-۱۶ پنجره برنامه CD Player

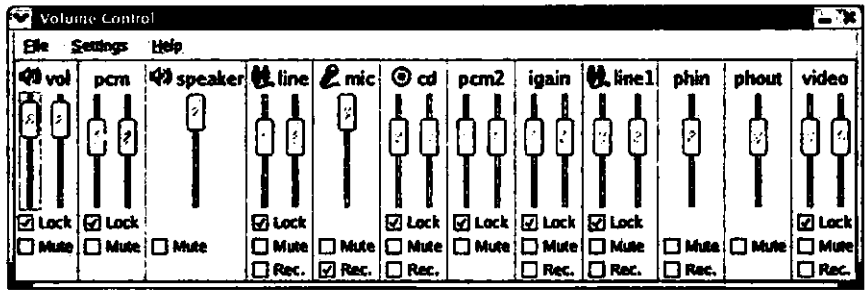
با کلیک روی عنوان موزیک جاری، عناوین موزیک‌های ضبط شده روی سایر شیارها نیز در قالب لیستی به نمایش درمی‌آید. به این ترتیب می‌توان موزیک موردنظر خود را جهت پخش انتخاب کرد. دکمه‌های موجود در سمت چپ عنوان موزیک جاری، امکان ویرایش مشخصات آن موزیک و تنظیمات برنامه CD Player را در اختیار می‌گذارد.

برنامه Sound Recorder

برنامه Sound Recorder جهت ضبط صدای ورودی از طریق میکروفن متصل به کارت صوتی طراحی شده است. این برنامه صدای ضبط شده را در قالب فایل صوتی wav. روی کامپیوتر ذخیره کرده و ضمناً امکان پخش آن‌را نیز در اختیار می‌گذارد. علاوه بر این، برنامه مذکور دارای قابلیت ترکیب صداها بوده و می‌توان شدت صدای حاصل از منابع مختلف را کنترل کرد.

برنامه Volume Control

برنامه Volume Control امکان‌شدت صدای ورودی یا خروجی از چندمنبع‌صوتی را دراختیار می‌گذارد. شکل ۶۱-۱۶ پنجره این برنامه را نشان می‌دهد.



شکل ۶۱-۱۶ پنجره برنامه Volume Control

برنامه Grip

برنامه Grip ابزاری برای ضبط و پخش CDهای صوتی است. (عنوان این برنامه کوتاه شده عبارت GNOME rip است.) برنامه مذکور، ضمن به خاطر سپردن گزینش کاربر در انتخاب موزیک‌های موردنظر خود از روی CD یا هارد دیسک، امکان مرتب‌سازی آن‌ها را پیش از ضبط روی CD نهایی در اختیار وی قرار می‌دهد. چنان‌که شکل ۶۲-۱۶ نیز نشان می‌دهد، پنجره برنامه Grip از بخش‌های مختلفی تشکیل شده است، اما با انتخاب هریک از این بخش‌ها، دکمه‌های کنترلی موجود در پایین این پنجره همواره‌قابل‌دستیابی‌خواهدبود. جدول ۷-۱۶ حاوی‌شرح‌مختصری درباره‌هریک از این بخش‌هاست.

شکل ۱۶-۶۲ پنجره برنامه Grip

جدول ۱۶-۷ شرح بخش‌های مختلف پنجره برنامه Grip

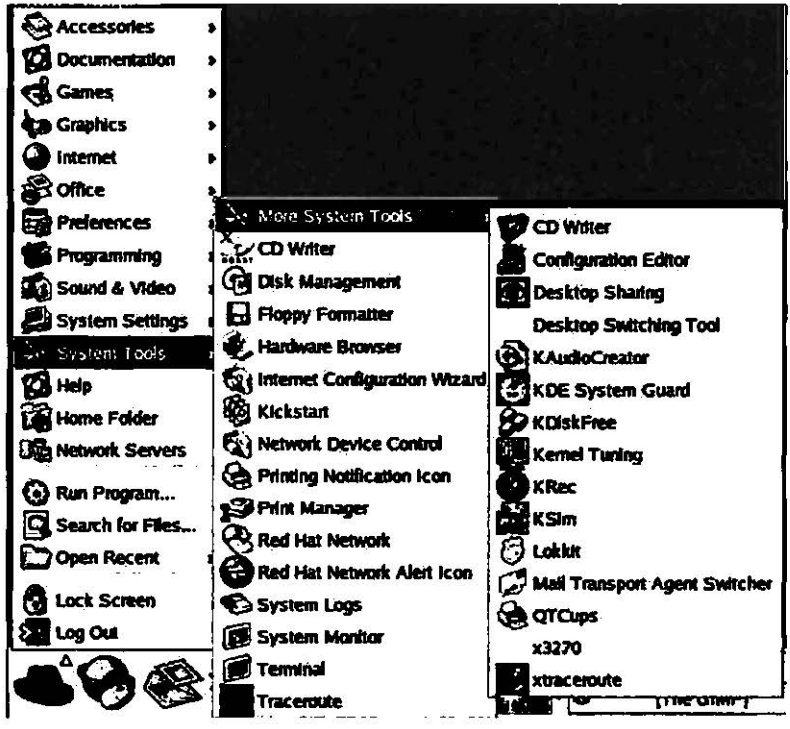
عنوان بخش	توضیح
Track	این بخش حاوی لیست عناوین موزیک‌های ضبط شده در شیارهای CD است. برای افزودن موزیک موردنظر به لیست موزیک‌های موردنظر جهت ضبط (اصطلاحاً لیست Rip) کافی است روی عنوان آن دابل کلیک کنید.
Rip	این بخش امکان ضبط موزیک‌های موجود در لیست Rip را روی CD در اختیار می‌گذارد.
Config	این بخش حاوی تنظیمات مختلفی درباره نحوه ضبط روی CD است.
Help	این بخش حاوی راهنمای استفاده از قابلیت‌های برنامه Grip است.
About	این بخش حاوی اطلاعاتی درباره برنامه Grip و آدرس وب سایت مربوطه است.

این برنامه فایل‌ها را در دو قالب ogg. و m3u. به ترتیب در فهرست ogg/~ و زیرفهرستی از ogg/~ که نام آن بیانگر نام خواننده مربوطه است، ذخیره می‌کند.

این کتاب به هیچ وجه مخاطب خود را به ضبط غیرقانونی آثار هنری تشویق نکرده و این اقدام را مورد تأیید قرار نمی‌دهد. قصد این کتاب از مطرح کردن موضوعاتی نظیر مبحث فوق تنها پرداختن به قابلیت‌های نهفته در برنامه‌های کاربردی Linux است.

گروه System Tools

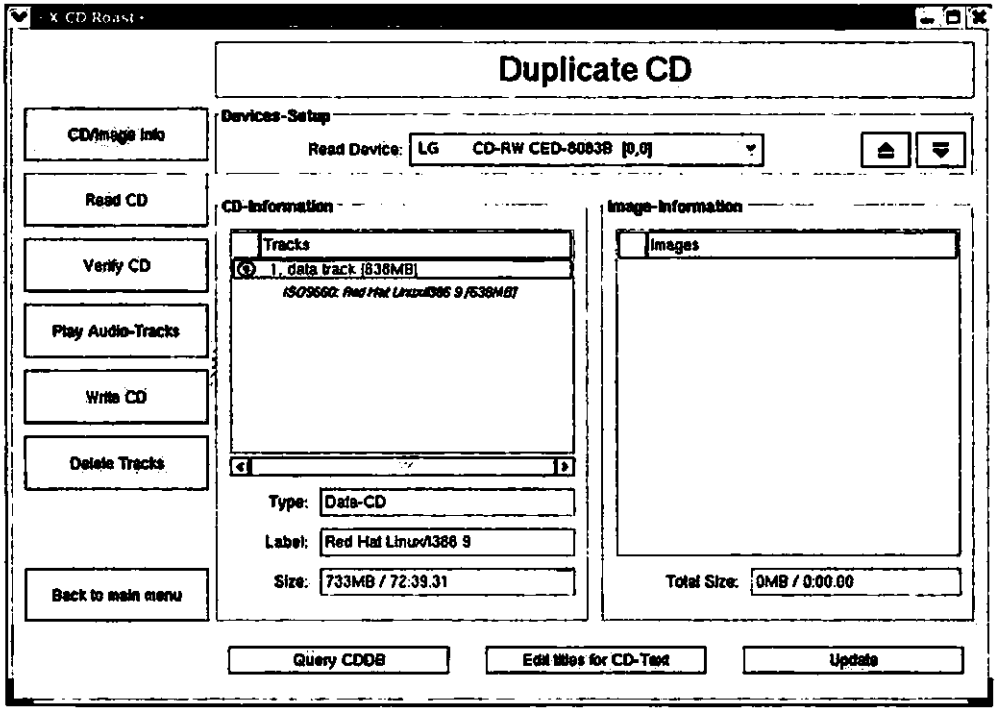
این گروه شامل مجموعه متنوعی از ابزارهای سیستمی است. برخی از این ابزارها را در فصل نوزدهم مورد بررسی قرار داده‌ایم. (چنان‌که می‌دانید، عنوان عمومی این گونه ابزارها redhat-config-* است.) در این قسمت بررسی برخی دیگر از این ابزارها را مورد بررسی قرار می‌دهیم. شکل ۱۶-۶۳ محتوای منوی System Tools را نشان می‌دهد.



شکل ۱۶-۶۳ محتوای منوی System Tools

ابزار X CD Writer

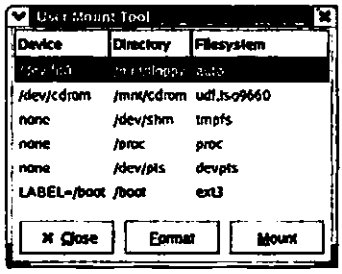
ابزار X CD Copy به منظور ضبط موسیقی و انواع داده‌ها روی CD طراحی شده است. شکل ۶۴-۱۶ پنجره این ابزار با عنوان X-CD-Roast را نشان می‌دهد. پیش از به کارگیری ابزار X CD Copy لازم است تنظیماتی را با انتخاب گزینه Setup واقع در منوی اصلی این ابزار انجام دهید. با این اقدام امکان دسترسی به تنظیمات مختلفی جهت شناسایی مشخصات CD مورد نظر، تغییر موقعیت ذخیره فایل تصویر CD (اصطلاحاً image) روی هارددیسک و سایر موارد مهیا می‌شود.



شکل ۶۴-۱۶ پنجره X-CD-Copy

ابزار Disk Management

ابزار Disk Management به منظور نمایش وضعیت فعلی سیستم فایل Linux طراحی شده است. شکل ۶۵-۱۶، پنجره این ابزار با عنوان User Mount Tool را نشان می‌دهد. در این پنجره امکاناتی نیز به منظور سوار کردن سیستم فایل‌ها و قالب‌بندی آن‌ها تعبیه شده است.



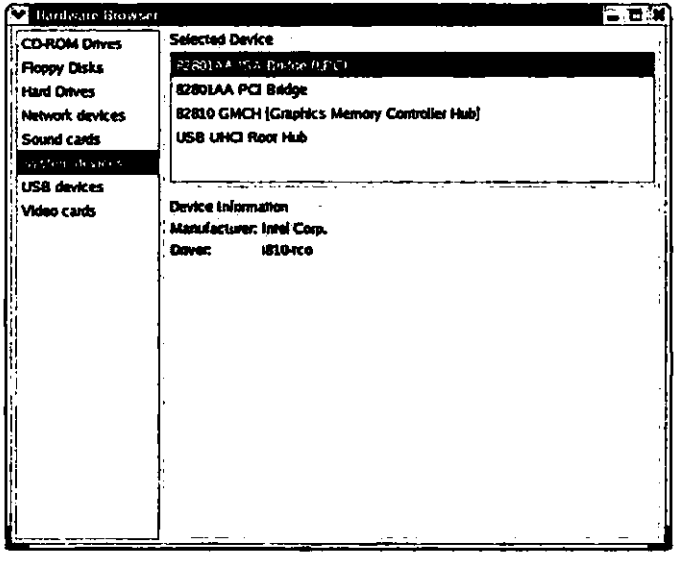
شکل ۱۶-۶۵ پنجره User Mount Tool

ابزار Floppy Formatter

ابزار Floppy Formatter به منظور قالب‌بندی دیسک‌های فلاپی طراحی شده است. این ابزار امکان انتخاب درایو حاوی دیسکت مورد نظر، تعیین ظرفیت دیسکت، برچسب مربوطه و حالت‌های مختلف قالب‌بندی را در اختیار می‌گذارد.

ابزار Hardware Browser

ابزار Hardware Browser تجهیزات سخت‌افزاری نصب شده روی کامپیوتر را تشخیص داده و نمایش می‌دهد. چنان‌که در شکل ۱۶-۶۶ مشاهده می‌کنید، ابزار مذکور صرفاً کاربرد اطلاع‌رسانی داشته و امکان انجام هیچ گونه تنظیماتی را در اختیار نمی‌گذارد.



شکل ۱۶-۶۶ پنجره برنامه Hardware Browser

ابزار Printing Notification Icon

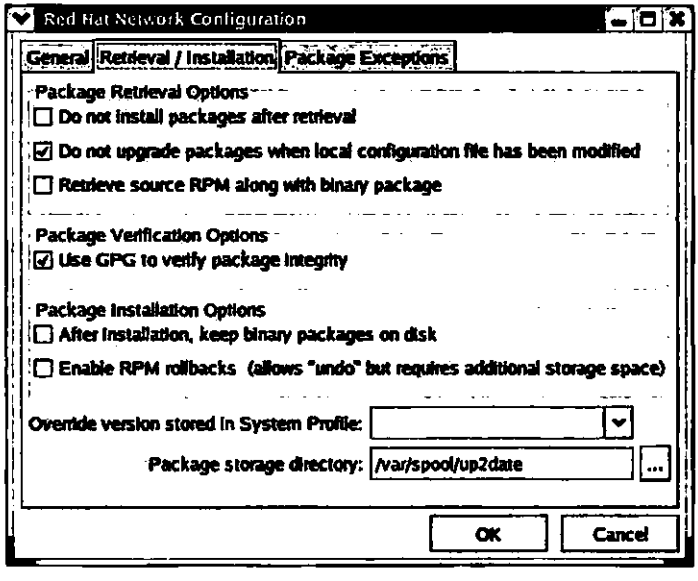
ابزار Printing Notification Icon امکان چاپ اسناد را به سادگی با درگ کردن سند موردنظر روی آیکن چاپگر فراهم می‌کند.

ابزار Print Manager

ابزار Print Manager امکانات موردنیاز برای مدیریت چاپگر و وظایف چاپی را در اختیار کاربر قرار می‌دهد. اگر قبلاً برای پیکربندی چاپگر اقدام نکرده باشید، این ابزار امکانات لازم برای انجام این کار را با راه‌اندازی ابزار redhat-config-printers فراهم می‌کند. (برای اطلاع بیشتر در این زمینه به فصل بیست و پنجم مراجعه کنید.)

ابزار Red Hat Network

ابزار Red Hat Network امکانات مفیدی را به منظور پیکربندی نحوه دسترسی به شبکه Red Hat و تعیین رفتار پیش‌فرض برنامه up2date در تعامل با سرورهای مستقر در این شبکه مهیا می‌کند. چنان‌که شکل ۱۶-۶۷ نشان می‌دهد، پنجره این برنامه با عنوان Red Hat Network Configuration از سه بخش تشکیل شده است. جدول ۱۶-۸ تنظیمات موجود در هر بخش را به اختصار شرح می‌دهد.



شکل ۱۶-۶۷ پنجره Red Hat Network Configuration

جدول ۸-۱۶ شرح بخش‌های مختلف پنجره ابزار Red Hat Network

عنوان بخش	توضیح
General	امکانات این بخش شامل یکسری تنظیمات عمومی در ارتباط با دسترسی به شبکه Red Hat است.
Remove/Installation	امکانات این بخش شامل تنظیماتی در رابطه با دسترسی، نصب و اطمینان از صحت بسته‌های نرم‌افزاری است.
Package Exceptions	تنظیمات این بخش امکان صرف نظر از برخی بسته‌هایی نرم‌افزاری و فایل‌ها را ضمن استفاده از برنامه up2date جهت ارتقای سیستم‌عامل Red Hat Linux در اختیار می‌گذارد.

برای اطلاع بیشتر درباره شبکه Red Hat به فصول سوم و دهم کتاب مراجعه کنید.

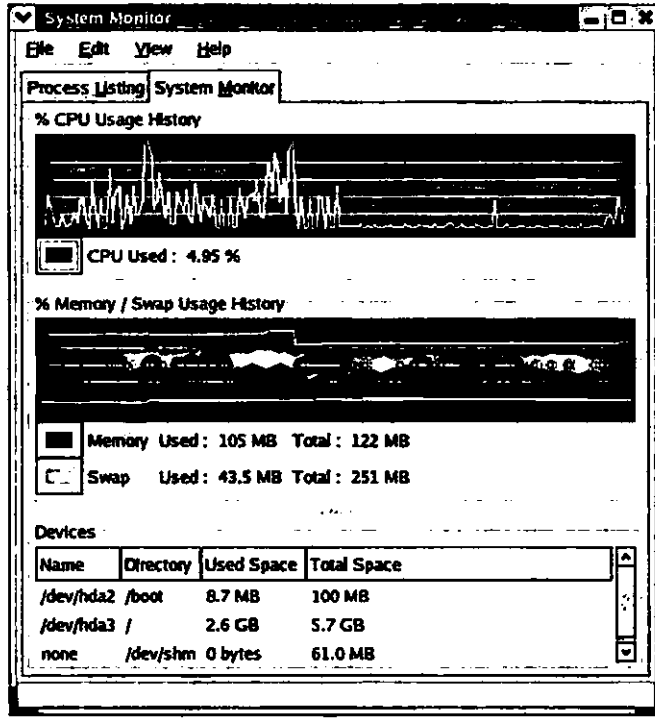
ابزار Red Hat Network Alert Icon

ابزار Red Hat Network Alert Icon یکی از سه آیکن طراحی شده برای این منظور را به طور چرخشی (نوبتی) روی نوار وظیفه مستقر می‌کند. در حال حاضر باید یکی از این آیکن‌ها به طور پیش‌فرض در موقعیت مذکور مستقر شده باشد. به شرح این سه آیکن توجه کنید:

- آیکنی با علامت check mark و به رنگ آبی بیانگر آن است که آخرین نسخه از بسته‌های نرم‌افزاری روی کامپیوتر میزبان نصب شده و از این‌رو نیازی به ارتقای آن‌ها نیست.
- آیکنی با علامت یک جفت پیکان سبز رنگ بیانگر آن است که کامپیوتر میزبان هم‌اینک در حال تعامل با شبکه Red Hat است.
- آیکنی با علامت تعجب و به رنگ قرمز بیانگر آن است که آخرین نسخه از بسته‌های نرم‌افزاری روی کامپیوتر میزبان نصب نشده و از این‌رو می‌توان به واسطه دسترسی به شبکه Red Hat برای ارتقای آن‌ها اقدام کرد.

ابزار System Monitor

ابزار System Monitor امکاناتی را به منظور نظارت بر فرآیندهای جاری، میزان فعالیت پردازنده و میزان استفاده از حافظه swap در اختیار می‌گذارد. این ابزار در واقع یک رابط گرافیکی قابل پیکربندی برای فرمان top به شمار می‌رود. شکل ۶۸-۱۶ پنجره این برنامه را نشان می‌دهد.



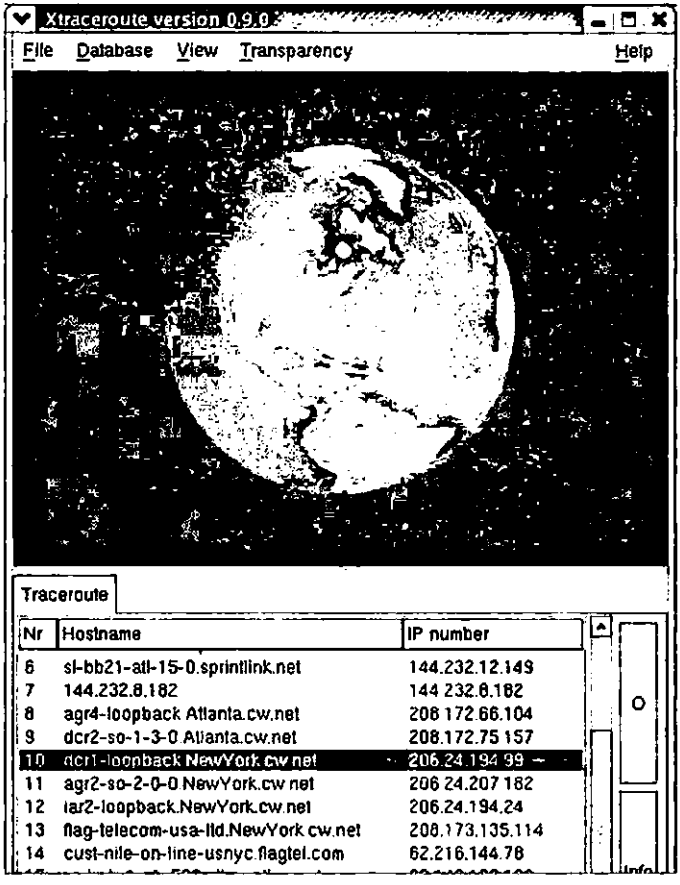
شکل ۶۸-۱۶ پنجره ابزار System Monitor

ابزار Terminal

ابزار Terminal در واقع همان رابط سطر فرمان استاندارد در سیستم‌عامل Linux است که برای محیط گرافیکی GNOME طراحی شده است. با وجود زمینه سیاه و فونت‌های سفید، میزان خوانایی محتوای درج شده در پنجره این ابزار بسیار مطلوب است. در قسمت‌های قبلی این کتاب نمونه این پنجره را مشاهده کرده‌اید.

ابزار Traceroute

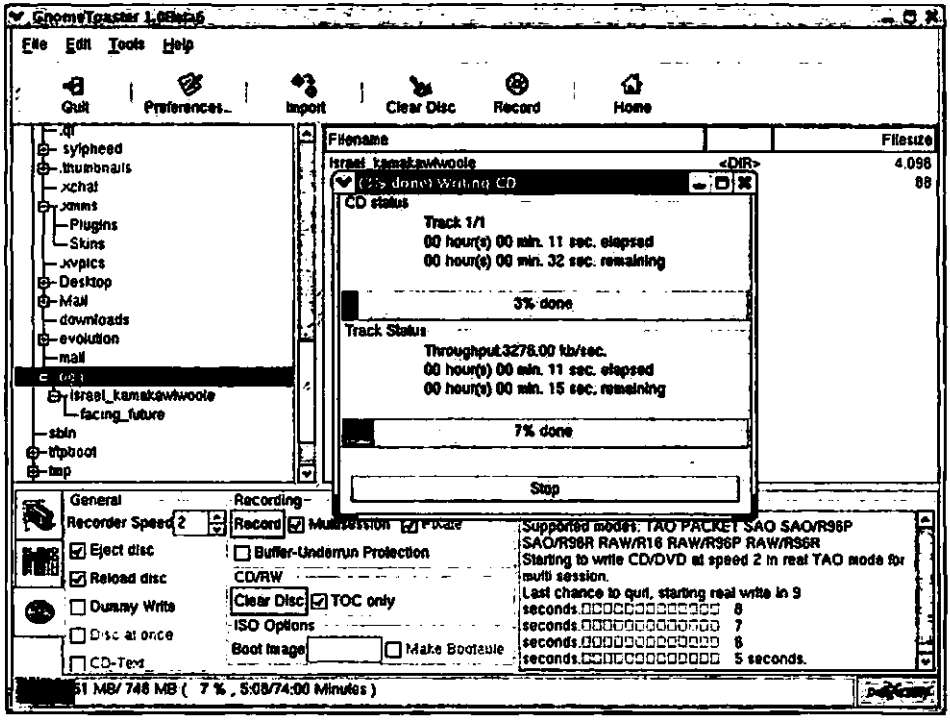
ابزار Traceroute به عنوان رابط گرافیکی فرمان traceroute مسیر انتقال داده‌ها از کامپیوتر میزبان به مقصد موردنظر را نشان می‌دهد. شکل ۶۹-۱۶ پنجره این برنامه با عنوان Xtraceroute را در حال نمایش مسیر انتقال داده‌ها از کامپیوتری واقع در ایالات متحده به کامپیوتر دیگری که در مصر واقع شده نشان می‌دهد.



شکل ۱۶-۶۹ پنجره Xtraceroute

ابزار CD Writer

ابزار CD Writer به منظور ذخیره انواع داده‌ها روی CD طراحی شده است. این ابزار تنظیمات بسیار متنوعی را به منظور پیکربندی در اختیار می‌گذارد. ضمناً ابزار مذکور از قابلیت drag and drop نیز پشتیبانی می‌کند، به این معنی که می‌توان فایل‌های موردنظر را جهت نوشتن در CD روی آیکن آن درگ کرد. شکل ۱۶-۷۰ پنجره این ابزار با عنوان GnomeToaster را نشان می‌دهد.

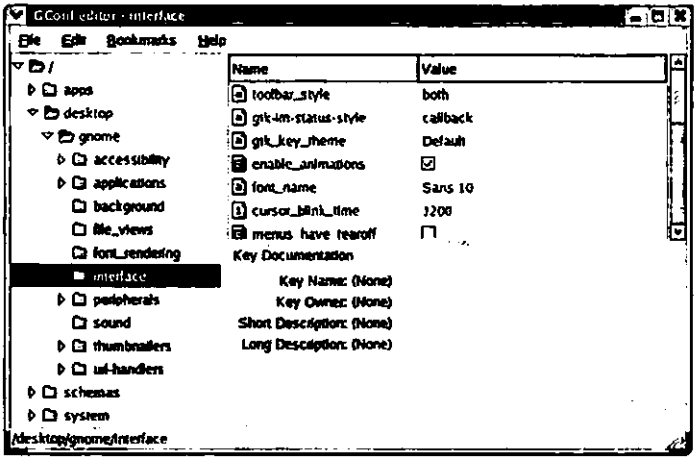


شکل ۷۰-۱۶ پنجره GnomeToaster

ابزار Configuration Editor

ابزار Configuration Editor به منظور ویرایش تنظیماتی که در قالب فایل‌های پیکربندی مختلف در فهرست خانگی کاربران ذخیره شده‌اند، امکانات لازم را در اختیار قرار می‌دهد. پنجره این ابزار با عنوان Gconf Editor بی‌شباهت به پنجره ابزار Registry در سیستم‌عامل ویندوز نیست. سهل‌انگاری در ویرایش این تنظیمات می‌تواند عواقب نامطلوبی هم‌چون عدم توانایی در دسترسی به محیط گرافیکی GNOME را به دنبال داشته باشد. با وجود این، ابزار مورد بحث، امکان پیکربندی تمام برنامه‌های کاربردی GNOME را تنها از طریق یک رابط گرافیکی در اختیار می‌گذارد. شکل ۷۱-۱۶ پنجره این ابزار را نشان می‌دهد.

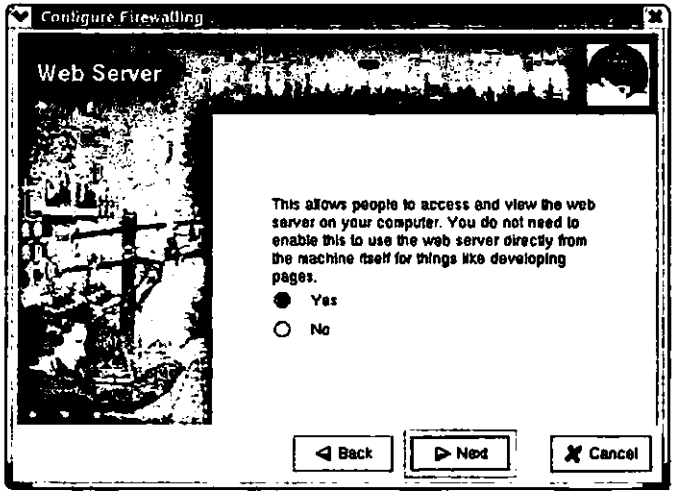
با مراجعه به وب سایت http://www.developer.gnome.org/feature/archive/gconf/gconf.html می‌توانید اطلاعات بیشتری را درباره امکانات این ابزار به دست آورید.



شکل ۱۶-۷۱ پنجره Gconf Editor

ابزار Lokkit

ابزار Lokkit جهت پیکربندی مکانیزم بازدارنده دیوار آتش طراحی شده است. علیرغم فرمان lokkit، که البته بی‌شباهت به ابزار پیکربندی redhat-config-firewall نیست، این ابزار ویزاردی را به منظور پیکربندی مکانیزم مذکور در اختیار می‌گذارد. شکل ۱۶-۷۲ بخشی از این ویزارد را که امکان دسترسی سایر کاربران به وب سرور مستقر روی کامپیوتر میزبان را مهیا می‌کند، نشان می‌دهد. (برای اطلاع بیشتر درباره ابزار پیکربندی redhat-config-firewall به فصل نوزدهم مراجعه کنید.)



شکل ۱۶-۷۲ پنجره ابزار Lokkit

با وجود این، یکی از نقاط ضعف ابزار Lokkit این است که امکان دسترسی از طریق سایر پورت‌های TCP/IP را در اختیار نمی‌گذارد. (برای اطلاع بیشتر درباره مکانیزم بازدارنده دیوار آتش به فصل بیست و دوم مراجعه کنید).

ابزار x3270

ابزار x3270 به منظور شبیه‌سازی ترمینال‌های متداول 3270 ساخت شرکت IBM جهت دسترسی به کامپیوترهای mainframe ساخت همین شرکت طراحی شده است. این ابزار کلیدهای عملیاتی ترمینال‌های نامبرده را به خوبی شبیه‌سازی می‌کند.

جمع‌بندی

در این فصل محیط گرافیکی GNOME را به عنوان محیط گرافیکی پیش‌فرض در سیستم‌عامل Red Hat Linux مورد بررسی قرار دادیم. بسیاری از ابزارهای قابل استفاده در این محیط گرافیکی شبیه به ابزارهایی است که سیستم‌عامل ویندوز نیز آن‌ها را در اختیار کاربران خود قرار می‌دهد. چنان‌که مشاهده‌کردید، برنامه‌های‌کاربردی باز را می‌توان مابین‌چهار دسک‌تاپ مجزا توزیع کرد. محیط گرافیکی GNOME را به سادگی می‌توان با توجه به نیازها پیکربندی کرد.

برنامه‌های کاربردی متعددی برای محیط گرافیکی GNOME توسعه داده شده که با وجود آن‌ها می‌توان مبالغ قابل توجهی در هزینه نرم‌افزار صرفه‌جویی کرد. این برنامه‌ها ابزارهای مفیدی هستند که اغلب کاربرد روزمره دارند. گروه برنامه‌های کاربردی Internet شامل مرورگرهای وب، ابزارهای مدیریت پیغام‌های الکترونیکی و برنامه‌های گپ‌زنی است. گروه Sound & Video نیز متشکل از برنامه‌های کاربردی مفیدی است که به منظور مدیریت، پردازش و ضبط صدا و تصویر طراحی شده‌اند. در محیط گرافیکی GNOME ابزارهای سیستمی مفیدی نیز جهت کمک به مدیران سیستم‌ها در انجام وظایف روزمره پیش‌بینی شده است.

در فصل بعد یکی دیگر از محیط‌های گرافیکی بسیار متداول سیستم عامل Linux با عنوان K Desktop Environment یا به اختصار KDE را مورد بررسی قرار می‌دهیم. در صورت آشنایی قبلی با محیط گرافیکی KDE، خواهید دید که سیستم‌عامل Red Hat Linux آن‌را به نحوی شبیه به محیط گرافیکی GNOME پیکربندی می‌کند.

فصل هفدهم

محیط گرافیکی KDE

مشابه نسخه‌های متعدد سیستم‌عامل Linux، محیط‌های گرافیکی متعددی نیز برای این سیستم‌عامل توسعه داده شده است. با وجود این، شاید بتوان محیط گرافیکی K Desktop Environment یا به اختصار KDE را مهم‌ترین جایگزین برای محیط گرافیکی GNOME تصور کرد. استفاده از هر دو محیط گرافیکی GNOME و KDE در میان کاربران سیستم‌عامل Linux بسیار رایج است. در واقع بسیاری از کاربران Linux استفاده از محیط گرافیکی KDE را به GNOME ترجیح می‌دهند. با وجودی که محیط گرافیکی GNOME در سیستم‌عامل Red Hat Linux به عنوان پیش‌فرض انتخاب شده است، هر دو محیط گرافیکی نامبرده در اغلب نسخه‌های توزیع شده Linux قابل دستیابی است.

در سیستم‌عامل Red Hat Linux تم خاصی با عنوان Bluecurve در قالب هر دو محیط گرافیکی GNOME و KDE پیاده‌سازی شده است. علاوه بر این، گزینه مربوط به تعدادی از ابزارهای متداول در منوی اصلی هر دو محیط مذکور تعبیه شده است. از آن‌جا که رقابت میان دو محیط گرافیکی GNOME و KDE به جدیت رقابت میان دو سیستم‌عامل ویندوز و Linux نبوده و ضمناً در سیستم‌عامل Red Hat Linux قابلیت‌های این دو محیط گرافیکی به تدریج در حال همگرایی است، تصمیم‌گیری درباره انتخاب یکی از آن دو بیشتر به سلیقه شخصی کاربران بستگی دارد.

محیط گرافیکی GNOME محصول محیط توسعه GTK+ و محیط گرافیکی KDE محصول محیط توسعه دیگری با عنوان Qt است. جعبه ابزار Qt در سال‌های اخیر به عنوان یک نرم‌افزار کد باز منتشر شده است. بیشتر کار توسعه محیط گرافیکی KDE در اروپا انجام شده و محبوبیت آن نیز در اروپا به مراتب بیشتر از آمریکای شمالی است، به طوری که برای مثال، دولت جمهوری فدرال آلمان رسماً آن‌را به عنوان محیط گرافیکی مورد استفاده در دستگاه‌های دولتی اعلام کرده است.

در این فصل به بررسی محیط گرافیکی KDE و هم‌چنین ابزارهایی می‌پردازیم که در قالب آن منتشر می‌شوند. علاوه بر این، امکانات موجود در مرکز کنترل محیط گرافیکی KDE را نیز مورد بررسی قرار می‌دهیم. چنان‌که در این فصل خواهید دید، توسعه دهندگان این محیط گرافیکی ابزارهای مدیریتی بسیارکارآمدی را در قالب این محیط گرافیکی پیاده‌سازی کرده‌اند که به اعتقاد بسیاری، از نظر عملکرد

و کارآیی با ابزارهای پیکربندی عرضه شده توسط شرکت Red Hat (با عنوان کلی *-redhat-config) قابل رقابت است.

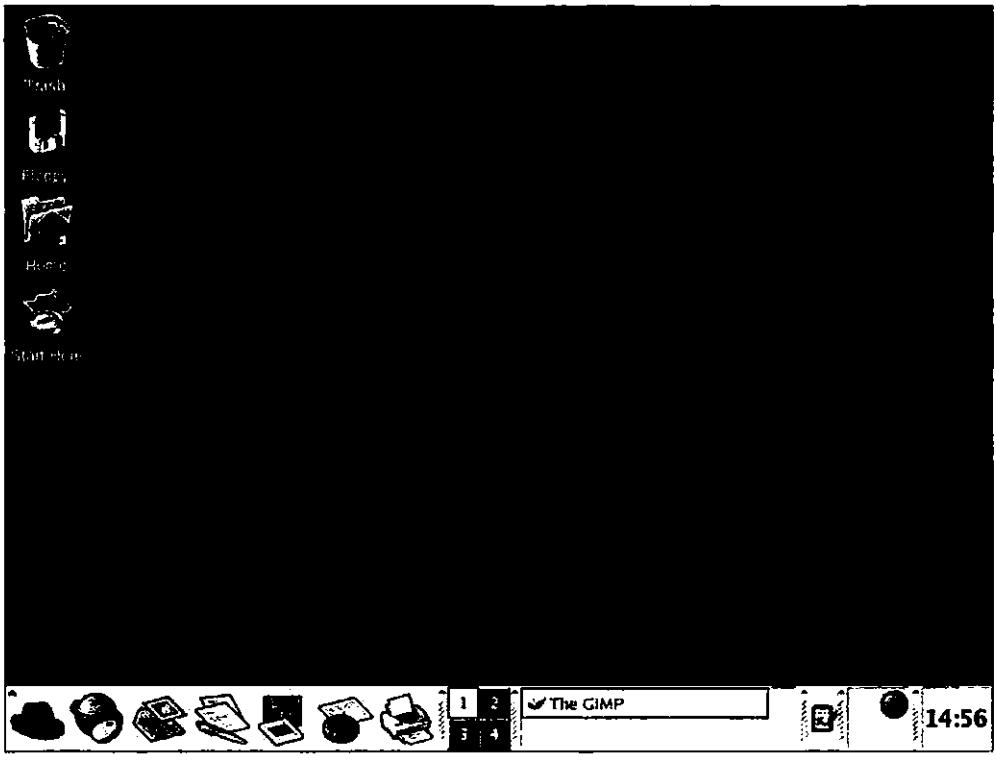
پیاده‌سازی محیط گرافیکی KDE در سیستم‌عامل Red Hat Linux به نحوی انجام شده که امکان استفاده از برنامه‌های کاربردی و ابزارهای محیط گرافیکی GNOME نیز وجود دارد. چنان‌چه فصل شانزدهم را مطالعه کرده باشید، متوجه شباهت‌هایی خواهید شده که حاکی از تلاش توسعه دهندگان شرکت Red Hat Linux برای استاندارد کردن محیط گرافیکی Linux است. ابزارهای مختلف محیط گرافیکی KDE (و هم‌چنین محیط گرافیکی GNOME و ابزارهای پیکربندی *-redhat-config) از طریق منوی اصلی این محیط گرافیکی قابل دستیابی هستند. موضوعات مورد بررسی در فصل حاضر به این شرح است:

- شناخت رابط‌های محیط گرافیکی KDE
- امکانات مرکز کنترل محیط گرافیکی KDE
- ابزارهای توسعه یافته برای محیط گرافیکی KDE

شناخت رابط‌های محیط گرافیکی KDE

مشخصات محیط گرافیکی KDE کم‌وبیش مشابه محیط گرافیکی سایر سیستم‌عامل‌ها است. این محیط شامل یک پانل، منوی اصلی و آیکن‌هایی است که با انتخاب آن‌ها می‌توان ابزارها و برنامه‌های کاربردی را مورد دستیابی قرار داد. هریک از این اجزا را می‌توان با توجه به نیازها پیکربندی کرد. علاوه بر این، حتی می‌توان رابط گرافیکی ابزارها برنامه‌های کاربردی را به طور یکسان پیکربندی کرد. کلیه امکانات مربوط به این کار در مرکز کنترل محیط گرافیکی KDE پیش‌بینی شده است. در صورت نصب بسته‌های نرم‌افزاری محیط گرافیکی KDE و پیکربندی آن به عنوان محیط گرافیکی پیش‌فرض، پس از راه‌اندازی سیستم‌عامل با صحنه‌ای مشابه شکل ۱-۱۷ مواجه می‌شوید.

پانل محیط گرافیکی KDE و GNOME را می‌توان به نوار وظیفه در ویندوز تشبیه کرد. هم‌چنین دکمه دسترسی به منوی اصلی در محیط گرافیکی GNOME و KDE را که به ترتیب با عناوین Main Menu Button و K Menu Button شناخته می‌شوند، می‌توان به دکمه Start در ویندوز تشبیه کرد.



شکل ۱-۱۷ محیط گرافیکی KDE

مروری اجمالی بر محیط گرافیکی KDE

رابط گرافیکی محیط KDE بسیار ساده است. چنان‌که در شکل ۱-۱۷ مشاهده می‌کنید، این محیط شامل آیکن‌های مختلفی از جمله آیکن سطل زباله با عنوان Trash، آیکن فلاپی‌دیسک با عنوان Floppy، آیکن دسترسی به فهرست خانگی با عنوان Home و بالاخره آیکن دسترسی به فهرست Start Here با همین عنوان است. با کلیک روی هریک از این آیکن‌ها برنامه Konqueror باز شده و امکانات لازم برای دسترسی به محتوای سطل زباله، فلاپی‌دیسک، فهرست خانگی و فهرست Start Here را در اختیار قرار می‌دهد. برنامه Konqueror ابزاری شبیه به برنامه Explorer در ویندوز است که امکان مدیریت فایل‌ها و پیکربندی محیط گرافیکی KDE را به سادگی فراهم می‌کند. با وجودی که در سیستم‌عامل Red Hat Linux مرورگر Mozilla به عنوان برنامه پیش‌فرض جهت دسترسی به وب پیکربندی شده است، در صورت تمایل می‌توان برنامه Konqueror را نیز به این منظور مورد استفاده قرار داد. توسعه این برنامه در قالب پروژه KDE انجام شده است.

پس از ورود به محیط گرافیکی KDE برای نخستین بار، کادر محاوره‌ای Kandalf's Useful Tips باز می‌شود. این کادر محاوره‌ای حاوی برخی نکات آموزنده است که مطالعه آن حتی برای کاربران کم‌تجربه نیز بسیار مفید خواهد بود.

دکمه وسط ماوس در محیط گرافیکی KDE کارآیی فوق‌العاده‌ای دارد. هم‌اینک تأثیر کلیک این دکمه را درحالی‌که اشاره‌گر ماوس روی آیکن دلخواهی از محیط گرافیکی قرار دارد، تجربه کنید. بار دیگر این تجربه را در حالی انجام دهید که اشاره‌گر ماوس روی هیچ آیکنی قرار ندارد. سپس نتایج حاصل را با یکدیگر مقایسه کنید.

در قسمت‌های بعد عملکرد دکمه‌های موجود روی پانل محیط گرافیکی KDE و هم‌چنین امکانات مرکز کنترل این محیط گرافیکی را مورد بررسی قرار می‌دهیم.

پانل محیط گرافیکی KDE

پانل محیط گرافیکی KDE حاوی امکانات لازم برای دسترسی به برنامه‌های کاربردی، سوییچ کردن بین پنجره‌های دو یا چند برنامه کاربردی در حال اجرا و حتی سوییچ کردن بین چند محیط کاری یا اصطلاحاً desktop است. شکل ۲-۱۷ نمونه‌ای از این پانل را نشان می‌دهد.

شکل ۲-۱۷ پانل محیط گرافیکی KDE

چنان‌که مشاهده می‌کنید، سمت چپ این پانل متشکل از شش آیکن است. جدول ۱-۱۷ به شرح مختصری درباره عملکرد این آیکن‌ها می‌پردازد.

جدول ۱-۱۷ عملکرد آیکن‌های موجود روی پانل محیط گرافیکی KDE

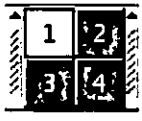
آیکن	توضیح
	با کلیک آیکن منوی اصلی، محیط گرافیکی KDE باز شده و امکان دسترسی به ابزارها و برنامه‌های کاربردی را در اختیار می‌گذارد. عملکرد این دکمه را می‌توان با دکمه Start در سیستم‌عامل ویندوز مقایسه کرد.
	با کلیک این آیکن پنجره مرورگر Mozilla باز می‌شود.

آیکن	توضیح
	با کلیک این آیکن پنجره برنامه مدیریت اطلاعات شخصی Evolution باز می‌شود. (کاربرد این برنامه مشابه برنامه Microsoft Outlook است.)
	با کلیک این آیکن پنجره برنامه واژه‌پرداز OpenOffice Writer باز می‌شود. (کاربرد این برنامه مشابه برنامه Microsoft World است.)
	با کلیک این آیکن پنجره برنامه مدیریت نمایش OpenOffice Impress باز می‌شود. (کاربرد این برنامه مشابه برنامه Microsoft PowerPoint است.)
	با کلیک این آیکن پنجره برنامه صفحه گسترده OpenOffice Calc باز می‌شود. (کاربرد این برنامه مشابه برنامه Microsoft Excel است.)
	با کلیک این آیکن پنجره برنامه GNOME Print Manager باز می‌شود.

نرم‌افزار OpenOffice که مجموعه‌ای از برنامه‌های کاربردی است، اغلب با عنوان OpenOffice.org یا Ooo نیز شناخته می‌شود. این نرم‌افزار تحت لیسانس GNU General Public License (به اختصار GPL) و Sun Industry Standards Source License منتشر می‌شود.

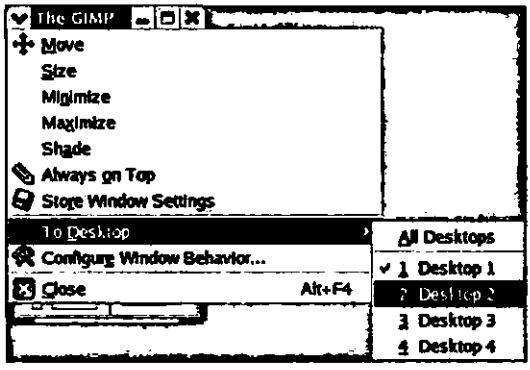
محیط کاری KDE

محیط گرافیکی KDE از این نظر که می‌توان پنجره برنامه‌های کاربردی را در محیط‌های کاری مختلف باز کرد، بسیار قابل انعطاف است. از این‌رو، به جای باز و بسته کردن پنجره‌ها، برای دسترسی به آن‌ها کافی است مابین محیط‌های کاری سوییچ کنید. به این ترتیب، می‌توان پنجره برنامه‌های کاربردی مختلف، مثلاً GIMP، OpenOffice Calc، OpenOffice Writer و پنجره ترمینال را در محیط‌های کاری اول تا چهارم باز کرده و برای دسترسی به محیط کاری مربوطه سوییچ کرد. شکل ۳-۱۷ بخشی از پانل محیط گرافیکی KDE را که نماینده چهار محیط کاری موجود است، نشان می‌دهد. چنان‌که مشاهده می‌کنید، محیط کاری فعلی از بقیه کاملاً متمایز است.



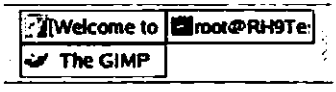
شکل ۳-۱۷ چهار محیط کاری موجود در محیط گرافیکی KDE

برای سوییچ به محیط کاری موردنظر، کافی است روی شماره مربوط به آن کلیک کنید. هم‌چنین برای انتقال پنجره برنامه کاربردی موردنظر از یک محیط کاری به دیگری، ابتدا گوشه بالای سمت چپ آن پنجره را کلیک کرده و سپس با دسترسی به منوی To Desktop محیط دلخواه خود را انتخاب کنید. شکل ۴-۱۷ نحوه انتقال پنجره برنامه کاربردی GIMP را از محیط کاری اول به دوم نشان می‌دهد.



شکل ۴-۱۷ انتقال پنجره برنامه کاربردی GIMP از محیط کاری اول به محیط کاری دوم

علاوه بر سوییچ کردن از یک محیط کاری به دیگری، می‌توان از پنجره یک برنامه کاربردی به دیگری نیز سوییچ کرد. برای این منظور، کافی است روی کنترل دسترسی مربوط به پنجره موردنظر از پانل محیط گرافیکی KDE کلیک‌کنید. شکل ۵-۱۷ بخشی از این پانل را که حاوی کنترل دسترسی مربوط به سه پنجره مختلف است، نشان می‌دهد.



شکل ۵-۱۷ کنترل‌های دسترسی به سه پنجره باز در محیط گرافیکی KDE

سایر عناصر موجود در پانل محیط گرافیکی KDE

در منتهی‌الیه سمت راست پانل محیط گرافیکی KDE سه آیکن دیگر نیز موجود است. آیکن نخست با عنوان Klipper جهت دسترسی به ابزاری برای انتقال محتوا از یک برنامه کاربردی به دیگری (به شیوه copy و paste) پیش‌بینی شده است. جهت پیکربندی این ابزار روی آیکن مزبور کلیک راست کرده و از منوی حاصل گزینه Configure Klipper را انتخاب کنید. آیکن بعدی ممکن است یکی از این موارد باشد:

- **دایره‌ای به رنگ قرمز شامل یک علامت تعجب:** نمایش‌این‌آیکن به‌معنی‌آن‌است که پیکربندی فعلی سیستم‌عامل Red Hat Linux فاقد جدیدترین نسخه برخی از بسته‌های نرم‌افزاری است. جدیدترین نسخه بسته‌های نرم‌افزاری منتشر شده را می‌توان از شبکه Red Hat دریافت کرد.
- **دایره‌ای به رنگ سبز شامل دو علامت پیکان:** نمایش این آیکن به‌این‌معنی است که کامپیوتر میزبان در حال تعامل با شبکه Red Hat است.
- **دایره‌ای به‌رنگ‌آبی حاوی علامت check mark:** نمایش‌این‌آیکن‌بدان‌معنی‌است‌که سیستم‌عامل فعلی با جدیدترین نسخه از بسته‌های نرم‌افزاری بوده و از این‌رو نیازی به ارتقای آن‌ها نیست.

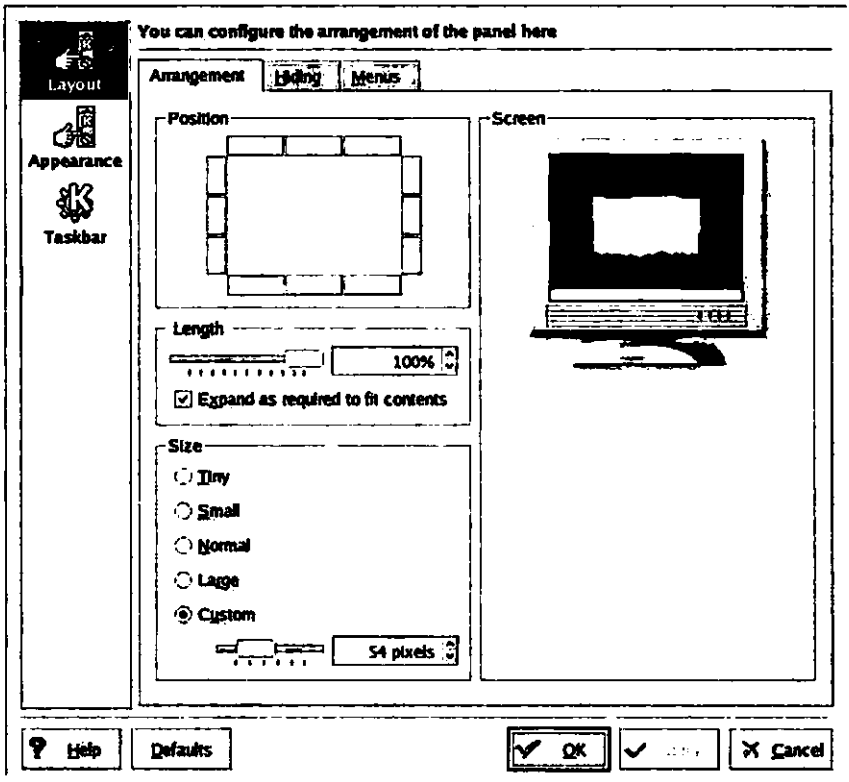
شکل ظاهری سه آیکن مزبور به این صورت است:

جهت پیکربندی پارامترهای دسترسی به شبکه Red Hat روی آیکن مزبور کلیک راست کرده و گزینه مربوطه را از منوی حاصل انتخاب کنید. (برای اطلاع بیشتر درباره چگونگی ارتقای بسته‌های نرم‌افزاری به جدیدترین نسخه‌های موجود، قسمت مربوط به برنامه up2date از فصل دهم را ببینید.) بسته به اجرای برنامه‌های کاربردی ممکن است آیکن‌های دیگری را نیز در این ناحیه از پانل محیط گرافیکی KDE مشاهده کنید.

آیکن سوم بیانگر ساعت فعلی است. با کلیک روی این آیکن تقویم ماه جاری به نمایش درمی‌آید. با کلیک راست روی این آیکن می‌توان تنظیماتی را در مورد ظاهر ساعت، ناحیه زمانی و قالب نمایش ساعت انجام داد.

پیکربندی پانل محیط گرافیکی نیز بسیار آسان است. برای این منظور کافی است روی بخشی از پانل که فاقد آیکن است کلیک راست کرده و گزینه Configure Panel را از منوی حاصل انتخاب کنید تا به این ترتیب پنجره حاوی تنظیمات موردنظر با عنوان KDE Control Module باز شود. شکل ۶-۱۷ این پنجره را نشان می‌دهد.

پنجره مزبور تنظیمات مختلفی را به منظور پیکربندی پانل محیط گرافیکی KDE چه از نظر ظاهر و موقعیت استقرار آن در صفحه و چه از نظر محتوای منوی اصلی این محیط (با عنوان Main Menu) در اختیار می‌گذارد.



شکل ۶-۱۷ پنجره حاوی تنظیمات پیکربندی پانل محیط گرافیکی KDE

منوی اصلی

در این قسمت نگاهی به منوی اصلی محیط گرافیکی KDE خواهیم داشت. برای شروع، روی آیکن کلاه قرمز در گوشه پایین و سمت چپ پانل کلیک کنید تا به این ترتیب منوی اصلی باز شود. شکل ۷-۱۷ محتوای این منو را نشان می‌دهد.

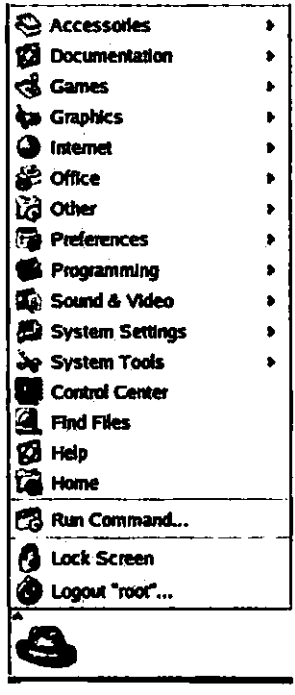
چنان‌که مشاهده می‌کنید، منوی اصلی حاوی گزینه‌های متعددی است که در جدول ۲-۱۷ به طور مختصر آن‌ها را شرح می‌دهیم.

جدول ۲-۱۷ شرح گزینه‌های مندرج در منوی اصلی محیط گرافیکی KDE

عنوان گزینه	توضیح
Accessories	این منوی فرعی حاوی مجموعه‌ای از برنامه‌های کوچک مانند ویرایشگرهای متن و ماشین حساب است.

عنوان گزینه	توضیح
Documentation	این منوی فرعی حاوی مستندات سیستم‌عامل Red Hat Linux است. (برای توضیح بیشتر به فصل شانزدهم مراجعه کنید.)
Games	این منوی فرعی حاوی بازی‌های قابل اجرا در محیط گرافیکی GNOME یا KDE است.
Graphics	این منوی فرعی حاوی برنامه‌های کاربردی با رابط گرافیکی است که به منظور ویرایش تصویر، عکس‌برداری از صفحه نمایش، ارسال و دریافت فاکس، بازخوانی اسناد PDF و سایر موارد طراحی شده‌اند.
Internet	این منوی فرعی حاوی مجموعه‌ای از برنامه‌های کاربردی است که امکان برقراری ارتباط با شبکه‌های TCP/IP از جمله اینترنت را در اختیار قرار می‌دهد.
Office	این منوی فرعی حاوی برنامه‌های کاربردی توزیع شده در قالب بسته نرم‌افزاری OpenOffice است. دسترسی به مجموعه برنامه‌های کاربردی KOffice از طریق منوی More Office Applications واقع در این منوی فرعی امکان‌پذیر است.
Other	این منوی فرعی حاوی مجموعه‌ای از ابزارهای جالب توجه قابل استفاده در محیط گرافیکی KDE است. برخی از این ابزارها کاربرد آموزشی دارند.
Preferences	این منوی فرعی حاوی ابزارهای پیکربندی مختلف، به ویژه پیکربندی محیط گرافیکی KDE است.
Programming	این منوی فرعی حاوی مجموعه‌ای از ابزارهای برنامه‌نویسی است. موضوع عجیب این که گزینه Emacs نیز در این منو واقع شده است.
Sound & Video	این منوی فرعی حاوی برنامه‌های کاربردی چند رسانه‌ای از جمله یک برنامه نوشتن روی CD است.
System Settings	این منوی فرعی حاوی مجموعه‌ای از ابزارهای پیکربندی است که اغلب با عنوان عمومی redhat-config-* می‌شناسیم. دسترسی به بیشتر این ابزارها تنها برای کاربر اصلی امکان‌پذیر است.
System Tools	این منوی فرعی حاوی مجموعه‌ای از ابزارهای سیستمی است. برخی از این ابزارها به طور خاص جهت استفاده در محیط گرافیکی KDE طراحی شده‌اند.
Control Center	این گزینه امکان دسترسی به مرکز کنترل محیط گرافیکی KDE را که حاوی مجموعه‌ای تقریباً کامل از ابزارهای پیکربندی است، در اختیار قرار می‌دهد.
Find Files	این گزینه ابزاری را به منظور جستجوی فایل‌ها، جستجو در درون فایل‌ها و مشاهده خصوصیات فایل‌ها در اختیار می‌گذارد.

عنوان گزینه	توضیح
Help	این گزینه راهنمای کار در محیط گرافیکی KDE را در قالب یک مرورگر ساده نمایش می‌دهد.
Home	این گزینه پنجره برنامه Konqueror را در حال نمایش فایل‌های موجود در فهرست خانگی باز می‌کند.
Run Command	این گزینه کادر محاوره‌ای Run Command را به منظور اجرای برنامه کاربردی یا فرمان موردنظر در اختیار قرار می‌دهد.
Lock Screen	این گزینه موجب اجرای برنامه محافظ صفحه نمایش (اصطلاحاً screensaver) می‌شود. تنها راه خروج از این برنامه و دسترسی مجدد به محیط گرافیکی KDE اطلاع از کلمه عبور مربوطه است.
Log Out	این گزینه موجب خروج از محیط گرافیکی KDE می‌شود.



شکل ۷-۱۷ محتوای منوی اصلی

برخی از این منوها را به طور مشروح در این فصل و برخی دیگر را در فصول بعدی توضیح می‌دهیم. تعدادی از برنامه‌های کاربردی قابل دستیابی از طریق این منوها را در فصل قبل بررسی کردیم. برنامه‌های کاربردی اصلی از جمله مجموعه OpenOffice و برنامه‌های گرافیکی را در فصل هجدهم مورد بررسی قرار می‌دهیم. بررسی ابزارهای خاص سیستم‌عامل Red Hat Linux را نیز به فصل نوزدهم موکول می‌کنیم. ضمناً در این کتاب از پرداختن به بازی‌ها Linux خودداری می‌کنیم.

گزینه‌های موجود در بالای منوی اصلی همواره مربوط به برنامه‌هایی هستند که اخیراً آن‌ها را اجرا کرده‌اید. به‌طور پیش‌فرض، گزینه‌های مربوط به حداکثر پنج برنامه‌کاربردی که اخیراً به اجرا درآمده‌اند، در بالای این منو نمایش داده می‌شود.

چنان‌چه گزینه‌ای از موارد مذکور در جدول ۲-۱۷ قابل مشاهده نباشد، ممکن است بسته یا بسته‌های نرم‌افزاری مربوطه نصب نشده باشد. برای مثال، مشاهده گزینه Games تنها در صورتی امکان‌پذیر است که بسته نرم‌افزاری kdegames-* یا gnome-games قبلاً روی کامپیوتر میزبان نصب شده باشد.

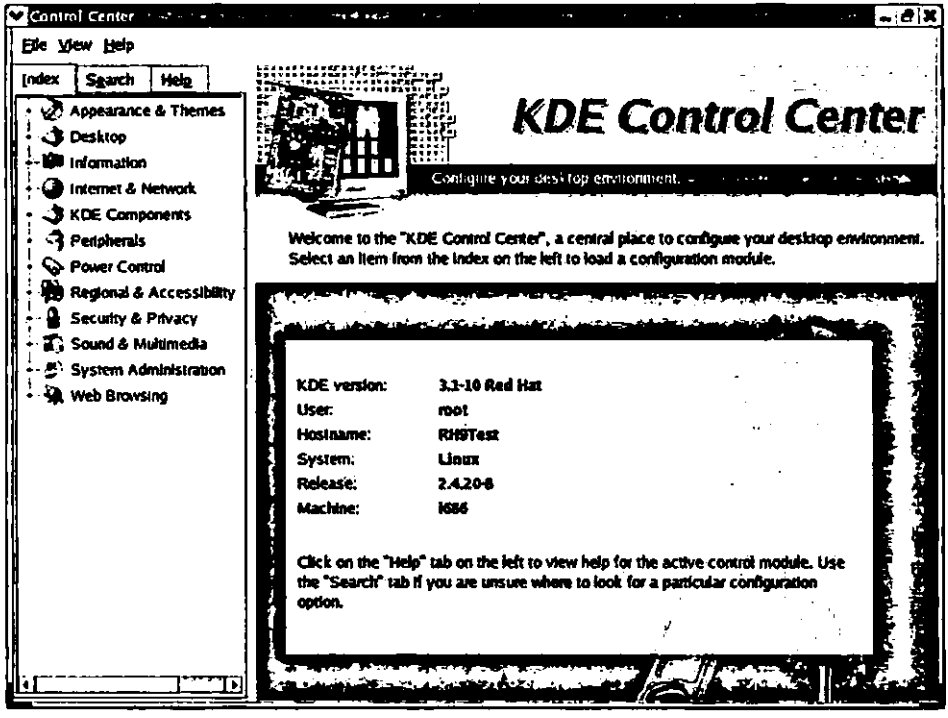
مرکز کنترل محیط گرافیکی KDE

در این قسمت مجموعه‌ای از ابزارهای پیکربندی مفید را که دسترسی به آن‌ها از طریق مرکز کنترل محیط گرافیکی KDE مهیا شده است، مورد بررسی قرار می‌دهیم. این ابزارها به منظور پیکربندی محیط گرافیکی طراحی شده‌اند. با وجود این تنظیمات دیگری را نیز در اختیار قرار می‌دهند. برای دسترسی به این ابزارها، کافی است گزینه Control Center از منوی اصلی را انتخاب کنید تا مشابه شکل ۸-۱۷ پنجره‌ای با عنوان Control Center باز شود.

چنان‌که مشاهده می‌کنید، امکانات پیکربندی درزمینه‌های مختلف از ظاهر محیط‌گرافیکی KDE گرفته تا نحوه دسترسی به وب فراهم شده است. کاربرد هریک از این ابزارها را به تدریج در قسمت‌های بعد توضیح خواهیم داد.

فراموش نکنید که پس از تغییر پیکربندی در هریک از این زمینه‌ها، برای ثبت آن‌ها در فهرست ~/.kde باید دکمه Apply را کلیک کنید. (از فصل هشتم به یاد دارید که علامت ~ به فهرست خانگی اشاره دارد.)

دسترسی به برخی از ابزارهای پیکربندی پنجره Control Center تنها توسط کاربر اصلی امکان‌پذیر است. کاربران عادی در مواقع مقتضی دکمه‌ای با عنوانAdministrator Mode را مشاهده خواهند کرد. پس از کلیک این دکمه و وارد کردن کلمه عبور کاربر اصلی در کادرمحاوره حاصل تحت عنوان Run As Root، کاربران عادی نیز می‌توانند چنین ابزارهایی را مورد استفاده قرار دهند.



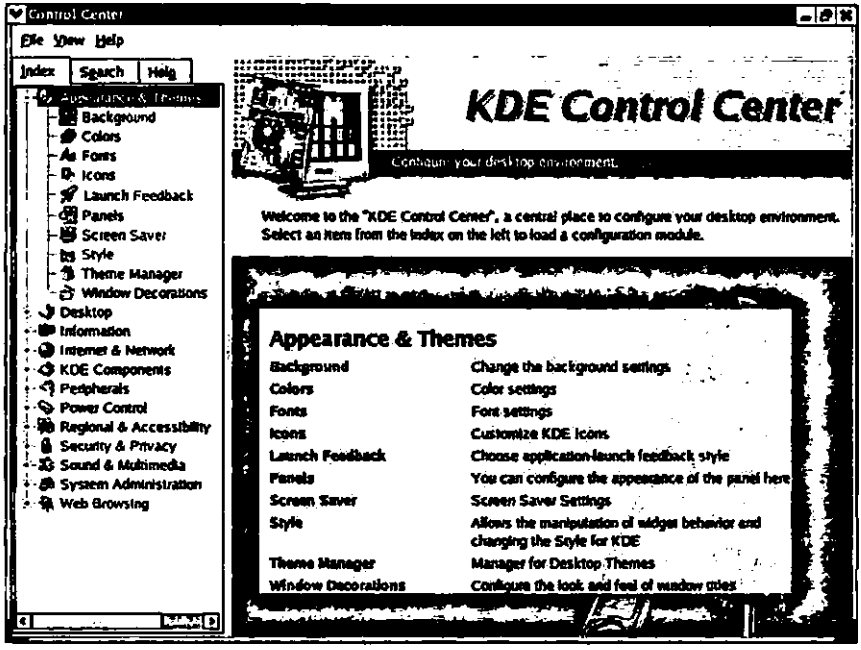
شکل ۸-۱۷ پنجره Control Center

ابزار Appearance & Themes

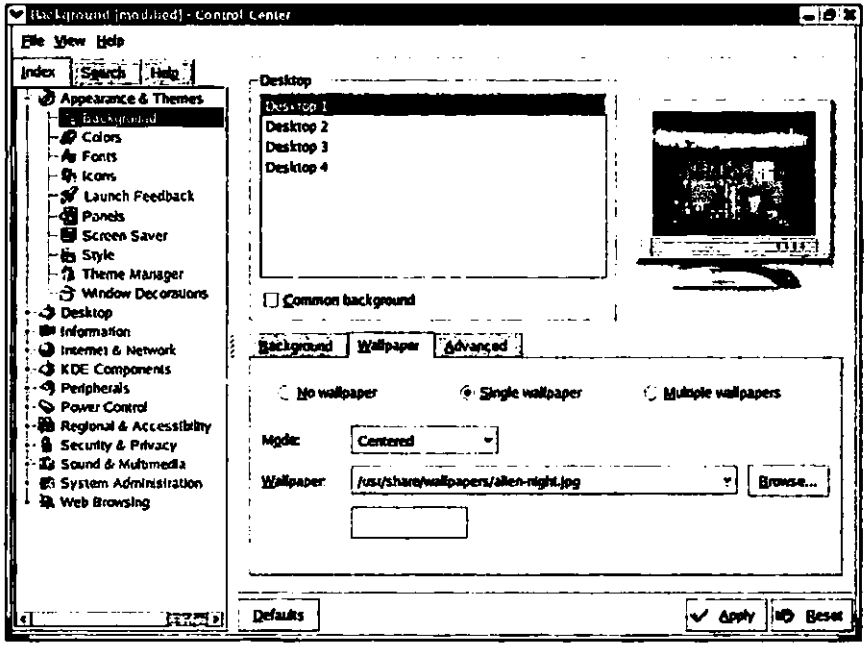
ابزار Appearance & Themes از پنجره Control Center امکانات متنوعی را به منظور تغییر ظاهر محیط گرافیکی KDE در اختیار می‌گذارد. به کمک تنظیماتی که در شکل ۹-۱۷ مشاهده می‌کنید، امکان پیکربندی موارد مختلف، از پس‌زمینه محیط کاری گرفته تا ظاهر پنجره‌ها مهیا شده است.

تنظیمات Background

به کمک این تنظیمات می‌توان ظاهر محیط‌های کاری را تغییر داد. در محیط گرافیکی KDE انجام این کار بسیار ساده است. چنان‌چه گزینه Common background فعال نشده باشد، در صورت تمایل حتی می‌توان پس‌زمینه محیط‌های کاری را به طور مستقل از یکدیگر پیکربندی کرد. شکل ۱۰-۱۷ این تنظیمات را نشان می‌دهد.



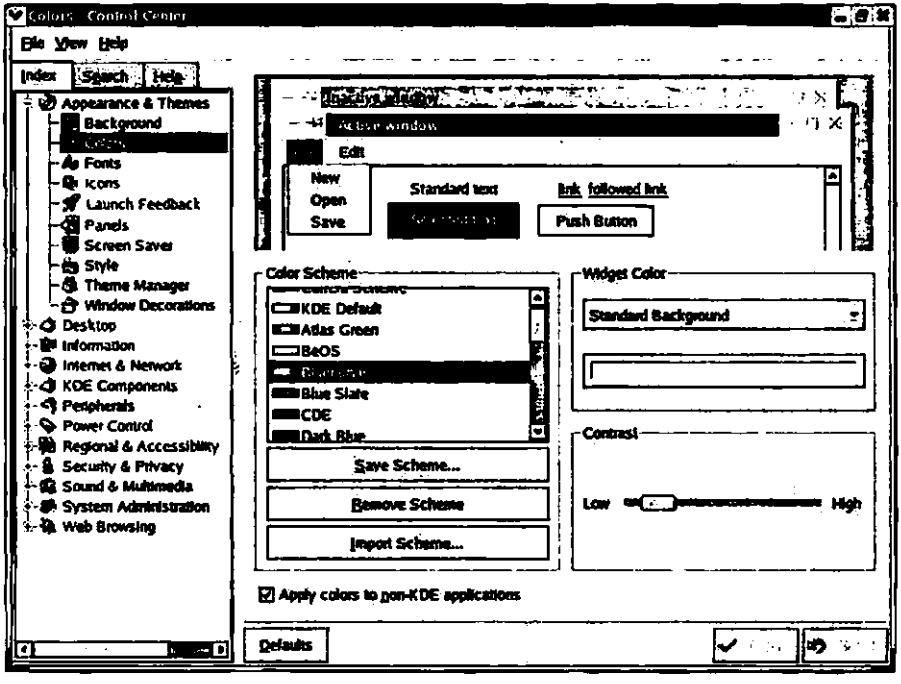
شکل ۹-۱۷ تنظیمات مختلف ابزار پیکربندی Appearance & Themes



شکل ۱۰-۱۷ تنظیمات Background

تنظیمات Colors

به کمک این تنظیمات می‌توان رنگ حاشیه پنجره‌ها، نوار عنوان پنجره‌ها، منوها، دکمه‌ها، پیوندها و سایر اجزا را تعیین کرد. در این مورد بیش از ۲۵ گزینه قابل پیکربندی وجود دارد. پس از انجام تنظیمات مورد نظر، در صورت تمایل می‌توان با کلیک دکمه Save Scheme پیکربندی حاصل را ذخیره کرد. هم‌چنین با کلیک دکمه Import Scheme و انتخاب الگوی پیکربندی موردنظر می‌توان این تنظیمات را به یکباره انجام داد. شکل ۱۱-۱۷ تنظیمات مورد بحث را نشان می‌دهد.



شکل ۱۱-۱۷ تنظیمات Colors

تنظیمات Fonts

این تنظیمات امکان انتخاب فونت‌های مورد استفاده در اجزای مختلف محیط گرافیکی KDE شامل منوها، نوار عنوان پنجره‌ها و مشابه آن‌ها را فراهم می‌کند.

تنظیمات Icons

این تنظیمات امکان تغییر آیکن‌های مورد استفاده در محیط گرافیکی KDE را فراهم می‌کند.

تنظیمات Launch Feedback

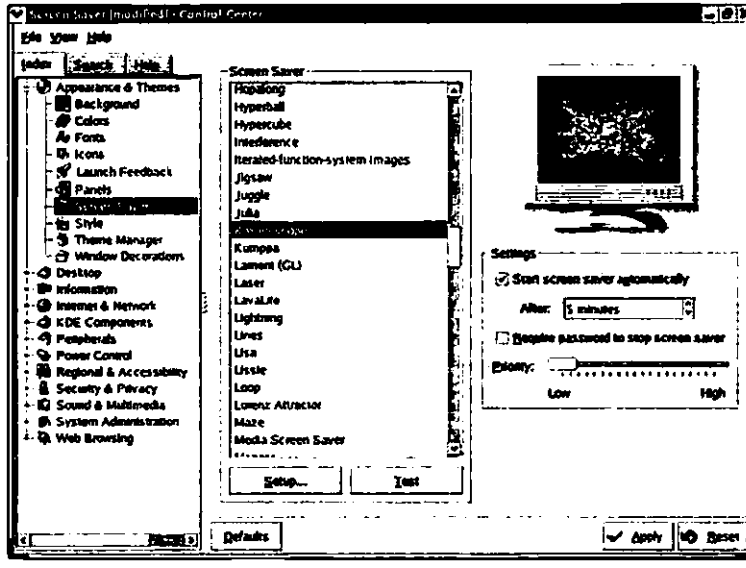
این تنظیمات امکان تعیین شکل مکان‌نمای ماوس حین بارگذاری برنامه‌های کاربردی بزرگی چون OpenOffice را در اختیار می‌گذارد. معمولاً برای این منظور از شکل یک ساعت شنی یا مشابه آن استفاده می‌شود.

تنظیمات Panels

این تنظیمات امکان تغییر رنگ دکمه‌های موجود روی پانل محیط گرافیکی KDE، از جمله دکمه منوی اصلی و برنامه‌های کاربردی را در اختیار می‌گذارد. تنظیمات Panels هم‌چنین امکان نمایش توصیف بسیار مختصری درباره هریک از این دکمه‌ها را در قالب خاصی تحت عنوان tooltip که با نگه‌داشتن اشاره‌گر ماوس روی آن دکمه‌ها به نمایش درمی‌آید، فراهم می‌کند.

تنظیمات Screen Saver

این تنظیمات به منظور پیکربندی محافظ صفحه نمایش (اصطلاحاً screensaver) پیش‌بینی شده است. چنان‌که شکل ۱۲-۱۷ نیز نشان می‌دهد، محیط گرافیکی KDE به همراه تعداد قابل توجهی محافظ صفحه نمایش عرضه شده است. تنظیمات Screen Saver امکان تعیین مدت زمان غیرفعال و هم‌چنین لزوم استفاده از کلمه عبور جهت دسترسی مجدد به محیط گرافیکی KDE را در اختیار می‌گذارد.



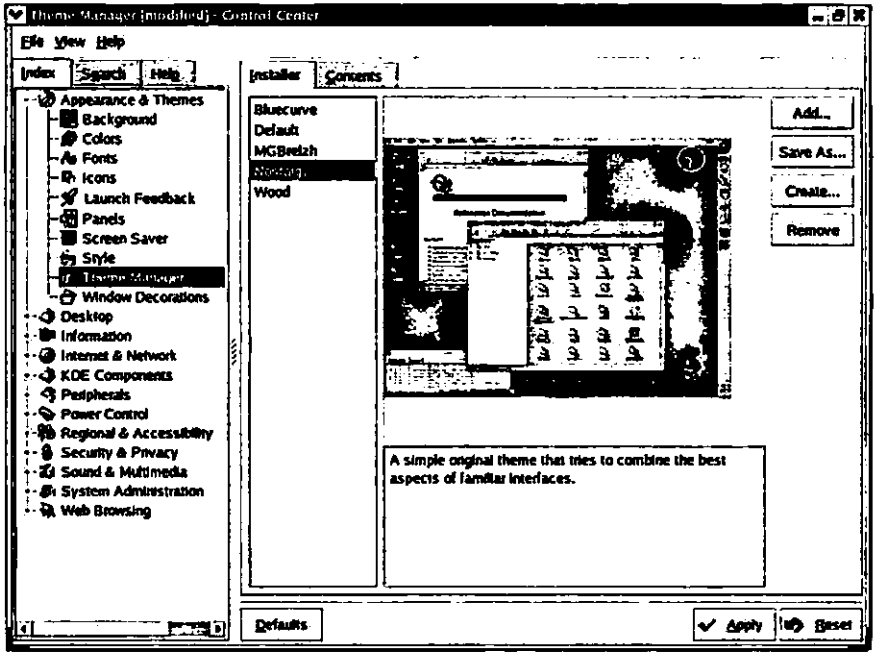
شکل ۱۲-۱۷ تنظیمات Screen Saver

تنظیمات Style

این تنظیمات امکان پیکربندی آرایش ظاهری دکمه‌ها، گزینه‌ها و سایر موارد را در قالب بیش از ۲۰ الگوی از پیش آماده در اختیار می‌گذارد. پس از تعیین آرایش مورد نظر، در صورت تمایل می‌توان تنظیمات بیشتری را به منظور پیکربندی آن انجام داد.

تنظیمات Theme Manager

این تنظیمات امکان انتخاب الگوی ظاهری محیط گرافیکی KDE را از میان الگوهای موجود در اختیار می‌گذارد. الگوی Bluecurve به عنوان الگوی پیش‌فرض در سیستم‌عامل Red Hat Linux در نظر گرفته شده است. پس از انتخاب الگوی مورد نظر، در صورت تمایل می‌توان تنظیمات دیگری را نیز انجام داد. شکل ۱۳-۱۷ امکانات موجود در این زمینه را نشان می‌دهد.



شکل ۱۳-۱۷ تنظیمات Theme Manager

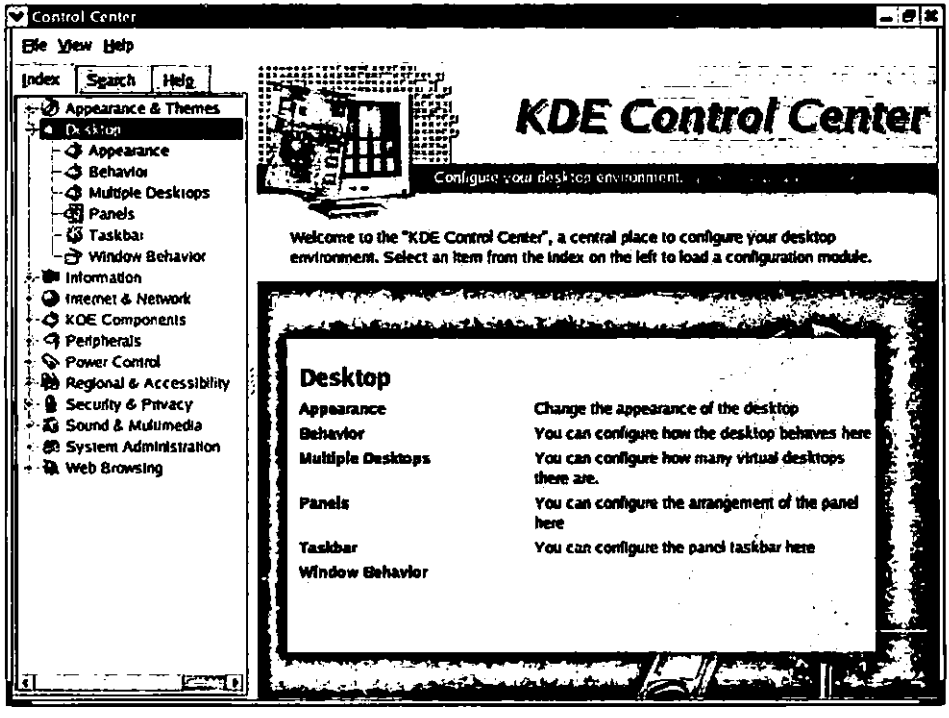
تنظیمات Window Decorations

این تنظیمات امکان تعیین شکل ظاهری پنجره‌ها، شامل حاشیه و نوار عنوان را با انتخاب الگوی موردنظر ازمیان‌الگوهای‌موجود فراهم می‌کند. به‌طور پیش‌فرض، شکل ظاهری پنجره‌ها در سیستم‌عامل

Red Hat Linux با الگوی Bluecurve، یعنی الگوی پیش‌فرض در سیستم‌عامل مذکور برای محیط گرافیکی KDE منطبق است.

ابزار Desktop

ابزار Desktop را می‌توان در واقع مکمل ابزار Appearance & Themes محسوب کرد، چرا که این ابزار نیز شامل تنظیماتی برای پیکربندی ظاهر محیط گرافیکی KDE است. چنان‌که شکل ۱۴-۱۷ نشان می‌دهد، به کمک ابزار Desktop می‌توان تنظیمات متنوعی از تعیین فونت‌های مورد استفاده در محیط گرافیکی KDE گرفته تا عکس‌العمل پنجره‌ها به حرکت اشاره‌گر ماوس را مشخص کرد. در ادامه به بررسی این تنظیمات می‌پردازیم.



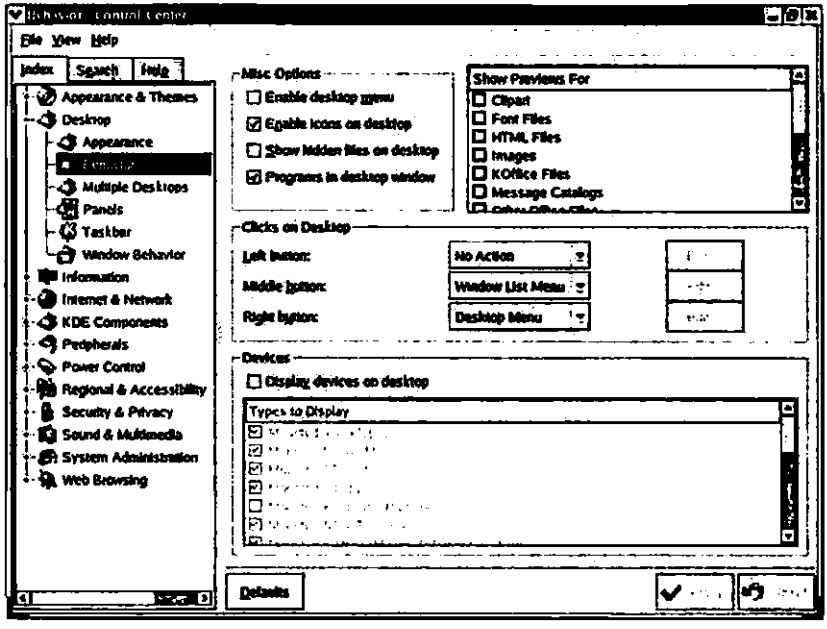
شکل ۱۴-۱۷ تنظیمات مختلف ابزار پیکربندی Desktop

تنظیمات Appearance

این تنظیمات امکان تعیین فونت مورد استفاده در محیط KDE و رنگ متون را در اختیار قرار می‌دهد.

تنظیمات Behavior

این تنظیمات امکان تغییر ظاهر آیکن‌های موجود در محیط گرافیکی گرافیکی KDE و برنامه Konqueror را (هنگامی که به عنوان ابزاری برای مدیریت فایل‌ها مورد استفاده قرار می‌گیرد) در اختیار می‌گذارد. تنظیمات Behavior هم‌چنین امکان تعیین عملکرد دکمه‌های ماوس و نیز امکان نمایش آیکن‌هایی را در محیط کاری KDE جهت اطلاع از قابل دسترسی بودن تجهیزات مختلف، هم‌چون پارتیشن‌ها، درایو CD و مانند آن فراهم می‌کند. شکل ۱۵-۱۷ این تنظیمات را نشان می‌دهد.



شکل ۱۵-۱۷ تنظیمات Behavior

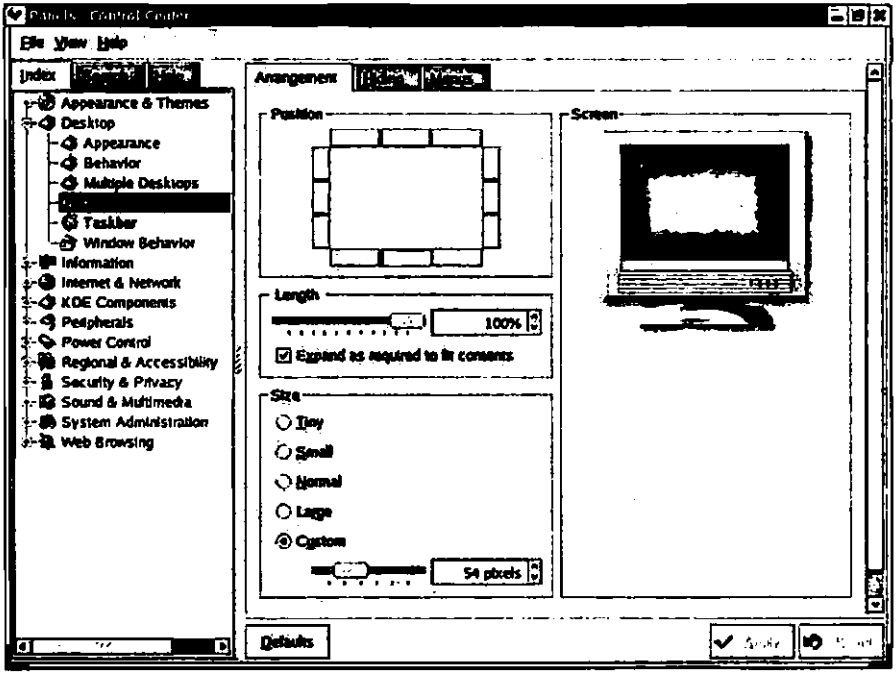
تنظیمات Multiple Desktop

محیط گرافیکی KDE به طور پیش‌فرض دارای چهار محیط کاری است. این تنظیمات امکان افزایش این را حداکثر تا ۱۶ محیط کاری در اختیار می‌گذارد.

تنظیمات Panels

این تنظیمات امکان تعیین موقعیت و اندازه پانل محیط گرافیکی KDE و هم‌چنین اندازه آیکن‌های مستقر روی آن‌را در اختیار می‌گذارد. در صورت تمایل می‌توان این تنظیمات را به نحوی انجام داد که

پانل مذکور پنهان شود. ضمناً تنظیمات مختلفی نیز در ارتباط با منوی اصلی پیش‌بینی شده است. شکل ۱۶-۱۷ تنظیمات Panels را نشان می‌دهد.



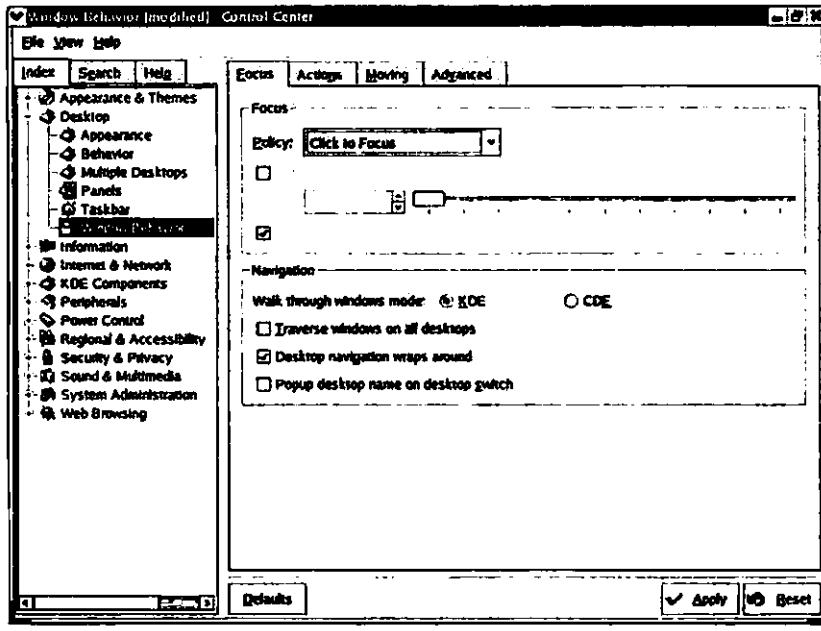
شکل ۱۶-۱۷ تنظیمات Panels

تنظیمات Taskbar

این ابزار امکان پیکربندی رفتار برنامه‌های کاربردی در حال اجرا و هم‌چنین تعیین عملکرد دکمه‌های ماوس را در اختیار می‌گذارد.

تنظیمات Window Behavior

این تنظیمات امکان تعیین رفتار پنجره‌ها را ضمن انتقال از یک موقعیت به موقعیت دیگر و هم‌چنین عکس‌العمل آن‌ها به حرکت اشاره‌گر ماوس را در اختیار قرار می‌دهد. تنظیمات پیشرفته شامل تعیین مشخصات حرکتی پنجره‌هاست. شکل ۱۷-۱۷ این تنظیمات را نشان می‌دهد.



شکل ۱۷-۱۷ تنظیمات Window Behavior

ابزار Information

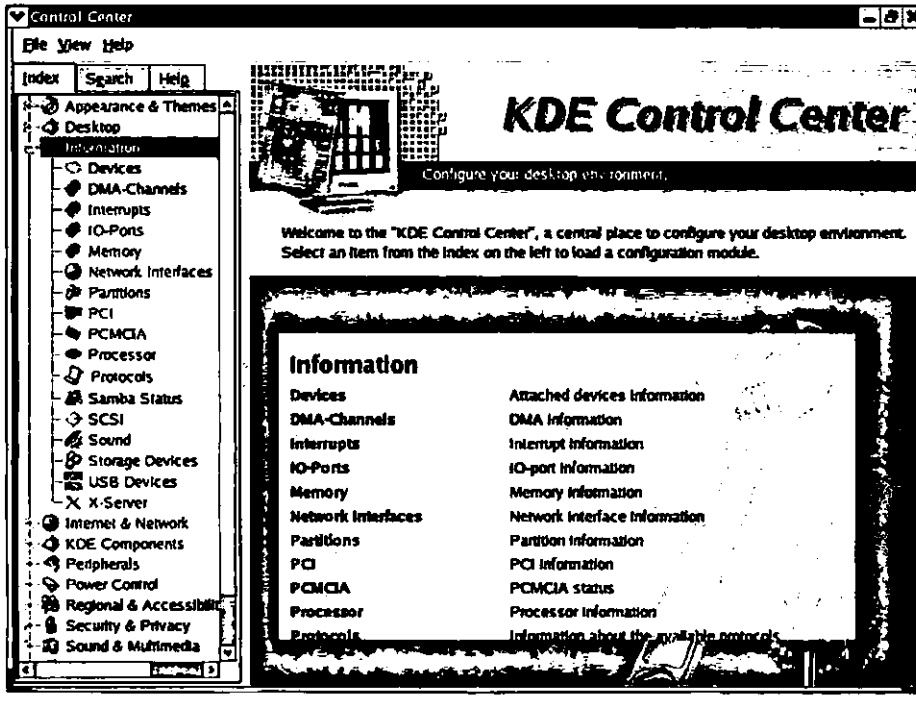
ابزار Information صرفاً جنبه اطلاع‌رسانی داشته و به منظور نمایش اطلاعاتی مربوط به تجهیزات سخت‌افزاری کامپیوتر میزبان طراحی شده است. ابزار مذکور بیشتر این اطلاعات را با مراجعه به زیرفهرست‌های proc/ مورد دستیابی قرار داده و نمایش می‌دهد. شرح مختصری از این تجهیزات سخت‌افزاری در جدول ۳-۱۷ آمده است. (برای توضیح بیشتر درباره فهرست proc/ به فصل یازدهم مراجعه کنید.) شکل ۱۸-۱۷ ابزار مورد بحث را نشان می‌دهد.

جدول ۳-۱۷ شرح گزینه‌های ابزار Information

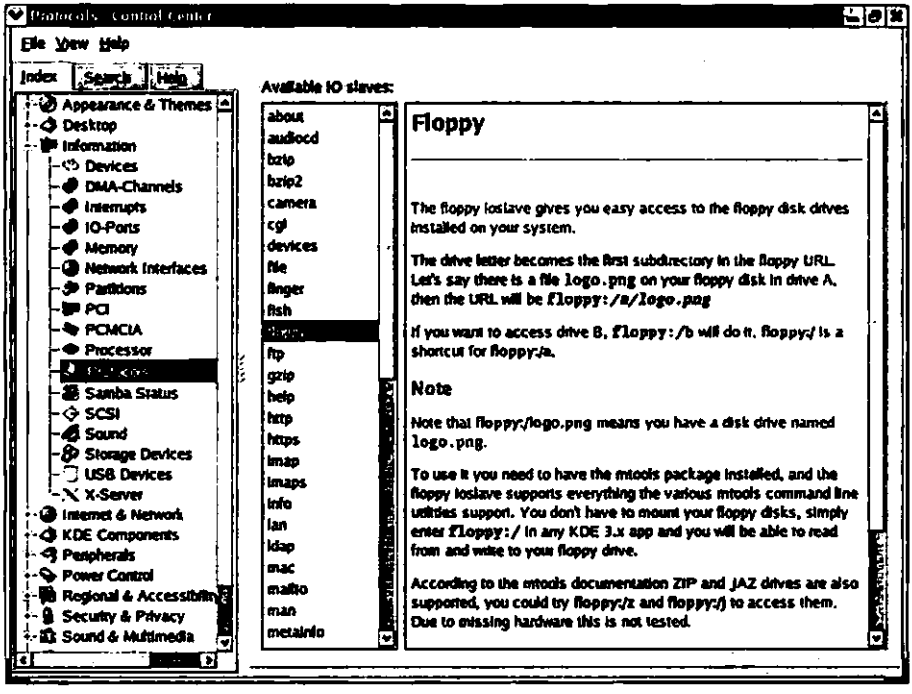
عنوان گزینه	توضیح
Devices	این گزینه فایل‌های سخت‌افزاری موجود در دو فهرست proc/devices/ و proc/misc/ را نمایش می‌دهد.
DMA-Channels	این گزینه با مراجعه به فهرست proc/dma/ اطلاعات مربوط به کانال‌های دسترسی مستقیم به حافظه موسوم به Direct Memory Access (به اختصار DMA) را اختیار می‌گذارد.

عنوان گزینه	توضیح
Interrupts	این گزینه با مراجعه به فهرست /proc/interrupts اطلاعات مربوط به کانال‌های درخواست وقفه یا Interrupt Request (به اختصار IRQ) را در اختیار می‌گذارد.
IO-Ports	این گزینه با مراجعه به فهرست /proc/ioports اطلاعات آدرس‌های ورودی و خروجی مربوط به تجهیزات سخت‌افزاری مختلف را در اختیار می‌گذارد.
Memory	این گزینه با مراجعه به فهرست /proc/meminfo وضعیت استفاده از حافظه RAM و فضای sawp را نمایش می‌دهد.
Network Interface	این گزینه آدرس IP کامپیوتر میزبان و مشخصات کارت یا کارت‌های شبکه متصل به آن‌را نمایش می‌دهد.
Partitions	این گزینه با مراجعه به فایل /etc/fstab، اطلاعاتی را درباره فهرست‌هایی که در حال حاضر روی سیستم فایل سوار شده‌اند، نمایش می‌دهد.
PCI	این گزینه با مراجعه به فهرست /proc/pci مشخصات کارت‌های PCI یا اصطلاحاً Peripheral Component Interconnect و کنترل کننده‌های مربوطه را در اختیار می‌گذارد. این اطلاعات ممکن است تجهیزات سخت‌افزاری پیکربندی نشده‌ای مانند کارت‌های شبکه یا مودم‌های طراحی شده برای کامپیوترهای ویندوز را نیز شامل شود.
PCMCIA	این گزینه با مراجعه به فهرست /proc/pci مشخصات کارتهای PCMCIA را که براساس استانداردی موسوم به Personal Computer Memory Card International Association ساخته شده‌اند، نمایش می‌دهد. استفاده از این گونه کارت‌ها که اغلب با عنوان کارت‌های PC نیز شناخته می‌شوند، در کامپیوترهای کیفی (اصطلاحاً laptop) متداول است.
Processor	این گزینه با مراجعه به فهرست /proc/cpuinfo مشخصات پردازنده‌های نصب شده روی کامپیوتر میزبان را نمایش می‌دهد.
Protocols	این گزینه تعاریف مربوط به تعدادی از پروتکل‌ها را در اختیار می‌گذارد. شکل ۱۹-۱۷ مثالی را در این زمینه نشان می‌دهد.
Samba Status	این گزینه وضعیت استفاده از سرویس Samba در شبکه میزبان را نمایش می‌دهد. (این سرویس جهت دسترسی مشترک به منابع مستقر در شبکه پیکربندی می‌شود.)
SCSI	این گزینه لیست انواع تجهیزات سخت‌افزاری موسوم به SCSI یا اصطلاحاً Small Computer System Interface راکه به‌کامپیوترمیزبان متصل شده است، نمایش می‌دهد.
Sound	این گزینه مشخصات کارت صوتی متصل به کامپیوتر میزبان را نمایش می‌دهد.

عنوان گزینه	توضیح
Storage Devices	این گزینه مشخصات تجهیزات ذخیره‌سازی سوار شده روی سیستم فایل کامپیوتر میزبان را نمایش می‌دهد. این اطلاعات در واقع بازتاب نتیجه اجرای فرمان mount است.
USB Devices	این‌گزینه مشخصات تجهیزات‌سخت‌افزاری USB نصب شده روی کامپیوتر میزبان را نشان می‌دهد.
X-Server	این گزینه با مراجعه به فهرست /etc/X11/XF86Config، مشخصات پیکربندی مربوط به تجهیزات نمایشی را در اختیار قرار می‌دهد.



شکل ۱۸-۱۷ ابزار Information



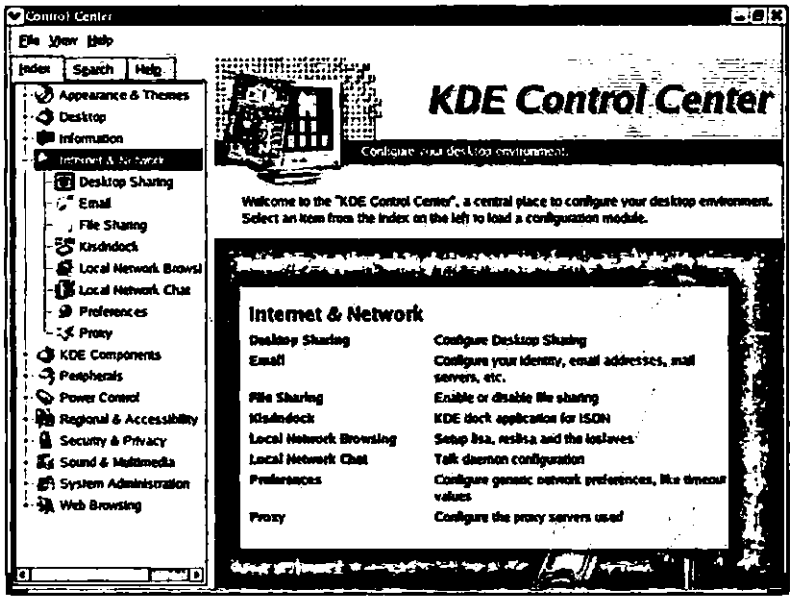
شکل ۱۹-۱۷ گزینه Protocols اطلاعات مربوط به برخی از پروتکل‌ها را در اختیار می‌گذارد.

ابزار Internet & Network

ابزار internet & Network تنظیمات متنوعی را به منظور پیکربندی پارامترهای شبکه و فهرست‌های مشترک در اختیار می‌گذارد. چنان‌که شکل ۲۰-۱۷ نشان می‌دهد، این تنظیمات مواردی مختلفی از قبیل پست الکترونیکی و سرورهای پروکسی را شامل می‌شود. چنان‌چه با انتخاب گزینه مربوط به هریک از این تنظیمات پیغام خطایی را مشاهده می‌کنید، به احتمال قوی هنوز بسته نرم‌افزاری مربوطه را نصب نکرده‌اید.

تنظیمات Desktop Sharing

این تنظیمات به منظور پیکربندی سرویس Virtual Network Computing یا به اختصار VNC پیش‌بینی شده است. به واسطه این سرویس، سایر کامپیوترها می‌توانند محیط گرافیکی کامپیوتر میزبان را از راه دور مورد دسترسی قرار دهند. (برای اطلاع بیشتر درباره سرویس VNC به فصل شانزدهم مراجعه کنید.)



شکل ۲۰-۱۷ ابزار Internet & Network

تنظیمات Email

این تنظیمات امکان تعیین مقادیر پیش‌فرض پارامترهای موردنیاز جهت ارسال پیغام‌های الکترونیکی، شامل نام و آدرس پست الکترونیکی ارسال کننده پیغام، آدرس الکترونیکی مقصد و آدرس سرور ارسال کننده پیغام (اصطلاحاً SMTP Server) را در اختیار می‌گذارد.

تنظیمات File Sharing

این تنظیمات امکان استفاده مشترک از فایل‌های موجود در فهرست خانگی را از طریق شبکه در اختیار سایر کاربران قرار می‌دهد. روش‌های متداول برای اشتراک فایل‌ها عبارتند از Network File System (یا به اختصار NFS) و Samba که برای توضیح بیشتر می‌توانید به فصول مربوطه از این کتاب، یعنی بیست و هشتم و بیست و نهم مراجعه کنید.

تنظیمات Kisdndock

این تنظیمات امکان پیکربندی تجهیزاتی را که قادر به استفاده در شبکه‌های ISDN یا اصطلاحاً Integrated Services Digital Network هستند در اختیار می‌گذارد. سرعت انتقال داده‌ها در این گونه شبکه‌ها تقریباً دو برابر سرعت انتقال داده‌ها در خطوط تلفن معمولی است. به دلیل استفاده گسترده از

شبکه‌های ISDN در اروپا، تعجبی ندارد که محیط گرافیکی KDE (که بیشتر کار توسعه آن در همین قاره انجام شده است) پشتیبانی جامعی از این شبکه به عمل آورد.

تنظیمات Local Network Browsing

این تنظیمات امکان تعیین شناسه کاربری و کلمه عبور پیش‌فرض به منظور دسترسی به فهرست‌ها و چاپگرهای مشترک را از طریق سرویس Samba در اختیار می‌گذارد. چنان‌که در فصل بیست و نهم توضیح داده شد، این یک روش‌متداول برای‌دسترسی‌به فهرست‌ها و چاپگرهای مشترک از کامپیوترهای ویندوز است.

تنظیمات Local Network Chat

این تنظیمات امکان پیکربندی سرویس گپ‌زنی در شبکه محلی را مهیا می‌کند. به واسطه این سرویس کاربران به سادگی می‌توانند از طریق شبکه محلی با یکدیگر گفتگو کنند.

تنظیمات Preferences

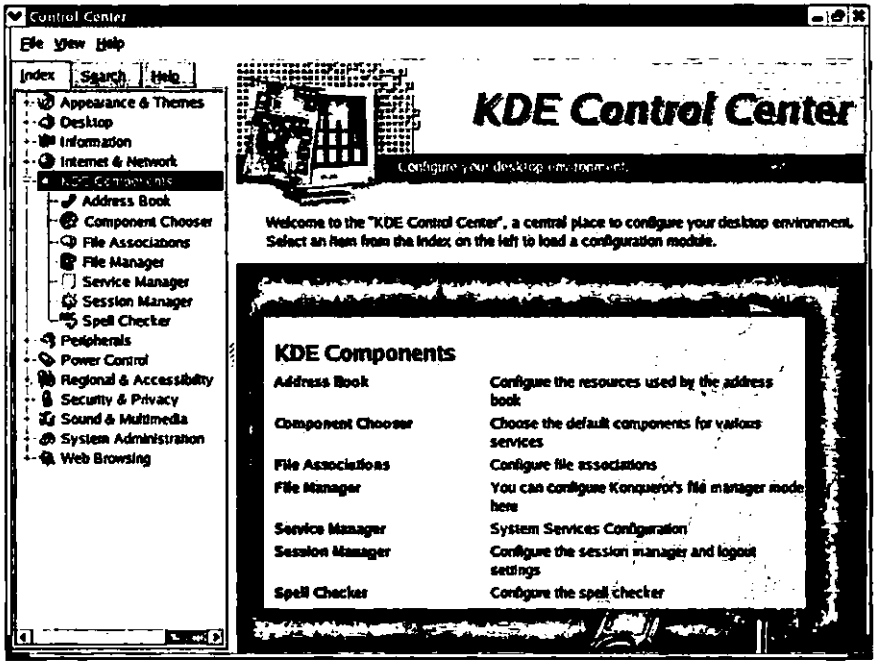
این تنظیمات امکان تعیین عکس‌العمل برخی از برنامه‌های KDE را هنگام برقراری ارتباط با یک شبکه خارجی هم‌چون اینترنت در اختیار می‌گذارد. برای مثال، به کمک تنظیمات فوق می‌توان حداکثر مدت زمان ارسال درخواست مکرر مرورگر وب برای دستیابی به وب سایت‌های کند را تعیین کرده و پارامترهای حالت غیرفعال (اصطلاحاً passive mode) را که برای دسترسی به برخی از سایت‌های FTP ضروری است، پیکربندی کرد.

تنظیمات Proxy

امنیت‌برخی از شبکه‌ها به واسطه وجود نوعی سرور با عنوان پروکسی تأمین می‌شود. چنان‌چه کامپیوتر میزبان در چنین شبکه‌ای مستقر شده باشد، با استفاده از این تنظیمات می‌توان دسترسی به شبکه‌های خارجی را از طریق سرور نامبرده مشخص کرد.

ابزار KDE Components

ابزار KDE Components تنظیماتی را به منظور پیکربندی ابزارهای مختلف محیط گرافیکی KDE در اختیار می‌گذارد. این تنظیمات مواردی از قبیل منابع کتاب آدرس (اصطلاحاً address book) تا خروج از محیط گرافیکی KDE را شامل می‌شود. شکل ۲۱-۱۷ این ابزار را نشان می‌دهد.



شکل ۲۱-۱۷ ابزار KDE Components

تنظیمات Address Book

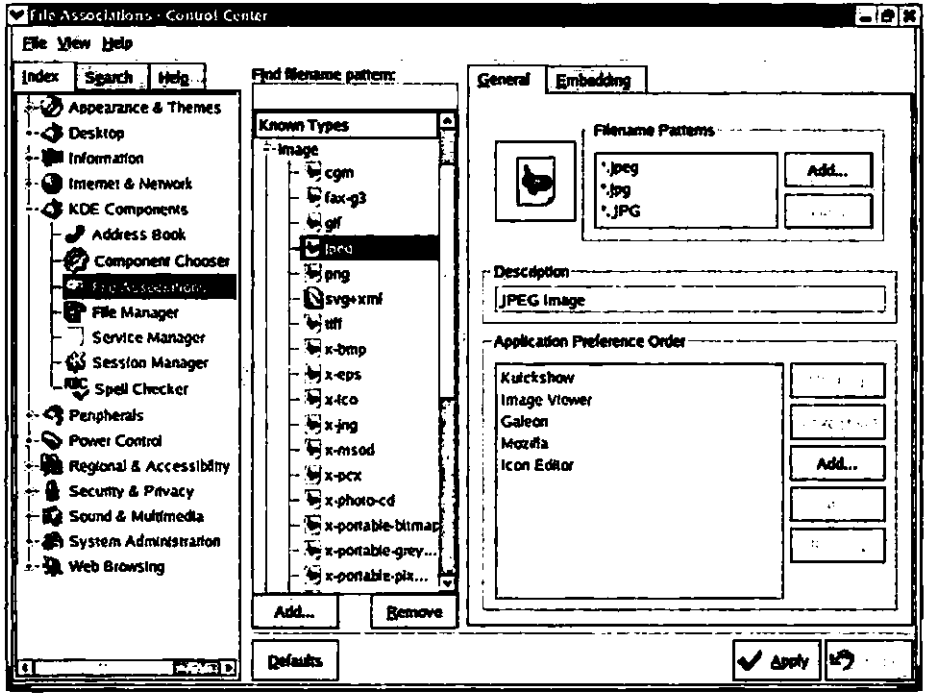
این تنظیمات امکان پیکربندی کتاب آدرس را به منظور استفاده از محتوای فایل‌های استاندارد vcf. و هم‌چنین سایر فایل‌ها و بانک‌های اطلاعاتی LDAP (اصطلاحاً Lightweight Directory Assistance Protocol) را در اختیار می‌گذارد.

تنظیمات Component Chooser

این تنظیمات امکان تعیین برخی موارد پیش فرض، از جمله برنامه کلاینت مورد استفاده جهت مدیریت پیغام‌های الکترونیکی، برنامه شبیه‌ساز ترمینال (اصطلاحاً terminal emulator) و ویرایشگر متنی مورد استفاده در سایر برنامه‌های کاربردی را در اختیار می‌گذارد.

تنظیمات File Associations

این تنظیمات امکان تعیین برنامه‌های کاربردی مورد استفاده برای پردازش انواع فایل‌ها را در اختیار می‌گذارد. برای مثال، شکل ۲۲-۱۷ برنامه‌های کاربردی مورد استفاده برای نمایش محتوای فایل‌های تصویری jpg. را نشان می‌دهد.



شکل ۲۲-۱۷ تنظیمات File Associations

تنظیمات File Manager

این تنظیمات امکاناتی را به منظور تغییر ظاهر گرافیکی و رفتار برنامه Konqueror در اختیار می‌گذارد. تنظیمات فوق مواردی از قبیل تعیین فونت، تعیین عکس‌العمل برنامه Konqueror هنگام ایجاد فهرست‌های جدید، لزوم تأیید عملیات حذف فایل‌ها و نمایش محتوای فایل‌های مختلف در قالب preview یا thumbnail را شامل می‌شود.

تنظیمات Service Manager

همان‌گونه که ضمن راه‌اندازی سیستم‌عامل Linux برخی از سرویس‌ها راه‌اندازی شده و برنامه‌های شبح مختلفی به اجرای درمی‌آید، ورود به محیط گرافیکی KDE نیز موجب راه‌اندازی برخی از سرویس‌ها می‌شود. این تنظیمات امکان تعیین سرویس‌هایی را که ضمن ورود به محیط گرافیکی KDE باید راه‌اندازی شوند و هم‌چنین سرویس‌هایی را که تنها در مواقع لزوم پس از ورود به این محیط گرافیکی باید راه‌اندازی شوند، فراهم می‌کند.

تنظیمات Session Manager

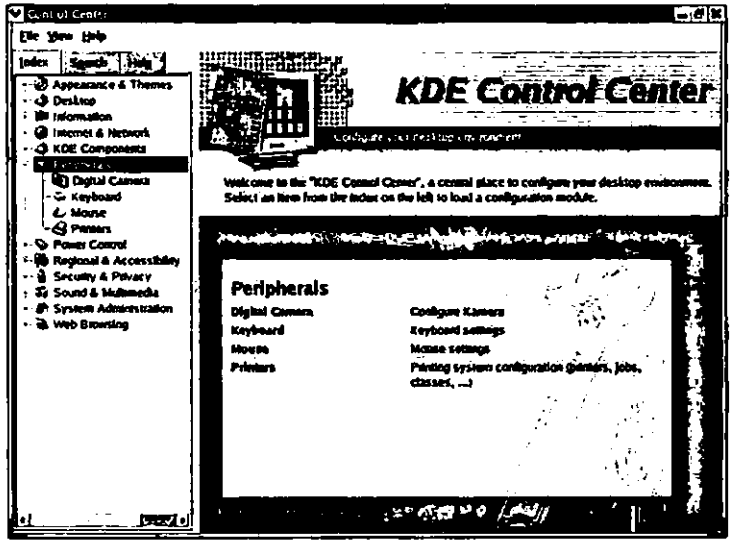
این تنظیمات امکان پیکربندی برخی از رفتارها را هنگام ورود به محیط گرافیکی KDE و خروج از آن فراهم می‌کند. برای نمونه، در صورت تمایل می‌توان ترتیبی داد تا برنامه‌هایی که هنگام خروج از محیط گرافیکی KDE باز بودند، طی دفعات آتی ورود به این محیط مجدداً به طور خودکار باز شوند. تنظیمات مورد بحث هم‌چنین امکان خروج از سیستم‌عامل Linux، راه‌اندازی مجدد کامپیوتر و حتی خاموش کردن کامپیوتر را در ازای خروج از محیط گرافیکی KDE در اختیار می‌گذارد.

تنظیمات Spell Checker

این تنظیمات امکان تعیین برنامه پیش‌فرض جهت بررسی املای واژگان مختلف را در اختیار می‌گذارد. تنوع‌این‌گونه برنامه‌ها به‌میزان پشتیبانی سیستم‌عامل Red Hat Linux از زبان‌های مختلف بستگی دارد. (برای‌پشتیبانی از یک زبان به‌خصوص باید بسته نرم‌افزاری مربوطه را روی کامپیوتر میزبان نصب کنید.)

ابزار Peripherals

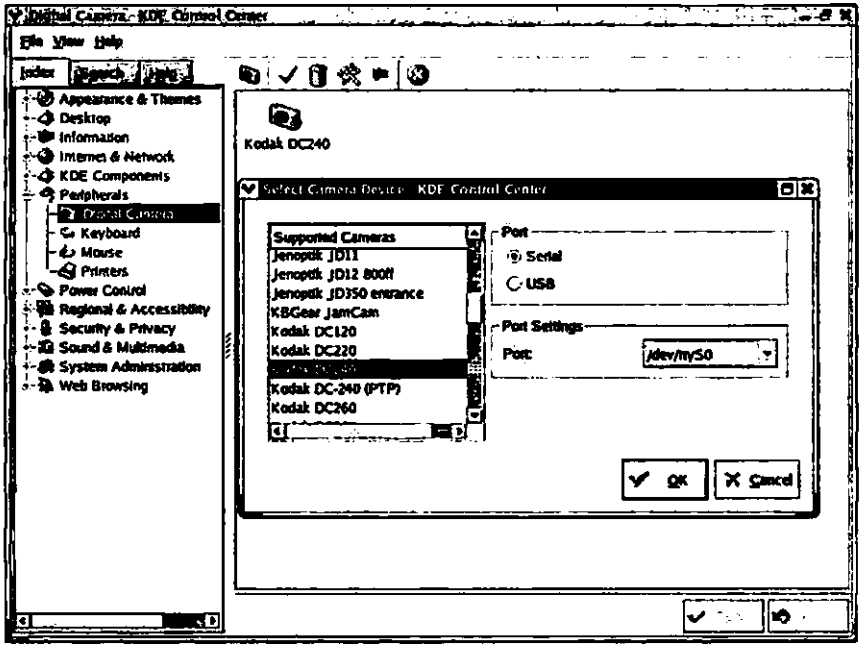
ابزار Peripherals تنظیمات لازم به منظور پیکربندی تجهیزات سخت‌افزاری خارجی شامل دوربین دیجیتالی، صفحه کلید، ماوس (یا عموماً ابزار اشاره‌گر) و چاپگر را در اختیار می‌گذارد. شکل ۲۳-۱۷ این ابزار را نشان می‌دهد.



شکل ۲۳-۱۷ ابزار Peripherals

تنظیمات Digital Camera

این تنظیمات امکان پیکربندی دوربین‌های دیجیتالی را به منظور دسترسی در محیط گرافیکی KDE در اختیار می‌گذارد. شکل ۲۴-۱۷ نحوه پیکربندی دوربین دیجیتالی مدل Kodak DC240 را نشان می‌دهد.



شکل ۲۴-۱۷ تنظیمات Digital Camera

تنظیمات Keyboard

این تنظیمات امکان پیکربندی برخی از پارامترهای صفحه کلید، هم‌چون فرکانس چشمک زدن مکان‌نما روی صفحه، وضعیت پیش‌فرض چراغ کلید Num Lock و پاسخ پیش‌فرض به برخی از اقدامات را در اختیار می‌گذارد.

تنظیمات Mouse

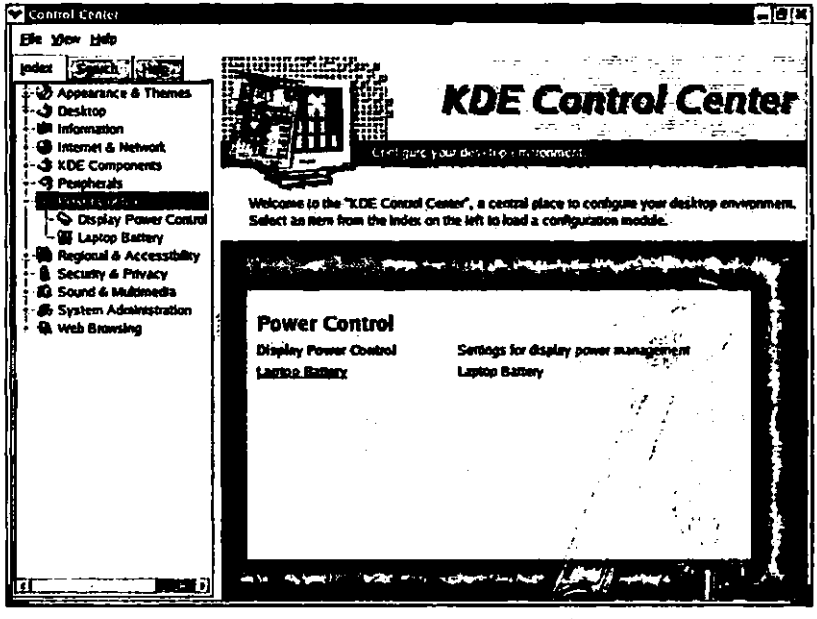
این تنظیمات به منظور پیکربندی کلیدهای ماوس، کلیک ساده و دابل کلیک و هم‌چنین نحوه رفتار اشاره‌گر ماوس پیش‌بینی شده است. در صورت تمایل می‌توان ترتیبی داد تا اشاره‌گر ماوس با فشار کلیدهای عددی مستقر در سمت راست صفحه کلید نیز به حرکت درآید.

تنظیمات Printers

در محیط گرافیکی KDE وظایف چاپی را علاوه بر چاپگر می‌توان برای دستگاه فاکس نیز ارسال یا در قالب یک فایل چاپ کرد. تنظیمات Printers امکانات لازم برای انجام این کار را در اختیار قرار می‌دهد.

ابزار Power Control

ابزار Power Control تنظیماتی را به منظور استفاده صحیح از منبع تغذیه در اختیار می‌گذارد. از این‌رو، به ویژه در صورت نصب سیستم‌عامل Red Hat Linux روی کامپیوترهای قابل حمل، می‌توان مقادیر قابل توجهی در مصرف برق صرفه‌جویی کرد. شکل ۲۵-۱۷ این ابزار را نشان می‌دهد.

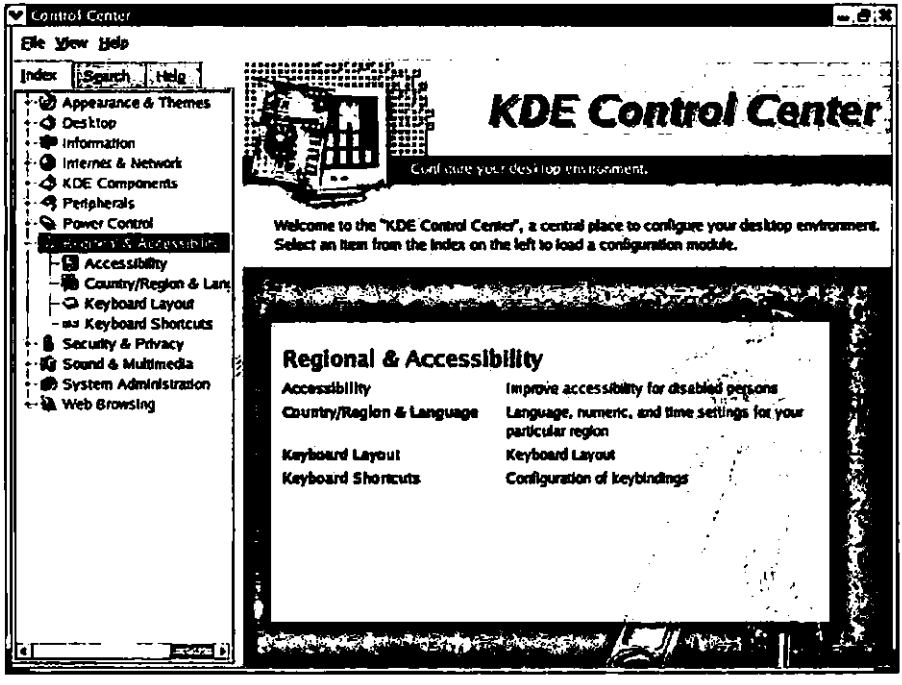


شکل ۲۵-۱۷ ابزار Power Control

تنظیمات Display Power Control امکان تعیین شرایطی را که کامپیوتر باید در یکی از حالات آماده به کار، تعلیق یا خاموش قرار بگیرد، فراهم می‌کند. این شرایط عموماً سپری شدن یک مدت زمان مشخص در حالت غیرفعال یا اصطلاحاً Inactivity است. (این حالت هنگامی محقق می‌شود که کاربر هیچ‌یک از دکمه‌های ماوس را کلیک نکرده و کلیدی را فشار نداده باشد.) تنظیمات Laptop Battery نیز امکاناتی را به منظور کنترل توان مصرفی و تعیین برخی از اقدامات پیش‌فرض در ازای افت توان باتری کامپیوتر به مقدار مشخص در اختیار می‌گذارد.

ابزار Regional & Accessibility

ابزارRegional & Accessibility تنظیماتی را به منظور تعیین نحوه قالب‌بندی و نمایش برخی اطلاعات با توجه به ملیت‌ها و زبان‌های مختلف در اختیار می‌گذارد. به کمک این تنظیمات می‌توان کلیدهای کنترلی را با کلیدهای موردنظر ترکیب کرده و کلید میانبر ایجاد کرد. هم‌چنین می‌توان ترتیبی داد تا با فشار کلیدهای موردنظر از بلندگوی داخلی کامپیوتر صدای بیپ به گوش برسد. شکل ۲۶-۱۷ این ابزار را نشان می‌دهد. جدول ۴-۱۷ حاوی شرح مختصری درباره تنظیماتی است که این ابزار در اختیار می‌گذارد.



شکل ۲۶-۱۷ ابزار Regional & Accessibility

جدول ۴-۱۷ شرح تنظیمات ابزار Regional & Accessibility

عنوان ابزار	توضیح
Accessibility	این تنظیمات امکان تولید صدای بیپ را در ازای فشار هر کلید و هم‌چنین قبول یا عدم قبول کلید فشار داده شده از جانب سیستم‌عامل را در اختیار می‌گذارد. علاوه بر این، امکاناتی را نیز به منظور تعیین برخی خصوصیات صفحه کلید، از جمله مدت

عنوان ابزار	توضیح
	زمان موردنیاز برای پایین نگه داشتن کلیدها برای تایپ کاراکترهای مورد نظر، فشار دادن پشت سرهم کلیدهای ترکیبی به جای پایین نگه داشتن یک یا دو کلید کنترلی و سپس فشار دادن کلید مورد نظر، و صرف نظر از تأثیر کلیدهایی را که به طور ناخواسته فشار داده شده‌اند، در اختیار قرار می‌دهد. مورد آخر معمولاً در مواقعی رخ می‌دهد که کاربر کلیدی را فشار داده و بلافاصله (یعنی در مدت زمانی که با این تنظیمات مشخص می‌شود) مجدداً همان کلید را به طور ناخواسته، مثلاً به دلیل لغزش دست یا موارد دیگر فشار می‌دهد.
Country/Region & Language	این تنظیمات امکان پیکربندی قالب نمایش اعداد، مبالغ پولی، تاریخ، ساعت و سیستم‌های اندازه‌گیری را در اختیار می‌گذارد.
Keyboard Layout	این تنظیمات امکان پیکربندی صفحه کلید را جهت تطبیق با چند زبان مختلف در اختیار می‌گذارد. علاوه براین، امکان تعریف کلیدهای میانبر را فراهم می‌کند. (کلیدهای میانبر با ترکیب یکی از کلیدهای کنترلی Alt، Ctrl، Shift، Caps Lock و مانند آن با کلیدهای موردنظر ساخته می شوند.)
Keyboard Shortcuts	این تنظیمات امکان پیکربندی کلیدهای میانبر را به منظور انجام طیف متنوعی از عملیات در اختیار می‌گذارد.

ابزار Security & Privacy

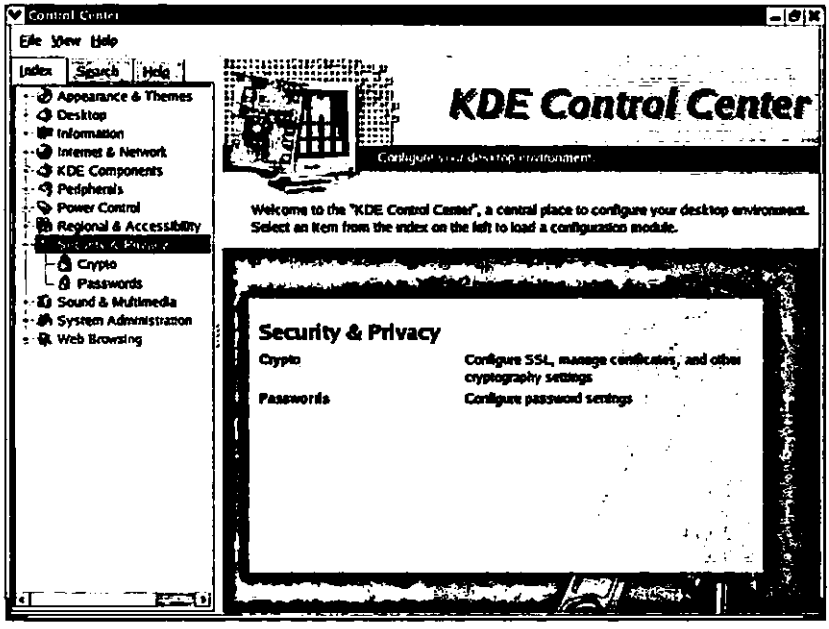
ابزار Security & Privacy تنظیماتی را به منظور رمزگذاری داده‌ها و تعیین کلمه عبور در اختیار می‌گذارد. شکل ۲۷-۱۷ این ابزار را نشان می‌دهد.

تنظیمات Crypto به منظور پیکربندی پارامترهای رمزگذاری پروتکل Secure Socket Layer (به اختصار SSL) پیش‌بینی شده است. تنظیمات Password نیز امکان بازتاب کلمه عبور تایپ شده را در اختیار می‌گذارد. تنظیمات مذکور هم‌چنین امکان تعیین مدت زمانی را که محیط گرافیکی KDE آخرین کلمات عبور وارد شده را به خاطر می‌سپارد، در اختیار می‌گذارد.

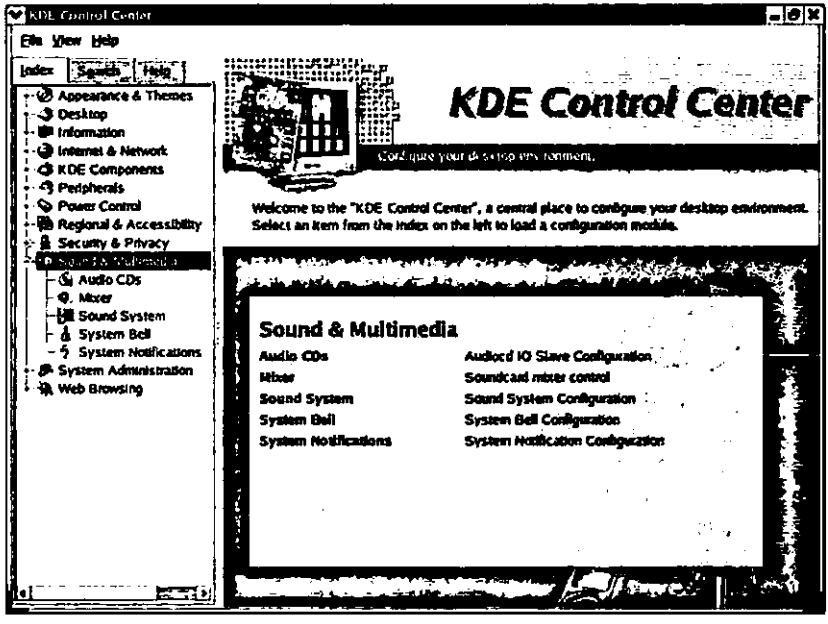
ابزار Sound & Multimedia

ابزار Sound & Multimedia تنظیماتی را به منظور پیکربندی کارت صوتی و تعیین مواردی چون شاخص فایل‌های موسیقی، تنظیمات پیش‌فرض شدت صدای خروجی، میکسر، نرخ ورودی، شدت صدای بیپ تولیدشده توسط سیستم و تعیین صداهای مرتبط با وقایع سیستمی را در اختیار می‌گذارد.

شکل ۲۸-۱۷ تنظیمات مختلف این ابزار را نشان می‌دهد.



شکل ۲۷-۱۷ ابزار Security & Privacy



شکل ۲۸-۱۷ ابزار Sound & Multimedia

تنظیمات Audio CDs

این تنظیمات در قالب چند گروه دسته‌بندی شده است. جدول ۵-۱۷ امکانات موجود در هر گروه را به اختصار شرح می‌دهد.

جدول ۵-۱۷ شرح امکانات پیکربندی موجود در گروه‌های مختلف ابزار Audio CDs

عنوان گروه	توضیح
CDDA	تنظیمات این گروه با عنوان Compact Disk Digital Audio امکان شناسایی CD و تصحیح خطا را در اختیار می‌گذارد.
CDDB	تنظیمات این گروه با عنوان Compact Disk Data Base امکان پیکربندی برنامه‌های پخش CD یا اصطلاحاً CD player را جهت دسترسی به اطلاعات بیشتر درباره ترانه‌ها و CD ها از طریق مراجعه به سرورهای مربوطه (اصطلاحاً CDDB server) در اختیار می‌گذارد. برخی از این سرورها از طریق آدرس freedb.org به طور رایگان قابل دستیابی هستند.
MP3	مکانیزم MPEG audio layer 3 یا اصطلاحاً MP3 روش متداولی برای فشرده‌سازی فایل‌های صوتی بدون از دست دادن کمترین کیفیت است. تنظیمات این گروه امکان تعیین مواردی چون مشخصات فشرده‌سازی، فیلترهای مورد استفاده در این زمینه و شیوه‌های کدگزاری را در اختیار قرار می‌دهد.
Ogg Vorbis	تنظیمات این گروه امکان پیکربندی مکانیزم دیگری برای فشرده‌سازی فایل‌های صوتی با عنوان Ogg Vorbis را در اختیار می‌گذارد. (عنوان این مکانیزم از یک بازی ویدیویی و شخصیت یکی از داستان‌ها اقتباس شده است.)

تنظیمات Mixer

این تنظیمات امکان تعیین شدت صدای خروجی و مقادیر پارامترهای میکسر را در اختیار می‌گذارد.

تنظیمات Sound System

این تنظیمات امکان پیکربندی سرور صوتی (اصطلاحاً sound server) محیط گرافیکی KDE با عنوان aRts را که در واقع یک سینتی‌سایزر آنالوگ است، در قالب چهار گروه مختلف فراهم می‌کند. شرح مختصری درباره هریک از این گروه‌ها در جدول ۶-۱۷ آمده است.

جدول ۶-۱۷ شرح امکانات پیکربندی موجود در گروه‌های مختلف تنظیمات Sound System

عنوان گروه	توضیح
aRts	تنظیمات این گروه امکان پیکربندی مشخصات سرور صوتی محیط گرافیکی KDE، از جمله تعیین اصوات مربوط به پیغام‌های مختلف سرور، شامل خطاها، اخطارها، پیغام‌های حاوی اطلاعات و هم‌چنین راهنمایی‌های لازم برای اشکال‌زدایی را در اختیار می‌گذارد.
Sound I/O	تنظیمات این گروه امکان پیکربندی ورودی و خروجی، کیفیت صدای خروجی و اندازه بافر مورد استفاده برای ذخیره اطلاعات صوتی را در اختیار می‌گذارد.
Mixer	تنظیمات این گروه امکان تعیین شدت صدای خروجی و مقادیر پارامترهای میکسر را در اختیار می‌گذارد.
MIDI	تنظیمات این گروه امکان پیکربندی رابط سینتی‌سایزر را بر اساس رابط دیجیتالی تجهیزات موسیقی (اصطلاحاً Musical Instrument Digital Interface) در اختیار می‌گذارد.

تنظیمات System Bell

این تنظیمات به منظور پیکربندی مشخصات صدای بیپ تولید شده توسط سیستم، از جمله شدت صدا و فرکانس پیش‌بینی شده است.

تنظیمات System Notifications

این تنظیمات امکان پیکربندی پیغام‌های صوتی و متنی مربوط به مجموعه متنوعی از رخدادها را در اختیار می‌گذارد. شکل ۲۹-۱۷ این تنظیمات را نشان می‌دهد.

با انتخاب گزینه موردنظر از لیست موجود در قسمت بالای شکل ۲۹-۱۷ می‌توان تنظیمات صوتی مربوط به رخدادهای آن گزینه به خصوص را انجام داد. جدول ۷-۱۷ تنظیماتی را که از طریق این گزینه‌ها قابل دستیابی است، به اختصار شرح می‌دهد.

جدول ۷-۱۷ شرح تنظیمات صوتی رخدادهای مختلف

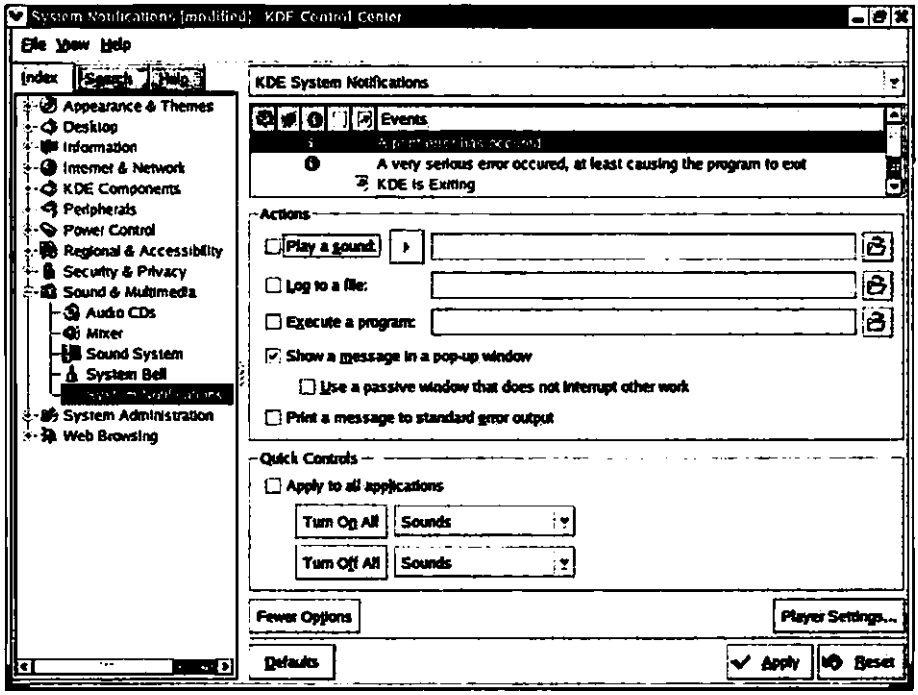
عنوان گزینه	توضیح
AOL IM Client	این گزینه امکان تنظیمات صوتی رخدادهای برنامه گپ‌زنی Gaim را در صورتی که به منظور دسترسی به سرور مربوطه از شبکه AOL پیکربندی شده باشد، در اختیار می‌گذارد.

عنوان گزینه	توضیح
Desktop Sharing	این گزینه امکان تنظیمات صوتی رخدادهای مربوط به برقراری ارتباط کامپیوتر میزبان با سایر کامپیوترهای مستقر در شبکه را در اختیار می‌گذارد.
KDE Screen Ruler	این گزینه امکان تنظیمات صوتی رخدادهای برنامه کاربردی KDE Screen Ruler را که از طریق منوی فرعی More Graphics Applications واقع در منوی Graphics از منوی اصلی محیط گرافیکی KDE قابل دستیابی است، در اختیار می‌گذارد.
KDE System Guard	این گزینه امکان تنظیمات صوتی رخدادهای ابزار KDE System Guard را که از طریق منوی فرعی More System Tools واقع در منوی System Tools از منوی اصلی محیط گرافیکی KDE قابل دستیابی است، در اختیار می‌گذارد.
KDE System Notifications	این گزینه امکان تنظیمات صوتی رخدادهای اصلی محیط گرافیکی KDE را در اختیار می‌گذارد.
KInetD	این گزینه امکان تنظیمات صوتی رخداد ناشی از برقراری ارتباط سایر کاربران با یکی از سرورهای xinetd را در اختیار می‌گذارد.
Kmail	این گزینه امکان تنظیمات صوتی رخداد ناشی از دریافت پیغام‌های الکترونیکی جدید را در اختیار می‌گذارد.
Ksirc	این گزینه امکان تنظیمات صوتی رخدادهای برنامه کاربردی Ksirc Internet Relay Chat را در اختیار می‌گذارد.
News Ticker	این گزینه امکان تنظیمات صوتی رخداد ناشی از دریافت اخبار جدید ارسالی از گروه‌های خبری را در اختیار می‌گذارد.
The KDE Window Manager	این گزینه امکان تنظیمات صوتی رخدادهای مربوط به کار با پنجره‌ها در محیط گرافیکی KDE را در اختیار می‌گذارد.

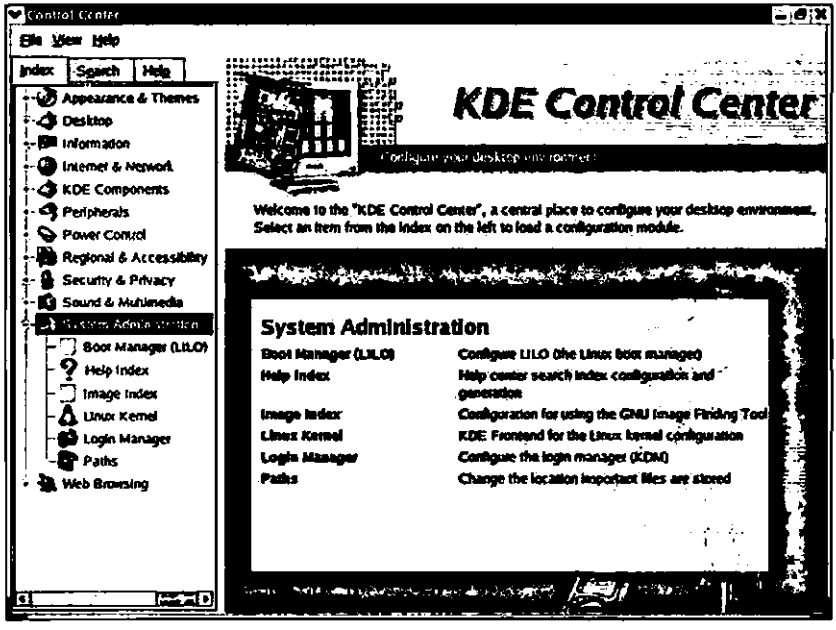
در صورت نصب بسته نرم‌افزاری kdegames-* می‌توان تنظیمات صوتی رخدادهای برخی از بازی‌ها را نیز انجام داد.

ابزار System Administration

ابزار System Administration تنظیماتی را به‌منظور پیکربندی ابزارهای سیستمی در اختیار می‌گذارد. شکل ۳۰-۱۷ این ابزار را نشان می‌دهد.



شکل ۲۹-۱۷ تنظیمات System Notifications



شکل ۳۰-۱۷ ابزار System Administration

تنظیمات Boot Manager (LILO)

این تنظیمات امکان پیکربندی برنامه LILO را از طریق یک رابط گرافیکی در اختیار قرار می‌دهد. مشخصات این پیکربندی در قالب فایل /etc/lilo.conf ذخیره شده و بلافاصله در بخشی از این تنظیمات با عنوان Expert Tab منعکس می‌شود. لازم به یادآوری است که برنامه bootmanager پیش‌فرض در سیستم‌عامل Red Hat Linux برنامه‌ای با عنوان Grand Unified Bootloader یا به اختصار GRUB است.

تنظیمات Help Index

این تنظیمات امکان پیکربندی شاخص‌های دسترسی به راهنمای محیط گرافیکی KDE را در اختیار می‌گذارد.

تنظیمات Image Index

این تنظیمات امکان پیکربندی ابزار GNU Image Finding Tool یا به اختصار GIFT را که به منظور جستجو در میان فایل‌هایی با محتوای تصویری طراحی شده است، در اختیار می‌گذارد.

تنظیمات Linux Kernel

در صورت نصب بسته نرم‌افزاری kernel-sources-*، این تنظیمات امکان پیکربندی مجدد هسته سیستم‌عامل Linux را در اختیار می‌گذارد.

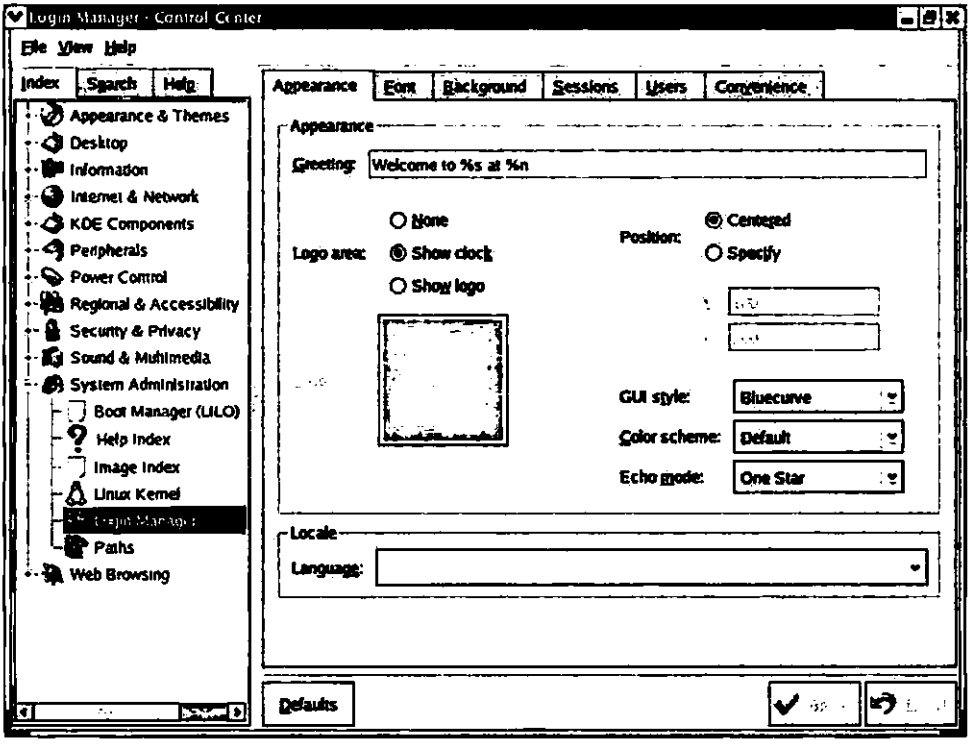
تنظیمات LogIn Manager

این تنظیمات امکان پیکربندی برنامه KDE Display Manager یا به اختصار KDM را در اختیار می‌گذارد. مشابه ابزار GDM، این ابزار شامل امکاناتی به منظور پیکربندی مشخصات ظاهری برنامه، زبان و قلم مورد استفاده، تصویر پس‌زمینه، جلسات، کاربران مجاز و تسهیلات دسترسی به سیستم است که از طریق بخش‌های مختلفی با عناوین Appearance، Font، Background، Sessions، Users و Convenience قابل دستیابی هستند. شکل ۳۱-۱۷ این تنظیمات را نشان می‌دهد.

تنظیمات Paths

این تنظیمات امکان تعیین موقعیت فهرست‌های حاوی تنظیمات محیط کار، فایل‌های حذف شده، اسناد محلی و فایل‌های پیکربندی راه‌اندازی خودکار سرویس‌ها را در اختیار می‌گذارد. فهرست‌های

نامبرده معمولاً در فهرست خانگی یا در یکی از زیرفهرست‌های آن مستقر هستند.



شکل ۱۷-۳۱ تنظیمات LogIn Manager

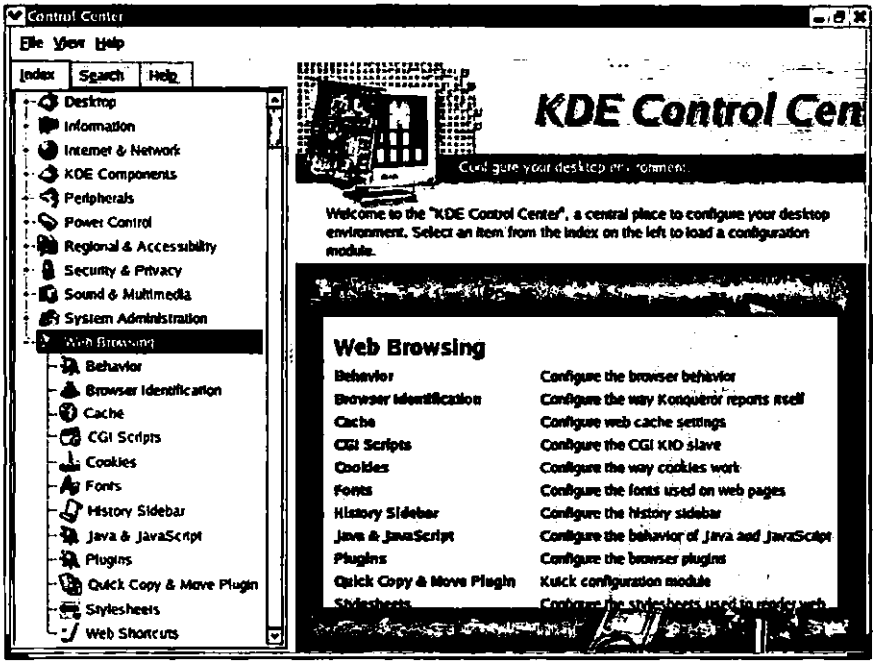
ابزار Web Browsing

ابزار Web Browsing تنظیماتی را به منظور پیکربندی مرورگر وب پیش‌فرض در محیط گرافیکی KDE یعنی Konqueror اختیار می‌گذارد. شکل ۱۷-۳۲ این ابزار را نشان می‌دهد. شرح مختصری درباره تنظیمات مزبور در جدول ۱۷-۸ آمده است.

جدول ۱۷-۸ شرح تنظیمات مختلف ابزار Web Browsing

عنوان تنظیمات	توضیح
Behavior	این تنظیمات امکان پیکربندی رفتار مرورگر وب را در زمینه‌های مختلفی از جمله نمایش اشاره‌گرها، تکمیل فرم‌ها، نمایش تصاویر و پیوندها و مواردی از این قبیل در اختیار می‌گذارد.

عنوان تنظیمات	توضیح
Browser Identification	این تنظیمات امکان تعیین مشخصاتی را که مرورگر وب هنگام معرفی‌خود در اختیار برنامه‌ها قرار می‌دهد، مهیا می‌کند. در صورت تمایل می‌توان این تنظیمات را به نحوی انجام داد که مرورگر Konqueror خود را به عنوان مرورگر Microsoft Internet Explorer 6 معرفی کند.
Cache	این تنظیمات امکان تعیین ظرفیتی از هارددیسک را که به منظور ذخیره صفحات وب بازدید شده مورد استفاده قرار می‌گیرد، در اختیار می‌گذارد.
CGI Scripts	این تنظیمات امکان دسترسی به برنامه‌های CGI را در اختیار می‌گذارد.
Cookies	این تنظیمات امکان تعیین خط‌مشی پذیرش کوکی‌های ارسالی از وب سایت‌های مختلف را در اختیار می‌گذارد.
Fonts	این تنظیمات امکان پشتیبانی از فونت‌های مورد استفاده در وب سایت‌هایی را که به زبان‌های مختلف طراحی شده‌اند، در اختیار می‌گذارد.
History Sidebar	این تنظیمات امکان دسترسی به آدرس‌هایی را که قبلاً مورد بازدید قرار گرفته‌اند، در اختیار می‌گذارد.
Java & JavaScript	این تنظیمات امکان پشتیبانی از برنامه‌های Java و JavaScript را در اختیار می‌گذارد.
Plugins	این تنظیمات امکان پیکربندی برنامه‌های plug-in قابل استفاده در مرورگر وب را در اختیار می‌گذارد.
Quick Copy & Move Plugin	این تنظیمات امکان کپی کردن و انتقال سریع محتوا را در اختیار می‌گذارد.
Stylesheets	این تنظیمات امکان پشتیبانی برگه مدهای Cascading Style Sheet یا به اختصار CSS را در اختیار می‌گذارد. (طراحی وب سایت با استفاده از برگه مدها، امکان نمایش صفحات وب را به شکلی یکپارچه و همگن فراهم می‌کند.)
Web Shortcuts	این تنظیمات امکان دسترسی به برخی از متداول‌ترین وب سایت‌ها و موتورهای جستجوی وب را در اختیار می‌گذارد.



شکل ۳۲-۱۷ ابزار Web Browsing

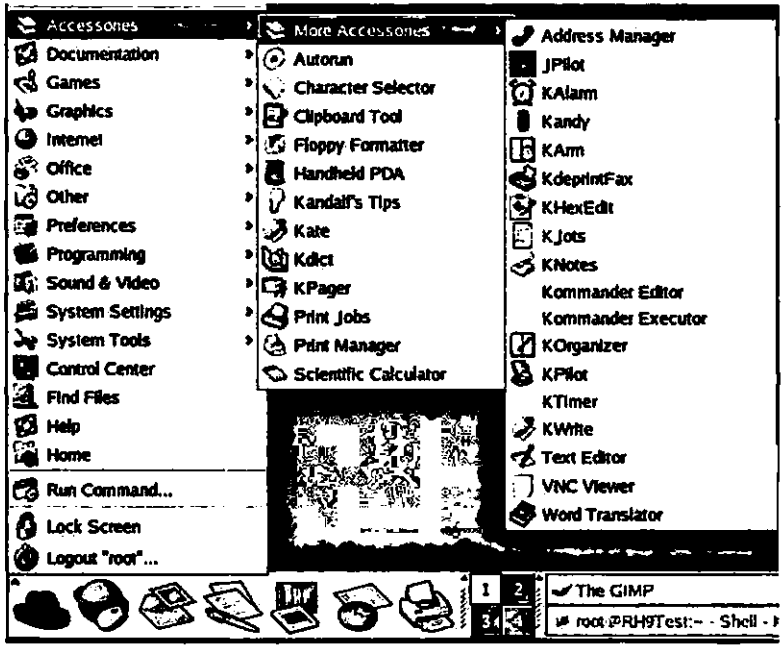
ابزارهای محیط گرافیکی KDE

محیط گرافیکی KDE حاوی برنامه‌های کاربردی متنوعی است که همگی از طریق منوی اصلی قابل دستیابی هستند. این برنامه‌ها در قالب گروه‌های مختلفی تحت عنوان Accessories، Internet، Other، Preferences، Programming، Multimedia و System Tools دسته‌بندی شده‌اند. در این قسمت تنها برخی از آن‌ها را مورد بررسی قرار داده و مابقی را به دو فصل آینده موکول می‌کنیم. اغلب این برنامه‌ها محصول پروژه KDE هستند. (برنامه‌های کاربردی محیط گرافیکی GNOME را قبلاً در فصل شانزدهم مورد بررسی قرار داده‌ایم.)

لیست برنامه‌های کاربردی موجود در کامپیوتر شما ممکن است با آن‌چه در این‌جا مشاهده می‌کنید، متفاوت باشد. عموماً گزینه‌های قابل دستیابی از طریق منوها به این موضوع بستگی دارد که کدام بسته‌های نرم‌افزاری را روی کامپیوتر خود نصب کرده‌اید.

گروه برنامه‌های Accessories

گروه Accessories شامل برنامه‌هایی است که به منظور ساده‌سازی وظایف کامپیوتری روزمره طراحی شده‌اند. چنان‌که شکل ۳۳-۱۷ نشان می‌دهد، این برنامه‌ها از طریق منوی فرعی Accessories از منوی اصلی قابل دستیابی هستند. منوی فرعی More Accessories از این منو خود حاوی تعداد دیگری از این برنامه‌هاست. برنامه‌هایی که در این قسمت از بررسی آن‌ها صرف‌نظر شده است، مربوط به محیط گرافیکی GNOME هستند. این گونه برنامه‌ها را قبلاً در فصل شانزدهم مورد بررسی قرار داده‌ایم.



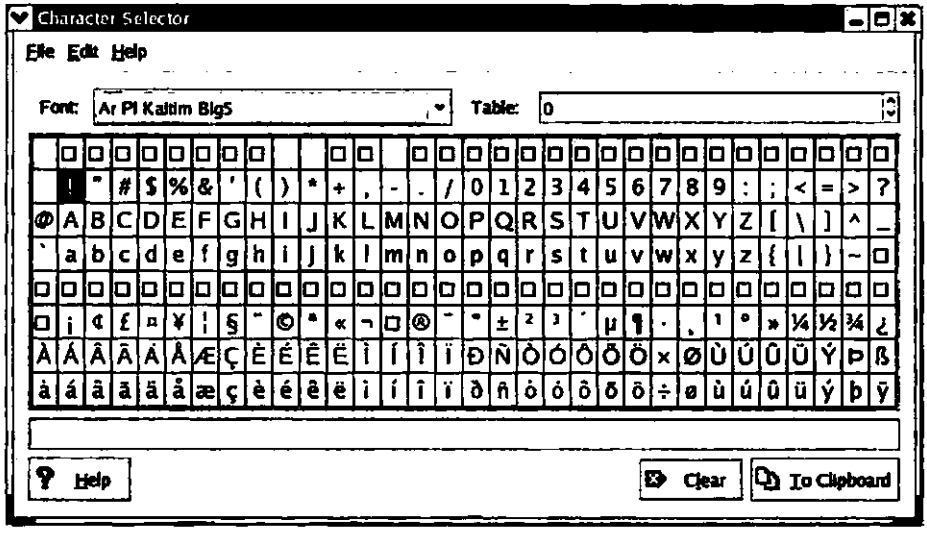
شکل ۳۳-۱۷ محتوای منوی Accessories

برنامه Autorun

این برنامه به منظور اجرای برنامه autorun مستقر روی CD موجود در درایو یا اجرای CD صوتی موجود در آن می‌شود. برای آن‌که کاربران عادی نیز امکان اجرای این گونه برنامه‌ها را داشته باشند، لازم است گزینه‌های user و exec را در خط مربوط به تنظیمات CD از فایل پیکربندی /etc/fstab درج کنید.

برنامه Character Selector

این برنامه که اغلب با عنوان KcharSelect نیز شناخته می‌شود، جهت دسترسی به کاراکترهای برخی از زبان‌های غیرانگلیسی که شامل الفبای لاتین هستند، پیش‌بینی شده است. چنان‌که شکل ۳۴-۱۷ نشان می‌دهد، پنجره این برنامه با عنوان Character Selector امکان دسترسی به کاراکترهای موردنظر را به راحتی در اختیار می‌گذارد.



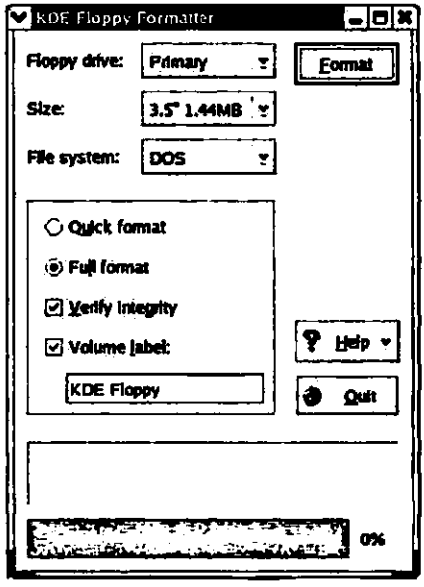
شکل ۳۴-۱۷ پنجره Character Selector

برنامه Clipboard Tool

این برنامه گزینه‌های پیکربندی ابزار Klipper را که قبلاً در همین فصل مورد بررسی واقع شد، در اختیار می‌گذارد.

برنامه Floppy Formatter

این برنامه که اغلب با عنوان KFloppy نیز شناخته می‌شود، امکان قالب بندی دیسک‌های فلاپی استاندارد را با سیستم فایل MS-DOS یا ext2 در اختیار می‌گذارد. چنان‌که شکل ۳۵-۱۷ نشان می‌دهد، کلیه امکانات لازم برای این منظور در پنجره KDE Floppy Formatter پیش‌بینی شده است.



شکل ۳۵-۱۷ پنجره KDE Floppy Formatter

برنامه Handheld PDA

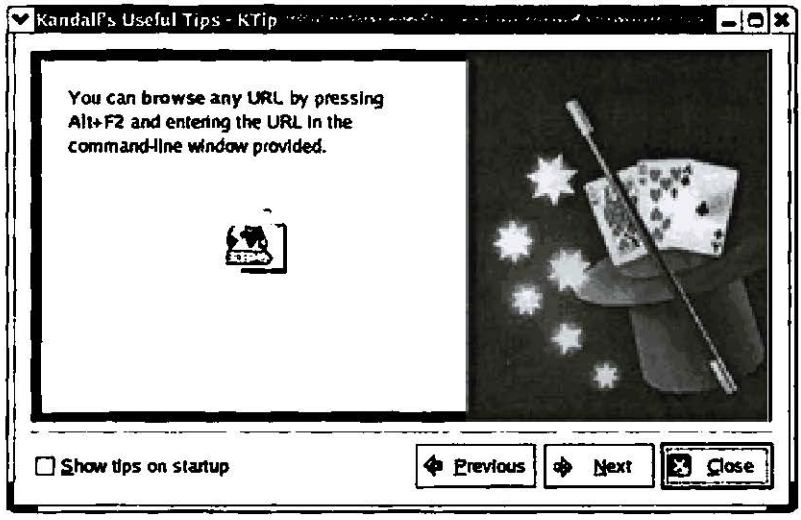
این برنامه امکان دسترسی به ابزار GNOME Pilot را که قبلاً در فصل شانزدهم توضیح داده شد، در اختیار می‌گذارد.

برنامه Kandalf's Tips

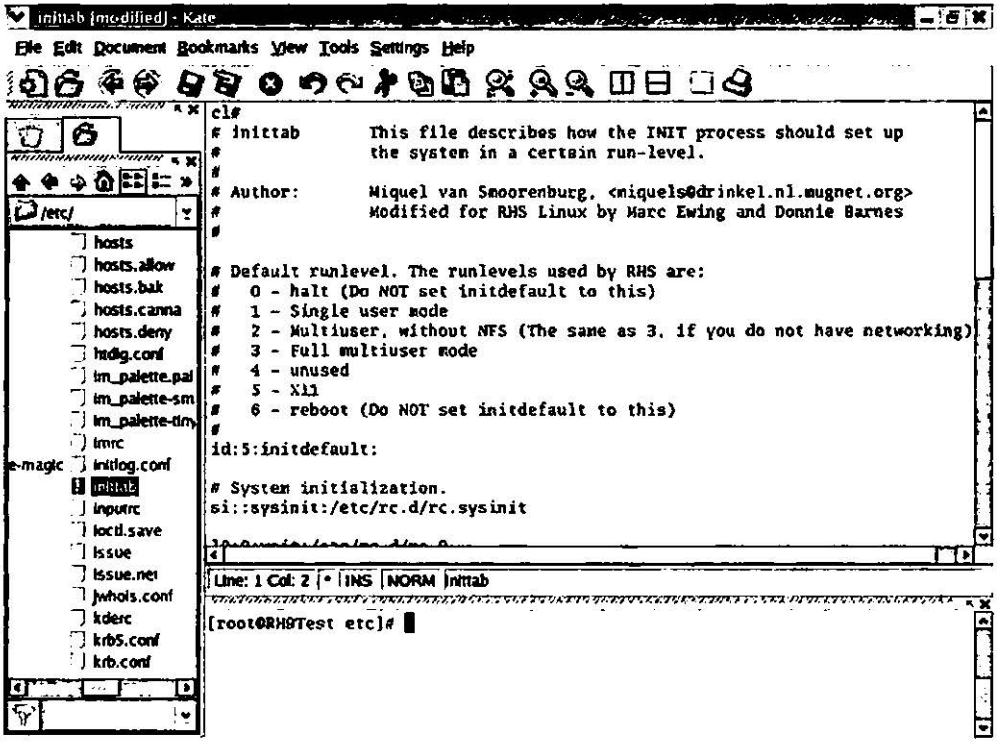
این برنامه به محض ورود به محیط گرافیکی KDE، راهنمایی‌های کاربردی ارزشمندی را در قالب پنجره‌ای با عنوان Kandalf'e Useful Tips به نمایش می‌گذارد. شکل ۳۶-۱۷ نمونه‌ای را در این رابطه نشان می‌دهد.

برنامه Kate

این برنامه با عنوان کامل KDE advanced text editor به منظور ویرایش فایل‌های متنی طراحی شده است. شکل ۳۷-۱۷ رابط گرافیکی این برنامه را که امکان دسترسی به سطر فرمان سیستم‌عامل Linux را نیز در اختیار می‌گذارد، نشان می‌دهد.



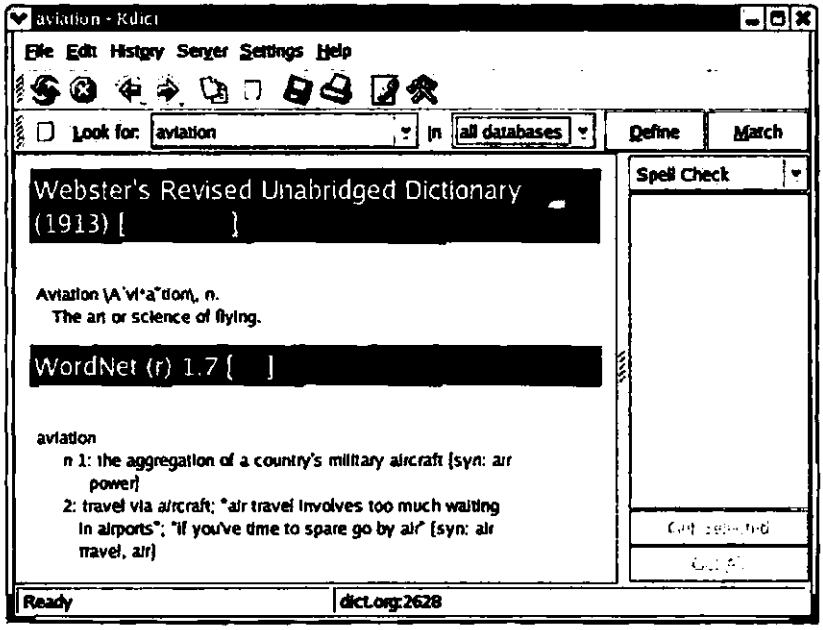
شکل ۱۷-۳۶ پنجره Kandalf's Useful Tips



شکل ۱۷-۳۷ رابط گرافیکی برنامه Kate

برنامه Kdict

این برنامه امکان دسترسی به دیکشنری online مستقر در آدرس dict.org را از طریق پورت شماره ۲۶۲۸ فراهم می‌کند. برای استفاده از این برنامه باید به اینترنت متصل شوید. شکل ۳۸-۱۷ رابط گرافیکی این برنامه را نشان می‌دهد.



شکل ۳۸-۱۷ رابط گرافیکی برنامه Kdict

برنامه Kpager

مشابه پانل محیط گرافیکی KDE، این برنامه نیز امکان مشاهده محیط‌های کاری موجود را در قالب یک پنجره کوچک فراهم می‌کند.

برنامه Print Jobs

این برنامه که با عنوان KJob View نیز شناخته می‌شود، امکان مدیریت وظایف چاپی موجود در صف چاپ را فراهم کرده و امکاناتی را به منظور تعلیق و ادامه چاپ و هم‌چنین حذف یا جابه‌جایی وظایف چاپی در اختیار می‌گذارد.

برنامه Print Manager

این برنامه امکان دسترسی به ابزار GNOME Print Manager را که قبلاً در فصل شانزدهم مورد بررسی قرار گرفت، فراهم می‌کند.

برنامه Scientific Calculator

این برنامه که با عنوان KCalc نیز شناخته می‌شود، یک ماشین حساب قابل پیکربندی است که از طریق بخش عددی صفحه کلید می‌توان آن‌را مورد استفاده قرار داد. بهره‌برداری از این برنامه در دو حالت Trigonometric و Statistical امکان‌پذیر است.

سایر برنامه‌های گروه Accessories

سایر برنامه‌های کاربردی عرضه شده برای محیط گرافیکی اغلب دارای کاربردهای محدودتری هستند. جدول ۹-۱۷ هر یک از آن‌ها را به اختصار شرح می‌دهد.

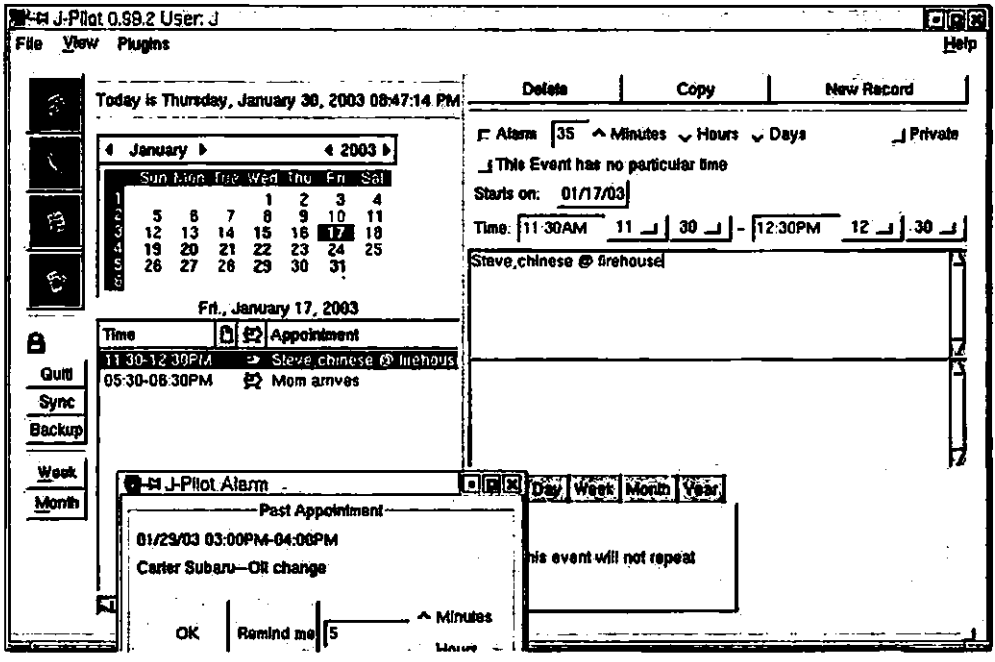
جدول ۹-۱۷ شرح سایر برنامه‌های کاربردی عرضه شده برای محیط گرافیکی KDE

عنوان برنامه	توضیح
Address Manager	این برنامه امکان مدیریت اطلاعات موجود در کتاب آدرس را در اختیار می‌گذارد.
JPilot	این برنامه به منظور هماهنگی داده‌ها میان محیط گرافیکی KDE و تجهیزات سخت‌افزاری قابل حملی که بر اساس استانداردهای PalmPilot و PalmOS ساخته شده‌اند، امکانات لازم را در اختیار می‌گذارد. شکل ۳۹-۱۷ پنجره این برنامه را نشان می‌دهد.
Kalarm	این برنامه امکان زمان‌بندی نمایش پیغام‌ها یا اجرای فرامین موردنظر را در اختیار می‌گذارد.
Kandy	این برنامه امکان هماهنگی داده‌ها میان کتاب آدرس محیط گرافیکی KDE و تلفن‌های همراه را در اختیار می‌گذارد.
KArm	این برنامه به منظور اطلاع از زمان صرف شده برای وظایف مختلف امکانات لازم را در اختیار می‌گذارد.
KdeprintFax	این برنامه امکان مشاهده محتوای فایلی را که جهت چاپ به دستگاه فاکس ارسال شده است، در اختیار می‌گذارد.

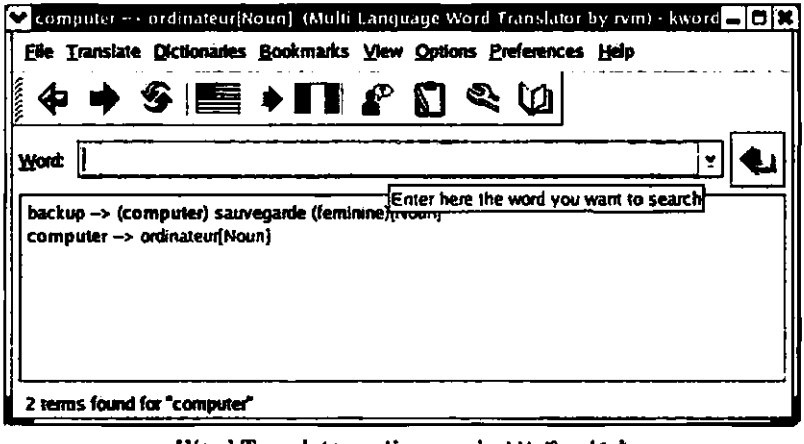
عنوان برنامه	توضیح
KHexEdit	این برنامه یک ویرایشگر هگزادسیمال (مبنای شانزده) است که امکان ویرایش داده‌های موجود در مبنای شانزده، هشت و دو را در اختیار می‌گذارد. علاوه بر این قادر است محتوای فایل‌های متنی را نیز نمایش دهد.
KJots	این برنامه امکان یادداشت برداری سریع را در قالبی سازمان‌دهی شده فراهم می‌کند، به نحوی که بتوان آن‌ها را سریعاً مورد دستیابی قرار داد.
KNotes	این برنامه امکان درج یادداشت‌های کوتاه را در قالب یک لیست قابل چاپ یا قابل ارسال از طریق پست الکترونیکی در اختیار می‌گذارد.
KOrganizer	این برنامه امکانات لازم برای سازمان‌دهی و زمان‌بندی وظایف مختلف را در اختیار می‌گذارد.
KPilot	این برنامه امکانات آخرین نسخه از نرم‌افزار Desktop HotSync را در اختیار می‌گذارد.
KTimer	این برنامه امکان اجرای فرمان دلخواهی را پس از سپری شدن مدت زمان معلوم (که به طور پیش‌فرض برابر با ۱۰۰ ثانیه است) در اختیار می‌گذارد.
KWrite	این برنامه یک ویرایشگر متنی مناسب برای برنامه‌نویسان است.
Text Editor	این برنامه که با عنوان KEdit نیز شناخته می‌شود، یک ویرایشگر متنی ساده بوده و به عنوان ویرایشگر متنی پیش‌فرض در محیط گرافیکی KDE در نظر گرفته شده است.
VNC Viewer	توضیح مربوط به این برنامه در فصل شانزدهم آمده است.
Word Translator	این برنامه یک مترجم چند زبانه است که جهت ترجمه از دیکشنری موجود در آدرس babylon.com استفاده می‌کند. شکل ۴۰-۱۷ پنجره این برنامه را نشان می‌دهد.

گروه برنامه‌های Internet

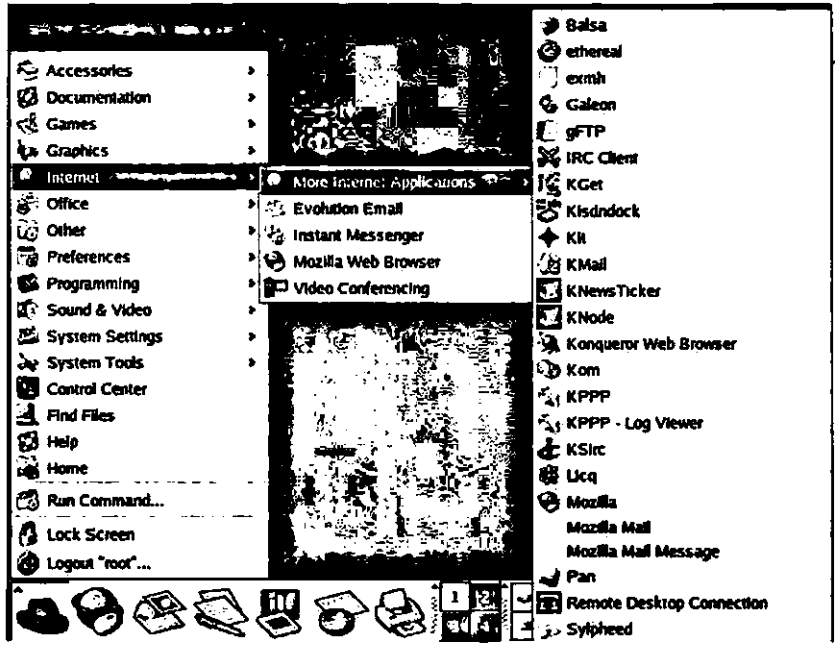
گروه Internet حاوی برنامه‌هایی است که جهت کار روی شبکه اینترنت پیش‌بینی شده‌اند. از این میان برای نمونه می‌توان به برنامه‌های کلاینت مورد استفاده جهت دسترسی به شبکه گپ‌زنی IRC و چندین ابزار متنوع برای دسترسی به اینترنت اشاره کرد. چنان‌که شکل ۴۱-۱۷ نشان می‌دهد، این برنامه‌ها از طریق منوی فرعی More Internet Applications واقع در منوی Internet از منوی اصلی قابل دستیابی هستند. تعدادی از این برنامه‌ها، از جمله Mozilla، gFTP، Instant Messenger، Video Conferencing، Balsa، exmh، Galeon، IRC Client، Sylpheed و Evolution را که کار توسعه آن‌ها در قالب پروژه GNOME انجام شده است، قبلاً در فصل شانزدهم مورد بررسی قرار دادیم. بررسی برنامه Ethereal را به فصل بیست و دوم موکول می‌کنیم.



شکل ۱۷-۳۹ پنجره برنامه JPilot



شکل ۱۷-۴۰ پنجره برنامه Word Translator



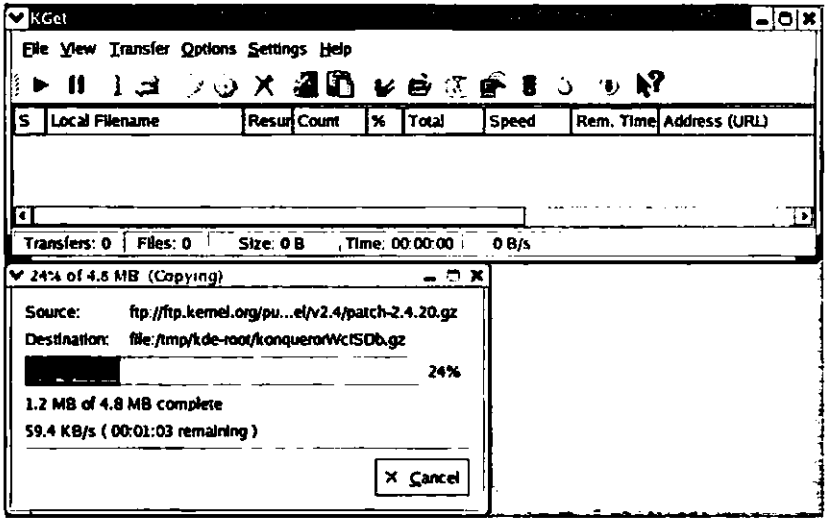
شکل ۴۱-۱۷ محتوای منوی فرعی More Internet Applications

برنامه KGget

این برنامه به منظور مدیریت بارگذاری فایل‌ها از شبکه اینترنت پیش‌بینی شده است. برنامه KGet که اغلب با عنوان Caitoo نیز شناخته می‌شود، امکانات لازم به منظور نظارت بر روند بارگذاری فایل‌ها و هم‌چنین تعلیق و ادامه این روند را در اختیار می‌گذارد. در صورت تمایل می‌توان این برنامه را در قالب مرورگر وب پیش‌فرض در محیط گرافیکی KDE با عنوان Konqueror نیز مورد استفاده قرار داد. شکل ۴۲-۱۷ پنجره برنامه مورد بحث را نشان می‌دهد.

برنامه Kisdndock

این برنامه به منظور پیکربندی تجهیزات سخت‌افزاری ISDN یا اصطلاحاً Integrated Services Digital Network پیش‌بینی شده است. سرعت انتقال داده‌ها در شبکه‌های ISDN تقریباً دو برابر شبکه‌های تلفن معمولی است. به دلیل رایج بودن شبکه ISDN در قاره اروپا، محیط گرافیکی KDE (که بیشتر کار توسعه آن در این‌قاره انجام شده است) پشتیبانی قابل توجهی از این گونه شبکه‌ها به عمل می‌آورد.



شکل ۴۲-۱۷ پنجره برنامه Kget

چنان‌چه تا به حال برای پیکربندی تجهیزات سخت‌افزاری ISDN اقدام نکردید، ابتدا باید این کار را با استفاده از ابزار پیکربندی redhat-config-network-druid انجام دهید. (برای‌اطلاع‌بیشتر در این زمینه به فصل بیست و یکم مراجعه کنید.)

ابزار پیکربندی redhat-config-network-druid در نسخه‌های قدیمی‌تر سیستم‌عامل Red Hat Linux با عنوان internet-druid معرفی شده است.

برنامه Kit

این‌برنامه به‌منظوراستفاده‌از سرویس‌ارسال‌سریع پیغام (اصطلاحاً Instant Messaging یا به اختصار IM) از طریق شبکه AOL طراحی شده است. هنگام اجرای این برنامه برای نخستین بار، امکان ایجاد حساب کاربری موردنیاز برای دسترسی به شبکه AOL از طریق یک ویزارد در اختیار قرار می‌گیرد. در نسخه‌های بعدی این برنامه، ممکن است قابلیت دسترسی به سایر شبکه‌ها نیز تعبیه شود.

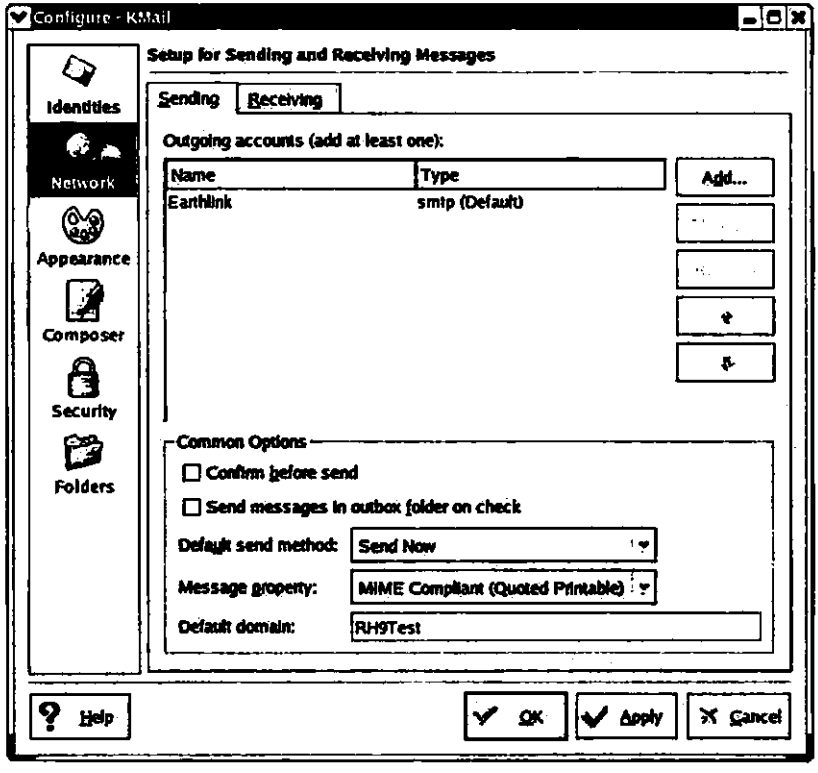
برنامه KMail

این برنامه از قابلیت پیکربندی بسیار بالایی برخوردار بوده و به عنوان برنامه پیش‌فرض مورد استفاده در محیط گرافیکی KDE جهت مدیریت پیغام‌های الکترونیکی محسوب می‌شود. در صورت تمایل، برای انجام هرچه ساده‌تر و سریع‌تر عملیات موردنظر می‌توان گزینه‌های میانبر مربوطه را در نوار ابزار این

برنامه تعبیه کرد. بدیهی است این برنامه تنظیماتی را نیز به منظور پیکربندی حساب کاربری در اختیار می‌گذارد.

برای مثال، می‌توان گزینه‌های میانبر مربوط به استفاده از فیلترها، علامت‌گذاری پیغام‌ها، پاسخ دادن به آن‌ها و موارد دیگر را روی نوار ابزار برنامه KMail قرار داد. برای این منظور بیش از ۱۰۰ گزینه میانبر پیش‌بینی شده است. ضمناً پیکربندی نوار ابزار اصلی نیز امکان‌پذیر است.

تعریف حساب کاربری جدید نیز بسیار ساده است. با انتخاب گزینه Configure KMail از منوی Settings پنجره‌ای باعنوان Configure KMail بازشده و امکانات‌پیکربندی‌برنامه را در اختیار می‌گذارد. شکل ۴۳-۱۷ پنجره مذکور را نشان می‌دهد.



شکل ۴۳-۱۷ پنجره Configure KMail

چنان‌که مشاهده می‌کنید، با انتخاب گزینه Network از قاب سمت چپ این پنجره، امکان تنظیم پارامترهای مربوط به ارسال و دریافت پیغام‌های الکترونیکی در اختیار قرار می‌گیرد.

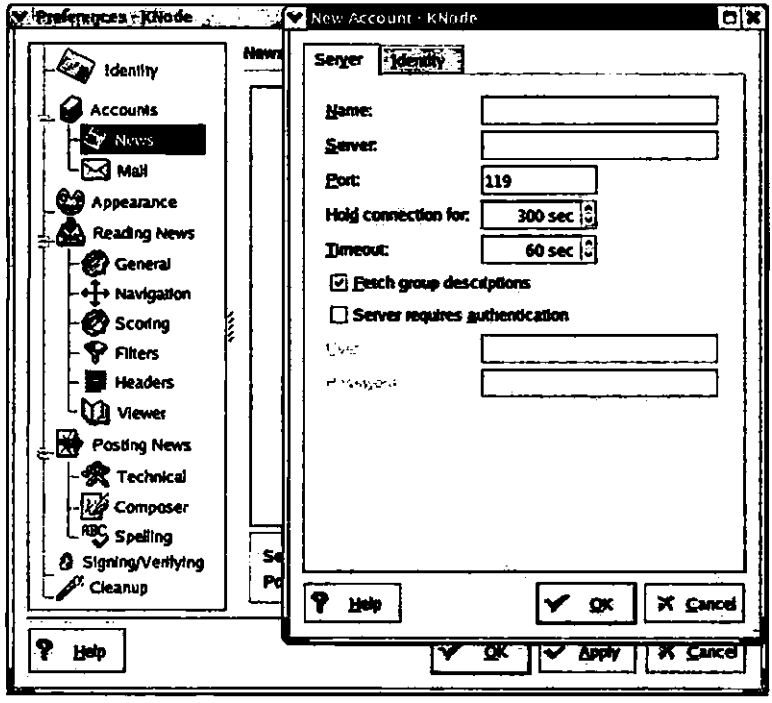
برنامه KNnewsTicker

این برنامه به منظور دسترسی به گروه‌های خبری و ارسال و دریافت اخبار منتشر شده پیش‌بینی شده است. جهت دسترسی هرچه سریع‌تر به این برنامه می‌توان گزینه مربوط به آن‌را روی پانل محیط گرافیکی KDE مستقر کرد.

برای این منظور، کافی است روی پانل مزبور کلیک راست کرده و از منوی حاصل ابتدا گزینه Add و سپس گزینه Applet و در نهایت گزینه KNewsTicker را انتخاب کنید.

برنامه KNode

این برنامه نیز جهت دسترسی به گروه‌های خبری طراحی شده و فرآیند پیکربندی آن به سادگی برنامه KMail است. برای دسترسی به پنجره حاوی تنظیمات پیکربندی با عنوان Preferences - Knode، کافی است گزینه Configure KNode را از منوی Settings انتخاب کنید. هم‌چنین برای تعریف حساب کاربری جدید روی دکمه New از این پنجره کلیک کنید تا کادر محاوره‌ای New Account - KNode باز شود. شکل ۴۴-۱۷، این کادر محاوره‌ای را نشان می‌دهد.

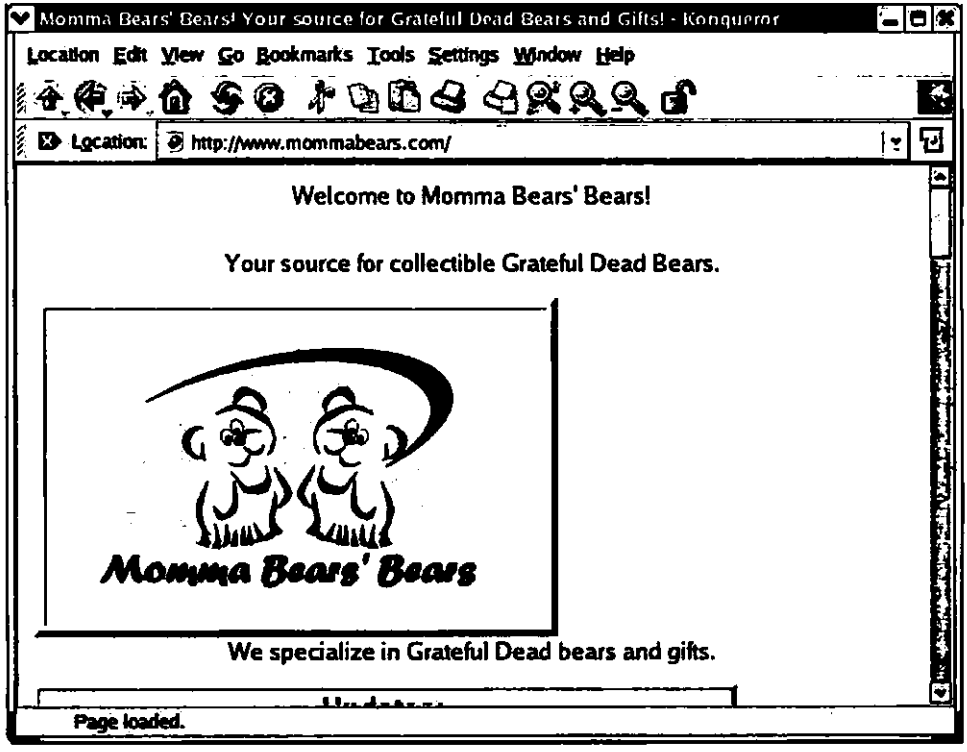


شکل ۴۴-۱۷ کادر محاوره‌ای New Account - KNode

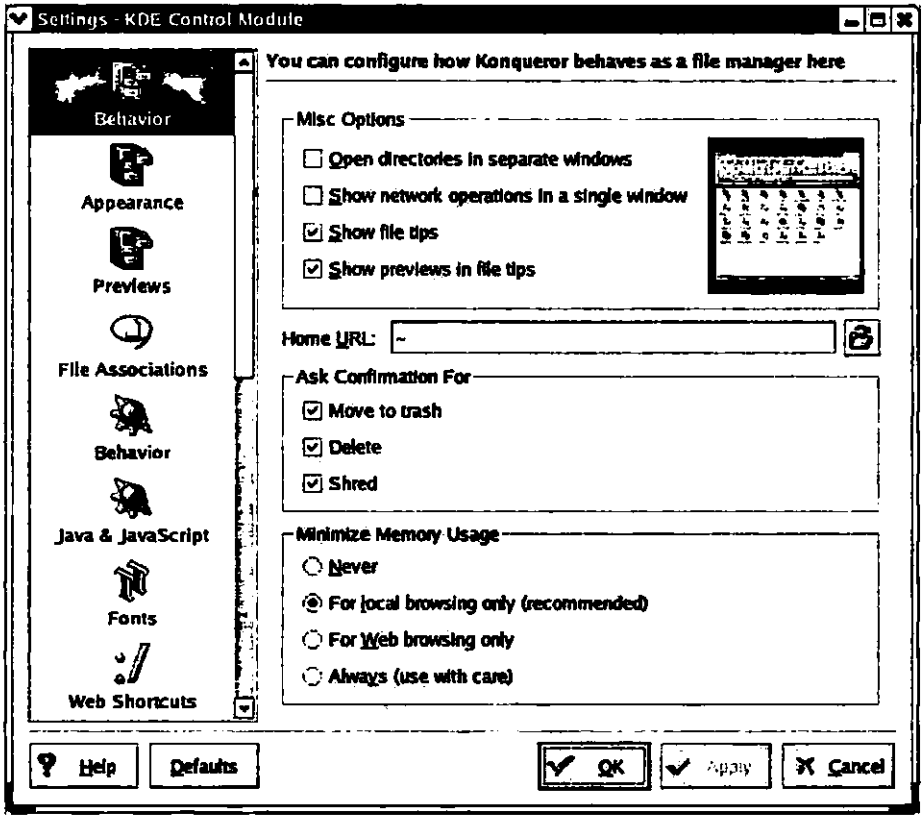
چنان‌که مشاهده می‌کنید، این برنامه از قابلیت پیکربندی بسیار خوبی برخوردار بوده و پیکربندی آن به سادگی امکان‌پذیر است.

برنامه Konqueror Web Browser

این برنامه به عنوان مرورگر وب پیش‌فرض در محیط گرافیکی KDE یک برنامه شناخته شده است. مشابه برنامه Nautilus در محیط گرافیکی GNOME، این برنامه نیز از قابلیت مدیریت فایل‌ها برخوردار است. پیشتر در قسمت "مرکز کنترل محیط گرافیکی KDE" از همین فصل با تنظیمات پیکربندی برنامه Konqueror آشنا شدید. این تنظیمات با انتخاب گزینه Configure Konqueror از منوی Setting قابل دستیابی است. شکل ۱۷-۴۵ پنجره این برنامه و شکل ۱۷-۴۶ پنجره حاوی امکانات پیکربندی آن‌را نشان می‌دهد.



شکل ۱۷-۴۵ پنجره برنامه Konqueror



شکل ۴۶-۱۷ پنجره حاوی امکانات پیکربندی برنامه Konqueror

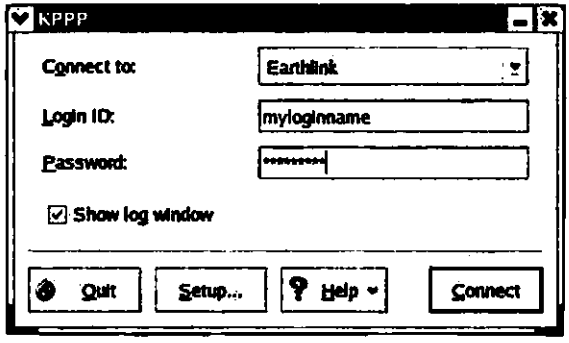
برنامه Korn

این برنامه جهت بازبینی صندوق پستی حاوی پیغام‌های الکترونیکی دریافتی پیش‌بینی شده است. برای استفاده از این ابزار ابتدا باید آن‌را جهت دسترسی به صندوق پستی محلی یا دسترسی از طریق پروتکل‌های POP3، IMAP4 یا نظیر آن پیکربندی کرد. با استقرار نماد برنامه Korn روی پانل محیط گرافیکی KDE، این برنامه به فواصل زمانی مشخص (به‌طور پیش‌فرض هر ۵ دقیقه یکبار) برای بازبینی صندوق یا صندوق‌های پستی موردنظر اقدام خواهد کرد.

برنامه KPPP

این برنامه که از قابلیت پیکربندی خوبی نیز برخوردار است، به منظور برقراری ارتباط با ISP موردنظر از طریق مودم طراحی شده است. تنظیمات این برنامه امکان پیکربندی یک یا چند حساب کاربری را جهت دسترسی به مرکز یا مراکز ISP موردنظر در اختیار می‌گذارد. چنان‌چه در پیکربندی مودم با

مشکلاتی روبرو شده‌اید، به کمک این برنامه می‌توانید برای رفع آن‌ها اقدام کنید. برنامه KPPP دارای مکانیزمی برای ثبت وقایع بوده و امکاناتی را نیز به منظور بررسی کارایی ارتباط برقرار شده با مرکز ISP در اختیار می‌گذارد. شکل ۴۷-۱۷ رابط این برنامه را نشان می‌دهد.



شکل ۴۷-۱۷ رابط برنامه KPPP

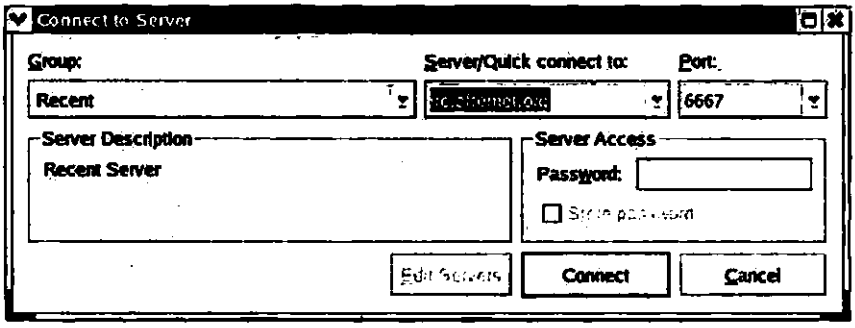
برنامه KPPP Log Viewer

این برنامه وقایع ثبت شده یک ماه اخیر برنامه KPPP را نمایش می‌دهد. این اطلاعات به ویژه در صورتی که هزینه اتصال به اینترنت بر اساس مدت زمان اتصال یا تعداد بایت‌های دریافتی محاسبه شود مفید خواهد بود. این وضعیت در مورد برخی از شبکه‌های بی‌سیم و هم‌چنین در برخی کشورهای اروپایی رایج است.

برنامه KSirc

این برنامه ابزار پیش‌فرض مورد استفاده در محیط گرافیکی KDE برای دسترسی به شبکه IRC و اتاق‌های گپ‌زنی آن است. با انتخاب گزینه New Server از منوی Connections کادر محاوره‌ای Connect to Server باز شده و امکانات لازم برای برقراری ارتباط با یک سرور جدید را در اختیار می‌گذارد. شکل ۴۸-۱۷ این کادر محاوره‌ای را نشان می‌دهد.

برای برقراری ارتباط با سرور جدید، کافی است گروه مربوطه را از لیست Group و عنوان سرور را از لیست Server/Quick connect to انتخاب کرده و پس از وارد کردن کلمه عبور (در صورت لزوم) روی دکمه Connect کلیک کنید. چنان‌چه این ارتباط با موفقیت برقرار شود، اتاق موردنظر در قالب پنجره‌ای جدید در دسترس قرار می‌گیرد.



شکل ۴۸-۱۷ کادر محاوره‌ای Connect to Server

برنامه Licq

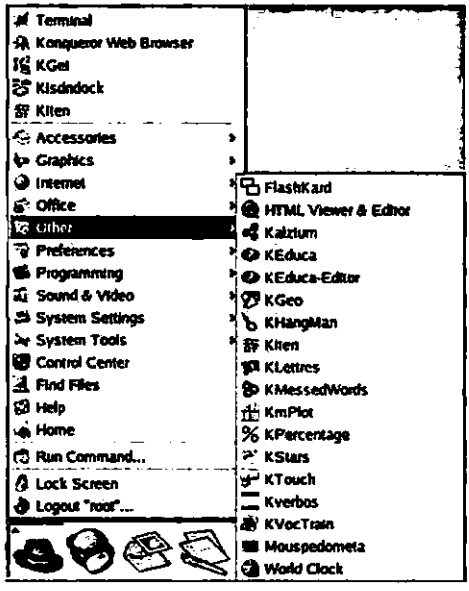
این برنامه نیز یکی دیگر از برنامه‌هایی است که می‌توان در محیط گرافیکی KDE جهت دسترسی به شبکه IRC مورد استفاده قرار داد.

سایر برنامه‌ها

محیط گرافیکی KDE دارای تعداد دیگری برنامه کاربردی است که به سادگی نمی‌توان آن‌ها را در قالب گروه‌های مختلف برنامه‌های کاربردی دسته بندی کرد. برخی از آن‌ها کاربرد آموزشی دارند، برای مثال، برنامه Kalzium به منظور آموزش جدول تناوبی عناصر و برنامه KVvocTrain جهت آموزش کاربرد کلمات طراحی شده‌اند. چنان‌که شکل ۴۹-۱۷ نشان می‌دهد، دسترسی به این برنامه‌ها از طریق منوی فرعی Other واقع در منوی اصلی فراهم شده است. از این میان، برنامه‌هایی را که کار توسعه آن‌ها در قالب پروژه KDE انجام نشده است، در این فصل مورد بررسی قرار نمی‌دهیم.

برنامه FlashKard

این برنامه ابزاری برای آموزش کاربردی واژگان زبان‌های مختلف است، به این ترتیب که پس از بارگذاری لیست واژگان موردنظر، می‌توانید دانش خود را در مورد معانی آن‌ها به بوته آزمایش بگذارید. لیست نمونه‌ای از واژگان زبان آلمانی در قالب فایلی با عنوان sample-de.kvtml از فهرست /usr/share/apps/kvoctrain/examples نگهداری می‌شود.



شکل ۴۹-۱۷ برنامه‌های کاربردی قابل دستیابی از طریق منوی فرعی Other

برنامه Kalzium

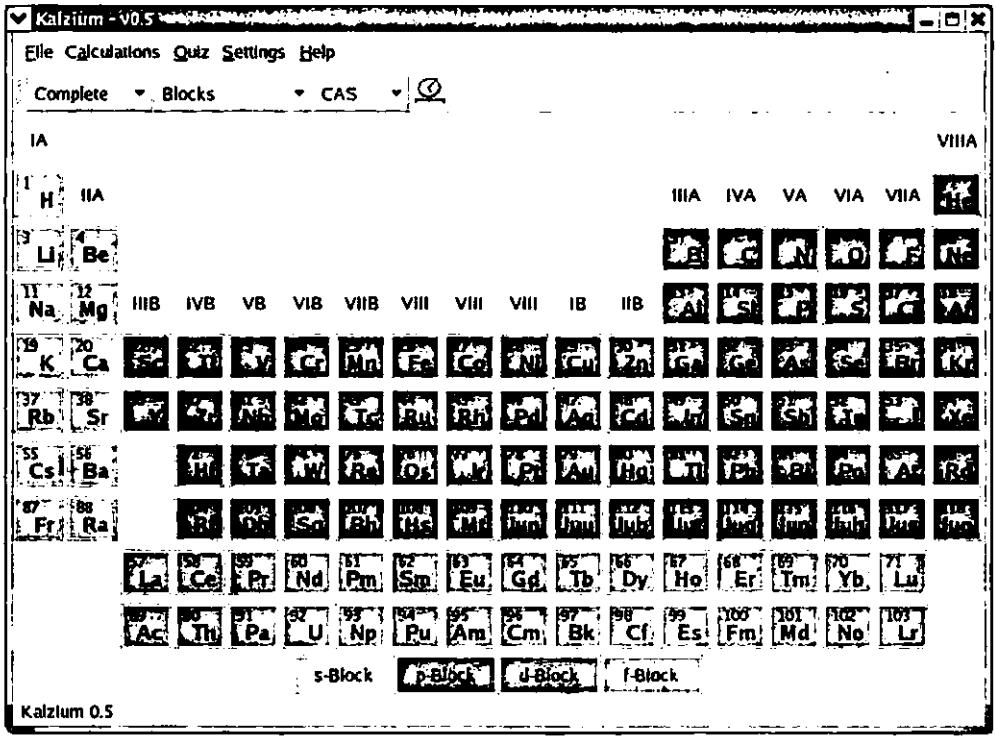
این برنامه ابزاری جهت آموزش جدول تناوبی عناصر است. چنان‌که شکل ۵۰-۱۷ نشان می‌دهد، این جدول حاوی نشانه و شماره مربوط به ۱۰۳ عنصر است. هر خانه این جدول یک دکمه قابل کلیک بوده و با کلیک روی آن می‌توان به اطلاعات بیشتری درباره عنصر موردنظر دست پیدا کرد. ضمناً تسهیلاتی نیز از همین طریق به منظور دسترسی به وب سایت دانشکده شیمی دانشگاه Split واقع در کشور کرواسی (به آدرس اینترنتی http://www.ktf-split.hr/en/index.html) پیش‌بینی شده است.

برنامه KEduca

این برنامه جهت ایجاد و آزمون‌های کتبی، طراحی شده است. پرسش‌ها را می‌توان با استفاده از ویرایشگر مخصوص این برنامه با عنوان KEduca-Editor در فرم آزمون وارد کرد. برای اطلاع بیشتر در این زمینه به آدرس http://www.sourceforge.net/projects/keduca مراجعه کنید.

برنامه KGeo

این برنامه یک ابزار محاوره‌ای برای آموزش هندسه است، به طوری که آموزگار هندسه به کمک آن می‌تواند اصول هندسه را به صورت مصور آموزش بدهد.



شکل ۱۷-۵۰ پنجره برنامه Kalzium

برنامه KHangMan

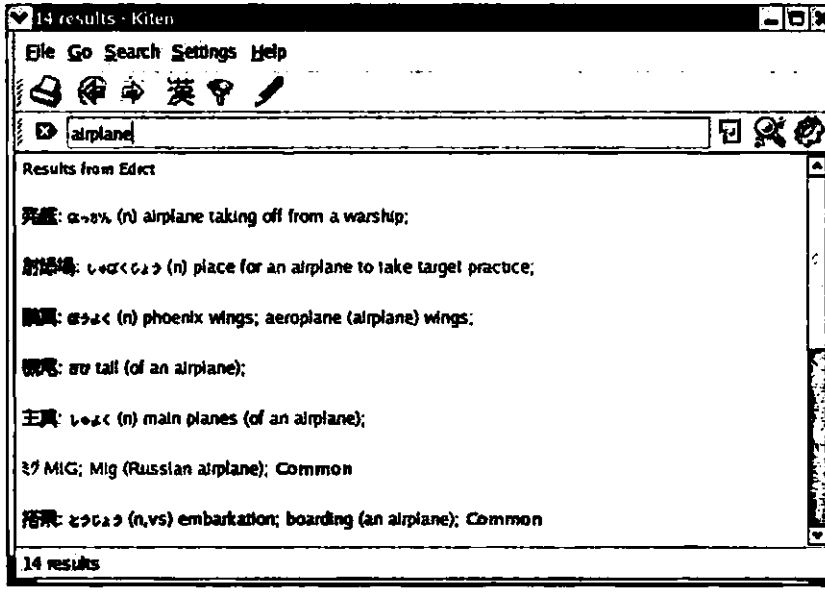
این برنامه یک نسخه کامپیوتری از یک بازی متداول است که به منظور آموزش واژه‌ها ابداع شده به طوری که بازیکن باید واژه موردنظر را از روی نشانه‌های موجود حدس بزنند.

برنامه Kiten

این برنامه یک دیکشنری محاوره‌ای است که به طور پیش‌فرض برای ترجمه لغات ژاپنی (با نگارش Kanji) و انگلیسی به یکدیگر طراحی شده است. شکل ۱۷-۵۱ نمونه‌ای از کاربرد این برنامه را نشان می‌دهد.

برنامه KLetters

این برنامه یک ابزار آموزشی برای فراگیری الفباست. نسخه فعلی آن‌را می‌توان جهت آموزش الفبای فرانسوی، دانمارکی و آلمانی مورد استفاده قرار داد.



شکل ۵۱-۱۷ برنامه Kiten در حال ترجمه واژهairplane به واژگان معادل یا مربوطه در نگارش متداول Kanji از زبان ژاپنی

برنامه KMessedWords

این برنامه نسخه‌ای از یک بازی نسبتاً متداول است.

برنامه KmPlot

این برنامه ابزاری برای رسم نمودار توابع ریاضی است. به کمک این ابزار می‌توان نمودار معادلات ریاضی مختلف را به سادگی ترسیم کرد.

برنامه KPercentage

این برنامه آزمونی برای محک زدن توانایی دانش‌آموزان در محاسبه درصد است.

برنامه KStars

این برنامه ابزاری برای آموزش ابتدایی علم نجوم است. نمای واضحی که این برنامه از آسمان شب در اختیار می‌گذارد، قابلیت دانش‌آموزان را در تشخیص نجوم بهبود می‌بخشد.

برنامه KTouch

این برنامه ابزاری برای آموزش تایپ است.

برنامه Kverbos

این برنامه ابزاری برای آموزش وجوه مختلف افعال در زبان اسپانیایی است.

برنامه KVocTrain

مشابه برنامه FlashKard، این برنامه نیز به منظور آموزش واژگان زبان‌های مختلف طراحی شده و مانند برنامه مذکور از بانک‌های اطلاعاتی kvtml. برای این منظور استفاده می‌کند.

برنامه Mousepedometa

این برنامه که اغلب با عنوان KOdometer نیز شناخته می‌شود، به منظور اندازه‌گیری میزان حرکت اشاره‌گر ماوس روی صفحه طراحی شده است.

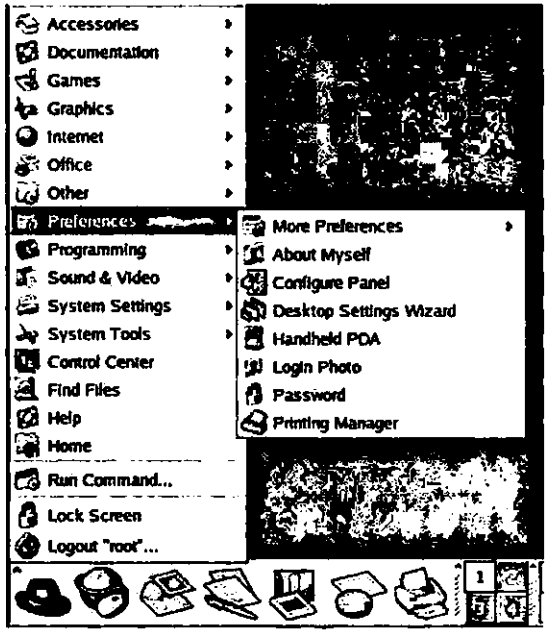
برنامه World Clock

این برنامه جهت اطلاع از ساعت فعلی در مناطق جغرافیایی مختلف و هم‌چنین اطلاع از موقعیت خورشید طراحی شده است.

گروه برنامه‌های Preferences

گروه Preferences شامل ابزارهای پیکربندی مختلف است. تنها تعداد کمی از این ابزارها محصول پروژه KDE هستند. شکل ۵۲-۱۷ منوی فرعی Preferences را نشان می‌دهد. شرح مختصر دو ابزار از این مجموعه در جدول ۱۰-۱۷ آمده است.

از آن‌جا که کار توسعه هیچ کدام از ابزارهای منوی فرعی More Preferences در قالب پروژه KDE انجام نشده است، از بررسی آن‌ها در این فصل صرف‌نظر می‌کنیم.



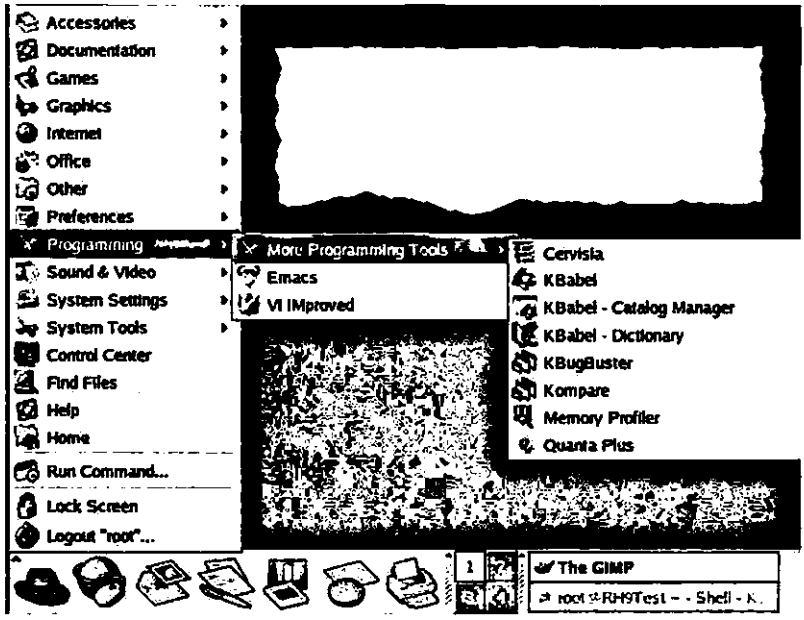
شکل ۵۲-۱۷ محتوای منوی فرعی Preferences

جدول ۱۰-۱۷ شرح مختصر دو ابزار قابل دستیابی از طریق منوی Preferences

عنوان ابزار	توضیح
Configure Panel	این ابزار تنظیمات مربوط به پانل محیط گرافیکی KDE را در قالب پنجره‌ای با عنوان Settings - KDE Control Module در اختیار می‌گذارد. نحوه پیکربندی پانل مذکور قبلاً در همین فصل مورد بررسی قرار گرفته است.
Desktop Settings Wizard	این ابزار ویزاردی را به منظور تعیین زبان مورد استفاده، موقعیت جغرافیایی، رفتار پیش‌فرض سیستم در موارد مختلف، جلوه‌های ویژه و آرایش محیط گرافیکی KDE در اختیار می‌گذارد.

گروه Programming

این گروه، شامل ابزارهای برنامه‌نویسی مفیدی است که درقالب دو منوی فرعی Programming و More Programming Tools از منوی اصلی قابل دستیابی هستند. شکل ۵۳-۱۷ محتوای این منوها را نشان می‌دهد. کار توسعه تعداد کمی از این ابزارها در قالب پروژه KDE انجام شده است. جدول ۱۱-۱۷ ابزارهای موجود در منوی فرعی More Programming Tools را به اختصار شرح می‌دهد.



شکل ۵۳-۱۷ محتوای منوی فرعی Programming و More Programming Tools

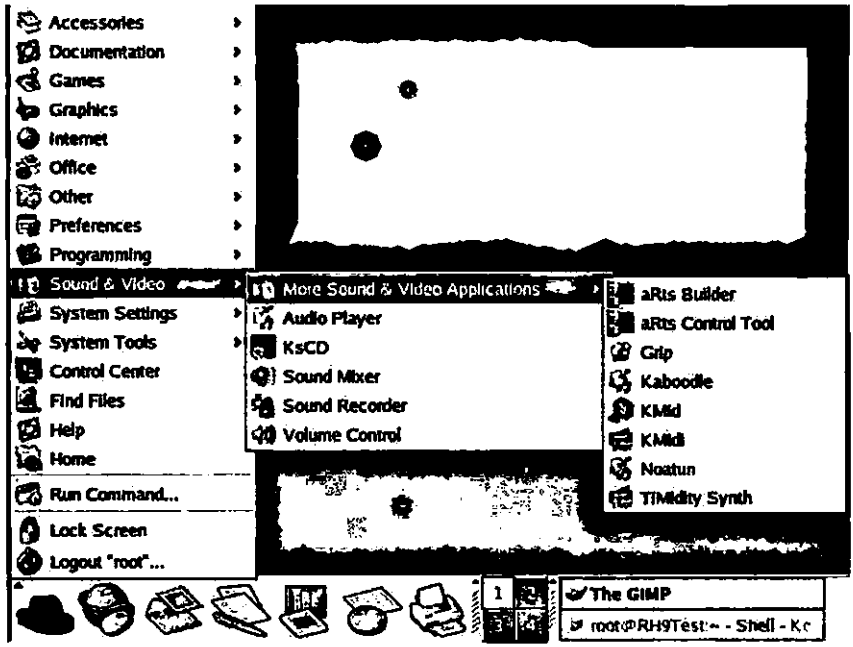
جدول ۱۱-۱۷ طرح مختصر ابزارهای منوی More Programming Tools

عنوان ابزار	توضیح
Cervista	این ابزار به واسطه مکانیزم Concurrent Versions System یا به اختصار CVS اطلاعات مربوط به نگارش‌های مختلف کد منبع برنامه‌ها را در اختیار می‌گذارد.
KBabel	این ابزار امکان استفاده از زبان‌های غیر انگلیسی را به منظور درج توضیحات و سایر راهنمایی‌ها در برنامه فراهم می‌کند.
KBabel - Catalog Manager	این ابزار امکان مدیریت فایل‌های PO (فایل‌هایی با پسوند po.) را در اختیار می‌گذارد.
KBabel - Dictionary	این ابزار که اغلب با عنوان PO Compendium نیز شناخته می‌شود، امکانات لازم برای ترجمه همگن و یکدست پیغام‌ها را در اختیار می‌گذارد.
KBugBuster	این ابزار با دسترسی به کامپیوتر میزبان، بانک اطلاعاتی حاوی اشکالات ثبت شده محیط گرافیکی KDE در آدرس www.kde.org امکان مدیریت اشکالات را در اختیار می‌گذارد.
Kompare	این ابزار به عنوان رابط گرافیکی برنامه diff، امکان مقایسه محتوای فایل‌های مختلف را در اختیار می‌گذارد.

عنوان ابزار	توضیح
Memory Profiler	این ابزار امکان نظارت بر حافظه مصرفی توسط برنامه‌ها را در اختیار می‌گذارد.
Quanta Plus	این‌ابزار امکاناتی را به‌منظور توسعه برنامه‌های‌کاربردی وب در اختیار می‌گذارد.

گروه برنامه‌های Sound & Video

گروه Sound & Video از برنامه‌ها شامل ابزارهایی برای پخش CD یا فایل‌های صوتی، کنترل صدا و مواردی از این قبیل است. چنان‌که شکل ۵۴-۱۷ نشان می‌دهد، این برنامه‌ها در قالب منوی فرعی Sound & Video از منوی اصلی دسته‌بندی شده‌اند.

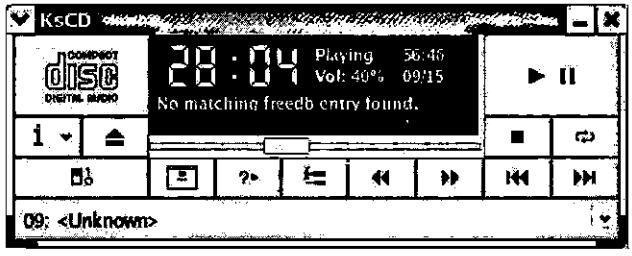


شکل ۵۴-۱۷ محتوای منوی فرعی Sound & Multimedia

برنامه KsCD

این برنامه با عنوان کامل KDE small/simple CD Player ابزاری ساده برای پخش موسیقی ضبط شده روی CDهای صوتی است. چنان‌که شکل ۵۵-۱۷ نشان می‌دهد، رابط گرافیکی این برنامه دارای دکمه‌های استانداردی است که کلیه امکانات لازم از جمله پخش موسیقی و دسترسی به موزیک قبلی و بعدی را در اختیار می‌گذارد. علاوه بر این، برنامه مورد بحث از قابلیت دسترسی به بانک اطلاعاتی

Compact Disk Data Base یا به اختصار CDDB را که قبلاً در همین فصل مورد بررسی قرار گرفت برخوردار است. با کلیک روی عنوان موزیک در حال پخش لیست موزیک‌های ضبط شده به نمایش درآمده و به این ترتیب امکان دسترسی به موزیک موردنظر فراهم می‌شود.



شکل ۵۵-۱۷ رابط گرافیکی برنامه KsCD

برنامه Sound Mixer

این برنامه که اغلب با عنوان KMix نیز شناخته می‌شود، امکان تنظیم صدای ورودی از منابع مختلف را در اختیار می‌گذارد.

برنامه aRts Builder

این برنامه یک ابزار گرافیکی است که جهت تنظیم مشخصات مختلف صدا طراحی شده است. (برنامه aRts سرور صوتی یا اصطلاحاً sound server محیط گرافیکی KDE است.)

برنامه aRts Control Tool

این برنامه ابزاری برای کنترل تنظیمات مختلف برنامه aRts است.

برنامه Kaboodle

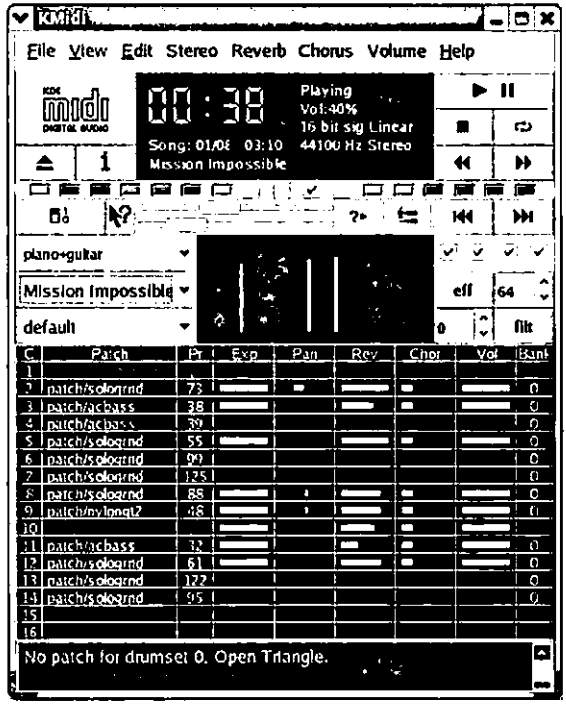
این برنامه ابزاری برای پخش فایل‌های صوتی (مانند فایل‌های wav.) است.

برنامه KMid

این برنامه ابزاری برای پخش فایل‌های صوتی mid. و kar. (فایل‌های Karaoke) است. برای استفاده از این برنامه، برخورداری کارت صوتی از قابلیت پشتیبانی فایل‌های MIDI ضروری است.

برنامه KMidi

این برنامه در واقع یک رابط گرافیکی برای دسترسی به قابلیت‌های برنامه TiMidity است. چنان‌چه کارت صوتی از فایل‌های MIDI پشتیبانی سخت‌افزاری به عمل نیاورد، باز هم ممکن است بتوان از این برنامه برای پخش فایل‌های mid. استفاده کرد. ضمن آن‌که فایل پیکربندی /etc/timidity.conf نیز باید موجود بوده و حاوی مشخصات پیکربندی این برنامه باشد. فهرست /usr/share/apps/kmidi/config حاوی نمونه‌ای از این فایل پیکربندی است. اگر در اجرای برنامه KMmidi با مشکل روبرو هستید، پیش از هر اقدامی مطمئن شوید که بسته نرم‌افزاری *-arts-devel روی کامپیوتر میزبان نصب شده است. شکل ۵۶-۱۷ پنجره برنامه KMidi را نشان می‌دهد.



شکل ۵۶-۱۷ پنجره برنامه KMidi

برنامه Noatum

این برنامه رابط گرافیکی برنامه سرور aRts است. با اجرای برنامه Noatun در نگاه نخست ممکن است چنین تصور شود که برنامه فاقد عملکرد است. در حقیقت این برنامه آیکنی را به پانل محیط گرافیکی KDE اضافه می‌کند که با کلیک راست روی آن، منوی اصلی برنامه Noatun باز می شود. مشابه برنامه

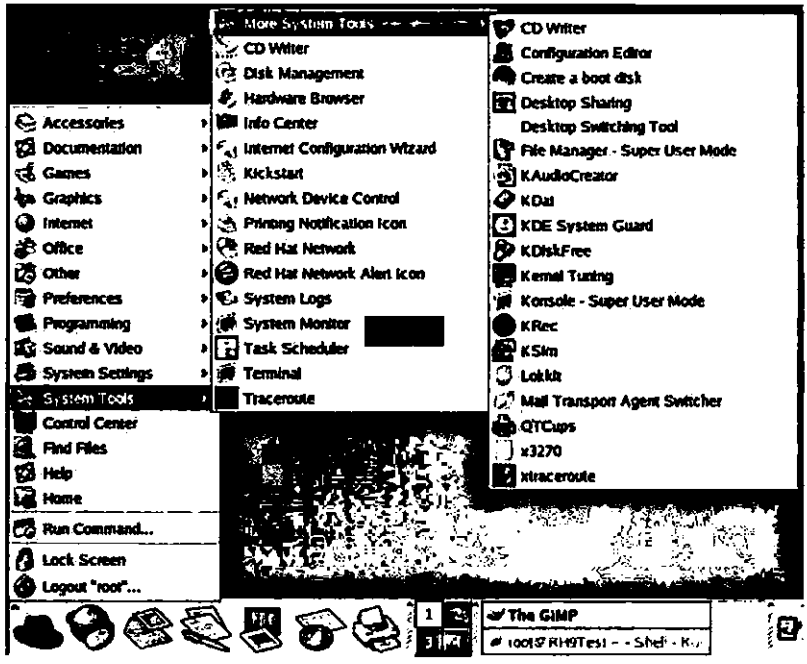
XMMS که در فصل شانزدهم مورد بررسی قرار گرفت، این برنامه نیز امکان دسترسی به اکولایزر و منوی حاوی لیست موزیک‌ها را در اختیار می‌گذارد.

برنامه TiMidity Synth

به توضیحات برنامه KMidi مراجعه کنید.

گروه System Tools

گروه System Tools شامل مجموعه‌ای از ابزارهای سیستمی مفید است. این ابزارها رابطه‌ای با ابزارهای پیکربندی *-redhat-config که در فصل نوزدهم به بررسی آن‌ها می‌پردازیم، ندارند. چنان‌که در شکل ۵۷-۱۷مشاهده می‌کنید، دسترسی به این ابزارها از طریق منوی فرعی System Tools امکان‌پذیر است.

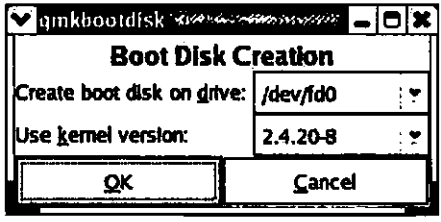


شکل ۵۷-۱۷ محتوای منوی System Tools

ابزار Create A Boot Disk

این ابزار به عنوان رابط گرافیکی فرمان mkbootdisk جهت تبدیل دیسکت ۱/۴۴ اینچی موجود در درایو مربوطه به دیسکی با قابلیت راه‌اندازی کامپیوتر طراحی شده است. برای اطلاع بیشتر در این

زمینه به بحث مربوط به فرمان mkbootdisk از فصل یازدهم مراجعه کنید. شکل ۵۸-۱۷ رابط گرافیکی ابزار مورد بحث را نشان می‌دهد.



شکل ۵۸-۱۷ رابط گرافیکی ابزار Create A Boot Disk

ابزار Desktop Sharing

این ابزار که قبلاً با عنوان krfb شناخته می‌شد، به‌منظورپشتیبانی ازمدیریت‌سرورهای xinetd پیش‌بینی شده است.

ابزار File Manager

این ابزار امکان دسترسی سریع کاربران به فهرست خانگی خود را در برنامه Konqueror فراهم می‌کند.

ابزار KAudioCreator

این‌ابزار امکان کپی‌کردن موزیک‌های موردنظر ازCDهای صوتی روی سایر CDها را در اختیار می‌گذارد. ضمن آن‌که از قابلیت دسترسی به بانک اطلاعاتی CDDB نیز برخوردار بوده و از این‌رو کاربران می‌توانند به اطلاعات بیشتری درباره قطعات موسیقی مورد علاقه خود دسترسی داشته باشند. ابزار مورد بحث به تعبیری در جای خود قرار نداشته و بهتر بود به همراه سایر برنامه‌های کاربردی چند رسانه‌ای در منوی Sound & Video واقع می‌شد.

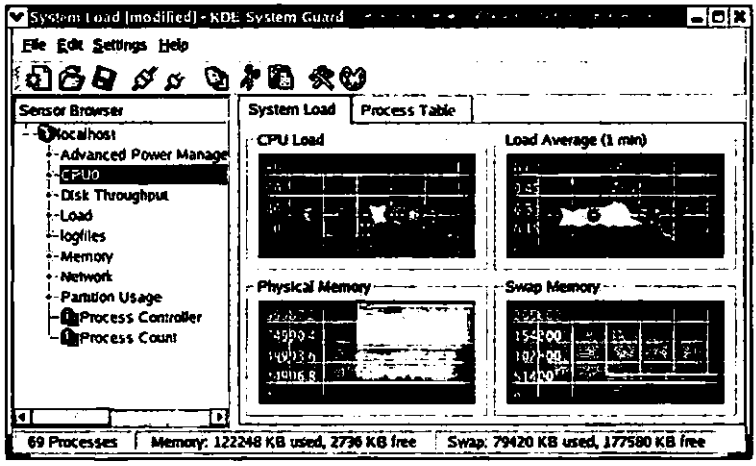
ابزار KDat

این ابزار به عنوان رابط گرافیکی فرمان tar امکان بایگانی مجموعه‌ای از فایل‌ها را در قالب فایلی واحد با پسوند tar. در اختیار می‌گذارد.

ابزار KDE System Guard

این ابزار که به اختصار ksysguard نامیده می‌شود، به‌منظور مدیریت‌وظایف و نظارت بر کارایی سیستم،

طراحی شده است. به طور پیش‌فرض، اطلاعاتی را که این ابزار درباره موارد مختلفی از جمله بار تحمیل شده به سیستم، میزان فعالیت پردازنده و میزان استفاده از حافظه (شامل حافظه اصلی و فضای swap) به نمایش می‌گذارد، با اجرای فرمان top در پشت صحنه تأمین می‌شود. در صورت تمایل می‌توان این ابزار را جهت نمایش نمودار گرافیکی مربوط به کارایی سایر اجزای سیستم نیز پیکربندی کرد. شکل ۵۹-۱۷ رابط گرافیکی این ابزار را نشان می‌دهد.



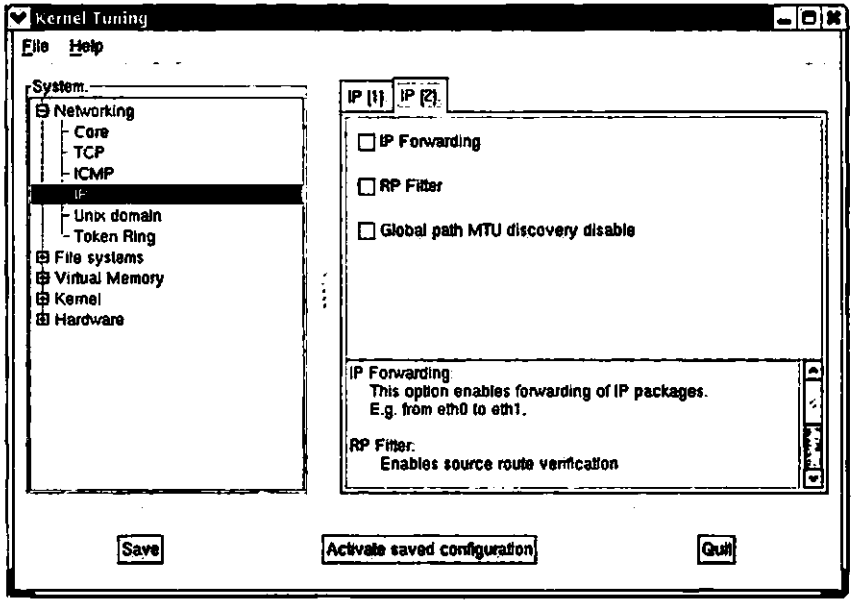
شکل ۵۹-۱۷ رابط گرافیکی ابزار KDE System Guard

ابزار KDiskFree

این ابزار به عنوان رابط گرافیکی فرمان df که در فصل هفتم به بررسی آن پرداختیم، امکان مشاهده فضای خالی قابل دسترس در تمام پارتیشن‌هایی را که هم‌اینک روی سیستم فایل سوار شده‌اند، در اختیار می‌گذارد.

ابزار Kernel Tuning

این ابزار به منظور پیکربندی مجدد برخی تنظیمات هسته سیستم‌عامل Linux پیش‌بینی شده است. چنان‌که از فصل یازدهم به خاطر دارید، این تنظیمات در قالب فهرست proc/ نگهداری می‌شوند. به عنوان مثال، برای آن‌که بتوانید کامپیوتر Linux را به عنوان دروازه میان دو شبکه پیکربندی کنید، باید مکانیزم IP Forwarding را فعال کنید. یکی از روش‌های متداول برای انجام این کار در فصل بیست و یکم مورد بررسی قرار خواهد گرفت. روش دیگر، چنان‌که در شکل ۶۰-۱۷ مشاهده می‌کنید، استفاده از برنامه Kernel Tuning است.



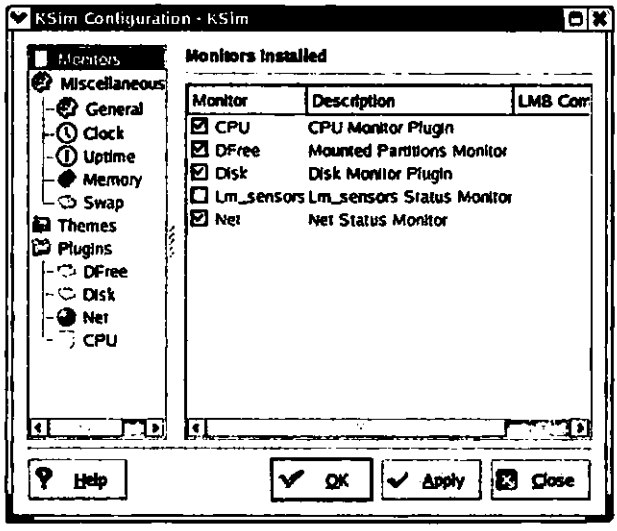
شکل ۶۰-۱۷ رابط گرافیکی ابزار Kernel Tuning

ابزار KRec

این ابزار به واسطه بهره‌گیری از قابلیت‌های برنامه aRts امکان ضبط صدا را در اختیار می‌گذارد. با توجه به کاربرد این ابزار، منوی Sound & Video جایگاه مناسب‌تری برای آن است.

ابزار KSim

این ابزار یک رابط گرافیکی است که به منظور بازبینی و نظارت بر کارایی سیستم طراحی شده است. مشابه ابزار KDE System Guard، اطلاعات مورد استفاده این ابزار به واسطه اجرای فرمان top در پشت صحنه تأمین می‌شود. آیکن ابزار KSim پس از اجرا روی پانل محیط گرافیکی KDE مستقر می‌شود. با کلیک راست‌روی این آیکن و انتخاب گزینه KSim Configuration از منوی حاصل، امکانات پیکربندی آن مشابه شکل ۶۱-۱۷ در اختیار قرار می‌گیرد. چنان‌که مشاهده می‌کنید، این ابزار از قابلیت پیکربندی بسیار خوبی برخوردار است.



شکل ۱۷-۶۱ امکانات پیکربندی ابزار KSim

ابزار QTCups

تا زمان نگارش کتاب حاضر، این ابزار از طریق منوی فرعی More System Tools واقع در منوی System Tools از منوی اصلی قابل دستیابی است. عملکرد این ابزار در نسخه‌های اخیر سیستم‌عامل Red Hat Linux توسط ابزار KDEPrint تحت‌الشعاع قرار گرفته است. (دسترسی به ابزار KDEPrint با اجرای فرمان kprinter امکان‌پذیر است.) ابزار KDEPrint در واقع رابطی میان ابزارهای قابل استفاده در محیط گرافیکی KDE و سرویس چاپ راه‌اندازی شده روی کامپیوتر میزبان است. چنان‌که در فصل بیست و پنجم خواهید دید، سرویس چاپ پیش‌فرض در سیستم‌عامل مذکور سرویسی با عنوان CUPS است.

جمع‌بندی

در این فصل محیط گرافیکی KDE را به طور مقدماتی مورد بررسی قرار دادیم. محیط KDE یکی از محیط‌های گرافیکی بسیار رایج در سیستم‌عامل Linux بوده و حاوی ابزارهای متعددی است. عملکرد برخی از این ابزارها شبیه به ابزارهای موجود در سیستم‌عامل ویندوز است. در محیط گرافیکی KDE می‌توان پنجره‌های برنامه‌های کاربردی را بین چهار محیط کاری یا بیشتر توزیع کرد. این محیط از قابلیت‌های پیکربندی بسیار خوبی متناسب با نیازهای کاربران برخوردار است.

ابزارها و برنامه‌های کاربردی متعددی در محیط گرافیکی KDE تعبیه شده‌اند که در صورت استفاده از آن‌ها به آسانی می‌توان به میزان قابل توجهی در هزینه تأمین نرم‌افزار صرفه جویی کرد. برخی از این ابزارها کاربردهای روزمره دارند. برای مثال، ابزارهای کار با اینترنت شامل مرورگرهای وب، برنامه‌های مدیریت پیغام‌های الکترونیکی و برنامه‌های گپ‌زنی و ابزارهای چندرسانه‌ای شامل برنامه‌هایی برای مدیریت، پردازش و ضبط صدا و تصویر هستند. ضمناً در این محیط گرافیکی مجموعه‌ای از ابزارهای سیستمی نیز جهت ساده کردن فعالیت مدیران سیستم‌ها پیش‌بینی شده است.

در فصل آینده برخی از مهم‌ترین برنامه‌های کاربردی عرضه شده برای سیستم‌عامل Linux را که دارای رابط گرافیکی هستند، مورد بررسی قرار می‌دهیم.

فصل هجدهم

برنامه‌های کاربردی با رابط گرافیکی

تعداد برنامه‌های کاربردی عرضه شده به همراه سیستم‌عامل Red Hat Linux، به طور قابل توجهی از تعداد برنامه‌هایی‌که به همراه سیستم‌عامل ویندوز عرضه می‌شوند، پیشی گرفته است. بهترین نمونه‌های قابل اشاره در این مورد چند نرم‌افزار اداری است که هر کدام به نوبه خود شامل مجموعه‌ای از رایج‌ترین برنامه‌های کاربردی هستند. استفاده از این گونه برنامه‌های کاربردی بدون شک صرفه‌جویی قابل ملاحظه‌ای را در تأمین نرم‌افزار مایحتاج به دنبال دارد.

هریک از نرم‌افزارهای اداری عرضه شده برای سیستم‌عامل Linux به طور مشخص متشکل از یک برنامه واژه‌پرداز، یک برنامه صفحه گسترده، یک برنامه گرافیکی، یک برنامه مدیریت نمایش و در نهایت برنامه‌ای برای زمان‌بندی پروژه‌ها هستند. برخی از این نرم‌افزارها برنامه‌های بیشتری را نیز شامل می‌شوند. گاهی اوقات لازم است برنامه‌های کاربردی موردنیاز خود را با دستیابی به شبکه اینترنت روی کامپیوتر خود بارگذاری کنید. اما نیازی نیست که برای این کار پول پرداخت کنید. تمام این برنامه‌ها مشابه نرم‌افزارهای اداری عرضه شده برای سیستم‌عامل Linux به رایگان قابل دستیابی و استفاده هستند. سه مجموعه نرم‌افزاری اداری مورد بحث در این فصل با عناوین OpenOffice، KOoffice و GNOME Office از جمله رایج‌ترین نرم‌افزارهای اداری سیستم‌عامل Linux محسوب می‌شوند.

علاوه بر این، چندین برنامه گرافیکی نیز در زمینه مشاهده و اسکن تصاویر، عکس‌برداری از صفحه نمایش و بازخوانی فایل‌های PDF به همراه سیستم‌عامل Red Hat Linux توزیع می‌شود.

در این فصل هریک از برنامه‌های کاربردی فوق را به طور خلاصه شرح می‌دهیم. اهمیت کاربرد برخی از این برنامه‌ها چنان است که کتاب‌های مختلفی در مورد آن‌ها به رشته تحریر درآمده است. موضوعات مورد بررسی در فصل حاضر به این قرار است:

- بررسی نرم‌افزار OpenOffice
- بررسی نرم‌افزار GNOME Office
- بررسی نرم‌افزار KOffice
- بررسی برنامه‌های گرافیکی

نرم‌افزار OpenOffice

نرم‌افزار OpenOffice به عنوان نرم‌افزار اداری پیش‌فرض در سیستم‌عامل Red Hat Linux بر اساس نرم‌افزار StarOffice (محصول شرکت Sun Microsystems) طراحی و پیاده‌سازی شده است. جدول ۱-۱۸ برنامه‌های کاربردی موجود در این نرم‌افزار را به اختصار شرح می‌دهد. برای اطلاع بیشتر درباره این نرم‌افزار به وب سایت رسمی آن در آدرس http://www.openoffice.org مراجعه کنید.

جدول ۱-۱۸ شرح مختصر برنامه‌های کاربردی توزیع شده در قالب نرم‌افزار OpenOffice

عنوان برنامه کاربردی	توضیح
Calc	این برنامه یک صفحه گسترده است.
Draw	این برنامه امکان رسم نمودارهای مختلف را در اختیار می‌گذارد.
Impress	این برنامه به منظور نمایش محتوا طراحی شده است.
Math	این برنامه امکان نوشتن فرمول‌های مختلف را در اختیار می‌گذارد.
Printer Setup	این برنامه رابطی برای مدیریت چاپگر است.
Repair	این برنامه امکان نصب سایر برنامه‌ها را در اختیار می‌گذارد.
Writer	این برنامه یک واژه پرداز است.

دسترسی به برنامه‌های کاربردی نرم‌افزار OpenOffice از هر محیط گرافیکی دلخواهی امکان‌پذیر است. در محیط گرافیکی GNOME این دسترسی از طریق منوی فرعی Office واقع در منوی اصلی فراهم می‌شود.

منوی اصلی محیط گرافیکی KDE دقیقاً مشابه منوی اصلی محیط گرافیکی GNOME است. هر دو منوی فوق با کلیک روی آیکن کلاه قرمز موجود در در گوشه پایین و سمت چپ صفحه باز می‌شوند. در این فصل بررسی‌های خود را در محیط گرافیکی GNOME یعنی محیط گرافیکی پیش‌فرض در سیستم‌عامل Red Hat Linux انجام می‌دهیم. دستورالعمل‌های مربوط به محیط گرافیکی KDE ممکن است با آن‌چه در این‌جا مطالعه می‌کنید، اندکی متفاوت باشد.

روش دیگر دسترسی به برنامه‌های کاربردی نرم‌افزار OpenOffice از طریق پانل محیط گرافیکی موجود در پایین صفحه است. چنان‌که در فصل‌های شانزدهم و هفدهم توضیح داده شد، دسترسی به برنامه

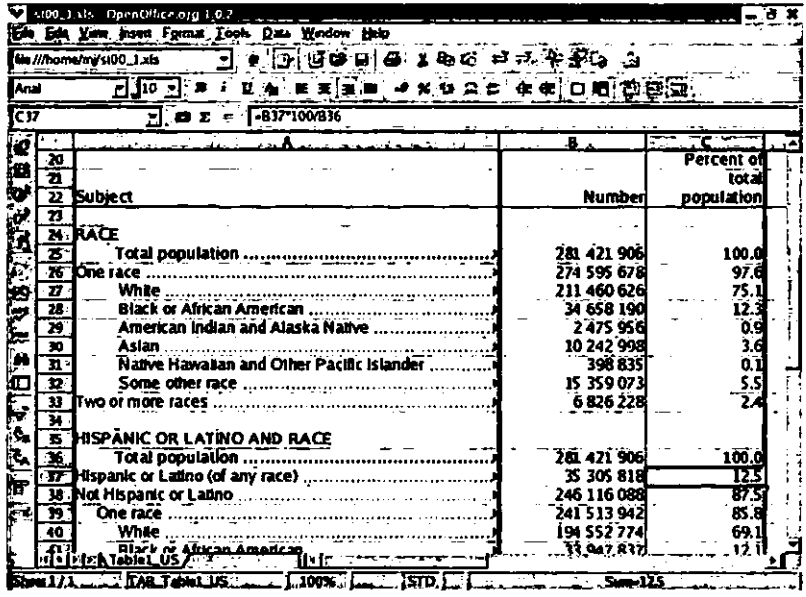
کاربردی Writer از این نرم‌افزار با کلیک روی آیکنی از پانل مزبور به شکل کاغذ و قلم امکان‌پذیر است. هم‌چنین امکان دسترسی به برنامه‌های کاربردی Impress از نرم‌افزار OpenOffice با کلیک روی آیکنی از همین پانل به شکل نمودار میله‌ای و اسلاید و بالاخره دسترسی به برنامه کاربردی Calc از نرم‌افزار نامبرده با کلیک روی آیکنی از پانل محیط گرافیکی به شکل نمودار مدور فراهم شده است.

برای اطلاع بیشتر درباره نرم‌افزار OpenOffice به وب سایت پروژه مربوطه در آدرس اینترنتی http://www.openoffice.org مراجعه کنید.

برنامه OpenOffice Calc

به احتمال قوی، نخستین برنامه تجاری مهمی که برای کامپیوترهای شخصی نوشته شد، یک صفحه گسترده یا اصطلاحاً spreadsheet بود. این گونه برنامه‌ها امکانات انجام محاسبات متنوعی را روی مجموعه‌ای از داده‌ها در اختیار می‌گذارند. برنامه‌های مزبور اغلب در تحلیل آماری، مدل‌سازی تجاری و برنامه‌ریزی مورد استفاده قرار می‌گیرند.

برای دستیابی به پنجره این برنامه، کافی است گزینه OpenOffice.org Calc را از منوی Office واقع در منوی اصلی انتخاب کرده یا فرمان oocalc را در سطر فرمان محیط گرافیکی موردنظر اجرا کنید. شکل ۱-۱۸ پنجره این برنامه را نشان می‌دهد.



شکل ۱-۱۸ پنجره برنامه OpenOffice Calc

چنان‌که مشاهده می‌کنید، ظاهر برنامه Calc شبیه به صفحه گسترده است. عملکرد این برنامه را می‌توان با برنامه Microsoft Excel مقایسه کرد. جدول ۲-۱۸ کاربرد نوار ابزارهای این برنامه را به اختصار شرح می‌دهد.

جدول ۲-۱۸ شرح کاربرد نوار ابزارهای برنامه OpenOffice Calc

عنوان نوار ابزار	توضیح
Formula	این نوار ابزار بیانگر موقعیت سلول جاری و فرمول‌های مورد استفاده برای محاسبه مقدار آن است.
Function	این نوار ابزار امکاناتی نظیر باز کردن سند، چاپ کردن سند و لغو آخرین عملیات را در اختیار می‌گذارد.
Hyperlink	این نوار ابزار امکان دسترسی به صفحات وب را در اختیار می‌گذارد.
Main	این نوار ابزار امکانات مختلفی از جمله رسم نمودار داده‌های مندرج در جدول، پشتیبانی از قالب‌بندی، بازبینی املای واژه‌ها، مرتب سازی و دسته بندی داده‌های مندرج در جدول را در اختیار می‌گذارد
Object	این نوار ابزار امکانات مربوط به قالب‌بندی داده‌ها، ازجمله تعیین فونت‌های مورد استفاده، تنظیم فواصل خانه‌های جدول، شماره‌گذاری، حاشیه بندی و تراز کردن داده‌های مندرج در جدول را در اختیار می‌گذارد.

برنامه OpenOffice Calc امکان پردازش فایل‌های مختلفی از جمله فایل‌های تولید شده توسط سایر برنامه‌های صفحه گسترده را دارد. جدول ۳-۱۸ شاخص مربوط به هریک از این فایل‌ها را توضیح می‌دهد.

جدول ۳-۱۸ شاخص فایل‌های قابل پردازش توسط برنامه OpenOffice Calc

شاخص فایل	توضیح
.sxc	این شاخص بیانگر صفحات گسترده تولید شده در برنامه OpenOfficeCalc است.
.stc	این شاخص بیانگر الگوهای مورد استفاده در برنامه OpenOffice Calc جهت ایجاد اسناد مربوطه است.
.dif	این شاخص (با عنوان Data Interchange Format) بیانگر فایل‌های تولید شده توسط برنامه VisiCalc است.
.dbf	این شاخص بیانگر بانک‌های اطلاعاتی تولید شده توسط نرم‌افزار dBASE یا FoxPro است.

شاخص فایل	توضیح
.xls	این شاخص بیانگر فایل‌های تولید شده در برنامه Microsoft Excel 95/5.0 یا Microsoft Escel 97/2000/XP است.
.xlt	این شاخص بیانگر الگوهای مورد استفاده در برنامه Microsoft Excel 95/5.0 یا Microsoft Escel 97/2000/XP جهت ایجاد اسناد مربوطه است.
.sdc	این شاخص بیانگر فایل‌هایی است که توسط برنامه صفحه گسترده نرم‌افزار StarOffice یعنی StarOffice Calc 5.0/4.0/3.0 تولید شده‌اند.
.vor	این شاخص بیانگر الگوهای مورد استفاده در برنامه صفحه گسترده نرم‌افزار StarOffice یعنی StarOffice Calc 5.0/4.0/3.0، جهت ایجاد اسناد مربوطه است.
.slk	این شاخص بیانگر پیوندهای نمادین یا اصطلاحاً symbolic link است.
.wks	این شاخص بیانگر فایل‌های تولید شده توسط برنامه Lotus1-2-3 است.
.csv	این شاخص بیانگر فایل‌هایی متنی به خصوصی است که اطلاعات مندرج در آن‌ها توسط علامت کاما از یکدیگر جدا شده‌اند. این گونه فایل‌ها صفحات گسترده‌ای هستند که در قالب متنی ذخیره شده‌اند.
.html	این شاخص بیانگر صفحات وب است.

توضیحی در باب فایل‌های CSV

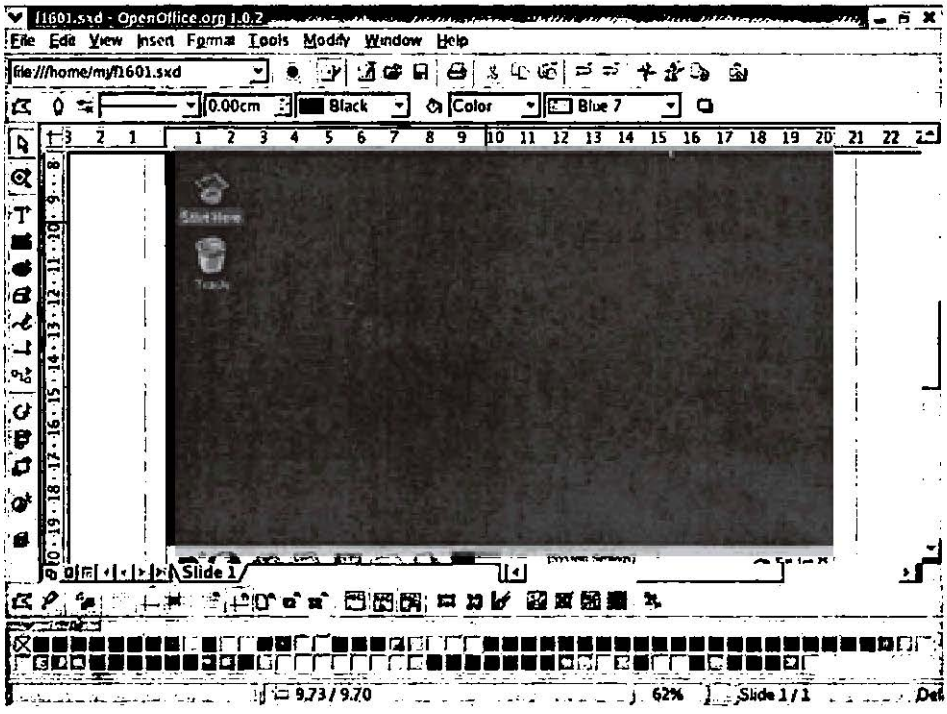
صفحات گسترده و سایر داده‌های جدولی را می‌توان در قالب فایل‌های متنی CVS ذخیره کرد. در این گونه فایل‌ها هر مقدار توسط علامت کاما از مقدار دیگر جدا می‌شود. به این ترتیب، چنان‌چه این داده‌ها در یک فایل متنی ذخیره شده باشند، هر کدام از آن‌ها را می‌توان در یکی از خانه‌های سطر دلخواهی از یک صفحه گسترده درج کرد:

```
height, 60, 61, 44, 78, 56, 66
```

برنامه OpenOffice Draw

این برنامه به منظور مدیریت طیف متنوعی از فایل‌های گرافیکی، از فایل‌های تولید شده در برنامه طراحی AutoCAD گرفته تا فایل‌های bitmap، مورد استفاده قرار می‌گیرد. به این ترتیب، برنامه مورد بحث به عنوان یک ابزار طراحی می‌تواند توسط کاربرانی که به نوعی با گرافیک در ارتباط هستند (از جمله مهندسان طراح و گرافیست‌ها) مورد بهره‌برداری قرار گیرد.

دسترسی به این برنامه با انتخاب گزینه OpenOffice.org Draw از منوی فرعی Office واقع در منوی اصلی یا با اجرای مستقیم فرمان oodraw در سطر فرمان محیط گرافیکی موردنظر امکان‌پذیر است. شکل ۲-۱۸ پنجره این برنامه را در محیط گرافیکی GNOME نشان می‌دهد.



شکل ۲-۱۸ پنجره برنامه OpenOffice Draw

چنان‌که مشاهده می‌کنید، این برنامه متشکل از نوار ابزارهای مختلفی است که تسهیلات لازم به منظور رنگ‌آمیزی، ترسیم اشکال، اضافه کردن عناصر جدید به طرح‌موجود و سایرموارد را در اختیار می‌گذارد. جدول ۴-۱۸ کاربرد این نوار ابزارها را به اختصار شرح می‌دهد.

جدول ۴-۱۸ شرح کاربرد نوار ابزارهای برنامه OpenOffice Draw

عنوان نوار ابزار	توضیح
Color	این نوار ابزار امکان انتخاب رنگ‌های مختلف را در اختیار می‌گذارد.
Function	این نوار ابزار امکان انجام عملیاتی چون باز کردن سند، چاپ سند و لغو آخرین عملیات را در اختیار می‌گذارد.

عنوان نوار ابزار	توضیح
Hyperlink	این نوار ابزار امکان دسترسی به صفحات وب را فراهم می‌کند.
Main	این نوار ابزار امکان انجام عملیاتی نظیر بزرگ‌نمایی، درج عناصر جدید از جمله متن و اشکال هندسی و ترازبندی عناصر موجود در سند را در اختیار می‌گذارد.
Object	این نوار ابزار امکان انجام عملیاتی نظیر درج و پیکربندی جدول، ویرایش متن، چرخش عناصر به اندازه مورد نظر، تغییر رنگ و مواردی از این قبیل را در اختیار می‌گذارد.
Option	این نوار ابزار امکان انجام تنظیمات مختلفی را در مورد خطوط از جمله تعیین پهنا و رنگ آن‌ها در اختیار می‌گذارد.

علاوه بر این، برنامه OpenOffice Draw امکان پردازش فایل‌های مختلفی را نیز فراهم می‌کند که در این میان می‌توان به فایل‌های تولید شده توسط برنامه Microsoft Excel و StarOffice Calc و هم‌چنین بانک‌های اطلاعاتی dBASE و FoxPro اشاره کرد. جدول ۵-۱۸ شاخص این قبیل فایل ها را توضیح می‌دهد.

جدول ۵-۱۸ شاخص فایل‌های قابل پردازش توسط برنامه OpenOffice Draw

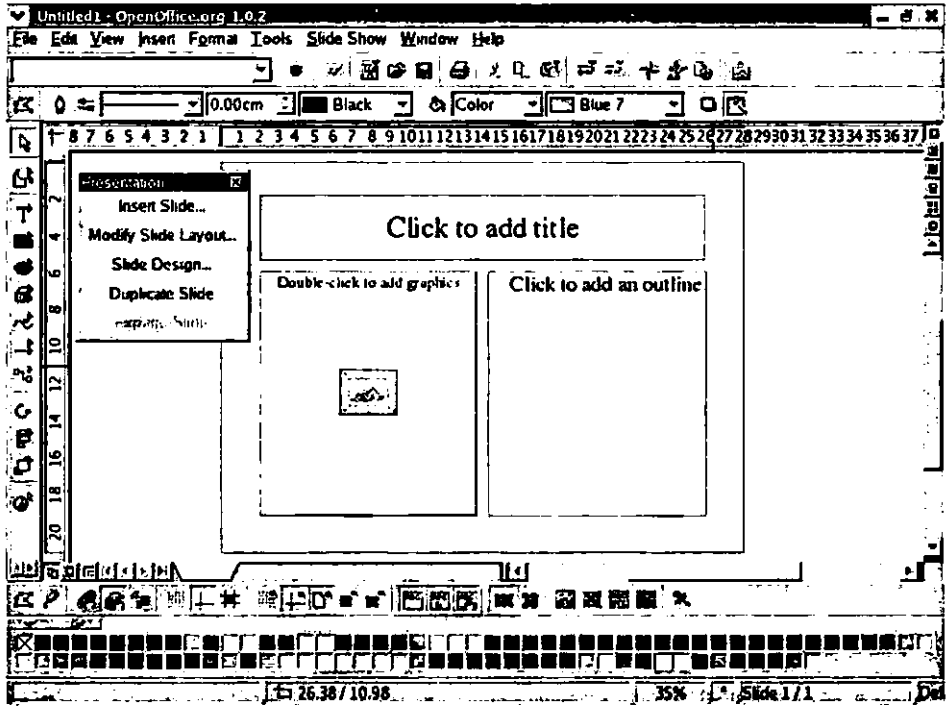
شاخص فایل	توضیح
.sxd	این شاخص بیانگر فایل‌های تولید شده توسط برنامه OpenOffice Draw است.
.std	این شاخص بیانگر الگوهای مورد استفاده در برنامه OpenOffice Draw جهت ایجاد اسناد مربوطه است.
.bmp	این شاخص بیانگر فایل‌های bitmap است.
.dxf	این شاخص بیانگر فایل‌های AutoCAD Interchange Format است.
.emf	این شاخص بیانگر فایل‌های Enhanced MetaFile است.
.eps	این شاخص بیانگر فایل‌های Enhanced PostScript است.
.gif	این شاخص بیانگر فایل‌های Graphics Interchange Format یا به اختصار GIF است.
.jpg	این شاخص بیانگر فایل‌های Joint Photographic Experts Group یا به اختصار JPEG است.
.met	این شاخص بیانگر فایل‌های OS/2 Metafile است.
.pbm	این شاخص بیانگر فایل‌های Portable bitmap است.
.pcd	این شاخص بیانگر فایل‌های Photo CD است.

شاخص فایل	توضیح
.pct	این شاخص بیانگر فایل‌های Macintosh Pict است.
.pcx	این شاخص بیانگر فایل‌های Zsoft Paintbrush است.
.pgm	این شاخص بیانگر فایل‌های Portable Gray Map است.
.png	این شاخص بیانگر فایل‌های Portable Network Graphic یا به اختصار PNG است.
.ppm	این شاخص بیانگر فایل‌های Portable Pixel Map است.
.psd	این شاخص بیانگر فایل‌های تولید شده توسط برنامه Adobe Photoshop است.
.ras	این شاخص بیانگر فایل‌های Sun raster Image است.
.sda	این شاخص بیانگر فایل‌های تولید شده توسط برنامه StarOffice 5.0 Draw است.
.sdd	این شاخص بیانگر فایل‌های تولید شده توسط برنامه StarOffice 3.0 Draw است.
.sgf	این شاخص بیانگر فایل‌های تولید شده توسط برنامه StarWriter است.
.sgv	این شاخص بیانگر فایل‌های تولید شده توسط برنامه StarDraw 2.0 است.
.svm	این شاخص بیانگر فایل‌های StarView Metafile است.
.tga	این شاخص بیانگر فایل‌های TrueVision Targa است.
.tiff	این شاخص بیانگر فایل‌های Tagged Image File Format یا به اختصار TIFF است.
.vor	این شاخص بیانگر الگوهای مورد استفاده در برنامه StarOffice 3.0Draw و StarOffice 5.0 Draw جهت ایجاد اسناد مربوطه است.
.wmf	این شاخص بیانگر فایل‌های Microsoft Windows Metafile است.
.xbm	این شاخص بیانگر فایل‌های X bitmap است.
.xpm	این شاخص بیانگر فایل‌های X pixmap است.

برنامه OpenOffice Impress

این برنامه به منظور تهیه اسلاید جهت نمایش محتوای موردنظر طراحی شده است. این گونه برنامه‌ها در اصل نوعی واژه‌پرداز به خصوص با قابلیت‌های گرافیکی هستند. معمولاً نمایش اسلاید با هدف ارایه مطالب موردنظر به صورت online یا برای مخاطبینی که در یک اتاق یا سالن اجتماعات گرد هم آمده‌اند، انجام می‌شود. برنامه OpenOffice Impress امکان ایجاد اسلاید نمایش را مانند برنامه‌هایی چون Microsoft PowerPoint و StarOffice Impress در اختیار می‌گذارد.

دسترسی به برنامه OpenOffice Impress با انتخاب گزینه OpenOffice از منوی فرعی Office واقع در منوی اصلی یا با اجرای مستقیم فرمان ooimpress در پنجرهٔ سطر فرمان محیط گرافیکی موردنظر امکان‌پذیر است. شکل ۳-۱۸ پنجره این برنامه را نشان می‌دهد.



شکل ۳-۱۸ پنجره برنامه OpenOffice Impress

چنان‌که مشاهده می‌کنید، برنامه OpenOffice Impress متشکل از تعدادی نوار ابزار است که به منظور رنگ‌آمیزی، ترسیم اشکال، درج و ویرایش متون و سایر عناصر پیش‌بینی شده‌اند. شرح مختصری درباره کاربرد این نوار ابزارها در جدول ۶-۱۸ آمده است.

جدول ۶-۱۸ شرح کاربرد نوار ابزارهای برنامه OpenOffice Impress

عنوان نوار ابزار	توضیح
Color	این نوار ابزار امکان انتخاب رنگ‌های موردنظر را در اختیار می‌گذارد.
Function	این نوار ابزار امکان انجام عملیاتی چون باز کردن سند، چاپ سند و لغو آخرین عملیات را در اختیار می‌گذارد.

عنوان نوار ابزار	توضیح
Hyperlink	این نوار ابزار امکان دسترسی به صفحات وب را فراهم می‌کند.
Main	این نوار ابزار امکان انجام عملیاتی نظیر بزرگ‌نمایی، درج عناصر جدید از جمله متن و اشکال هندسی، تراز بندی عناصر و مواردی از این قبیل را در اختیار می‌گذارد.
Object	این نوار ابزار امکان انجام عملیاتی نظیر درج و پیکربندی جدول، ویرایش متن، چرخش عناصر به اندازه موردنظر و مواردی از این قبیل را در اختیار می‌گذارد.
Option	این نوار ابزار امکان انجام تنظیمات مختلفی را در مورد خطوط، از جمله تعیین پهنا و رنگ آن‌ها در اختیار می‌گذارد.
Presentation	این نوار ابزار امکانات موردنیاز برای طراحی هر اسلاید را در اختیار می‌گذارد.

به محض بازشدن پنجره برنامه OpenOffice Impress ویزاردی تحت عنوان AutoPilot Presentation، امکانات لازم برای ایجاد اسلاید را با نمایش یک صفحه خالی و یک الگوی طراحی در اختیار قرار می‌دهد. در مورد هر اسلاید جدید، برنامه مذکور پیکربندی مواردی از قبیل طرح، رسانه خروجی و نکات ابتدایی مربوط به آن اسلاید را انجام می‌دهد.

علاوه بر این، برنامه OpenOffice Impress امکان پردازش فایل‌های دیگری از جمله فایل‌های تولید شده توسط برنامه‌های کاربردی Microsoft PowerPoint، StarDraw، StarImpress و عموماً هر برنامه کاربردی که امکان ذخیره فایل را در قالب cgm. فراهم کند، در اختیار می‌گذارد. جدول ۷-۱۸ شاخص این فایل‌ها را به اختصار شرح می‌دهد.

جدول ۷-۱۸ شاخص فایل‌های قابل پردازش توسط برنامه OpenOffice Impress

شاخص فایل	توضیح
.sxi	این شاخص بیانگر فایل‌های تولید شده توسط برنامه OpenOffice Impress است.
.sti	این شاخص بیانگر الگوهای مورد استفاده در برنامه OpenOffice Impress است.
.sxd	این شاخص بیانگر فایل‌های تولید شده توسط برنامه OpenOffice Draw است.
.ppt	این شاخص بیانگر فایل‌های تولید شده توسط برنامه Microsoft PowerPoint 97/2000/XP است.
.pot	این شاخص بیانگر الگوهای مورد استفاده در برنامه Microsoft PowerPoint 97/2000/XP برای ایجاد اسناد مربوطه است.
.sda	این شاخص بیانگر فایل‌های فایل‌های ایجاد شده توسط برنامه StarDraw 5.0 است.

شاخص فایل	توضیح
.sdd	این شاخص بیانگر فایل‌های فایل‌های ایجاد شده توسط برنامه‌های StarDraw 3.0 و StarImpress 4.0/5.0 است.
.vor	این شاخص بیانگر الگوهای مورد استفاده در برنامه StarImpress 4.0/5.0 برای ایجاد اسناد مربوطه است.

برنامه OpenOffice Writer

یکی از مشکلات پردازش اسناد در دنیای کامپیوترها وجود قالب‌های بسیار متنوع است. به عنوان مثال، تبدیل قالب اسناد تولید شده توسط برنامه Microsoft Word به قالب اسنادی که برنامه Corel WordPerfect یا StarOffice Write تولید می‌کند، مستلزم انجام فرآیندی برای ترجمه این اسناد است. البته بیشتر برنامه‌های واژه پرداز، از جمله برنامه OpenOffice Writer دارای این قابلیت هستند. با وجود این، برخی از برنامه‌ها این کار را به درستی انجام نمی‌دهند.

برنامه OpenOffice Writer در زمینه تبدیل قالب اسناد یک شاهکار محسوب می‌شود. با این همه، برخی کاربران (از جمله ناشران) انتظارات ویژه‌ای دارند که این برنامه به خوبی از عهده آن‌ها برنمی‌آید. علیرغم این موضوع، برنامه مذکور برای بیشتر کاربردها، از جمله امور تجاری و مانند آن به اندازه کافی مناسب است.

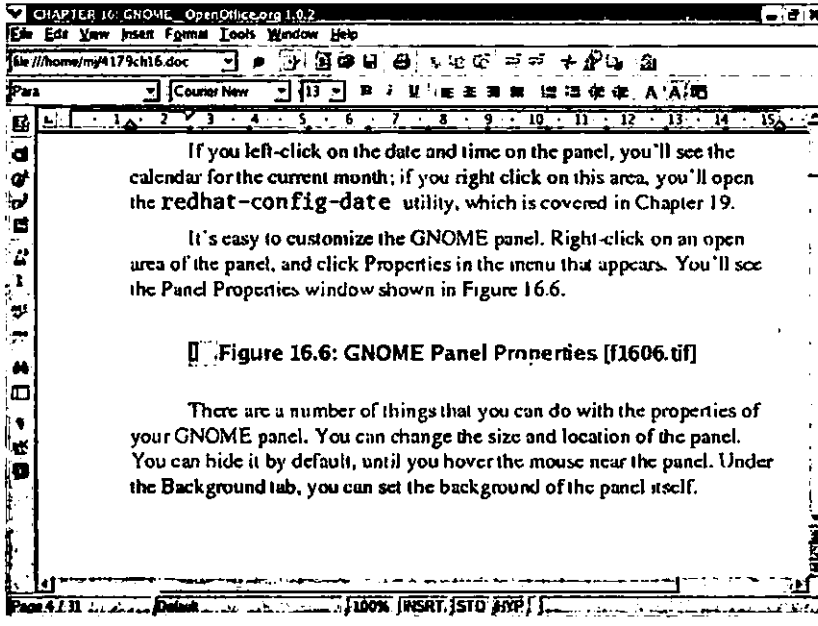
دسترسی به برنامه OpenOffice Writer با انتخاب گزینه OpenOffice Writer واقع در منوی فرعی Office از منوی اصلی یا با اجرای مستقیم فرمان oowriter در سطر فرمان محیط گرافیکی مورد استفاده امکان‌پذیر است. اسناد تولید شده توسط این برنامه دارای تمام ویژگی‌هایی اسناد تولید شده توسط برنامه Microsoft Word است. شکل ۴-۱۸ پنجره برنامه OpenOffice Writer را نشان می‌دهد.

چنان‌که مشاهده می‌کنید، این برنامه دارای نوار ابزارهای مختلفی است. جدول ۸-۱۸ کاربرد آن‌ها را به اختصار شرح می‌دهد.

جدول ۸-۱۸ کاربرد نوار ابزارهای برنامه OpenOffice Writer

عنوان نوار ابزار	توضیح
Function	این نوار ابزار امکان انجام عملیاتی چون باز کردن سند، چاپ سند و لغو آخرین عملیات را در اختیار می‌گذارد.
Hyperlink	این نوار ابزار امکان دسترسی به صفحات وب را فراهم می‌کند.

عنوان نوار ابزار	توضیح
Main	این نوار ابزار امکان انجام عملیاتی نظیر بررسی املای واژه‌ها، بزرگ‌نمایی، درج عناصر جدید از جمله متن و اشکال هندسی، تراز بندی، ایجاد فرم و مواردی از این قبیل را در اختیار می‌گذارد.
Object	این نوار ابزار امکان پیکربندی فونت‌ها، تعیین نحوه آرایش سند، قالب‌بندی متن، استفاده از رنگ و مواردی از این قبیل را در اختیار می‌گذارد.



شکل ۴-۱۸ پنجره برنامه OpenOffice Writer

علاوه بر این، برنامه OpenOffice Writer امکان پردازش فایل‌های دیگری از جمله فایل‌های تولید شده توسط سایر واژه پردازها را نیز در اختیار می‌گذارد. جدول ۹-۱۸ شاخص این گونه فایل‌ها را به اختصار شرح می‌دهد.

کاربران حرفه‌ای سیستم‌عامل Linux برای کارهای نشر، اغلب از ابزارهای متنی دیگری به ویژه دو ابزار TeX و LaTeX استفاده می‌کنند. این ابزارها فرامینی را به منظور قالب‌بندی عناوین، حروف ایتالیک و مواردی از این قبیل در اختیار قرار می‌دهند. البته این‌گونه فرامین در برنامه‌های کاربردی مختلفی از جمله Corel WordPerfect 5.2 نیز پشتیبانی شده‌اند.

جدول ۹-۱۸ شاخص فایل‌های قابل پردازش توسط برنامه OpenOffice Writer

شاخص فایل	توضیح
.sxw	این شاخص بیانگر فایل‌های تولید شده توسط برنامه OpenOffice Writer است. قالب این گونه فایل‌ها از نوع متن نیست.
.stw	این شاخص بیانگر الگوهای مورد استفاده در برنامه OpenOffice Writerبرای تولید اسناد مربوطه است.
.doc	این شاخص بیانگر فایل‌های تولید شده در برنامه Microsoft Word 95/97/2000/XP/6.0 است.
.html	این شاخص بیانگر فایل‌های HTML است.
.rtf	این شاخص بیانگر فایل‌های Rich Text Format یا به اختصار RTF است. این قالب توسط اغلب واژه پردازها قابل پردازش است.
.sdw	این شاخص بیانگر فایل‌های تولید شده توسط برنامه StarWriter 3.0/4.0/5.0 است.
.vor	این شاخص بیانگر الگوهای مورد استفاده در برنامه‌های StarWriter 3.0/4.0/5.0 برای تولید اسناد مربوطه است.
.txt	این شاخص بیانگر فایل‌های متنی معمولی است.

ابزارهای موجود در نرم‌افزار OpenOffice

علاوه بر برنامه‌های کاربردی مورد بحث، ابزارهای مفیدی نیز در قالب نرم‌افزار OpenOffice تعبیه شده که مهم‌ترین آن‌ها به این شرح است:

- **ابزار OpenOffice Math**: این ابزار به منظور قالب‌بندی معادلات پیچیده متشکل از توابع مثلثاتی، انتگرال، حد، توابع نمایی و موارد مشابه طراحی شده است. برای دستیابی به آن کافی است فرمان oomath را از سطر فرمان محیط گرافیکی مورد استفاده اجرا کنید.
- **ابزار OpenOffice Printer Setup**: این ابزار جهت پیکربندی چاپگر و قالب چاپ اسناد تولید شده توسط برنامه‌های کاربردی نرم‌افزار OpenOffice طراحی شده است. برای دستیابی به آن کافی است فرمان oopadmin را از سطر فرمان محیط گرافیکی مورد استفاده اجرا کنید.
- **ابزار OpenOffice Repair**: این ابزار امکان حذف و اضافه یا اصلاح اجزای نرم‌افزار OpenOffice را در اختیار می‌گذارد. برای دستیابی به آن کافی است فرمان oosetup را از سطر فرمان محیط گرافیکی مورد استفاده اجرا کنید.

سخنی در باب نرم‌افزار CrossOver Office

نرم‌افزار CrossOver Office به منظور استفاده از برخی برنامه‌های کاربردی سیستم‌عامل ویندوز تحت سیستم‌عامل Linux توسعه یافته است. این نرم‌افزار که با قیمت ۵۴/۹۵ دلار توزیع می‌شود، بخشی از پروژه WINE (یا WINE Is Not an Emulator) است. در حال حاضر، این نرم‌افزار امکان اجرای برخی از متداول‌ترین برنامه‌های کاربردی سیستم‌عامل ویندوز را برای کاربران Linux فراهم می‌کند. این برنامه‌های کاربردی عبارتند از:

- Microsoft Word 97/2000*
- Microsoft Excel 97/2000*
- Microsoft Outlook 97/2000
- Microsoft PowerPoint 97/2000*
- Microsoft Visio 2000
- Microsoft Internet Explorer 5.0/5.5
- Intuit Quicken 2002
- Lotus Notes R5

طبق ادعای شرکت توسعه دهنده این نرم‌افزار یعنی CodeWeavers، عملکرد برنامه‌هایی که در لیست مذکور با علامت ستاره مشخص شده‌اند در هر دو سیستم‌عامل ویندوز و Linux کاملاً یکسان است. در حالی که سایر برنامه‌ها ممکن است دارای اشکالات قابل توجهی باشند. برای اطلاع بیشتر در این زمینه به وب سایت شرکت CodeWeavers در آدرس http://www.codeweavers.com مراجعه کنید.

نرم‌افزار GNOME Office

نرم‌افزار GNOME Office نیز مشابه نرم‌افزار OpenOffice حاوی مجموعه‌ای از برنامه‌های کاربردی است. با وجودی که توسعه این برنامه‌های کاربردی به طور کاملاً مستقل انجام شده است، امروزه تمام آن‌ها در قالب نرم‌افزار GNOME Office توزیع می‌شوند. برنامه‌های کاربردی مزبور توسط برنامه‌نویسان پروژه GNOME توسعه داده شده‌اند. جدول ۱۰-۱۸ کاربرد این برنامه‌ها را به اختصار شرح می‌دهد.

در این قسمت تمام برنامه‌های ذکر شده در جدول فوق را توضیح نمی‌دهیم. برای مثال، دو برنامه Galeon و Evolution را در فصل شانزدهم مورد بررسی قرار دادیم، اما برنامه GIMP را در همین فصل توضیح خواهیم داد. ضمناً تمام این برنامه‌ها به همراه سیستم‌عامل Red Hat Linux توزیع نمی‌شوند. برای نمونه، برنامه Agnubis هم‌چنان در حال توسعه و پیشرفت بوده و از این‌رو هنوز در قالب RPM توزیع نشده است.

جدول ۱۰-۱۸ شرح مختصری درباره کاربرد برنامه‌های موجود در نرم‌افزار GNOME Office

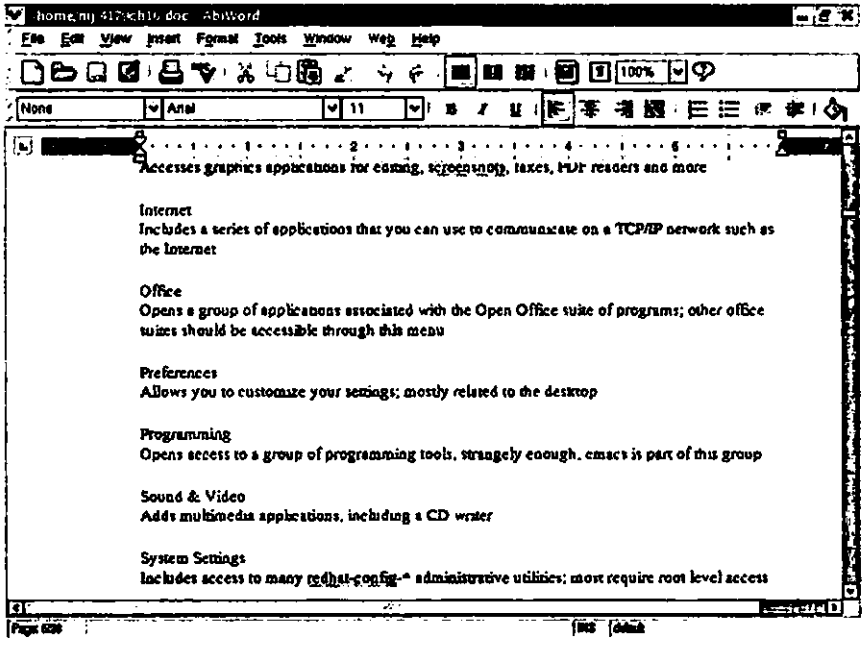
عنوان برنامه کاربردی	توضیح
AbiWord	این برنامه یک واژه‌پرداز است.
Agnubis	این برنامه ابزاری برای قالب بندی محتوا به منظور نمایش اسلاید است و از آن‌جا که بسته نرم‌افزاری آن در قالب RPM در دسترس نیست، به همراه سیستم‌عامل Red Hat Linux توزیع نمی‌شود.
Balsa	این برنامه ابزاری برای مدیریت پیغام‌های الکترونیکی است.
Dia	این برنامه ابزاری برای رسم نمودار است.
Evolution	این برنامه ابزاری برای مدیریت اطلاعات شخصی است.
Galeon	این برنامه یک مرورگر وب است.
GIMP	این برنامه ابزاری برای ویرایش تصاویر است.
GnuCash	این برنامه ابزاری برای مدیریت مالی شخصی است.
Gnumeric	این برنامه یک صفحه گسترده است.
Guppi	این برنامه ابزاری برای چاپ نمودار است و با برنامه Gnumeric نیز تعامل نزدیکی دارد.
MrProject	این برنامه ابزاری برای مدیریت پروژه است.
Sketch	این برنامه ابزاری برای ترسیم نمودارهای vector است و به همراه سیستم‌عامل Red Hat Linux توزیع نمی‌شود.
Sodipodi	این برنامه ابزاری برای ترسیم نمودارهای vector است و به همراه سیستم‌عامل Red Hat Linux توزیع نمی‌شود.
Toutdoux	این برنامه ابزاری برای مدیریت پروژه است و به همراه سیستم‌عامل Red Hat Linux توزیع نمی‌شود.

تا زمان انتشار کتاب حاضر، طبق اظهارات مندرج در وب سایت رسمی پروژه GNOME Office به آدرس http://www.gnome.org/gnome-office تمام برنامه‌های کاربردی نرم‌افزار OpenOffice در بسته قالب نرم‌افزاری GNOME Office توزیع خواهند شد. با وجود این، کار توسعه برنامه‌های کاربردی موجود در این بسته نرم‌افزاری هم‌چنین ادامه خواهد داشت.

تعدادی از برنامه‌های کاربردی نرم‌افزار GNOME Office هنوز مراحل آزمایشی خود را طی می‌کنند و از این‌رو، استفاده از آن‌ها به عنوان یک محصول نرم‌افزاری قابل اطمینان امکان پذیر نیست. برای اطلاع بیشتر درباره این موضوع گزینه About از منوی Help برنامه کاربردی موردنظر را انتخاب کنید. عموماً نگارش شماره 1.0 برنامه‌ها (و نگارش‌های بالاتر) به عنوان محصولات نرم‌افزاری قابل استفاده توزیع می‌شوند، اما این موضوع به معنی عدم وجود اشکال در این برنامه‌ها نیست. فراموش نکنید که کار توسعه و نگهداری بیشتر این برنامه‌ها توسط کاربران داوطلب انجام می‌شود و حتی پس از توزیع نگارش شماره 1.0 نیز کار توسعه آن‌ها هم‌چنان ادامه می‌یابد.

برنامه AbiWord

این برنامه به عنوان یک واژه پرداز قادر است اسنادی با قالب‌های مختلف را مورد پردازش قرار دهد. قابلیت‌های برنامه AbiWord برای بیشتر کاربردها مناسب است. با وجود این، پشتیبانی آن از اسناد تولید شده توسط برنامه Microsoft Word به خوبی برنامه OpenOffice Writer نیست. برای مثال، شکل ۵-۱۸ بخش‌هایی از یک سند Microsoft Word را که قالب جدولی دارد در پنجره این برنامه نشان می‌دهد.



شکل ۵-۱۸ سندی از نوع Microsoft Word که در برنامه AbiWord باز شده است.

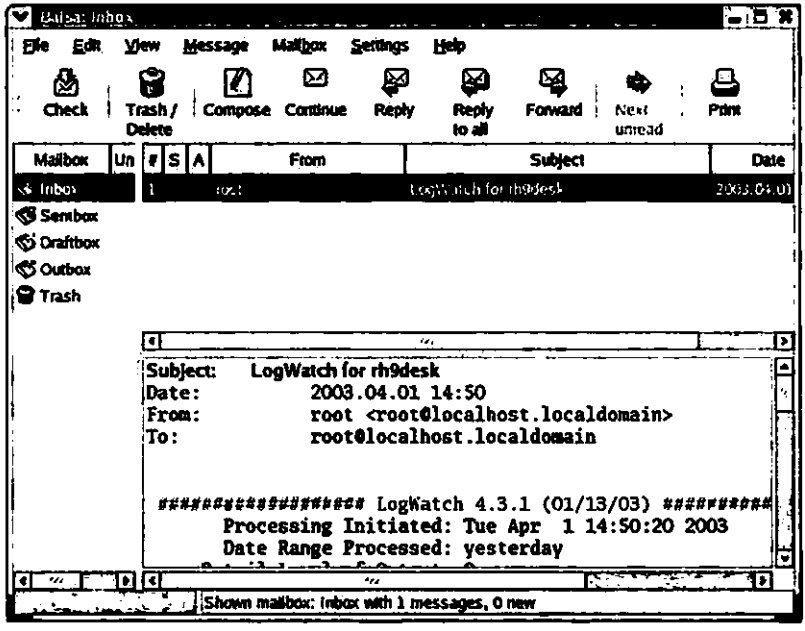
برخلاف بیشتر برنامه‌های کاربردی نرم‌افزار OpenOffice، دسترسی به برنامه AbiWord از طریق منوی فرعی More Office Applications واقع در منوی فرعی Office از منوی اصلی امکان‌پذیر است. البته با اجرای مستقیم فرمان abiword از سطر فرمان محیط گرافیکی مورد استفاده نیز می‌توان این برنامه را اجرا کرد. جدول ۱۱-۱۸ فایل‌های قابل پردازش توسط واژه پرداز AbiWord را به اختصار شرح می‌دهد.

جدول ۱۱-۱۸ فایل‌های قابل پردازش توسط برنامه AbiWord

شاخص فایل	توضیح
.abi	این شاخص بیانگر فایل‌های تولید شده توسط واژه پرداز AbiWord است.
.aw	این شاخص بیانگر فایل‌های Applix Words است.
.awt	این شاخص بیانگر الگوهای مورد استفاده در واژه‌پرداز AbiWord است.
.dbk	این شاخص بیانگر فایل‌های DocBook است.
.doc	این شاخص بیانگر فایل‌های Microsoft Word است.
.fo	این شاخص بیانگر فایل‌های Extensible Stylesheet Language است.
.html, .htm	این شاخص‌ها بیانگر فایل‌های Hypertext Markup Language است.
.xhtml	این شاخص بیانگر فایل‌های Extensible Hypertext Markup Language است.
.isc, iscii	این شاخص‌ها بیانگر فایل‌های Indian Script Code for Information Interchange است.
.kwd	این شاخص بیانگر فایل‌های تولید شده توسط برنامه KOffice Word یا به اختصار Kword است.
.latex	این شاخص بیانگر فایل‌های تولید شده توسط برنامه Lamport TeX یا به اختصار LaTeX است که به منظور قالب بندی اسناد متن مورد استفاده قرار می‌گیرد.
.pdb	این شاخص بیانگر فایل‌های PalmDoc است.
.psitext, .psiword	این شاخص‌ها بیانگر اسناد مورد استفاده در کامپیوترهای دستی هستند.
.rtf	این شاخص بیانگر فایل‌های Rich Text Format ای به اختصار RTF است.
.txt, .text	این شاخص‌ها بیانگر فایل‌های متنی یا فایل‌های متنی رمزگذاری شده هستند.
.nws	این شاخص بیانگر فایل‌های متنی مورد استفاده در گروه‌های خبری است.
.wml	این شاخص بیانگر فایل‌های Wireless Markup Language است.

برنامه Balsa

این برنامه ابزاری برای مدیریت پیغام‌های الکترونیکی است. به مانند برنامه‌های مشابه که در فصل شانزدهم و هفدهم مورد بررسی واقع شد، این برنامه امکانات لازم به منظور ارسال و دریافت پیغام‌های الکترونیکی ارسالی و سازمان‌دهی آن‌ها در اختیار می‌گذارد. شکل ۶-۱۸ پنجره این برنامه را در حال نمایش متن پیغامی که برای کاربر اصلی (اصطلاحاً root) ارسال شده است نشان می‌دهد.



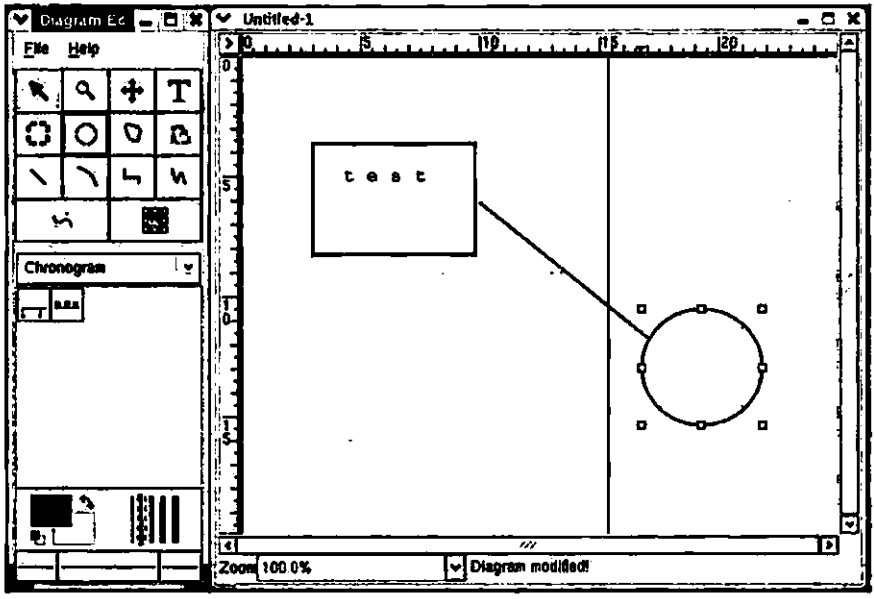
شکل ۶-۱۸ پنجره برنامه Balsa

دسترسی به برنامه Balsa با انتخاب گزینه مربوطه از منوی فرعی More Internet Applications واقع در منوی فرعی Internet از منوی اصلی یا با اجرای مستقیم فرمان balsa در سطر فرمان محیط گرافیکی مورد استفاده امکان‌پذیر است.

پس از اجرای این برنامه برای نخستین بار، تنظیمات مربوط به پیکربندی ارسال و دریافت پیغام‌های الکترونیکی به نمایش درمی‌آید. این تنظیمات را می‌توان در مواقع لزوم با انتخاب گزینه مربوطه از منوی Settings انجام داد. تخصیص یک شناسه به هر کدام از حساب‌ها کاربری الزامی است.

برنامه Dia

این برنامه ابزاری برای رسم و ویرایش نمودارهاست. شکل ۷-۱۸ پنجره این برنامه را در حال رسم یا ویرایش یک نمودار ساده نشان می‌دهد.



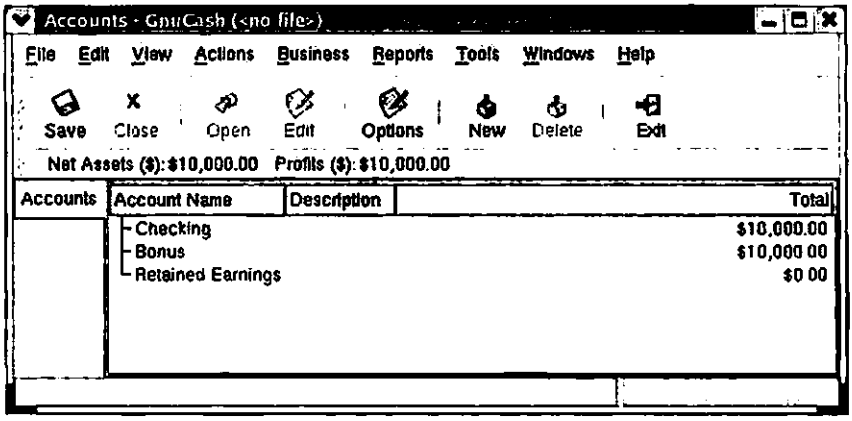
شکل ۷-۱۸ پنجره برنامه Dia

چنان‌که در این شکل مشاهده می‌کنید، امکانات مختلفی به منظور رسم اشکال مختلف، مشابه آن‌چه در برنامه Microsoft Visio وجود دارد، پیش‌بینی شده است.

برنامه GnuCash

این برنامه ابزاری برای مدیریت اطلاعات مالی است که به منظور کاربردهای شخصی طراحی شده است. برنامه GnuCash دارای قابلیت کار با فایل‌های تولید شده توسط برنامه Quicken است. شکل ۸-۱۸ پنجره این برنامه را نشان می‌دهد.

برای دسترسی به برنامه، کافی است گزینه GnuCash را از منوی فرعی More Office Applications واقع در منوی فرعی Office از منوی اصلی انتخاب کرده یا این‌که فرمان gnucash را مستقیماً در سطر فرمان محیط گرافیکی مورد استفاده اجرا کنید.



شکل ۸-۱۸ پنجره برنامه GnuCash

پس از اجرای برنامه GnuCash برای نخستین بار، اعلان مربوط به تعریف حساب کاربری جدید جهت مدیریت موجودی، درآمدها، بدهی‌ها و هزینه‌ها به نمایش درمی‌آید. این برنامه حتی امکان پردازش فایل‌های تولید شده توسط برنامه Quicken 2002 را نیز در اختیار می‌گذارد.

برنامه Gnumeric

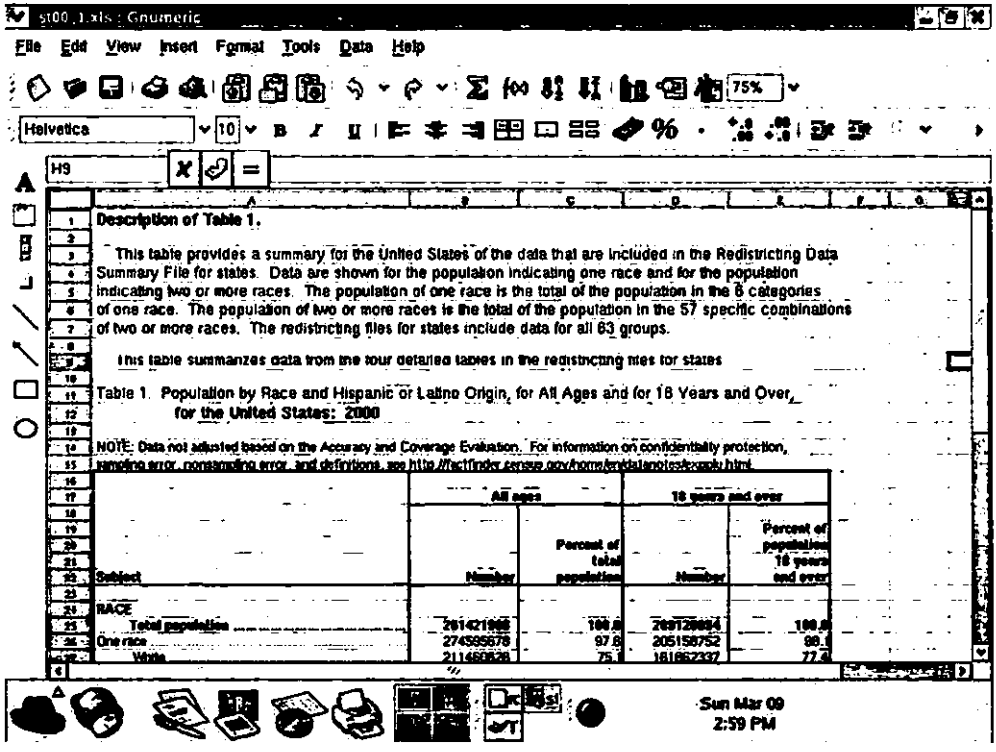
این برنامه یک صفحه گسترده است. شکل ۹-۱۸ پنجره این برنامه را نشان می‌دهد.

برای دسترسی به برنامه Gnumeric کافی است گزینه مربوطه را از منوی فرعی More Office Applications واقع در منوی فرعی Office از منوی اصلی انتخاب کرده یا این‌که فرمان gnumeric را مستقیماً در سطر فرمان محیط گرافیکی مورد استفاده اجرا کنید. جدول ۱۲-۱۸ فایل‌های قابل پردازش توسط این برنامه را به اختصار شرح می‌دهد.

جدول ۱۲-۱۸ فایل‌های قابل پردازش توسط برنامه GnuCash

شاخص فایل	توضیح
.dif	این شاخص بیانگر فایل‌های Data Interchange Format است.
.div	این شاخص بیانگر فایل‌های تولید شده توسط پردازشگر متنی groff است.
.gnumeric	این شاخص بیانگر قالب پیش‌فرض فایل‌های XML در برنامه Gnumeric است.
.tex	این شاخص بیانگر فایل‌های LaTex 2e است.
.xls	این شاخص بیانگر فایل‌های Microsoft Excel است.

شاخص فایل	توضیح
.csv	این شاخص بیانگر فایل‌های متنی CSV است. (اطلاعات مندرج در این گونه فایل‌ها با علامت کاما از یکدیگر جدا می‌شوند.)
.me	این شاخص بیانگر فایل‌های تولید شده توسط پردازشگر متنی Troff است.



شکل ۹-۱۸ پنجره برنامه Gnumeric

یکی از قابلیت‌های صفحات گسترده امکان چاپ نمودار است. برنامه Guppi چنین امکانی را در اختیار برنامه Gnumeric قرار می‌دهد. برای اطلاع بیشتر درباره قابلیت‌های برنامه Guppi به وب سایت مربوطه در آدرس http://www.gnome.org/projects/guppi/ مراجعه کنید. یکی از صفحات این وب سایت به آدرس http://www.gnome.org/projects/guppi/otherprogs.shtml شامل معرفی برنامه‌های مشابه در این زمینه است.

برنامه MrProject

این‌برنامه ابزاری برای‌مدیریت‌پروژه است. برای دسترسی به‌آن، کافی است گزینهProject Management را از منوی فرعی Office واقع در منوی اصلی انتخاب کرده یا این‌که فرمان mrproject را مستقیماً در سطر فرمان محیط گرافیکی مورد استفاده اجرا کنید. این برنامه شامل تمام ابزارهای استاندارد برای مدیریت پروژه، از جمله لیست منابع، ابزار رسم نمودار گانت و لیست وظایف است. با وجود این، در حال حاضر هیچ امکانی را به منظور پردازش فایل‌های تولید شده توسط برنامه‌های مشابه هم‌چون Microsoft Project در اختیار قرار نمی‌دهد.

نرم‌افزار KOffice

نرم‌افزار KOffice یکی از سه نرم‌افزار کد باز مطرح در زمینه برنامه‌های اداری است که در قالب پروژه KDE توسعه یافته است. با وجودی که برنامه‌های کاربردی موجود در نرم‌افزار KOffice به طور خاص برای استفاده در محیط گرافیکی KDE طراحی شده‌اند، برخی از آن‌ها را می‌توان در محیط گرافیکی GNOME نیز اجرا کرد. دسترسی به برنامه‌های کاربردی مورد بحث از طریق منوی فرعی More Office Applications واقع در منوی فرعی Office از منوی اصلی امکان‌پذیر است.

منوی اصلی محیط گرافیکی GNOME کاربرد مشابهی با منوی اصلی محیط گرافیکی KDE دارد. در سیستم‌عامل Red Hat Linux هر دو منو با کلیک روی آیکن کلاه قرمز مستقر در گوشه پایین سمت چپ صفحه قابل دستیابی است.

نرم‌افزار KOffice متشکل از چندین برنامه کاربردی است که بیشتر آن‌ها به عنوان بخشی از یک نرم‌افزار بزرگ طراحی شده‌اند. جدول ۱۳-۱۸ هریک از این برنامه‌ها را به اختصار شرح می‌دهد.

برای نصب بسته نرم‌افزاری KDE از ابزار redhat-config-packages که قبلاً در فصل نوزدهم توضیح داده شد، استفاده کنید. پس از نصب این بسته نرم‌افزاری، با استفاده از ابزار switchdesk می‌توانید آن‌را به عنوان محیط گرافیکی پیش‌فرض پیکربندی کنید. برای اطلاع بیشتر در این زمینه به فصل پانزدهم مراجعه کنید.

جدول ۱۳-۱۸ شرح برنامه‌های کاربردی نرم‌افزار KOffice

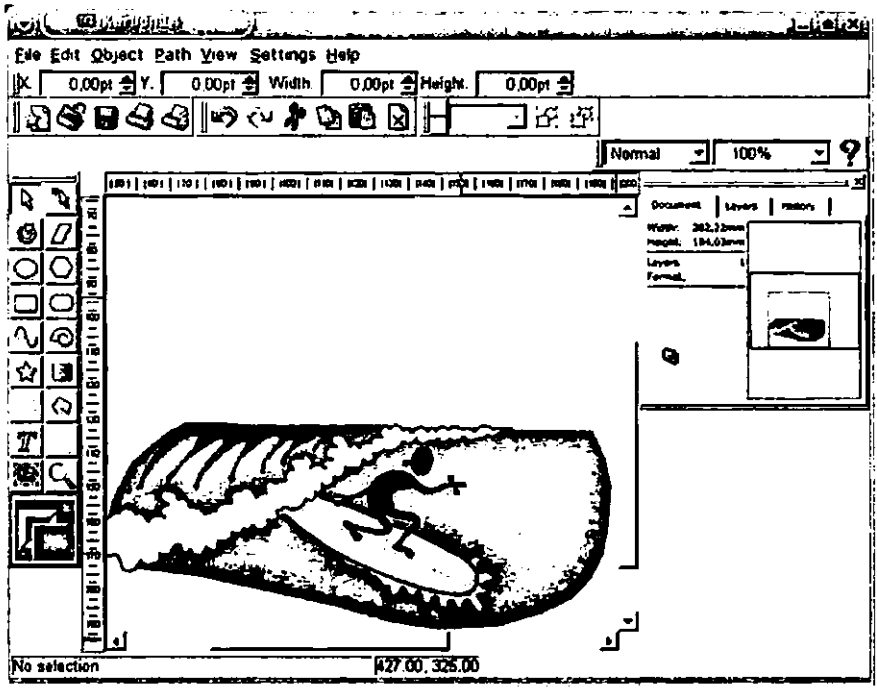
عنوان برنامه کاربردی	توضیح
Karbon14	این برنامه کاربردی امکان رسم خطوط و شکل‌های مختلف را در اختیار می‌گذارد.
KChart	این برنامه کاربردی امکان رسم نمودار را در اختیار می‌گذارد.
KFormula	این برنامه کاربردی امکان قالب‌بندی و ویرایش فرمول‌های ریاضی را در اختیار می‌گذارد.
Kivio	این برنامه کاربردی امکان رسم و ویرایش نمودارها را در اختیار می‌گذارد.
KOffice Workspace	این برنامه رابطی برای دسترسی به‌سایر برنامه‌های کاربردی نرم‌افزار KOffice است.
Kontour	این برنامه کاربردی امکان ترسیم خطوط و شکل‌های مختلف را در اختیار می‌گذارد. عملکرد آن شبیه به برنامه Karbon14 است.
KPresenter	این برنامه کاربردی، ابزاری برای تهیه اسلاید است.
KSpread	این برنامه کاربردی، یک صفحه گسترده است.
KThesaurus	این برنامه کاربردی، نوعی فرهنگ لغات است.
Kugar	این برنامه کاربردی امکان تهیه گزارش‌های تجاری را در اختیار می‌گذارد.
KWord	این برنامه کاربردی یک واژه‌پرداز است.

برخی از برنامه‌های کاربردی نرم‌افزار Koffice هنوز مراحل آزمایشی خود را طی می‌کنند. برای اطلاع از این موضوع گزینه About را از منوی Help برنامه کاربردی موردنظر انتخاب کنید. عموماً نگارش شماره 1.0 برنامه‌ها (و نگارش‌های بالاتر) به عنوان محصولات نرم‌افزاری قابل استفاده توزیع می‌شوند، اما این موضوع به معنی عدم وجود اشکال در این برنامه‌ها نیست. فراموش نکنید که کار توسعه و نگهداری بیشتر این برنامه‌ها توسط کاربران داوطلب انجام می‌شود و حتی پس از توزیع نگارش شماره 1.0 نیز کار توسعه آن‌ها هم‌چنان ادامه می‌یابد.

برنامه Karbon14

این برنامه ابزاری برای ترسیم خطوط و شکل‌های مختلف است. برای دسترسی به آن، کافی است گزینه Karbon14 راازمنوی‌فرعی More Office Applications واقع‌درمنوی‌فرعی Office ازمنوی‌اصلی انتخاب کرده یا این‌که مستقیماً فرمان karbon را در سطر فرمان محیط گرافیکی مورد استفاده اجرا کنید.

تا زمان انتشار کتاب حاضر، آخرین نسخه این برنامه تحت عنوان Karbon14 0.001 به همراه سیستم‌عامل Red Hat Linux توزیع شده است. از این‌رو، کاملاً واضح است که برنامه مزبور هنوز در مراحل آزمایشی بوده و آماده بهره‌بردرای حرفه‌ای نیست. با وجود این، چنان‌که شکل ۱۰-۱۸ نشان می‌دهد، می‌توان عملکرد آن‌را تجربه کرد. با ارتقای بسته نرم‌افزاری koffice-* همواره می‌توانید به جدیدترین نسخه این برنامه دسترسی پیدا کنید.

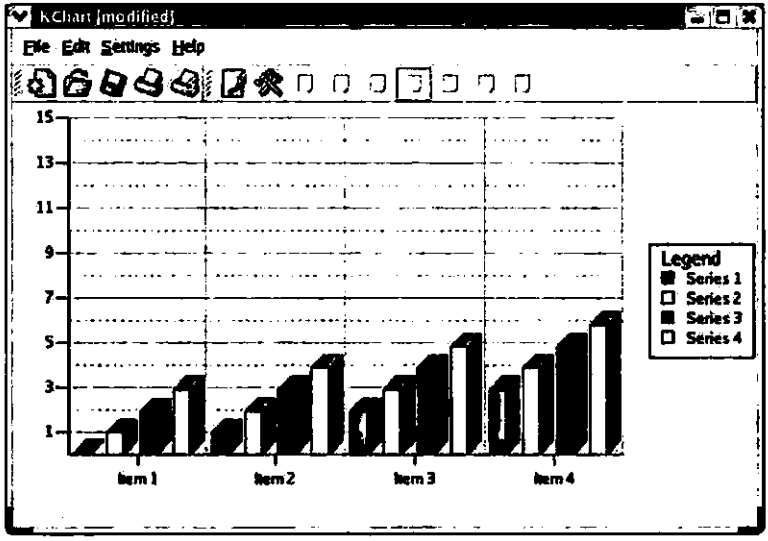


شکل ۱۰-۱۸ پنجره برنامه Karbon14

برنامه KChart

این برنامه ابزاری برای رسم نمودار است و اغلب به همراه برنامه کاربردی KSpread مورد استفاده قرار می‌گیرد. برای دسترسی به برنامه KChart کافی است گزینه مربوطه را از منوی فرعی More Office Applications واقع در منوی فرعی Office از منوی اصلی انتخاب کرده یا این‌که مستقیماً فرمان kchart را در سطر فرمان محیط گرافیکی مورد استفاده اجرا کنید.

برنامه مورد بحث قادر است نمودارها را در قالب میله‌ای، مدور، منحنی و به صورت رنگی نمایش دهد. شکل ۱۱-۱۸ پنجره این برنامه را در حال نمایش یک نمودار میله‌ای نشان می‌دهد.



شکل ۱۱-۱۸ پنجره برنامه KChart

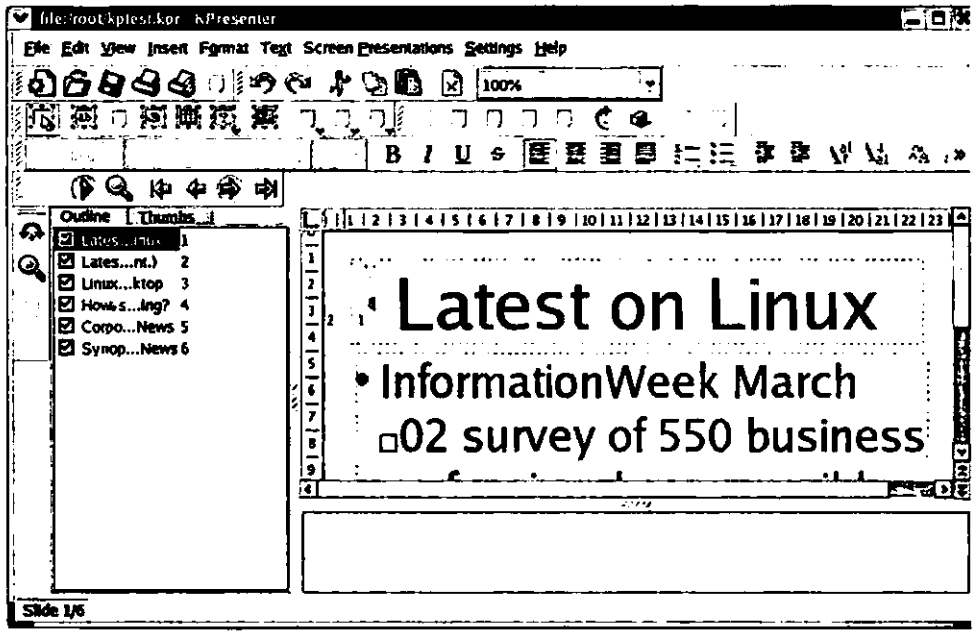
برنامه Kivio

این برنامه ابزاری برای رسم و ویرایش نمودار است، به طوری که می‌توان قابلیت‌های آن‌را با دو برنامه GNOME Dia و Microsoft Visio مقایسه کرد. برای دسترسی به این برنامه کافی است گزینه Kivio را از منوی فرعی More Office Applications واقع در منوی فرعی Office از منوی اصلی انتخاب کرده یا مستقیماً فرمان kivio را در سطر فرمان محیط گرافیکی مورد استفاده اجرا کنید.

برنامه KPresenter

این برنامه ابزاری برای تهیه اسلاید است. این گونه برنامه‌ها در اصل نوعی واژه پرداز به خصوص با قابلیت‌های گرافیکی هستند. معمولاً نمایش اسلاید با هدف ارایه مطالب موردنظر به صورت online یا برای مخاطبینی که در یک اتاق یا سالن اجتماعات گرد هم آمده‌اند، انجام می‌شود. دسترسی به برنامه مورد بحث با انتخاب گزینه KPresent از منوی فرعی More Office Applications واقع در منوی فرعی Office از منوی اصلی یا با اجرای مستقیم فرمان kpresenter در سطر فرمان محیط گرافیکی مورد استفاده امکان‌پذیر است.

برنامه KPresenter امکان ایجاد اسلاید نمایش را مانند برنامه‌هایی چون Microsoft PowerPoint و StarOffice Impress در اختیار می‌گذارد. شکل ۱۲-۱۸ پنجره این برنامه را در حال ویرایش سندی که توسط برنامه Microsoft PowerPoint تولید شده است، نشان می‌دهد.



شکل ۱۲-۱۸ پنجره برنامه KPresenter

چنان‌که مشاهده می‌کنید، این برنامه دارای نوار ابزارهای متنوعی است که امکانات مختلفی نظیر کنترل رنگ، رسم خطوط و شکل‌های مورد نظر، مدیریت متن، درج عناصر جدید و مانند آن‌را در اختیار می‌گذارد. شرح مختصری راجع به کاربرد این نوار ابزارها در جدول ۱۴-۱۸ آمده است.

جدول ۱۴-۱۸ شرح کاربرد نوار ابزارهای برنامه KPresenter

عنوان نوار ابزار	توضیح
Edit	این نوار ابزار امکان ویرایش سند و بزرگ‌نمایی آن‌را در اختیار می‌گذارد.
File	این نوار ابزار امکان باز کردن فایل جدید، چاپ محتوا و نمایش اسلاید را در اختیار می‌گذارد.
Format	این نوار ابزار امکان قالب بندی خطوط و شکل‌های مندرج در سند را فراهم می‌کند.
Insert	این نوار ابزار امکان درج عناصری چون متن، جداول، تصاویر، خطوط و مانند آن‌را در اختیار می‌گذارد.
Presentation	این نوار ابزار امکان مدیریت و سازمان‌دهی اسلایدها را در اختیار می‌گذارد.
Text	این نوار ابزار امکان مدیریت متون را در اختیار می‌گذارد.

عنوان نوار ابزار	توضیح
Tools	این نوار ابزار امکانات مختلفی نظیر بزرگنمایی و چرخش عناصر مندرج در سند را فراهم می‌کند.

برای تهیه یک سند جدید در این برنامه می‌توانید از الگوهای پیش‌ساخته یا اسناد موجود استفاده کرده یا این‌که سند موردنظر خود را بدون استفاده آن‌ها تهیه کنید.

توانایی برنامه KPresenter در ویرایش فایل‌ها محدود به فایل‌های XML، Microsoft PowerPoint و فایل‌های تولید شده توسط همین برنامه است. اما در عین حال قادر است اسناد نهایی را برای نمایش در برنامه KWord و هم‌چنین به صورت HTML و RTF قالب‌بندی کند.

برنامه KSpread

این برنامه یک صفحه گسترده است. این گونه برنامه‌ها امکانات انجام محاسبات متنوعی را روی مجموعه‌ای از داده‌ها در اختیار می‌گذارند. برنامه‌های مزبور اغلب در تحلیل آماری، مدل‌سازی تجاری و برنامه‌ریزی مورد استفاده قرار می‌گیرند.

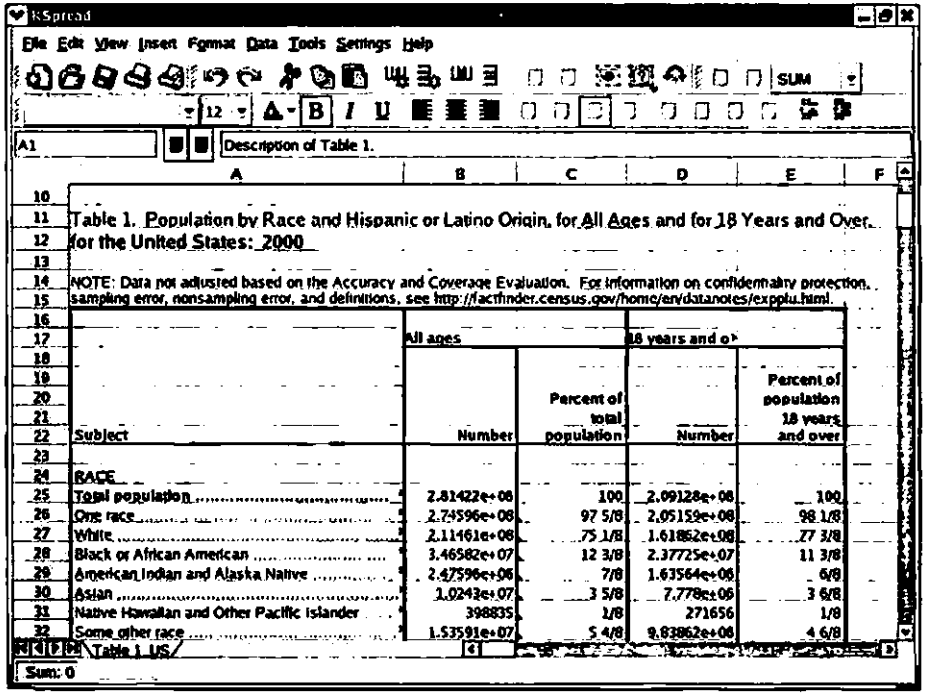
برای دستیابی به این برنامه کافی است گزینه KSpread را از منوی فرعی More Office Applications واقع در منوی فرعی Office از منوی اصلی انتخاب کرده یا این‌که مستقیماً فرمان kspread را در سطر فرمان محیط گرافیکی مورد استفاده اجرا کنید. شکل ۱۳-۱۸ پنجره این برنامه را در حال نمایش بخشی از نتایج سرشماری سال ۲۰۰۰ در ایالات متحده نشان می‌دهد.

چنان‌که مشاهده می‌کنید، برنامه KSpread از تمامی مشخصات یک صفحه گسترده استاندارد برخوردار است. امکانات این برنامه از طریق نوار ابزارهای مختلفی قابل دستیابی است. جدول ۱۵-۱۸ کاربرد این نوار ابزارها را به اختصار شرح می‌دهد.

جدول ۱۵-۱۸ شرح کاربرد نوار ابزارهای برنامه KSpread

عنوان نوار ابزار	توضیح
Color/Border	این نوار ابزار امکاناتی را به منظور پیکربندی خانه‌های جدول و حاشیه آن‌را در اختیار می‌گذارد.
Edit	این نوار ابزار امکاناتی را به منظور ویرایش و مرتب‌سازی داده‌ها و هم‌چنین رسم نمودار را در اختیار می‌گذارد.
File	این نوار ابزار امکان دسترسی به فایل موردنظر و چاپ محتوای آن‌را در اختیار می‌گذارد.

عنوان نوار ابزار	توضیح
Format	این نوار ابزار امکان قالب‌بندی متون و اعداد مندرج در خانه‌های جدول را فراهم می‌کند.
Math	این نوار ابزار امکان پیکربندی فرمول‌های ریاضی هریک از خانه‌های جدول را در اختیار می‌گذارد.



شکل ۱۳-۱۸ پنجره برنامه KSpread

علاوه بر این، برنامه KSpread قادر است فایل‌های مختلفی شامل فایل‌های تولید شده توسط سایر صفحات گسترده، از جمله Microsoft Excel، Applix، Gnumeric، Quattro Pro و هم‌چنین فایل‌های CSV را مورد پردازش قرار دهد. جدول ۱۶-۱۸ فایل‌های قابل پردازش توسط این برنامه را به اختصار شرح می‌دهد.

جدول ۱۶-۱۸ شرح مختصر فایل‌های قابل پردازش توسط برنامه KSpread

شاخص فایل	توضیح
.asa	این شاخص بیانگر فایل‌های تولید شده توسط برنامه Applix است.
.csv	این شاخص بیانگر فایل‌های CSV است.
.gnumeric	این شاخص بیانگر فایل‌های تولید شده توسط برنامه Gnumeric است.
.html	این شاخص بیانگر فایل‌های HTML (صفحات وب) است.
..ksp	این شاخص بیانگر فایل‌های تولید شده توسط برنامه KSpread است.
.wb2	این شاخص بیانگر فایل‌های تولید شده توسط برنامه Quattro Pro است.
.xls	این شاخص بیانگر فایل‌های تولید شده توسط برنامهMicrosoft Excel 97/2000/XP/95/5.0 است.

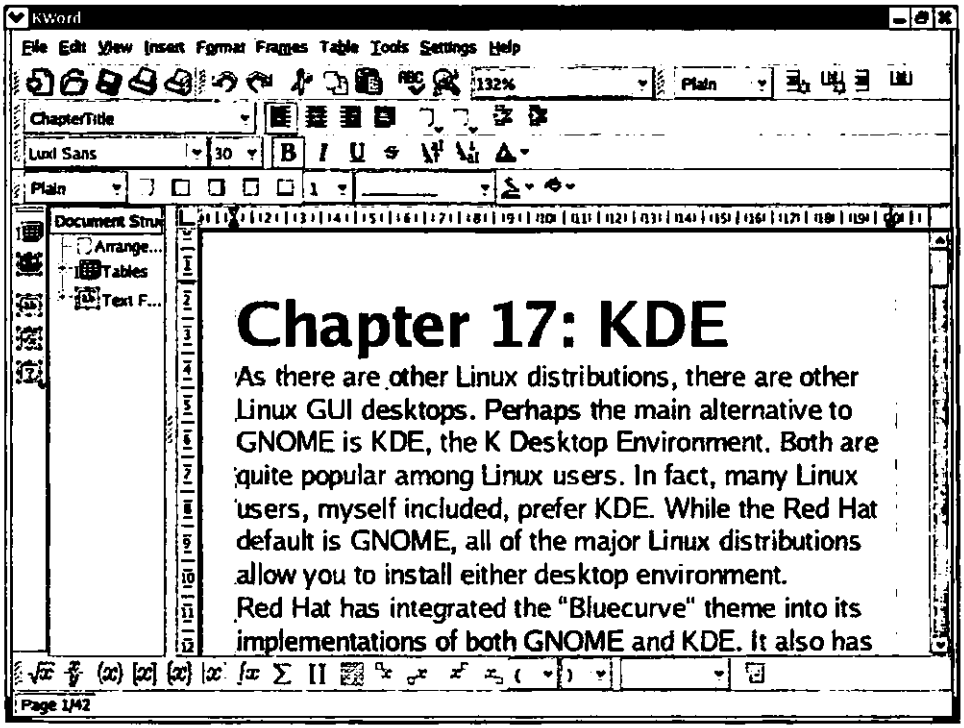
برنامه KWord

یکی از مشکلات پردازش اسناد در دنیای کامپیوترها وجود قالب‌های بسیار متنوع است. به عنوان مثال، تبدیل قالب اسناد تولید شده توسط برنامه Microsoft Word به قالب اسنادی که برنامه Corel WordPerfect یا AbiWord تولید می‌کند، مستلزم انجام فرآیندی برای ترجمه این اسناد است. البته بیشتر برنامه‌های واژه‌پرداز، از جمله برنامه KWord دارای این قابلیت هستند. با وجود این، برخی از برنامه‌ها این کار را به درستی انجام نمی‌دهند.

برنامه KWord بخشی از انتظاراتی را که کاربران مختلف از یک واژه‌پرداز دارند، به درستی برآورده نمی‌کند. با این همه، برنامه مذکور برای بیشتر کاربردهای تجاری و مانند آن به اندازه کافی مناسب است. امکانات این برنامه تقریباً شامل تمام مواردی است که در واژه‌پرداز Microsoft Word وجود دارد.

برای دسترسی به برنامه KWord کافی است گزینه‌مربوطه را ازمنوی‌فرعیMore Office Applications واقع در منوی فرعی Office از منوی اصلی انتخاب کرده یا مستقیماً فرمان kword را در سطر فرمان محیط گرافیکی مورد استفاده اجرا کنید شکل ۱۴-۱۸ پنجره این برنامه را در حال نمایش محتوای سندی از نوع Microsoft Word نشان می‌دهد.

چنان‌که مشاهده می‌کنید، برنامه KWord دارای پنج نوار ابزار پیش‌فرض با عناوین File، Edit، Insert، Paragraph و Format است. قابلیت‌های برنامه مذکور جمعاً در هشت نوار ابزار مختلف قالب‌بندی شده است. جدول ۱۷-۱۸ کاربرد هر یک از این نوار ابزارها را به اختصار شرح می‌دهد.



شکل ۱۴-۱۸ پنجره برنامه KWord

جدول ۱۷-۱۸ شرح مختصر کاربرد نوار ابزارهای برنامه KWord

عنوان نوار ابزار	توضیح
Borders	این نوار ابزار امکان پیکربندی حاشیه‌ها را در اختیار می‌گذارد.
Edit	این نوار ابزار امکان ویرایش، بزرگ‌نمایی و تغییر اندازه سند را در اختیار می‌گذارد
File	این نوار ابزار امکان دسترسی به فایل موردنظر و چاپ آن‌را در اختیار می‌گذارد.
Format	این نوار ابزار امکان امکان قالب‌بندی متن و ویرایش رنگ‌های مورد استفاده را در اختیار می‌گذارد.
Formula	این نوار ابزار امکان امکان قالب‌بندی فرمول‌های ریاضی را در اختیار می‌گذارد.
Insert	این نوار ابزار امکان درج جداول، تصاویر و سایر عناصر را در اختیار می‌گذارد.
Paragraph	این نوار ابزار امکان قالب‌بندی پاراگراف‌ها، ترازبندی و هم‌چنین نشانه‌های bullet را در اختیار می‌گذارد.
Table	این نوار ابزار امکان پیکربندی جداول را در اختیار می‌گذارد.

علاوه بر این، برنامه KWord از قابلیت پردازش فایل‌های تولید شده توسط سایر واژه پردازها نیز برخوردار است. جدول ۱۸-۱۸ این فایل‌ها را به اختصار شرح می‌دهد.

جدول ۱۸-۱۸ شرح مختصر فایل‌های قابل پردازش توسط برنامه KWord

شاخص فایل	توضیح
.kwd	این شاخص بیانگر فایل‌های تولید شده در واژه‌پرداز KWord است.
.doc	این شاخص بیانگر فایل‌های تولید شده در واژه‌پرداز Microsoft Word است.
.html	این شاخص بیانگر فایل‌های HTML (صفحات وب) است.
.rtf	این شاخص بیانگر فایل‌های Rich Text Format یا به اختصار RTF است. این نوع فایل یک قالب استاندارد قابل قبول توسط بیشتر واژه پردازها محسوب می‌شود.
.sam	این شاخص بیانگر فایل‌های تولید شده در برنامه AmiPro است.
.tex	این شاخص بیانگر فایل‌های TeX است.
.txt	این شاخص بیانگر فایل‌های متنی است.
.wpd	این شاخص بیانگر فایل‌های تولید شده در واژه پرداز WordPerfect است.

سایر برنامه‌های کاربردی نرم‌افزار KOffice

دسترسی به سایر برنامه‌های کاربردی نرم‌افزار KOffice از طریق منوی فرعی More Office Applications واقع در منوی فرعی Office از منوی اصلی امکان‌پذیر است. به توضیح مختصری درباره این برنامه‌ها توجه کنید:

- **برنامه KFormula**: این برنامه ابزاری برای قالب بندی فرمول‌های پیچیده است. این قابلیت از طریق دسترسی به توابع مثلثاتی و لگاریتمی، انتگرال، حد و مانند آن فراهم شده است. از این‌رو، توانایی آن‌را می‌توان با برنامه OpenOffice Math مقایسه کرد. دسترس به این برنامه با اجرای مستقیم فرمان kformula از سطر فرمان محیط گرافیکی مورد استفاده امکان‌پذیر است.
- **برنامه KOffice Workspace**: این برنامه رابطی برای دسترسی به سایر برنامه‌های کاربردی نرم‌افزار KOffice است. برای دسترسی به این برنامه، کافی است فرمان koshell را مستقیماً در سطر فرمان محیط گرافیکی مورد استفاده اجرا کنید.
- **برنامه Kontour**: این برنامه ابزاری برای کار با تصاویر گرافیکی است. نتیجه اسکن تصاویر را می‌توان مستقیماً از اسکنر به این برنامه ارسال کرد. دسترسی به آن با اجرای مستقیم فرمان

kontour در سطر فرمان محیط گرافیکی مورد استفاده امکان‌پذیر است.

- **برنامه KThesaurus**: این برنامه نوعی فرهنگ لغات است که امکان مقایسه واژه‌ها را در سه زمینه مختلف، شامل گروه مترادف‌ها، واژه‌های عمومی (اصطلاحاً hypernyms) و واژه‌های تخصصی (اصطلاحاً hyponyms) در اختیار می‌گذارد. دسترسی به این برنامه با اجرای مستقیم فرمان kthesaurus در سطر فرمان محیط گرافیکی مورد استفاده امکان‌پذیر است.
- **برنامه Kugar**: این برنامه ابزاری برای مدیریت گزارش‌هاست و اغلب به همراه برنامه دیگری با عنوان Kugar Designer که ابزاری برای تهیه گزارش است، مورد استفاده قرار می‌گیرد. الگوهای مورد استفاده این برنامه با مراجعه به فهرست /usr/share/apps/kugar/templates قابل دستیابی است.

برنامه‌های گرافیکی

سیستم‌عامل Linux بستر بسیار مناسبی برای کارهای گرافیکی است، به طوری که برخی از تولید کنندگان انیمیشن و طراحان جلوه‌های ویژه پروژه‌های خود را روی کامپیوترهای Linux انجام می‌دهند. به این ترتیب، مناسب است که در این قسمت با برخی از برنامه‌های گرافیکی تحت Linux آشنا شوید.

تعدادی از این برنامه‌ها به همراه سیستم‌عامل Red Hat Linux توزیع می‌شوند. در این میان می‌توان به برنامه‌های مورد استفاده برای بازخوانی محتوای فایل‌های PDF (اصطلاحاً Portable Document Format)، مشاهده تصاویر و عکسبرداری از صفحه نمایش اشاره کرد. دسترسی به این برنامه‌ها از طریق منوی فرعی Graphics واقع در منوی اصلی امکان‌پذیر است. برخی از آن‌ها نیز در منوی فرعی More Graphics Applications از منوی Graphics واقع شده‌اند.

برنامه‌های بازخوانی اسناد

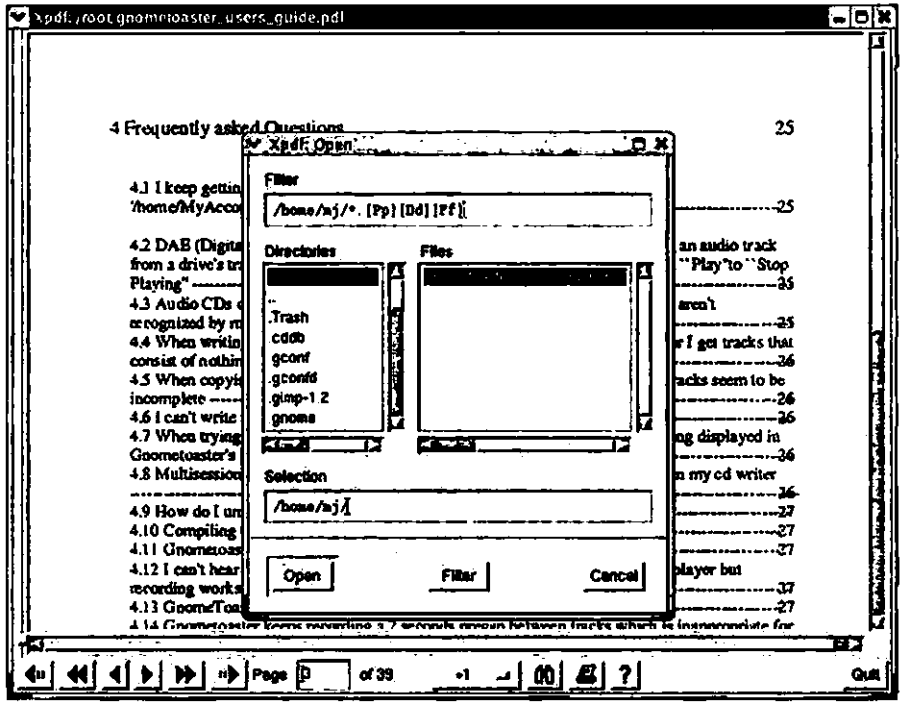
سه قالب Portable Document Format، PostScript و Device Independent یا به اختصار PDF، PS و DVI قالب‌های گرافیکی اسناد در سیستم‌عامل Linux هستند.

علاوه بر دسترسی رایگان به برنامه Adobe Acrobat Reader، در سیستم‌عامل Red Hat Linux دو برنامه xpdf و PS/PDF Viewer به منظور بازخوانی اسناد PDF پیش‌بینی شده است. ضمناً اسناد PostScript را با استفاده از برنامه‌ای به نام GNOME Ghostview (به اختصار GGV) و اسناد DVI را به کمک برنامه DVI Viewer می‌توان مورد بازخوانی قرار داد.

به عنوان نکته‌ای عجیب، برنامه KDE Fax Viewer (به اختصار Kfax) به منظور ارسال و دریافت فاکس طراحی نشده است. برنامه مذکور صرفاً جهت مشاهده محتوای فایل‌های دریافتی از طریق برنامه‌های ارسال و دریافت فاکس امکانات لازم را در اختیار می‌گذارد. برای اطلاع از برنامه‌ای که در سیستم‌عامل Linux به منظور ارسال و دریافت فاکس طراحی شده است به وب سایت مربوطه در آدرس http://www.cce.com/efax مراجعه کنید.

برنامه xpdf

برای دسترسی به این برنامه گزینه PDF Viewer را از منوی فرعی Graphics واقع در منوی اصلی انتخاب کرده یا این‌که فرمان xpdf را مستقیماً در سطر فرمان محیط گرافیکی مورد استفاده اجرا کنید. پنجره این برنامه فاقد نوار ابزار است. برای دسترسی به منوی اصلی این برنامه دکمه راست ماوس را فشار دهید. سپس جهت باز کردن سند موردنظر گزینه مربوطه را از منوی مزبور انتخاب کرده یا آن‌که کلید o را فشار دهید. با این اقدام کادر محاوره‌ای Open مطابق شکل ۱۵-۱۸ باز شده و امکانات لازم برای دسترسی به سند PDF موردنظر را در اختیار می‌گذارد.



شکل ۱۵-۱۸ پنجره برنامه xpdf

پس از باز کردن سند PDF، با استفاده کلیدهای جهت‌دار موجود در پایین صفحه می‌توانید به صفحه موردنظر از آن دسترسی پیدا کنید. هم‌چنین به کمک فرامینی که شرح آن‌ها در جدول ۱۹-۱۸ آمده است، می‌توانید برای انجام این کار اقدام کنید. علاوه بر این، فرامین دیگری نیز موجود است که با کلیک روی دکمه Question می‌توانید از جزییات مربوطه اطلاع حاصل کنید.

جدول ۱۹-۱۸ شرح برخی از فرامین برنامه xpdf

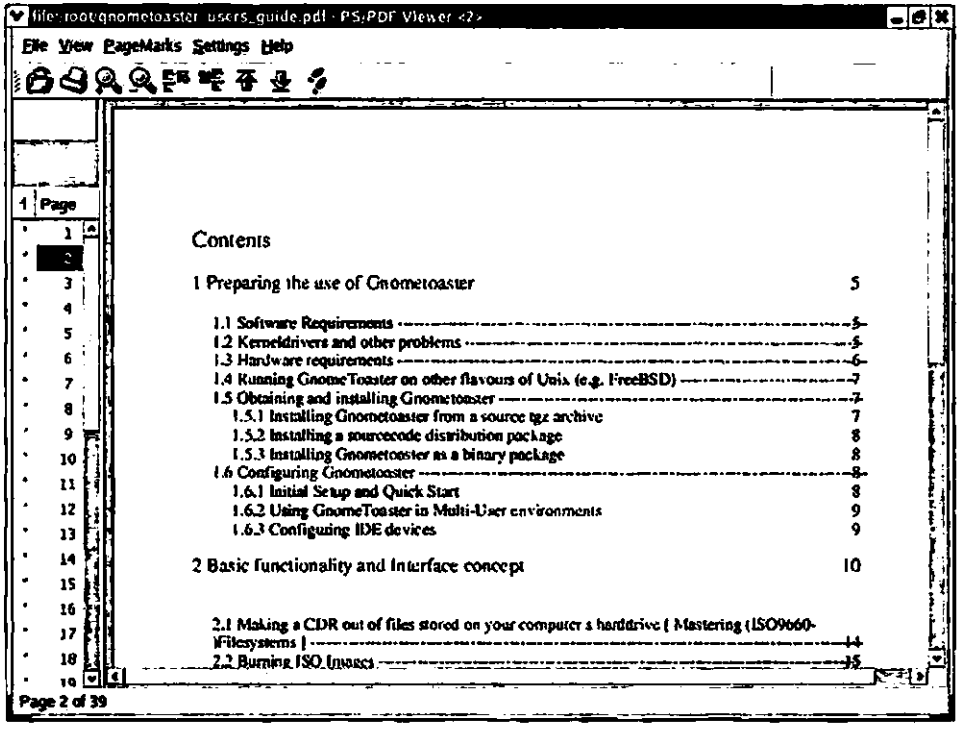
عنوان فرمان	توضیح
o	این فرمان، امکانات لازم برای بازکردن یک سند PDF را در اختیار می‌گذارد.
f	این فرمان، امکانات لازم برای جستجوی متن را در اختیار می‌گذارد.
n	این فرمان، موجب نمایش محتوای صفحه بعد می‌شود.
p	این فرمان، موجب نمایش محتوای صفحه قبل می‌شود.

برنامه PS/PDF Viewer

برای دسترسی به این برنامه که اغلب با عنوان KGhostView نیز شناخته می‌شود، گزینه PS/PDF Viewer را از منوی فرعی More Graphics Applications واقع در منوی Graphics از منوی اصلی انتخاب کرده یا این‌که مستقیماً فرمان pdfviewr را در سطر فرمان محیط گرافیکی مورد استفاده اجرا کنید. رابط گرافیکی این برنامه کلیه امکانات لازم برای دسترسی به فایل‌های PDF و PS و بازخوانی آن‌ها را در اختیار می‌گذارد. شکل ۱۶-۱۸ پنجره این برنامه را در حال نمایش فایلی از نوع PDF نشان می‌دهد.

برنامه PostScript Viewer

این برنامه که اغلب با عنوان GNOME Ghostview یا به اختصار GGV نیز شناخته می‌شود، به منظور بازخوانی محتوای فایل‌های PDF و PS طراحی شده است. برای دسترسی به این برنامه، گزینه PostScript Viewer را از منوی فرعی More Graphics Applications واقع در منوی فرعی Graphics از منوی اصلی انتخاب کرده یا این‌که مستقیماً فرمان ggv را در سطر فرمان محیط گرافیکی مورد استفاده اجرا کنید. عملکرد و رابط گرافیکی این برنامه شبیه به برنامه KGghostView است.



شکل ۱۶-۱۸ پنجره برنامه KghostView در حال نمایش سندی از نوع PDF

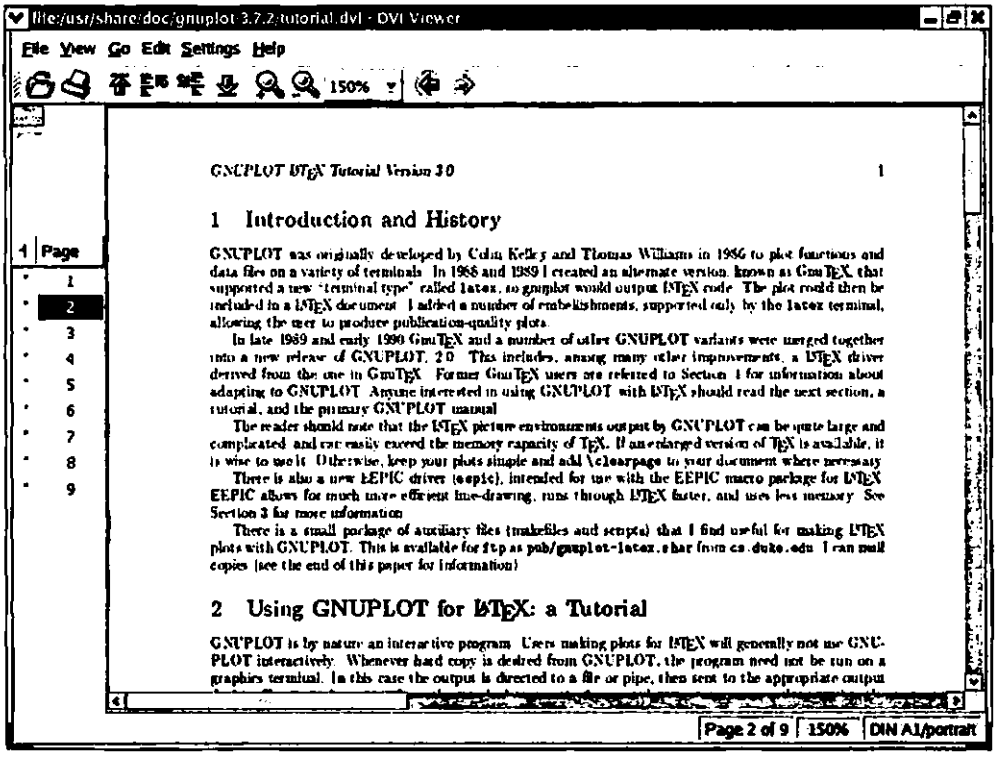
برنامه DVI Viewer

یکی از محصولات پردازش فایل‌های متنی توسط زبان قالب‌بندی Tex فایل‌هایی از نوع DVI یا اصطلاحاً Device Independent است. برای بازخوانی این نوع فایل‌ها برنامه‌ای نام DVI Viewer طراحی شده که اغلب با عنوان KGghostView نیز شناخته می‌شود. در ظاهر، اسناد PDF و DVI بسیار شبیه به یکدیگر هستند.

برای دسترسی به این برنامه کافی است فرمان kghostview را مستقیماً در سطرفرمان محیط گرافیکی مورد استفاده اجرا کنید. جهت برخورداری از تمام قابلیت‌های این برنامه باید بسته نرم‌افزاری *-tetex را نیز روی کامپیوتر میزبان نصب کنید. شکل ۱۷-۱۸ پنجره این برنامه را در حال نمایش محتوای سندی از نوع DVI نشان می‌دهد.

برنامه‌های دیگری نیز برای بازخوانی محتوای فایل‌های DVI موجود است. در این زمینه دو برنامه KDVI و XDVI دو برنامه متداول محسوب می‌شوند. دسترسی به برنامه KDVI با انتخاب گزینه DVI Viewer از منوی فرعی Graphics واقع در منوی اصلی و دسترسی به برنامه XDVI با انتخاب همان

گزینه از منوی فرعی More Graphics Applications واقع در منوی فرعی Graphics از منوی اصلی امکان‌پذیر است.



شکل ۱۷-۱۸ پنجره برنامه KGhostView در حال نمایش سندی از نوع DVI

TeX و LaTex عناوین دو زبان قالب‌بندی متداول در سیستم‌عامل‌ها UNIX و Linux هستند که به منظور قالب بندی فایل‌های متنی و با هدف نشر مورد استفاده قرار می‌گیرند.

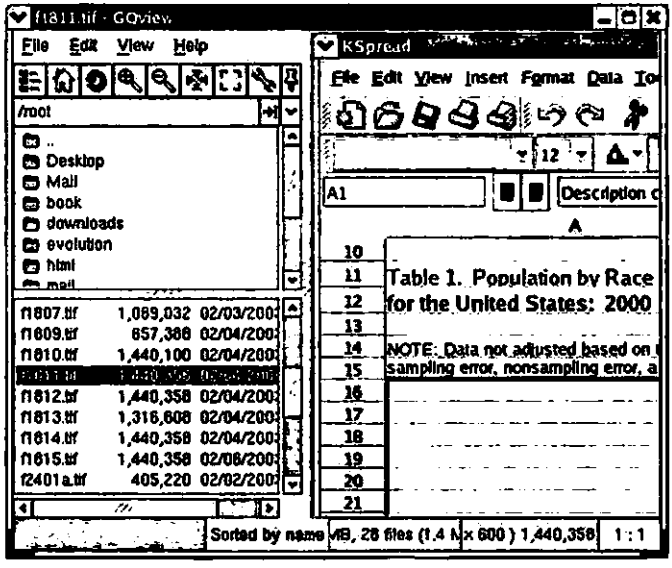
برنامه‌های بازبینی تصویر

سیستم‌عامل Red Hat Linux حاوی برنامه‌های گرافیکی متعددی برای بازبینی تصاویر است. برخی از آن‌ها علاوه بر بازبینی تصاویر امکان ویرایش آن‌ها را نیز در اختیار می‌گذارند. هر کدام از این برنامه‌ها دارای قابلیت‌های مختلفی هستند. برای مثال، در برنامه GQview قابلیتی به منظور تهیه تصاویر thumbnail از روی نسخه اصلی آن‌ها پیش‌بینی شده است. برنامه Kuickshow نیستی از اسامی تصاویر

موجود در فهرست موردنظر را در اختیار می‌گذارد. برنامه Icon Editor نیز امکان ویرایش آیکن‌ها را در اختیار قرار می‌دهد. در ادامه به بررسی این برنامه‌ها می‌پردازیم.

برنامه GQview

این برنامه ابزاری برای مشاهده محتوای فایل های گرافیکی، نمایش اسلاید، سازمان‌دهی تصاویر و مواردی از این قبیل است. برای دسترسی به آن کافی است گزینه GQview Image Viewer را از منوی فرعی Graphics واقع در منوی اصلی انتخاب کرده یا این‌که فرمان gqview را مستقیماً در سطر فرمان محیط گرافیکی مورد استفاده اجرا کنید. چنان‌که در شکل ۱۸-۱۸ مشاهده می‌کنید، کار با رابط گرافیکی این برنامه بسیار ساده است.

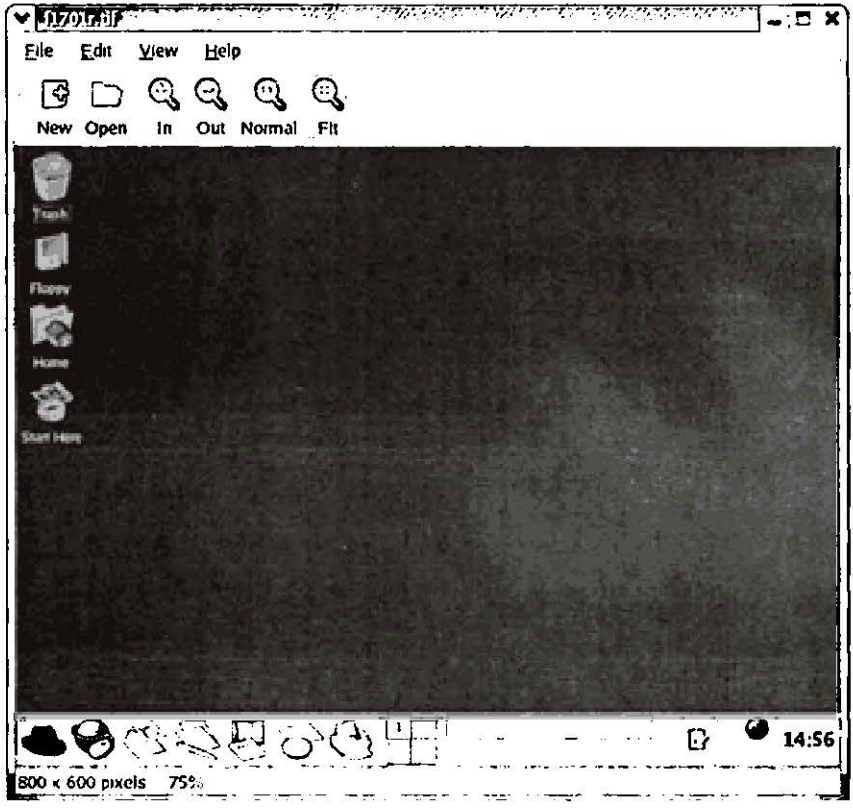


شکل ۱۸-۱۸ پنجره برنامه GQview

برنامه Eye of GNOME

این برنامه به منظور بازبینی محتوای فایل‌های گرافیکی طراحی شده و از این رو کاربردی شبیه به برنامه GQview دارد. با وجود این، تنوع تولیدات این برنامه به چند نوع فایل گرافیکی به خصوص محدود شده است، چنان‌که به طور پیش فرض، امکان ذخیره کردن فایل‌های ویرایش شده در این برنامه تنها در دو قالب JPEG و PNG میسر است.

برای‌دسترسی به این برنامه، گزینهEye of GNOME را از منوی فرعی More Graphics Applications واقع در منوی فرعی Graphics از منوی اصلی انتخاب کرده یا این‌که فرمان eog را مستقیماً در سطر فرمان محیط گرافیکی مورد استفاده اجرا کنید. چنان‌که شکل ۱۹-۱۸ نشان می‌دهد، کار با رابط گرافیکی این برنامه بسیار ساده است.



شکل ۱۹-۱۸ پنجره برنامه Eye of GNOME

برنامه Icon Editor

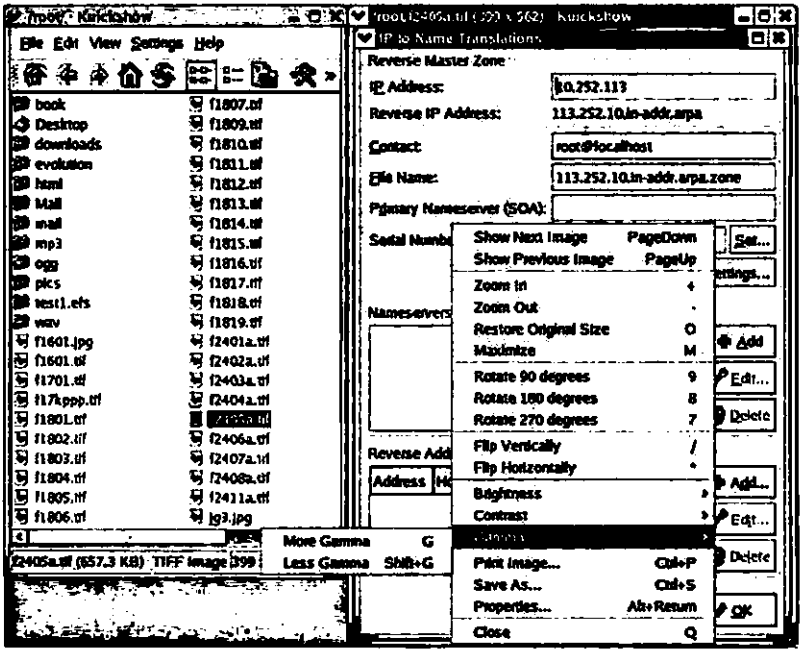
این برنامه که اغلب با عنوان KIconEditor نیز شناخته می‌شود، به منظور ویرایش آیکن‌ها طراحی شده است. برای دسترسی به این برنامه، گزینه Icon Editor را از منوی فرعی More Graphics Applications واقع در منوی فرعی Graphics از منوی اصلی انتخاب کرده یا این‌که فرمان kiconedit را مستقیماً در سطر فرمان محیط گرافیکی مورد استفاده اجرا کنید.

برنامه Image Viewer

این برنامه که اغلب با عنوان KView نیز شناخته می‌شود، به منظور بازبینی محتوای فایل‌های گرافیکی طراحی شده و از این‌رو کاربرد آن شبیه به دو برنامه GQview و Eye of GNOME است. برخلاف برنامه Eye of GNOME، این برنامه قادر است فایل‌های ویرایش شده را در قالب‌های گرافیکی متنوعی ذخیره کند. برای دسترسی به آن، کافی است گزینه Image Viewer را از منوی فرعی More Graphics Applications واقع در منوی فرعی Graphics از منوی اصلی انتخاب کرده یا این‌که فرمان kview را مستقیماً در سطر فرمان محیط گرافیکی مورد استفاده اجرا کنید.

برنامه Kuickshow

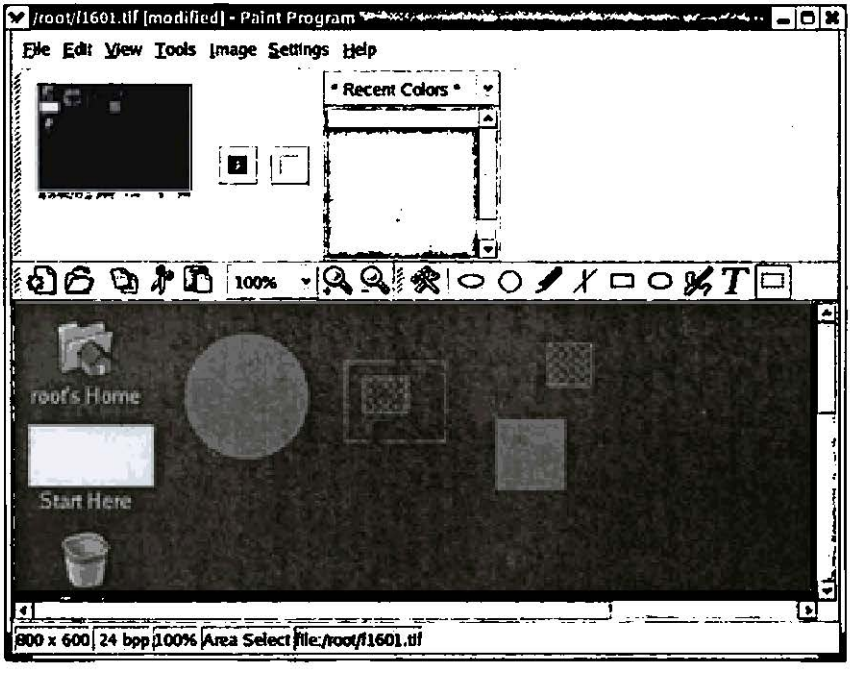
این برنامه لیستی از فایل‌های گرافیکی موجود در فهرست موردنظر را جهت انتخاب و بازبینی محتوای آن‌ها در اختیار می‌گذارد. برای دسترسی به آن، گزینه Kuickshow را از منوی فرعی More Graphics Applications واقع در منوی فرعی Graphics از منوی اصلی انتخاب کرده یا این‌که فرمان kuickshow را مستقیماً در سطر فرمان محیط گرافیکی مورد استفاده اجرا کنید. شکل ۲۰-۱۸ پنجره این برنامه را نشان می‌دهد.



شکل ۲۰-۱۸ پنجره برنامه Kuickshow

برنامه Paint Program

این برنامه که اغلب با عنوان KPaint نیز شناخته می‌شود، به منظور نمایش و ویرایش تصاویر طراحی شده است. برای دسترسی به‌آن، گزینه Paint Program را ازمنوی‌فرعیMore Graphics Applications واقع در منوی فرعی Graphics از منوی اصلی انتخاب کرده یا این‌که فرمان kpaint را مستقیماً در سطر فرمان محیط گرافیکی مورد استفاده اجرا کنید. شکل ۲۱-۱۸ پنجره این برنامه را در حال نمایش یک تصویر نشان می‌دهد.



شکل ۲۱-۱۸ پنجره برنامه KPaint

برنامه‌های عکسبرداری از صفحه نمایش

گاهی اوقات به دلایلی لازم است از صفحه نمایش عکسبرداری شود. برای مثال، چنان‌چه قصد دارید محیط کاری کامپیوترتان را برای یکی از دوستان خود توصیف کنید، بهترین روش این است که تصویری از آن‌را برای وی ارسال کنید.

برخی از برنامه‌ها امکان دریافت خروجی ارسالی از سایر تجهیزات سخت‌افزاری هم‌چون دوربین‌های دیجیتال و اسکنرها را نیز در اختیار می‌گذارند. حال آن‌که بعضی دیگر تنها به منظور عکسبرداری از

صفحه نمایش طراحی شده‌اند. در ادامه به بررسی چند برنامه در این زمینه می‌پردازیم.

دوربین‌های دیجیتال

تاکنون برنامه‌های کاربردی متعددی با رابط گرافیکی برای بهره‌برداری از بسته نرم‌افزاری gphoto2-* طراحی شده است. Kamera و Digital Camera Tool عناوین دو نمونه از این گونه برنامه‌ها هستند که اولی به طور خاص جهت استفاده در محیط گرافیکی KDE و دومی توسط شرکت Red Hat طراحی شده است. برای دسترسی به برنامه Digital Camera Tool گزینه مربوطه را از منوی فرعی Graphics واقع در منوی اصلی انتخاب کرده یا فرمان gtcam را مستقیماً در سطر فرمان محیط گرافیکی مورد استفاده اجرا کنید. لیست اسامی دوربین‌های دیجیتالی موجود که این برنامه در اختیار می‌گذارد به هیچ وجه کامل نیست. برای اطلاع بیشتر به آدرس http://www.gphoto.org مراجعه کنید.

دو سند Kodak-Digitalcam-HOWTO و USB-Digital-Camera-HOWTO اطلاعات مفیدی را درباره دوربین‌های دیجیتال ساخت شرکت Kodak و عموماً دوربین‌های دیجیتالی که از طریق پورت USB به کامپیوتر متصل می‌شوند، در اختیار می‌گذارند. دسترسی به این اسناد با مراجعه به وب سایت http://www.tldp.org امکان‌پذیر است.

اسکن تصویر

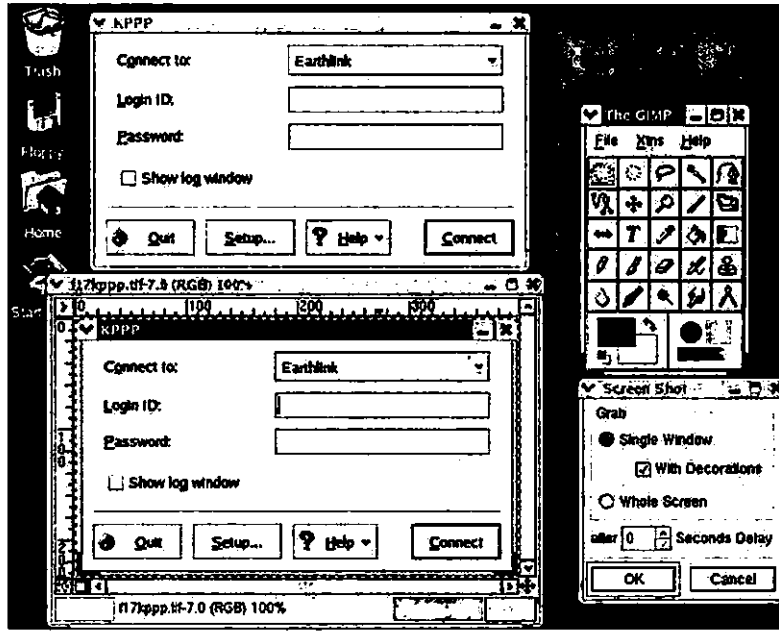
برنامه xscan ابزاری با رابط گرافیکی است که توسط شرکت Red Hat به منظور اسکن تصاویر طراحی شده است. دسترسی به آن با انتخاب گزینه Scanning از منوی فرعی Graphics از منوی فرعی یا با اجرای مستقیم فرمان xscan در سطر فرمان محیط گرافیکی مورد استفاده امکان‌پذیر است. چنان‌چه این برنامه قادر به شناسایی اسکنر نباشد، پیغامی را در همین رابطه نمایش می‌دهد. تحت این شرایط پنجره برنامه xscan باز نمی‌شود.

برنامه Kooka نیز ابزاری برای اسکن تصاویر است که به طور خاص برای استفاده در محیط گرافیکی KDE تهیه شده است. این برنامه ضمن پشتیبانی از برنامه xscan از قابلیت تشخیص کاراکترها نیز برخوردار است. برای‌دسترسی به آن، گزینه Scan & OCR Program را از منوی فرعی More Graphics Applications واقع در منوی فرعی Graphics از منوی اصلی انتخاب کرده یا این‌که فرمان kooka را مستقیماً در سطر فرمان محیط گرافیکی مورد استفاده اجرا کنید.

برنامه GIMP

یکی از برنامه‌های گرافیکی متداول در سیستم‌عامل Linux برنامه‌ای با عنوان GIMP یا اصطلاحاً GNU Image Manipulation Program است. بسیاری از کاربران این سیستم‌عامل استفاده از برنامه GIMP را به سایر برنامه‌ها از جمله Photoshop و Paint Shop Pro ترجیح می‌دهند. این برنامه زیرمجموعه نرم‌افزاری است که برای کاربردهای اداری طراحی شده است. برای دسترسی به این برنامه گزینه GIMP را از منوی فرعی Graphics واقع در منوی اصلی انتخاب کرده یا این‌که فرمان gimp را مستقیماً در سطر فرمان محیط گرافیکی مورد استفاده اجرا کنید.

این برنامه علاوه بر ویرایش تصاویر، امکان عکسبرداری از صفحه نمایش را نیز در اختیار می‌گذارد. برای این منظور ابتدا گزینه Screen Shot را از منوی Acquire واقع در منوی File انتخاب کنید تا پنجره Screen Shot باز شود. هنگامی که آماده عکسبرداری شدید، دکمه OK را از پنجره مذکور کلیک کنید. با این اقدام اشاره‌گر ماوس به علامت + تبدیل شده و به این ترتیب امکان انتخاب ناحیه عکسبرداری فراهم می‌شود. پس از انتخاب ناحیه موردنظر دکمه راست ماوس را کلیک کرده و از منوی حاصل گزینه مربوط به ذخیره تصویر عکسبرداری شده را انتخاب کنید. شکل ۲۲-۱۸ روند عکسبرداری از پنجره برنامه KPPP را نشان می‌دهد.

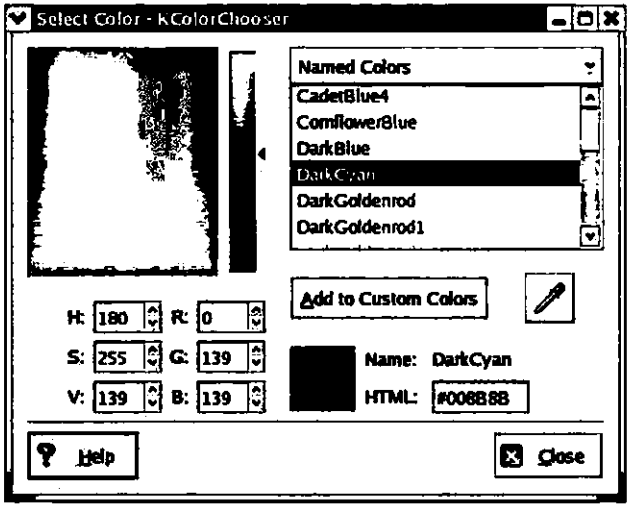


شکل ۲۲-۱۸ برنامه GIMP در حال عکسبرداری از پنجره برنامه KPPP

برنامه گرافیکی KColorChooser

برنامه KColorChooser که اغلب با عنوان KColorEdit نیز شناخته می‌شود، به منظور اطلاع از مشخصات رنگ موردنظر طراحی شده است. برای دسترسی به این برنامه، گزینه Color Chooser را از منوی فرعی More Graphics Applications واقع در منوی فرعی Graphics از منوی اصلی انتخاب کرده یا این‌که فرمان kcolorchooser را مستقیماً در سطر فرمان محیط گرافیکی مورد استفاده اجرا کنید.

شکل ۲۳-۱۸ موقعیت رنگ Dark Cyan را در الگوی استاندارد رنگ‌ها نشان می‌دهد. به موقعیت‌های نسبی سه رنگ اصلی قرمز، سبز و آبی توجه کنید. تمام رنگ‌ها با ترکیب نسبت‌های معینی از این سه رنگ ساخته می‌شوند.



شکل ۲۳-۱۸ پنجره برنامه KColorChooser

جمع‌بندی

سیستم‌عامل Red Hat Linux حاوی تعداد قابل توجهی برنامه کاربردی با رابط گرافیکی است که در این میان می‌توان به سه نرم‌افزار اداری شامل برنامه‌های کاربردی مفید و چند برنامه گرافیکی کارآمد اشاره کرد.

سه نرم‌افزار اداری OpenOffice، GNOME Office و KOffice که هر کدام شامل واژه‌پرداز، صفحه گسترده، برنامه رسم نمودار، برنامه ویرایش تصاویر و نمایش اسلاید هستند. علاوه بر این، برنامه‌های

دیگری نیز با کاربرد مدیریت پروژه، قالب‌بندی فرمول‌های ریاضی، مدیریت مالی و مانند آن در قالب این نرم‌افزارها توزیع می‌شود.

برنامه‌های گرافیکی عرضه شده در قالب نرم‌افزارهای نامبرده هم برای کاربردهای ساده (برنامه GQview) و هم برای کاربردهای پیچیده (برنامه GIMP) طراحی شده‌اند. برنامه‌هایی نیز با کاربرد بازخوانی اسناد PDF، PS و DVI در همین قالب توزیع شده است.

در فصل نوزدهم برخی از ابزارهای مدیریتی عرضه شده توسط شرکت Red Hat را که دارای رابط گرافیکی هستند، مورد بررسی قرار می‌دهیم. عنوان عمومی این ابزارها redhat-config-* است، چرا که اسامی تمام آن‌ها با عنوان مذکور آغاز می‌شود. بیشتر این ابزارها از طریق منوی فرعی System Settings واقع در منوی اصلی قابل دستیابی هستند.

فصل نوزدهم

برنامه‌های کاربردی شرکت Red Hat

در این فصل تعدادی از ابزارهای گرافیکی را که توسط شرکت Red Hat و به منظور پیکربندی و مدیریت سیستم طراحی شده‌اند مورد بررسی قرار می‌دهیم. البته محتوای این فصل به احتمال قوی برای کاربران قدیمی سیستم‌عامل Linux چندان خوشایند نیست، چرا که این قبیل کاربران استفاده از سطر فرمان سیستم‌عامل را به ابزارها و برنامه‌هایی که دارای رابط گرافیکی هستند، ترجیح می دهند.

کاربران با تجربه شدیداً به این نکته معتقدند که کارهای بیشتری را می‌توان از طریق سطر فرمان انجام داد. ابزارهای گرافیکی مورد بررسی در این فصل هم‌چنان در حال توسعه و پیشرفت هستند. این ابزارها در واقع رابطی برای ویرایش فایل‌های پیکربندی موجود هستند. (به ابزارها یا برنامه‌هایی که چنین نقشی را ایفا می‌کنند اصطلاحاً front-end گفته می‌شود. ـ مترجم) به واسطه این ابزارها مطمئناً کار با سیستم‌عامل Linux برای کاربران کم تجربه خوشایندتر خواهد بود.

ابزارهای مورد بحث در این فصل کلیه امکانات لازم برای پیکربندی تجهیزات سخت‌افزای، سرویس‌های محلی، سرویس‌های شبکه و مدیریت سیستم را در اختیار قرار می‌دهند. چنان‌چه پس از پیکربندی موارد فوق محتوای فایل پیکربندی مربوطه را مورد بررسی قرار دهید، اطمینان می‌دهیم که تجربه بیشتری درباره سیستم‌عامل Linux به دست خواهید آورد.

با وجود این، به خاطر داشته باشید که مدت زمان زیادی از ظهور این ابزارها سپری نشده است. از این‌رو، توصیه می‌کنیم پس از ویرایش فایل‌های پیکربندی موردنظر محتوای آن‌ها را برای اطمینان بیشتر مورد بررسی قرار داده و به این ترتیب از عملکرد صحیح ابزار مورد استفاده مطمئن شوید.

برای اطلاع از ابزارهای پیکربندی موجود فرمان redhat-config-* را اجرا کرده و سپس کلید Tab را دو بار فشار دهید. شکل ۱-۱۹ نتیجه اجرای این فرمان را نشان می‌دهد. بدیهی است که باید بتوانید ابزارهای موجود در این لیست را مورد استفاده قرار دهید. کار بررسی برخی از این ابزارها را در فصل‌های مختلف این کتاب انجام داده‌ایم.

```
[root@RH9Desk root]# redhat-config-
redhat-config-bind           redhat-config-packages
redhat-config-bind-gui       redhat-config-printer
redhat-config-date           redhat-config-printer-gui
redhat-config-httpd          redhat-config-printer-tui
redhat-config-keyboard       redhat-config-proc
redhat-config-kickstart      redhat-config-rootpassword
redhat-config-language       redhat-config-samba
redhat-config-mouse          redhat-config-securitylevel
redhat-config-network        redhat-config-services
redhat-config-network-cmd    redhat-config-soundcard
redhat-config-network-druid  redhat-config-time
redhat-config-network-gui    redhat-config-users
redhat-config-network-tui    redhat-config-xfree86
redhat-config-nfs
[root@RH9Desk root]# redhat-config-
```

شکل ۱-۱۹ لیست ابزارهای گرافیکی redhat-config-*

بیشتر این ابزارها از طریق منوی فرعی System Tools یا System Settings واقع در منوی اصلی محیط گرافیکی GNOME و KDE قابل دستیابی هستند. (ظاهر دکمه دسترسی به منوی اصلی در هر دو محیط گرافیکی مذکور مشابه است. با وجود این، در محیط گرافیکی GNOME از اصطلاح Main Menu button و در محیط گرافیکی KDE از اصطلاح K Menu button برای اشاره به آن استفاده می‌شود.) دسترسی به برخی از این ابزارها مستلزم برخورداری از مجوزهای مربوطه است. چنان‌چه سیستم را به عنوان کاربر اصلی (اصطلاحاً root) یا کاربری که مجوزهای لازم را در اختیار دارد، مورد دسترسی قرار نداده‌اید، هنگام دسترسی به این گونه ابزارها اعلانی را برای ورود کلمه عبور مشاهده خواهید کرد.

هم‌چنین در صورتی که ابزار موردنظر خود را در لیست شکل ۱-۱۹ یا منوهای فرعی تامبرده مشاهده نمی‌کنید، باید بسته نرم‌افزاری مربوط را نصب کنید. در بیشتر موارد، اسامی بسته‌های نرم‌افزاری شبیه به اسامی این ابزارهاست. برای مثال، بسته نرم‌افزاری redhat-config-somba-* حاوی ابزار پیکربندی Samba است.

از آن‌جا که شرکت Red Hat، مجموعه ابزارهای redhat-config-* را به هیچ ترتیب خاصی دسته‌بندی نکرده است، در این فصل ترتیب بررسی آن‌ها را به دلخواه انجام خواهیم داد. موضوعات مورد بررسی در فصل حاضر به این شرح است:

- ابزارهای پیکربندی تنظیمات اولیه
- ابزارهای پیکربندی شبکه

- ابزارهای مدیریت سیستم
- ابزارهای پیکربندی سرویس‌ها

ابزارهای پیکربندی تنظیمات اولیه

برای پیکربندی تنظیمات اولیه در سیستم‌عامل Red Hat Linux چندین ابزار تهیه شده که تمام آن‌ها را می‌توان از طریق منوی فرعی System Settings واقع در منوی اصلی محیط گرافیکی GNOME مورد دستیابی قرار داد. این ابزارها امکانات لازم برای تنظیم تاریخ و ساعت، صفحه کلید، زبان مورد استفاده پیش فرض، عملکرد ماوس و کارت صوتی را در اختیار می‌گذارند. جدول ۱-۱۹ کاربرد این ابزارها را به اختصار شرح می‌دهد.

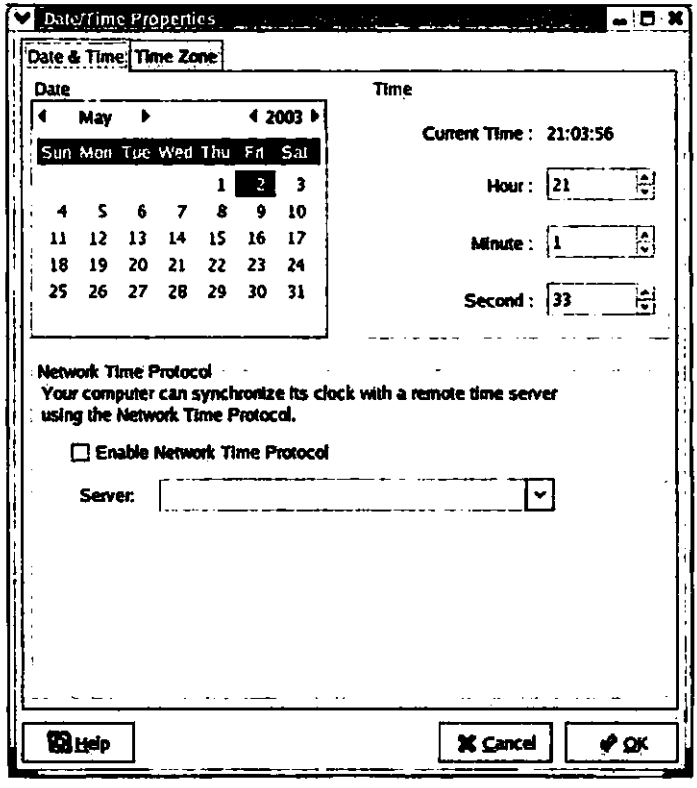
جدول ۱-۱۹ شرح کاربرد ابزارهای پیکربندی تنظیمات اولیه

عنوان ابزار	توضیح
redhat-config-date redhat-config-time	این دو ابزار امکان تنظیم تاریخ و ساعت و هم‌چنین دسترسی به سرور یا سرورهای NTP یا اصطلاحاً Network Time Protocol را در اختیار می‌گذارند.
redhat-config-keyboard	این ابزار امکان تنظیم صفحه کلید را در اختیار می‌گذارد.
redhat-config-language	این ابزار امکان تعیین زبان پیش‌فرض مورد استفاده در محیط گرافیکی را در اختیار می‌گذارد.
redhat-config-mouse	این ابزار امکان تنظیم ماوس یا تجهیزات سخت‌افزاری شبیه به آن را در اختیار می‌گذارد.
redhat-config-soundcard	این ابزار امکان شناسایی و پیکربندی کارت صوتی را در اختیار می‌گذارد.

تنظیم تاریخ و ساعت

تنظیم تاریخ و ساعت کامپیوتر یکی از کارهای بااهمیت است. چنان‌چه از طریق اینترنت با کامپیوترهای سرور مستقر در مناطق جغرافیایی مختلف در ارتباط هستید، باید تاریخ و ساعت کامپیوتر خود را با آن‌ها هماهنگ کنید. سیستم‌عامل Red Hat Linux این هماهنگی را به واسطه پروتکلی با عنوان Network Time Protocol یا به اختصار NTP، که عضوی از مجموعه پروتکل‌های TCP/IP است انجام می‌دهد.

برای انجام این تنظیمات گزینه Date & Time را از منوی فرعی System Settings واقع در منوی اصلی انتخاب کرده یا این‌که یکی از فرامین redhat-config-date یا redhat-config-time را در مستقیماً در سطر فرمان محیط گرافیکی مورد استفاده اجرا کنید تا به این ترتیب پنجره Date/Time Properties باز شود. شکل ۲-۱۹ این پنجره را نشان می‌دهد.

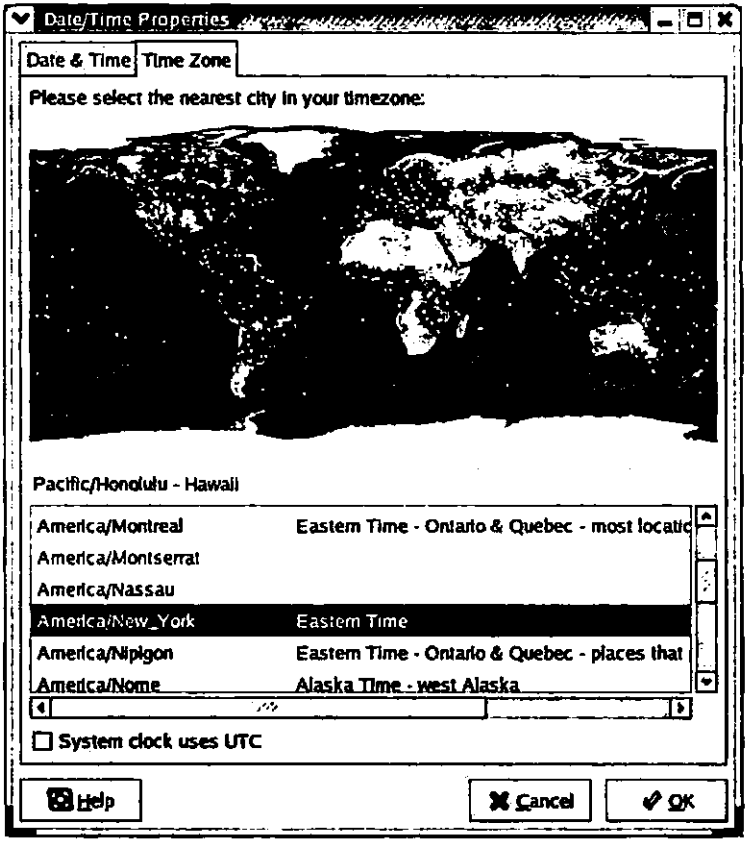


شکل ۲-۱۹ پنجره Date/Time Properties

با استفاده از امکانات موجود در این پنجره می‌توانید تاریخ و ساعت کامپیوتر را تنظیم کنید. البته با این اقدام ساعت سخت‌افزاری کامپیوتر نیز تنظیم خواهد شد. هم‌چنین می‌توانید تاریخ و ساعت کامپیوتر خود را با ساعت یک کامپیوتر دیگر که از طریق شبکه به آن دسترسی دارید، هماهنگ کنید. سیستم‌عامل Linux قادر است پیغام‌های لازم برای این هماهنگی را از طریق پروتکل NTP به کامپیوتر سروری که به همین منظور پیکربندی شده است، ارسال کند. (به چنین کامپیوتری اصطلاحاً time server یا NTP server گفته می‌شود.)

اگر کنترل تنظیم تاریخ و ساعت کامپیوتر خود را با NTP server از دست دهید، پنجره Date/Time Properties امکان انجام این تنظیمات را به طور مستقل در اختیار قرار نخواهد داد.

به کمک تنظیمات موجود در بخش Time Zone از پنجره Date/Time Properties می‌توانید ناحیه جغرافیایی مستقر در آن را تعیین کنید. شکل ۳-۱۹ بخش مذکور از این پنجره را نشان می‌دهد.



شکل ۳-۱۹ بخش تنظیمات Time Zone از پنجره Data/Time Properties

چنان‌که مشاهده می‌کنید، در این مورد گزینه مربوط به سواحل شرقی ایالات متحده آمریکا یعنی America/New_York به عنوان گزینه پیش‌فرض انتخاب شده است.

گزینه System Clock Uses UTC را مگر در صورتی که کامپیوتر خود را به منظور راه‌اندازی با سیستم‌عامل دیگری غیر از Linux (از جمله ویندوز) پیکربندی یا اصطلاحاً آن‌را "dual boot" کرده

باشید، فعال کنید. اصطلاح UTC کوتاه شده عبارت فرانسوی معادل Coordinated Universal Time است که به ساعت جهانی یعنی ساعت مشهور گرینویچ (اصطلاحاً Greenwich Mean Time) اشاره دارد. با انتخاب این گزینه، ساعت سخت‌افزاری کامپیوتر با این ساعت مبنا هماهنگ شده و اختلاف آن با ساعت محلی محاسبه خواهد شد.

تنظیمات این پیکربندی در فایلی تحت عنوان /etc/sysconfig/clock ذخیره می‌شود. ضمناً اطلاعات مربوط به سرورهای NTP مورد استفاده نیز در فایل دیگری با عنوان /etc/ntp/ntpservers به ثبت می‌رسد. بدیهی است در صورت تمایل می‌توان محتوای این فایل‌ها را مستقیماً مورد ویرایش قرار داد. به احتمال قوی معتبرترین وب سایت موجود در مورد این سرورها متعلق به دانشگاه Delaware واقع در در ایالات متحده است. این وب سایت به آدرس http://www.eecis.udel.edu/~ntp حاوی لیستی از سرورهای NTP فعال در نقاط مختلف زمین است.

ابزار Date/Time Properties در سیستم‌عامل Red Hat Linux سرویس Network Time Protocol با عنوان ntpd را به نحوی پیکربندی می‌کند که طی دفعات آتی راه‌اندازی این سیستم‌عامل به طور خودکار در سطوح اجرایی سوم و پنجم به اجرا درآید. برای تحقیق موضوع فوق کافی است این فرمان را اجرا کنید:

```
# chkconfig --list ntpd
```

در صورت وجود مکانیزم بازدارنده دیوار آتش، ابزار Date/Time Properties قوانین مربوط به این مکانیزم را چنان تغییر می‌دهد که کامپیوتر میزبان از امکان دریافت اطلاعات ارسالی توسط سرورهای NTP برخوردار باشد. برای مثال، به نمونه‌ای از تنظیماتی مکانیزم دیوار آتش که امکان دسترسی به سروری از نوع NTP را در اختیار کامپیوتر میزبان قرار می‌دهد، توجه کنید: (برای مشاهده لیست کامل قوانین دیوار آتش فرمان iptables -L را اجرا کنید.)

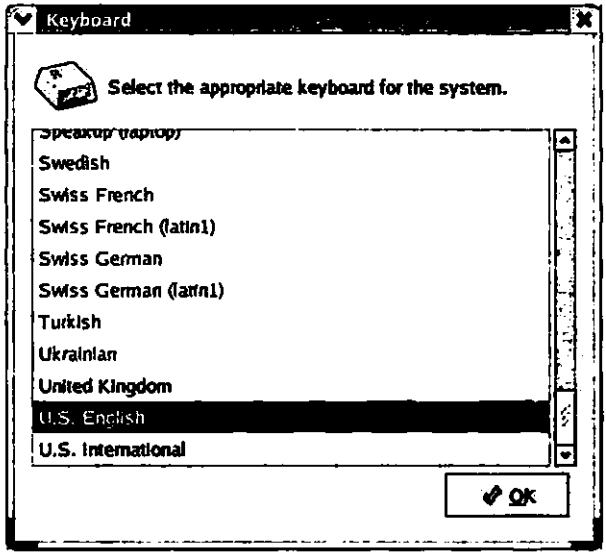
```
Accept udp -- ns3.oit.unc.edu anywhere udp spt:ntp dpt:ntp
```

توجه کنید که در تنظیمات فوق عبارت ns3.oit.unc.edu بیانگر نام کامل حوزه میزبان سرور NTP موردنظر است.

پیکربندی صفحه کلید

ابزار redhat-config-keyboard به منظور پیکربندی صفحه کلید طراحی شده است. به کمک امکانات این ابزار می‌توان عملکرد صفحه کلید را با زبان موردنظر تطبیق داد.

برای دسترسی به ابزار مذکور، گزینه Keyboard را از منوی فرعی System Settings واقع در منوی اصلی انتخاب کرده یا این‌که فرمان redhat-config-keyboard را مستقیماً در سطر فرمان محیط گرافیکی مورد استفاده اجرا کنید. شکل ۴-۱۹ پنجره این ابزار را نشان می‌دهد.



شکل ۴-۱۹ ابزار پیکربندی صفحه کلید

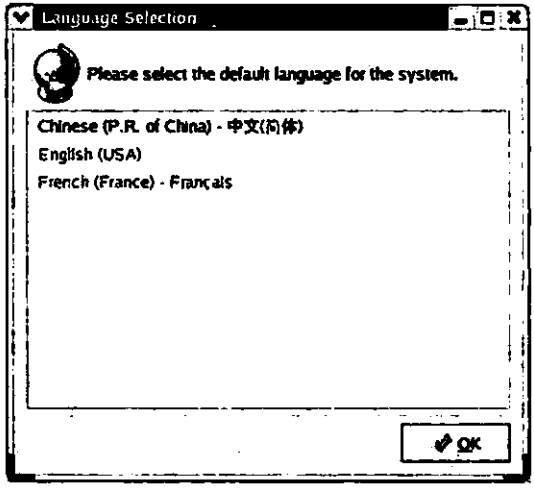
چنان‌که مشاهده می‌کنید، در مورد برخی از زبان‌ها می‌توان تنظیمات مختلفی را با توجه به موقعیت کشور مربوطه انتخاب کرد. پس از انتخاب زبان مورد نظر، با فشار کلید OK می‌توان تنظیمات را در فایل پیکربندی /etc/sysconfig/keyboard ثبت کرد.

چنان‌چه فرمان redhat-config-keyboard را در یک کنسول متنی (اصطلاحاً text-mode console) به اجرا درآورید، تنظیمات شکل ۴-۱۹ در صفحه‌ای به رنگ آبی و با وضوح پایین قابل دستیابی خواهد بود.

انتخاب زبان

ابزار redhat-config-language به منظور تنظیم زبان مورد استفاده در محیط گرافیکی سیستم‌عامل Red Hat Linux طراحی شده است. برای دسترسی به این ابزار، گزینه Language را از منوی فرعی System Settings واقع در منوی اصلی انتخاب کرده یا این‌که فرمان redhat-config-language را

مستقیماً در سطر فرمان محیط گرافیکی مورد استفاده اجرا کنید. با این اقدام مطابق شکل ۵-۱۹ پنجره Language Selection باز شده و امکان انتخاب زبان موردنظر را از میان زبان‌های موجود در اختیار می‌گذارد.



شکل ۵-۱۹ پنجره Language Selection

چنان‌چه درباره این موضوع که آیا بسته‌های نرم‌افزاری حاوی زبان موردنظر را قبلاً به همراه سیستم‌عامل Red Hat Linux نصب کرده‌اید یا خیر، تردید دارید، اکنون برای اطمینان می‌توانید آن‌ها را نصب کنید. برای این منظور ابتدا باید از لیست بسته‌های نرم‌افزاری حاوی زبان موردنظر مطلع باشید. چنین لیستی را می‌توانید در فایل comps.xml که هم روی نخستین CD نصب سیستم‌عامل Red Hat Linux و هم در فهرست /usr/share/comps/i386 مستقر شده است، پیدا کنید. برای مثال، برای نصب بسته‌های نرم‌افزاری حاوی فایل‌های پشتیبان زبان کره‌ای، به بخش Korean Support از فایل نامبرده رجوع کنید. محتوای بخش مزبور را برای سادگی در این‌جا تکرار می‌کنیم: (برای اطلاع بیشتر درباره فایل comps.xml از جمله زبان‌های موجود به فصل پنجم از فصول اینترنتی کتاب حاضر در وب سایت مربوطه به آدرس http://www.sybex.com مراجعه کنید.)

```
<packagelist>
  <packagereq type="mandatory">nvi-m17n</packagereq>
  <packagereq type="optional" requires="kdelibs">
       kde-i18n-Korean</packagereq>
  <packagereq type="optional" requires="man-pages">
       man-pages-ko</packagereq>
  <packagereq type="optional"requires="XFree86">ami
```

```
</packagereq>
  <packagereq type="optional" requires="XFree86">
       hanterm-xf</packagereq>
  <packagereq type="mandatory">h2ps</packagereq>
  <packagereq type="mandatory">nhpf</packagereq>
  <packagereq type="mandatory">ttfonts-ko</packagereq>
</packagelist>
```

کمترین توصیه این است که بسته‌های نرم‌افزاری ضروری را (که با مقداردهی type="mandatory" مشخص شده‌اند) نصب کنید. سپس فایل پیکربندی /etc/sysconfig/i18n را باز کرده و مقدار متغیر SUPPORTED مربوط به زبان کره‌ای را مورد ویرایش قرار دهید. مشخصات زبان‌های مختلف و مجموعه‌های کاراکتری مربوطه با مراجعه به فهرست /usr/X11R6/lib/X11/locale قابل دستیابی هستند. برای مثال، زبان کره‌ای و نوع کاراکترهای آن در فهرست مذکور با این عنوان مشخص شده است:

```
ko_KR.UTF-8
```

اکنون فایل پیکربندی /etc/sysconfig/i18n را باز کرده و مشخصات زبان موردنظر را طبق این الگو در آن درج کنید:

language_locale.chartype:language_locale:language

برای نمونه، الگوی فوق را در مورد زبان کره‌ای باید به این صورت قالب‌بندی کنید:

```
ko_KR.UTF-8:ko_KR:ko
```

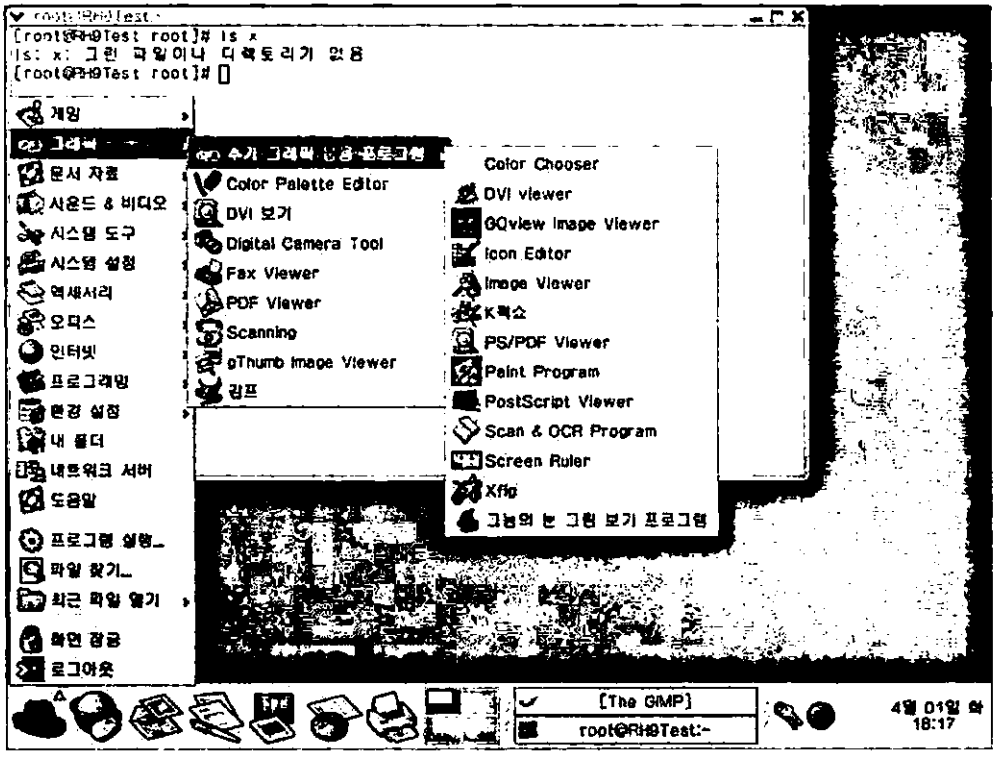
شکل ۶-۱۹ بخشی از فایل پیکربندی /etc/sysconfig/i18n را که حاوی تنظیمات مربوط به زبان‌های چینی، انگلیسی آمریکایی، فرانسوی و کُره‌ای است، نشان می‌دهد.

```
LANG="en_US.UTF-8"
SUPPORTED="zh_CN.GB18030:zh_CN:zh:en_US.UTF-8:en_US:en:fr_FR.UTF-8:fr_FR:fr:ko_K
R.UTF-8:ko_KR:ko"
SYSFONT="latarcyrheb-sun16"
~
~
~
```

شکل ۶-۱۹ بخشی از فایل پیکربندی /etc/sysconfig/i18n که حاوی تنظیمات مربوط به پشتیبانی از زبان‌های چینی، انگلیسی آمریکایی، فرانسوی و کره‌ای است.

به این ترتیب، هنگام دستیابی‌های آتی به ابزار redhat-config-language باید بتوانید گزینه زبان کره‌ای را نیز در پنجره مربوط به این ابزار مشاهده کنید. پس از انتخاب زبان مورد نظر، پیغامی با این

مضمون به نمایش درمی‌آید که تغییرات انجام شده طی دفعات آتی ورود به سیستم قابل مشاهده خواهد بود. شکل ۷-۱۹ نتیجه انتخاب زبان کره‌ای را در مورد محتوای منوی اصلی و برخی منوهای فرعی و هم‌چنین سطر فرمان محیط گرافیکی GNOME نشان می‌دهد.



شکل ۷-۱۹ تأثیر انتخاب زبان کره‌ای در محیط گرافیکی GNOME

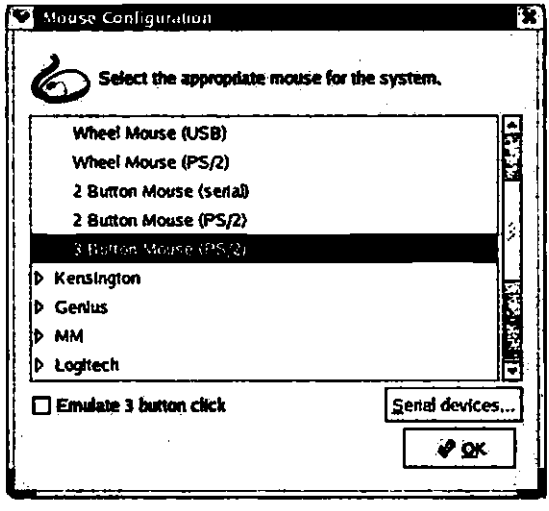
البته پشتیبانی از یک زبان به خصوص در برخی از برنامه‌های کاربردی مستلزم نصب بسته‌های نرم‌افزاری خاصی است که خارج از حوزه کاربرد ابزار redhat-config-language و این کتاب است. برای اطلاع بیشتر در مورد نحوه تنظیم زبان به مستندات مربوطه از وب سایت Linux Documentation Project به آدرس http://www.tldp.org مراجعه کنید.

چنان‌که در فصل هفدهم اشاره شد، تنظیمات زبان مورد استفاده در محیط گرافیکی KDE از طریق ابزاری که به همین منظور در پنجره KDE Control Center پیش‌بینی شده امکان‌پذیر است.

پیکربندی ماوس

ابزار redhat-config-mouse به منظور پیکربندی انواع تجهیزات اشاره‌گر (اصطلاحاً pointing device) طراحی شده است. با وجود این، رایج‌ترین نوع این تجهیزات ماوس است. هر چند که در متون مختلف و هم‌چنین رابط گرافیکی ابزار نامبرده از الفاظ ماوس و ابزار اشاره‌گر به جای یکدیگر نیز استفاده شده است.

برای دسترسی به این ابزار، کافی است گزینه Mouse را از منوی‌فرعی System Settings واقع در منوی اصلی انتخاب کرده یا فرمان redhat-config-mouse را مستقیماً در سطر فرمان محیط گرافیکی مورد استفاده اجرا کنید. با این اقدام رابط گرافیکی ابزار مورد بحث، با عنوان Mouse Configuration باز خواهد شد. شکل ۸-۱۹ رابط مذکور را نشان می‌دهد.



شکل ۸-۱۹ رابط گرافیکی ابزار پیکربندی ماوس

تنظیمات ماوس بر اساس فایل پیکربندی /etc/sysconfig/mouse انجام شده و هر تغییری در تنظیمات ماوس در این فایل به ثبت می‌رسد. در صورت استفاده از ماوس‌هایی که تنها دارای دو دکمه هستند، به سادگی می‌توانید عملکرد دکمه وسط را با فعال کردن گزینه Emulate 3 Button Click شبیه‌سازی کنید، به طوری که اگر دکمه‌های چپ و راست ماوس را به طور هم‌زمان کلیک کنید، عملکرد دکمه وسط شبیه سازی خواهد شد. چنان‌که از فصل هفدهم به خاطر دارید، کلیک دکمه وسط ماوس در محیط گرافیکی KDE منویی از فرامین را در اختیار می‌گذارد.

در صورتی که ماوس به پورت سریال متصل شده باشد، دکمه Serial Devices نیز قابل دستیابی خواهد بود. با کلیک این دکمه فایل‌های سخت‌افزاری (اصطلاحاً device file) مربوط به پورت‌های سریال به نمایش درمی‌آید. هر کدام از این فایل‌ها معادل یکی از پورت‌های COM1 تا COM4 در سیستم‌عامل ویندوز است. جدول ۲-۱۹ این موضوع را شرح می‌دهد.

جدول ۲-۱۹ فایل‌های سخت‌افزاری پورت‌های سریال

عنوان فایل سخت‌افزاری	پورت سریال معادل در سیستم‌عامل ویندوز
/dev/ttyS0	COM1
/dev/ttyS1	COM2
/dev/ttyS2	COM3
/dev/ttyS3	COM4

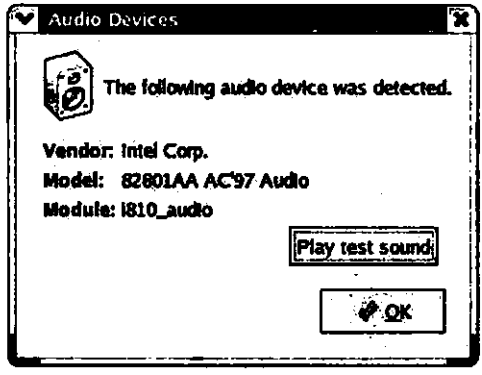
با استفاده از همین ابزار می‌توانید پیکربندی مودم را نیز انجام دهید. چنان‌چه قبلاً مودم را در سیستم‌عامل ویندوز پیکربندی کرده باشید، پورت سریال مربوطه را یادداشت کرده و با توجه به جدول فوق فایل سخت‌افزاری معادل با آن‌را در سیستم‌عامل Linux انتخاب کنید. فرمان ls -l /dev/modem فایل سخت‌افزاری مورد استفاده برای این منظور را نشان می‌دهد.

پس از انجام تغییرات موردنظر و بستن پنجره ابزار redhat-config-mouse، سیستم‌عامل Linux کنسول ماوس را متوقف کرده و مجدداً آن‌را راه‌اندازی خواهد کرد.

لزومی ندارد که پیکربندی ماوس را در محیط گرافیکی انجام دهید. اگر فرمان redhat-config-mouse در حالت متنی (اصطلاحاً text-mode) اجرا کنید، همین امکانات را در اختیار خواهید داشت.

پیکربندی کارت صوتی

ابزار redhat-config-soundcard جهت پیکربندی انواع مختلف کارت‌های صوتی طراحی شده است. برای دسترسی به آن کافی است گزینه Soundcard Detection را از منوی فرعی System Settings واقع در منوی اصلی انتخاب کرده یا این که فرمان redhat-config-soundcard را مستقیماً در سطر فرمان محیط گرافیکی مورد استفاده اجرا کنید. با این اقدام رابط گرافیکی ابزار پیکربندی کارت صوتی با عنوان Audio Devices به نمایش درمی‌آید. شکل ۹-۱۹ رابط مذکور را نشان می‌دهد.



شکل ۹-۱۹ رابط گرافیکی ابزار پیکربندی کارت صوتی

ابزار redhat-config-soundcard پس از شناسایی کارت صوتی نصب شده روی کامپیوتر مشخصات آن‌را در قالب شکل فوق نمایش می‌دهد. برای اطمینان از صحت نتایج، می‌توانید روی دکمه Play Test Sound کلیک کنید. به این ترتیب، در صورت نصب کارت صوتی و اتصال خروجی آن به بلندگو باید صدای حاصل را بشنوید. با اقدام فوق پیغامی نیز جهت تأیید به نمایش در می‌آید که در صورت شنیدن صدا می‌توانید آن‌را تأیید کنید. در خاتمه دکمه OK را کلیک کنید. چنان‌چه پشتیبانی از کارت صوتی مستلزم بارگذاری ماجول به خصوصی در هسته سیستم‌عامل Linux باشد، اقدامات لازم برای این کار انجام شده و تغییرات ناشی از آن در فایل /etc/modules.conf به ثبت خواهد رسید.

در صورت نصب بسته نرم‌افزاری *-sndconfig می‌توانید ابزار sndconfig را که به منظور پیکربندی کارت صوتی پیش‌بینی شده است از طریق سطر فرمان سیستم‌عامل مورد بهره‌برداری قرار دهید. این ابزار علاوه بر قابلیت‌های فوق، امکان تعیین آدرس سخت‌افزاری خاص کارت صوتی را نیز در اختیار می‌گذارد. با وجود این، شرکت Red Hat از توزیع این بسته نرم‌افزاری به همراه نسخه‌های اخیر سیستم‌عامل خود صرف‌نظر کرده و این اقدام بدان معنی است که در نسخه‌های بعدی از آن پشتیبانی نخواهد کرد. این‌دلیل موجهی بر اطمینان شرکت نامبرده به ابزار پیکربندی redhat-config-soundcard است.

دسترسی به شبکه

در سیستم‌عامل Red Hat Linux ابزارهای متعددی برای پیکربندی کامپیوتر جهت دسترسی به شبکه پیش‌بینی شده است. برخی از این ابزارها به طور خاص جهت پیکربندی سرویس‌های شبکه طراحی

شده‌اند. این قبیل ابزارها در فصل‌های مربوطه از کتاب حاضر مورد بررسی قرار گرفته‌اند. در این قسمت ابزارهای گرافیکی تهیه شده توسط شرکت Red Hat در این زمینه را مورد بررسی قرار می‌دهیم.

شرح مختصری از کاربرد این ابزارها در جدول ۳-۱۹ آمده است. دقت کنید که ابزارهای نامبرده در این جدول تنها نمونه‌هایی از ابزارهای موجود در زمینه پیکربندی شبکه محسوب می‌شوند.

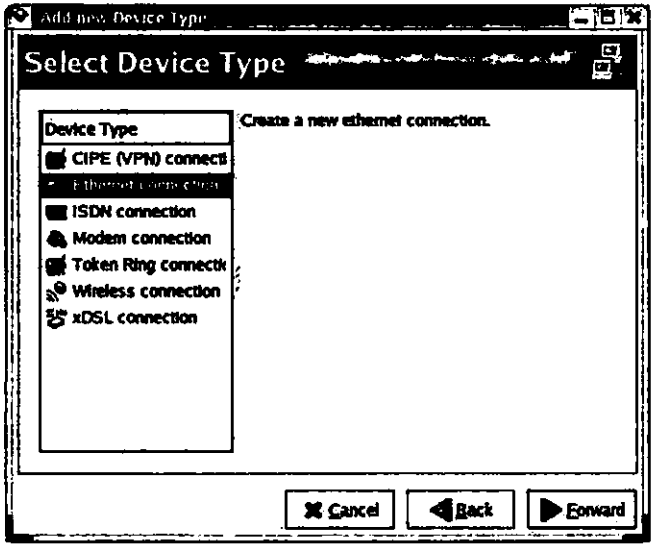
جدول ۳-۱۹ شرح کاربرد ابزارهای تهیه شده توسط شرکت Red Hat برای پیکربندی شبکه

عنوان ابزار	توضیح
redhat-config-network-druid	این ابزار تنظیمات موردنیاز برای دسترسی به شبکه را در اختیار می‌گذارد.
redhat-config-network-tui	این ابزار تنظیمات موردنیاز برای دسترسی به شبکه از طریق سطر فرمان (اصطلاحاً کنسول متن یا text console) را در اختیار می‌گذارد.
redhat-config-network redhat-config-network-gui	این دو ابزار تنظیمات مربوط به پیکربندی کارت‌های شبکه را نمایش می‌دهد.
redhat-config-httpd	این ابزار تنظیمات موردنیاز برای پیکربندی وب سرور Apache را در اختیار می‌گذارد.
redhat-config-bind	این ابزار تنظیمات موردنیاز برای پیکربندی سرور DNS را در اختیار می‌گذارد.
redhat-config-nfs	این ابزار تنظیمات موردنیاز برای پیکربندی سرور NFS را در اختیار می‌گذارد.
redhat-config-samba	این ابزار تنظیمات موردنیاز برای پیکربندی سرور Samba را در اختیار می‌گذارد.
Samba Web Administration Tool	این ابزار به عنوان یک برنامه کاربردی تحت وب تنظیمات موردنیاز برای پیکربندی سرور Samba را در اختیار می‌گذارد.

تنظیمات اولیه شبکه

دو ابزار redhat-config-network و redhat-config-network-druid به منظور تنظیمات اولیه شبکه طراحی شده‌اند، به‌طوری‌که با استفاده از آن‌ها می‌توان تجهیزات‌شبکه مستقرروی‌کامپیوتر را پیکربندی کرد.

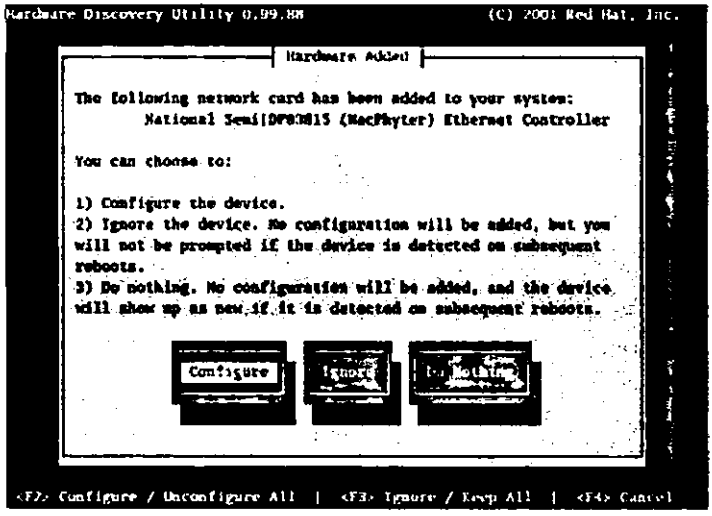
برای دسترسی به ابزار redhat-config-network-druid گزینه Internet Configuration Wizard را از منوی فرعی System Settings واقع در منوی اصلی انتخاب کرده یا این‌که فرمانی به همین نام را مستقیماً در سطر فرمان محیط گرافیکی مورد استفاده اجرا کنید. با این اقدام پنجره Add New Device Type مطابق شکل ۱۰-۱۹ به نمایش درمی‌آید.



شکل ۱۰-۱۹ پنجره Add New Device Type

اگر سیستم‌عامل Red Hat Linux علیرغم به کارگیری ابزارهای فوق در شناسایی کارت شبکه هم‌چنان ناموفق باشد، می‌توانید ابزار دیگری با نام Hardware Discovery Utility را که اغلب با عنوان kudzu نیز شناخته می‌شود، مورد استفاده قرار دهید. به کارگیری ابزار kudzu در شناسایی تجهیزات سخت‌افزاری اغلب مؤثر واقع می‌شود.

این ابزار هنگام راه‌اندازی کامپیوتر به طور خودکار راه‌اندازی می‌شود. با وجود این، پس از نصب یک کارت شبکه جدید، هم‌چون نصب کارت PC شبکه در شکاف PCMCIA یک کامپیوتر قابل حمل، ممکن است لازم باشد تا ابزار kudzu را مجدداً به منظور شناسایی آن مورد استفاده قرار دهید. چنان‌چه این ابزار موفق به شناسایی تجهیزات سخت‌افزاری مورد‌نظر شود، مطابق این شکل پیش از پیکربندی آن پیغامی را نمایش می‌دهد:

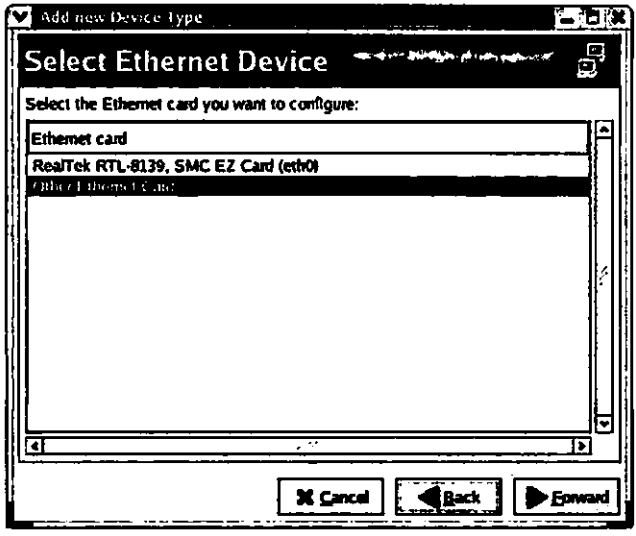


برای اطلاع از نحوه پیکربندی مودم با استفاده از ابزار redhat-config-network-druid به فصل بیست و یکم مراجعه کنید.

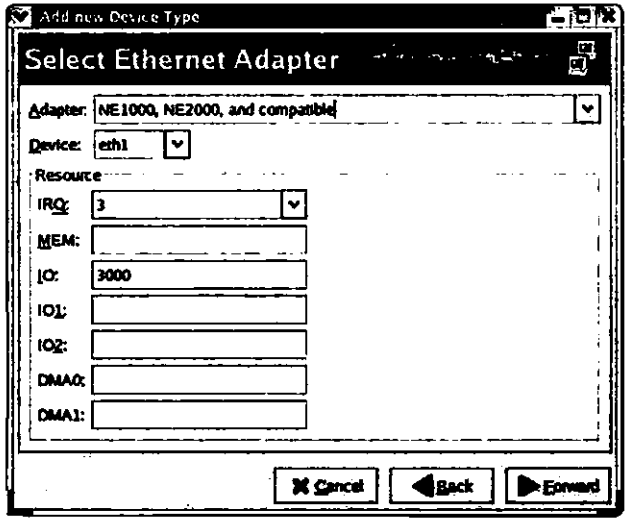
در این قسمت نحوه پیکربندی کارت شبکه‌ای از نوع Ethernet را به عنوان دومین کارت شبکه نصب شده روی کامپیوتر بررسی می‌کنیم. برای شروع، ابتدا گزینه Ethernet Connection را از لیست DeviceType واقع در پنجره Add New Device Type انتخاب کرده و سپس روی دکمه Forward کلیک کنید. با این اقدام صفحه‌ای مطابق شکل ۱۱-۱۹ با عنوان Select Ethernet Device در قالب پنجره مذکور به نمایش درآمده و مشخصات کارت شبکه Ethernet شناسایی شده را نمایش می‌دهد.

چنان‌چه شناسایی با موفقیت انجام شده باشد، کار به همین جا ختم می‌شود اما فرض می‌کنیم که چنین موفقیتی حاصل نشده باشد؛ در این صورت گزینه Other Ethernet Card را از صفحه نامبرده انتخاب کرده و مجدداً روی دکمه Forward کلیک کنید.

این اقدام موجب نمایش صفحه دیگری با عنوان Select Ethernet Adapter در قالب پنجره Select New Device Type خواهد شد. با امکانات موجود در این صفحه می‌توانید درایور کارت شبکه موردنظر و آدرس‌های سخت‌افزاری مربوطه را تنظیم کنید. شکل ۱۲-۱۹ این تنظیمات را نشان می‌دهد.



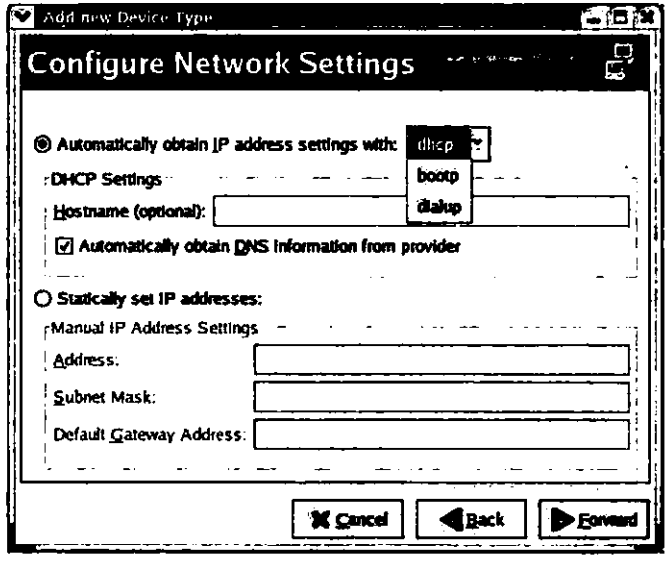
شکل ۱۱-۱۹ صفحه Select Ethernet Device از پنجره Add New Device Type



شکل ۱۲-۱۹ صفحه Select Ethernet Adapter از پنجره Add New Device Type

در مرحله آخر لازم است تنظیمات دسترسی به سرور DHCP یا BOOTP یا استفاده از آدرس IP اختصاصی را در مورد کارت شبکه جدید انجام دهید. این تنظیمات، چنان‌که شکل ۱۳-۱۹ نشان می‌دهد، در قالب صفحه‌ای با عنوان Configure Network Settings از پنجره Add New Device Type

قابل دستیابی است. (برای اطلاعات بیشتر درباره سرویس‌های DHCP و BOOTP به فصل بیست و چهارم مراجعه کنید.)



شکل ۱۳-۱۹ صفحه Configure Network Settings از پنجره Add New Device Type

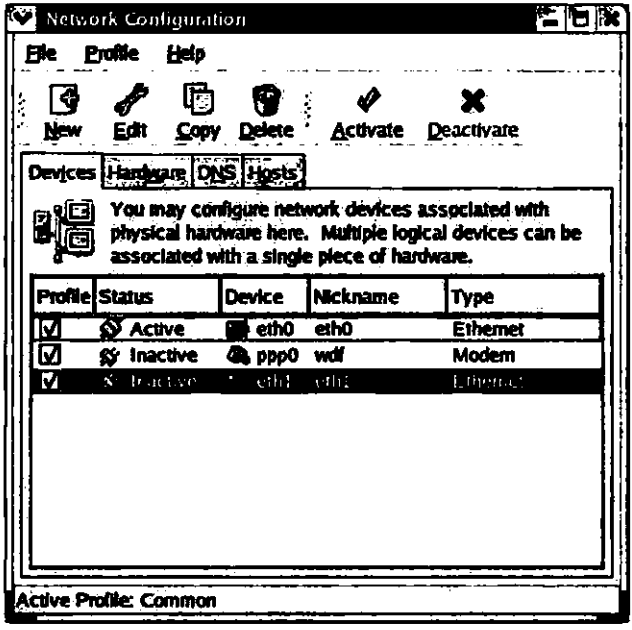
ضمناً گزینه Dialup به شرطی در لیست Automatically Obtain IP Address Settings With قابل دستیابی خواهد بود که در مرحله نخست به جای گزینه Ethernet Connection گزینه Modem Connection انتخاب شده باشد. برای اطلاع بیشتر درباره نحوه تخصیص آدرس‌های IP به فصل بیستم مراجعه کنید.

پس از تأیید تنظیمات فوق پنجره Network Configuration مطابق شکل ۱۴-۱۹ باز می‌شود. این پنجره در واقع رابط گرافیکی ابزار redhat-config-network بوده و دسترسی به آن با انتخاب گزینه Network از منوی فرعی System Settings واقع در منوی اصلی نیز امکان‌پذیر است.

پیکربندی کارت شبکه لزوماً به معنی فعال‌سازی آن کارت نیست. فرآیند فعال‌سازی کارت شبکه ضمن راه‌اندازی کامپیوتر به طور خودکار انجام می‌شود. علاوه بر این، چنان‌که شکل ۱۴-۱۹ نیز نشان می‌دهد، با انتخاب کارت موردنظر و کلیک روی دکمه Activate نیز می‌توان برای فعال کردن آن اقدام کرد.

مشخصات پیکربندی هریک از کارت‌های شبکه در قالب فایل‌هایی در فهرست /etc/sysconfig/networking/devices نگهداری می‌شود. عنوان عمومی فایل‌های حاوی مشخصات

پیکربندی کارت‌های شبکه Ethernet عبارت از ifcfg-eth*n* است که در آن متغیر *n* بیانگر شناسه کارت مورد نظر، هم‌چون 0، 1 و مانند آن است.



شکل ۱۴-۱۹ پنجره Network Configuration

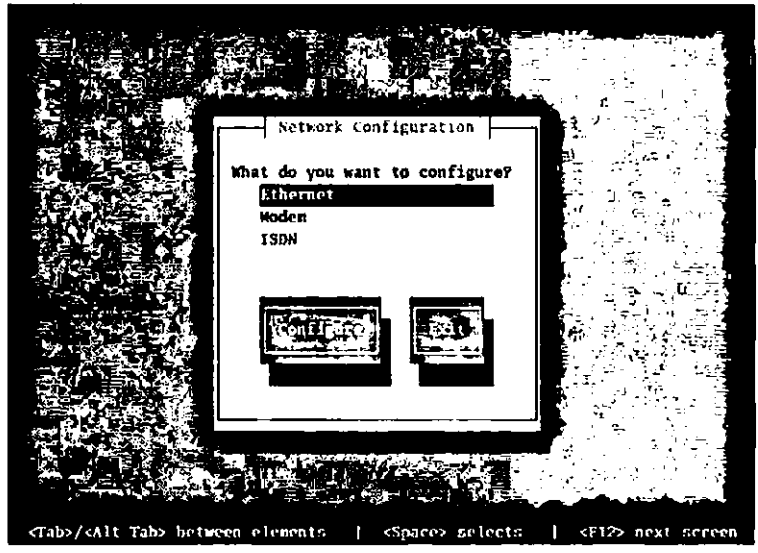
تنظیمات مکمل شبکه

تنظیمات دیگری را نیز می‌توان در پنجره ابزار پیکربندی redhat-config-network، یعنی Network Configuration انجام داد. این تنظیمات در قالب سه بخش مختلف از پنجره مذکور دسته‌بندی شده‌اند:

- **بخش Hardware**: این بخش حاوی مشخصات کارت‌های شبکه‌ای است که روی کامپیوتر میزبان نصب و پیکربندی شده‌اند.
- **بخش DNS**: این بخش حاوی امکاناتی برای تنظیم نام کامپیوتر میزبان، مشخصات حداکثر سه کامپیوتر میزبان سرور DNS و امکاناتی برای جستجوی سرور DNS است. نام کامپیوتر میزبان در فایل پیکربندی /etc/sysconfig/network و مشخصات کامپیوترهای میزبان سرور DNS در فایل پیکربندی /etc/resolv.conf به ثبت می‌رسد.
- **بخش Hosts**: این بخش حاوی اسامی کامپیوترهای میزبان یا حوزه میزبان آن کامپیوترها و آدرس‌های IP مربوطه است. تنظیمات این بخش در فایل پیکربندی /etc/hosts نگهداری می‌شود.

ابزارهای پیکربندی شبکه در حالت متنی

ابزار redhat-config-network-tui جهت انجام تنظیمات دسترسی به شبکه در حالت متنی یا اصطلاحاً text-mode طراحی شده است. با اجرای فرمانی به همین نام امکانات پیکربندی کارت شبکه Ethernet، مودم و تجهیزات دسترسی به شبکه ISDN در قالب صفحه‌ای تحت عنوان Network Configuration به نمایش درمی‌آید. شکل ۱۵-۱۹ صفحه مذکور را نشان می‌دهد.

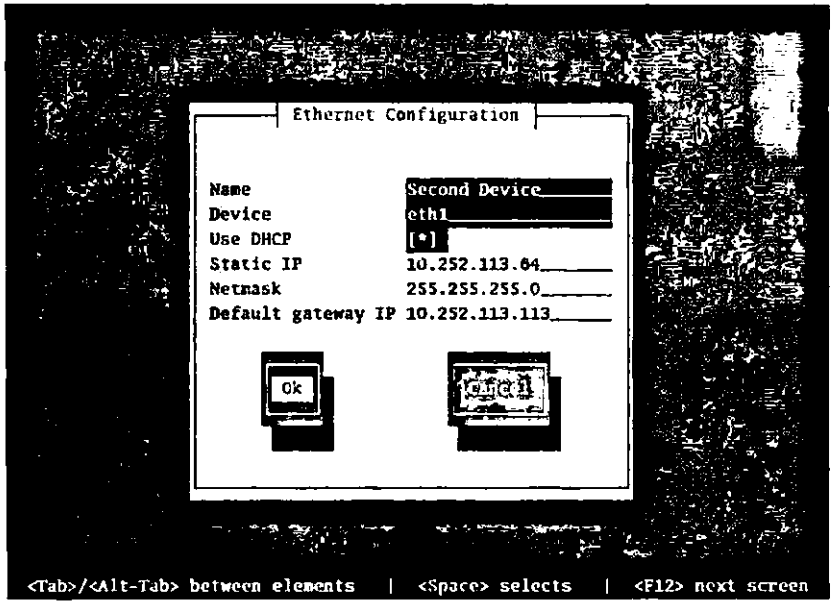


شکل ۱۵-۱۹ صفحه Network Configuration

برای پیکربندی کارت شبکه Ethernet ابتدا گزینه مربوطه را انتخاب کرده و کلید Tab را جهت دسترسی به گزینه Configure فشار دهید. سپس کلید Enter را به منظور دستیابی به تنظیمات موردنظر فشار دهید. با این اقدام صفحه دیگری تحت عنوان Ethernet Configuration باز می‌شود. شکل ۱۶-۱۹ امکانات پیکربندی موجود در این صفحه را نشان می‌دهد. (برای کسب اطلاع درباره سرویس DHCP به فصل بیست و چهارم و برای اطلاع از نحوه تنظیم آدرس‌های IP به فصل بیستم مراجعه کنید.)

مشابه ابزار گرافیکی redhat-config-network، در این مورد نیز کلیه تنظیمات در قالب فایل‌هایی از فهرست /etc/sysconfig/networking/devices نگهداری می‌شود.

عنوان عمومی فایل‌های حاوی مشخصات پیکربندی کارت‌های شبکه Ethernet عبارت از ifcfg-eth*n* است که در آن متغیر *n* بیانگر شناسه کارت مورد نظر، هم‌چون 0، 1 و مانند آن است.

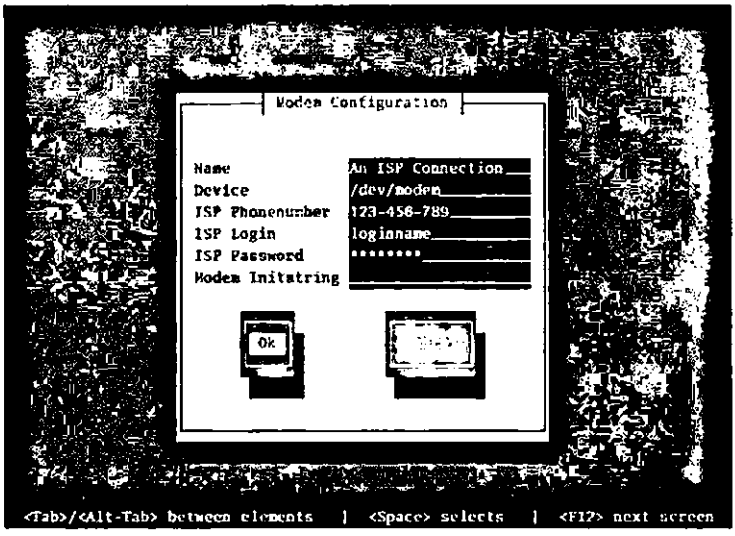


شکل ۱۶-۱۹ صفحه Ethernet Configuration

جهت دسترسی به تنظیمات مودم با استفاده از ابزار redhat-config-network-tui کافی است در صفحه شکل ۱۵-۱۹ با عنوان Network Configuration گزینه Modem را انتخاب کرده و به دنبال آن ابتدا کلید Tab و سپس کلید Enter را فشار دهید تا به این ترتیب صفحه حاوی تنظیمات موردنظر با عنوان Modem Configuration به نمایش درآید. شکل ۱۷-۱۹ این صفحه را نشان می‌دهد.

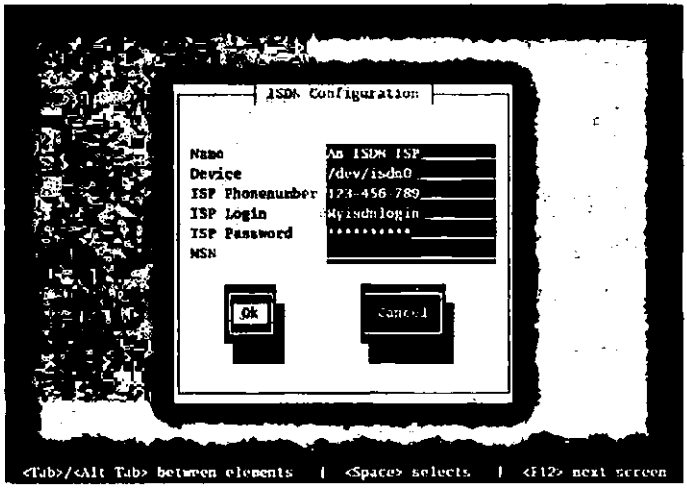
در فیلد Name می‌توانید عنوان دلخواه خود را وارد کنید. چنان‌چه مودم به درستی شناسایی شود، باید پیوند لازم جهت دسترسی به فایل سخت‌افزاری /dev/modem موجود باشد. سایر اطلاعات را می‌توانید از تأمین‌کننده خدمات اینترنت طرف قرارداد به دست آورید. ضمناً در حالت کلی نیازی نیست که فیلد Modem Initstring را مقداردهی کنید.

برای اطلاع بیشتر درباره هریک از این گزینه‌ها به فصل بیست و یکم مراجعه کنید. چنان‌چه فرآیند پیکربندی مودم با موفقیت انجام شود، مشخصات آن در قالب فایلی از فهرست /etc/sysconfig/networking/devices به ثبت می‌رسد. عنوان عمومی فایل‌های حاوی مشخصات پیکربندی مودم‌ها، عبارت از ifcfg-ppp*n* است که در آن‌متغیر *n* بیانگر شناسه مودم مورد نظر، هم‌چون 0، 1 و مانند آن است.



شکل ۱۷-۱۹ صفحه Modem Configuration

به طور مشابه، جهت دسترسی به تنظیمات مربوط به تجهیزات سخت‌افزاری ISDN از طریق ابزار پیکربندی redhat-config-network-tui کافی است در صفحه شکل ۱۵-۱۹ با عنوان Network Configuration گزینه ISDN را انتخاب کرده و به دنبال آن ابتدا کلید Tab و سپس کلید Enter را فشار دهید تا به این ترتیب صفحه حاوی تنظیمات موردنظر با عنوان ISDN Configuration به نمایش درآید. شکل ۱۸-۱۹ این صفحه را نشان می‌دهد.



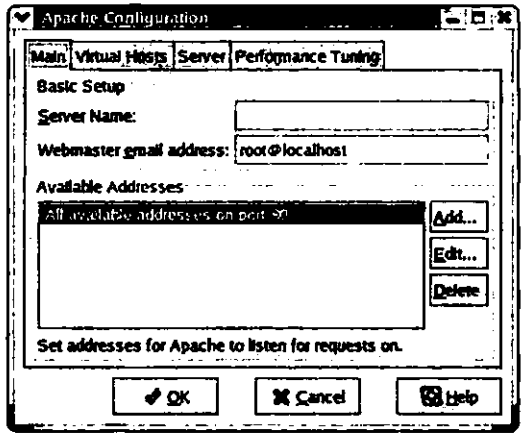
شکل ۱۸-۱۹ صفحه ISDN Configuration

تنظیمات موجود در این صفحه را با توجه به اطلاعاتی که تأمین کننده خدمات اینترنت طرف قرارداد در اختیارتان می‌گذارد، انجام دهید. مقدار فیلد MSN یا اصطلاحاً Multiple Subscriber Number نیز از جانب تأمین کننده مزبور تعیین می‌شود. چنان‌چه فرآیند پیکربندی با موفقیت انجام شود، مشخصات آن در قالب فایلی از فهرست /etc/sysconfig/networking/devices به ثبت می‌رسد. عنوان عمومی فایل‌های حاوی مشخصات پیکربندی تجهیزات ISDN عبارت از ifcfg-isdn*n* است که در آن متغیر *n* بیانگر شناسه تجهیزات مورد نظر، هم‌چون 0، 1 و مانند آن است.

شبکه‌های ISDN یا اصطلاحاً Integrated Services Digital Network به منظور ارتباطات تلفنی دیجیتال ابداع شدند. امروزه استفاده از این گونه شبکه‌ها بیشتر در کشورهای اروپایی رایج است. سرعت انتقال داده‌ها در شبکه‌های ISDN از ۱۲۸ تا ۱۴۴ کیلو بیت در ثانیه، بسته به نوع پیکربندی متغیر است.

پیکربندی سرویس وب

ابزار گرافیکی redhat-config-httpd به منظور پیکربندی وب سرور Apache طراحی شده است. برای دسترسی به این ابزار کافی است گزینه HTTP Server را از منوی فرعی Server Settings واقع در منوی فرعی System Settings از منوی اصلی انتخاب کنید. با این اقدام رابط گرافیکی ابزار مورد بحث در قالب پنجره‌ای با عنوان Apache Configuration به نمایش درمی‌آید. شکل ۱۹-۱۹ این رابط گرافیکی را نشان می‌دهد. (برای اطلاع بیشتر درباره چگونگی انجام این تنظیمات به فصل سی‌ام مراجعه کنید.)

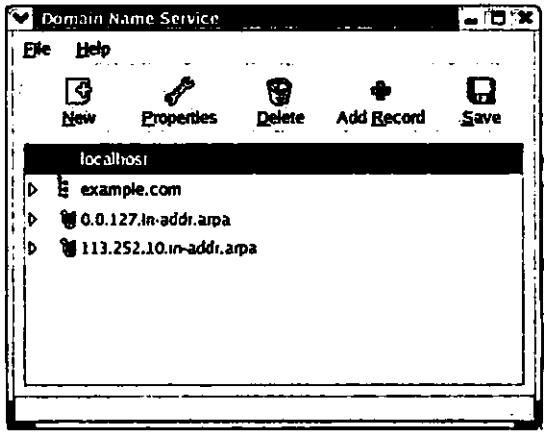


شکل ۱۹-۱۹ پنجره Apache Configuration

اگر در حال حاضر وب سرور Apache روی کامپیوتر میزبان پیکربندی شده باشد، با استفاده از همین ابزار می‌توانید تنظیمات مربوطه را مورد بازبینی قرار دهید. تنظیمات وب سرور Apache در فایل پیکربندی /etc/httpd/conf/httpd.conf ذخیره می‌شود.

پیکربندی سرویس DNS

ابزار گرافیکی redhat-config-bind به منظور پیکربندی سرویس DNS یا اصطلاحاً Domain Name Service طراحی شده است. دسترسی به تنظیماتی که این ابزار در اختیار می‌گذارد با انتخاب گزینه Domain Name Service از منوی فرعی Server Settings واقع در منوی فرعی System Settings از منوی اصلی امکان‌پذیر است. شکل ۲۰-۱۹ پنجره حاوی این تنظیمات با عنوان Domain Name Service را نشان می‌دهد. (برای اطلاع بیشتر درباره سرویس DNS و تنظیمات مربوطه به فصل بیست و چهارم مراجعه کنید.)



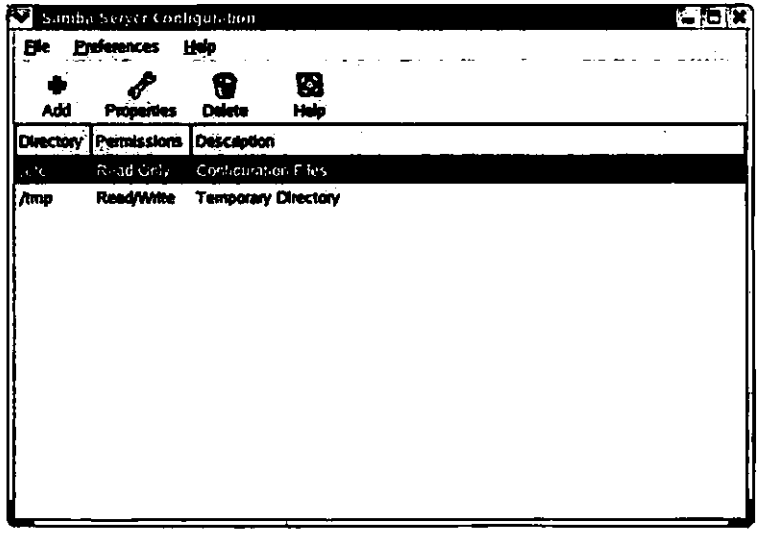
شکل ۲۰-۱۹ پنجره Domain Name Service

اگر در حال حاضر سرویس DNS روی کامپیوتر میزبان پیکربندی شده باشد، با استفاده از همین ابزار می‌توانید تنظیمات مربوطه را مورد بازبینی قرار دهید. تنظیمات این سرویس در فایل پیکربندی /etc/named.conf و هم‌چنین فایل‌هایی از دو فهرست /etc/ و /var/named ذخیره می‌شود.

پیکربندی سرویس NFS

ابزار گرافیکی redhat-config-nfs به‌منظورپیکربندی سرویس NFS یا اصطلاحاًNetwork File System

و توسط شرکت Red Hat طراحی شده است. برای دسترسی به این ابزار، کافی است گزینه Samba Server را از منوی فرعی Server Settings واقع در منوی فرعی System Settings از منوی اصلی محیط گرافیکی GNOME یا KDE انتخاب کنید. شکل ۲۲-۱۹ پنجره این ابزار با عنوان Samba Server Configuration را نشان می‌دهد.



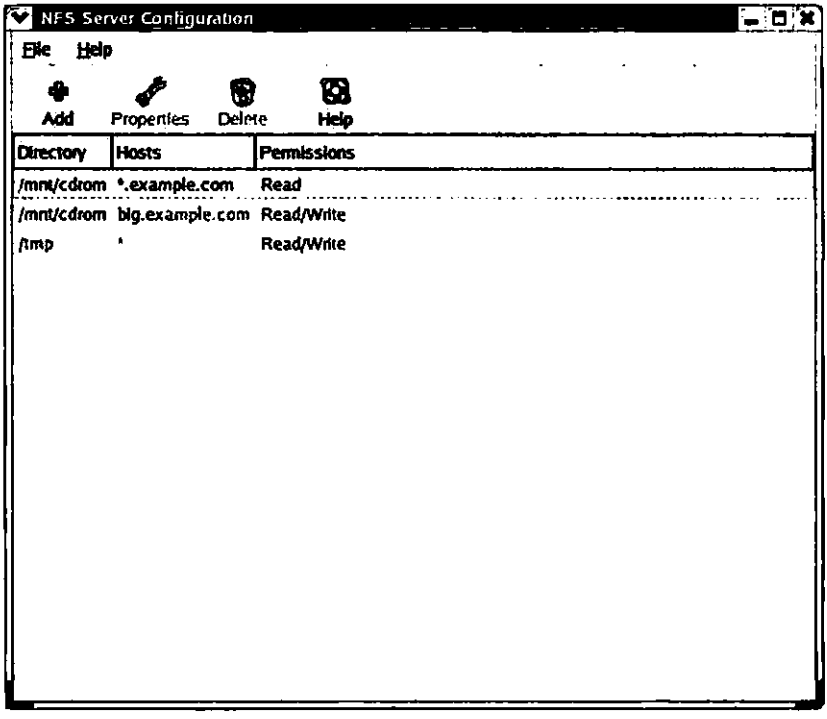
شکل ۲۲-۱۹ پنجره Samba Server Configuration

ابزاردیگر با عنوان samba-swat یک برنامه کاربردی تحت وب است که توسط توسعه دهندگان سرویس Samba طراحی شده است. دسترسی به این ابزار کاملاً با روش دسترسی به ابزارهای redhat-config-* تفاوت دارد. برای‌این منظور کافی است در نوار آدرس پنجره مرورگر دلخواه خود عبارت localhost:901 را وارد کرده و کلید Enter را فشار دهید. چنان‌چه سرویس‌های موردنیاز فعال شده باشد، اقدام فوق برنامه کاربردی تحت وب Samba Web Administration Tool یا به اختصار SWAT را مطابق شکل ۲۳-۱۹ در اختیار قرار می‌دهد.

دسترسی به ابزار SWAT تنها در صورت نصب بسته نرم‌افزاری samba-swat-* و فعال کردن سرویس Samba در فایل پیکربندی /etc/xinetd.d/swat امکان‌پذیر است.

هر دو ابزار redhat-config-samba و samba-swat امکان انجام تنظیمات موردنظر را در قالب فایل پیکربندی /etc/samba/smb.conf در اختیار می‌گذارند. (برای اطلاع بیشتر درباره کاربرد این ابزارها به فصل بیست و نهم مراجعه کنید.)

طراحی شده است. دسترسی به تنظیماتی که این ابزار در اختیار می‌گذارد با انتخاب گزینه NFS Server از منوی فرعی Server Settings واقع در منوی فرعی System Settings از منوی اصلی امکان‌پذیر است. شکل ۲۱-۱۹ پنجره حاوی این تنظیمات با عنوان NFS Server Configuration را نشان می‌دهد. (برای اطلاع بیشتر درباره سرویس NFS و تنظیمات مربوطه به فصل بیست و چهارم مراجعه کنید.)

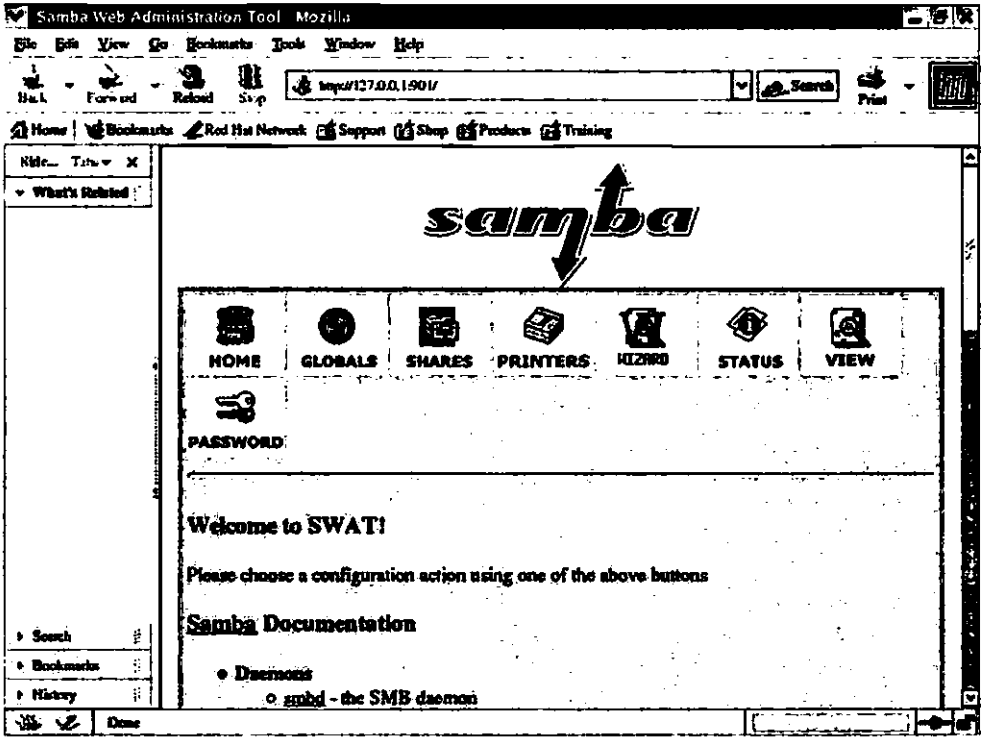


شکل ۲۱-۱۹ پنجره NFS Server Configuration

اگر در حال حاضر سرویس NFS روی کامپیوتر میزبان پیکربندی شده باشد، با استفاده از همین ابزار می‌توانید تنظیمات مربوطه را مورد بازبینی قرار دهید. تنظیمات این سرویس در فایل پیکربندی /etc/exports ذخیره می‌شود.

پیکربندی سرویس Samba

برای پیکربندی سرویس Samba دو ابزار گرافیکی redhat-config-samba و samba-swat موجود است. ابزار نخست یعنی redhat-config-samba عضوی از مجموعه ابزارهای پیکربندی redhat-config-* بوده



شکل ۲۳-۱۹ ابزار Samba Web Administration Tool

ابزارهای مدیریتی

شرکت Red Hat ابزارهای گرافیکی متعددی را نیز به منظور مدیریت سیستم جهت ساده کردن امور روزمره مدیران سیستم‌های Linux طراحی کرده است. این ابزارها هم‌اینک در مراحل مختلفی از توسعه هستند. از این‌رو می‌توان انتظار داشت که در نسخه‌های آتی سیستم‌عامل Red Hat Linux شاهد ظهور ابزارهای مدیریتی کارآمدتری باشیم.

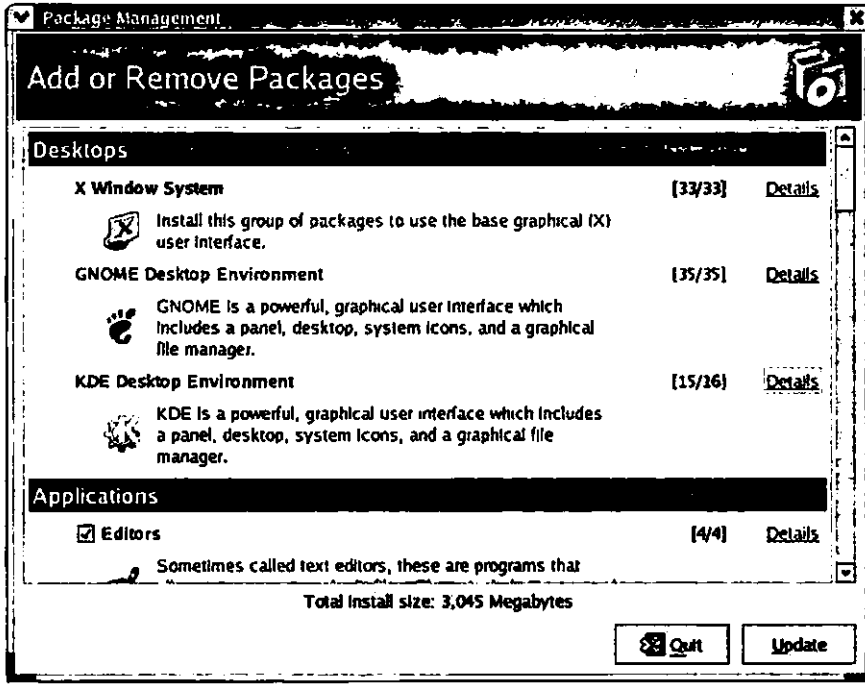
شرح مختصری درباره برخی از ابزارهای گرافیکی طراحی شده توسط این شرکت به منظور مدیریت سیستم در جدول ۴-۱۹ آمده است. علاوه بر این‌ها، تعدادی از ابزارهای مورد بررسی در این فصل را نیز می‌توان به نوعی ابزار مدیریتی محسوب کرد.

جدول ۴-۱۹ شرح مختصری درباره کاربرد ابزارهای مدیریتی

عنوان ابزار	توضیح
redhat-config-packages	این ابزار امکان مدیریت گروه‌های نرم‌افزاری را در اختیار می‌گذارد.
redhat-config-rootpassword	این ابزار امکان تغییر کلمه عبور کاربر اصلی را در اختیار وی قرار می‌دهد.
redhat-config-users	این ابزار امکان مدیریت کاربران (هم‌چون تعریف کاربران جدید) را در اختیار می‌گذارد.
redhat-config-xfree86	این ابزار امکان پیکربندی رابط گرافیکی کاربر (اصطلاحاً Graphical User Interface یا به اختصار GUI) را در اختیار می‌گذارد.
redhat-logviewer	این ابزار امکان بازبینی محتوای فایل‌های ثبت وقایع یا اصطلاحاً Log file را در اختیار می‌گذارد.
redhat-update-gnome-font-install redhat-update-gnome-font-install2	این دو ابزار جهت به روز رساندن فونت‌ها طراحی شده است.
redhat-config-kickstart	این ابزار امکان مکانیزه کردن فرآیند نصب سیستم‌عامل و بسته‌های نرم‌افزاری توزیع شده به همراه آن را به واسطه مکانیزم Kickstart در اختیار می‌گذارد.
redhat-config-securitylevel	این ابزار امکان پیکربندی مکانیزم بازدارنده دیوار آتش یا اصطلاحاً firewall را در اختیار می‌گذارد.
redhat-config-proc	این ابزار امکان ویرایش تنظیمات هسته سیستم‌عامل را که در قالب فهرستی با عنوان proc/ نگهداری می‌شود، در اختیار می‌گذارد.
authconfig-gtk	این ابزار امکان مدیریت بانک اطلاعاتی حاوی اسامی کاربران و کلمات عبور آن‌ها را در اختیار می‌گذارد.
authconfig	این ابزار نسخه متنی ابزار گرافیکی authconfig-gtk است.

مدیریت گروه‌های نرم‌افزاری

ابزار گرافیکی redhat-config-pckages به منظور بازبینی، نصب و حذف بسته‌های نرم‌افزاری موجود طراحی شده است. برای دسترسی به آن، کافی است گزینه Add/Remove Applications را از منوی فرعی System Settings واقع در منوی اصلی انتخاب کنید تا پنجره مربوطه با عنوان Package Management باز شود. شکل ۲۴-۱۹ این پنجره را نشان می‌دهد.

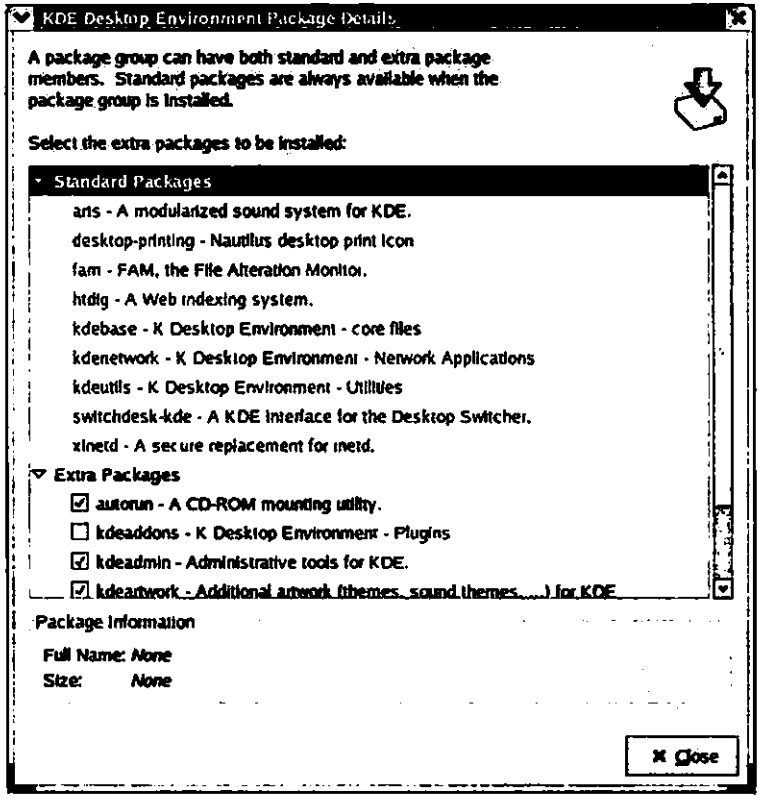


شکل ۲۴-۱۹ پنجره Package Management

اگر سیستم‌عامل Red Hat Linux را طبق دستورالعمل‌های فصل سوم نصب کرده باشید، اکنون باید این شکل را به خاطر بیاورید. چنان‌که مشاهده می‌کنید، بسته‌های نرم‌افزارها به همان ترتیبی که قبلاً در فصل سوم مشاهده کردید، گروه‌بندی شده‌اند.

پس از دستیابی به این پنجره در صورت تمایل می‌توانید بسته‌های نرم‌افزاری موردنظر از چند گروه مختلف را انتخاب کرده و آن‌ها را نصب‌کرده یا چنان‌چه در حال حاضر روی کامپیوتر نصب شده باشند، آن‌ها را حذف کنید. برای مشاهده محتوای هریک از گروه‌ها، گزینه Detail واقع در سمت راست آن‌را کلیک کنید. با این اقدام شرحی از محتوای آن گروه در قالب پنجره دیگری به نمایش درمی‌آید. برای مثال، شکل ۲۵-۱۹ پنجره حاوی جزییات مربوط به گروه KDE Desktop Environment را که به همین ترتیب مورد دستیابی قرار گرفته است، نشان می‌دهد.

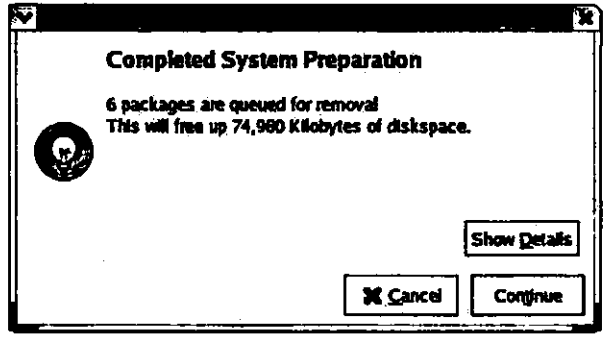
چنان‌که در این شکل مشاهده می‌کنید، بسته‌های نرم‌افزاری در قالب دو گروه مختلف با عناوین Standard و Extra سازمان‌دهی شده‌اند. این دو گروه، با توجه به اطلاعات مندرج در فایل comps.xml، به ترتیب شامل بسته‌های نرم‌افزاری ضروری و اختیاری هستند. (برای اطلاع بیشتر درباره محتوای این فایل به فصل پنجم از فصول اینترنتی کتاب مراجعه کنید.)



شکل ۲۵-۱۹ بسته‌های نرم‌افزاری موجود در گروه KDE Desktop Environment

پس از سازمان‌دهی گروه‌ها و بسته‌های نرم‌افزاری نصب شده روی کامپیوتر میزبان، دکمه Close را کلیک کنید تا به این ترتیب، پنجره Package Management مجدداً در دسترس قرار گیرد. با کلیک روی دکمه Update از این پنجره اعلانی مشابه شکل ۲۶-۱۹ در قالب یک کادر محاوره‌ای به نمایش درآمده و شانس لغو تغییرات را در اختیار قرار خواهد داد. به منظور اطلاع از بسته‌های نرم‌افزاری مشمول این تغییرات روی دکمه Show Details از کادر محاوره‌ای نامبرده کلیک کنید.

نصب بسته‌های نرم‌افزاری جدید اندکی پیچیده‌تر است، چرا که برای این منظور باید به فایل‌های RPM آن‌ها دسترسی داشته باشید. چنان‌چه ابزار redhat-config-package را با اجرای فرمانی به همین نام از طریق سطر فرمان مورد دسترسی قرار داده باشید، اعلان درخواست CD حاوی این قبیل فایل‌ها را مشاهده خواهید کرد.



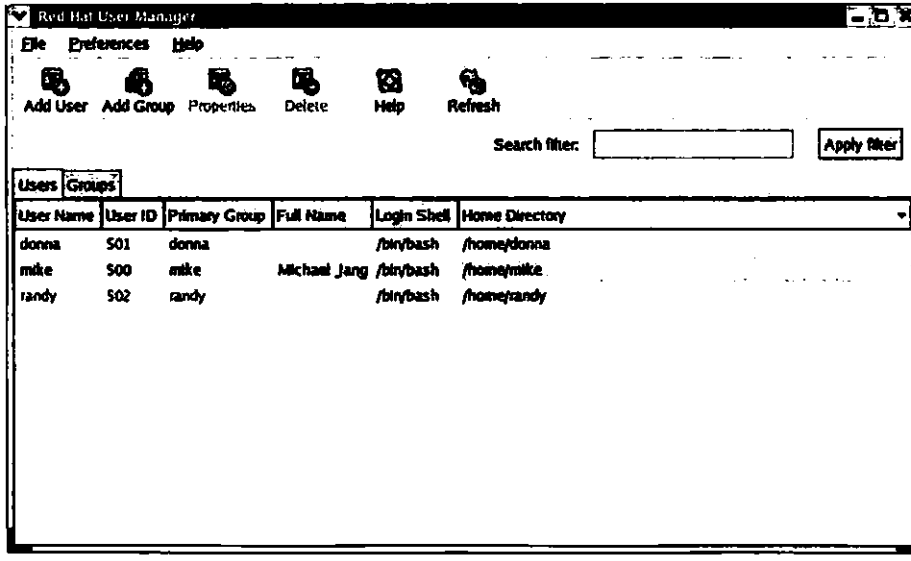
شکل ۲۶-۱۹ اعلانی که پیش از تأیید عملیات حذف بسته‌های نرم‌افزاری موردنظر از روی کامپیوتر به نمایش درمی‌آید.

اگر بسته‌های نرم‌افزاری RPM روی کامپیوتری از شبکه مستقر باشد، نیازی به این CDها ندارید. برای مثال، فرض کنید فهرست /RedHat/RPMS حاوی مجموعه‌ای از بسته‌های نرم‌افزاری RPM بوده و روی سیستم فایل /mnt/source سوار شده باشد. در این صورت جهت دسترسی به آن‌ها کافی است فرمان redhat-config-packages --tree=/mnt/source را اجرا کنید. چنان‌چه مانعی برای دسترسی به بسته‌های نرم‌افزاری RPM از طریق شبکه وجود نداشته باشد، با اقدام فوق امکان نصب این بسته‌های نرم‌افزاری از طریق ابزار redhat-config-packages در اختیار قرار می‌گیرد.

هر هفته لیست جدیدی از بسته‌های نرم‌افزاری نصب شده روی کامپیوتر در فایل /var/log/rpmpkgs ثبت می‌شود. هنگام نصب سیستم‌عامل Red Hat Linux نیز لیست مشابهی در فایل /root/install.log به ثبت می‌رسد.

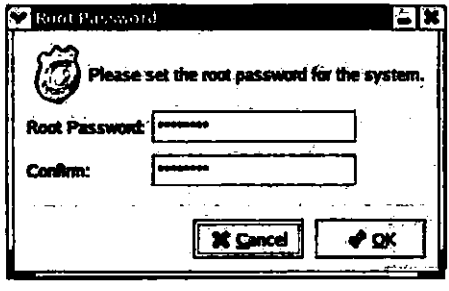
تغییر کلمه عبور کاربر اصلی

ابزار redhat-config-rootpassword به منظور تغییر کلمه عبور کاربر اصلی طراحی شده است. برای دسترسی به این ابزار گزینه Root Password از منوی فرعی System Settings را واقع در منوی اصلی انتخاب کنید. چنان‌چه به عنوان یک کاربر عادی، یعنی بدون وارد کردن شناسه کاربری root و کلمه عبور مربوطه وارد سیستم شده باشید، اعلانی را در قالب یک کادر محاوره‌ای به منظور دریافت کلمه عبور مشاهده خواهید کرد. شکل ۲۷-۱۹ این کادر محاوره‌ای را نشان می‌دهد.



شکل ۲۷-۱۹ این اعلان در صورتی به نمایش درمی‌آید که یک کاربر عادی ابزار گرافیکی redhat-config-password را به منظور تغییر کلمه عبور کاربر اصلی (با شناسه root) مورد دسترسی قرار داده باشد.

پس از وارد کردن کلمه عبور کاربر اصلی در کادر محاوره‌ای فوق، کادر محاوره‌ای دیگری با عنوان Root Password مطابق شکل ۲۸-۱۹ به نمایش درآمده و امکان تغییر کلمه عبور کاربر اصلی را در اختیار قرار خواهد داد. بدیهی است که طی دفعات بعدی ورود به سیستم، کاربر اصلی باید از کلمه عبور جدید استفاده کند. (چنان‌چه به عنوان کاربر اصلی برای ورود به سیستم اقدام کرده باشید، کادر محاوره‌ای شکل ۲۷-۱۹ نمایش داده نشده و تنها کادر محاوره‌ای Root Password جهت تغییر کلمه عبور کاربر اصلی در اختیار قرار خواهد گرفت.)

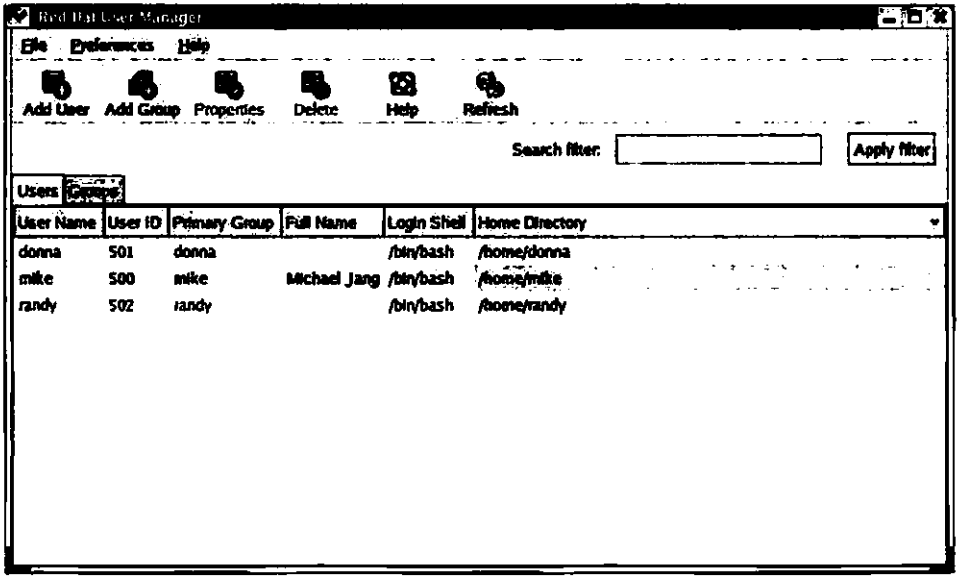


شکل ۲۸-۱۹ کادر محاوره‌ای Root Password

مدیریت کاربران

ابزار گرافیکی redhat-config-users به منظور مدیریت کاربران و گروه‌ها طراحی شده است. (برای اطلاع از فایل‌های پیکربندی مربوطه به فصل نهم مراجعه کنید.)

دسترسی به این ابزار با انتخاب گزینه Users and Groups از منوی فرعی System Settings واقع در منوی اصلی امکان‌پذیر است. شکل ۲۹-۱۹ پنجره این ابزار با عنوان Red Hat User Manager را نشان می‌دهد.

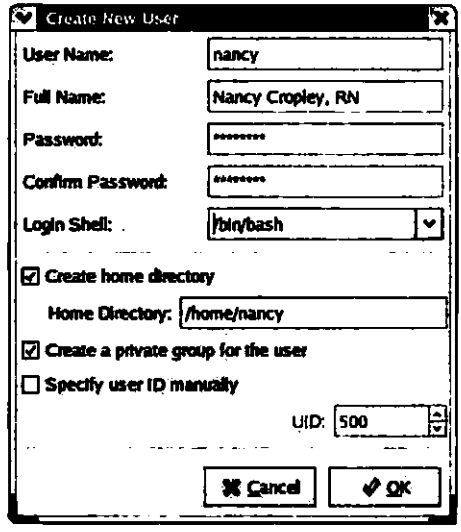


شکل ۲۹-۱۹ پنجره Red Hat User Manager

چنان‌که مشاهده می‌کنید، پنجره مذکور از دو بخش Users و Groups تشکیل شده است. بخش Users مشخصات کاربران موجود را با توجه به محتوای فایل /etc/passwd در اختیار می‌گذارد. در صورت اطلاع از ساختار این فایل، مطمئناً با مفاهیم مندرج در بخش Users نیز آشنا خواهید بود. برای اضافه کردن کاربر جدید روی دکمه Add User کلیک کنید تا به این ترتیب کادر محاوره‌ای Create New User مطابق شکل ۳۰-۱۹ باز شده و امکانات موردنیاز را در اختیار قرار دهد.

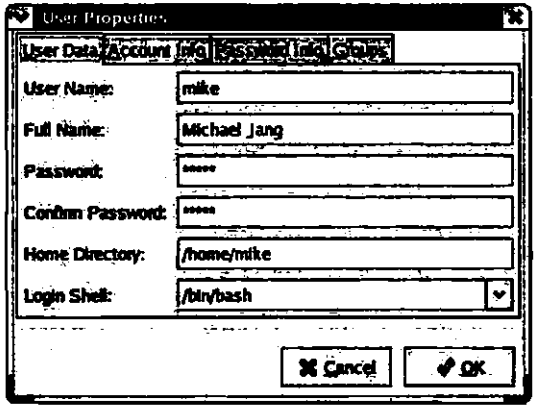
در کادر محاوره‌ای مذکور می‌توانید اطلاعات کاربر جدید از جمله کلمه عبور موردنیاز برای دسترسی به سیستم را وارد کنید. تخصیص شناسه User ID به کاربر جدید با توجه به شناسه‌های موجود به طور

خودکار انجام می‌شود. با وجود این، در صورت فعال کردن گزینه Specify User ID Manually می‌توانید این شناسه را به طور دستی در فیلد UID وارد کنید.



شکل ۳۰-۱۹ کادر محاوره‌ای Add New User

علاوه بر اطلاعات فوق، در صورت تمایل می‌توانید اطلاعات دیگری را نیز در مورد هریک از کاربران در اختیار سیستم قرار دهید. برای این منظور سطر حاوی اطلاعات کاربر موردنظر خود را از بخش Users انتخاب کرده و سپس روی دکمه Properties کلیک کنید. با این اقدام کادر محاوره‌ای User Properties مطابق شکل ۳۱-۱۹ باز می‌شود.



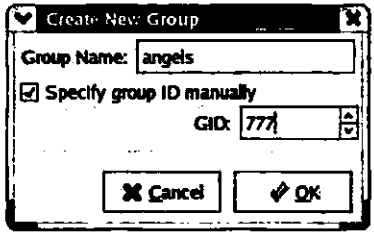
شکل ۳۱-۱۹ کادر محاوره‌ای User Properties

امکانات موجود در این کادر محاوره‌ای در قالب چهار بخش مختلف به شرح جدول ۵-۱۹ دسته‌بندی شده است.

جدول ۵-۱۹ شرح امکانات موجود در بخش‌های مختلف کادر محاوره‌ای User Properties

عنوان بخش	توضیح
User Data	این بخش امکان درج اطلاعات اصلی درباره کاربر موردنظر را در اختیار می‌گذارد. اطلاعات مندرج در این بخش در دو فایل /etc/passwd و /etc/shadow ذخیره می‌شود.
Account Info	این‌بخش امکان قفل کردن یا تعیین مدت اعتبار حساب کاربری موردنظر را در اختیار می‌گذارد. اطلاعات مندرج در این بخش در فایل /etc/shadow ذخیره می‌شود.
Password Info	این بخش امکان تنظیم پارامترهای مربوط به انقضای اعتبار حساب کاربری موردنظر را در اختیار می‌گذارد. اطلاعات مندرج در این بخش در فایل /etc/shadow ذخیره می‌شود.
Group	این بخش امکان تنظیمات مربوط به عضویت کاربر موردنظر را در گروه‌های موجود در اختیار می‌گذارد. اطلاعات مندرج در این بخش در قالب فایل /etc/group ذخیره می‌شود.

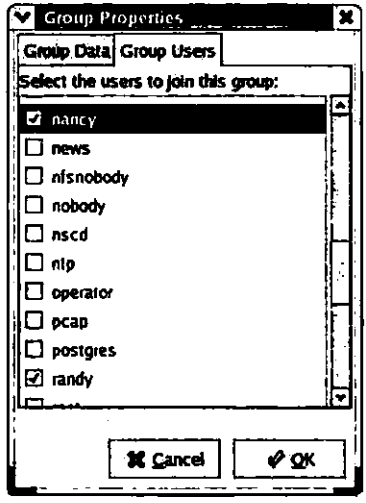
پس از انجام تنظیمات مورد نظر، جهت دستیابی مجدد به پنجره Red Hat User Manager روی دکمه OK از کادر محاوره‌ای User Properties کلیک کنید. بخش Groups از این پنجره مشخصات گروه‌های موجود را با توجه به محتوای فایل /etc/group در اختیار می‌گذارد. برای ایجاد گروه جدید روی دکمه Add Group کلیک کنید. با این اقدام کادر محاوره‌ای Create New Group مطابق شکل ۳۲-۱۹ باز می‌شود.



شکل ۳۲-۱۹ کادر محاوره‌ای Creating New Group

به طور پیش‌فرض، هر کاربری عضو گروهی هم‌نام با شناسه کاربری خود و با شناسه‌ای مشابه شناسه کاربری خود است. برای مثال، کاربری با عنوان donna و شناسه 501 در گروهی با همین عنوان و همین شناسه عضویت دارد. (این مکانیزم با عنوان User Private Group در فصل نهم مورد بررسی قرار گرفته است.)

با وجود این بهتر است شناسه گروه‌های جدید را از بازه کاملاً متفاوتی با شناسه کاربران انتخاب کنید. تنظیمات شکل ۳۲-۱۹ مربوط به تعریف گروه جدیدی با عنوان angles و شناسه 777 است. پس از ایجاد این گروه، با کلیک دکمه Properties از بخش Group واقع در پنجره Red Hat User Manager و دستیابی به کادر محاوره‌ای Group Properties می‌توان کاربران موردنظر را به عضویت این گروه جدید درآورد. شکل ۳۳-۱۹ اقدام مدیر سیستم برای عضویت دو کاربر nancy و randy در گروه موردنظر را نشان می‌دهد.



شکل ۳۳-۱۹ با تنظیمات موجود در بخش Group Users از کادر محاوره‌ای Group Properties می‌توان کاربران موردنظر را به عضویت یک گروهی درآورد.

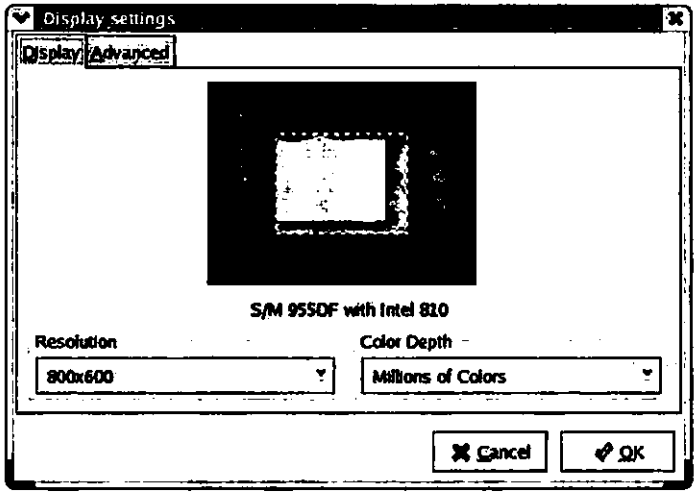
پیکربندی رابط گرافیکی کاربر

ابزار گرافیکی redhat-configxfree86 که قبلاً در فصل پانزدهم مورد بررسی قرار گرفت، به منظور پیکربندی بخش کلاینت از زیرسیستم گرافیکی X Window طراحی شده است. برای دسترسی به این ابزار، گزینهDisplay از منوی فرعی System Settings واقع در منوی اصلی را انتخاب کنید. با این اقدام پنجره‌ای مطابق شکل ۳۴-۱۹ با عنوان Display Settings به نمایش درمی‌آید.

در بیشتر موارد، حتی اگر ضمن نصب سیستم‌عامل Red Hat Linux نرم‌افزارهای گرافیکی را جهت نصب روی کامپیوتر میزبان انتخاب نکرده باشید، می‌توانید ابزار redhat-config-xfree86 را از طریق سطر فرمان مورد دستیابی قرار دهید. نتیجه تنظیمات انجام شده با این ابزار در فایل /etc/X11/XF86Config ذخیره می‌شود. چنان‌چه تا به حال ابزار redhat-config-xfree86 را جهت

پیکربندی زیرسیستم X Window مورد استفاده قرار داده باشید، این توضیح را در ابتدای فایل مذکور مشاهده خواهید کرد:

```
# XFree86 4 configuration created by redhat-config-xfree86
```



شکل ۳۴-۱۹ کادر محاوره‌ای Display Settings

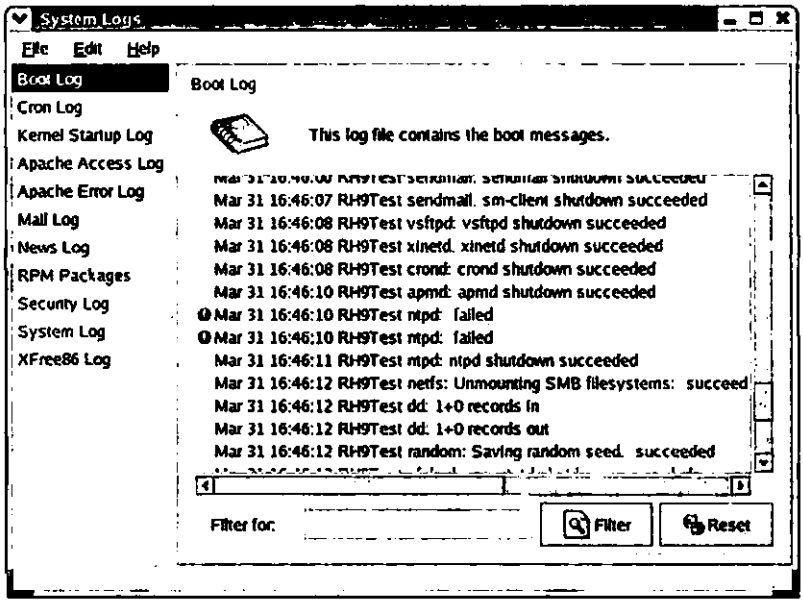
اما در صورتی که پیکربندی زیرسیستم گرافیکی X Window را ضمن نصب سیستم‌عامل Red Hat Linux انجام داده باشید، اکنون این عبارت در ابتدای فایل /etc/X11/XF86Config درج شده است:

```
# XFree86 4 configuration created by pyxf86config
```

فایل‌های ثبت وقایع

ابزار گرافیکی redhat-logviewer به منظور بازبینی وقایع سیستمی ثبت شده در قالب فایل‌های مختلف طراحی شده است. برای دسترسی به این ابزار گزینه System Logs از منوی فرعی System Tools واقع در منوی اصلی را انتخاب کنید. شکل ۳۵-۱۹ پنجره ابزار مورد بحث با عنوان System Logs را نشان می‌دهد.

با انتخاب هریک از موارد موجود در قاب سمت چپ این پنجره می‌توان وقایع مربوطه را در قاب سمت راست آن مشاهده کرد. برای مثال، چنان‌که در وقایع مربوط به راه‌اندازی سیستم (Boot Log) مشاهده می‌کنید، وجود علامت ! و پیغام خطای "failed" در مورد سرویس ntpd (اصطلاحاً Network Time Protocol) حاکی از وقوع نوعی خطا در راه‌اندازی این سرویس است.



شکل ۳۵-۱۹ پنجره System Logs

با استفاده از امکانات موجود در این پنجره می‌توان به جستجوی پیغام‌های موردنظر پرداخت. برای این منظور کافی است عبارت مورد جستجوی خود را در فیلد متنی Filter For وارد کرده و کلید Enter را فشار دهید تا به این ترتیب تنها پیغام‌های مربوط به آن موضوع به نمایش درآید. این ابزار فرآیند جستجو را با استفاده از برنامه grep انجام می‌دهد.

ابزار redhat-logviewer برای دسترسی به محتوای فایل‌های ثبت وقایع استاندارد پیکربندی شده است. به کمک تنظیمات موجود در کادر محاوره‌ای Preferences که با انتخاب گزینه‌ای به همین نام از منوی Edit امکان‌پذیر است، می‌توان فایل‌های دیگری را برای این منظور انتخاب کرد.

جدول ۶-۱۹ حاوی عناوین گزینه‌های مربوط به وقایع استاندارد و فایل‌هایی است که جزییات مربوطه در آن‌ها به ثبت می‌رسد.

جدول ۶-۱۹ عناوین گزینه‌های مربوط به وقایع استاندارد و فایل‌های حاوی جزییات آن‌ها

عنوان گزینه	فایل مربوطه
Boot	/var/log/boot.log
Cron	/var/log/cron
Kernel Startup	/var/log/dmesg

عنوان گزینه	فایل مربوطه
Apache Access	/var/log/httpd/access_log
Apache Error	/var/log/httpd/error_log
Mail	/var/log/maillog
News	/var/log/spooler
RPM Packages	/var/log/rpmpkgs
Security	/var/log/secure
System	/var/log/messages
XFree86	/var/log/XFree86.0.log

چنان‌چه گزینه‌ای از جدول فوق را در لیست موجود از قاب سمت چپ پنجره System Logs مشاهده نمی‌کنید، احتمال زیادی دارد که سرویس مربوطه قبلاً راه‌اندازی نشده یا هنوز مورد دسترسی قرار نگرفته باشد. برای مثال، اگر گزینه Apache Access Log در قاب سمت چپ این پنجره موجود نباشد، می‌توان نتیجه گرفت که وب سرور Apache (سرویس httpd) قبلاً راه‌اندازی نشده یا از زمان راه‌اندازی تاکنون مورد دسترسی قرار نگرفته است.

فونت‌ها

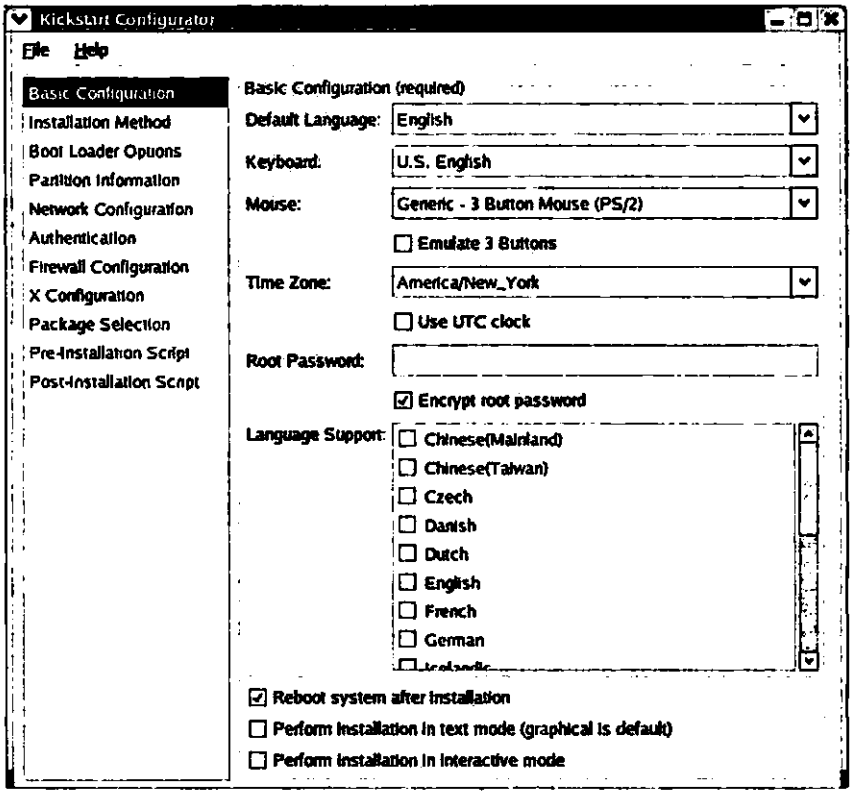
دو ابزار redhat-update-gnome-font-install و redhat-update-gnome-font-install2 به منظور پشتیبانی از چاپ اسناد تولیدی توسط برنامه‌های کاربردی مختلف در محیط گرافیکی GNOME طراحی شده‌اند. هر دو ابزار فوق این فایل‌های پیکربندی را تحت تأثیر قرار می‌دهند:

```
/etc/gnome/fonts/gnome-print-rpm.fontmap
/etc/gnome/libgnomeprint-2.0/fonts/libgnomeprint-rpm.fontmap
```

فایل Kickstart

ابزار گرافیکی redhat-config-kickstart به منظور پیکربندی مکانیزمی با عنوان Kickstart جهت مکانیزه کردن فرآیند نصب سیستم‌عامل Red Hat Linux طراحی شده است. (برای توضیح بیشتر در این زمینه به فصل پنجم مراجعه کنید.) دسترسی به این ابزار با انتخاب گزینه Kickstart از منوی فرعی System Tools واقع در منوی اصلی امکان‌پذیر است. شکل ۳۶-۱۹ پنجره مربوط به این ابزار با عنوان Kickstart Configuration را نشان می‌دهد.

فایل حاصل از این پیکربندی با عنوان ks.cfg ذخیره می‌شود. نمونه‌ای از فایل‌های Kickstart تحت عنوان /root/anaconda-ks.cfg موجود است.

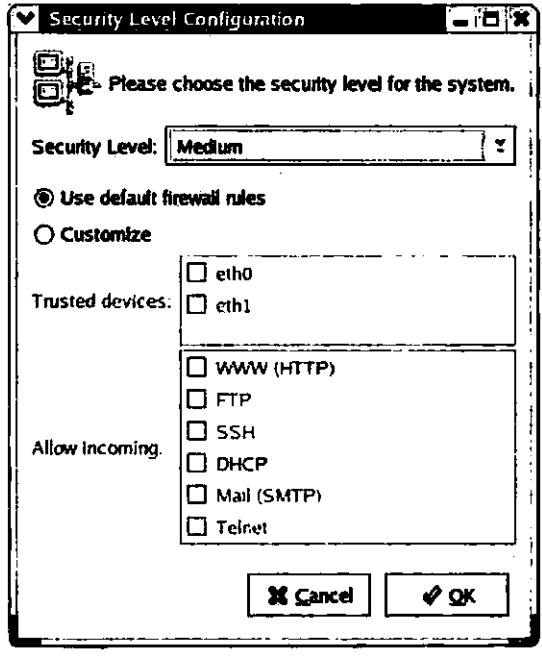


شکل ۳۶-۱۹ پنجره Kickstart Configuration

سطوح امنیتی

ابزار گرافیکی redhat-config-securitylevel به منظور تنظیم عملکرد مکانیزم بازدارنده دیوار آتش طراحی شده است. (این ابزار را در فصول سوم و چهارم در قالب فرآیند نصب سیستم‌عامل Red Hat Linux مورد استفاده قرار داده‌اید.) دسترسی به این ابزار با انتخاب گزینه Security Level از منوی فرعی System Settings واقع در منوی اصلی امکان‌پذیر است. شکل ۳۷-۱۹ پنجره این ابزار با عنوان Security Level Configuration را نشان می‌دهد.

این ابزار امکان تنظیم شدت بازدارندگی مکانیزم دیوار آتش را در سه سطح مختلف با عناوین High، Medium و None در اختیار می‌گذارد. (انتخاب سطح None به معنی عدم استفاده از قابلیت‌های بازدارندگی این مکانیزم است.)



شکل ۳۷-۱۹ پنجره Security Level Configuration

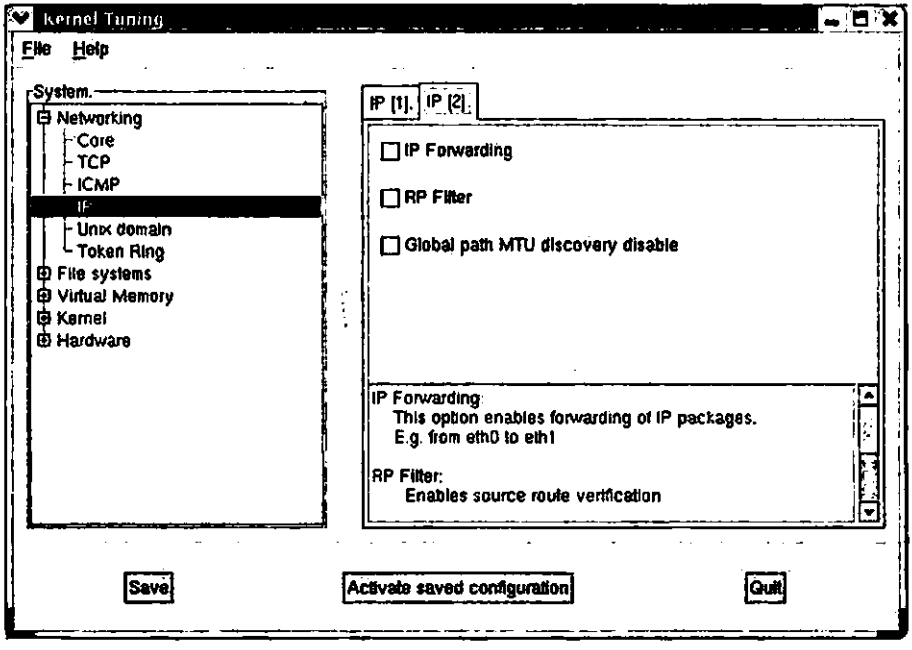
تنظیمات بیشتری را نیز می‌توانید به کمک این ابزار انجام دهید. برای مثال، اگر یکی از کارت‌های شبکه تنها به شبکه محلی متصل باشد، ممکن است مایل باشید تا آن‌را به عنوان نوعی تجهیزات قابل اعتماد (اصطلاحاً trusted device) پیکربندی کنید. چنان‌که می‌دانید، ترافیک عبوری از چنین تجهیزاتی مشمول قوانین بازدارندگی مکانیزم دیوار آتش نمی‌شود. علاوه بر این، در صورت تمایل می‌توانید با انتخاب پروتکل‌های موردنظر از قاب پایینی پنجره شکل ۳۷-۱۹ امکان دریافت داده‌های ارسالی بر اساس آن‌ها را فراهم کنید.

در صورتی که برای پیکربندی مکانیزم بازدارنده دیوار آتش از برنامه iptables استفاده کرده باشید، تنظیماتی که به واسطه ابزار پیکربندی redhat-config-securitylevel انجام می‌دهید در فایل /etc/sysconfig/iptables به ثبت خواهد رسید. (برای اطلاع بیشتر درباره فرامین برنامه iptables به فصل بیست و دوم مراجعه کنید.)

ابزار redhat-config-securitylevel و برنامه lokkit (که پیشتر در فصل شانزدهم مورد بررسی قرار گرفت.) از این نظر که هر دو به واسطه پارامترهای مشابه امکان پیکربندی مکانیزم دیوار آتش را در اختیار می‌گذارند، بسیار شبیه به یکدیگر هستند.

پیکربندی هسته سیستم‌عامل Linux

ابزار گرافیکی redhat-config-proc به منظور ویرایش تنظیمات موجود در فهرست proc/ طراحی شده است. در فصل یازدهم برخی از فایل‌های موجود در این فهرست را به طور اجمالی مورد بررسی قرار دادیم. برای دسترسی به این ابزار می‌توانید فرمانی به همین نام را در سطر فرمان محیط گرافیکی مورد استفاده اجرا کنید. (دسترسی به این ابزار از طریق منوی اصلی محیط گرافیکی امکان‌پذیر نیست.) شکل ۳۸-۱۹ پنجره مربوط به این ابزار با عنوان Kernel Tuning را نشان می‌دهد.



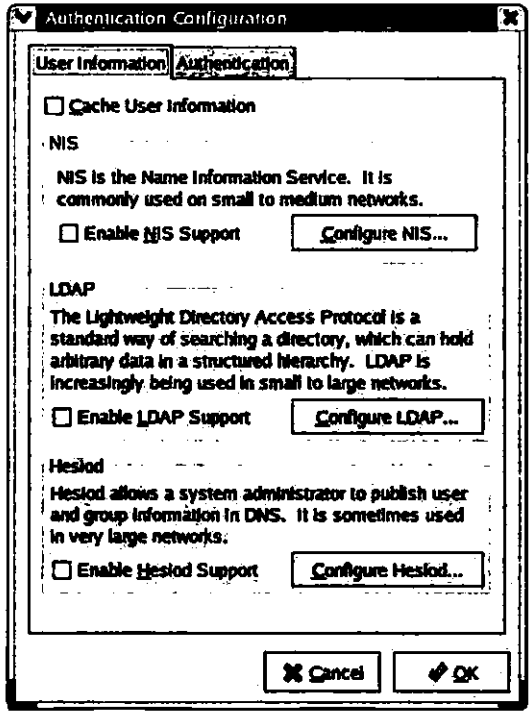
شکل ۳۸-۱۹ پنجره Kernel Tuning

در استفاده از ابزار redhat-config-proc کاملاً احتیاط کنید. پیش از هر اقدامی دست کم از فایل پیکربندی sysctl.conf/، یک نسخه پشتیبان تهیه کرده و آن‌را در جای مطمئنی نگهداری کنید. هر نوع تنظیم نامطلوبی که عملکرد هسته را تحت تأثیر قرار دهد می‌تواند به عدم توانایی سیستم‌عامل در سرویس‌دهی منجر شود.

چنان‌که مشاهده می‌کنید، این تنظیمات امکان برخورداری از مکانیزم IP Forwarding را نیز در اختیار می‌گذارد. (به واسطه این مکانیزم، می‌توان کامپیوترهای Linux را به عنوان دروازه میان دو یا چند شبکه پیکربندی کرد.) تنظیمات انجام شده از طریق این ابزار در فایل پیکربندی /etc/sysctl.conf ذخیره می‌شود.

احراز هویت

ابزار authconfig-gtk به منظور پیکربندی بانک اطلاعاتی حاوی اسامی کاربران و کلمات عبور مربوطه طراحی شده است. در واقع این ابزار را ضمن نصب سیستم‌عامل Red Hat Linux در فصول سوم و چهارم مورد استفاده قرار دادید. برای دسترسی به آن، گزینه Authentication را از منوی فرعی System Settings واقع در منوی اصلی انتخاب کنید. شکل ۳۹-۱۹ پنجره این ابزار با عنوان Authentication Configuration را نشان می‌دهد.



شکل ۳۹-۱۹ پنجره Authentication Configuration

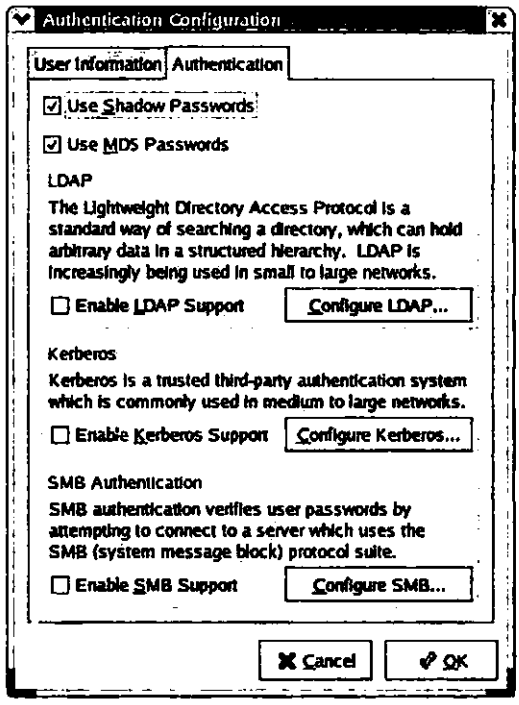
بسته به شیوه نصب سیستم‌عامل Red Hat Linux، هم‌اینک ممکن است به این ابزار دسترسی داشته باشید. (برای اطلاع بیشتر در این زمینه به فصول سوم و چهارم مراجعه کنید.) در این قسمت کلیه تنظیمات ابزار authconfig-gtk را مورد بررسی قرار می‌دهیم. جدول ۷-۱۹ تنظیمات بخش User Information از پنجره Authentication Configuration را به طور مختصر شرح می‌دهد.

جدول ۷-۱۹ شرح تنظیمات موجود در بخش User Information

عنوان تنظیمات	توضیح
Cache User Information	این گزینه امکان ثبت اطلاعات کاربر را روی سرور محلی در اختیار می‌گذارد.
Enable NIS Support	این گزینه امکان احراز هویت را از طریق سرویس NIS در اختیار می‌گذارد.
Configure NIS	این‌گزینه امکان تعیین‌نام کامپیوتر میزبان سرور NIS و حوزه میزبان آن کامپیوتر را در اختیار می‌گذارد.
Enable LDAP Support	این گزینه امکان احراز هویت را از طریق مکانیزم LDAP یا اصطلاحاً Lightweight Directory Assistance Protocol در اختیار می‌گذارد.
Configure LDAP	این گزینه امکان تعیین نام کامپیوتر میزبان سرور LDAP و بانک اطلاعاتی مورد استفاده آن و هم‌چنین امکان استفاده از مکانیزم TLS (اصطلاحاً Transmission Layer Security) را که در واقع عنوان دیگر پروتکل Secure Socket Layer یا به اختصار SSL است، در اختیار می‌گذارد.
Hesiod	این‌گزینه امکان تعیین‌نام کامپیوتر میزبان‌سرور DNS و حوزه میزبان آن کامپیوتر را در اختیار می‌گذارد.
Configure Hesiod	این گزینه امکان تعیین مقادیر پارامترهایی از حمله Hesiod LHS و Hesiod RHS را که به ترتیب بیانگر بخش ابتدایی و انتهایی نام حوزه میزبان سرور DNS هستند، در اختیار می‌گذارد. برای مثال، در مورد نام حوزه میزبان nameserve.mommabears.com مقادیر این دو پارامتر به ترتیب بیانگر عبارت nameserv و mommabears.com خواهد بود.

شکل ۴۰-۱۹ امکانات پیکربندی موجود در بخش Authentication از پنجره مورد بحث را نشان می‌دهد. جدول ۸-۱۹ حاوی شرح مختصری درباره این تنظیمات است.

تنظیمات انجام شده از طریق ابزار authconfig-gtk در فایل پیکربندی /etc/sysconfig/authconfig به ثبت می‌رسد.



شکل ۴۰-۱۹ تنظیمات بخش Authentication از پنجره Authentication Configuration

جدول ۸-۱۹ تنظیمات بخش Authentication

عنوان گزینه	توضیح
Enable LDAP Support	این گزینه امکان احراز هویت را از طریق مکانیزم LDAP یا اصطلاحاً Lightweight Directory Assistance Protocol در اختیار می‌گذارد.
Configure LDAP	این گزینه امکان تعیین نام کامپیوتر میزبان سرور LDAP و بانک اطلاعاتی مورد استفاده آن و هم‌چنین امکان استفاده از مکانیزم TLS (اصطلاحاً Transmission Layer Security) را که در واقع عنوان دیگر پروتکل Secure Socket Layer یا به اختصار SSL است، در اختیار می‌گذارد.
Use Shadow Passwords	این گزینه امکان استفاده از مکانیزم Shadow Password Suite را به واسطه محافظت از حساب کاربران، کلمات عبور و اطلاعات گروه‌ها در قالب فایل‌های /etc/shadow و /etc/gshadow در اختیار می‌گذارد.
Use MD5 Passwords	این گزینه امکان استفاده از مکانیزم رمزگذاری MD5 را به منظور محافظت از کلمات عبور در اختیار می‌گذارد.

عنوان گزینه	توضیح
Enable Kerberos Support	این گزینه امکان استفاده از یک مکانیزم رمزگذاری پیچیده با عنوان Kerberos را که به منظور محافظت از کلمات عبور و سایر اطلاعات محرمانه (از جمله اعتبارنامه‌ها) تهیه شده است، در اختیار می‌گذارد. این مکانیزم محصول تلاش محققان انستیتو تکنولوژی ماساچوست در ایالات متحده است.
Configure Kerberos	این گزینه امکان تنظیمات مختلف مکانیزم Kerberos از جمله تعیین نام حوزه میزبان سرور Kerberos، مقدار پارامتر KDC یا اصطلاحاً Kerberos Domain Controller (که بیانگر نام کامپیوتر میزبان سرور Kerberos است) و پورت TCP/IP مربوطه یعنی ۸۸، و تعیین مشخصات سرورهایی را که از طریق پورت شماره ۴۷۹ امکان مدیریت سرور Kerberos را در اختیار می‌گذارند، فراهم می‌کند.
Enable SMB Support	این گزینه امکان احراز هویت را از طریق کامپیوترهای ویندوز یا کامپیوترهای میزبان سرور Samba که در شبکه‌ای از نوع ویندوز مستقر شده‌اند، در اختیار می‌گذارد.
Configure SMB	این گزینه امکان تعیین نام گروه کاری یا کنترل کننده حوزه را در شبکه‌های ویندوز فراهم می‌کند.

برای پیکربندی Kerberos 5 روی کامپیوتر موردنظر ابتدا باید ساعت آن کامپیوتر را با کامپیوتری که میزبانی سروری از نوع NTP را به عهده دارد، هماهنگ کنید. برای این منظور می‌توانید از ابزار پیکربندی redhat-time-config که پیشتر به بررسی آن پرداختیم، استفاده کنید.

نسخه متنی ابزار Authentication Configuration متشکل از دو صفحه متنی است که می‌توانید تنظیمات موجود در دو بخش User Information و Authentication از پنجره ابزار گرافیکی مشابه را از طریق آن‌ها انجام دهید. برای دسترسی به نسخه متنی کافی است فرمان authconfig را اجرا کنید.

ابزارهای پیکربندی سرویس‌ها

شرکت Red Hat مجموعه‌ای از ابزارهای گرافیکی را به منظور انجام وظایف مدیریتی روزمره در ارتباط با سرویس‌های مختلف سیستم‌عامل Linux از جمله سطوح اجرایی، چاپگرها، پست الکترونیکی و سرویس‌های مشابه طراحی شده است. شرح مختصری از کاربرد این ابزارها در جدول ۹-۱۹ آمده است.

جدول ۹-۱۹ ابزارهای پیکربندی سرویس‌های سیستم‌عامل Red Hat Linux

عنوان ابزار	توضیح
redhat-config-service	این ابزار به منظور راه‌اندازی سرویس‌ها را در سطوح اجرایی مختلف طراحی شده است.
redhat-config-printer	این ابزار به منظور پیکربندی چاپگرهای LPD و CUPS طراحی شده است.
redhat-config-printer-tui	این ابزار نسخه متنی ابزار گرافیکی redhat-config-printer است.
redhat-switch-printer	این ابزار به منظور سوییچ کردن از سیستم چاپ LPD به CUPS طراحی شده است.
redhat-switch-printer-nox	این ابزار نسخه متنی ابزار گرافیکی redhat-switch-printer است.
redhat-switch-mail	این ابزار به منظور سوییچ کردن از یک سرور پست الکترونیکی به دیگری طراحی شده است.
switchdesk	این ابزار جهت سوییچ کردن به محیط گرافیکی پیش‌فرض طراحی شده است.

راه‌اندازی سرویس‌ها در سطوح اجرایی مختلف

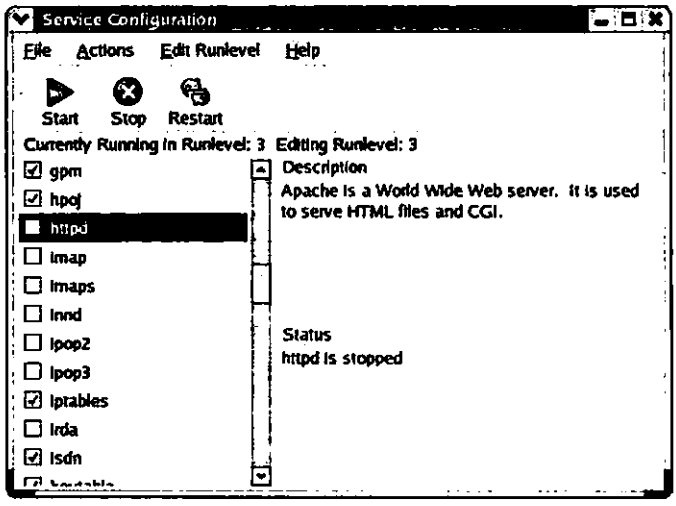
ابزار گرافیکی redhat-config-service جهت مدیریت سرویس‌ها و راه‌اندازی آن‌ها در سطوح اجرایی مختلف طراحی شده است. بخشی از قابلیت‌های این ابزار شامل امکاناتی است که برنامه chkconfig در اختیار می‌گذارد. (جهت اطلاع از امکانات این برنامه به فصل سیزدهم مراجعه کنید.) دسترسی به این ابزار با انتخاب گزینه Services از منوی فرعی Server Settings واقع در منوی فرعی System Settings از منوی اصلی امکان‌پذیر است. شکل۴۱-۱۹ پنجره این ابزار را با عنوان Service Configuration نشان می‌دهد.

به محض انتخاب گزینه فوق پنجره Service Configuration باز شده و سرویس‌های مربوط به سطح اجرایی پیش‌فرض (با توجه به تنظیمات موجود در فایل پیکربندی /etc/inittab) به نمایش درمی‌آید. هم‌چنین با کلیک روی سرویس موردنظر در قاب سمت چپ این پنجره، توضیحات مربوطه و وضعیت فعلی آن در قاب‌های سمت راست نمایش داده می‌شود.

با انتخاب گزینه‌های Start، Stop و Restart منوی Actions می‌توان به ترتیب برای راه‌اندازی، توقف و راه‌اندازی مجدد سرویس موردنظر اقدام کرد. تأثیر انتخاب گزینه‌های فوق معادل اجرای این فرامین است:

```
# service servicename start
# service servicename stop
```

```
# service servicename restart
```

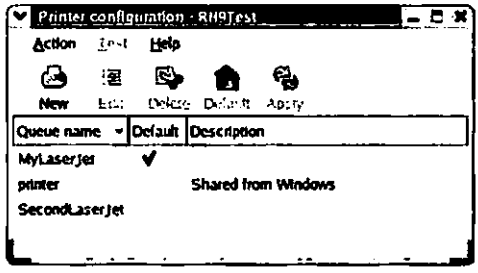


شکل ۴۱-۱۹ پنجره Service Configuration

منوی Edit Runlevel امکان دسترسی به سرویس‌هایی را که در سطوح اجرایی سوم، چهارم و پنجم به اجرا درمی‌آیند، فراهم می‌کند. نتیجه تنظیمات نهایی در قالب فایلی با عنوان عمومی /etc/rc.d/rc*n*.d که در آن متغیر *n* بیانگر سطح اجرایی موردنظر است، به ثبت می‌رسد. در این فایل پیکربندی به هر سرویس فعال، یکسری دستورالعمل‌های راه‌انداز و به هرسرویس غیرفعال یکسری دستورالعمل بازدارنده منسوب می‌شود. به این ترتیب، طی دفعات آتی راه‌اندازی کامپیوتر، سیستم‌عامل Linux با مراجعه به دستورالعمل‌های مذکور می‌تواند در مورد راه‌اندازی سرویس‌های مختلف تصمیم‌گیری کند. (برای اطلاع بیشتر درباره سطوح اجرایی و نحوه راه‌اندازی یا توقف سرویس‌ها به فصل سیزدهم مراجعه کنید.)

پیکربندی چاپگر

ابزار گرافیکی redhat-config-printer به منظور پیکربندی چاپگر طراحی شده است. این ابزار در واقع یک رابط گرافیکی برای ویرایش فایل پیکربندی سرویس LPD یا CUPS است. (برای اطلاع درباره این سرویس‌ها به فصل بیست و پنجم مراجعه کنید.) دسترسی به این ابزار با انتخاب گزینه Printing از منوی فرعی System Settings واقع در منوی اصلی امکان‌پذیر است. شکل ۴۲-۱۹ پنجره این ابزار را با عنوان Printer Configuration نشان می‌دهد.

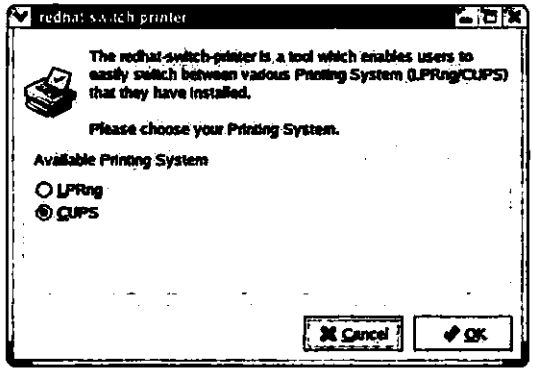


شکل ۴۲-۱۹ پنجره Printer Configuration

علاوه بر این، با اجرای مستقیم فرمان redhat-config-printer در سطر فرمان محیط گرافیکی مورد استفاده نیز می‌توانید به این ابزار دسترسی پیدا کنید. ضمناً نسخه متنی ابزار مورد بحث با اجرای فرمان redhat-config-printer-tui قابل دستیابی است. (برای اطلاع بیشتر درباره کاربردها و قابلیت‌های این ابزار به فصل بیست و پنجم مراجعه کنید.)

سوییچ کردن بین سرویس‌های چاپ

چنان‌که در فصل بیست و پنجم نیز توضیح داده شد، دو سرویس LPD و CUPS متداول‌ترین سرویس‌های چاپ در سیستم‌عامل Linux محسوب می‌شوند. ابزار گرافیکی redhat-switch-printer به منظور سوییچ کردن بین این دو سرویس چاپ طراحی شده است. در صورتی که هر دو سرویس فوق را روی کامپیوتر میزبان نصب و پیکربندی کرده باشید، با استفاده از ابزار نامبرده همواره می‌توانید یکی از این دو سرویس را به عنوان سرویس چاپ فعال انتخاب کنید. برای دسترسی به این ابزار گزینه Printer System Switcher را از منوی فرعی More system Settings واقع در منوی فرعی System Settings از منوی اصلی انتخاب کنید. شکل ۴۳-۱۹ پنجره این ابزار را نشان می‌دهد.

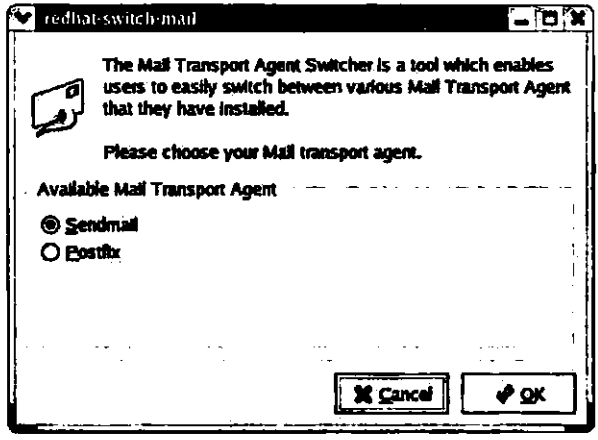


شکل ۴۳-۱۹ پنجره ابزار redhat-switch-printer

نسخه متنی این ابزار با اجرای فرمان redhat-switch-printer-nox قابل دستیابی است. نتیجه تنظیمات انجام شده توسط این ابزار موجب راه‌اندازی یکی از دو سرویس چاپ LPD یا CUPS در سطح اجرایی موردنظر می‌شود.

سوییچ کردن بین سرویس‌های پست الکترونیکی

چنان‌که از فصل بیست و پنجم به یاد دارید، سرویس‌های پست الکترونیکی متعددی به همراه سیستم‌عامل Red Hat Linux عرضه می‌شود. ابزار redhat-switch-mail به منظور سوییچ کردن بین این سرویس‌ها طراحی شده است. در صورتی که بیش از یک سرویس پست الکترونیکی را روی کامپیوتر میزبان نصب و پیکربندی کرده باشید، با استفاده از ابزار نامبرده همواره می‌توانید یکی از این سرویس‌ها را به عنوان سرویس پست الکترونیکی فعال انتخاب کنید. نتیجه تنظیمات انجام شده توسط این ابزار موجب راه‌اندازی سرویس پست الکترونیکی منتخب در سطح اجرایی موردنظر می‌شود. تا زمان انتشار کتاب حاضر دسترسی به این ابزار از طریق منوی اصلی امکان‌پذیر نبوده و اجرای مستقیم فرمان redhat-switch-mail تنها راه دسترسی به ابزار مورد بحث است. شکل ۴۴-۱۹ پنجره این ابزار را نشان می‌دهد.

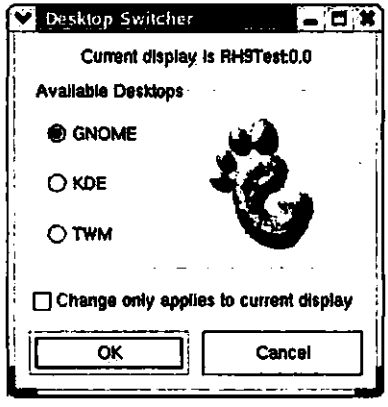


شکل ۴۴-۱۹ پنجره ابزار redhat-switch-mail

سوییچ کردن بین محیط‌های گرافیکی

چنان‌که از فصل پانزدهم به یاد دارید، محیط‌های گرافیکی متعددی از جمله GNOME، KDE و twm در سیستم‌عامل Red Hat Linux قابل دستیابی است. ابزار switchdesk به منظور سوییچ کردن بین محیط‌های گرافیکی طراحی شده است. در صورتی که روی کامپیوتر میزبان بیش از یک محیط گرافیکی

پیکربندی شده باشد، با استفاده از این ابزار می‌توانید بین آن‌ها سوییچ کنید. (محیط گرافیکی پیش‌فرض هر کاربر در فایل ~/.Xclients-default از فهرست خانگی وی ثبت شده است.) دسترسی به این ابزار با انتخاب Desktop Switching Tool از منوی فرعی More System Settings واقع در منوی فرعی System Settings از منوی اصلی امکان‌پذیر است. شکل ۴۵-۱۹پنجره این ابزار را با عنوان Desktop Switcher نشان می‌دهد.



شکل ۴۵-۱۹ پنجره Desktop Switcher

جمع‌بندی

در این فصل ابزارهای گرافیکی طراحی شده توسط شرکت Red Hat به منظور پیکربندی سیستم‌عامل Red Hat Linux را مورد بررسی قرار دادیم. بیشتر این ابزارها با اجرای فرامینی به همان نام قابل دستیابی هستند. عناوین اغلب این ابزارها با عبارت redhat-config- آغاز می‌شود.

ابزارهای گرافیکی در واقع چیزی بیش از رابط گرافیکی فرامین موجود نیستند. این ابزارها امکان ویرایش فایل‌های پیکربندی مختلف را از طریق یک رابط گرافیکی در اختیار قرار می‌دهند. با وجود این، نمی‌توان مقادیر تمام پارامترهای پیکربندی را از طریق این گونه ابزارها ویرایش کرد. در حال حاضر کار روی این ابزارها ادامه دارد. از این‌رو، پس از استفاده از آن‌ها محتوای فایل‌های پیکربندی ویرایش شده را جهت اطمینان از حصول نتیجه مطلوب به دقت مورد بررسی قرار دهید.

از طرف دیگر، ابزارهای گرافیکی امکان بسیار مناسبی برای کاربران کم‌تجربه Linux محسوب می‌شوند. مدیران سیستم‌ها می‌توانند تنظیمات موردنظر خود را با استفاده از این ابزارها انجام داده و نتایج تغییرات را در فایل‌های پیکربندی مربوطه مشاهده کنند.

در این فصل بررسی ابزارهای گرافیکی را در قالب چهار گروه مختلف انجام دادیم. ابزارهای پیکربندی تنظیمات اولیه جهت انجام تنظیمات مربوط به ساعت سیستم، صفحه کلید، زبان سیستم، ماوس و کارت صوتی طراحی شده‌اند. ابزارهای پیکربندی شبکه به منظور انجام تنظیمات کارت‌های شبکه، وب سرور Apache و سرویس‌هایی چون DNS، NFS و Samba طراحی شده‌اند.

ابزارهای مدیریت سیستم به منظور نصب و حذف بسته‌های نرم‌افزاری، تغییر کلمه عبور کاربر اصلی، مدیریت‌گروه‌ها و کاربران، پیکربندی محیط گرافیکی، بازبینی وقایع سیستمی، نصب فونت‌ها، پیکربندی فایل Kickstart (جهت مکانیزه کردن فرآیند نصب سیستم‌عامل Red Hat Linux)، پیکربندی مکانیزم بازدارنده دیوار آتش و پیکربندی هسته سیستم‌عامل طراحی شده‌اند. ابزارهای پیکربندی سرویس‌ها نیز جهت کنترل سرویس‌ها و راه‌اندازی آن‌ها در سطوح اجرایی مختلف، سوییچ کردن بین سرویس‌های چاپ و سرویس‌های پست الکترونیکی موجود و هم‌چنین سوییچ کردن بین محیط‌های گرافیکی مختلف طراحی شده‌اند.

در فصل بعد به بررسی قابلیت‌های شبکه در سیستم‌عامل Linux می‌پردازیم. پیش از آغاز این بررسی ابتدا مفاهیم مربوط به پروتکل‌های TCP/IP و آدرس‌های IP را توضیح خواهیم داد. علاوه بر این، به بررسی ابزارهای موردنیاز جهت پیکربندی آدرس‌های IP اختصاصی در شبکه‌های محلی خواهیم پرداخت. با مطالعه فصل بعد آمادگی لازم برای فراگیری مدیریت سیستم‌عامل Linux در شبکه‌های محلی، ایمن‌سازی شبکه‌های Linux و موضوعات مشابه را به دست خواهید آورد.

بخش پنجم

قابلیت‌های سیستم‌عامل Linux در ارتباط با شبکه

اهداف:

- بررسی پروتکل TCP/IP
- مدیریت سیستم‌عامل Linux در یک شبکه محلی
- تأمین امنیت شبکه‌های Linux

فصل بیستم

بررسی پروتکل TCP/IP

اغلب توسعه‌دهندگان سیستم‌عامل UNIX در توسعه شبکه‌ای که امروزه آن‌را با عنوان اینترنت می‌شناسیم، سهیم بوده‌اند. در رسیدن به این هدف، مجموعه‌ای از پروتکل‌های استاندارد با نام TCP/IP طراحی شد. از آن‌جا که سیستم‌عامل Linux نیز از اعضای خانواده سیستم‌عامل UNIX محسوب می‌شود، پروتکل‌های مزبور در قالب این سیستم‌عامل نیز پیاده‌سازی شد. با وجود این، TCP/IP تنها یکی از چند پروتکل مهم مورد استفاده در شبکه‌هاست.

عنوان TCP/IP از دو جزء مهم این پروتکل، یعنی Transport Communications Protocol و Internet Protocol یا به اختصار TCP و IP اقتباس شده است. در واقع TCP/IP مجموعه‌ای متشکل از صدها پروتکل مختلف است. به این دلیل، برای اشاره به آن اغلب از عنوان "مجموعه پروتکلTCP/IP" یا اصطلاحاً TCP/IP Protocol Suite استفاده می‌شود. (جهت سادگی، در فصل حاضر به جای عنوان نسبتاً طولانی فوق از عبارت "پروتکل TCP/IP" استفاده خواهیم کرد. ـ مترجم)

پیش از پرداختن به جزییات پروتکل TCP/IP، اجازه دهید مقداری به عقب بازگشته و اصول شبکه‌ها را در دو مقیاس بزرگ و کوچک به طور مختصر مورد بررسی قرار دهیم. در هر شبکه‌ای به روشی برای شناسایی کامپیوترهای موجود در آن شبکه و شیوه استانداردی برای انتقال داده‌ها نیازمندیم. برای این منظور می‌توان از پروتکل‌های دیگری نیز استفاده کرد. در این فصل به بررسی دو پروتکل موجود در این زمینه یعنی NetBEUI و IPX/SPX نیز خواهیم پرداخت.

پروتکل NetBEUI یا NetBIOS Enhanced User Interface حاصل همکاری مشترک دو شرکت Microsoft و IBM است. عنوان پروتکل IPX/SPX نیز از دو جزء مهم آن یعنی Internetwork Packet Exchange و Sequenced Packet Exchange یا به اختصار IPX و SPX گرفته شده است. مشابه پروتکل TCP/IP، ساختار این پروتکل نیز شامل تعداد قابل توجهی پروتکل مختلف است.

برای آن‌که توسعه دهندگان نرم‌افزار با اطمینان خاطر بیشتری بتوانند به امر پیاده‌سازی این پروتکل‌ها بپردازند باید مشخصات دقیقی از آن‌ها در دسترس باشد. در همین راستا، سازمان استانداردسازی جهانی یا International Organization for Standardization (به اختصار ISO) مدلی متشکل از هفت لایه با

عنوان Open Standards Interconnection یا OSI را به عنوان استانداردی برای پیاده‌سازی شبکه‌ها توسعه داده است.

با وجودی که مدل OSI در اغلب موارد به عنوان مرجع پیاده‌سازی پروتکل TCP/IP مورد استفاده قرار می‌گیرد، برخی از طراحان نرم‌افزار ترجیح می‌دهند از مدل ساده‌تری که تنها شامل چهار لایه است، استفاده کنند.

چنان‌چه به مباحث نظری شبکه علاقه ندارید می‌توانید مستقیماً مبحث مربوط به آدرس‌دهی IP را در انتهای همین فصل مورد مطالعه قرار دهید. برای آدرس‌دهی دو شیوه موجود است. شیوه IPv4 که برای سال‌ها به منظور آدرس‌دهی مورد استفاده قرار می‌گرفته و هم‌اینک نیز یک روش متداول برای انجام این کار محسوب می‌شود. با وجود این، استفاده از شیوه جدیدتر با عنوان IPv6 به تدریج در حال گسترش است. در فصل حاضر این موضوعات را مورد بررسی قرار خواهیم داد:

- بررسی اصول شبکه‌ها
- مجموعه پروتکل‌ها یا protocol stack
- آشنایی با مبانی TCP/IP
- آدرس‌دهی IP

اصول شبکه‌ها

شبکه مجموعه‌ای متشکل از دو یا چند کامپیوتر است که به طریقی می‌توانند با یکدیگر در ارتباط باشند. چنان‌که مشاهده می‌کنید، در تعریف فوق به نحوه ارتباط و رسانه مورد استفاده برای این منظور اشاره‌ای نشده است. از این‌رو، ارتباط بین کامپیوترهای شبکه ممکن است به واسطه کابل‌های موازی، مودم، کارت‌های Ethernet، تجهیزات بی‌سیم یا هر نوع رسانه دیگری که امکان برقراری ارتباط میان کامپیوترها را فراهم می‌کند، برقرار شود. چنان‌چه ارتباط میان کامپیوترهای موردنظر به طور مستقیم یا از طریق نوعی تجهیزات شبکه با عنوان هاب (اصطلاحاً hub) برقرار شود، شبکه حاصل با عنوان شبکه محلی (اصطلاحاً Local Area Network یا LAN) شناخته می‌شود. هر شبکه محلی دارای یک آدرس IP به خصوص با عنوان آدرس شبکه یا network address است.

فاصله بین کامپیوترهای موجود در شبکه‌های محلی، هم‌چون شبکه محلی یک شرکت یا یک ساختمان اداری قابل توجه نیست. اینترنت مجموعه‌ای از دو یا چند شبکه محلی است که به یکدگر متصل شده‌اند. برخی از اینترنت‌ها دارای چنان ابعاد بزرگی هستند که اغلب با عنوان شبکه‌های مقیاس بزرگ (اصطلاحاً Wide Area Network یا WAN) شناخته می‌شوند. در واقع این‌گونه شبکه‌ها متشکل از

شبکه‌های کوچک‌تری هستند که در موقعیت‌های جغرافیایی مجزایی مستقر شده‌اند. چنان‌که می‌دانید بزرگ‌ترین این شبکه‌ها شبکه جهانی اینترنت است.

به هر شبکه یا مجموعه‌ای از شبکه‌ها که مدیریت آن‌ها در قالب یک گروه واحد انجام شود، اصطلاحاً حوزه یا domain گفته می‌شود. برای مثال، می‌توان دو شبکه مجزای linux.sybex.com و windows.sybex.com را در قالب حوزه واحدی با عنوان sybex.com پیکربندی کرد.

شبکه‌های محلی و مقیاس بزرگ

شبکه‌های محلی Linux اغلب بر اساس استاندارد IEEE 802.3 یا اصطلاحاً Ethernet پیاده‌سازی می‌شوند. سرعت انتقال داده‌ها در این نوع شبکه‌ها به مراتب بیشتر از شبکه‌هایی است که بر اساس مودم و خطوط تلفن پیاده‌سازی می‌شوند. در حال حاضر سرعت شبکه‌های Ethernet معادل ۱۰ مگابیت بر ثانیه و نوع به خصوصی از آن با عنوان Fast Ethernet معادل ۱۰۰ مگابیت بر ثانیه است. با وجود این، برخی شرکت‌ها از نوع جدیدی از این شبکه با عنوان Gigabit Ethernet که سرعتی معادل ۱۰۰۰ مگابیت بر ثانیه را در اختیار می‌گذارد، استفاده می‌کنند. علاوه بر این، نوعی شبکه Ethernet با سرعتی معادل ۱۰ گیگابیت بر ثانیه نیز در حال توسعه است.

در واقع Ethernet یک اصطلاح تجاری است. عنوان فنی این‌گونه شبکه‌ها IEEE 802.3 است که توسط انستیتوی مهندسان برق و الکترونیک یا Institute of Electrical and Electronics Engineers پیشنهاد شده است. به طور مشابه، عنوان فنی اصطلاحات تجاری Fast Ethernet و Gigabit Ethernet نیز به ترتیب IEEE 802.3u و IEEE 802.3ae است.

بسته به نوع اتصال میان کامپیوترهای موجود در شبکه‌های Ethernet فاصله بین آن‌ها به چند صد متر محدود شده است. هرچند که شبکه‌های محلی، محدوده کوچکی را تحت پوشش قرار می‌دهند، سرعت انتقال داده‌ها در این گونه شبکه‌ها قابل توجه است. در مقابل، شبکه‌های مقیاس بزرگ به واسطه اتصال میان چندین شبکه محلی، محدوده بزرگی را پوشش می‌دهند، اما سرعت انتقال داده‌ها در آن‌ها به مراتب کمتر از سرعت انتقال داده‌ها در یک شبکه محلی است. سرعت شبکه‌های مقیاس بزرگ به ۱/۴ مگابیت بر ثانیه یا کمتر محدود است.

این محدودیت سرعت با توجه به هزینه صرف شده برای پیاده‌سازی شبکه‌های بزرگ مقیاس متغیر است. سرعت انتقال داده‌ها در ستون فقرات شبکه جهانی اینترنت (که یک شبکه مقیاس بزرگ یا WAN محسوب می‌شود) بالغ بر چندین گیگابیت بر ثانیه است، اما دستیابی به چنین سرعتی مستلزم صرف هزینه بسیار بالایی است. پهنای باند این شبکه مابین مشتریان آن تقسیم می‌شود.

شبکه جهانی اینترنت

حتی اگر تجربه‌ای در نصب و راه‌اندازی شبکه نداشته باشید، به احتمال قوی به واسطه کار با شبکه جهانی اینترنت تجربه کار با یک شبکه را دارید. اغلب کاربران و مدیران سیستم‌عامل Linux برای اتصال به این شبکه از طریق یک مرکز ارایه دهنده خدمات اینترنت یا ISP (اصطلاحاً Internet Service Provider) اقدام می‌کنند. در مورد شبکه‌های بزرگ ممکن است تسهیلاتی مشابه مراکز ارایه دهنده خدامات اینترنت جهت دستیابی مستقیم به اینترنت فراهم شده باشد.

در هر صورت، فرآیند اتصال به شبکه اینترنت از طریق دروازه ISP (اصطلاحاً gateway) انجام می‌شود. دروازه ISP کامپیوتری است که مرکز موردنظر را به شبکه اینترنت متصل می‌کند. هنگامی که نام حوزه‌ای مانند www.mommabears.com را مورد جستجو قرار می‌دهید، در واقع آدرس کامپیوتر میزبان آن حوزه را جستجو می‌کنید. در شبکه اینترنت، هر کامپیوتری دارای یک آدرس IP است. آدرس‌های IP روی سرورهایی با عنوان DNS یا Domain Name Service نگهداری می‌شوند.

حوزه‌ها

هنگام نصب سیستم‌عامل Red Hat Linux روی کامپیوتر میزبان ممکن است از عنوان ساده‌ای مثل computer1 یا نام کامل حوزه (اصطلاحاً Fully Qualified Domain name یا به اختصار FQDN)، مانند linux1.mommabears.com برای نام‌گذاری آن کامپیوتر استفاده کرده باشید. در صورتی که چنین کامپیوتری مستقیماً به شبکه اینترنت متصل نشده باشد، اهمیتی ندارد که از چه عنوانی برای نام‌گذاری آن استفاده کرده‌اید. با وجود این، در صورت استفاده از نام کامل حوزه برای نام‌گذاری کامپیوتر میزبان، به خا، داشته باشید که هنگام نصب سیستم‌عامل Red Hat Linux روی سایر کامپیوترهای شبکه نیز باید از همین عنوان استفاده کنید.

برخی از مراکز ارایه دهنده خدمات اینترنت ممکن است به برخی از کامپیوترهایی که از طریق آن مرکز به شبکه اینترنت متصل می‌شوند یک نام کامل حوزه تخصیص دهند. این شیوه بیشتر در مواردی که دستیابی به شبکه اینترنت از طریق مودم‌های کابلی یا خطوط پرسرعت DSL (اصطلاحاً Digital Subscriber Line) صورت گرفته باشد، مورد استفاده واقع می‌شود.

هر حوزه‌ای را می‌توان به چند حوزه فرعی تقسیم کرد. به این ترتیب، هر حوزه فرعی می‌تواند نماینده یک‌شبکه‌محلی‌باشد. برای مثال، حوزه‌های linux.mommabears.com، windows.mommabears.com و other.mommabears.com ممکن است نماینده سه شبکه محلی مستقل باشند.

نام میزبان

برای نام‌گذاری کامپیوترهای مستقر در شبکه به جای نام کامل حوزه می‌توان از نام ساده‌ای مانند computer1 به عنوان نام میزبان استفاده کرد. در واقع نام کامل حوزه متشکل از نام حوزه و نام میزبان است. برای مثال، چنان‌چه نام میزبان کامپیوتر شما berkeley و نام حوزه مربوطه california.now باشد، نام کامل حوزه آن berkeley.california.now خواهد بود. تمام اسامی میزبان و اسامی کامل حوزه متناظر با یک آدرس عددی، هم‌چون یک آدرس IP هستند.

آدرس‌های سخت‌افزاری

ارتباط میان کامپیوترهای یک شبکه در سطح سخت‌افزار از طریق مشخصه کارت‌های شبکه آن‌ها که با عنوان آدرس سخت‌افزاری شناخته می‌شود، صورت می‌گیرد. آدرس‌های سخت‌افزاری مجموعه‌ای متشکل از ارقام هگزادسیمال (مبنای شانزده) مانند 00-60-08-8D-41-93 هستند. امروزه تمام کارت‌های شبکه دارای یک آدرس سخت‌افزاری منحصر به فرد هستند. هنگام پیکربندی شبکه‌ای از نوع TCP/IP لازم است به هر آدرس سخت‌افزاری یک آدرس IP نسبت دهید.

تعداد ارقام هگزادسیمال شانزده عدد بوده و متشکل از 0، 1، 2، 3، 4، 5، 6، 7، 8، 9، A، B، C، D، E و F است.

مجموعه پروتکل‌ها

چنان‌که در این قسمت خواهید دید، کامپیوترهای مستقر در یک شبکه برای برقراری ارتباط با یکدیگر به عناصر مختلفی از جمله نام حوزه، آدرس عددی، آدرس سخت‌افزاری و تسهیلات لازم برای مدیریت ارتباطات و هم‌چنین پروتکل‌هایی در سطح برنامه‌های کاربردی به منظور استفاده از سرویس پست الکترونیکی، دسترسی به صفحات وب، دسترسی به فایل سرورها و مانند آن نیاز دارند. این عناصر را می‌توان در قالب یک مجموعه پروتکل (اصطلاحاً protocol stack) دسته‌بندی کرد.

یک مجموعه پروتکل در اصل قراردادی برای تقسیم وظایف است. برخی از پروتکل‌ها به منظور استفاده از سرویس پست الکترونیکی یا DNS و برخی نیز جهت استفاده از اسامی حوزه‌ها، آدرس‌های IP و

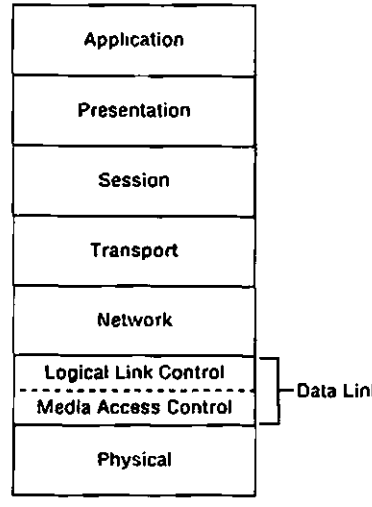
آدرس‌های سخت‌افزاری تنظیم شده‌اند. برخی دیگر از پروتکل‌ها نیز به منظور رمزگذاری داده‌ها، کنترل کدهای باینری و موارد دیگر تنظیم شده‌اند.

در مجموع دو روش برای تقسیم این قبیل وظایف ابداع شده است. یکی از این روش‌ها مدلی با عنوان OSI است که توسط سازمان استانداردسازی جهانی معرفی شده است. در این قسمت به بررسی مدل OSI و دو مجموعه پروتکل با عناوین NetBEUI و IPX/SPX خواهیم پرداخت. روش دیگر مدلی با عنوان TCP/IP است که در همین فصل آن‌را مورد بررسی قرار خواهیم داد.

مباحثات انجام شده در پشتیبانی از مدل‌های OSI و TCP/IP به شدت مباحثاتی است که در پشتیبانی از دو سیستم‌عامل Linux و Windows درمی‌گیرد، به طوری که طرفداران افراطی مدل OSI معمولاً سعی دارند مدل TCP/IP را در قالب مدل OSI توضیح دهند.

لایه‌های مدل OSI

مدل OSI یک مدل هفت لایه است. پیش از ارسال پیغام یک کامپیوتر از طریق شبکه، این پیغام با گذر از لایه‌های مختلف به مجموعه‌ای از صفر و یک‌ها ترجمه شده و این مجموعه از طریق شبکه ارسال می‌شود. برنامه‌های مستقر در هریک از این لایه‌ها عملیات مختلفی مانند رمزگذاری، تصحیح خطا و مسیریابی را انجام می‌دهند. شکل ۱-۲۰ ساختار مدل OSI را نشان می‌دهد.



شکل ۱-۲۰ مدل هفت لایه OSI

در ادامه لایه‌های مختلف مدل OSI را به طور خلاصه مورد بررسی قرار می‌دهیم. در این بررسی به اعداد نسبت داده شده به هر لایه توجه کنید:

- **لایه برنامه کاربردی یا Application Layer**: این لایه هفتمین لایه مدل OSI بوده و فرآیند ترجمه پیغام‌های ارسالی از این لایه آغاز می‌شود. برای مثال، پروتکل HTTP که یکی از پروتکل‌های لایه برنامه کاربردی است، اطلاعات ارسالی از طریق مرورگرهای وب، مانند Mozilla را ترجمه می‌کند. دروازه یا gateway به کامپیوتری اطلاق می‌شود که فرآیند ترجمه را در سطح لایه برنامه کاربردی میان دو شبکه انجام می‌دهد.
- **لایه نمایش یا Presentation Layer**: این لایه ششمین لایه مدل OSI است. در این سطح ارقام و حروف به سطح پایین‌تری ترجمه می‌شود. برای مثال، پروتکل ASCII کاراکترهای موجود روی صفحه کلید را به کدهای متناظر تبدیل می‌کند. تمام پروتکل‌های رمزگذاری مانند Secure Sockets Layer یا به اختصار SSL از جمله پروتکل‌های این لایه محسوب می‌شوند.
- **لایه جلسه یا Session Layer**: این لایه پنجمین لایه مدل OSI بوده و وظیفه آن مدیریت زمان صرف شده روی یک شبکه است. پروتکل‌های این لایه زمان ارسال و دریافت پیغام‌ها توسط کامپیوترهای مستقر در شبکه را به دقت مورد توجه قرار می‌دهند. برای مثال، نرم‌افزار پیاده‌سازی شده به عنوان لایه جلسه در کارت شبکه می‌تواند تشخیص دهید که ارسال و دریافت داده‌ها از طریق شبکه به کدام‌یک از روش‌های یک سویه (اصطلاحاً half-duplex) یا دو سویه هم‌زمان (اصطلاحاً full-duplex) انجام می‌شود.
- **لایه انتقال یا Transport Layer**: این لایه چهارمین لایه مدل OSI است. وظیفه پروتکل‌های این لایه ارسال پیغام و اطمینان از دریافت صحیح آن به واسطه تأیید دریافت پیغام ارسالی (اصطلاحاً acknowledgment) از جانب مقصد و ارسال مجدد آن در صورت عدم تأیید دریافت پیغام ارسالی از جانب مقصد یا ارسال پیغام موردنظر و بیشترین تلاش برای دریافت آن در مقصد است. دو پروتکل TCP و UDP مهم‌ترین پروتکل‌های این لایه به شمار می‌روند. پروتکل‌های این لایه پیغام ارسالی را پیش از ارسال به بسته‌های کوچکی تقسیم می‌کنند. اگر در ارسال پیغام از پروتکل TCP استفاده شده باشد، دریافت کننده پیغام باید دریافت آن‌را با ارسال پیغامی به فرستنده مورد تأیید قرار دهد. چنان‌چه پس از سپری شدن مدت زمان مشخصی فرستنده چنین پیغامی را از جانب مقصد دریافت نکند برای ارسال مجدد آن پیغام اقدام خواهد کرد. در پروتکل UDP هیچ الزامی برای تأیید دریافت پیغام در مقصد مشخص نشده است.

چرخه زندگی بسته‌های TCP

صرف‌نظر از پیغام‌های بسیار کوچک، هیچ پیغامی به طور یکجا برای مقصد ارسال نمی‌شود. در لایه انتقال، هر پیغام به عناصر کوچک‌تری تقسیم شده و هرکدام از آن‌ها تحت عنوان یک بسته یا packet قالب‌بندی می‌شود. همین بسته‌ها در لایه‌های پایین‌تر مدل OSI ممکن است باز هم به عناصر کوچک‌تری تقسیم شوند. برخی از پروتکل‌ها، این بسته‌ها یا عناصر کوچک‌تر را از مسیرهای مختلفی به مقصد ارسال می‌کنند. هریک از این بسته‌ها علاوه بر داده‌های اصلی حاوی اطلاعات مسیریابی و هم‌چنین اطلاعاتی است که موقعیت آن بسته را در میان سایر بسته‌های ارسالی به منظور بازسازی پیغام اصلی مشخص می‌کند. برای مثال، در شبکه‌های Ethernet اندازه این گونه بسته‌ها در لایه پیوند داده‌ها باید حداکثر برابر با ۱۵۱۸ بایت باشد که ۱۵۰۰ بایت آن شامل داده‌های اصلی و ۱۸ بایت آن شامل اطلاعات مسیریابی و نحوه بازسازی پیغام ارسالی است.

طراحی شبکه، فرآیند نسبتاً پیچیده‌ای است. به احتمال زیاد می‌توان کتاب Computer Networks نوشته پروفسور Andrew Tanenbaum را که در سال ۲۰۰۲ توسط انتشارات Prentice Hall منتشر شده است، مناسب‌ترین مرجع موجود در این زمینه دانست.

- **لایه شبکه یا Network Layer**: این لایه سومین لایه مدل OSI بوده و وظیفه آن ارسال داده‌ها از کامپیوتری به کامپیوتر دیگر و از شبکه‌ای به شبکه دیگر است. به طور یقین پروتکل IP را باید مهم‌ترین پروتکل این لایه محسوب کرد. برای ارسال پیغام‌ها از یک شبکه به شبکه دیگر اطلاع از آدرس IP مقصد ضروری است. روترها (که نوعی تجهیزات مورد استفاده در شبکه‌ها هستند) با استفاده از اطلاعات همین لایه و بهره‌گیری از الگوریتم‌های پیچیده، ترافیک بین شبکه‌ها را کنترل می‌کنند.
- **لایه پیوند داده‌ها یا Data-Link Layer**: این لایه دومین لایه مدل OSI بوده و وظیفه اصلی آن اطمینان از صحت داده‌های دریافتی در مقصد است. این لایه اغلب در قالب دو لایه فرعی با عناوین Logical Link Control و Media Access Control یا به اختصار LLC و MAC پیاده‌سازی می‌شود. وظیفه پروتکل‌های لایه LLC کسب اطمینان از این موضوع است که پیغام‌های ارسالی به ترتیب و بدون خطا در مقصد دریافت شده‌اند. به بیان دیگر، وظیفه پروتکل‌های این لایه را می‌توان در مرتب‌سازی فریم‌ها و بررسی وجود خطا خلاصه کرد. پروتکل‌های لایه MAC نیز تسهیلات لازم برای برقراری ارتباط کامپیوترها با یکدیگر را در اختیار قرار می‌دهند. به همین دلیل است که به آدرس سخت‌افزاری کارت شبکه اغلب آدرس MAC نیز گفته می‌شود. سوییچ‌ها

و پل‌ها (که نوعی تجهیزات مورد استفاده در شبکه‌ها هستند) با استفاده از اطلاعات همین لایه فرعی، ترافیک موجود در یک شبکه را کنترل می‌کنند.

- **لایه فیزیکی یا Physical Layer:** این لایه نخستین لایه مدل OSI بوده و وظیفه آن ترجمه داده‌ها در قالب مجموعه‌ای از صفر و یک‌هاست. پروتکل‌های این لایه ارتباط بی‌واسطه‌ای با تجهیزات فیزیکی شبکه از جمله کابل‌ها و اتصالات دارند.

هنگام خرید تجهیزات شبکه به خاطر داشته باشید که اغلب فروشندگان لایه‌ای از شبکه را که عملکرد تجهیزات موردنظر به آن مربوط می‌شود، ذکر می‌کنند. برای مثال، از آن‌جا که عملکرد سوییچ‌های استاندارد به لایه دوم و عملکرد روترهای استاندارد به لایه سوم مربوط است، معمولاً از عنوان سوییچ لایه دوم و روتر لایه سوم برای اشاره به این تجهیزات استفاده می‌شود. با این وجود، مرز میان لایه‌ها همواره شفاف نیست. برای مثال، برخی از سوییچ‌ها قابلیت مسیریابی و انتقال داده‌ها را نیز دارند و از این‌رو به آن‌ها سوییچ لایه سوم یا سوییچ لایه چهارم نیز اطلاق می‌شود.

پروتکل NetBEUI

این پروتکل که عنوان آن کوتاه شده عبارت NetBIOS Extended User Interface است، شامل مجوعه‌ای از پروتکل‌های توسعه یافته توسط دو شرکت Microsoft و IBM است. پروتکل مزبور براساس مجموعه‌ای از فرامین با عنوان Network Basic Input Output System یا به اختصار NetBIOS توسعه یافته است. به واسطه فرامین NetBIOS می‌توان داده‌های مستقر روی یک کامپیوتر را از طریق شبکه به کامپیوتر دیگری از همان شبکه ارسال کرد. هم‌چنین می‌توان اطلاعات موجود در فهرست‌های مشترک کامپیوترهای یک شبکه را در اختیار سایر کامپیوترهای آن شبکه قرار داد.

متأسفانه داده‌های ارسالی روی شبکه‌های NetBEUI یا از طریق مکانیزم NetBIOS فاقد اطلاعات مسیریابی است. به بیان دیگر، نمی‌توان یک شبکه NetBEUI را به شبکه دیگری از جمله شبکه جهانی اینترنت متصل کرد. از طرف دیگر، در هر شبکه NetBEUI حداکثر می‌توان تعداد ۲۵۵ کامپیوتر را مورد استفاده قرار داد.

با وجود این، شرکت Microsoft در سال‌های اخیر مجموعه فرامین NetBIOS را به منظور تطبیق آن با پروتکل‌هایی مانند TCP/IP و IPX/SPX که دارای قابلیت مسیریابی هستند، بازنویسی کرده است. چنان‌چه مدیریت شبکه‌ای شامل کامپیوترهایی با سیستم‌عامل Windows را به عهده دارید باید با فرامین مهم NetBIOS از جمله net view و net use آشنا باشید.

استفاده از سرویس Samba مستلزم اجرای مجموعه فرامینی با عنوان Server Message Block یا به اختصار SMB است. قالب این فرامین شباهت زیادی به قالب فرامین NetBIOS دارد. در فصل بیست و نهم با نحوه اجرای این فرامین آشنا می‌شوید. از آن‌جا که سرویس Samba در اصل نسخه پیاده‌سازی شده‌ای از فرامین NetBIOS تحت سیستم‌عامل UNIX و Linux است، شباهت فرامین آن از جمله net view و new use نباید باعث تعجب باشد.

پروتکل IPX/SPX

پروتکل SPX/IPX نیز مشابه TCP/IP مجموعه‌ای متشکل از پروتکل‌هاست که تسهیلات لازم به منظور ارتباط میان شبکه‌ها را در اختیار قرار می‌دهد. این پروتکل توسط شرکت Novell و به منظور پشتیبانی از سیستم‌عامل NetWare توسعه یافته است.

سیستم عامل NetWare در بسیاری از شبکه‌های قدیمی مورد استفاده قرار گرفته است. با وجود این، حتی در صورتی که هدف موردنظر، دستیابی به یک شبکه NetWare باشد، به دلیل پشتیبانی این سیستم‌عامل از پروتکل TCP/IP نیازی به استفاده از پروتکل IPX/SPX نیست.

قابلیت مسیریابی یکی از مشخصه‌های بارز پروتکل IPX/SPX محسوب می‌شود. در نسخه‌های ابتدایی سیستم‌عامل Windows پروتکل IPX/SPX تنها گزینه ممکن برای دستیابی به شبکه‌های مختلف محسوب می‌شد.

برای دستیابی به شبکه‌ای با پروتکل IPX/SPX از طریق کامپیوتری با سیستم‌عامل Linux لازم است بسته‌های نرم‌افزاری *-mars-new، *-ipxutils و *-ncpfs را روی کامپیوتر موردنظر نصب کنید. در صورت نصب بسته نرم‌افزاری نخست می‌توانید کامپیوتر Linux را جهت سرویس‌دهی فایل و چاپ (به عنوان file server و print server) روی شبکه‌ای از نوع NetWare پیکربندی کنید. بسته نرم‌افزاری دوم، حاوی نرم‌افزارهای موردنیاز برای پشتیبانی از پروتکل IPX/SPX است. بسته نرم‌افزاری آخر نیز شامل فرامینی است که به کمک آن‌ها می‌توانید به عنوان کلاینت از سرویس‌های شبکه NetWare استفاده کنید.

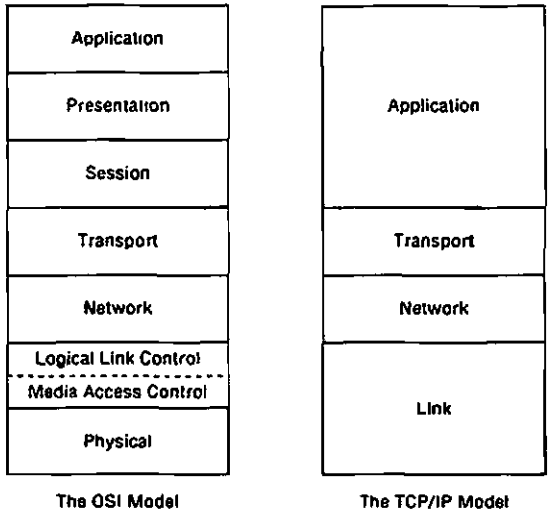
علاوه بر پروتکل‌های فوق، می‌توان به پروتکل‌های مهم دیگری نیز اشاره کرد. از میان آن‌ها به سه پروتکل System Network Architecture (به اختصار SNA)، Xerox Network System (به اختصار XSN) و Digital Equipment Corporation network (به اختصار DECnet) که به ترتیب توسط شرکت‌های IBM، Xerox و DEC توسعه یافته‌اند، متداول‌تر از سایر پروتکل‌ها هستند. (شرکت DEC مدتی است که به مالکیت شرکت Hewlett-Packard درآمده است.)

الفبای پروتکل TCP/IP

پروتکل TCP/IP در حال حاضر مهم‌ترین پروتکل شبکه است. شرکت Novell نیز سال‌هاست که آن‌را در سیستم‌عامل NetWare مورد پشتیبانی قرار می‌دهد. شرکت Microsoft نیز با وجود توسعه مجموعه NetBIOS از این پروتکل پشتیبانی به عمل آورده است. پروتکل TCP/IP در واقع زبان گفتگو روی شبکه جهانی اینترنت بوده و از این‌رو، احتمالاً تنها پروتکلی است که آشنایی با مشخصات آن ضرورت دارد.

مدل TCP/IP

مدل TCP/IP از چهار لایه تشکیل شده است. این مدل تقریباً با مدل OSI قابل قیاس است. چنان‌که شکل ۲-۲۰ نیز نشان می‌دهد، عملکرد لایه برنامه کاربردی یا Application در مدل TCP/IP معادل با عملکرد سه لایه بالایی مدل OSI است. هم‌چنین عملکرد لایه پیوند یا Link در مدل TCP/IP معادل عملکرد دولایه پایینی مدل OSI است.



شکل ۲-۲۰ مدل چهار لایه TCP/IP در مقایسه با مدل هفت لایه OSI

بدیهی است استفاده از مدل TCP/IP برای پیاده‌سازی پروتکل‌های TCP/IP مناسب‌تر از مدل OSI است. برای مثال، در فصل بیست و هفتم نسخه‌هایی از سرویس FTP با ایمنی بالا را مورد بررسی قرار خواهیم داد. یکی از وظایف این سرویس‌ها تبدیل داده‌ها به کدهای ASCII یا باینری است که در مدل

OSI متناظر با عملکرد لایه نمایش یا Presentation است. وظیفه دیگر این سرویس‌ها ترجمه فرامین FTP است که در مدل OSI از جمله عملکردهای لایه برنامه کاربردی یا Application به شمار می‌رود.

بررسی پروتکل‌های TCP/IP

مجموعه پروتکل TCP/IP شامل صدها پروتکل است. احتمالاً تاکنون با برخی از آن‌ها از جمله FTP، HTTP، SMTP، TCP SNMP، IP و چند پروتکل دیگر آشنایی دارید. در قسمت‌های بعد برخی از این پروتکل‌ها را مورد بررسی قرار خواهیم داد.

پروتکل‌های لایه برنامه کاربردی

برای مشاهده لیست کامل پروتکل‌های لایه برنامه کاربردی مدل TCP/IP کافی محتوای فایل /etc/services را مورد توجه قرار دهید. چنان‌که شکل ۳-۲۰ نیز نشان می‌دهد، این فایل شامل اسامی سرویس‌ها (مانند ftp، ssh و smtp)، شماره پورت‌های مربوطه و توضیحاتی در ارتباط با آن‌هاست.

```
# 21 is registered to ftp, but also used by fsp
ftp             21/tcp
ftp             21/udp          fsp fspd
ssh             22/tcp                          # SSH Remote Login Protocol
ssh             22/udp                          # SSH Remote Login Protocol
telnet          23/tcp
telnet          23/udp
# 24 - private mail system
smtp            25/tcp          mail
smtp            25/udp          mail
time            37/tcp          timserver
time            37/udp          timserver
rlp             39/tcp          resource        # resource location
rlp             39/udp          resource        # resource location
nameserver      42/tcp          name            # IEN 116
nameserver      42/udp          name            # IEN 116
nicname         43/tcp          whois
nicname         43/udp          whois
tacacs          49/tcp                          # Login Host Protocol (TACACS)
tacacs          49/udp                          # Login Host Protocol (TACACS)
re-mail-ck      50/tcp                          # Remote Mail Checking Protocol
re-mail-ck      50/udp                          # Remote Mail Checking Protocol
domain          53/tcp                          # name-domain server
```

شکل ۳-۲۰ محتوای فایل /etc/services

تعداد ۶۵۵۳۶ پورت را می‌توان به پروتکل‌های TCP/IP تخصیص داد. هر پورت مشابه یک کانال تلویزیونی است. هنگامی که سیستم‌عامل Linux پورت به خصوصی را مورد دستیابی قرار می‌دهد،

اطلاعات جاری شده از طریق آن پورت مانند امواج تلویزیونی ارسال شده به یک کانال در اختیار قرار می‌گیرد. سازمانی با عنوان Internet Assigned Numbers Authority (به اختصار IANA) عهده‌دار تخصیص برخی از این پورت‌ها به پروتکل‌های TCP/IP است. به مجموعه پورت‌های تخصیص داده شده توسط این سازمان اصطلاحاً پورت‌های شناخته شده یا well-known ports گفته می‌شود. این پورت‌ها را نمی‌توان به پروتکل دیگری تخصیص داد. برای مثال، سازمان مذکور پورت شماره 80 را به پروتکل HTTP (برای دریافت صفحات وب)، پورت شماره 21 را به پروتکل FTP (به منظور ارسال و دریافت فایل) و پورت شماره 110 را به پروتکل POP3 (جهت دریافت پیغام‌های الکترونیکی) اختصاص داده است.

جدول ۱-۲۰ شامل لیستی از پروتکل‌های مهم لایه برنامه کاربردی مدل TCP/IP است. در هر مورد پورت مربوطه مشخص شده است.

جدول ۱-۲۰ برخی از پروتکل‌های لایه برنامه کاربردی مدل TCP/IP

عنوان پروتکل	شماره پورت مربوطه	توضیح
FTP	21	این پروتکل با عنوان File Transfer Protocol جهت ارسال و دریافت فایل مورد استفاده قرار می‌گیرد.
SSH	22	این پروتکل با عنوان Secure Shell داده‌های ارسالی از یک کامپیوتر به کامپیوتر دیگر را رمزگذاری می‌کند.
Telnet	23	این پروتکل امکان برقراری ارتباط با یک کامپیوتر راه دور را به منظور ارسال و دریافت پیغام‌ها در قالب متنی فراهم می‌کند.
SMTP	25	این پروتکل با عنوان Simple Mail Transfer Protocol جهت ارسال پیغام های الکترونیکی مورد استفاده قرار می‌گیرد.
HTTP	30	این پروتکل با عنوان Hypertext Transfer Protocol امکان دستیابی به صفحات وب را در اختیار می‌گذارد.
POP3	110	این پروتکل با عنوان Post Office Protocol به منظور دریافت پیغام‌های الکترونیکی مورد استفاده قرار می‌گیرد.
SNMP	161	این پروتکل با عنوان Simple Network Management Protocol جهت عیب‌یابی شبکه‌ها مورد استفاده قرار می‌گیرد.
HTTPS	443	این پروتکل با عنوان Secure HTTP امکانات پروتکل HTTP را در چارچوبی با امنیت بالاتر در اختیار قرار می‌دهد.

عنوان پروتکل	شماره پورت مربوطه	توضیح
IPP	631	این پروتکل با عنوان Internet Print Protocol تسهیلات لازم برای استفاده از سیستم چاپ متداول در UNIX (اصطلاحاً Common Unix Print System یا به اختصار CUPS) در اختیار می‌گذارد.
SWAT	901	این پروتکل با عنوان Samba Web Administration Tool تسهیلات لازم برای مدیریت سرویس Samba از طریق وب را فراهم می‌کند.
NFS	2049	این پروتکل با عنوان Network File Services تسهیلات لازم برای برقراری ارتباط میان کامپیوترهای UNIX و Linux را فراهم می‌کند.

پروتکل‌های لایه انتقال

دو پروتکل TCP و UDP مهم‌ترین پروتکل‌های لایه انتقال مدل TCP/IP به شمار می‌روند. هر دو پروتکل نامبرده با دریافت نام کامل حوزه یک کامپیوتر (مانند www.sybex.com) اقدامات لازم برای ارسال پیغام‌های موردنظر به آن کامپیوتر را انجام می‌دهند. پروتکل TCP یا Transmission Control Protocol تا جایی اقدام به ارسال مجدد یک پیغام می‌کند که تأیید دریافت آن پیغام از جانب مقصد به فرستنده برسد. پروتکل TCP از نوع پروتکل‌های "اتصال مدار" یا اصطلاحاً connection-oriented است. از طرف دیگر، پروتکل UDP یا User Datagram Protocol اصراری بر تأیید دریافت پیغام در مقصد ندارد. این پروتکل چنین فرض می‌کند که شبکه مورد استفاده برای انتقال داده‌ها از چنان قابلیت اعتمادی برخوردار است که از دست رفتن بخشی از داده نیز آن چنان تأثیر گذار نیست. پروتکل UDP از نوع پروتکل‌های "بدون اتصال" یا اصطلاحاً connectionless است.

پروتکل‌های لایه شبکه

پروتکل اصلی لایه انتقال پروتکلی با عنوان IP یا Internet Protocol است. در این لایه، از آدرس IP به منظور ارسال داده‌ها از طریق شبکه استفاده می‌شود. هر دو شیوه آدرس‌دهی IPv4 و IPv6 را در همین فصل مورد بررسی قرار خواهیم داد.

پروتکل ICMP یا Internet Control Message Protocol یکی دیگر از پروتکل‌های حایز اهمیت در این لایه است. برنامه ping ابزار متداولی است که با بهره‌گیری از این پروتکل امکان بازبینی اتصال میان

کامپیوتر میزبان با هریک از کامپیوترهای مستقر در شبکه را فراهم می‌کند. در فصل بیست و یکم ابزار ping را به همراه سایر ابزارهای مفید شبکه مورد بررسی قرار خواهیم داد.

در مدل TCP/IP به لایه شبکه اصطلاحاً لایه اینترنت نیز گفته می‌شود.

پروتکل‌های لایه پیوند

در مدل TCP/IP لایه پیوند ارتباط نزدیکی با تکنولوژی‌های شبکه مانند Ethernet، Token Ring و ATM دارد. در این لایه پیغام موردنظر در قالب مجموعه‌ای از صفر و یک‌ها بسته‌بندی شده و از طریق کابل شبکه یا رسانه دیگری که به منظور انتقال داده‌ها در نظر گرفته شده است به سمت مقصد گسیل می‌شود.

با وجودی که Ethernet امروزه متداول‌ترین تکنولوژی مورد استفاده در شبکه‌ها به شمار می‌رود، سایر تکنولوژی‌های موجود در این زمینه را نباید نادیده گرفت. در ادامه به شرح برخی از آن‌ها توجه کنید:

- **Ethernet**: واژه Ethernet یک اصطلاح تجاری برای اشاره به استاندارد IEEE 802.3 است. در شبکه‌های Ethernet بسته‌ها را می‌توان حداکثر با سرعت ۱۰ مگابیت بر ثانیه از مبدأ به مقصد ارسال کرد. هنگامی که ترافیک این گونه شبکه‌ها زیاد باشد، برای پیشگیری از برخورد بسته‌ها با یکدیگر از ارسال آن‌ها تا زمان کاهش ترافیک جلوگیری به عمل می‌آید. از این‌رو، سرعت واقعی در شبکه‌های Ethernet کمتر از نصف حداکثر سرعت است.
- **Fast Ethernet**: عبارت Fast Ethernet یک اصطلاح تجاری است که برای اشاره به استاندارد IEEE 802.3u به کار می‌رود. در شبکه‌های Fast Ethernet بسته‌ها را می‌توان حداکثر با سرعت ۱۰۰ مگابیت بر ثانیه از مبدأ به مقصد ارسال کرد. در این گونه شبکه‌ها کابل‌هایی با مشخصه Category 5 یا به اختصار Cat 5 مورد استفاده قرار می‌گیرد.
- **Gigabit Ethernet**: عبارت Gigabit Ethernet یک اصطلاح تجاری برای اشاره به استاندارد IEEE 802.3ae است. در شبکه‌های Gigabit Ethernet بسته‌ها را می‌توان حداکثر با سرعت ۱۰۰۰ مگابیت بر ثانیه از مبدأ به مقصد ارسال کرد. در این‌گونه شبکه‌ها از کابل‌های فیبر نوری برای انتقال داده‌ها استفاده می‌شود.
- **Token Ring**: عبارت Token Ring نیز یک اصطلاح تجاری است که برای اشاره به استاندارد IEEE 802.5 مورد استفاده قرار می‌گیرد. در شبکه‌های Token Ring بسته‌ها را می‌توان حداکثر با سرعت ۱۶ مگابیت بر ثانیه از مبدأ به مقصد ارسال کرد. از آن‌جا که در شبکه‌های Token Ring

تنها کامپیوتری قادر به ارسال داده‌هاست که نشانه ویژه‌ای با عنوان token را در اختیار دارد، عملکرد این گونه شبکه‌ها دست کم در مقوله حداکثر سرعت انتقال داده‌ها نسبت به شبکه‌های Ethernet بهتر است.

- **Asynchronous Transfer Mode یا ATM**: شبکه‌های ATM یکی از گزینه‌های متداول برای دستیابی به سرعت بالا در انتقال داده‌ها محسوب می‌شود. در شبکه‌های ATM، بسته‌ها را می‌توان با سرعت ۱۵۵ یا ۶۲۲ مگابیت بر ثانیه ارسال کرد. با آن‌که پشتیبانی از این گونه شبکه‌ها در مراحل آزمایشی است، لیستی از کارت‌های شبکه ATM در مستندات Linux Hardware-HOWTO به چشم می‌خورد. هم‌اینک توسعه‌دهندگان تکنولوژی ATM مشغول فعالیت برای دستیابی به سرعتی بیش از ۲ گیگابیت بر ثانیه هستند.
- **Point-to-Point Protocol یا PPP**: هیچ بحثی در مورد پروتکل‌های شبکه بدون پرداختن به پروتکل PPP کامل نیست. این پروتکل سالهاست که امکان انتقال داده‌ها را از طریق مودم و خطوط تلفن در اختیار بسیاری از کاربران قرار داده است. با وجودی که سرعت انتقال داده با استفاده از پروتکل PPP به ۵۶ کیلوبایت (و در ایالات متحده آمریکا به ۵۳ کیلوبایت) محدود شده است، سرویس‌دهی آن برای مدتها بسیار مطلوب بوده است و البته این روند هم‌چنان ادامه دارد. به خاطر داشته باشید که تا زمان انتشار این کتاب تنها ۲۰ درصد از کاربران اینترنت در ایالات متحده آمریکا به خطوط پرسرعت از جمله مودم‌های کابلی یا DSL دسترسی دارند.

لایه پیوند مدل TCP/IP اغلب با عنوان لایه دسترسی به شبکه یا Network Access Layer نیز شناخته می‌شود.

تعریف چند سرویس مهم

در این قسمت چند سرویس مهم شبکه‌های TCP/IP را مورد بررسی قرار می‌دهیم. چنان‌چه با این قبیل شبکه‌ها آشنایی چندانی ندارید، مطالعه این قسمت کمک می‌کند تا ایده مناسبی درباره سرویس‌های قابل استفاده در شبکه‌های TCP/IP به دست آورید. با این وجود در فصل‌های بعد جزییات پیکربندی برخی از این سرویس‌ها را به طور دقیق مورد بررسی قرار خواهیم داد.

- **سرویس Domain Name System یا DNS**: این سرویس یک بانک اطلاعاتی شامل اسامی کامل حوزه‌ها و آدرس‌های IP (مانند linux.mommabears.com و 192.168.1.231) است. جستجوی وب سایتی مانند www.redhat.com روی اینترنت در واقع منجر به جستجوی یک سرور DNS می‌شود. پس از ترجمه آدرس وب سایت موردنظر به آدرس IP متناظر توسط سرویس DNS،

آدرس IP مزبور از کامپیوتری به کامپیوتر دیگر ارسال می‌شود تا در نهایت به وب سایت Red Hat می‌رسد.

- **سرویس Dynamic Host Configuration Protocol یا DHCP**: تخصیص دستی آدرس‌های IP به کامپیوترهای مستقر در شبکه می‌تواند مشکلاتی را به همراه داشته باشد. برای مثال، چنان‌چه این کار با دقت کافی انجام نشود، ممکن است یک آدرس IP واحد به دو کامپیوتر مختلف تخصیص داده شود که این امر منجر به مشکلات بعدی و اختلال در عملکرد شبکه خواهد شد. سرویس DHCP فرآیند تخصیص آدرس‌های IP به کامپیوترهای مستقر در شبکه را به طور خودکار انجام می‌دهد.
- **سرویس Address Resolution Protocol یا ARP**: این سرویس آدرس IP کامپیوترهای مستقر در شبکه را به آدرس سخت‌افزاری کارت شبکه آن کامپیوترها نسبت می‌دهد. چنان‌که قبلاً نیز گفته شد، آدرس سخت‌افزاری با عنوان آدرس MAC نیز شناخته می‌شود. در واقع کامپیوترهای مستقر در شبکه از طریق آدرس‌های سخت‌افزاری با یکدیگر ارتباط برقرار می‌کنند. چنان‌چه اشتباهی در انجام این کار صورت گیرد، به طوری که آدرس IP یک کامپیوتر به آدرس سخت‌افزاری یک کامپیوتر دیگر نسبت داده شود، ممکن است عملکرد شبکه با مشکل مواجه شود.

آدرس‌دهی IP

پیش از آن‌که یک شبکه TCP/IP بتواند با سایر شبکه‌ها ارتباط برقرار کند، لازم است به هر کدام از کامپیوترهای مستقر در آن شبکه یک آدرس IP تخصیص داده شود. برای مثال، ممکن است مرکز خدمات ISP یک آدرس IP دایمی به کامپیوترتان تخصیص داده باشد یا هر بار که از طریق این مرکز به اینترنت متصل می‌شوید، به واسطه سرویس DHCP یک آدرس IP موقتی اما منحصر به فرد به کامپیوتر شما تخصیص داده شود.

تخصیص آدرس IP به یک کامپیوتر با در دست داشتن آدرس IP شبکه و یک ماسک شبکه (اصطلاحاً network mask) امکان‌پذیر است. کامپیوترهایی که آدرس IP آن‌ها تلفیقی از یک آدرس شبکه و یک ماسک شبکه واحد باشد روی یک شبکه مستقر هستند. تمام آدرس‌های شبکه عضو یکی از پنج کلاس موجود (یعنی A، B، C، D، و E) هستند. هر ماسک شبکه مجموعه‌ای از آدرس‌های IP را مشخص می‌کند که می‌توان به کامپیوترهای یک شبکه تخصیص داد.

برای اتصال یک شبکه به سایر شبکه‌ها باید آدرس IP دروازه اتصال در دسترس باشد. در سیستم‌عامل Linux برای تعیین محدودیت‌های دسترسی از یک شبکه به سایر شبکه‌ها یا دسترسی از سایر شبکه‌ها

به آن شبکه کافی است دو فایل /etc/hosts.allow و /etc/hosts.deny را مورد ویرایش قرار داده یا به کمک فرمان iptables یا ipchains مکانیزم دیوار آتش را به نحو مطلوب پیکربندی کنید.

آدرس‌دهی IPv4

از دهه ۱۹۷۰ تاکنون آدرس‌دهی IP به روش خاصی با عنوان IP version 4 یا به اختصار IPv4 انجام می‌شود. این گونه آدرس‌های IP از نوع ۳۲ بیتی هستند. با یک عملیات ریاضی ساده، یعنی محاسبه حاصل ۲ به توان ۳۲ (که عدد ۴٫۲۹۴٫۹۶۷٫۲۹۶ به دست می‌آید) می‌توان متوجه شد که به روش فوق می‌توان بیش از ۴ میلیارد آدرس IP تولید کرد. این تعداد آدرس IP برای نخستین سال‌های پس از ظهور شبکه اینترنت کافی بود. با وجود این، امروزه با وضعیت کاملاً متفاوتی مواجه هستیم، به طوری که حتی ۴ میلیارد آدرس IP نیز به نظر کافی نمی‌رسد. از این‌رو، روش دیگری با عنوان IP version 6 یا به اختصار IPv6 برای آدرس‌دهی IP ابداع شد که به تدریج در حال جای‌گزینی با روش قدیمی IPv4 است.

با وجود این، آدرس‌های IPv4 از نظر مفهوم و پیکربندی نسبت به آدرس‌های IPv6 بسیار ساده‌ترند. بسیاری عقیده دارند که آدرس‌های IPv4 در سال‌های آینده نیز هم‌چنان مورد استفاده خواهند بود. چنان‌که در فصل بعد خواهید دید، با بهره‌گیری از روش آدرس‌دهی IPv4 به سادگی می‌توان شبکه‌های مجازی (اصطلاحاً private network) را پیکربندی کرد.

آدرس‌های IPv4 را می‌توان در دو قالب باینری و دسیمال (یا دودویی و دهدهی) بیان کرد. برای مثال، این آدرس IPv4 به شیوه باینری بیان شده است:

```
11000000 10101000 00000001 00100000
```

شیوه فوق احتمالاً تا اندازه زیادی نامفهوم است. با وجود این، فراموش نکنید که شیوه دودیی اساس کار کامپیوترهاست. به دلیل راحتی کار با ارقام صفر تا ۹ ساده‌تر آن است که اعداد باینری یعنی دنباله‌های شامل صفر و یک‌ها را به اعداد دسیمال متناظر تبدیل کنیم. شیوه دسیمال برای بیان یک آدرس IPv4 این است که هر بخش از آدرس را به عدد دسیمال متناظر تبدیل کرده و آن‌ها را با علامت نقطه از یکدیگر جدا کنیم. به این ترتیب، آدرس IPv4 فوق را می‌توان به صورت 192.168.1.32 نیز بیان کرد. در قسمت بعد جزییات مربوط به نحوه تبدیل آدرس IPv4 از قالب باینری به دسیمال را مورد بررسی قرار می‌دهیم.

ساختار آدرس‌های IPv4

هر بیت بیانگر یک رقم باینری است. ساختار اعداد باینری تنها از دو رقم صفر و یک تشکیل می‌شود. ساختار سخت‌افزاری کامپیوترهای دیجیتال برای کار با اعداد باینری بسیار ایده‌آل است. برای بیان ارقام صفر و یک در این گونه کامپیوترها معمولاً از سوییچ استفاده می‌شود. بسته بودن سوییچ بیانگر رقم صفر و باز بودن آن بیانگر رقم یک است.

از سوی دیگر، هر بایت مجموعه‌ای متشکل از ۸ بیت تعریف شده است. در سیستم کدگذاری ASCII به هریک از حروف و ارقام موجود روی صفحه کلیدهای زبان انگلیسی کد منحصر به فردی برابر با یک بایت تخصیص داده می‌شود. به همین دلیل است که آدرس‌های IPv4 (که اندازه‌ای برابر با ۳۲ بیت دارند) در قالب چهار گروه هشت بایتی بیان می‌شوند. برای مثال، این آدرس IPv4 از چهار گروه هشت بایتی تشکیل شده است:

```
11000000 10101000 00000001 00100000
```

به احتمال قوی با نحوه محاسبه معادل دسیمال هر عدد باینری آشنا هستید. برای مثال، عدد باینری 00000001 معادل دسیمال 1 است. به همین ترتیب، عدد باینری 00000010 معادل دسیمال 2 و به همین ترتیب عدد باینری 00000011 معادل دسیمال 3 است. جدول ۲-۲۰ مثال‌های متعددی را در این زمینه نشان می‌دهد.

جدول ۲-۲۰ نمونه‌هایی از چند عدد باینری و معادل دسیمال آن‌ها

معادل دسیمال	عدد باینری
0	00000000
1	00000001
2	00000010
4	00000100
8	00001000
16	00010000
32	00100000
64	01000000
128	10000000

اکنون نخستین بایت از آدرس فوق، یعنی 11000000 را در نظر بگیرید. چنان‌که مشاهده می‌کنید، این بایت حاصل‌جمع دو عدد باینری 10000000 و 01000000 است. از آن‌جا که معادل دسیمال این دو عدد باینری به ترتیب برابر با اعداد 128 و 64 است، معادل دسیمال حاصل‌جمع برابر با عدد 192 یعنی

مجموع دو عدد 128 و 64 خواهد بود. این عدد بیانگر نخستین بخش از آدرس IP در قالب دسیمال است. به طور مشابه، معادل دسیمال بایت 10101000 برابر با عدد 168 و معادل دسیمال دو بایت 00000001 و 00010000 نیز به ترتیب برابر با اعداد 1 و 32 است. از این‌رو، آدرس IP فوق را می‌توان در قالب دسیمال به صورت 192.168.1.32 بیان کرد.

دقت کنید که معادل دسیمال بایت 11111111 برابر با عدد 255 است.

کلاس‌های آدرس‌دهی

محدوده آدرس‌های IPv4 از 0.0.0.0 تا 255.255.255.255 متغیر است. این آدرس‌ها را می‌توان در پنج کلاس مختلف از A تا E دسته بندی کرد. چنان‌چه آدرس‌های IP سه کلاس A، B و C در دسترس باشند، می‌توان آن‌ها را تخصیص داد. محدوده مربوط به هریک از این کلاس‌ها در جدول ۳-۲۰ تشریح شده است.

جدول ۳-۲۰ کلاس‌های آدرس‌دهی به روش IPv4

عنوان کلاس	محدوده آدرس‌دهی	توضیح
A	از 1.0.0.0 تا 127.255.255.255	این محدوده امکان آدرس‌دهی حداکثر ۱۶ میلیون کامپیوتر را در اختیار می‌گذارد.
B	از 128.0.0.0 تا 191.255.255.255	این محدوده امکان آدرس‌دهی حداکثر ۶۵,۰۰۰ کامپیوتر را در اختیار می‌گذارد.
C	از 192.0.0.0 تا 223.255.255.255	این محدوده امکان آدرس‌دهی حداکثر ۲۵۴ کامپیوتر را در اختیار می‌گذارد.
D	از 244.0.0.0 تا 239.255.255.255	این محدوده از آدرس‌های رزرو شده است.
E	از 240.0.0.0 تا 255.255.255.255	این محدوده از آدرس‌های رزرو شده است.

تمام آدرس‌های IP این جدول (حتی آدرس‌های سه کلاس A، B و C) قابل استفاده نیستند. در این زمینه به چند نکته مهم توجه کنید

- نخستین آدرس از مجموعه آدرس‌های IPv4 یک شبکه به خود آن شبکه منسوب می‌شود.
- آخرین آدرس از مجموعه آدرس‌های IPv4 یک شبکه به عنوان آدرس همگانی (اصطلاحاً broadcast address) در نظر گرفته می‌شود.
- آدرس 127.0.0.0 همواره به عنوان آدرس loopback در نظر گرفته می‌شود.

- تعدادی از آدرس‌های IPv4 به عنوان آدرس‌های خصوصی جهت پیکربندی شبکه‌های خصوصی (اصطلاحاً virtual LAN) که از طریق یک مکانیزم دفاعی با عنوان دیوار آتش یا اصطلاحاً fire wall به شبکه اینترنت متصل می‌شوند، در نظر گرفته شده است.

در فصل بعد هریک از این آدرس‌ها را به طور کامل مورد بررسی قرار خواهیم داد. علاوه بر این، مفاهیم مهمی چون آدرس شبکه، آدرس همگانی و ماسک‌ها را در قالب یک شبکه مجازی متصل به اینترنت توضیح خواهیم داد.

ساختار آدرس‌های IPv6

چنان‌که در قسمت قبل اشاره شد، ۴ میلیارد آدرس IP برای اهداف آینده کافی نخواهد بود. در حال حاضر بخش عمده‌ای از آدرس‌های IPv4 تخصیص داده شده‌اند. با وجودی که ممکن است بتوان با پرداختن بهای اضافی صاحب یک آدرس IPv4 شد، تلاش زیادی برای استفاده از IPv6 در شبکه اینترنت صورت گرفته است.

آدرس‌های IPv6 دارای ساختار ۱۲۸ بیتی هستند. این بدان معنی است که تعداد آدرس‌ها از ۴ میلیارد به بیش از ۳۴۰٬۰۰۰٬۰۰۰٬۰۰۰٬۰۰۰٬۰۰۰٬۰۰۰٬۰۰۰٬۰۰۰٬۰۰۰٬۰۰۰٬۰۰۰٬۰۰۰ خواهد رسید. برای تسهیل در جایگزینی، به هر آدرس IPv4 یک آدرس IPv6 نسبت داده شده است. به این ترتیب باز هم بیش از ۳۴۰٬۰۰۰٬۰۰۰٬۰۰۰٬۰۰۰٬۰۰۰٬۰۰۰٬۰۰۰٬۰۰۰٬۰۰۰٬۰۰۰٬۰۰۰٬۰۰۰ آدرس باقی می‌ماند. ضمناً آدرس‌های IPv4 اعتبار خود را هم‌چنان حفظ خواهند کرد.

ساختار آدرس‌های IPv6 چنان است که به سادگی می‌توان یک آدرس IPv4 را به آن تبدیل کرد. برای مثال، این آدرس IPv4 را در نظر بگیرید:

```
192.168.1.32
```

آدرس IPv6 معادل با آدرس فوق به این قرار است:

```
::192.168.1.32
```

با وجود این، آدرس‌های IPv6 با بهره‌گیری از ارقام هگزادسیمال (مبنای شانزده) یعنی 0، 1، 2، 3، 4، 5، 6، 7، 8، 9، a، b، c، d، e و f بیان می‌شوند. نمونه‌ای از یک آدرس IPv6 به این صورت است:

```
4aed:0a21:3c53:7dab:0000:0000:0000:0451
```

تبدیل آدرس IPv4 به آدرس IPv6 متناظر ساده است. به عنوان نمونه، با در نظر گرفتن آدرس IPv4 فوق، ابتدا معادل آن‌را به باینری بنویسید:

```
11000000 10101000 00000001 00100000
```

سپس با علم به این‌که توان چهارم عدد ۲ برابر با ۱۶ است، می‌توان این دنباله از صفر و یک‌ها را به دسته‌های چهارتایی تقسیم کرده و معادل هگزادسیمال هر دسته را مشخص کرد. به این ترتیب، آدرس IPv4 که قبلاً در قالب چهار گروه هشت بیتی بیان می‌شد، این‌بار به هشت گروه چهار بیتی تقسیم خواهد شد: (به هر گروه چهاربیتی اصطلاحاً nibble گفته می‌شود.)

```
1100 0000 1010 1000 0000 0001 0010 0000
```

برای سادگی، ابتدا معادل دسیمال هریک از این گروه‌های چهار بیتی را بنویسید:

```
12 0 10 8 0 1 2 0
```

سپس معادل هگزادسیمال هریک از آن‌ها را بنویسید:

```
c0a8:0120
```

به این ترتیب، آدرس IPv4 موردنظر معادل این آدرس IPv6 خواهد بود:

```
0000: 0000: 0000: 0000: 0000: 0000:c0a8:0120
```

جمع‌بندی

توسعه سیستم‌عامل UNIX مقارن با توسعه شبکه‌ای بود که امروزه آن‌را با عنوان اینترنت می‌شناسیم. پروتکل TCP/IP نیز جهت استفاده در شبکه اینترنت طراحی شد. سیستم‌عامل Linux به عنوان عضوی از خانواده UNIX امکانات قابل توجهی را به منظور بهره‌برداری از شبکه اینترنت در اختیار قرار می‌دهد.

شبکه به مجموعه‌ای متشکل از دو یا چند کامپیوتر اطلاق می‌شود که با یکدیگر در ارتباط باشند. شبکه محلی یا LAN به شبکه‌ای گفته می‌شود که فاصله کامپیوترهای مستقر در آن زیاد نباشد. شبکه‌های مقیاس وسیع یا WAN مجموعه‌ای از شبکه‌های محلی است که معمولاً فاصله قابل توجهی از یکدیگر دارند. با این مشخصات، شبکه جهانی اینترنت بزرگترین شبکه WAN محسوب می‌شود. در مجموع سرعت انتقال داده‌ها در شبکه‌های محلی بیشتر از شبکه‌های مقیاس بزرگ است. در هر صورت، برقراری ارتباط و انتقال داده‌ها در هر نوع شبکه‌ای مستلزم در اختیار داشتن اسامی کامل حوزه‌ها، اسامی میزبان‌ها، آدرس‌های IP و آدرس‌های سخت‌افزاری است.

پروتکل‌های شبکه از جمله TCP/IP، NetBEUI و IPX/SPX شامل مجموعه‌ای از پروتکل‌ها هستند. اغلب به چنین مجموعه‌هایی protocol stack گفته می‌شود. اغلب پروتکل‌های شبکه بر اساس مدل هفت لایه OSI طراحی شده‌اند.

از آن‌جا که مجموعه پروتکل TCP/IP زبان اینترنت است یک پروتکل بسیار مهم محسوب می‌شود. این مجموعه پروتکل بر اساس یک مدل چهار لایه با همین نام توسعه یافته است. عملکرد هریک از پروتکل‌ها و سرویس‌های این مجموعه از جمله FTP، HTTP، SNMP، TCP، UDP و IP را به خوبی

می‌توان در قالب این لایه‌ها توصیف کرد. سرویس‌ها DNS، DHCP و ARP از جمله سایر سرویس‌های مهمی هستند که در قالب این مجموعه پروتکل پیاده‌سازی شده‌اند.

تمام کامپیوترهای مستقر روی یک شبکه TCP/IP باید دارای آدرس IP منحصر به فرد باشند. سال‌هاست که از روشی با عنوان IPv4 برای آدرس‌دهی IP استفاده می‌شود. کلیه این آدرس‌ها در قالب پنج کلاس مختلف دسته‌بندی شده‌اند. به دلیل محدودیت در تعداد آدرس‌های تعیین شده به روش IPv4، طراحان مربوطه روش دیگری با عنوان IPv6 را برای جای‌گزینی آن با IPv4 ابداع کرده‌اند. با وجود این، آدرس‌دهی به روش IPv4 هم‌چنان متداول است، به ویژه این‌که به هر آدرس IP تولید شده به روش IPv4 یک آدرس متناظر که به روش IPv6 تولید شده است، تخصیص می‌یابد.

در فصل بعد با نحوه پیکربندی کامپیوترهای مستقر در شبکه و هم‌چنین پیکربندی خود شبکه آشنا می‌شوید. علاوه بر این، چگونگی اتصال یک شبکه Linux به شبکه جهانی اینترنت را فرامی‌گیرید.

فصل بیست‌ویکم

مدیریت شبکه‌های Linux

پس‌ازمطالعه جنبه‌های نظری شبکه در فصل‌بیستم، اکنون‌آماده‌ایم تا به طور عملی قابلیت سیستم‌عامل Linux را در ارتباط با شبکه مورد بررسی قرار دهیم.

ابتدا مختصری درباره تجهیزات سخت‌افزاری شبکه صحبت خواهیم کرد. چنان‌که خواهید دید، هاب وسیله‌ای است که کامپیوترهای مستقر در یک شبکه محلی (اصطلاحاً LAN) را به یکدیگر متصل می‌کند. سوییچ وسیله‌ای است که یک شبکه محلی را به بخش‌های مختلف تقسیم می‌کند به طوری که کنترل ترافیک شبکه را می‌توان به طور مؤثرتری انجام داد. روتر نیز وسیله‌ای است که چندین شبکه را به یکدیگر متصل کرده و به این ترتیب ترافیک جاری شده از یک شبکه را به شبکه دیگر هدایت می‌کند.

سپس فرآیند پیکربندی نمونه‌ای از یک کامپیوتر مستقر در شبکه را جهت دستیابی به شبکه و استفاده از آن مورد بررسی قرار خواهیم داد. در این فرآیند، ابتدا باید کارت شبکه متصل به کامپیوتر را پیکربندی کنید. (این کار مستلزم استفاده از فرامین ifconfig و arp است.) برای پیکربندی نام کامپیوتر در شبکه‌های معمولی و NIS (اصطلاحاً Network Information System) می‌توانید از فرامین متعددی استفاده کنید. چنان‌چه فرآیند پیکربندی را به طور صحیح انجام دهید، تنظیمات مربوطه را می‌توانید در قالب فایل‌هایی چون /etc/hosts ، /etc/host.conf ، /etc/sysconfig/network و /etc/resolve.conf مشاهد کنید.

پس از پیکربندی کامپیوتر مستقر در شبکه به بررسی نحوه پیکربندی یک شبکه محلی با آدرس‌های خصوصی IPv4 خواهیم پرداخت. چنان‌که خواهید دید، در صورت استفاده از آدرس‌های IPv4 فرآیند پیکربندی شبکه محلی به سادگی امکان‌پذیر خواهد بود. با پیکربندی نحوه مسیریابی و استفاده از یک آدرس IPv4 عمومی می‌توان یک چنین شبکه محلی را به شبکه اینترنت متصل کرد.

در سیستم‌عامل Red Hat Linux ابزارهای متنوعی برای اتصال کامپیوتر میزبان به شبکه اینترنت پیش‌بینی شده است. برخی از این ابزارها مانند Internet Configuration Wizard دارای رابط گرافیکی بوده و برخی نیز مانند minicom تنها از طریق سطر فرمان قابل استفاده هستند (هر دو ابزار مذکور توسط شرکت Red Hat توسعه یافته است).

در پایان فصل فرامینی را بررسی خواهیم کرد که استفاده از آن‌ها کمک شایانی را به منظور رفع اشکالات شبکه در اختیار قرار می‌دهد. چنان‌که خواهید دید، به کمک فرمان netstat می‌توان ترافیک پورت‌های مختلف TCP/IP را اندازه‌گیری کرد و به کمک فرمان ping از صحت اتصال مطمئن شد. هم‌چنین با بهره‌گیری از فرمان traceroute می‌توان مسیری را مشخص کرد که توسط بسته‌های ارسالی از مبدأ به مقصد در یک شبکه مقیاس بزرگ مانند اینترنت طی شده است. به طور خلاصه، در فصل حاضر به بررسی این موضوعات می‌پردازیم:

- آشنایی با تجهیزات سخت‌افزاری شبکه
- نحوه پیکربندی کامپیوترهای مستقر در شبکه
- نحوه پیکربندی شبکه‌های خصوصی و عمومی
- نحوه اتصال شبکه محلی به اینترنت
- اشکال‌زدایی شبکه

آشنایی با تجهیزات سخت‌افزاری شبکه

پیش از پرداختن به نحوه پیکربندی کامپیوتر برای استقرار در شبکه Linux اجازه دهید مقداری به عقب بازگشته و به لایه فیزیکی شبکه بیندیشیم. بیشتر مشکلات شبکه از نوع فیزیکی هستند. کابل‌های ضعیف، قطعی اتصالات، نشست گرد و غبار روی مدارهای الکترونیکی هاب یا روتر و مسایلی از این قبیل از جمله علت‌های متداول خرابی شبکه محسوب می‌شوند. با توجه به مدل OSI که در فصل بیستم مورد بررسی قرار گرفت، تجهیزات سخت‌افزاری یک شبکه محلی را می‌توان در یکی از این پنج گروه دسته‌بندی کرد:

- رسانه‌های انتقال در لایه فیزیکی
- هاب لایه فیزیکی
- سوییچ لایه پیوند داده‌ها
- روتر لایه شبکه
- دروازه‌های لایه برنامه کاربردی

رسانه‌های انتقال

انتقال‌داده‌ها از یک کامپیوتر به کامپیوتر دیگر از شبکه درقالب مجموعه‌هایی از صفر و یک‌ها و از طریق

رسانه انتقال انجام می‌شود. این داده‌ها ممکن است به صورت سیگنال‌های الکتریکی از طریق کابل منتقل شود یا این‌که به صورت علایم نوری از طریق فیبرهای نوری منتقل شود یا حتی به صورت امواج رادیویی در هوا منتشر شود. در هر صورت، عملکرد رسانه انتقال به لایه فیزیکی مدل OSI مربوط می‌شود.

تمام رسانه‌های مورد استفاده برای انتقال داده‌ها مشمول محدودیت‌هایی هستند. برای مثال، چنان‌چه در یک شبکه Ethernet طول زوج سیم به هم‌تابیده (اصطلاحاً twisted pair) که هر کدام از کامپیوترها را به هاب متصل کرده بیش از ۱۰۰ متر باشد، عملکرد شبکه نامطلوب خواهد بود. ملاحظات مربوط به رسانه‌های مورد استفاده برای انتقال داده‌ها را به طور خلاصه می‌توان به این صورت بیان کرد:

- **بازبینی اتصالات:** علت بسیاری از خرابی‌های شبکه را می‌توان در اتصال نادرست کابل‌ها جستجو کرد. از این‌رو، همواره باید این اتصالات را مورد بازبینی قرار دهید.
- **استفاده از کابل‌هایی با طول مناسب:** یکی از عوامل محدودیت عملکرد شبکه‌ها طول کابل‌های مورد استفاده برای انتقال داده‌هاست. برای مثال، چنان‌چه طول کابل‌های استاندارد Category 5 (یا به اختصار Cat 5) مورد استفاده در شبکه‌های Fast Ethernet بیش از ۱۰۰ متر باشد، نمی‌توان از حداکثر ظرفیت آن کابل‌ها استفاده کرد.
- **استفاده صحیح از کابل‌ها:** کابل‌ها را بیش از اندازه خم نکنید، چرا که در این صورت بخشی از کابل کشیده شده و به این ترتیب قابلیت انتقال داده‌ها در آن قسمت از کابل کاهش می‌یابد.

هاب

هاب کانون بسیاری از شبکه‌های محلی مدرن را تشکیل می‌دهد. نوع سیمی هاب جعبه‌ای شامل چند محل اتصال کابل است. از طریق این اتصالات و با بهره‌گیری از کابل مناسب می‌توان کامپیوترها را به هاب متصل کرد. پیکربندی کامپیوترهای متصل به یک هاب شبیه پره‌هایی است که به مرکز یک چرخ متصل شده‌اند. به این نوع پیکربندی اصطلاحاً star گفته می‌شود.

توان سیگنال‌ها با فاصله بین مبدأ و مقصد رابطه معکوس دارد، به طوری که با افزایش این فاصله توان سیگنال کاهش می‌یابد. هاب این قابلیت را دارد که سیگنال دریافتی را مجدداً بازسای کرده و با همان توان اولیه به مقصد ارسال کند. از آن‌جا که داده‌ها در قالب مجموعه‌هایی از صفر و یک‌ها انتقال می‌یابد، هاب را می‌توان در لایه فیزیکی مدل OSI نیز مورد استفاده قرار داد.

سوییچ

سوییچ نوعی تجهیزات سخت‌افزاری است که اغلب به منظور تقسیم شبکه‌های محلی بزرگ به دو یا چند قسمت مورد استفاده قرار می‌گیرد. به دلیل آن‌که سوییچ از کلیه آدرس‌های سخت‌افزاری کامپیوترهای شبکه مطلع است می‌توان آن‌را در لایه دوم مدل OSI یعنی لایه پیوند داده‌ها مورد استفاده قرار داد.

پس از برقراری نخستین ارتباط میان دو کامپیوتر از یک شبکه، تبادل داده‌ها میان آن دو از طریق آدرس‌های سخت‌افزاری مربوطه صورت می‌گیرد. به دلیل اطلاع سوییچ از تمام آدرس‌های سخت‌افزاری کامپیوترهای مستقر در شبکه، مشابه هاب از قابلیت بازسازی کلیه پیغام‌ها و ارسال آن‌ها به مقصد نیز برخوردار است.

گاهی اوقات برای اشاره به سوییچ‌های قدیمی از واژه پل (اصطلاحاً bridge) استفاده می‌شود. هم سوییچ‌های قدیمی و هم‌سوییچ‌های جدید به منظور سرویس‌دهی در لایه دوم مدل OSI طراحی شده‌اند.

روتر

این نوع تجهیزات سخت‌افزاری قادر است داده‌ها را بین دو یا چند شبکه محلی انتقال دهد. هر روتر از طریق یک کارت شبکه مجزا به هرکدام از شبکه های محلی متصل می‌شود. در شبکه‌های TCP/IP هر کارت شبکه دارای یک آدرس IP منحصر به فرد است. از این‌رو، روترها در لایه شبکه مدل OSI مورد استفاده قرار می‌گیرند.

در برخی موارد، آدرس دروازه شبکه (اصطلاحاً gateway) که در یک فایل پیکربندی مانند /etc/sysconfig/network به ثبت رسیده است، نماینده آدرس IP روتر متصل به آن شبکه است.

در صورت تمایل می‌توان کامپیوتری با سیستم‌عامل Linux را به عنوان یک روتر پیکربندی کرد. برای این منظور باید دو یا چند کارت شبکه را به چنین کامپیوتری متصل کنید. (تعداد کارت‌های شبکه به تعداد شبکه‌های محلی بستگی دارد که از طریق کامپیوتر مزبور به یکدیگر متصل خواهند شد.) سپس لازم است قابلیت IP Forwarding هسته سیستم‌عامل Linux را فعال کنید. این اقدام را می‌توان با تغییر تنظیمات ساده‌ای در فهرست proc/ به این صورت انجام داد:

```
# echo 1 > /proc/sys/net/ipv4/ip_forward
```

در صورت لزوم، با تغییر پیکربندی چنین روتری می‌توان عملکرد آن‌را تا اندازه سوییچ (یا حتی هاب) کاهش داد. برای اطمینان از این‌که تغییرات فوق طی راه‌اندازی‌های بعدی کامپیوتر هم‌چنان حفظ می‌شود، کافی است متغیر net.ipv4.ip_forward از فایل پیکربندی /etc/sysctl.conf را به این صورت مقداردهی کنید:

```
net.ipv4.ip_forward = 1
```

دروازه

عملکرد دروازه از بسیاری جهات شبیه به روتر است. برای مثال، شبکه‌ای را در نظر بگیرید که از طریق یک کارت Ethernet (با مشخصه eth0) و به واسطه یک روتر به شبکه‌ای دیگر متصل شده باشد. چنین اتصالی را می‌توان در فایل ifcfg-eth0 از فهرست /etc/sysconfig/networking/devices به عنوان آدرس IP دروازه مشخص کرد.

دروازه دارای این قابلیت است که چند شبکه محلی با پروتکل‌های مختلفی چون TCP/IP و IPX/SPX را به یکدیگر متصل کند. این نوع تجهیزات سخت‌افزاری در لایه برنامه کاربردی مدل OSI مورد استفاده قرار می‌گیرد.

پیکربندی کارت شبکه

با وجودی که سیستم‌عامل Red Hat Linux اقدامات لازم برای پیکربندی کارت شبکه کامپیوتر میزبان را جهت دستیابی به شبکه محلی انجام می‌دهد، به دلایل متعدد ممکن است مایل باشید تا این پیکربندی را تغییر دهید. برای مثال، فرض کنید سیستم‌عامل Linux را روی کامپیوتر قابل حمل نصب کرده و اکنون قصد دارید تا آن کامپیوتر را به یک شبکه محلی متصل کنید. یا این‌که کارت شبکه دیگری را روی کامپیوتر میزبان نصب کرده و اکنون باید آن‌را پیکربندی کنید. علاوه بر موارد فوق، چنان‌چه سیستم‌عامل Red Hat Linux به هر دلیل قادر به تشخیص کارت شبکه نباشد باید آن‌را به طور دستی پیکربندی کنید. در تمام موارد فوق و موارد مشابه باید کامپیوترهای موردنظر را جهت دستیابی به شبکه پیکربندی کنید.

ضمن فرآیند نصب سیستم‌عامل Red Hat Linux پیکربندی کارت شبکه نیز به طور خودکار انجام می‌شود. چنان‌چه کارت شبکه مورد استفاده توسط این سیستم‌عامل قابل شناسایی باشد، در صورت وجود سرور DHCP در شبکه (یا به بیان دیگر، کامپیوتری که سرویس Dynamic Host Configuration Protocol روی آن راه‌اندازی شده باشد)، یک آدرس IP منحصر به فرد به کارت شبکه کامپیوتر میزبان تخصیص داده می‌شود. در غیر این صورت، باید آدرس IP و سایر اطلاعات مربوطه را به طور دستی وارد

کنید. چنان‌چه کامپیوتر میزبان را به یک شبکه محلی از نوع NIS متصل کرده باشید، ممکن است لازم باشد تا این اطلاعات را ضمن نصب سیستم‌عامل Red Hat Linux مشخص کنید. شبکه‌های NIS را در فصل بیست‌وهشتم مورد بررسی قرار خواهیم داد.

هنگام مواجهه با هر گونه مشکلی باید دقیقاً بدانید که برای رفع آن از کجا اقدام کنید. در ارتباط با شبکه، برای این منظور می‌توانید از دو فرمان ifconfig و arp (به منظور پیکربندی کارت شبکه) و فرامین مشابه استفاده کنید.

هم‌چنین باید با فایل‌های پیکربندی شبکه نیز آشنا باشید. چنان‌که به زودی خواهید دید، فایل /etc/sysconfig/network یکی از فایل‌های پیکربندی مهم در این زمینه محسوب می‌شود.

پیکربندی کارت شبکه با استفاده از فرمان ifconfig

فرمان ifconfig را می‌توان مهمترین فرمان پیکربندی شبکه در سیستم‌عامل Linux دانست. فایل برنامه این فرمان در فهرست /sbin واقع است. این فرمان امکانات لازم برای تخصیص آدرس IP، پورت سخت‌افزاری، تعیین ماسک مورد استفاده و هم‌چنین فعال و غیرفعال کردن کارت شبکه را در اختیار قرار می‌دهد. بازبینی پیکربندی موجود کارت شبکه نیز با استفاده از این فرمان امکان‌پذیر است. برای مثال، با توجه به شکل ۱-۲۱ می‌توان دو کارت شبکه فعال را تشخیص داد. اولی یک کارت شبکه Ethernet با مشخصه eth0 و دومی مکانیزمی از نوع loopback با مشخصه lo است. چنان‌که مشاهده می‌کنید، کارت شبکه eth0 جهت اتصال به شبکه محلی پیکربندی شده است.

```
[root@RH9Test root]# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:40:F4:3C:05:58
          inet addr:10.252.113.3  Bcast:10.252.113.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:9 errors:0 dropped:0 overruns:0 frame:0
          TX packets:8 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:1640 (1.6 Kb)  TX bytes:1632 (1.5 Kb)
          Interrupt:5 Base address:0x8000

lo        Link encap:Local Loopback
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:67692 errors:0 dropped:0 overruns:0 frame:0
          TX packets:67692 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:4624266 (4.4 Mb)  TX bytes:4624266 (4.4 Mb)

[root@RH9Test root]#
```

شکل ۱-۲۱ نتیجه اجرای فرمان ifconfig

چنان‌که گفته شد، تخصیص یک آدرس IP جدید به کارت شبکه با استفاده از فرمان ifconfig به سادگی امکان‌پذیر است. برای مثال، این فرمان آدرس Ipv4 جدیدی را به کارت شبکه eth1 تخصیص می‌دهد:

```
# ifconfig eth1 10.122.238.3
```

همان‌گونه که در قسمت‌های بعد از همین فصل خواهید دید، ماسک استاندارد شبکه برای آدرس IP فوق عبارت از 255.0.0.0 است. با وجود این، در صورت تمایل می‌توانید ماسک دیگری را به این صورت مورد استفاده قرار دهید:

```
# ifconfig eth1 netmask 255.255.255.0 10.122.238.3
```

در نسخه‌های قبلی سیستم‌عامل Red Hat Linux همواره مشکلاتی در ارتباط با تخصیص پورت‌های IRQ یا آدرس‌های ورودی و خروجی به دومین کارت شبکه نصب شده روی کامپیوتر به وجود می‌آمد. فرمان ifconfig امکان تخصیص آدرس‌های سخت‌افزاری مختلفی را به یک کارت شبکه در اختیار می‌گذارد. برای مثال، با اجرای این فرامین پورت IRQ 9 و آدرس ورودی و خروجی 0x300 به دومین کارت شبکه نصب شده روی کامپیوتر میزبان (با مشخصه eth1) تخصیص داده می‌شود:

```
# ifconfig eth1 irq 9
# ifconfig eth1 io_addr 0x300
```

همان طور که شکل ۱-۲۱ نیز نشان می‌دهد، این تنظیمات در خروجی فرمان ifconfig با عناوین Interrupt و Base address مشخص می‌شوند. مواجهه با خطا در اجرای فرامین فوق ممکن است به این دلیل باشد که قبلاً پورت IRQ و آدرس ورودی و خروجی تخصیص داده شده یا این‌که پورت IRQ و آدرس ورودی و خروجی موردنظر به منظور دیگری رزرو شده است.

فعال و غیرفعال کردن کارت شبکه نیز با استفاده از فرمان ifconfig به سادگی امکان‌پذیر است. برای مثال، این فرامین را به ترتیب می‌توان جهت فعال و غیرفعال کردن نخستین کارت شبکه Ethernet با مشخصه eth0 مورد استفاده قرار داد:

```
# ifconfig eth0 down
# ifvonfig eth0 up
```

پیکربندی کارت شبکه با استفاده از فرمان arp

فرمان arp برای تخصیص آدرس‌های IP به آدرس‌های سخت‌افزاری کارت‌های شبکه مورد استفاده قرار می‌گیرد. پس از برقراری نخستین ارتباط میان دو کامپیوتر از یک شبکه، آدرس‌های سخت‌افزاری میان آن دو رد و بدل شده و روی هریک از کامپیوترها ذخیره می‌شود. با استفاده از فرمان arp می‌توان این اطلاعات را مورد بازبینی قرار داد. به نمونه‌ای از خروجی فرمان arp توجه کنید:

```
# arp
Address         Hwtype  HWaddress           Flags Mask   Iface
192.168.7.2     ether   00:12:B5:64:3B:B2   C            eth0
RH91aptop       ether   00:60:0B:8A:41:93   C            eth0
192.168.7.2     ether   52:AS:CB:32:52:A2   C            eth0
experimental    ether   00:20:78:09:D3:6A   C            eth0
```

بسته به نوع اتصال، ستون Address ممکن است حاوی آدرس IP یا نام یک کامپیوتر راه دور باشد. نام کامپیوتر با توجه به فایل /etc/hosts تعیین می‌شود. ستون HWtype نوع کارت شبکه را نشان می‌دهد. ستون HWaddress نیز حاوی لیست آدرس‌های سخت‌افزاری است که با استفاده از ارقام هگزادسیمال نشان داده می‌شود.

چنان‌که در این مثال مشاهده می‌کنید، به دو کارت شبکه مختلف یک آدرس IP واحد تخصیص داده شده است. چنین وضعیتی می‌تواند منجر به اختلال در شبکه شود. برای حذف مشخصات کامپیوتر موردنظر از جدول فوق کافی است فرمان arp -d *computername* را که در آن متغیر computername بیانگر آدرس IP یا نام کامپیوتر موردنظر است، اجرا کنید.

فرامین مربوط به پیکربندی نام میزبان

برای تعریف یا مشاهده لیست اسامی یک کامپیوتر در شبکه‌های مختلف فرامین متعددی را می‌توان مورد استفاده قرار داد. شرح این فرامین در جدول ۱-۲۱ آمده است. منهای فرمان dnsdomainname، به کمک هریک از این فرامین می‌توان نام کامپیوتر موردنظر را تعریف کرد. برای مثال، فرمان hostname ilovehackers نام کامپیوتر میزبان را به ilovehackers تغییر می‌دهد.

جدول ۱-۲۱ فرامین مربوط به پیکربندی نام میزبان

عنوان فرمان	توضیح
hostname	این فرمان امکان تعریف نام کامپیوتر میزبان یا نمایش نام فعلی آن‌را در اختیار قرار می‌دهد.
domainname	این فرمان امکان تعریف نام حوزه NIS کامپیوتر میزبان یا نمایش نام حوزه NIS فعلی آن‌را در اختیار قرار می‌دهد.
dnsdomainname	این فرمان نام کامل حوزه یا اصطلاحاً FQDN سرور DNS مستقر در شبکه را نمایش می‌دهد.
nisdomainname	عملکرد این فرمان مشابه فرمان domainname است.
ypdomainname	عملکرد این فرمان مشابه فرمان domainname است.

فایل‌های پیکربندی شبکه

سیستم‌عامل Red Hat Linux از فایل‌های متعددی به منظور پیکربندی شبکه استفاده می‌کند. برخی از این فایل‌های پیکربندی از جمله /etc/hosts، /etc/resolve.conf و /etc/host.conf را می‌توان در سایر نسخه‌های سیستم‌عامل Linux نیز یافت. علاوه بر این گونه فایل‌های پیکربندی، سیستم‌عامل Red Hat Linux حاوی فایل‌های پیکربندی دیگری است که در فهرست /etc/sysconfig مستقر شده است.

به نظر می‌رسد که شرکت Red Hat خط‌مشی یکپارچه‌سازی فایل‌های پیکربندی، به ویژه در مورد تنظیمات شبکه را دنبال می‌کند. (وجود مجموعه‌ای از فایل‌های پیکربندی در فهرست /etc/sysconfig دلیل بر این مدعاست.) چنان‌چه از موقعیت فایل پیکربندی موردنظر خود مطلع نیستید، توصیه می‌کنیم جستجو را همواره از این فهرست آغاز کنید.

اسامی استاتیک میزبان‌ها: فایل پیکربندی /etc/hosts

در نخستین روزها پس از ظهور شبکه جهانی ARPAnet تنها کامپیوترهای معدودی به آن دسترسی داشتند. این مجموعه کوچک متشکل از کامپیوترهایی با سیستم‌عامل UNIX بود و روی هرکدام از آن‌ها یک فایل استاتیک با عنوان /etc/hosts لیستی از اسامی کامپیوترهای مستقر در شبکه و آدرس‌های IP متناظر با هریک از آن‌ها نگهداری می‌شد. چنان‌چه یک دانشگاه یا سازمان دولتی قصد داشت کامپیوتر جدیدی را روی این شبکه مستقر کند، کافی بود نام و آدرس IP آن کامپیوتر در فایل /etc/hosts درج شده و نسخه جدید آن فایل مجدداً بین تمام کامپیوترهای مستقر در شبکه توزیع شود.

با وجودی که استفاده از فایل /etc/hosts برای ثبت مشخصات کامپیوترهای مستقر در شبکه اینترنت عملاً غیرممکن است، بهره‌برداری از این مکانیزم در شبکه‌های کوچک‌تر کاملاً عملی است. تنها نکته مهم این است که باید نسخه جدیدی از این فایل را بعد از نصب یک یا چند کامپیوتر در شبکه مابین تمام کامپیوترهای مستقر در آن شبکه توزیع کرد.

ساختار فایل /etc/hosts بسیار ساده است. هر خط از این فایل شامل یک آدرس IP، نام کامل حوزه یا نام میزبان است. به خط نمونه‌ای از این فایل توجه کنید:

```
192.168.23.121    linux.mommabears.com    linux1
```

مشخصات سرورهای DNS: فایل پیکربندی /etc/resolve.conf

به جای توزیع فایل /etc/hosts در میان تمام کامپیوترهای مستقر در شبکه، می‌توان از سرویسی با عنوان Domain Name Service یا به اختصار DNS استفاده کرد. در سیستم‌عامل Linux سرویس DNS نسخه‌ای از سرویس Berkeley Internet Name Domain (به اختصار BIND) است که با استفاده از شبح named تا حد امکان ساده شده است. (در فصل بیست و چهارم سرویس DNS را مورد بررسی قرار خواهیم داد.) برای بهره‌برداری از این مکانیزم کافی است آدرس IP سرور یا سرورهای DNS (کامپیوترهای میزبان سرویس DNS) را در فایل پیکربندی /etc/resolve.conf درج کنید.

ساخار فایل مزبور بسیار ساده است، به طوری که هریک از خطوط آن حاوی نام سرور DNS و آدرس IP مربوطه است. در صورتی که از طریق یک مرکز ISP به شبکه اینترنت متصل می شوید، ممکن است لازم باشد تا آدرس IP سرور DNS مستقر در آن مرکز را در فایل پیکربندی /etc/resolve.conf درج کنید. به خط نمونه‌ای از این فایل توجه کنید:

```
nameserver 207.217.126.81
```

ترتیب جستجوی میزبان‌ها: فایل پیکربندی /etc/host.conf

چنان‌که در قسمت‌های قبل گفته شد، برای نگهداری اسامی کامپیوترهای مستقر در شبکه و آدرس‌های IP مربوطه می‌توان از فایل پیکربندی /etc/hosts یا سرور DNS استفاده کرد. ترتیب جستجوی کامپیوترها را می‌توان با استفاده از فایل پیکربندی /etc/host.conf مشخص کرد. محتوای این فایل معمولاً تنها شامل یک خط است. به نمونه‌ای از محتوای این فایل توجه کنید:

```
order hosts,bind
```

با توجه به خط فوق، کامپیوتر میزبان برای جستجوی آدرس IP موردنظر ابتدا فایل /etc/hosts را مورد توجه قرار داده و سپس به سرور DNS مراجعه می‌کند. (چنان‌که در قسمت آخر این فصل خواهید دید، اصطلاح bind در سیستم‌عامل Linux برای اشاره به سرور DNS مورد استفاده قرار می‌گیرد.) در صورت تمایل حتی می‌توان سرور NIS را نیز در لیست جستجوی فوق قرار داد. (برای اطلاع بیشتر در این زمینه می‌توانید بحث مربوط به فایل پیکربندی /etc/nsswitch.conf از فصل بیست و چهارم را مطالعه کنید.)

تنظیمات ابتدایی شبکه: فایل پیکربندی /etc/sysconfig/network

تنظیمات ابتدایی شبکه در فایل پیکربندی /etc/sysconfig.network درج شده است. در صورت مشاهده هرگونه مشکلی در ارتباط با عملکرد شبکه، می‌توانید فرآیند عیب‌یابی را با بررسی محتوای این

فایل آغاز کنید. در ابتدای این فایل متغیر NETWORKING به صورت NETWORKING=yes مقداردهی شده است. جدول ۲-۲۱ مفهوم متغیر فوق و سایر متغیرهای مورد استفاده در این فایل را نشان می‌دهد. در صورت استفاده از سرور DHCP در شبکه، نیازی به مقداردهی برخی از این متغیرها نیست. برخی دیگر از این متغیرها را می‌توان از طریق فایل‌های پیکربندی موجود در فهرست /etc/sysconfig/networking/devices مقداردهی کرد. (فهرست مزبور شامل فایل‌های پیکربندی کارت‌های شبکه است.)

جدول ۲-۲۱ متغیرهای موجود در فایل پیکربندی /etc/ysconfig/network

عنوان متغیر	توضیح
NETWORKING	چنان‌چه مقدار این متغیر برابر با yes باشد، سیستم‌عامل Red Hat Linux امکانات استفاده از شبکه را در اختیار قرار می‌دهد.
HOSTNAME	این متغیر بیانگر نام کامپیوتر میزبان است.
GATEWAY	این متغیر بیانگر آدرس IP دروازه کامپیوتر میزبان است.
GATEWAYDEV	این متغیر بیانگر مکانیزمی (هم‌چون eth1) است که امکان اتصال به شبکه را از طریق دروازه فراهم می‌کند. چنان‌چه بیش از یک کارت شبکه روی کامپیوتر میزبان نصب شده باشد، استفاده از این متغیر ضروری است.
NISDOMAIN	در صورتی که شبکه از نوع NIS باشد، این متغیر بیانگر نام حوزه کامپیوتر میزبان است.

پیکربندی شبکه‌های خصوصی و عمومی

در فصل بیستم با اصول آدرس‌دهی به شیوه IPv4 آشنا شدید. در این قسمت نحوه بهره‌برداری از این روش آدرس‌دهی را به منظور پیکربندی یک شبکه محلی جهت اتصال به اینترنت مورد بررسی قرار می‌دهیم.

هنگام پیکربندی شبکه محلی برای اتصال به اینترنت بدیهی است که نمی‌توان از هر آدرس IP دلخواهی استفاده کرد. با وجودی که در شبکه‌های محلی می‌توان مجموعه‌ای از آدرس‌های IP خصوصی را مورد استفاده قرار داد، برای اتصال هر شبکه محلی به اینترنت وجود دست‌کم یک آدرس IP عمومی ضروری است. از طریق این آدرس IP عمومی تمام کامپیوترهای مستقر در شبکه می‌توانند به طور هم‌زمان به شبکه اینترنت دسترسی داشته باشند.

متأسفانه در حال حاضر بیشتر آدرس‌های IP عمومی اشغال شده و آدرس‌های باقیمانده عموماً از طریق مراکز ISP واگذار می‌شود.

آدرس‌های IP عمومی به منظور ارتباط بین کامپیوترها و شبکه‌های مستقر در اینترنت مورد استفاده قرار می‌گیرد. از سوی دیگر، آدرس‌های IP یکسانی را می‌توان در شبکه‌های خصوصی مختلف مورد استفاده قرار داد. به این دلیل، آدرس‌های IP خصوصی برای برقراری ارتباط میان کامپیوترهای مستقر در شبکه اینترنت معتبر نیستند.

استفاده از آدرس‌های IP خصوصی در شبکه‌های محلی بلامانع است. چنین شبکه‌ای را می‌توان از طریق دروازه‌ای با آدرس IP عمومی به اینترنت متصل کرد. برای دستیابی به آدرس IP عمومی باید با یکی از مراکز IP مذاکره کنید. در صورت توافق، مرکز ISP یک آدرس IP استاتیک با ماسک شبکه را در اختیار قرار داده یا دستورالعمل‌های لازم برای دستیابی به آدرس IP موردنظر از طریق یک سرور DHCP را دریافت خواهید کرد.

تعریف چند اصطلاح

پیش از پرداختن به ادامه موضوع، اجازه دهید تا با چند اصطلاح مهم در ارتباط با آدرس IP آشنا شویم:

- **آدرس شبکه:** هر آدرس IP از دو بخش تشکیل می‌شود. بخش نخست شامل آدرس شبکه بوده و بخش دوم شاخصی است متشکل از چند عدد که یک کامپیوتر به خصوص را روی آن شبکه مشخص می‌کند. آدرس شبکه یک آدرس IP است که شبکه‌ای را مشخص می‌کند. برای مثال، آدرس شبکه‌ای مانند 192.168.22.0 از نوع آدرس C بوده و شبکه‌ای با محدوده آدرس‌های 192.168.22.1 تا 192.168.22.254 را مشخص می‌کند.
- **ماسک شبکه:** ماسک شبکه یک آدرس IP به خصوص است که امکان تعریف محدوده‌ای از آدرس‌های IP یک شبکه محلی را در اختیار قرار می‌دهد. سه ماسک شبکه 255.0.0.0، 255.255.0.0 و 255.255.255.0 تنها ماسک‌های استاندارد هستند. به ماسک شبکه اغلب ماسک زیرشبکه (اصطلاحاً subnetwork mask یا subnet mask) نیز گفته می‌شود.
- **آدرس همگانی:** آدرس همگانی (اصطلاحاً broadcast address) یک آدرس IP به خصوص است که به منظور برقراری ارتباط با تمام کامپیوترهای مستقر در یک شبکه مورد استفاده قرار می‌گیرد.

آدرس همگانی هر شبکه آخرین آدرس IP قابل تعریف در آن شبکه است. برای مثال، در شبکه‌ای با آدرس 192.168.22.0 آدرس همگانی عبارت از 192.168.255.255 خواهد بود.

- **آدرس IP خصوصی:** آدرس IP به خصوصی است که به یک شبکه محلی خصوصی اختصاص می‌یابد. با این وجود آدرس می‌توان شبکه محلی موردنظر را از طریق کامپیوتری با آدرس IP عمومی به اینترنت متصل کرد. اغلب آدرس‌های IP یکسانی به عنوان آدرس IP خصوصی شبکه‌های مختلف مورد استفاده قرار می‌گیرند. با استفاده از آدرس IP خصوصی نمی‌توان شبکه محلی را مستقیماً به اینترنت متصل کرد.
- **آدرس IP عمومی:** آدرسی است که یک شبکه محلی با آدرس IP خصوصی می‌تواند از طریق آن به اینترنت متصل شود.
- **مکانیزم CIDR:** این مکانیزم با عنوان Classless Inter-Domain Routing روشی برای تعیین ماسک‌های غیراستاندارد شبکه است. به کمک مکانیزم می‌توان آدرس‌های IP استاندارد را به زیرمجموعه‌هایی تقسیم کرده یا آن‌ها را با یکدیگر ترکیب کرد.

شبکه‌های خصوصی

پیکربندی کامپیوترهای موجود در شبکه‌ای با آدرس‌های IP خصوصی مستلزم در اختیار داشتن آدرس شبکه و ماسک شبکه است. به کمک این دو عامل می‌توان محدوده آدرس‌های IP کامپیوترهای مستقر در شبکه را مشخص کرد. چنان‌که در فصل بیستم نیز اشاره شد، سه مجموعه از آدرس‌های IP را تحت عنوان سه کلاس A، B و C می‌توان برای این منظور مورد استفاده قرار داد. شرح این سه مجموعه در جدول ۳-۲۱ آمده است.

جدول ۳-۲۱ محدوده‌های مربوط به آدرس‌های IP خصوصی

عنوان کلاس	محدوده آدرس‌دهی	توضیح
A	از 10.0.0.1 تا 10.255.255.254	در این کلاس می‌توان حدود ۱۶ میلیون کامپیوتر را در قالب یک حوزه، آدرس‌دهی کرد.
B	از 172.168.0.1 تا 172.168.255.254	در این کلاس می‌توان حدود ۶۵۰۰۰ کامپیوتر را در قالب یک حوزه آدرس‌دهی کرد.
C	از 192.168.0.1 تا 192.168.255.254	در این کلاس می‌توان تعداد حداکثر ۲۵۴ کامپیوتر را در قالب یک حوزه آدرس‌دهی کرد.

در واقع با تعیین آدرس شبکه و ماسک شبکه در واقع یکی از محدوده‌های آدرس‌دهی جدول ۳-۲۱ مشخص می‌شود. برای مثال، چنان‌چه آدرس IP شبکه 10.0.0.0 و ماسک شبکه 255.255.255.0 باشد، محدوده آدرس‌های IP کامپیوترهای مستقر در شبکه موردنظر از 10.0.0.0 تا 10.0.0.255 خواهد بود که بالغ بر ۲۵۶ آدرس IP مختلف است. این مجموعه از آدرس‌ها در واقع نماینده یک زیرشبکه (اصطلاحاً subnetwork یا subnet) است.

همان گونه که از فصل بیستم به خاطر دارید، نخستین آدرس این زیرشبکه، یعنی 10.0.0.0 به عنوان آدرس شبکه و آخرین آدرس آن یعنی 10.0.0.255 به عنوان آدرس همگانی مورد استفاده قرار می‌گیرد. به این ترتیب، نمی‌توان دو آدرس فوق را به هیچ یک از کامپیوترهای مستقر در این زیرشبکه تخصیص داد. به بیان دیگر، تنها ۲۵۴ آدرس IP باقیمانده را می‌توان به کامپیوترهای مستقر دراین زیرشبکه تخصیص داد.

ماسک شبکه

به کمک ماسک شبکه می‌توان وجود آدرس IP به خصوصی را در یک شبکه محلی تشخیص داد. ماسک شبکه هم‌چنین امکان تشخیص آدرس شبکه از آدرس کامپیوترهای مستقر در شبکه را در اختیار قرار می‌دهد. با ترکیب آدرس شبکه و ماسک شبکه می‌توان محدوده آدرس‌های IP قابل تخصیص به کامپیوترهای مستقر در شبکه را تعیین کرد.

جدول ۴-۲۱ مثال‌هایی را در این مورد نشان می‌دهد. ستون "محدوده آدرس‌های IP قابل تخصیص" از این جدول شامل محدوده‌ای از آدرس‌های IP است که می‌توان به کامپیوترهای مستقر در شبکه تخصیص داد.

جدول ۴-۲۱ مثال‌هایی در مورد نحوه تعیین آدرس‌های IP قابل تخصیص به کامپیوترهای مستقر در یک شبکه با در دست داشتن آدرس و ماسک آن شبکه

آدرس شبکه	ماسک شبکه	محدوده آدرس‌های IP قابل تخصیص	تعداد آدرس‌های قابل تخصیص
10.0.0.0	255.0.0.0	از 10.0.0.1 تا 10.255.255.254	۱۶٫۷۷۷٫۲۱۴
10.21.92.0	255.255.255.0	از 10.21.92.1 تا 10.21.92.254	۲۵۴
10.182.0.0	255.255.0.0	از 10.182.0.1 تا 10.182.255.254	۶۵٫۵۳۴
172.168.78.0	255.255.255.0	از 172.168.78.1 تا 172.168.78.254	۲۵۴

آدرس شبکه	ماسک شبکه	محدوده آدرس‌های IP قابل تخصیص	تعداد آدرس‌های قابل تخصیص
172.168.0.0	255.255.0.0	از 172.168.0.1 تا 172.168.255.254	۶۵،۵۳۴
192.168.3.0	255.255.255.0	از 192.168.3.1 تا 192.168.3.254	۲۵۴

با توجه به جدول فوق، می‌توان این قوانین را در مورد نحوه آدرس‌دهی IP نتیجه گرفت:

- آدرس IP شبکه را نمی‌توان به هیچ یک از کامپیوترهای مستقر در شبکه تخصیص داد. این آدرس بخشی از آدرس IP کامپیوترهای شبکه را تشکیل می‌دهد.
- با استفاده از اعداد 255 در ساختار ماسک شبکه می‌توان به آدرس آن شبکه پی برد. برای مثال، چنان‌چه آدرس IP کامپیوتری از شبکه 10.162.4.23 و ماسک شبکه 255.255.255.0 باشد، آدرس آن شبکه 10.162.4.0 و شاخص آدرس IP کامپیوتر موردنظر 23 خواهد بود. برای اطلاع از موارد استثنای این قانون به قسمت "مکانیزم Classless Inter-Domain Routing یا CIDR" در همین فصل مراجعه کنید.
- آخرین آدرس IP از یک محدوده آدرس‌های IP مجاز آدرس همگانی آن شبکه محسوب می‌شود. برای مثال، آدرس همگانی شبکه مربوط به آخرین سطر جدول ۴-۲۱ عبارت از 192.168.3.255 است.
- سه ماسک شبکه 255.0.0.0، 255.255.0.0 و 255.255.255.0 تنها ماسک‌های استاندارد هستند. در قسمت "مکانیزم Classless Inter-Domain Routing یا CIDR" از همین فصل به بررسی ماسک‌های غیراستاندارد خواهیم پرداخت.

نحوه پیکربندی شبکه

پیش از پیکربندی پروتکل TCP/IP در یک شبکه محلی، ابتدا باید محدوده آدرس‌های IP قابل تخصیص به کامپیوترهای مستقر در آن شبکه را مشخص کنید. برای این منظور، چنان‌که در قسمت‌های قبل مشاهده کردید، ابتدا باید آدرس شبکه و ماسک شبکه را مشخص کنید. با در دست داشتن این دو عامل می‌توانید محدوده‌ای از آدرس‌های IP قابل تخصیص به کامپیوترهای مستقر در شبکه را مشخص کنید.

به احتمال قوی، ماسک شبکه 255.255.255.0 متداول‌ترین ماسک به شمار می‌رود. چنان‌که قبلاً نیز اشاره شد، با استفاده از این ماسک می‌توان تعداد ۲۵۴ آدرس IP را به کامپیوترهای مستقر در شبکه

تخصیص داد. برای مثال، در صورتی که آدرس شبکه 10.168.0.0 باشد، با بهره‌گیری از این ماسک می‌توان آدرس‌های 10.168.0.1، 10.168.0.2، 10.168.0.3 تا 10.168.0.254 را به ۲۵۴ کامپیوتر مستقر در شبکه تخصیص داد.

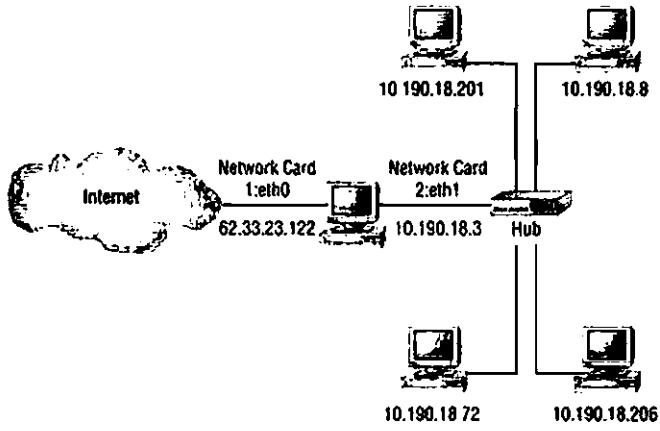
به خاطر داشته باشید که اولین و آخرین آدرس IP از محدوده آدرس‌های IP مجاز یک شبکه (یعنی آدرس‌های 10.168.0.0 و 10.168.0.255 در مثال فوق) به ترتیب آدرس شبکه و آدرس همگانی آن شبکه محسوب می‌شوند.

برای تخصیص آدرس‌های IP مجاز به کامپیوترهای مستقر در شبکه می‌توان به یکی از دو روش موجود اقدام کرد. در روش نخست، چنان‌که قبلاً نیز توضیح داده شد، باید با استفاده از فرامینی مانند ifconfig آدرس IP هر کامپیوتر را به طور جداگانه به آن تخصیص دهید. علاوه بر این، در روش فوق باید آدرس IP سرور DNS و دروازه پیش‌فرض را نیز به طور دستی مشخص کنید. برای اجتناب از روش دستی می‌توانید روش دوم یعنی استفاده از یک سرور DHCP را مورد توجه قرار دهید. برای این منظور، کافی است محدوده آدرس‌های IP مجاز را برای سرور DHCP مشخص کنید. همان گونه که در فصل بیست‌وچهارم خواهید دید، سرور DHCP می‌تواند آدرس‌های IP مجاز را به کامپیوترهای مستقر در شبکه تخصیص دهد. علاوه براین، سرور DHCP قادر است اطلاعات مربوط به سرور DNS و آدرس دروازه پیش‌فرض شبکه را بین کامپیوترهای مستقر در شبکه توزیع کند.

دروازه شبکه

دروازه شبکه کامپیوتری است که از یک سو به شبکه محلی و از سویی به یک شبکه دیگر مانند اینترنت متصل باشد. در شبکه‌های محلی اغلب تنها یک کامپیوتر مستقیماً به شبکه دیگر متصل است. بدیهی است چنین کامپیوتری باید دست‌کم دارای دو یا چند کارت شبکه باشد، به طوری که یکی از آن‌ها به شبکه محلی و آن یکی به شبکه دیگر متصل شود. در این پیکربندی، هر کارت شبکه دارای یک آدرس IP مستقل است. آدرس IP دروازه شبکه، به آدرس IP کارت شبکه‌ای اطلاق می‌شود که آن کامپیوتر را به شبکه محلی متصل می‌کند.

شکل ۲-۱۲ نمایی از این پیکربندی را که شامل پنج کامپیوتر است، نشان می‌دهد. کامپیوتری که بین هاب و شبکه اینترنت مستقر شده است نقش دروازه شبکه را ایفا می‌کند. آدرس IP دروازه شبکه از دید تمام کامپیوترهای مستقر در شبکه محلی عبارت از 10.190.18.3 است. این در واقع همان آدرسی است که دروازه شبکه برای ارتباط با سایر کامپیوترهای مستقر در شبکه محلی از آن استفاده می‌کند.



شکل ۲-۲۱ نمونه‌ای از یک شبکه محلی که از طریق دروازه به اینترنت متصل شده است.

چنان‌که مشاهده می‌کنید، آدرس IP تخصیص داده شده به دومین کارت شبکه (در این مورد 62.33.23.122) یک آدرس IP عمومی است.

مکانیزم Classless Inter-Domain Routing یا CIDR

اجازه دهید در همین ابتدا به این نکته اشاره کنیم که فراگیری مکانیزم Classless Inter-Domain Routing یا به اختصار CIDR مستلزم دقت فراوان است.

بیشتر اوقات تنها ماسک‌های شبکه موردنیاز در شبکه‌های IPv4 (شبکه‌هایی که آدرس‌دهی IP در آن به روش IPv4 انجام می‌شود.) همان ماسک‌های استاندارد، یعنی 255.0.0.0، 255.255.0.0 و 255.255.255.0 است. این سه ماسک شبکه به ترتیب متناظر با شبکه‌هایی از نوع کلاس A، B و C هستند.

به واسطه استفاده از سه ماسک شبکه فوق به سادگی می‌توان آدرس IP یک شبکه را از آدرس IP کامپیوترهای مستقر در آن شبکه تشخیص داد. برای مثال، چنان‌چه آدرس IP کامپیوتری از یک شبکه 192.168.38.48 و ماسک مورد استفاده در آن شبکه 255.255.255.0 باشد، می‌توان نتیجه گرفت که آدرس IP آن شبکه به طور قطع 192.168.38.0 است. به این ترتیب، آدرس IP سایر کامپیوترهای مستقر در آن شبکه از 192.168.38.1 تا 192.168.38.254 متغیر خواهد بود.

جایگاه بیت‌ها در آدرس‌های IPv4

برای درک مکانیزم CIDR لازم است با جایگاه بیت‌ها در آدرس‌های IPv4 آشنا شوید. هر آدرس IPv4 متشکل از ۳۲ بیت است. این بیت‌ها به چهار گروه یک بایتی با ارزش عددی صفر تا ۲۵۵ تقسیم می‌شوند. هر بایت متشکل از ۸ بیت و هر بیت نماینده یک عدد متفاوت است. برای مثال، این دو سطر را در نظر بگیرید:

```
  1    1    1    1    1    1    1    1
128   64   32   16    8    4    2    1
```

سطر بالا نماینده بیت‌های یک بایت و سطر پایین شامل اعداد دسیمال متناظر با آن بیت‌هاست. از این‌رو، ارزش عددی دو بایت 10000000 و 00010000 به ترتیب معادل با 128 و 16 است. ارزش بایت 11111111 معادل حاصل‌جمع 1+2+4+8+16+32+64+128 یعنی 255 است.

به عنوان مثال، فرض کنید می‌خواهیم شبکه‌ای از نوع کلاس C با آدرس 192.168.38.0 را پیکربندی کنیم. با وجودی که ممکن است قصد استفاده از هر ۲۵۴ آدرس IP قابل دسترس در این کلاس را نداشته باشیم، می‌توانیم از مکانیزم CIDR به عنوان روش مفیدی برای پیکربندی دو شبکه محلی واقع در دو ساختمان مختلف بهره‌برداری کرده و آدرس‌های IP موجود را به کامپیوترهای مستقر در این دو شبکه محلی تخصیص دهیم.

برای درک بهتر موضوع اجازه دهید تا کمی به عقب بازگشته و بیت‌های تشکیل دهنده آدرس‌های IP را مجدداً مورد توجه قرار دهیم. این دو مجموعه از بیت‌ها را که نماینده دو آدرس IP یعنی 192.168.38.48 و 255.255.255.0 هستند، در نظر بگیرید:

```
11000000 10101000 00100110 00110000
11111111 11111111 11111111 00000000
```

چنان‌که قبلاً نیز عنوان شد، عدد 255 در ماسک شبکه شاخصی برای آدرس IP شبکه یعنی 192.168.38.0 است. اجازه دهید تا آدرس شبکه مزبور را به این صورت بر حسب مجموعه‌ای از بیت‌ها بیان کنیم:

```
11000000 10101000 00100110 00000000
```

به تأثیر ماسک شبکه 255.255.255.0 روی ۲۴ بیت از آدرس IP توجه کنید. در قالب مکانیزم CIDR می‌توانیم آدرس شبکه و ماسک شبکه را به صورت 192.168.38.0/24 نمایش دهیم.

ماسک فوق موجب صفر شدن هشت بیت سمت راست می‌شود، در حالی‌که سایر بیت‌ها دست نخورده باقی می‌ماند. با هشت بیت می‌توان ۲۵۶ آدرس IP را متمایز کرد. همان گونه که قبلاً نیز بارها عنوان شد، اولین و آخرین آدرس IP از این مجموعه به ترتیب نماینده آدرس شبکه و آدرس همگانی هستند. از این‌رو نمی‌توان آن‌ها را به هیچ یک از کامپیوترهای مستقر در شبکه تخصیص داد. با این حساب تنها تعداد ۲۵۴ آدرس IP جهت آدرس‌دهی کامپیوترهای مستقر در شبکه قابل استفاده خواهد بود. برای درک بهتر موضوع اجازه دهید تا وضعیت فوق را پس از اضافه کردن یک بیت به ماسک شبکه مجدداً مورد بررسی قرار دهیم:

```
11000000 10101000 00100110 00110000
11111111 11111111 11111111 10000000
```

مجموعه بیت‌های متناظر با یک‌های ماسک شبکه معادل آدرس شبکه 192.168.38.0 است. ماسک فوق موجب صفر شدن هفت بیت سمت راست شده، در حالی‌که سایر بیت‌ها دست نخورده باقی می‌ماند. با هفت بیت می‌توان ۱۲۸ آدرس IP را متمایز کرد. بار دیگر، اولین و آخرین آدرس IP از این مجموعه به ترتیب نماینده آدرس شبکه و آدرس همگانی هستند. از این‌رو، نمی‌توان آن‌ها را به هیچ یک از کامپیوترهای مستقر در شبکه تخصیص داد. با این حساب تنها تعداد ۱۲۶ آدرس IP جهت آدرس‌دهی کامپیوترهای مستقر در شبکه قابل استفاده خواهد بود. به این ترتیب، آدرس این شبکه 192.168.38.0 و آدرس همگانی 192.168.38.127 و ماسک شبکه نیز 255.255.255.128 خواهد بود.

به تأثیر ماسک شبکه 255.255.255.128 روی ۲۵ بیت از آدرس IP توجه کنید. در قالب مکانیزم CIDR می‌توانیم آدرس شبکه و ماسک شبکه را به صورت 192.168.38.0/25 نمایش دهیم.

اکنون آدرس IP دیگری با عنوان 192.168.38.166 و همان ماسک شبکه را مجدداً در نظر بگیرید:

```
11000000 10101000 00100110 10110000
11111111 11111111 11111111 10000000
```

این بار ماسک فوق شبکه‌ای با آدرس 192.168.38.128 و آدرس همگانی 192.168.38.255 را مشخص می‌کند. از آن‌جا که نمی‌توان این دو آدرس IP را به هیچ یک از کامپیوترهای مستقر در شبکه تخصیص داد، تنها ۱۲۶ آدرس IP برای تخصیص به کامپیوترهای مستقر در شبکه باقی می‌ماند.

نتیجه این‌که با استفاده از ماسک شبکه کلاس C یعنی 255.255.255.0 می‌توان ۲۵۴ آدرس IP را به کامپیوترهای مستقر در شبکه‌ای با آدرس 192.168.38.0 تخصیص داد. این در حالی است که با استفاده از ماسک 255.255.255.128 می‌توان دوشبکه‌محلی مختلف شامل ۱۲۶ کامپیوتر را آدرس‌دهی کرد.

نحوه اتصال به اینترنت

علیرغم وجود امکانات مخابراتی پرسرعت برای اتصال به اینترنت، مجموعه عظیمی از کاربران هم‌چنان از طریق مودم و خطوط تلفن با سرعتی حداکثر ۵۶ کیلوبیت بر ثانیه به اینترنت متصل می‌شوند. با وجود این، امروزه استفاده از اینترنت پرسرعت حتی برای شرکت‌های تجاری کوچک که دسترسی به اینترنت از بسیاری جهات برای آن‌ها یک ضرورت محسوب می‌شود، مقرون به صرفه است. اغلب برای اشاره به خطوط پرسرعت اینترنت از اصطلاح "باند پهن" یا broadband استفاده می‌شود.

سرویس‌های اینترنتی ارایه شده از طریق ماهواره‌ها و تکنولوژی‌هایی نظیر مادون قرمز، بی‌سیم، مودم‌های کابلی و DSL (اصطلاحاً Digital Subscriber Line) از جمله سرویس‌های باند پهن محسوب می‌شوند. چنین سرویس‌هایی امکان ارسال و دریافت داده‌ها را با سرعت ۱۴۴ کیلوبیت بر ثانیه فراهم می‌کنند. به دلیل این رقابت بسیاری از شرکت‌های تلفن هزینه استفاده از سرویس‌های باند پهن خود از جمله خطوط T1 (با سرعت انتقال ۱٫۵۴۴ مگابیت بر ثانیه) و ISDN (اصطلاحاً Integrated Services Digital Network با سرعت ۱۲۸ کیلوبیت بر ثانیه) را به میزان قابل توجهی کاهش دادند.

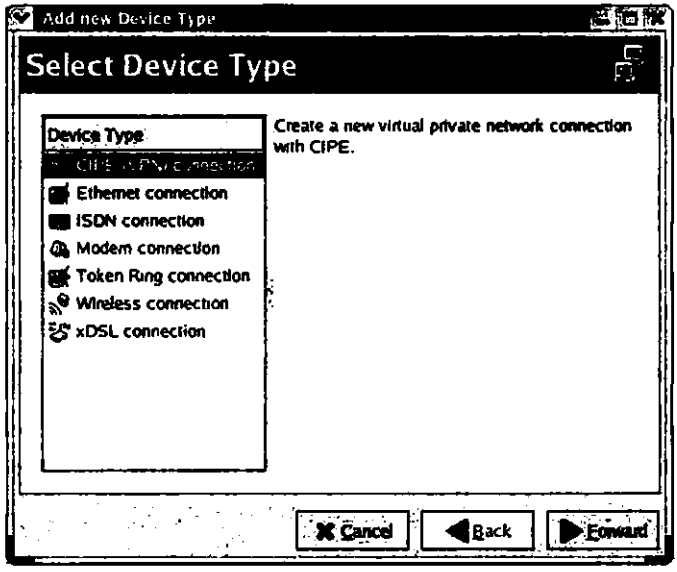
در بیشتر موارد فرآیند اتصال به یک سرویس باند پهن چیزی بیش از اتصال کامپیوتر به یک روتر نیست. معمولاً روتر موردنیاز را مرکز ارایه دهنده سرویس باند پهن با پرداخت هزینه مربوطه در اختیار قرار می‌دهد. برای دریافت آدرس IP ممکن است لازم باشد تا به روشی که در فصل بیست و چهارم شرح خواهیم داد، به سرور DHCP مستقر در آن مرکز متصل شوید. در سایر موارد مرکز مزبور آدرس IP دروازه شبکه و سرورهای DNS را در اختیار قرار می‌دهد.

برنامه minicom احتمالاً متداول‌ترین‌برنامه‌متنی‌مورداستفاده برای‌اتصال‌کامپیوترهای Linux به اینترنت از طریق مودم است. در سیستم‌عامل Red Hat Linux برنامه‌ای با عنوان Internet Configuration Wizard پیش‌بینی شده که امکان اتصال کامپیوتر به اینترنت را از طریق مودم و سرویس‌های باند پهن به سادگی در اختیار قرار می‌دهد.

برنامه Internet Configuration Wizard

قابلیت‌های برنامه Internet Configuration Wizard با امکاناتی که برنامه مشابه در سیستم‌عامل ویندوز در اختیار می‌گذارد، متفاوت است. برای دستیابی به رابط گرافیکی این برنامه کافی است فرمان redhat-config-network-druid را در سطر فرمان محیط گرافیکی GNOME یا KDE اجرا کنید. با این اقدام نخستین صفحه از برنامه Internet Configuration Wizard با عنوان Select Device Type را که شامل‌گزینه‌های مختلف برای پیکربندی سرویس‌های مختلف اتصال به شبکه اینترنت است مشاهده

خواهید کرد. شکل ۳-۲۱ پنجره مذکور را نشان می‌دهد.



شکل ۳-۲۱ نخستین صفحه از برنامه Internet Configuration Wizard با عنوان Select Device Type

با وجودی که موضوع اصلی این قسمت نحوه اتصال به اینترنت از طریق مودم است، اجازه دهید تا سایر گزینه‌های موجود در این زمینه را نیز به طور خلاصه مورد توجه قرار دهیم:

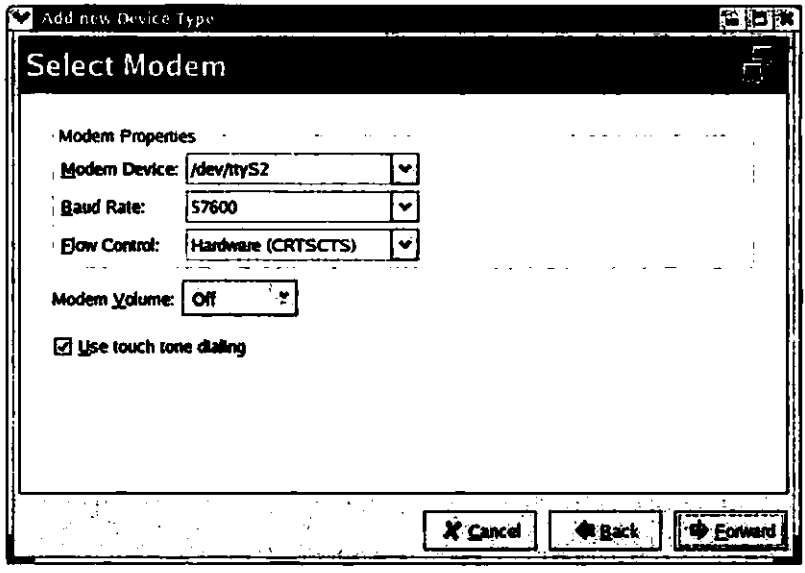
- **گزینه CIPE (VPN) Connection**: مکانیزم Crypto IP Encapsulation یا به اختصار CIPE (که معمولاً تحت عنوان Virtual Private Network یا اصطلاحاً VPN نیز شناخته می‌شود) روشی برای پیکربندی شبکه‌هایی با ضریب امنیتی بالا از طریق شبکه‌های عمومی مانند اینترنت است. این گزینه امکانات لازم برای پیکربندی آدرس IP طرفین اتصال و کلید رمزگشایی موردنیاز را در اختیار قرار می‌دهد.
- **گزینه Ethernet Connection**: این گزینه کلیه امکانات لازم برای تعیین کارت شبکه، درایور مربوطه و منابعی مانند پورت IRQ و آدرس ورودی و خروجی و هم‌چنین کانال‌های DMA را فراهم می‌کند. تنظیمات فوق به واسطه فرمان ifconfig امکان شناسایی کارت شبکه و ارتباط با آن‌را در اختیار سیستم‌عامل Linux قرار می‌دهد. در صورت تمایل می‌توان پیکربندی را به نحوی انجام داد که اطلاعات مربوط به آدرس IP از طریق سرور DHCP تأمین شود. ضمناً می‌توان تنظیمات فوق را به صورت دستی نیز انجام داد. چنان‌چه سرور DHCP روی یک کامپیوتر راه دور

مستقر باشد، برای دستیابی به آن باید از پروتکل BOOTP استفاده کنید.

- **گزینه ISDN Connection**: مشابه گزینه قبل، این گزینه نیز امکانات لازم برای تعیین درایور و منابع موردنیاز برای بهره‌برداری از تجهیزات ISDN را در اختیار قرار می‌دهد. از آن‌جا که شبکه‌های ISDN بیشتر در اروپا متداول است، تنظیمات مربوطه را می‌توان برای کشورهای مختلف اروپایی انجام داد.
- **گزینه Token Ring Connection**: این گزینه امکاناتی کم‌وبیش مشابه گزینه Ethernet Connection را در اختیار قرار می‌دهد.
- **گزینه Wireless Connection**: این گزینه علاوه بر امکانات گزینه Ethernet Connection امکانات دیگری را نیز به‌منظور پیکربندی کانال‌های بی‌سیم و کلید رمزگشایی موردنیاز را در اختیار قرار می‌دهد.
- **گزینه xDSL Connection**: نسخه‌های مختلفی از سرویس DSL موجود است که هریک امکان انتقال داده‌ها را در سرعتی متفاوت در اختیار می‌گذارد. این گزینه امکانات لازم برای بهره‌برداری از سرویس DSL از طریق کارت شبکه Ethernet و تعیین حساب کاربری شامل نام کاربری و کلمه عبور را فراهم می‌کند. همین پیکربندی را می‌توان در مورد بیشتر مودم‌های کابلی نیز مورد استفاده قرار داد.

اکنون اجازه دهید تا به موضوع پیکربندی مودم از طریق برنامه Internet Configuration Wizard بپردازیم. برای شروع، گزینه Modem Connection از منوی Device Type را انتخاب کرده و دکمه Forward را کلیک کنید. با این اقدام برنامه مزبور تلاشی را برای شناسایی مودم انجام می‌دهد. (در صورت عدم شناسایی مودم بحث مربوط به Winmodems را از فصل دوم ببینید.) در هر صورت، بعد از این مرحله صفحه‌ای مشابه شکل ۴-۲۱ با Select Modem را مشاهده خواهید کرد. صفحه مزبور شامل امکاناتی برای انتخاب کانال ارتباط مودم و تعیین برخی از پارامترهای آن است.

کانال ارتباط مودم را در سیستم‌عامل Linux می‌توان به پورت‌های سریال COM در سیستم‌عامل ویندوز تشبیه کرد، به طوری که برای مثال کانال /dev/tty0 متناظر با COM1 و کانال /dev/tty1 متناظر با COM2 است. چنان‌که در شکل ۴-۲۱ مشاهده می‌کنید، سیستم‌عامل Linux مودم را روی کانال ارتباطی متناظر با پورت سریال COM3 شناسایی کرده است. به این ترتیب، با تشخیص پورت سریال مودم در سیستم‌عامل ویندوز، می‌توانید از کانال ارتباطی متناظر با آن در سیستم‌عامل Linux استفاده کنید.

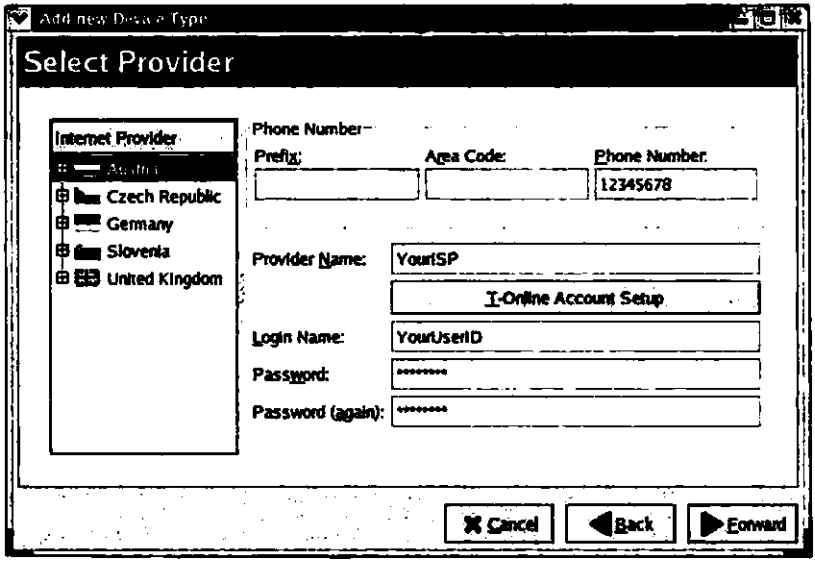


شکل ۴-۲۱ پیکربندی مودم

پارامتر baud rate عموماً باید دو یا سه برابر سرعت اتصال مودم انتخاب شود. از این‌رو، برای مودم‌های ۵۶ کیلوبیت بر ثانیه (۵۳ کیلوبیت بر ثانیه در ایالات متحده آمریکا) مقدار پارامتر مزبور باید برابر با ۱۱۵،۲۰۰ یا ۲۳۰،۴۰۰ بیت بر ثانیه انتخاب شود. معمولاً مقدار پیش‌فرض پارامتر Flow Control یعنی Hardware (CRTSCTS) برای اغلب کاربردها مناسب است. پس از انجام این تنظیمات دکمه Forward را برای ادامه عملیات کلیک کنید.

برای مشاهده کانال ارتباطی مودم (که متناظر با یک فایل سخت‌افزاری است) فرمان ls -l /dev/modem را اجرا کنید. عنوان عمومی کانال مزبور به صورت /dev/ttyx است.

با این اقدام صفحه دیگری مشابه شکل ۵-۲۱ با عنوان Select Provider را مشاهده خواهید کرد. در این صفحه پارامترهای لازم برای برقراری ارتباط با مرکز ISP شامل نام مرکز مزبور، شماره تلفن، شناسه کاربری و کلمه عبور را وارد کنید. در صورتی که از مقادیر معتبر این پارامترها مطلع باشید، نیازی نیست که گزینه مربوط به کشور خود را از لیست Internet Provider انتخاب کنید. (چنان‌چه به حساب معتبری از نوع T-Online در اروپا دسترسی دارید، دکمه T-Online Account Setup را کلیک کرده و تنظیمات مربوطه را انجام دهید.)

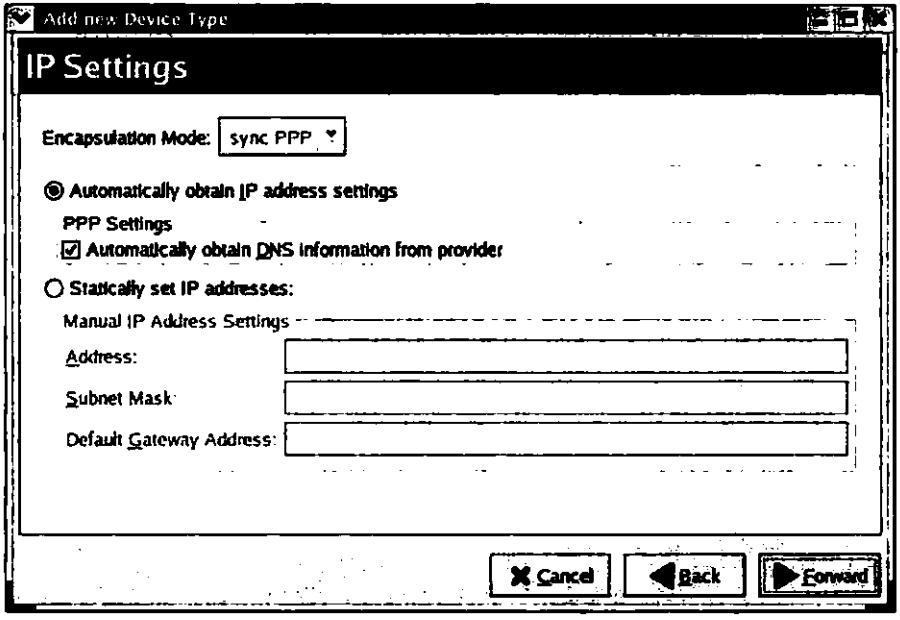


شکل ۵-۲۱ تنظیمات مربوط به حساب کاربری و مرکز ISP مورد نظر

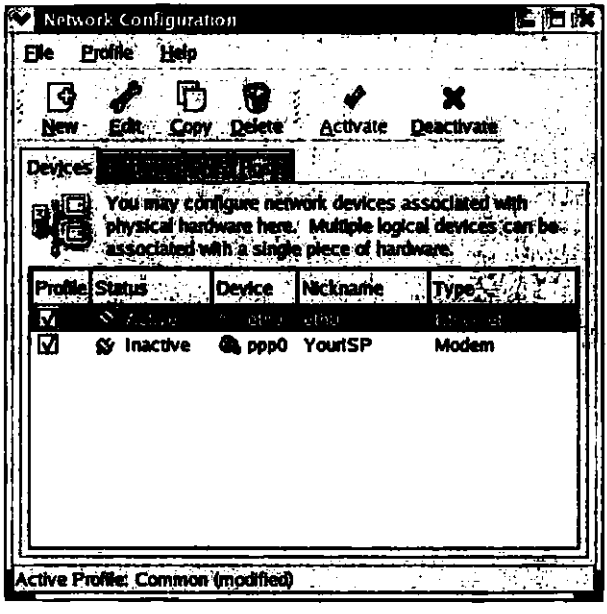
بار دیگر دکمه Forward را کلیک کنید. با این اقدام صفحه جدیدی مشابه شکل ۶-۲۱ با عنوان IP Settings را مشاهده خواهید کرد. معمولاً مراکز ISP به هر کامپیوتری که از طریق شماره‌گیری برای اتصال به شبکه اینترنت اقدام کرده باشد، به طور خودکار یک آدرس IP تخصیص می‌دهند. در صورتی که مرکز ISP برای این منظور یک آدرس IP استاتیک اختصاص دهد، لازم است ماسک شبکه و آدرس دروازه پیش‌فرض را نیز در فیلدهای مربوطه وارد کنید.

دکمه Forward و به دنبال آن دکمه Apply را کنید. با این اقدام پنجره‌ای مشابه شکل ۷-۲۱ با عنوان Network Configuration را که شامل تنظیمات مربوط به کارت‌های شبکه است، مشاهده خواهید کرد. وضعیت Inactive در دومین سطر از این شکل به معنی غیرفعال بودن مودم است. برای تغییر این وضعیت کافی است آن‌را انتخاب کرده و دکمه Activate را کلیک کنید. چنان‌چه بلندگوی مودم را نیز فعال کرده باشید، باید صدای حاصل از شماره‌گیری آن‌را بشنوید.

برای غیرفعال کردن مودم کافی است پنجره Network Configuration را باز کرده و پس از انتخاب مودم موردنظر دکمه Deactivate را کلیک کنید.



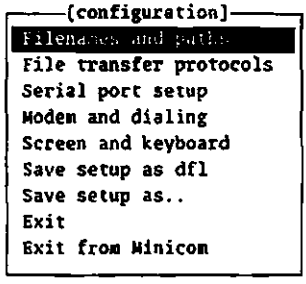
شکل ۶-۲۱ تنظیمات مربوط به آدرس IP



شکل ۷-۲۱ پنجره Network Configuration

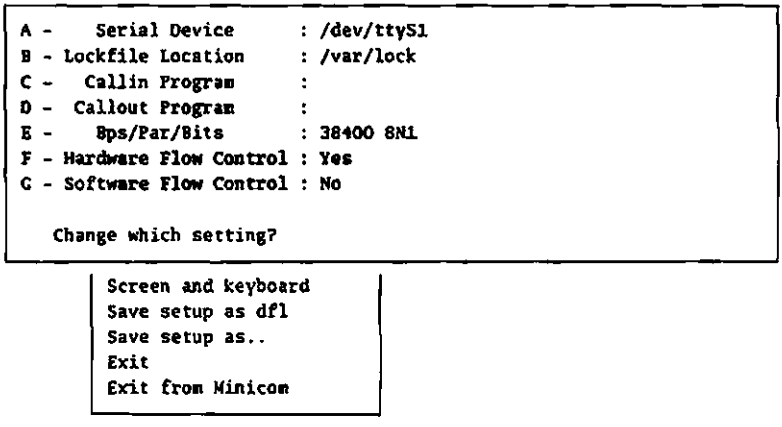
برنامه minicom

یکی از ابزارهای سطر فرمان متداول برای پیکربندی و بهره‌برداری از مودم برنامه‌ای با عنوان minicom است. پیش از هر چیز ابتدا باید این ابزار را پیکربندی کنید. برای این منظور کافی است فرمان minicom -s را اجرا کنید. شکل ۸-۲۱ منوی حاصل از اجرای این فرمان با عنوان Configuration را نشان می‌دهد.



شکل ۸-۲۱ منوی Configuration برنامه minicom

قبل از به کارگیری برنامه minicom باید آن‌را جهت اتصال به مودم پیکربندی کنید. برای انجام این کار گزینه Serial Port Setup از منوی Configuration را انتخاب کرده و کلید Enter را فشار دهید. با این اقدام منویی مشابه شکل ۹-۲۱ را مشاهده خواهید کرد.



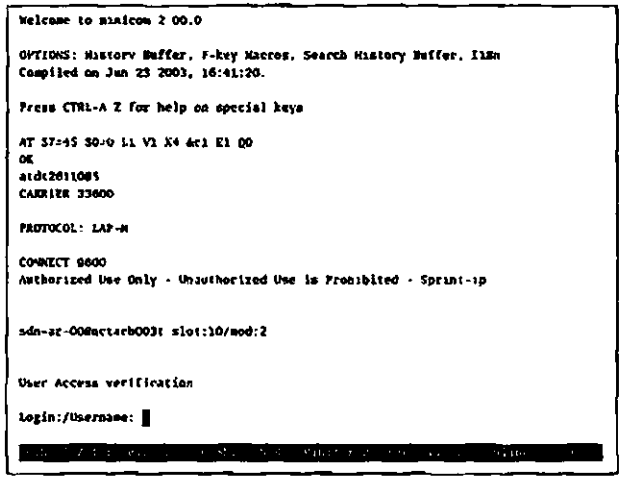
شکل ۹-۲۱ پیکربندی پورت سریال

بسته به مودم مورد استفاده ممکن است لازم باشد تا مقادیر این گزینه‌ها را تغییر دهید:

- **گزینه Serial Device:** این گزینه کانال ارتباطی مودم را در قالب یک فایل سخت‌افزاری مشخص می‌کند. چنان‌چه با اجرای فرمان ls -l /dev/modem کانالی مانند /dev/ttyS0 را مشاهده کردید، می‌توانید از آن به عنوان مقدار این گزینه استفاده کنید. در غیر این صورت ممکن است لازم باشد تا روش سعی و خطا را در پیش بگیرید.
- **گزینه Bps/Par/Bits:** این گزینه نحوه انتقال داده‌ها توسط مودم را مشخص می‌کند. در این میان پارامتر Bps بیانگر تعداد بیت‌های منتقل شده در هر ثانیه یا اصطلاحاً bits per second بوده و مقدار آن باید دو تا چهار برابر سرعت مودم که حداکثر ۵۶ کیلوبیت بر ثانیه (۵۳ کیلوبیت بر ثانیه در ایالات متحده آمریکا) است، انتخاب شود، چرا که اکثر مودم‌های امروزی یک فرآیند فشرده‌سازی را پیش از انتقال داده‌ها روی آن‌ها انجام می‌دهند. در صورتی که از مودم‌های قدیمی استفاده نمی‌کنید، باید مقدار پیش‌فرض 8N1 را برای پارامترهای Par و Bits (که به ترتیب بیانگر parity و stop bit هستند) بپذیرید.

در مورد سایر پارامترها از جمله bps و hardware flow control به دفترچه راهنمای مودم خود مراجعه کنید. پس از پایان فرآیند پیکربندی مودم گزینه Save Setup As dfl از منوی اصلی را انتخاب کنید. برای ارزیابی عملکرد مودم گزینه Exit را انتخاب کنید. با این اقدام سیگنال‌های لازم به مودم ارسال شده و صفحه اصلی برنامه minicom مجدداً به نمایش درمی‌آید.

بهترین راه برای ارزیابی عملکرد مودم شماره‌گیری مرکز ISP است. برای انجام این کار کافی است فرمان atdt و در مقابل آن شماره تلفن مرکز ISP موردنظر را وارد کنید. شکل ۱۰-۲۱ نمونه یک چنین اقدامی را نشان می‌دهد.



شکل ۱۰-۲۱ ارزیابی عملکرد مودم

برنامه minicom از مجموعه فرامین متداول AT برای برقراری ارتباط با مودم استفاده می‌کند. برای مثال، فرمان atdt که کوتاه شده عبارت Attention, use Touch-Tone dialing است مودم را وادار می‌کند تا به روش Tone شماره‌گیری کند.

اشکال‌زدایی شبکه

پیشتر روش‌های اشکال‌زدایی مختلفی را در این کتاب مورد بررسی قرار دادیم. اشکال‌زدایی شبکه نیز تفاوت‌های عمده‌ای با روش‌های قبلی ندارد. در صورت مواجهه با مشکل، پس از جمع‌آوری اطلاعات مربوطه باید علل احتمالی را بررسی کرده و راه‌حلی را برای رفع آن پیدا کنید.

چنان‌که قبلاً نیز اشاره شد، بیشترین اشکالات مربوط به شبکه مربوط به لایه فیزیکی است. اتصالات نادرست، کابل‌ها و منابع تغذیه معیوب و مواردی مانند آن حاکی از وجود مشکل در لایه فیزیکی شبکه است. مدیران شبکه‌های Linux ابزارهای اشکال‌زدایی متعددی را در اختیار دارند. برای مثال، با استفاده از ابزار netstat می‌توان به جمع‌آوری اطلاعات درباره شبکه پرداخته و به کمک دو ابزار ping و tracerout به علت مشکل موردنظر پی برد. در قسمت‌های باقیمانده از این فصل به بررسی نحوه انجام این کار خواهیم پرداخت.

بازبینی وضعیت شبکه

بازبینی وضعیت شبکه یک فرآیند دو مرحله‌ای است. نخست باید با استفاده از فرمان ifconfig از فعال بودن کارت شبکه اطمینان حاصل کرد. چنان‌که قبلاً نیز اشاره شد، با اجرای فرمان ifconfig eth0 up می‌توان کارت شبکه eth0 را فعال کرد. در صورت فعال بودن کارت شبکه می‌توان وضعیت شبکه را با استفاده از فرمان netstat مورد بازبینی قرار داد.

فرمان netstat جداول مسیریابی، اتصالات شبکه موردنظر با سایر شبکه‌ها و سایر اطلاعات مفید را در اختیار قرار می‌دهد. برای مثال، فرمان netstat -a کلیه اتصالات موجود را نمایش می‌دهد. چنان‌که در شکل ۱۱-۲۱ مشاهده می‌کنید، ستون Local Address شامل اسامی پروتکل‌ها و شماره پورت‌های مربوطه است که در فصل‌های قبل در مورد آن صحبت کردیم. ستون Foreign Address نیز نشان‌دهنده اتصالاتی از نوع telnet، http و ssh است که بین کامپیوتر میزبان و دو کامپیوتر دیگر مستقر در شبکه برقرار شده است.

```
[root@RH9Test root]# netstat -a | more
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 *:1024                  *:*                     LISTEN
tcp        0      0 RH9Test:1025            *:*                     LISTEN
tcp        0      0 RH9Test:783             *:*                     LISTEN
tcp        0      0 *:sunrpc                *:*                     LISTEN
tcp        0      0 *:x11                   *:*                     LISTEN
tcp        0      0 *:ssh                   *:*                     LISTEN
tcp        0      0 RH9Test:ipp             *:*                     LISTEN
tcp        0      0 RH9Test:smtp            *:*                     LISTEN
tcp        0      1 10.252.113.3:2836       RH9Test:ipp             SYN_SENT
tcp        0      0 10.252.113.3:2831       laptop2:netbios-ssn     ESTABLISHED
udp        0      0 *:1024                  *:*
udp        0      0 *:687                   *:*
udp        0      0 *:bootpc                *:*
udp        0      0 *:bootpc                *:*
udp        0      0 *:sunrpc                *:*
udp        0      0 *:631                   *:*
udp        0      0 10.252.113.1:ntp        *:*
udp        0      0 RH9Test:ntp             *:*
udp        0      0 *:ntp                   *:*
Active UNIX domain sockets (servers and established)
```

شکل ۱۱-۲۱ نمونه‌ای از خروجی فرمان netstat -a

جدول مسیریابی (اصطلاحاً routing table) شامل کلیه مسیرهای موجود از کامپیوتر میزبان به کامپیوتری مستقر در همان شبکه یا در شبکه‌ای دیگر است. سیستم‌عامل Linux از این مسیرها برای یافتن کامپیوترهایی استفاده می‌کند که از طریق کامپیوتر میزبان قصد دارید تا به آن‌ها متصل شوید. فرمان netstat جداول مسیریابی را در اختیار می‌گذارد. شکل ۱۲-۲۱ جدول مسیریابی ساده‌ای را که به واسطه اجرای فرمان netstat -nr تولید شده است، نشان می‌دهد. این جدول شامل سه نوع آدرس IP مختلف است. جدول ۵-۲۱ این آدرس‌ها را شرح می‌دهد.

```
[root@RH9Test root]# netstat -nr
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
10.252.113.0    0.0.0.0         255.255.255.0   U         0 0          0 eth0
127.0.0.0       0.0.0.0         255.0.0.0       U         0 0          0 lo
0.0.0.0         10.252.113.113  0.0.0.0         UG        0 0          0 eth0
[root@RH9Test root]#
```

شکل ۱۲-۲۱ نمونه‌ای از یک جدول مسیریابی

در صورت تمایل با استفاده از فرمان route می‌توان اطلاعاتی را در جدول مسیریابی درج کرد.برای مثال، فرض کنید اخیراً شبکه محلی جدیدی را با آدرس 10.0.0.0 و ماسک شبکه 255.255.0.0 پیکربندی و به کارت شبکه‌ای با شناسه eth1 متصل کرده‌اید. با اجرای این فرمان می‌توانید مشخصات

شبکه مزبور را در جدول مسیریابی درج کنید:

```
# route add -net 10.0.0.0 netmask 255.255.0.0 dev eth1
```

جدول ۵-۲۱ شرح آدرس‌های IP یک جدول مسیریابی

آدرس IP مقصد	توضیح
10.252.113.0	این آدرس IP بیانگر آدرس IP شبکه بوده و از این‌رو هیچ دروازه‌ای برای دستیابی به آن موردنیاز نیست.
127.0.0.1	این آدرس IP بیانگر آدرس IP کامپیوتر میزبان (اصطلاحاً آدرس loopback) بوده و از این‌رو هیچ دروازه‌ای برای دستیابی به آن موردنیاز نیست.
0.0.0.0	این آدرس IP نماینده کلیه آدرس‌های IP است که پیشتر در جدول مسیریابی ذکر نشده‌اند. برای دستیابی به تمام این آدرس‌های IP به طور پیش‌فرض از دروازه 10.252.113.113 استفاده خواهد شد. (دقت کنید که در ستون Destination از جدول مسیریابی ممکن است به جای آدرس 0.0.0.0 از عنوان default استفاده شده باشد.)

بازبینی اتصالات شبکه با استفاده از فرامین ping و traceroute

هنگام مواجهه با اشکالاتی نظیر عدم توانایی کاربران در استفاده از سرویس وب یا پست الکترونیکی، ابتدا بهتر است با کاربران به گفتگو نشسته و اطمینان حاصل کنید که آن‌ها از نحوه دسترسی به سرویس یا سرویس‌های موردنظر اطلاع کافی دارند. علاوه بر این، در صورت تمایل می‌توانید با استفاده از فرامین ssh و telnet، کامپیوتر هریک از کاربران را از راه دور مورد دستیابی قرار داده و بازبینی‌های لازم را شخصاً انجام دهید.

در سیستم‌عامل Linux ابزارهای متعدد و بسیار مفیدی برای بازبینی عملکرد شبکه پیش‌بینی شده است. در این میان دو ابزار ping و traceroute امکانات قابل توجهی را به منظور عیب‌یابی شبکه در اختیار قرار می‌دهند. برای عیب‌یابی شبکه این اقدامات را انجام دهید: (در هر مرحله با فشار کلید ترکیبی Ctrl+C می‌توانید عملیات را متوقف کنید.)

۱- فرمان ping 127.0.0.1 را جهت اطمینان از عملکرد صحیح کامپیوتر میزبان در شبکه اجرا کنید. اگر با اجرای این فرمان به طور پیوسته پاسخی نظیر ...64 bytes from 127.0.0.1 را مشاهده کردید، می‌توانید مطمئن باشید که نرم‌افزار TCP/IP به خوبی روی آن کامپیوتر نصب شده است.

برای اجتناب از ارسال نامحدود بسته‌های ping ارسالی به کامپیوتر مقصد می‌توانید تعداد این بسته‌ها را با استفاده از سوییچ c- مشخص کنید. برای مثال، فرمان ping -c 4 *ip_address* تنها چهار بسته ping را به کامپیوتر مقصد که آدرس آن توسط متغیر *ip*_address مشخص می‌شود، ارسال می‌کند. علاوه بر این، با اجرای فرمان alias ping = 'ping -c 4' می‌توانید ترتیبی دهید تا با اجرای فرمان ping همواره تنها چهار بسته ping به کامپیوتر مقصد ارسال شود. (برای اطلاع بیشتر درباره فرمان alias به فصل هشتم مراجعه کنید.)

۲- فرمان ping *your_ip_address* را که در آن متغیر *your_ip_address* بیانگر آدرس IP کامپیوتر میزبان است، اجرا کنید. (برای پی بردن به آدرس IP کامپیوتر میزبان کافی است فرمان ifconfig را اجرا کنید.) در صورتی که با اجرای این فرمان به طور پیوسته پاسخی نظیر پاسخ مرحله قبل را دریافت کردید، پیکربندی کارت شبکه کامپیوتر میزبان به درستی انجام شده است.

۳- فرمان ping *your_host_name* را که در آن متغیر *your_host_name* بیانگر نام کامپیوتر میزبان است، اجرا کنید. برای پی بردن به‌نام‌کامپیوتر میزبان کافی است به فایل /etc/sysconfig/network مراجعه کنید. در صورت مشاهده پاسخی نظیر پاسخ مراحل قبل پیکربندی نام میزبان نیز به درستی انجام شده است.

۴- فرمان ping *another_ip_address* را که در آن متغیر *another_ip_address* گویای آدرس IP کامپیوتر دیگری از شبکه محلی است، اجرا کنید. برای پی بردن به آدرس IP سایر کامپیوترهای مستقر در شبکه کافی است فرمان ifconfig را اجرا کنید. (فرمان متناظر در سیستم‌عامل ویندوز IPCONFIG است.) در صورت مشاهده پاسخی نظیر پاسخ مراحل قبل ارتباط میان کامپیوترهای مستقر در شبکه به خوبی برقرار می‌شود. به بیان دیگر، می‌توان مطمئن شد که دست‌کم این دو کامپیوتر (یعنی‌کامپیوتر میزبان و کامپیوتری که آدرس IP آن توسط متغیر *another_ip_address* مشخص شده است) با استفاده از یک آدرس شبکه و یک ماسک واحد روی شبکه میزبان پیکربندی شده‌اند. همین فرآیند را با آدرس IP دروازه شبکه نیز انجام دهید تا از برقراری ارتباط کامپیوتر میزبان با دروازه شبکه اطمینان حاصل کنید.

۵- فرمان ping *another_hostname* را که در آن متغیر *another*_hostname بیانگر نام یکی از کامپیوترهای مستقر در شبکه میزبان یا یک شبکه دیگر است، اجرا کنید. چنان‌چه به شبکه اینترنت دسترسی دارید، در این مورد می‌توانید فرمان ping www.sybex.com را اجرا کنید. در صورتی که این فرمان با موفقیت اجرا شود، پیکربندی دروازه شبکه یا روتری که شبکه محلی را به شبکه مزبور متصل کرده است به درستی انجام شده و ارتباط میان شبکه محلی با شبکه موردنظر

به درستی برقرار می‌شود.

۶- فرمان traceroute *another_hostname* را که در آن متغیر *another_hostname* بیانگر نام یکی از کامپیوترهای شبکه میزبان یا یک شبکه دیگر است، اجرا کنید. بار دیگر، چنان‌چه به شبکه اینترنت دسترسی دارید، در این مورد می‌توانید فرمان traceroute www.sybex.com را اجرا کرده و مسیری را که داده‌های ارسالی از کامپیوتر میزبان به وب سایت Sybex به آدرس اینترنتی http://www.sybex.com طی کرده‌اند، مورد توجه قرار دهید. در صورتی که فرآیند عیب‌یابی ارتباط میان دو یا چند شبکه را انجام می‌دهید، دقت کنید که عملیات ناشی از این فرمان به محض رسیدن داده‌های ارسالی به مقصد یا در مواجهه با دروازه یا روتری که به نوعی دارای مشکل است، متوقف خواهد شد.

برای مثال، در صورتی که اجرای فرمان ping در ارتباط با آدرس IP دروازه یا روتر موردنظر با مشکل مواجه نشود، می‌توانید آدرس IP برخی از کامپیوترهای مستقر در شبکه را برای این منظور مورد بازبینی قرار دهید. چنان‌چه ارتباط با این کامپیوترها نیز با مشکل مواجه شود، ممکن است اشکال از کابل‌ها یا اتصالات شبکه باشد. در غیر این صورت باید اشکال را در تجهیزات سخت‌افزاری مانند روتر جستجو کرد.

جمع‌بندی

در این فصل با برخی از اقدامات اولیه موردنیاز برای پیکربندی شبکه‌های Linux آشنا شدید. برای ایجاد شبکه‌ای از کامپیوترها به تجهیزات سخت‌افزاری متنوعی نیاز دارید. رسانه انتقال داده‌ها معمولاً از نوع کابل‌های ساده یا فیبرنوری انتخاب می‌شود. هاب نوعی‌تجهیزات‌سخت‌افزاری است که کامپیوترهای مستقر در یک شبکه را به یکدیگر متصل می‌کند. سوییچ‌ها نیز تجهیزات سخت‌افزاری خاصی هستند که معمولاً به منظور تقسیم یک شبکه به بخش‌های مختلف مورد استفاده قرار می‌گیرند. روترها وظیفه انتقال داده‌ها بین دو یا چند شبکه را به عهده دارند. دروازه‌ها می‌توانند عمل ترجمه یک پروتکل به دیگری مانند ترجمه پروتکل TCP/IP به IPX/SPX را انجام دهند.

به دلایل متعدد ممکن است مایل باشید تا پیکربندی شبکه را پس از اتمام فرآیند نصب سیستم‌عامل Linux تغییر دهید. فرمان ifconfig را شاید بتوان مهم‌ترین فرمان در زمینه پیکربندی کارت‌های شبکه به حساب آورد. با استفاده از این فرمان می‌توان پورت‌های سخت‌افزاری و آدرس IP موردنظر را به کارت‌های شبکه تخصیص داد. به کمک این فرمان حتی می‌توان کارت‌های شبکه را فعال یا غیرفعال کرد. فرمان arp یکی از فرامین مهم دیگر است که با استفاده از آن می‌توان از منحصر به فرد بودن آدرس‌های IP کامپیوترهای مستقر در شبکه اطمینان حاصل کرد. فرامین مربوط به اسامی میزبان

شامل hostname، domainname، dnsdomainname، nisdomainname و ypdomainname امکان نام‌گذاری کامپیوترهای مستقر در شبکه را به منظور بهره‌بردرای از سرویس‌های مختلف شبکه فراهم می‌کند. فایل‌های /etc/hosts، /etc/resolve.conf، /etc/host.conf و /etc/sysconfig/network از جمله مهم‌ترین فایل‌های پیکربندی شبکه در سیستم‌عامل Linux به شمار می‌روند.

در صورت تمایل می‌توانید فرآیند آدرس‌دهی در شبکه را به روش IPv4 انجام دهید. برای این منظور باید محدوده‌ای از آدرس‌های IP خصوصی را به کامپیوترهای مستقر در شبکه موردنظر تخصیص دهید. برای استفاده از محدوده آدرس‌های IP خصوصی کلاس A، B یا C کافی است ماسک شبکه مربوطه را انتخاب کنید. هم‌چنین برای اتصال چنین شبکه‌ای به اینترنت باید یک آدرس IP عمومی در اختیار داشته باشید. مکانیزم CIDR امکان استفاده از ماسک‌های شبکه غیراستاندارد را در اختیار می‌گذارد.

در حالی که استفاده از باند پهن جهت اتصال به شبکه اینترنت برای بسیاری از کاربردهای تجاری کاملاً مقرون به صرفه است، بسیاری از کاربران اینترنت هم‌چنان از خطوط تلفن و مودم برای این منظور استفاده می‌کنند. برنامه Internet Configuration Wizard در سیستم‌عامل Red Hat Linux امکانات بسیار متنوعی را برای اتصال به اینترنت در اختیار قرار می‌دهد. یکی از این موارد امکان پیکربندی مودم برای اتصال به شبکه اینترنت است. برنامه minicom نیز یک ابزار سطر فرمان مفید برای اتصال کامپیوتر میزبان به شبکه اینترنت محسوب می‌شود.

هنگام اشکال‌زدایی شبکه به خاطر داشته باشید که بیشتر اشکالات مربوط به لایه فیزیکی است. از این‌رو، پیش از هر اقدامی کابل‌ها و اتصالات شبکه را مورد بازبینی قرار دهید. در صورتی که اشکال از لایه فیزیکی نباشد، پس از جمع‌آوری اطلاعات باید با توجه به علایم علت را پیدا کرده و برای رفع آن اقدام کنید.

چنان‌چه هیچ یک از راهکارهای فوق مفید نباشد باید از فرامین مفیدی مانند ifconfig، netstat، ping و tracerouteکه سیستم‌عامل Linux در اختیار قرار داده است برای جمع‌آوری اطلاعات و تشخیص مشکل استفاده کنید. با بهره‌گیری از فرمان ifconfig می‌توانید از فعال بودن کارت شبکه اطمینان حاصل کنید. فرمان netstat امکان بازبینی وضعیت شبکه و جداول مسیریابی را فراهم می‌کند. فرامین ping و traceroute نیز امکاناتی را به منظور بازبینی اتصالات شبکه و اطمینان از صحت آن‌ها در اختیار قرار می‌دهند.

پس از آشنایی با اصول پیکربندی شبکه، آماده‌اید تا مطالعه فصل بیست و دوم را که به بررسی موضوع امنیت شبکه می‌پردازد، آغاز کنید. چنان‌که خواهید دید، در سیستم‌عامل Red Hat Linux امکان بهره‌بردرای از دو مکانیزم امنیتی مهم با عنوان Pluggable Authentication Modules (به اختصار PAM) و دیوار آتش فراهم شده است.

فصل بیست‌ودوم

امنیت شبکه‌های Linux

امنیت یکی از موضوعات مهم در زمینه شبکه‌های کامپیوتری محسوب می‌شود. روزانه خرابکاران بسیاری به واسطه نقاط ضعف شبکه‌های کامپیوتری در این شبکه‌ها نفوذ می‌کنند. در حالی که برخی از آن‌ها این کار را صرفاً به منظور تفریح کردن انجام می‌دهند، اهداف جنایی انگیزه‌ای است که برخی دیگر از این خرابکاران را وادار به هر کاری می‌کند.

در این فصل مطالعه خود را با بهترین روش‌های موجود برای تأمین امنیت شبکه‌ها آغاز می‌کنیم. برخی از این روش‌ها مستلزم مهارت کافی در بهره‌برداری از سیستم‌عامل Linux است که البته در این کتاب به بررسی تمام این موارد پرداخته شده است. شیوه‌های رمزگذاری، بهره‌برداری از مکانیزم بازدارنده دیوار آتش، استفاده مناسب از کلمات عبور و بالاخره امنیت فیزیکی موضوعات مهمی هستند که در این فصل به بررسی آن‌ها می‌پردازیم.

در سیستم‌عامل Red Hat Linux فرآیند احراز هویت کاربران نه تنها هنگام ورود آن‌ها به سیستم انجام می‌شود، بلکه هنگام اجرای بعضی از فرامین و دستیابی به برخی سرویس‌ها نیز صورت می‌گیرد. مکانیزم Pluggable Authentication Module یا به اختصار PAM یک مکانیزم امنیتی پویاست که می‌توان آن‌را برای بسیاری از کاربردها پیکربندی کرد.

مکانیزم دیوار آتش (اصطلاحاً firewall) یک مکانیزم بازدارنده است که با استفاده از برنامه iptables می‌توان آن‌را برای محافظت از سرویس‌ها و پورت‌های موردنظر پیکربندی کرده و مورد بهره‌برداری قرار داد. استفاده از فرامین موردنیاز برای پیکربندی مکانیزم دیوار آتش کاملاً ساده است. پس از آشنایی با برنامه iptables به سادگی می‌توانید مکانیزم بازدارنده دیوار آتش را روی کامپیوتر موردنظر پیکربندی کنید. این مکانیزم دفاعی بدون آن‌که دسترسی کاربران به سرویس‌های موردنیاز را محدود کند، امنیت لازم را تأمین می‌کند.

مکانیزم نقاب‌زنی (اصطلاحاً masquerading) مکانیزم‌امنیتی دیگری است که هویت واقعی کامپیوترهای مستقر در شبکه محلی را از دید کاربران اینترنت پنهان می‌کند. مشابه مکانیزم بازدارنده دیوار آتش، برنامه iptables امکانات لازم برای پیکربندی این مکانیزم را نیز در اختیار قرار می‌دهد.

از آن‌جا که تمام مکانیزم‌های امنیتی به نوعی دارای نقطه ضعف هستند، همواره باید امکان نفوذ خرابکاران به شبکه را مورد بررسی قرار دهید. در این رابطه ابزارهایی مانند Ethereal امکان بازبینی متونی را که از طریق شبکه جابه‌جا می‌شود، در اختیار قرار می‌دهد. با استفاده از این ابزار می‌توان فایل‌هایی چون wtmp را به منظور تشخیص کاربرانی که بدون احراز هویت وارد سیستم شده‌اند، مورد بازبینی قرار داد. سایر ابزارها از جمله Tripwire امکان تشخیص هر گونه تغییری در فایل‌های حیاتی سیستم را فراهم می‌کنند.

وسواس بیش از اندازه نیز درباره امنیت سیستم‌ها می‌تواند به مشکلات دیگری منتهی شود. اگر کاربران از رعایت خط مشی انتخاب کلمات عبور پرهیز می‌کنند، ممکن است رعایت آن خط مشی بیش از اندازه مشکل باشد. هم‌چنین اگر کاربران به سرویس‌های موردنیاز دسترسی ندارند، ممکن است در پیکربندی مکانیزم دیوار آتش بیش از حد لازم سخت‌گیری صورت گرفته باشد. در سایر فصل‌های کتاب‌حاضر به‌بررسی مشخصات یک سیستم‌امنیتی‌خوب، از رمزگذاری گرفته تا پیکربندی سرویس‌های شبکه خواهیم پرداخت. موضوعات مهم مورد بررسی در فصل حاضر به این قرار است:

- بهترین روش‌های موجود برای تأمین امنیت شبکه‌ها
- بهره‌برداری از مکانیزم امنیتی Pluggable Authentication Module
- بهره‌برداری از مکانیزم بازدارنده دیوار آتش
- بهره‌برداری از مکانیزم نقاب‌زنی
- تشخیص تهاجم به سیستم
- رفع مشکلات دسترسی کاربران به سرویس‌ها

بهترین روش‌های موجود برای تأمین امنیت شبکه‌ها

برای ایمن‌سازی شبکه باید اقدامات مختلفی انجام دهید. برخی از این اقدامات روش‌های متداولی هستند که اغلب به عنوان خط مشی عمومی برای تأمین امنیت شبکه‌ها مورد استفاده قرار می‌گیرند. روش پیکربندی کامپیوترهای مستقر در شبکه نیز به نوبه خود می‌تواند موجب افزایش امنیت شبکه شود. چنان‌که خواهید دید، رمزگذاری داده‌ها امنیت آن‌ها را ضمن انتقال از طریق شبکه تا اندازه‌ای تضمین می‌کند. انتخاب صحیح کلمات عبور نیز کمک شایانی به حفظ امنیت کامپیوترها می‌کند و بالاخره مکانیزم بازدارنده دیوار آتش امکانات مناسبی را به منظور تأمین امنیت شبکه در اختیار قرار می‌دهد.

تأمین امنیت شبکه در سطح لایه فیزیکی

روش مورد استفاده برای حفاظت از کامپیوترها و تجهیزات سخت‌افزاری شبکه به اهمیت آن‌ها و خطرات موجود در محیط بستگی دارد.

در شبکه‌های خانگی بدیهی است که باید تجهیزاتی مانند هاب و روتر را دور از دسترس کودکان و در محلی با شرایط مناسب مستقر کرد. عموماً نگرانی خاصی در مورد خرابکاری‌های فیزیکی شبکه‌های خانگی وجود ندارد.

از طرف دیگر، در شبکه‌های شرکتی باید تلاش زیادی برای ایمن‌سازی کامپیوترها در مقابل خرابکارانی که به طور عمدی یا غیرعمد اقدام به خرابکاری می‌کنند، صورت داد. بسته به شرایط موجود ممکن است لازم باشد تا سرورها و هم‌چنین تجهیزاتی مانند هاب، سوییچ و روتر را در اتاق کاملاً محافظت شده‌ای مستقر کنید. چنین اتاق‌هایی برای نگهداری نسخه‌های پشتیبان از داده‌ها نیز بسیار مناسب هستند. با وجود این باید مطمئن شوید که شرایط محیطی این گونه مکان‌ها از نظر دما و تهویه هوا برای نگهداری تجهیزات سخت‌افزاری نامبرده کاملاً مناسب است.

توجه به پیکربندی موجود در مواقعی که باید سیستم‌عامل Linux را مجدداً نصب کنید بسیار حایز اهمیت است.

در محیط‌های نظامی یا شبیه به آن که امنیت بسیار بالایی موردنیاز است، باید سخت‌گیری بیشتری به خرج داد. برای مثال، در چنین محیط‌هایی بهتر است درایوهای فلاپی را از روی کامپیوترها جدا کرده یا به نوعی آن‌ها را قفل کرد. بسته به شرایط موجود، باید اقدامات امنیتی مختلفی برای حفاظت از سرورها، ایستگاه‌های کاری و تجهیزات شبکه صورت بگیرد. علاوه بر این، باید تدابیر ویژه‌ای نیز برای محافظت از شبکه‌های داخلی در مقابل نفوذ خرابکاران از طریق شبکه اینترنت در نظر گرفته شود.

صرف نظر از محیط کاری، تحت هر شرایطی همواره می‌توان از دوربین‌های مخفی، آژیر، سیستم‌های احراز هویت و سیستم‌های امنیتی مشابه برای حفاظت از تجهیزات فیزیکی استفاده کرد.

رمزگذاری

رمزگذاری داده‌های با اهمیتی که انتقال آن‌ها از طریق شبکه صورت می‌گیرد، یک ضرورت است. در بیشتر موارد برای این منظور از یک کلید خصوصی (اصطلاحاً private key) برای رمزگذاری داده‌های ارسالی استفاده می‌شود. در سمت گیرنده کاربران با در دست داشتن یک کلید عمومی (اصطلاحاً public key) می‌توانند داده‌ها را رمزگشایی کنند.

هنگام نصب سیستم‌عامل Red Hat Linux می‌توان سرویس‌های مختلف و سایر سیستم‌ها را با استفاده از کلمات عبور محافظت کرد. شیوه‌های مختلفی برای استفاده از مکانیزم رمزگذاری موجود است که در ادامه به شرح آن‌ها می‌پردازیم:

- **مکانیزم MD5**: در این مکانیزم از کلیدی شامل ۳۲ رقم هگزادسیمال (۱۲۸ بیت) برای محافظت داده‌ها استفاده می‌شود. (لازم به یادآوری است که سیستم‌عامل Linux کلمات عبوری شامل حداکثر ۲۵۶ کاراکتر را مورد پشتیبانی قرار می‌دهد.)
- **مکانیزم Shadow Password Suite**: در این مکانیزم نسخه رمزگذاری شده‌ای از کلمات عبور در فایل /etc/shadow نگهداری می‌شود. دستیابی به این فایل تنها توسط کاربر اصلی مقدور است. این مکانیزم به طور پیش‌فرض در سیستم‌عامل Linux فعال است. (برای اطلاع بیشتر در این زمینه به فصل نهم مراجعه کنید.)
- **مکانیزم Kerberos**: استفاده از این مکانیزم رمزگذاری، ضرورت ارسال کلمات عبور از طریق شبکه را از میان برمی‌دارد. مکانیزم مزبور احراز هویت کلاینت و سرور را به واسطه سرویسی با عنوان Ticket-Generating Service یا به اختصار TGS انجام می‌دهد. مکانیزم Kerberos یک سیستم رمزگذاری کامل است که استفاده از آن به همراه مکانیزم Shadow Password Suite مقدور نبوده اما تا اندازه‌ای با مکانیزم Pluggable Authentication Modules یا به اختصار PAM (که به زودی آن‌را مورد بحث قرار خواهیم داد) سازگار است. این مکانیزم توسط انستیتو تکنولوژی ماساچوست در ایالات متحده آمریکا توسعه یافته است.
- **مکانیزم GNU Privacy Guard یا GPG**: این مکانیزم برای رمزگذاری پیغام‌های الکترونیکی (اصطلاحاً e-mail) طراحی شده و معمولاً به همراه نسخه‌ای از مکانیزم Pretty Good Privacy یا به اختصار PGP که برای سیستم‌عامل Linux توسعه یافته است، مورد استفاده قرار می‌گیرد. از این مکانیزم به منظور احراز هویت در بارگذاری نرم‌افزارها از جمله بسته‌های نرم‌افزاری RPM نیز بهره‌برداری می‌شود. (برای اطلاع بیشتر در این زمینه به فصل دهم مراجعه کنید.)
- **مکانیزم RSA و DSA**: مکانیزم Digital Signature Algorithms یا به اختصار DSA در قالب مکانیزم دیگری با عنوان Secure Shell یا SSH به منظور دستیابی به شبکه مورد استفاده قرار می‌گیرد. (برای اطلاع بیشتر درباره نحوه بهره‌برداری از مکانیزم SSH به همراه DSA به فصل بیست و سوم مراجعه کنید.)

امنیت کلمات عبور

امنیت حاصل از کلمات عبور را می‌توان در مجموع به سه سطح مختلف شامل کامپیوتر میزبان، برنامه bootloader و سیستم‌عامل تقسیم کرد. در هر یک از این سطوح باید در مورد لزوم استفاده از کلمه عبور و نوع آن و هم‌چنین لزوم تغییر آن در پریودهای زمانی مشخص تصمیم‌گیری شود. (برای اطلاع بیشتر درباره مسایل مربوط به کلمات عبور به فصل نهم مراجعه کنید.)

محافظت از کامپیوتر میزبان با استفاده از کلمه عبور

برنامه سیستم ورودی و خروجی پایه یا اصطلاحاً BIOS کامپیوترهای شخصی امروزی را می‌توان با استفاده از گزینه‌ای که به همین منظور پیش‌بینی شده است، محافظت کرد. برنامه مزبور مجموعه‌ای از گزینه‌های متنوع را در اختیار قرار می‌دهد که تغییر نامناسب مقادیر برخی از آن‌ها می‌تواند برای داده‌ها تهدیدآمیز باشد.

با وجود این، هر گونه تغییری در مقادیر گزینه‌های برنامه BIOS مستلزم دسترسی فیزیکی به کامپیوتر شخصی است. به این ترتیب، در صورتی که کامپیوتر موردنظر از لحاظ فیزیکی محافظت شده باشد، به استفاده از کلمه عبور برای محافظت از برنامه BIOS نیاز نیست.

محافظت از برنامه bootloader با استفاده از کلمه عبور

چنان‌که قبلاً نیز بارها اشاره شد، دو برنامه GRUB و LILO به عنوان برنامه‌های bootloader در سیستم‌عامل Linux پیش‌بینی شده‌اند. در این میان بیشتر کاربران استفاده از برنامه GRUB را ترجیح می‌دهند، چرا که این برنامه را می‌توان با بهره‌گیری از کلمه عبور محافظت کرد. در صورت عدم محافظت از برنامه bootloader هر گونه تغییری در فایل پیکربندی برنامه مزبور، تغییر کلمه عبور کاربر اصلی (به واسطه راه‌اندازی سیستم‌عامل Linux در حالت تک‌کاربره یا اصطلاحاً single-user mode) و یا راه‌اندازی سیستم‌عامل دیگری مانند Windows که برنامه مورد بحث امکان راه‌اندازی آن‌را در اختیار قرار می‌دهد، وجود دارد. (برای اطلاع بیشتر درباره برنامه GRUB که برنامه bootloader پیش‌فرض در سیستم‌عامل Red Hat Linux محسوب می‌شود، به فصل یازدهم مراجعه کنید.) با به کارگیری تکنیک‌های مورد بحث در فصل یازدهم می‌توانید دسترسی به سایر سیستم‌عامل‌ها از طریق برنامه bootloader را محدود کنید. برای مثال، فرض کنید برنامه GRUB پیکربندی شده روی یک کامپیوتر امکان راه‌اندازی آن با یکی از دو سیستم‌عامل Linux و Windows را در اختیار قرار می‌دهد. در این صورت، با تغییر محتوای فایل پیکربندی برنامه مزبور با عنوان /boot/grub/grub.conf می‌توان ترتیبی

داد تا راه‌اندازی آن کامپیوتر با سیستم‌عامل Windows تنها با وارد کردن کلمه عبور مربوطه امکان‌پذیر باشد. به نحوه انجام این کار توجه کنید:

```
title DOS
      lock
      password --md5 sf934^(^$asjl
      rootnoverify (hd0,0)
      chainloader +1
```

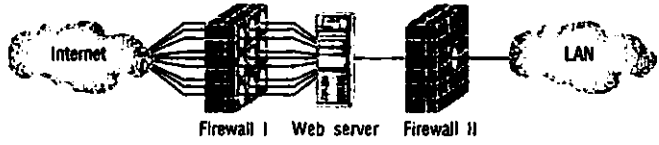
فرمان lock در فایل پیکربندی برنامه GRUB از راه‌اندازی کامپیوتر با سیستم‌عامل مربوطه (در این‌جا سیستم‌عامل Windows که با برچسب DOS مشخص شده است) جلوگیری به عمل می‌آورد، به طوری که هر تلاشی در این زمینه با پیغام خطای must be authenticated مواجه می‌شود. با وجود تغییرات فوق، ابتدا باید کلمه عبور موردنیاز به منظور ویرایش فایل پیکربندی برنامه GRUB را وارد کنید. سپس با وارد کردن کلمه عبور MD5 مربوطه می‌توانید کامپیوتر را با سیستم‌عامل Windows راه‌اندازی کنید.

مکانیزم بازدارنده دیوار آتش و نواحی DMZ

مکانیزم دیوار آتش را با توجه به نحوه عملکرد می‌توان به سه نوع مختلف تقسیم کرد. در نوع اول تمام بسته‌های اطلاعاتی ارسالی به شبکه میزبان مورد بازبینی قرار گرفته و با توجه به محتوای آن بسته‌ها در مورد تحویل آن‌ها به شبکه، تصمیم‌گیری می‌شود. عملکرد نوع دوم مربوط به سرویس‌هایی چون Samba، NFS و Apache است. همان گونه که در فصل‌های مربوطه نیز اشاره شد، نحوه دسترسی به داده‌ها از طریق این سرویس‌ها به واسطه مکانیزم‌های محدود کننده‌ای که عملکرد آن‌ها کم‌وبیش شبیه به مکانیزم بازدارنده دیوار آتش است، کنترل می‌شود و بالاخره چنان‌که در فصل بیست و سوم خواهید دید، نوع سوم مربوط به سرویس‌هایی است که بر اساس شبح xinetd توسعه یافته‌اند.

در سیستم‌عامل Red Hat Linux مکانیزم بازدارنده دیوار آتش در قالب برنامه‌ای با عنوان iptables پیاده‌سازی شده است. چنان‌که به زودی در همین فصل خواهید دید، می‌توان این برنامه را به نحوی پیکربندی کرد که از ترافیک به خصوصی جلوگیری به عمل آورد. هم‌چنین می‌توان آن‌را به گونه‌ای پیکربندی کرد که منهای ترافیک ناشی از برخی سرویس‌ها از تمام ترافیک جلوگیری به عمل آورد. اگر مکانیزم دیوار آتش روی کامپیوتری که به عنوان دروازه شبکه مورد استفاده قرار گرفته است، پیکربندی شود، می‌تواند از حملات خارجی (که از شبکه‌هایی چون اینترنت صورت می‌گیرد) به شبکه میزبان جلوگیری به عمل آورد. اغلب به چنین کامپیوتری bastion host گفته می‌شود.

مکانیزم دیوار آتش را می‌توان روی کامپیوترهای مختلف شبکه به گونه‌های متفاوتی پیکربندی کرد. برای مثال، در مورد یک وب سرور این پیکربندی ممکن است شبیه به شکل ۱-۲۲ باشد. در این شکل مکانیزم بازدارنده نخست با عنوان Firewall I به منظور کمترین بازدارندگی (شامل فرامین پیشگیری از حملاتی از قبیل ping مرگبار یا اصطلاحاً ping of death) و مکانیزم بازدارنده دوم با عنوان Firewall II به منظور بازدارندگی کامل (ایمن‌سازی شبکه در برابر تهاجمات اینترنتی) پیکربندی شده‌اند. ایمن‌سازی شبکه در مقابل حمله ping مرگبار و سایر موارد را به زودی در همین فصل مورد بررسی قرار خواهیم داد.



شکل ۱-۲۲ ایمن‌سازی شبکه با استفاده از دو مکانیزم بازدارنده دیوار آتش

حمله ping مرگبار از نوع حملات DoS یا اصطلاحاً Denial-of-Service است. در این حمله با استفاده از فرمان ping بسته‌های اطلاعاتی بسیار زیادی برای سرور موردنظر ارسال می‌شود.

مکانیزم Pluggable Authentication Modules یا PAM

مکانیزم Pluggable Authentication Modules یا به اختصار PAM یکی دیگر از مکانیزم‌های امنیتی قابل توجه است. عملکرد این مکانیزم بر اساس مجموعه‌ای از ماجول‌هایی استوار است که امکان دسترسی کاربر اصلی به برخی از برنامه‌ها مانند halt یا redhat-config-network را محدود می‌کند. با بهره‌گیری از این ماجول‌ها می‌توان امکان دسترسی به برنامه‌های موردنظر را تنها در اختیار یک یا چند کاربر به خصوص قرار داد. هم‌چنین می‌توان ترتیبی داد تا دسترسی مزبور تنها از طریق کامپیوتر یا کامپیوترهای خاصی از شبکه امکان‌پذیرباشد. بابهره‌گیری از نشانه‌های کنترلی (اصطلاحاًcontrol flags) می‌توان میزان تأثیر فرامین PAM را در ارتباط با تعیین صلاحیت کاربر جهت اجرای برنامه موردنظر مشخص کرد.

تعاریف و اصطلاحات مورد استفاده در رابطه با مکانیزم PAM گاهی اوقات تا اندازه‌ای مبهم است. برای اجتناب از ابهام، واژه "برنامه" را برای اشاره به فرامینی مورد استفاده قرار می‌دهیم که منجر به فراخوانی ماجول‌های PAM (یا به طور دقیق اجرای فرامین PAM) می‌شوند.

ساختار فرامین PAM

مکانیزم PAM شامل مجموعه‌ای از ماجول‌هاست که می‌توان آن‌ها را به منظور محدود کردن دسترسی کاربران به برنامه‌های کاربردی مورد استفاده قرار داد. فایل‌های پیکربندی این مکانیزم در فهرست /etc/pam.d و کلیه ماجول‌ها در فهرست /lib/security مستقر شده‌اند. مستندات مربوط به این ماجول‌ها را می‌توان با مراجعه به فهرست /usr/share/doc/pam-*version*/txts مورد مطالعه قرار داد.

الگوی عمومی بهره‌برداری از مکانیزم امنیتی PAM به این صورت است:

```
module_type control_flag module_location arguments
```

در قسمت‌های بعد به بررسی انواع ماجول‌ها و نشانه‌های کنترلی خواهیم پرداخت. موقعیت ماجول که در الگوی فوق با متغیر module_location مشخص شده است به موقعیت فایل مربوطه (عموماً فهرست /lib/security) اشاره دارد. هر ماجول شامل آرگومان‌هایی است که می‌توان به منظور کنترل بیشتر آن‌ها را مورد استفاده قرار داد.

انواع ماجول‌ها

در مجموع چهار نوع ماجول PAM به این شرح موجود است:

- **ماجول‌های نوع Password:** کنسولی که سیستم‌عامل Linux برای ورود کاربر به سیستم در اختیار وی قرار می‌دهد، از تلاش مکرر کاربر برای ورود به سیستم جلوگیری به عمل می‌آورد. این رفتار به دلیل وجود ماجولی از نوع Password است که علاوه بر محدود کردن تعداد دفعات اقدام کاربر جهت ورود به سیستم، طول کلمه عبور را نیز محدود می‌کند.
- **ماجول‌های نوع Session:** این نوع ماجول‌ها تنظیمات مربوط به یک برنامه را به عهده دارند. با استفاده از این نوع ماجول‌ها می‌توان تعداد دفعاتی را که یک کاربر به خصوص می‌تواند برای ورود به سیستم اقدام کند، مشخص کرد.
- **ماجول‌های نوع Account:** این نوع ماجول‌ها امکان دسترسی کاربران را با توجه به خط مشی‌ها کنترل می‌کنند. با استفاده از این نوع ماجول‌ها می‌توان دسترسی کاربران را براساس لیستی از اسامی آن‌ها، زمان دستیابی یا با توجه به موعد انقضای کلمه عبور کاربران کنترل کرد.
- **ماجول‌های نوع Auth:** این نوع ماجول‌ها به منظور شناسایی کاربران مورد استفاده قرار می‌گیرند. با استفاده از این نوع ماجول‌ها می‌توان برای دریافت نام کاربری و کلمه عبور کاربران جهت احراز هویت آن‌ها اقدام کرد.

پارامتر service=system-auth یکی از متداول‌ترین پارامترهایی است که به همراه ماجول‌های فوق مورد بهره‌برداری قرار می‌گیرد. استفاده از این پارامتر کاربر را ملزم می‌کند تا برای وارد کردن نام کاربری و کلمه عبور خود اقدام کند.

نشانه‌های کنترلی

در فرامین مربوط به مکانیزم PAM می‌توان از چهار نشانه کنترلی که شرح آن‌ها در جدول ۱-۲۲ آمده است، استفاده کرد. این نشانه‌های کنترلی عملکرد برنامه موردنظر را با توجه به موفقیت یا عدم موفقیت ماجول‌های مکانیزم PAM مشخص می‌کنند.

جدول ۱-۲۲ شرح نشانه‌های کنترلی مورد استفاده در فرامین مربوط به مکانیزم PAM

عنوان نشانه کنترلی	توضیح
optional	این نشانه کنترلی به معنی بی‌تأثیر بودن ماجول موردنظر است، مگر آن‌که در ساختار سایر فرامین نیز از این نشانه کنترلی استفاده شده باشد.
required	چنان‌چه عملکرد ماجول موردنظر موفقیت‌آمیز نباشد، استفاده از این نشانه کنترلی موجب پیشگیری از اجرای برنامه می‌شود.
requisite	چنان‌چه عملکرد ماجول موردنظر موفقیت‌آمیز نباشد، بلافاصله فرآیند احراز هویت متوقف شده و از اجرای فرمان مربوطه جلوگیری به عمل می‌آید. هم‌چنین از اجرای سایر فرامین نیز صرف نظر می‌شود.
sufficient	چنان‌چه عملکرد ماجول موردنظر موفقیت‌آمیز باشد، بلافاصله فرآیند احراز هویت متوقف شده و فرمان مربوطه به اجرا درمی‌آید. ضمناً از اجرای سایر فرامین صرف نظر می‌شود.

بررسی مثال‌هایی در مورد نحوه عملکرد مکانیزم امنیتی PAM

بررسی خط به خط فایل‌های پیکربندی مکانیزم امنیتی PAM در درک هر چه بهتر نحوه عملکرد این مکانیزم بسیار مؤثر است. تمام این فایل‌های پیکربندی به طور پیش‌فرض در فهرست /etc/pam.d مستقر هستند. مثال‌هایی را که در ادامه مورد بررسی قرار می‌دهیم، از فایل پیکربندی مربوط به برنامه redhat-config-xfree86 اقتباس شده‌اند.

```
auth sufficient pam_rootok.so
```

با توجه به نوع ماجول، یعنی auth می‌توان نتیجه گرفت که فرمان فوق وظیفه احراز هویت کاربر را به عهده دارد. از طرفی وجود نشانه کنترلی sufficient موجب می‌شود تا در صورت اجرای موفقیت آمیز این فرمان، برنامه موردنظر یعنی redhat-config-xfree86 به اجرا درآید. چنان‌چه کاربری که برای اجرای برنامه مذکور اقدام کرده است کاربر اصلی (اصطلاحاً root) باشد، ماجول pam_rootok.so که در فهرست /lib/security واقع شده است مقدار PAM_SUCCESS را بازمی‌گرداند. به بیان دیگر، در صورتی که کاربر اصلی برنامه redhat-config-xfree86 را اجرا کند، از اجرای سایر فرامین موجود در این فایل پیکربندی صرف‌نظر شده و اجرای برنامه نامبرده آغاز می‌شود.

```
auth sufficient pam_timestamp.so
```

با توجه به نوع ماجول، یعنی auth این فرمان نیز مانند فرمان قبل وظیفه احراز هویت کاربر را به عهده داشته و ضمناً از نشانه کنترلی sufficient در ساختار آن استفاده شده است. چنان‌چه کاربری غیر از **کاربر اصلی ظرف ۵ دقیقه اخیر فرمان sudo را اجرا کرده باشد، ماجول pam_timestamp.so مقدار** PAM_SUCCESS را بازمی‌گرداند.

```
auth required pam_stack.so srvice=system-auth
```

با توجه به نوع ماجول، یعنی auth فرمان فوق نیز مانند دو فرمان قبل وظیفه احراز هویت کاربران را به عهده دارد با این تفاوت که این‌بار در ساختار آن از نشانه کنترلی required استفاده شده است. به واسطه وجود پارامتر service=system-auth استفاده از کلمه عبور کاربر اصلی الزامی است. چنان‌چه کلمه عبور کاربر اصلی به درستی وارد شود ماجول pam_stack.so مقدار PAM_SUCCESS را بازمی‌گرداند.

```
session required pam_permit.so
```

در فرمان فوق ماجولی از نوع session به همراه نشانه کنترلی required مورد استفاده قرار گرفته است. از آن‌جا که ماجول pam_permit.so همواره مقدار PAM_SUCCESS را بازمی‌گرداند، فرمان بعد نیز اجرا می‌شود.

```
session optional pam_xauth.so
```

در فرمان فوق ماجولی از نوع session به همراه نشانه کنترلی optional مورد استفاده قرار گرفته است. ماجول pam_xauth.so ـ هیچ مقداری دال بر موفقیت‌آمیز بودن یا نبودن عملیات بازنمی‌گرداند. وجود نشانه کنترلی optional در این فرمان ماجول pam_xauth.so را بی‌تأثیر می‌کند. با وجود این، می‌توان آرگومان debug را جهت ثبت هرگونه دسترسی به برنامه موردنظر در فایل /var/log/messages مورد استفاده قرار داد.

```
session optional pam_timestamp.so
```

در این فرمان نیز مانند فرمان قبل ماجولی از نوع session به همراه نشانه کنترلی optional مورد استفاده قرار گرفته است. ماجول pam_timestamp.so تمام فایل‌های ثبت زمان (اصطلاحاً فایل‌های timestamp) موجود را که عموماً در فهرست /var/run/sudo مستقر هستند، به روز می‌کند. ساختار آخرین فرمان به این شکل است:

```
account required pam_permit.so
```

در این فرمان ماجولی از نوع account به همراه نشانه کنترلی required مورد استفاده قرار گرفته است. چنان‌که قبلاً نیز گفته شد، ماجول pam_permit.so همواره مقدار PAM_SUCCESS را بازمی‌گرداند.

بهره‌برداری از مکانیزم بازدارنده دیوار آتش

به هر نوع مکانیزمی که از ترافیک ورودی به کامپیوتر یا شبکه ممانعت به عمل آورد، دیوار آتش یا اصطلاحاً firewall گفته می‌شود. در فصول بعد برخی از این مکانیزم‌ها را که در قالب فرامین یا فایل‌های پیکربندی پیاده‌سازی شده‌اند، بررسی خواهیم کرد. در این قسمت برنامه iptables را که در سیستم‌عامل Linux ابزار اصلی مورد استفاده به عنوان مکانیزم بازدارنده دیوار محسوب می‌شود، مورد بررسی قرار می‌دهیم. این ابزار متشکل از فرامینی است که می‌توان آن‌ها را به طور زنجیروار به یکدیگر متصل کرد. فرامین مزبور کلیه امکانات لازم برای عبور دادن یا متوقف کردن ترافیک ناشی از پروتکل‌های را در اختیار می‌گذارد.

سایر برنامه‌های مورد استفاده در سیستم‌عامل Linux به عنوان دیوار آتش

دو برنامه ipfwadm و ipchains تا پیش از این به طور گسترده‌ای در سیستم‌عامل Linux به عنوان مکانیزم بازدارنده دیوار آتش مورد استفاده قرار می‌گرفتند. برنامه ipfwadm که در قالب نسخه‌هایی از هسته سیستم‌عامل Linux به شناسه عمومی 2.0.x پیاده‌سازی می‌شد اکنون دیگر منسوخ شده است. این در حالی است که برنامه iptables در قالب نسخه‌هایی از هسته سیستم‌عامل Linux به شناسه عمومی 2.2.x پیاده‌سازی شده و هم‌چنان در نسخه‌هایی از هسته سیستم‌عامل Linux با شناسه عمومی 2.4.x نیز مورد پشتیبانی قرار گرفته است.

در سال‌های اخیر برنامه‌های خوبی بر اساس برنامه ipchains به عنوان مکانیزم دیوار آتش توسعه یافته که برای استفاده از آن‌ها باید این موارد را رعایت کنید:

۱- با اجرای فرمان service iptables stop سرویس iptables را متوقف کنید.

۲- با استفاده از فرمان rmmod ماجول‌های برنامه iptables (به همراه ماجول‌های مربوطه) را از حافظه تخلیه کنید.

۳- بسته نرم‌افزاری *-ipchains را نصب کنید.

۴- با استفاده از فرمان insmod ماجول ipchains.o را فعال کنید.

پس از انجام این اقدامات می‌توانید قوانین موردنظر خود را در فایل پیکربندی /etc/sysconfig/ipchains درج کرده و با اجرای فرمان service ipchains start سرویس مربوط به مکانیزم ipchains را فعال کنید. اقدامات لازم برای فعال شدن مکانیزم بازدارنده ipchains (به جای مکانیزم iptables) در دفعات آتی راه‌اندازی کامپیوتر میزبان انجام دهید. برای این منظور می‌توانید فرمان مناسبی از مجموعه فرامین chkconfig را مورد استفاده قرار دهید.

عملکرد برنامه iptables در ارتباط با ترافیک ناشی از داده‌ها

برنامه iptables می‌تواند جریان داده‌های ورودی به یک کامپیوتر و داده‌های خروجی از آن و هم‌چنین جریان داده‌هایی را که از طریق آن کامپیوتر منتقل می‌شود، تحت تأثیر قرار دهد. به بیان دیگر، می‌توان برنامه ipconfig را چنان روی یک کامپیوتر پیکربندی کرد که ترافیک ورودی از یک شبکه خارجی به آن کامپیوتر متوقف شود. هم‌چنین می‌توان برنامه ipconfig را طوری روی یک کامپیوتر پیکربندی کرد که امکان خروج ترافیک از آن کامپیوتر میسر نباشد و بالاخره می‌توان این برنامه را به نحوی روی یک کامپیوتر پیکربندی کرد که مانع عبور ترافیک ارسالی از طریق آن کامپیوتر شود. به این ترتیب، می‌توان برنامه iptables را چنان روی یک کامپیوتر پیکربندی کرد که از ترافیک بین یک شبکه محلی و اینترنت جلوگیری به عمل آورد.

استفاده از دیوارهای آتش به صورت زنجیروار

تنوع کاربردهای برنامه iptables به عنوان مکانیزم بازدارنده دیوار آتش بسیار زیاد است. اغلب این گونه مکانیزم‌ها با ترکیب زنجیروار چند برنامه iptables پیکربندی می‌شوند. در این قسمت چنین مکانیزم ساده‌ای را که براساس یک مکانیزم بازدارنده بسیار مطمئن که هنگام نصب سیستم‌عامل Red Hat Linux روی کامپیوتر میزبان نصب می‌شود، مورد بررسی قرار می‌دهیم. شکل ۲-۲۲ محتوای فایل پیکربندی /etc/sysconfig/iptables را به عنوان فایلی که سیستم‌عامل نامبرده فرامین مربوط به مکانیزم بازدارنده دیوار آتش را در آن‌جا ذخیره می‌کند، نشان می‌دهد.

```
# Firewall configuration written by lokkit
# Manual customization of this file is not recommended.
# Note: ifup-post will punch the current nameservers through the
#       firewall; such entries will *not* be listed here.
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
:RH-Lokkit-0-50-INPUT - [0:0]
-A INPUT -j RH-Lokkit-0-50-INPUT
-A RH-Lokkit-0-50-INPUT -i lo -j ACCEPT
-A RH-Lokkit-0-50-INPUT -p udp -m udp -s 207.217.126.81 --sport 53 -d 0/0 -j ACCEPT
-A RH-Lokkit-0-50-INPUT -p udp -m udp -s 207.217.120.83 --sport 53 -d 0/0 -j ACCEPT
-A RH-Lokkit-0-50-INPUT -p tcp -m tcp --syn -j REJECT
-A RH-Lokkit-0-50-INPUT -p udp -m udp -j REJECT
COMMIT
~
~
~
~
~
~
~
```

شکل ۲-۲۲ فایل پیکربندی برنامه iptables که به عنوان مکانیزم بازدارنده دیوار آتش در سیستم‌عامل Linux مورد استفاده قرار می‌گیرد.

در حال حاضر تنها چهار زنجیره مختلف موجود در این فایل با عناوین INPUT، FORWARD، OUTPUT و RH-Lokkit-0-50-INPUT را مورد توجه قرار دهید. سه زنجیره نخست زنجیره‌های پیش فرضی هستند که امکان عبور هر گونه ترافیک از طریق دیوار آتش (یا به بیان بهتر، از میان آن) را فراهم می‌کنند. تمام فرامینی که با A- آغاز شده‌اند به انتهای زنجیره RH-Lokkit ضمیمه می‌شوند. در قسمت‌های بعد فرامین برنامه iptables و گزینه‌های آن‌ها را با جزییات مربوطه مورد بررسی قرار می‌دهیم.

ساختار فرمان iptables

در این قسمت به بررسی جزییات فرمان iptables می‌پردازیم. این فرمان شامل جزییات مفصلی است، به طوری که تاکنون درباره آن کتاب‌های متعددی به چاپ رسیده است. ضمن آن‌که بررسی گزینه‌های مربوط به نقاب‌زنی (اصطلاحاً masquerading) را به قسمت‌های بعدی همین فصل موکول می‌کنیم. اجازه دهید تا عملکرد گزینه‌های مهم‌تر را در قالب این الگوی عمومی مورد بررسی قرار دهیم:

```
iptables -t table option pattern -j target
```

با استفاده از گزینه t- می‌توان یکی از دو جدول filter و nat را (به جای متغیر *table* در الگوی فوق) مشخص کرد. جدول nat از مکانیزم Network Address Translation یا به اختصار NAT به همراه

تکنیک نقاب‌زنی پشتیبانی به عمل می‌آورد. جدول filter نیز امکان عبور دادن یا بلوکه کردن انواع ترافیک شبکه را در اختیار قرار می‌دهد. از آن‌جا که در این مورد جدول filter گزینه پیش‌فرض محسوب می‌شود، در اغلب موارد از درج عبارت t filter- صرف نظر به عمل می‌آید.

گزینه‌های فرمان iptables

بار دیگر سه نوع زنجیره پیش‌فرض با عناوین INPUT، OUTPUT و FORWARD را در نظر بگیرید. فرمان iptables دارای چهار گزینه است که در این میان سه گزینه L-، A- و D- به ترتیب برای نمایش دادن، ضمیمه کردن و حذف کردن قانون موردنظر و گزینه F- به منظور بی‌اثر کردن تمام قوانین مربوط به یک زنجیره پیش‌بینی شده‌اند.

فرمان iptables -L کلیه قوانین جاری مربوط به تمام زنجیره‌ها را نمایش می‌دهد. چنان‌چه مکانیزم دیوار آتش موردنظر از پیچیدگی زیادی برخوردار باشد، نمایش قوانین مربوط به یک زنجیره خاص در برخی موارد می‌تواند مفید باشد. با اجرای فرمان iptables -L INPUT می‌توان تمام قوانین موجود در ارتباط با ترافیک ورودی به کامپیوتر میزبان را مشاهده کرد. شکل ۳-۲۲ کلیه قوانین مربوط به یک مکانیزم بازدارنده نمونه را نشان می‌دهد.

```
[root@RH9Test root]# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
RH-Lokkit-0-50-INPUT  all  --  anywhere             anywhere

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
RH-Lokkit-0-50-INPUT  all  --  anywhere             anywhere

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination

Chain RH-Lokkit-0-50-INPUT (2 references)
target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere
ACCEPT     udp  --  rns1.earthlink.net   anywhere           udp spt:domain
ACCEPT     udp  --  rns3.earthlink.net   anywhere           udp spt:domain
REJECT     tcp  --  anywhere             anywhere           tcp flags:SYN,RST,ACK/
SYN reject-with icmp-port-unreachable
REJECT     udp  --  anywhere             anywhere           udp reject-with icmp-p
ort-unreachable
[root@RH9Test root]# []
```

شکل ۳-۲۲ نمونه‌ای از قوانین جاری یک مکانیزم بازدارنده

وضع یک قانون جدید عموماً با ضمیمه کردن آن به انتهای یکی از زنجیره‌های موجود انجام می‌شود. برای مثال، این فرمان قانونی را مبنی بر این‌که در هر ثانیه تنها امکان ارسال یک بسته ping از طریق

کامپیوتر میزبان وجود دارد به زنجیره FORWARD ضمیمه کرده و به این ترتیب از حمله ping مرگبار جلوگیری به عمل می‌آید:

```
# iptables -A FORWARD -p icmp --icmp-type echo-request -m
limit --limit 1/s -j ACCEPT
```

برای حذف یک قانون موجود باید زنجیره موردنظر و موقعیت آن قانون را درون آن زنجیره مشخص کنید. برای مثال، با توجه به شکل ۳-۲۲ قانون مربوط به rns3.earthlink.net سومین قانون موجود در زنجیره RH-Lokkit-0-50-INPUT است. از این‌رو، برای حذف آن کافی است این فرمان را اجرا کنید:

```
# iptables -D RH-Lokkit-0-50-INPUT 3
```

حذف کلیه قوانین موجود در یک زنجیره بسیار ساده‌تر بوده و برای این منظور کافی است با استفاده از گزینه F- زنجیره موردنظر را مشخص کنید. به عنوان مثال، با اجرای این فرمان تمام قوانین زنجیره FORWARD حذف خواهد شد:

```
# iptables -F FORWARD
```

با این حال اقدام فوق می‌تواند بسیار خطرناک باشد. چنان‌چه در اجرای فرمان iptables -F هیچ زنجیره‌ای مشخص نشود کلیه قوانین موجود در تمام زنجیره‌ها حذف خواهد شد. جدول ۲-۲۲ گزینه‌های فرمان iptables را شرح می‌دهد.

جدول ۲-۲۲ شرح گزینه‌های فرمان iptables

عنوان گزینه	توضیح
-A *chain rule*	با استفاده از این گزینه می‌توان قانونی را به انتهای زنجیره *chain* ضمیمه کرد.
-D *chain number*	با استفاده از این گزینه می‌توان قانونی با شماره *number* را از زنجیره *chain* حذف کرد.
-F *chain*	با استفاده از این گزینه می‌توان تمام قوانین زنجیره *chain* را حذف کرد.
-I *chain number rule*	با استفاده از این گزینه می‌توان قانون *rule* را در موقعیتی با شاخص *number* از زنجیره *chain* درج کرد.
-L *chain*	با استفاده از این گزینه می‌توان تمام قوانین موجود در زنجیره *chain* را مشاهده کرد.
-N *chain*	با استفاده از این گزینه می‌توان زنجیره *chain* را به عنوان یک زنجیره غیراستاندارد از قوانین تعریف کرد.
-X *chain*	با استفاده از این گزینه می‌توان زنجیره غیراستاندارد *chain* را حذف کرد.

الگوهای مورد استفاده در فرمان iptables

در این قسمت قصد داریم فرمان iptables را از دیدگاه دیگری مورد بررسی قرار دهیم. پیشتر با چگونگی درج قوانین در یک زنجیره آشنا شدید. اکنون باید به نحوی الگوی اعمال این قوانین را تعیین کنیم. با استفاده از چنین الگوهایی می‌توانیم آدرس IP ارسال کنندگان یا دریافت کنندگان پیغام‌ها را، پورت‌هایی که پیغام‌های موردنظر از طریق آن‌ها ردوبدل می‌شود و هم‌چنین پروتکل‌های مورد استفاده برای انتقال پیغام‌ها را مشخص کنیم. در قسمت‌های بعد هریک از این موارد را بررسی خواهیم کرد.

الگوی آدرس IP

بار دیگر قانونی را که در قسمت‌های قبل به منظور پیشگیری از حمله ping مرگبار در زنجیره FORWARD درج کردیم، در نظر بگیرید. فرض کنید به دلایلی مایلیم تا این قانون را تنها به یک آدرس IP به خصوص یعنی 199.88.77.66 اعمال کرده و به این ترتیب تعداد بسته‌های ارسالی از کامپیوتری با آدرس IP فوق را به یک بسته در هر ثانیه محدود کنیم. برای این منظور کافی است این فرمان را اجرا کنید:

```
# iptables -A FORWARD -s 199.88.77.66 -p icmp --icmp-type
echo-request -m limit --limit 1/s -j ACCEPT
```

به نحوه مشخص کردن آدرس IP موردنظر با استفاده از سوییچ s- دقت کنید. در صورت تمایل **می‌توانیم تأثیر این فرمان را با قرار دادن علامت ! درست قبل از آدرس IP فوق معکوس کرده و به این ترتیب امکان ارسال تعداد بیش از یک بسته ping را تنها در اختیار کامپیوتری با آدرس 199.88.77.66** قرار دهیم. به نحوه انجام این کار توجه کنید:

```
# iptables -A FORWARD -s !199.88.77.66 -p icmp --icmp-type
echo-request -m limit --limit 1/s -j ACCEPT
```

با مشاهده علامت ! فرمان iptables متوجه می‌شود که آن‌چه در پی می‌آید یک استثنا بوده و باید از اعمال قانون موردنظر به آن صرف نظر کند.

امکان تعیین محدوده‌ای از آدرس‌های IP یک شبکه نیز بسیار مفید است. برای مثال، در این دو فرمان آدرس IP شبکه به روش معمول و CIDR با یک ماسک شبکه ترکیب شده و به این ترتیب محدوده‌ای از آدرس‌های IP مشخص شده است: (برای اطلاع بیشتر درباره مکانیزم Classless Inter-Domain Routing یا به اختصار CIDR به فصل بیست و یکم مراجعه کنید.)

```
# iptables -A FORWARD -s 199.88.77.0/255.255.255.0 -p
icmp --icmp-type echo-request -m limit --limit 1/s -j ACCEPT
```

```
# iptables -A FORWARD -s 199.88.77.0/24 -p icmp --icmp-type
echo-request -m limit --limit 1/s -j ACCEPT
```

شرح سوییچ‌های فرمان iptables در جدول ۳-۲۲ آمده است.

جدول ۳-۲۲ شرح سوییچ‌های فرمان iptables

عنوان سوییچ	توضیح
--dport *port*	به کمک این سوییچ می‌توان شماره پورت مقصد را مشخص کرد.
--icmp-type *message*	به کمک این سوییچ می‌توان نوع پیغام ICMP ارسالی را مشخص کرد. شاخص echo-request بیانگر پیغام ارسالی توسط فرمان ping است.
-j *action*	به کمک این سوییچ می‌توان ترتیبی داد تا در ازای تطبیق با یک الگوی مشخص، فرمان iptables یکی از چهار عملیات ACCEPT، DROP، REJECT یا LOG را در ارتباط با ترافیک ارسالی به اجرا درآورد.
--limit *time*	به کمک این سوییچ می‌توان نرخ ارسال پیغام (تعداد پیغام‌های ارسالی در واحد زمان شامل ثانیه، دقیقه، ساعت یا روز) را مشخص کرد. برای مثال، نرخ 2/s به معنی ارسال ۲ پیغام در هر ثانیه است.
-m *condition*	به کمک این سوییچ می‌توان عواملی مانند نوع پروتکل (از جمله tcp یا udp) را جهت تطبیق مشخص کرد.
-p *protocol*	به کمک این سوییچ می‌توان پروتکل مورد استفاده برای ارسال داده‌ها را مشخص کرد.
-s *ip_address*	به کمک این سوییچ می‌توان آدرس IP مبدأ را مشخص کرد.
--sort *port*	به کمک این سوییچ می‌توان شماره پورت مبدأ را مشخص کرد.
--tcp-flags *f1,...*	به کمک این سوییچ می‌توان نشانه‌های موجود در یک بسته TCP را مورد توجه قرار داد. بسته حاوی نشانه SYN (یا synchronize) از سوی کلاینت ارسال شده و برای دریافت پاسخ از جانب سرور منتظر می‌ماند. بسته حاوی نشانه ACK (یا acknowledgment) از سوی سرور در پاسخ به بسته حاوی نشانه SYN ارسال می‌شود. بسته حاوی نشانه FIN (یا finish) آخرین بسته ارسالی در تعامل میان کلاینت و یرور است. بسته حاوی نشانه RST (یا reset) به نشانه رد درخواست از جانب سرور برای کلاینت ارسال می‌شود. برای مثال، سوییچ --tcp-flags SYN, RST, ACK, SYN SYN از بین بسته‌هایی حاوی نشانه‌های SYN، RST و ACK تنها امکان عبور بسته‌های حاوی نشانه SYN را فراهم می‌کند.

الگوی پروتکل‌ها

چنان‌که قبلاً نیز اشاره شد، فرمان iptables قادر است تمام بسته‌های ورودی، خروجی یا ارسالی از طریق کامپیوتر میزبان را تحت تأثیر قرار دهد. در صورت تمایل می‌توان ترتیبی داد تا این اقدام با توجه به یک پروتکل خاص انجام شود. در این رابطه سه پروتکل TCP، UDP و ICMP از سایر پروتکل‌ها **متداول‌تر هستند. با استفاده از سوییچ p- می‌توان نوع پروتکلی را که فرمان iptables باید مورد توجه** قرار دهد، مشخص کرد. برای مثال، سوییچ p- icmp در فرمان پیشگیری از حمله ping مرگبار که در قسمت‌های قبل مشاهده کردید بیانگر ارسال بسته‌هایی از نوع ICMP است. (برای اطلاع بیشتر درباره پروتکل ICMP به فصل بیستم مراجعه کنید.)

الگوی پورت‌ها

همان‌گونه که از فصل بیستم به خاطر دارید، برای شبکه‌های TCP/IP بیش از ۶۵۰۰۰ پورت در نظر گرفته شده که در این میان بسیاری از آن‌ها به سرویس‌های استاندارد اختصاص یافته است. برای مثال، با اجرای این فرمان هر گونه تلاشی از جانب شبکه 199.88.77.0/24 برای ارسال بسته‌های TCP به پورت شماره ۲۱ که به سرویس استاندارد FTP اختصاص دارد، جلوگیری به عمل می‌آید:

```
# iptables -A FORWARD -s 199.88.77.0/24 -p tcp --dport 21
-j REJECT
```

اقدام برنامه iptables در ازای تطبیق بسته‌های دریافتی با الگوی مورد نظر

فرض کنید با استفاده از فرمان iptables الگویی را به منظور تطبیق بسته‌های ورودی به کامپیوتر میزبان یا خروجی از آن و هم‌چنین داده‌هایی که از طریق آن کامپیوتر به یک شبکه خارجی ارسال می‌شود، پیکربندی کرده‌اید. اکنون باید عملیاتی را مشخص کنید که برنامه iptables در ازای تطبیق این بسته‌ها با الگوی مزبور باید انجام دهد.

هنگام تطبیق بسته‌ها با الگوی مورد نظر، برنامه iptables به واسطه وجود گزینه j- یکی از چهار نوع عملیات ACCEPT، DROP، REJECT یا LOG را به شرحی که در جدول ۴-۲۲ آمده است، انجام می‌دهد.

جدول ۴-۲۲ شرح عملیات برنامه iptables هنگام مواجهه با بسته‌های قابل تطبیق با الگو

نوع عملیات	توضیح
ACCEPT	این عملیات منجر به عبور بسته‌ها از دیوار آتش می‌شود.
DROP	این عملیات منجر به بلوکه شدن یا توقف جریان بسته‌ها می‌شود.
REJECT	این عملیات منجر به بلوکه شدن یا توقف جریان بسته‌ها شده و متعاقب آن پیغام مناسبی برای فرستنده بسته‌ها ارسال می‌شود.
LOG	به واسطه این عملیات گزارشی مبنی بر تطبیق بسته‌ها با الگوی موردنظر در فایل /var/log/messages به ثبت می‌رسد.

جمع‌بندی

پس از بررسی جزییات فرمان Iptables اکنون می‌توانید قوانین حاکم بر مکانیزم بازدارنده دیوار آتش را تألیف کنید. علیرغم ابزارهای گرافیکی موجود در این زمینه (از جمله برنامه redhat-config-firewall که در فصل نوزدهم به بررسی آن پرداختیم.) بهتر است دست کم با نحوه حذف یا اضافه کردن قوانین به دیوار آتش آشنا باشید.

به عنوان تمرین در این قسمت مکانیزم دیوار آتش را روی کامپیوتری که فاقد چنین مکانیزمی است، پیکربندی می‌کنیم. فرض کنید شبکه میزبان متشکل از دست کم دو کامپیوتر باشد. ابتدا یک نسخه پشتیبان از فایل پیکربندی /etc/sysconfig/iptables تهیه کنید. قانون پیشگیری از حمله ping مرگبار را به قوانین موجود در فایل مذکور ضمیمه کنید. این قانون را به نحوی تغییر دهید که ارسال بسته‌های ping به بیرون از شبکه امکان‌پذیر نباشد.

در انجام این تمرین فرض بر آن است که شبکه‌ای با آدرس 192.168.0.0/24 را در اختیار داریم. هنگام انجام تمرین بدیهی است که باید آدرس شبکه خود را با آدرس IP فوق تعویض کنید:

۱- پیش از شروع، نسخه‌ای از فایل پیکربندی /etc/sysconfig/iptables را به عنوان پشتیبان در فهرست خانگی خود ذخیره کنید.

۲- با اجرای فرمان iptables -F کلیه قوانین دیوار آتش فعلی را حذف کنید.

۳- قانون پیشگیری از حمله ping مرگبار را به منظور جلوگیری از دریافت بسته‌های ping ارسالی از سایر کامپیوترها به کامپیوتر میزبان اضافه کنید. برای این کار کافی است این فرمان را اجرا کنید:

```
# iptables -A INPUT -s 192.168.0.0/24 -p icmp --icmp-type
echo-request -j DROP
```

۴- فرمان ping 127.0.0.1 را روی کامپیوتر میزبان اجرا کنید. با انجام این کار خواهید دید که هیچ مانعی در ارسال بسته‌های ping از کامپیوتر میزبان برای خود آن کامپیوتر وجود ندارد.

۵- اکنون سعی کنید تا از یک کامپیوتر دیگر مستقر در شبکه، بسته‌های ping را برای کامپیوتر میزبان ارسال کنید. با انجام این کار خواهید دید که قانون فوق موجب پیشگیری از دریافت بسته‌های ping ارسالی می‌شود.

۶- در صورت لزوم فایل /etc/sysconfig/iptables را از روی نسخه پشتیبان (که پیش از این در فهرست خانگی خود ذخیره کردید) بازیابی کنید.

بار دیگر تمرین فوق را تکرار کنید. این بار به جای عملیات DROP برنامه iptables را وادار کنید تا در ازای دریافت بسته‌های ping عملیات REJECT را انجام دهد. نتایج به دست آمده از این دو تمرین را به دقت مقایسه کنید.

نحوه درج قوانین دیوار آتش

بار دیگر شکل ۳-۲۲ را که شامل مجموعه‌ای از قوانین دیوار آتش است، در نظر بگیرید. بخشی از قوانین فعلی دیوار آتش به این صورت است:

```
Chain RH-Lokkit-0-50-INPUT (1 references)
target  port opt  source               destination
ACCEPT  all  --   anywhere             anywhere
ACCEPT  udp  --   rns1.earthlink.net   anywhere udp spt:domain
ACCEPT  udp  --   rns3.earthlink.net   anywhere udp spt:domain
REJECT  tcp  --   anywhere             anywhere tcp flags:SYN,
RST,ACK/SYN reject-with icmp-port-unreachable
REJECT  udp  --   anywhere             anywhere udp reject-with
icmp-port-unreachable
```

چنان‌چه در آینده قصد داشته باشید تا برنامه‌ای از نوع وب سرور را روی کامپیوتر میزبان نصب کنید، لازم است تغییراتی در این قوانین بدهید. برای این منظور باید قانون جدیدی را به مجموعه قوانین دیوار آتش اضافه کنید تا به این ترتیب امکان دریافت بسته‌های ارسالی به پورت شماره ۸۰ یعنی پورتی که برنامه وب سرور درخواست‌های ارسالی را از آن طریق دریافت می‌کند، فراهم شود. ساختار این قانون را می‌توانیم در قالب چند مرحله به این صورت توضیح دهیم:

- ابتدا باید جایگاه قانون را در زنجیره RH-Lokkit-0-50-INPUT مشخص کنیم. با بهره‌گیری از گزینه I- RH-Lokkit-0-50-INPUT می‌توانیم این قانون را به عنوان دومین قانون زنجیره مزبور درج کنیم.
- بسته‌های ارسالی به وب سرور از نوع TCP است. (دقت کنید که هر گونه ارتباط با برنامه وب سرور مستلزم تأیید آن برنامه است.) با بهره‌گیری از گزینه p tcp- می‌توانیم این موضوع را مشخص کنیم.
- با توجه به محتوای فایل /etc/services ارتباط با برنامه وب سرور از طریق پورت TCP شماره ۸۰ برقرار می‌شود. با بهره‌گیری از گزینه m tcp --dport 80- می‌توانیم این موضوع را مشخص کنیم.
- بسته‌های دریافتی توسط وب سرور باید حاوی نشانه SYN باشند. برای اطمینان از آن‌که این بسته‌ها توسط برنامه‌های دیگری از نوع سرور ارسال نشده‌اند، لازم است از بین بسته‌های ارسالی حاوی نشانه‌های SYN، RST و ACK تنها امکان دریافت بسته‌های حاوی نشانه SYN فراهم شود. با بهره‌گیری از گزینه --tcp-flags SYN,RST,ACK SYN- می‌توانیم این موضوع را مشخص کنیم.
- بدیهی است که مکانیزم بازدارنده دیوار آتش نباید از عبور بسته‌هایی با شرایط فوق ممانعت به عمل آورد. با بهره‌گیری از گزینه ACCEPT j- می‌توان این موضوع را مشخص کرد.

برای درج قانون فوق در زنجیره RH-Lokkit-0-50-INPUT از دیوار آتش کافی است این قانون را اجرا کنید:

```
# iptables -I RH-Lokkit-0-50-INPUT 2 -p tcp -m tcp --dport 80
--tcp-flags SYN,RST,ACK SYN -j ACCEPT
```

تغییرات زنجیره RH-Lokkit-0-50-INPUT پس از اجرای فرمان فوق به این صورت خواهد بود:

```
Chain RH-Lokkit-0-50-INPUT (1 references)
target  port opt  source              destination
ACCEPT  all  --   anywhere            anywhere
ACCEPT  all  --   anywhere              anywhere tcp dpt:http
flags:SYN,RST,ACK/SYN
ACCEPT  udp  --   rns1.earthlink.net  anywhere udp spt:domain
ACCEPT  udp  --   rns3.earthlink.net  anywhere udp spt:domain
REJECT  tcp  --   anywhere            anywhere tcp flags:SYN,
RST,ACK/SYN reject-with icmp-port-unreachable
REJECT  udp  --   anywhere          anywhere udp reject-with
icmp-port-unreachable
```

پس از انجام این کار باید تغییرات جدید را ذخیره کنید.

ذخیره تغییرات فایل پیکربندی /etc/sysconfig/iptables

برای ذخیره تغییرات فایل پیکربندی /etc/sysconfig/iptables فرمان service iptables save را اجرا کنید.

به دلیل اهمیت مکانیزم بازدارنده دیوار آتش در تأمین امنیت کامپیوتر میزبان و شبکه، همواره بهتر است وضعیت آن‌را مورد توجه و بازبینی قرار دهید. این اقدام با استفاده از فرمان chkconfig به سادگی امکان‌پذیر است. به عنوان نمونه، برای تشخیص آن‌که سیستم‌عامل Linux سرویس iptables را در کدام سطوح اجرایی راه‌اندازی می‌کند، کافی است این فرمان را اجرا کنید:

```
# chkconfig --list iptables
iptables  0:off 1:off 2:on 3:on 4:on 5:on 6:off
```

علاوه بر این، با اجرای فرمان chkconfig می‌توانید ترتیبی دهید تا سرویس iptables در سطوح اجرایی موردنظر از سیستم‌عامل Linux راه‌اندازی شود. برای مثال، پس از اجرای این فرمان سرویس iptables در راه‌اندازی‌های آتی سیستم‌عامل Linux در سطوح اجرایی دوم، سوم و پنجم راه‌اندازی خواهد شد:

```
# chkconfig --level 235 iptables
```

به خاطر داشته باشید که سیستم‌عامل Linux از سطح اجرایی چهارم استفاده نمی‌کند. (برای اطلاع بیشتر درباره سطوح اجرایی به فصل یازدهم مراجعه کنید.)

تکنیک نقاب‌زنی IP

نقاب‌زنی IP یا IP masquerading، روشی است که به کمک آن می‌توان آدرس IP کامپیوترهای مستقر در یک شبکه را پنهان کرد. در این روش آدرس IP کامپیوترهای مستقر در شبکه با آدرس IP دروازه شبکه تعویض شده و به این ترتیب از کامپیوترهای مزبور در مقابل حملات خارجی محافظت به عمل می‌آید.

تکنیک نقاب‌زنی IP در واقع همان مکانیزم NAT است. روش دیگر انجام این کار استفاده از یک سرور پروکسی است.

مکانیزم دیوار آتش و نقاب‌زنی IP معمولاً روی یک کامپیوتر واحد از شبکه پیاده‌سازی می‌شوند. چنین کامپیوتری همان دروازه شبکه است که ارتباط میان شبکه محلی را با یک شبکه خارجی مانند اینترنت فراهم می‌کند. از این‌رو، توسعه دهندگان برنامه iptables گزینه‌های لازم برای پشتیبانی از تکنیک

نقاب‌زنی IP را در این برنامه تعبیه کرده‌اند.

بررسی نحوه عملکردتکنیک نقاب‌زنی IP

چنان‌که در فصل بیست و یکم اشاره شد، دروازه شبکه، کامپیوتری است که شبکه محلی از آن طریق به شبکه دیگری مانند اینترنت متصل می‌شود. در این پیکربندی به هریک از کامپیوترهای مستقر در شبکه یک آدرس IP خصوصی و به کامپیوتری که شبکه مزبور از طریق آن به اینترنت متصل می‌شود، یک آدرس IP عمومی تخصیص داده می‌شود.

برای کامل کردن چنین اتصالی لازم است مکانیزم IP Forwarding را به صورتی که قبلاً در فصل بیست و یکم توضیح دادیم روی دروازه شبکه پیکربندی کنید. هم‌چنین با استفاده از فرمان iptables باید تنظیمات لازم در مورد دیوار آتش را نیز انجام دهید.

با وجود پیکربندی فوق چنان‌چه کاربری از شبکه به اینترنت متصل شود، تمام بسته‌های ارسالی وی به اینترنت از دروازه شبکه عبور خواهد کرد. برای مثال، فرض کنید یکی از کاربران شبکه در حال جستجوی وب سایت موردنظر خود روی اینترنت است. در این صورت، آدرس منبع (یعنی آدرس IP کامپیوتر وی روی شبکه محلی) با آدرس IP عمومی دروازه شبکه جایگزین شده و فرمان iptables شماره یک پورت غیراستاندارد را به بسته‌های ارسالی ضمیمه می‌کند. در این عملیات دروازه شبکه آدرس IP منبع و شماره پورت غیراستاندارد ضمیمه شده را ذخیره می‌کند.

به محض دریافت بسته‌های ارسالی از وب سایت موردنظر عملیات در جهت معکوس انجام می‌شود، به این معنی که شماره پورت ضمیمه شده به بسته‌های ارسالی از آن وب سایت و هم‌چنین آدرس IP کامپیوتر منبع با موارد مشابه که روی دروازه شبکه ذخیره شده‌اند، مورد مقایسه قرار گرفته و به این ترتیب کامپیوتر منبع و پورت مربوطه شناسایی می‌شود. سپس دروازه شبکه بسته‌های مزبور را به کامپیوتر منبع تحویل می‌دهد.

فرامین مربوط به نقاب‌زنی IP

بار دیگر الگوی فرمان iptables را در نظر بگیرید. چنان‌که قبلاً نیز اشاره شد، جدول پیش‌فرض که با استفاده از گزینه t- مشخص می‌شود از نوع filter است. این جدول در واقع عملکرد مکانیزم دیوار آتش را مشخص می‌کند:

```
iptables -t table option pattern -j target
```

با بهره‌گیری از جدول نوع nat (گزینه t nat-) می‌توان فرمان iptables را به منظور پیاده‌سازی تکنیک نقاب‌زنی IP مورد استفاده قرار داد. برای مثال، در این فرمان فرض بر آن است که آدرس شبکه

10.0.0.0/24 بوده و شاخص کارت شبکه‌ای که دروازه از طریق آن شبکه را به اینترنت متصل کرده، eth2 است:

```
# iptables -t nat -A POSTROUTING -s 10.0.0.0/24 -o eth2
-j MASQUERADE
```

فرمان فوق به واسطه گزینه A- POSTROUTING آدرس IP بسته‌های ارسالی به اینترنت را تغییر می‌دهد. این تغییر به واسطه گزینه j- MASQUERADE تنها شامل آدرس‌های IP خصوصی شبکه می‌شود.

تشخیص تهاجم

برای تشخیص تهاجم به سیستمی از نوع Linux دو روش وجود دارد. روش نخست کنترل ورود و خروج کاربران به سیستم است که در فایلی با عنوان /var/log/wtmp به ثبت می‌رسد و روش دیگر بررسی فعالیت‌های کاربران است که به واسطه بازبینی فایل‌های ثبت وقایع مختلف حاصل می‌شود.

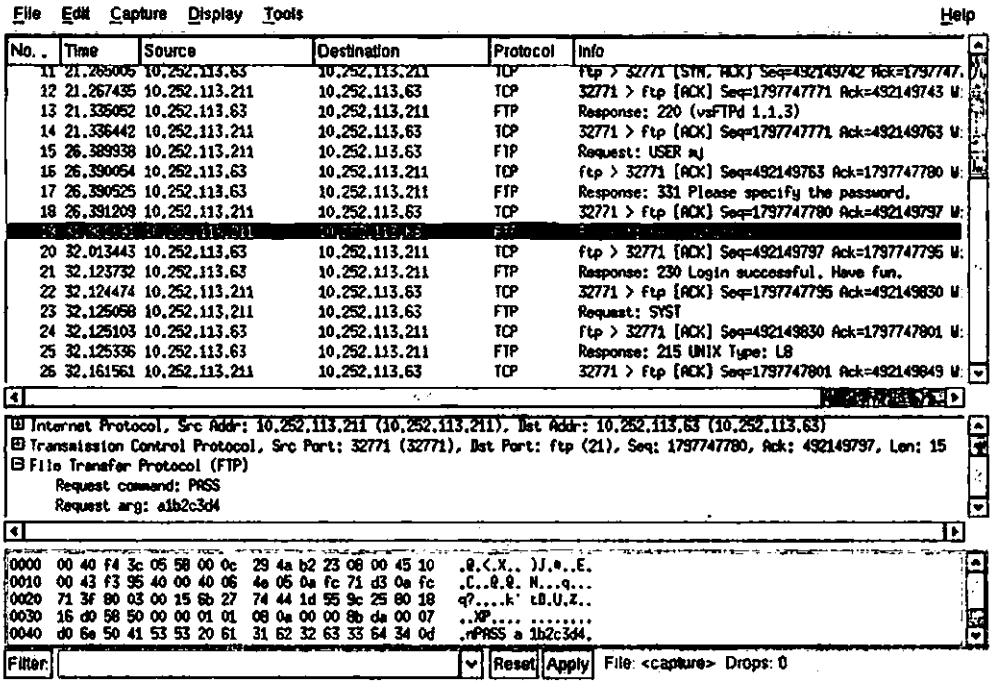
یکی از روش‌های متداولی که مهاجمان برای ورود به سیستم از آن استفاده می‌کنند دستیابی به کلمات عبور است که کاربران جهت ورود به سیستم، آن‌ها را در قالب متنی ساده (اصطلاحاً clear text) از طریق شبکه ارسال می‌کنند. برنامه Ethereal یک ابزار بسیار مفید برای بازبینی ترافیک شبکه است. این برنامه یک ابزار تحلیل کننده پروتکل است که نسخه‌های مختلف آن برای سیستم‌عامل UNIX، Linux و Windows توسعه یافته است. برای استفاده از این ابزار تحت سیستم‌عامل Red Hat Linux کافی است بسته‌های نرم‌افزاری ethereal-* را نصب کنید.

استفاده از ابزار Ethereal

در گفتگوهای روزمره ابزارهای تحلیل کننده پروتکل‌ها معمولاً با عنوان ابزارهای بوکشیدن (اصطلاحاً sniffer) شناخته می‌شوند. چنین ابزارهایی امکان ثبت دقیق ترافیک شبکه را در اختیار قرار می‌دهند. در مورد شبکه‌های Ethernet با استفاده از این گونه ابزارها می‌توان هر نوع ارتباط میان کامپیوترهای مستقر در شبکه را ثبت کرد.

چنان‌چه پیغامی در قالب متنی ساده ارسال شود، برنامه Ethereal آن‌را به قالبی قابل خواندن تبدیل می‌کند. شکل ۴-۲۲ بسته‌های ارسالی از طریق شبکه را از دیدگاه برنامه Ethereal نشان می‌دهد. در این میان بسته شماره ۱۹ را به دقت مورد توجه قرار دهید.

همان گونه که مشاهده می‌کنید، بسته شماره ۱۹ حاوی کلمه عبور a1b2c3d4 است که کاربری با شناسه mj برای اتصال به سرور FTP از آن استفاده کرده است.



شکل ۴-۲۲ آشکارسازی کلمات عبور توسط برنامه Ethereal

این موضوع اهمیت برقراری امنیت فیزیکی شبکه را بیش از پیش نشان می‌دهد. چنان‌چه مهاجمی بتواند به طور فیزیکی یک شبکه را مورد دستیابی قرار دهد، با استفاده از برنامه Ethereal می‌تواند کلمات عبوری را که در قالب متنی ساده از طریق آن شبکه ارسال شده‌اند، به سادگی تشخیص دهد.

برنامه Ethereal تنها یکی از ابزارهای بسیار کارآمدی است که مهاجمان برای دستیابی به مقاصد خود از آن‌ها استفاده می‌کنند. در صورتی که به کمک این ابزار بتوانید کلمات عبور ارسال شده در قالب متنی ساده را تشخیص دهید، مطمئن باشید که مهاجمان نیز قادر هستند به سادگی این کار را انجام دهند.

پس از نصب بسته‌های نرم‌افزاری *-ethereal با اجرای فرمان ethereal می‌توانید برنامه Ethereal را راه‌اندازی کنید.

کنترل ورود و خروج کاربران به سیستم

بررسی فایل‌های ثبت وقایع یکی از روش‌های مؤثر تشخیص فعالیت‌های مشکوک در شبکه است. ورود و خروج کلیه کاربران به سیستم در یک چنین فایلی با عنوان /var/log/wtmp به ثبت می‌رسد. از آن‌جا

که این فایل از نوع غیرمتنی یا اصطلاحاً باینری است، برای بازخوانی محتوای آن باید از برنامه ویژه‌ای استفاده کنید. برنامه utmpdump امکانات لازم برای انجام این کار را در اختیار قرار می‌دهد، به طوری که با اجرای فرمان utmpdump /var/log/wtmp می‌توانید محتوای آن‌را در قالب متنی مشاهده کنید. شکل ۵-۲۲ نمونه‌ای از خروجی این فرمان را نشان می‌دهد.

```
    ] [Fri Mar 28 10:21:34 2003 EST]
[5] [02082] [5   ] [        ] [             ] [2.4.20-8          ] [0.0.0.0
    ] [Fri Mar 28 10:21:34 2003 EST]
[5] [02083] [6   ] [        ] [             ] [2.4.20-8          ] [0.0.0.0
    ] [Fri Mar 28 10:21:34 2003 EST]
[5] [02084] [x   ] [        ] [             ] [2.4.20-8          ] [0.0.0.0
    ] [Fri Mar 28 10:21:34 2003 EST]
[6] [02078] [1   ] [LOGIN   ] [tty1         ] [                  ] [0.0.0.0
    ] [Fri Mar 28 10:21:34 2003 EST]
[6] [02079] [2   ] [LOGIN   ] [tty2         ] [                  ] [0.0.0.0
    ] [Fri Mar 28 10:21:34 2003 EST]
[6] [02080] [3   ] [LOGIN   ] [tty3         ] [                  ] [0.0.0.0
    ] [Fri Mar 28 10:21:34 2003 EST]
[6] [02081] [4   ] [LOGIN   ] [tty4         ] [                  ] [0.0.0.0
    ] [Fri Mar 28 10:21:34 2003 EST]
[6] [02082] [5   ] [LOGIN   ] [tty5         ] [                  ] [0.0.0.0
    ] [Fri Mar 28 10:21:34 2003 EST]
[6] [02083] [6   ] [LOGIN   ] [tty6         ] [                  ] [0.0.0.0
    ] [Fri Mar 28 10:21:34 2003 EST]
[7] [02138] [:0  ] [root    ] [:0           ] [                  ] [128.99.1.64
    ] [Fri Mar 28 10:21:51 2003 EST]
[7] [02246] [/0  ] [root    ] [pts/0        ] [:0.0              ] [0.0.0.0
    ] [Fri Mar 28 10:22:25 2003 EST]
```

شکل ۵-۲۲ بخشی از محتوای فایل /var/log/wtmp

مورد یکی به آخر در این شکل بسیار قابل توجه است. چنان‌که مشاهده می‌کنید، در این مورد آدرس IP کامپیوتری که کاربر از طریق آن برای ورود به سیستم اقدام کرده، 128.99.1.64 است. در صورتی که این آدرس IP عضو مجموعه آدرس‌های مجاز برای دستیابی به سیستم موردنظر نباشد باید احتمال بدهید که کسی به طور غیرمجاز قصد نفوذ به این سیستم را دارد. با مشاهده چنین آدرس‌هایی لازم است با استفاده از برنامه iptables اقدام لازم برای بلوکه کردن این گونه آدرس‌ها یا آدرس شبکه‌ای را که مهاجم از آن طریق برای نفوذ اقدام کرده است، انجام دهید.

استفاده از برنامه Tripwire در تشخیص فعالیت‌های مشکوک

در فصل سیزدهم با پیکربندی فایل‌های ثبت وقایع از طریق فایل /etc/syslog.conf آشنا شدید. بیشتر فایل‌های ثبت وقایع در فهرست /var/log مستقر هستند. هریک از وقایع به همراه زمان وقوع در این

گونه فایل‌ها به ثبت رسیده‌اند. برای تشخیص فعالیت‌های مشکوک به ویژه در مواقعی که هیچ گونه فعالیتی نباید در ارتباط با سیستم موردنظر یا شبکه صورت گرفته باشد، لازم است محتوای این فایل‌ها را به طور متناوب مورد بررسی قرار دهید.

با وجود این، یک مهاجم با تجربه می‌تواند به نحوی عمل کند که مدیر سیستم متوجه فعالیت‌های مشکوک نشده و به اشتباه چنین تصور کند که هیچ حمله‌ای به سیستم موردنظر یا شبکه صورت نگرفته است. برای مثال، پس از آن‌که مهاجم، سیستم موردنظر را به عنوان کاربر اصلی یا اصطلاحاً root مورد دستیابی قرار داد می‌تواند فایل‌های موجود در فهرست /var/log را دستکاری کرده یا آن‌ها را با فایل های جعلی جایگزین کند.

برنامه Tripwire یکی از ابزارهای بسیار مفید برای اطمینان از صحت فایل‌هاست. تا زمان انتشار کتاب حاضر هم نسخه کد باز (اصطلاحاً open source) و هم نسخه تجاری این برنامه قابل تهیه است. نسخه کد باز این برنامه در قالب یک بسته نرم‌افزاری RPM به همراه سیستم‌عامل Red Hat Linux منتشر شده است. مستندات مربوط به این برنامه را می‌توانید از طریق مراجعه به وب سایت مربوطه در آدرس اینترنتی http://www.tripwire.org دریافت کنید. نسخه تجاری برنامه Tripwire نیز در قالب نرم‌افزاری تحت عنوان TriSentry از طریق مراجعه به وب سایت شرکت Psionic Technologies به آدرس اینترنتی http://www.psionic.com قابل تهیه است.

برنامه Tripwire کلیه امکانات لازم برای اطمینان از صحت فایل‌های پیکربندی را در اختیار می‌گذارد. برای استفاده مؤثرتر از این برنامه در اولین فرصت آن‌را روی کامپیوتر موردنظر نصب کنید، چرا که برنامه مزبور قادر نیست تغییراتی را که قبل از نصب آن به فایل‌های پیکربندی اعمال شده است، تشخیص دهد.

پس از نصب برنامه Tripwire باید تنظیمات مربوطه را برای آماده‌سازی آن انجام داده و یک بانک اطلاعاتی ایجاد کنید. سپس با بهره‌گیری از فرمان cron می‌توانید تغییرات اعمال شده به فایل‌های پیکربندی را در قالب یک وظیفه زمان بندی شده به طور پیوسته مورد بررسی قرار دهید.

تنظیم برنامه Tripwire

فرآیند تنظیم برنامه Tripwire بسیار ساده است. برای این منظور کافی است فایل اجرایی /etc/tripwire/twinstall.sh را از سطر فرمان سیستم‌عامل Linux به اجرا درآورید. از آن‌جا که این فایل یک قالب متنی دارد، در صورت لزوم می‌توانید با استفاده از یک ویرایشگر متنی محتوای آن‌را به نحو مطلوب تغییر دهید. برنامه Tripwire تحت لیسانس GPL منتشر شده و شرایط استفاده از آن در قالب همین فایل آمده است.

با اجرای این فایل اعلانی برای دریافت کلمات عبور مورد استفاده جهت محافظت از دسترسی به برنامه Tripwire به نمایش درمی‌آید. ضمناً فایل پیکربندی برنامه نامبرده به همراه فایل خط‌مشی این برنامه (اصطلاحاً policy file) در فهرست /etc/tripwire ذخیره می‌شوند.

برای ایجاد بانک اطلاعاتی اولیه موردنیاز برای برنامه Tripwire کافی است فرمان tripwire --init را اجرا کنید. با توجه به فایل خط‌مشی برنامه Tripwire با عنوان tw.pol، اجرای این فرمان ممکن است چند دقیقه به طول بینجامد. هم‌چنین به دلیل عدم وجود برخی از فایل‌های مورد جستجوی این فرمان ممکن است چند پیغام خطا نیز به نمایش درآید.

با ویرایش فایل /etc/tripwire/twpol.txt می‌توان فایل خط‌مشی برنامه Tripwire را به روز رساند. برای مثال، در صورت عدم نصب برنامه Z Shell می‌توان بدون هیچ پیامد نامطلوبی مرجع برنامه /bin/zsh را حذف کرد. پس از ویرایش فایل مزبور برای به روز رسانی فایل خط‌مشی برنامه Tripwire کافی است این فرمان را اجرا کنید:

```
# tripwire --update-policy /etc/tripwire/twpol.txt
```

برنامه Tripwire ابزار دفاعی مهمی برای کامپیوتر میزبان محسوب می‌شود. با وجود این، مهاجمان باتجربه سعی می‌کنند برخی از فایل‌های این برنامه را به منظور جلوگیری از ردیابی آن‌ها تغییر دهند. برای پیشگیری از این وضعیت می‌توانید فایل‌های برنامه Tripwire را روی رسانه‌ای مانند CD-ROM که تنها قابلیت خواندن دارد، مستقر کنید.

عملکرد برنامه Tripwire

چنان‌چه بسته نرم‌افزاری Tripwire را که به همراه سیستم‌عامل Red Hat Linux منتشر شده است نصب کنید، بانک اطلاعاتی این برنامه به طور روزانه مورد بررسی قرار می‌گیرد. این کار به واسطه فایل اجرایی tripwire-check که در فهرست /etc/cron.daily مستقر است، انجام می‌شود. همان گونه که در فصل سیزدهم نیز اشاره شد، با توجه به فایل پیکربندی /etc/crontab کلیه فایل‌های اجرایی موجود در فهرست /etc/cron.daily رأس ساعت ۴:۰۲ هر روز صبح به اجرا درمی‌آیند.

در صورت تمایل می‌توانید با ویرایش فایل اجرایی tripwire-chesk خروجی حاصل از اجرای آن‌را در موقعیت موردنظر ذخیره کنید. برای مثال، با این تغییر، خروجی مزبور در فایل /var/log/tripwire ثبت خواهد شد:

```
/usr/sbin/tripwire --check >> /var/log/tripwire
```

روی یک کامپیوتر نمونه، فایل /sbin/poweroff موقتاً حذف شده و سپس فایل tripwire-check به اجرا درآمده است. خروجی حاصل از این اقدام که در فایل /var/log/tripwire به ثبت رسیده چنین است:

```
---------------------------
Rule Name: Critical Utility Sym-Link (/sbin/poweroff)
Security Level:100
---------------------------

Removed:
"/sbin/poweroff"
```

خروجی فوق حاکی از آن است که فایل /sbin/poweroff از سیستم میزبان حذف شده و بنابراین امکان اجرای فرمان poweroff وجود ندارد.

رفع اشکالات مربوط به دسترسی

در برخی موارد مدیران سیستم‌ها چنان در تأمین امنیت آن‌ها زیاده‌روی می‌کنند که کاربران از دسترسی به سرویس‌های موردنیاز محروم می‌شوند.

چنان‌چه به واسطه زیاده‌روی در تأمین امنیت سیستم امکان دسترسی کاربران به سرویس خاصی وجود نداشته باشد، باید سرویس مشابهی را جایگزین آن کرده یا به نحوی با شرایط موجود که نتیجه ملاحظات بیش از اندازه برای تأمین امنیت سیستم است، کنار بیایید.

تحت چنین شرایطی ممکن است شکایاتی درباره عملکرد نامطلوب سیستم به گوش برسد. برای مثال، خروجی حاصل از به کارگیری گزینه DROP در فرمان iptables ممکن است برای کاربران نامفهوم یا گیج کننده باشد.

زیاده‌روی در تأمین امنیت سیستم‌ها

زیاده‌روی در تأمین امنیت سیستم‌ها کاربران را از انجام برخی امور محروم خواهد کرد. با وجود این، برخی از سرویس‌ها چنان خطرناک هستند که باید جایگزین دیگری را در اختیار کاربران قرار دهید.

برای مثال، یکی از روش‌های متداول برای دستیابی به یک سیستم راه دور استفاده از سرویس Telnet است. با وجود این، بهتر است کاربران را در استفاده از سرویس Secure Shell یا SSH به عنوان جایگزین Telnet تشویق کنید. سرویس SSH برخلاف Telnet کلمات عبور کاربران را در قالب متنی

ساده از طریق شبکه ارسال نکرده بلکه پیش از ارسال آن‌ها را رمزگذاری می‌کند. (برای اطلاع بیشتر درباره سرویس SSH به فصل بیست و سوم مراجعه کنید.)

سرویس قابل ذکر دیگر Network File System یا به اختصار NFS است که در فصل بیست و هشتم به بررسی آن می‌پردازیم. به طوری که خواهید دید، استفاده از این سرویس مستلزم دسترسی به سرویس‌های nfs، portmap، rpc.mountd و rpc.nfsd است. با وجودی که سرویس NFS از طریق پورت شماره ۲۰۴۹ قابل دستیابی است، مکانیزم‌های بازدارنده دیوار آتش در سیستم‌عامل Red Hat Linux دسترسی به پورت شماره ۱۱۱ را که سرویس RPC از طریق آن قابل دستیابی است، محدود می‌کنند.

جلوگیری از دسترسی کاربران به سرویس‌ها

نتیجه دسترسی به سرویس‌هایی که توسط مکانیزم دیوار آتش محافظت شده‌اند، بستگی به ساختار فرمان iptables به ویژه استفاده از گزینه DROP یا REJECT دارد. برای مثال، با اجرای هریک از این فرامین می‌توان ترتیبی داد تا دسترسی کاربران مستقر در شبکه 192.168.0.0/24 به سرویس Telnet محدود شود:

```
# iptables -A INPUT -s 192.168.0.0/24 -p tcp -dport 23 -j DROP
# iptables -A INPUT -s 192.168.0.0/24 -p tcp -dport 23 -j REJECT
```

پورت شماره ۲۳ برای سرویس TCP رزرو شده است. برای اطلاع از شماره پورت‌های تخصیص داده شده به سرویس‌های استاندارد محتوای فایل /etc/services را ببینید.

فرض کنید به واسطه استفاده از گزینه DROP در فرمان iptables دسترسی کاربران شبکه به سرویس Telnet محدود شده باشد. تحت این شرایط، چنان‌چه کاربری از شبکه مزبور سرویس Telnet را جهت دسترسی به سرور RHL9 مورد دستیابی قرار دهد، با این پیغام مواجه خواهد شد:

```
# telnet RHL9
Trying 192.168.0.34
```

با مشاهده پیغام فوق کاربر ممکن است در مورد کارکرد نامطلوب سرویس Telnet اعتراض کند. اکنون فرض کنید این محدودیت به واسطه استفاده از گزینه REJECT ایجاد شده باشد. تحت این شرایط، چنان‌چه کاربری از شبکه مزبور سرویس Telnet را جهت دسترسی به سرور RHL9 مورد دستیابی قرار دهد، با این پیغام مواجه خواهد شد:

```
# telnet RHL9
```

```
Trying 192.168.0.34
telnet: connect to address 192.168.0.34: Connection refused
```

با مشاهده پیغام فوق کاربر متوجه می‌شود که امکان دسترسی به سرور RHL9 از طریق سرویس Telnet وجود ندارد. در صورتی که کاربر علت را جویا شود، می‌توانید آموزش‌های لازم درباره استفاده از یک سرویس جایگزین مانند SSH که امنیت بیشتری را نیز تضمین می‌کند، در اختیار وی قرار دهید.

جمع‌بندی

چنان‌چه مدیریت شبکه‌ای را به عهده دارید که با هیچ شبکه دیگری به ویژه اینترنت در ارتباط نیست، از نظر تأمین امنیت شبکه بسیار خوش شانس هستید. در چنین شرایطی کافی است سرورها و تجهیزات شبکه را در اتاق محافظت شده‌ای نگهداری کنید و اگر به کاربران شبکه نیز اعتماد دارید نیازی نیست که برای تأمین امنیت آن اقدام خاصی انجام دهید.

با وجود این، امروزه بیشتر شبکه‌ها به یکدیگر متصل هستند و دسترسی به اینترنت برای بسیاری از کاربران یک ضرورت شمار می‌رود. متأسفانه دسترسی کاربران به اینترنت مجال خوبی برای مهاجمانی که قصد نفوذ به شبکه‌ها را دارند، فراهم کرده است.

برای تأمین امنیت شبکه‌ها روش‌های بسیار مؤثری وجود دارد که از آن جمله می‌توان به موارد مهمی چون محافظت فیزیکی چند لایه از سرورها و تجهیزات شبکه، پیکربندی چند لایه مکانیزم دیوار آتش برای محافظت از وب سرور و شبکه، استفاده از مکانیزم‌های رمزگذاری پیچیده هم‌چون Kerberos و GPG، رمزگذاری کلمات عبور با بهره‌گیری از مکانیزم‌هایی مانند MD5، Shadow Password Suite و بالاخره استفاده از کلمه عبور برای محافظت از برنامه BIOS و bootloader اشاره کرد.

به کمک مکانیزم Pluggable Authentication Modules یا به اختصار PAM می‌توان امکان دسترسی به برنامه‌های کاربردی را محدود کرد. فایل‌های پیکربندی این مکانیزم که در فهرست /etc/pam.d مستقر شده‌اند، خط مشی دسترسی به برنامه‌های کاربردی را مشخص می‌کنند. عملکرد مکانیزم PAM براساس چهار نوع ماجول password، session، account و auth استوار است. عملکرد هر یک از این ماجول‌ها را به نوبه خود می‌توان با استفاده از چهار نشانه کنترلی optional، required، requisite و sufficient تغییر داد.

برنامه iptables ابزار اصلی مورد استفاده برای پیکربندی مکانیزم بازدارنده دیوار آتش در سیستم‌عامل Red Hat Linux است. چندین فرامین iptables را می‌توان به صورت یک زنجیره به یکدیگر متصل کرده و ترافیک ناشی از جریان داده‌ها را در سه جهت INPUT، OUTPUT و FORWARD، یعنی ورود به شبکه، خروج از شبکه و گذر از شبکه کنترل کرد. این فرمان iptables امکان مشخص کردن

الگوهایی را براساس آدرس‌های IP و شماره پورت‌ها در اختیار قرار می‌دهد. خط‌مشی مکانیزم بازدارنده دیوار آتش را در ازای تشخیص بسته‌هایی مطابق با الگوی موردنظر می‌توان با استفاده از گزینه‌های ACCEPT، DROP، REJECT یا LOG تعیین کرد. به کمک فرمان iptables حتی می‌توان از وقوع حملات ping مرگبار نیز پیشگیری به عمل آورد.

علاوه بر این موارد، فرمان iptables امکان پیاده‌سازی تکنیکی با عنوان IP Masquerading یا نقاب‌زنی IP را نیز در اختیار قرار می‌دهد. به کمک این تکنیک که با عنوان Network Address Translation یا NAT نیز شناخته شده است، می‌توان آدرس IP کامپیوترهای مستقر در یک شبکه را از دید شبکه‌های خارجی مانند اینترنت پنهان کرد. به هریک از درخواست‌های ارسالی از این کامپیوترها به شبکه خارجی یک شماره پورت بلااستفاده تخصیص داده می‌شود. هنگام دریافت پاسخ از شبکه خارجی، با توجه به این شماره پورت، کامپیوتر موردنظر شناسایی شده و بسته ارسالی از شبکه خارجی در اختیار آن کامپیوتر قرار می‌گیرد.

برای تشخیص تهاجم به سیستمی از نوع Linux روش‌های مختلفی وجود دارد. یکی از این روش‌ها توجه به محتوای فایل /var/log/wtmp است. روش دیگر استفاده از برنامه Tripwire است. بازرسی ترافیک شبکه با استفاده از برنامه Ethereal نیز روشی مؤثر برای پیشگیری از تهاجم محسوب می‌شود. با بهره‌گیری از این برنامه می‌توان به اقدام خطرناک برخی از کاربران جهت ارسال کلمات عبور خود در قالب متنی ساده پی برد.

برخی از مدیران سیستم‌ها در تأمین امنیت آن‌ها زیاده‌روی می‌کنند، به طوری که دسترسی کاربران به سرویس‌های موردنیاز محدود می‌شود. از طرف دیگر نحوه پیکربندی فرمان iptables نیز می‌تواند موجب گمراهی کاربران شود.

در فصل بعد با روش‌های دیگری برای دسترسی به کامپیوترهای شبکه آشنا می‌شوید. چنان‌که خواهید دید، برخی از این روش‌ها مانند Remote Shell و Telnet از ایمنی پایینی برخوردار هستند. این درحالی است که سرویس Secure Shell کاملاً قابل اعتماد است، چرا که هر گونه ارتباطی در یک قالب رمزگذاری شده انجام می‌شود. هم‌چنین مطالب مفیدی را نیز درباره مکانیزم TCP Wrapper فرامی‌گیرید. این مکانیزم نوعی مکانیزم کنترل دسترسی است که امکان محافظت از سرویس‌هایی با ضریب امنیتی پایین را در اختیار می‌گذارد.

بخش ششم

سرویس‌های شبکه در سیستم‌عامل Linux

اهداف:

- بررسی نحوه استفاده از سرویس xinetd و سرویس دسترسی از راه دور
- بررسی سرویس‌های DNS و DHCP
- بررسی مدیریت چاپ و دو برنامه CUPS و LPD
- بررسی سرویس‌های انتقال پیغام‌های الکترونیکی

فصل بیست‌وسوم

سرویس دسترسی از راه دور و شبح xinetd

شبکه‌های کامپیوتری کلیه امکانات لازم را به منظور بازخوانی فایل‌ها و اجرای برنامه‌ها در اختیار کاربران قرار می‌دهند. با وجود این، گاهی اوقات لازم است این گونه عملیات از راه دور، یعنی بدون دسترسی فیزیکی به کامپیوتر موردنظر انجام شود. در سیستم‌عامل Linux سرویس‌هایی به منظور دسترسی از راه دور پیش‌بینی شده است.

برای دسترسی از راه دور به سیستمی از نوع Linux روش‌های مختلفی وجود دارد. دسته‌ای از سرویس‌ها که توسط برنامه‌ای با عنوان xinetd یا Extended Internet Services Daemon کنترل می‌شوند، امکان فوق را در اختیار قرار می‌دهند. برنامه مذکور که در واقع یک شبح است، همواره در حال شنود پورت مربوط به سرویس‌هایی مانند FTP و Telnet است. چنان‌چه سرویس مربوطه روی کامپیوتر میزبان نصب شده باشد، برنامه xinetd در صورت لزوم آن‌ها را راه‌اندازی خواهد کرد.

شبح xinetd عملیات تعدادی از سرویس‌ها شامل Remote Shell یا RSH، Telnet، FTP و POP3 را کنترل می‌کند. پس از نصب این سرویس‌ها، فایل‌های پیکربندی مربوطه در فهرست /etc/xinetd.d مستقر می‌شوند. فعال‌سازی سرویس‌های نامبرده از طریق این فایل‌های پیکربندی امکان پذیر است. در برخی موارد حتی می‌توان مکانیزم بازدارنده دیوار آتش را به طور خاص برای یک سرویس به خصوص پیکربندی کرد.

مکانیزم TCP Wrapper امکان پیکربندی مکانیزم بازدارنده دیوار آتش را برای سرویس‌های شبح xinetd در اختیار می‌گذارد. جهت کنترل دسترسی به تمام یا برخی از سرویس‌های شبح xinetd کافی است فایل‌های پیکربندی /etc/hosts.all و /etc/hosts.deny را ویرایش کنید. این کار را می‌توانید با استفاده از فرمان iptables نیز انجام دهید. (برای اطلاع بیشتر درباره چگونگی انجام این کار به فصل بیست و دوم مراجعه کنید.)

برخی از سرویس‌های شبح xinetd بسته‌ها را در قالب متنی ساده ارسال می‌کنند. چنان‌که در فصل بیست و دوم مشاهده کردید، این رفتار می‌تواند کلمات عبور کاربران را در معرض دید مهاجمان قرار دهد. یکی از روش‌های بسیار مطمئن برای دسترسی از راه دور به سیستمی از نوع Linux استفاده از

سرویس Secure Shell یا به اختصار SSH است. برای این منظور، کافی است مکانیزم SSH را با استفاده از کلیدهای خصوصی و عمومی جهت رمزگذاری بسته‌های ارسالی از طریق شبکه پیکربندی کنید.

صرف نظر از ملاحظات امنیتی فوق، عیب‌یابی سرویس‌ها همواره کار ساده‌ای نیست. چنان چه کاربران در دسترسی به یک سرویس به خصوص ناموفق باشند، لازم است تمام مکانیزم‌های بازدارنده دیوار آتش را به طور دقیق مورد بررسی قرار دهید. البته موارد دیگری چون عدم فعال بودن سرویس موردنظر و پیکربندی نادرست فرمان iptables یا عملکرد نامطلوب مکانیزم TCP Wrapper در محدود کردن دسترسی کاربران به آن سرویس نیز می‌تواند منجر به عدم موفقیت کاربران در دسترسی به سرویس مزبور باشد. در فصل حاضر این موضوعات را مورد بررسی قرار خواهیم داد:

- استفاده از سرویس‌های توسعه یافته
- کنترل دسترسی به سرویس‌ها با بهره‌گیری از مکانیزم TCP Wrapper
- بهره‌برداری از سرویس Secure Shell
- رفع موانع دسترسی کاربران به سرویس‌های موردنیاز

استفاده از سرویس‌های توسعه یافته

سرویس‌های توسعه یافته در سیستم‌عامل Linux سرویس‌هایی هستند که توسط شبح xinetd کنترل می‌شوند. سرویس‌های RSH، Telnet، FTP و POP3 نمونه‌هایی از این گونه سرویس‌ها هستند. برای مشاهده اسامی سرویس‌های توسعه یافته‌ای که هم‌اینک روی کامپیوتر میزبان نصب شده‌اند، کافی است به فهرست /etc/xinetd.d مراجعه کنید.

شبح xinetd شامل دو سطح از فایل‌های پیکربندی است. سطح نخست شامل یک فایل پیکربندی با عنوان /etc/xinetd.conf است که در آن از عناوین فایل‌های پیکربندی سطح دوم استفاده شده است. سطح دوم شامل فایل‌های پیکربندی مربوط به هر یک از سرویس‌های شبح xinetd است. این فایل‌ها در فهرست /etc/xinetd.d مستقر شده‌اند.

برخی از سرویس‌های شبح xinetd فاقد مکانیزم رمزگذاری هستند. با وجود این، درچنین سرویس‌هایی از مکانیزم‌های خاص آن سرویس‌ها برای تأمین امنیت آن‌ها استفاده می‌شود. در صورت بهره‌گیری از این مکانیزم‌ها برای محدود کردن دسترسی کاربران به سرویس‌های مربوطه میزان نفوذپذیری آن‌ها کاهش خواهد یافت. چنان‌چه مدیریت سیستمی از نوع Linux را به عهده دارید باید در مورد استفاده از این مکانیزم‌ها برای تأمین امنیت سیستم به دقت تصمیم‌گیری کنید.

ساختار فایل پیکربندی /etc/xinetd.conf

فایل پیکربندی اصلی برنامه Extended Internet Services Daemon یا همان شبح xinetd فایلی با عنوان /etc/xinetd.conf است. تنظیمات موجود در این فایل شامل تمام سرویس‌هایی است که مدیریت آن‌ها توسط برنامه xinetd انجام می‌شود. شکل ۱-۲۳ تنظیمات پیش‌فرض این فایل پیکربندی را در سیستم‌عامل Red Hat Linux نشان می‌دهد.

```
#
# Simple configuration file for xinetd
#
# Some defaults, and include /etc/xinetd.d/

defaults
{
        instances               = 60
        log_type                = SYSLOG authpriv
        log_on_success          = HOST PID
        log_on_failure          = HOST
        cps                     = 25 30
}

includedir /etc/xinetd.d

~
~
~
~
~
~
~
"/etc/xinetd.conf" 18L, 289C
```

شکل ۱-۲۳ محتوای فایل پیکربندی /etc/xinitd.conf

جدول ۱-۲۳ پارامترهای مورد استفاده در این فایل پیکربندی را شرح می‌دهد. چنان‌که مشاهده می‌کنید، در این فایل با بهره‌گیری از پارامتر instances تعداد سرویس‌های فعال شبح xinetd به ۶۰ عدد محدود شده است. هم‌چنین برخی از پارامترهای مربوط به ثبت وقایع (شامل log_type، log_on_success و log_on_failure) مقداردهی شده است. علاوه بر این، به واسطه پارامتر cps تعداد اتصالات به ۲۵ اتصال در هر ثانیه محدود شده است و بالاخره با استفاده از پارامتر includedir محتوای کلیه فایل‌های پیکربندی موجود در فهرست /etc/xinetd.d در فایل پیکربندی /etc/xinetd.conf گنجانده شده است.

جدول ۱-۲۳ شرح پارامترهای فایل پیکربندی /etc/xinetd.conf

عنوان پارامتر	توضیح
instances	با استفاده از این پارامتر می‌توان تعداد سرورهای فعال از هر نوع را محدود کرد.
log_type	با استفاده از این پارامتر می‌توان نحوه ثبت وقایع را مشخص کرد. مقدار SYSLOG authpriv بیانگر این است که وقایع مربوط به سرویس‌های شبح xinetd در فایل /var/log/secure به ثبت می‌رسد.
log_on_success	با استفاده از این پارامتر می‌توان اطلاعاتی را که باید در ازای راه‌اندازی و متوقف کردن موفقیت آمیز هر سرویس به ثبت برسد، مشخص کرد. مقادیر متغیرهای PID، HOST و USERID مفیدترین اطلاعات در این زمینه محسوب می‌شوند.
log_on_failure	با استفاده از این پارامتر می‌توان اطلاعاتی را که باید در ازای عدم موفقیت در راه‌اندازی هر سرویس به ثبت برسد مشخص کرد. مقادیر متغیرهای HOST و USERID مفیدترین اطلاعات در این زمینه محسوب می‌شوند.
cps	با استفاده از این پارامتر می‌توان تعداد درخواست‌های ارسال شده در ثانیه به هر سرور را محدود کرد. برای مثال، با توجه به شکل ۱-۲۳، چنان‌چه تعداد درخواست‌های ارسال شده در ثانیه به هر سرور از ۲۵ درخواست متجاوز شود، سرور مزبور برای مدت ۳۰ ثانیه از سرویس‌دهی بازایستاده و به این ترتیب روند تلاش مهاجمان برای اختلال در آن سرویس کند می‌شود.
includedir	با استفاده از این پارامتر می‌توان محتوای فایل‌های موجود در یک فهرست به خصوص را در فایل پیکربندی /etc/xinetd.conf درج کید.
only_from	بااستفاده از این پارامتر می‌توان آدرس IP کامپیوترهای‌مجاز برای دسترسی به سرویس‌های شبح xinetd را مشخص کرد.
no_access	با استفاده از این پارامتر می‌توان آدرس IP کامپیوترهایی را مشخص کرد که امکان دسترسی به سرویس‌های شبح xinetd از طریق آن‌ها وجود ندارد.
access_times	با استفاده از این پارامتر می‌توان مدت زمانی را مشخص کرد که دسترسی به سرویس‌های شبح xinetd امکان‌پذیر است. برای مثال، چنان‌چه این پارامتر به صورت access_times = 08:00-23:00 مقداردهی شود، صرف‌نظر از سایر شرایط، دسترسی به سرویس‌های شبح xinetd از ساعت ۸ صبح تا ۱۱ شب بلامانع خواهد بود.

در صورت لزوم می‌توان هریک ازاین پارامترها را در فایل‌های‌پیکربندی موجود درفهرست /etc/xinetd.d نیز مقداردهی کرد. هم‌چنین برای مشخص کردن آدرس‌های IP می‌توان از روش معمول یا CIDR استفاده کرد.

فعال‌سازی سرویس‌های شبح xinetd

برای فعال کردن هریک از سرویس‌های شبح xinetd می‌توان فایل پیکربندی سرویس موردنظر را مستقیماً ویرایش کرد. روش دیگر فعال کردن سرویس‌های شبح xinetd با استفاده از فرمان chkconfig است. برای مثال، چنان‌چه بسته نرم‌افزاری *-telnet-server روی کامپیوتر میزبان نصب شده باشد، فایل پیکربندی مربوطه در فهرست /etc/xinetd.d موجود خواهد بود. این فایل را در یک ویرایشگر متنی باز کنید. متغیر disable در این فایل پیکربندی به این صورت مقداردهی شده است:

```
disable = yes
```

به بیان دیگر، سرویس Telnet به طور پیش‌فرض غیرفعال است. برای فعال کردن سرویس مزبور کافی است مقدار پارامتر disable را به این صورت تغییر دهید: `disable = no`

علاوه بر ویرایش مستقیم فایل پیکربندی سرویس مورد نظر، برای فعال کردن آن سرویس می‌توانید فرمان chkconfig را به این صورت مورد استفاده قرار دهید:

```
# chkconfig service_name on
```

متغیر *service_name* در فرمان فوق بیانگر عنوان سرویس موردنظر است. به ترتیب مشابه می‌توان هریک از سرویس‌های xinetd را غیرفعال کرد: `# chkconfig service_name off`

پس از انجام تغییرات باید ترتیبی دهید تا شبح xinetd فایل پیکربندی آن سرویس را مجدداً مورد بازخوانی قرار دهد. به عبارت دیگر باید فایل پیکربندی شبح xinetd را مجدداً بارگذاری کنید. برای این منظور کافی است فرمان service را به این صورت اجرا کنید:

```
# service xinetd reload
```

علاوه بر روش فوق، برای بارگذاری مجدد فایل پیکربندی شبح xinetd می‌توانید سیستم‌عامل Linux را مجدداً راه‌اندازی کنید. با وجود این، توجه کنید که راه‌اندازی مجدد سیستم‌عامل Linux به ندرت موردنیاز است.

با اجرای فرمان service تمام برنامه‌های اسکریپت موجود در فهرست /etc/rc.d/init.d نیز به اجرا درمی‌آید. به این ترتیب، اجرای فرمان service xinetd reload عملاً معادل اجرای فرمان /etc/rc.d/init.d/xinetd reload است.

سرویس Remote Shell

چنان‌چه روی کامپیوترهای مختلفی از یک شبکه، حساب کاربری معتبری داشته باشید، با استفاده از سرویس Remote Shell یا به اختصار RSH به آسانی می‌توانید کامپیوتر دلخواه خود را مورد دستیابی قرار دهید. برای‌استفاده از این سرویس ابتدا باید بسته نرم‌افزاری *-rsh را روی کامپیوتر یا کامپیوترهای کلاینت و بسته نرم‌افزاری *-rsh-server را روی کامپیوتر سرور نصب و پیکربندی کرده، سپس سرویس RSH را فعال کنید.

برای بهره‌برداری از سرویس RSH چهار فرمان rsh، rlogin، rexec و rcp که به فرامین r شهرت دارند، پیش‌بینی شده است. با نصب برنامه سرور RSH (بسته نرم‌افزاری *-rsh-server) سه فایل پیکربندی مربوط به سه فرمان نخست یعنی rsh، rlogin و rexec در فهرست /etc/xinetd.d مستقر می‌شوند. پیش از به کارگیری این فرامین لازم است با استفاده از روش‌هایی که در قسمت قبل مورد بررسی قرار گرفت، آن‌ها را فعال کنید. هم‌چنین فراموش نکنید که باید فایل پیکربندی شبح xinetd را مجدداً بارگذاری کنید. برای مثال، به عملیاتی که کاربری با شناسه mj جهت دستیابی به کامپیوتر RHL9 از راه دور انجام داده است، توجه کنید:

```
[mj] $ rlogin RHL9
Password:
Last login: Tue Mar 17 10:27:43 from tty2
```

چنان‌که مشاهده می‌کنید، کاربر مذکور ملزم به وارد کردن کلمه عبور است. با وجود این، انجام این کار ضروری نیست. در صورتی که کاربر مورد بحث فایلی با عنوان rhosts. را در فهرست خانگی خود روی هریک از کامپیوترهایی که قصد دستیابی به آن‌ها را دارد، ایجاد کرده و اسامی کامپیوترهای کلاینت و سرور را در آن فایل‌ها ذکر کند، نیازی نیست که کلمه عبور خود را مرتباً در عملیات دسترسی از راه دور به کامپیوتر موردنظر وارد کند. علاوه بر این، چنان‌چه مدیر سیستم همین اطلاعات را در فایل /etc/hosts.equiv وارد کند، هر کاربری که روی یک کامپیوتر راه دور دارای یک حساب کاربری معتبر باشد، نیازی نیست که برای دستیابی به آن، کلمه عبور خود را وارد کند.

دستیابی به یک کامپیوتر راه دور با استفاده از شناسه‌های کاربری مختلف نیز به سادگی امکان‌پذیر است. به عنوان مثال، کاربری با شناسه mj برای دستیابی به کامپیوتر راه دور RHL9 با استفاده از شناسه کاربری lula می‌تواند این فرمان را اجرا کند:

```
[mj] $ rlogin -l lula RHL9
Password:
Last login: Tue Mar 17 10:29:26 from tty2
```

به این ترتیب، یک مهاجم با اطلاع از حساب کاربران موجود روی یک سرور Linux و تغییر محتوای فایل rhosts. یا /etc/hosts.equiv می‌تواند کامپیوتر دلخواه خود را از راه دور مورد دستیابی قرار دهد. از این‌رو، برای پیشگیری از چنین وضعیتی بهتر است ترتیبی دهید تا امکان تغییر محتوای این فایل‌ها وجود نداشته باشد. برای این منظور می‌توانید فرمان chattr +i *filename* را که در آن متغیر *filename* نام فایل موردنظر است، اجرا کنید. در مورد فایل‌های rhosts. و /etc/hosts.equiv کافی است این فرامین را اجرا کنید:

```
# chattr +i .rhosts
# chattr +i /etc/hosts.equiv
```

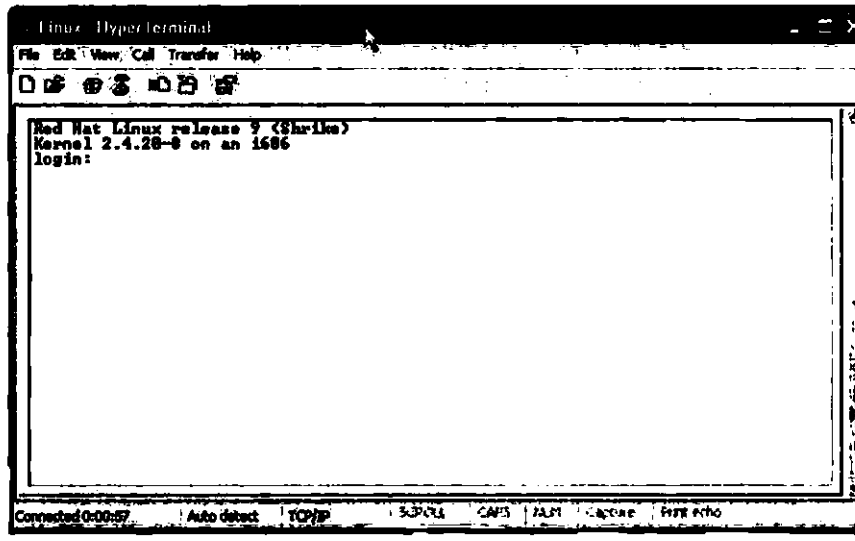
علیرغم اقدام فوق، مهاجم با اطلاع از حساب کاربری مدیر سیستم (کاربر اصلی یا اصطلاحاً root) می‌تواند تنظیمات فوق را با اجرای فرمان chattr-i *filename* بی‌اثر کند.

سرویس Telnet

سرویس Telnet یکی از روش‌های بسیار ساده برای دستیابی به یک کامپیوتر راه دور است. استفاده از این سرویس کاملاً آسان است به طوری که اغلب کاربران با آن آشنایی دارند. سرویس Telnet امکان پیکربندی سریع مجموعه‌ای از ترمینال‌های Linux را در اختیار می‌گذارد. علاوه بر این، پیکربندی سایر سرویس‌های شبح xinetd نیز از طریق سرویس Telnet امکان‌پذیر است. با وجود این، سرویس مزبور هر گونه اطلاعاتی از جمله کلمات عبور را در قالب متنی ساده ارسال می‌کند. از این‌رو، استفاده از این سرویس باید به شبکه‌هایی که از ایمنی بالایی برخوردار هستند، محدود شود.

بسته‌های نرم‌افزاری telnet-* و telnet-server-* که برنامه‌های کلاینت و سرور موردنیاز برای استفاده از سرویس Telnet هستند به همراه سیستم‌عامل Red Hat Linux توزیع می‌شوند.

پس از برقراری ارتباط میان برنامه‌های کلاینت و سرور، برای استفاده از سرویس Telnet می‌توان از طریق سطر فرمان سیستم‌عامل Linux اقدام کرد. یکی از مزایای سرویس Telnet این است که نسخه‌های مختلفی از آن برای انواع سیستم‌عامل‌های موجود توسعه یافته است. شکل ۲-۲۳ استفاده از برنامه کلاینت سرویس Telnet تحت سیستم‌عامل Windows XP را برای اتصال به برنامه سرور مربوطه که روی کامپیوتری از نوع Linux مستقر است، نشان می‌دهد.



شکل ۲-۲۳ استفاده از برنامه کلاینت سرویس Telnet تحت سیستم‌عامل Windows XP برای اتصال به برنامه سرور مربوطه که روی کامپیوتری از نوع Linux مستقر است.

برقراری ارتباط میان برنامه‌های کلاینت و سرور سرویس Telnet ممکن است به واسطه پیغام‌های ارسالی از برنامه سرور با مشکل مواجه شود. با تغییر مقدار متغیر TERM به این صورت اغلب مشکلات ناشی از برقراری ارتباط رفع می‌شود:

```
TERM=vt100
```

مشابه سایر سرویس‌های شبح xinetd فعال کردن سرویس Telnet نیز با ویرایش فایل پیکربندی /etc/xinetd.d/telnet و بارگذاری مجدد فایل پیکربندی برنامه xinetd امکان‌پذیر است. پس از این اقدام می‌توان سرویس Telnet را با اجرای فرمان telnet *hostname* از طریق سایر کامپیوترها مورد دستیابی قرار داد.

سرویس FTP

پروتکل FTP یکی از قدیمی‌ترین پروتکل‌های TCP/IP است. این پروتکل به طور خاص جهت انتقال فایل‌ها طراحی شده است. از این‌رو کارایی آن حتی نسبت به پروتکل‌های جدیدی مانند HTTP که امکان انتقال فایل‌ها را نیز در اختیار قرار می‌دهند، بهتر است. بارگذاری فایل‌های سیستم‌عامل Red Hat Linux از وب سایت شرکت Red Hat به منظور ایجاد CDهای نصب این سیستم‌عامل با استفاده از همین پروتکل انجام می‌شود.

در فصل بیست و هفتم برنامه‌های کلاینت و سرور مربوط به سرویس FTP را مورد بررسی قرار خواهیم داد و در این قسمت تنها به بررسی نحوه فعال کردن سرویس FTP می‌پردازیم. یکی از برنامه‌های سرور FTP برنامه‌ای با عنوان WU-FTP است که که در دانشگاه واشنگتن توسعه یافته است. البته بسته نرم‌افزاری RPM موردنیاز برای نصب این برنامه به همراه نسخه‌های اخیر سیستم‌عامل Red Hat Linux منتشر نشده است. با وجود این، در صورت تمایل می‌توانید از طریق آدرس ftp.wu-ftpd.org یا کتابخانه SpeakEasy RPM به آدرس http://www.rpmfind.net آن‌را مورد دستیابی قرار دهید. پس از نصب بسته نرم‌افزاری wu-ftpd-* فایل پیکربندی مربوطه در فهرست /etc/xinetd.d مستقر می‌شود. مشابه سایر سرویس‌های شبح xinetd برای فعال کردن سرویس FTP لازم است متغیر disable از این فایل پیکربندی را به صورت disable = yes مقداردهی کنید.

سایر سرویس‌های شبح xinetd

علاوه بر سرویس‌هایی که در قسمت قبل مورد بررسی قرار گرفت، شبح xinetd کنترل سرویس‌های دیگری را نیز به عهده دارد. تنوع این سرویس‌ها بسیار قابل توجه است. برای مثال، به کمک سرویس finger می‌توان اطلاعات بیشتری را درباره کاربر موردنظر به دست آورد. هم‌چنین با استفاده از دو سرویس pop3s و imaps کاربران می‌توانند پیغام‌های الکترونیکی خود را از راه دور و با ضریب امنیتی بالا مورد دستیابی قرار دهند. شرح برخی از این سرویس‌ها در جدول ۲-۲۳ آمده است.

جدول ۲-۲۳ شرح برخی از سرویس‌های شبح xinetd

عنوان سرویس	توضیح
amanda	این سرویس که عنوان آن کوتاه شده عبارت Advanced Maryland Automatic Network Disk Archiver است امکان تهیه نسخه پشتیبان از کامپیوترهای مستقر در شبکه را روی یک رسانه واحد با ظرفیت ذخیره‌سازی بالا (هم‌چون نوارگردان) فراهم می‌کند.
finger	این سرویس امکان مشاهده اطلاعات مربوط به کاربران را که در فایل /etc/passwd ذخیره شده است، فراهم می‌کند. (کاربران در صورت تمایل می‌توانند این اطلاعات را با استفاده از فرمان chfn تغییر دهند.)
imap	این سرویس امکان دستیابی راه دور به سرور IMAP4 را فراهم می‌کند.
ipop3	این سرویس امکان دستیابی راه دور به سرور POP3 را فراهم می‌کند.
rlogin	این سرویس امکان استفاده از فرمان rlogin را فراهم می‌کند.

عنوان سرویس	توضیح
rsh	این سرویس امکان دستیابی به سرور RSH را فراهم می‌کند.
swat	این سرویس امکان بهره‌برداری از ابزار Samba Web Administration Tool را در اختیار می‌گذارد. (برای اطلاع بیشتر در این زمینه به فصل بیست و نهم مراجعه کنید.)
telnet	این سرویس امکان دستیابی به سرور Telnet را فراهم می‌کند.
wu-ftpd	این سرویس امکان دستیابی به سرور WU0FTP را فراهم می‌کند. (برای اطلاع بیشتر در این زمینه به فصل بیست و هفتم مراجعه کنید.)

کنترل دسترسی با استفاده از مکانیزم TCP Wrapper

بهترین روش مقابله با نفوذمهاجمان به سیستم Linux، این است که تا حد امکان سرویس‌های بیشتری را غیرفعال کرده یا از روی سیستم حذف کنید؛ برای مثال، چنان‌چه بسته نرم‌افزاری telnet-server-* را روی سیستم نصب نکرده باشید، حتی باتجربه‌ترین مهاجمان نیز نمی‌توانند به آن سیستم نفوذ کنند.

سرویس‌های غیرضروری شبح xinetd را از طریق فایل پیکربندی مربوطه که در فهرست /etc/xinetd.d مستقر است، غیرفعال کنید. در بیشتر موارد غیرفعال کردن تمام سرویس‌ها به غیر از سرویس‌های ضروری کافی به نظر می‌رسد.

با وجود این، برخی از کاربران نیاز دارند تا پیغام‌های الکترونیکی خود را از راه دور مورد دستیابی قرار دهند. برخی دیگر نیازمند استفاده از سرویس Telnet هستند. سرویس FTP نیز برای کاربرانی که از راه دور جهت دسترسی به فایل‌ها اقدام می‌کنند، موردنیاز است.

با استفاده از مکانیزم TCP Wrapper می‌توان دسترسی به این سرویس‌ها را کنترل کرد.

عملکرد مکانیزم TCP Wrapper

برای کاهش خطر دسترسی به سیستم‌های نوع Linux دو روش موجود است. در روش نخست مجوز دسترسی به سرویس‌ها از طریق دستکاری فایل‌های پیکربندی مربوطه به کاربران یا کامپیوترهای مشخصی اعطا می‌شود. چنان که در قسمت‌های قبل اشاره شد، فایل‌های پیکربندی مربوط به برخی از این سرویس‌ها در فهرست /etc/xinetd.d مستقر است. روش دوم برای کنترل دسترسی استفاده از مکانیزم TCP Wrapper است که از طریق فایل‌های /etc/hosts.allow و /etc/hosts.deny انجام می‌شود. در این قسمت به بررسی روش دوم می‌پردازیم.

برای محدود کردن دسترسی به سرویس‌های موردنظر کافی است قوانینی را در دو فایل مذکور درج کنیم. اولویت در بازخوانی این قوانین چنین است:

۱- فایل /etc/hosts.allow مورد بازخوانی قرار گرفته و امکان دسترسی از طریق کامپیوترهای مجاز فراهم می‌شود.

۲- فایل /etc/hosts.deny مورد بازخوانی قرار گرفته و دسترسی از طریق کامپیوترهای غیرمجاز منع می‌شود.

۳- چنان‌چه شناسه یا آدرس IP یک کامپیوتر در هیچ کدام از فایل‌های فوق مشخص نشده باشد، امکان دسترسی از طریق آن کامپیوتر فراهم شده و شبح xinetd برای راه‌اندازی سرویس اقدام می کند.

۴- چنان‌چه شناسه یا آدرس IP یک کامپیوتر در هر دو فایل فوق مشخص شده باشد، امکان دسترسی از طریق آن کامپیوتر مجاز شمرده می‌شود. به بیان دیگر، فایل /etc/hosts.allow در اولویت بالاتری نسبت به فایل /etc/hosts.allow قرار داد.

برای مثال، اگر قوانین مذکور در فایل /etc/hosts.allow چنان باشد که کامپیوتری با شناسه A در دسترسی به سرویس موردنظر مجاز بوده و از طرفی قوانین مذکور در فایل /etc/hosts.deny همان کامپیوتر را از دسترسی به آن سرویس منع کند، کامپیوتر A در دسترسی به سرویس موردنظر موفق خواهد بود.

علاوه بر این، تأثیر هر تغییری در فایل‌های /etc/hosts.allow /etc/hosts.deny بدون راه‌اندازی مجدد سیستم‌عامل Linux یا بارگذاری مجدد فایل پیکربندی شبح xinetd منعکس می‌شود.

پیاده‌سازی مکانیزم دیوار آتش با استفاده از شبح xinetd

درج قوانین موردنظر در فایل‌های /etc/hosts.allow و /etc/hosts.deny مشمول قواعد خاصی است. در این فایل‌ها خطوط خالی و توضیحات (خطوطی که با علامت # آغاز می‌شوند) مورد بازخوانی قرار نمی‌گیرند. الگوی عمومی قوانین مندرج در این فایل‌ها به این صورت است:

```
daemon: client: spawn command
```

درالگوی‌فوق متغیر *daemon* بیانگر نام سرویس‌موردنظر و متغیر *client* بیانگر مجموعه‌ای از کامپیوترها یا آدرس‌های IP است. متغیر *command* نیز بیانگر فرمانی است که در ازای دسترسی از طریق آن کامپیوترها به سرویس موردنظر به اجرا درمی‌آید.

ساده‌ترین شکل در پیاده‌سازی الگوی عمومی فوق به این صورت است: `ALL: ALL`

قانون فوق با تمام سرویس‌های شبح xinted و کلیه کامپیوترها مطابقت می‌کند. در قسمت‌های بعد متغیرهای الگوی عمومی فوق، شامل *daemon*، *client* و *command* را مورد بررسی قرار می‌دهیم.

متغیر daemon

این متغیر بیانگر عنوان سرویس موردنظر است، که البته ممکن است با آن‌چه مورد انتظار شماست متفاوت باشد. برای مثال، عنوان in.telnetd به سرویس Telnet اشاره دارد.

جهت اشاره به چندین سرویس کافی است عناوین آن‌ها را با یک جای خالی از یکدیگر جدا کنید. برای مثال، به واسطه درج این قانون در فایل /etc/hosts.deny دسترسی تمام کاربران به سرویس‌های Telnet و RSH محدود می‌شود: `in.telnetd in.rshd: ALL`

چنان‌چه در مورد عنوان یک سرویس خاص تردید دارید، مقدار متغیر server از فایل پیکربندی مربوط به آن را که در فهرست /etc/xinetd.d مستقر است، مورد توجه قرار دهید.

متغیر client

این متغیر بیانگر اسامی کامپیوترها یا آدرس‌های IP است. برای تعیین مقدار این متغیر می‌توان از نشانه‌های جانشین (اصطلاحاً wildcard) نیز استفاده کرد.

برای مشخص کردن کامپیوترهای موردنظر چندین روش وجود دارد. یک روش این است که اسامی آن‌ها را به طور مجزا بنویسیم. برای مثال، به واسطه درج این قانون در فایل /etc/hosts.deny از دسترسی کامپیوترهایی با عناوین sugaree و delilah به دو سرویس Telnet و RSH ممانعت به عمل خواهد آمد: `in.rshd in.telnetd: sugaree delilah`

روش دیگر استفاده از نام کامل حوزه یا FQDN کامپیوتر موردنظر مانند sugaree.mommabears.com است. در صورت تمایل می‌توان از نشانه‌های جانشین در قالب اسامی کامل حوزه‌ها استفاده کرد. برای مثال، نام کامل حوزه mammabears.com. تمام کامپیوترهای مستقر در شبکه mommabears.com را شامل می‌شود.

علاوه بر این می‌توان کامپیوتر به خصوصی از یک مجموعه را مشخص کرد. برای مثال، این قانون تمام کامپیوترهای موجود در شبکه mammabears.com به غیر از کامپیوتر delilah.mommabears.com را شامل می‌شود:

```
in.rshd: .mammabears.com EXCEPT delilah.mommabears.com
```

همین روش‌ها را می‌توان در مورد آدرس‌های IP نیز به کار گرفت. برای مثال، قانونی را که در ادامه ملاحظه می‌کنید، تمام کامپیوترهای مستقر در شبکه 192.168.0.0 به غیر از کامپیوتری با آدرس 192.168.0.102 را تحت تأثیر قرار می‌دهد: (نقطه موجود در انتهای آدرس .192.168.0 به کلیه آدرس‌های IP بین 192.168.0.0 و 192.168.0.255 اشاره دارد.)

```
in.rshd: 192.168.0. EXCEPT 192.168.0.102
```

استفاده از روش CIDR برای بیان آدرس‌های IP (هم‌چون 192.168.0.0/24) در قوانین مندرج در فایل‌های /etc/hosts.allow و /etc/hosts.deny امکان‌پذیر نیست.

جدول ۳-۲۳ نشانه‌های جانشین قابل استفاده به جای نام میزبان، نام کامل حوزه و آدرس IP را شرح می‌دهد.

جدول ۳-۲۳ شرح نشانه‌های جانشین قابل استفاده به جای نام میزبان، نام کامل حوزه و آدرس IP در ساختار قوانین مکانیزم TCP Wrapper

نشانه جانشین	توضیح
ALL	این نشانه کلیه کامپیوترها از جمله کامپیوتر میزبان را شامل می‌شود.
EXCEPT	این نشانه کامپیوترهایی را مشخص می‌کند که مشمول قانون موردنظر نمی‌شوند.
KNOWN	این نشانه کامپیوترهایی را شامل می‌شود که لیست آن‌ها در بانک اطلاعاتی سرویس DNS یا فایل /etc/hosts موجود است.
LOCAL	این نشانه کامپیوترهایی را شامل می‌شود که دارای عنوانی ساده (هم‌چون sugaree) بوده یا به بیان دیگر در عنوان آن‌ها از علامت نقطه استفاده نشده باشد.
PARANOID	این نشانه کامپیوترهایی را شامل می‌شود که نام میزبان یا نام کامل حوزه آن‌ها با آدرس IP آن‌ها مطابقت نمی‌کند.
UNKNOWN	این نشانه کامپیوترهایی را شامل می‌شود که که نام آن‌ها در بانک اطلاعاتی سرویس DNS یا فایل /etc/hosts موجود نیست.

متغیر command

هر گونه تلاشی برای راه‌اندازی یکی از سرویس‌های شبح xinetd در فایل /var/log/messages به ثبت می‌رسد. با این حال، به کمک فرمان spawn می‌توان ترتیبی داد تا در ازای راه‌اندازی هریک از این

سرویس‌ها، عملیات دیگری انجام شود. برای مثال، این قانون موجب می‌شود تا در ازای دسترسی به سرویس Telnet یک پیغام الکترونیکی به آدرس mj@example.com ارسال شود:

```
in.telnetd: ALL: spawn /bin/mail -s "Telnet security alert"
mj@example.com
```

اقدام مناسب دیگر در این زمینه عبارت است از درج پیغام مربوط به راه‌اندازی سرویس موردنظر در یکی از فایل‌های فهرست /var/log با ثبت تاریخ و ساعتی که سرویس مزبور مورد دستیابی قرار گرفته است.

برنامه Secure Shell یا SSH

چنان‌چه ارسال پیغام‌های شبکه در قالب متنی ساده را به هر دلیل خطرناک تشخیص می‌دهید، می‌توانید از برنامه Secure Shell یا به اختصار SSH استفاده کنید. این برنامه هرگونه بسته ارسالی را از طریق شبکه رمزگذاری می‌کند. از این‌رو می‌توان آن‌را جایگزین مناسبی برای فرامین مربوط به دو سرویس RSH و Telnet دانست.

نصب برنامه SSH

استفاده از برنامه SSH مستلزم نصب چندین بسته نرم‌افزاری است. شرح این بسته‌های نرم‌افزاری در جدول ۴-۲۳ آمده است. چنان‌که در فصل دهم اشاره شد، با استفاده از فرمان rpm می‌توانید برای نصب این بسته‌های نرم‌افزاری اقدام کنید.

جدول ۴-۲۳ شرح بسته‌های نرم‌افزاری موردنیاز برای استفاده از برنامه SSH

عنوان بسته نرم‌افزاری	توضیح
openssh-*	این بسته نرم‌افزاری شامل فایل‌های اصلی موردنیاز برای استفاده از برنامه SSH هم در سمت کلاینت و هم در سمت سرور است.
openssh-askpass-gnome-*	این بسته نرم‌افزاری شامل فایل‌های موردنیاز برای مدیریت کلمات عبور در محیط گرافیکی GNOME است.
openssh-askpass-*	این بسته نرم‌افزاری شامل فایل‌های موردنیاز برای مدیریت کلمات عبور در محیط گرافیکی است.
openssh-clients-*	این بسته نرم‌افزاری شامل فایل‌های برنامه کلاینت است که امکان ارتباط با برنامه سرور SSH را فراهم می‌کند.
openssh-server-*	این بسته نرم‌افزاری شامل فایل‌های برنامه سرور SSH است.

استفاده از برنامه SSH تحت سیستم‌عامل Windows نیز امکان‌پذیر است. تا زمان انتشار کتاب حاضر نسخه رایگان بسته نرم‌افزاری Open SSH را می‌توان با مراجعه به وب سایت شرکت Network Simplicity به آدرس اینترنتی http://www.networksimplicity.com مورد دستیابی قرار داد. پس از نصب و پیکربندی این برنامه می‌توان آن‌را مشابه نسخه تحت Linux مورد استفاده قرار داد.

پیکربندی برنامه SSH

فایل اصلی پیکربندی برنامه SSH فایلی با عنوان /etc/ssh/sshd_config است. با وجودی که تنظیمات پیش‌فرض این فایل پیکربندی برای اغلب کاربردها قابل استفاده است، در صورت تمایل می‌توان آن‌ها را تغییر داد. این تغییرات ممکن است با هدف محدود کردن دسترسی به دسته‌ای از آدرس‌های IP، تنظیم اندازه کلیدهای رمزگذاری، تغییر نحوه احراز هویت سرویس RSH و بهره‌برداری از مکانیزم امنیتی Kerberos انجام شود.

پس از نصب بسته‌های نرم‌افزاری موردنیاز، لازم است کلیدهای خصوصی و عمومی مورد استفاده برای رمزگذاری و رمزگشایی پیغام‌های ارسالی را تعریف کنید. کلید خصوصی روی کامپیوتری نگهداری می‌شود که برنامه سرور SSH روی آن نصب شده است. برنامه کلاینت SSH با در اختیار داشتن کلید عمومی می‌تواند پیغام‌های ارسالی به سرور را رمزگذاری کند. پیغام‌های ارسالی از سرور نیز توسط کلید خصوصی رمزگذاری می‌شوند. این پیغام‌های حاوی کلید عمومی موردنیاز برای رمزگشایی پیغام ارسالی به کامپیوتر موردنظر هستند. از آن‌جا که این کلیدها اعداد تصادفی ۵۱۲ بیتی هستند، کشف آن‌ها با استفاده از یک کامپیوتر شخصی مستلزم صرف زمانی معادل چند هفته است.

کلیدهای خصوصی و عمومی را می‌توان با استفاده از فرامین ssh-kegen -t rsa و ssh-keygen -t dsa ایجاد کرد. فرمان نخست (گزینه -t rsa) کلید موردنظر را بر اساس الگوریتم RSA Security و فرمان دوم (گزینه -t dsa) آن‌را بر اساس الگوریتم Digital Secure Algorithm ایجاد می‌کند.

کلیدهای خصوصی و عمومی به طور پیش‌فرض در قالب فایلی در زیرفهرست ssh. از فهرست خانگی کاربر، یعنی در فهرست ssh./~ ایجاد می‌شوند. جدول ۵-۲۳ اسامی فایل‌های حاوی کلیدهای خصوصی و عمومی ایجاد شده به واسطه اجرای هریک از این فرامین را نشان می‌دهد.

پس از ایجاد کلیدهای خصوصی و عمومی باید برای ایجاد یک اعتبارنامه (اصطلاحاً passphrase) اقدام کنید. چنان‌چه این کار را انجام ندهید، مهاجمان به سادگی می‌توانند کلید خصوصی مورد استفاده در تبادل پیغام‌ها را بربایند. در برخی موارد این اقدام مهاجمان به آن‌ها اجازه می‌دهد تا از شناسه دیجیتالی قربانی به منظور استفاده از کارت‌های اعتباری وی بهره‌برداری کرده یا قراردادهایی را به نام

او امضا کنند.

جدول ۵-۲۳ فایل‌های حاوی کلیدهای خصوصی و عمومی ایجاد شده با استفاده از الگوریتم‌های DSA و RSA

نوع الگوریتم	فایل حاوی کلید خصوصی	فایل حاوی کلید عمومی
DSA	~/.ssh/id_dsa	~/.ssh/ide_dsa.pub
RSA	~/.ssh/id_rsa	~/.ssh/id_rsa.pub

بررسی یک مثال

پس از نصب بسته‌های نرم‌افزاری کلاینت و سرور موردنیاز برای استفاده از برنامه SSH و ایجاد کلیدهای عمومی و خصوصی مورد نظر، می‌توانید بهره‌برداری از این برنامه را آغاز کنید. در صورت لزوم می‌توانید با اجرای فرمان service sshd status از راه‌اندازی موفقیت آمیز سرویس SSH اطمینان حاصل کنید.

اکنون با در اختیار داشتن یک حساب کاربری معتبر روی یک کامپیوتر دیگر می‌توانید به آن متصل شوید. برای مثال، فرض کنید نام کاربری شما tblair بوده و از یک حساب کاربری واحد روی کامپیوتر خود و کامپیوتر دیگری از شبکه با نام کامل حوزه sugaree.mommabears.com برخوردار هستید. در این صورت، کافی است برای اتصال به آن کامپیوتر فرمان ssh sugaree.mommabears.com را اجرا کنید.

نخستین مرتبه‌ای که با استفاده از فرمان ssh (یا فرامین مرتبط) برای اتصال اقدام می‌کنید، پیغامی شبیه به این را مشاهده خواهید کرد:

```
The authenticity of host 'sugaree.mommabears.com' can't be
established. RSA key fingerprint is
34:21:d2:3c:34:83:40:23:d2:c2:9f:34:90:e3:a3. Are you sure
you want to continue connecting (yes/no)?
```

در پاسخ به پرسش فوق پاسخ yes را انتخاب کرده و کلمه عبور خود را جهت دستیابی به کامپیوتر موردنظر وارد کنید. پس از برقراری اتصال لازم می‌توانید با کامپیوتر sugaree.mommabears.com مشابه کامپیوتر خود به کار بپردازید. هر گونه تبادل پیغام میان این دو کامپیوتر به صورت رمزگذاری شده انجام خواهد شد. با در اختیار داشتن یک حساب کاربری دیگر روی کامپیوتر مذکور می‌توانید مجدداً با استفاده از آن وارد سیستم شوید. برای مثال، جهت ورود مجدد به همان سیستم با استفاده از حساب کاربری vputin کافی است این فرمان را اجرا کنید:

```
# ssh vputin@sugaree.mommabears.com
```

هم‌چنین در صورت تمایل می‌توانید از سرویس FTP قابل اعتمادی که به همراه برنامه SSH روی کامپیوتر نصب می‌شود جهت انتقال فایل استفاده کنید. برای مثال، فرض کنید چندین بسته نرم‌افزاری RPM شامل کامپایلر زبان برنامه‌نویسی C که توسط سازمان GNU منتشر شده است در فهرست خانگی کاربر vputin موجود باشد. در صورت اطلاع از کلمه عبور این کاربر می‌توانید از سرویس FTP مزبور برای انتقال بسته‌های نرم‌افزاری موردنظر اقدام کنید. به عنوان نمونه، با اجرای این فرامین می‌توانید بسته نرم‌افزاری حاوی کامپایلر زبان برنامه‌نویسی C را از فهرست خانگی کاربر vputin که روی کامپیوتر راه دور مستقر است، به فهرست tmp/ از کامپیوتر خود منتقل کنید:

```
# sftp vputin@sugaree.mommabears.com
sftp> get gcc-3.9.8.src.rpm /tmp
```

رفع مشکلات مربوط به دسترسی

به دلیل وجود لایه‌های امنیتی متعدد، تشخیص مشکلات مربوط به دسترسی کار واقعاً مشکلی است. با این حال، هنگام وقوع مشکلات مربوط به دسترسی کاربران به سرویس‌های موردنظر می‌توان این اقدامات را انجام داد:

- از نصب سرویس موردنظر روی کامپیوتر اطمینان حاصل کنید.
- مطمئن شوید که سرویس موردنظر فعال است.
- فایل‌های پیکربندی مربوط به آن سرویس را مورد بازبینی قرار دهید.
- چنان‌چه سرویس موردنظر از نوع xinetd است فایل‌های /etc/hosts.allow و /etc/hosts.deny را مورد بازبینی قرار دهید.
- با اجرای فرمان iptables -L زنجیره‌های دیوار آتش را مورد بازبینی قرار دهید.

اطمینان از نصب سرویس

اطمینان از نصب سرویس بسیار ساده است. چنان‌که در فصل دهم نیز توضیح داده شد، برای اطلاع از نصب یک بسته نرم‌افزاری RPM کافی است فرمان rpm -q *packagename* را که در آن متغیر *packagename* عنوان بسته نرم‌افزاری موردنظر است، اجرا کنید.

فراموش نکنید که برای نصب کامل سرویس‌هایی چون Telnet، FTP و SSH نصب هر دو بسته نرم‌افزاری کلاینت و سرور ضروری است.

اطمینان از فعال بودن سرویس

همان گونه که در فصل سیزدهم نیز اشاره شد، به ازای هر سرویس یک فایل اجرایی در فهرست /etc/rc.d/init.d موجود است که به کمک آن می‌توان از وضعیت سرویس مربوطه اطلاع حاصل کرد. برای این منظور کافی است فرمان /etc/rc.d/init.d/*script* status یا service *script* status را که در آن متغیر *script* به فایل اجرایی موردنظر اشاره دارد، اجرا کنید.

در صورتی که سرویس موردنظر غیرفعال باشد با تغییرات جزیی در فایل پیکربندی مربوطه در فهرست /etc/xinetd.d می‌توانید آن‌را فعال کنید. برای این منظور باید متغیر disable را که به طور پیش‌فرض با مقدار yes تنظیم شده است، به no تغییر دهید.

علاوه بر این فراموش نکنید که به کمک ابزاری مانند chkconfig از این موضوع که سرویس موردنظر در راه‌اندازی‌های بعدی سیستم‌عامل Linux هم‌چنان فعال خواهد بود، اطمینان حاصل کنید. برای مثال، با اجرای این فرمان می‌توان از راه‌اندازی سرویس HTTP (یا httpd) در سطوح اجرایی دوم، سوم و پنجم اطمینان حاصل کرد:

```
# chkconfig --list 235 httpd on
```

نحوه انجام این کار در مورد سرویس‌های شبح xinetd اندکی متفاوت است. با اجرای این فرمان می‌توان شبح xinetd را فعال کرد:

```
# chkconfig swat on
```

همین اقدام کافی است تا کلیه سرویس‌های شبح xinetd در تمام سطوح موجود فعال شوند.

بازبینی فایل‌های پیکربندی سرویس‌ها

برخی از سرویس‌ها دارای فایل‌های پیکربندی به‌خصوصی هستند که با استفاده از آن می‌توان دسترسی کاربران را به سرویس موردنظر محدود کرد. دسترسی به سرویس‌هایی مانند Apache و Samba از طریق فایل‌های پیکربندی اصلی این سرویس‌ها امکان‌پذیر است. با وجود این، امنیت برخی از سرویس‌های xinetd از جمله FTP به واسطه تنظیمات فایل‌های خاصی (هم‌چون /etc/ftpaccess در مورد سرویس FTP) تأمین می‌شود. این گونه فایل‌ها را در فصول مربوط به هریک از این سرویس‌ها مورد بررسی قرار خواهیم داد.

بازبینی فایل‌های کنترل دسترسی به سرویس‌های xinetd

چنان‌که در این فصل مشاهده کردید، دسترسی به سرویس‌های شبح xinetd را می‌توان از طریق فایل‌های /etc/hosts.allow و /etc/hosts.deny به خوبی کنترل کرد. کنترل دسترسی به این سرویس‌ها

از طریق فایل‌های پیکربندی موجود در فهرست /etc/xinetd.s نیز امکان پذیر است.

بازبینی زنجیره‌های دیوار آتش

پیکربندی مکانیزم دیوار آتش را می‌توان ضمن نصب سیستم‌عامل Red Hat Linux یا بعد از نصب آن به کمک یکی از دو ابزار پیکربندی redhat-config-securitylevel یا lokkit انجام داد. هر دو ابزار پیکربندی مذکور که به طور خاص برای سیستم‌عامل Red Hat Linux طراحی شده‌اند، امکان تعیین سطوح امنیتی پیش‌فرض (شامل High و Medium) را در اختیار قرار می‌دهند.

در صورت تمایل، به کمک برنامه iptables می‌توانید برای پیکربندی مکانیزم دیوار آتش اقدام کنید. (جهت اطلاع بیشتر در این زمینه به فصل بیست و دوم مراجعه کنید.)

با استفاده از قوانین مشخصی می‌توان دسترسی کاربران به پورت‌های موردنظر را محدود کرد. برای مثال، جهت اعطای مجوز دسترسی به سرور Apache با استفاده از فرمان iptables می‌توان به سادگی قانونی را با توجه به مطالب عنوان شده در فصل بیست و دوم وضع کرده یا این‌که یکی از ابزارهای lokkit یا redhat-config-securitylevels را جهت اعطای مجوز دسترسی به پورت موردنظر یعنی پورت شماره ۸۰ مورد استفاده قرار داد. (برای اطلاع از پورت‌های مربوط به سرویس‌های مختلف TCP/IP به فایل /etc/services مراجعه کنید.)

جمع‌بندی

کاربران اغلب نیاز دارند تا فایل‌های مورد نظر خود را از یک موقعیت راه دور مورد دستیابی قرار دهند. در سیستم‌عامل Linux مجموعه‌ای از سرویس‌های دسترسی از راه دور برای این منظور پیش‌بینی شده است. برخی از این سرویس‌ها تحت عنوان Extended Internet Services Daemon یا به اختصار شبح xinetd شناخته شده‌اند.

شبح xinetd وظیفه کنترل دسترسی کاربران به سرویس‌ها و هم‌چنین راه‌اندازی آن‌ها را به عهده دارد. کنترل دسترسی به این سرویس‌ها از طریق فایل پیکربندی /etc/xinetd.conf و فایل‌های پیکربندی مربوطه که در فهرست /etc/xinetd.d موجود است، انجام می‌پذیرد. سرویس‌های مزبور به طور پیش‌فرض غیرفعال هستند. از این‌رو، برای بهره‌برداری از این سرویس‌ها ابتدا باید آن‌ها را فعال کرد. سه سرویس FTP، Telnet و RSH سرویس‌های اصلی شبح xinetd در زمینه دسترسی از راه دور محسوب می‌شوند.

دسترسی به سرویس‌های شبح xinetd را می‌توان از طریق مکانیزم TCP Wrapper نیز کنترل کرد. برای این منظور باید خط‌مشی دسترسی را در دو فایل /etc/hosts.allow و /etc/hosts.deny مشخص کرد. با درج فرامین پیکربندی مناسب در این فایل‌ها به سادگی می‌توان دسترسی کامپیوترها یا شبکه‌ها را به سرویس‌های موردنظر کنترل کرد. هم‌چنین می‌توان ترتیبی داد تا در ازای دسترسی به سرویس یا سرویس‌های موردنظر فرمان به خصوصی اجرا شود. این گونه فرامین اغلب به منظور نمایش یک پیغام اخطار یا ثبت جزییات مربوط به دسترسی انجام می‌شوند.

سرویس Secure Shell امکانات لازم برای رمزگذاری پیغام‌های ارسالی در فرآیند تبادل پیغام‌ها را در اختیار می‌گذارد. با نصب بسته‌های نرم‌افزاری *-openssh می‌توان از مکانیزم‌های RSA یا DSA به منظور رمزگذاری پیغام‌های ارسالی از طریق شبکه بهره‌برداری کرد. برای رمزگذاری و رمزگشایی پیغام‌های ارسالی از کلیدهای خصوصی و عمومی استفاده می‌شود. محافظت از کلید خصوصی بسیار حایز اهمیت است، چرا که مهاجمان با در اختیار داشتن آن می‌توانند پیغام‌های ارسالی را رمزگشایی کنند. با بهره‌گیری از فرامین مربوط به سرویس SSH و برخورداری از یک حساب کاربری معتبر روی یک کامپیوتر راه دور می‌توان برای اتصال به آن کامپیوتر اقدام کرده و حتی از امکانات یک سرویس FTP مطمئن که در قالب سرویس SSH قابل دستیابی است برای انتقال فایل‌های موردنظر از کامپیوتر راه دور روی کامپیوتر محلی استفاده کرد.

به دلیل وجود مکانیزم دیوار آتش و پیکربندی لایه‌های امنیتی متعدد تشخیص و رفع اشکالات دسترسی به سرویس‌ها تا اندازه‌ای پیچیده است. با وجود این، برخی اقدام‌ها مانند اطمینان از نصب سرویس موردنظر و فعال بودن آن می‌تواند در انجام این کار مؤثر باشد. برای تأمین امنیت برخی سرویس‌ها فایل‌های پیکربندی به خصوصی پیش‌بینی شده که برای تشخیص و رفع اشکالات دسترسی کاربران به این گونه سرویس‌ها باید دقیقاً مورد بازبینی قرار بگیرند. با این‌که تأمین امنیت سرویس‌های شبح xinetd از طریق دو فایل /etc/hosts.allow و /etc/hosts.deny امکان‌پذیر است، در صورت لزوم می‌توان با استفاده از برنامه iptables جهت پیکربندی مکانیزم دیوار آتش (به منظور کنترل دسترسی به این سرویس‌ها) اقدام کرد.

در فصل بیست و چهارم جزییات مربوط به پیکربندی دو سرویس مهم از سرویس‌های قابل استفاده در سیستم‌عامل Linux یعنی Domain Name Service یا DNS و Dynamic Host Configuration Protocol یا DHCP را مورد بررسی قرار می‌دهیم.

فصل بیست‌وچهارم

سرویس‌های DNS و DHCP

سیستم عامل Linux به کمک دو سرویس DNS و DHCP مدیریت اسامی میزبان‌ها و آدرس‌های IP را انجام می‌دهد. سرویس DNS یا Domain Name Service در قالب یک بانک اطلاعاتی از اسامی میزبان‌ها یا اسامی حوزه‌ها و آدرس‌های IP متناظر پیکربندی می‌شود. سرویس DHCP یا Dynamic Host Configuration Protocol امکانات لازم برای تخصیص آدرس‌های IP به کامپیوترهای مستقر در شبکه را فراهم می‌کند. هر دو سرویس DNS و DHCP مشابه بیشتر سرویس‌های سیستم‌عامل Linux شامل یک برنامه سرور و یک برنامه کلاینت هستند.

سرویس DNS در سیستم‌عامل Linux بر اساس نرم‌افزار BIND یاBerkeley Internet Name Domain پیاده‌سازی شده و پیکربندی آن به واسطه مجموعه‌ای از فایل‌ها که در دو فهرست /etc و /var/named مستقر هستند، امکان‌پذیر است. هر کامپیوتری که سیستم‌عامل Linux روی‌آن نصب شده و جهت استفاده از پروتکل TCP/IP پیکربندی شده باشد، برنامه کلاینت DNS به طور پیش‌فرض روی آن نصب می‌شود. چنین کامپیوتری می‌تواند به عنوان کلاینت DNS عمل کند. هنگامی که با استفاده از این گونه کامپیوترها وب سایتی را مورد دستیابی قرار می‌دهید، آن کامپیوتر به واسطه استفاده از سرویس DNS، آدرسIP آن وب سایت را تشخیص داده و در تبادل پیغام‌ها از طریق اینترنت آن آدرس را مورد بهره‌برداری قرار می‌دهد.

سرویس DHCP امکان تخصیص آدرس‌های IP به کامپیوترهای مستقر در شبکه را فراهم می‌کند. این سرویس را می‌توان به منظور دستیابی به شبکه‌های خارجی، دستیابی به سایر سرویس‌های موردنیاز و موارد دیگر پیکربندی کرد. عنوان نسخه‌ای از برنامه کلاینت سرویس DHCP که به همراه سیستم‌عامل Red Hat Linux منتشر می‌شود، در نسخه‌های اخیر این سیستم‌عامل بارها دستخوش تغییر شده است، با وجود این، تغییری در قابلیت آن داده نشده است. این برنامه یک آدرس IP را از برنامه سرور DHCP دریافت کرده و به جمع‌آوری سایر اطلاعات موردنیاز از آن سرور می‌پردازد. موضوعات مورد بررسی در فصل حاضر به این شرح است:

- پیکربندی سرور DNS
- استفاده از برنامه‌های کلاینت DNS

- پیکربندی سرور DHCP
- استفاده از برنامه‌های کلاینت DHCP و BOOTP

پیکربندی سرور DNS

سرویس Domain Name Service یا DNS متشکل از یک بانک اطلاعاتی شامل اسامی کامل حوزه‌ها یا اصطلاحاً FQDN مانند www.sybex.com و آدرس‌های IP مانند 63.99.198.12 است. پیاده‌سازی این سرویس در سیستم‌عامل Red Hat Linux بر اساس نرم‌افزار BIND که بسیاری از سرویس‌های DNS کارآمد مستقر در اینترنت از آن سود می‌برند، انجام شده است.

بانک اطلاعاتی هیچ کدام از سرورهای DNS مستقر در اینترنت شامل تمام اسامی کامل حوزه‌ها و آدرس‌های IP متناظر با آن‌ها نیست. چنان‌چه بانک اطلاعاتی یک سرور DNS فاقد نام کامل حوزه موردنظر باشد، سرور مزبور برای پی بردن به آدرس IP متناظر با آن از طریق سایر سرورهای DNS اقدام کرده و در صورت موفقیت، نام کامل حوزه و آدرس IP متناظر با آن‌را در بانک اطلاعاتی خود درج می‌کند.

پیکربندی سرور DNS از طریق دو فایل /etc/named.conf و /etc/named.custom و هم‌چنین فایل‌های موجود در فهرست /var/named امکان‌پذیر است. برای پیکربندی سرور DNS بهتر است این فایل‌ها را مستقیماً مورد ویرایش قرار دهید.

با وجود این، شرکت Red Hat مدیران سیستم‌ها را هم‌چنان به استفاده از برنامه redhat-config-bind جهت پیکربندی سرور DNS تشویق می‌کند. پیکربندی سرور DNS فرآیند ساده‌ای نیست. از این‌رو، استفاده از برنامه redhat-config-bind برای مدیران کم‌تجربه مناسب‌تر است. استفاده از این برنامه تنها در یک محیط گرافیکی مانند GNOME یا KDE امکان‌پذیر است.

بسته‌های نرم‌افزاری موردنیاز برای بهره‌برداری از سرویس DNS

تمام بسته‌های نرم‌افزاری RPM موردنیاز برای استفاده از سرویس DNS به طور پیش‌فرض روی کامپیوتر میزبان نصب نمی‌شود. جدول ۱-۲۴ بسته‌های نرم‌افزاری موردنیاز برای استفاده از این سرویس را شرح می‌دهد. چنان‌که در فصل دهم اشاره شد، با اجرای فرمان rpm -q *packagename* می‌توانید از نصب بسته نرم‌افزاری موردنظر که در این فرمان با متغیر *packagename* نشان داده شده است، اطلاع حاصل کنید. پس از نصب بسته‌های نرم‌افزاری مورد نیاز، با اجرای فرمان rpm -ql *packagename* می‌توانید فایل‌های مربوطه را مشاهده کنید.

جدول ۱-۲۴ شرح بسته‌های نرم‌افزاری موردنیاز برای استفاده از سرویس DNS

عنوان بسته نرم‌افزاری	توضیح
bind-*	این بسته نرم‌افزاری شامل برنامه سرور DNS است.
bind-devel-*	این بسته نرم‌افزاری شامل فایل‌های موردنیاز برای توسعه قابلیت‌های سرویس DNS بوده و نصب آن برای استفاده از سرویس DNS ضروری نیست.
bind-utils-*	این بسته نرم‌افزاری شامل برنامه‌های کمکی از جمله dig و host است.
caching-nameserver-*	این بسته نرم‌افزاری شامل فایل‌های پیکربندی اصلی برای سرور DNS مورد استفاده برای نگهداری موقت اسامی کامل حوزه‌ها و آدرس‌های IP متناظر است. دوفایل‌پیکربندی‌نمونه‌باعناوین /etc/named.conf و /var/named/localhost.zone نیز در قالب این بسته نرم‌افزاری نصب می‌شود.
redhat-config-bind-*	این بسته نرم‌افزاری شامل برنامه‌ای با یک رابط گرافیکی است که امکانات لازم برای پیکربندی سرویس را در اختیار می‌گذارد. نصب این برنامه برای استفاده از سرویس مزبور ضروری است.

مفاهیم مربوط به سرویس DNS

چنان‌که در قسمت‌های قبل نیز گفته شد، بانک اطلاعاتی هیچ کدام از سرورهای DNS مستقر در اینترنت شامل تمام اسامی کامل حوزه‌ها (اصطلاحاً FQDN) و آدرس‌های IP متناظر با آن‌ها نیست. متمرکز کردن این اطلاعات به دلیل حجم زیاد آن‌ها غیرعملی است. از این‌رو، سرورهای DNS مستقر در اینترنت به گونه‌ای سازمان‌دهی شده‌اند که هر سرور DNS وظیفه سرویس‌دهی یک ناحیه یا اصطلاحاً zone را که در واقع بخشی از یک حوزه یا domain محسوب می‌شود، به عهده داشته باشد. تقسیم‌بندی این نواحی بر اساس روش سازمان‌دهی اسامی کامل حوزه‌ها انجام شده است.

برای شروع نام کامل حوزه .www.mommabears.com را در نظر بگیرید. به نقطه موجود در سمت راست com. توجه کنید. به این نقطه اصطلاحاً ناحیه ریشه یا root zone گفته می‌شود. (در نگارش نام کامل حوزه‌ها اغلب این نقطه حذف می‌شود.)

اسامی سرورهای DNS ریشه (اصطلاحاً root DNS servers) به عنوان بخشی از بسته نرم‌افزاری caching-nameserver-* در فهرست /var/named/named.ca ذخیره می‌شود.

عباراتی مثل .com، .net، .org و مانند آن بیانگر حوزه‌های سطح بالا یا اصطلاحاً top-level domain هستند. در مورد نام کامل حوزه www.mammabears.com. جمله mommabears بیانگر حوزه فرعی com. و جمله www بیانگر نام یا به عبارت دیگر نام مستعار (اصطلاحاً alias) کامپیوتر میزبان وب سرور موردنظر است.

سرور DNS اصلی (اصطلاحاً master) مستقر در شبکه mommabears.com. سرور DNS قابل اعتماد در آن ناحیه محسوب می‌شود. از دیدگاه دیگر، به mommabears.com. اصطلاحاً Forward Master Zone یا Primary Master Zone گفته می‌شود.

علاوه بر ترجمه اسامی کامل حوزه‌ها به آدرس‌های IP متناظر باید امکانات لازم برای تبدیل معکوس، یعنی ترجمه آدرس‌های IP به اسامی کامل حوزه‌ها نیز موجود باشد. به بانک اطلاعاتی حاوی اطلاعات موردنیاز برای این تبدیل معکوس، اصطلاحاً Reverse Master Zone گفته می‌شود.

سرورهای DNS را می‌توان به یکی از چهار روش Master، Slave، Caching-only و Forwarding پیکربندی کرد. چنان‌که از فصل بیست و یکم به خاطر دارید، آدرس IP تمام سرورهای DNS مورد استفاده باید در فایل پیکربندی /etc/resolve.conf درج شود. به شرح این چهار نوع سرور DNS توجه کنید:

- **سرور DNS نوع Master**: این نوع سرور در واقع سرور DNS قابل اعتماد برای یک منطقه خاص، مانند sybex.com محسوب می‌شود. کلیه درخواست‌های ارسالی از شبکه sybex.com برای ترجمه اسامی کامل حوزه‌ها به آدرس‌های IP و بالعکس به این سرور ارسال می‌شود. سایر انواع سرورهای DNS موجود از این نوع سرور DNS به منظور دستیابی به سایر شبکه‌ها و کامپیوترهای موجود در شبکه sybex.com بهره می‌برند.
- **سرور DNS نوع Slave**: درخواست‌های ارسالی از کامپیوترهای مستقر در شبکه‌ای مانند sybex.com برای ترجمه اسامی کامل حوزه‌ها به آدرس‌های IP و بالعکس می‌تواند توسط این نوع سرور DNS مدیریت شود. سرور DNS نوع Slave برای انجام چنین ترجمه‌ای از بانک اطلاعاتی مستقر در یک سرور DNS نوع Master بهره می‌برد.
- **سرور DNS نوع Caching-only**: این نوع سرور DNS تنها درخواست‌های ارسالی اخیر برای ترجمه اسامی کامل حوزه‌ها به آدرس‌های IP و بالعکس را نگهداری می‌کند. با وجود چنین سروری در شبکه محلی، به ویژه در صورتی که سرور DNS اصلی (نوع Master یا Slave) در یک شبکه راه‌دور مستقر باشد، سرعت پاسخ‌دهی به‌درخواست‌های‌ارسالی اغلب افزایش قابل ملاحظه‌ای می‌یابد.

- **سرور DNS نوع Forwarding**: این نوع سرور DNS مستقیماً هیچ اقدامی را برای ترجمه اسامی کامل حوزه‌ها به آدرس‌های IP و بالعکس انجام نداده بلکه درخواست موردنظر را برای سرور DNS دیگری که مشخصات آن در فایل پیکربندی /etc/named.conf ذکر شده است، ارسال می‌کند.

پیکربندی سرور DNS

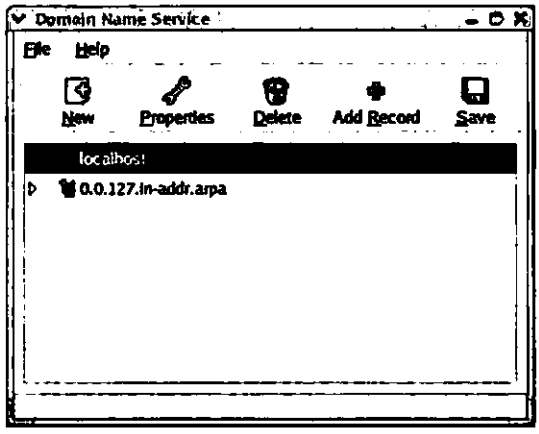
توصیه‌های زیادی برای پیکربندی سرویس‌های سیستم‌عامل Linux از طریق سطر فرمان این سیستم‌عامل شده است. با انجام این کار، ضمن فراگیری مطالب بیشتر درباره سرویس‌های مورد نظر، می‌توانید امکانات بهتری را جهت تنظیمات سرور DNS به خدمت بگیرید.

با وجود این، شرکت Red Hat جهت پیکربندی سرورهای DNS مدیران، سیستم‌ها را به استفاده از ابزار گرافیکی redhat-config-bind که توسط این شرکت توسعه داده شده است، تشویق می‌کند. حتی وجود خطاهای جزیی در فایل اصلی پیکربندی سرور DNS یعنی /etc/named.conf می‌تواند مانع از سرویس‌دهی شود. چنان‌چه در استفاده از سیستم‌عامل Linux تجربه زیادی ندارید، برای کاهش احتمال خطا توصیه می‌کنیم از ابزار گرافیکی redhat-config-bind به منظور پیکربندی سرور DNS استفاده کنید. تنظیماتی را که ابزار گرافیکی مزبور از آن‌ها پشتیبانی به عمل نمی‌آورد، می‌توانید مستقیماً با ویرایش فایل پیکربندی /etc/named.custom انجام دهید. ساختار این فایل مشابه ساختار فایل پیکربندی سرویس چاپ LPD است که در فصل بیست و پنجم آن‌را مورد بررسی قرار می‌دهیم.

فایل پیکربندی /etc/named.conf را می‌توانید به طور مستقیم و بدون استفاده از ابزار گرافیکی redhat-config-bind مورد ویرایش قرار دهید. با وجود این، دقت کنید که ویرایش‌های اعمال شده به فایل مذکور با استفاده از ابزار گرافیکی redhat-config-bind محتوای آن فایل را تحت تأثیر قرار می‌دهد. اگر قصد ندارید فایل پیکربندی /etc/named.conf را مستقیماً ویرایش کنید، لزومی ندارد که بسته نرم‌افزاری redhat-config-bind-* را نصب کنید. هم‌چنین می‌توانید از مطالعه قسمت بعد نیز صرف نظر کنید.

پیکربندی سرور DNS نوع Master

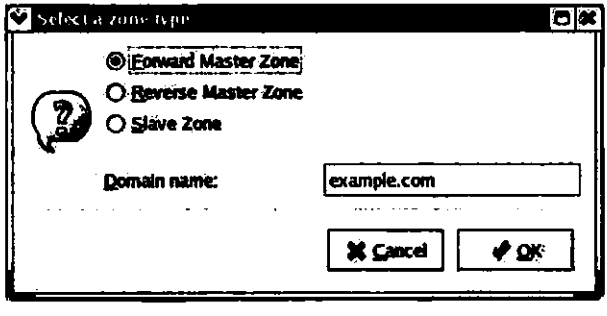
برای پیکربندی سرور DNS اصلی (اصطلاحاً Primary یا Master) ابتدا محیط گرافیکی موردنظر خود مانند GNOME یا KDE را راه‌اندازی کرده و سپس برنامه redhat-config-bind را از سطر فرمان سیستم‌عامل Linux اجرا کنید. با این اقدام پنجره‌ای مشابه شکل ۱-۲۴ با عنوان Domain Name Service باز می‌شود.



شکل ۱-۲۴ پنجره حاصل از اجرای فرمان redhat-config-bind

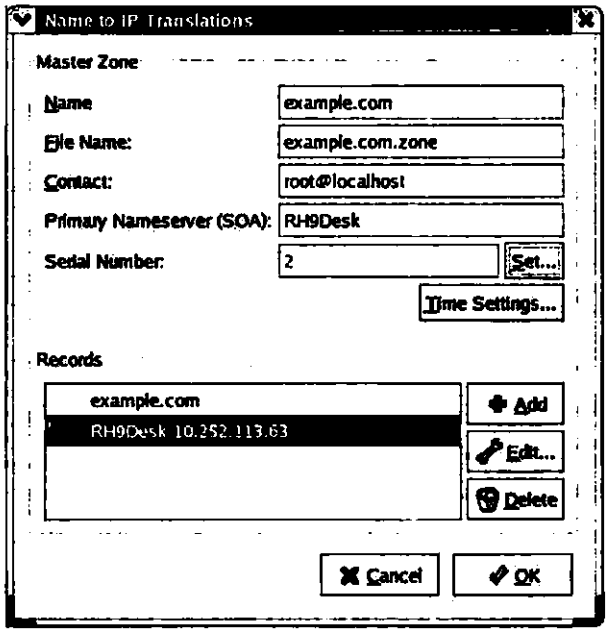
اجرای برنامه redhat-config-bind در محیط گرافیکی GNOME یا KDE با انتخاب گزینه Domain Name Service از منوی Server Settings واقع در منوی فرعی System Settings از منوی اصلی یعنی Main Menue (یا K Menue در محیط گرافیکی KDE) امکان‌پذیر است.

پیکربندی سرور DNS اصلی در واقع چیزی جز ویرایش فایل پیکربندی /etc/named.conf و فایل‌های پیکربندی موجود در فهرست /var/named نیست. دکمه New از پنجره Domain Name Service را کلیک کنید. سپس گزینه Forward Master Zone از کادر محاوره‌ای Select A Zone Type را انتخاب و نام حوزه موردنظر خود را در فیلد متنی Domain Name وارد کنید. در صورت تمایل، می‌توانید از عنوان example.com که یک نام حوزه عمومی است برای این منظور استفاده کنید. شکل ۲-۲۴ کادر محاوره‌ای Select A Zone Type را نشان می‌دهد.



شکل ۲-۲۴ کادر محاوره‌ای Select A Zone Type

با کلیک دکمه OK از کادر محاوره‌ای مزبور، مشابه شکل ۳-۲۴ کادر محاوره‌ای دیگری با عنوان Name To IP Translations باز می‌شود. نام کامپیوتر میزبان سرور DNS را در فیلد متنی Primary Nameserver (SOA) وارد کرده و در انتهای آن کاراکتر نقطه را درج کنید.

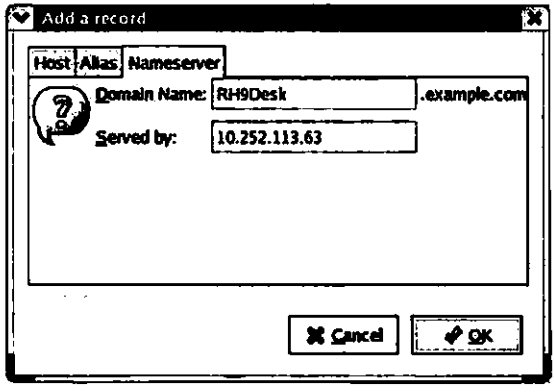


شکل ۳-۲۴ کادر محاوره‌ای Name To IP Translations

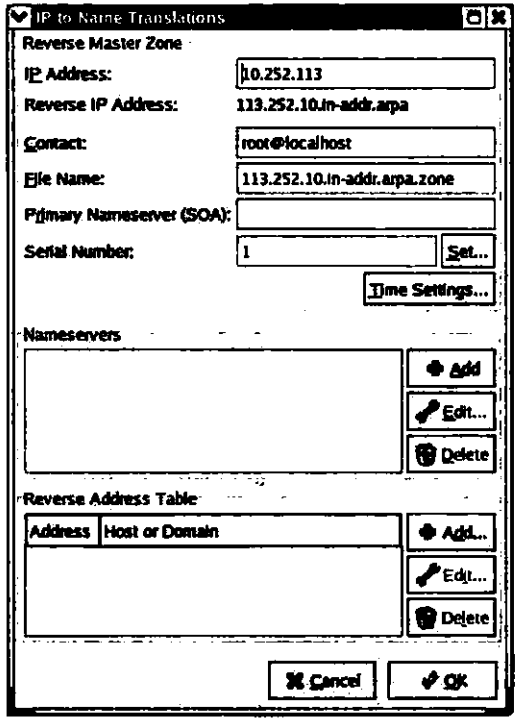
علاوه بر این باید آدرس IP کامپیوتر میزبان سرور DNS را نیز وارد کنید. برای این منظور دکمه Add از کادر محاوره‌ای مزبور را کلیک کنید تا مشابه شکل ۴-۲۴ کادر محاوره‌ای دیگری با عنوان Add a Record باز شود. نام کامپیوتر میزبان سرور DNS را در فیلد متنی Domain Name وارد کنید. هم‌چنین توجه کنید که مابقی نام کامل حوزه در کنار کادر محاوره‌ای مزبور درج شده است. آدرس IP این کامپیوتر را در فیلد متنی Served By وارد کنید. برای دستیابی مجدد به پنجره Domain Name Service دکمه OK را دو بار کلیک کنید.

بار دیگر دکمه New را کلیک کنید تا کادر محاوره‌ای Select a Zone Type باز شود. این بار گزینه Reverse Master Zone از کادر محاوره‌ای مزبور را انتخاب کنید. با این اقدام خواهید دید که عنوان فیلد متنی به صورت IP Address (first 3 Octets) تغییر خواهد کرد. چنان‌که قبلاً نیز اشاره شد، آدرس‌های IPv4 متشکل از چهار عدد هستند که با علامت نقطه از یکدیگر جدا شده‌اند. به هریک از این اعداد اصطلاحاً یک octet گفته می‌شود. در فیلد متنی فوق باید سه octet نخست از آدرس IP

موردنظر را وارد کنید. برای مثال، در صورتی که آدرس IP موردنظر 10.252.113.0 باشد، کافی است در فیلد متنی مورد بحث سه octet نخست یعنی 10.252.113 را درج کرده و دکمه OK را کلیک کنید. با انجام این کار مشابه شکل ۵-۲۴ کادر محاوره‌ای دیگری با عنوان IP To Name Translations باز می‌شود.



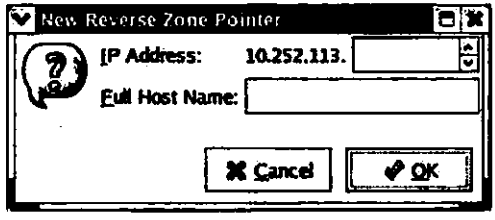
شکل ۴-۲۴ کادر محاوره‌ای Add a Record



شکل ۵-۲۴ کادر محاوره‌ای IP To Name Translations

این بار نیز باید نام کامپیوتر میزبان سرور DNS را در فیلد متنی Primary Nameserver (SOA) درج کنید. هم‌چنین باید دکمه Add از بخش Nameservers را کلیک کرده و دست کم آدرس IP سرور DNS را به لیست موجود اضافه کنید. در صورت لزوم می‌توانید این اقدام را تکرار کرده و آدرس IP سرورهای DNS دیگری را نیز به لیست مزبور اضافه کنید.

دکمه Add از بخش Reverse Address Table را کلیک کنید. با این اقدام مشابه شکل ۶-۲۴ کادر محاوره‌ای دیگری با عنوان New Reverse Zone Pointer باز می‌شود. در فیلدهای متنی IP Address و Full Host Name از این کادرمحاوره‌ای به‌ترتیب آدرس IP و نام یا نام کامل حوزه یکی از کامپیوترهای مستقر در شبکه محلی را وارد کنید.



شکل ۶-۲۴ کادر محاوره‌ای New Reverse Zone Pointer

با تکرار فرآیند فوق آدرس IP و نام یا نام کامل حوزه تمام کامپیوترهای مستقر در شبکه (شامل کامپیوتر میزبانی سرور DNS) را در فیلدهای متنی مربوطه از کادر محاوره‌ای New Reverse Zone Pointer درج کنید. دکمه OK را برای خروج از کادر محاوره‌ای IP To Name Translations و بازگشت به پنجره Domain Name Service کلیک کنید. اکنون عملیات پیکربندی سرور DNS اصلی به پایان رسیده است. برای ذخیره این پیکربندی کافی است دکمه Save از این پنجره را کلیک کنید. با این اقدام مشخصات پیکربندی سرور DNS اصلی در فایل /etc/named.conf و فایل‌های موجود در فهرست /var/named ذخیره می‌شود.

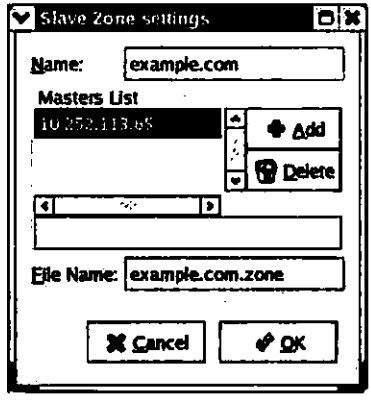
پس از پیکربندی سرور DNS، به شیوه‌ای‌که در قسمت "راه‌اندازی سرور DNS" از همین فصل توضیح خواهیم داد، می‌توانید آن‌را راه‌اندازی کنید. با بهره‌گیری از ابزارگرافیکی redhat-config-bind هم‌چنین می‌توانید سرور DNS نوع Slave را نیز پیکربندی کنید. علاوه بر این، با ویرایش مستقیم فایل‌های پیکربندی مربوطه می‌توانید انواع سرورهای DNS را پیکربندی کنید.

پیکربندی سرور DNS نوع Slave

ابزار گرافیکی redhat-config-bind امکانات لازم برای پیکربندی سرورهای DNS نوع Slave را نیز در اختیار قرار می‌دهد. این نوع سرورهای DNS اغلب روی کامپیوتر دیگری مستقل از کامپیوتر میزبان سرور DNS اصلی مستقر می‌شوند. با وجود این، اطلاعات آن‌ها از بانک اطلاعاتی سرور DNS اصلی تأمین می‌شود.

برای پیکربندی سرور DNS نوع Slave ابتدا برنامه redhat-config-bind را اجرا کرده و سپس دکمه New از پنجره حاصل را کلیک کنید تا کادر محاوره‌ای Select A Zone Type مشابه شکل ۲-۲۴ باز شود. گزینه Slave Zone از این کادر محاوره‌ای را انتخاب کرده و نام حوزه موردنظر خود را در فیلد متنی Domain Name وارد کنید. برای مثال می‌توانید از عنوان example.com استفاده کنید. دکمه Ok را برای ادامه عملیات کلیک کنید.

با این اقدام کادر محاوره‌ای Slave Zone Settings مشابه شکل ۷-۲۴ باز شده و نام حوزه به همراه عنوان فایل حاوی بانک اطلاعاتی موردنظر به طور خودکار در فیلدهای Name و File Name به نمایش درمی‌آید. آدرس IP کامپیوتر میزبان سرور DNS اصلی را در لیست Master List وارد کرده و دکمه Add را کلیک کنید.



شکل ۷-۲۴ کادر محاوره‌ای Slave Zone Settings

فایل‌های پیکربندی سرور DNS

پیکربندی سرورهای DNS از طریق ویرایش فایل /etc/named.conf و فایل‌های موجود در فهرست /var/named انجام می‌شود. ابزار گرافیکی redhat-config-bind کلیه امکانات لازم برای این تنظیمات را در اختیار می‌گذارد. علاوه بر این، در صورت تمایل می‌توان این فایل‌ها را با استفاده از یک ویرایشگر

متنی مستقیماً مورد ویرایش قرار داد. در قسمت‌های بعد محتوای این فایل‌های پیکربندی را بررسی خواهیم کرد.

فایل پیکربندی /etc/named.conf

فایل اصلی پیکربندی سرور DNS فایلی با عنوان /etc/named.conf است. شکل ۸-۲۴ محتوای چنین فایلی را که تنظیمات آن با بهره‌گیری از ابزار گرافیکی redhat-config-bind انجام شده است، نشان می‌دهد. در صورت اطلاع از ساختار این فایل به سادگی می‌توان با استفاده از یک ویرایشگر متنی آن‌را ایجاد کرد. تنظیماتی را که ابزار گرافیکی redhat-config-bind از آن‌ها پشتیبانی به عمل نمی‌آورد، می‌توانید مستقیماً با ویرایش فایل /etc/named.custom انجام دهید.

```
# Generated automatically by redhat-config-bind, alchemist et al.
# Any changes not supported by redhat-config-bind should be put
# in /etc/named.custom
#
controls {
        inet 127.0.0.1 allow { localhost; } keys { rndckey; };
};

include "/etc/named.custom";

include "/etc/rndc.key";


zone  "0.0.127.in-addr.arpa" {
        type master;
        file  "0.0.127.in-addr.arpa.zone";
};
zone  "113.252.10.in-addr.arpa" {
        type master;
        file  "113.252.10.in-addr.arpa.zone";
};


zone  "localhost" {
        type master;
        file  "localhost.zone";
};
zone  "example.com" {
        type master;
        file  "example.com.zone";
};
```

شکل ۸-۲۴ محتوای یک فایل /etc/named.conf

اجازه دهید تنظیمات موجود در این فایل را به طور دقیق مورد بررسی قرار دهیم. این دستورالعمل امکان استفاده از فرمان rndc به منظور مدیریت از سرور DNS را تنها در اختیار کاربران محلی قرار می‌دهد:

```
controls {
      inet 127.0.0.1 allow { localhost; } keys { rndckey; };
};
```

```
};
zone "localhost" {
      type master;
      file "localhost.zone"
};
zone "example.com" {
      type master;
      file "example.com.zone"
};
```

اما این شامل بانک اطلاعاتی تمام اینترنت نمی‌شود. با وجود این، سرور DNS باید به روشی بتواند بانک اطلاعاتی مزبور را مورد دستیابی قرار دهد. فایل /var/named/named.ca را که حاوی این بانک اطلاعاتی است می‌توان در قالب بسته نرم‌افزاری caching-nameserver-* نصب کرد. برای ارسال درخواست‌ها به سرورهای DNS ریشه‌که روی اینترنت مستقر هستند، کافی است این دستورالعمل را به فایل پیکربندی /etc/named.conf ضمیمه کنید:

```
zone "." {
      type hint;
      file "named.ca"
};
```

در صورت استفاده از ابزار گرافیکی redhat-config-bind برای پیکربندی سرور DNS دستورالعمل zone در فایل /etc/named.custom درج خواهد شد.

پیکربندی سرور DNS نوع Slave باید چنان انجام شود که به بانک اطلاعاتی سرور DNS اصلی دسترسی داشته باشد. برای مثال، اگر سرور DNS نوع Slave در شبکه example.com مستقر بوده و آدرس IP کامپیوتر میزبان سرور DNS اصلی 192.168.0.213 باشد، با درج این دستورالعمل در فایل پیکربندی /etc/named.conf می‌توان امکان دستیابی به بانک اطلاعاتی سرور DNS اصلی را برای سرور DNS نوع Slave فراهم کرد:

```
zone "example.com" {
      type slave;
      file "example.com.zone";
      masters {
            192.168.0.213
      }
};
```

در پیکربندی سرور DNS نوع Forwarding باید با استفاده از دستورالعمل options آدرس IP سایر سرورهای DNS (در این‌جا 10.11.12.13، 10.11.12.14 و 10.11.12.15) برای ارسال درخواست‌ها مشخص شود:

```
options {
        directory "/var/named";
        forward only;
        forwarders {
                10.11.12.13;
                10.11.12.14;
                10.11.12.15;
        }
};
```

برای پیکربندی سرور DNS نوع Caching-only نصب بسته نرم‌افزاری caching-nameserver-* ضروری است. فایل پیکربندی /etc/named.conf که به همراه این بسته نرم‌افزاری روی کامپیوتر میزبان نصب می‌شود، برای بسیاری از کاربردها مناسب است. اغلب مکانیزم‌های دیوار آتش انتظار دارند که دستیابی به سرویس DNS تنها از طریق پورت شماره ۵۳ انجام شود. از این‌رو، در صورت وجود چنین مکانیزمی باید علامت // را از ابتدای این خط حذف کنید:

```
// query-source address * port 53
```

با وجود این، از آن‌جا که در نسخه‌های اخیر نرم‌افزار BIND (یعنی نرم‌افزار مرجع برای پیاده‌سازی سرویس DNS در سیستم‌عامل Linux) از پورت‌های مختلف جهت ارسال درخواست استفاده شده است، اقدام فوق ممکن است از ارسال درخواست به سایر سرورهای DNS ممانعت به عمل آورد.

فایل‌های حاوی بانک اطلاعاتی سرور DNS

فایل‌های حاوی بانک اطلاعاتی سرور DNS به طور پیش‌فرض در فهرست /var/named مستقر می‌شوند. تنوع این فایل‌ها به عواملی چون نام حوزه، آدرس IP شبکه میزبان و نوع سرور DNS بستگی دارد. شرح برخی از این فایل‌ها را در جدول ۲-۲۴ مشاهده می‌کنید.

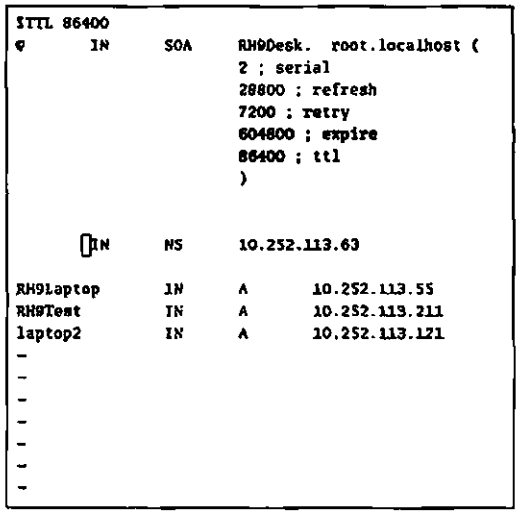
برای روشن شدن موضوع اجازه دهید تا محتوای دو نمونه از این نوع فایل‌ها را مورد بررسی قرار دهیم. شکل ۹-۲۴ محتوای فایل حاوی اطلاعات موردنیاز را برای ترجمه اسامی میزبان شبکه example.com به آدرس‌های IP متناظر با عنوان /var/named/example.com.zone نشان می‌دهد.

جدول ۲-۲۴ شرح برخی از فایل‌های حاوی بانک اطلاعاتی سرور DNS که به طور پیش‌فرض در فهرست var/named/ مستقر می‌شوند.

عنوان فایل	توضیح
0.0.127.in-addr.arpa.zone	این فایل حاوی اطلاعات موردنیاز برای ترجمه آدرس IP کامپیوتر محلی (اصطلاحاً localhost) به نام متناظر با آن است.
netaddr.in-addr.arpa.zone	این فایل حاوی اطلاعات موردنیاز برای ترجمه آدرس‌های IP با اسامی متناظر با آنهاست. متغیر *netaddr* بیانگر سه بخش نخست از آدرس شبکه موردنظر است که به طور معکوس نوشته می‌شود. برای مثال، چنان‌چه آدرس IP شبکه‌ای 192.168.4.0 باشد، عنوان این فایل 4.168.192.in-addr.arpa.zone خواهد بود.
domain.zone	این‌فایل حاوی اطلاعات موردنیاز برای ترجمه‌اسامی کامپیوترها به‌آدرس‌های IP متناظر است. متغیر *domain* بیانگر شبکه میزبان (مانند example.com) است.
localhost.zone	این فایل شامل اطلاعات موردنیاز برای ترجمه نام کامپیوتر محلی (اصطلاحاً localhost) به آدرس IP متناظر است.
named.ca	این فایل شامل اسامی سرورهای DNS اصلی مستقر در اینترنت است که در قالب بسته نرم‌افزاری caching-nameserver-* روی کامپیوتر میزبان نصب می‌شود.
named.local	این فایل حاوی اطلاعات موردنیاز برای ترجمه نام کامپیوتر محلی (اصطلاحاً localhost) به آدرس IP متناظر است.

چنان‌که تصدیق می‌کنید، ساختار این فایل متشکل از تعدادی پارامتر عجیب و غریب است. در این فایل کامپیوتری با نام RH9 از شبکه example.com به عنوان کامپیوتری که وظیفه ترجمه اسامی کامپیوترهای مستقر در شبکه به آدرس‌های IP متناظر را به عهده دارد، معرفی شده است. این شبکه علاوه بر کامپیوتر نامبرده شامل سه کامپیوتر دیگر با عناوین RH9Laptop، RH9Test و laptop2 است. در صورت تمایل می‌توانید با درج پارامترهای مربوطه در فایل مورد بحث انواع دیگری از سرورها را در این شبکه معرفی کنید. برای مثال، با درج این خطوط می‌توان دو سرور mail.example.com و mail2.example.com را جهت پشتیبانی از سرویس پست الکترونیکی یا اصطلاحاً mail server در این شبکه معرفی کرد:

```
MX      10 mail.example.com ; Primary Email Server
MX      20 mail2.example.com ; Secondary Email Server
```



```
$TTL 86400
@       IN      SOA     RH9Desk.  root.localhost (
                        2 ; serial
                        28800 ; refresh
                        7200 ; retry
                        604800 ; expire
                        86400 ; ttl
                        )


        IN      NS      10.252.113.63

RH9Laptop       IN      A       10.252.113.55
RH9Test         IN      A       10.252.113.211
laptop2         IN      A       10.252.113.121
~
~
~
~
~
~
~
```

شکل ۹-۲۴ محتوای فایل /var/named/example.com.zone

در صورت پیکربندی سرویس‌های مختلف روی یک کامپیوتر واحد باید از اسامی مستعار استفاده کنید. برای مثال، با درج این خطوط در فایل مزبور می‌توان یک سرور خبری (اصطلاحاً news server) و یک وب سرور را روی کامپیوتر واحدی با نام مستعار ftp پیکربندی کرد:

```
ftp     IN      A               192.168.0.34
www     IN      CNAME           ftp
news    IN      CNAME           ftp
```

جدول ۳-۲۴ برخی از پارامترهای مورد استفاده در فایل‌های بانک اطلاعاتی سرور DNS را شرح می‌دهد.

جدول ۳-۲۴ شرح پارامترهای مورد استفاده در فایل‌های حاوی بانک اطلاعاتی سرور DNS

عنوان پارامتر	توضیح
$TTL	این پارامتر مدت زمان اعتبار رکوردهای موجود در بانک اطلاعاتی را برحسب ثانیه مشخص می‌کند. با وجود این می‌توان از عباراتی مثل 3D (به عنوان 3 days) و مانند آن نیز استفاده کرد.
@	این پارامتر برای اشاره به مقدار پارامتر origin مورد استفاده قرار می‌گیرد.
IN	این پارامتر بیانگر آن است که ساختار رکوردهای مورد استفاده در فایل جاری مشابه رکوردهای کلاس اینترنت یا اصطلاحاً Internet class data است.

عنوان پارامتر	توضیح
SOA	این پارامتر رکوردی شامل برخی از پارامترهای مهم سرور DNS از جمله serial، refresh و retry است.
root.localhost	این پارامتر که معادل root@localhost است، آدرس پست الکترونیکی مدیر سرور DNS را مشخص می‌کند.
serial	این پارامتر شماره سریالی را که به فایل جاری نسبت داده می‌شود، مشخص می‌کند. به روز رساندن این شماره سریال بعد از هر بار تغییر پیکربندی سرور DNS امری ضروری است، چه در غیر این صورت سایر سرورهای DNS ممکن است از دستیابی به آن محروم شوند.
refresh	چنان‌چه اطلاعات سرور DNS اصلی دستخوش تغییر شود، با استفاده از این پارامتر می‌توان مدت زمانی را مشخص کرد که پس از سپری شدن آن، سرور DNS نوع Slave باید برای ارسال درخواست به سرور DNS اصلی اقدام کند.
retry	اگر تلاش نخست برای ارسال درخواست سرور DNS نوع Slave به سرور DNS اصلی ناموفق باشد، با استفاده از این پارامتر می‌توان مدت زمانی را بر حسب ثانیه مشخص کرد که پس از سپری شدن آن سرور DNS نوع Slave مجدداً می‌تواند برای دستیابی به سرور DNS اصلی اقدام کند.
expire	به کمک این پارامتر می‌توان مدت زمانی را بر حسب ثانیه مشخص کرد که پس از سپری شدن آن هر تلاشی برای دستیابی سرور DNS نوع Slave به سرور DNS باید متوقف شود.
ttl	به کمک این پارامتر می‌توان مدت زمان اعتبار رکورد موردنظر از بانک اطلاعاتی را مشخص کرد.
NS	با استفاده از این پارامتر می‌توان عنوان کامپیوتر میزبان سرور DNS را مشخص کرد.
A	به کمک این پارامتر می‌توان آدرس IP موردنظر را مشخص کرد.
CNAME	به کمک این پارامتر می‌توان نام مستعار سرور موردنظر را مشخص کرد.
MX	با استفاده از این پارامتر می‌توان سرور پست الکت‌ونیکی موردنظر را معرفی کرد.
PTR	به کمک این پارامتر می‌توان نام یک کامپیوتر را به آدرس IP متناظر با آن نسبت داد.

شکل ۱۰-۲۴ نمونه دیگری از فایل بانک اطلاعاتی سرور DNS با نام 113.252.10.in-addr.arpa.zone را نشان می‌دهد. برخلاف فایل قبل، این فایل به منظور ترجمه آدرس‌های IP به اسامی متناظر کامپیوترها مورد استفاده قرار می‌گیرد. چنان‌که مشاهده می‌کنید، در ساختار این فایل از پارامترهای به کار رفته در فایل شکل ۹-۲۴ به ویژه پارامتر PTR استفاده شده است.

```
$TTL 86400
@       IN      SOA     RH9Desk.example.com.    root.localhost (
                        3 ; serial
                        28800 ; refresh
                        7200 ; retry
                        604800 ; expire
                        86400 ; ttk
                        )


@       IN      NS      10.252.113.63.

121     IN      PTR     laptop2.example.com.
122     IN      PTR     laptop3.example.com.
63      IN      PTR     RH9Desk.example.com.
~
~
~
~
~
~
~
```

شکل ۱۰-۲۴ محتوای فایل /var/named/113.252.10.in-addr.arpa.zone

برای دستیابی به آدرس IP متناظر با نام کامپیوتر موردنظر، اطلاع از شماره رکورد PTR مربوطه و البته نام این فایل ضروری است. برای مثال، شماره نخستین رکورد PTR در فایل مورد بحث121 و نام کامل کامپیوتر ثبت شده در این رکورد laptop2.example.com است. با توجه به نام این فایل، یعنی 113.252.10.in-addr.arpa.zone آدرس IP کامپیوتری با عنوان laptop2.example.com چیزی جز 10.242.113.121 نیست.

راه‌اندازی سرور DNS

پس از پیکربندی سرور DNS، می‌توانید برای راه‌اندازی آن اقدام کنید. ساده‌ترین روش برای انجام این کار در سیستم‌عامل Red Hat Linux استفاده از برنامه service است. چنان که به خاطر دارید، شبح named وظیفه سرویس‌دهی‌DNS را در سیستم‌عامل Linux به عهده دارد. از این‌رو، با اجرای این فرمان می‌توانید سرور DNS را راه‌اندازی کنید:

```
# service named start
```

پس از این اقدام باید از صحت عملکرد سرور DNS اطمینان حاصل کنید. چنان‌که در فصل بیست و یکم نیز توضیح داده شد، آدرس IP سرورهای DNS در فایلی با عنوان /etc/resolv.conf درج می‌شود. به محض اجرای سرور DNS می‌توانید نحوه عملکرد آن‌را مورد بررسی قرار دهید. فرمان dig در سیستم‌عامل Linux برای این منظور پیش‌بینی شده است. با استفاده از این فرمان می‌توانید نام کامل

حوزه مورد نظر خود را مورد دستیابی قرار دهید. شکل ۱۱-۲۴ نحوه عملکرد این فرمان را نشان می‌دهد. به خط حاوی واژه SERVER در انتهای خروجی حاصل از این فرمان دقت کنید. این خط بیانگر آن است که درخواست موردنظر از کامپیوتری با آدرس 10.252.113.63 واقع در شبکه محلی برای سرور DNS ارسال شده است.

```
[root@RH9Desk root]# dig www.mommabears.com

; <<>> DiG 9.2.1 <<>> www.mommabears.com
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 64701
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 3, ADDITIONAL: 0

;; QUESTION SECTION:
;www.mommabears.com.            IN      A

;; ANSWER SECTION:
www.mommabears.com.     1685    IN      A       66.36.97.32

;; AUTHORITY SECTION:
mommabears.com.         1685    IN      NS      ns3.hosting4u.net.
mommabears.com.         1685    IN      NS      ns.hosting4u.net.
mommabears.com.         1685    IN      NS      ns2.hosting4u.net.

;; Query time: 262 msec
;; SERVER: 10.252.113.63#53(10.252.113.63)
;; WHEN: Mon Mar  3 18:03:23 2003
;; MSG SIZE  rcvd: 118

[root@RH9Desk root]#
```

شکل ۱۱-۲۴ خروجی فرمان dig

در صورتی که این خروجی مطابق انتظار باشد، باید ترتیبی بدهید که سرویس named طی دفعات آتی راه‌اندازی سیستم‌عامل Linux به طور خودکار راه‌اندازی شود. برای این منظور کافی است فرمان chkconfig --level 235 named را اجرا کنید. این فرمان شبح named را در سطوح اجرایی دوم، سوم و پنجم راه‌اندازی خواهد کرد.

چنان‌چه سرور DNS را ضمن راه‌اندازی سیستم‌عامل Linux راه‌اندازی کنید می‌توانید پیغام‌های مربوط به این فرآیند را که در فایل /var/log/messages به ثبت می‌رسد، مورد توجه قرار دهید. در صورت وجود مشکلاتی نظیر وجود خطاهای دستوری در فایل /etc/named.custom پیغام مربوطه در فایل /var/log/messages به ثبت خواهد رسید.

استفاده از برنامه کلاینت DNS

اگر کامپیوترتان را به منظور اتصال با اینترنت پیکربندی کرده باشید، هم‌اینک به یک برنامه کلاینت DNS دسترسی دارید. تحت این شرایط، هنگامی که برای دستیابی به کامپیوتر دیگری اقدام می‌کنید، در واقع جستجویی را در یک بانک اطلاعاتی از اسامی میزبان‌ها و آدرس‌های IP ترتیب می‌دهید.

چنان‌که در فصل بیست و یکم نیز اشاره شد، دو بانک اطلاعاتی از اسامی میزبان‌ها و آدرس‌های IP موجود است که در قالب فایل‌های /etc/hosts و /etc/resolv.conf (فایل حاوی مشخصات سرورهای DNS) پیکربندی شده‌اند. ترتیب جستجوی این بانک‌های اطلاعاتی در فایل /etc/host.conf مشخص شده است. محتوای این فایل متشکل از یک دستورالعمل ساده با مضمون order hosts,bind است. این دستورالعمل بدان معنی است که جستجوی آدرس‌های IP در فایل /etc/hosts اولویت بالاتری نسبت به جستجوی سرورهای DNS که لیست مشخصات آن‌ها در فایل /etc/resolv.conf موجود است، دارد. در این رابطه هیچ پیکربندی دیگری موردنیاز نیست.

پیکربندی سرور DHCP

سرویس DHCP یا Dynamic Host Configuration Protocol به طور خودکار کلیه اطلاعات موردنیاز برای برقراری ارتباط میان کامپیوترهای مستقر در یک شبکه TCP/IP را در اختیار آن‌ها قرار می‌دهد. این اطلاعات شامل آدرس IP روترها، سرورهای DNS و سایر موارد است.

برای پیکربندی کامپیوتر موردنظر به عنوان یک سرور DHCP، کارت شبکه متصل به آن کامپیوتر باید از نوع multicast باشد. (در صورت وجود کامپیوترهای قدیمی‌تر با سیستم‌عامل Windows باید از آدرس همگانی شبکه به منظور ارسال پیغام استفاده کنید.) تنظیمات مربوط به سرویس DHCP را می‌توان از طریق فایل پیکربندی /etc/dhcp.conf انجام داد. چنان‌چه قصد دارید سرور DHCP را به منظور سرویس‌دهی شبکه‌های راه دور مورد استفاده قرار دهید، باید برنامه‌ای با عنوان dhcrelay را روی کامپیوتری که از آن به عنوان روتر یا دروازه شبکه استفاده می‌کنید، نصب کرده و پیکربندی‌های لازم را انجام دهید. (این برنامه در قالب بسته نرم‌افزاری dhcp-* روی کامپیوتر میزبان نصب می‌شود.) برنامه dhcrelay سرویسی است که به منظور پشتیبانی از پروتکل BOOTP پیاده‌سازی شده است. پیش از هر چیز اجازه دهید به بررسی بسته‌های نرم‌افزاری موردنیاز برای بهره‌برداری از سرویس DHCP بپردازیم.

بسته‌های نرم‌افزاری موردنیاز جهت بهره‌برداری از سرویس DHCP

تمام بسته‌های نرم‌افزاری موردنیاز برای بهره‌برداری از سرویس DHCP به طور پیش‌فرض (یعنی ضمن نصب سیستم‌عامل Linux) روی کامپیوتر میزبان نصب نمی‌شوند. شرح کلیه بسته‌های نرم‌افزاری موردنیاز برای استفاده از سرویس DHCP در جدول ۴-۲۴ آمده است. چنان‌که از فصل دهم و مطالب این فصل به خاطر دارید، با اجرای فرمان rpm -q *packagename* می‌توانید از نصب بسته نرم‌افزاری موردنظر که در این‌جا با متغیر *packagename* مشخص شده است، اطمینان حاصل کنید. هم‌چنین با اجرای فرمان rpm -ql *packagename* می‌توانید فایل‌هایی را که به واسطه نصب بسته نرم‌افزاری موردنظر روی کامپیوتر کپی شده‌اند، مشاهده کنید.

جدول ۴-۲۴ شرح بسته‌های نرم‌افزاری موردنیاز برای بهره‌برداری از سرویس DHCP

عنوان بسته نرم‌افزاری	توضیح
dhcp-*	این بسته نرم‌افزاری حاوی برنامه سرور DHCP است.
dhcp-devel-*	این بسته نرم‌افزاری که نصب آن غیرضروری است، حاوی ابزارهای موردنیاز برای توسعه قابلیت‌های سرویس DHCP است.
dhclient-*	این بسته نرم‌افزاری حاوی برنامه کلاینت DHCP است.

پیکربندی اولیه سرور DHCP

کارت شبکه کامپیوتری با سیستم‌عامل Linux که به عنوان سرور DHCP پیکربندی شده است باید از قابلیت multicast برخوردار بوده و هم‌چنین قابلیت ارسال پیغام به آدرس همگانی شبکه (اصطلاحاً broadcast address) موجود باشد.

پشتیبانی از این قابلیت ممکن است در قالب کارت شبکه تعبیه شده یا این‌که در قالب هسته سیستم‌عامل Linux پیاده‌سازی شده باشد. برای اطلاع از این موضوع فرمان ifconfig را اجرا کنید. با این اقدام اطلاعات مربوط به کارت شبکه یا کارت‌های شبکه متصل به کامپیوتر میزبان به نمایش درمی‌آید. چنان‌چه قابلیت multicast به نوعی پشتیبانی شده باشد باید خط یا خطوطی شبیه به این را در خروجی ملاحظه کنید:

```
UP BROADCAST RUNNING MULTICAST MTU:1500 METRIC:1
```

در صورتی که خط فوق فاقد واژه MULTICAST باشد، باید شبکه میزبان را به منظور پشتیبانی از این قابلیت پیکربندی کنید. برای اطلاع از نحوه انجام این کار به فصل دوازدهم مراجعه کنید.

علاوه بر این، در برخی موارد لازم است یک آدرس همگانی (اصطلاحاً broadcast address) را به منظور ارسال پیغام در نظر بگیرید. برای مثال، در صورت وجود کامپیوترهای قدیمی‌تر با سیستم‌عامل Windows 95 باید از آدرس همگانی شبکه یعنی 255.255.255.255 به منظور ارسال پیغام استفاده کنید، چرا که در غیر این صورت کامپیوترهای مزبور از وجود سرور DHCP در شبکه مطلع نخواهند شد. از این‌رو، در صورتی که شبکه میزبان سرور DHCP شامل چنین کامپیوترهایی باشد، کافی است این فرمان را اجرا کنید: `# route add -host 255.255.255.255 dev eth0`

فایل پیکربندی /etc/dhcpd.conf

در این قسمت به بررسی فایل پیکربندی اصلی سرور DHCP یعنی /etc/dhcpd.conf می‌پردازیم. اجازه دهید این بررسی را با فایل پیکربندی نمونه‌ای با عنوان dhcp.conf.sample که به همراه بسته نرم‌افزاری ***-dhcp روی کامپیوتر میزبان نصب می‌شود، آغاز کنیم. پس از نصب این بسته نرم‌افزاری** فایل مزبور در فهرست /usr/share/doc/dhcp-*versnum* مستقر می‌شود. این فایل نمونه شامل لیستی از آدرس‌های IP است که با توجه تنظیمات شبکه خود باید آن‌ها را تغییر دهید.

با بررسی جزییات این فایل پیکربندی، آشنایی بیشتری با عملکرد سرورهای DHCP پیدا خواهید کرد. از این‌رو اجازه دهید تا محتوای این فایل را خط به خط مورد بررسی قرار دهیم. نخستین خط شیوه به‌روزرسانی سرور DNS توسط سرور DHCP را مشخص می‌کند. عموماً برای این کار از دو روش ad-hoc DNS update mode و interim DHCP-DNS interaction draft update mode یا به اختصار ad-hoc و interim استفاده می‌شود. روش ad-hoc تقریباً منسوخ شده است به طوری که در نسخه‌های جدید سیستم‌عامل Linux غالباً روش interim برای این منظور مورد استفاده قرار می‌گیرد. با این وجود، استفاده از روش interim مستلزم پشتیبانی سرور DNS از قابلیت DDNS یا Dynamic DNS است:

```
ddns-update-style interim;
```

خط دوم از هر گونه تلاش کاربران شبکه برای تغییر اسامی کامپیوترها یا آدرس IP آن‌ها ممانعت به عمل می‌آورد:

```
ignore client-updates;
```

با تغییر خط فوق به صورت allow client-updates می‌توان امکان تغییر اسامی کامپیوترها یا آدرس IP آن‌ها را در اختیار کاربران شبکه قرار داد.

خط بعدی محدوده پیش‌فرض آدرس‌های IP را مشخص می‌کند. برخی از این آدرس‌ها ممکن است در خطوط بعد به کامپیوترهای به خصوصی تخصیص داده شود:

```
subnet 192.168.0.0 netmask 255.255.255.0 {
```

چنان‌چه شبکه میزبان به شبکه دیگری متصل شده باشد، باید آدرس IP دروازه شبکه میزبان به این صورت مشخص شود: `option routers 192.168.0.1;`

خط بعد ماسک شبکه را مشخص می‌کند. عملکرد این خط بسیار ساده بوده و نیازی به توضیح اضافی ندارد: `option subnet-mask 255.255.255.0;`

در صورت استفاده از بانک اطلاعاتی NIS در شبکه می‌توانید حوزه عملکرد آن‌را مشخص کنید. در این‌جا از عنوان فرضی domain.org برای این منظور استفاده کرده‌ایم: (برای اطلاع بیشتر درباره بانک اطلاعاتی NIS به فصل بیست و هشتم مراجعه کنید.)

```
option nis-domain "domain.org";
```

در اغلب موارد شبکه موردنظر نام‌گذاری می‌شود. با توجه به مثال‌هایی که قبلاً در این فصل مورد بررسی قرار دادیم، نام شبکه عنوانی شبیه به example.com است. بار دیگر، در این‌جا از عنوان فرضی domain.org استفاده کرده‌ایم: `option domain-name "domain.org";`

در صورت استفاده از سرور DNS در شبکه باید آدرس آن‌را مشخص کنید تا به این ترتیب سرور DHCP قادر به شناسایی آن بوده و در صورت لزوم اطلاعات آن‌را به روز برساند:

```
option domain-name-servers 192.168.1.1;
```

اقدام مشابهی را می‌توانید در مورد سرور ارسال کننده (option smtp-server) یا دریافت کننده پیغام‌های الکترونیکی (option pop-server)، وب سرور (option www-server) یا سرور مورد استفاده به منظور نگهداری از فایل‌های ثبت وقایع (option log-server) انجام دهید.

خط بعد به منظور تنظیم ساعت شبکه مورد استفاده قرار می‌گیرد. در این مورد، واحد اندازه‌گیری ثانیه بوده و نسبت به ساعت مرجع GMT یا Greenwich Mean Time محاسبه می‌شود. ساعت استاندارد EST یا Eastern Standard Time به میزان ۱۸۰۰۰ ثانیه یا ۵ ساعت عقب‌تر از ساعت استاندارد GMT است. این خط با توجه به ساعت استاندارد EST پیکربندی شده است. چنان‌چه در ناحیه جغرافیایی دیگری مستقر هستید باید این تنظیمات را به طور مناسبی تغییر دهید:

```
option time-offset -18000; #Eastern Standard Time
```

سرعت ساعت تمام کامپیوترها با یکدیگر برابر نیست، به طوری که با کاهش توان باتری یک کامپیوتر ساعت آن نیز کند می‌شود. اگر چندین کامپیوتر در حال اجرای یک فرآیند واحد باشند (برای مثال، برنامه وب سرور روی چندین کامپیوتر از شبکه نصب شده و در حال اجرا باشد) هماهنگ‌سازی ساعت کامپیوترها از اهمیت زیادی برخوردار خواهد بود. این اقدام را می‌توان با بهره‌گیری از یک سرور NTP یا Network Time Protocol انجام داد. (پیکربندی‌این‌سرور بااستفاده‌از ابزارگرافیکی redhat-config-time امکان‌پذیر است.) این خط آدرس IP سرور NTP مستقر در شبکه را مشخص می‌کند:

```
option ntp-servers 192.168.1.1;
```

در صورت تمایل می‌توان کامپیوترهایی با سیستم‌عامل Linux را در شبکه‌های Window پیکربندی کرده و جهت امور مختلف مورد استفاده قرار داد. یکی از سرویس‌های مهم در این گونه شبکه‌ها سرویسی با عنوان WINS یا Windows Internet Naming Service است که بر اساس پروتکل NetBIOS پیاده‌سازی شده است. این خط آدرس IP سرور WINS را مشخص می‌کند:

```
option netbios-name-servers 192.168.1.1;
```

در صورت تمایل می‌توان سرور DHCP را به صورت p-node پیکربندی کرد، به طوری که سرور WINS فایلی از نوع LMHOSTS یا LAN Manager HOSTS را به منظور ترجمه اسامی میزبان‌ها به آدرس‌های IP متناظر با آن‌ها مورد جستجو قرار داده و از انتظار سراسری پیغام (اصطلاحاً broadcast) خودداری کند. این خط امکان مزبور را در اختیار قرار می‌دهد:

```
option netbios-node-type 2;
```

هم‌چنین می‌توان بازه‌ای از آدرس‌های IP را مشخص کرد به طوری که سرور DHCP آدرس‌هایی از این بازه را به کامپیوترهای مستقر در شبکه‌های راه دور تخصیص دهد. بدیهی است آدرس‌های موجود در چنین بازه‌ای باید در محدوده آدرس‌های مجاز این شبکه‌ها باشد. نحوه انجام این کار چنین است:

```
range dynamic-bootp 192.168.0.128 192.168.0.254
```

سرور DHCP آدرس‌های IP را به طور موقت به کامپیوترهای مستقر در شبکه موردنظر تخصیص می‌دهد. اولین مرتبه‌ای که سرور مزبور ممکن است برای تخصیص مجدد آدرس‌های IP اقدام کند به این صورت با استفاده از پارامتر default-lease-time بر حسب ثانیه تعیین می‌شود. برای مثال، با این وجود خط سرور DHCP ممکن است پس از سپری شدن ۲۱۶۰۰ ثانیه (معادل ۶ ساعت) برای تخصیص مجدد آدرس‌های IP اقدام کند: `default-lease-time 21600`

در هر صورت، پس از سپری شدن مدت زمان تعیین شده توسط پارامتر max-lease-time سرور DHCP برای تخصیص مجدد آدرس‌های IP اقدام خواهد کرد. برای مثال، با این وجود خط سرور DHCP پس از سپری شدن ۴۳۲۰۰ ثانیه (معادل ۱۲ ساعت) برای تخصیص مجدد آدرس‌های IP اقدام خواهد کرد: `max-lease-time 43200`

در صورت تمایل می‌توان آدرس IP ثابتی را بر اساس آدرس سخت‌افزاری کارت شبکه کامپیوتر موردنظر به آن تخصیص داد. پارامتر next-server در این تنظیمات به سرور DNS مربوطه (host ns) اشاره دارد:

```
host ns {
        next-server marvin.redhat.com
        hardware ethernet 12:23:34:45:AB:CD
        fixed-address 207.175.42.254
}
```

پس از اعمال تغییرات موردنظر به این فایل آن‌را ذخیره کنید.

راه‌اندازی سرور DHCP

برای راه‌اندازی سرور DHCP روی کامپیوتر مورد نظر، کارت شبکه آن کامپیوتر باید دارای یک آدرس IP معتبر باشد. در غیر این صورت، چنان‌که در فصل بیست و یکم نیز اشاره شد، با استفاده از فرمان ifconfig می‌توانید آدرس IP موردنظر را به آن تخصیص دهید.

راه‌اندازی سرور DHCP فرآیند ساده‌ای است. برای این منظور کافی است فرمان service dhcpd start را اجرا کنید. این فرمان موجب اجرای برنامه dhcpd خواهد شد. به کمک فرمان chkconfig می‌توانید ترتیبی دهید تا سرور DHCP طی راه‌اندازی‌های بعدی سیستم‌عامل Linux در سطح یا سطوح اجرایی موردنظر راه‌اندازی شود.

سرویس DHCP و شبکه‌های راه دور

سرور DHCP برای سرویس‌دهی کامپیوترهای مستقر در یک شبکه راه دور به حمایت نیاز دارد. (در این رابطه به پارامتر dynamic-bootp در قسمت قبل توجه کنید.) دلیل این امر بسیار ساده است. در حالت عادی، دروازه یا روتر بین شبکه‌ها از ارسال پیغام‌های سرور DHCP ممانعت به عمل می‌آورد. در چنین شرایطی است که استفاده از سرویس BOOTP کاملاً مؤثر خواهد بود، چرا که این مکانیزم مسیری را از میان دروازه یا روتر جهت انتقال پیغام‌های ارسالی از سرور DHCP مستقر در یک شبکه به شبکه دیگر باز می‌کند.

برای استفاده از این مکانیزم ابتدا باید برنامه dhcrelay را که در واقع یک شبح است، روی کامپیوتر مورد استفاده به عنوان روتر یا دروازه شبکه نصب کرده و پیکربندی لازم را از طریق فایل /etc/sysconfig/dhcrelay انجام دهید. (این برنامه در قالب بسته نرم‌افزاری dhcp-*- نصب می‌شود.) برای مثال، با درج این خطوط در فایل پیکربندی مزبور برنامه dhcrelay هر دو کارت شبکه eth0 و eth1 را مورد توجه قرار می‌دهد:

```
INTERFACES = "eth0 eth1"
DHCPSERVERS = "192.168.0.213"
```

متغیر DHCPSERVERS باید دست کم با آدرس IP یکی از این کارت‌های شبکه مقداردهی شود. هم‌چنین فراموش نکنید که باید شبح dhcrelay را با اجرای فرمان service dhcrelay start راه‌اندازی کرده و به کمک فرمان chkconfig ترتیبی بدهید تا ضمن راه‌اندازی سیستم‌عامل Linux در سطح یا سطوح اجرایی موردنظر راه‌اندازی شود.

یکی از اشتباهات متداولی که برخی از مدیران سیستم‌ها هنگام ارتباط با سرویس‌دهی DHCP به شبکه‌های راه دور مرتکب می‌شوند، این است که در فایل پیکربندی /etc/sysconfig/dhcrelay تنها کارت‌های متصل به شبکه‌هایی را که نیازمند دریافت سرویس DHCP راه دور هستند، مشخص می‌کنند. این در حالی است که مشخص کردن کارت متصل به شبکه میزبان سرور DHCP در این فایل پیکربندی کاملاً ضروری است.

بانک اطلاعاتی سرویس DHCP

سرور DHCP عملیات آدرس‌دهی کامپیوترهای مستقر در شبکه موردنظر را در قالب یک بانک اطلاعاتی (فایلی با عنوان /var/lib/dhcp/dhcp.lease) ثبت می‌کند. شکل ۱۲-۲۴ محتوای یک چنین فایلی را نشان می‌دهد. چنان‌که در این فایل مشاهده می‌کنید، سرور DHCP در این مورد آدرس 192.168.0.254 را به کارت شبکه‌ای با مشخصه 00:60:08:8d:41:93 و آدرس 192.168.0.253 را به کارت شبکه دیگری با مشخصه 00:10:b5:64:3b:b2 تخصیص داده است.

```
# All times in this file are in UTC (GMT), not your local timezone.   This is
# not a bug, so please don't ask about it.   There is no portable way to
# store leases in the local timezone, so please don't request this as a
# feature.   If this is inconvenient or confusing to you, we sincerely
# apologize.   Seriously, though - don't ask.
# The format of this file is documented in the dhcpd.leases(5) manual page.
# This lease file was written by isc-dhcp-V3.0pl1

lease 192.168.0.254 {
  starts 1 2002/10/14 14:35:09;
  ends 1 2002/10/14 20:35:09;
  binding state active;
  next binding state free;
  hardware ethernet 00:60:08:8d:41:93;
}
lease 192.168.0.253 {
  starts 1 2002/10/14 14:37:59;
  ends 1 2002/10/14 20:37:59;
  binding state active;
  next binding state free;
  hardware ethernet 00:10:b5:64:3b:b2;
}
~
```

شکل ۱۲-۲۴ محتوای یک فایل /var/lib/dhcp/dhcp.lease

پیکربندی کامپیوترهای کلاینت به منظور بهره‌برداری از سرویس DHCP و BOOTP

پیکربندی کامپیوترهای کلاینت بسیار آسان است. برای این منظور کافی است فایل پیکربندی کارت شبکه را برای دستیابی به سرور DHCP مورد ویرایش قرار دهید. با این اقدام، کامپیوتر موردنظر طی راه‌اندازی بعدی درخواستی را به منظور دستیابی به آن سرور DHCP منتشر خواهد کرد.

اما پیش از هر چیز باید از فعال بودن قابلیت دستیابی به شبکه در کامپیوتر موردنظر اطمینان حاصل کنید. با این هدف، فایل پیکربندی /etc/sysconfig/network را باز کنید. با مشاهده این خط می‌توانید از موضوع فوق مطمئن شوید:

```
NETWORKING = yes
```

اکنون فایل پیکربندی کارت شبکه را مورد بازبینی قرار دهید. این فایل معمولاً در فهرست /etc/sysconfig/network-scripts مستقر است. در صورتی که مشخصه کارت شبکه موردنظر eth0 باشد، عنوان این فایل ifcfg-eth0 بوده و باید حاوی این تنظیمات باشد:

```
DEVICE = eth0
BOOTPROTO = dhcp
ONBOOT = yes
```

سایر مقادیر پارامتر BOOTPROTO عبارت از bootp و dialup است. مقدار bootp در صورتی مورد استفاده قرار می‌گیرد که سرور DHCP در یک شبکه راه دور مستقر باشد. مقدار dialup نیز هنگامی مورد استفاده واقع می‌شود که برقراری ارتباط با کامپیوتر میزبان سرور DHCP از طریق شماره‌گیری میسر باشد.

پس از اقدامات فوق، با اجرای برنامه کلاینت dhclient می‌توان امکان دستیابی کامپیوتر موردنظر به سرور DHCP را فراهم کرد. شکل ۱۳-۲۴ نتیجه حاصل از اجرای این فرمان را نشان می‌دهد.

در سال‌های اخیر شرکت Red Hat اسامی برنامه کلاینت مورد استفاده در سیستم‌عامل Red Hat Linux برای دستیابی به سرور DHCP را بارها تغییر داده است. عناوین dhcpcd و pump عناوین برنامه موردنظر در نسخه‌های قبلی این سیستم‌عامل هستند.

```
[root@RH9Test root]# dhclient
Internet Software Consortium DHCP Client V3.0pl1
Copyright 1995-2001 Internet Software Consortium.
All rights reserved.
For info, please visit http://www.isc.org/products/DHCP

Listening on LPF/eth1/00:10:b5:64:3b:b2
Sending on   LPF/eth1/00:10:b5:64:3b:b2
Listening on LPF/lo/
Sending on   LPF/lo/
Listening on LPF/eth0/00:40:f4:3c:05:58
Sending on   LPF/eth0/00:40:f4:3c:05:58
Sending on   Socket/fallback
DHCPDISCOVER on eth1 to 255.255.255.255 port 67 interval 7
DHCPDISCOVER on eth0 to 255.255.255.255 port 67 interval 5
DHCPOFFER from 10.252.113.113
DHCPREQUEST on eth0 to 255.255.255.255 port 67
DHCPACK from 10.252.113.113
bound to 10.252.113.3 -- renewal in 125720 seconds.
[root@RH9Test root]#
```

شکل ۱۳-۲۴ نتیجه اجرای فرمان dhclient برای دستیابی به سرور DHCP

جمع‌بندی

در این فصل با نحوه پیکربندی برنامه‌های کلاینت و سرور موردنیاز برای بهره‌برداری از سرویس‌های DNS و DHCP آشنا شدید. چنان‌که مشاهده کردید، سیستم‌عامل Linux برای برقراری ارتباط با سایر کامپیوترهای مستقر در یک شبکه TCP/IP به شدت وابسته به دو سرور کلیدی DNS و DHCP است.

سرور DNS یک بانک اطلاعاتی شامل اسامی کامل حوزه‌ها (اصطلاحاً FQDN) و آدرس IP متناظر با آن‌هاست. این نوع سرور را می‌توان به یکی از چهار طریق ممکن یعنی Master، Slave، Caching-only یا Forwarding پیکربندی کرد. شرکت Red Hat به استفاده از ابزار گرافیکی redhat-config-bind برای پیکربندی سرور DNS که به معنی ویرایش فایل /etc/named.conf و برخی از فایل‌های موجود در فهرست /var/named است، تأکید دارد. در صورت استفاده از این ابزار برای تنظیمات بیشتر باید فایل /etc/named.custom را نیز به طور دستی مورد ویرایش قرار دهید. پس از پیکربندی سرور DNS، به کمک برنامه شبح named می‌توانید آن‌را راه‌اندازی کنید. برای این منظور کافی است فرمان service named start را اجرا کنید.

در اغلب موارد کامپیوتری که به عنوان کلاینت یا درخواست کننده سرویس DNS مورد استفاده قرار می‌گیرد، به پیکربندی نیاز ندارد. چنین کامپیوتری معمولاً محتوای فایل /etc/hosts را پیش از ارسال درخواست به سرورهای DNS که مشخصات آن از طریق فایل /etc/resolv.conf قابل دستیابی است، مورد بازبینی قرار می‌دهد.

از سوی دیگر، سرور DHCP امکان مدیریت آدرس‌های IP را در شبکه میزبان به سادگی فراهم می‌کند. در صورت تمایل می‌توان اطلاعات مفید دیگری از جمله مشخصات دروازه شبکه، سرورهای DNS، سرورهای NIS و حتی سرورهای SMTP مستقر در شبکه را در قالب فایل پیکربندی این سرور با عنوان /etc/dhcpd.conf مشخص کرد. در صورت برخورداری کامپیوتر میزبان سرور DHCP از یک کارت شبکه و آدرس IP معتبر، با اجرای فرمان service named dhcpd می‌توان سرور مزبور را راه‌اندازی کرد. علاوه بر این، به واسطه سرویس dhcrelay می‌توان راهی را از میان دروازه شبکه میزبان به سایر شبکه‌ها برای ارسال پیغام‌های DHCP باز کرد. پس از پیکربندی سرور DHCP، با اجرای فرمان dhclient می‌توان آدرسی را از آن سرور درخواست کرد. آدرس‌های تخصیص داده شده به این ترتیب در بانک اطلاعاتی /var/lib/dhcp/dhcpd.lease ثبت می‌شوند.

پیکربندی یک کامپیوتر به عنوان کلاینت یا درخواست کننده سرویس DHCP بسیار ساده است. فایل کلیدی مورد استفاده برای این منظور همان فایل پیکربندی کارت شبکه بوده و معمولاً در فهرست /etc/sysconfig/network-scripts مستقر است. چنان‌چه شبکه میزبان از یک سرور DHCP برخوردار باشد، با اجرای فرمان dhclient بلافاصله می‌توان آدرس IP موردنیاز را درخواست کرد.

در فصل بعد دو سرویس چاپ متداول در سیستم‌عامل Linux با عناوین Common Unix Print System یا CUPS و Line Print Daemon یا LPD را مورد بررسی قرار خواهیم داد.

فصل بیست‌وپنجم

بهره‌برداری از سرویس‌های چاپ CUPS و LPD در سیستم‌عامل Linux

سیستم‌عامل Red Hat Linux به خودی خود قادر به شناسایی چاپگر متصل به کامپیوتر میزبان یا مستقر در شبکه نیست. از این‌رو، اطلاع از نحوه پیکربندی چاپگر برای مدیران این گونه سیستم‌ها کاملاً ضروری است.

سیستم عامل Red Hat Linux دو سرویس چاپ CUPS و LPD را مورد پشتیبانی قرار می‌دهد، که در این میان سرویس CUPS یا Common Unix Print System سرویس چاپ پیش‌فرض محسوب می‌شود. با وجود این، سرویس LPD یا Line Print Daemon تا پیش از انتشار سیستم‌عامل Red Hat Linux 9 سرویس چاپ پیش‌فرض محسوب می‌شد. شرکت Red Hat با توسعه نرم‌افزارهایی موفق شده است فرامین و برنامه‌های کاربردی موردنیاز برای بهره‌برداری از سرویس چاپ LPD را با سرویس چاپ CUPS تطبیق دهد.

سرویس چاپ CUPS که بر اساس نسخه شماره 1.1 از پروتکل IPP یا Internet Print Protocol توسعه یافته است، امکانات لازم برای سازمان‌دهی چاپگرهای مستقر در شبکه‌ها را در قالب گروه‌های مختلف فراهم می‌کند. در ادبیات مربوط به سرویس چاپ CUPS معمولاً از واژه "کلاس" برای اشاره به هریک از این گروه‌ها استفاده می‌شود. پیکربندی این سرویس از طریق وب امکان‌پذیر است. ضمناً سرویس مزبور را می‌توان برای چاپگر محلی نیز مورد استفاده قرار داد.

به واسطه امکانات سرویس چاپ CUPS به سادگی می‌توان سازمان‌دهی تعداد زیادی چاپگر را از طریق وب انجام داد. با وجود این، اطلاع از محتوای فایل‌های پیکربندی مربوطه که در فهرست /etc/cups مستقر هستند، کمک شایانی را در اختیار قرار خواهد داد. محتوای این فایل‌ها شباهت زیادی به محتوای فایل‌های پیکربندی وب سرور Apache دارد که در فصل سی‌ام آن‌را مورد بررسی قرار خواهیم داد.

در مقابل، سرویس چاپ LPD که نخستین بار در سیستم‌عامل BSD معرفی شد، برای شبکه‌های کوچکی که تنها یک چاپگر در آن‌ها مستقر شده، مناسب است. شرکت Red Hat در نسخه‌های بعدی سیستم‌عامل خود از سرویس چاپ LPD پشتیبانی نخواهد کرد.

هر دو سیستم‌عامل BSD و Linux از خانواده Unix محسوب می‌شوند. (اصطلاح BSD کوتاه شده عبارت Berkeley Standard Distribution است.)

با وجود امکانات سرویس چاپ CUPS بهره‌برداری از برنامه‌های کاربردی طراحی شده به منظور استفاده از سرویس چاپ LPD کاملاً امکان‌پذیر است. اگر قبلاً از فرامین سرویس چاپ LPD به طور جدی استفاده می‌کردید، اکنون می‌توانید بهره‌برداری از سرویس چاپ CUPS را نیز موردنظر قرار دهید. سرویس چاپ CUPS به واسطه یکی از سرویس‌های xinetd به خوبی امکان استفاده از فرامین سرویس چاپ LPD شامل lpr و lpq را در اختیار می‌گذارد. بدیهی است برای بهره‌برداری از سرویس چاپ موردنظر باید بسته نرم‌افزاری مربوطه را نصب کرده و پیکربندی لازم را انجام دهید. چنان‌چه از سرویس چاپ CUPS استفاده می‌کنید، برای بهره‌برداری از فرامین سرویس چاپ LPD باید شبح cups-lpd را نیز فعال کنید. موضوعات مورد بررسی در فصل حاضر به این قرار است:

- بهره‌برداری از پروتکل IPP یا Internet Print Protocol
- استفاده از سرویس چاپ CUPS یا Common Unix Print System
- استفاده از سرویس چاپ LPD یا Line Print Daemon

بهره‌برداری از پروتکل IPP یا Internet Print Protocol

در گذشته روش چندان منسجمی برای انجام کارهای چاپی در سیستم‌های Unix و سیستم‌های مشابه مانند Linux وجود نداشت، به طوری که شرکت‌هایی مانند AT&T، HP و Sun که هریک نسخه‌ای از سیستم‌عامل Unix را توسعه داده بودند، روش‌های به خصوصی را نیز برای انجام امور چاپی در این سیستم‌ها تعبیه کرده بودند. نرم‌افزارهای موردنیاز برای پشتیبانی از امور چاپی در سیستم‌عامل Linux بر اساس سرویس LPD یا Line Print Protocol پیاده‌سازی شد. این وضعیت به مرور زمان تغییر کرده و پروتکل IPP یا Internet Print Protocol به عنوان یک استاندارد منسجم در این زمینه به مقبولیت چشمگیری دست یافت.

سرویس چاپ CUPS یکی از دستاوردهای این استاندارد است که امروزه به طور گسترده در سیستم‌عامل‌ها Unix و Linux مورد بهره‌برداری قرار می‌گیرد. این سرویس به طور مشترک توسط

شرکت‌های Novell و Xerox توسعه یافت. در انجام این کار چهار هدف اصلی به این شرح موردنظر قرار گرفت:

- شناسایی چاپگرهای قابل استفاده در شبکه
- ارسال امور چاپی به چاپگر مورد نظر
- بازبینی وضعیت امور چاپی
- لغو امور چاپی مورد نظر

سرویس چاپ CUPS امکان ارسال امور چاپی به چاپگر موردنظر را به واسطه تعیین آدرس URI آن چاپگر (هم‌چون parallel: /dev/lp0) در اختیار قرار می‌دهد.

اصطلاح URI کوتاه شده عبارت Uniform Resource Identifier است. به احتمال قوی تاکنون بارها با اصطلاح URL (کوتاه شده عبارت Uniform Resource Locator) برخورد کرده‌اید. در حالی که هر دو اصطلاح به قالب خاصی از آدرس‌ها اشاره دارند، آدرس‌های URL نوع به خصوصی از آدرس‌های URI محسوب می‌شوند. چنان‌که می‌دانید، آدرس‌های URL در مرورگرهای وب یا web browsers جهت دستیابی به سایت‌هایی چون ftp://ftp.redhat.com یا http://www.bsd.org مورد استفاده قرار می‌گیرند. حوزه کاربرد آدرس‌های URI نسبت به URL وسیع‌تر است. برای مثال، سه آدرس mailto:abc@def.ghi، smb://comp1/printername و parallel:/dev/lp1 از نوع آدرس‌های URI هستند.

چنان‌که گفته شد، سرویس چاپ CUPS حاصل توسعه پروتکلی با عنوان IPP است. جدول ۱-۲۵ تعدادی از فرامین استاندارد مورد استفاده در این سرویس چاپ را شرح می‌دهد. (در صورت استفاده از سرویس چاپ LPD انتظار می‌رود که با این فرامین آشنایی داشته باشید.) برای مشاهده لیست کامل این فرامین به وب سایت توسعه دهندگان سرویس CUPS یعنی Easy Software Products در آدرس http://www.easysw.com مراجعه کنید.

جدول ۱-۲۵ شرح برخی از فرامین مورد استفاده در سرویس چاپ CUPS

عنوان فرمان	توضیح
Print	این فرمان فایلی را جهت چاپ به چاپگری با آدرس URI مشخص ارسال می‌کند.
Validate	این فرمان در مورد صحت یک وظیفه چاپی از نظر اولویت چاپ، چاپگر مناسب و مواردی از این قبیل اطمینان می‌دهد.

عنوان فرمان	توضیح
Create	این فرمان یک وظیفه چاپی تهی ایجاد می‌کند، به نحوی که هیچ سندی برای چاپ به چاپگر ارسال نمی‌شود.
Send	این فرمان فایلی را به عنوان یک وظیفه چاپی جهت پردازش به چاپگر ارسال می‌کند.
Cancel	این فرمان وظیفه چاپی موردنظر را لغو می‌کند.
Pause	این فرمان عملیات چاپ را موقتاً متوقف می‌کند.
Resume	این فرمان موجب ادامه عملیات چاپ می‌شود.
Purge	این فرمان کلیه وظایف چاپی را لغو می‌کند.

علاوه بر این، سرویس چاپ CUPS فرامین مدیریتی دیگری را نیز در اختیار قرار می‌دهد. شرح برخی از این فرامین در جدول ۲-۲۵ آمده است. برای مشاهده لیست کامل این فرامین به وب سایت توسعه دهندگان سرویس CUPS مراجعه کنید.

جدول ۲-۲۵ شرح برخی از فرامین مدیریتی سرویس چاپ CUPS

عنوان فرمان	توضیح
CUPS-Get-Default	این فرمان آدرس URI چاپگر پیش‌فرض را در اختیار می‌گذارد.
CUPS-Get-Printers	این فرمان آدرس URI کلیه چاپگرهای پیکربندی شده در شبکه به منظور سرویس‌دهی توسط سرویس چاپ CUPS را در اختیار قرار می‌دهد.
CUPS-Add-Modify-Printers	این فرمان چاپگر جدیدی را به جمع چاپگرهای موجود اضافه کرده یا مشخصات یکی از چاپگرهای موجود را تغییر می‌دهد.
CUPS-Delete-Printer	این‌فرمان چاپگر موردنظر را ازکلاس چاپگرهای CUPS موجود حذف می‌کند.
CUPS-Get-Classes	این فرمان نوع چاپگرهای موجود در هریک از کلاس‌های CUPS را مشخص می‌کند.
CUPS-Add-Modify-Classes	این فرمان کلاس چاپگر جدیدی را به جمع کلاس‌های موجود اضافه کرده یا مشخصات یکی از کلاس‌های موجود را تغییر می‌دهد.
CUPS-Delete-Class	این فرمان کلاس چاپگر موردنظر را حذف می‌کند.
CUPS-Accept-Jobs	این‌فرمان چاپگر یا کلاس‌چاپگرموردنظر را وادار به‌قبول وظایف چاپی می‌کند.
CUPS-Reject-Jobs	این فرمان چاپگر یا کلاس چاپگر موردنظر را وادار به رد وظایف چاپی می‌کند.

با اطلاع از جزییات فوق اکنون می‌توانیم به نحوه پیکربندی سرویس چاپ CUPS روی کامپیوتر یا شبکه موردنظر بپردازیم.

پیکربندی سرویس چاپ CUPS

پیکربندی سرویس چاپ CUPS یا Common Unix Print System در بسیاری موارد، فرآیند ساده‌ای است. به شرط نصب بسته‌های نرم‌افزاری مربوطه، سرویس CUPS به عنوان سرویس چاپ پیش‌فرض ممکن است هم‌اینک روی کامپیوتر شما فعال شده باشد. برخی از فرامین سرویس چاپ LPD را می‌توان هنگام استفاده از چاپگرهای CUPS نیز مورد بهره‌برداری قرار داد. البته برای این منظور باید یکی از سرویس‌های xinetd با عنوان cups-lpd را روی کامپیوتر موردنظر نصب کنید.

پیکربندی چاپگرهای CUPS از طریق وب کاملاً امکان‌پذیر است. سرویس چاپ CUPS از طریق پورت TCP/IP شماره ۶۳۱ یعنی پورت مربوط به پروتکل IPP قابل دستیابی است. با وجود این، برای پیکربندی مجموعه‌ای از چاپگرهای CUPS باید با نحوه ویرایش فایل‌های پیکربندی سرویس چاپ CUPS واقع در فهرست /etc/cups آشنا باشید.

برای شروع ابتدا از نصب بسته‌های نرم‌افزاری موردنیاز برای بهره‌برداری از سرویس چاپ CUPS اطلاع حاصل کنید. جدول ۳-۲۵ این بسته‌های نرم‌افزاری را شرح می‌دهد.

جدول ۳-۲۵ شرح بسته‌های نرم‌افزاری موردنیاز برای بهره‌برداری از سرویس چاپ CUPS

عنوان بسته نرم‌افزاری	توضیح
cups-*	این بسته نرم‌افزاری حاوی فایل‌های اصلی موردنیاز برای بهره‌برداری از سرویس چاپ CUPS شامل فرامین اصلی و فایل‌های پیکربندی پیش‌فرض است.
cups-libs-*	این بسته نرم‌افزاری امکان استفاده از فرامین سرویس چاپ CUPS را بدون نیاز به استفاده از فرامین سرویس چاپ LPD مانند lpr در اختیار می‌گذارد.
cups-devel-*	این بسته نرم‌افزاری حاوی فایل‌های موردنیاز برای توسعه قابلیت‌های سرویس چاپ CUPS است.
cups-drivers-*	این بسته نرم‌افزاری حاوی درایورهای موردنیاز برای استفاده از چاپگرهای CUPS است. برای دستیابی به این درایورها ممکن است مجبور باشید تا به منابعی مانند وب سایت http://www.rpmfind.net مراجعه کنید. ضمناً بسته نرم‌افزاری redhat-config-printer-* خود شامل مجموعه‌ای از درایورهاست.

عنوان بسته نرم‌افزاری	توضیح
foomatic-*	این بسته نرم‌افزاری حاوی یک بانک اطلاعاتی از چاپگرها بوده و به منظور پشتیبانی از ابزار گرافیکی redhat-config-printer موردنیاز است.
hpijs-*	این بسته نرم‌افزاری حاوی درایور چاپگرهای HP است.

در قسمت‌های بعد ابتدا امکانات موجود برای پیکربندی سرویس چاپ CUPS از طریق وب را مورد بررسی قرار داده و سپس به بررسی فایل‌های پیکربندی این سرویس که پس از نصب بسته‌های نرم‌افزاری مربوطه در فهرست /etc/cups مستقر می‌شوند، خواهیم پرداخت. در انتها نیز فرامین سرویس چاپ CUPS و هم‌چنین سرویس cups-lpd را که امکان استفاده از فرامین سرویس چاپ LPD را فراهم می‌کند، مورد بررسی قرار خواهیم داد.

اسامی فایل‌های مربوط به سرویس چاپ CUPS، برنامه‌های شبح و هم‌چنین برنامه‌های اجرایی مربوطه ممکن است تا اندازه‌ای گمراه کننده باشد. شبح مربوط به سرویس چاپ CUPS با عنوان cupsd در فهرست /usr/sbin واقع شده است. با وجود این، برای راه‌اندازی این سرویس در سیستم‌عامل Red HatLinux کافی است برنامه cups واقع در فهرست /etc/rc.d/init.d را اجرا کنید. ضمناً فایل پیکربندی سرویس مورد بحث با عنوان cupsd.conf در فهرست /etc/cups مستقر است.

امکانات گرافیکی موجود برای پیکربندی چاپگرهای CUPS

پیکربندی چاپگرهای CUPS از طریق وب امکان‌پذیر است. در حال حاضر ممکن است بسته‌های نرم‌افزاری موردنیاز برای استفاده از سرویس چاپ CUPS روی کامپیوترتان نصب شده و سرویس cupsd نیز راه‌اندازی شده باشد. تحت چنین شرایطی برای بهره‌برداری از سرویس مزبور کافی است پورت TCP/IP شماره ۶۳۱ را با استفاده از مرورگر وب (هم‌چون برنامه Mozilla) مورد دستیابی قرار دهید.

در صورت نیاز می‌توانید با استفاده از مرورگر وب برنامه پیکربندی سرویس چاپ CUPS را که روی یک کامپیوتر راه دور مستقر است، اجرا کنید. بدیهی است برای انجام چنین اقدامی هیچ مکانیزم بازدارنده‌ای نباید از دسترسی به پورت TCP/IP شماره ۶۳۱ ممانعت به عمل آورد. هر چند اقدام فوق را توصیه نمی‌کنیم، اما به دلایلی ممکن است انجام این کار قابل قبول باشد.

تغییر سرویس چاپ پیش‌فرض از LPD به CUPS

در صورت استفاده از سیستم‌عامل Red Hat Linux 8 یا نسخه‌های قدیمی‌تر، به احتمال قوی سرویس LPD به عنوان سرویس چاپ پیش‌فرض پیکربندی شده است. با ارتقای این سیستم‌عامل به نسخه جدیدتر مانند Red Hat Linux 9 سرویس چاپ پیش‌فرض از LPD به CUPS ارتقا نمی‌یابد. به بیان دیگر، سرویس LPD هم‌چنان به عنوان سرویس چاپ پیش‌فرض باقی می‌ماند.

برای جایگزین کردن سرویس مزبور با سرویس CUPS به عنوان چاپ پیش‌فرض، ابتدا باید ترتیبی دهید که شبح lpd هنگام راه‌اندازی سیستم‌عامل Linux راه‌اندازی نشود. سپس باید امکان راه‌اندازی سرویس cupsd را در سطح یا سطوح اجرایی موردنظر فراهم کنید. (فایل مربوط به سرویس cupsd در فهرست /usr/sbin واقع شده است.) با اجرای این فرامین می‌توانید اقدامات فوق را انجام دهید:

```
# chkconfig --level 2345 lpd off
# chkconfig --level 2345 cups on
```

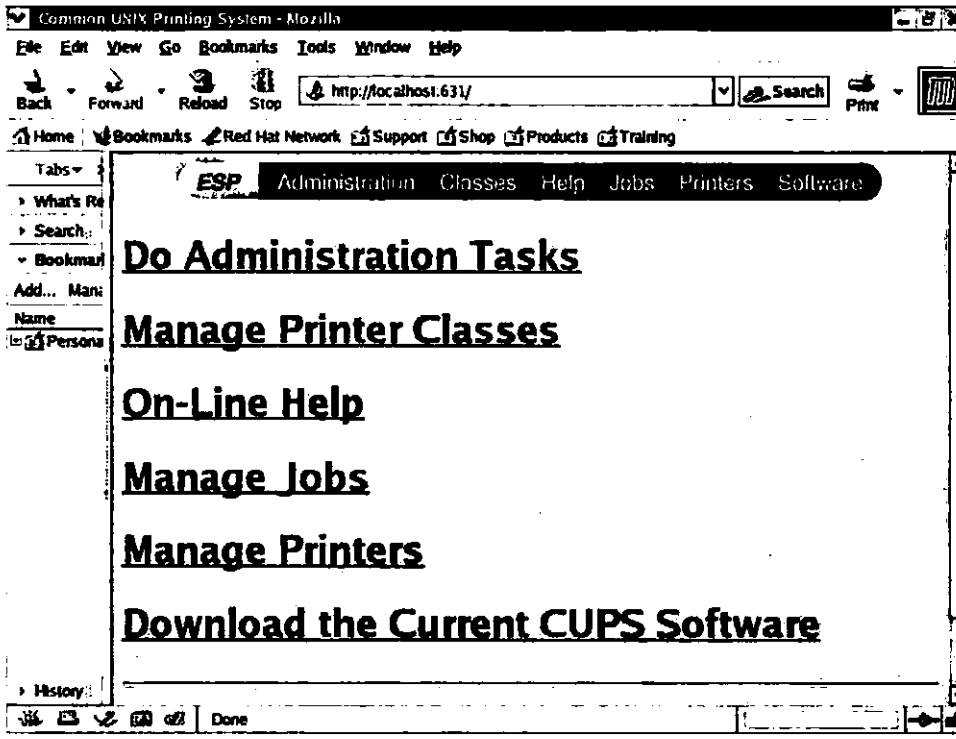
پس از اجرای این فرامین، برای بهره‌برداری از چاپگرهای CUPS باید برنامه redhat-switch-printer را به منظور جایگزینی سرویس چاپ CUPS با LPD اجرا کنید. (گاهی اوقات برای اشاره به سرویس LPD از عنوان بسته نرم‌افزاری مربوطه یعنی LPRng یا Line Print Request, next generation استفاده می‌شود.)

اکنون آدرس http://localhost:631 را در نوار آدرس مرورگر وب مورد نظرتان وارد کرده و کلید Enter را فشار دهید. شکل ۱-۲۵ نتیجه این اقدام را در مرورگر Mozilla نشان می‌دهد.

پس از اقدام فوق، در صورت نمایش این پیغام مطمئن شوید که شبح cupsd راه‌اندازی شده و هیچ مکانیزم بازدارنده‌ای از دستیابی به پورت TCP/IP شماره ۶۳۱ ممانعت به عمل نمی‌آورد:

```
The connection was refused when attempting to contact
servername:631
```

چنان‌که در این شکل مشاهده می‌کنید، برای پیکربندی سرویس CUPS گزینه‌های متعددی پیش‌بینی شده است. گزینه ESP در بالای این صفحه امکان برقراری ارتباط با توسعه دهندگان سرویس CUPS در شرکت Easy Software Products (به آدرس http://www.easysw.com) را فراهم می‌کند. شرح این گزینه‌ها در جدول ۴-۲۵ آمده است.



شکل ۱-۲۵ امکانات پیکربندی سرویس چاپ CUPS

جدول ۴-۲۵ شرح گزینه‌های منوی پیکربندی سرویس چاپ CUPS

عنوان گزینه	توضیح
ESP	این گزینه امکان دستیابی به وب سایت http://www.easysw.com را فراهم می‌کند.
Do Administration Tasks	این گزینه امکان مدیریت چاپگرها، کلاس‌ها و وظایف چاپی را در اختیار می‌گذارد.
Manage Printer Classes	این گزینه امکان مدیریت مجموعه‌ای از چاپگرها را در قالب یک کلاس فراهم می‌کند.
On-Line Help	این گزینه امکان دستیابی به مستندات سرویس CUPS را فراهم می‌کند. این مستندات در دو قالب HTML و PDF قابل دستیابی است.
Manage Jobs	این گزینه امکان مدیریت وظایف چاپی جاری را در اختیار می‌گذارد.
Manage Printers	این گزینه امکان مدیریت چاپگرها را در فراهم می‌کند.

عنوان گزینه	توضیح
Download The Current CUPS Software	این گزینه امکان دستیابی به وب سایت http://www.cups.org (جدیدترین نسخه نرم‌افزاری CUPS را در اختیار قرار می‌دهد.)

از آن‌جا که گزینه Administration کلیه امکانات موردنیاز برای پیکربندی را در اختیار قرار می‌دهد، گزینه‌های فوق را به ترتیب معکوس بررسی می‌کنیم تا به این ترتیب از تکرار مطالب جلوگیری به عمل آید.

پیش از هر اقدامی از کلیه فایل‌های موجود در فهرست /etc/cups نسخه پشتیبان تهیه کنید، چرا که به نسخه اصلی این فایل‌ها در قسمت‌های بعدی همین فصل نیاز داریم.

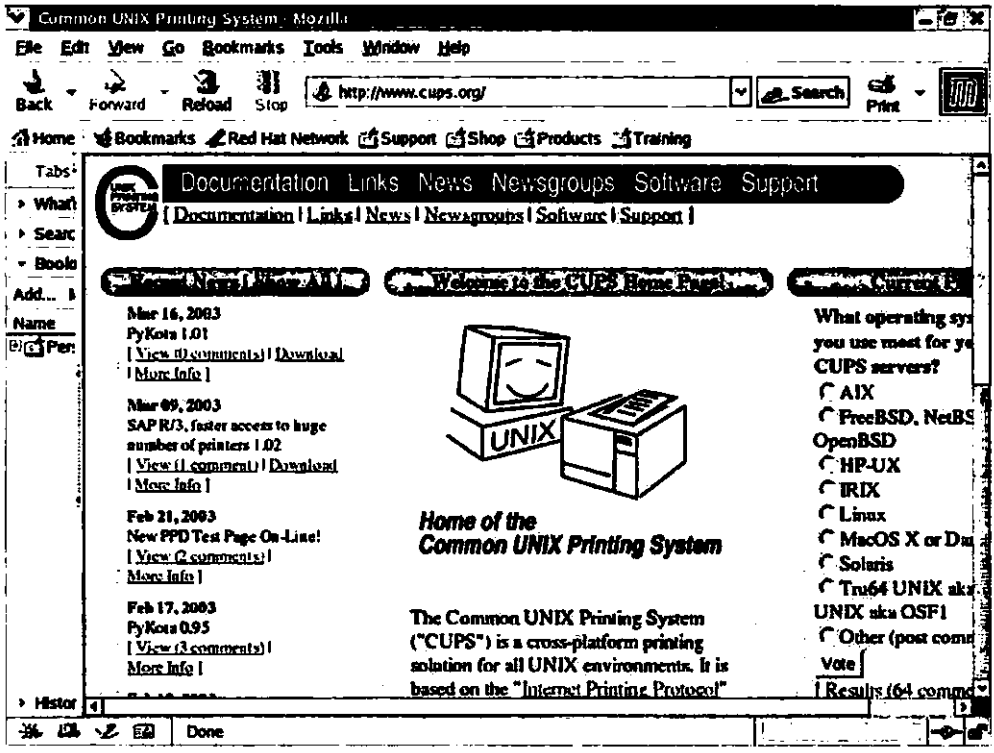
ابزار گرافیکی redhat-config-printer که در همین فصل به بررسی آن خواهیم پرداخت امکانات لازم برای پیکربندی چاپگرها را در اختیار قرار می‌دهد. اگر در عین حال تنها یکی از برنامه‌های شبح cupsd یا lpd فعال شده باشد، ابزار گرافیکی مزبور را می‌توان برای پیکربندی چاپگرها به همراه دو سرویس چاپ CUPS یا LPD مورد استفاده قرار داد.

ابزار گرافیکی redhat-config-printer دسترسی بسیار آسانی را به مجموعه متنوعی از درایور چاپگرها که بر اساس مدل و شرکت سازنده طبقه‌بندی شده‌اند، فراهم می‌کند.

دستیابی به نرم‌افزار CUPS

برای دستیابی به جدیدترین نسخه نرم‌افزار CUPS کافی است به وب سایت مربوطه در آدرس http://www.cups.org مراجعه کنید. شکل ۲-۲۵ صفحه آغازین این وب سایت را نشان می‌دهد. تا زمان انتشار کتاب حاضر، وب سایت مزبور تنها امکان دستیابی به نسخه tarball این نرم‌افزار را فراهم می‌کند. به بیان دیگر، در این وب سایت هیچ نسخه خاصی از نرم‌افزار CUPS برای سیستم‌عامل Red Hat Linux منتشر نشده است.

پشتیبانی از وب سایت http://www.cups.org به عهده شرکت Easy Software Products است. آدرس وب سایت این شرکت http://www.easysw.com است. با وجود این، نرم‌افزار CUPS از نوع کد باز بوده و تحت لیسانس GPL منتشر می‌شود.



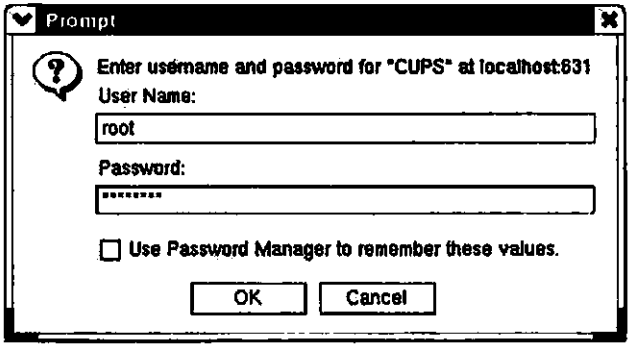
شکل ۲-۲۵ صفحه آغازین وب سایت CUPS به آدرس http://www.cups.org

از این‌رو، در صورت استفاده از سیستم‌عامل Red Hat Linux بهتر است برای دریافت جدیدترین نسخه نرم‌افزار CUPS سرور FTP این شرکت را مورد دستیابی قرار دهید. چنان‌که در فصل دهم نیز توضیح داده شد، در صورت استفاده از سیستم‌عامل Red Hat Linux جهت دستیابی به جدیدترین نسخه نرم‌افزار CUPS می‌توانید به بانک‌اطلاعاتی Rawhide مراجعه کرده یا ابزار up2date را مورد بهره‌برداری قرار دهید.

مدیریت چاپگرها

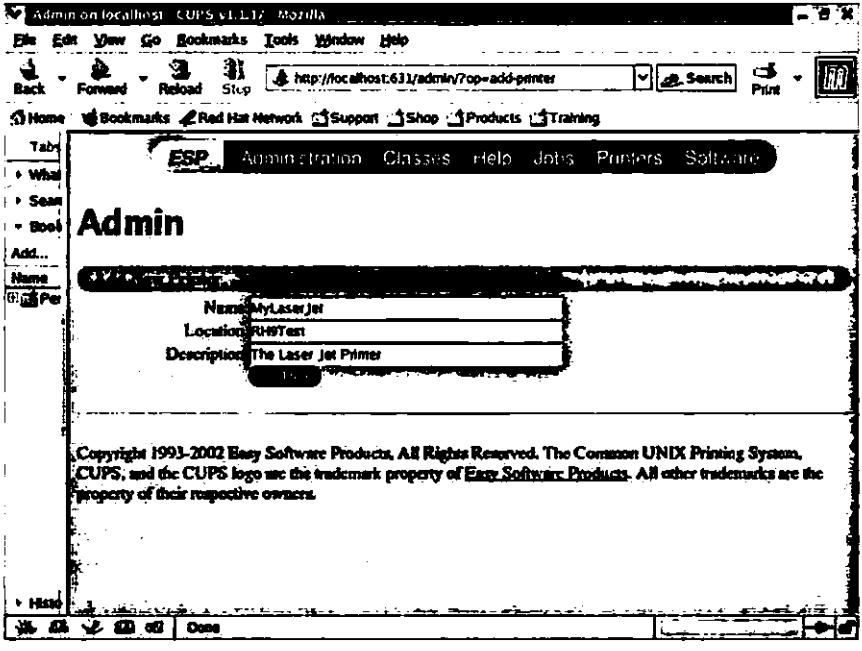
هر دو پیوند Printers و Manage Printers امکانات لازم برای مدیریت چاپگرها را در اختیار قرار می‌دهد. با کلیک یکی از این دو پیوند، لیستی از چاپگرهایی که هم‌اینک پیکربندی شده‌اند، به نمایش درمی‌آید. برای اضافه کردن یک چاپگر جدید به این لیست، دکمه Add Printer را کلیک کنید. حتی اگر در ابتدا با عنوان کاربر اصلی برای ورود به سیستم اقدام کرده باشید، باید شناسه کاربری و کلمه

عبور موردنیاز برای مدیریت چاپگرها را در فیلدهای مربوطه از کادر محاوره‌ای Prompt وارد کنید. شکل ۳-۲۵ این کادر محاوره‌ای را نشان می‌دهد.



شکل ۳-۲۵ کادر محاوره‌ای Prompt امکان دریافت

پس از وارد کردن شناسه کاربری و کلمه عبور معتبر در کادر محاوره‌ای Prompt و کلیک روی دکمه OK از این کادر محاوره‌ای، مطابق شکل ۴-۲۵ صفحه‌ای شامل امکانات لازم برای اضافه کردن چاپگر جدید به نمایش درمی‌آید.



شکل ۳-۲۵ تعیین مشخصات چاپگر جدید

در این صفحه باید نام، موقعیت و توضیح مختصری درباره چاپگر جدید را در فیلدهای متنی مربوطه وارد کنید. شرح این فیلدها در جدول ۵-۲۵ آمده است.

جدول ۵-۲۵ شرح فیلدهای مربوط به اضافه کردن چاپگر جدید

عنوان فیلد متنی	توضیح
Name	محتوای این فیلد عنوان چاپگر جدید را مشخص می‌کند.
Location	محتوای این فیلد عنوان کامپیوتر میزبان یا حوزه میزبان چاپگر جدید مانند RH81Test یا HPLaser.mommabears.com را مشخص می‌کند.
Description	محتوای این فیلد توصیف دلخواهی درباره چاپگر جدید را مشخص می‌کند. برای مثال می‌توان موقعیت فیزیکی چاپگر جدید را در این فیلد وارد کرد.

پس از وارد کردن مقادیر موردنظر در این فیلدها دکمه Continue را کلیک کنید.

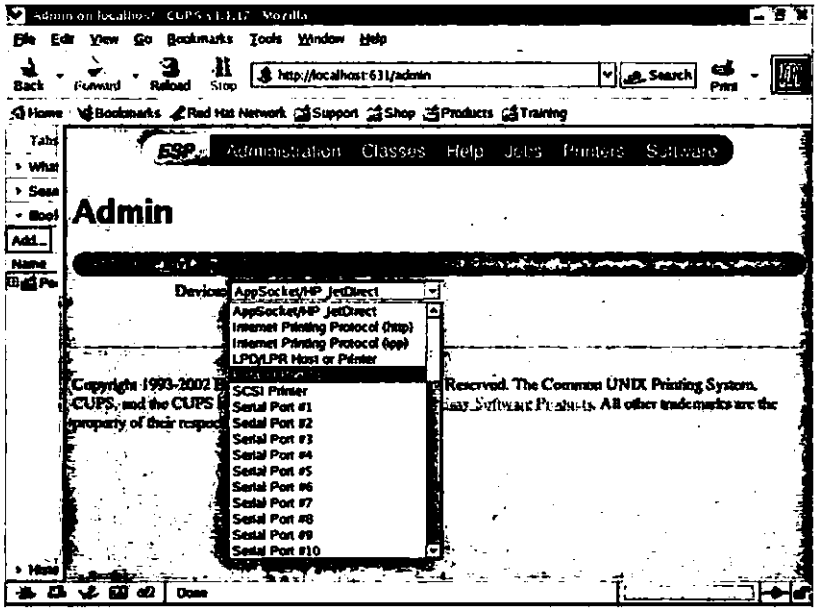
تعیین مشخصات چاپگر

با اقدام اخیر صفحه‌ای مطابق شکل ۵-۲۵ به نمایش درمی‌آید. چنان‌که مشاهده می‌کنید، این صفحه شامل لیستی از مشخصات چاپگر است. نرم‌افزار CUPS قادر است از چاپگرهای متصل به پورت‌های فیزیکی یا سرورهای مختلف بهره‌برداری کند. شرح برخی از گزینه‌های موجود در این زمینه که از طریق منوی Device قابل دستیابی است، در جدول ۶-۲۵ آمده است.

جدول ۶-۲۵ شرح برخی از گزینه‌های منوی Device

عنوان گزینه	توضیح
AppSocket/HP JetDirect	این گزینه را در صورتی انتخاب کنید که چاپگر موردنظر به یک سرور چاپ از نوع Hewlett-Packard JetDirect متصل باشد.
Internet Printing Protocol (http)	اگر نرم‌افزار CUPS از طریق پورت TCP/IP شماره ۸۰ با چاپگر موردنظر در ارتباط است، این گزینه را انتخاب کنید. در این صورت چاپگر مزبور از طریق آدرس http://*printername* که در آن متغیر ***printername*** بیانگر نام چاپگر است، قابل دستیابی خواهد بود.
Internet Print Protocol (ipp)	اگر نرم‌افزار CUPS از طریق پورت مخصوص پروتکل IPP به شماره ۶۳۱ با چاپگر موردنظر در ارتباط است، این گزینه را انتخاب کنید. در این صورت چاپگر مزبور از طریق آدرس ipp://*printername* که در آن متغیر

عنوان گزینه	توضیح
	printername بیانگر نام چاپگر است، قابل دستیابی خواهد بود.
LPD/LPR Host Or Printer	اگر مدیریت چاپگر موردنظر از طریق سرویس چاپ LPD انجام می‌شود، این گزینه را انتخاب کنید.
Parallel Printer	این گزینه را در صورتی انتخاب کنید که چاپگر موردنظر به پورت موازی کامپیوتر میزبان متصل باشد.
SCSI Printer	این گزینه را در صورتی انتخاب کنید که چاپگر موردنظر از طریق یک رابط SCSI به کامپیوتر میزبان متصل باشد.
Serial Port #*x*	این گزینه را در صورتی انتخاب کنید که چاپگر موردنظر به یکی از پورت‌های سریال کامپیوتر میزبان با شماره *x* متصل باشد.
USB Printer #*x*	این گزینه را در صورتی انتخاب کنید که چاپگر موردنظر به یکی از پورت‌های USB کامپیوتر میزبان با شماره *x* متصل باشد.
Windows Printer Via SAMBA	این گزینه را در صورتی انتخاب کنید که دستیابی به چاپگر موردنظر به واسطه کامپیوتری با سیستم‌عامل Windows و از طریق سرویس Samba مهیا شده باشد.

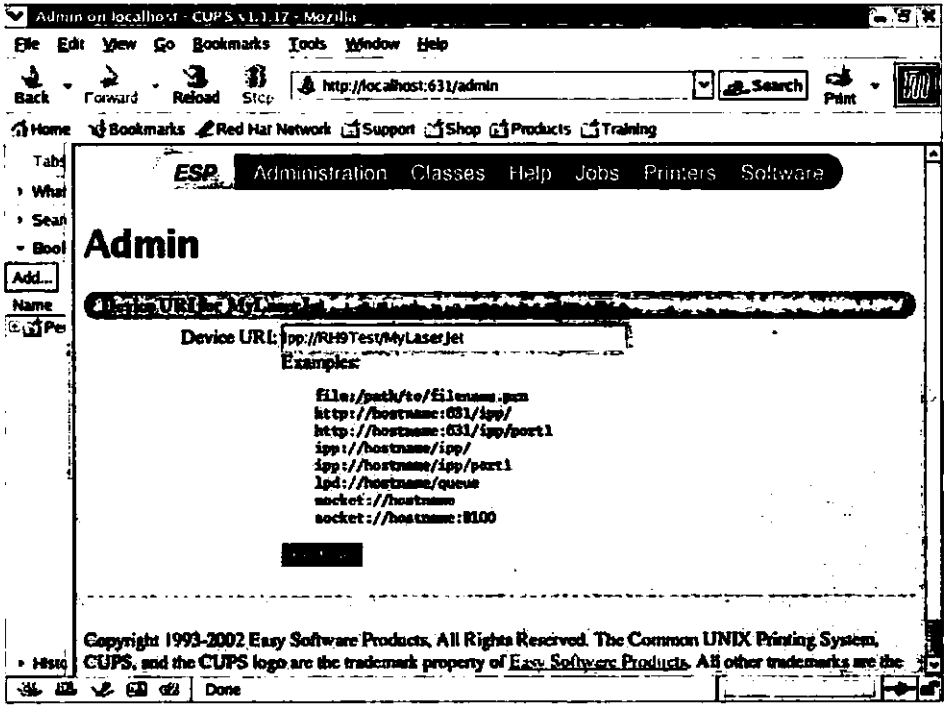


شکل ۵-۲۵ تعیین مشخصات چاپگر

پس از انتخاب گزینه موردنظر دکمه Continue را کلیک کنید.

تعیین آدرس URI جهت دسترسی به چاپگر مورد نظر

در این مرحله باید آدرس URI چاپگر موردنظر را مشخص کنید. البته نرم‌افزار CUPS بخش نخست این آدرس شامل lpd://، smb://، socket:// یا http:// را در فیلد Device URI از صفحه مربوطه نمایش می‌دهد. برای مثال، چنان‌چه در مرحله قبل (شکل ۵-۲۵) گزینه Internet Print Protocol (IPP) را به عنوان مشخصه چاپگر انتخاب کرده باشید، نرم‌افزار CUPS در این مرحله عنوان ipp:// را در فیلد مذکور نمایش خواهد داد. چنان‌که در شکل ۶-۲۵ مشاهده می‌کنید، چاپگر موردنظر با عنوان MyLaserJet به کامپیوتری با نام RH9Test متصل است. از این‌رو، با توجه به مشخصه ipp:// آدرس URI عبارت از ipp://RH9Test/MyLaserJet خواهد بود.



شکل ۶-۲۵ تعیین آدرس URI چاپگر

چنان‌چه در مرحله قبل (شکل ۵-۲۵) شماره پورت فیزیکی به خصوصی را از لیست Device انتخاب کرده باشید، نیازی به تعیین آدرس URI نبوده و از این‌رو صفحه مربوط به تعیین آدرس مزبور (شکل ۶-۲۵) به نمایش درنمی‌آید.

در صورتی که کامپیوتر میزبان دارای بیش از یک پورت چاپگر باشد، می‌توانید مشخصه آن‌را به این صورت به انتهای آدرس URI ضمیمه کنید:

```
ipp://RH9Test/MyLaserJet/dev/lp0
```

اگر چاپگر موردنظر در شبکه‌ای از نوع Windows مستقر بوده و آن‌را به واسطه سرویس Samba مورد دستیابی قرار داده‌اید، آدرس URI با مشخصه smb:// آغاز شده و با نام چاپگر خاتمه می‌یابد. برای مثال، تحت شرایط فوق آدرس URI چاپگری با نام myprint که به کامپیوتری با عنوان printserv متصل شده، چنین است:

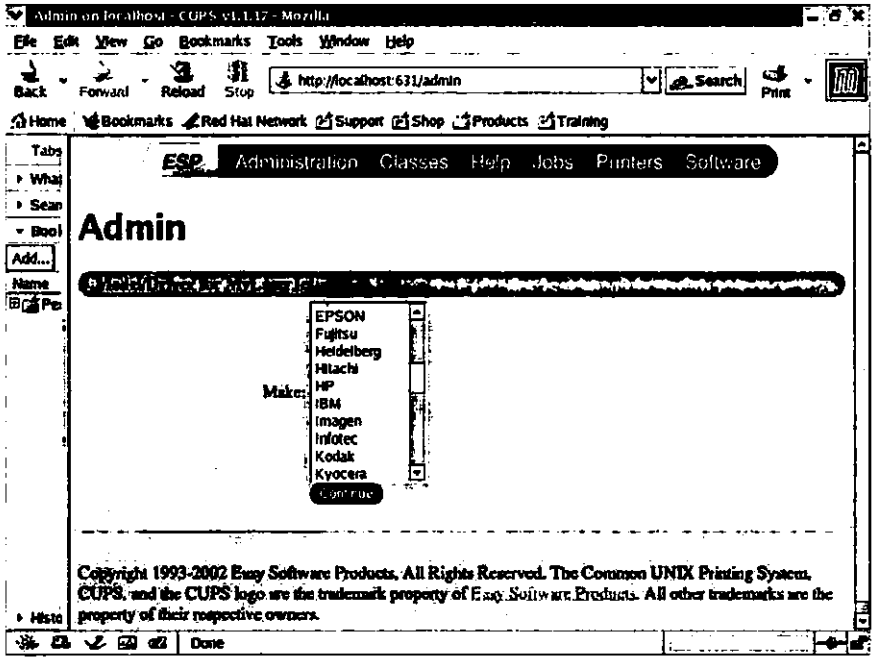
```
smb://printserv/myprint
```

پس از تعیین آدرس URI چاپگر موردنظر در فیلد مربوطه دکمه Continue را کلیک کنید.

تعیین مدل چاپگر

تعیین مدل چاپگر فرآیند بسیار ساده‌ای است. نرم‌افزار CUPS از طریق این تنظیمات فیلتر چاپ موردنیاز برای چاپگر را تشخیص می‌دهد. برای این منظور کافی است شرکت سازنده چاپگر موردنظر را از لیست شکل ۷-۲۵ انتخاب کنید. اگر نام شرکت سازنده چاپگر را در این لیست مشاهده نمی‌کنید، چاپگر موردنظر ممکن است از نوع PostScript باشد، که در این صورت باید گزینه PostScript را انتخاب کنید. هم‌چنین اگر چاپگر مزبور نیازی به فیلتر چاپ نداشته باشد، باید گزینه Raw را انتخاب کنید. این گونه چاپگرها می‌توانند خروجی را به صورت قالب‌بندی نشده (اصطلاحاً خروجی خام یا raw output) چاپ کنند.

اگر تنها مدل‌های معدودی را در این لیست مشاهده می‌کنید به این علت است که شرکت Red Hat بر استفاده از ابزار گرافیکی redhat-config-printer تأکید دارد. این ابزار به واسطه بسته نرم‌افزاری foomatic-* امکان برخورداری از تعداد زیادی درایور را در اختیار می‌گذارد. در سایر نسخه‌های سیستم‌عامل Red Hat Linux دسترسی به درایورهای بیشتر به واسطه بسته نرم‌افزاری cups-drivers-* فراهم می‌شود. برای مثال، بسته نرم‌افزاری مزبور به همراه سیستم‌عامل Red Hat Linux 8.0 توزیع شده است. پس از انتخاب گزینه موردنظر دکمه Continue را کلیک کنید.



شکل ۷-۲۵ انتخاب مدل چاپگر

انتخاب درایور چاپگر

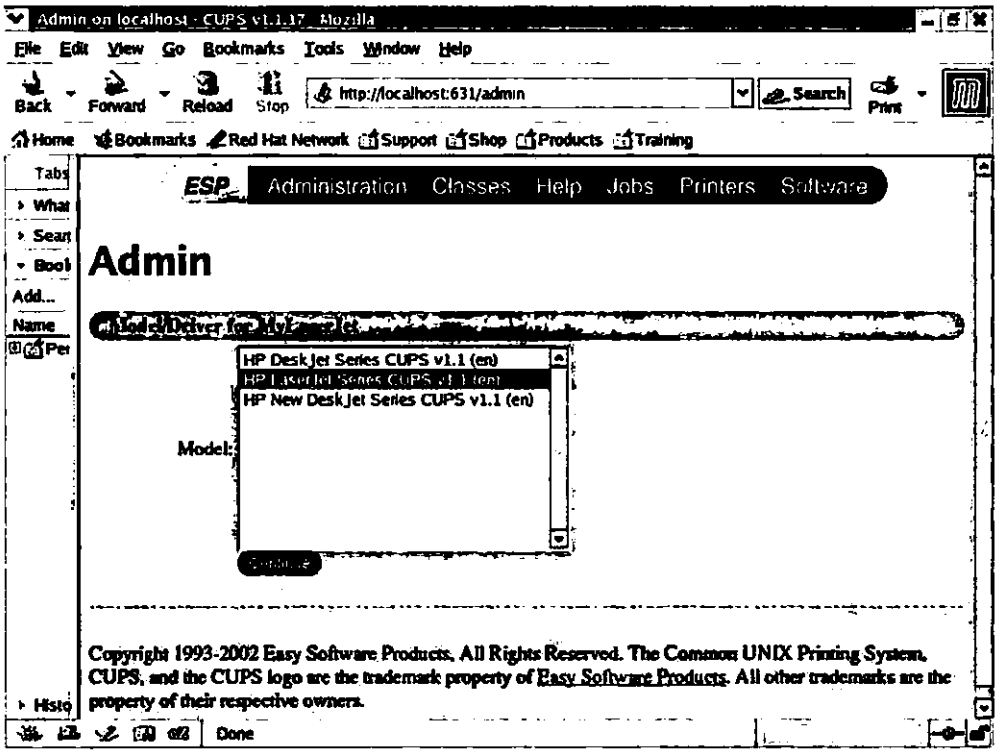
در این مرحله باید درایور چاپگر را انتخاب کنید. بدیهی است گزینه‌های مربوطه بسته به مدل چاپگر متفاوت خواهد بود. چنان‌چه در این مورد بیش از یک گزینه وجود داشته باشد با کمی سعی و خطا می‌توانید گزینه مناسب را تشخیص دهید. شکل ۸-۲۵ صفحه مربوط به این گزینش را نشان می‌دهد.

پس از انتخاب گزینه موردنظر دکمه Continue را کلیک کنید. با این اقدام پیغامی شبیه به این را مشاهده خواهید کرد:

```
Printer MyLaserJet has been added successfully.
```

چنان‌که مشاهده می‌کنید، نام چاپگر (در این‌جا MyLaserJet) در قالب یک فراپیوند (اصطلاحاً hyperlink) نمایش داده شده است، به طوری که با کلیک روی آن می‌توانید وضعیت فعلی چاپگر را مشاهده کنید.

جهت مشاهده مجدد منوی اصلی نرم‌افزار CUPS کافی است آدرس http://localhost:631 را مورد دستیابی قرار دهید. (برای این منظور آدرس فوق را در نوار آدرس مرورگر اینترنت درج کرده و کلید Enter را فشار دهید.)

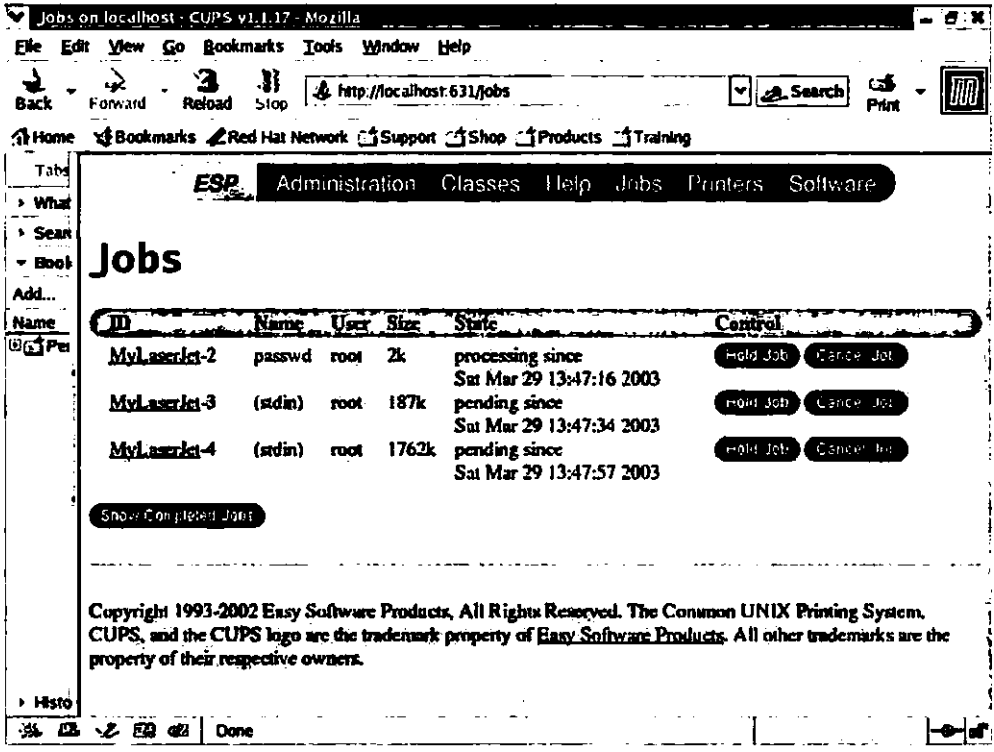


شکل ۸-۲۵ انتخاب درایور چاپگر

مدیریت وظایف چاپی

بازبینی صف مربوط به وظایف چاپی کار ساده‌ای است. برای این منظور کافی است فراپیوند Jobs یا Manage Jobs از منوی اصلی نرم‌افزار CUPS را کلیک کنید. این وظایف در قالب فایل‌هایی در فهرست /var/spool/cups سازمان‌دهی می‌شوند. در صورت وجود وظایف چاپی آن‌ها را در قالب صفحه‌ای مشابه شکل ۹-۲۵ مشاهده خواهید کرد.

امکان توقف یا لغو وظایف چاپی به واسطه دکمه‌های Hold Job و Cancel Job فراهم شده است. وظایف چاپی متوقف شده هم‌چنان در فهرست /var/spool/cups نگهداری شده و سایر وظایف پیش از آن‌ها پردازش می‌شوند. (وظایف چاپی متوقف شده وظایفی هستند که به طور موقت از صف خارج شده‌اند. چنین وظایفی را می‌توان در صورت تمایل مجدداً درون صف قرار داد.) با کلیک روی شناسه هر وظیفه چاپی (مقادیر مندرج در ستون ID) می‌توان اطلاعات بیشتری را درباره آن به دست آورد.



شکل ۹-۲۵ لیست وظایف چاپی موجود

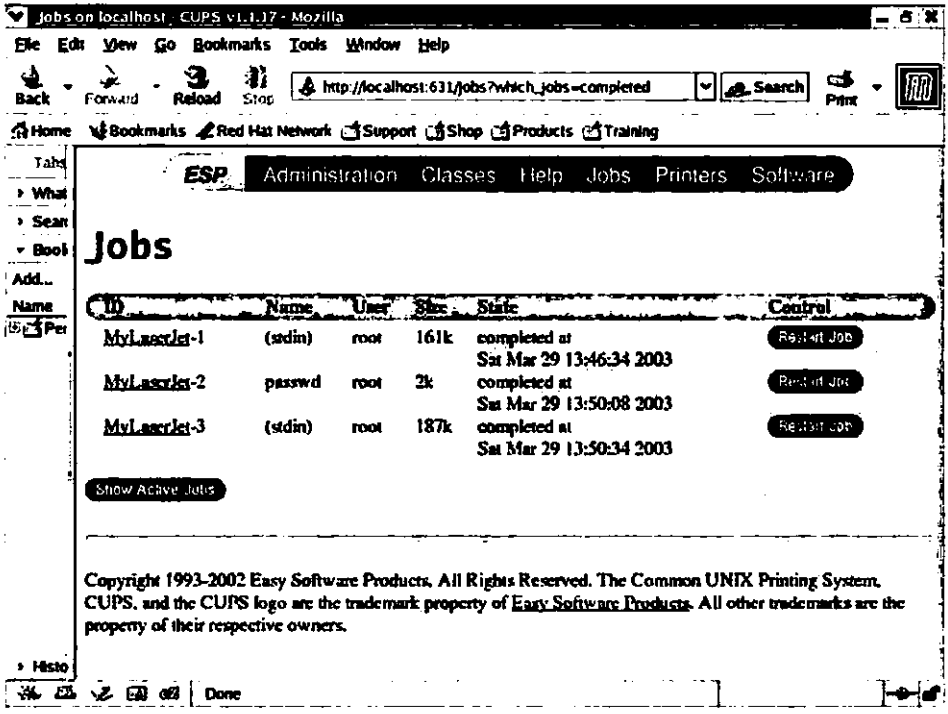
یکی از ویژگی‌های مفید نرم‌افزار CUPS این است که زمان دقیق تکمیل وظایف چاپی انجام شده را نمایش داده و امکان انجام مجدد آن‌ها را در اختیار می‌گذارد. برای مشاهده لیست وظایف تکمیل شده کافی است دکمه Show Completed Jobs را کلیک کنید. شکل ۱۰-۲۵ چنین لیستی را نشان می‌دهد. به واسطه این قابلیت می‌توانید از فعالیت چاپگرها در رابطه با تکمیل وظایف چاپی اطلاع حاصل کنید.

اگر در چاپ با نرم‌افزار CUPS با مشکل مواجه شده‌اید، به دلایلی ممکن است حالت LPD فعال شده باشد.

استفاده از راهنمای نرم‌افزار CUPS

هنگام استفاده از نرم‌افزار CUPS می‌توانید اسناد حاوی راهنمای این نرم‌افزار را مورد دستیابی قرار دهید. برای این منظور روی گزینه Help یا On-Line Help از منوی اصلی کلیک کنید. با این اقدام به مستندات نرم‌افزار CUPS که در قالب بسته نرم‌افزاری *-cups روی کامپیوتر میزبان نصب شده است،

دست خواهید یافت. شرح مختصری از محتوای این مستندات در جدول ۷-۲۵ آمده است. مستندات دیگری نیز برای توسعه دهندگان قابلیت‌های نرم‌افزار CUPS پیش‌بینی شده است.



شکل ۱۰-۲۵ لیست حاوی وظایف چاپی تکمیل شده

جدول ۷-۲۵ شرح محتوای مستندات نرم‌افزار CUPS

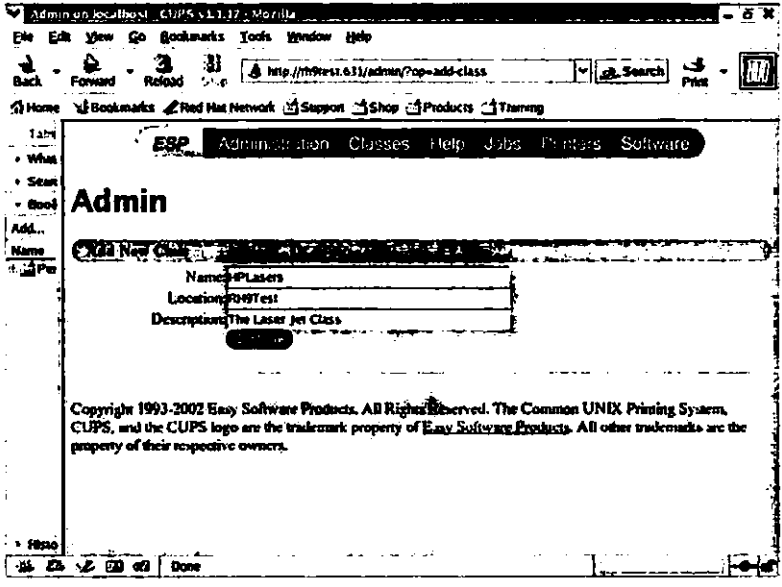
عنوان سند	توضیح
An overview of the Common Unix Printing System	این سند ساختار اصلی نرم‌افزار CUPS، نحوه تعامل آن از طریق پروتکل IPP 1.1 و میزان پشتیبانی آن از فرامین LPD را شرح می‌دهد.
Software Users Manual	این سند نحوه استفاده از فرامین نرم‌افزار CUPS جهت چاپ اسناد و مدارک را شرح می‌دهد.
Software Administrators Manual	این سند نحوه نصب نرم‌افزار CUPS و ساختار فایل‌های پیکربندی آن‌را که در فهرست /etc/cups مستقر هستند، شرح می‌دهد.
CUPS Implementation of IPP	این سند به مقایسه میان قابلیت‌های نرم‌افزار CUPS و مشخصات پروتکل IPP می‌پردازد.

بار دیگر، با درج آدرس http://localhost:631 در نوار آدرس مرورگر وب و فشار کلید Enter منوی اصلی نرم‌افزاری CUPS را مورد دستیابی قرار دهید.

سازمان‌دهی چاپگرها

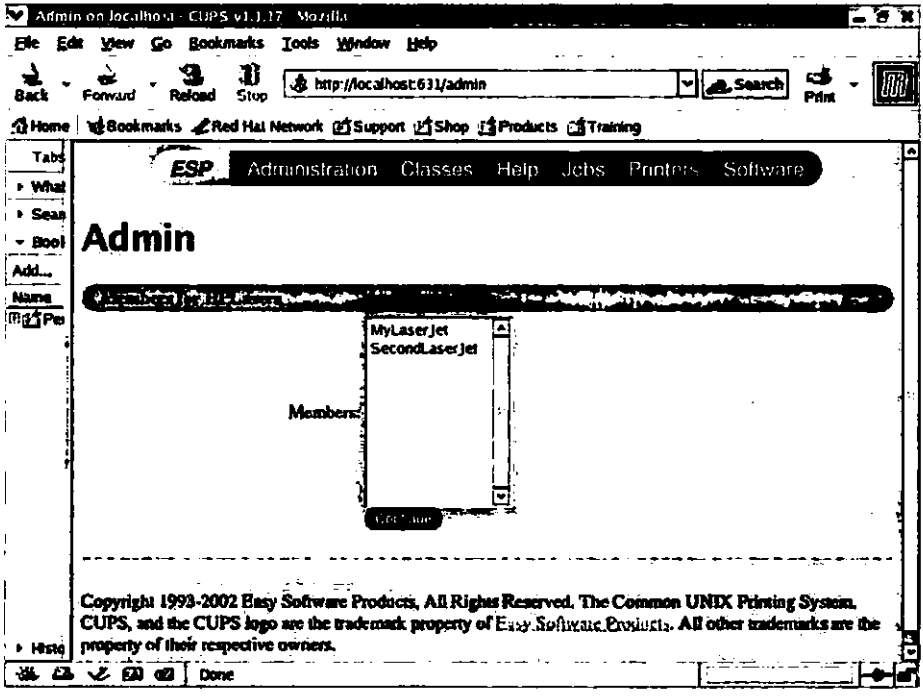
یکی از بارزترین نقاط قوت نرم‌افزار CUPS توانایی آن در سازمان‌دهی چاپگرهاست، به طوری که می‌توان آن‌ها را در قالب کلاس‌های مختلفی دسته‌بندی کرد. پس از ارسال یک وظیفه چاپی به کلاسی از چاپگرها آن وظیفه توسط نخستین چاپگر قابل دستیابی در کلاس پردازش می‌شود. به بیان دیگر، نیازی نیست که کاربران برای دستیابی به چاپگر یا چاپگرهای موردنظر خود منتظر بمانند.

برای مدیریت کلاس‌ها روی گزینه Classes از منوی اصلی نرم‌افزار CUPS کلیک کنید. با این اقدام لیست چاپگرهایی را که در قالب کلاس‌های مختلف سازمان‌دهی شده‌اند، مشاهده خواهید کرد. برای ایجاد کلاس جدید دکمه Add Class را کلیک کنید تا به این ترتیب مطابق شکل ۱۱-۲۵ صفحه‌ای با عنوان Add New Class به نمایش درآید. چنان‌که در این شکل مشاهده می‌کنید، از عنوان HPLasers که مشابه نام هیچ یک از چاپگرها نیست، برای نام‌گذاری کلاس جدید استفاده شده است. کاربرد فیلدهای متنی Location و Description دقیقاً مشابه فیلدهای متنی هم‌نام در فرآیند تعریف یک چاپگر جدید است، به طوری که فیلد متنی Location موقعیت کامپیوتر مورد استفاده به عنوان سرور چاپ و فیلد متنی Description توضیح مربوط به کلاس جدید را مشخص می‌کند.



شکل ۱۱-۲۵ تعیین مشخصات کلاس جدید

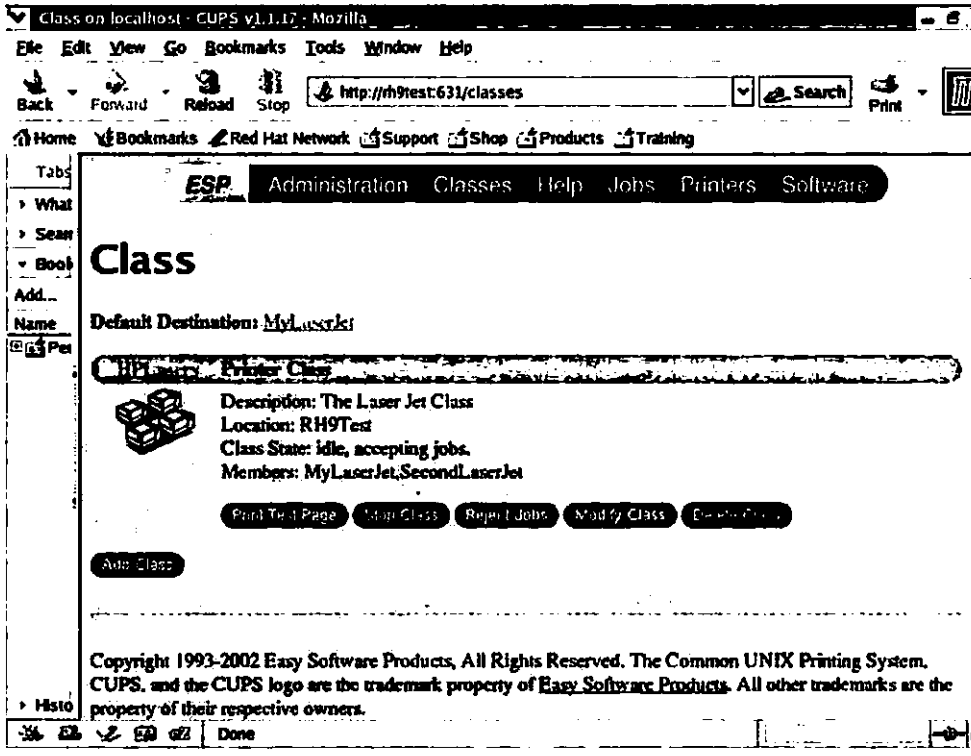
پس از درج مقادیر موردنظر در فیلدهای متنی فوق روی دکمه Continue کلیک کنید. با این اقدام صفحه‌ای با عنوان Members For *PrintClassName* را که در آن متغیر *PrintClassName* بیانگر نام کلاس موردنظر است، مشاهده خواهید کرد. این صفحه شامل تمام چاپگرهایی است که به عنوان چاپگر CUPS پیکربندی شده‌اند. صفحه مزبور علاوه بر چاپگرهای کلاس جدید، چاپگرهای متعلق به سایر کلاس‌ها را نیز نمایش می‌دهد. برای اضافه کردن چاپگرهای موردنظر از این صفحه به کلاس جدید کافی است آن‌ها را انتخاب کرده و دکمه Continue را کلیک کنید. با این کار نرم‌افزار CUPS پیغامی را با این مضمون که کلاس HPLasers به جمع کلاس‌های موجود اضافه شده است، نمایش خواهد داد. اکنون می‌توانید وظایف چاپی موردنظر را جهت چاپ به کلاس HPLasers ارسال کنید. چنان‌که قبلاً نیز گفته شد، وظایف چاپی ارسال شده به یک کلاس توسط اولین چاپگر قابل دستیابی در آن کلاس چاپ می‌شوند.



شکل ۱۲-۲۵ اضافه کردن چاپگرهای موردنظر به کلاس جدید

پس از انجام اقدامات فوق دکمه Classes را کلیک کنید. با این کار مشخصات کلاس جدید را مشاهده خواهید کرد. شکل ۱۳-۲۵ کلاس جدید با عنوان HPLasers را که تنها شامل دو چاپگر با اسامی

MyLaserJet و SecondLaserJet1 است، نشان می‌دهد.

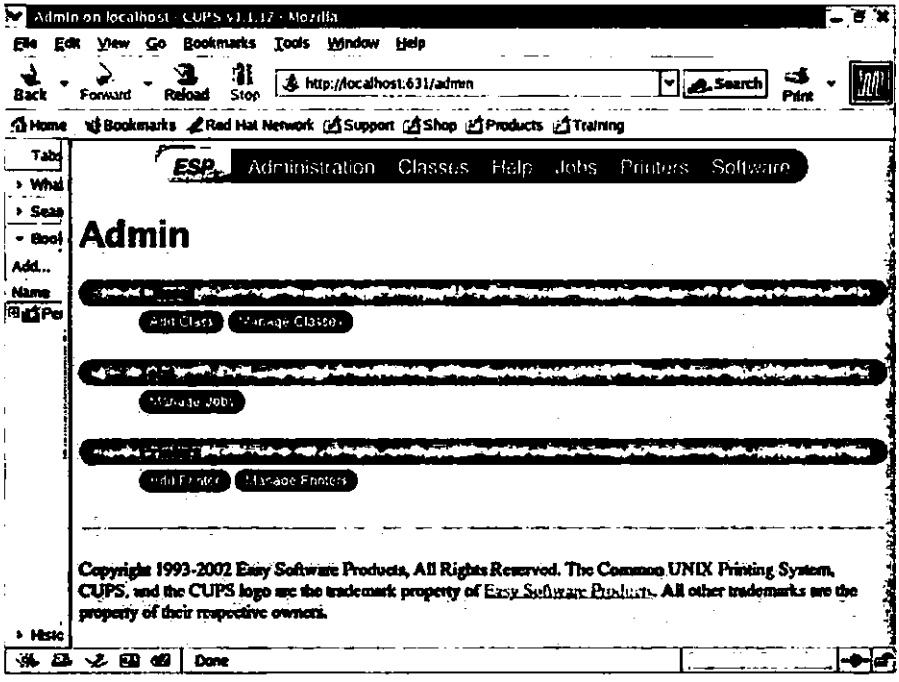


شکل ۱۳-۲۵ مشخصات کلاس HPLasers

بار دیگر، برای بازگشت به منوی اصلی نرم‌افزار CUPS آدرس http://localhost:631 را در نوار آدرس مرورگر وب درج کرده و کلید Enter را فشار دهید.

وظایف مدیریتی

با کلیک روی گزینه Administration یا Do Administration Tasks از منوی اصلی نرم‌افزار CUPS می‌توانید امکانات موردنیاز برای مدیریت کلاس‌ها، وظایف چاپی و چاپگرها را مورد دستیابی قرار دهید. شکل ۱۴-۲۵ این امکانات را نشان می‌دهد.



شکل ۱۴-۲۵ منوی مربوط به وظایف مدیریتی

فرمان lpadmin

در حالی که مدیران با تجربه‌تر همواره از رابط سطر فرمان سیستم‌عامل Linux برای انجام وظایف مدیریتی استفاده می‌کنند، افراد تازه‌کار معمولاً استفاده از رابط گرافیکی را برای انجام این امور ترجیح می‌دهند. حقیقت این است که رابط سطر فرمان سیستم‌عامل از قابلیت اطمینان بیشتری نسبت به رابط گرافیکی برخوردار است. نکته جالب این‌که مدیریت چاپگرهای CUPS با بهره‌گیری از فرمان lpadmin نیز امکان‌پذیر است. با وجود این، به واسطه تنوع روزافزون چاپگرها به تدریج از جنبه عملی این فرمان کاسته می‌شود.

علیرغم این موضوع، وظایف مدیریتی قابل توجهی را می‌توان از طریق سطر فرمان سیستم‌عامل Linux در ارتباط با چاپگرها انجام داد. یکی از کاربردهای جالب در این زمینه سهمیه‌بندی دسترسی کاربران به چاپگرهاست. با انجام این کار می‌توان میزان بهره‌برداری از چاپگرها را به خوبی کنترل کرد. فرمان lpadmin امکان سهمیه‌بندی استفاده از یک چاپگر به خصوص از شبکه را در اختیار قرار می‌دهد. برای مثال، با اجرای این فرمان کاربران می‌توانند روزانه حداکثر ۱۰ صفحه را برای چاپ به چاپگر MyLaserJet ارسال کنند:

```
# lpadmin -p MyLaserJet -o job-quota-period=86400
-o job-page-limit=10
```

در صورت تمایل، با استفاده از سوییچ job-k-limit -o می‌توان محدودیت بهره‌برداری از چاپگر را با توجه به اندازه اسناد ارسالی به آن (بر حسب کیلوبایت) مشخص کرد.

به روش مشابه می‌توان دسترسی به چاپگرها را تنها برای برخی از کاربران مهیا کرد. برای مثال، این فرمان امکان بهره‌برداری از چاپگری با عنوان MyLaserJet را تنها در اختیار دو کاربر ez و tblair قرار می‌دهد:

```
# lpadmin -p MyLaserJet -u allow:ez,tblair
```

و بالاخره در صورت لزوم می‌توان دسترسی برخی از کاربران به چاپگرها را محدود کرد. برای مثال، این فرمان از دسترسی کاربری با شناسه mj به چاپگری با عنوان MyLaserJet ممانعت به عمل می‌آورد:

```
# lpadmin -p MyLaserJet -u deny:mj
```

با هر بار اجرای فرمان lpadmin به یکی از روش‌های فوق فایل پیکربندی /etc/cups/printers.conf دستخوش تغییر می‌شود.

فرمان lpstat

فرمان lpstat امکان بازبینی وضعیت چاپگرها و کلاس‌ها را فراهم می‌کند. استفاده از این فرمان بسیار ساده است، به طوری که گزینه -c *class* لیست اعضای یک کلاس به خصوص و گزینه -v *printer* لیست مشخصات چاپگر را در اختیار قرار می‌دهد.

فایل‌های پیکربندی نرم‌افزار CUPS

فایل‌های پیکربندی نرم‌افزار CUPS در فهرست /etc/cups مستقر هستند. ساختار این فایل‌ها شباهت زیادی به فایل‌های پیکربندی وب سرور Apache دارد. (وب سرور نامبرده را در فصل سی‌ام مورد بررسی قرار می‌دهیم.)

فراموش نکنید که در فایل‌های پیکربندی نرم‌افزار CUPS تمام چاپگرها با آدرس URI مربوطه مانند ipp://RH9/MyLaserJet مورد اشاره قرار می‌گیرند. چنان‌که می‌دانید قالب آدرس‌های URL به صورت http://www.sybex.com است. شرح فایل‌های پیکربندی نرم‌افزار CUPS در جدول ۸-۲۵ آمده است. در قسمت بعد محتوای فایل پیکربندی /etc/cups/cups.conf را مورد بررسی قرار می‌دهیم.

جدول ۸-۲۵ شرح فایل‌های پیکربندی نرم‌افزار CUPS

عنوان فایل	توضیح
classes.conf	این فایل نحوه دسته بندی چاپگرها را در قالب کلاس‌ها مشخص می‌کند. به محض ایجاد یک کلاس جدید از چاپگرها مشخصات آن در این فایل درج می‌شود.
client.conf	این فایل حاوی نام کامپیوتر میزبان سرور چاپ است.
cupsd.conf	این فایل در واقع فایل پیکربندی اصلی نرم‌افزار CUPS است.
mime.convs	این فایل حاوی فیلترهای موردنیاز برای چاپ اسناد مختلف مانند اسناد متنی یا تصاویر است.
mime.types	این فایل حاوی انواع فایل‌هایی است که چاپگرهای CUPS قادر به پردازش آن‌ها هستند.
printers.conf	محتوای این فایل حاوی مشخصات چاپگرها بوده و ضمن پیکربندی آن‌ها دستخوش تغییر می‌شود.
pstoraster.convs	این فایل حاوی فیلتری برای تبدیل فایل‌های Gostscript است، به طوری که بتوان از چاپگرهای PostScript برای چاپ آن‌ها استفاده کرد.

ساختار فایل پیکربندی /etc/cups/cupsd.cinf

هر چند به کمک رابط گرافیکی نرم‌افزار CUPS که از طریق مرورگر وب قابل دستیابی است، می‌توان چاپگرها و کلاس‌های موردنظر را پیکربندی کرد، برای مدیریت چاپگرها باید با ساختار فایل پیکربندی اصلی این نرم‌افزار با عنوان /etc/cups/cupsd.conf آشنا باشید. در این قسمت ساختار نسخه پیش‌فرض این فایل را مورد بررسی قرار می‌دهیم. چنان‌که خواهید دید، محتوای فایل مزبور مجموعه‌ای از دستورالعمل‌هاست. برخی از این دستورالعمل‌ها به واسطه وجود علامت # در ابتدای آن‌ها غیرفعال شده‌اند. بدیهی است با حذف علامت # می‌توان این گونه دستورالعمل‌ها را فعال کرد.

ترتیب بررسی متغیرها در این قسمت دقیقاً مطابق با ترتیبی نیست که این متغیرها در فایل پیکربندی /etc/cups/cupsd.conf درج شده‌اند، به طوری که برای مثال، متغیرهای مربوط به فایل‌های ثبت وقایع را تحت عنوان یک موضوع مورد بررسی قرار خواهیم داد.

متغیرهای متنوعی در فایل پیکربندی cupsd.conf مقداردهی شده‌اند. برای اطلاع بیشتر درباره آن‌ها کافی است گزینه On-Line Help از شکل ۱-۲۵ را کلیک کرده و سند CUPS Software Administrator's Manual را مورد دستیابی و مطالعه قرار دهید.

بار دیگر یادآوری می‌کنیم که وجود علامت # در ابتدای خط بیانگر توضیح است. توضیحات عناصر غیرفعال بوده و نقشی در پیکربندی ندارند. برای فعال کردن دستورالعمل‌های مندرج در چنین خطوطی کافی است علامت # را از ابتدای خط حذف کنید. برخی از آن‌ها دستورالعمل‌های پیش‌فرض هستند.

متغیرهای سرور

متغیرهای سرور شامل دو متغیر ServerName و ServerAdmin هستند. متغیر ServerName نام کامپیوتر میزبان سرور چاپ نرم‌افزار CUPS را مشخص می‌کند. مقدار پیش‌فرض این متغیر نام کامپیوتر محلی است. دستورالعمل مقداردهی متغیر ServerName در فایل پیکربندی cupsd.conf چنین است:

```
# ServerName myhost.domain.com
```

نام این کامپیوتر که در دستورالعمل فوق با عنوان myhost.domain.com مشخص شده است، باید با مقدار متغیر ServerName در فایل پیکربندی /etc/cups/client.conf مطابقت کند. از طرف دیگر، متغیر ServerAdmin آدرس پست الکترونیکی مدیر سرور CUPS (اصطلاحاً webmaster) را مشخص می‌کند. دستورالعمل مربوطه چنین است:

```
# ServerAdmin root@your.domain.com
```

فهرست‌های استاندارد

فایل پیکربندی cupsd.conf حاوی اسامی متعددی از فایل‌هاست. چنان‌چه اسامی این فایل‌ها از طریق آدرس‌دهی نسبی مشخص شده باشد، موقعیت آن‌ها با توجه به مقدار متغیر ServerRoot که به طور پیش‌فرض مقدار آن برابر با /etc/cups است، سنجیده می‌شود. دستورالعمل مربوطه چنین است:

```
# ServerRoot /etc/cups
```

نرم‌افزار CUPS فایل‌های حاوی فونت‌ها، مجموعه‌های کاراکتری و مانند آن‌ها را به طور پیش‌فرض در فهرست /usr/share/cups نگهداری می‌کند. در فایل پیکربندی cupsd.conf موقعیت فهرست مزبور توسط متغیر DataDir مشخص شده که در صورت تمایل می‌توان مقدار آن‌را تغییر داد. به دستورالعمل مربوطه توجه کنید:

```
# DataDir /usr/share/cups
```

وظایف چاپی در قالب فایل‌هایی درون سبد چاپ (اصطلاحاً spool) سازمان‌دهی می‌شوند. این فایل‌ها تا زمانی که چاپگر آن‌ها را مورد پردازش قرار دهد در فهرست به خصوصی که در فایل پیکربندی

cupsd.conf توسط متغیر RequestRoot مشخص شده است، مستقر می‌شوند. مقدار پیش‌فرض این متغیر /var/spool/cups است. به دستورالعمل مربوطه توجه کنید:

```
# RequestRoot /var/spool/cups
```

نرم‌افزار CUPS فهرست موقتی را در اختیار تمام کاربران قرار می‌دهد تا به این ترتیب بتوانند فایل‌های موردنیاز خود را در آن کپی کنند. معمولاً کاربران فیلترهایی را پیش از پردازش وظایف چاپی موردنظر در این فهرست کپی می‌کنند. به طور پیش‌فرض فهرست /var/tmp برای این منظور در نظر گرفته شده است. با وجود این، در سیستم‌عامل Red Hat Linux از فهرست /var/spool/cups/tmp برای این کار استفاده می‌شود. در فایل پیکربندی cupsd.conf موقعیت این فهرست توسط متغیر TempDir مشخص شده است. به دستورالعمل مربوطه توجه کنید:

```
# TempDir /var/spool/cups/tmp
```

در صورت تمایل می‌توانید فهرست دیگری را برای این منظور ایجاد کنید. پس از آن‌که چنین فهرستی را به عنوان کاربر اصلی (اصطلاحاً root) ایجاد کردید، با اجرای این فرمان می‌توانید مجوزهای دسترسی به آن‌را تغییر دهید: (در این فرمان از فهرست /tmpdir به عنوان فهرست موقت استفاده شده است.)

```
# chmod a+t /tmpdir
```

برای درک بهتر این موضوع به خروجی حاصل از اجرای فرمان ls -l /var/spool/cups توجه کنید:

```
drwx------T   2 lp  sys   4096 Mar  3 12:48 tmp
```

متغیرهای مربوط به فایل‌های ثبت وقایع

چنان‌که در فصل سیزدهم نیز اشاره شد، بیشتر فایل‌های ثبت وقایع در فهرست /var/log مستقر هستند. این موضوع در مورد نرم‌افزار CUPS نیز صدق می‌کند، به طوری که فایل‌های ثبت وقایع این نرم‌افزار در فهرست /va/log/cups مستقر می‌شوند. مقادیر سه متغیر AccessLog، ErrorLog و PageLog موقعیت این فایل‌ها را مشخص می‌کند. دستورالعمل‌های مربوطه چنین است:

```
# AccessLog /var/log/cups/access_log
# ErrorLog /var/log/cups/error_log
# PageLog /var/log/cups/page_log
```

مقادیری که در دستورالعمل‌های فوق مشاهده می‌کنید مقادیر پیش‌فرض این متغیرها هستند. بدیهی است در صورت تمایل می‌توانید از فهرست دیگری برای نگهداری فایل‌های ثبت وقایع نرم‌افزار CUPS استفاده کنید. شرح این فایل‌ها در جدول ۹-۲۵ آمده است.

جدول ۹-۲۵ شرح فایل‌های ثبت وقایع نرم‌افزار CUPS

عنوان فایل	توضیح
access_log	این فایل حاوی لیست اسامی فایل‌هایی است که از طریق ابزار مدیریتی نرم‌افزار CUPS (شکل ۱-۲۵) مورد دستیابی قرار گرفته‌اند
error_log	این فایل حاوی پیغام‌های خطا، اخطارها، پیغام‌های مورد استفاده در فرآیند اشکال‌زدایی و هم‌چنین پیغام‌های اطلاعاتی است. قالب این پیغام‌ها منطبق بر قالب استاندارد فایل‌های ثبت وقایع در سیستم‌عامل UNIX است.
page_log	این فایل حاوی مشخصات صفحات ارسالی به چاپگر است.

چنان‌که در فصل سیزدهم اشاره شد، فایل‌های ثبت وقایع در سیستم‌عامل Red Hat Linux پس از گذشت یک هفته بایگانی می‌شوند. به کمک MaxLogSize می‌توان شرایط بایگانی فایل‌های ثبت وقایع نرم‌افزار CUPS را با توجه به اندازه این فایل‌ها مشخص کرد، به طوری که اگر اندازه فایل‌های مزبور از مقدار متغیر MaxLogSize متجاوز شود، سیستم‌عامل Linux برای بایگانی آن‌ها اقدام خواهد کرد. در صورتی که این متغیر مقداردهی نشده باشد، بایگانی فایل هنگامی انجام می‌شود که اندازه آن از یک مگابایت متجاوز شود. هم‌چنین اگر متغیر MaxLogSize به این صورت با عدد صفر مقداردهی شده باشد، هیچ اقدامی برای بایگانی فایل‌های مورد بحث انجام نخواهد شد:

```
MaxLogSize 0
```

وضعیت فوق ممکن است به واسطه مکانیزم دیگری دستخوش تغییر شود. برای مثال، چنان‌چه فرآیند بایگانی فایل‌های مزبور در قالب یکی از وظایف فهرست /etc/cron.daily درج شده باشد، بایگانی آن‌ها به طور روزانه انجام خواهد شد.

علاوه بر موضوع فوق در فصل سیزدهم به این نکته نیز اشاره شد که عملکرد مکانیزم ثبت وقایع بر اساس تنظیمات فایل پیکربندی /etc/syslog.conf انجام می‌شود. جدول ۱۰-۲۵ سطوح مختلف این مکانیزم را که توسط متغیر LogLevel مشخص می‌شود، شرح می‌دهد. مقدار پیش‌فرض این متغیر info است. به دستورالعمل مربوطه توجه کنید:

```
LogLevel info
```

جدول ۱۰-۲۵ شرح سطوح مختلف عملکرد مکانیزم ثبت وقایع در نرم‌افزار CUPS

عنوان سطح	توضیح
emerg	در این سطح تنها وقایعی به ثبت می‌رسد که از عملکرد نرم‌افزار CUPS جلوگیری به عمل آورده‌اند.
alert	در این سطح وقایعی به ثبت می‌رسد که بلافاصله باید در مورد آن‌ها اقدامات لازم را به عمل آورد.
crit	در این سطح آن دسته از خطاهای اساسی به ثبت می‌رسد که ممکن است از عملکرد نرم‌افزار CUPS جلوگیری به عمل نیاورند.
error	در این سطح خطاهای عمومی به ثبت می‌رسد.
warn	در این سطح اخطارها به ثبت می‌رسد.
notice	در این سطح خطاهای موقتی به ثبت می‌رسد.
info	در این سطح تمام درخواست‌ها به ثبت می‌رسد.
debug	در این سطح اطلاعات اولیه مربوط به اشکال‌زدایی به ثبت می‌رسد.
debug2	در این سطح کلیه اطلاعات مربوط به اشکال‌زدایی به ثبت می‌رسد.

متغیرهای مربوط به طبقه‌بندی اسناد و مجموعه‌های کاراکتری

در صورت تمایل می‌توانید سرصفحه‌ای را در هر یک از صفحات ارسالی به چاپگر درج کنید. چنان‌چه در مورد اسناد چاپی قوانین امنیتی ویژه‌ای موجود باشد بسته‌به‌نیاز می‌توانید یکی از این دستورالعمل‌ها را فعال کنید:

```
# Classification classified
# Classification confidential
# Classification secret
# Classification topsecret
# Classification unclassified
```

هیچ یک از این دستورالعمل‌ها به طور پیش‌فرض فعال نیستند. با وجود این، در صورت فعال بودن یکی از آن‌ها دستورالعمل دیگری با عنوان ClassifyOverride نیز قابل استفاده خواهد بود. این متغیر را تنها می‌توان با یکی از مقادیر On یا Off مقداردهی کرد. چنان‌چه مقدار این متغیر On باشد، کاربران می‌توانند ویژگی طبقه‌بندی مربوط به یک وظیفه چاپی به خصوص را تغییر دهند. مقدار پیش‌فرض این متغیر Off است. به دستورالعمل مربوطه توجه کنید: `ClassifyOverride Off`

مجموعه کاراکترهای مورد استفاده در رابط گرافیکی پیکربندی نرم‌افزار CUPS (شکل ۱-۲۵) توسط متغیر DefaultCharset مشخص می‌شود. دو مقدار iso-8859-1 و windows-1251 مقادیر متداول این متغیر هستند. با وجود این، در صورت استفاده از متغیر دیگری با عنوان DefaultLanguage متغیر DefaultCharset تأثیر خود را از دست خواهد داد.

متغیر DefaultLanguage زبان مورد استفاده را مشخص می‌کند. زبان پیش‌فرض انگلیسی (با شاخص en) است. سایر گزینه‌ها عبارتند از آلمانی، اسپانیایی، فرانسوی و ایتالیایی که به ترتیب با شاخص‌های de، es، fr و it مشخص می‌شوند. به دستورالعمل مربوطه توجه کنید:

```
# DefaultLanguage en
```

مشابه فایل پیکربندی وب سرور Apache، در فایل پیکربندی cupsd.conf فهرست ریشه اسناد HTML توسط متغیر DocumentRoot مشخص می‌شود. به طور پیش‌فرض این فهرست عبارت از /usr/share/doc/cups-*versionnumber* است که البته در صورت تمایل می‌توان آن‌را تغییر داد. به دستورالعمل مربوطه توجه کنید:

```
# DocumentRoot /usr/share/doc/cups-versionnumber
```

در سیستم‌عامل Linux امور مربوط به فایل‌های PostScript با استفاده از برنامه Gostscript انجام می‌شود. چاپ این گونه فایل‌ها با استفاده از فونت‌هایی انجام می‌شود که موقعیت آن‌ها توسط متغیر FontPath مشخص شده است. برای این منظور، به طور پیش‌فرض از فونت‌های مستقر در فهرست /usr/share/cups/fonts استفاده می‌شود. به دستورالعمل مربوطه توجه کنید:

```
# FontPath /usr/share/cups/fonts
```

متغیرهای مربوط به مدیریت وظایف چاپی

در ارتباط با مدیریت وظایف چاپی، متغیرهای متعددی پیش بینی شده که در این قسمت به بررسی آن‌ها می‌پردازیم. متغیر PreserveJobHistory امکان حفظ وظایف چاپی قبلی را فراهم می‌کند. مقدار پیش‌فرض این متغیر Yes است. (در صورت استفاده از مقدار No سرور چاپ نرم‌افزار CUPS از حفظ وظایف چاپی قبلی صرف نظر خواهد کرد.) به دستورالعمل مربوطه توجه کنید:

```
# PreserveJobHistory Yes
```

متغیر PreserveJobFiles امکان حفظ فایل‌های موجود در سبد چاپ (اصطلاحاً spool) را در اختیار قرار می‌دهد به نحوی که بتوان آن‌ها را مجدداً چاپ کرد. با این حال، مقدار پیش‌فرض متغیر PreserveJobFiles برابر با No است. بدیهی است برای برخورداری از قابلیت فوق باید این مقدار را به Yes تغییر دهید. به دستورالعمل مربوطه توجه کنید:

```
# PreserveJobFiles No
```

مقدار متغیر MaxJobs حداکثر تعداد وظایف چاپی قبلی را که می‌توان سرور چاپ نرم‌افزار CUPS را وادار به حفظ آن‌ها کرد، مشخص می‌کند. مقدار پیش‌فرض این متغیر برابر با ۵۰۰ است. به دستورالعمل مربوطه توجه کنید:

```
# MaxJobs 500
```

متغیر MaxCopies محدودیت تعداد نسخه‌های چاپی از یک سند را مشخص می‌کند. مقدار پیش‌فرض این متغیر برابر با ۱۰۰ است. به دستورالعمل مربوطه توجه کنید:

```
# MaxCopies 100
```

چنان‌که در قسمت مربوط به فرمان lpadmin نیز توضیح داده شد، برای کنترل میزان بهره‌برداری از چاپگرها بهتر است از مکانیزم سهمیه بندی استفاده کنید. در حالت عادی پس از انجام یک وظیفه چاپی هیچ اقدامی برای پاکسازی داده‌های مربوطه از کامپیوتر صورت نمی‌گیرد.

در صورتی که از مکانیزم سهمیه بندی استفاده نکنید، لزومی ندارد که میزان بهره‌برداری از چاپگرها را کنترل کنید.

چنان‌چه مقدار متغیر AutoPurgeJobs را برابر با Yes قرار دهید، داده‌های مربوط به وظایف چاپی انجام شده به طور خودکار از روی کامپیوتر حذف خواهند شد. مقدار پیش‌فرض این متغیر برابر با No است. به دستورالعمل مربوطه توجه کنید:

```
# AutoPurgeJobs No
```

متغیر Printcap امکان تغییر چاپگرهای قابل استفاده را فراهم می‌کند. لیست این چاپگرها معمولاً در فایلی با قالب استاندارد هم‌چون /etc/printcap درج می‌شود. به دستورالعمل مربوطه توجه کنید:

```
# Printcap /etc/printcap
```

فایل /etc/printcap برای استفاده در سیستم چاپ LPD و جهت بهره‌برداری در سیستم‌عامل‌ها مبتنی بر BSD (هم‌چون FreeBSD و OpenBSD) طراحی شده است. با وجودی که قالب مشابهی نیز برای سیستم‌عامل Solaris توسعه یافته، قالب پیش‌فرض همان قالبی است که برای سیستم‌عامل‌های شبه BSD طراحی شده است. در هر صورت، با استفاده از متغیر PrintcapFormat می‌توان قالب موردنظر را تعیین کرد. به دستورالعمل مربوطه توجه کنید:

```
# PrintcapFormat BSD
# PrintcapFormat Solaris
```

متغیر PrintcapGUI تنها در صورت استفاده از سیستم‌عامل IRIX باید مقداردهی شود. (سیستم عامل مزبور توسط شرکت Silicon Graphics توسعه یافته است.)

انجام برخی از وظایف چاپی نیازمند اندکی کمک از جانب یک برنامه است. موقعیت این گونه برنامه‌ها توسط‌متغیر ServerBin مشخص می‌شود. مقدارپیش‌فرض‌این‌متغیر /usr/lib/cups است. به دستورالعمل مربوطه توجه کنید:

```
# ServerBin /usr/lib/cups
```

متغیر RIPCache میزان حافظه مورد استفاده برای پردازش تصویر در حالت نقطه به نقطه (اصطلاحاً Raster mode) را مشخص می‌کند. مقدار حافظه‌ای که به طور پیش‌فرض برای این منظور در نظر گرفته شده برابر با ۸ مگابایت است. علاوه بر واحد مگابایت (با شاخص m) مقدار حافظه موردنظر را می‌توان برحسب واحدهای دیگری از جمله کیلوبایت یا گیگابایت (با شاخص‌های k و g) نیز بیان کرد. این متغیر معمولاً هنگام استفاده از فیلترهای چاپ تخصصی از جمله imagetoraster یا pstoraster مورد بهره‌برداری قرار می‌گیرد. به دستورالعمل مربوطه توجه کنید:

```
# RIPCache 8m
```

> اصطلاح RIP برای اشاره به پروتکل Routing Information Protocol نیز به کار می‌رود، اما در این مورد هیچ ارتباطی به پروتکل مزبور ندارد.

در صورتی که پردازش وظایف چاپی توسط نرم‌افزار CUPS موجب کاهش کارایی سرور میزبان شده باشد، به کمک متغیر FilterLimit می‌توانید این تأثیر نامطلوب را کاهش دهید. مقدار پیش‌فرض این متغیر برابر با صفر است، به این معنی که عملکرد نرم‌افزار CUPS در ارتباط با پردازش وظایف چاپی مشمول هیچ محدودیتی نیست. به دستورالعمل مربوطه توجه کنید:

```
# FilterLimit 0
```

بهترین مقدار متغیر FilterLimit را می‌توانید با سعی و خطا به دست آورید. هنگام انجام این کار باید به این نکات توجه کنید. اگر تنها از یک چاپگر معمولی استفاده می‌کنید مقدار این متغیر را برابر با 200 قرار دهید. در صورت استفاده از چند چاپگر معمولی از عدد بزرگ‌تری برای این منظور استفاده کنید. اگر مقدار متغیر FilterLimit را کمتر از 200 قرار دهید، نرم‌افزار CUPS هر بار تنها یک وظیفه چاپی را مورد پردازش قرار خواهد داد.

متغیرهای مربوط به رمزگذاری

گاهی اوقات رمزگذاری درخواست‌های ارسالی از طریق شبکه به یک ضرورت اجتناب‌ناپذیر تبدیل می‌شود. به کمک متغیرهایی که در این بخش توضیح خواهیم داد، می‌توانید ترتیبی دهید که نرم‌افزار CUPS درخواست‌های رمزگذاری شده ارسالی را موردپردازش قرار دهد. شناسه یا اصطلاحاً certificate و کلید موردنیاز برای انجام این فرآیند را می‌توان با استفاده از دو متغیر ServerCertificate و

ServerKey مشخص کرد. به دستورالعمل‌های مربوطه توجه کنید:

```
# ServerCertificate /etc/cups/ssl/server.crt
# ServerKey /etc/cups/ssl/server.key
```

با مقداردهی متغیر RootCertDuration می‌توان ترتیبی داد که هر دو عامل فوق پس از سپری شدن دوره زمانی مشخصی (برحسب ثانیه) دستخوش تغییر شوند. مقدار پیش‌فرض این متغیر برابر با ۳۰۰ است، به این معنی که پس از گذشت ۳۰۰ ثانیه عوامل مزبور تغییر خواهند کرد. به دستورالعمل مربوطه توجه کنید:

```
# RootCertDuration 300
```

متغیرهای مربوط به حساب کاربران نرم‌افزار CUPS

با وجودی که سرور چاپ نرم‌افزار CUPS توسط کاربر اصلی (اصطلاحاً root) راه‌اندازی می‌شود، وظایف چاپی توسط سایر کاربران که از دسترسی محدودتری به این نرم‌افزار برخوردار هستند ارسال می‌شود. اگر نرم‌افزار CUPS را از کامپیوتر دیگری غیر از کامپیوتری که نرم‌افزار CUPS روی آن نصب شده است، مورد دستیابی قرار دهید، این نرم‌افزار شناسه کاربری متفاوتی را به شما تخصیص خواهد داد. این شناسه توسط متغیر RemoteRoot مشخص می‌شود. مقدار پیش‌فرض این متغیر برابر با remroot است. به دستورالعمل مربوطه توجه کنید:

```
# RemoteRoot remroot
```

متغیرهای User و Group با مقادیر پیش‌فرض lp و sys به ترتیب نام کاربر و نام گروه استاندارد را مشخص می‌کنند. به دستورالعمل‌های مربوطه توجه کنید:

```
# User lp
# Group sys
```

برای بی‌تأثیر کردن این تنظیمات کافی است متغیر RunAsUser را به این صورت مقداردهی کنید:

```
RunAsUser Yes
```

تنظیمات اولیه مربوط به شبکه

نرم‌افزار CUPS برای شبکه‌های TCP/IP طراحی شده است. از این‌رو می‌توانید آن‌را به نحوی پیکربندی کنید که از طریق یک پورت مشخص پیغام‌های ارسالی از جانب کامپیوترهای به خصوصی از شبکه را دریافت کند. برای مثال، این دستورالعمل‌ها ترتیبی می‌دهند تا نرم‌افزار CUPS از طریق پورت شماره ۶۳۱ پیغام‌های ارسالی از کامپیوتری با نام linux.mommabears.com و شبکه‌ای با آدرس 192.168.22.0 را دریافت کند:

```
Port 631
Listen linux.mommabears.com
Listen 192.168.22.0
```

اگر مایلید تا مشابه دومین دستورالعمل فوق (یعنی Listen linux.mommabears.com) از نام کامپیوتر موردنظر استفاده کنید، باید متغیر HostNameLookups را به این صورت مقداردهی کنید:

HostNameLookups On

در صورت تمایل می‌توانید این تنظیمات را با یکدیگر ترکیب کنید. برای مثال، دستورالعمل زیر ترتیبی می‌دهد تا نرم‌افزار CUPS از طریق پورت شماره ۸۰ درخواست‌های ارسالی از شبکه‌ای با آدرس 10.11.12.0 را دریافت کند:

```
Listen 10.11.12.0:80
```

در نسخه 2.0.x از وب سرور Apache دستورالعمل Listen جایگزین دستورالعمل Port شده است. (برای اطلاع بیشتر در این زمینه به فصل سی‌ام مراجعه کنید.)

در فایل پیکربندی cupsd.conf بهتر است به جای اسامی میزبان‌ها از آدرس‌های IP متناظر استفاده شود، چرا که مراجعه به سرور DNS برای ترجمه اسامی میزبان‌ها به آدرس‌های IP موجب اتلاف وقت شده و در نتیجه از سرعت عملیات سرور چاپ نرم‌افزار CUPS کاسته خواهد شد. با وجود این، در صورت تمایل به استفاده از اسامی میزبان‌ها در فایل پیکربندی cupsd.conf لازم است متغیر HostNameLookups را به نحو گفته شده مقداردهی کنید. با آن‌که مقدار پیش‌فرض این متغیر برابر با Off است، این دستورالعمل غیرفعال در فایل پیکربندی cupsd.conf از سیستم‌عامل Red Hat Linux به چشم می‌خورد:

```
# HostNameLookups On
```

نرم‌افزار CUPS درحالت عادی به واسطه مقدار پیش‌فرض متغیر KeepAlive یعنی مقدار On اقدامی را برای بستن اتصال ایجاد شده با وب سرور صورت نمی‌دهد. با وجود این، در صورت استفاده از مرورگرهای قدیمی‌تر مانند Netscape 2.x متغیر نامبرده کاملاً بی‌تأثیر است. تحت این شرایط باید حداکثر مدت زمانی را که این نرم‌افزار برای دریافت پاسخ از وب سرور منتظر می‌ماند، مشخص کنید. طی این مدت نرم‌افزار CUPS برای بستن اتصال ایجاد شده با وب سرور موردنظر اقدام نخواهد کرد. متغیر KeepAliveTimeout جهت تعیین این شاخص پیش‌بینی شده است. از این‌رو، برای تعیین مدت زمان مذکور بر حسب ثانیه کافی است این متغیر را مقداردهی کنید. دستورالعمل‌های مربوطه چنین است:

```
# KeepAlive On
# KeepAliveTimeout 60
```

متغیرهای مربوط به محدودیت دسترسی کاربران

بدیهی است که کاربران هر شبکه‌ای به هنگام نیاز، درخواست‌های خود را برای سرور چاپ مستقر در شبکه ارسال می‌کند. متغیر MaxClients در فایل پیکربندی cupsd.conf به منظور محدود کردن تعداد درخواست‌های ارسالی کاربران شبکه به سرور چاپ نرم‌افزار CUPS پیش‌بینی شده و مقدار پیش‌فرض آن برابر با ۱۰۰ است، به این معنی تنها ۱۰۰ کاربر می‌توانند به طور هم‌زمان درخواست‌های خود را به این سرور ارسال کنند. به دستورالعمل مربوطه توجه کنید:

```
# MaxClients 100
```

در صورت تمایل می‌توان چندین مرتبه برای ورود به کامپیوتر میزبان اقدام کرد. این تعداد به طور متوسط برابر با یک دهم مقدار متغیر MaxClients است.

گاهی اوقات لازم است وظایف چاپی بسیار بزرگ را به دیگر سرورهای چاپ ارجاع داد. متغیر MaxRequestSize امکان تعیین حداکثر اندازه وظایف چاپی ارسالی به سرور چاپ نرم‌افزار CUPS را بر حسب بایت یا مگابایت در اختیار می‌گذارد. مقدار پیش‌فرض این متغیر برابر با صفر است به این معنی که هیچ محدودیتی در اندازه وظایف چاپی ارسالی به سرور مزبور وجود ندارد. به دستورالعمل مربوطه توجه کنید:

```
# MaxRequestSize 0
```

در این زمینه دو متغیر دیگر با عناوین MaxJobsPerPrinter و MaxJobsPerUser نیز در فایل پیکربندی cupsd.conf پیش‌بینی شده است. به کمک این متغیرها می‌توان تعداد وظایف چاپی ارسالی به هریک از چاپگرها و هم‌چنین تعداد وظایف چاپی ارسالی از جانب هر کاربر را محدود کرد.

چنان‌چه بعد از برقراری ارتباط لازم میان برنامه کاربردی و سرور چاپ نرم‌افزار CUPS برنامه مزبور وظیفه چاپی موردنظر را با تأخیری بیش از آن‌چه توسط متغیر Timeout (بر حسب ثانیه) مشخص شده است، ارسال کند، سرور چاپ ارتباط را قطع خواهد کرد. مقدار پیش‌فرض این متغیر برابر با ۳۰۰ است. به دستورالعمل مربوطه توجه کنید:

```
# Timeout 300
```

متغیرهای مربوط به بازبینی چاپگرها

این دسته از متغیرها در ارتباط با امکان مشاهده چاپگرهای CUPS توسط کامپیوترهای مستقر در شبکه میزبان (یا حتی سایر شبکه‌ها) پیش‌بینی شده‌اند. دراین میان مقدار پیش‌فرض متغیر Browsing برابر با On است. سایر متغیرها به نحوه مشاهده چاپگرهای CUPS توسط کامپیوترهای مستقر در شبکه مربوط می‌شوند.

برای مشاهده چاپگرهای CUPS توسط کامپیوترهای مستقر در شبکه دو پروتکل با عناوین CUPS و SLPv2 در نظر گرفته شده است. پروتکل CUPS اطلاعات مربوط به چاپگرهای CUPS را در سرتاسر شبکه توزیع می‌کند. پروتکل SLPv2 که دومین نسخه از پروتکل Service Location Protocol یا به اختصار SLP است، این امکان را در اختیار کامپیوترها قرار می‌دهد که از وجود سرویس‌های قابل استفاده موجود در شبکه اطلاع حاصل کنند.

هر دو پروتکل فوق را می‌توان به منظور جمع‌آوری و توزیع اطلاعات چاپگرهای قابل استفاده موجود در شبکه مورد بهره‌برداری قرار داد. با وجود این، پروتکل CUPS در این مورد پروتکل پیش‌فرض محسوب می‌شود. برای استفاده از پروتکل SLPv2 دست کم باید نسخه‌ای از سرویس SLPv2 directory agent روی شبکه نصب شده باشد. در صورت تمایل می‌توان یکی از دو پروتکل CUPS یا SLPv2 یا هر دو را فعال کرد. به دستورالعمل‌های مربوطه توجه کنید:

```
# BrowseProtocols cups
# BrowsProtocols slp
# BrowseProtocols all
```

سرور چاپ نرم‌افزار CUPS برای توزیع اطلاعات موردنظر به یک آدرس همگانی نیاز دارد. این آدرس همگانی که معمولاً همان آدرس IP شبکه است توسط متغیر BrowseAddress مشخص می‌شود. چنان‌چه شبکه موردنظر شامل اتصالاتی از نوع شماره‌گیری (اصطلاحاً dial-up) باشد، مقدار متغیر مزبور را برابر با @LOCAL قرار دهید. هم‌چنین اگر مایلید تا امکان مشاهده چاپگرهای CUPS را تنها از طریق کارت شبکه‌ای با شاخص eth2 فراهم کنید مقدار این متغیر را برابر با @IF(eth2) قرار دهید. محدودیتی در تعداد دفعات مقداردهی متغیر BrowseAddress وجود ندارد. در این زمینه به چند مثال توجه کنید:

```
# BrowsAddress 192.168.99.255
# BrowsAddress 10.255.255.255
# BrowsAddress @IF(eth1)
```

در صورتی که برای نام‌گذاری چاپگرها از اسامی توصیفی هم‌چون hplaser@joescomp استفاده شده باشد، نیازی نیست که موقعیت آن‌ها را مشخص کنید. بهره‌گیری از این قابلیت مستلزم آن است که مقدار متغیر BrowseShortNames برابر با No باشد. اگر تعداد چاپگرهای مورد استفاده قابل توجه نباشد استفاده از اسامی کوتاه مانند "hplaser3" برای نام‌گذاری آن‌ها معقول بوده و مقدار پیش‌فرض متغیر BrowseShortNames یعنی Yes مناسب است. به دستورالعمل مربوطه توجه کنید:

```
# BrowseShortNames Yes
```

هر بار که چاپگر جدیدی را به مجموعه چاپگرهای CUPS موجود اضافه می‌کنید، نرم‌افزار CUPS باید برای به روز رسانی لیست اسامی چاپگرهای قابل دستیابی اقدام کند. متغیر BrowseInterval دوره تناوب این اقدام نرم‌افزار CUPS را بر حسب ثانیه مشخص می‌کند. به طور پیش فرض، لیست مزبور هر ۳۰ ثانیه یک بار به‌روزرسانی می‌شود. به دستورالعمل مربوطه توجه کنید:

```
# BrowseInterval 30
```

اگر برای مقداردهی این متغیر از عدد صفر استفاده شود، توزیع اطلاعات مربوط به آن دسته از چاپگرهای CUPS که اخیراً به مجموعه اضافه شده‌اند، به طور خودکار انجام نمی‌شود. با وجود این، به کمک متغیر BrowsePoll می‌توان آدرس و شماره پورت TCP/IP کامپیوتری را مشخص کرد که از آن طریق امکان دستیابی به لیست چاپگرهای CUPS موجود فراهم می‌شود. برای مثال، به واسطه این دستورالعمل می‌توان چنین لیستی را از طریق پورت TCP/IP شماره ۶۳۱ کامپیوتری با آدرس 192.168.0.222 مورد دستیابی قرار داد:

```
# BrowsePoll 192.168.0.222:631
```

متغیر دیگر در این زمینه BrowseTimeout است. نکته مهم در مورد متغیر مذکور این است که هرگز نباید مقدار آن کمتر از مقدار متغیر BrowseInterval باشد. در غیر این صورت، پیش از آن‌که چاپگرها قابل دستیابی باشند، از لیست چاپگرهای CUPS موجود حذف خواهند شد. مقدار پیش‌فرض این متغیر برابر با ۳۰۰ است. به دستورالعمل مربوطه توجه کنید:

```
# BrowseTimeout 300
```

متغیر BrowseRelay امکان دستیابی به سایر شبکه‌ها را فراهم می‌کند. دستورالعمل‌هایی که در ادامه ملاحظه می‌کنید نحوه مقداردهی این متغیر را جهت ارسال لیست چاپگرهای CUPS موجود به کامپیوترهای مستقر در سایر شبکه‌ها نشان می‌دهد. آدرس نخست باید روی شبکه محلی مستقر باشد. در صورت استفاده از آدرس‌های IP برای این منظور، آدرس دوم می‌تواند آدرس همگانی شبکه موردنظر باشد:

```
# BrowseRelay 192.168.0.222 10.12.15.255
# BrowseRelay 192.168.0.0/24 10.12.15.255
```

پورت TCP/IP شماره ۶۳۱ پورت پیش‌فرض برای توزیع همگانی اطلاعات توسط نرم‌افزار CUPS است. این پورت در واقع پورت مخصوص پروتکل Internet Print Protocol یا به اختصار IPP است. در صورت تمایل می‌توانید پورت دیگری را جهت انجام این عملیات انتخاب کرده و از این‌رو ضریب امنیتی را نیز افزایش دهید. برای این منظور باید متغیر BrowsePort را با شماره پورت TCP/IP موردنظر مقداردهی کنید. مقدار پیش‌فرض این متغیر برابر با ۶۳۱ است. به دستورالعمل مربوطه توجه کنید:

```
# BrowsePort 631
```

متغیرهای تضمین کننده امنیت در دسترسی به اطلاعات چاپگرهای CUPS

به کمک این متغیرها می‌توانید دسترسی به لیست چاپگرهای CUPS موجود را محدود کنید. در حالی که متغیر BrowseAllow امکان دسترسی به این اطلاعات را در اختیار کامپیوترهای موردنظر از شبکه قرار می‌دهد، متغیر BrowseDeny از دسترسی آن‌ها به اطلاعات مزبور جلوگیری می‌کند. نکته قابل توجه این‌که به کمک متغیر BrowseAllow می‌توان دسترسی تمام کامپیوترهای شبکه را به اطلاعات موردنظر فراهم کرد. این در حالی است که به کمک متغیر BrowseDeny نمی‌توان از دسترسی تمام کامپیوترهای شبکه به این اطلاعات ممانعت به عمل آورد. تعیین آدرس شبکه در قالب آدرس IP یا نام حوزه مربوطه به طرق مختلف امکان‌پذیر است. در این مورد به چند مثال توجه کنید:

```
# BrowsAllow 10.12.0.0/24
# BrowsAllow 10.12.0.0/255.255.0.0
# BrowsAllow all
# BrowsDeny *.example.com
# BrowsDeny none
# BrowsDeny @IF(eth1)
```

ترتیب تأثیرگذاری این متغیرها توسط متغیر دیگری با عنوان BrowseOrder مشخص می‌شود. فرض کنید متغیر مذکور به این صورت مقداردهی شده باشد:

```
# BrowseOrder allow,deny
```

تحت این شرایط، غیر از کامپیوترهایی که توسط متغیر BrowseDeny مشخص شده‌اند، دسترسی سایر کامپیوترها به اطلاعات موردنظر بلامانع خواهد بود. اکنون فرض کنید که متغیر BrowseOrder به این صورت مقداردهی شده باشد:

```
# BrowseOrder deny,allow
```

تحت چنین شرایطی، غیر از کامپیوترهایی که توسط متغیر BrowseAllow مشخص شده‌اند، دسترسی سایر کامپیوترها به اطلاعات موردنظر امکان‌پذیر نخواهد بود.

برای استفاده از اسامی حوزه‌ها و اسامی میزبان‌ها در فایل پیکربندی cupsd.conf باید مقدار متغیر HostNameLookups را برابر با On قرار دهید.

متغیرهای مربوط به امنیت سیستم

مکانیزم امنیتی به کار رفته در فایل پیکربندی cupsd.conf بسیار شبیه به مکانیزم امنیتی مورد استفاده در فایل پیکربندی وب سرور Apache است، به طوری که با بهره‌گیری از فرم‌های مختلف

دستورالعمل <container /> می‌توان دسترسی از طریق کامپیوترهای موردنظر را به کلاس‌ها و چاپگرهای CUPS، وظایف چاپی و سایر موارد محدود کرد. تنظیمات پیش‌فرض فایل پیکربندی cupsd.conf در سیستم‌عامل Red Hat Linux چنان است که دسترسی به سرور چاپ نرم‌افزار CUPS را تنها در اختیار کامپیوتر محلی قرار می‌دهد. به بخش مربوطه از این فایل توجه کنید:

```
<Location />
Order Deny,Allow
Deny from All
Allow From 127.0.0.1
</Location>
```

در صورت تمایل می‌توانید نحوه دسترسی سایر کامپیوترها به سرور چاپ نرم‌افزار CUPS را با ذکر آدرس IP مربوطه درقالب‌عادی‌یابه‌شیوه CIDR مشخص‌کنید.چنان‌چه‌مقدارمتغیر HostNameLookups برابر با On باشد، علاوه بر آدرس IP می‌توانید از اسامی میزبان‌ها و اسامی حوزه‌ها نیز برای این منظور استفاده کنید. به این دو مثال توجه کنید:

```
<Location /AnyPrinter>
Order Deny,Allow
Deny from All
Allow From 127.0.0.1
</Location>

<Location /AnyPrinter/HPLaserJet>
Order Deny,Allow
Deny from All
Allow From 127.0.0.1
</Location>
```

چنان‌که مشاهده می‌کنید، در مثال نخست دسترسی به کلاس AnyPrinter و در مثال دوم دسترسی به چاپگر HPLaserJet از کلاس AnyPrinter محدود شده است. شرح فرم‌های مختلف دستورالعمل <Location /> در جدول ۱۱-۲۵ آمده است.

جدول ۱۱-۲۵ شرح فرم‌های مختلف دستورالعمل <Location />

عنوان دستورالعمل	توضیح
<Location />	این دستورالعمل جهت محدود کردن هرگونه عملیات چاپی نرم‌افزار CUPS مورد استفاده قرار می‌گیرد.

عنوان دستورالعمل	توضیح
<Location /admin>	این دستورالعمل جهت محدود کردن عملیات مدیریتی نرم‌افزار CUPS مورد استفاده قرار می‌گیرد.
<Location /classes>	این دستورالعمل جهت محدود کردن دسترسی به کلاس‌ها مورد استفاده قرار می‌گیرد.
<Location /classes/*classname*>	این دستورالعمل برای محدود کردن یک کلاس به خصوص که در این‌جا با متغیر *classname* مشخص شده است، مورد استفاده قرار می‌گیرد.
<Location /jobs>	این دستورالعمل برای محدود کردن مدیریت وظایف چاپی مورد استفاده قرار می‌گیرد.
<Location /printers>	این دستورالعمل برای محدود کردن مدیریت تمام چاپگرها مورد استفاده قرار می‌گیرد.
<Location /printers/*printername*>	این دستورالعمل برای محدود کردن یک چاپگر به خصوص که در این‌جا با منغیر *printername* مشخص شده است، مورد استفاده قرار می‌گیرد.

انتهای هریک از این دستورالعمل‌ها را باید با علامت < Location/> مشخص کنید. علاوه بر فرامین Order، Deny و Allow فرامین دیگری را نیز می‌توان در قالب دستورالعمل </ Location> مورد استفاده قرار داد. جدول ۱۲-۲۵ تمام این فرامین را شرح می‌دهد.

جدول ۱۲-۲۵ شرح فرامین قابل استفاده در دستورالعمل </ Location>

عنوان فرمان	توضیح
Allow	به کمک این فرمان می‌توان امکان دسترسی کامپیوترهای موردنظر به یک چاپگر یا کلاس به خصوص را مهیا کرد.
Anonymous	با استفاده از این فرمان می‌توان فرآیند دسترسی به منبع موردنظر را به صورت ناشناس یعنی بدون نیاز به نام کاربری کلمه عبور انجام داد. به طور پیش فرض، دسترسی به صورت ناشناس انجام می‌شود.
AuthClass	با استفاده از این فرمان می‌توان اطلاعات موردنیاز برای احراز هویت را مشخص کرد. گزینه‌های مربوطه عبارتند از Anonymous، User، System و Group.

عنوان فرمان	توضیح
AuthGroupName	با استفاده از این فرمان می‌توان گروه موردنظر برای احراز هویت را مشخص کرد.
AuthType	با استفاده از این فرمان می‌توان نوع احراز هویت را مشخص کرد. گزینه‌های مربوطه عبارتند از None، Basic، Digest و Basic Digest.
Deny	به کمک این فرمان می‌توان دسترسی کامپیوترهای موردنظر را به یک چاپگر یا کلاس به خصوص محدود کرد.
Encryption	با استفاده از این فرمان می‌توان خط مشی رمزگذاری اسامی کاربران و کلمات عبور را مشخص کرد. گزینه‌های مربوطه عبارتند از Never، IFRequested، Required و Always.
Limit	با استفاده از این فرمان می‌توان فرامین مجاز نرم‌افزار CUPS را مشخص کرد.
LimitExcept	با استفاده از این فرمان می‌توان فرامین غیرمجاز نرم‌افزار CUPS را مشخص کرد.
Order	با استفاده از این فرمان می‌توان اولویت تأثیرگذاری فرامین Allow و Deny را مشخص کرد.
Require	با استفاده از این فرمان می‌توان دسترسی به یک گروه، کاربر یا تمام کاربران را محدود کرد.

متغیرهای مربوط به کلاس‌ها

با بهره‌گیری از متغیر ImplicitClases می‌توان چاپگرهای هم‌نام را در قالب کلاس‌های مختلفی که به طور ضمنی ایجاد می‌شوند، دسته‌بندی کرد. برای این منظور کافی است مقدار این متغیر را برابر با On قرار دهید. (مقدار پیش‌فرض این متغیر برابر با On است.) به دستورالعمل مربوطه توجه کنید:

```
# ImplicitClasses On
```

برای ایجاد کلاس‌های ضمنی کافی است متغیر ImplecitAnyClasses را به صورت ImplicitAnyClasses On مقداردهی کنید. مقدار پیش‌فرض این متغیر برابر با Off است. به دستورالعمل مربوطه توجه کنید:

```
# ImplicitAnyClasses Off
```

در صورت استفاده از قابلیت کلاس‌های ضمنی، به کمک متغیر HideImplicitMembers می‌توانید ترتیبی دهید که لیست چاپگرهای موجود در این گونه کلاس‌ها قابل دستیابی نباشد. برای این منظور کافی است متغیر مزبور را به صورت HideImplicitMembers On مقداردهی کنید. مقدار پیش‌فرض این متغیر برابر با On است. به دستورالعمل مربوطه توجه کنید:

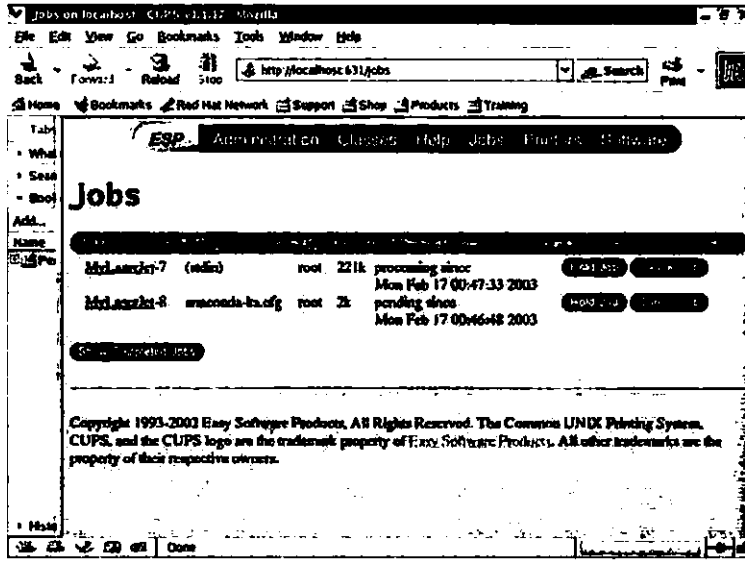
```
# HideImplicitMembers On
```

مدیریت چاپگرها

پس از پیکربندی نرم‌افزار CUPS می‌توان به مدیریت وظایف چاپی پرداخت. رابط گرافیکی نرم‌افزار مذکور امکانات لازم برای این کار را در اختیار می‌گذارد. علاوه بر این، در صورت تمایل می‌توان سرویس cups-lpd را نیز به منظور بهره‌برداری از فرامین استاندارد سیستم چاپ LPD شامل lpr، lpq و lprm نصب و پیکربندی کرد. (فرامین مذکور را به زودی در همین فصل مورد بررسی قرار خواهیم داد.) و بالاخره با بازبینی فایل‌های ثبت وقایع نرم‌افزار CUPS که در فهرست /var/log/cups مستقر هستند، می‌توان از وجود خطاهای احتمالی و دسترسی غیرمجاز به سرویس چاپ CUPS و موارد مفید دیگر اطلاع حاصل کرد.

مدیریت وظایف چاپی

مدیریت وظایف چاپی در نرم‌افزار CUPS بسیار ساده است. تمام امکانات لازم برای انجام این کار از طریق منوی Jobs قابل دستیابی است. شکل ۱۵-۲۵ منوی مزبور را که شامل مشخصات دو وظیفه چاپی با عناوین MyLaserJet-7 و MyLaserJet-8 است، نشان می‌دهد. در صورت تمایل می‌توانید با کلیک روی دکمه Hold Job مربوط به وظیفه چاپی MyLaserJet-7 ترتیبی دهید تا وظیفه چاپی MyLaserJet-8 قبل از آن انجام شود. با این کار پیغام "Job 7 has been held from printing" به نمایش درآمده و اقدامات لازم برای انجام وظیفه چاپی MyLaserJet-8 به طور خودکار انجام می‌شود.



شکل ۱۵-۲۵ مدیریت وظایف چاپی با استفاده امکانات منوی Jobs

ضمناً وظیفه چاپی MyLaserJet-7 هم‌چنان در صف چاپ باقی می‌ماند تا این‌که با مراجعه مجدد به منوی Jobs و کلیک روی دکمه Release Job مربوط به وظیفه چاپی مزبور آن‌را فعال کنید.

بهره‌برداری از فرامین سیستم چاپ LPD

برای استفاده از فرامین سیستم چاپ LPD در نرم‌افزار CUPS باید سرویس cups-lpd را که در فهرست /etc/xinetd.d واقع شده، راه‌اندازی کنید. برای این منظور فرمان chkconfig service cups-lpd on را اجرا کنید. (جهت اطلاع بیشتر درباره سرویس‌های xinetd به فصل بیست و سوم مراجعه کنید.)

راه‌اندازی سرویس cups-lpd در مورد آن دسته از برنامه‌های کاربردی که مکانیزم چاپ آن‌ها به طور خاص برای استفاده از سیستم چاپ LPD طراحی شده ضروری است.

فایل‌های ثبت وقایع نرم‌افزار CUPS

فایل‌های ثبت وقایع نرم‌افزار CUPS در فهرست /var/cups/log مستقر شده‌اند. یکی از این فایل‌ها با عنوان access_log شامل لیست کامپیوترهایی است که سرور CUPS را مورد دستیابی قرار داده‌اند. در هر مورد تاریخ و ساعت دسترسی به سرور CUPS نیز ثبت می‌شود. شکل ۱۶-۲۵ محتوای یک چنین فایلی را نشان می‌دهد. چنان‌چه مشاهده می‌کنید، کلیه دسترسی‌ها از طریق کامپیوتری با شناسه localhost (کامپیوتر میزبان سرور CUPS) انجام شده است.

```
localhost - root [29/Mar/2003:13:57:21 -0500] "POST /admin/ HTTP/1.1" 200 342
localhost - root [29/Mar/2003:13:57:18 -0500] "POST /admin HTTP/1.1" 200 1780
localhost - - [29/Mar/2003:13:57:24 -0500] "POST / HTTP/1.1" 200 220
localhost - - [29/Mar/2003:13:57:25 -0500] "GET /classes/HPLasers HTTP/1.1" 200
0
localhost - - [29/Mar/2003:13:57:25 -0500] "POST / HTTP/1.1" 200 77
localhost - - [29/Mar/2003:13:57:28 -0500] "POST / HTTP/1.1" 200 125
localhost - - [29/Mar/2003:13:57:28 -0500] "POST / HTTP/1.1" 200 125
localhost - - [29/Mar/2003:13:57:25 -0500] "GET /classes/HPLasers HTTP/1.1" 200
3170
localhost - - [29/Mar/2003:13:57:29 -0500] "GET /images/classes.gif HTTP/1.1" 20
0 591
localhost - - [29/Mar/2003:13:57:29 -0500] "GET /images/stop-class.gif HTTP/1.1"
 200 245
localhost - - [29/Mar/2003:13:57:29 -0500] "GET /images/delete-class.gif HTTP/1.
1" 200 259
localhost - - [29/Mar/2003:13:57:29 -0500] "GET /images/modify-class.gif HTTP/1.
1" 200 267
localhost - - [29/Mar/2003:13:57:28 -0500] "POST / HTTP/1.1" 200 220
localhost - - [29/Mar/2003:13:57:31 -0500] "GET /classes HTTP/1.1" 200 0
localhost - - [29/Mar/2003:13:57:31 -0500] "POST / HTTP/1.1" 200 77
localhost - - [29/Mar/2003:13:57:32 -0500] "POST / HTTP/1.1" 200 77
localhost - - [29/Mar/2003:13:57:31 -0500] "GET /classes HTTP/1.1" 200 3010
```

شکل ۱۶-۲۵ محتوای فایل access_log

محتوای فایل error_log چیزی بیش از خطاهای استاندارد است. این فایل حاوی لیست فعالیت‌های سرور CUPS در ارتباط با وظایف چاپی و سایر موارد است. شکل ۱۷-۲۵ محتوای یک چنین فایلی را نشان می‌دهد.

```
I [29/Mar/2003:13:54:11 -0500] Started "/usr/lib/cups/cgi-bin/jobs.cgi" (pid=240
9)
E [29/Mar/2003:13:54:11 -0500] cancel_job: "" not authorized to delete job id 4
owned by "root"!
I [29/Mar/2003:13:54:14 -0500] Started "/usr/lib/cups/cgi-bin/jobs.cgi" (pid=241
0)
I [29/Mar/2003:13:54:28 -0500] Started "/usr/lib/cups/cgi-bin/printers.cgi" (pid
=2411)
I [29/Mar/2003:13:54:33 -0500] Started "/usr/lib/cups/cgi-bin/admin.cgi" (pid=24
12)
I [29/Mar/2003:13:55:07 -0500] Started "/usr/lib/cups/cgi-bin/admin.cgi" (pid=24
15)
I [29/Mar/2003:13:55:15 -0500] Started "/usr/lib/cups/cgi-bin/admin.cgi" (pid=24
16)
I [29/Mar/2003:13:55:20 -0500] Started "/usr/lib/cups/cgi-bin/admin.cgi" (pid=24
17)
I [29/Mar/2003:13:55:23 -0500] Started "/usr/lib/cups/cgi-bin/admin.cgi" (pid=24
18)
I [29/Mar/2003:13:55:25 -0500] Setting SecondLaserJet device-uri to "parallel:/d
ev/lp0" (was "".)
I [29/Mar/2003:13:55:25 -0500] Setting SecondLaserJet printer-is-accepting-jobs
to 1 (was 0.)
#
```

شکل ۱۷-۲۵ محتوای فایل error_log

فایل page_log حاوی لیست وظایف چاپی مستقر شده در صف چاپ است. این لیست حتی وظایف چاپی لغو شده را نیز شامل می‌شود. شکل ۱۸-۲۵ محتوای یک چنین فایلی را نشان می‌دهد.

استفاده از سیستم چاپ LPD

سرور چاپ CUPS به عنوان سرور چاپ پیش‌فرض در سیستم‌عامل Red Hat Linux مورد استفاده واقع می‌شود. با وجود این، برخی از کاربران به دلایل مختلف استفاده از سیستم چاپ LPD را ترجیح می‌دهند. علیرغم امکانات مختلف، این سیستم چاپ، فاقد برخی از ویژگی‌های بارز سیستم چاپ CUPS از جمله امکان پیکربندی کلاس‌های چاپ است. از طرف دیگر، سیستم چاپ CUPS براساس پروتکل IPP که امروزه توسط بسیاری از سیستم‌عامل‌ها مورد پشتیبانی قرار گرفته پیاده‌سازی شده است.

```
MyLaserJet root 1 [29/Mar/2003:13:46:32 -0500] 1 1
MyLaserJet root 2 [29/Mar/2003:13:47:18 -0500] 1 1
MyLaserJet root 3 [29/Mar/2003:13:50:10 -0500] 1 1
MyLaserJet root 4 [29/Mar/2003:13:50:34 -0500] 1 1
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
"/var/log/cups/page_log" 4L, 208C
```

شکل ۱۸-۲۵ محتوای فایل page_log

کلیه ملزومات سیستم چاپ LPD تنها در قالب یک بسته نرم‌افزاری با عنوان LPRng-* توزیع می‌شود. از این‌رو، برای استفاده از این سیستم چاپ LPD کافی است بسته نرم‌افزاری مزبور را روی کامپیوتر موردنظر نصب کنید. فایل پیکربندی اصلی سیستم چاپ LPD یعنی /etc/printcap در قالب بسته نرم‌افزاری setup-* نصب می‌شود. ویرایش این فایل به طور دستی یا با استفاده از ابزار گرافیکی redhat-config-printer امکان‌پذیر است. پس از پیکربندی چاپگر مورد نظر، با بهره‌گیری از فرامینی مانند lpr، lpq، lpc و lprm می‌توانید از امکانات سیستم چاپ LPD برای مدیریت وظایف چاپی استفاده کنید.

پیکربندی LPD به عنوان سیستم چاپ پیش‌فرض

در نسخه‌های اخیر سیستم‌عامل Red Hat Linux سرویس cupsd به طور پیش‌فرض فعال می‌شود. با وجود این، می‌توانید با اجرای دو فرمان service cups stop و service lpd start سرویس مزبور را غیرفعال و سرویس lpd را فعال کنید. سپس فرمان chkconfig cups-lpd off را برای غیرفعال کردن سرویس cups-lpd اجرا کرده و در نهایت با استفاده از ابزار redhat-switch-printer سیستم چاپ LPD را با CUPS جایگزین کنید.

در صورت تمایل، با استفاده از فرمان chkconfig می‌توانید ترتیبی دهید که سرویس lpd هنگام راه‌اندازی سیستم‌عامل Linux در سطح یا سطوح اجرایی موردنظر راه‌اندازی شود. (برای اطلاع بیشتر در این زمینه به فصل سیزدهم مراجعه کنید.)

فایل پیکربندی اصلی سرویس چاپ LPD

کاربران با تجربه سیستم‌عامل Linux ترجیح می‌دهند تا فایل‌های پیکربندی را مستقیماً در یک ویرایشگر متنی مورد ویرایش قرار دهند. با وجود این، در مورد فایل پیکربندی سیستم چاپ LPD باید دقت زیادی را صرف کنید، چرا که فرامین پیکربندی مورد استفاده در این فایل نسبتاً نامفهوم است. شکل ۱۹-۲۵ محتوای چنین فایلی را نشان می‌دهد.

```
HPLaser:\
        :ml#0:\
        :mx#0:\
        :sd=/var/spool/lpd/HPLaser:\
        :af=/var/spool/lpd/HPLaser/HPLaser.acct:\
        :sh:\
        :lp=/dev/lp0:\
        :lpd_bounce=true:\
        :if=/usr/share/printconf/util/mf_wrapper:

printer:\
        :ml#0:\
        :mx#0:\
        :sd=/var/spool/lpd/printer:\
        :af=/var/spool/lpd/printer/printer.acct:\
        :sh:\
        :lp=/dev/lp0:\
        :lpd_bounce=true:\
        :if=/usr/share/printconf/util/mf_wrapper:

printer1:\
        :ml#0:\
        :mx#0:\
```

شکل ۱۹-۲۵ محتوای نمونه‌ای از یک فایل پیکربندی اصلی سیستم چاپ LPD (فایل /etc/printcap)

در سیستم‌عامل Red Hat Linux دو فایل /etc/printcap و /etc/printcap.local برای پیکربندی سیستم چاپ LPD پیش‌بینی شده است. با وجود این، تنظیمات انجام شده از طریق ابزار گرافیکی redhat-config-printers در فایل /etc/printcap ثبت شده به طوری که تنظیمات قبلی رونویسی می‌شود.

در صورت تمایل می‌توانید پیکربندی چاپگرها را به طور دستی و بدون استفاده از ابزار گرافیکی مذکور نیز انجام دهید. برای این منظور باید فرامین موردنظر خود را مستقیماً در فایل پیکربندی /etc/printcap.local وارد کنید. محتوای این فایل پس از راه‌اندازی مجدد سرویس lpd در فایل پیکربندی /etc/printcap درج خواهد شد.

فایل پیکربندی /etc/printcap حاوی علایم و پارامترهای متعددی است. شرح برخی از آن‌ها را در جدول ۱۳-۲۵ مشاهده می‌کنید.

جدول ۱۳-۲۵ شرح برخی از علایم و پارامترهای مورد استفاده در فایل پیکربندی سرویس چاپ LPD (فایل /etc/printcap)

علامت یا پارامتر	توضیح
:	این علامت حد فاصل میان خطوط مندرج در فایل پیکربندی /etc/printcap را مشخص می‌کند.
\	این علامت دو خط مجزا را به یکدیگر متصل کرده و به این ترتیب علامت خط جدید (اصطلاحاً new line) را بی‌تأثیر می‌کند.
af	این پارامتر فیلتری از نوع accounting (اصطلاحاً accounting filter یا af) را مشخص می‌کند.
if	این پارامتر فیلتری از نوع ورودی (اصطلاحاً input filter یا به اختصار if) را مشخص می‌کند.
lp	این پارامتر اسباب چاپ خطی (اصطلاحاً line print یا lp) مربوط به چاپگر موردنظر را مشخص می‌کند.
lp_bounce	این پارامتر وضعیت ارسال وظایف چاپی از طریق یک فیلتر چاپ را مشخص می‌کند. برای ارسال وظایف چاپی از طریق فیلتر چاپ باید مقدار این پارامتر برابر با true باشد.
ml	این پارامتر وضعیت کاراکترهای غیرچاپی را مشخص می‌کند، به طوری که اگر مقدار آن غیر صفر باشد، از چاپ بیشتر فایل‌های باینری جلوگیری به عمل می‌آید.
mx	این پارامتر حداکثر اندازه فایل ارسالی برای چاپ را مشخص می‌کند. اگر مقدار این پارامتر برابر با صفر باشد، اندازه فایل ارسالی برای چاپ مشمول هیچ محدودیتی نخواهد بود.
sd	این پارامتر فهرست مورد استفاده به عنوان سبد چاپ یا اصطلاحاً spool را مشخص می‌کند.

علامت یا پارامتر	توضیح
sh	استفاده از این پارامتر موجب جلوگیری از چاپ سرصفحه یا اصطلاحاً header می‌شود.
pl	این پارامتر طول صفحه را بر حسب تعداد خطوط مندرج در آن مشخص می‌کند.
pw	این پارامتر عرض صفحه را بر حسب تعداد کاراکترهای مندرج در خطوط آن مشخص می‌کند.

از این‌رو، می‌توان گفت که در شکل ۱۹-۲۵ تنها سه سطر فرمان وجود دارد، چرا که علامت \ برای اتصال خطوط به یکدیگر مورد استفاده قرار می‌گیرد. به بیان دیگر، این علامت خط جاری را به خط بعد از خود متصل می‌کند؛ بنابراین، تأثیر این خطوط مشابه خط ساده print:ml#0 است:

```
printer:\
        :ml#0
```

علاوه بر فایل‌های پیکربندی /etc/printcap و /etc/printcap.local در ارتباط با سیستم چاپ LPD دو فایل پیکربندی /etc/lpd.conf و /etc/lpd.perms نیز پیش‌بینی شده‌اند. نسخه پیش‌فرض این فایل‌ها برای بسیاری از کاربردها مناسب است، به طوری که برخلاف فایل پیکربندی /etc/printcap محتوای این دو فایل به ندرت مورد ویرایش قرار می‌گیرد. از این‌رو، در این‌جا تنها به کاربرد آن‌ها اشاره می‌کنیم. فایل /etc/lpd.conf حاوی تنظیمات پیش‌فرض چاپگرها و فایل /etc/lpd.perms نیز حاوی تنظیمات مربوط به مجوزهای دسترسی به برنامه‌ای موسوم به spooler است. (وظیفه این برنامه کنترل سیستم spooling یا به بیان دیگر استقرار و حذف وظایف چاپی موجود در صف چاپ است. ـ مترجم)

در صورت استفاده از سیستم چاپ CUPS فایل پیکربندی /etc/printcap شامل لیستی از چاپگرها و کلاس‌ها خواهد بود.

مدیریت چاپگرها

اغلب امور چاپی در سیستم چاپ LPD با استفاده از چهار فرمان اصلی که به فرامین lp شهرت دارند، انجام می‌شود. این فرامین عبارتند از lpr یا Line Printer Request، lpq یا Line Printer Query، lprm یا Line Printer Remove و lpc یا Line Printer Control.

در صورت فعال کردن سرویس cups-lpd می‌توانید فرامین فوق را در سیستم چاپ CUPS نیز مورد استفاده قرار دهید. با وجودی که عملکرد این فرامین در سیستم چاپ CUPS کاملاً شبیه به عملکرد آن‌ها در سیستم چاپ LPD نیست، نتایج نهایی مشابه هستند.

فرمان lpr

هنگامی که با استفاده از فرمان cat محتوای فایلی را مورد مشاهده قرار می‌دهید، مفسر سطر فرمان یا اصطلاحاً shell محتوای موردنظر را برای خروجی استاندارد ارسال می‌کند، به طوری که می‌توانید آن‌را روی صفحه نمایش مشاهده کنید. در مقابل، هنگام استفاده از فرمان lpr این خروجی درون فایلی روی کامپیوتر محلی قالب‌بندی شده و سپس برای سرور چاپ ارسال می‌شود. در نهایت سرور چاپ آن فایل را جهت چاپ برای چاپگر ارسال می‌کند. به این ترتیب فرمان lpr را می‌توان یک برنامه کلاینت محسوب کرد. فایلی که این برنامه آن‌را قالب بندی می‌کند توسط یک برنامه سرور (مشخصاً سرور چاپ یا print server) مستقر روی کامپیوتر محلی یا راه دور مورد پردازش قرار می‌گیرد.

از این‌رو، به محض اجرای فرمانی مانند lpr *file* مفسر سطر فرمان محتوای فایل *file*را برای چاپگری که در فایل /etc/printcap به عنوان چاپگر پیش‌فرض پیکربندی شده است، ارسال می‌کند. با وجود این، در صورت تمایل می‌توانید وظیفه چاپی موردنظر (در این‌جا چاپ محتوای فایل *file*) را برای چاپگر دیگری غیر از چاپگر پیش‌فرض ارسال کنید. برای مثال، چنان‌چه چاپگر دیگری با عنوان colorprinter را در فایل /etc/printcap پیکربندی کرده باشید، با اجرای این فرمان می‌توانید فایل *file1*را جهت چاپ به آن چاپگر ارسال کنید:

```
# lpr -Pcolorprinter file1
```

در فرمان فوق نباید هیچ فاصله‌ای بین گزینه P- و نام چاپگر موردنظر وجود داشته باشد.

جدول ۱۴-۱۵ شکل‌های مختلف فرمان lpr را شرح می‌دهد.

جدول ۱۴-۲۵ شرح شکل‌های مختلف فرمان lpr

فرمان	توضیح
lpr -h *file1*	این فرمان فایل *file1*را بدون چاپ صفحه کنترل وظیفه چاپی یا اصطلاحاً job control page که شامل حساب کاربری و نام کامپیوتر منبع بوده و اغلب با عنوان صفحه burst نیز شناخته می‌شود، چاپ می‌کند.

فرمان	توضیح
lpr -P*other file1*	این فرمان فایل *file1* را جهت چاپ برای چاپگری با عنوان *other* (که در قالب فایل /etc/printcap پیکربندی شده است) ارسال می‌کند.
lpr -s *file1*	این فرمان یک پیوند نمادین (اصطلاحاً symbolic link) با فایل *file1* ایجاد می‌کند، تا به این ترتیب نیازی به ایجاد فایل spool مربوطه نباشد. فرمان lpr در سیستم‌عامل BSD این اقدام را برای تمام فایل‌هایی که اندازه آن‌ها بزرگ‌تر از یک مگابایت باشد، انجام می‌دهد. برنامه lpr در سیستم‌عامل Red Hat Linux چنین ضرورتی را ایجاب نمی‌کند.

فرمان lpq

فرمان lpq صف چاپ (اصطلاحاً print queue) را نمایش می‌دهد. این اطلاعات شامل شناسه وظایف چاپی نیز می‌شود. اطلاع از شناسه وظایف چاپی در برخی موارد هنگام استفاده از فرمان lprm موردنیاز است. جدول ۱۵-۲۵ شکل‌های مختلف فرمان lpq را شرح می‌دهد.

جدول ۱۵-۲۵ شرح شکل‌های مختلف فرمان lpq

فرمان	توضیح
lpq	این فرمان صف چاپ مربوط به چاپگری را که در فایل پیکربندی /etc/printcap به عنوان چاپگر پیش‌فرض مشخص شده است، نشان می‌دهد.
lpq -P *printer*	این فرمان صف چاپ مربوط به چاپگری با عنوان *printer* را که در فایل پیکربندی /etc/printcap به عنوان یکی از چاپگرهای قابل استفاده مشخص شده است، نشان می‌دهد.

فرمان lprm

اگر حافظه چاپگر عاری از وظایف چاپی باشد، با استفاده از فرمان lprm می‌توان وظایف چاپی موجود در صف چاپ را حذف کرد. تحت این شرایط وظیفه چاپی موردنظر را می‌توان با تعیین شناسه مربوطه، شناسه کاربر یا شناسه چاپگر حذف کرد. جدول ۱۶-۲۵ شکل‌های مختلفی از این فرمان را نشان می‌دهد.

جدول ۱۶-۲۵ مثال‌هایی دراستفاده از فرمان lprm

فرمان	توضیح
lprm 188	این فرمان وظیفه چاپی با شناسه 188 را حذف می‌کند. (به کمک فرمان lpq می‌توان از شناسه وظایف چاپی اطلاع حاصل کرد.)

فرمان	توضیح
lprm -P hp2 mj	این فرمان آن دسته از وظایف چاپی مربوط به کاربری با شناسه mj را که برای چاپگری با عنوان hp2 ارسال خواهد شد، حذف می‌کند.

فرمان lpc

فرمان lpc امکان کنترل چاپگرها را در اختیار قرار می‌دهد. با استفاده از این فرمان می‌توان ضمن پی بردن به وضعیت چاپگرها، وظایف چاپی ارسالی به یک چاپگر را حذف یا آن‌ها را برای چاپگر دیگری ارسال کرد. جدول ۱۷-۲۵ کاربردهای مختلف این فرمان را شرح می‌دهد.

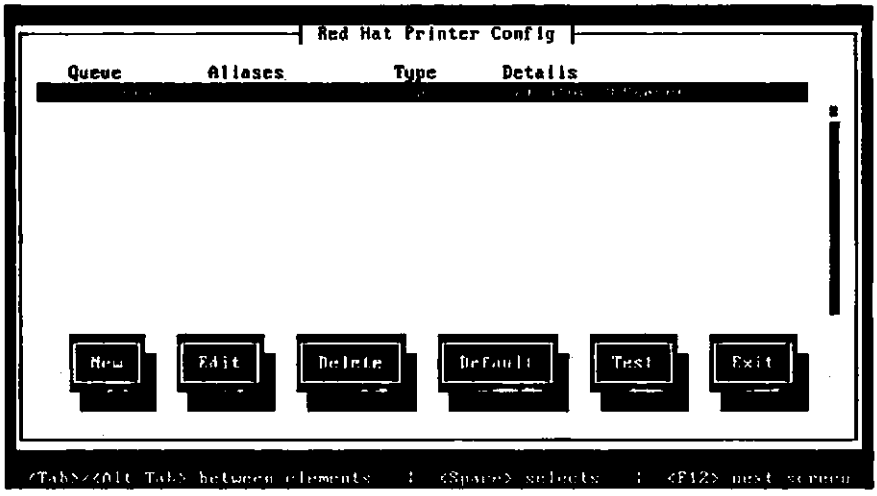
جدول ۱۷-۲۵ کاربردهای مختلف فرمان lpc

فرمان	توضیح
lpc -P canon1 status	این فرمان وضعیت چاپگری با عنوان canon1 را نشان می‌دهد. به کمک خروجی حاصل از این فرمان می‌توان به تعداد وظایف موجود در صف این چاپگر پی برد و در مورد امکان ارسال وظایف چاپی به آن اطلاع حاصل کرد.
lpc disable	این فرمان قابلیت ارسال وظایف چاپی به صف چاپ مربوط به چاپگر پیش‌فرض را غیرفعال می‌کند. برای فعال کردن این قابلیت کافی است فرمان lpc enable را اجرا کنید.
lpc start	این فرمان وظایف چاپی موجود در صف چاپ را برای چاپگر پیش‌فرض ارسال می‌کند.
lpc stop	این فرمان فرآیند ارسال وظایف چاپی موجود در صف چاپ به چاپگر پیش‌فرض را متوقف می‌کند.

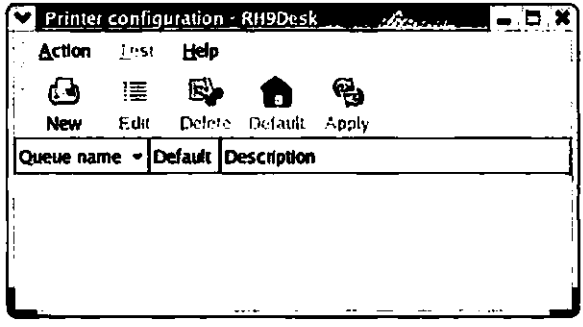
استفاده از ابزارهای گرافیکی سیستم‌عامل Red Hat Linux برای پیکربندی چاپگر

به دلیل ساختار به خصوص فایل‌های پیکربندی /etc/cups/cupsd.conf و /etc/printcap بسیاری از کاربران پیکربندی سیستم چاپ CUPS یا LPD را با استفاده از ابزارهای گرافیکی انجام می‌دهند. در سیستم‌عامل Red Hat Linux دو ابزار گرافیکی redhat-config-printer و redhat-config-printer-gui برای همین منظور پیش‌بینی شده است. پیش از به کارگیری این ابزارها باید بسته‌های نرم‌افزاری مربوطه را نصب کنید. با وجودی که ظاهر گرافیکی برنامه‌ها با یکدیگر تفاوت دارد، هر دو برنامه

امکانات یکسانی را در اختیار قرار می‌دهند. شکل‌های ۲۰-۲۵ و ۲۱-۲۵ به ترتیب رابط گرافیکی برنامه‌های redhat-config-print و redhat-config-print-gui را نشان می‌دهد.



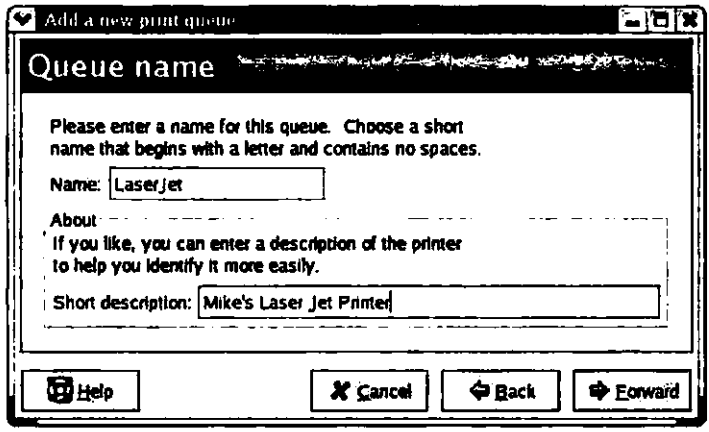
شکل ۲۰-۲۵ رابط گرافیکی برنامه redhat-config-print



شکل ۲۱-۲۵ رابط گرافیکی برنامه redhat-config-print-gui

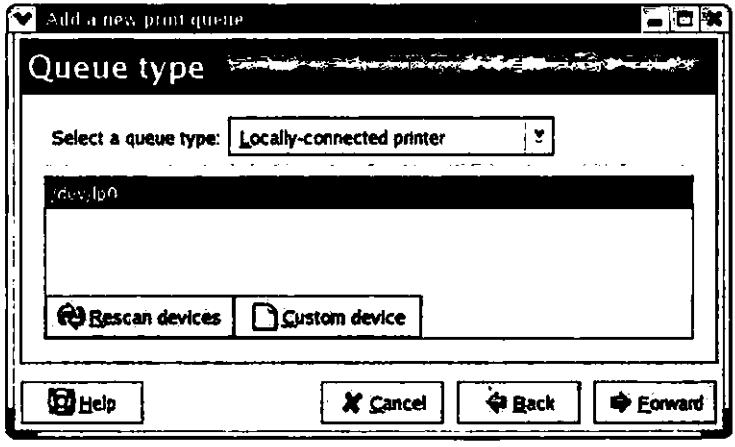
پیکربندی چاپگر با استفاده از امکانات این برنامه‌ها بسیار ساده است. به مراحل انجام این کار در برنامه redhat-config-printer-gui توجه کنید:

۱- برنامه redhat-config-printer-gui را اجراکرده و درپنجره حاصل با عنوانPrinter Configuration روی گزینه New کلیک کنید تا به این ترتیب کادر محاوره‌ای Add A New Print Queue باز شود. برای ادامه عملیات دکمه Forward را کلیک کنید. شکل ۲۲-۲۵ نتیجه این اقدام را نشان می‌دهد.



شکل ۲۲-۲۵ تعیین نام چاپگر مورد نظر

۲- نام‌چاپگر موردنظر را در کادرمتنی Name و توصیف‌مربوط به‌آن‌را در کادرمتنیShort description وارد کرده و دکمه Forward را برای ادامه عملیات کلیک کنید. شکل ۲۳-۲۵ نتیجه این اقدام را نشان می‌دهد.



شکل ۲۳-۲۵ تعیین پورت موردنظر برای ارتباط با چاپگر

۳- در این مرحله برنامه redhat-config-printer-gui پورت‌های موازی یا اصطلاحاً parallel موجود را جهت ارتباط با چاپگر نمایش می‌دهد. برای مثال، پورت /dev/lp0 بیانگر نخستین پورت موازی است. اگر چاپگر موردنظر مستقیماً به کامپیوتر میزبان متصل باشد، گزینه Locally-connected printer را از لیست Select A Queue Type انتخاب کرده و سپس پورت موازی موردنظر را

مشخص کنید. در نهایت دکمه Forward را برای ادامه عملیات کلیک کنید. در غیر این صورت، یکی از این اقدامات را انجام دهید:

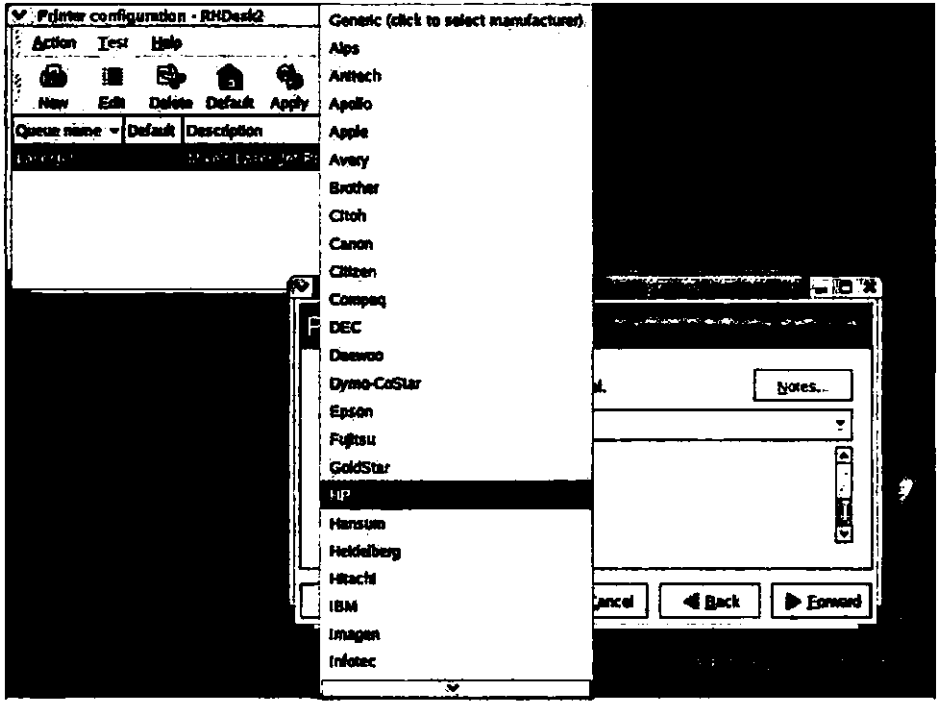
- اگر پورت موازی موردنظر را در لیست پورت‌ها مشاهده نمی‌کنید، روی دکمه Rescan Devices کلیک کنید.
- چنان‌چه پس از اقدام فوق باز هم پورت موازی موردنظر را مشاهده نمی‌کنید، روی دکمه Custom Device کلیک کرده و پورت موازی موردنظر را از لیست پورت‌های موجود انتخاب کنید.
- اگر چاپگر مستقیماً به کامپیوتر متصل نشده باشد، گزینه دیگری را از لیست Select A Queue Type انتخاب کنید. شرح این گزینه‌ها در جدول ۱۸-۲۵ آمده است.

جدول ۱۸-۲۵ شرح گزینه‌های موجود در لیست Select A Queue Type

عنوان گزینه	توضیح
Networked CUPS (IPP)	این گزینه را در صورتی انتخاب کنید که چاپگر موردنظر به یک سرور CUPS راه دور متصل باشد. در این صورت باید نام حوزه یا نام کامپیوتر میزبان سرور CUPS را در قالب پروتکل IPP مشخص کنید.
Networked Unix (LPD)	این گزینه را در صورتی انتخاب کنید که چاپگر موردنظر به یک سرور LPD راه دور متصل باشد. در این صورت باید نام حوزه یا نام کامپیوتر میزبان سرور LPD و هم‌چنین نام چاپگر را مشخص کنید.
Networked Windows (SMB)	این گزینه را در صورتی انتخاب کنید که چاپگر موردنظر روی شبکه‌ای از نوع Microsoft Windows مستقر باشد. در این صورت برنامه redhat-config-printer-gui آن چاپگر را به طور خودکار تشخیص می‌دهد.
Networked Novell (NCP)	این گزینه را در صورتی انتخاب کنید که چاپگر موردنظر روی شبکه‌ای از نوع Novell مستقر باشد. در این صورت باید نام حوزه یا کامپیوتر میزبان سرور چاپ، نام چاپگر و هم‌چنین نام کاربری و کلمه عبور لازم برای دستیابی به آن‌را مشخص کنید.
Networked JetDirect	این گزینه را در صورتی انتخاب کنید که چاپگر موردنظر به یک سرور چاپ JetDirect راه دور متصل باشد. در این صورت باید نام چاپگر را مشخص کنید.

۴- در این مرحله باید درایور چاپگر موردنظر را مشخص کنید. در انجام این کار دو نکته را مورد توجه قرار دهید:

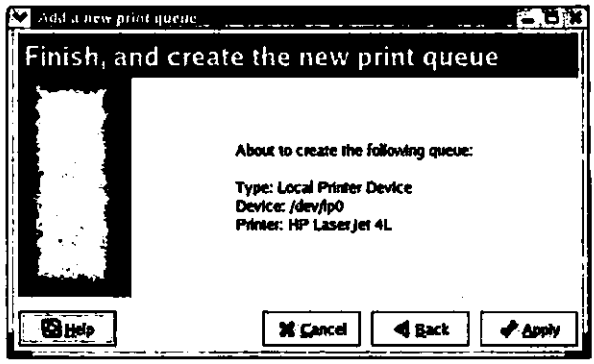
- برخی از چاپگرها با استفاده از درایور PostScript راه‌اندازی می‌شوند. می‌توان چاپگرهایی را که قابلیت چاپ داده‌های خام را دارند، با استفاده از درایور Raw Print Queue راه‌اندازی کرد. در مورد چاپگرهای متنی یا ماتریسی نیز می‌توان از درایورهای عمومی استفاده کرد.
- گزینه Generic (Click To Select Manufacturer) را برای انتخاب یک مدل به خصوص چاپگر کلیک کنید. با این اقدام لیستی از اسامی شرکت‌های سازنده چاپگر را مطابق شکل ۲۴-۲۵ مشاهده خواهید کرد. پس از تعیین شرکت سازنده می‌توانید مدل چاپگر موردنظر را انتخاب کنید.



شکل ۲۴-۲۵ تعیین شرکت سازنده چاپگر

دکمه Forward را برای ادامه عملیات کلیک کنید.

۵- چنان‌که در شکل ۲۵-۲۵ مشاهده می‌کنید، در این مرحله خلاصه‌ای از گزینش‌های مراحل قبل به نمایش درمی‌آید. برای تأیید گزینه‌های منتخب کافی است دکمه Apply را کلیک کنید.



شکل ۲۵-۲۵ خلاصه گزینش‌های مراحل قبل

۶- اگر از اتصال کامپیوترتان به چاپگر موردنظر مطمئن هستید، در این مرحله فرصت آن‌را دارید که صفحه‌ای را جهت آزمایش و اطمینان از صحت عملیات فوق برای چاپ به چاپگر موردنظر ارسال کنید. برای این منظور کافی است روی دکمه Yes کلیک کنید.

پس از تکمیل این عملیات مجدداً پنجره Printer Configuration را مشاهده خواهید کرد. اکنون باید بتوانید عنوان چاپگر موردنظر و توصیف آن‌را به ترتیب در ستون‌های Queue name و Description مشاهده کنید. برای ویرایش تنظیمات کافی است پس از انتخاب چاپگر روی گزینه Edit کلیک کنید تا به این ترتیب کادر محاوره‌ای Edit A Print Queue باز شود. این کادر محاوره‌ای از پنج بخش تشکیل شده که جدول ۱۹-۲۵ به شرح آن‌ها می‌پردازد.

جدول ۱۹-۲۵ شرح بخش‌های مختلف کادر محاوره‌ای Edit A Print Queue

عنوان بخش	توضیح
Queue Name	با استفاده از امکانات موجود در این بخش می‌توانید نام چاپگر را تغییر دهید.
Queue Type	با استفاده از امکانات موجود در این بخش می‌توانید پورت موازی مورد استفاده برای ارتباط با چاپگر محلی یا نحوه ارتباط با چاپگر متصل به شبکه را تغییر دهید.
Queue Options	با استفاده از امکانات موجود در این بخش می‌توانید تنظیماتی را در مورد حاشیه صفحات و فیلترهای چاپ انجام دهید.
Printer Driver	با استفاده از امکانات موجود در این بخش می‌توانید درایور مورد استفاده برای راه‌اندازی چاپگر را تغییر دهید.
Driver Options	با استفاده از امکانات موجود در این بخش می‌توانید تنظیمات بیشتری را در ارتباط با درایور موردنیاز برای راه‌اندازی چاپگر انجام دهید.

پیش از بستن پنجره برنامه redhat-config-printer-gui دکمه Apply را کلیک کنید. اقدام فوق باعث می‌شود تا این تنظیمات در فایل /etc/cups/cupsd.conf ذخیره شود. (در صورت استفاده از سیستم چاپ LPD این تنظیمات در فایل /etc/printcap ذخیره خواهد شد.) به عنوان آخرین اقدام، لازم است سرویس cupsd را مجدداً راه‌اندازی کنید. (در صورت استفاده از سیستم چاپ LPD باید این اقدام را در مورد سرویس lpd انجام دهید.)

جمع‌بندی

در این فصل به بررسی دو سیستم چاپ مورد استفاده در سیستم‌عامل UNIX یعنی CUPS و LPD پرداختیم. در نسخه‌های اخیر سیستم‌عامل Red Hat Linux سیستم چاپ CUPS به عنوان سیستم چاپ پیش مورد استفاده قرار می‌گیرد. با این‌که سیستم چاپ LPD برای مدت‌ها به عنوان سیستم چاپ پیش‌فرض مطرح بوده است، پشتیبانی از آن در نسخه‌های بعدی سیستم‌عامل Red Hat Linux بعید به نظر می‌رسد. از این‌رو، آشنایی با سیستم چاپ CUPS کاملاً ضروری است.

نرم‌افزار CUPS (کوتاه شده عبارت Common Unix Print System) امکان برخورداری از ویژگی‌های پروتکل Internet Print Protocol یا IPP را تحت نسخه‌های مختلف سیستم‌عامل UNIX و Linux فراهم می‌کند. پروتکل IPP در سال‌های اخیر به عنوان استانداردی برای سرور چاپ مطرح شده است. به این ترتیب، استفاده از نرم‌افزار CUPS کاملاً منطقی است.

رابط گرافیکی نرم‌افزار CUPS را می‌توان از طریق پورت TCP/IP شماره ۶۳۱ و با بهره‌گیری از یک مرورگر وب مورد دستیابی قرار داد. این رابط گرافیکی کلیه امکانات لازم برای پیکربندی چاپگرها، کلاس‌های مختلفی از چاپگرها و وظایف چاپی را در اختیار می‌گذارد. در صورت تمایل می‌توان گروهی از چاپگرها را در قالب یک کلاس واحد تعریف کرده و وظایف چاپی را به جای ارسال به یک چاپگر مشخص به آن کلاس ارسال کرد. در این صورت، وظیفه چاپی مزبور توسط اولین چاپگر قابل دستیابی در آن کلاس انجام خواهد شد.

پس از نصب نرم‌افزار CUPS فایل‌های پیکربندی مربوطه در فهرست /etc/cups مستقر می‌شود. فایل پیکربندی اصلی این نرم‌افزار با عنوان cupsd.conf شامل تنظیمات نسبتاً زیادی بوده و قالب آن شبیه به فایل‌های پیکربندی وب سرور Apache است. به کمک این تنظیمات می‌توان مواردی مانند حداکثر اندازه وظایف چاپی، موقعیت فایل‌های ثبت وقایع، امنیت دستیابی به رابط گرافیکی مورد استفاده برای مدیریت نرم‌افزار CUPS و موارد دیگر را مشخص کرد.

پس از پیکربندی چاپگرها و کلاس‌ها، با بهره‌گیری از رابط گرافیکی نرم‌افزار CUPS که از طریق مرورگر وب قابل دستیابی است، می‌توان مدیریت چاپگرها و وظایف چاپی را به سادگی انجام داد. برای مثال، منوی Jobs از این رابط گرافیکی امکانات لازم متوقف کردن وظایف چاپی را در اختیار می‌گذارد. با این کار امکان انجام وظایف چاپی با اولویت بالاتر فراهم می‌شود. پیکربندی چاپگرها در سیستم‌عامل Red Hat Linux از طریق برنامه گرافیکی redhat-config-printer نیز امکان‌پذیر است. فرامین lpstat و lpadmin اطلاعات لازم در مورد وضعیت فعلی چاپگرها را در اختیار قرار می‌دهند. با راه‌اندازی سرویس cups-dlp می‌توان امکان بهره‌برداری از فرامین سیستم چاپ LPD را در سیستم چاپ CUPS فراهم کرد.

برای استفاده از سیستم چاپ LPD کافی است بسته نرم‌افزار LPRng-* را نصب کنید. در صورت تمایل می‌توانید تنظیمات موردنظر را مستقیماً در فایل پیکربندی /etc/printcap.local وارد کرده یا آن‌ها را از طریق برنامه گرافیکی redhat-config-printer در فایل پیکربندی /etc/printcap درج کنید. به منظور مدیریت چاپگرها و وظایف چاپی فرامین متعددی از جمله lpr، lpq، lprm و lpc در این سیستم چاپ پیش‌بینی شده است.

در فصل بیست‌وششم برنامه‌های کلاینت و سرور موردنیاز برای بهره‌برداری از سرویس پست الکترونیکی یا به اختصار e-mail را مورد بررسی قرار داده و به‌طورخاص به بررسی نحوه پیکربندی برنامه sendmail خواهیم پرداخت.

فصل بیست‌وششم

استفاده از سرویس پست الکترونیکی

دراین‌فصل به بررسی سرویس‌پست‌الکترونیکی‌می‌پردازیم. بدون‌شک، این‌سرویس برای‌تمام کامپیوترهای متصل به شبکه، یکی از سرویس‌های ضروری محسوب می‌شود. برنامه‌های متعددی به منظور ارسال و دریافت پیغام‌های الکترونیکی یا اصطلاحاً e-mail از طریق سرویس پست الکترونیکی توسعه یافته‌اند که هر کدام یک یا چند پروتکل را مورد پشتیبانی قرار می‌دهند. با وجودی که پیکربندی برنامه‌های کلاینت موردنیاز برای استفاده ازاین سرویس پست الکترونیکی نسبتاً ساده است، پیکربندی برنامه‌های سرور مانند هر برنامه سرور دیگری از پیچیدگی خاصی برخوردار هستند.

چندین پروتکل از مجموعه پروتکل‌های TCP/IP با سرویس پست الکترونیکی در ارتباط هستند. در این میان، دو پروتکل Post Office Protocol یا POP و Internet Message Access Protocol یا IMAP برای دریافت پیغام‌ها و پروتکل Simple Mail Transfer Protocol یا SMTP برای ارسال پیغام‌ها از طریق شبکه‌های TCP/IP طراحی شده‌اند.

برنامه sendmail متداول‌ترین برنامه سرور SMTP یا به بیان دیگر متداول‌ترین برنامه‌ای است که مشخصات پروتکل SMTP در قالب آن پیاده‌سازی شده است. پیکربندی این برنامه یک فرآیند پیچیده است. با وجود این، در سیستم‌عامل Red Hat Linux تسهیلاتی برای این منظور پیش‌بینی شده است. این تسهیلات چیزی نیست جز یک فایل ماکرو یا اصطلاحاً macro file که پس از اعمال تغییرات موردنظر در آن با استفاده از یک پردازنده ماکرو (اصطلاحاً macro processor) می‌توان فایل پیکربندی برنامه sendmail را تولید کرد. این فایل پیکربندی امکانات موردنیاز برای تأمین امنیت لازم را در اختیار قرار می‌دهد. به بیان دقیق‌تر، به واسطه تنظیمات فایل پیکربندی برنامه sendmail می‌توان از ارسال پیغام به حوزه‌های موردنظر اجتناب کرده و پیغام از پیش تعیین شده‌ای را برای حوزه‌های ناشناخته ارسال کرد.

دو برنامه سرور بسیار متداول بر اساس پروتکل‌های IMAP4 و POP3 (نسخه‌های جدید پروتکل‌های IMAP و POP) توسعه یافته است. در صورت تمایل می‌توانید برای ایجاد برنامه سرور موردنیاز جهت دریافت پیغام‌های الکترونیکی ارسالی از طریق سرویس پست الکترونیکی اقدام کرده یا برنامه‌های کلاینت را به نحوی پیکربندی کنید که از این برنامه‌های سرور به نحو مطلوب بهره‌برداری کنند. هر دو

برنامه سرور نامبرده (هم در نسخه عادی و هم در نسخه‌ای با ایمنی بالا) در قالب یک بسته نرم‌افزاری واحد به همراه سیستم‌عامل Red Hat Linux توزیع می‌شود.

بیشتر کاربران کامپیوتر دست کم با یکی از برنامه‌های کلاینت پست الکترونیکی آشنا هستند. این گونه برنامه‌ها پیغام‌های الکترونیکی ارسالی را دریافت کرده و آن‌ها را به نحو مطلوب قالب‌بندی می‌کنند، به طوری که کاربران به راحتی بتوانند آن‌ها را بخوانند و در صورت لزوم به آن‌ها پاسخ دهند. برنامه‌های مختلفی در دو قالب متنی و گرافیکی به همراه نسخه‌های مختلف سیستم‌عامل Linux توزیع می‌شود. در فصل حاضر به بررسی این موضوعات می‌پردازیم:

- نگاهی کلی به سرویس پست الکترونیکی
- پیکربندی برنامه sendmail
- استفاده از برنامه‌های سرور پست الکترونیکی
- پیکربندی برنامه‌های کلاینت پست الکترونیکی

نگاهی کلی به سرویس پست الکترونیکی

در مجموع سه نوع سرویس پست الکترونیکی با عناوین Message Transfer Agents، Mail Delivery Agents و Mail User Agent یا به اختصار MTA، MDA و MUA موجود است. برنامه‌های سرور متعددی به منظور پیاده‌سازی این سرویس‌ها توسعه یافته‌اند.

برنامه‌های MTA پیغام‌های الکترونیکی را از طریق یک شبکه ارسال می‌کنند. در سیستم‌عامل Linux برنامه sendmail بر اساس پروتکل SMTP این پیغام‌ها را از طریق شبکه‌های TCP/IP مانند اینترنت ارسال می‌کند.

برنامه‌های MDA در واقع پردازنده پیغام‌ها هستند. این گونه برنامه‌ها پیغام‌های الکترونیکی ارسالی از طریق شبکه اینترنت را دریافت کرده و آن‌ها را در اختیار برنامه‌های MUA (مانند pine، Evolution، KMail و Mozilla Mail) قرار می‌دهند. برنامه procmail را می‌توان متداول‌ترین برنامه در این زمینه به حساب آورد. بسته نرم‌افزاری *-procmail در سیستم‌عامل Red Hat Linux به طور پیش‌فرض روی کامپیوتر میزبان نصب می‌شود. معمولاً تعامل بدون نقصی میان این برنامه و برنامه sendmail (و سایر برنامه‌های سرور مشابه) وجود دارد.

برنامه‌های MUA به دسته‌ای از برنامه‌های کاربردی اطلاق می‌شود که امکان ارسال و دریافت پیغام‌های الکترونیکی را از طریق برنامه‌های MTA و MDA در اختیار قرار می‌دهند. بیشتر کاربران دست کم با یکی از این گونه برنامه‌ها آشنایی دارند. در واقع کاربران برای ارسال پیغام‌های الکترونیکی موردنظر

خود با استفاده از یک برنامه MUA آن پیغام‌ها را به برنامه‌ای از نوع MTA (مانند برنامه sendmail) ارسال می‌کنند.

دو پروتکل POP3 و IMAP4 متداول‌ترین پروتکل‌ها برای دریافت پیغام‌های الکترونیکی هستند.

برای پیکربندی این پروتکل‌ها کافی است فایل‌های پیکربندی مربوطه (یعنی pop3s و imaps) در فهرست /etc/xinetx.d را فعال کنید. (برای اطلاع بیشتر در این زمینه به فصل بیست و سوم مراجعه کنید.)

پروتکل‌های اصلی برای ارسال و دریافت پیغام‌های الکترونیکی

چنان‌که قبلاً نیز اشاره شد، پروتکل‌های متعددی از مجموعه پروتکل‌های TCP/IP درگیر فرآیند ارسال پیغام‌های الکترونیکی از یک کاربر به کاربر دیگر هستند. از میان آن‌ها به بررسی سه پروتکل اصلی SMTP، POP3 و IMAP4 در این زمینه می‌پردازیم.

به عنوان مدیر سیستم Linux دیر یا زود درگیر پیکربندی و راه‌اندازی یک برنامه SMTP خواهید شد. (منظور از برنامه SMTP برنامه‌ای است که کلیه مشخصات پروتکل SMTP در قالب آن پیاده‌سازی شده باشد.) با وجودی که برنامه sendmail متداول‌ترین نوع این گونه برنامه‌ها محسوب می‌شود، در صورت تمایل می‌توانید برنامه‌های مشابه دیگری مانند Exim، Postfix و Qmail را برای این منظور مورد بهره‌برداری قرار دهید.

علاوه بر این، به عنوان مدیر سیستم Linux گاهی اوقات لازم است در پیکربندی برنامه‌های MUA کاربران را راهنمایی کنید. عموماً باید با اسامی سرورهای دریافت کننده پیغام‌های الکترونیکی مستقر در شبکه میزبان یا ISP موردنظر آشنا باشید. (برای اطلاع بیشتر در این زمینه به فصل بیست و چهارم مراجعه کنید.) با وجود این، در فصل حاضر بیشتر به بررسی فرآیند ارسال پیغام‌های الکترونیکی و نحوه پیکربندی برنامه سرور مربوطه (مشخصاً sendmail) خواهیم پرداخت.

در نسخه‌های قدیمی‌تر این گونه برنامه‌ها، که بر اساس پروتکل Unix-to-Unix Copy یا به اختصار UUCP پیاده‌سازی می‌شدند، پیغام موردنظر مستقیماً از کامپیوتر مبدأ به کامپیوتر مقصد ارسال می‌شد. اگر قرار بود پیغام موردنظر از طریق یک شبکه واسط ارسال شود، لازم بود تمام کامپیوترهای مستقر در مسیر ارسال آن پیغام دقیقاً مشخص شود. نیازی به گفتن نیست که این شیوه برای ارسال پیغام‌های الکترونیکی از طریق شبکه اینترنت کاملاً غیر عملی است.

نگاهی کلی به برنامه‌های سرور پست الکترونیکی

در این فصل به طور خاص برنامه sendmail را به عنوان متداول‌ترین برنامه MTA مورد بررسی قرار می‌دهیم. با این همه، برنامه‌های MTA دیگری نیز وجود دارد که در ادامه نگاه کوتاهی به آن‌ها خواهیم داشت. جدای از نسخه تجاری برنامه sendmail با عنوان Sendmail (به حرف S بزرگ توجه کنید.) بسته‌های نرم‌افزاری موردنیاز برای نصب این برنامه‌ها را می‌توان از طریق مراجعه به منابع نرم‌افزاری مختلف، از جمله وب سایت http://www.rpmfind.net تهیه کرد. اکنون به توضیح کوتاهی در مورد هر یک از این برنامه‌ها توجه کنید:

- **برنامه Sendmail**: این برنامه نسخه تجاری برنامه sendmail است که به همراه سیستم‌عامل Red Hat Linux توزیع می‌شود. برنامه مزبور برای استفاده در شرکت‌ها و سازمان‌ها طراحی شده و توانایی سرویس‌دهی هم‌زمان به هزاران کاربر را دارد. این برنامه را حتی می‌توان برای کاربرانی که همواره در یک موقعیت مشخص مستقر نیستند (اصطلاحاً mobile clients) پیکربندی کرد. برای اطلاع بیشتر در این زمینه به وب سایت مربوطه در آدرس اینترنتی http://www.sendmail.com مراجعه کنید.
- **برنامه Exim**: این برنامه در دانشگاه کمبریج انگلستان توسعه یافته و تحت لیسانس GPL منتشر شده است. علیرغم آن‌که توسعه برنامه Exim بر اساس برنامه قدیمی‌تری با عنوان Smail انجام شده، به خوبی می‌تواند از قبول پیغام‌های ارسالی از آدرس‌های مشخصی امتناع ورزد. به این ترتیب، می‌توان تعداد هرزنامه‌های ارسالی به کاربران را به حداقل کاهش داد. برای اطلاع بیشتر درباره این برنامه به وب سایت مربوطه در آدرس اینترنتی http://www.exim.org مراجعه کنید.
- **برنامه Postfix**: این برنامه به عنوان یکی از برنامه‌های جایگزین sendmail مطرح شده است. به طوری که بسیاری از مدیران سیستم‌های Linux استفاده از آن‌را مورد توجه قرار داده‌اند. برنامه Postfix در حقیقت جایگزین دو برنامه Vmailer و IBM Secure Mailer شده است. چنان‌که در فصل نوزدهم نیز توضیح داده شد، با استفاده از امکانات برنامه Mail Transport Agent Switcher (که با اجرای فرمان redhat-switch-mail دستیابی به آن امکان‌پذیر است.) می‌توان مابین این گونه برنامه‌ها سوییچ کرد. برای اطلاع بیشتر درباره برنامه Postfix به وب سایت مربوطه در آدرس اینترنتی http://www.postfix.org مراجعه کنید.
- **برنامه Qmail**: این برنامه نیز به عنوان جایگزینی برای برنامه sendmail مطرح شده است. طبق آمار منتشر شده در وب سایت رسمی این برنامه یعنی http://www.qmail.org تعداد بسیار زیادی از وب سایت‌ها از برنامه Qmail به عنوان برنامه سرور پست الکترونیکی استفاده می‌کنند. آقای

D. J. Bernstein به عنوان توسعه دهنده این برنامه جایزه‌ای را برای نخستین فردی که بتواند یک حفره امنیتی در این برنامه پیدا کند در نظر گرفته است. برای اطلاع بیشتر در این زمینه به آدرس اینترنتی http://cr.yp.to/qmail/guarantee.html مراجعه کنید.

- **برنامه Smail:** این برنامه به لحاظ پیکربندی ساده‌تر از برنامه sendmail بوده و ضمناً از قابلیت بلوکه کردن پیغام‌ها نیز برخوردار است. علاوه بر این، برنامه Smail قادر است پیغام‌هایی را که قصد دارند منبع ارسال کننده را یک وب سایت شناخته شده جا بزنند، تشخیص دهد. (برای اطلاع بیشتر درباره توسعه دهندگان این برنامه می‌توانید به وب سایت http://www.planix.com مراجعه کنید.)

پیکربندی برنامه sendmail

مشابه بیشتر برنامه‌های پیچیده سیستم‌عامل Linux، برنامه sendmail نیز در قالب چندین بسته نرم‌افزاری RPM به همراه سیستم‌عامل Red Hat Linux توزیع شده است. علاوه بر فایل پیکربندی sendmail.cf و ماکروی sendmail.mc فایل‌های پیکربندی مهم دیگری نیز وجود دارد.

در نسخه‌های اخیر برنامه sendmail فایل‌های پیکربندی به دو گروه مشخص تقسیم شده‌اند. برنامه مزبور به محض دریافت و ارسال یک پیغام الکترونیکی به ترتیب ماکروهای sendmail.cf و submit.cf را مورد بهره‌برداری قرار می‌دهد.

پس از نصب و آماده‌سازی برنامه sendmail جهت بهره‌برداری، در صورت تمایل می‌توانید امنیت آن‌را از طریق تنظیمات فایل‌های پیکربندی این برنامه افزایش دهید.

پرداختن به موضوع فوق از حوزه این کتاب خارج است. کتب ۱۰۰۰ صفحه‌ای متعددی درباره این برنامه به رشته تحریر درآمده که از آن جمله می‌توان به Linux Sendmail Administration تألیف Craig Hunt اشاره کرد. کار نشر این کتاب در سال ۲۰۰۱ توسط انتشارات Sybex انجام شده است.

بسته‌های نرم‌افزاری موردنیاز برای نصب برنامه sendmail

برای استفاده از برنامه sendmail کافی است بسته نرم‌افزاری sendmail-* را نصب کنید. (این بسته نرم‌افزاری به طور پیش‌فرض به همراه سیستم‌عامل Red Hat Linux روی کامپیوتر میزبان نصب می‌شود.) با وجود این، بسته‌های نرم‌افزاری دیگری نیز در ارتباط با این برنامه منتشر شده که شرح مختصری از آن‌ها را در جدول ۱-۲۶ ملاحظه می‌کنید. چنان‌که از فصل دهم به خاطر دارید، با اجرای

فرمان rpm -q *packagename* می‌توانید از نصب بسته نرم‌افزاری موردنظر که در این‌جا با متغیر *packagename* نشان داده شده است، اطلاع حاصل کنید. پس از نصب بسته نرم‌افزاری دلخواه، با اجرای فرمان rpm -ql *packegename* می‌توانید لیست فایل‌هایی را که در قالب بسته نرم‌افزاری موردنظر روی کامپیوتر میزبان نصب شده است، مشاهده کنید.

جدول ۱-۲۶ بسته‌های نرم‌افزاری مربوط به برنامه sendmail

عنوان بسته نرم‌افزاری	توضیح
sendmail-*	این بسته نرم‌افزاری حاوی فایل‌های موردنیاز برای استفاده از برنامه sendmail است.
sendmail-cf-*	این بسته نرم‌افزاری حاوی برنامه‌های کمکی برای ایجاد فایل‌های پیکربندی برنامه sendmail است.
sendmail-devel-*	این بسته نرم‌افزاری حاوی کتابخانه‌های لازم برای توسعه قابلیت‌های برنامه sendmail است.
sendmail-doc-*	این بسته نرم‌افزاری حاوی مستندات برنامه sendmail از جمله پرسش و پاسخ‌های متداول (اصطلاحاً FAQs) است.

فایل‌های پیکربندی اصلی برنامه sendmail

علاوه بر فایل پیکربندی اصلی برنامه sendmail یعنی sendmail.cf عملکرد این برنامه به فایل‌های دیگری نیز وابسته است. در پاراگراف‌های قبل به ماکروی sendmail.mc اشاره کردیم. مشابه اغلب برنامه‌های سرور، یکی از فایل‌های پیکربندی مربوط به برنامه sendmail در فهرست /etc/sysconfig مستقر است. از طریق تنظیمات فایل /etc/aliases می‌توان پیغام الکترونیکی را به جای ارسال به کاربر موردنظر به کاربر دیگری ارسال کرد. فایل‌های پیکربندی دیگری نیز در فهرست /etc/mail موجود است.

فایل پیکربندی /etc/sysconfig/sendmail

فایل پیکربندی /etc/sysconfig/sendmail دارای ساختار ساده‌ای به این شکل است:

```
DAEMON=yes
QUEUE=1h
```

دستورالعمل DAEMON=yes برنامه sendmail را وادار می‌کند تا به پورت TCP/IP شماره ۲۵ یعنی پورت مخصوص پروتکل SMTP گوش فرا دهد. دستورالعمل QUEUE=1h نیز این برنامه را وادار می‌کند که پیغام‌های موجود در صف را پس از گذشت یک ساعت به مقصد موردنظر ارسال کند.

فایل پیکربندی /etc/aliases

ساختار فایل /etc/aliases نیز بسیار ساده است. محتوای این فایل کاربران دریافت کننده پیغام‌ها را مشخص می‌کند. برای مثال، پس از درج‌این‌خط در فایل پیکربندی مزبور، پیغام‌های ارسالی به سرویس FTP مستقر روی کامپیوتر میزبان یعنی آدرس ftp@localhost به آدرس root@localhost تغییر مسیر می‌دهند:

```
ftp:  root
```

هم‌چنین با درج این خط در فایل پیکربندی /etc/aliases می‌توان پیغام‌های ارسالی به کاربری با شناسه byeltsin برای کاربر دیگری با شناسه vputin ارسال شود:

```
byeltsin:   vputin
```

فایل‌های پیکربندی موجود در فهرست /etc/mail

در ارتباط با برنامه sendmail و بانک‌های اطلاعاتی مورد استفاده این برنامه فایل‌های پیکربندی متعددی در فهرست /etc/mail پیش‌بینی شده است. برای فعال کردن این فایل‌ها عموماً باید دستورالعمل مربوطه را در فایل sendmail.mc درج کنید. در بیشتر موارد با استفاده از فرمان makemap می‌توانید یک فایل متنی را به فایل db. متناظر تبدیل کنید.

- **فایل access یا access.db:** این فایل شامل تنظیمات مربوط به حوزه‌ها یا آدرس‌های پست الکترونیکی است. وجود پارامتر DISCARD در این فایل بیانگر آن است که پیغام‌های ارسالی از منابع فوق نادیده گرفته می‌شود. پارامتر REJECT بیانگر آن است که ضمن نادیده گرفتن پیغام‌های ارسالی از این منابع، پیغام خطایی نیز نمایش داده شود و بالاخره پارامتر RELAY بیانگر این است که پیغام ارسالی از منابع مزبور به آدرس مشخصی ارسال شود. به این ترتیب، در صورت تمایل می‌توان پیغام‌های ناخواسته ارسالی از حوزه‌ها یا آدرس‌های پست الکترونیکی مشخص را به واسطه استفاده از پارامتر DISCARD یا REJECT به حداقل ممکن کاهش داد. فایل /etc/mail/access حاوی مثال‌هایی در این زمینه است.
- **فایل domaintable یا domaintable.db:** این فایل تناظر میان حوزه‌های مختلف را مشخص می‌کند، به طوری که اگر نام یک حوزه به هر دلیل تغییر کند و کاربران پیغام‌های خود را هم‌چنان

برای حوزه قدیمی ارسال کنند، این پیغام‌ها برای حوزه متناظر با آن ارسال شده و به این ترتیب هیچ پیغامی از دست نمی‌رود. برای مثال، اگر به هر دلیل نام حوزه‌ای را از dictatorsrus.com به democracysus.com تغییر داده باشید، با درج این خط در یکی از دو فایل domaintable یا domaintable.db می‌توانید ترتیبی دهید که پیغام‌های ارسالی به حوزه dictatorsus.com برای حوزه democracysus.com ارسال شود:

```
dictatorsus.com    democracy.com
```

- **فایل helpfile**: این فایل حاوی توضیحاتی درباره فرامینی است که می‌توانید آن‌ها را از طریق اعلان برنامه sendmail اجرا کنید. اعلان مزبور با اجرای فرمان telnet localhost 25 در اختیار قرار می‌گیرد.
- **فایل local-host-names**: این فایل شامل اسامی مستعار کامپیوتر میزبانی است که برنامه سرور sendmail روی آن مستقر شده است. برای تعیین اسامی مستعار چنین کامپیوتری کافی است آن‌ها را در خطوط جداگانه این فایل درج کنید.
- **فایل mailertable یا mailertable.db**: این فایل حاوی دستورالعمل‌های موردنیاز برای مسیریابی حوزه‌های به خصوص بوده و به ندرت مورد استفاده قرار می‌گیرد.
- **فایل Makefile**: این فایل امکان کامپایل مجدد برنامه sendmail با گزینه‌های مختلف را در اختیار قرار می‌دهد. به این ترتیب می‌توان آن‌را جایگزین فایل sendmail.mc دانست.
- **فایل‌های sendmail.cf و sendmail.mc**: به کمک این فایل‌ها می‌توان برنامه sendmail را پیکربندی کرد. فایل sendmail.cf فایل پیکربندی اصلی برنامه sendmail و فایل sendmail.mc فایلی است که به کمک آن می‌توان فایل پیکربندی sendmail.cf را تولید کرد. برای توضیح بیشتر درباره این فایل‌ها به قسمت‌های مربوطه در همین فصل مراجعه کنید.
- **فایل statistics**: این فایل حاوی اطلاعات آماری درباره میزان بهره‌برداری از برنامه sendmail است. برای بازخوانی محتوای این فایل کافی است فرمان mailstats را اجرا کنید.
- **فایل submit.cf و submit.mc**: به کمک این فایل‌ها می‌توان امکان بهره‌برداری از برنامه sendmail را برای گروه مشخصی محدود کرد. ساختار نسخه پیش‌فرض فایل submit.mc شبیه به فایل sendmail.mc است. برای توضیح بیشتر درباره فایل submit.mc به قسمت مربوطه در همین فصل مراجعه کنید.
- **فایل trusted-users**: این فایل حاوی شناسه کاربرانی است که می‌توانند از جانب سایر کاربران برای ارسال پیغام الکترونیکی اقدام کنند. فایل مزبور به ندرت مورد استفاده قرار می‌گیرد، چرا که

در اغلب موارد موضوع ارسال پیغام از جانب یک کاربر دیگر قابل توجیه نیست.

- **فایل virtualusertable یا virtualusertable.db:** این فایل امکان تغییر مسیر پیغام ارسالی را در اختیار قرار می‌دهد. در مورد کاربران خارجی عملکرد این فایل مشابه فایل /etc/aliases است.

فایل /etc/mail/sendmail.mc

فایل اصلی پیکربندی برنامه sendmail یعنی /etc/mail/sendmail.cf بالغ بر ۲۰۰۰ خط است! در مقابل، فایل /etc/mail/sendmail.mc متشکل از تقریباً ۷۰ خط بوده و از خوانایی خوبی نیز برخوردار است. پس از پیکربندی فایل /etc/mail/sendmail.mc، با استفاده از فرمان make یا پردازنده ماکروی m4 می‌توان برای تولید فایل پیکربندی /etc/mail/sendmail.cf اقدام کرد. در این قسمت محتوای فایل مذکور را مورد بررسی قرار می‌دهیم. چنان‌که خواهید دید، توضیحات لازم در لابه‌لای خطوط این فایل گنجانده شده است. با وجود این، از آن‌جا که بیشتر قسمت‌های این فایل به ندرت دستخوش تغییر می‌شود، توضیحات زیادی موردنیاز نیست. به دلیل پیچیدگی برنامه sendmail توصیه می‌کنیم کتاب Linux Sendmail Administration را که توسط Craig Hunt تألیف شده است، مطالعه کنید.

نحوه استفاده از علایم کوتیشن در داخل پرانتز ممکن است تا اندازه‌ای عجیب به نظر برسد. به طوری که ملاحظه خواهید کرد، از علامت ` یا back quote برای باز کردن کوتیشن و از علامت ' یا single quote برای بستن آن استفاده شده است. علامت ` کلید بالایی Tab در صفحه کلیدهای آمریکایی است.

فرمان divert(-1) یکی از روش‌های استاندارد برای فعال کردن فایل sendmail.mc است. خطوط مابین فرمان فوق و فرمان divert(0) مانند توضیحات بی‌تأثیرند.

تمام خطوطی که با فرمان dnl آغاز شده‌اند به عنوان توضیح تعبیر می‌شوند. این نوع توضیحات به خصوص شامل روشی برای پردازش فایل sendmail.mc است. در هر صورت، با اجرای این فرمان می‌توان برای تولید فایل پیکربندی /etc/mail/sendmail.cf از روی فایل /etc/mail/sendmail.mc اقدام کرد:

```
m4 sendmail > sendmail.cf
```

اکنون به محتوای فایل /etc/mail/sendmail.cf و توضیحات مربوطه توجه کنید:

```
dnl #
dnl # This is the sendmail macro config file for m4. If you
dnl # make changes to /etc/mail.mc, you will need to
```

```
dnl # regeneratethe /etc/mail/sendmail.cf file by confirming
dnl # that the sendmail-cf package is installed and then
dnl # performing a
dnl #
dnl #      make -C /etc/mail
dnl #
```

این خط استفاده از فرمان cf.m4 را به عنوان:

```
include(`/usr/share/sendmail-cf/m4/cf.m4')dnl
```

برچسب VERSIONID شاخص فایل پیکربندی برنامه sendmail را مشخص می‌کند. به دستورالعمل مربوطه توجه کنید:

```
VERSIONID(`setup for Red Hat Linux')dnl
```

فرمان OSTYPE نوع سیستم‌عامل (در این مورد linux) را مشخص می‌کند. دستورالعمل مربوطه چنین است:

```
OSTYPE(`linux')dnl
```

این فرمان define تعامل میان برنامه sendmail و سرور SMTP را که عموماً در خارج از شبکه میزبان مستقر است، هماهنگ می‌کند. برای فعال کردن این فرمان باید فرمان dnl را از ابتدای خط مربوطه حذف کرده و عبارت smtp.your.provider را با آدرس سرور SMTP واقعی جایگزین کنید. دستورالعمل مربوطه چنین است:

```
dnl #
dnl # Uncomment and edit the following line if your outgoing
dnl # mail needs to be sent out through an external mail
dnl # server:
dnl #
dnl define(`SMART_HOST', `smtp.your.provider')
dnl #
```

عموماً نیازی نیست که فرامین زیر را تغییر دهید. برای توضیح بیشتر در این زمینه به کتاب Linux Sendmail Administration مراجعه کنید:

```
define(`confDEF_USER_ID',``8:12'')dnl
define(`confTRUSTED_USER', `smmsp')dnl
dnl define(`confAUTO_REBUILD')dnl
define(`confTO_CONNECT', `1m')dnl
define(`confTRY_NULL_MX_LIST',true)dnl
define(`confDONT_PROBE_INTERFACES',true)dnl
```

```
define(`PROCMAIL_MAILER_PATH',`/usr/bin/procmail')dnl
define(`ALIAS_FILE',`/etc/aliases')dnl
dnl define(``STATUS_FILE',`/etc/mail/statiscics')dnl
define(`UUCP_MAILER_MAX',`2000000')dnl
define(`confUSERDB_SPEC',`/etc/mail/userdb.db')dnl
define(`confPRIVACY_FLAGS',`authwarnings,novrfy,noexpn,
restrictrqrun')dnl
```

این دو فرمان define جمع‌ناپذیرند، به این معنی که در عین حال تنها می‌توان یکی از آن‌ها را فعال کرد. اصطلاح TLS که به مکانیزم Transport Layer Security اشاره دارد جانشین مکانیزمی با عنوان SSL یا Secure Socket Layer است:

```
define(`confAUTH_OPTIONS',`A')dnl
dnl #
dnl # The following allows relaying if the user authenticates
dnl # and disallows plaintext authentication (PLAIN/LOGIN) on
dnl # non-TLS links
dnl #
dnl define(`confAUTH_OPTIONS',`A p')dnl
dnl #
dnl # PLAIN is the prefered plaintext authentication method
dnl # andused by Mozilla Mail and Evolution, though Outlook
dnl # Express and other MUAs do use LOGIN. Other mechanisms
dnl # should be used if the connection is not garanteed
dnl # secure.
dnl #
```

برای اجتناب از به کارگیری متون ساده جهت دستیابی به برنامه sendmail کافی است این دو خط را فعال کنید:

```
dnl define(`confAUTH_OPTIONS',`A')dnl
define(`confAUTH_OPTIONS',`A p')dnl
```

این فرامین به روش احراز هویت برنامه sendmail مربوط بوده و چنان‌که مشاهده می‌کنید به طور پیش‌فرض فعال هستند:

```
dnl TRUST_AUTH_MECH(`EXTERNAL DIGEST-MD5 CRAM-MD5 LOGIN PLAIN')dnl
dnl define('confAUTH_MECHANISMS',`EXTERNAL GSSAPI DIGEST-MD5 CRAM-
MD5 LOGIN PLAIN)dnl
```

به واسطه این فرامین می‌توان احراز هویت کاربران برای دستیابی به کامپیوتر میزبان برنامه sendmail را براساس مکانیزم SSL انجام داد. (برای اطلاع بیشتر درباره این مکانیزم به فصل سی‌ام مراجعه کنید.) روشی که در فصل مزبور برای دستیابی به کامپیوتر میزبان سرور Apache توضیح داده شده است در مورد برنامه sendmail نیز قابل استفاده است:

```
dnl #
dnl # Rudimentary information on creating certificates for
dnl # sendmail TLS:
dnl #     make -C /usr/share/ssl/certs usage
dnl #
dnl define(`confCACERT_PATH',`/usr/share/ssl/certs')
dnl define(`confCACERT',`/usr/share/ssl/certs/ca-bundle.crt')
dnl define(`confSERVER_CERT',`/usr/share/ssl/serts/sendmail.pem')
dnl define(`confSERVER_KEY',`/usr/share/ssl/serts/sendmail.pem')
dnl #
```

این فرامین امکان برخورداری از پروتکل Lightweight Directory Assistance Protocol یا LDAP را در اختیار می‌گذارد، به طوری که می‌توان به جزییات اطلاعات مربوط به کاربران دسترسی داشت. از این‌رو می‌توان آن‌را جایگزین فایل‌های /etc/aliases و /etc/mail/virtusertable.db دانست. تعامل برنامه sendmail و پروتکل LDAP موضوع پیچیده‌ای بوده و بررسی آن از حوزه این کتاب خارج است:

```
dnl # This allows sendmail to use a keyfile that is shared
dnl # with OpenLDAP's slapd, which requires the file to be
dnl # readable by group ldap
dnl #
dnl define(`confDONT_BLAME_SENDMAIL',`groupreadablekeyfile')dnl
dnl #
```

این فرامین در صورتی اجرا می‌شود که مقصد پیغام الکترونیکی ارسالی قابل تشخیص نباشد:

```
dnl define(`confTO_QUEUEWARN',`4h')dnl
dnl define(`confTO_QUEUERETURN',`5d')dnl
dnl define(`confQUEUE_LA',`12')dnl
dnl define(`confREFUSE_LA',`18')dnl
define(`confTO_IDENT',`0')dnl
dnl FEATURE(delay_checks)dnl
FEATURE(`on_default_msa',`dnl')dnl
```

این خطوط مشخصات سطر فرمان برنامه sendmail با عنوان smrsh را مشخص می‌کند: (فایل mailertable.db حاوی اسامی حوزه‌های متفاوتی است.)

```
FEATURE(`smrsh',`/usr/sbin/smrsh')dnl
FEATURE(`mailertable',`hash -o/etc/mail/mailertable.db')dnl
FEATURE(`virtusertable',`hash -o/etc/mail/virtusertable.db')dnl
FEATURE(redirect)dnl
FEATURE(always_add_domain)dnl
FEATURE(use_cw_file)dnl
FEATURE(use_ct_file)dnl
dnl #
dnl # The -t option will retry delivery if e.g. the user runs
dnl # over the quota.
dnl #
FEATURE(local_procmail,``,`procmail -t -Y -a $h -d $u')dnl
FEATURE(`access_db',`hash -T<TMPF> -o/etc/mail/access.db')dnl
FEATURE(`blacklist_recipients')dnl
```

فرمان EXPOSED_USER آدرس پست الکترونیکی کاربر اصلی (اصطلاحاً root) را به طور کامل مشخص می‌کند. به دستورالعمل مربوطه توجه کنید:

```
EXPOSED_USER(`root')dnl
dnl #
dnl # The following causes sendmail to only listen on the
dnl # Ipv4 loopback address 127.0.0.1 and not on any other
dnl # network restriction to accept email from the internet
dnl # or intranet.
dnl #
```

برنامه sendmail به طور پیش‌فرض تنها پیغام‌های ارسالی از کامپیوتر محلی را مورد توجه قرار داده و پردازش می‌کند. برای تغییر این رفتار به طوری که برنامه مزبور پیغام‌های ارسالی از کلیه کامپیوترهای مستقر در شبکه را مورد توجه قرار دهد، کافی است فرمان dnl را در ابتدای نخستین خط از این خطوط درج کنید:

```
DAEMON_OPTIONS(`Port=smtp,Addr=127.0.0.1,Name=MTA')dnl
dnl #
dnl # The following causes sendmail to additionally listen to
dnl # port 587 for mail from MUAs that authenticate. Roaming
dnl # users who can't reach their prefered sendmail daemon
dnl # due to port 25 being blocked or redirected find this
dnl # useful.
dnl #
```

با فعال‌کردن این فرمان برنامه sendmail از طریق پورت TCP/IP شماره ۵۸۷ پیغام‌های الکترونیکی ارسالی را که شامل شناسه کاربری و کلمه عبور هستند، مورد توجه قرار می‌دهد: این قابلیت برای کاربرانی که به واسطه عدم دسترسی به پورت شماره ۲۵ یا به هر دلیل دیگر نمی‌توانند برنامه sendmail را مورد دستیابی قرار دهند، مفید است:

```
dnl DAEMON_OPTIONS(`Port=submission,Name=MSA,M=Ea')dnl
dnl #
dnl # The following causes sendmail to additionally listen to
dnl # port 465, but starting immediately in TLS mode upon
dnl # connecting. Port 25 or 587 followed by STARTTLS is
dnl # preferred, butroaming clients using Outlook Express
dnl # can't do STARTTLS on ports other than 25. Mozilla Mail
dnl # can ONLY use STARTTLS and doesn't support the
dnl # deprecated smtps; Evolution <1.1.1 uses smtps when SSL
dnl # is enabled-- STARTTLS support is available in version 1.1.1.
dnl #
dnl # For this to work yourOpenSSL certificates must be
dnl # configured.
dnl #
```

با فعال کردن این فرمان می‌توانید ترتیبی دهید که دسترسی به برنامه sendmail در قالبی حفاظت شده انجام شود. این قابلیت مستلزم استفاده از مکانیزم TLS است. با وجود این، چنان‌که در توضیحات نیز ملاحظه می‌کنید، در صورت استفاده از برنامه Microsoft Outlook Express و نسخه 1.1.1 یا نسخه‌های پایین‌تر از برنامه Evolution از فعال کردن این فرمان پرهیز کنید:

```
dnl DAEMON_OPTIONS(`Port=smtps,Name=TLSMTA,M=s')dnl
dnl #
dnl # The following causes sendmail to additionally listen on
dnl # the Ipv6 loopback device. Remove the loopback address
dnl # restriction listen to the network.
dnl #
dnl # NOTE: binding both Ipv4 and Ipv6 daemon to the same
dnl # port requires a kernel patch
dnl #
```

در صورتی که شبکه میزبان را برای استفاده از آدرس‌های IPv6 پیکربندی کرده‌اید این فرمان را فعال کنید. (برای اطلاع بیشتر درباره ساختار آدرس‌های IPv6 به فصل بیستم مراجعه کنید.) این فرمان

معادل فرمانی است که قبلاً در مورد محدود کردن پیغام‌های الکترونیکی به کامپیوتر محلی (با آدرس 127.0.0.1) مشاهده کردید:

```
dnl DAEMON_OPTIONS(`port=smtp,Addr=::1,Name=MTA-v6,Family=inet6')dnl
dnl #
dnl # We strongly recommend not accepting unresolvable
dnl # domains if you want to protect yourself from spam.
dnl # However, the laptop and users on computers that do not
dnl # have 24x7 DNS do need this.
dnl #
```

فعال بودن این فرمان بدان معنی است که برنامه sendmail از مکانیزم DNS معکوس استفاده نمی‌کند. این فرمان را تنها در صورتی غیرفعال کنید که امکان دسترسی قابل اعتماد به سرور DNS موجود نبوده و امکان کنترل ترافیک اضافی وجود نداشته باشد:

```
FEATURE(`accept_unresolvable_domains')dnl
dnl #
```

این فرمان امکان استفاده از مکانیزم MX یا Mail Exchanger را در اختیار می‌گذارد: (مکانیزم مشابهی نیز در مورد سرویس DNS وجود دارد. برای اطلاع بیشتر در این زمینه به فصل بیست و چهارم مراجعه کنید.)

```
dnl FEATURE(`relay_based_on_MX')dnl
dnl #
dnl # Also accept email sent to "localhost.localdomain" as
dnl # local email.
dnl #
```

به کمک فرمان LOCAL_DOMAIN می‌توان نام مستعار کامپیوتر محلی را مشخص کرد. نام مستعاری که به طور پیش‌فرض در فایل /etc/hosts ثبت شده localhost.localdomain است. به دستورالعمل مربوطه توجه کنید:

```
LOCAL_DOMAIN(`localhost.localdomain')dnl
dnl #
dnl # The following example makes mail from this host and any
dnl # additional specified domains appear to be sent from
dnl # mydomain.com
dnl #
```

به کمک فرمان MASQUERADE_AS می‌توان برچسبی را که برنامه sendmail به پیغام‌های الکترونیکی ارسالی ضمیمه می‌کند، تغییر داد. برای این منظور، کافی است عنوان برچسب موردنظر را با

mydomain.com جایگزین کنید. این اقدام اغلب جهت مشخص کردن پیغام‌های ارسالی از یک حوزه فرعی (اصطلاحاً subdomain) انجام می‌شود. برای مثال، چنان‌چه مشخصه شبکه میزبان mommabears.com باشد، می‌توان از برچسبی مانند linux.mommabears.com برای این منظور استفاده کرد. به دستورالعمل‌های مربوطه توجه کنید:

```
dnl MASQUERADE_AS(`mydomain.com')dnl
dnl #
dnl # masquerade not just the headers,but the envelope as well
dnl #
dnl FEATURE(masquerade_envelope)dnl
dnl #
dnl # masquerade not just @mydomainalias.com, but
dnl # @*.mydomainaliase.com as well
dnl #
dnl FEATURE(masquerade_entire_domain)dnl
dnl #
```

به کمک فرمان MASQUERADE_DOMAIN می‌توان برنامه sendmail را وادار کرد تا با آدرس‌های پست الکترونیکی مربوط به سایر حوزه‌ها نیز به ترتیب مشابه رفتار کند. برای مثال، در صورت فعال کردن این فرامین، برنامه sendmail آدرس‌های پست الکترونیکی مربوط به حوزه‌های فرعی localhost، localhost.localdomain، mydomainalias.com و mydomain.lan را مشابه آدرس‌های پست الکترونیکی مربوط به حوزه‌ای خواهد داشت که توسط فرمان MASQUERADE_AS مشخص شده است:

```
dnl MASQUERADE_DOMAIN(localhost)dnl
dnl MASQUERADE_DOMAIN(localhost.localdomain)dnl
dnl MASQUERADE_DOMAIN(mydomainalias.com)dnl
dnl MASQUERADE_DOMAIN(mydomain.lan)dnl
```

به کمک فرمان MAILER می‌توان نوع سرور ارسال کننده پیغام الکترونیکی را مشخص کرد. برای نمونه، به این دستورالعمل‌ها توجه کنید:

```
MAILER(smtp)dnl
MAILER(procmail)dnl
```

فایل /etc/mail/sendmail.mc

پیش از هر اقدامی، از فایل‌های sendmail.cf و sendmail.mc مستقر در فهرست /etc/mail یک نسخه پشتیبان تهیه کنید.

اکنون باید تنظیمات پیش‌فرض فایل sendmail.mc را تغییر دهید. این دستورالعمل برنامه sendmail را وادار می‌کند تا پیغام‌های الکترونیکی را صرفاً به یک آدرس مشخص یعنی 127.0.0.1 که بیانگر آدرس کامپیوتر محلی است، ارسال کند:

```
DAEMON_OPTIONS(`Port=smtp,Addr=127.0.0.1, Name=MTA')
```

در صورت دسترسی به یک سرور DNS قابل اعتماد و برخورداری از اینترنت پرسرعت، این دستورالعمل را غیرفعال کنید:

```
FEATURE(`accept_unresolve_domains')dnl
```

دستورالعمل فوق موجب می‌شود تا برنامه sendmail از کسب اطمینان درباره حوزه مربوط به آدرس الکترونیکی مربوط به پیغام‌های دریافتی صرف نظر کند. برای غیرفعال کردن دستورالعمل مزبور کافی است در ابتدای خط مربوطه نشانه dnl را درج کنید. البته فراموش نکنید که باید سرویس sendmail را مجدداً راه‌اندازی کنید.

فایل submit.mc

فایل submit.mc ماکرویی است که به منظور تولید فایل submit.cf یعنی فایل پیکربندی برنامه sendmail برای پیغام‌های ارسالی پیش‌بینی شده است. فایل submit.mc کم‌وبیش شبیه به فایل sendmail.mc بوده اما از ساختار ساده‌تری برخوردار است. عموماً نیازی به ویرایش این فایل نیست. با وجود این، اطلاع از ساختار آن بسیار مفید است. اجازه دهید تا به بررسی محتوای این فایل بپردازیم. عملکرد این دستورالعمل‌ها را قبلاً در قالب فایل پیکربندی sendmail.mc توضیح دادیم و بنابراین از توضیح مجدد صرف‌نظر می‌کنیم:

```
divert(-1)dnl
divert(0)dnl
include(`/usr/share/sendmail-cf/m4/cf.m4')
VERSIONID(`linux setup for Red Hat Linux')dnl
```

دستورالعمل confCF_VERSION شاخص مربوط به فایل پیکربندی را مشخص می‌کند:

```
define(`confCF_VERSION',`Submit')dnl
```

این دستورالعمل، مشابه دستورالعمل OSTYPE(`linux')dnl که قبلاً آن‌را در قالب فایل پیکربندی sendmail.mc مشاهده کردید، نوع سیستم‌عامل را مشخص می‌کند:

```
define(`__OSTYPE__',`')dnl dirty hack to keep proto.m4 from
complaining
```

شاخص DECNET بیانگر نوعی پیکربندی شبکه است که در کامپیوترهای mainframe و میکروکامپیوترهای قدیمی مورد بهره‌برداری قرار می‌گرفت. به دستورالعمل مربوطه توجه کنید:

```
define(`_USE_DECNET_SYNTAX_',`1')dnl support DECnet
```

متغیر confTIME_ZONE برچسب زمان (شامل تاریخ و ساعت) را مشخص می‌کند. به دستورالعمل مربوطه توجه کنید:

```
define(`confTIME_ZONE',`USE_TZ')dnl
```

این دستورالعمل از مراجعه به بانک اطلاعاتی NIS به منظور دستیابی به اسامی کاربران و کلمات عبور جلوگیری به عمل می‌آورد: (به واسطه ذخیره اسامی کاربران و کلمات عبور در بانک اطلاعاتی NIS می‌توان این بانک اطلاعاتی را منبع جایگزینی برای فایل /etc/passwd در نظر گرفت.)

```
define(`confDONT_INIT_GROUPS',`True')dnl
```

این دستورالعمل موقعیت فایل حاوی شناسه فرآیندها (اصطلاحاً process identifier یا PID) را مشخص می‌کند:

```
define(`confPID_FILE',`/var/run/sm-client.pid')dnl
```

این دستورالعمل امکان استفاده از فرم استاندارد اسامی میزبان (اصطلاحاً canonical host names) را در اختیار قرار می‌دهد:

```
dnl define(`confDIRECT_SUBMISSION_MODIFIERS',`C')
```

این دستورالعمل امکان دستیابی به فایل /etc/mail/trusted-users را در مورد کاربران استاندارد فراهم می‌کند:

```
FEATURE(`use_ct_file')dnl
dnl
dnl If you use IPv6 only, change [127.0.0.1] to [Ipv6::::1]
```

این دستورالعمل امکان دستیابی به برنامه تبادل پیغام (اصطلاحاً Message Submission Program یا MSP) موجود روی کامپیوتر محلی را در اختیار می‌گذارد:

```
FEATURE(`msp',`[127.0.0.1]')dnl
```

در بیشتر موارد نیازی نیست که محتوای این فایل را تغییر دهید. با وجود این، در صورتی که قصد هر گونه تغییری را در ساختار این فایل دارید، بهتر است ابتدا از آن یک نسخه پشتیبان تهیه کنید.

چنان‌چه بسته نرم‌افزاری sendmail-doc-*RPM را نصب کرده باشید، با مراجعه به فایل README.cf در فهرست /usr/share/doc/sendmail می‌توانید اطلاعات بیشتری درباره این فایل به دست آورید.

راه‌اندازی مجدد برنامه sendmail

اگر تا به حال برای تهیه نسخه پشتیبان از فایل پیکربندی sendmail.cf اقدام نکردید، اکنون بهتر است این کار را انجام دهید. پس از اعمال تغییرات موردنظر به این فایل، کافی است برنامه m4 یا فرمان make -C /etc/mail را اجرا کنید تا به این ترتیب نسخه جدیدی از فایل پیکربندی sendmail.cf تولید شود. سپس جهت راه‌اندازی مجدد سرویس sendmail این فرمان را اجرا کنید:

```
# m4 /etc/mail/submit.mc > /etc/mail/submit.cf
# service sendmail restart
```

تأثیر فرمان اخیر تنها در صورتی قابل مشاهده است که بسته نرم‌افزاری sendmail-cf-* را نصب کرده باشید.

برنامه‌های مورد استفاده برای دریافت پیغام‌های الکترونیکی

در حال حاضر جهت دریافت پیغام‌های الکترونیکی ارسالی از دو برنامه متداول استفاده می‌شود. یکی از این دو برنامه بر اساس پروتکل POP3 و دیگری بر اساس پروتکل IMAP4 پیاده‌سازی شده است. در سیستم‌عامل Red Hat Linux هر دو پروتکل مزبور در قالب بسته نرم‌افزاری imap-* پیاده‌سازی شده و تحت عنوان سرویس xinetd قابل بهره‌برداری است. (برای اطلاع بیشتر درباره سرویس xinetd به فصل بیست و سوم مراجعه کنید.)

برای دریافت پیغام‌های الکترونیکی ارسالی نیازی به نصب این برنامه‌ها نبوده و می‌توان سرویس‌های مشابهی را که از طریق وب سایت‌هایی چون mail.com یا yahoo.com قابل دستیابی است مورد بهره‌برداری قرار داد. به بیان دیگر، نصب این برنامه‌ها تنها در صورتی ضرورت دارد که مایل باشید تا سرویس دریافت پیغام‌های الکترونیکی را در اختیار کاربران قرار دهید. پس از نصب برنامه مورد نظر، برای فعال کردن پیکربندی مربوطه کافی است فرمان service *servername* on را اجرا کرده و سپس فرمان service xinetd reload را جهت اطمینان از بازخوانی فایل پیکربندی مزبور توسط سرویس xinetd اجرا کنید.

چنان‌چه در شبکه محلی خود از یک سرور DNS استفاده می‌کنید، برای پیکربندی برنامه مورد بحث می‌توانید رکورد MX جدیدی را در بانک اطلاعاتی مربوطه از فهرست /var/named درج کنید. (برای

اطلاعات بیشتر درباره سرویس DNS به فصل بیست و چهارم مراجعه کنید.)

پروتکل POP3 کاربردهای اینترنتی متداول‌تری نسبت به پروتکل IMAP4 دارد. به محض آن‌که از طریق یک برنامه کلاینت مانند Netscape ،Evolution یا برنامه‌های مشابه برای استفاده از سرویس پست الکترونیکی اقدام می‌کنید، سرور POP3 (یعنی برنامه‌ای که بر اساس این پروتکل پیاده‌سازی و روی سرور نصب و پیکربندی شده و آماده سرویس‌دهی است.) اقدامات لازم برای بارگذاری پیغام‌های الکترونیکی را انجام می‌دهد. بیشتر برنامه‌های کلاینت امکان نگهداری نسخه‌ای از پیغام‌های الکترونیکی را روی سرور در اختیار قرار می‌دهند.

در مقابل، پروتکل IMAP4 نسبت به POP3 دارای انعطاف بیشتری است. در صورت استفاده از سرور IMAP4 (یعنی برنامه‌ای که بر اساس پروتکل IMAP4 پیاده‌سازی و روی سرور نصب و پیکربندی شده و آماده سرویس‌دهی است.) امکان سازمان‌دهی پیغام‌های الکترونیکی را در قالب فهرست‌های مختلف روی سرور در اختیار قرار می‌دهند، به طوری که می‌توان پیغام‌های الکترونیکی را بر اساس کلمات کلیدی جستجو و تنها پیغام‌های موردنظر را بارگذاری کرد. این قابلیت برای آن دسته از کاربرانی مفید است که در محل‌کار خود از چندین کامپیوتر استفاده می‌کنند. چنین کاربرانی می‌توانند تمام پیغام‌های الکترونیکی خود را تنها از طریق یک منبع واحد مورد دسترسی قرار دهند.

سرور POP3

پس از فعال کردن سرور POP3 لازم است برای آن دسته از کاربرانی که قصد دسترسی به سرور مزبور را دارند، حساب کاربری باز کنید. با وجود این، نیازی نیست که برای هر کدام از کاربران یک فهرست خانگی (اصطلاحاً home directory) ایجاد کنید.

چنان‌که از فصل نهم به خاطر دارید، اجرای فرمان useradd *username* به طور خودکار برای کاربری با شناسه *username* یک فهرست خانگی ایجاد می‌کند. با وجود این، اگر به واسطه ویرایش محتوای فایل /etc/passwd برای تعریف یک کاربر جدید اقدام کرده باشید، لزومی ندارد که فهرست خانگی جدیدی را نیز به طور دستی برای آن کاربر ایجاد کنید. با اجرای فرمان passwd *username* می‌توانید کلمه عبور جدیدی را به نام کاربری *username* نسبت دهید.

پس از ایجاد یک حساب کاربری جدید، لازم است اطلاعاتی را درباره تنظیمات موردنیاز شامل تعیین نام کاربری و نام کامل حوزه مربوط به سرور POP3 موردنظر را در اختیار آن کاربر قرار دهید. نحوه انجام این تنظیمات را در برنامه‌های کلاینت مختلف به طور مفصل در انتهای همین فصل مورد بررسی قرار خواهیم داد.

سرور IMAP4

مشابه سرور POP3، پس از فعال کردن سرور IMAP4 نیز لازم است برای آن دسته از کاربرانی که قصد دسترسی به سرور مزبور را دارند، حساب کاربری باز کنید. به بیان دیگر، کاربرانی که قصد دسترسی به سرور IMAP4 را دارند باید از یک حساب کاربری معتبر روی کامپیوتر میزبان سرور مزبور برخوردار باشند. با وجود این، برخلاف سرور POP3، این گونه کاربران باید از یک فهرست خانگی نیز روی کامپیوتر میزبان سرور IMAP4 برخوردار باشند.

چنان‌که در فصل نهم نیز اشاره شد، اجرای فرمان useradd *username* به طور خودکار منجر به ایجاد فهرست خانگی کاربری با شناسه *username* می‌شود. با اجرای فرمان passwd *username* نیز می‌توان کلمه عبور جدیدی را به کاربری با شناسه *username* منسوب کرد.

بار دیگر، مشابه سرور POP3، پس از ایجاد یک حساب کاربری جدید لازم است اطلاعاتی را درباره تنظیمات موردنیاز شامل تعیین نام کاربری و نام کامل حوزه مربوط به سرور IMAP4 موردنظر را در اختیار آن کاربر قرار دهید.

پیکربندی برنامه‌های کلاینت مورد استفاده جهت استفاده از سرویس پست الکترونیکی

اغلب کاربران از برنامه‌های گرافیکی چون Evolution و Netscape به عنوان برنامه کلاینت موردنیاز جهت بهره‌برداری از سرویس پست الکترونیکی استفاده می‌کنند. با وجود این، استفاده از برنامه‌های متنی برای این منظور در میان کاربران سیستم عامل‌های UNIX و Linux هم‌چنان رایج است. به ویژه مدیران با تجربه سیستم‌عامل Linux، که برای امور روزمره خود ازسطر فرمان این سیستم‌عامل استفاده می‌کنند، بهره‌گیری از برنامه‌های متنی را نیز به استفاده از برنامه‌های گرافیکی ترجیح می‌دهند. با وجودی که برنامه‌های گرافیکی از ظاهر زیباتری برخوردار هستند، چنان‌چه تعداد کاربرانی که به طور هم‌زمان از چنین برنامه‌هایی استفاده می‌کنند قابل توجه باشد، سرور پست الکترونیکی به خوبی قادر به سرویس‌دهی نخواهد بود.

در برخی موارد ممکن است لازم باشد تا مدیران سیستم‌ها راهنمایی‌هایی را نیز به منظور پیکربندی این گونه برنامه‌ها در اختیار کاربران قرار دهند.

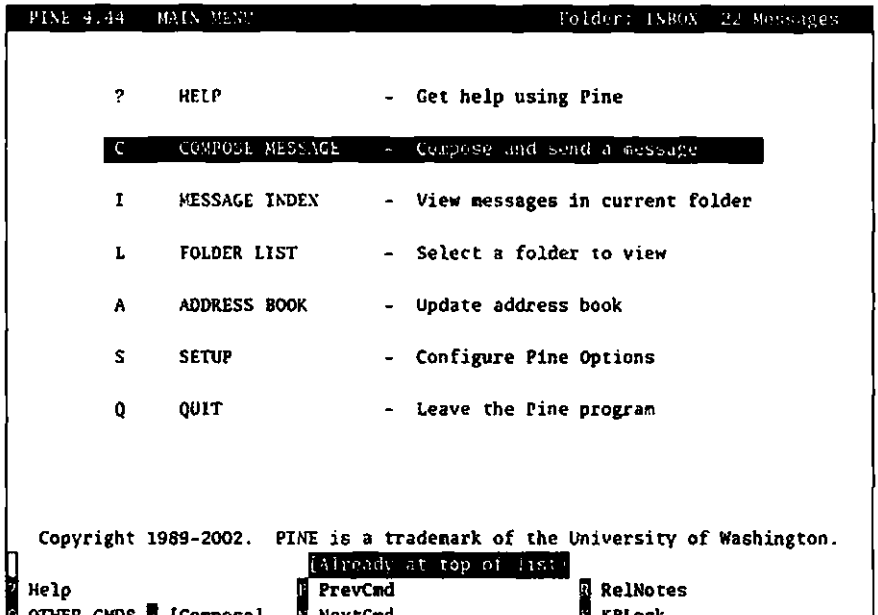
برنامه‌های متنی مورد استفاده جهت بهره‌برداری از سرویس پست الکترونیکی

برنامه mail در سیستم‌عامل Linux به منظور ارسال و دریافت پیغام‌های الکترونیکی پیش‌بینی شده است. با وجود این، کاربران کم‌تجربه استفاده از برنامه‌های گرافیکی را برای این منظور ترجیح می‌دهند. این در حالی است که کاربران حرفه‌ای، به ویژه در دانشگاه‌ها استفاده گسترده‌ای از برنامه‌های متنی به عمل می‌آورند. به احتمال قوی می‌توان دو برنامه pine و elm را متداول‌ترین برنامه‌های متنی مورد استفاده در سیستم‌عامل Linux جهت بهره‌برداری از سرویس پست الکترونیکی محسوب کرد. با وجودی که در نسخه‌های آتی سیستم‌عامل Red Hat Linux امکان حذف برنامه pine (یا Program for Internet News and E-mail) وجود دارد، این برنامه نسبت به برنامه elm کاربرپسندتر است. از این‌رو، در این قسمت به شرح برنامه مذکور خواهیم پرداخت.

چنان‌چه برنامه pine به همراه سیستم‌عامل Red Hat Linux روی کامپیوتر میزبان نصب نشده باشد، به سادگی می‌توان جهت نصب بسته نرم‌افزاری RPM مربوطه با عنوان *-pine اقدام کرد. پس از نصب بسته نرم‌افزاری مزبور، برنامه pine به محض اجرای فرمانی با همین نام قابل بهره‌برداری خواهد بود. متأسفانه شرکت Red Hat در نسخه‌های آتی سیستم‌عامل خود قصد صرف نظر کردن از این برنامه را دارد. از این‌رو، ممکن است لازم باشد تا از برنامه‌های دیگری استفاده کنید. در قسمت بعد به شرح برخی از برنامه‌های گرافیکی موجود برای بهره‌برداری از سرویس پست الکترونیکی خواهیم پرداخت. با وجود این، در صورتی که به برنامه‌های متنی علاقه‌مند باشید، به جای استفاده از برنامه pine می‌توانید برنامه دیگری با عنوان mutt را مورد بهره‌برداری قرار دهید.

چنان‌که در شکل ۱-۲۶ مشاهده می‌کنید، به محض اجرای برنامه pine اطلاعات مختصری درباره این برنامه به همراه منوی اصلی ظاهر می‌شود. به منظور تعامل با برنامه pine می‌توانید از فرامین موجود در قسمت بالا (شامل ?، C، I، L، A، S، و Q) و گزینه‌های موجود در قسمت پایین این منو (شامل ?، P، R، O، >، N، و K) استفاده کنید.

فرامین منوی برنامه pine از جمله موارد بسیار نادری است که سیستم‌عامل Linux تفاوتی میان بزرگ و کوچک قایل نمی‌شود، چنان‌که برای مثال جهت صدور فرمان **P** می‌توان از گزینه **p** نیز استفاده کرد.

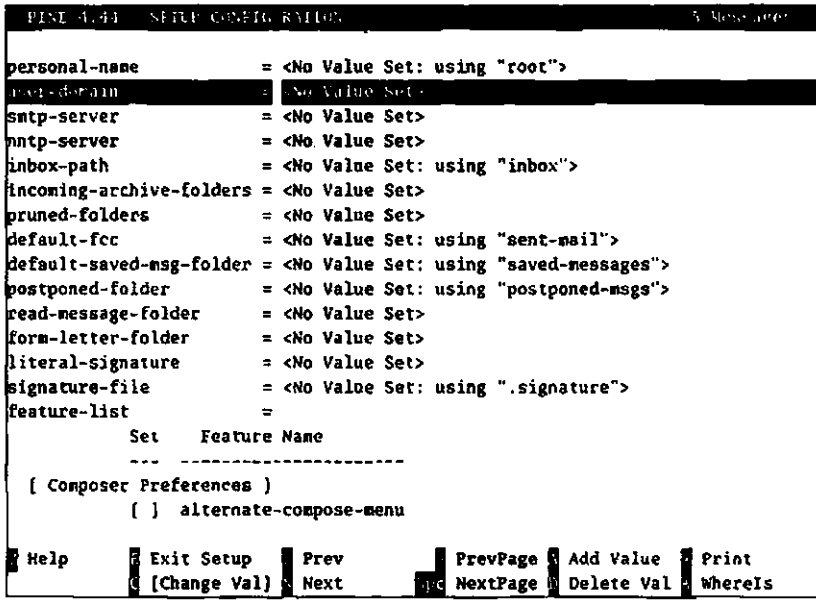


شکل ۱-۲۶ منوی اصلی برنامه pine

در برنامه pine فرمان **C** برای نوشتن پیغام جدید، فرمان **I** برای مشاهده متن پیغام جاری و فرمان **L** برای مشاهده محتوای پوشه حاوی پیغام‌ها پیش‌بینی شده‌اند. برای‌آن‌که بازخوانی پیغام‌ها توسط برنامه pine انجام شود باید آن‌را پیکربندی کنید. فرمان **S** برای همین منظور پیش‌بینی شده است. پس از صدور فرمان مزبور، برای پیکربندی اولیه فرمان **C** را صادر کنید. شکل ۲-۲۶ نتیجه حاصل از این اقدام را نشان می‌دهد.

چنان‌که مشاهده می‌کنید، تعداد گزینه‌های مربوط پیکربندی برنامه pine نسبتاً زیاد است. با وجود این، به فرض آن‌که آدرس الکترونیکی شما abcd@example.com بوده و آدرس سرور پست الکترونیکی مورد استفاده برای دریافت پیغام‌ها mail.example.com باشد، برای تنظیم این برنامه به نحوی که بتوان آن‌را برای ارسال و دریافت پیغام‌های الکترونیکی مورد استفاده قرار داد، کافی است این سه اقدام را انجام دهید:

- متغیر personal-name را برابر با عنوان ارسال کننده پیغام الکترونیکی قرار دهید.
- متغیر user-domain را برابر با نام حوزه میزبان آدرس الکترونیکی abcd@example.com یعنی **example.com** قرار دهید.



شکل ۲-۲۶ گزینه‌های مربوط به پیکربندی برنامه pine

- متغیر inbox-path را به نحو مطلوب تنظیم کنید. برای مثال، چنان‌چه سرور mail.example.com از نوع POP3 باشد، کافی است متغیر inbox-path را برابر با دنباله کاراکتری **{mail.example.com/pop3/user=abcd}INBOX** و در صورتی که از نوع IMAP4 باشد برابر با **{mail.example.com/user=abcd}** قرار دهید.

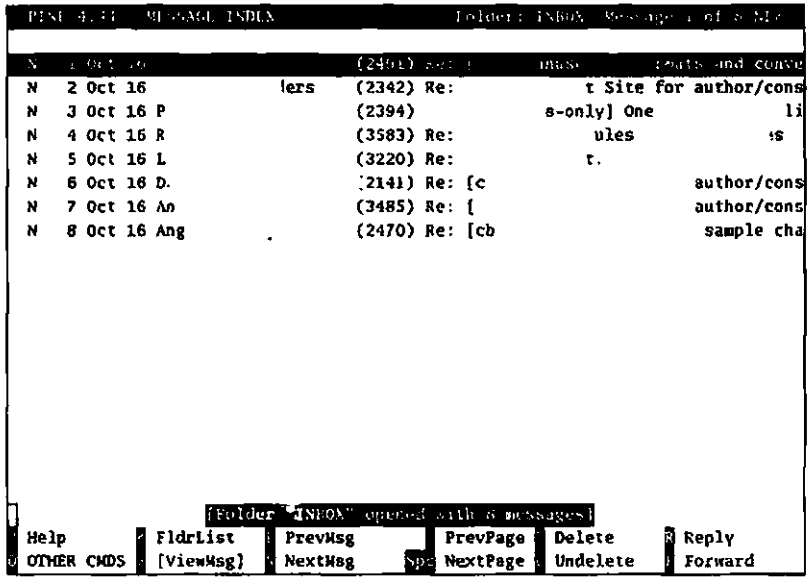
برخی از سرورهای پست الکترونیکی به تنظیمات خاصی نیاز دارند. برای مثال، در مورد برخی از حوزه‌ها تعیین دقیق آدرس الکترونیکی، هم‌چون abcd@example.com ضروری است. هم‌چنین ممکن است نام حوزه متفاوتی برای سرور پست الکترونیکی مورد استفاده برای دریافت پیغام‌های ارسالی (که توسط متغیر user-domain مشخص می‌شود) موردنیاز باشد. برای اطلاع دقیق از این موضوع با ارایه کننده خدمات پست الکترونیکی خود مشورت کنید.

در صورت استفاده از یک سرور SMTP خارجی (مانند سرور SMTP مستقر در ISP) می‌توانید مشخصات آن‌را ضمن پیکربندی برنامه pine وارد کنید. برای این منظور، کلید Page Down را فشار داده و گزینه مورد نظر خود را انتخاب کنید.

نسخه 4.x برنامه pine و نسخه‌های قدیمی‌تر آن امکان دستیابی به سرور POP3 را در اختیار قرار نمی‌دهند.

پس از انجام تنظیمات مورد نظر، فرمان E را برای خروج از حالت Setup Configuration صادر کنید. سپس حرف Y را برای تأیید عملیات تایپ کنید. با این اقدام منوی اصلی برنامه pine را مجدداً مشاهده خواهید کرد. ضمن مشاهده این منو، پس از صدور فرمان L گزینه INBOX را انتخاب کرده و کلید Enter را فشار دهید. نخستین مرتبه‌ای که این اقدام را انجام می‌دهید، برنامه pine امکان تعیین کلمه عبور را در اختیار قرار خواهد داد.

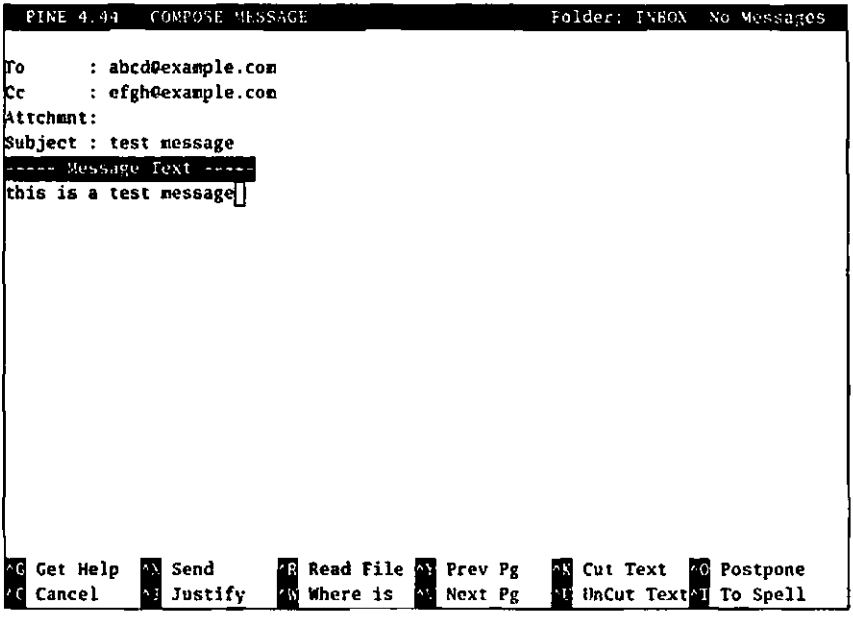
سپس برنامه pine با دسترسی به سرور پست الکترونیکی اقدام لازم برای دریافت آخرین پیغام‌ها را انجام خواهد داد. شکل ۳-۲۶ نتیجه حاصل از این اقدام را نشان می‌دهد. کاربرد فرامین موجود در قسمت پایین صفحه کاملاً آشکار بوده و نیازی به توضیح نیست. برای مشاهده محتوای پیغام موردنظر کافی است آن‌را انتخاب کرده و کلید Enter را فشار دهید.



شکل ۳-۲۶ مشاهده لیست پیغام‌ها در برنامه pine

ایجاد پیغام جدید در برنامه pine به سادگی امکان‌پذیر است. برای این منظور، پس از دستیابی به منوی اصلی، فرمان C را جهت نوشتن متن پیغام موردنظر صادر کنید. اگر تا به حال برای ارسال پیغام‌های الکترونیکی اقدام کرده باشید، به احتمال قوی صفحه‌ای مشابه صفحه شکل ۴-۲۶ را مشاهده کرده‌اید.

فرامین موجود در قسمت پایین این صفحه به خوبی امکانات لازم را در اختیار قرار می‌دهد. برای مثال، پس از پیکربندی پیغام الکترونیکی موردنظر کافی است فرمان Ctrl+X را صادر کرده و در ادامه کلید Y را جهت تأیید عملیات فشار دهید تا به این ترتیب پیغام مزبور به مقصد ارسال شود. در صورت استفاده از سرور SMTP یا فعال بودن سرویس sendmail، برنامه pine پیغام الکترونیکی را به طور خودکار ارسال خواهد کرد.



شکل ۴-۲۶ ایجاد یک پیغام جدید در برنامه pine

برنامه‌های گرافیکی

در سیستم‌عامل Linux سه برنامه Evolution، Mozilla و Kmail به عنوان برنامه‌های گرافیکی مورد استفاده برای ارسال و دریافت پیغام‌های الکترونیکی در نظر گرفته شده‌اند. عملیات اصلی این برنامه‌ها را قبلاً در قسمت چهارم کتاب مورد بررسی قرار دادیم. در این قسمت به بررسی نحوه پیکربندی این برنامه‌ها می‌پردازیم.

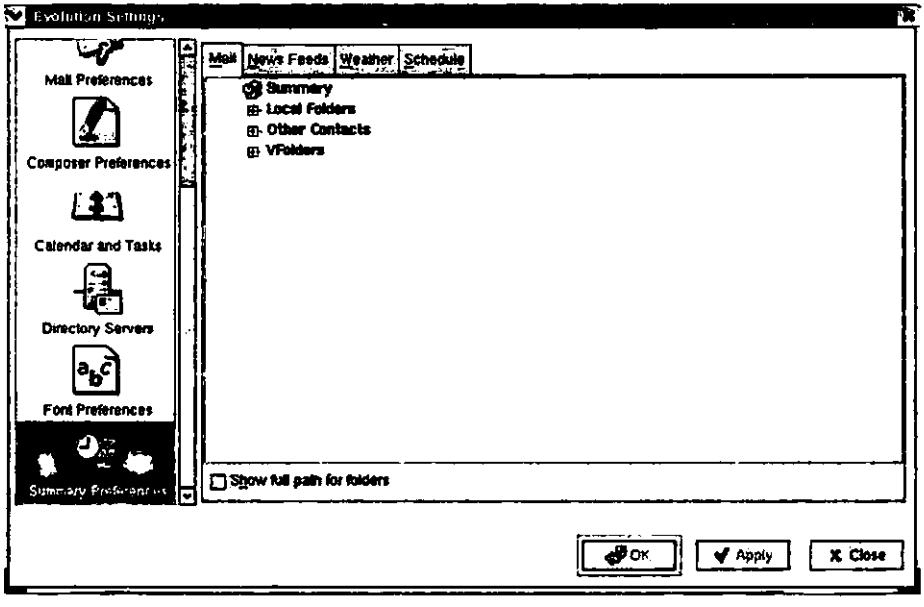
پیکربندی تمام برنامه‌های کلاینت مورد استفاده برای ارسال و دریافت پیغام‌های الکترونیکی کم‌وبیش مشابه است. چنان‌که در مورد برنامه pine نیز مشاهده کردید، دست کم باید به اطلاعات مندرج در جدول ۲-۲۶ دسترسی داشته باشد.

جدول ۲-۲۶ اطلاعات موردنیاز برای پیکربندی برنامه‌های کلاینت مورد استفاده جهت ارسال و دریافت پیغام‌های الکترونیکی

عنوان اطلاعات	توضیح
Name	نام یا شناسه ارسال کننده پیغام
Domain Name	دنباله کاراکتری موجود بعد از علامت @ در آدرس پست الکترونیکی
Inbox Server	نام کامل حوزه میزبان سرور مورد استفاده برای دریافت پیغام‌های الکترونیکی (این نام گاهی اوقات تحت عنوان Host یا Server Name قابل دستیابی است.)
Username	نام کاربری مورد استفاده برای دسترسی به سرور (معمولاً دنباله کاراکتری موجود قبل از علامت @ در آدرس پست الکترونیکی)

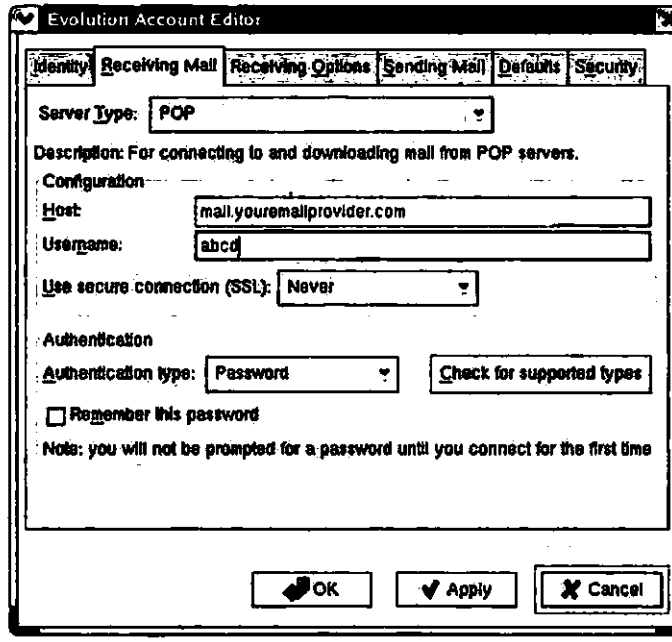
پیکربندی برنامه Evolution

در صورت استفاده از برنامه Evolution آن‌را در محیط گرافیکی موردنظر خود باز کرده و سپس گزینه Settings را از منوی Tools انتخاب کنید. با این اقدام پنجره Evolution Settings را مشاهده خواهید کرد. شکل ۵-۲۶ نمایی از این پنجره را نشان می‌دهد.



شکل ۵-۲۶ پنجره Evolution Settings

در سمت چپ این پنجره روی آیکن Mail Accounts کلیک کنید. سپس به منظور ایجاد یک حساب جدید روی گزینه Add کلیک کنید. هم‌چنین می‌توانید یکی از حساب‌های موجود را انتخاب کرده و گزینه Edit را جهت ویرایش آن کلیک کنید. با این اقدام کادر محاوره‌ای Evolution Account Editor باز خواهد شد. شکل ۶-۲۶ کادر محاوره‌ای مزبور را نشان می‌دهد. اطلاعات اصلی مربوط به حساب کاربری موردنظر خود را در بخش Identity از این کادر محاوره‌ای وارد کنید. سپس در صورت نیاز نوع سرور را از لیست مربوطه با عنوان Server Type از بخش Receiving Mail کادر محاوره‌ای مورد بحث انتخاب کرده و نام کامل حوزه میزبان سرور پست الکترونیکی را در کادر متنی Host و نام کاربری مورد استفاده برای دسترسی به سرور مزبور را در کادر متنی Username وارد کنید. در فصل هجدهم به توضیح مفصل‌تری از این برنامه پرداخته شده است.

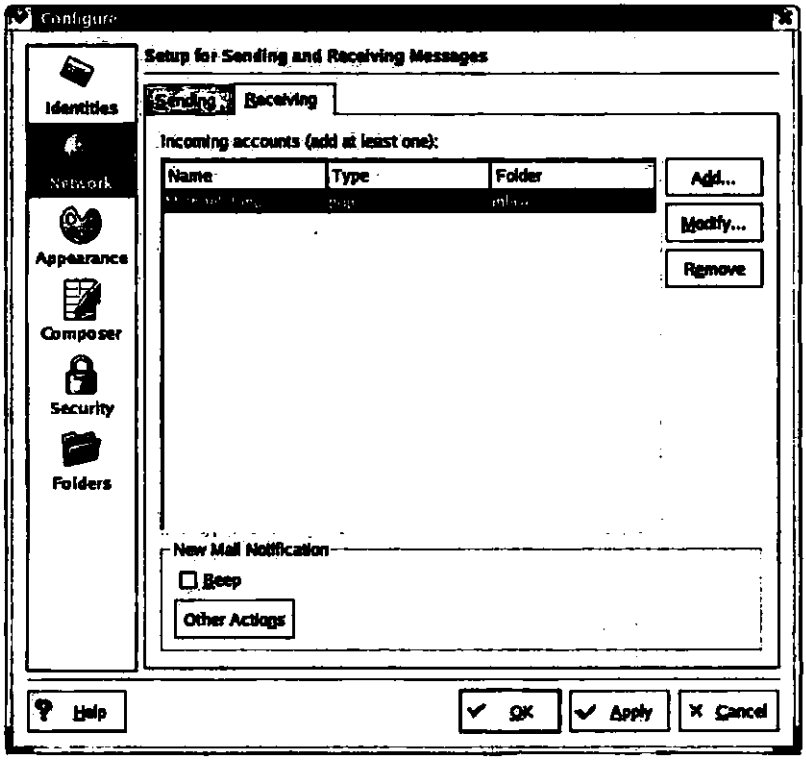


شکل ۶-۲۶ بخش Receiving Mail از کادر محاوره‌ای Evolution Account Editor

پیکربندی برنامه KMail

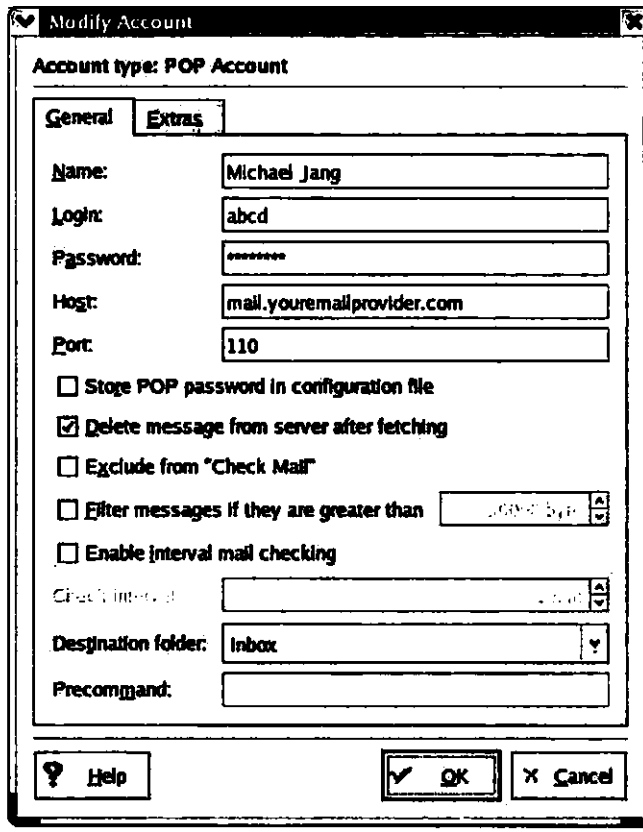
در صورت استفاده از برنامه KMail آن‌را در محیط گرافیکی موردنظر خود باز کرده و گزینه Configure Kmail را از منوی Settings انتخاب کنید تا به این ترتیب کادر محاوره‌ای Configure KMail باز شود. شکل ۷-۲۶ این کادر محاوره‌ای را نشان می‌دهد. در سمت چپ کادر محاوره‌ای مزبور گزینه Network

را انتخاب کرده و سپس در بخش Receiving دکمه Add را به منظور ایجاد یک حساب کاربری جدید کلیک کنید. با این اقدام امکانات لازم جهت تعیین نوع حساب، شامل local، POP3، IMAP4 و Maildir در اختیارتان قرار می‌گیرد. برای تغییر مشخصات یک حساب کاربری موجود کافی است آن‌را انتخاب کرده و دکمه Modify را کلیک کنید.



شکل ۷-۲۶ کادر محاوره‌ای Configure KMail

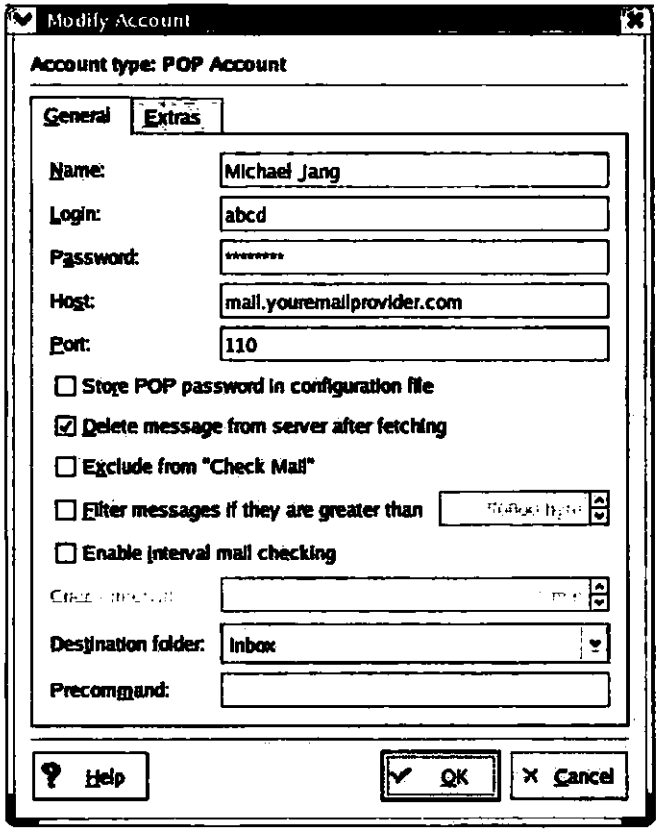
با توجه به نوع عملیات، یعنی ایجاد یک حساب کاربری جدید یا تغییر مشخصات یک حساب کاربری موجود، یکی از دو کادر محاوره‌ای Add Account - Kmail یا Modify Account - Kmail باز خواهد شد. تنها تفاوت میان این دو کادر محاوره‌ای در عنوان آنهاست. برای نمونه، شکل ۸-۲۶ کادر محاوره‌ای Modify Account - Kmail را نشان می‌دهد. شناسه ارسال کننده پیغام را در کادر متنی Name و کلمه عبور موردنظر را در کادر متنی Password وارد کنید. سپس نام کامل حوزه میزبان سرور پست الکترونیکی را در کادر متنی Host و شناسه کاربری خود روی آن سرور را در کادر متنی Login وارد کنید. در فصل هفدهم به توضیح مفصل‌تری از این برنامه پرداخته شده است.



شکل ۸-۲۶ کادر محاوره‌ای Modify Account - KMail

پیکربندی برنامه Mozilla Mail

چنان‌چه تا به حال از برنامه Mozilla Mail استفاده کرده باشید به طور قطع متوجه شباهت آن با برنامه کلاینت تعبیه شده در نرم‌افزار Netscape 6.x جهت ارسال و دریافت پیغام‌های الکترونیکی شده‌اید. (شرکت Netscape نرم‌افزارهای خود را تحت لیسانس GPL منتشر می‌کند.) برای استفاده از قابلیت‌های برنامه Mozilla Mail آن‌را در محیط گرافیکی موردنظر باز کنید. سپس از منوی Edit گزینه Mail & Newsgroups Account Settings را انتخاب کنید تا به این ترتیب کادر محاوره‌ای مربوطه با عنوان Mail & Newsgroups Account Settings باز شود. چنان‌چه قبلاً برای ایجاد حساب کاربری اقدام نکرده باشید، برای شروع باید از طریق ابزار Mozilla Mail Account Wizard این کار را صورت دهید. شکل ۹-۲۶ کادر محاوره‌ای مزبور را نشان می‌دهد.



شکل ۹-۲۶ کادر محاوره‌ای Mail & Newsgroups Account Settings

در کادر محاوره‌ای Mail & Newsgroups Account Settings حساب کاربری موردنظر را انتخاب کنید. در صورت تمایل می‌توانید اطلاعات بیشتری را درباره این حساب در کادرهای متنی مربوطه درج کنید. سپس گزینه Server Settings را انتخاب کنید. با این اقدام عنوان سرور پست الکترونیکی را در کادر متنی Server Name مشاهده خواهید کرد. (برای اطلاع بیشتر درباره برنامه Mozilla Mail به فصل شانزدهم مراجعه کنید.)

بسیاری از اعضای جامعه کاربران نرم‌افزارهای کدباز و نرم‌افزارهای رایگان (اصطلاحاً FSF) از این بابت که شرکت Netscape نرم‌افزارهای خود را تحت لیسانس GPL منتشر می‌کند، اظهار رضایت نمی‌کنند. برای نمونه به آدرس اینترنتی http://www.gnu.org/philosophy/netscape-npl.html مراجعه کنید.

جمع‌بندی

سرورهای پست الکترونیکی را با توجه به کاربرد می‌توان به دو نوع تقسیم کرد: سرورهایی که وظیفه ارسال پیغام‌های الکترونیکی را به عهده دارند و سرورهایی که وظیفه دریافت آن‌ها را انجام می‌دهند. این سرورها وظیفه ارسال و دریافت پیغام‌های الکترونیکی را براساس پروتکل‌های TCP/IP شامل SMTP، POP3 و IMAP4 انجام می‌دهند. برای ارسال و دریافت پیغام‌های الکترونیکی بر اساس این پروتکل‌ها می‌توان یکی از سرویس‌های مربوطه شامل MTA، MDA و MUA را انتخاب کرد. سرویس MTA که برنامه sendmail نمونه پیاده‌سازی شده آن است، جهت ارسال پیغام‌های الکترونیکی از طریق شبکه پیش بینی شده است. سرویس MDA که برنامه procmail نمونه پیاده‌سازی شده آن است، پیغام‌های الکترونیکی را از شبکه اینترنت دریافت کرده و آن‌ها را روی سرورهای دریافت کننده پیغام‌های الکترونیکی ذخیره می‌کند. سرویس MUA نیز جهت دستیابی به پیغام‌های الکترونیکی پیش‌بینی شده است. برنامه‌های pine، Kmail، Mozilla Mail و Evolution نمونه‌های پیاده‌سازی شده‌ای از این سرویس محسوب می‌شوند.

برنامه sendmail در حال حاضر متداول‌ترین سرور مورد استفاده برای ارسال پیغام‌های الکترونیکی از طریق شبکه اینترنت است. به دلیل دشوار بودن ویرایش فایل پیکربندی sendmail.cf در سیستم‌عامل Red Hat Linux فایل ماکرویی با عنوان sendmail.mc پیش‌بینی شده که به لحاظ ویرایش و بازخوانی بسیار ساده‌تر از آن است. فایل sendmail.mc را به کمک پردازنده ماکروی m4 می‌توان به فایل پیکربندی sendmail.cf تبدیل کرد. دو فایل پیکربندی دیگر برنامه sendmail با عنوان /etc/aliases و /etc/sysconfig/sendmail نیز به جهاتی حایز اهمیت هستند. تعداد دیگری از فایل‌های پیکربندی این برنامه نیز در فهرست /etc/mail مستقر شده‌اند. پس از ویرایش فایل پیکربندی sendmail.cf با اجرای فرمان service sendmail restart باید ترتیبی داد تا این فایل توسط برنامه sendmail مورد بازخوانی قرار بگیرد.

سرورهای پست الکترونیکی متعددی بر اساس پروتکل‌های POP3 و IMAP4 پیاده‌سازی شده‌اند. تمام این سرویس‌ها را می‌توان به عنوان سرویس‌های xinetd در قالب بسته نرم‌افزاری *-imap نصب کرد. پس از نصب و راه‌اندازی سرویس مورد نظر، به واسطه ایجاد حساب کاربری و اطلاع از نام کامل حوزه میزبان آن سرور، کاربران می‌توانند از امکانات آن بهره‌مند شوند. در صورت استفاده از سرور IMAP4 علاوه بر این موارد باید برای هر یک از کاربران یک فهرست خانگی جهت ذخیره فایل‌های حاوی پیغام‌های الکترونیکی ایجاد کرد.

برنامه‌های متنی و گرافیکی متعددی برای ارسال و دریافت پیغام‌های الکترونیکی جهت استفاده کاربران طراحی شده است. برنامه pine در میان برنامه‌های متنی از قابلیت پیکربندی خوبی برخوردار است. برنامه‌های گرافیکی Evolution، Mozilla Mail و Kmail نیز از جمله برنامه‌های گرافیکی متداول در این زمینه محسوب می‌شوند.

در فصل آینده به بررسی برنامه‌های کلاینت و سرور مورد استفاده جهت بهره‌برداری از سرویس انتقال فایل یا FTP می‌پردازیم. برنامه‌های کلاینت FTP بسیار منعطف هستند، به طوری که با استفاده از فرامین FTP می‌توان بسته‌های نرم‌افزاری RPM را به نسخه‌های بالاتر ارتقا داد. چنان‌که خواهید دید، بهره‌برداری از سرورهای FTP ناشناس، استاندارد و حتی سرورهای FTP امن روی کامپیوترهایی با سیستم‌عامل Red Hat Linux کاملاً عملی است.

بخش هفتم

سرویس‌های اشتراک فایل در سیستم‌عامل Linux

اهداف:

- استفاده از سرویس FTP
- استفاده از سرویس‌های NFS و NIS
- استفاده از سرویس Samba
- استفاده از سرویس‌های وب

فصل بیست‌وهفتم

استفاده از سرویس FTP

سرویس File Transfer Protocol یا به اختصار FTP یکی از قدیمی‌ترین اعضای مجموعه پروتکل‌های TCP/IP است. با وجود این، بهره‌برداری از این سرویس هم‌چنان رو به افزایش است. چنان‌که از نام آن پیداست، سرویس FTP به منظور انتقال فایل از یک کامپیوتر به کامپوتر دیگر طراحی شده است. با وجودی که انتقال فایل به واسطه پروتکل‌های دیگری چون HTTP و سرویس‌های رمزگذاری شده‌ای مانند SFTP نیز امکان‌پذیر است، انجام این کار با استفاده از سرویس FTP سریع‌تر است. به واسطه همین سرویس می‌توانید نسخه جدید سیستم‌عامل Red Hat Linux را به محض انتشار از طریق وب سایت شرکت مربوطه دریافت کنید. در صورت استفاده از خطوط DSL و در شرایط کاملاً برابر (یعنی استفاده از رسانه انتقال کاملاً مشابه) سرویس FTP معمولاً سرعتی دو برابر پروتکل HTTP را در اختیار قرار می‌دهد.

مشابه برخی از دیگر سرویس‌ها، سرویس FTP نیز در قالب دو بخش کلاینت و سرور پیاده‌سازی شده است. برنامه‌های کلاینت FTP مجموعه‌ای از فرامین متنوع را در اختیار می‌گذارند. برای مثال، در صورت استفاده صحیح از فرمان ftp می‌توان بسته‌های نرم‌افزاری RPM موردنظر را مستقیماً به نسخه‌های بالاتر ارتقا داد. علاوه بر این فرامین، امروزه برنامه‌های کلاینت FTP با رابط گرافیکی نیز بسیار متداول شده‌اند.

از میان برنامه‌های سرور FTP متعدد قابل استفاده تحت سیستم‌عامل Linux، در این فصل دو برنامه متداول Very Secure FTP و Washington University's FTP یا به اختصار vsFTP و WU-FTP را مورد بررسی قرار خواهیم داد. هر دو برنامه فوق را می‌توان به منظور دسترسی ناشناس (یا اصطلاحاً anonymous) پیکربندی کرد. در حال حاضر برنامه vsFTP برنامه سرور FTP پیش‌فرض سیستم‌عامل Red Hat Linux محسوب می‌شود. با وجودی که برنامه WU-FTP برنامه سرور FTP پیش‌فرض در سیستم‌عامل Red Hat Linux 8.0 بود، شرکت Red Hat از توزیع آن در نسخه‌های بعدی سیستم‌عامل صرف نظر کرد. هر چند ضریب امنیتی هیچ یک از این برنامه‌ها در حد بسیار مطلوب نیست، دسترسی کاربران و کامپیوترها را می‌توان به واسطه فایل‌های پیکربندی این دو برنامه کنترل کرد. هر دو برنامه

مزبور روش‌هایی را به منظور حفاظت از فایل‌ها و فهرست‌ها در اختیار قرار می‌دهند. در فصل حاضر به بررسی این موضوعات می‌پردازیم:

- استفاده از برنامه کلاینت FTP
- پیکربندی سرور FTP با ضریب ایمنی بالا
- پیکربندی سرور FTP به منظور دسترسی ناشناس
- پیکربندی برنامه WU-FTP با کاربران واقعی کامپیوتر میزبان

استفاده از برنامه کلاینت FTP

سرویس FTP قدمتی طولانی دارد به‌طوری که تعدادی از فرامین آن پیش از ظهور برخی از پوسته‌های سیستم‌عامل UNIX از جمله bash نیز مورد استفاده قرار می‌گرفتند. نحوه استفاده از برنامه کلاینت FTP، حداقل به این دلیل که ارتقای بسته‌های نرم‌افزاری کلیدی سیستم‌عامل Red Hat Linux از طریق سرور FTP انجام می‌شود، برای کاربران این سیستم‌عامل کاملاً ضروری است. مشابه سایر برنامه‌های کلاینت سیستم‌عامل Linux، برنامه‌های کلاینت FTP با رابط گرافیکی (از جمله برنامه gFTP یا به بیان دقیق‌تر GNOME FTP) تنها تسهیلات ساده‌تری را به منظور اجرای فرامین مربوط به سرویس FTP در اختیار قرار می‌دهند. بدیهی است این فرامین را می‌توان از سطر فرمان سیستم‌عامل Linux نیز اجرا کرد.

در قسمت‌های بعد نحوه ارتباط برنامه کلاینت FTP با سایت FTP شرکت Red Hat به آدرس ftp.redhat.com را مورد بررسی قرار می‌دهیم. این سایت، به ویژه در ساعات کاری ایالات متحده از ترافیک زیادی برخوردار است. از این‌رو، شرکت مزبور امکان دسترسی به فایل‌های موجود روی این سایت را از طریق آدرس www.redhat.com/download/mirror.html نیز در دسترس قرار داده است. چنان‌چه به هر دلیل دسترسی به سایت ftp.redhat.com امکان‌پذیر نباشد، توصیه می‌کنیم آدرس فوق را امتحان کنید.

فرامین اصلی موردنیاز برای استفاده از سرویس FTP

چنان‌که در شکل ۱-۲۷ مشاهده می‌کنید، برنامه کلاینت FTP فرامین متعددی را جهت استفاده از سرویس FTP در اختیار قرار می‌دهد. در این قسمت تنها به بررسی فرامین اصلی می‌پردازیم. با اجرای فرمان man ftp می‌توانید راهنمای مربوط به تمام فرامین FTP (حتی فرامینی که معمولاً به ندرت مورد استفاده قرار می‌گیرند) را مشاهده کنید. برای اطلاع از جزییات یک فرمان به‌خصوص، کافی است

در مقابل اعلان <ftp ، فرمان help *command* را که در آن متغیر *command* نماینده فرمان موردنظر است، وارد کنید.

```
Commands may be abbreviated.  Commands are:

!               debug           mdir            sendport        site
$               dir             mget            put             size
account         disconnect      mkdir           pwd             status
append          exit            mls             quit            struct
ascii           form            mode            quote           system
bell            get             modtime         recv            sunique
binary          glob            mput            reget           tenex
bye             hash            newer           rstatus         tick
case            help            nmap            rhelp           trace
cd              idle            nlist           rename          type
cdup            image           ntrans          reset           user
chmod           lcd             open            restart         umask
close           ls              prompt          rmdir           verbose
cr              macdef          passive         runique         ?
delete          mdelete         proxy           send
ftp> help rmdir
rmdir           remove directory on the remote machine
ftp> help open
open            connect to remote ftp
ftp> help close
close           terminate ftp session
ftp>
```

شکل ۱-۲۷ فرامین برنامه کلاینت FTP

جدول ۱-۲۷ برخی از مهم‌ترین فرامین FTP را شرح می‌دهد. با کمی دقت متوجه می‌شوید که تعدادی از این فرامین شبیه به فرامین پوسته bash هستند.

جدول ۱-۲۷ شرح برخی از فرامین FTP

عنوان فرمان	توضیح
!command	این فرمان موجب اجرای فرمان *command* در پوسته سیستم‌عامل می‌شود.
ascii	این فرمان موجب می‌شود تا فرآیند انتقال فایل‌ها در حالت ASCII انجام شود. این حالت برای انتقال فایل‌های متنی مناسب است.
binary	این فرمان موجب می‌شود تا فرآیند انتقال فایل‌ها در حالت Binary انجام شود. این حالت برای انتقال فایل‌های باینری (از جمله فایل‌های اجرایی و فشرده) مناسب است.
bye	این فرمان موجب خروج از برنامه ftp می‌شود. تأثیر این فرمان شبیه به تأثیر فرمان exit است.

عنوان فرمان	توضیح
cd	این فرمان فهرست جاری را به فهرست موردنظر تغییر می‌دهد. تأثیر این فرمان شبیه به تأثیر فرمان مشابه در سیستم‌عامل Linux است.
dir	این فرمان محتوای فهرست جاری کامپیوتر میزبان سرور FTP را نشان می‌دهد. تأثیر این فرمان شبیه به اجرای فرمان ls -l در سیستم‌عامل Linux است.
get *ftpfile localfile*	این فرمان فایل *ftpfile* از کامپیوتر میزبان سرور FTP را تحت عنوان *localfile* روی کامپیوتر میزبان برنامه کلاینت FTP کپی می‌کند. فرمان mget نسخه مشابهی از فرمان get است که امکان استفاده از تکنیک globbing (به‌کارگیری کاراکترهای جانشین جهت تعیین الگوی عمومی فایل‌ها) را در اختیار قرار می‌دهد.
ls	عملکرد این فرمان شبیه به فرمان dir است.
put *localfile ftpfile*	این فرمان فایل *localfile* از کامپیوتر میزبان برنامه کلاینت FTP را تحت عنوان *ftpfile* روی کامپیوتر میزبان سرور FTP کپی می‌کند. فرمان mput نسخه مشابهی از فرمان put است که امکان استفاده از تکنیک globbing (به‌کارگیری کاراکترهای جانشین جهت تعیین الگوی عمومی فایل‌ها) را در اختیار قرار می‌دهد.
pwd	این فرمان موقعیت فهرست جاری را در سیستم فایل کامپیوتر میزبان سرور FTP نمایش می‌دهد. چنان‌چه سرور FTP را جهت برخورداری از ضریب امنیتی بالا پیکربندی کرده باشید، فهرست ریشه نمایش داده شده در ازای اجرای این فرمان، فهرست میزبان فایل‌های برنامه سرور FTP یعنی فهرست /var/ftp خواهد بود.
user	این فرمان امکان وارد کردن شناسه کاربری را در اختیار قرار داده و به دنبال آن اعلان مربوط به کلمه عبور را نمایش می‌دهد.

استفاده از برنامه کلاینت FTP جهت برقراری ارتباط با سرور FTP مستقر روی ماشین ftp.redhat.com

در این قسمت قصد داریم تا برخی از فرامین برنامه کلاینت FTP را در عمل مورد استفاده قرار دهیم. با فرض این‌که کامپیوتر میزبان این برنامه به اینترنت متصل است، فرمان ftp ftp.redhat.com را از سطر فرمان آن اجرا کنید. برخلاف توضیحات مندرج در جدول ۱-۲۷، سایت FTP شرکت Red Hat تنها امکان دسترسی ناشناس یا اصطلاحاً anonymous را در اختیار کاربران قرار می‌دهد. از این‌رو، برای دستیابی به آن نیازی به ورود کلمه عبور نیست. با وجود این، انتظار می‌رود که کاربران در مقابل اعلان مربوط به کلمه عبور، آدرس پست الکترونیکی خود را وارد کنند.

سرویس FTP را روی شبکه‌های محلی نیز می‌توان راه‌اندازی کرده و مورد بهره‌برداری قرار داد. در قسمت "نحوه راه‌اندازی سرویس FTP با قابلیت دسترسی ناشناس" از این فصل با جزییات مربوط به این کار آشنا می‌شوید. پس از راه‌اندازی یک چنین سروری، با اجرای فرمان ftp localhost از کامپیوتر میزبان می‌توانید به آن متصل شوید.

```
[root@RH9Desk root]# ftp ftp.redhat.com
Trying 66.77.185.6...
Connected to ftp.redhat.com (66.77.185.6).
220 Red Hat FTP server ready. All transfers are logged.
Name (ftp.redhat.com:root): anonymous
331 Please specify the password.
Password:
230 Login successful. Have fun.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

شکل ۲-۲۷ جزییات روند اتصال به یک سرور FTP

پس از برقراری ارتباط میان دو برنامه کلاینت و سرور FTP می‌توانید در مقابل اعلان ftp> فرامین موردنظر خود را وارد کنید، برای نمونه برخی از فرامینی را که در قسمت قبل به شرح آن‌ها پرداختیم در مقابل اعلان مزبور وارد کرده و نتایج حاصل را مورد بررسی قرار دهید. با وجود این، دقت کنید که برخی از فرامین، عملکرد مورد انتظار را به دنبال ندارند. برای مثال، از آن‌جا که به واسطه دسترسی ناشناس نمی‌توان فایل‌های موردنظر را روی کامپیوتر میزبان سرورFTP شرکت Red Hat کپی کرد، اجرای فرمان put نتیجه مورد انتظار را به دست نمی‌دهد.

به‌طور پیش‌فرض، دسترسی به هیچ یک از سرورهای FTP مستقر در شبکه برای کاربر اصلی یا اصطلاحاً root امکان‌پذیر نیست، به طوری که حتی با وجود در اختیار داشتن کلمه عبور کاربر اصلی نیز نمی‌توان تحت این عنوان سرور FTP را مورد دستیابی قرار داد.

به عنوان مثال، فهرست جاری را به فهرست حاوی بسته‌های نرم‌افزاری Rawhide مربوط به پردازنده‌های *i386* تغییر دهید. تا زمان انتشار کتاب حاضر، این بسته‌های نرم‌افزاری در قالب فهرست /pub/redhat/linux/rawhide/i386/RedHat/RPMS سازمان‌دهی شده‌اند. با دستیابی به این فهرست بسته‌های نرم‌افزاری بسیار متنوعی را در اختیار خواهید داشت.

با وجودی که شرکت Red Hat بسته‌های نرم‌افزاری RPM را برای سایر پردازنده‌ها نیز بازنویسی کرده است، در حال حاضر، بسته‌های نرم‌افزاری مربوط به پردازنده‌های *i386* متداول‌تر از بقیه هستند. با وجودی که بسته‌های نرم‌افزاری مزبور برای سایر پردازنده‌های ساخت شرکت Intel بهینه‌سازی نشده‌اند، می‌توان آن‌ها را روی چنین کامپیوترهایی نیز نصب کرده و مورد استفاده قرار داد. در فصل دهم این موضوع به طور مفصل مورد بررسی قرار گرفته است.

فهرست Rawhide از سایت FTP شرکت Red Hat حاوی جدیدترین بسته‌های نرم‌افزاری است. اگر به استفاده از برنامه up2date علاقه ندارید، می‌توانید بسته‌های نرم‌افزاری نصب شده روی کامپیوتر را به روش دیگری ارتقا دهید. (جهت اطلاع بیشتر درباره برنامه up2date به فصل دهم مراجعه کنید.) برای این منظور، باید بسته‌های نرم‌افزاری موردنظر را از فهرست Rawhide روی کامپیوتر خود کپی کنید. شکل ۳-۲۷ روند انجام این کار را با استفاده از فرامین FTP نشان می‌دهد. با دراختیار داشتن بسته‌های نرم‌افزاری، اکنون می‌توانید برای نصب یا ارتقای آن‌ها اقدام کنید.

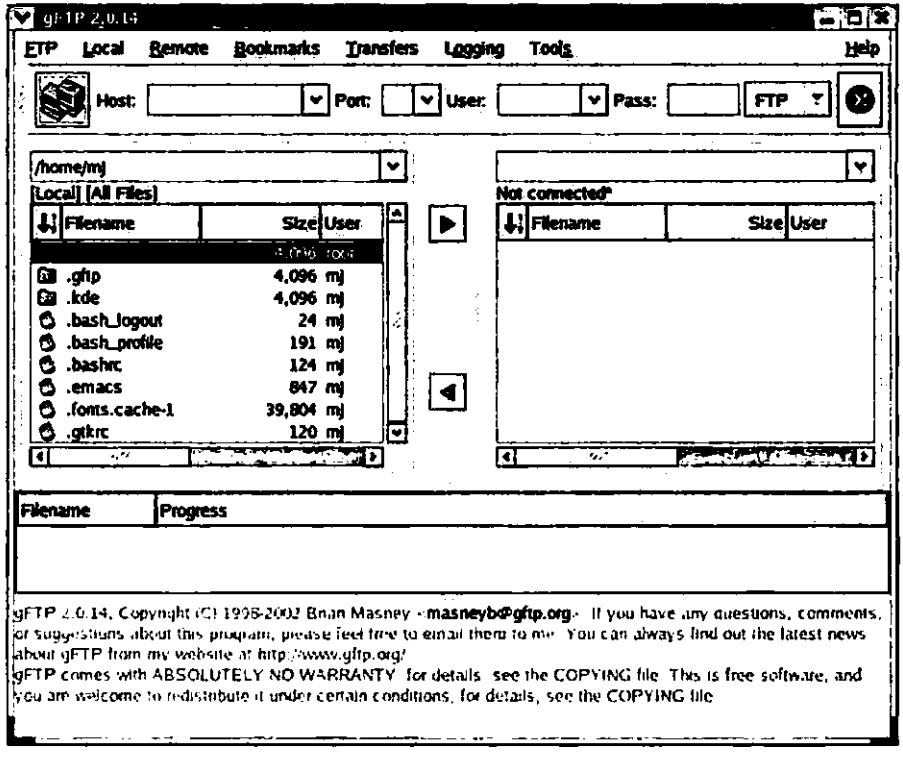
```
ftp> cd RPMS
250 CWD command successful.
ftp> ls z*
227 Entering Passive Mode (10,252,113,155,11,207).
125 Data connection already open; Transfer starting.
-rwxrwxrwx   1 owner    group         1011615 Feb 25 13:42 zebra-0.93b-1.i386.rp
m
-rwxrwxrwx   1 owner    group          113724 Feb 24  0:40 zip-2.3-16.i386.rpm
-rwxrwxrwx   1 owner    group           15425 Feb 24  0:40 zisofs-tools-1.0.4-2.
i386.rpm
-rwxrwxrwx   1 owner    group           33793 Feb 24 13:47 zlib-1.1.4-8.i386.rpm
-rwxrwxrwx   1 owner    group           70750 Feb 24 13:47 zlib-devel-1.1.4-8.i3
86.rpm
-rwxrwxrwx   1 owner    group         1407003 Feb 24  0:41 zsh-4.0.6-5.i386.rpm
226 Transfer complete.
ftp> mget zip*
mget zip-2.3-16.i386.rpm? y
227 Entering Passive Mode (10,252,113,155,11,209).
125 Data connection already open; Transfer starting.
WARNING! 385 bare linefeeds received in ASCII mode
File may not have transferred correctly.
226 Transfer complete.
113724 bytes received in 2.02 secs (55 Kbytes/sec)
ftp> bye
221
[root@RH9Desk root]#
```

شکل ۳-۲۷ انتقال بسته‌های نرم‌افزاری موردنظر با استفاده از فرامین FTP

چنان‌چه این روش را به هر دلیل مناسب تشخیص نمی‌دهید، به کمک فرمان rpm می‌توانید جدیدترین نسخه از بسته نرم‌افزاری موردنظر را مستقیماً روی کامپیوتر خود نصب کنید. (برای اطلاع بیشتر درباره این فرمان به فصل دهم مراجعه کنید.)

برنامه‌های کلاینت FTP با رابط گرافیکی

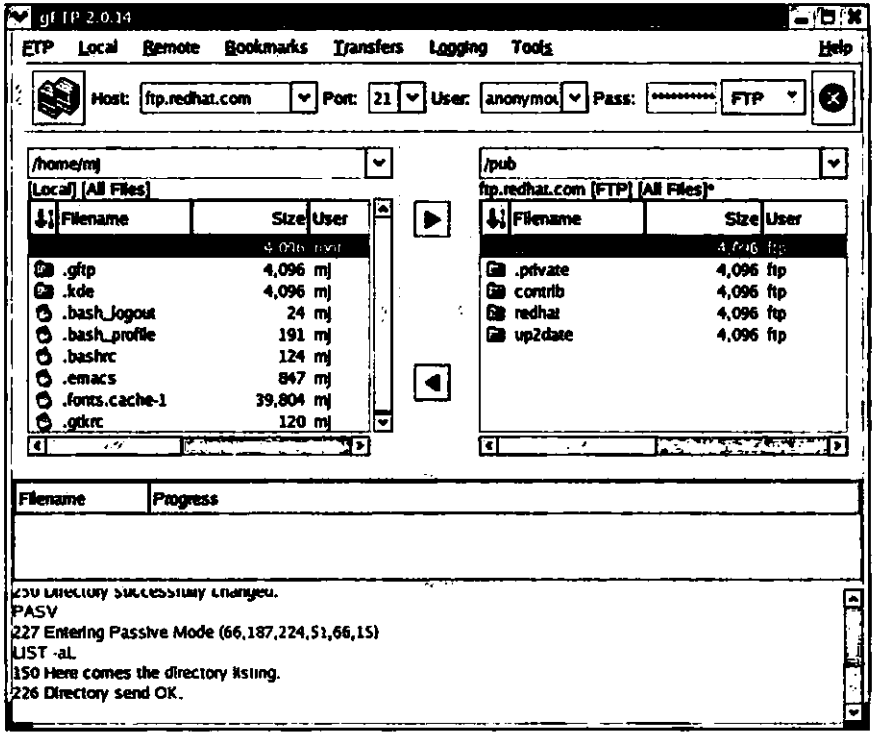
نسخه‌هایی از برنامه‌های کلاینت FTP با رابط گرافیکی نیز موجود است. در این قسمت به بررسی برنامه gFTP که یکی از متداول‌ترین برنامه‌های کلاینت FTP با رابط گرافیکی است، می‌پردازیم. برای دستیابی به این برنامه کافی است فرمان gftp را در سطر فرمان محیط گرافیکی موردنظر خود (همچون GNOME یا KDE) وارد کنید. شکل ۴-۲۷ پنجره اصلی برنامه gFTP را نشان می‌دهد.



شکل ۴-۲۷ پنجره اصلی برنامه gFTP

چنان‌چه فرمان gftp را در یک کنسول مجازی اجرا کنید، برنامه gFTP در حالت متنی باز شده و امکانات لازم به منظور استفاده از فرامین FTP را در اختیار قرار خواهد داد.

کار با برنامه gFTP بسیار ساده است. در منوی Bookmarks از این برنامه امکان دستیابی به چندین سایت FTP متداول از پیش فراهم شده است. برای مثال، جهت دستیابی به فهرست Rawhide از سایت FTP شرکت Red Hat، گزینه RH Rawhide را از منوی RedHat Sites واقع در منوی Bookmarks انتخاب کنید. این شیوه روش بسیار ساده‌ای برای دستیابی به سایت‌های FTP است. شکل ۵-۲۷ نتیجه انتخاب گزینه RH Main از منوی RedHat Sites واقع در منوی Bookmarks را نشان می‌دهد.



شکل ۵-۲۷ دستیابی به فهرست اصلی سایت FTP شرکت Red Hat با استفاده از امکانات برنامه gFTP

دو شکل ۴-۲۷ و ۵-۲۷ باهم مقایسه کنید. به محض انتخاب گزینه موردنظر از فهرست Bookmark مقادیری در فیلدهای متنی مختلف درج خواهد شد. شرح مختصری از این فیلدها در جدول ۲-۲۷ آمده است.

تغییر فهرست جاری به فهرست موردنظر از کامپیوتر میزبان سرور FTP نیز به سادگی امکان‌پذیر است. برای این منظور، کافی است روی عنوان فهرست موردنظر خود دابل کلیک کنید. علاوه بر این، با دابل کلیک روی علامت دو نقطه (..) می‌توانید فهرست میزبان فهرست جاری را مورد دستیابی قرار دهید.

پس از تعیین فایل یا فهرستی که مایلید نسخه‌ای از آن‌را به کامپیوتر خود انتقال دهید، روی دکمه‌ای با علامت پیکان کلیک کنید.

جدول ۲-۲۷ شرح فیلدهای متنی موجود در برنامه gFTP

فیلد متنی	توضیح
Host	این فیلد متنی بیانگر نام کامل حوزه‌ای است که کامپیوتر میزبان سرور FTP روی آن مستقر شده است.
Port	این فیلد متنی بیانگر پورت TCP/IP مورد استفاده جهت برقراری ارتباط برنامه gFTP با سرور FTP است. (پورت شماره ۲۱ به طور پیش‌فرض جهت ارتباط میان برنامه‌های کلاینت و سرور FTP در نظر گرفته شده است.)
User	این فیلد متنی بیانگر شناسه کاربری است که برای برقراری ارتباط میان برنامه gFTP با سرور FTP موردنظر اقدام کرده است. هنگام دسترسی ناشناس به سرور FTP، در این فیلد متنی مقدار anonymous درج می‌شود.
Pass	این فیلد متنی بیانگر کلمه عبور کاربری است که برای برقراری ارتباط میان برنامه gFTP با سرور FTP اقدام کرده است. هنگام دسترسی ناشناس به سرور FTP، انتظار می‌رود که کاربر آدرس الکترونیکی خود را در این فیلد متنی درج کند.

قاب پایین پنجره برنامه gFTP فرامین و پیغام‌های مفیدی را درارتباط با عملیات جاری (از جمله تعویض فهرست جاری به فهرست مورد نظر، انتقال فایل یا فهرست و مواردی از این قبیل) نشان می‌دهد.

پیکربندی سرور FTP با ضریب ایمنی بالا

چنان‌چه سرور FTP به درستی پیکربندی نشود، ممکن است امنیت کامپیوتر میزبان با مخاطره مواجه شود. متأسفانه، تأمین امنیت سرور FTP به شیوه رمزگذاری پیغام‌های ارسالی از سرور به برنامه کلاینت ممکن است موجب کاهش کارایی آن شود. (برای اطلاع بیشتر درباره این موضوع به فصل بیست و سوم مراجعه کنید.) از طرف دیگر، استفاده از مجموعه فرامین غیراستاندارد sftp نیز ممکن است مشکلاتی را به همراه داشته باشد.

یکی از راه‌حل‌های موجود در این زمینه استفاده از برنامه سرور Very Secure FTP یا به اختصار vsFTP است. در همین راستا، شرکت Red Hat نیز این برنامه را به عنوان برنامه سرور FTP پیش‌فرض

در نظر گرفته و تنها همین یک برنامه سرور FTP را در قالب سیستم‌عامل Red Hat Linux 9 منتشر کرده است. در واقع بررسی برنامه WU-FTP در این فصل تنها از آن جهت انجام می‌شود که برنامه مزبور در نسخه‌های قبلی سیستم‌عامل Red Hat Linux به عنوان برنامه سرور FTP مطرح بوده و کاربران بسیاری کار با آن‌را تجربه کرده‌اند.

برنامه vsFTP بدون نیاز به رمزگذاری پیغام‌های ارسالی از سرور به برنامه کلاینت بر بسیاری از مشکلات امنیتی برنامه WU-FTP چیره شده است. امروزه این برنامه به عنوان یک برنامه سرور FTP استاندارد در بسیاری سایت‌ها، از جمله ftp.redhat.com مورد استفاده قرار می‌گیرد. این برنامه را می‌توان هم به منظور دسترسی کاربران ناشناس هم به منظور دسترسی کاربران واقعی پیکربندی کرد. طبق اظهاراتی که در صفحه آغازین وب سایت برنامه vsFTP به آدرس http://vsftpd.beasts.org آمده، عملکرد این برنامه سریع‌تر از برنامه WU-FTP است.

البته برنامه vsFTP شباهت‌هایی نیز با برنامه WU-FTP دارد. در قسمت‌های بعد که به بررسی برنامه vsFTP اختصاص دارد، تا حد امکان به فایل‌های پیکربندی برنامه WU-FTP نیز اشاره شده است.

ویژگی‌های امنیتی برنامه vsFTP

فرامین برنامه vsFTP به نحوی پیکربندی شده‌اند که کمترین مجوزهای دسترسی را در اختیار کاربران قرار دهند. همین موضوع موجب شده تا خطر سوء استفاده از فرامین مزبور جهت دسترسی غیرمجاز به کامپیوتر میزبان کاهش پیدا کند.

فایل‌های پیکربندی

فایل‌های پیکربندی برنامه vsFTP در فهرست etc/ واقع شده‌اند. در این میان، دو فایل پیکربندی vsftpd.ftpusers و vsftpd.user_list به منظور جلوگیری از دسترسی غیرمجاز پیش‌بینی شده‌اند. ساختار این فایل‌ها بسیار ساده بوده و شامل لیستی از شناسه کاربران است که امکان دسترسی مجاز برای آن‌ها فراهم شده است. فایل پیکربندی اصلی با عنوان /etc/vsftpd/vsftpd.conf شامل مجموعه‌ای از پارامترهاست. در ادامه به بررسی خط به خط این فایل پیکربندی خواهیم پرداخت. برای اطلاع بیشتر درباره ساختار فایل مزبور فرمان man vsftpd.conf را اجرا کنید. (برخی توضیحات صرفاً به منظور راهنمایی بیشتر درج شده‌اند.)

```
# Example config file /etc/vsftpd.conf
#
# The default compiled in settings are very paranoid. This
```

```
# sample file loosens things up a bit, to make the ftp daemon
# more usable.
#
# Allow anonymous FTP?
anonymous_enable=YES
```

خطوطی که با علامت # آغاز شده‌اند شامل توضیحات هستند. دقت کنید که نخستین خط حاوی توضیحات موقعیت واقعی فایل پیکربندی vsftpd.conf را به درستی اعلام نمی‌کند. (فایل پیکربندی مذکور در فهرست /etc/vsftpd/vsftpd.conf واقع شده است.) مقداردهی پارامتر anonymous_enable به صورت فوق امکان دسترسی ناشناس به سرور FTP را در اختیار کاربران قرار می‌دهد، به طوری که کاربران با شناسه anonymous یا ftp می‌توانند از امکانات سرویس FTP استفاده کنند.

```
# Uncomment this to allow local users to log in.
local_enable=YES
```

مقداردهی پارامتر local_enable به صورت فوق امکان دسترسی به سرور FTP را در اختیار کاربران محلی قرار می‌دهد. به بیان دیگر، کاربران محلی کامپیوتر میزبان سرور FTP نیز می‌توانند از امکانات سرویس FTP استفاده کنند.

```
# Uncomment this to enable any form of FTP write command.
write_enable=YES
```

مقداردهی پارامتر write_enable به صورت فوق امکان دسترسی به تمام فهرست‌های کامپیوتر میزبان سرور FTP، از جمله فهرست ریشه (با نماد /) را در اختیار کاربران قرار می‌دهد. در اغلب موارد بهتر است با مقداردهی write_enable=NO امکان دسترسی کاربران به سیستم فایل کامپیوتر میزبان را محدود کنید. علاوه بر این، با مقداردهی پارامتر nopriv_user می‌توانید کاربری با حداقل مجوزهای دسترسی را تعریف کنید. (برای اطلاع بیشتر به توضیحات مربوط به این پارامتر مراجعه کنید.)

به منظور کاهش مشکلات احتمالی، با مقداردهی chroot_local_user=YES می‌توانید از دسترسی کاربران به فهرست ریشه کامپیوتر میزبان سرور FTP جلوگیری به عمل آورید. با وجود این، کاربرانی که از امکان بارگذاری فایل‌ها در فهرست خانگی خود برخوردار هستند، با ارسال فایل‌های اجرایی می‌توانند امنیت کامپیوتر میزبان را تهدید کنند.

تنظیمات پیش‌فرض فایل پیکربندی /etc/vsftpd/vsftpd.conf به نحوی است که کاربران واقعی در صورت تمایل می‌توانند فایل‌های موجود در فهرست خانگی خود را حذف کنند. بدیهی است کاربران ناشناس از این امکان برخوردار نیستند.

```
# Default umask for local users is 077. You may wish to
# change this to 022, if your users expect that (022 is used
```

```
local_umask=022
```

بدون مقداردهی فوق، مجوز خواندن و نوشتن فایل‌های بارگذاری شده روی کامپیوتر میزبان تنها در اختیار مالک آن فایل‌ها خواهد بود. با وجود مقداردهی local_umask=022 تمام کاربران دست کم از مجوز خواندن فایل‌های بارگذاری شده روی کامپیوتر میزبان برخوردار می‌شوند.

```
# Uncomment this to allow the anonymous FTP user to upload
# files. This only has an effect if the above global write
# enable is activated. Also, you will obviously need to
# create a directory writable by the FTP user.
#anon_upload_enable=YES
```

گاهی اوقات به دلایلی مایل هستیم امکان بارگذاری فایل‌ها را در اختیار کاربران ناشناس نیز قرار دهیم. هر چند که این اقدام خطر اشباع پارتیشن میزبان سیستم فایل var/ را به دنبال دارد، با سوار کردن سیستم فایل مذکور روی پارتیشنی دیگر می‌توان این خطر را نیز کاهش داد. (برای اطلاع بیشتر درباره چگونگی سوار کردن سیستم فایل‌ها به فصل هفتم مراجعه کنید.) چنان‌که به زودی خواهید دید، برای آن‌که کاربران ناشناس بتوانند فایل‌های موردنظر خود را در فهرستی از کامپیوتر میزبان سرور FTP (هم‌چون var/ftp/pub/) بارگذاری کنند، لازم است مجوز لازم را در اختیار آن‌ها قرار دهید. البته تنظیمات پیش‌فرض فایل پیکربندی vsftpd.conf چنین مجوزی را در اختیار کاربران ناشناس قرار نمی‌دهد.

```
# Uncomment this if you want the anonymous FTP user to be
# able to create new directories.
#anon_mkdir_write_enable=YES
```

هم‌چنین در مواقعی مایل هستیم به واسطه مقداردهی anon_mkdir_write_enable=YES و اعطای مجوزهای لازم امکان ایجاد فهرست‌های جدید را در اختیار کاربران ناشناس قرار دهیم. (این مقداردهی به دلیل وجود علامت # در ابتدای خط مربوطه بی‌تأثیر شده است.) ضمناً برای آن‌که کاربران بتوانند فایل‌های موردنظر خود را در این فهرست کپی کنند، علاوه بر مقداردهی فوق باید مقداردهی anon_other_write_enable=YES را نیز انجام دهید.

```
# Activate directory messages - messages given to remote
# users when they go into a certain directory.
dirmessage_enable=YES
```

با مقداردهی فوق کاربران می‌توانند محتوای فایل‌های message. از فهرست‌های مختلف را مورد مشاهده قرار دهند. به محض تغییر موقعیت یک کاربر از فهرست جاری به فهرست میزبان یک فایل

message. محتوای آن فایل (یا در صورت مقداردهی message_file=*filename* محتوای فایلی از آن فهرست با عنوان *filename*) به نمایش درمی‌آید.

```
# Activate logging of uploads/downloads.
xferlog_enable=YES
```

با مقداردهی فوق اقدام کاربران برای بارگذاری فایل‌ها روی کامپیوتر میزبان سرور FTP در فایلی با عنوان /var/log/vsftpd.log به ثبت می‌رسد. در صورت تمایل، با مقداردهی xferlog_file=*filename* می‌توان فایل *filename*را برای این منظور در نظر گرفت.

```
# Make sure PORT transfer connections originate from
# port 20 (ftp-data).
connect_from_port_20=YES
```

مقداردهی فوق برای دسترسی برخی از برنامه‌های کلاینت به سرور FTP ضروری است. پورت شماره ۲۰ یکی از پورت‌های TCP/IP به ثبت رسیده در فایل /etc/services است.

```
# If you want, you can arrange for uploaded anonymous files
# to be owned by a different user. Note! Using "root" for
# uploaded files is not recommended!
#chown_uploads=YES
#chown_username=whoever
```

به واسطه دو مقداردهی فوق، کاربری که برای بارگذاری یک فایل اقدام می‌کند، ضرورتی ندارد که لزوماً مالک آن فایل باشد. (هر دو مقداردهی به دلیل وجود علامت # در ابتدای خطوط مربوطه بی‌تأثیر شده‌اند.) برخلاف تنظیمات پیش‌فرض فایل پیکربندی vsftpd.conf، این دو مقداردهی مالکیت تمام فایل‌های بارگذاری شده را به نام کاربری با شناسه mj ثبت خواهد کرد:

```
chown_uploads=YES
chown_username=mj
```

موقعیت فایل ثبت وقایع سرور FTP با مقداردهی متغیر xferlog_file مشخص می‌شود:

```
# You may override where the log file goes if you like. The
# default is shown below.
#xferlog_file=/var/log/vsftpd.log
```

به طور پیش فرض، وقایع مربوط به سرور vsFTP در فایل /var/log/vsftpd.log به ثبت می‌رسد. در صورت تمایل، با مقداردهی متغیر xferlog_file می‌توان فایل دیگری را برای این منظور در نظر گرفت.

```
# If you want, you can have your log file in standard ftpd
# xferlog format
xferlog_std_format=YES
```

با مقداردهی فوق وقایع مربوط‌به‌بارگذاری فایل‌ها روی کامپیوتر میزبان سرور FTP در قالب استانداردی که برای مدت‌ها در برنامه WU-FTP نیز متداول بود، به ثبت می‌رسد. البته قالب غیراستاندارد برنامه vsFTP از خوانایی بیشتری برخوردار است. برای تحقیق این موضوع کافی است پس از درج علامت # در ابتدای خط حاوی مقداردهی xfrelog_std_format=YES فایل پیکربندی vsftpd.conf را ذخیره کرده و فایل دلخواهی را روی کامپیوتر میزبان سرور FTP بارگذاری کنید. سپس فایل حاوی ثبت وقایع یعنی /var/log/vsftpd.log را باز کرده و مورد مطالعه قرار دهید.

```
# You may change the default value for timing out an idle
# session.
#idle_session_timeout=600
```

مقداردهی فوق موجب می‌شود تا در صورتی که کاربری پس از گذشت ۶۰۰ ثانیه (معادل ۱۰ دقیقه) از زمان اتصال به سرور vsFTP هیچ فعالیتی برای استفاده از سرور مزبور نشان ندهد، اتصال وی با سرور قطع شود. البته مدت زمان پیش‌فرض برای این منظور برابر با ۳۰۰ ثانیه (معادل ۵ دقیقه) است. اگر مایل به استفاده از این ویژگی هستید، توصیه می‌کنیم مدت زمان مزبور را برابر با ۱۰ دقیقه در نظر بگیرید.

```
# You may change the default value for timing out a data
# connection.
#data_connection_timeout=120
```

گاهی اوقات ضمن انتقال فایل‌ها از کامپیوتر کلاینت به سرور یا بالعکس خطایی رخ می‌دهد. این وضعیت موجب می‌شود تا کامپیوتر کلاینت مجدداً برای برقراری ارتباط با سرور تلاش کند. مقدار متغیر data_connection_timeout بیانگر مدت زمانی است که کامپیوتر کلاینت فرصت برقراری ارتباط مجدد با سرور را دارد. مدت زمان پیش‌فرض برای این منظور برابر با ۳۰۰ ثانیه (معادل ۵ دقیقه) است. پس از سپری شدن مدت زمان مزبور، چنان‌چه برنامه کلاینت در برقراری ارتباط با سرور موفق نباشد، دست از تلاش برمی‌دارد. تحت این شرایط، کاربر کامپیوتر کلاینت می‌تواند با صدور فرامین مربوطه برای برقراری ارتباط مجدد با سرور FTP اقدام کند. اگر مایل به استفاده از این ویژگی هستید، توصیه می‌کنیم مدت زمان مزبور را برابر با ۲ دقیقه در نظر بگیرید.

```
# It is recommended that you define on your system a unique
# user which the ftp server can use as a totally isolated and
# unprivileged user.
#nopriv_user=ftpsecure
```

متغیر nopriv_user امکان تعیین شناسه کاربر به خصوصی را در اختیار می‌گذارد که از هیچ امتیازی برخوردار نیست. بدیهی است مشخصات این کاربر باید مشابه کاربران عادی در فایل /etc/passwd موجود باشد.

کاربری با ویژگی فوق معمولاً با عنوان "میهمان" (اصطلاحاً guest) از سرویس FTP استفاده می‌کند. شناسه چنین کاربری در اختیار تمام کاربران متصل به سرور FTP قرار می‌گیرد. در صورت تمایل می‌توانید با تغییر رکورد مربوط به این کاربر در فایل /etc/passwd از دسترسی مستقیم کاربران میهمان به سرور FTP جلوگیری به عمل آورید. برای این منظور، کافی است پوسته /sbin/nologin را به عنوان پوسته پیش‌فرض مورد استفاده این کاربر مشخص کنید:

```
ftpsecure:x:601:601::/home/ftpsecure:/sbin/nologin
```

برخی از برنامه‌های کلاینت FTP به محض انصراف کاربر از انتقال فایل‌ها واکنش نامطلوبی از خود نشان می‌دهند. با مقداردهی متغیر async_abor_enable به این صورت می‌توانید امکان انصراف از انتقال فایل‌ها را بدون چنین واکنش‌هایی فراهم کنید:

```
# Enable this and the server will recognize asynchronous
# ABOR requests. Not recommended for security (the code is
# non-trivial). Not enabling it, however, may confuse older
# FTP clients.
#async_abor_enable=YES
```

مقداردهی فوق در مورد کاربران عادی که از طریق سطر فرمان سیستم‌عامل خود با سرور FTP ارتباط برقرار می‌کنند، ضروری نیست.

```
# By default the server will pretend to allow ASCII mode but
# in fact ignore the request. Turn on the below options to
# have the server actually do ASCII mangling on files when in
# ASCII mode.
# Beware that turning on ascii_download_enable enables
# malicious remote parties to consume your I/O resources, by
# issuing the command "SIZE /big/file" in ASCII mode.
# These ASCII options are split into upload and download
# because you may wish to enable ASCII uploads (to prevent
# uploaded scripts etc. from breaking), without the DoS risk
# of SIZE and ASCII downloads. ASCII mangling should be on
# the client anyway..
```

```
#ascii_upload_enable=YES
#ascii_download_enable=YES
```

به واسطه دو مقداردهی ascii_upload_enable=YES و ascii_download_enable=YES امکان انتقال فایل‌ها در حالت ASCII (اصطلاحاً ascii mode) فراهم می‌شود. البته این اقدام حتی هنگام انتقال فایل‌های متنی به ندرت ضرورت دارد، مگر آن‌که این کار به منظور اطمینان از حفظ قالب‌بندی فایل‌ها انجام شود.

```
# You may fully customise the login banner string:
#ftpd_banner=Welcome to blah FTP service.
```

مقدار متغیر ftpd_banner بیانگر پیغامی است که درست پیش از برقراری ارتباط برنامه کلاینت با سرور FTP موردنظر به نمایش درمی‌آید. برای مثال، در صورتی که تنها دسترسی ناشناس به سرور FTP مجاز باشد، این پیغام مناسب خواهد بود:

```
# ftp_banner=Welcome. Type ftp at the prompt for an anonymous login.
```

گاهی اوقات برخی از کاربران خرابکار تلاش می‌کنند تا با اجرای فرمان ping به شیوه‌ای که در فصل بیست و دوم شرح داده شد، ماشین میزبان سرور FTP را از کار بیندازند.

```
# You may specify a file of disallowed anonymous e-mail
# addresses. Apparently useful for combatting certain DoS
# attacks.
#deny_email_enable=YES
# (default follows)
#banned_email_file=/etc/vsftpd.banned_emails
```

به واسطه مقداردهی deny_email_enable=YES می‌توان لیست کلمات عبور کاربرانی را که باید دسترسی آن‌ها به سرور FTP محدود شود، در قالب فایل /etc/vsftpd.banned_emails مشخص کرد. مقدار متغیر banned_email_file بیانگر فایلی است که برای این منظور در نظر گرفته شده است. به این ترتیب، اقدام کاربرانی که با استفاده از ابزارهای مختلف سعی در مختل کردن سرویس FTP دارند، با ناکامی مواجه خواهد شد.

```
# You may specify an explicit list of local users to chroot()
# to their home directory. If chroot_local_user is YES, then
# this list becomes a list of users to NOT chroot().
#chroot_list_enable=YES
# (default follows)
#chroot_list_file=/etc/vsftpd.chroot_list
```

با مقداردهی chroot_list_enable=YES می‌توان ترتیبی داد تا گروه مشخصی از کاربران بتوانند فهرست خانگی خود را تحت عنوان فهرست ریشه (با نماد /) مورد دستیابی قرار دهند. به طور پیش فرض، لیست مشخصات این کاربران در فایل /etc/vsftpd.chroot_list درج می‌شود. در صورت تمایل، با مقداردهی مجدد متغیر chroot_list_file می‌توان فایل دیگری را برای این منظور در نظر گرفت. با مقداردهی chroot_local_user=YES تأثیر فوق برای این دسته از کاربران معکوس خواهد شد.

```
# You may activate the "-R" option to the builtin ls. This is
# disabled by default to avoid remote users being able to
# cause excessive I/O on large sites. However, some broken
# FTP clients such as "ncftp" and "mirror" assume the
# presence of the "-R" option, so there is a strong case for
# enabling it.
#ls_recurse_enable=YES
```

به واسطه این مقداردهی، امکان اجرای فرمان ls -R در تمام سطوح در اختیار برنامه‌های کلاینت قرار می‌گیرد. به این ترتیب، کاربران می‌توانند محتوای زیرفهرست‌ها را مورد دستیابی قرار دهند. البته این قابلیت به طور پیش‌فرض غیرفعال است، چرا که کاربران با اجرای مکرر فرمان ls -R می‌توانند بار قابل توجهی را به کامپیوتر میزبان سرور FTP تحمیل کنند.

```
pam_service_name=vsftpd
```

مقدار متغیر pam_service_name ماجول PAM مربوط به برنامه vsFTP را مشخص می‌کند. (برای اطلاع بیشتر درباره ماجول‌های PAM یا Pluggable Authentication Modules به فصل بیست و دوم مراجعه کنید.)

```
userlist_enable=YES
```

مقداردهی فوق موجب می‌شود تا برنامه vsFTP شناسه‌های کاربری مندرج در فایل /etc/vsftpd.user_list را به منظور تشخیص کاربرانی که دسترسی آن‌ها به سرویس FTP محدود شده است، مورد توجه قرار دهد.

```
# enable for standalone mode
listen=YES
```

این مقداردهی موجب می‌شود تا برنامه vsFTP در قالب یک سرویس مستقل اجرا شود. (برنامه راه‌انداز این سرویس با عنوان vsftpd در فهرست /etc/rc.d/init.d مستقر است.) در غیر این صورت، برنامه نامبرده به عنوان یکی از سرویس‌های xinetd اجرا خواهد شد. (برای توضیح بیشتر به فصل بیست و سوم مراجعه کنید.)

پیکربندی سرور FTP به منظور دسترسی ناشناس

با وجودی که پیکربندی سرور FTP جهت دسترسی ناشناس فرآیند کار چندان دشواری نیست، تأمین امنیت چنین سروری مستلزم رعایت جزییات ظریفی است. اگر تمام نکات ایمنی رعایت شود، کاربران تنها می‌توانند فهرست var/ftp/ را مورد دستیابی قرار دهند. به ویژه، دسترسی به فهرست ریشه (با نماد /) به هیچ وجه امکان‌پذیر نخواهد بود. پیکربندی پیش‌فرض سرویس FTP در سیستم‌عامل Red Hat Linux بر اساس برنامه vsFTP انجام شده است.

در این قسمت جزییات پیکربندی سرور FTP را به منظور دسترسی ناشناس (اصطلاحاً anonymous) مورد بررسی قرار می‌دهیم. لازم به ذکر است که هر دو برنامه vsFTP و WU-FTP از قابلیت چنین پیکربندی برخوردار هستند. با تنظیماتی که در این قسمت به بررسی آن‌ها خواهیم پرداخت، می‌توان سرور FTP را به نحو دلخواه جهت دسترسی ناشناس پیکربندی کرد.

پیکربندی برنامه vsFTP

پس از نصب بسته‌های نرم‌افزاری برنامه مورد نظر، لازم است سرویس مربوطه را راه‌اندازی کنید. با فرض این‌که برنامه vsFTP را نصب کرده‌اید، فرمان service vsftpd start را به منظور راه‌اندازی سرویس FTP اجرا کنید. با استفاده از فرمان chkconfig می‌توانید مطمئن شوید که سرویس مزبور ضمن راه‌اندازی‌های بعدی سیستم‌عامل Linux به طور خودکار راه‌اندازی خواهد شد. (برای اطلاع بیشتر در این زمینه به فصل سیزدهم مراجعه کنید.)

چنان‌که در قسمت‌های قبل اشاره شد، تنظیمات پیش‌فرض فایل پیکربندی برنامه vsFTP یعنی /etc/vsftpd/vsftpd.conf به نحوی است که امکان دسترسی ناشناس به سرویس FTP را در اختیار کاربران قرار می‌دهد. متغیر کلیدی موردنیاز برای این منظور anonymous_enable است. در قسمت بعد به بررسی نحوه پیکربندی برنامه WU-FTP می‌پردازیم.

پیکربندی برنامه WU-FTP

اگر از برنامه WU-FTP به عنوان سرور FTP استفاده می‌کنید، باید تنظیمات موردنیاز را از طریق فایل‌های پیکربندی متعددی با عنوان عمومی /etc/ftp* انجام دهید. در قسمت بعد تحت عنوان "پیکربندی برنامه WU-FTP با کاربران واقعی" جزییات پیکربندی این برنامه را مورد بررسی قرار خواهیم داد.

برنامه WU-FTP به همراه نسخه‌های اخیر سیستم‌عامل Red Hat Linux توزیع نمی‌شود. در صورت تمایل به استفاده از این برنامه می‌توانید به سایت ftp.wu-ftpd.org یا کتابخانه SpeakEasy RPM به آدرس http://www.rpmfind.net مراجعه کنید.

فهرست‌های پیش‌بینی شده برای دسترسی ناشناس

به سادگی می‌توان سرویس FTP با دسترسی ناشناس را از طریق برنامه WU-FTP در اختیار کاربران قرار داد. با نصب بسته نرم‌افزاری anonftp-* فهرست‌های متعددی حاوی فایل‌ها و فرامین موردنیاز کاربران در فهرست var/ftp/ مستقر خواهد شد. شرح مختصری از محتوای این فهرست‌ها در جدول ۳-۲۷ آمده است.

جدول ۳-۲۷ شرح محتوای زیرفهرست‌های var/ftp/

عنوان زیرفهرست	توضیح
/var/ftp/bin	این فهرست حاوی تعداد محدودی فرامین پوسته است.
/var/ftp/etc	این فهرست حاوی فایل‌های پیکربندی (به طور پیش‌فرض، نسخه‌های جزیی از دو فایل etc/passwd/ و etc/group/) است.
/var/ftp/lib	این فهرست حاوی فایل‌های کتابخانه‌ای موردنیاز برای اجرای فرامین است.
/var/ftp/pub	این فهرست حاوی فایل‌های کاربران است. در صورت تمایل می‌توان مجوز بارگذاری فایل‌ها در این فهرست را به کاربران اعطا کرد.

توجه کنید که برنامه WU-FTP به عنوان یکی از سرویس‌های xinetd به اجرا درمی‌آید. (برای اطلاع بیشتر در این زمینه به فصل بیست و سوم مراجعه کنید.) از این‌رو، باید مطمئن شوید که سرویس مزبور به واسطه تنظیمات فایل پیکربندی etc/xinetd.d/wu-ftpd/ غیرفعال نشده و دستیابی به آن از طریق تنظیمات فایل پیکربندی etc/hosts.deny/ یا قوانین مکانیزم بازدارنده دیوار آتش (به ویژه برنامه iptables) محدود نشده است.

محدود کردن دسترسی به سرور FTP

به سادگی می‌توان ترتیبی داد که تنها کاربران ناشناس امکان دسترسی به سرور FTP را داشته باشند. برای این منظور، ابتدا فایل پیکربندی etc/ftpaccess/ را باز کنید. به طور پیش فرض، بخشی از تنظیمات فایل مزبور باید به این صورت باشد:

```
class   all   real,guest,anonymous   *
```

مطابق با این تنظیمات، امکان دسترسی به سرویس FTP برای کاربران واقعی، میهمان و ناشناس فراهم شده است. برای محدود کردن دسترسی فوق به کاربران ناشناسی که از شبکه 192.168.0.0/24 برای استفاده از سرویس FTP اقدام می‌کنند، کافی است تنظیمات فوق را به این صورت تغییر دهید:

```
class   all   anonymous   192.168.0.0/24
```

امنیت سرور FTP با قابلیت دسترسی ناشناس

چنان‌چه برنامه WU-FTP را به عنوان سرور FTP با قابلیت دسترسی ناشناس پیکربندی کرده‌اید، باید ملاحظاتی را که به طور پیش‌فرض برای تأمین امنیت آن پیش‌بینی شده‌اند، بشناسید. در قسمت‌های بعد به بررسی این موضوع می‌پردازیم.

محدود کردن دسترسی

به طور پیش فرض، تمام دسترسی‌های ناشناس به فهرست /var/ftp ختم می‌شود. با فعال کردن این خط از فایل /etc/ftpaccess می‌توان محدودیت فوق را در مورد برخی از کاربران بی‌تأثیر کرد:

```
# realuser user1, user2
```

چنان‌چه علامت # از ابتدای خط مزبور حذف شود، کاربرانی که شناسه آن‌ها در اینجا با متغیرهای *user1* و *user2* مشخص شده از حقوق دسترسی کاربران واقعی برخوردار می‌شوند به طوری که پس از برقراری ارتباط با سرور FTP امکان دسترسی به فهرست خانگی در اختیار آن‌ها قرار می‌گیرد. ضمناً این گونه کاربران می‌توانند فهرست‌های سطوح بالاتر از جمله فهرست ریشه (با نماد /) را نیز مورد دستیابی قرار دهند.

اگر مایلید دسترسی تمام کاربران به فهرست /var/ftp ختم شود، از فعال کردن خط مذکور صرف نظر کنید.

قفس chroot

محافظت در برابر دسترسی کاربران به فهرست‌های موجود روی کامپیوتر میزبان سرور FTP با عنوان قفس chroot (اصطلاحاً chroot jail) شناخته شده است. بنا به تعریف، هیچ فهرستی بالاتر از فهرست ریشه (با نماد /) موجود نیست. فرمان chroot */abc/def* فهرست ریشه را به فهرست */abc/def* تغییر می‌دهد.

کاربران ناشناس پس از اتصال به سرور FTP، چنین می‌پندارند که فهرست /var/ftp از ماشین میزبان آن سرور همان فهرست ریشه است. بدیهی است که این حس به واسطه فرمان chroot /var/ftp ایجاد

می‌شود. چنان‌چه یک کاربر ناشناس با اجرای فرمانی چون cd /var یا cd /etc برای دسترسی به فهرست‌های مزبور اقدام کند، تلاش وی با شکست مواجه خواهد شد، چرا که فهرست‌های سطوح بالاتر به واسطه قفس chroot محافظت می‌شوند.

محدودیت در اجرای فرامین

علاوه بر موارد فوق می‌توان دسترسی به فرامین خطرناک را نیز محدود کرد. تنظیمات پیش‌فرض فایل پیکربندی /etc/ftpaccess امکان اجرای چهار فرمان خطرناک chmod، delete، overwrite و rename را از کاربران ناشناس سلب می‌کند. (بدیهی است در صورت نیاز می‌توان فرامین دیگری را نیز به این مجموعه اضافه کرد.) به بخش مربوطه از فایل پیکربندی /etc/ftpaccess توجه کنید:

```
chmod       no      guest,anonymous
delete      no      anonymous
overwrite   no      anonymous
rename      no      anonymous
```

پیکربندی سرور WU-FTP با کاربران واقعی کامپیوتر میزبان

مشابه قسمت قبل، مطالب مندرج در این قسمت راجع به برنامه WU-FTP است. چنان‌که قبلاً نیز اشاره شد، شرکت Red Hat بسته نرم‌افزاری حاوی این برنامه را به همراه نسخه‌های اخیر سیستم‌عامل خود توزیع نمی‌کند؛ بنابراین برای دستیابی به آن باید از طریق منابع دیگری اقدام کرد. در قسمت‌های قبل نحوه پیکربندی سرور FTP را به منظور دستیابی کاربران ناشناس مورد بررسی قرار دادیم. در این قسمت به بررسی فایل‌های پیکربندی برنامه WU-FTP و چگونگی اعمال تأثیر آن‌ها روی کاربران عادی سیستم خواهیم پرداخت.

فایل‌های پیکربندی برنامه WU-FTP

برنامه WU-FTP دارای فایل‌های پیکربندی متعددی است که همگی در فهرست /etc مستقر شده‌اند. عناوین این فایل‌ها عبارت از ftpaccess، ftpconversion، ftpgroups، ftphosts و ftpusers است.

در نسخه‌های اخیر برنامه WU-FTP فایل پیکربندی ftpusers به کلی منسوخ شده و فایل ftpgroups نیز به ندرت مورد استفاده قرار می‌گیرد. کلیه تنظیماتی که قبلاً از طریق این دو فایل انجام می‌شد، اکنون در قالب فایل ftpaccess قابل پیکربندی است. در این قسمت علاوه بر فایل پیکربندی ftpaccess به بررسی دو فایل پیکربندی ftphosts و ftpconversion نیز خواهیم پرداخت.

فایل پیکربندی /etc/ftpaccess

تا این‌جا به برخی از تنظیمات پیش‌فرض فایل پیکربندی /etc/ftpaccess اشاره کردیم. در این قسمت قصد داریم تا این فایل را خط به خط مورد بررسی قرار دهیم. برای شروع، به چند خط نخست از این فایل توجه کنید:

```
deny-uid %-99 %65534-
deny-gid %-99 %65534-
allow-uid ftp
allow-gid ftp
```

چنان‌که مشاهده می‌کنید، به استثنای شناسه کاربری ftp و شناسه گروه ftp تنظیمات فوق امکان دسترسی به شناسه کاربران و شناسه گروه‌هایی با شاخص کوچک‌تر از ۹۹ و بزرگ‌تر از ۶۵۵۳۴ را محدود کرده است. با توجه به محتوای فایل‌های /etc/passwd و /etc/group شناسه‌هایی که در محدوده مذکور واقع شده‌اند به مدیران سیستم تعلق دارند. با یک تغییر جزیی در تنظیمات فوق می‌توان امکان دسترسی به شناسه تمام کاربران و گروه‌ها را به استثنای شناسه کاربری ftp و شناسه گروه ftp محدود کرد:

```
deny-uid *
deny-gid *
allow-uid ftp
allow-gid ftp
```

پارامتر guestuser امکان ساخت قفس chroot را در اختیار قرار می‌دهد. به این ترتیب، دسترسی هر کابری به فهرست خانگی خود ختم شود: (برای مثال، دسترسی کاربری با شناسه mj به فهرست /home/mj ختم خواهد شد.)

```
guestuser *
```

درباره تأثیر پارامتر realuser در قسمت‌های قبل صحبت کردیم. جهت یادآوری، هیچ کاربری از امکان دسترسی به فهرست‌هایی که در سطوح بالاتر از فهرست خانگی خود قرار دارند، برخوردار نیست، مگر آن‌که شناسه وی به عنوان یکی از مقادیر پارامتر realuser مزبور در مقابل آن پارامتر درج شده و علامت # نیز از ابتدای خط حاوی این تنظیمات حذف شود:

```
# realuser user1,user2
```

فراموش نکنید که وجود علامت # در ابتدای خطی از یک فایل پیکربندی موجب بی‌تأثیر شدن آن خط می‌شود. با حذف این علامت، کاربرانی که شناسه آن‌ها در این‌جا با متغیرهای user1 و user2 نشان داده شده است، از حقوق دسترسی کامل به سیستم فایل کامپیوتر میزبان سرور FTP برخوردار خواهند

شد. این تأثیر را می‌توان با تنظیمات پارامتر guestuser محدود کرد. برای مثال، فرض کنید تنظیمات فوق به صورت * realuser باشد. به این ترتیب، تمام کاربران از حقوق دسترسی کامل به سیستم فایل کامپیوتر میزبان سرور FTP برخوردار خواهند شد. اکنون چنان‌چه مشخصات گروهی با شناسه ftpchroot در فایل /etc/group درج شده باشد، به این صورت می‌توان حقوق دسترسی کامل به سیستم فایل کامپیوتر میزبان سرور FTP را از کاربران عضو آن گروه سلب کرد: (البته به شرطی که علامت # از ابتدای خط حاوی این تنظیمات حذف شود.)

```
# gusetgroup ftpchroot
```

ساختار فایل‌های پیکربندی کاربران و گروه‌ها (به ترتیب /etc/passwd و /etc/group) در فصل نهم مورد بررسی قرار گرفته است.

چنان‌که قبلاً نیز اشاره شد، با استفاده از پارامتر class می‌توان امکان دسترسی به سرور FTP را برای کاربران به‌خصوصی مهیا کرد. برای مثال، با این تنظیمات امکان دسترسی به سرور FTP برای کاربران واقعی، میهمان و ناشناس فراهم می‌شود:

```
class    all    real,guest,anonymous    *
```

با فعال کردن این تنظیمات امکان دسترسی به سرور FTP تنها در اختیار آن دسته از کاربران واقعی قرار می‌گیرد که از شبکه‌ای با مشخصه 192.168.0.0/24 جهت برقراری ارتباط با سرور مزبور اقدام کرده‌اند:

```
# class    all    real    192.168.0.0/24
```

یکی از خطرات بالقوه تنظیمات فوق این است که کلمات عبور کاربران به‌صورت رمزگذاری نشده (یعنی در قالب متنی ساده) از طریق شبکه محلی برای کامپیوتر میزبان سرور FTP ارسال می‌شود.

چنان‌چه پارامتر guestuser به صورت * guestuser تنظیم شده باشد، در خط فوق می‌توان مقدار real را با guest جایگزین کرد:

```
class    all    guset    192.168.0.0/24
```

اگر وظیفه مدیریت سیستم را به عهده دارید، آدرس پست الکترونیکی خود را به عنوان مقدار پارامتر email وارد کنید:

```
email root@localhost
```

پارامتر loginfails امکان محدود کردن تعداد دفعاتی را که برای برقراری ارتباط با سرور FTP اقدام می‌شود، در اختیار می‌گذارد. برای مثال، به واسطه این تنظیمات سرور FTP پس از پنج بار تلاش ناموفق برنامه کلاینت ارتباط را قطع می‌کند:

```
loginfails 5
```

فایل‌های *README در سیستم‌عامل‌ها Linux و UNIX جهت مستندسازی دستورالعمل‌ها یا در اختیار گذاشتن اطلاعات بیشتر راجع به بسته‌های نرم‌افزاری مستقر در یک فهرست به‌خصوص قالب‌بندی می‌شوند. به واسطه این تنظیمات، هر بار که کاربر پس از برقراری ارتباط موفقیت‌آمیز با سرور FTP برای دسترسی به فهرستی حاوی یک فایل README اقدام می‌کند، پیغام Please read the file README به نمایش درمی‌آید:

```
readme      README*     login
readme      README*     cwd=*
```

به عنوان مدیر سیستم می‌توانید ترتیبی دهید تا در این گونه مواقع سرور FTP پیغام متفاوتی را نمایش دهد. برای مثال، به این تنظیمات توجه کنید:

```
message     /welcome.msg     login
message     .message         cwd=*
```

خط نخست از تنظیمات فوق باعث می‌شود تا پیغام مندرج در فایل welcome.msg/ پس از برقراری ارتباط با سرور FTP به نمایش درآید. خط دوم نیز باعث می‌شود تا به محض تغییر موقعیت کاربر از فهرست جاری به فهرست دیگر، محتوای پیغام موجود در فایل message. از آن فهرست به نمایش درآید. (تغییر موقعیت از یک فهرست به فهرست دیگر با استفاده از فرمان cd انجام می‌شود.)

تأثیر این تنظیمات در شکل ۶-۲۷ نشان داده شده است. چنان‌که مشاهده می‌کنید، به محض برقراری ارتباط با سرور FTP پیغام مندرج در فایل README از فهرست var/ftp/ به نمایش درآمده است. هم‌چنین پس از تغییر فهرست جاری به فهرست etc/ (که با استفاده از فرمان cd انجام شده) پیغام مندرج در فایل message. از آن فهرست به نمایش درآمده است.

اغلب نگهداری بسته‌های نرم‌افزاری در قالب فشرده روی سرور FTP مفید است. این تنظیمات، به واسطه فرامین مذکور در فهرست etc/ftpconversions/ امکان بازکردن بسته‌های نرم‌افزاری فشرده را در اختیار کاربرانی که به آن‌ها دسترسی دارند، می‌دهد: (برای اطلاع بیشتر به قسمت "فایل پیکربندی etc/ftpconversions/" از همین فصل مراجعه کنید.)

```
compress    yes     all
tar         yes     all
```

چنان‌چه پارامتر guestuser را به صورت * guestuser تنظیم کرده باشید، با اندکی تغییرات در فایل پیکربندی etc/ftpaccess/ (که در ادامه با حروف bold نشان داده شده است) می‌توان از اجرای فرامین موردنظر توسط کاربران جلوگیری به عمل آورد. برای مثال، با وجود این تنظیمات هیچ کاربری نمی‌تواند فرامین chmod، delete، overwrite و rename را به اجرا درآورد:

```
chmod       no      guest,anonymous
delete      no      guest,anonymous
overwrite   no      guest,anonymoys
rename      no      guest,anonymous
```

```
Connected to RH9Test (10.252.113.63).
220 RH9Test FTP Server (Version wu-2.6.2-8) ready.
Name (RH9Test:root): anonymous
331 Guest login ok, send your complete e-mail address as password.
Password:
230-This is a test message welcoming users to a new FTP server
230-
230-You can add the rules or requests of your choice to the welcome.msg.
230-
230-Using this file makes sense for an Anonymous FTP server; otherwise, you'd ha
ve to add welcome messages to each user's home directory.
230-
230-Please read the file README
230-  it was last modified on Sat Apr 5 15:34:29 2003 - 0 days ago
230 Guest login ok, access restrictions apply.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> cd etc/
250-This is a test message warning about the embedded /var/ftp/etc directory
250-
250-Please be careful about anything you might add to this directory.
250-
250 CWD command successful.
ftp>
```

شکل ۶-۲۷ پیغام‌هایی که پس از برقراری ارتباط با سرور FTP و تغییر موقعیت از یک فهرست به فهرست دیگر به نمایش درآمده است.

به طور پیش‌فرض، ارتباط کاربران با سرور FTP در فایل /var/log/messages و اقدام کاربران برای بارگذاری فایل‌ها روی کامپیوتر میزبان سرور FTP یا از روی آن در فایل /var/log/xferlog به ثبت می‌رسد. تنظیمات مربوطه چنین است:

```
log transfer anonymous,guest,real inbound,outbound
```

اجرای فرمان ftpshut به واسطه ایجاد فایل موقتی با عنوان /etc/shutmsg سرور FTP را در جریان توقف قریب‌الوقوع قرار می‌دهد. به این ترتیب، سرور FTP از قبول برقراری ارتباط برنامه‌های کلاینت با آن جلوگیری به عمل می‌آورد. به تنظیمات مربوطه توجه کنید:

```
shutdown /etc/shutmsg
```

چنان‌که قبلاً نیز اشاره شد، انتظار می‌رود که کاربران ناشناس هنگام برقراری ارتباط با سرور FTP آدرس پست الکترونیکی خود را در مقابل اعلان کلمه عبور وارد کنند. در این صورت کلمات عبور آن‌ها در فایل /var/log/messages به ثبت می‌رسد. در غیر این صورت، با انجام این تنظیمات می‌توان

اخطاری را در این زمینه نمایش داد. کاربران ناشناس با وجود وارد کردن یک آدرس پست الکترونیکی غیرمعتبر نیز می‌توانند سرور FTP را مورد دستیابی قرار دهند:

```
passwd-check rfc822 warn
```

محدود کردن تعداد دسترسی‌های هم‌زمان به سرور FTP و میزان بارگذاری فایل‌ها روی کامپیوتر میزبان سرور FTP یا از روی آن

چنان‌چه سرور FTP را جهت دسترسی از طریق شبکه اینترنت پیکربندی کرده‌اید، لازم است تعداد دسترسی‌های هم‌زمان به آن‌را محدود کنید. با این اقدام تمام کاربرانی که موفق به برقراری ارتباط با سرور FTP شده‌اند، در بارگذاری فایل‌های موردنظر خود از سرعت مناسب برخوردار خوهند بود. یک شیوه ساده برای انجام این کار تنظیم مقدار پارامترlimit در فایل /etc/ftpaccess است. برای مثال، به واسطه این تنظیمات حداکثر ۲۰ کاربر می‌توانند سرور FTP را به طور هم‌زمان مورد دستیابی قرار دهند. چنان‌چه در صورت تکمیل ظرفیت، کاربری برای برقراری ارتباط با سرور FTP اقدام کند، پیغام مندرج در فایل warning.msg به نمایش درمی‌آید:

```
limit    all    20    Any    warning.msg
```

با انجام این تنظیمات می‌توان تعداد دسترسی‌های هم‌زمان به سرور FTP را طی ساعات کاری (۸ صبح تا ۵ بعدازظهر) به ۲۰ کاربر محدود کرد:

```
limit    all    20    Wk0800-1700    warning.msg
```

بیان ساعت موردنظر در مقداردهی پارامتر limit براساس مشخصات مندرج در فایل l.sys انجام می‌شود. برای اطلاع از موقعیت فایل مزبور کافی است عنوان آن‌را مورد جستجو قرار دهید.

گروه‌های خبری منبع بسیار ارزشمندی برای کاربران Linux محسوب می‌شود. فراموش نکنید که این سیستم‌عامل از سوی جامعه جهانی کاربران و توسعه‌دهندگان دایماً در حال توسعه و گسترش است. اعضای این جامعه به طور مرتب مسایل خود را از طریق گروه‌های خبری و سایر منابع با یکدیگر در میان می‌گذارند. برای‌دستیابی به گروه‌های خبری موجود به آدرس http://groups.google.com مراجعه کنید.

علاوه بر محدود کردن تعداد دسترسی‌های هم‌زمان به سرور FTP، در صورت تمایل می‌توان میزان بارگذاری فایل‌ها از کامپیوتر میزبان سرور FTP یا روی آن‌را نیز محدود کرد. برای مثال، به واسطه این تنظیمات هر کاربری تنها می‌تواند به اندازه ۱۰۰ مگابایت از کامپیوتر میزبان سرور FTP بارگذاری کند:

```
byte-limit    out    100000000    all
```

چنان‌چه در تنظیمات فوق مقدار out با in جایگزین شود میزان بارگذاری روی کامپیوتر میزبان سرور FTP به ۱۰۰ مگابایت محدود خواهد شد و بالاخره استفاده از مقدار total به جای مقادیر فوق میزان محدودیت در بارگذاری را در هر دو جهت، یعنی بارگذاری روی کامپیوتر میزبان سرور FTP و از روی آن مشخص می‌کند.

فایل پیکربندی /etc/ftpconversions

فایل پیکربندی /etc/conversions امکان اجرای فرامین منتخب ضمن فرآیند بارگذاری را در اختیار می‌گذارد. برای مثال، اگر فایل فشرده‌ای حاوی تصاویر با عنوان pictures.gz روی کامپیوتر میزبان سرور FTP مستقر باشد، به واسطه سومین خط از فایل /etc/ftpconversions می‌توان با اجرای این فرمان برای باز کردن و خارج کردن تصاویر از قالب فشرده اقدام کرد:

```
ftp> get pictures
```

شکل ۷-۲۷ محتوای این فایل را نشان می‌دهد.

```
:.Z:   :  :/usr/bin/compress -d -c %s:T_REG|T_ASCII:O_UNCOMPRESS:UNCOMPRESS
:      : :.Z:/usr/bin/compress -c %s:T_REG:O_COMPRESS:COMPRESS
:.gz:  :  :/bin/gzip -cd %s:T_REG|T_ASCII:O_UNCOMPRESS:GUNZIP
:      : :.gz:/bin/gzip -9 -c %s:T_REG:O_COMPRESS:GZIP
:      : :.tar:/bin/tar -c -f - %s:T_REG|T_DIR:O_TAR:TAR
:      : :.tar.Z:/bin/tar -c -Z -f - %s:T_REG|T_DIR:O_COMPRESS|O_TAR:TAR+COMPRESS
:      : :.tar.gz:/bin/tar -c -z -f - %s:T_REG|T_DIR:O_COMPRESS|O_TAR:TAR+GZIP
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
"/etc/ftpconversions" 8L, 543C
```

شکل ۷-۲۷ محتوای فایل /etc/ftpconversions

در اجرای فرمان موردنظر نیازی نیست که پسوند فایل (در این‌جا gz.) را مشخص کنید، چرا که سرور FTP به طور خودکار و با توجه به محتوای فایل /etc/ftpconversions برای بازیابی فایل‌های فشرده اقدام خواهد کرد.

فایل پیکربندی /etc/ftphosts

فایل پیکربندی /etc/ftphosts قابلیت‌هایی نظیر دو فایل /etc/hosts.allow و /etc/hosts.deny از سرویس‌های xinetd را در اختیار می‌گذارد. (برای اطلاع بیشتر در این زمینه به فصل بیست و سوم مراجعه کنید.) به کمک تنظیمات این فایل می‌توان امکان هر یک از کاربران به دسترسی به سرور FTP را به خوبی کنترل کرد. با وجود این، عملکرد فایل مزبور کاملاً با آن‌چه که ممکن است انتظار داشته باشید، یکسان نیست.

برای مثال، با این تنظیمات دسترسی به سرور FTP تنها در اختیار کاربری با شناسه hdean قرار داده می‌شود، به شرطی که کاربر نامبرده این کار را از طریق کامپیوتری با مشخصه 192.168.0.32 انجام دهد. به بیان دیگر، هیچ کاربر دیگری از طریق هیچ یک از کامپیوترها امکان دسترسی به سرور FTP را ندارد: (به جای آدرس IP می‌توان نام کامل حوزه کامپیوتر موردنظر را بیان کرد.)

```
allow    hdean    192.168.0.32
```

به طور مشابه، این تنظیمات دسترسی کاربری با شناسه glock به سرور FTP را تنها از طریق کامپیوتری با مشخصه linux.example.com منع می‌کند:

```
deny    glock    linux.example.com
```

فرامین سرور FTP

این فرامین امکانات لازم برای تعیین زمان توقف و راه‌اندازی سرور FTP و اطلاع از کاربرانی که در حال حاضر سرور مزبور را مورد دستیابی قرار داده‌اند، در اختیار می‌گذارد. برای مثال، این تنظیمات از توقف سرور FTP ظرف پانزده دقیقه آتی یا رأس ساعت ۳:۳۰ بعدازظهر خبر می‌دهد:

```
ftpshut +15 "The FTP Server will close in 15 minutes"
ftpshut 1530 "The FTP server will stop at 3:30 PM"
```

همین تنظیمات را می‌توان در قالب یک اسکریپ نوشت و ترتیبی داد تا شبح cron رأس موعد مشخص آن‌را به اجرا درآورد. (برای اطلاع بیشتر در این زمینه به فصل سیزدهم مراجعه کنید.) بدیهی است این شیوه امکان استفاده از قابلیت‌های شبح cron را نیز در اختیار می‌گذارد. شرح سایر فرامین سرور FTP در جدول ۴-۲۷ آمده است.

جدول ۴-۲۷ شرح فرامین سرور FTP

عنوان فرمان	توضیح
ftpwho	این فرمان لیستی از شناسه کاربران و آدرس IP کامپیوترهایی را که به منظور برقراری ارتباط با سرور FPT مورد استفاده قرار داده‌اند، نمایش می‌دهد.
ftpcount	این فرمان تعداد کاربرانی را که در حال حاضر سرور FTP را مورد دستیابی قرار داده‌اند، نمایش می‌دهد.
ftpshut	این فرمان امکان توقف سرور FTP را بلافاصله بعد از اجرای فرمان یا در موعد مشخص در اختیار می‌گذارد.
ftprestart	این فرمان سرور FTP را متوقف کرده و مجدداً آن‌را راه‌اندازی می‌کند.

امکان بارگذاری فایل‌ها روی کامپیوتر میزبان سرور FTP توسط کاربران ناشناس

به طور پیش‌فرض، کاربران ناشناس از امکان بارگذاری فایل‌ها روی کامپیوتر میزبان سرور FTP یا به طور مشخص در فهرست var/ftp/ و زیرفهرست‌های آن برخوردار نیستند. با وجود این، گاهی اوقات به دلایلی مایل هستیم امکان بارگذاری در فهرست var/ftp/pub/ و زیرفهرست‌های آن را در اختیار کاربران ناشناس قرار دهیم. این کار را می‌توان با ویرایش فایل پیکربندی etc/ftpaccess/ و تغییر مجوزهای دسترسی به فهرست موردنظر انجام داد. برای مثال، با درج این تنظیمات در فایل پیکربندی مذکور امکان بارگذاری در فهرست var/ftp/letter/ فراهم می‌شود:

```
upload /var/ftp /letter yes cindy ywow 0660
```

به واسطه تنظیمات فوق، مالکیت فایل‌های بارگذاری شده در فهرست var/ftp/letter/ از آن کاربری با شناسه cindy و گروه کاربران ywow است. کاربر نامبرده و اعضای گروه مزبور می‌توانند فایل‌های بارگذاری شده در این فهرست را به منظور خواندن و نوشتن (مجوز 0660) مورد دستیابی قرار دهند. علاوه بر این، باید مجوزهای دسترسی به فهرست var/ftp/letter/ را دست کم به منظور نوشتن در آن (جهت بارگذاری فایل‌ها) تغییر دهید. در این مورد، با اجرای فرمان chmod 733 /var/ftp/letter می‌توان مجوز دسترسی را به نحو مطلوب تغییر داد، چراکه برای نوشتن در یک فهرست برخورداری از دست کم دو مجوز خواندن و اجرا کردن ضروری است. البته در صورتی که مایل باشید تا کاربران عادی کامپیوتر میزبان سرور FTP نیز از امکان دستیابی به فایل‌های مستقر در فهرست var/ftp/letter/

برخوردار شوند، می‌توانید مجوز خواندن آن فهرست را در اختیار آن‌ها نیز قرار دهید. (برای اطلاع بیشتر درباره چگونگی تنظیم مجوزهای دسترسی به فایل‌ها و فهرست‌ها به فصل ششم مراجعه کنید.)

جمع‌بندی

علیرغم قدمت پروتکل FTP یا File Transfer Protocol استفاده از آن هنوز متداول است. پروتکل مزبور یکی از شیوه‌های مناسب جهت به اشتراک گذاشتن فایل‌ها بوده و سرعت بارگذاری آن بسیار مطلوب است. برای مثال، با بهره‌گیری از این پروتکل می‌توان در مدت زمان قابل قبولی یک فایل بزرگ مانند فایل موجود در CD نصب سیستم‌عامل Red Hat Linux با اندازه‌ای بیش از ۶۵۰ مگابایت را بارگذاری کرد.

برنامه‌های کلاینت FTP به منظور استفاده از پروتکل FTP جهت دستیابی به فایل‌های مشترک طراحی شده و با دو رابط متنی و گرافیکی موجود هستند. برنامه‌های کلاینت FTP با رابط گرافیکی از ظاهری شکیل برخوردار بوده و امکان اجرای فرامین FTP را به سادگی فراهم می‌کنند. این فرامین را که تعداد آن‌ها نسبتاً قابل توجه است می‌توان در مقابل اعلان <ftp وارد کرده و به اجرا درآورد. به کمک همین فرامین می‌توان جدیدترین نسخه از بسته‌های نرم‌افزاری RPM را از سایت FTP شرکت Red Hat مورد دستیابی قرار داد. یکی از مزایای برنامه‌هایی مانند gFTP که دارای رابط گرافیکی هستند، تسهیلاتی است که این گونه برنامه‌ها در اختیار کاربران قرار می‌دهند. برای مثال، برنامه نامبرده امکان برقراری ارتباط با سرور FTP بسیاری از سایت‌های متداول را تنها با انتخاب گزینه مربوطه در اختیار کاربران قرار داده است.

توسعه‌دهندگان برنامه سرور FTP پیش‌فرض در سیستم‌عامل Red Hat Linux با عنوان vsFTP یا Very Secure FTP بر این باور هستند که این برنامه از بسیاری جهات بر WU-FTP یعنی برنامه سرور FTP پیش‌فرض در نسخه‌های قدیمی‌تر این سیستم‌عامل برتری دارد. علیرغم آن‌که نقل و انتقال داده‌ها توسط برنامه vsFTP در قالب متنی ساده یا رمزگذاری نشده انجام شده و این خود می‌تواند خط دسترسی به کلمات عبور کاربران را به دنبال داشته باشد، برنامه مزبور به هیچ وجه خطرات استفاده از برنامه WU-FTP را که به نوعی امکان دستیابی به فهرست ریشه کامپیوتر میزبان سرور FTP را فراهم می‌کند، به دنبال ندارد. پیشگیری از دستیابی به فهرست ریشه به واسطه مقداردهی مناسب متغیر مربوطه از فایل پیکربندی برنامه vsFTP با عنوان /etc/vsftpd.conf امکان‌پذیر است. در فایل مزبور متغیرهایی نیز به منظور پیکربندی دسترسی ناشناس، ثبت وقایع، بارگذاری فایل‌ها روی کامپیوتر میزبان سرور FTP و سایر موارد پیش‌بینی شده است.

دسترسی ناشناس به کامپیوتر میزبان سرور FTP یک سنت دیرینه است. برخورداری از این قابلیت در سیستم‌عامل Linux مستلزم بسته نرم‌افزاری anonftp-* است. با نصب این بسته نرم‌افزاری و پیکربندی چند پارامتر ساده، کاربران ناشناس می‌توانند فهرست var/ftp/ را مورد دستیابی قرار دهند. این موضوع در مورد هر دو برنامه vsFTP و WU-FTP صدق می‌کند. البته دستیابی به فهرست‌های واقع در سطوح بالاتر از این فهرست برای کاربران ناشناس غیرممکن است. چنین قابلیتی به واسطه مکانیزم قفس chroot به دست می‌آید. به سادگی می‌توان برنامه vsFTP را برای دسترسی ناشناس پیکربندی کرد. هم‌چنین می‌توان برنامه WU-FTP را به سادگی چنان پیکربندی کرد که امکان دسترسی به سرور FTP تنها در اختیار کاربران ناشناس بوده و ضمناً امکان اجرای فرامین بالقوه خطرناک از آن‌ها سلب شود.

در صورت تمایل می‌توان برنامه WU-FTP را به نحوی پیکربندی کرد تا مجوز دسترسی به سرور FTP تنها در اختیار کاربرانی باشد که مشخصات آن‌ها در فایل etc/passwd/ به ثبت رسیده است. پس از نصب این برنامه، فایل‌های پیکربندی کلیدی آن (شامل ftpaccecc، ftpconversions و ftphosts) در فهرست etc/ مستقر می‌شوند. تعیین مواردی چون محدودیت تعداد کاربرانی که به طور هم‌زمان می‌توانند سرور FTP را مورد دستیابی قرار دهند، محدودیت بارگذاری یک کاربر به‌خصوص یا مجموع تمام کاربران و امکان بارگذاری توسط کاربران ناشناس از طریق همین فایل‌ها قابل پیکربندی است. فرامین ftpwho، ftpcount، ftpshut و ftprestart به منظور مدیریت برنامه WU-FTP به عنوان سرور FTP پیش‌بینی شده است.

در فصل بعد برخی از سرویس‌های مفیدی را که برای شبکه‌های Linux و UNIX طراحی شده‌اند، مورد بررسی قرار می‌دهیم. چنان‌که خواهید دید، سرویس Network File System یا NFS امکان به اشتراک گذاشتن فایل‌ها را در چنین شبکه‌هایی فراهم می‌کند. هم‌چنین خواهید دید که چگونه با استفاده از سرویس Network Information System یا NIS می‌توان یک بانک اطلاعاتی متمرکز شامل فایل‌های پیکربندی موردنیاز کاربران شبکه ایجاد کرد.

فصل بیست‌وهشتم

استفاده از سرویس‌های NFS و NIS

مدیران شبکه‌های UNIX و Linux معمولاً از دو سرویس متداول Network File System و Network Information Service یا به اختصار NFS و NIS جهت به اشتراک گذاشتن فایل‌ها و فهرست‌ها میان کامپیوترهای مستقر در این گونه شبکه استفاده می‌کنند. سرویس NFS امکان سوار کردن فهرست‌های راه دور را به شکلی یکپارچه روی ماشین میزبان در اختیار قرار می‌دهد. سرویس NIS نیز یک بانک اطلاعاتی (با عنوان map) از فایل‌های پیکربندی کلیدی را در اختیار کامپیوترهای مستقر در شبکه قرار می‌دهد.

هنگامی که با استفاده از سرویس NFS یک فهرست راه دور را روی ماشین میزبان سوار می‌کنید، هیچ تفاوتی را نمی‌توانید میان آن فهرست و فهرست‌های محلی (که از قبل روی کامپیوتر میزبان مستقر بودند) تشخیص دهید. برای مثال، با بهره‌گیری از امکانات این سرویس می‌توانید فهرست‌های خانگی تمام کاربران را با یکدیگر به اشتراک گذاشته و سپس کامپیوترهای کلاینت مستقر در شبکه را به نحوی پیکربندی کنید که ضمن راه‌اندازی آن‌ها فهرست home/ نیز روی هر یک از آن‌ها سوار شود. سرویس NFS از این جهت که برای سرویس‌دهی از شش برنامه شبح استفاده می‌کند ممکن است تا حدودی پیچیده به نظر برسد. با این حال، فرامین موردنیاز برای بهره‌برداری از این سرویس و هم‌چنین ساختار فایل‌های پیکربندی آن نسبتاً ساده است. اگر از تجربه کافی در استفاده از سرویس NFS برخوردار نیستید، بهتر است ابزار redhat-config-nfs را جهت پیکربندی آن به خدمت بگیرید. در این فصل مخاطرات احتمالی در بهره‌برداری از سرویس NFS و نحوه مدیریت آن‌ها را نیز مورد بررسی قرار خواهیم داد.

در کامپیوترهای Linux از فایل‌های پیکربندی به خصوصی هم‌چون /etc/passwd و /etc/group به منظور مدیریت کاربران استفاده می‌شود. در مورد شبکه‌های محلی بدیهی است که تخصیص یک شناسه کاربری و کلمه عبور واحد به تمام کاربران فرآیند بسیار ساده‌تری است. بدون در نظر گرفتن سرویس NIS، مطلب فوق بدان معنی است که برای هر کاربر یک حساب مجزا با شاخص کاربری و شاخص گروهی مشابه سایر کاربران ایجاد کنیم. (این دو شاخص را معمولاً با عناوین UID و GID می‌شناسیم.) کاملاً واضح است که این فرآیند کار دشواری است. با وجود سرویس NIS می‌توانیم از یک

بانک اطلاعاتی واحد شامل اسامی کاربران، کلمات عبور و تعدادی فایل پیکربندی استفاده کرده و فرآیند فوق را به روش بسیار ساده‌تری انجام دهیم. در فصل حاضر به بررسی این موضوعات خواهیم پرداخت:

- پیکربندی سرویس NFS
- نحوه استفاده کلاینت‌ها از سرویس NFS
- پیکربندی سرویس NIS
- نحوه استفاده کلاینت‌ها از سرویس NIS

پیکربندی سرویس NFS

سرویس Network File System یا به اختصار NFS یکی از سرویس‌های اساسی سیستم‌عامل Linux است. بد نیست بدانید که یکی از فایل‌های پیکربندی اصلی این سرویس با عنوان /etc/exports در همان بسته نرم‌افزاری *-setup که فایل‌های پیکربندی /etc/passwd و /etc/profile در آن مستقر هستند، قالب‌بندی شده و روی ماشین میزبان نصب می‌شود. علاوه بر این، مدیریت سرویس NFS مستلزم داشتن توجه ویژه به تعدادی برنامه شبح است. تنظیم نحوه صدور فهرست‌ها از یک سرور NFS نیز کار نسبتاً ساده‌ای است. برای این منظور کافی است به ازای هر فهرست مشترک خط جدیدی را در فایل /etc/exports درج کرده و آن‌را با سایر کامپیوترهای مستقر در شبکه به اشتراک بگذارید، اما در مورد نحوه قالب‌بندی فرمان مربوطه دقت بسیاری به خرج دهید، چرا که با واسطه فرامین درست می‌توانید امنیت فهرست‌هایی را که از طریق سرویس NFS آن‌ها را با سایر کامپیوترها به اشتراک می‌گذارید، تأمین کنید.

یکی از مکانیزم‌های کلیدی سرویس NFS مکانیزمی با عنوان Remote Procedure Call یا به اختصار RPC است که امکان اجرای فرامین مورد نیازی را در مورد فهرست‌هایی که از راه دور روی سیستم فایل محلی سوار شده‌اند، در اختیار می‌گذارد. نکته قابل ذکر این است که تمام برنامه‌های شبح درگیر در سرویس NFS به نوعی این مکانیزم را مورد بهره‌برداری قرار می‌دهند.

ابزار گرافیکی redhat-config-nfs در سیستم‌عامل Red Hat Linux به منظور پیکربندی سرویس NFS پیش‌بینی شده و تسهیلات لازم برای این منظور را در اختیار قرار می‌دهد. فراموش نکنید که ابزار گرافیکی نامبرده صرفاً تسهیلاتی است برای آن‌چه که در این فصل به منظور پیکربندی سرویس NFS خواهید آموخت.

بسته‌های نرم‌افزاری موردنیاز برای بهره‌برداری از سرویس NFS

بسته‌های نرم‌افزاری موردنیاز برای استفاده از سرویس NFS هم‌اینک ممکن است روی ماشین میزبان نصب شده باشد. برخی از این بسته‌های نرم‌افزاری برای راه‌اندازی و بهره‌برداری از سیستم‌عامل Linux ضروری است. جدول ۱-۲۸ شامل شرح مختصری از این بسته‌های نرم‌افزاری است. چنان‌که در فصل دهم نیز توضیح داده شد، با اجرای فرمان rpm -qi *packagename* می‌توانید اطلاعات بیشتری درباره بسته اطلاعاتی موردنظر که با متغیر *packagename* مشخص شده است، به دست آورید.

جدول ۱-۲۸ شرح‌مختصری درباره‌بسته‌های نرم‌افزاری موردنیاز برای استفاده از سرویس NFS

عنوان بسته نرم‌افزاری	توضیح
setup-*	این بسته نرم‌افزاری حاوی یکی از فایل‌های پیکربندی کلیدی سرویس NFS با عنوان /etc/exports است.
initscripts-*	این بسته نرم‌افزاری حاوی برنامه‌های موردنیاز جهت سوار کردن فهرست‌های شبکه ضمن راه‌اندازی ماشین میزبان است.
nfs-utils-*	این بسته نرم‌افزاری حاوی برنامه‌های شبح و فرامین اصلی موردنیاز جهت بهره‌برداری از سرویس NFS است.
portmap-*	این بسته نرم‌افزاری حاوی فایل‌های موردنیاز برای پشتیبانی از مکانیزم RPC است.
quota-*	این بسته نرم‌افزاری حاوی فایل rpc.rquotad است که به منظور سهمیه‌بندی فهرست‌های به اشتراک گذاشته شده روی شبکه مورد استفاده قرار می‌گیرد. نصب این بسته نرم‌افزاری جهت بهره‌برداری از سرویس NFS ضروری نیست.

برنامه‌های شبح موردنظر برای بهره‌برداری از سرویس NFS

بهره‌برداری از سرویس NFS مستلزم راه‌اندازی دست کم پنج سرویس مختلف سیستم‌عامل Linux است. هریک از این سرویس‌ها وظایف به خصوصی (از سوار کردن فهرست‌ها روی سیستم فایل گرفته تا اطمینان خاطر از عملکرد صحیح مکانیزم RPC) به عهده دارند. سرویس‌های مورد بحث با اجرای برنامه‌های nfs، nfslock و portmap از فهرست /etc/rc.d/init.d راه‌اندازی می‌شوند. به شرح مختصری درباره این سرویس‌ها توجه کنید:

- **سرویس rpc.nfsd:** این سرویس با اجرای برنامه nfs از فهرست /etc/rc.d/init.d راه‌اندازی می‌شود. این سرویس به نوبه خود سرویس دیگری با عنوان rpc.mountd را فعال کرده و فرآیند صدور فهرست‌های مشترک را انجام می‌دهد. چنان‌چه مایل به تغییر پیکربندی این سرویس هستید، باید سرویس NFS را متوقف و سپس مجدداً راه‌اندازی کنید.
- **سرویس rpc.mountd:** با وجودی که فرمان mount امکان اتصال به فهرست‌های محلی (هم‌چون فهرست‌های مستقر روی یک فلاپی دیسک) و فهرست‌های شبکه (هم‌چون فهرست‌های قابل دستیابی از طریق یک سرور Samba) را در اختیار می‌گذارد، سرویس rpc.mountd به طور خاص جهت سوار کردن فهرست‌های NFS پیش‌بینی شده است.
- **سرویس portmap:** با وجودی که سرویس portmap تنها به منظور پشتیبانی از مکانیزم RPC طراحی شده است، وجود آن برای بهره‌بردرای از سرویس NFS کاملاً ضروری است. چنان‌چه سرویس portmap راه‌اندازی نشده باشد، برنامه‌های کلاینتی که سرویس NFS را به منظور دسترسی به فهرست‌های مشترک مورد استفاده قرار می‌دهند، قادر به یافتن این فهرست‌ها نخواهند بود.
- **سرویس rpc.statd و rpc.lockd:** در مواقعی هم‌چون راه‌اندازی مجدد ماشین میزبان ممکن است ارتباط برنامه‌های کلاینت با سرور NFS قطع شود. تحت چنین شرایطی وجود سرویس‌های rpc.statd به همراه سرویس rpc.lockd امکان برقراری ارتباط مجدد با سرور NFS را پس از راه‌اندازی مجدد آن فراهم می‌کند.
- **سرویس rpc.lockd:** به محض باز کردن یک فایل از فهرستی که به واسطه سرویس NFS به اشتراک گذاشته شده است، قفلی روی آن فایل نصب می‌شود. این قفل سایر کاربران را از رونویسی آن فایل بازمی‌دارد. این فرآیند توسط سرویس rpc.lockd که به واسطه برنامه nfslock راه‌اندازی می‌شود، صورت می‌پذیرد.

نحوه تعیین منابع مشترک

اطلاعاتی که بر مبنای آن فهرست موردنظر از طریق سرویس NFS به اشتراک گذاشته می‌شوند باید در فایل پیکربندی /etc/exports به ثبت برسد. این اطلاعات علاوه بر عنوان فهرست موردنظر شامل مشخصات کامپیوترهایی است که مایلیم فهرست مزبور را با آن‌ها به اشتراک بگذاریم. ضمناً کیفیت دسترسی به آن فهرست را نیز می‌توانیم در قالب همین اطلاعات محدود کنیم. الگوی عمومی برای انجام این کار به این صورت است: `sharedirectory hosts(specs)`

در الگوی فوق متغیر *sharedirectory* عنوان فهرست موردنظر و متغیر *hosts* مشخصه کامپیوترهایی است که مایل هستیم آن فهرست را از طریق سرویس NFS با آن‌ها به اشتراک بگذاریم. متغیر *specs* نیز بیانگر محدودیت‌هایی در کیفیت دسترسی به فهرست موردنظر است. برای مثال، فرض کنید مایل هستیم درایو CD-ROM را که روی ماشین میزبان سرور NFS مستقر است با سایر کامپیوترهای مستقر در شبکه به اشتراک بگذاریم. علاوه بر این، مایل هستیم دسترسی به فهرست /tmp را نیز از طریق همین سرویس فراهم کنیم. با توجه به الگوی فوق و در نظر گرفتن این نکته که محتوای CD روی فهرست /mnt/cdrom سوار می‌شود، کافی است این خطوط را در فایل پیکربندی /etc/exports درج کنیم:

```
/mnt/cdrom *.example.com(ro,sync) big.example.com(rw,sync)
/tmp *(rw,insecure,sync,no_wdelay,anonuid=600)
```

برای تعیین کامپیوترهایی که قصد داریم فهرستی را از طریق سرویس NFS با آن‌ها به اشتراک بگذاریم روش‌های متعددی وجود دارد. با وجود امکان استفاده از آدرس‌های IP باید به این نکته توجه کنید که سرویس NFS قادر به تشخیص آدرس‌هایی که به روش CIDR بیان می‌شوند نیست. جدول ۲-۲۸ مثال‌هایی را در این زمینه نشان می‌دهد.

جدول ۲-۲۸ مثال‌هایی از نحوه تعیین میزبان‌های موردنظر در فایل پیکربندی /etc/exports

مثال	توضیح
*.example.com	تمام کامپیوترهای مستقر در حوزه example.com
newcomp	کامپیوتری با نام newcomp
10.11.12.13/255.255.255.0	شبکه‌ای با آدرس 10.11.12.13 و ماسک زیر شبکه 255.255.255.0

پس از تعیین کامپیوترهای مورد نظر، در صورت لزوم می‌توانیم محدودیت دسترسی به فهرست‌های مشترک را مشخص کنیم. آیا برنامه‌های کلاینت تنها می‌توانند فهرست مشترک را جهت خواندن مورد دستیابی قرار دهند یا این‌که قادر هستند محتوای آن‌را نیز ـ ستخوش تغییر کنند؟ آیا دسترسی به فهرست مشترک شامل تمام زیرفهرست‌های آن نیز می‌شود؟ آیا کاربر اصلی (اصطلاحاً root) می‌تواند از طریق کامپیوتر دلخواهی فهرست مشترک را در مقام خود (یعنی به عنوان کاربر اصلی) مورد دستیابی قرار دهد؟ تعیین تمام محدودیت‌های فوق از طریق به کارگیری مشخصه‌هایی امکان‌پذیر است. با وجودی که شرح مختصری از این مشخصه‌ها در جدول ۳-۲۸ آمده است، کاربرد آن‌ها ممکن است تا اندازه‌ای پیچیده به نظر برسد.

جدول ۳-۲۸ مشخصه‌های قابل استفاده در فایل پیکربندی /etc/exports

مشخصه	توضیح
ro	این مشخصه بیانگر آن است که فهرست مشترک را تنها به منظور خواندن (اصطلاحاً read-only) می‌توان مورد دستیابی قرار داد.
rw	این مشخصه بیانگر آن است که فهرست مشترک به منظور خواندن و نوشتن (اصطلاحاً read-write) می‌تواند مورد دستیابی قرار بگیرد.
sync	این مشخصه بیانگر آن است که به محض صدور درخواست باید تمام داده‌ها روی دیسک نوشته شود.
async	این مشخصه بیانگر آن است که با وجود صدور درخواست، سرویس NFS می‌تواند اقدامی را در پاسخ به آن انجام دهد.
secure	این مشخصه بیانگر آن است که تمام درخواست‌های ارسالی به سرویس NFS به طور پیش‌فرض از طریق یک پورت TCP/IP مطمئن، یا به طور مشخص یکی از پورت‌های صفر تا ۱۰۲۳ انجام می‌شود. چنان‌چه قوانین مکانیزم دیوار آتش به منظور تأمین امنیت در حد متوسط یا در حد زیاد تنظیم شده باشد، تلاش برای دسترسی به این پورت‌ها با شکست مواجه می‌شود.
insecure	این مشخصه بیانگر آن است که تمام درخواست‌های ارسالی به سرویس NFS از طریق یک پورت عادی TCP/IP (پورت شماره ۱۰۲۴ یا پورت‌هایی با شماره بالاتر) انجام می‌شود.
wdelay	این مشخصه بیانگر آن است که اگر به واسطه یک درخواست ارسالی فرآیند نوشتن روی دیسک در آستانه وقوع باشد، هر درخواست دیگری که منجر به نوشتن روی دیسک شود، به تأخیر می‌افتد.
no_wdelay	این مشخصه بیانگر آن است که درخواست بیش از یک کامپیوتر جهت نوشتن روی دیسک بدون هیچ تأخیری اتفاق می‌افتد. در صورت فعال بودن مشخصه async نیازی به فعال کردن این مشخصه نیست.
hide	این مشخصه بیانگر آن است که هیچ‌یک از زیرفهرست‌های یک فهرست مشترک به اشتراک گذاشته نمی‌شوند. برای مثال، چنان‌چه فهرست /home/mj از طریق سرویس NFS به اشتراک گذاشته شده باشد، دسترسی به زیرفهرست /home/mj/.kde امکان‌پذیر نخواهد بود.
no_hide	این مشخصه بیانگر آن است که تمام زیرفهرست‌های یک فهرست مشترک به اشتراک گذاشته می‌شود.

مشخصه	توضیح
subtree_check	این مشخصه بیانگر آن است که در صورت صدور زیرفهرستی مانند /usr/sbin سرویس NFS امکان دسترسی به فهرست مادر (در این‌جا فهرست /usr) را نیز مورد بررسی قرار می‌دهد.
no_subtree_check	این مشخصه بیانگر آن است که در صورت صدور زیرفهرستی مانند /home/mj سرویس NFS امکان دسترسی به فهرست مادر (در این‌جا فهرست /home) را مورد بررسی قرار نمی‌دهد.
insecure_locks	این مشخصه بیانگر آن است که هیچ اقدامی برای اطمینان از این‌که آیا کاربر از مجوز دسترسی به فایل مورد درخواست برخوردار است یا خیر، انجام نمی‌شود. تأثیر این مشخصه مشابه مشخصه no_auth_nlm است.
secure_locks	این مشخصه بیانگر آن است که اقدامات لازم برای اطمینان از این‌که آیا کاربر از مجوز دسترسی به فایل مورد درخواست برخوردار است یا خیر توسط سرویس NFS انجام نمی‌شود. تأثیر این مشخصه مشابه مشخصه auth_nlm است.
all_squash	این مشخصه بیانگر آن است که کاربران ناشناس یا اصطلاحاً anonymous نیز می‌توانند فهرست مشترک را مورد دسترسی قرار دهند. چنین امکانی در مورد فهرست‌های عمومی مفید است.
no_all_squash	این مشخصه بیانگر آن است که کاربران ناشناس یا اصطلاحاً anonymous از امکان دسترسی به فایل‌های مشترک محروم هستند.
root_squash	این مشخصه بیانگر آن است که با تمام درخواست‌های ارسالی از جانب کاربر اصلی (اصطلاحاً root) مشابه درخواست‌های ارسالی از کاربران ناشناس برخورد می‌شود.
no_root_squash	این مشخصه بیانگر آن است که کاربر اصلی می‌تواند بدون کمترین محدودیتی فهرست مشترک را مورد دستیابی قرار دهد.
anonid=xyz	این مشخصه بیانگر آن است که شناسه کاربران ناشناس عبارت از xyz است. شناسه مزبور در فایل /etc/passwd از ماشین میزبان سرور NFS به ثبت می‌رسد.
anongid=xyz	این مشخصه بیانگر آن است که شناسه گروه مربوط به کاربران ناشناس عبارت از xyz است. شناسه مزبور درفایل /etc/passwd از ماشین میزبان سرور NFS به ثبت می‌رسد.

لازم به‌ذکر است که تمام فهرست‌های مشترک به طور پیش‌فرض از مشخصه‌های ro، secure، wdelay، subtree_check، secure_locks، no_all_squash و root_squash برخوردار هستند.

در سیستم‌عامل Red Hat Linux 8.0 و نسخه‌های بعد از آن هر فهرستی که به واسطه سرویس NFS به اشتراک گذاشته می‌شود باید دارای یکی از دو مشخصه sync یا async باشد. به این ترتیب، خط مشی سیستم‌عامل در مورد این‌که آیا تمام داده‌ها باید به محض صدور درخواست روی دیسک نوشته شوند یا آن‌که پیش از انجام به این کار سرویس NFS باید در ازای صدور آن درخواست اقدام خاصی را انجام دهد، مشخص می‌شود.

حال که با نقش کلیدی فایل پیکربندی /etc/exports آشنا شدید، مجدداً مثال قبل را در نظر بگیرید. اکنون باید بتوانید آن‌را به خوبی درک کنید:

```
/mnt/cdrom *.example.com(ro,sync) big.example.com(rw,sync)
/tmp *(rw,insecure,sync,no_wdelay,anonuid=600)
```

خط نخست، فهرست /mnt/cdrom را با تمام کامپیوترهای مستقر در حوزه example.com به اشتراک می‌گذارد. کامپیوترهای مزبور این فهرست را تنها به منظور خواندن می‌توانند مورد دستیابی قرار دهند، مگر آن‌که درخواست از جانب کامپیوتری با مشخصه big.example.com صادر شده باشد. (بدیهی است که این موضوع تنها در مورد CD های قابل نوشتن صدق می‌کند.)

خط دوم، فهرست /tmp را با تمام کامپیوترها به اشتراک می‌گذارد. با توجه به مشخصه rw، این کامپیوترها می‌توانند فهرست مزبور را به دو منظور خواندن و نوشتن مورد دستیابی قرار دهند. هم‌چنین با توجه به مشخصه insecure، درخواست دسترسی به فهرست مورد بحث به واسطه یکی از پورت‌های عادی TCP/IP (پورت شماره ۱۰۲۴ یا پورت‌هایی با شماره بالاتر) انجام می‌شود. مشخصه sync بیانگر آن است که تغییرات مورد درخواست پیش از هر اقدامی در فهرست /tmp منعکس می‌شود. مشخصه no_wdelay به این معنی است که حتی اگر سایر کامپیوترهایی که فهرست /tmp را به طور مشترک مورد استفاده قرار می‌دهند در آستانه دسترسی به فایلی از این فهرست باشند، داده‌ها بلافاصله روی دیسک ذخیره خواهد شد و بالاخره مشخصه anonuid با مقدار 600 بیانگر آن است که به محض سوار کردن فهرست /tmp روی سیستم فایل ماشین میزبان سرور NFS شناسه کاربران ناشناس در فایل /etc/passwd از ماشین مزبور به طور مناسب تغییر خواهد کرد.

ایمن‌سازی سرویس NFS

امنیت فهرست‌هایی را که از طریق سرویس NFS به اشتراک گذاشته می‌شوند می‌توان به واسطه تنظیمات فایل پیکربندی /etc/exports یا به کمک مکانیزم بازدارنده دیوار آتش تأمین کرد. پیش از این درباره مشخصه‌هایی‌از فایل‌پیکربندی /etc/exports که امکان محدودکردن دسترسی به فهرست‌های مشترک را در اختیار قرار می‌دهند، صحبت کردیم. به کمک صورت مناسبی از فرمان iptables یا حتی

تنظیمات موجود در فایل‌های /etc/hosts.allow و /etc/hosts.deny می‌توان دسترسی به فهرست‌های مشترک از خارج شبکه میزبان را محدود کرد.

با وجود این، گاهی اوقات لازم است امکان دسترسی به فهرست‌های مشترک را از طریق مکانیزم بازدارنده دیوار آتش فراهم کنیم. علیرغم آن‌که دسترسی به این گونه فهرست‌ها از طریق اینترنت می‌تواند بسیار خطرناک باشد، با رعایت نکات ایمنی می‌توان ترتیبی داد تا شبکه‌های مختلف یک شرکت واحد در یک چارچوب مطمئن امکان دسترسی به فهرست‌های مشترک مستقر روی شبکه میزبان را داشته باشند.

در ارتباط با مکانیزم بازدارنده دیوار آتش و تأمین امنیت فهرست‌هایی که از طریق سرویس NFS به اشتراک گذاشته می‌شوند باید دو پورت TCP/IP به شماره‌های ۱۱۱ و ۲۰۴۹ را به خاطر داشته باشید. با توجه به محتوای فایل /etc/services، پورت‌های مذکور به ترتیب مربوط به سرویس‌های portmap و NFS هستند.

بهره‌گیری از برنامه iptables جهت تأمین امنیت فهرست‌های مشترک

در فصل بیست و دوم به طور مفصل درباره برنامه iptables صحبت کردیم. چنان‌که از فصول سوم و نوزدهم نیز به خاطر دارید، دو برنامه lokkit و redhat-config-security در سیستم‌عامل Red Hat Linux امکانات لازم به منظور پیکربندی مکانیزم دیوار آتش را در دو سطح بازدارندگی متوسط و شدید در اختیار قرار می‌دهند.

مکانیزم بازدارندگی در سطح شدید (اصطلاحاً high-security firewall) تمام ارتباطات ممکن میان دو شبکه به جز پاسخ‌های ارسالی از سرورهای DNS را بلوکه می‌کند. به این ترتیب، هر گونه تلاش برای دستیابی به پورت‌های ۱۱۱ و ۲۰۴۹ نیز با شکست مواجه می‌شود.

از طرف دیگر، مکانیزم بازدارندگی در سطح متوسط (اصطلاحاً medium-security firewall)، (چنان‌که در شکل ۱-۲۸ مشاهده می‌کنید) تمام ارتباطات برقرار شده از طریق پورت‌های صفر تا ۱۰۲۳ را بلوکه می‌کند. به این ترتیب پورت شماره ۱۱۱ یعنی پورت موردنیاز برای دستیابی به سرویس portmap نیز بلوکه می‌شود. علاوه بر این، مکانیزم مزبور به طور صریح هر گونه تلاش برای دستیابی به پورت شماره ۲۰۴۹ یعنی پورت موردنیاز برای دستیابی به سرویس NFS را نیز بلوکه می‌کند.

```
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
RH-Lokkit-0-50-INPUT  all  --  anywhere             anywhere

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
RH-Lokkit-0-50-INPUT  all  --  anywhere             anywhere

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination

Chain RH-Lokkit-0-50-INPUT (2 references)
target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere
REJECT     tcp  --  anywhere             anywhere            tcp dpts:0:1023 flags:
SYN,RST,ACK/SYN reject-with icmp-port-unreachable
REJECT     tcp  --  anywhere             anywhere            tcp dpt:nfs flags:SYN,
RST,ACK/SYN reject-with icmp-port-unreachable
REJECT     udp  --  anywhere             anywhere            udp dpts:0:1023 reject
-with icmp-port-unreachable
REJECT     udp  --  anywhere             anywhere            udp dpt:nfs reject-wit
h icmp-port-unreachable
REJECT     tcp  --  anywhere             anywhere            tcp dpts:x11:6009 flag
s:SYN,RST,ACK/SYN reject-with icmp-port-unreachable
REJECT     tcp  --  anywhere             anywhere            tcp dpt:xfs flags:SYN,
RST,ACK/SYN reject-with icmp-port-unreachable
[root@RH9Test root]#
```

شکل ۱-۲۸ بخشی از تنظیمات مربوط به یک مکانیزم دیوار آتش با شدت بازدارندگی متوسط

برای اطلاع بیشتر درباره نحوه استفاده از برنامه iptables جهت پیکربندی مکانیزم دیوار آتش به فصل بیست و دوم مراجعه کنید.

برای تغییر این تنظیمات به نحوی که کامپیوترهای مستقر روی سایر شبکه‌های محلی نیز امکان دستیابی به فهرست‌های مشترک را داشته باشند، ابتدا قوانین محدود کننده دسترسی به سرویس NFS را حذف کنید. با توجه به شکل ۱-۲۸، قوانین سوم و پنجم در زنجیره RH-Lokkit-050-INPUT دسترسی به سرویس NFS را بلوکه می‌کند. برای حذف این قوانین کافی است فرامینی را به این ترتیب اجرا کنید:

```
# iptables -D RH-Lokkit-0-50-INPUT 5
# iptables -D RH-Lokkit-0-50-INPUT 3
```

سپس باید مطمئن شوید که تلاش برای دستیابی به پورت شماره ۱۱۱ بلوکه نمی‌شود. چنان‌که از فصل بیست و دوم به یاد دارید، با استفاده از سوییچ I- فرمان iptables می‌توان قانون جدیدی را به مجموعه قوانین موجود اضافه کرد. از این‌رو، با اجرای این فرامین می‌توانید ترتیبی دهید تا مکانیزم بازدارنده دیوار آتش اقدامی را به منظور بلوکه کردن درخواست‌های TCP و UDP ارسالی از طریق پورت شماره ۱۱۱ انجام ندهد:

```
# iptables -I rh-lokkit-0-50-Input 2 -p tcp -m tcp
--dport 111 -j ACCEPT
```

```
# iptables -I rh-lokkit-0-50-Input 3 -p udp -m udp
--dport 111 -j ACCEPT
```

در نهایت با اجرای این فرمان تغییرات را در فایل مربوطه ذخیره کنید. تأثیر این تغییرات را در دفعات بعدی راه‌اندازی کامپیوتر میزبان مشاهده خواهید کرد:

```
# iptables-save > /etc/sysconfig/iptables
```

اکنون با وجود مکانیزم بازدارنده دیوار آتش باید بتوانید فهرست‌هایی را که از طریق سرویس NFS به اشتراک گذاشته شده‌اند از خارج شبکه میزبان نیز مورد دستیابی قرار دهید.

چنان‌که در فصل بیست و دوم نیز توضیح دادیم، با اجرای فرمان service iptables save نیز می‌توانید تغییرات موردنظر را در قالب فایل /etc/sysconfig/iptables ذخیره کنید.

بهره‌گیری از مکانیزم TCP Wrapper جهت تأمین امنیت فهرست‌های مشترک

در فصل بیست و سوم مکانیزم بازدارنده دیگری در سیستم‌عامل Linux را که با سرویس‌های xinetd مربوط است، مورد بررسی قرار دادیم. چنان‌که مشاهده کردید، با وجود فرامین نادرست مندرج در فایل /etc/hosts.deny دسترسی به سرویس‌های portmap، rpc.mountd، rpc.rquotad، statd و lockd بلوکه خواهد شد. برای مثال، با درج این خط در فایل /etc/hosts.deny دسترسی به تمام سرویس‌ها بلوکه می‌شود:

```
ALL : ALL
```

به یاد بیاورید که پیش از راه‌اندازی سرویس‌های xinetd محتوای فایل /etc/hosts.allow مورد بازخوانی قرار می‌گیرد. از این‌رو، با درج تنظیمات ساده‌ای در فایل مزبور می‌توان امکان دسترسی به سرویس portmap را فراهم کرد. برای مثال، با درج این تنظیمات در فایل /etc/hosts.allow می‌توان امکان دسترسی به سرویس portmap را برای شبکه‌ای با آدرس 192.168.0.0 فراهم کرد:

```
portmap: 192.168.0.0/255.255.255.0
```

با همین روش می‌توان دسترسی به سرویس‌هایی را که به نوعی با سرویس NFS در ارتباط هستند فراهم کرد. به خاطر داشته باشید که آدرس‌دهی به شیوه CIDR هم‌چون 192.168.0.0/24 در هیچ یک از فایل‌های پیکربندی /etc/hosts.allow و /etc/hosts.deny مجاز نیست.

راه‌اندازی سرویس NFS

پس از تعیین مشخصه‌های موردنظر در /etc/exports و پیکربندی مکانیزم بازدارنده دیوار آتش، برای صدور فهرست‌های مشترک کافی است سرویس NFS را راه‌اندازی کنید.

برای شروع، فرمان rpcinfo -p را اجرا کنید. اگر سرویس NFS راه‌اندازی شده باشد، اجرای این فرمان نشان می‌دهد که سه برنامه portmap، nfs و rpc.mountd در حال اجرا هستند. چنین وضعیتی به وضوح در شکل ۲-۲۸ قابل تشخیص است.

```
[root@RH9Test root]# rpcinfo -p
   program vers proto   port
    100000    2   tcp    111  portmapper
    100000    2   udp    111  portmapper
    100024    1   udp   1024  status
    100024    1   tcp   1024  status
    391002    2   tcp   1025  sgi_fam
    100011    1   udp    947  rquotad
    100011    2   udp    947  rquotad
    100011    1   tcp    950  rquotad
    100011    2   tcp    950  rquotad
    100003    2   udp   2049  nfs
    100003    3   udp   2049  nfs
    100021    1   udp   1026  nlockmgr
    100021    3   udp   1026  nlockmgr
    100021    4   udp   1026  nlockmgr
    100005    1   udp   1027  mountd
    100005    1   tcp   2068  mountd
    100005    2   udp   1027  mountd
    100005    2   tcp   2068  mountd
    100005    3   udp   1027  mountd
    100005    3   tcp   2068  mountd
[root@RH9Test root]# []
```

شکل ۲-۲۸ اطمینان از راه‌اندازی سرویس NFS

در غیر این صورت می‌توان نتیجه گرفت که سرویس NFS راه‌اندازی نشده و بنابراین باید برای اجرای برنامه‌های نامبرده اقدام کنید. فرمان service nfs start را برای اجرای برنامه‌های rpc.mountd و nfs و فرمان service portmap start را جهت اجرای برنامه portmap به اجرا درآورید.

پس از راه‌اندازی سرویس NFS، با اجرای فرمان exportfs می‌توانید جهت به اشتراک گذاشتن فهرست‌های موردنظر اقدام کنید. جدول ۴-۲۸ شکل‌های مختلف این فرمان را شرح می‌دهد.

جدول ۴-۲۸ شکل‌های مختلف فرمان exportfs

عنوان فرمان	توضیح
exportfs -a	این فرمان تمام فهرست‌های مذکور در فایل /etc/exports را به اشتراک می‌گذارد.
exportfs -r	چنان‌چه لیست فهرست‌های مذکور در فایل /etc/exports دستخوش تغییر شود، با اجرای این فرمان می‌توان این فهرست‌ها را به اشتراک گذاشت.
exportfs -u	این فرمان لیست حاوی فهرست‌های مشترک را خالی می‌کند، به نحوی که هیچ فهرست مشترکی باقی نمی‌ماند.
exportfs -v	این فرمان لیست تمام فهرست‌های مشترک را نشان می‌دهد.

اکنون اجازه دهید تا نحوه دسترسی به فهرست‌های مشترک از طریق سرویس NFS را مورد بررسی قرار دهیم. پیش از هر چیز مطمئن شوید که کلیه سرویس‌های موردنیاز برای انجام این کار طی دفعات بعدی راه‌اندازی سیستم‌عامل Linux به طور خودکار راه‌اندازی خواهند شد. چنان‌که از فصل سیزدهم به خاطر دارید، با استفاده از فرمان chkconfig می‌توانید از این موضوع اطمینان حاصل کنید. برای مثال، جهت پی بردن به این موضوع که سرویس‌های nfs و portmap در کدام سطوح اجرایی راه‌اندازی می‌شوند، کافی است این فرامین را اجرا کنید:

```
# chkconfig --list nfs
# chkconfig --list portmap
```

در صورت لزوم می‌توانید این فرامین را به منظور اطمینان از این‌که سرویس‌های nfs و portmap در سطوح اجرایی موردنظر راه‌اندازی می‌شوند، به اجرا درآورید: (راه‌اندازی سرویس nfs خود موجب راه‌اندازی سرویس rpc.mountd و rpc.rquotad می‌شود.)

```
# chkconfig --level 235 portmap on
# chkconfig --level 235 nfs on
```

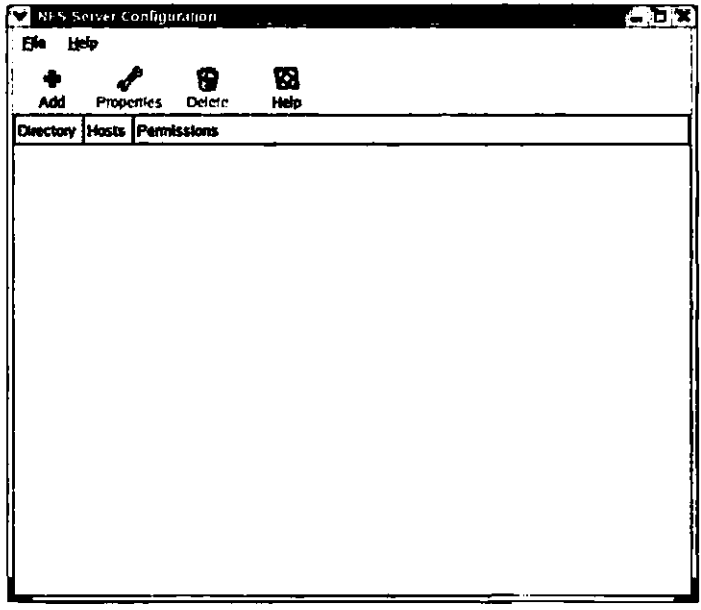
پیکربندی‌سرویس NFS بااستفاده ازبرنامه redhat-config-nfs

برنامه redhat-config-nfs رابط گرافیکی موردنیاز به منظور پیکربندی سرویس NFS را در اختیار قرار می‌دهد. برای اجرای این برنامه فرمان redhat-config-nfs را از سطر فرمان سیستم‌عامل Red Hat Linux به اجرا درآورده یا گزینه NFS Server را از منوی Server Settings واقع در منوی فرعی System Settings از منوی اصلی Main Menu (یا K Menu) انتخاب کنید. این اقدام پنجره حاوی امکانات پیکربندی مربوط به سرویس NFS با عنوان NFS Server Configuration را در اختیار می‌گذارد. شکل ۳-۲۸ این پنجره را نشان می‌دهد.

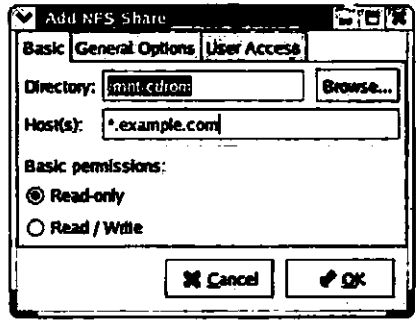
با کلیک روی گزینه Add در نوار ابزار این پنجره، کادر محاوره‌ای Add NFS Share باز می‌شود. شکل ۴-۲۸ امکانات موجود در بخش Basic از این کادر محاوره‌ای را نشان می‌دهد.

چنان‌که در این شکل مشاهده می‌کنید، فهرست /mnt/cdrom به عنوان یک فهرست فقط خواندنی با کامپیوترهای مستقر در حوزه example.com.* به اشتراک گذاشته شده است. در صورت تمایل می‌توان فهرست دیگری چون /mnt/cdrom یا /tmp را به عنوان فهرستی با قابلیت خواندن و نوشتن با کامپیوتر مشخصی مانند big.example.com از حوزه نامبرده به اشتراک گذاشت.

شکل ۵-۲۸ گزینه‌های موجود در بخش General Options از کادر محاوره‌ای Add NSF Share را نشان می‌دهد. همان‌گونه که مشاهده می‌کنید، از میان گزینه‌های موجود تنها گزینه Sync Operations On Request به طور پیش‌فرض فعال است. جدول ۵-۲۸ حاوی فرامین متناظر با این گزینه‌هاست.



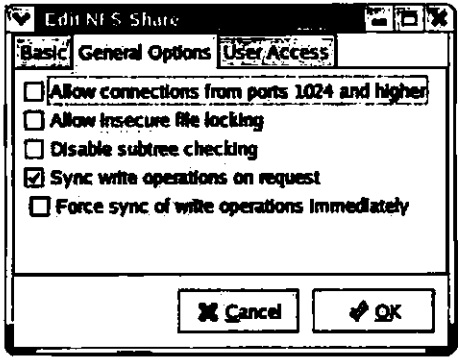
شکل ۳-۲۸ پنجره NFS Server Configuration



شکل ۳-۲۸ کادر محاوره‌ای Add NFS Share

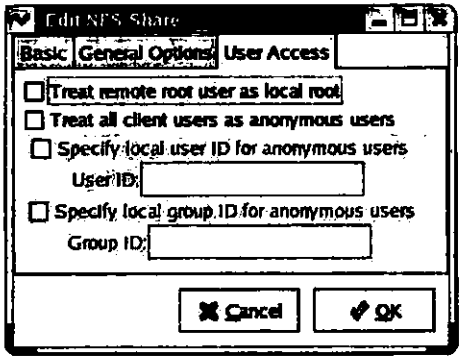
جدول ۵-۲۸ فرامین متناظر با گزینه‌های موجود در بخش General Options از کادر محاوره‌ای Add NFS Share

عنوان گزینه	فرمان متناظر
Allow Connections From Ports 1024 And High	insecure
Allow Insecure File Locking	insecure_locks
Disable Subtree Checking	no_subtree_check
Sync Write Operations On Request	sync
Force Sync Of Write Operations Immediately	no_wdelay



شکل ۵-۲۸ امکانات بخش General Options از کادر محاوره‌ای Add NFS Share

شکل ۶-۲۸ گزینه‌های موجود در بخش User Access از کادر محاوره‌ای Add NFS Share را نشان می‌دهد. جدول ۶-۲۸ حاوی فرامین متناظر با این گزینه‌هاست.



شکل ۶-۲۸ امکانات User Access از کادر محاوره‌ای Add NFS Share

جدول ۶-۲۸ فرامین متناظر با گزینه‌های موجود در بخش User Access از کادر محاوره‌ای Add NFS Share

عنوان گزینه	فرمان متناظر
Treat Remote Root User As Local Root	no_root_squash
Treat All Client Users As Anonymous Users	all_squash
Specify Local User ID for Anonymous Users UID	anonuid=*userid*
Specify Local Group ID for Anonymous Users Group UID	anongid=*groupid*

دقت کنید که دو گزینه نخست در تناقض هستند به طوری که تنها یکی از آن‌ها را می‌توان فعال کرد. به بیان دیگر، در صورتی که تمام کاربران NFS از نوع ناشناس باشند، نمی‌توان دسترسی از راه دور را به عنوان دسترسی کاربر اصلی (اصطلاحاً root) مجاز شمرد.

علاوه بر این، برای هیچ یک از دو گزینه Specify Local User ID و Specify Local Group ID فرمان متناظری وجود ندارد. در واقع وجود فرمان برای این دو گزینه کاملاً بی‌معنی بوده و فعال کردن گزینه‌های مربوطه به معنی تعیین یک شناسه کاربری یا شناسه گروه است. (برای اطلاع بیشتر در مورد دو مفهوم شناسه کاربری و شناسه گروه به فصل نهم مراجعه کنید.)

پس از انجام این تنظیمات محتوای فایل پیکربندی /etc/exports نسبت به قبل تا حدودی متفاوت خواهد بود. برای نمونه، چنان‌که در این‌جا مشاهده می‌کنید، تنظیمات دسترسی به فهرست‌های مشترک با مجوز فقط خواندنی و مجوزهای خواندن و نوشتن که به عنوان مثال مطرح شد، در سه خط مجزا قالب‌بندی شده‌اند:

```
/mnt/cdrom *.example.com(ro,sync)
/mnt/cdrom big.example.com(rw,sync)
/tmp  *(rw,insecure,sync,no_wdelay,all_squash,anonuid=600)
```

به خاطر داشته باشید که پیکربندی سرویس NFS تنها با استفاده از ابزار گرافیکی redhat-config-nfs امکان‌پذیر نیست. برای مثال، به کمک این ابزار هیچ روشی برای اطمینان از این موضوع وجود ندارد که آیا مکانیزم بازدارنده دیوار آتش کاربران را از دسترسی به فهرست‌های مشترک بازمی‌دارد یا خیر. هم‌چنین روشی برای اطمینان از این موضوع که آیا طی دفعات بعدی راه‌اندازی سیستم‌عامل Linux، سرویس‌های nfs و portmap به طور خودکار در سطوح اجرایی موردنظر راه‌اندازی خواهند شد یا خیر، وجود ندارد.

نحوه دسترسی به فهرست‌های مشترک از طریق کامپیوترهای کلاینت

اطلاع از وجود فهرست‌های مشترک، نحوه سوار کردن صحیح آن‌ها روی سیستم فایل و نحوه پیکربندی این فهرست‌ها به گونه‌ای که طی راه‌اندازی‌های آتی سیستم‌عامل Linux به طور خودکار روی سیستم فایل سوار شوند، تمام آن چیزی است که جهت دستیابی به فهرست‌های مشترک از طریق سرویس NFS نیاز دارید. در قسمت‌های بعد به بررسی این موضوعات می‌پردازیم.

اطلاع از فهرست‌های مشترک

اطلاع از نام کامپیوتر میزبان سرور NFS یا آدرس IP آن به منظور اطلاع از لیست فهرست‌هایی که از طریق سرویس NFS به اشتراک گذاشته شده‌اند، ضروری است. برای نمونه، این فرمان لیست فهرست‌هایی را نمایش می‌دهد که به واسطه سرویس NFS مستقر روی کامپیوتری با عنوان RHL9 به اشتراک گذاشته شده‌اند:

```
# showmount -e RHL9
Export list for RHL9:
/home/gb RHL9*
/tmp  *.example.com
```

با اجرای فرمان showmount -e از سطر فرمان سیستم‌عامل کامپیوتر میزبان سرور NFS می‌توان لیست فهرست‌های مشترک نامبرده در فایل پیکربندی /etc/exports را مشاهده کرد.

چنان‌که مشاهده می‌کنید، فرمان فوق دو فهرست /home/gb و /tmp را به عنوان فهرست‌های مشترک و نیز کامپیوترهایی را که امکان دسترسی به این فهرست‌ها را دارند، مشخص کرده است. چنان‌چه نتیجه اجرای این فرمان صحیح نبوده یا فرمان showmount -e به هر دلیل قابل اجرا نباشد این اقدامات را انجام دهید:

- **وضعیت سرویس‌ها را بررسی کنید.** مطمئن شوید که سرویس‌های nfs، portmap و mountd راه‌اندازی شده‌اند.
- **میزان بازدارندگی مکانیزم دیوار آتش را بررسی کنید.** مطمئن شوید که برنامه iptables دسترسی به پورت‌های ۱۱۱ و ۲۰۴۹ را بلوکه نکرده است. هم‌چنین مطمئن شوید که دسترسی به سرویس NFS در فایل پیکربندی /etc/hosts.deny بلوکه نشده باشد.
- **مطمئن شوید که فهرست‌های مشترک را در فایل پیکربندی /etc/exports مشخص کرده‌اید.** برای این منظور، فرمان showmount -e را از سطر فرمان سیستم‌عامل ماشین میزبان سرور NFS اجرا کنید. فراموش نکنید که اگر لیست فهرست‌های مشترک مذکور در این فایل را به هر دلیل دستخوش تغییر کرده‌اید، با اجرای فرمان exportfs -s از سطر فرمان مزبور باید سرویس NFS را در جریان فهرست‌های مشترک جدید قرار دهید.

در صورتی که با انجام اقدامات فوق نتیجه مطلوب حاصل نشود، به مباحث فصل بیست و یکم درباره عیب‌یابی و اشکال‌زدایی شبکه مراجعه کنید. فرامین متعددی برای اطمینان از اتصالات شبکه وجود دارد. با وجود این، بیشتر اشکالات شبکه ناشی از وجود نقص در اتصالات فیزیکی است.

سوار کردن فهرست‌های مشترک روی سیستم فایل

با فرض این‌که عملکرد سرور کاملاً مطابق انتظار باشد، بار دیگر فرمان showmount -e *NFSserver* را اجرا کنید. (متغیر *NFSserver* در این فرمان بیانگر نام کامپیوتر میزبان سرور NFS است.) با در اختیار داشتن لیست فهرست‌های مشترک، اکنون می‌توانید برای سوار کردن آن‌ها روی سیستم فایل موردنظر از کامپیوتر کلاینت اقدام کنید. برای مثال، با اجرای این فرمان می‌توانید فهرست مشترک /tmp را به واسطه سرویس NFS (که روی ماشینی با نام RHL9 مستقر است) روی سیستم فایل /tmp از کامپیوتر کلاینت سوار کنید:

```
# mount -t nfs RHL9:/tmp /tmp
```

به زبان ساده، فرمان فوق فهرست مشترک /tmp را به واسطه سرویس NFS (گزینه -t nfs) مستقر روی کامپیوتری با نام RHL9 روی سیستم فایل /tmp از کامپیوتر محلی (کلاینت) سوار می‌کند. با وجود این، در صورتی که سرویس NFS یا اتصالات شبکه به هر دلیل مختل شود، اشکالاتی پیش می‌آید. برای مثال، فرض کنید کنسول سطر فرمان قفل شود. تحت چنین شرایطی کامپیوتر محلی با وجود غیردسترس بودن سرویس NFS برای دسترسی به آن تلاش خواهد کرد. از این‌رو، همواره بهتر است فرمان فوق را به این صورت با استفاده از گزینه -o اجرا کنید:

```
# mount -t nfs -o soft,intr,timeo=50 RHL9:/tmp /tmp
```

با اجرای فرمان فوق، چنان‌چه به هر دلیل ارتباط کامپیوتر محلی با ماشین میزبان سرور NFS (جهت سوار کردن فهرست مورد نظر) ظرف مدت پنجاه دهم ثانیه (معادل ۵ ثانیه) برقرار نشود، کامپیوتر مزبور دست از تلاش بر می‌دارد. با توجه به مباحث فصل هفتم، فرمان فوق را می‌توان ساده‌تر کرد. برای این منظور، ابتدا این خط را در فایل /etc/fstab درج کنید:

```
RHL9:/tmp   /tmp  nfs   soft,intr,timeo=50   0 0
```

سپس با اجرای این فرمان ساده از سطر فرمان سیستم‌عامل ماشین محلی می‌توانید فهرست مشترک /tmp را تحت همان شرایط مورد دسترسی قرار دهید:

```
# mount /tmp
```

پیکربندی سرویس NIS

سرویس Network Information Service یا به اختصار NIS تسهیلاتی برای دستیابی به یک بانک اطلاعاتی غیرمتمرکز یا توزیع‌شده (اصطلاحاً distributed database) است. به کمک این سرویس

کامپیوترهای کلاینت مستقر در شبکه می‌توانند مجموعه‌ای از فایل‌های پیکربندی را مورد دستیابی قرار دهند. مدیران شبکه‌ها نیز با بهره‌گیری از این سرویس می‌توانند پیکربندی مجموعه‌ای از کامپیوترهای کلاینت را از یک نقطه واحد انجام دهند.

به دلیل شباهت فایل‌های پیکربندی اولیه تمام کامپیوترهای Linux استفاده از سرویس NIS جهت پیکربندی و نگهداری از یک بانک اطلاعاتی شامل این فایل‌های پیکربندی راه‌حل ساده‌تری نسبت به نگهداری نسخه‌های مختلفی از این فایل‌ها روی کامپیوترهای کلاینت مستقر در شبکه است.

برای مثال، فرض کنید مایلیم تا کاربران شبکه بتوانند با استفاده از شناسه کاربری و کلمه عبور خود تمام کامپیوترهای مستقر در آن شبکه را مورد دستیابی قرار دهند. یک روش برای دستیابی به هدف فوق این است که نسخه‌ای از فایل‌های /etc/passwd و /etc/group را روی تمام کامپیوترهای مستقر در شبکه کپی کنیم. در حالی که با وجود سرویس NIS کافی است شناسه کاربری و کلمات عبور تمام کاربران را در قالب یک بانک اطلاعاتی که اصطلاحاً به آن map گفته می‌شود، روی کامپیوتر میزبان سرور NIS مستقر کرده و به همان قابلیت دست پیدا کنیم.

به عنوان مثال دیگر، فرض کنید شبکه محلی حاوی تعداد نسبتاً قابل توجهی کامپیوتر بوده و به دلایلی از جمله دشواری‌های مربوط به پیکربندی سرور DNS تمایلی چندانی به استفاده از این سرور نداریم. با وجودی که می‌توانیم یک نسخه از فایل /etc/hosts را روی تمام کامپیوترهای مستقر در شبکه کپی کنیم، در صورت افزایش تعداد کامپیوترها اقدام فوق پیچیدگی‌هایی را به دنبال خواهد داشت. به عنوان یک راه‌حل بسیار مناسب، کافی است فایل /etc/hosts را در قالب بانک اطلاعاتی map روی ماشین میزبان سرور NIS مستقر کرده و به واسطه سرویس NIS امکان دسترسی کامپیوترهای مستقر در شبکه را به فایل نامبرده فراهم کنیم.

با وجودی که پیکربندی سرویس DNS کار چندان دشواری نیست، اقدام به این کار به معنای راه‌اندازی یک سرویس است. برخی از مدیران سیستم‌ها ترجیح می‌دهند تا تعداد سرویس‌های فعال را به حداقل ممکن کاهش دهند. یک روش برای انجام این کار آن است که به جای پیکربندی سرویس DNS در شبکه محلی، دسترسی مشترک به فایل /etc/hosts را از طریق سرویس NIS برای تمام کامپیوترهای مستقر در آن شبکه مهیا کنیم.

کلیه بسته‌های نرم‌افزاری موردنیاز به منظور پشتیبانی از سرویس NIS 2.2 به همراه سیستم‌عامل Red Hat Linux 9 توزیع شده است. در این فصل اشاراتی نیز به برنامه nisplus شده است. برنامه مزبور در صورت استفاده از سرویس NIS 3.x قابل بهره‌برداری بوده و البته تاکنون اشکالاتی نیز در استفاده از آن

گزارش شده است.

در قسمت‌های بعد ضمن شرح مختصری درباره بسته‌های نرم‌افزاری موردنیاز جهت بهره‌برداری از سرویس NIS، مفهوم "حوزه" را در ارتباط با سرویس NIS توضیح داده و درباره مکانیزم این سرویس صحبت خواهیم کرد. ضمناً نحوه راه‌اندازی سرویس NIS و چگونگی تولید بانک اطلاعاتی map را نیز مورد بررسی قرار خواهیم داد.

نقطه ضعف سرویس NIS امنیت آن است. چنان‌چه سرویس مزبور را روی کامپیوتری از یک شبکه نصب کرده‌اید، باید آن‌را در پس مکانیزم بازدارنده دیوار آتش مستقر کنید. ضمناً نباید هیچ مکانیزم بازدارنده‌ای را مابین کامپیوتر میزبان سرور NIS و کامپیوترهای کلاینت فعال کنید. با وجودی که به واسطه پیکربندی‌های مختلف مکانیزم مزبور تا اندازه زیادی می‌توان سرویس NIS را محافظت کرد، انجام این کار مشکلاتی را در پی خواهد داشت. یک جستجوی ساده در مورد دو واژه NIS و security در اینترنت آدرس هزاران وب سایت را در اختیار می‌گذارد که حاوی مقالات و پیغام‌هایی درباره مشکلات امنیت مربوط به سرویس NIS هستند.

بسته‌های نرم‌افزاری موردنیاز جهت بهره‌برداری از سرویس NIS

استفاده از سرویس NIS مستلزم نصب چهار بسته نرم‌افزاری است. شرح مختصری از این بسته‌های نرم‌افزاری درجدول ۷-۲۸ آمده‌است. چنان‌که مشاهده می‌کنید، بسته نرم‌افزاری portmap-* نیز یکی از این‌بسته‌های‌نرم‌افزاری‌است. با اجرای فرمان rpm -qi *packagename* می‌توانید اطلاعات بیشتری درباره بسته نرم‌افزاری موردنظر که در این فرمان با متغیر *packagename* مشخص شده است، به دست آورید.

جدول ۷-۲۸ شرح بسته‌های نرم‌افزاری موردنیاز جهت بهره‌برداری از سرویس NIS

عنوان بسته نرم‌افزاری	توضیح
portmap-*	این بسته نرم‌افزاری حاوی مکانیزم موردنیاز جهت دسترسی از راه دور به شیوه Remote Procedure Call یا به اختصار RPC است.
ypbind-*	این بسته نرم‌افزاری حاوی برنامه کلاینت NIS است. ارتباط این برنامه با برنامه سرور NIS (بسته نرم‌افزاری ypserv-*) از طریق مکانیزم RPC (بسته نرم‌افزاری portmap-*) مهیا می‌شود.
ypserv-*	این بسته نرم‌افزاری حاوی برنامه سرور NIS است.
yp-tools-*	این بسته نرم‌افزاری حاوی فرامین مربوط به سرویس NIS است.

سرویس NIS توسط شرکت Sun Microsystems ابداع شد. عنوان اصلی این سرویس در اصل Yellow Pages بود، اما از آن‌جا که عنوان مزبور قبلاً به ثبت رسیده بود، عنوان آن به Network Information Service یا به اختصار NIS تغییر کرد. با وجود این، در برخی متون از هر دو عنوان فوق برای اشاره به این سرویس استفاده می‌شود. ـ مترجم

مفهوم حوزه در ارتباط با سرویس NIS

کامپیوترهای میزبان سرور NIS (کامپیوترهای سرور) و کامپیوترهایی که از سرویس NIS استفاده می‌کنند (کامپیوترهای کلاینت) در قالب حوزه‌هایی سازمان‌دهی می‌شوند. مفهوم حوزه در رابطه با سرویس NIS با مفهوم متداول آن یعنی مکانیزم سازمان‌دهی و نام‌گذاری کامپیوترهای مستقر در یک شبکه و هم‌چنین با مفهوم آن در شبکه‌های ویندوز کاملاً متفاوت است.

برای اطلاع از نام حوزه NIS یک کامپیوتر کافی است فرمان domainname را از سطر فرمان آن اجرا کنید. چنان‌چه کامپیوتر موردنظر فاقد نام حوزه NIS باشد، فرمان مزبور در پاسخ واژه none را نمایش خواهد داد.

فرمان domainname امکان نسبت دادن نام حوزه NIS را نیز در اختیار قرار می‌دهد. برای مثال، با اجرای این فرمان از سطر فرمان یک کامپیوتر می‌توان نام nistest را به عنوان نام حوزه NIS به آن کامپیوتر نسبت داد:

```
# domainname nistest
```

علاوه بر اقدام فوق، برای آن‌که طی دفعات بعدی راه‌اندازی کامپیوتر نیز به طور خودکار همین نام به عنوان نام حوزه NIS موردنظر به آن کامپیوتر نسبت داده شود، لازم است این عبارت نسبت‌دهی را در فایل پیکربندی /etc/sysconfig/network درج کنید:

```
NISDOMAIN=nisntest
```

تعیین فایل‌های مشترک

پس از نصب بسته‌های نرم‌افزاری موردنیاز و نسبت دادن نام حوزه NIS به کامپیوتر مورد نظر، باید برای پیکربندی سرور NIS اقدام کنید. این کار با ویرایش فایل Makefile از فهرست /var/yp آغاز می‌شود. فایل مزبور حاوی پارامترهایی است که در صورت لزوم می‌توانید مقادیر آن‌ها را تنظیم کنید. پس از انجام تنظیمات موردنظر، به کمک یک برنامه اسکریپت به‌خصوص با عنوان ypinit می‌توانید برای تولید بانک اطلاعاتی map اقدام کنید. در این قسمت به شرح پارامترهای مزبور می‌پردازیم.

در صورت تمایل می‌توان سرویس NIS را به نحوی پیکربندی کرد تا کامپیوترهایی را نیز که در بانک اطلاعاتی NIS موجود نیستند، مورد توجه قرار دهد. با فعال کردن این تنظیمات (که با حذف علامت #

از ابتدای خط امکان‌پذیر است)، سرویس NIS اطلاعات بیشتر در این زمینه را از طریق سرورهای DNS به دست می‌آورد:

```
#B=-b
```

در شبکه‌های بزرگ‌تر می‌توان برای اطمینان بیشتر از یک یا چند سرور NIS پشتیبان نیز بهره گرفت. در این صورت باید مقدار true را در این تنظیمات به false تغییر دهید: (با انجام این کار سرویس NIS فایل /var/yp/ypservers را به منظور اطلاع از اسامی سرورهای NIS پشتیبان مورد توجه قرار خواهد داد.)

```
NOPUSH=true
```

به طور پیش فرض، شناسه کاربران عادی و شناسه گروه‌هایی که این کاربران عضو آن‌ها هستند با عدد 500 یا اعداد بزرگ‌تر مشخص می‌شود. اعداد کوچکتر از 500 به عنوان شناسه کاربرانی که وظایف مدیریتی دارند و شناسه گروه‌هایی که این گونه کاربران عضو آن‌ها هستند، مورد استفاده قرار می‌گیرد. این تنظیمات اعداد کوچک‌تر از 500 را از لیست بانک اطلاعاتی map حذف می‌کند:

```
MINUID=500
MINGID=500
```

در صورت تمایل، به واسطه تنظیم پارامترهای فوق با اعداد بزرگ‌تر از 500 می‌توان برخی از کاربران را به عنوان کاربران محلی از سایر کاربران متمایز کرد. به عنوان مثال، استفاده از عدد 505 برای این منظور موجب خواهد شد تا پنج کاربر نخست از تمام کامپیوترهای عضو آن حوزه NIS به عنوان کاربران محلی از سایر کاربران متمایز شوند.

چنان‌چه کاربر اصلی (اصطلاحاً root) برای اتصال به یک سرور NIS از یک حوزه NIS اقدام کند، به موجب این تنظیمات شناسه کاربری وی به شناسه کاربری به‌خصوصی با عنوان nobody که نسبت به کاربر اصلی از امتیازات کمتری نیز برخوردار است، تنزل پیدا می‌کند:

```
NFSNOBODYUID=65534
NFSNOBODYGID=65534
```

چنان‌که از فصل نهم به خاطر دارید، کلمات عبور کاربران و گروه‌ها به ترتیب در قالب دو فایل /etc/shadow و /etc/gshadow نگهداری می‌شود. در صورتی که سیستم‌عامل Linux به صورت فوق پیکربندی شده باشد، به موجب این تنظیمات کلمات عبور در قالب بانک اطلاعاتی map نیز درج خواهند شد:

```
MERG_PASSWD=true
MERG_GROUP=true
```

این تنظیمات بیانگر موقعیت برخی از فهرست‌های استاندارد در سیستم‌عامل Linux هستند. از این‌رو، در صورتی که موقعیت فایل‌هایی چون /etc/passwd را تغییر نداده باشید، نیازی نیست که این تنظیمات را تغییر دهید:

```
YPSRCDIR = /etc
YPPWDDIR = /etc
YPBINDDIR = /usr/lib/yp
YPSBINDDIR = /usr/sbin
YPDIR = /var/yp
YPMAPDIR = $(YPDIR)/$(DOMAIN)
```

برخی از تنظیماتی که در ادامه مشاهده می‌کنید، استاندارد هستند. برای مثال، به دلیل آن‌که مقدار پارامتر YPPWDDIR از تنظیمات فوق برابر با /etc است، مقدار پارامتر GROUP در این تنظیمات بیانگر موقعیت فایل پیکربندی /etc/group خواهد بود. چنان‌چه پیش از این موقعیت فایل‌های پیکربندی را تغییر داده‌اید، لازم است مقدار پارامتر مربوطه را نیز در این تنظیمات تغییر دهید:

```
GROUP      = $(YPPWDDIR)/group
PASSWD     = $(YPPWDDIR)/passwd
SHADOW     = $(YPPWDDIR)/shadow
GSHADOW    = $(YPPWDDIR)/gshadow
ADJUNCT    = $(YPPWDDIR)/passwd.adjunct
#ALIASES   = $(YPSRCDIR)/aliases  # could be in /etc/mail
ALIASES    = /etc/aliases
ETHERS     = $(YPSRCDIR)/ethers
BOOTPARAMS = $(YPSRCDIR)/bootparams
HOSTS      = $(YPSRCDIR)/hosts
NETWORKS   = $(YPSRCDIR)/networks
PRINTCAP   = $(YPSRCDIR)/printcap
PROTOCOLS  = $(YPSRCDIR)/protocols
PUBLICKEYS = $(YPSRCDIR)/publickey
RPC        = $(YPSRCDIR)/rpc
SERVICES   = $(YPSRCDIR)/services
NETGROUP   = $(YPSRCDIR)/netgroup
NETID      = $(YPSRCDIR)/netid
AMD_HOME   = $(YPSRCDIR)/amd.home
AUTO_MASTER= $(YPSRCDIR)/auto.master
AUTO_HOME  = $(YPSRCDIR)/auto.home
AUTO_LOCAL = $(YPSRCDIR)/auto.local
```

```
TIMEZONE    = $(YPSRCDIR)/timezone
LOCALE      = $(YPSRCDIR)/locale
NETMASKS    = $(YPSRCDIR)/netmasks
YPSERVERS   = $(YPDIR)/ypservers
```

اکنون می‌توانید فایل‌هایی را که مایلید از طریق سرویس NIS به اشتراک بگذارید، مشخص کنید. فایل‌هایی را که لیست آن‌ها را در ادامه مشاهده می‌کنید، فایل‌هایی هستند که به طور پیش‌فرض از طریق این سرویس به اشتراک گذاشته می‌شوند. در صورت تمایل می‌توانید برخی از آن‌ها را از لیست مزبور حذف کرده یا مواردی را به آن اضافه کنید: (با حذف علامت # از ابتدای هر یک از این خطوط می‌توانید فایل‌هایی را که اسامی آن‌ها در این خطوط ذکر شده‌اند به جمع فایل‌هایی که از طریق سرویس NIS به اشتراک گذاشته می‌شوند، اضافه کنید.)

```
all: passwd group hosts rpc services netid protocols mail \
  # netgrp shadow publickey networks ethers bootparams \
  # printcap amd.home auto.master auto.home auto.local \
  # passwd.adjunct timezone locale netmasks
```

بخش‌های دیگر فایل Makefile حاوی برنامه اسکریپت موردنیاز برای پردازش این تنظیمات است. از آن‌جا که بررسی کامل این برنامه در حوزه کتاب حاضر نیست، از بررسی آن‌ها صرف‌نظر می‌کنیم، با این توضیح که برنامه مزبور پاسخ‌گوی نیاز بسیاری از کاربران است.

تولید بانک اطلاعاتی Map

پس از تنظیم پارامترهای موجود در فایل پیکربندی /var/yp/Makefile وقت آن است تا سرور NIS را راه‌اندازی کنید. از آن‌جا که سرویس مزبور یکی از سرویس‌های استاندارد سیستم‌عامل Linux است، با اجرای این فرمان می‌توان برای راه‌اندازی آن اقدام کرد: `# service ypserv start`

> در صورتی که نام حوزه NIS سرور موردنظر قبلاً تعریف نشده باشد، برنامه ypserv قادر به راه‌اندازی سرویس NIS نخواهد بود. چنان‌چه در قسمت‌های قبل توضیح دادیم، به کمک فرمان domainname می‌توانید برای تعریف نام حوزه NIS اقدام کنید.

اکنون برای تولید بانک اطلاعاتی map کافی است فرمان /usr/lib/yp/ypinit -m را اجرا کنید. اجرای این فرمان به معنی اقدام برای پردازش فایل پیکربندی Makefile و تولید بانک اطلاعاتی map است. این بانک اطلاعاتی در فهرستی با عنوان */var/yp/domainname* که در آن متغیر *domainname* بیانگر نام حوزه NIS است، مستقر می‌شود. از آن‌جا که احتمالاً فهرست /usr/lib/yp در قالب متغیر سیستمی

PATH مشخص نشده است، برای اجرای برنامه ypinit لازم است موقعیت دقیق فهرست میزبان آن‌را ذکر کنید. (برای اطلاع بیشتر درباره این متغیر به فصل نهم مراجعه کنید.)

مطمئن شوید که سرویس NIS طی دفعات بعدی راه‌اندازی کامپیوتر میزبان به طور خودکار راه‌اندازی خواهد شد. برای این منظور فرمان chkconfig --level 345 ypserv on را اجرا کنید. با اجرای این فرمان، سرویس NIS طی دفعات بعدی راه‌اندازی کامپیوتر میزبان در سطوح اجرایی سوم، چهارم و پنجم راه‌اندازی خواهد شد.

پس از اجرای فرمان فوق باید اسامی کامپیوترهایی را که مایلید تا به عضویت در حوزه NIS موردنظر درآیند مشخص کنید. (در این مثال، عنوان RHL9 به کامپیوتر میزبان سرور NIS اشاره دارد. با وجود این، کامپیوتر میزبان این سرور ممکن است عنوانی شبیه به linux.example.com داشته باشد.) این اسامی در فایلی تحت عنوان /var/yp/ypservers قالب بندی می‌شوند. به این ترتیب، در صورت تمایل می‌توانید هریک از آن‌ها را به عنوان یک سرور NIS پشتیبان پیکربندی کنید:

```
# /usr/lib/yp/ypinit -m

At this point, we have to construct a list of the hosts which
will run NIS servers. RHL9 is in the list of NIS server
hosts. Please continue to add the names for the other hosts,
one per line. When you are done with the list, type
a <control D>
        next host to add: RHL9
        next host to add:
```

پس از تعیین اسامی کامپیوترهای عضو حوزه NIS باید لیست حاوی آن اسامی را تأیید کنید. برای تأیید این لیست کافی است حرف y را تایپ کنید. (در صورتی که حرف n را به نشانه عدم تأیید لیست مورد بحث تایپ کنید، برای تعیین لیست جدید باید مجدداً اقدام کنید.) با انجام این کار، فرمان ypinit فایل Makefile را مورد پردازش قرار داده و پیغام‌هایی شبیه به شکل ۲۸-۷ را در خروجی نمایش می‌دهد.

مشاهده پیغام failed to send 'clear' to local ypserv در این مرحله به معنای آن است که هنوز سرور NIS راه‌اندازی نشده است. برای راه‌اندازی این سرور فرمان service ypserv start # را اجرا کنید.

```
The current list of NIS servers looks like this:

RHL9
RHL9laptop

Is this correct?  [y/n: y]  y
We need a few minutes to build the databases...
Building /var/yp/nistest/ypservers...
Running /var/yp/Makefile...
gmake[1]: Entering directory `/var/yp/nistest'
Updating passwd.byname...
Updating passwd.byuid...
Updating group.byname...
Updating group.bygid...
Updating hosts.byname...
Updating hosts.byaddr...
Updating rpc.byname...
Updating rpc.bynumber...
Updating services.byname...
Updating services.byservicename...
Updating netid.byname...
Updating protocols.bynumber...
Updating protocols.byname...
Updating mail.aliases...
gmake[1]: Leaving directory `/var/yp/nistest'

RHL9 has been set up as a NIS master server.

Now you can run ypinit -s RHL9 on all slave server.
[root@RHL9 root]#
```

شکل ۷-۲۸ روند پردازش فایل پیکربندی Makefile توسط برنامه ypinit به منظور تولید بانک اطلاعاتی map

به‌روز رسانی بانک اطلاعاتی Map

برای به‌روز رسانی بانک اطلاعاتی map، فهرست جاری را به /var/yp تغییر داده و فرمان make را اجرا کنید. چنان‌که از فصل دوازدهم به خاطر دارید، این اقدام اغلب جهت پردازش فایلی با عنوان Makefile به منظورهای مختلف (از جمله آماده‌سازی بسته‌های نرم‌افزاری جهت نصب) انجام می‌شود. برای به‌روز رسانی بانک اطلاعاتی NIS نیز می‌توانید از همین روش استفاده کنید.

سرورهای NIS پشتیبان

در شبکه‌های بزرگ همواره استفاده از تجهیزات و سرویس‌های پشتیبان یک اقدام مفید تلقی می‌شود. سرورهای NIS پشتیبان، حاوی اطلاعاتی هستند که کامپیوترهای مستقر در شبکه ممکن است به

آن‌ها نیاز داشته باشند. برای پیکربندی یک سرور NIS پشتیبان لازم است تنظیماتی را هم روی کامپیوتر میزبان سرور NIS و هم روی کامپیوتر میزبان سرور NIS پشتیبان انجام دهید. در دو قسمت بعد نحوه انجام این کار را توضیح می‌دهیم.

پیکربندی کامپیوتر میزبان سرور NIS اصلی

پیش از هر اقدامی روی کامپیوتر میزبان سرور NIS اصلی، مطمئن شوید که اسامی هر دو کامپیوتر را در لیست کامپیوترهای عضو حوزه NIS (فایل /var/yp/ypservers) درج کرده‌اید. (در قسمت‌های قبل این کار را با اجرای فرمان /usr/lib/yp/ypinit -m انجام دادیم.)

سپس باید فایل پیکربندی /var/yp/Makefile را مورد ویرایش قرار داده و مقدار پارامتر NOPUSH را از true به false تغییر دهید تا به این ترتیب سرور NIS اصلی بتواند با اجرای فرمان yppush نسخه‌ای از بانک اطلاعاتی map را در اختیار سرور NIS پشتیبان قرار دهد.

علاوه بر این، لازم است سرویس انتقال بانک اطلاعاتی map از یک سرور NIS به سرور NIS دیگر با عنوان ypxfrd را نیز راه‌اندازی کنید. برای این منظور کافی است فرمان service ypxfrd start را اجرا کنید. برای اطمینان از این‌که طی دفعات بعدی راه‌اندازی کامپیوتر میزبان سرویس ypxfrd نیز به طور خودکار در سطوح اجرایی سوم، چهارم و پنجم راه‌اندازی خواهد شد، این فرمان را اجرا کنید:

```
# chkconfig --level 345 ypxfrd on
```

پیکربندی کامپیوتر میزبان سرور NIS پشتیبان

پس از آماده‌سازی سرور NIS اصلی، اکنون باید اقدامات لازم برای آماده‌سازی سرور NIS پشتیبان را انجام دهید. پیش از هر چیز باید مطمئن شوید که سرور NIS پشتیبان به عنوان کلاینت سرور NIS اصلی پیکربندی شده است. (برای اطلاع بیشتر در این زمینه به قسمت بعد مراجعه کنید.)

هم‌چنین مطمئن شوید که کامپیوتر میزبان سرور NIS پشتیبان، امکان برقراری ارتباط با سرور NIS اصلی را دارد. در صورتی که پیش از این نام حوزه NIS را روی کامپیوتر میزبان سرور NIS پشتیبان تنظیم کرده باشید، با اجرای فرمان ypbind امکان برقراری این ارتباط به خودی خود فراهم خواهد شد. علاوه بر این، دقت کنید که سرویس ypserv نیز باید راه‌اندازی شده باشد. برای بررسی این موضوع کافی است فرمان service ypserv status را اجرا کنید. سپس این فرمان را اجرا کنید: (عنوان RHL9 نام کامپیوتر میزبان سرور NIS اصلی است.)

```
# /usr/lib/yp/ypinit -s RHL9
```

در صورت اجرای موفقیت‌آمیز فرمان فوق پیغام‌های متعددی را مبنی بر انتقال فایل‌های پیکربندی از کامپیوتر میزبان سرور NIS اصلی به کامپیوتر میزبان سرور NIS پشتیبان مشاهده خواهید کرد. به نمونه‌ای از این پیغام‌ها توجه کنید:

```
Transfering passwd.byname...
Trying ypxfrd ... success
```

اما در صورتی که اجرای فرمان مزبور با اشکال مواجه شود، پیغام‌های دیگری را نیز علاوه بر پیغام انتقال فایل‌ها مشاهده خواهید کرد. (برای مشاهده پیغام‌های مربوط به اشکال‌زدایی می‌توانید فرمان ypbind -debug را نیز اجرا کنید.) تحت این شرایط، پس از بررسی اتصالات سخت‌افزاری شبکه و تنظیمات نرم‌افزاری مربوطه، پیکربندی سرور NIS اصلی را مورد بازبینی قرار دهید. هم‌چنین مطمئن شوید که در فایل پیکربندی Makefile از سرور مزبور عبارت نسبت‌دهی NOPUSH=false درج شده باشد. در پایان از راه‌اندازی سرویس‌های موردنیاز روی کامپیوتر میزبان سرور NIS پشتیبان اطمینان حاصل کنید.

به طور پیش‌فرض، سرور NIS جهت سرویس‌دهی از سرویس DNS استفاده نمی‌کند. از این‌رو، اطلاعات مربوط به سرور NIS اصلی دست کم باید در فایل /etc/hosts از کامپیوتر میزبان سرور NIS پشتیبان درج شده باشد.

نحوه استفاده کلاینت‌ها از سرویس NIS

پیکربندی کامپیوترهای کلاینت به منظور استفاده از سرویس NIS فرآیند ساده‌ای است. برای انجام این کار کافی است فایل پیکربندی /etc/yp.conf را مورد ویرایش قرار داده و سپس فرمان ypbind را اجرا کنید. در صورت تمایل می‌توانید با اجرای فرمان chkconfig --level 345 ypbind on ترتیبی دهید تا طی دفعات بعدی راه‌اندازی کامپیوتر سرویس ypbind در سطوح اجرایی سوم، چهارم و پنجم راه‌اندازی شده و بنابراین نقش آن به عنوان کلاینت سرویس NIS هم‌چنان حفظ شود.

به کمک تعدادی از فرامین "yp" (فرامینی که عناوین آن‌ها با yp آغاز می‌شود.) می‌توانید از صحت ارتباط میان کامپیوترهای میزبان برنامه‌های کلاینت و سرور NIS اطمینان حاصل کنید. هم‌چنین برای اطمینان از دسترسی کامپیوتر میزبان برنامه کلاینت NIS به فایل‌های بانک اطلاعاتی map باید فایل پیکربندی /etc/nsswitch.conf را مورد ویرایش قرار دهید.

فایل پیکربندی /etc/yp.conf

پیکربندی کامپیوتر میزبان برنامه کلاینت NIS از طریق ویرایش فایل /etc/yp.conf انجام می‌شود. چنان‌که این فایل را در یک ویرایشگر متنی باز کنید، این سه خط را مشاهده خواهید کرد:

```
domain NISDOMAIN server HOSTNAME
domain NISDOMAIN broadcast
ypserver HOSTNAME
```

اکنون باید متغیرهای *NISDOMAIN* و *HOSTNAME* را به ترتیب با نام حوزه NIS و نام کامپیوتر میزبان سرور NIS جایگزین کنید. هم‌چنین اگر پیش از این کامپیوتری را به عنوان سرور NIS پشتیبان پیکربندی کرده‌اید، لازم است این فرمان را در فایل /etc/yp.conf درج کنید:

```
domain NISDOMAIN server NISSLAVEHOSTNAME
```

نیازی به توضیح نیست که باید متغیر *NISSLAVEHOSTNAME* را با نام کامپیوتر میزبان سرور NIS پشتیبان جایگزین کنید. اکنون با اجرای فرمان service ypbind start برنامه کلاینت NIS را جهت بهره‌برداری از سرویس NIS راه‌اندازی کنید.

چنان‌چه برقراری ارتباط میان برنامه ypbind و سرور NIS موفقیت‌آمیز نباشد، ممکن است مکانیزم بازدارنده دیوار آتش مستقر روی کامپیوتر میزبان سرور NIS دسترسی برنامه کلاینت به سرور NIS را بلوکه کرده باشد. در این صورت تنظیمات مربوط به این مکانیزم را مورد بازبینی قرار دهید. مکانیزم بازدارنده شبکه‌ای که سرویس NIS روی آن پیکربندی شده است، عموماً تنها باید دسترسی‌های خارج از آن شبکه را بلوکه کند.

فرامین مربوط به برنامه کلاینت NIS

در ارتباط با برنامه کلاینت NIS فرامین متعددی موجود است که عناوین تمام آن‌ها با yp آغاز می‌شود. این فرامین به منظور تغییر کلمه عبور موردنیاز برای دسترسی به بانک اطلاعاتی map مستقر روی ماشین میزبان سرور NIS، اطمینان از صحت برقراری ارتباط میان برنامه‌های کلاینت و سرور NIS، دستیابی به فایل‌های بانک اطلاعاتی مزبور و سایر موارد دیگر پیش‌بینی شده‌اند. در قسمت‌های بعد به شرح این فرامین می‌پردازیم.

فرمان ypcat

این فرمان جهت دستیابی به فایل‌های بانک اطلاعاتی map مستقر روی کامپیوتر میزبان سرور NIS

پیش‌بینی شده است. مشابه فرمان cat در سیستم‌عامل Linux، این فرمان محتوای فایل موردنظر را نمایش می‌دهد. با وجود این، آن‌چه روی کامپیوتر میزبان برنامه کلاینت NIS به نمایش درمی‌آید، ممکن است تا اندازه‌ای با محتوای فایل مندرج روی کامپیوتر میزبان برنامه سرور NIS متفاوت باشد. برای مثال، به فرض آن‌که مقادیر هر دو پارامتر MINUID و MINGID از فایل پیکربندی Makefile برابر با 500 باشد، این فرمان اطلاعات مربوط به کاربرانی با شناسه کاربری 500 یا بزرگ‌تر از 500 را از فایل /etc/passwd بازیابی کرده و نمایش می‌دهد:

```
# ypcat passwd
```

فرمان ypchfn

این فرمان امکان تغییر برخی اطلاعات درج شده در بانک اطلاعاتی map را در اختیار می‌گذارد. مشابه فرمان chfn در سیستم‌عامل Linux، این فرمان اطلاعات مربوط به کاربر فعلی را ملاک قرار می‌دهد. با وجود این، کاربر اصلی (اصطلاحاً root) می‌تواند با اجرای فرمان *username* chfn اطلاعات مربوط به کاربر موردنظر را که در این‌جا شناسه وی با متغیر *username* مشخص شده است، تغییر دهد.

چنان‌که در فصل بیست و سوم توضیح داده شد، در فیلد پنجم از رکوردهای مندرج در فایل /etc/passwd می‌توان اطلاعاتی چون نام و شماره تلفن کاربران را وارد کرد.

با اجرای این فرمان اعلانی در مورد تغییر اطلاعات مربوط به کاربری با شناسه mj روی کامپیوتری با نام RHL9 که میزبان سرور NIS است، به نمایش درمی‌آید. این فرمان هم‌چنین راهنمایی‌های لازم به منظور دستیابی به اطلاعات این کاربر را در اختیار می‌گذارد:

```
# ypchfn mj
Changing NIS account information for mj on RHL9.
Please enter root password:

Changing full name for mj on RHL9.
To accept the default, simply press return. To enter an empty
field, type the word "none".
Name [Michael Jang]:
```

فرمان ypchsh

فرمان ypchsh *username* امکان تغییر سطر فرمان (اصطلاحاً shell) مربوط به کاربری با شناسه *username* را در اختیار قرار می‌دهد. این اطلاعات در فایل /etc/passwd از کامپیوتر میزبان سرور NIS درج می‌شود. عملکرد این فرمان شبیه به فرمان ypchfn است. با اجرای فرمان ypchsh ابتدا اعلانی

برای دریافت کلمه عبور کاربر اصلی کامپیوتر میزبان سرور NIS نمایش داده شده و سپس اعلان دیگری به منظور تغییر سطر فرمان به نمایش درمی‌آید.

فرمان ypmatch

فرمان ypmatch *username* passwd جهت دستیابی به رکورد کاربری با شناسه *username* در فایل /etc/passwd از کامپیوتر میزبان سرور NIS اصلی جستجویی را در بانک اطلاعاتی map ترتیب می‌دهد.

فرمان yppasswd

فرمان yppasswd *username* امکان تغییر کلمه عبور کاربری با شناسه *username* را روی ماشین میزبان سرور NIS در اختیار می‌گذارد. پس از این تغییر، کاربر موردنظر برای دستیابی به هریک از کامپیوترهای میزبان برنامه کلاینت NIS باید از کلمه عبور جدید استفاده کند. مشابه فرامین ypchfn و ypchsh پیش از نمایش اعلان مربوط به تغییر کلمه عبور کاربر مورد نظر، اعلانی برای ورود کلمه عبور کاربر اصلی (اصطلاحاً root) به نمایش درمی‌آید.

فرمان yppush

چنان‌چه بانک اطلاعاتی map مستقر روی کامپیوتر میزبان سرور NIS اصلی دستخوش تغییر شده باشد، این فرمان سرور مزبور را وادار می‌کند تا نسخه جدید بانک اطلاعاتی را برای تمام کامپیوترهایی که میزبانی سرورهای NIS پشتیبان را به عهده دارند، ارسال کند. لیست اسامی این کامپیوترها در فایل /var/yp/ypservers درج شده است.

پیکربندی فایل /etc/nsswitch.conf

در صورت وجود سرور NIS در شبکه باید مطمئن شوید که فایل /etc/nsswitch.conf از کامپیوتر میزبان برنامه کلاینت NIS برای دستیابی به هر یک از فایل‌های پیکربندی مستقر روی کامپیوتر میزبان سرور NIS اقدام می‌کند. فایل مزبور هم‌چنین ممکن است توجه کامپیوتر کلاینت را به منابع دیگری مانند فایل‌های پیکربندی محلی جلب کند.

برای مثال، در صورت عدم وجود سرور NIS در شبکه، محتوای فایل /etc/nsswitch.conf ممکن است حاوی فرامین ساده‌ای به این شکل باشد:

```
passwd: files
shadow: files
group:  files
```

```
hosts:  files dns
```

در هریک از این فرامین ترتیب جستجو مشخص می‌شود. به عنوان نمونه، آخرین فرمان بیانگر آن است که جستجوی فایل محلی /etc/hosts باید قبل از ارسال درخواست جستجو به سرور DNS موردنظر (با توجه به محتوای فایل /etc/host.conf) انجام شود. از طرف دیگر، چنان‌چه کامپیوتری از شبکه به عنوان سرور NIS پیکربندی شده باشد، باید وجود آن‌را در فایل /etc/nssswitch.conf منعکس کنید. برای مثال، خطوط زیر حاوی فرامینی است که جستجو در بانک اطلاعاتی map را نسبت به سایر منابع در اولویت قرار می‌دهد:

```
passwd: nis files
shadow: nis files
group:  nis files
```

بدیهی است که در خطوط فوق واژه دستورالعمل nis به سرور NIS مستقر در شبکه اشاره دارد. در صورت استفاده از NIS 3.x باید این دستورالعمل را به nisplus تغییر دهید.

چنان‌چه مایل به استفاده از بانک اطلاعاتی /etc/hosts مستقر روی کامپیوتر میزبان سرور NIS باشید، لازم است دستورالعمل مربوطه را در فایل پیکربندی /etc/host.conf درج کنید. برای مثال، این فرمان کامپیوتر میزبان را وادار می‌کند تا ابتدا بانک اطلاعاتی /etc/hosts مستقر روی کامپیوتر میزبان سرور NIS، سپس بانک اطلاعاتی محلی /etc/hosts و در نهایت سرورهای DNS را (با مراجعه به فایل /etc/resolv.conf) مورد جستجو قرار دهد:

```
order nis,hosts,bind
```

جمع‌بندی

سرویس استاندارد Network File Service یا به اختصار NFS جهت به اشتراک گذاشتن فایل‌های مستقر روی کامپیوترهای Linux و UNIX طراحی شده است. بهره‌برداری از این سرویس مستلزم اجرای چندین برنامه اسکریپت مستقر در فهرست /etc/rc.d/init.d شامل nfs، nfslock و portmap است. پیکربندی سرویس NFS از طریق مقداردهی پارامترهای موجود در فایل /etc/exports انجام می‌شود. فرمان exportfs نیز به منظور صدور فهرست‌های مشترک پیش‌بینی شده است. چنان‌چه مکانیزم بازدارنده دیوار آتش به واسطه برنامه iptables تأمین شده باشد، دسترسی به سرویس NFS را می‌توان از طریق پورت‌های TCP/IP شماره ۱۱۱ و ۲۰۴۹ محدود کرد. هم‌چنین، در صورت استفاده از مکانیزم کنترل دسترسی TCP Wrapper می‌توان امکان دسترسی به این سرویس را با ویرایش فایل‌های /etc/hosts.allow و /etc/hosts.deny محدود کرد.

پس از به اشتراک گذاشتن فهرست موردنظر از طریق سرویس NFS، با دسترسی به کامپیوتر میزبان برنامه کلاینت NFS می‌توان آن‌را روی سیستم فایل محلی سوار کرد. مشاهده لیست فهرست‌هایی که از طریق این سرویس به اشتراک گذاشته شده‌اند با اجرای فرمان showmount -e *NFSserver* امکان‌پذیر است. سوار کردن این فهرست‌ها روی سیستم فایل به سادگی سوار کردن یک فهرست محلی یا راه دور است. با درج یک فرمان مناسب در فایل /etc/fstab می‌توان از تلاش بیهوده کامپیوتر کلاینت در مواقعی که به دلایلی (از جمله نقص در شبکه) امکان دسترسی به سرویس NFS موجود نیست، جلوگیری به عمل آورد.

همان‌گونه که سرویس NFS امکان دسترسی مشترک به فایل‌های موردنظر را برای کامپیوترهای Linux و UNIX مستقر در شبکه فراهم می‌کند، سرویس دیگری با عنوان Network Information Service یا به اختصار NIS امکانات لازم جهت دسترسی مشترک به فایل‌های پیکربندی را در اختیار این کامپیوترها قرار می‌دهد. برای نمونه، به کمک این سرویس می‌توان اسامی کاربران و کلمات عبور آن‌ها را با تبدیل فایل‌های /etc/passwd و /etc/groups به یک بانک اطلاعاتی متمرکز روی سرور با عنوان map مستقر کرده و امکان دسترسی مشترک به آن‌را برای کاربران فراهم کرد. جهت بهره‌برداری از سرویس NIS تعریف نام حوزه ضروری است. لیست اسامی فایل‌های مشترک قابل دسترسی توسط کاربران در فایل پیکربندی /var/yp/Makefile مشخص می‌شود. پس از آماده‌سازی این فایل، با اجرای فرمان ypinit می‌توان بانک اطلاعاتی map را تولید کرد. علاوه بر این، با اجرای فرمان make از فهرست /var/yp می‌توان کلیه تغییرات اعمال شده به فایل /var/yp/Makefile را از زمان تولید آخرین نسخه از بانک اطلاعاتی map مورد پردازش قرار داده و به این ترتیب جهت به‌روز رسانی آن اقدام کرد. پیکربندی سرورهای NIS پشتیبان نیز با اجرای فرمان ypinit و به‌روز رسانی آن‌ها با اجرای فرمان yppush امکان‌پذیر است.

پیکربندی کامپیوترهای میزبان برنامه کلاینت NIS بسیار ساده است. فرمان ypbind ارتباط میان برنامه کلاینت NIS را با سرور NIS موردنظر برقرار می‌کند. پس از برقراری این ارتباط، با اجرای فرامین مناسب می‌توان بانک اطلاعاتی map را مورد دستیابی قرار داد. در نهایت، با پیکربندی مناسب فایل /etc/nsswitch.conf امکان دستیابی برنامه کلاینت NIS به بانک اطلاعاتی موردنظر از کامپیوتر میزبان سرور NIS فراهم می شود.

در فصل بعد که به بررسی سرویس Samba اختصاص دارد، نحوه دسترسی مشترک به فایل‌ها و فهرست‌ها را از کامپیوترهای UNIX ،Linux و Microsoft Windows مستقر در شبکه مورد بحث قرار خواهیم داد.

فصل بیست‌ونهم

استفاده از سرویس Samba

سرویس Samba امکانات موردنیاز به منظور استفاده از کامپیوترهای Linux را در شبکه‌هایی از نوع Microsoft Windows فراهم می‌کند. در این فصل نحوه پیکربندی کامپیوتری با سیستم‌عامل Linux را جهت میزبانی برنامه کلاینت و سرور Samba در شبکه‌ای از نوع Microsoft Windows بررسی خواهیم کرد.

کامپیوترهایی که نسخه‌ای از سیستم‌عامل Microsoft Windows را مورد استفاده قرار می‌دهند به خوبی می‌توانند از طریق پروتکل Server Message Block یا به اختصار SMB با یکدیگر ارتباط برقرار کنند. (از این پس برای اشاره به چنین کامپیوترهایی اصطلاح "کامپیوتر ویندوز" و به کامپیوترهایی که از سیستم‌عامل Linux استفاده می‌کنند "کامپیوتر Linux" را به کار خواهیم برد.) کامپیوترهای ویندوز به واسطه پروتکل Common Internet File System یا به اختصار CIFS قادر هستند در شبکه‌ای از نوع TCP/IP فایل‌ها را با یکدیگر به اشتراک گذاشته و از چاپگرهای موجود در شبکه به طور مشترک استفاده کنند. سرویس Samba به خوبی امکان برقراری ارتباط با پروتکل‌های SMB و CIFS را در اختیار کامپیوترهای Linux قرار می‌دهد.

با نصب و پیکربندی سرویس Samba در شبکه، کامپیوترهای ویندوز در تشخیص کامپیوترهای Linux دچار اشتباه شده و آن‌ها را نیز کامپیوتر ویندوز تلقی می‌کنند. مشابه سرویس CUPS که در فصل بیست و پنجم به بررسی آن پرداختیم، سرویس Samba نیز دارای مجموعه‌ای از ابزارهای پیکربندی تحت وب با عنوان SWAT است.

پس از نصب بسته‌های نرم‌افزاری موردنیاز سرویس Samba روی یک کامپیوتر Linux می‌توان آن کامپیوتر را به عنوان کلاینت یا سرور Samba پیکربندی کرده و از امکانات موجود جهت اشتراک فایل‌ها و چاپگرها استفاده کرد. کامپیوترهای کلاینت Samba در حالت متنی (اصطلاحاً text mode یا terminal mode) می‌توانند فهرست‌های مشترک واقع در شبکه ویندوز را مورد دستیابی قرار دهند.

فایل /etc/samba/smb.conf کلید اصلی برای پیکربندی سرویس Samba است. برخی از مدیران سیستم‌ها ترجیح می‌دهند به جای استفاده از ابزارهای پیکربندی SWAT تنظیمات موردنظر خود را از طریق یک ویرایشگر متنی انجام دهند. در این فصل با نحوه انجام این کار به منظور استفاده مشترک از

فهرست‌ها و چاپگرها آشنا خواهید شد. چنان‌که خواهید دید، اشکال‌یابی و اطمینان از صحت تنظیمات فایل پیکربندی smb.conf کار ساده‌ای است.

برای پیکربندی سرویس Samba در سیستم‌عامل Red Hat Linux دو ابزار با رابط گرافیکی پیش‌بینی شده است. ابزار نخست با عنوان SWAT یا Samba Web Administration Tool یک برنامه کاربردی تحت وب بوده و شامل مجموعه کاملی از امکانات پیکربندی سرویس Samba است. دسترسی به این برنامه از طریق پورت TCP/IP شماره ۹۰۱ امکان‌پذیر است. ابزار دیگر با عنوان redhat-cinfig-samba جهت تنظیمات اولیه سرور Samba و فهرست‌های مشترک طراحی شده است. موضوعات مورد بررسی در فصل حاضر به شرح زیر است:

- برقراری ارتباط میان کامپیوترهای ویندوز و Linux
- پیکربندی سرویس Samba روی کامپیوتر کلاینت
- فایل‌های پیکربندی سرویس Samba
- مدیریت کاربران سرویس Samba
- استفاده از ابزار پیکربندی SWAT
- استفاده از ابزار پیکربندی redhat-config-samba

برقراری ارتباط میان کامپیوترهای ویندوز و Linux

سرویس Samba به خوبی ارتباط میان کامپیوترهای ویندوز و Linux را برقرار می‌کند. این بدان معنی است که سرویس مزبور می‌تواند با هر دو سیستم‌عامل Microsoft Windows و Linux ارتباط برقرار کند. از این‌رو، بدیهی است که می‌توان سرویس Samba را جهت به اشتراک گذاشتن فهرست‌ها و چاپگرها در شبکه‌ای از نوع ویندوز مورد استفاده قرار داد.

امکان دستیابی به کامپیوترهای Linux در یک شبکه ویندوز

یکی از مزایای سرویس Samba این است که امکان پیکربندی کامپیوترهای Linux یا UNIX را در شبکه‌ای از نوع ویندوز فراهم می‌کند. در این صورت، کاربران شبکه مزبور به هیچ وجه احساس نمی‌کنند که در حال تعامل با کامپیوتری از نوع Linux هستند. به‌واسطه‌سرویس Samba، کامپیوترهای Linux مستقر در یک شبکه ویندوز را می‌توان برای این اهداف پیکربندی کرد:

- عضویت در یکی از گروه‌های کاری ویندوز

- عضویت در یکی از حوزه‌های ویندوز
- میزبانی Member Server
- کنترل کننده اصلی حوزه (اصطلاحاً Primary Domain Controller یا PDC)

ویرایش شماره 2.2.7 سرویس Samba (که به همراه سیستم‌عامل Red Hat Linux 9 توزیع می‌شود، امکان پیکربندی کامپیوترهای Linux را به عنوان کنترل کننده پشتیبان حوزه (اصطلاحاً Backup Domain Controller یا BDC) در اختیار قرار نمی‌دهد. با وجود این، دستیابی به چنین قابلیتی امکان‌پذیر است. (برای اطلاع بیشتر در این زمینه به بخش Samba BDC HOWTO از وب سایت http://www.samba.org مراجعه کنید.) توسعه دهندگان سرویس Samba در تلاش هستند تا این قابلیت را در قالب ویرایش شماره 3.0 پیاده‌سازی کنند.

سرویس Samba ابتدا بر اساس سیستم‌عامل Microsoft LAN Manager توسعه پیدا کرد. در چنین شبکه‌هایی کامپیوترهای کلاینت از پروتکلی با عنوان NetBIOS over TCP/IP یا به اختصار NBT جهت برقراری ارتباط با سرور استفاده می‌کردند. از این‌رو، نیازی به استفاده از پروتکل NetBEUI نبود. (برای اطلاع بیشتر درباره پروتکل‌های NetBIOS و NetBEUI به فصل بیستم مراجعه کنید.)

حقوق استفاده از سرویس Samba

استفاده از سرویس Samba مستلزم رعایت نکات ذکر شده در سند GPL است. بسته نرم‌افزاری Samba رایگان بوده و به همراه سیستم‌عامل‌های نوع UNIX از جمله Red Hat Linux توزیع می‌شود.

سرویس Samba امکانات لازم به منظور پیکربندی و استفاده از کامپیوترهای Linux را در شبکه‌های ویندوز فراهم می‌کند. به این ترتیب می‌توان تعداد کامپیوترهای ویندوز موردنیاز در شبکه را کاهش داد. تا زمان انتشار کتاب حاضر، لزومی ندارد که برای استفاده از سرویس Samba در شبکه‌های ویندوز مبلغی به شرکت مایکروسافت پرداخت کنید.

ظاهراً شرکت مایکروسافت به زودی قصد دارد استفاده مجانی از سرویس Samba جهت دسترسی به شبکه‌های ویندوز را متوقف کند. شکی نیست که بسیاری از شرکت‌ها با این اقدام مخالف هستند. با این همه، به نظر می‌رسد که اگر این شرکت‌ها از توسعه‌دهندگان Samba پشتیبانی به عمل بیاورند، اقدام فوق برای چند سالی به تعویق بیفتد. تا آن زمان، به واسطه پیشرفت فناوری احتمالاً امکان استفاده از ابزارهای دیگری برای این منظور فراهم خواهد شد.

تعاریف

در این فصل با اصطلاحاتی سروکار داریم که یا صرفاً به سرویس Samba مربوط می‌شوند یا این‌که علاوه بر آن در موضوعات مربوط به شبکه‌های ویندوز نیز مورد استفاده قرار می‌گیرند. از این‌رو پیش از پرداختن به ادامه بحث اجازه دهید تا تعاریف هریک از آن‌ها را باهم مرور کنیم:

- **کنترل کننده اصلی حوزه (Primary Domain Controller یا PDC)**: این اصطلاح به کامپیوتری اشاره دارد که میزبان بانک اطلاعاتی حاوی اسامی کاربران و کلمات عبور شبکه است. چنین کامپیوتری اغلب میزبان یک بانک اطلاعاتی متمرکز حاوی پروفایل‌های کاربران در شبکه‌های ویندوز است.
- **کنترل کننده پشتیبان حوزه (Backup Domain Controller یا BDC)**: این اصطلاح به کامپیوتری اشاره دارد که یک نسخه پشتیبان از بانک اطلاعاتی مستقر در کامپیوتر PDC روی آن نگهداری می‌شود. هر دو مفهوم PDC و BDS در حوزه شبکه‌های ویندوز مورد استفاده قرار می‌گیرند.
- **لیست منابع مشترک (Browse List)**: این اصطلاح به لیست منابع مشترک مستقر در شبکه اشاره دارد.
- **کامپیوتر میزبان لیست منابع مشترک (Browse Master)**: این اصطلاح به کامپیوتری اشاره دارد که لیست منابع مشترک مستقر در شبکه روی آن نگهداری می‌شود.
- **حوزه (Domain)**: این اصطلاح به شبکه‌ای با یک بانک اطلاعاتی متمرکز که حداقل شامل اسامی کاربران و کلمات عبور آن‌هاست، اشاره دارد. این مفهوم کاملاً با مفهوم اسامی حوزه‌های اینترنتی (اصطلاحاً Internet Domain Names) متفاوت است.
- **کامپیوتر میزبان Member Server**: این اصطلاح به کامپیوتری از یک شبکه ویندوز اطلاق می‌شود که وظیفه به اشتراک گذاشتن فهرست‌ها و چاپگرها را به عهده دارد. چنین کامپیوتری نه یک PDC و نه یک BDC است.
- **نظیر به نظیر (Peer-to-Peer)**: این اصطلاح به گروهی از کامپیوترهای مستقر در یک شبکه محلی اطلاق می‌شود که می‌توانند عملکردی به عنوان سرور داشته باشند. این مفهوم در ارتباط با مفهوم گروه کاری مورد استفاده قرار می‌گیرد.
- **سرور**: این اصطلاح به کامپیوتری اطلاق می‌شود که فهرست‌ها و چاپگرها را مابین کاربران شبکه به اشتراک می‌گذارد.

- **منبع مشترک (Share)**: این اصطلاح به فهرست یا چاپگری اطلاق می‌شود که به طور مشترک در اختیار کاربران شبکه قرار داد.
- **گروه کاری (Workgroup)**: این اصطلاح به نوعی شبکه محلی اشاره دارد که فاقد یک سرور مشخص باشد. در چنین شبکه‌ای نگهداری از اسامی کاربران و کلمات عبور هریک از کامپیوترها به عهده خود آنهاست. کاربران این گونه شبکه‌ها معمولاً برخی از فهرست‌ها و چاپگرهای خود را با سایر اعضای آن شبکه به اشتراک می‌گذارند.

در این فصل از اصطلاح "سرور مایکروسافت" جهت اشاره به یک کامپیوتر ویندوز که جهت به اشتراک گذاشتن فهرست‌ها یا چاپگرها پیکربندی شده است، استفاده خواهیم کرد. به طور مشابه، برای اشاره به یک کامپیوتر Linux که جهت به اشتراک گذاشتن فهرست‌ها یا چاپگرها پیکربندی شده است از اصطلاح "سرور Samba" استفاده خواهیم کرد.

بسته‌های نرم‌افزاری موردنیاز برای بهره‌برداری از سرویس Samba

برای استفاده از سرویس Samba پنج بسته نرم‌افزاری به شرحی که در جدول ۱-۲۹ آمده پیش‌بینی شده است. اگر مایلید تا کامپیوتر Linux را تنها به عنوان کلاینت در شبکه‌ای از نوع ویندوز مورد استفاده قرار دهید، کافی است دو بسته نرم‌افزاری samba-client-* و samba-common-* را روی آن کامپیوتر نصب کنید. نصب سه بسته نرم‌افزاری دیگر تنها در صورتی ضروری است که بخواهید از کامپیوتر Linux به عنوان سرور شبکه‌ای از نوع ویندوز استفاده کنید.

جدول ۱-۲۹ شرح بسته‌های نرم‌افزاری موردنیاز برای استفاده از سرویس Samba

عنوان بسته نرم‌افزاری	توضیح
samba-*	این بسته نرم‌افزاری حاوی فایل‌های موردنیاز برای نصب برنامه سرور Smaba و فرامینی برای تطبیق اسامی کاربران و کلمات عبور در دو کامپیوتر ویندوز و Linux است.
samba-client-*	این بسته نرم‌افزاری حاوی فایل‌هایی است که امکان دسترسی به فایل‌های مشترک مستقر روی کامپیوترهای ویندوز و ارسال وظایف چاپی روی چاپگرهای متصل به آن کامپیوترها را در اختیار کامپیوتر Linux قرار می‌دهد.
samba-common-*	این بسته نرم‌افزاری حاوی فایل‌های موردنیاز برای پیکربندی کامپیوتر Linux به عنوان کلاینت یا سرور Samba است.

عنوان بسته نرم‌افزاری	توضیح
samba-swat-*	این بسته نرم‌افزاری حاوی ابزارهای گرافیکی موردنیاز به منظور تغییر تنظیمات فایل‌های پیکربندی سرویس Samba به ویژه فایل smb.conf است. برنامه redhat-config-samba امکانات مشابهی را هر چند به صورت محدودتر در اختیار قرار می‌دهد.
redhat-config-samba-*	این بسته نرم‌افزاری حاوی ابزارهایی برای پیکربندی سرویس Samba است. کار با این ابزارها ساده‌تر از ابزارهای SWAT بوده اما امکانات و کنترل کمتری را برای این منظور در اختیار قرار می‌دهد.

پیکربندی برنامه Samba به عنوان کلاینت

پس از نصب بسته‌های نرم‌افزاری samba-client-* و samba-common-* روی کامپیوتر Linux می‌توان فهرست‌ها و چاپگرهایی را که از جانب کامپیوترهای ویندوز مستقر در شبکه به اشتراک گذاشته‌اند، مورد دستیابی قرار داد. دستیابی به این فهرست‌های مشترک را می‌توانید به دو شیوه انجام دهید. در شیوه نخست باید فهرست مشترک موردنظر را روی سیستم فایل کامپیوتر Linux سوار کنید. شیوه دیگر این است که فهرست مشترک را از طریق ترمینال کامپیوتر Linux مورد دستیابی قرار دهید. (این روش به نحوه برقراری ارتباط برنامه کلاینت FTP با سرور مربوطه شباهت دارد.) علاوه بر فهرست‌های مشترک باید با نحوه دستیابی به چاپگرهای مشترک نیز آشنا باشید.

دستیابی به فهرست‌های مشترک

به سادگی می‌توان لیست فهرست‌های مشترک موجود در یک شبکه ویندوز را از طریق یک سرور مایکروسافت مشاهده کرد. چنان‌که شکل ۱-۲۹ نشان می‌دهد، کافی است فرمان smbclient را به همراه نام یا آدرس IP سرور موردنظر اجرا کنید. ظاهر این فرمان تا اندازه‌ای نامتعارف است. (به وجود علامت \\ قبل از عنوان کامپیوتر موردنظر توجه کنید.)

با دقت در نتایج حاصل اجرای فرمان smbclient در شکل مذکور می‌توان فهرست‌های مشترک جالب توجهی را تشخیص داد. چنان‌چه مجوزهای دسترسی روی سرور مایکروسافت به خوبی تنظیم شده باشند، به آسانی می‌توان هر یک از این فهرست‌های مشترک را روی سیستم فایل کامپیوتر Linux سوار کرد. برای مثال، با اجرای این فرمان فهرست مشترکی با عنوان Download از کامپیوتری با نام laptop2 روی فهرست /root/downloads از کامپیوتر Linux سوار می‌شود: (البته انجام این کار مستلزم وارد کردن کلمه عبور است.)

```
[root@RH9Test root]# smbclient -L \\laptop2
added interface ip=10.252.113.63 bcast=10.252.113.255 nmask=255.255.255.0
Password:
Domain=[WORKGROUP] OS=[Windows 5.1] Server=[Windows 2000 LAN Manager]

        Sharename       Type      Comment
        ---------       ----      -------
        IPC$            IPC       Remote IPC
        D$              Disk      Default share
        SharedDocs      Disk
        print$          Disk      Printer Drivers
        ftproot         Disk
        Downloads       Disk
        HPLaserJ        Printer   Comment Test
        Temp            Disk
        RedHat          Disk
        OEDboot         Disk
        ADMIN$          Disk      Remote Admin
        C$              Disk      Default share
        Proposals       Disk
        ml3             Disk
        RedHatOld       Disk

        Server               Comment
        ---------            -------

        Workgroup            Master
        ---------            -------
[root@RH9Test root]#
```

شکل ۱-۲۹ مشاهده فهرست‌های مشترک از طریق یک سرور مایکروسافت مستقر در شبکه‌ای از نوع ویندوز

```
# mount '//laptop2/downloads' /root/downloads
Password:
```

فرمان mount در واقع رابطی برای اجرای فرمان mount.smbfs است که به واسطه نصب بسته نرم‌افزاری samba-client-* روی کامپیوتر Linux اکنون قابل استفاده است.

در اجرای فرمان mount می‌توان با استفاده از سوییچ t- smbfs- نوع سیستم فایل را نیز مشخص کرد. از آن‌جا که فرمان mount منجر به اجرای فرمان mount.smbfs می‌شود، نیازی به این کار نیست.

چنان‌که در فرمان فوق مشاهده می‌کنید، اشاره‌ای به شناسه کاربری نشده است. از این‌رو، شکل فوق از فرمان mount تنها مناسب گروه‌های کاری است. (اعضای این گونه گروه‌ها معمولاً فهرست‌هایی را به طور مشترک مورد استفاده قرار می‌دهند.) به بیان دیگر، فرمان مورد بحث فهرست مشترکی از یک کامپیوتر ویندوز 95، 98 یا ME یا عموماً فهرست مشترکی از یک کامپیوتر ویندوز را که بتوان با شناسه کاربری Everyone به آن دسترسی داشت، مورد دستیابی قرار می‌دهد. کلمه عبور موردنیاز برای

دستیابی به فهرست مشترک موردنظر ضروری است. (کامپیوترهای ویندوز NT، 2000 و XP را می‌توان به این شیوه پیکربندی کرد.)

با وجود این، در اغلب شبکه‌ها محدودیت‌هایی جهت دسترسی به منابع مشترک وجود دارد. برای مثال، در مورد سرورهای مایکروسافت می‌توان امکان دسترسی به این منابع را تنها در اختیار کاربران یا گروه‌های خاصی قرار داد. تحت چنین شرایطی، ضمن برخورداری از شناسه کاربری و کلمه عبور معتبر باید مجوز دسترسی به فهرست موردنظر را نیز در اختیار داشته باشید. گزینه o- از فرمان mount امکان تعیین شناسه کاربری، کلمه عبور و اطلاعات موردنیاز دیگر را در اختیار قرار می‌دهد. با این همه بهتر است هنگام استفاده از گزینه مزبور تنها شناسه کاربری را وارد کنید تا به این ترتیب از ارسال کلمه عبور در قالب متن ساده خودداری کرده باشید. در این صورت اعلان کلمه عبور را پس از اجرای فرمان mount مشاهده خواهید کرد: (کلمه عبور وارد شده در مقابل این اعلان به صورت رمزگذاری شده ارسال می‌شود.)

```
# mount -o username=michael '//laptop2/downloads' /root/downloads
Password:
```

علاوه بر این، در صورت تمایل می‌توانید سطوح دسترسی کاربران را نیز مشخص کنید. برای مثال، می‌توانید ترتیبی دهید تا کاربران برخوردار از شناسه کاربری و کلمه عبور معتبر از امکان دسترسی به فهرست‌های مشترک جهت خواندن و نوشتن و در مقابل کاربران میهمان تنها از امکان خواندن آن‌ها برخوردار باشند.

بحث مربوط به محافظت از فهرست‌های مشترک در شبکه‌های ویندوز از حوزه این کتاب خارج است. جدول ۲-۲۹ برخی از پارامترهای گزینه o- از فرمان mount را شرح می‌دهد.

جدول ۲-۲۹ شرح برخی از پارامترهای گزینه o- از فرمان mount

عنوان پارامتر	توضیح
username=*winuser*	این پارامتر امکان تعیین یک شناسه کاربری معتبر در شبکه ویندوز را که در این‌جا با متغیر *winuser* مشخص شده است، فراهم می‌کند.
password=*winpass*	این پارامتر امکان تعیین کلمه عبور مربوط به یک شناسه کاربری معتبر در شبکه ویندوز را که در این‌جا با متغیر *winpass* مشخص شده است، فراهم می‌کند. چنان‌چه در اجرای فرمان mount تنها شناسه کاربری تعیین شده باشد، اعلان مربوط به دریافت کلمه عبور به طور خودکار نمایش داده خواهد شد.

عنوان پارامتر	توضیح

credentials=*file*	این پارامتر امکان بازخوانی یک شناسه کاربر معتبر در شبکه ویندوز و کلمه عبور مربوطه را از فایلی که در این‌جا با متغیر *file* مشخص شده است، فراهم می‌کند. این فایل ممکن است یک‌فایل‌حفاظت شده توسط سیستم‌عامل (مانند فایل /etc/shadow) باشد. استفاده از این روش جهت سوار کردن فهرست‌های مشترک به طور خودکار روی سیستم فایل کامپیوتر Linux مفید است. برای این منظور کافی است فرمان مربوطه را در فایل /etc/fstab که ضمن فرآیند راه‌اندازی کامپیوتر Linux مورد بازخوانی قرار می‌گیرد، وارد کنید. الگوی عمومی جهت تعیین شناسه کاربری و کلمه عبور به این صورت است:
	`username=winuser`
	`password=winpass`

uid=*linuser*	این پارامتر امکان تعیین مالکیت فهرست‌های مشترکی را که روی سیستم فایل کامپیوتر Linux سوار شده‌اند، فراهم می‌کند. متغیر *linuser* بیانگر شناسه کاربری یا شماره شناسایی کاربری است که مالکیت فهرست‌های مشترک در اختیار وی قرار می‌گیرد.
workgroup=*winwork*	این پارامتر امکان تعیین گروه کاری میزبان فهرست مشترک را که در این‌جا با متغیر *winwork* مشخص شده است، فراهم می‌کند.

در مباحث فوق فرض بر این است که نام یا آدرس IP سرور ویندوز در سرور DNS به ثبت رسیده یا در در فایل /etc/hosts درج شده است.

دسترسی به فهرست مشترک از طریق سطر فرمان کامپیوتر Linux

مشابه دسترسی به فایل‌های موردنظر از سرور FTP، با در دست داشتن نام کامپیوتر ویندوز میزبان فهرست‌های مشترک و عنوان فهرست مشترک موردنظر می‌توانید برای دسترسی به آن اقدام کنید. پس از برقراری ارتباط با کامپیوتر ویندوز، امکان بارگذاری روی کامپیوتر ویندوز یا از روی آن به سادگی فراهم می‌شود. شکل ۲-۲۹ فرآیند دسترسی به یک کامپیوتر ویندوز با عنوان laptop2 و تغییر فهرست جاری به فهرست Other Stuff و نتیجه اجرای فرامین dir و help را نمایش می‌دهد. به نحوه استفاده از جفت علامت "" برای تعیین فهرستی از کامپیوتر ویندوز که عنوان آن شامل دو کلمه مجزای Other و Stuff است، توجه کنید.

```
[root@RH9Test root]# smbclient //laptop2/ml3 -U michael
added interface ip=10.252.113.63 bcast=10.252.113.255 nmask=255.255.255.0
Password:
Domain=[WORKGROUP] OS=[Windows 5.1] Server=[Windows 2000 LAN Manager]
smb: \> cd "Other Stuff"
smb: \Other Stuff\> dir
  .                                   D        0  Wed Apr  2 19:05:15 2003
  ..                                  D        0  Wed Apr  2 19:05:15 2003
  4179CoverCopy.doc                   A    24064  Tue Mar 11 09:57:36 2003
  4179CoverCopy_mj.doc                A    26624  Tue Mar 11 10:15:36 2003
  4179CoverCopy_mja.doc               A    28672  Tue Mar 11 13:57:46 2003
  4179EP1.doc                         A    52224  Mon Mar 31 16:09:49 2003
  4179EP4.doc                         A    51712  Mon Mar 31 16:09:08 2003

                45778 blocks of size 524288. 28963 blocks available
smb: \Other Stuff\> help
?              altname        archive        blocksize      cancel
cd             chmod          chown          del            dir
du             exit           get            help           history
lcd            link           lowercase      ls             mask
md             mget           mkdir          more           mput
newer          open           print          printmode      prompt
put            pwd            q              queue          quit
rd             recurse        rename         rm             rmdir
setmode        symlink        tar            tarmode        translate
!
smb: \Other Stuff\>
```

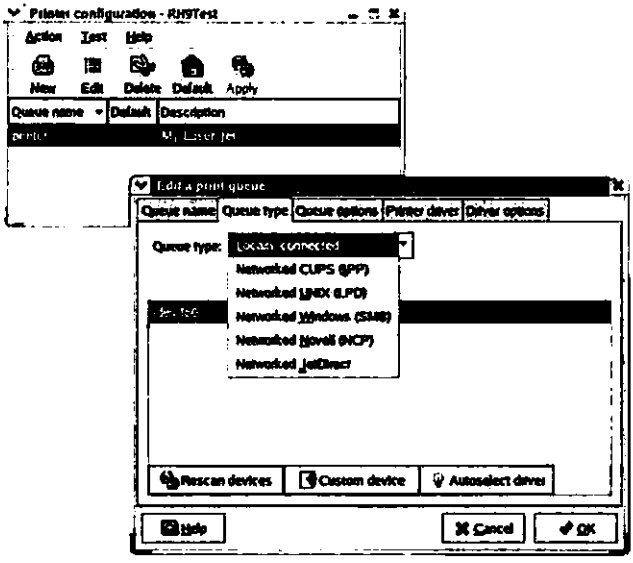
شکل ۲-۲۹ دسترسی به کامپیوتر ویندوز موردنظر با اجرای فرمان smbclient

هم‌چنین به لیست فرامین قابل استفاده توجه کنید. برخی از آن‌ها را در فصل بیست و هفتم نیز مشاهده کردید. نکته قابل ذکر دیگر این‌که سرویس Samba به واسطه مکانیزم امنیتی قفس chroot از دسترسی به فهرست ریشه جلوگیری به عمل می‌آورد.

دسترسی به چاپگر مشترک

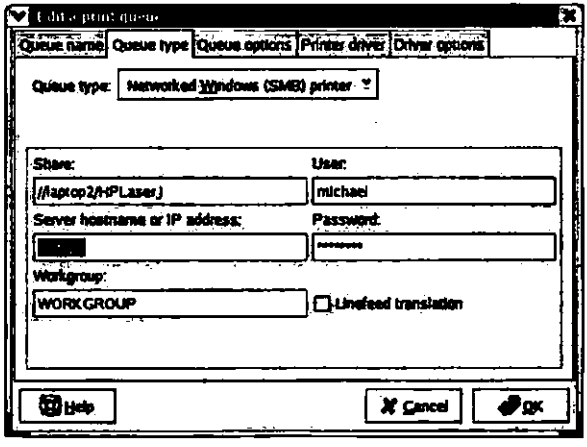
به واسطه سرویس Samba، دسترسی به چاپگرهای مستقر در شبکه ویندوز از طریق کامپیوترهای Linux به فرآیند ساده‌ای تبدیل شده است، به طوری که کافی است چاپگر موردنظر خود را از کادر محاوره‌ای Queue Type که با اجرای برنامه redhat-config-printer در اختیار قرار می‌گیرد، انتخاب کنید. (برای اطلاع بیشتر به فصل بیست و پنجم مراجعه کنید.)

اما این روش همیشه کارساز نیست. برای مثال، به دلایلی ممکن است امکان انتخاب چاپگر موردنظر مقدور نبوده یا عنوان آن در لیست عناوین چاپگرهای مستقر در شبکه موجود نباشد. در چنین مواردی بهتر است با اجرای برنامه redhat-config-printer برای پیکربندی یک چاپگر محلی اقدام کرده و تنظیمات آن‌را به هنگام مقتضی تغییر دهید. شکل ۳-۲۹ مراحل نخست این اقدام را نشان می‌دهد.



شکل ۳-۲۹ پیکربندی یک چاپگر محلی با استفاده از امکانات برنامه redhat-config-printer

تغییر پیکربندی چنین چاپگری به عنوان یک چاپگر راه دور نیز فرآیند ساده‌ای است. برای این منظور ابتدا گزینه Networked Windows (SMB) printer را از لیست Queue Type واقع در کادر محاوره‌ای Edit A Printer Queue انتخاب کنید. شکل ۴-۲۳ قالب پارامترهایی را که باید در این کادر محاوره‌ای وارد کنید، نشان می‌دهد. شرح مقادیر این پارامترها در جدول ۳-۲۹ آمده است.



شکل ۴-۲۹ نحوه مقداردهی پارامترهای موجود در بخش Queue Type از کادر محاوره‌ای Edit A Printer Queue به منظور پیکربندی چاپگر Samba

جدول ۳-۲۹ شرح مقادیر پارامترهای مربوط به پیکربندی چاپگر Samba

عنوان پارامتر	توضیح
Share	مقدار این پارامتر عنوان چاپگر مشترک را در قالب عمومی *//servername/printername* مشخص می‌کند.
Server Name Or IP Address	مقدار این پارامتر نام یا آدرس IP کامپیوتری را مشخص می‌کند که چاپگر موردنظر را به اشتراک گذاشته است.
Workgroup	مقدار این پارامتر نام گروه کاری میزبان کامپیوتری را مشخص می‌کند که چاپگر موردنظر را به اشتراک گذاشته است. مقداردهی این پارامتر تنها در صورتی ضروری است که کامپیوتر مزبور در یک گروهی کاری مستقر باشد.
User	مقدار این پارامتر شناسه کاربری معتبری را جهت دستیابی به کامپیوتری که چاپگر موردنظر را به اشتراک گذاشته است، مشخص می‌کند.
Password	مقدار این پارامتر کلمه عبور مربوط به شناسه کاربری مورد استفاده به عنوان مقدار پارامتر User را مشخص می کند.

فایل‌های پیکربندی سرویس Samba

سرویس Samba دارای سه فایل پیکربندی است که همگی در فهرست /etc/samba مستقر شده‌اند. دو فایل پیکربندی lmhosts و smbusers ساختار ساده‌ای دارند. در این قسمت ساختار، فایل smb.conf را به عنوان فایل پیکربندی اصلی سرویس Samba مورد بررسی قرار می‌دهیم.

فهرست /etc/smba ممکن است حاوی فایل دیگری با عنوان secrets.tdb نیز باشد. این فایل در صورت وجود شامل کد امنیتی (اصطلاحاً Security Identifier یا SID) مورد استفاده کامپیوتر Linux در شبکه ویندوز است.

پیش از هر اقدامی بهتر است از هر سه فایل مذکور یک نسخه پشتیبان تهیه کرده و در فهرست دیگری ذخیره کنید. به این ترتیب، در صورت لزوم می‌توانید آن‌ها را بدون نصب مجدد بسته‌های نرم‌افزاری مربوطه بازیابی کنید.

فایل smb.conf شامل توضیحات مفصلی راجع به نحوه پیکربندی سرویس Smaba است. اگر در انجام این کار تجربه ندارید، به این سه دلیل توصیه می‌کنیم از فایل مزبور یک نسخه پشتیبان تهیه کرده و آن‌را در فهرست دیگری نگهداری کنید:

- توضیحات مندرج در فایل پیکربندی smb.conf برای یادگیری بیشتر درباره سرویس Samba بسیار مناسب است.
- پیکربندی سرویس Samba به واسطه ابزارهایی چون SWAT و redhat-config-samba در مواردی موجب حذف توضیحات مندرج در فایل smb.conf می‌شود.
- پیکربندی سرویس Samba به واسطه ابزارهایی چون SWAT و redhat-config-samba در مواردی موجب حذف تنظیمات پیش‌فرض مانند workgroup=WORKGROUP از فایل smb.conf می‌شود.

برنامه‌های شبح موردنیاز برای راه‌اندازی سرویس Samba

سرویس Samba دارای دو برنامه شبح با عناوین smbd و nmbd است. پس از پیکربندی این سرویس بدیهی است که باید آن‌را راه‌اندازی کنید. چنان‌چه تغییراتی در فایل اصلی پیکربندی سرویس Samba یعنی /etc/samba/smb.conf داده باشید، لازم است با اجرای فرمان service smb reload فایل مزبور را مجدداً بارگذاری کنید. در صورتی که این تغییرات قابل توجه باشد، بهتر است هر دو برنامه smbd و nmbd را مجدداً راه‌اندازی کنید. برای این منظور، کافی است این فرمان را اجرا کنید:

```
# start smb restart
```

سایر فایل‌های پیکربندی سرویس Samba

چنان‌که قبلاً نیز اشاره شد، دو فایل پیکربندی lmhosts و smbusers دارای ساختار ساده‌ای هستند. فایل‌های دیگری نیز ممکن است ضمن پیکربندی سرویس Samba به جمع این فایل‌ها اضافه شود. در این قسمت به بررسی دو فایل مذکور می‌پردازیم.

فایل پیکربندی /etc/samba/lmhosts

مشابه فایل پیکربندی /etc/hosts، فایل پیکربندی /etc/samba/lmhosts نیز یک بانک اطلاعاتی از آدرس‌های IP و اسامی NetBIOS است. اسامی NetBIOS عناوینی برای شناسایی کامپیوترهای ویندوز در شبکه هستند. تعداد کاراکترهای هریک از این اسامی به ۱۵ عدد محدود شده است. نسخه اصلی فایل پیکربندی lmhosts تنها حاوی این خط است: (در سیستم‌عامل ویندوز نیز از عنوان localhost جهت اشاره به کامپیوتر میزبان استفاده می‌شود.)

```
127.0.0.1 localhost
```

فایل پیکربندی /etc/samba/smbusers

فایل پیکربندی /etc/samba/smbusers یک بانک اطلاعاتی از اسامی کاربران کامپیوترهای ویندوز و Linux است. نسخه اصلی فایل مزبور تنها شامل این دو خط است:

```
root = administrator admin
nobody = guest pcguest smbguest
```

به بیان دیگر، کاربر اصلی کامپیوتر Linux (اصطلاحاً root) در کامپیوتر ویندوز با عناوین admin و administrator شناخته می‌شود. هم‌چنین کاربری با شناسه nobody در کامپیوتر Linux با عناوین guest، pcguest و smbguest در کامپیوتر ویندوز شناسایی می‌شود.

با استفاده از فرمان smbadduser می‌توان خطوط مشابه دیگری را نیز برای سایر شناسه‌ها در این فایل درج کرد. برای مثال، فرض کنید کاربری با شناسه jp از کامپیوتر Linux و کاربر دیگری با شناسه Jean-Paul از کامپیوتر ویندوز را در شبکه‌ای از نوع ویندوز در نظر بگیرید. به واسطه اقداماتی که در شکل ۵-۲۹ مشاهده می‌کنید، کاربر jp می‌تواند فایل‌های موجود در کامپیوتر کاربر Jean-Paul را مورد دستیابی قرار دهد.

```
[root@RH9Test root]# smbadduser jp:Jean-Paul
Adding: jp to /etc/samba/smbpasswd
Added user jp.
Adding: (jp = Jean-Paul) to /etc/samba/smbusers
------------------------------------------------------------
ENTER password for jp
New SMB password:
Retype new SMB password:
Password changed for user jp.
Password changed for user jp.
[root@RH9Test root]#
```

شکل ۵-۲۹ روند تعریف یک کاربر جدید در فایل پیکربندی /etc/samba/smbusers

فرامینی را که در شکل فوق مشاهده می‌کنید منجر به درج این خط ساده در فایل پیکربندی /etc/samba/smbusers می‌شود:

```
jp = Jean-Paul
```

با وجود این، مادامی که این خط را در فایل پیکربندی smb.conf فعال نکرده باشید، کلیه تنظیمات فایل پیکربندی /etc/samba/smbusers بی‌تأثیر خواهد بود:

```
; username map = /etc/samba/smbusers
```

دقت کنید که استفاده از هر دو علامت # و ; جهت درج توضیحات در فایل‌های پیکربندی سرویس Samba مجاز است. جهت فعال کردن خط مورد بحث، فایل پیکربندی /etc/samba/smbusers.conf را در یک ویرایشگر متنی باز کرده و سپس علامت ; را از ابتدای آن خط حذف کنید. تعدادی از خطوط مندرج در فایل smb.conf با علامت ; آغاز می‌شود. در ادامه فصل حاضر جزییات این فایل پیکربندی را مورد بررسی قرار داده و تأثیر فعال کردن خطوطی از آن‌را که به واسطه درج علامت ; در ابتدای آن‌ها بی‌تأثیر شده‌اند، توضیح می‌دهیم.

در صورت تعریف کاربران جدید در فایل پیکربندی /etc/samba/smbusers، فایل دیگری با عنوان smbpasswd در فهرست /etc/samba ایجاد می‌شود. این فایل حاوی نسخه رمزگذاری شده کلمات عبور آن دسته از کاربران کامپیوترهای ویندوز خواهد بود که شناسه کاربری آن‌ها در فایل پیکربندی مذکور درج شده است.

فایل پیکربندی smb.conf

فایل اصلی پیکربندی سرویس Samba با عنوان /etc/samba/smb.conf حاوی توضیحات ارزنده‌ای است. همین توضیحات فایل نامبرده را به یک منبع اطلاعاتی غنی درباره سرویس Samba تبدیل کرده است. با وجود این، برخی از این توضیحات ممکن است برای مبتدیان مبهم باشد. اگر تاکنون برای تهیه نسخه پشتیبان از این فایل اقدام نکرده‌اید، بی‌درنگ یک نسخه پشتیبان از آن تهیه کرده و در فهرست دیگری ذخیره کنید.

اگر سرویس Samba را قبلاً پیکربندی کرده‌اید، ممکن است برخی از توضیحات مندرج در فایل پیکربندی smb.conf را از دست داده باشید. جبران این موضوع بسیار ساده است. ابتدا یک کپی از نسخه فعلی فایل smb.conf را به عنوان پشتیبان در فهرستی ذخیره کرده و سپس آن‌را از فهرست /etc/samba حذف کنید. سپس با اجرای فرمان rpm -Uvh --force samba-common-* بسته نرم‌افزاری samba-common-* را مجدداً نصب کنید تا نسخه پیش‌فرض فایل پیکربندی smb.conf در فهرست /etc/samba مستقر شود. فراموش نکنید که پس از انجام تمرینات موردنظر باید نسخه پشتیبان فایل smb.conf را در فهرست /etc/samba کپی کنید.

فایل پیکربندی smb.conf شامل یکسری تنظیمات سراسری است که به منظور برقراری ارتباط با شبکه‌های ویندوز پیش‌بینی شده است. این فایل هم‌چنین دارای مجموعه‌ای از تنظیمات پیش‌فرض جهت سهولت در به اشتراک گذاشتن فهرست‌ها و چاپگرها با سایر کاربران شبکه است. تنوع این

تنظیمات چنان است که امکان دسترسی به منابع مشترک مستقر در گروه‌های کاری ویندوز، کامپیوترهای میزبان Member Server و حتی کامپیوترهای PDC و BDC را به راحتی فراهم می‌کند. در این قسمت تنظیمات پیش‌فرض فایل پیکربندی smb.conf را مورد بررسی قرار داده و پرداختن به ابزارهای پیکربندی SWAT و redhat-config-samba را به قسمت‌های بعد فصل موکول می‌کنیم. آن‌چه در ادامه مطالعه خواهید کرد، بررسی تنظیمات نسخه‌ای از فایل پیکربندی smb.conf است که به واسطه نصب بسته نرم‌افزاری *-samba روی سیستم‌عامل Red Hat Linux در فهرست /etc/samba مستقر شده است. برخی تنظیمات این نسخه از فایل smb.conf با تنظیمات پیش‌فرض سرویس Samba متفاوت است.

تنظیمات سراسری سرویس Samba

فایل پیکربندی smb.conf حاوی تعداد قابل توجهی متغیر سراسری است که با عنوان [global] مشخص شده‌اند. چنان‌چه متغیری از این مجموعه را مقداردهی نکنید، مقدار پیش‌فرض آن در نظر گرفته خواهد شد.

متغیرهای سراسری این امکانات را در اختیار قرار می‌دهند:

- محدود کردن آدرس‌های IP مجاز جهت دسترسی به سرور
- مشاهده چاپگرهای موجود در شبکه به عنوان منابع مشترک قابل دستیابی
- پیکربندی حساب کاربری میهمان و فایل‌های ثبت وقایع
- پیکربندی سرویس Samba به منظور تطبیق با خط مشی امنیتی ویندوز به عنوان خط مشی امنیتی حاکم بر شبکه
- برخورداری از یکسری تنظیمات مربوط به کلمات عبور
- تطبیق اسامی کاربران کامپیوترهای Linux و ویندوز
- تغییر فایل‌های پیکربندی جهت استفاده در کامپیوترهای مختلف
- محدود کردن عملیات احراز هویت سرویس Samba به واسطه ماجول‌هایی موسوم به PAM یا Pluggable Authentication Modules (برای توضیح بیشتر به فصل بیست و دوم مراجعه کنید.)
- پیکربندی‌سرویس Samba به منظور ارسال داده‌ها از طریق رابط‌های مختلف و در قالب بسته‌هایی با اندازه‌های متفاوت
- تنظیم لیست منابع مشترک بر اساس کامپیوترهای اصلی مستقر در آن شبکه

- تطبیق سرویس Samba با پارامترهای اساسی شبکه ویندوز
- نگهداری پروفایل‌ها روی کامپیوتر Linux
- پیکربندی سرویس Samba به منظور تعامل با سرویس‌های WINS و DNS

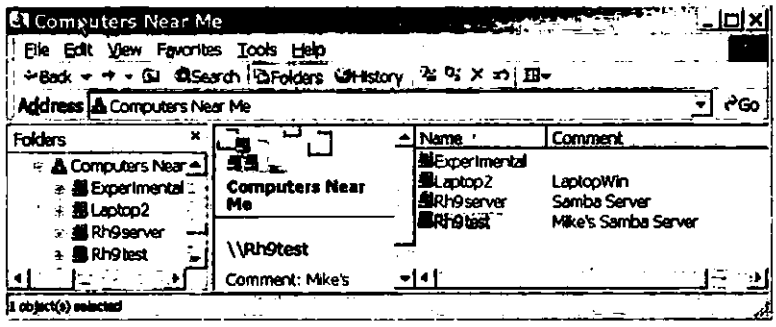
چنان‌که می‌دانید، سیستم‌عامل Linux برخلاف سیستم‌عامل ویندوز نسبت به بزرگی و کوچکی حروف حساس است. سرویس Samba به خوبی این تفاوت را درک کرده و ارتباط میان این دو را به نحو مطلوب برقرار می‌کند.

تعیین نوع شبکه

نخستین متغیر سراسری با عنوان workgroup به منظور تعیین نوع شبکه موردنظر پیش‌بینی شده است. مقدار این متغیر ممکن است بیانگر نام یک گروه کاری یا یک حوزه ویندوز باشد. برای مثال، چنان‌چه نام حوزه موردنظر bignet باشد، متغیر workgroup را باید به این صورت مقداردهی کنید:

```
workgroup=BIGNET
```

علاوه بر این، با مقداردهی متغیر server string می‌توان توصیفی از کامپیوتر میزبان سرور Samba را در کامپیوترهای ویندوز نمایش داد. شکل ۶-۲۹ تأثیر مقداردهی این متغیر را در یکی از کامپیوترهای ویندوز مستقر در شبکه نشان می‌دهد: `server string = Mike's Samba Server`



شکل ۶-۲۹ توصیف کامپیوتر میزبان سرور Samba در یک کامپیوتر ویندوز

محدودیت دسترسی به سرویس Samba

دسترسی به سرویس Samba را می‌توان با استفاده از فرامین برنامه iptables محدود کرد. (برای اطلاع بیشتر درباره این برنامه و فرامین آن به فصل بیست و دوم مراجعه کنید.) محدودیت‌های بیشتر به واسطه مقداردهی متغیر hosts allow امکان‌پذیر است. برای مثال، به واسطه این تنظیمات می‌توان

امکان دسترسی به سرویس Samba را تنها در اختیار کامپیوتر میزبان و شبکه‌ای با آدرس 10.122.33.0 قرار داد:

```
hosts allow = 10.122.33. 127.
hosts allow = 10.122.33.0/255/255/255/0 127.
```

تنظیمات مربوط به چاپگرها

چاپگرها به طور پیش‌فرض در لیست منابع مشترک قرار دارند. با این تنظیمات لیست چاپگرهای CUPS از فایل /etc/printcap بارگذاری می‌شود:

```
printcap name = /etc/printcap
load printers = yes
printing = cups
```

علیرغم املای نادرست برخی از متغیرهای فایل پیکربندی smb.conf عملکرد آن‌ها مورد انتظار است. برای مثال، املای صحیح متغیرهای browsable و writable به صورت browseable و writeable است.

در صورت استفاده از چاپگرهای LPD از این تنظیمات استفاده کنید: (برای اطلاع بیشتر درباره چاپگرهای CUPS و LPR به فصل بیست و پنجم مراجعه کنید.)

```
printcap name = /etc/printcap
load printers = yes
printing = lprng
```

حساب کاربر میهمان

مقدار متغیر guest account بیانگر شناسه کاربر میهمان است. برای مثال، چنان‌چه یک ایستگاه کاری را به منظور اطلاع‌رسانی در معرض دسترسی عموم قرار داده باشید، مطمئناً قصد ندارید که کاربران این ایستگاه کاری، دسترسی نامحدودی به منابع داشته باشند. به عنوان نمونه، شاید قصد شما این است که صرفاً آگهی‌های تبلیغاتی محصولات شرکت خود را در دسترس آن‌ها قرار دهید. در این صورت با حذف علامت ; از ابتدای این خط می‌توانید شناسه کاربر میهمان را فعال کنید: (مطمئن شوید که شناسه pcguest یک شناسه کاربری واقعی روی کامپیوتر Linux است.)

```
; guest account = pcguest
```

فایل‌های ثبت وقایع

دو متغیر log file و max log size به منظور پیکربندی فایل‌های ثبت وقایع مربوط به هریک از کامپیوترهای متصل به ماشین میزبان سرور Samba پیش‌بینی شده‌اند. برای مثال، با انجام این تنظیمات فایل ثبت وقایع مربوط به کامپیوتری از نوع ویندوز با نام Havel تحت عنوان havel.log در فهرست /var/log/samba ذخیره می‌شود. مقداردهی متغیر max log size به صورتی که در این‌جا مشاهده می‌کنید بیانگر آن است که محدودیتی برای اندازه این فایل در نظر گرفته نشده است. محدودیت موردنظر برای اندازه فایل ثبت وقایع را می‌توان بر حسب کیلوبایت مشخص کرد:

```
log file = /var/log/samba/%m.log
max log size = 0
```

شاخص‌هایی که در فایل پیکربندی با علامت % آغاز می‌شوند، قابل تغییر هستند. برای مثال، شاخص %m بیانگر نام کامپیوتر کلاینت است که البته از کامپیوتری به کامپیوتر دیگر فرق می‌کند و از این‌رو می‌تواند نماینده اسامی مختلفی باشد.

امنیت دسترسی به منابع مشترک

در ارتباط با دسترسی به منابع مشترک مستقر در شبکه‌های ویندوز خط‌مشی‌های امنیتی مختلفی قابل اتخاذ است. انتخاب خط‌مشی موردنظر عموماً بر اساس شرایط دسترسی به فهرست‌های مشترک و نوع شبکه میزبان انجام می‌شود. جدول ۴-۲۹ هریک از این خط مشی‌ها را به طور مختصر شرح می‌دهد. مقدار متغیر security از فایل پیکربندی smb.conf بیانگر خط‌مشی امنیتی موردنظر است:

```
security = share
security = user
security = server
security = domain
```

جدول ۴-۲۹ شرح خط‌مشی‌های امنیتی مختلف

عنوان خط‌مشی	توضیح
share	با انتخاب این خط‌مشی دسترسی به فهرست‌های مشترک تنها با در اختیار داشتن کلمه عبور موردنیاز امکان‌پذیر خواهد بود. حالت امنیتی share معمولاً برای کامپیوترهای مستقر در گروه‌های کاری Peer-to-Peer مناسب است. (در این گونه گروه‌های کاری کامپیوتر مشخصی به عنوان سرور پیکربندی نمی‌شود.)

عنوان خط‌مشی	توضیح
user	با انتخاب این خط‌مشی دسترسی به فهرست‌های مشترک با در اختیار داشتن شناسه کاربری و کلمه عبور امکان‌پذیر خواهد بود. حالت امنیتی user برای کامپیوترهایی با سیستم‌عامل ویندوز 2000، XP و هم‌چنین کامپیوترهای Linux مستقر در گروه‌های کاری Peer-to-Peer مناسب است.
server	این خط‌مشی برای کامپیوترهایی مناسب است که اسامی کاربران و کلمات عبور در قالب یک بانک اطلاعاتی متمرکز روی آن‌ها نگهداری می‌شود. در صورت عدم وجود این بانک اطلاعاتی، خط‌مشی server به واسطه مقداردهی security = user به خط مشی user تغییر ماهیت می‌دهد.
domain	این خط‌مشی برای کامپیوترهایی مناسب است که عضوی از یک حوزه ویندوز باشند. استفاده از این خط‌مشی مستلزم وجود دو فایل /etc/samba/smbuser و /etc/samba/smbpasswd است.

تنظیمات مربوط به کلمات عبور

برای انجام تنظیمات مربوط به کلمات عبور، گزینه‌های متعددی پیش‌بینی شده است. اگر کامپیوتری را به منظور نگهداری از شناسه‌های کاربری و کلمات عبور پیکربندی کرده‌اید، با استفاده از گزینه مناسب می‌توانید نقش آن‌را مشخص کنید. علاوه بر این، حتی می‌توانید کامپیوتری از نوع Linux را به واسطه سرویس Samba به عنوان یک PDC در شبکه‌ای از نوع ویندوز مورد بهره‌برداری قرار دهید.

چنان‌چه خط‌مشی امنیتی را به یک از دو صورت security = share یا security = domain تنظیم کرده باشید، لازم است کلمات عبور موردنیاز برای دسترسی به شبکه را نیز به واسطه مقداردهی متغیر password server تعیین کنید. برای مثال، اگر اسامی کامپیوترهای PDC و BDC به ترتیب ntserv1 و ntserv2 باشد، متغیر مذکور را به این صورت مقداردهی کنید:

```
password server = ntserv1 ntserv2
```

در صورت عدم اطلاع از اسامی کامپیوترهای PDC و BDC متغیر password server را به این صورت مقداردهی کنید تا به این ترتیب سرور Samba خود برای جستجوی این اسامی اقدام کند:

```
password server = *
```

در برخی از نسخه‌های سیستم‌عامل ویندوز ترکیب حروف بزرگ و کوچک به منظور انتخاب کلمات عبور مناسب نیست. مقدار متغیرهای password level و username level بیانگر تعداد مجاز حروف بزرگ در ساختار کلمات عبور و شناسه‌های کاربری است. با فعال کردن این تنظیمات (به واسطه حذف

علامت ; از ابتدای آن‌ها) استفاده از حروف بزرگ در ساختار کلمات عبور و شناسه‌های کاربری ممکن خواهد بود:

```
; password level = 8
; username level = 8
```

مقدار متغیر encrypt passwords بیانگر این خط‌مشی ارسال کلمات عبور در قالب متنی ساده یا رمزگذاری شده است. مقدار متغیر smb passwd file فایل حاوی کلمات عبور را مشخص می‌کند. فایل مذکور شناسه‌های کاربری و کلمات عبور درج شده با فرمان smbadduser را نیز شامل می‌شود. با وجود این، تمام کامپیوترهای ویندوز قادر به رمزگشایی آن‌ها نیستند:

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

بدون تنظیمات فوق کلمات عبور در قالب متنی ساده ارسال شده و از رمزگذاری آن‌ها خودداری خواهد شد. البته این خط‌مشی در مورد برخی از نسخه‌های سیستم‌عامل ویندوز که قادر به رمزگشایی کلمات عبور دریافتی نیستند، مناسب است.

در صورت پیکربندی سرویس Samba جهت استفاده از مکانیزم امنیتی Secure Socket Layer (به اختصار SSL) این تنظیمات را فعال کنید:

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

چنان‌چه کاربران سیستم‌عامل‌های ویندوز، کلمات عبور خود را تغییر دهند، با فعال کردن این تنظیمات کلمات عبور مربوطه روی کامپیوتر Linux نیز به طور مناسب دستخوش تغییر خواهد شد:

```
unix password sync = yes
passwd program = /usr/bin/passwd %u
passwd chat = *New*password* %n\n *Retype*new*password* %n\n
*passwd: *all*authentication*tokens*updateed*successfully*
```

با مقداردهی متغیر pam password change به طور مناسب، سرویس Samba به واسطه مکانیزم امنیتی Pluggable Authentication Modules (اصطلاحاً PAM) محافظت بیشتری از کلمات عبور به عمل می‌آورد. (برای اطلاع بیشتر درباره این مکانیزم به فصل بیست و دوم مراجعه کنید.) لازم به توضیح است که متغیر مذکور نسبت به متغیر password program ارجحیت دارد:

```
pam password change = yes
```

در ارتباط با مکانیزم امنیتی PAM متغیر دیگری نیز با عنوان obey pam restrictions وجود دارد. چنان‌چه متغیر مذکور به این صورت مقداردهی شود، در صورت انتقال کلمات عبور در قالب متنی ساده، کنترل دسترسی به کامپیوتر میزبان بر عهده مکانیزم PAM خواهد بود:

```
obey pam restrictions = yes
```

تطبیق کاربران کامپیوترهای Linux و ویندوز

چنان‌که قبلاً نیز توضیح داده شد، اسامی کاربری متفاوتی از کامپیوترهای Linux و ویندوز را می‌توان با یکدیگر مطابقت داد. در صورت استفاده از فرمان smbadduser نتایج این تطبیق در فایلی تحت عنوان /etc/samba/smbusers ذخیره می‌شود. البته ویرایش مستقیم این فایل نیز امکان‌پذیر است. برای برخورداری از مکانیزم مزبور کافی است این تنظیمات را فعال کنید:

```
; username map = /etc/samba/smbusers
```

فایل‌های پیکربندی اختصاصی

سرویس Samba را می‌توان برای هریک از کامپیوترهای راه دور به طور مجزا پیکربندی کرد. با فعال کردن این تنظیمات هر کامپیوتری از فایل پیکربندی مخصوص به خود برخوردار خواهد شد. این فایل‌ها قبلاً باید با عنوان عمومی /etc/samba/smb.conf.*computername* (که در آن متغیر *computername* بیانگر نام کامپیوتر موردنظر است.) روی کامپیوتر میزبان سرور Samba ایجاد شوند. برای مثال، چنان‌چه عنوان یکی از کامپیوترها Chirac باشد، فایل پیکربندی سرویس Samba برای آن کامپیوتر به خصوص فایلی با عنوان /etc/samba/smb.conf.Chirac خواهد بود:

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

افزایش کارایی سرویس Samba

متغیر socket options به منظور بهبود عملکرد سرویس Samba پیش‌بینی شده است. مقداردهی این متغیر به اندازه شبکه میزبان و ترافیک آن بستگی دارد. مقدار TCP_NODELAY در اغلب موارد کارایی سرویس Samba را به میزان دو برابر افزایش می‌دهد. مقادیر متغیرهای SO_RCVBUF و SO_SNDBUF اندازه حافظه ورودی و خروجی را بر حسب بایت مشخص می‌کند. این مقادیر را به بهترین نحو ممکن می‌توان با توجه به ترافیک کامپیوتر میزبان سرور Samba مشخص کرد. برای دستیابی به مقدار مناسب این متغیرها، مقادیر فعلی آن‌ها را به اندازه یک کیلو بایت تغییر دهید: (برای مثال، مقداردهی SO_RCVBUF = 7168 یا SO_RCVBUF = 9216 را آزمایش کنید.)

```
socket options = TCP_NODELAY SO_RCVBUF=8192 SO_SNDBUF=8192
```

رابط‌های شبکه

کامپیوترهای سرور معمولاً با چندین کارت شبکه پیکربندی می‌شوند. در صورت تمایل می‌توان ترتیبی داد تا سرور Samba تنها به یکی از این کارت‌ها دسترسی داشته یا امکان دسترسی به این سرور تنها از یک شبکه به خصوص امکان‌پذیر باشد. برای مثال، با این تنظیمات ارتباط سرور Samba تنها با

کامپیوترهای مستقر در شبکه 172.168.33.0/24 و از طریق کارت شبکه‌ای با مشخصه eth1 امکان‌پذیر خواهد بود:

```
interfaces = eth1 172.168.33.0/24
```

اطلاع از منابع مشترک موجود

در شبکه‌های ویندوز اغلب برای اشاره به توانایی کامپیوترها در مشاهده فهرست‌ها و چاپگرهای مشترک قابل دسترسی، از اصطلاح browsing استفاده می‌شود. در این گونه شبکه‌ها تمام اطلاعات مربوط به منابع مشترک قابل دسترسی معمولاً روی یکی از کامپیوترها با عنوان master browser مستقر است. (استفاده از عناوین دیگری شامل browse master، local master browser و browse server نیز برای اشاره به چنین کامپیوتری متداول است. ـ مترجم) سایر کامپیوترهای شبکه اطلاعات خود را در زمینه وجود منابع مشترک قابل دسترسی در اختیار این کامپیوتر قرار می‌دهند.

مقدار متغیر remote browse sync، کامپیوتر master browser مستقر در یک شبکه راه دور را مشخص می‌کند. اگر آدرس IP چنین کامپیوتری در دست نباشد می‌توان آدرس همگانی شبکه میزبان آن‌را مورد استفاده قرار داد. برای مثال، با این تنظیمات تبادل لازم بین شبکه میزبان سرور Samba و شبکه‌ای با آدرس 192.168.1.0 به منظور یکی کردن لیست منابع مشترک مستقر در این شبکه‌ها انجام می‌شود:

```
remote browse sync = 192.168.1.255
```

با این تنظیمات سرور Samba اطلاعاتی را که راجع به منابع مشترک مستقر در شبکه میزبان در اختیار دارد برای کامپیوتر master browser ارسال می‌کند. بار دیگر، در صورت عدم اطلاع از آدرس IP این کامپیوتر می‌توان آدرس همگانی شبکه مربوطه را مورد استفاده قرار داد:

```
remote annonce = 192.168.1.255
```

چنان‌که گفته شد، یکی از کامپیوترهای مستقر در شبکه‌های ویندوز به عنوان master browser مورد استفاده قرار می‌گیرد. برای تعیین چنین کامپیوتری معمولاً یک گزینش انجام می‌شود. به این ترتیب، حتی کامپیوتر میزبان سرور Samba نیز ممکن است به عنوان کامپیوتر master browser انتخاب شود. برای پیشگیری از این رویداد کافی است از فعال کردن این تنظیمات خودداری کنید:

```
; local master = no
```

اگر مایلید تا کامپیوتر میزبان سرور Samba نیز در گزینش کامپیوتر master browser شرکت کند، با فعال کردن این فرمان شانس آن‌را افزایش دهید. در این صورت، کامپیوتر مزبور جز در رقابت با کنترل کننده حوزه و کامپیوتر میزبان ویندوز NT سرور، گوی سبقت را از سایر کامپیوترهای مستقر در شبکه خواهد ربود:

```
; os level = 33
```

با فعال کردن این تنظیمات می‌توانید ترتیبی دهید تا کامپیوتر میزبان سرور Samba با قطعیت تمام به عنوان کامپیوتر master browser انتخاب شود:

```
; domain master = yes
```

هم‌چنین با فعال کردن این تنظیمات می‌توانید کامپیوتر میزبان سرور Samba را به عنوان کامپیوتر موردنظر خود به عنوان master browser معرفی کنید:

```
; preferred master = yes
```

(اقدام فوق را به عنوان تضمین هرچه بیشتر تنظیمات domain master = yes انجام دهید. با وجود این دقت کنید که اگر تنظیمات فوق در مورد چندین کامپیوتر مختلف از جمله کامپیوتر میزبان سرور Samba و کامپیوترهای ویندوز 95 یا NT مستقر در شبکه فعال شده باشد، این کامپیوترها برای تصدی نقش کامپیوتر master browser با یکدیگر رقابت خواهند کرد. این موضوع باعث می‌شود تا پیغام‌های متعددی از جانب این کامپیوترها به آدرس همگانی شبکه ارسال شده و ترافیک آن‌را افزایش دهد. ـ مترجم)

مدیریت دسترسی کاربران به سرویس Samba

چنان‌چه شبکه موردنظر میزبان مجموعه‌ای از کامپیوترهای ویندوز و Linux باشد، با فعال کردن این تنظیمات می‌توان ترتیبی داد تا سرور Samba به عنوان کنترل کننده اصلی حوزه (اصطلاحاً PDC) وظیفه مدیریت بانک اطلاعاتی حاوی شناسه‌های کاربری و کلمات عبور را به عهده بگیرد:

```
; domain logons = yes
```

اقدام فوق مستلزم وجود مکانیزمی به منظور تأمین امنیت در سطح کاربر و البته وجود فهرستی با عنوان netlogon است. (توضیحات بیشتر در ادامه خواهد آمد.)

خط‌مشی دسترسی به شبکه‌های ویندوز را می‌توان بر اساس شناسه کاربری یا نام کامپیوتر مورد استفاده کاربر پیکربندی کرد. در هر مورد، برنامه اسکریپت مربوطه باید روی کامپیوتر میزبان سرور Samba موجود باشد. شاخص‌های %m و %U به ترتیب نماینده نام کامپیوتر و شناسه کاربری هستند:

```
; logon script = %m.bat
; logon script = %U.bat
```

با تهیه یک پروفایل برای هر کدام از کاربران و استقرار آن‌ها روی کامپیوتر موردنظر (از جمله کامپیوتر میزبان سرور Samba) کاربران هنگام دسترسی به سرویس Samba حس بهتری خواهند داشت. این تنظیمات، که در آن شاخص %L نماینده نام کامپیوتر میزبان پروفایل‌ها و شاخص %U نماینده شناسه‌های کاربری است، برای همین منظور پیش‌بینی شده است:

```
; logon path = \\%L\Profiles\%U
```

تنظیمات مربوط به سرویس‌های WINS و DNS

سرویس Windows Internet Name Service یا به اختصار WINS شبیه به سرویس DNS است با این تفاوت که بانک اطلاعاتی مورد استفاده آن حاوی اسامی NetBIOS و آدرس‌های IP متناظر است. سرور Samba جهت اطلاع از نام کامپیوتر موردنظر خود به بانک اطلاعاتی /etc/hosts مراجعه می‌کند. چنان‌چه اقدام سرور مزبور در این رابطه موفقیت‌آمیز نباشد، به واسطه برخی تنظیمات می‌توان ترتیبی داد تا بانک‌های اطلاعاتی دو سرویس WINS و DNS را نیز برای این منظور مورد جستجو قرار دهد.

با فعال کردن این تنظیمات امکان برخورداری از سرویس WINS و استفاده از بانک اطلاعاتی آن در اختیار سرور Samba قرار می‌گیرد:

```
; wins support = yes
```

با فعال کردن تنظیمات مربوط به متغیر wins server می‌توان ترتیبی داد تا سرور Samba کامپیوتر دیگری را به منظور استفاده از سرویس WINS مورد جستجو قرار دهد. مقدار متغیر مذکور بیانگر آدرس IP کامپیوتری است که سرور Samba امکان وجود سرور WINS را روی آن مورد بررسی قرار می‌دهد. به این ترتیب، سرور Samba خود در نقش کلاینت ظاهر می‌شود. برای مثال، با فعال کردن این تنظیمات سرور Samba امکان وجود سرویس WINS را روی کامپیوتری به آدرس 192.168.0.22 مورد بررسی قرار می‌دهد:

```
; wins server = 192.168.0.22
```

چنان‌چه شبکه ویندوز متشکل از کامپیوترهای قدیمی باشد، با فعال کردن این تنظیمات می‌توان امکان دسترسی به بانک اطلاعاتی سرویس WINS را در اختیار آن کامپیوترها قرار داد:

```
; wins proxy = yes
```

اگر عنوان کامپیوتر موردنظر سرور Samba در بانک اطلاعاتی سرویس WINS موجود نباشد، با فعال کردن این تنظیمات سرور Samba جستجوی مشابهی را در بانک اطلاعاتی سرویس DNS انجام خواهد داد:

```
; dns proxy = yes
```

کنترل تأثیر تفاوت بزرگی و کوچکی حروف در دو سیستم‌عامل ویندوز و Linux

سیستم عامل Linux برخلاف ویندوز نسبت به بزرگی و کوچکی حروف به کار رفته در اسامی فایل‌ها حساس است. تنظیمات پیش‌فرض سرویس Samba چنان است که پس از انتقال فایل‌ها از مبدأ به مقصد، بزرگی یا کوچکی این حروف هم‌چنان حفظ می‌شود. با وجود این، در صورت لزوم می‌توان این تنظیمات را برای تبدیل حروف بزرگ به کوچک یا بالعکس تغییر داد. با فعال کردن این تنظیمات، اندازه حروف تشکیل دهنده اسامی فایل‌ها پس از انتقال به مقصد بر اساس مقدار متغیر default dase تغییر خواهد کرد. مقدار متغیر preserve case فایل‌های با اسامی بلند و مقدار متغیر short preserve

case فایل‌هایی را که در قالب 8.3 (هم‌چون abcdefgh.123) نام‌گذاری شده‌اند، تحت تأثیر قرار می‌دهد.

```
; preserve case = no
; short preserve case = no
```

برای مثال، با فعال کردن این تنظیمات کلیه حروف کوچک تشکیل دهنده اسامی فایل‌ها به حروف بزرگ متناظر تبدیل خواهند شد:

```
; default case = upper
```

در صورتی که تمام کاربران شبکه قواعد استفاده از حروف بزرگ و کوچک در نام‌گذاری فایل‌ها را به دقت رعایت کنند، با فعال کردن این تنظیمات می‌توان ترتیبی داد تا سرور Samba نیز نسبت به استفاده از حروف بزرگ و کوچک در نام‌گذاری فایل‌ها حساسیت نشان دهد:

```
; case sensitive = yes
```

با وجود این، از آن‌جا که سیستم‌عامل ویندوز نسبت به استفاده از حروف بزرگ و کوچک در نام‌گذاری فایل‌ها حساس نیست، به واسطه سهل‌انگاری برخی از کاربران در استفاده از حروف بزرگ و کوچک جهت نام‌گذاری فایل‌ها، اقدام فوق ممکن است مشکلاتی را به دنبال داشته باشد.

پیکربندی سرویس Samba به عنوان کنترل کننده اصلی حوزه (اصطلاحاً PDC) موضوع کاملاً پیچیده‌ای است، به طوری که می‌توان در مورد آن کتاب مستقلی تألیف کرد. برای دستیابی به اطلاعات جامع در این زمینه توصیه می‌کنیم مستندات موجود در این آدرس را مورد مطالعه قرار دهید:
http://us1.samba.org/docs/Samba-HOWTO-Collection.html

مقادیر پیش‌فرض متغیرهای سراسری

جدول ۵-۲۹ حاوی مقادیر پیش‌فرض متغیرهای سراسری فایل پیکربندی /etc/samba/smb.conf است. چنان‌چه قصد دارید مقدار پیش‌فرض یک متغیر سراسری را مورد استفاده قرار دهید، نیازی نیست که آن‌را در فایل پیکربندی مذکور درج کنید. در صورت انجام این کار، ابزارهای پیکربندی SWAT و redhat-config-samba هنگام به روز رسانی فایل /etc/samba/smb.conf این تنظیمات را از فایل نامبرده حذف خواهند کرد.

جدول ۵-۲۹ مقادیر پیش‌فرض متغیرهای سراسری فایل پیکربندی /etc/samba/smb.conf

عنوان متغیر سراسری	مقدار پیش فرض
case sensitive	no
default case	lower
dnss proxy	yes

عنوان متغیر سراسری	مقدار پیش فرض
domain logons	no
encrypt passwords	no
guest account	nobody
hosts allow	تمام کامپیوترها از مجوز دسترسی به سرویس Samba برخوردار هستند.
include	این متغیر فاقد مقدار پیش‌فرض است.
interfaces	به استثنای کارت شبکه مجازی loop-back به آدرس 127.0.0.1، دسترسی به تمام کارت‌های شبکه فعالی که ارسال پیغام همگانی از طریق آن‌ها مقدور باشد، امکان‌پذیر است.
load printers	yes
local master	yes
log file	این متغیر فاقد مقدار پیش‌فرض است.
logon path	\\%N\%U\profile (شاخص‌های N% و U% به ترتیب نماینده سرور NIS و شناسه کاربری هستند.)
logon script	این متغیر فاقد مقدار پیش‌فرض است.
max logsize	5000 (بر حسب کیلو بایت)
obey pam restrictions	no
pam password change	no
passwd chat	*new*password* %n\n *new*password* %n\n* changed*
passwd program	/bin/passwd
passwd server	این متغیر فاقد مقدار پیش‌فرض است.
password level	0
preferred master	auto
preserve case	yes
printcap name	/etc/printcap
printing	این متغیر فاقد مقدار پیش‌فرض است.
remote announce	این متغیر فاقد مقدار پیش‌فرض است.
remote browse sync	این متغیر فاقد مقدار پیش‌فرض است.
security	user
server string	Samba%v (شاخص %v بیانگر شماره ویرایش برنامه Samba است.)
short preserve case	yes

عنوان متغیر سراسری	مقدار پیش فرض
smb password file	این متغیر فاقد مقدار پیش‌فرض است.
socket options	TCP_NODELAY
ssl CA certFile	/usr/local/ssl/certs/trustedCAs.pem
unix password sync	no
username level	0
username map	این متغیر فاقد مقدار پیش‌فرض است.
wins proxy	no
wins server	این متغیر فاقد مقدار پیش‌فرض است.
wins support	no
workgroup	WORKGROUP

پیکربندی منابع مشترک

در این قسمت دسته‌ای از تنظیمات فایل /etc/samba/smb.conf را که به پیکربندی منابع مشترک مربوط می‌شود، مورد بررسی قرار می‌دهیم. فایل مذکور حاوی هفت پیکربندی نمونه است. با مطالعه این مثال‌ها مطمئناً به ایده‌های خوبی در این رابطه دست پیدا خواهید کرد.

پیکربندی فهرست مشترک [homes]

به واسطه این تنظیمات، کاربران کامپیوترهای ویندوز در صورت برخورداری از یک حساب کاربری معتبر روی کامپیوتر Linux می‌توانند فهرست خانگی خود را به منظور خواندن و نوشتن مورد دسترسی قرار دهند:

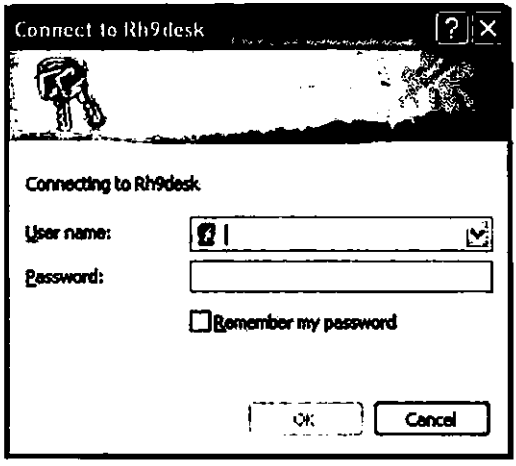
```
[homes]
 comment = Home Directories
 browseable = no
 writeable = yes
 valid users = %S
 create mode = 0664
 directory mode = 0775
```

شرح مختصری از این تنظیمات در جدول ۶-۲۹ آمده است.

جدول ۶-۲۹ شرح تنظیمات دسترسی به فهرست خانگی کاربران

عنوان برچسب یا تنظیمات	توضیح
[homes]	این برچسب بیانگر بخش ویژه‌ای از فایل پیکربندی smb.conf شامل تنظیمات دسترسی به فهرست خانگی کاربران است.
comment = Home Directories	این تنظیمات بیانگر توصیفی است که هنگام دسترسی به فهرست خانگی در پنجره برنامه Network Neighborhood یا My Network Places یا هنگام اجرای فرمان smbclient -L \\hostname به نمایش درمی‌آید.
browseable = no	به موجب این تنظیمات از نمایش فهرست خانگی در پنجره برنامه Network Neighborhood یا My Network Places جلوگیری به عمل می‌آید. این موضوع شامل کاربری که مالک آن فهرست است، نمی‌شود.
writeable = yes	به موجب این تنظیمات امکان نوشتن در فهرست خانگی فراهم می‌شود. معادل دیگر این تنظیمات مقداردهی read only = no است.
valid users = %S	به موجب این تنظیمات دسترسی به سرویس موردنظر برای تمام کاربران فراهم می‌شود. شاخص %S بیانگر نام سرویس است.
create mode = 0644	به موجب این تنظیمات مجوز دسترسی به فایل‌های جدید به صورت rw-r--r-- پیکربندی می‌شود. این تنظیمات موجب نقض مجوزهایی که روی کامپیوترهای ویندوز NT، 2000 یا XP پیکربندی شده‌اند، نمی‌شود. عنوان دیگر این متغیر create mask است.
directory mode = 0775	به موجب این تنظیمات مجوز دسترسی به فهرست‌های جدید به صورت rw-r--r-- پیکربندی می‌شود. این تنظیمات موجب نقض مجوزهایی که روی کامپیوترهای ویندوز NT، 2000 یا XP پیکربندی شده‌اند، نمی‌شود. عنوان دیگر این متغیر directory mask است.

کاربران برای دسترسی به فهرست خانگی خود کافی است شناسه کاربری و کلمه عبور موردنیاز را در فیلدهای متنی کادر محاوره‌ای Connect To *Computername* (که در آن متغیر *Computername* بیانگر نام کامپیوتر میزبان آن فهرست است.) وارد کنند. شکل ۷-۲۹ این کادر محاوره‌ای را نشان می‌دهد.



شکل ۷-۲۹ دسترسی به فهرست خانگی با وارد کردن شناسه کاربری و کلمه عبور در فیلدهای متنی این کادر محاوره‌ای امکان‌پذیر است.

پیکربندی فهرست مشترک [tmp]

معمولاً فهرست /tmp به عنوان فهرستی که کاربران شبکه فایل‌های خود را در آن‌جا به اشتراک می‌گذارند، مورد استفاده قرار می‌گیرد. به تنظیمات مربوطه توجه کنید:

```
[tmp]
  comment = Temporary file space
  path = /tmp
  read only = no
  public = yes
```

مقدار متغیر comment توصیفی است که هنگام دسترسی به فهرست /tmp در پنجره Windows Network Neighborhood یا My Network Places به نمایش درمی‌آید. مقداردهی read only = no بیانگر آن است که کاربران مجاز از امکان نوشتن در این فهرست برخوردار هستند. مقداردهی public = yes معادل مقداردهی guest ok = yes است، به این معنی که دسترسی به این فهرست مستلزم در اختیار داشتن کلمه عبور نیست.

پیکربندی منبع مشترک [public]

در برخی موارد، به دلایلی لازم است تا دسترسی به فهرست مشخصی را برای تمام کاربران فراهم کنید. مشابه مکانیزم User Private Group که در فصل نهم به بررسی آن پرداختیم، در صورت تمایل

می‌توان امکان خواندن فهرست‌ها را در اختیار تمام کاربران قرار داد، اما امکان نوشتن در آن فهرست‌ها را تنها برای عده‌ای از آن‌ها فراهم کرد. به تنظیمات مربوطه توجه کنید:

```
[public]
  comment = Public Stuff
  path = /home/samba
  public = yes
  writable = yes
  printable = no
  write list = @staff
```

پیش از انجام تنظیمات فوق باید از وجود فهرست home/samba/ و هم‌چنین درج مشخصات گروهی با عنوان staff در فهرست etc/groups/ اطمینان حاصل کنید.

پیکربندی منبع مشترک [public] (نمونه دوم)

گاهی ممکن است یکسری از تنظیمات برای موارد مشابه متعددی مناسب باشد. تنظیماتی را که در این قسمت مشاهده می‌کنید، فهرست usr/somewhere/else/public/ را چنین پیکربندی می‌کند که امکان خواندن و نوشتن در آن برای تمام کاربران مهیا شود. با وجود این، مقداردهی only guest = yes صراحتاً به معنی آن است که اختیارات این کاربران تنها در حد کاربر میهمان است. اطمینان از صحت مقدار متغیر path، یعنی وجود فهرست usr/somewhere/else/public/ ضروری است:

```
[public]
  path = /usr/somewhere/else/public
  public = yes
  only guest = yes
  writable = yes
  printable = no
```

پیکربندی منبع مشترک جهت دسترسی دو کاربر مشخص

یکی از اقدامات متداول در پیکربندی یک منبع مشترک این است که امکان دسترسی به آن‌را تنها برای کاربران مشخصی فراهم کنیم. تنظیماتی که در ادامه مشاهده می‌کنید، امکان دسترسی به فهرست usr/somewhere/shared/ را تنها در اختیار دو تن از کاربران با شناسه‌های mary و fred قرار می‌دهد. با وجودی که فهرست مذکور از نوع عمومی نبوده به این معنی که توسط تمام کاربران قابل دسترس نیست، مقداردهی browseable یکی از تنظیمات پیش‌فرض است. به بیان دیگر، هر چند که سایر کاربران نیز می‌توانند فهرست usr/somewhere/shared/ را به عنوان یک فهرست مشترک تشخیص

دهند، دسترسی به آن تنها با استفاده از دو شناسه کاربری مذکور و اطلاع از کلمات عبور مربوطه ممکن خواهد بود:

```
[myshare]

  path = /usr/somewhere/shared
  valid users = mary fred
  public = no
  writable = yes
  printable = no
  create mask = 0765
```

تنظیمات فوق در صورتی صحیح است که فایل /usr/somewhere/shared روی کامپیوتر میزبان سرور Samba موجود بوده و دو حساب کاربری mary و fred از قبل تعریف شده باشد.

پیکربندی فهرست‌های خصوصی

علاوه بر فهرست خانگی کاربران، در صورت لزوم می‌توان فهرستی را نیز به منظور دسترسی خصوصی برای هریک از آن‌ها پیکربندی کرد. برای مثال، این تنظیمات فهرست /usr/somewhere/private را به عنوان یک فهرست خصوصی برای کاربری با شناسه fred ایجاد می‌کند. مقداردهی public = no از دسترسی کاربران میهمان به این فهرست جلوگیری به عمل می‌آورد:

```
[fredsdir]

  path = /usr/somewhere/private
  valid users = fred
  public = no
  writable = yes
  printable = no
```

پیکربندی فهرست مشترک جهت دسترسی از یک کامپیوتر به خصوص

گاهی اوقات لازم است فهرست به خصوصی تنها از طریق یک کامپیوتر مشخص قابل دستیابی باشد. به بیان دیگر، دسترسی به چنین فهرستی تنها برای کاربرانی که روی آن کامپیوتر دارای حساب کاربری معتبر هستند، امکان‌پذیر است. برای مثال، کاربرانی که در شیفت‌های کاری مختلف یک کارخانه روی یک کامپیوتر واحد کار می‌کنند، به واسطه چنین تنظیماتی می‌توانند یک فهرست مشخص را مورد دستیابی قرار دهند. به نمونه‌ای از این تنظیمات توجه کنید:

```
[pchome]
  comment = PC Directories
  path = /usr/local/pc/%m
  public = no
  writable = yes
```

بدیهی است فهرست /usr/local/pc/%m باید موجود باشد. شاخص %m بیانگر نام کامپیوتر میزبان است. برای مثال، در صورتی که نام این کامپیوتر factory1 باشد، مقدار متغیر path در تنظیمات فوق موجب دسترسی به فهرست /usr/local/pc/factory1 خواهد شد.

پیکربندی چاپگر مشترک

حتی اگر سرویس چاپ CUPS را قبلاً پیکربندی کرده باشید، برای دسترسی به چاپگر مشترک باید تنظیماتی را انجام دهید. با وجودی که فایل smb.conf به طور پیش‌فرض برای استفاده از چاپگرهای LPD پیکربندی شده است، به واسطه این تنظیمات می‌توان چاپگرهای CUPS را نیز مورد دستیابی قرار داد:

```
[printers]
  comment = All Printers
  path = /var/spool/samba
  browseable = no
  guest ok = no
  writable = no
  printable = yes
```

در صورت تمایل می‌توان امکان دسترسی به چاپگری از نوع LPD را منحصراً در اختیار یک کاربر به خصوص قرار داد. برای مثال، به واسطه این تنظیمات از پیش پیکربندی شده در فایل smb.conf، دسترسی به چاپگر LPD تنها برای کاربری با شناسه fred مقدور خواهد بود:

```
[fredsprn]
                    rinter
  valid users = fred
  path = /home/fred
  printer = freds_printer
  public = no
  writable = no
  printable = yes
```

مقداردهی writeable در این تنظیمات تأثیری روی سبد چاپ (فهرست حاوی فایل‌های چاپی یا اصطلاحاً spool directory) ندارد، به طوری که در صورت لزوم می‌توان فایل‌هایی را جهت چاپ به این سبد اضافه کرد.

مدیریت فهرست‌های حاوی حساب کاربران

اگر کامپیوتر میزبان سرور Samba را به عنوان کنترل کننده اصلی یا پشتیبان حوزه (اصطلاحاً PDC یا BDC) پیکربندی کرده باشید، لازم است تنظیماتی را در ارتباط با فهرست‌های حاوی حساب دسترسی کاربران به امکانات مستقر در حوزه موردنظر انجام دهید. بار دیگر، قبل از هر اقدامی باید از این وجود فهرست‌ها اطمینان حاصل کنید.

این تنظیمات به فرض وجود فهرست /usr/local/samba/lib/netlogon (مقدار متغیر path) انجام شده است:

```
[netlogon]
  comment = Network Logon Service
  path = /usr/local/samba/lib/netlogon
  guest ok = yes
  writable = no
  share modes = no
```

مقداردهی share modes = no به منظور اطمینان از پیشگیری مهاجمین در دسترسی به این فهرست می‌شود.

با درج مشخصات کاربران در فهرست /usr/local/samba/profiles از کامپیوتر میزبان سرور Samba و انجام این تنظیمات، کاربران می‌توانند برای دسترسی به حوزه موردنظر از طریق این کامپیوتر اقدام کنند:

```
[Profiles]
  path = /usr/local/samba/profiles
  browseable = no
  guest ok = yes
```

مقادیر پیش‌فرض متغیرهای مربوط به پیکربندی منابع مشترک

جدول ۷-۲۹ حاوی مقادیر پیش‌فرض متغیرهای مربوط به پیکربندی فهرست‌ها و چاپگرهای مشترک است. چنان‌چه قصد دارید مقدار پیش‌فرض یک متغیر سراسری را مورد استفاده قرار دهید، نیازی نیست که آن‌را در فایل پیکربندی مذکور درج کنید. در صورت انجام این کار، ابزارهای پیکربندی

SWAT و redhat-config-samba هنگام به روز رسانی فایل /etc/samba/smb.conf این تنظیمات را از فایل نامبرده حذف خواهند کرد.

جدول ۷-۲۹ مقادیر پیش‌فرض متغیرهای مربوط به پیکربندی منابع مشترک

عنوان متغیر	مقدار پیش‌فرض
browseable	yes
comment	این متغیر فاقد مقدار پیش‌فرض است.
create mode	0744 (تأثیر این متغیر مشابه مقداردهی create mask = 0744 است.)
directory mode	0755 (تأثیر این متغیر مشابه مقداردهی directory mask = 0755 است.)
guest ok	no
path	این متغیر فاقد مقدار پیش‌فرض است.
printable	no
public	no (تأثیر این متغیر مشابه مقداردهی guest ok = no است.)
read only	yes
writeable	no (تأثیر این متغیر مشابه مقداردهی read only = yes است.)
write list	این متغیر فاقد مقدار پیش‌فرض است.
valid users	این متغیر فاقد مقدار پیش‌فرض است. (به طور پیش‌فرض، تمام کاربرانی که دارای حساب کاربری معتبر هستند، از امکان دسترسی به منبع مشترک موردنظر برخوردارند.)

اشکال‌زدایی سرویس Samba

به دلیل تنوع و تعداد زیاد تنظیمات موجود در فایل‌های پیکربندی سرویس Samba به ویژه smb.conf، کمترین سهل‌انگاری در انجام این تنظیمات می‌تواند منجر به خطا شود. از این‌رو، اشکال‌زدایی سرویس مذکور در برخی موارد مستلزم صرف زمان قابل توجهی برای بازبینی این تنظیمات است.

نخستین اقدام در جهت اشکال‌زدایی سرویس Samba بررسی تنظیمات فایل پیکربندی smb.conf است. هنگام انجام این بررسی علایم درج توضیحات (یعنی ; و #) را به دقت مورد توجه قرار دهید، چرا که ممکن است ضمن پیکربندی این فایل علامتی را به طور ناخوسته حذف کرده باشید. گام بعدی این است که لیست منابع مشترک را که روی کامپیوتر میزبان سرور Samba نگهداری می‌شود، مورد بررسی قرار دهید. چنان‌چه این لیست محلی فاقد اشکال باشد، لازم است منابع مشترک مستقر در شبکه را به دقت بررسی کنید. لازم به ذکر است که برخی از تنظیمات فایل پیکربندی smb.conf نیز ممکن است

منجر به مشکلاتی شود.

بررسی فایل پیکربندی smb.conf

اطمینان از صحت تنظیمات فایل پیکربندی smb.conf کار ساده‌ای است، چرا که برنامه testparm به سادگی قادر است خطاهای ناشی از تنظیمات نادرست را تشخیص دهد. این برنامه به طور پیش‌فرض فهرست etc/samba/ را جهت دسترسی به فایل smb.conf و انجام بررسی‌ها مورد جستجو قرار می‌دهد. برای استفاده از قابلیت‌های برنامه testparm، کافی است آن‌را پیش از راه‌اندازی مجدد سرور Samba یا بارگذاری مجدد فایل پیکربندی smb.conf اجرا کنید. در این صورت، چنان‌چه در تنظیمات فایل مذکور خطایی هرچند کوچک مرتکب شده باشید، برنامه testparm راهنمایی‌های ارزنده‌ای را جهت تشخیص منبع خطا در اختیارتان قرار خواهد داد. به این ترتیب، نیازی نیست که زحمت بازبینی انبوهی از تنظیمات را به جان بخرید.

بررسی لیست منابع مشترک

پس از راه‌اندازی مجدد سرویس Samba، با اجرای فرمان smbclient لیست محلی حاوی منابع مشترک را مورد بازبینی قرار دهید. همین لیست باید روی کامپیوترهای ویندوز مستقر در شبکه نیز موجود باشد. برای مثال، با اجرای این فرمان لیست محلی مربوط به کامپیوتری با عنوان RH9test که حاوی مشخصات منابع مشترک است، به نمایش درمی‌آید. عنوان mj شناسه کاربری معتبری از این کامپیوتر است:

```
# smbclient -L \\RH9test -U mj
```

با اجرای فرمان فوق اعلانی جهت دریافت کلمه عبور مربوط به شناسه کاربری mj نمایش داده می‌شود. پس از وارد کردن کلمه عبور معتبر لیست محلی حاوی منابع مشترک به نمایش درمی‌آید. شکل ۸-۲۹ نتیجه یک چنین اقدامی را نشان می‌دهد. چنان‌که مشاهده می‌کنید، علاوه بر لیست مذکور، اسامی گروه‌های کاری (با عناوین WORKGROUP و MYGROUP) نیز به نمایش درآمده است.

فراموش نکنید که مشخصات کاربران سرویس Samba باید در فایل /etc/samba/smbusers درج شده باشد. در مثال فوق چنین فرض شده که قبلاً با استفاده از فرمان smbadduser این اقدام صورت گرفته است.

```
[root@RH9Desk root]# smbclient -L \\RH9Test -U mj
added interface ip=10.252.113.211 bcast=10.252.113.255 nmask=255.255.255.0
Password:
Domain=[WORKGROUP] OS=[Unix] Server=[Samba 2.2.7a]

        Sharename       Type      Comment
        ---------       ----      -------
        mao             Disk      Mao's Home Directory
        var             Disk      Logs and More
        IPC$            IPC       IPC Service (the samba server)
        ADMIN$          Disk      IPC Service (the samba server)
        MyLaserJet      Printer
        HPLasers        Printer
        printer         Printer
        SecondLaserJe   Printer
        mj              Disk      Home Directories

        Server               Comment
        ---------            -------
        LAPTOP2              LaptopWin
        RH9DESK              samba server
        RH9SERVER
        RH9TEST              the samba server

        Workgroup            Master
        ---------            -------
        MYGROUP              RH9DESK
        WORKGROUP            RH9TEST
[root@RH9Desk root]#
```

شکل ۸-۲۹ بررسی لیست محلی حاوی منابع مشترک

بررسی شبکه

چنان‌که در فصل بیست و یکم نیز اشاره شد، اغلب مشکلات شبکه‌ها ناشی از اشکال در تجهیزات فیزیکی، هم‌چون نارسایی کابل، قطعی برق هاب و موارد مشابه است. در فصل بیست و یکم فرامینی مانند ping و netstat را به عنوان ابزارهایی که امکان بررسی وضعیت شبکه را فراهم می‌کنند، مورد بررسی قرار دادیم.

یکی از مشکلات متداول ناشی از مکانیزم بازدارنده دیوار آتش است. پیکربندی این مکانیزم روی کامپیوتر میزبان سرور Samba می‌تواند منجر به بلوکه شدن درخواست‌های ارسالی از کامپیوترهای کلاینت برای ارتباط با سرور شود. چنان‌چه سرور Samba قادر به مشاهده کلاینت‌ها نباشد، بدیهی است که امکان دسترسی به منابع مشترک نیز وجود ندارد.

سایر مشکلات

بسیاری از مشکلات سرویس Samba ناشی از خطاهایی است که هنگام ویرایش فایل پیکربندی smb.conf رخ می‌دهد. با آن‌که برنامه testparm قادر به تشخیص بسیاری از این خطاهاست، وجود برخی از آن‌ها مانع از شناسایی سرور Samba در شبکه میزبان می‌شود. گاهی اوقات با مراجعه به فایل‌های ثبت وقایع منشأ این خطاها مشخص می‌شود. چنان‌که قبلاً نیز اشاره شد، فایل‌های ثبت وقایع هریک از کلاینت‌ها روی کامپیوتر میزبان سرور Samba نگهداری می‌شود. برای‌مثال، کلیه درخواست‌های ارسالی از کامپیوتری با عنوان laptop2 به سرور Samba در شکل ۹-۲۹ قابل تشخیص است.

```
[2002/12/09 13.35 42, 0] client/smbmount.c.send_fs_socket(383)
  mount smbfs: entering daemon mode for service \\laptop2\redhatbeta, pid=12182
[2002/12/09 13.36:13, 0] client/smbmount.c.send_fs_socket(383)
  mount smbfs  entering daemon mode for service \\laptop2\redhat, pid=12188
[2002/12/09 15.38:45, 0] client/smbmount.c:send_fs_socket(383)
  mount smbfs: entering daemon mode for service \\laptop2\redhatbeta, pid=3738
[2002/12/09 15.41:05, 0] client/smbmount c.send_fs_socket(383)
  mount smbfs  entering daemon mode for service \\laptop2\redhat, pid=3801
[2002/12/09 19.26:34, 0] client/smbmount.c:send_fs_socket(383)
  mount smbfs. entering daemon mode for service \\laptop2\redhatbeta, pid=2017
[2002/12/10 09:18 42, 0] client/smbmount c.send_fs_socket(383)
  mount.smbfs: entering daemon mode for service \\laptop2\redhatbeta, pid=2003
[2002/12/10 11:15 38, 0] client/smbmount.c send_fs_socket(383)
  mount smbfs: entering daemon mode for service \\laptop2\downloads, pid=3489
[2002/12/10 11 16:54, 0] client/smbmount c.send_fs_socket(383)
  mount smbfs  entering daemon mode for service \\laptop2\downloads, pid=3526
[2002/12/10 11:18.44, 0] client/smbmount c.send_fs_socket(383)
  mount smbfs  entering daemon mode for service \\laptop2\downloads, pid=3535
[2002/12/10 11:23.42, 0] client/smbmount.c:send_fs_socket(383)
  mount.smbfs: entering daemon mode for service \\laptop2\downloads, pid=3543
[2002/12/11 14 19:40, 0] client/smbmount.c:send_fs_socket(383)
  mount.smbfs: entering daemon mode for service \\laptop2\redhatbeta, pid=2301
~
~
~
~
"smbmount log" 22L, 1552C
```

شکل ۹-۲۹ محتوای فایل ثبت وقایع مربوط به یکی از کلاینت‌ها

خطاهای متداول در تنظیمات فایل پیکربندی smb.conf را می‌توان به این صورت دسته‌بندی کرد:

- **پیکربندی نادرست گروه کاری:** متغیر workgroup گروه کاری کامپیوتر میزبان سرور Samba را مشخص می‌کند. علیرغم مقدار پیش‌فرض، این متغیر یعنی WORKGROUP، در فایل پیکربندی smb.conf به صورت workgroup = MYGROUP مقداردهی شده است. چنان‌چه

کامپیوتر مزبور در یک حوزه مستقر شده اما نام حوزه به درستی تعیین نشده باشد، این موضوع مشکلات جدی‌تری را در پی خواهد داشت.

- **مشکلات ناشی از مقداردهی browseable = no**: با این وجود مقداردهی، مشاهده منابع مشترک در پنجره Windows Network Neighborhood و My Network Places امکان‌پذیر نخواهد بود.
- **پیکربندی نادرست منابع مشترک**: چنان‌که در قسمت قبل اشاره شد، روش‌های متعددی برای پیکربندی منابع مشترک بر اساس کاربران عادی، کاربران میهمان، گروه‌ها و عموم کاربران وجود دارد. در صورتی که این پیکربندی به درستی انجام نشود، دسترسی کاربران به به منابع مشترک ممکن است به طرز نادرستی محدود شود.
- **مشکلات ناشی از مقداردهی writeable = no**: با این وجود مقداردهی، امکان نوشتن در فهرست‌های مشترک از کاربران سلب می‌شود. (مقداردهی فوق یکی از تنظیمات پیش‌فرض فایل پیکربندی smb.conf است.)
- **پیکربندی نادرست مکانیزم‌های بازدارنده**: مکانیزم‌های بازدارنده استاندارد در سیستم‌عامل Red Hat Linux از هر گونه اقدامی جهت دسترسی به سرور Samba جلوگیری به عمل می‌آورند. در صورت مقداردهی متغیر hosts allow، کاربران کامپیوترهایی که مشخصه آن‌ها به عنوان مقدار این متغیر در فایل پیکربندی smb.conf درج نشده باشد، از دسترسی به سرور Samba منع می‌شوند.

ابزار پیکربندی SWAT

بسته نرم‌افزاری samba-swat-* حاوی یک ابزار پیکربندی تحت وب با عنوان Samba Web Administration Tool یا به اختصار SWAT است. پیش از به کارگیری ابزار مذکور لازم است با اجرای این فرمان سرویس موردنیاز از xinetd را فعال کنید:

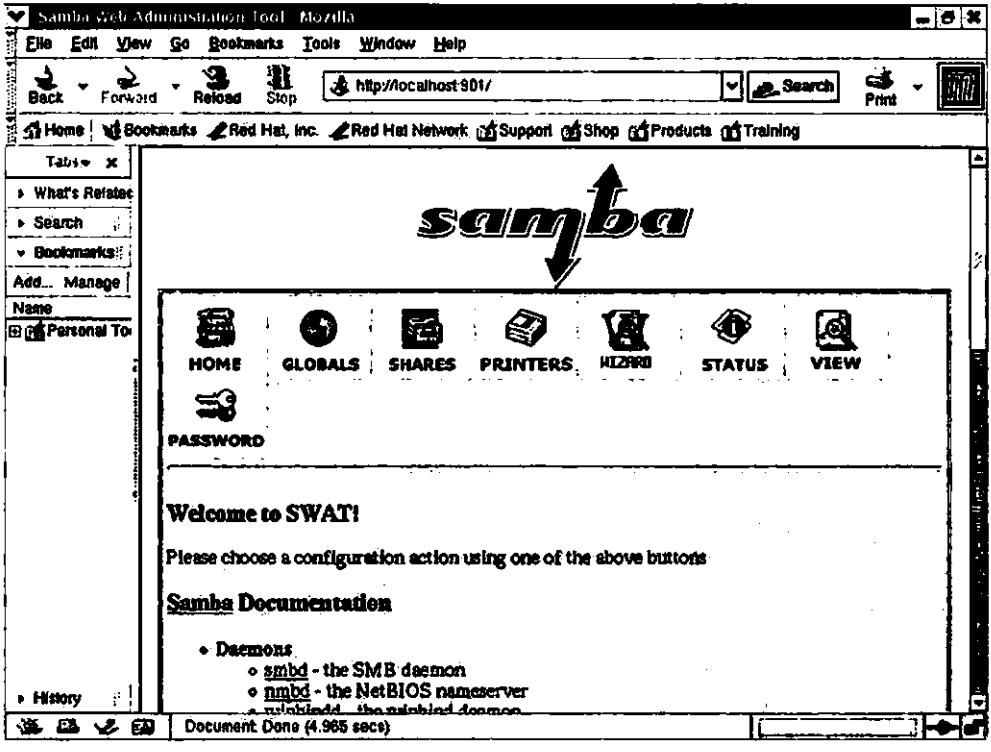
```
# chkconfig swat on
```

ابزار پیکربندی SWAT حاوی منوهای متعددی است که در قسمت‌های بعد به طور مفصل آن‌ها را شرح خواهیم داد. به طور خلاصه، هریک از این منوها امکانات لازم برای پیکربندی موردنظر را در اختیار قرار می‌دهد. پس از انجام تغییرات، برای ثبت دایمی آن‌ها کافی است دکمه Commit Changes را کلیک کنید.

به منظور مشاهده تأثیر این پیکربندی باید سرویس‌های smbd و nmbd را مجدداً راه‌اندازی کنید. گزینه موردنیاز برای انجام این کار در منوی Service پیش‌بینی شده است. علاوه بر این، با اجرای فرمان service smb restart نیز می‌توانید برای راه‌اندازی مجدد سرویس موردنظر اقدام کنید.

منوی Home

برای دسترسی به ابزار پیکربندی SWAT ابتدا مرورگر وب موردنظر خود را باز کرده و عبارت localhost:901 را در نوار آدرس آن وارد کنید. حتی در صورتی که با حساب کاربر اصلی (اصطلاحاً root) وارد سیستم شده باشید، اعلان مربوط به دریافت شناسه کاربری و کلمه عبور را مشاهده خواهید کرد. پس از وارد کردن این اطلاعات، منوی Home از ابزار SWAT مطابق شکل ۱۰-۲۹ به نمایش درمی‌آید.

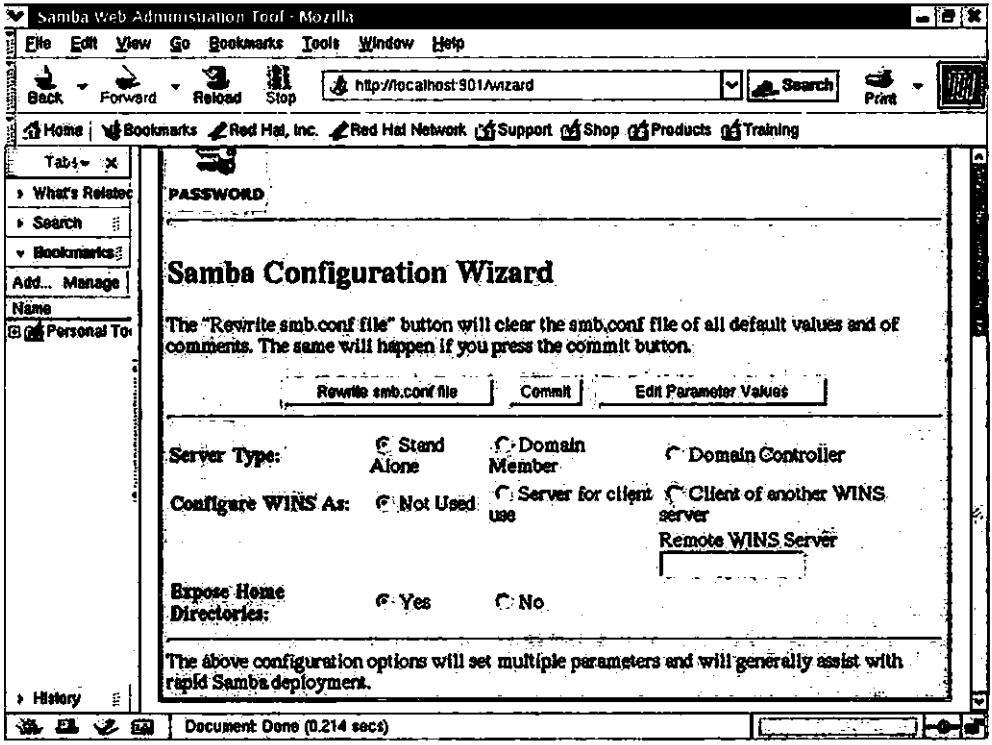


شکل ۱۰-۲۹ منوی Home از ابزار پیکربندی SWAT

چنان که در این شکل مشاهده می‌کنید، منوی Home امکان دسترسی به سایر منوهای ابزار SWAT را در اختیار قرار می‌دهد. در قسمت‌های بعد به بررسی هریک از این منوها خواهیم پرداخت. علاوه بر این، دسترسی به مستندات مفیدی درباره سرویس Samba، از جمله مستندات مربوط به برخی از فرامین و فایل‌ها و هم‌چنین مستنداتی تحت عنوان HOWTO و بالاخره نسخه الکترونیکی نخستین ویرایش از کتاب *Using Samba* از طریق همین منو امکان‌پذیر است.

برنامه Samba Configuration Wizard

برنامه Samba Configuration Wizard یکی از امکانات ابزار پیکربندی SWAT است که امکان انجام سه پیکربندی اساسی سرویس Samba را در قالب سه گروه Server Type، Configure WINS As و Expose Home Directories فراهم می‌کند. برای مشاهده این تنظیمات روی پیوند Wizard کلیک کنید. شکل ۱۱-۲۹ این تنظیمات را نشان می‌دهد.



شکل ۱۱-۲۹ امکانات برنامه Samba Configuration Wizard

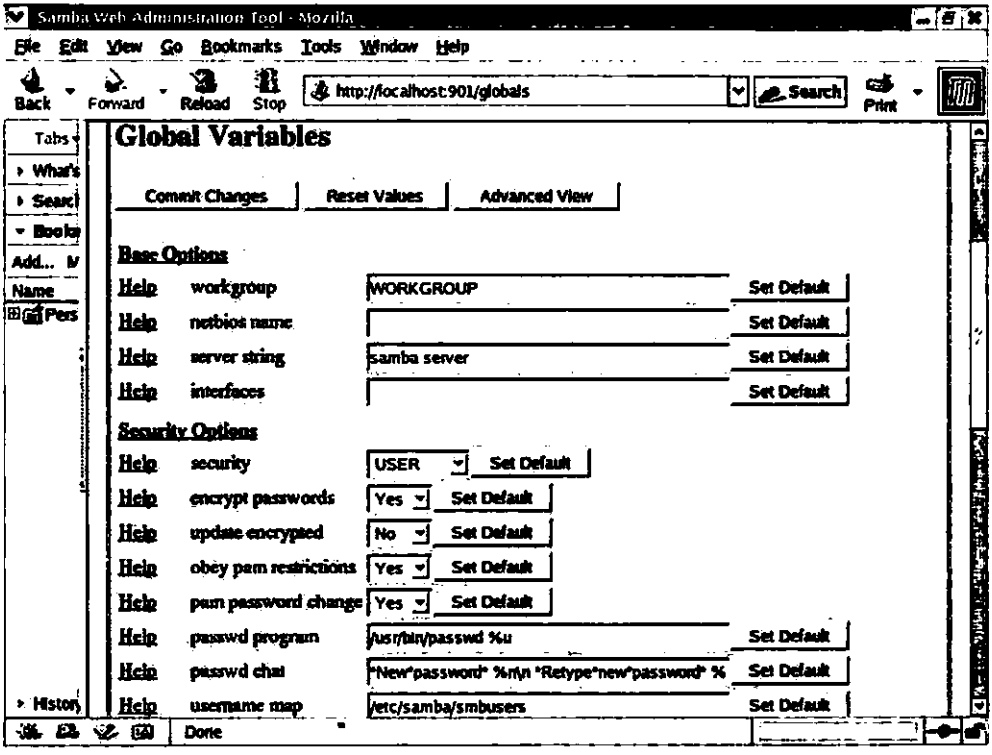
به شرح تنظیمات هر یک از این سه گروه توجه کنید:

- **گروه Server Type**: این دسته از تنظیمات که شامل سه گزینه است، امکان انتخاب یکی از انواع سرورهای مورد استفاده در شبکه‌های ویندوز یعنی Stand Alone، Domain Member و Domain Controller (کنترل کننده اصلی یا پشتیبان حوزه) را در اختیار قرار می‌دهد. چنان‌چه کامپیوتر میزبان سرور Samba در یک گروه کاری Peer-to-Peer مستقر شده باشد، گزینه Stand Alone تنها انتخاب مناسب است.
- **گروه Configure WINS As**: این دسته از تنظیمات نیز شامل سه گزینه بوده و امکان تعیین نقش سرور WINS را در اختیار قرار می‌دهد. انتخاب گزینه نخست به معنی انصراف از به کارگیری سرور WINS در شبکه است. گزینه دوم جهت پیکربندی کامپیوتر میزبان سرور Samba به عنوان سرور WINS پیش‌بینی شده است. گزینه سوم کامپیوتر میزبان سرور Samba را به عنوان کلاینتی برای سرور WINS پیکربندی می‌کند. در صورت انتخاب گزینه سوم لازم است آدرس IP کامپیوتر میزبان سرور WINS را در فیلد متنیRemote WINS Server وارد کنید. این دسته از تنظیمات مقادیر متغیرهای wins server و wins support از فایل پیکربندی smb.conf را تحت تأثیر قرار می‌دهند.
- **گروه Expose Home Directories**: این دسته از تنظیمات امکان مشاهده فهرست‌های خانگی کاربران را در اختیار آن‌ها قرار می‌دهد. تنظیمات مذکور مشخصات پیکربندی فهرست [home] را تحت تأثیر قرار می‌دهند. (برای اطلاع بیشتر به قسمت "پیکربندی فهرست مشترک [home] " در همین فصل مراجعه کنید.)

پس از انتخاب گزینه‌های موردنظر دکمه Commit را کلیک کنید. به احتمال قوی، برنامه Samba Configuration Wizard انتظارات شما را از یک برنامه ویزارد برآورده نمی‌کند، چرا که قبل از راه‌اندازی سرور Samba باید کارهای زیادی را انجام دهید.

منوی Globals

با استفاده از گزینه‌های موجود در منوی Globals می‌توانید تنظیمات مربوط به فهرست مشترک [global] در فایل پیکربندی smb.conf را تحت تأثیر قرار دهید. شکل ۱۲-۲۹ امکانات موجود در این منو را نشان می‌دهد.



شکل ۱۲-۲۹ منوی Globals

برای کسب راهنمایی درباره هریک از این گزینه‌ها کافی است روی پیوند Help موجود در کنار گزینه موردنظر کلیک کنید. با این اقدام مستندات فایل پیکربندی smb.conf در قالب نمونه جدیدی از پنجره مرورگر اینترنت باز شده و بخش مربوط به آن گزینه به نمایش درمی‌آید.

در تمام منوهای برنامه Samba Configuration Wizard از جمله منوی Globals سه دکمه Commit Values، Reset Values و Advanced View پیش‌بینی شده است. علاوه بر این، وجود دکمه Set Default در کنار هریک از تنظیمات قابل توجه است. جدول ۸-۲۹ عملکرد این دکمه‌ها را شرح می‌دهد.

چنان‌چه قسمت "تنظیمات سراسری سرویس Samba" را از این فصل مطالعه کرده باشید، اکنون با تنظیمات مختلفی آشنا هستید. با وجودی که قصد نداریم بحث مربوط به نحوه انجام این تنظیمات را تکرار کنیم، گروه‌بندی متغیرها مطمئناً به درک هر چه بیشتر این تنظیمات کمک خواهد کرد. شرح مختصری درباره هریک از این گروه‌ها در جدول ۹-۲۹ آمده است. تنظیمات برخی از گروه‌ها تنها با

کلیک دکمه Advanced View قابل دستیابی است. (به منظور حفظ جامعیت متن، از ترجمه عناوین گروه‌ها صرف نظر شده است. ـ مترجم)

جدول ۸-۲۹ شرح عملکرد دکمه‌های مورد استفاده در تنظیم مقادیر متغیرها

عنوان دکمه	توضیح عملکرد
Commit Changes	با کلیک این دکمه کلیه تغییرات انجام شده در فایل پیکربندی smb.conf به ثبت می‌رسد.
Reset Values	با کلیک این دکمه کلیه مقادیر متغیرها ری‌ست می‌شود، به این معنی که مقادیر اولیه متغیرها مجدداً به آن‌ها منسوب می‌گردد.
Advanced View	با کلیک این دکمه گزینه‌های پیشرفته مربوط به آن تنظیمات در اختیار قرار می‌گیرد.
Set Default	با کلیک این دکمه مقدار پیش‌فرض متغیر به آن منسوب می‌شود.

جدول ۹-۲۹ گروه‌بندی متغیرهای سراسری

عنوان گروه	توضیح
Base	این گروه شامل تنظیمات اولیه سرور Samba است.
Security	این گروه شامل تنظیمات مربوط به حساب کاربران و اعطای مجوز لازم برای دسترسی به سرور Samba است.
Logging	این گروه شامل تنظیمات مربوط به فایل‌های ثبت وقایع است.
Protocol	این گروه شامل تنظیماتی درباره چگونگی تعامل با پروتکل‌های مختلف ویندوز است.
Tuning	این گروه شامل تنظیماتی به منظور بهبود کارایی سرور Samba است.
Printing	این گروه شامل تنظیمات اولیه پروتکل مورد استفاده جهت تعامل با چاپگر است. گزینه‌های استاندارد سیستم‌عامل Linux در این رابطه شامل cups و lprng است.
Filename Handling	این گروه شامل تنظیماتی جهت مدیریت انتقال فایل‌هایی با اسامی کوتاه و بلند از یک کامپیوتر به دیگری است.
Domain	این گروه شامل تنظیمات مربوط به کاربران ارشد (مدیران) و کاربران میهمان است. این تنظیمات در صورتی مفید است که کامپیوتر میزبان سرور Samba به عنوان کنترل کننده اصلی یا پشتیبان حوزه (PDC یا BDC) پیکربندی شده باشد.
Logon	این گروه شامل تنظیماتی جهت کنترل دسترسی کاربران به سرور Samba است.

عنوان گروه	توضیح
	این تنظیمات در صورتی مفید است که کامپیوتر میزبان سرور Samba به عنوان کنترل کننده اصلی یا پشتیبان حوزه (PDC یا BDC) پیکربندی شده باشد.
Browse	این گروه شامل تنظیمات لازم برای پیکربندی کامپیوتر میزبان سرور Samba به عنوان master browser، یعنی کامپیوتر حاوی لیست منابع مشترک موجود در شبکه است.
WINS	این گروه شامل تنظیمات اولیه جهت استفاده از سرویس‌های WINS و DNS است.
Locking	این گروه شامل تنظیمات لازم جهت قفل کردن فایل‌هاست به طوری که تغییر هم‌زمان محتوای یک فایل توسط چند کاربر امکان‌پذیر نباشد..
MSDfs	این گروه شامل تنظیمات لازم جهت دسترسی به سیستم فایل MSDfs یا اصطلاحاً Microsoft Distributed Filesystem است.
Winbind	این گروه شامل تنظیمات لازم جهت استفاده از فایل پیکربندی /etc/nsswitch.conf به منظور ترجمه اسامی کامپیوترها به آدرس‌های IP است.

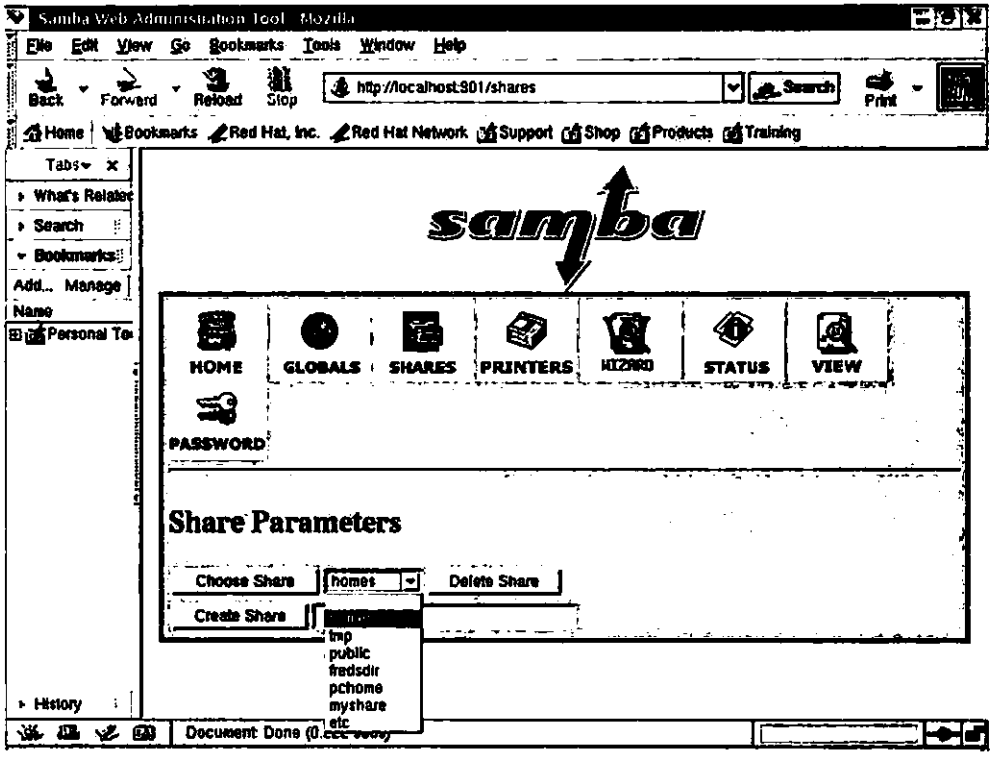
پس از انجام تغییرات مورد نظر، دکمه Commit را به منظور ثبت دایمی آن‌ها در فایل پیکربندی smb.conf کلیک کنید.

در کنار عنوان هریک از متغیرها در منوی Globals پیوندی با عنوان Help پیش‌بینی شده که با کلیک آن اطلاعات مفیدی درباره متغیرها به نمایش درمی‌آید.

منوی Shares

با امکانات موجود در منوی Shares می‌توانید فهرست‌های مشترک موجود را پیکربندی کرده یا فهرست جدیدی را به لیست منابع مشترک موجود اضافه کنید. شکل ۱۳-۲۹ محتوای این منو را نشان می‌دهد. پیش از پیکربندی فهرست مشترک موردنظر ابتدا باید آن‌را انتخاب کنید.

مشخصات مربوط به فهرست‌های مشترک، از جمله اسامی و شرایط دسترسی به آن‌ها در فایل smb.conf درج می‌شود. (در این میان می‌توان به دو نمونه [homes] و [tmp] اشاره کرد.) برای تغییر تنظیمات فهرست مشترک مورد نظر، ابتدا آن‌را از لیست فهرست‌های مشترک موجود انتخاب کرده و سپس دکمه Choose Share را کلیک کنید.

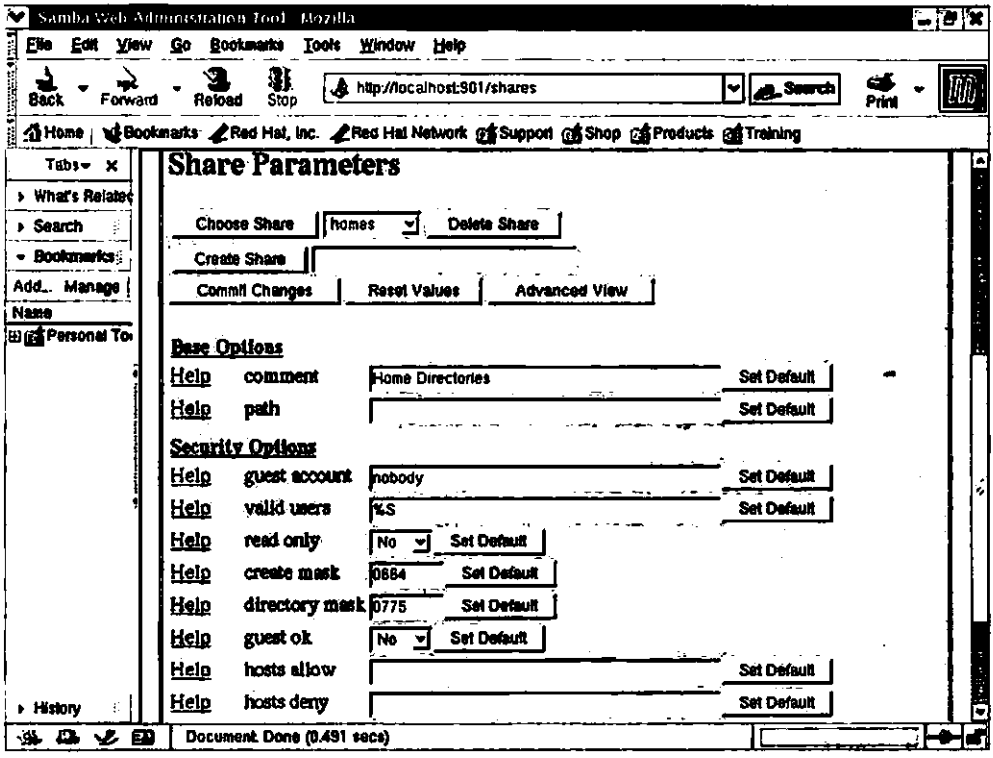


شکل ۱۳-۲۹ منوی Shares

برای اضافه کردن یک فهرست مشترک جدید به لیست فهرست‌های مشترک موجود نام آن فهرست را در فیلد متنی مقابل دکمه Create Share وارد کرده و دکمه نامبرده را کلیک کنید تا به این ترتیب منوی تنظیمات مربوط به آن باز شود. شکل ۱۴-۲۹ محتوای این منو را نشان می‌دهد.

چنان‌که مشاهده می‌کنید، این شکل حاوی تنظیمات فهرست مشترک [homes] است. (این تنظیمات را قبلاً در همین فصل مورد بررسی قرار دادیم.) برای دستیابی به تنظیمات پیشرفته‌تر، دکمه Advanced View را کلیک کنید.

پس از انجام تنظیمات موردنظر دکمه Commit Changes را به منظور ثبت دایمی آن‌ها در فایل پیکربندی smb.conf کلیک کنید.

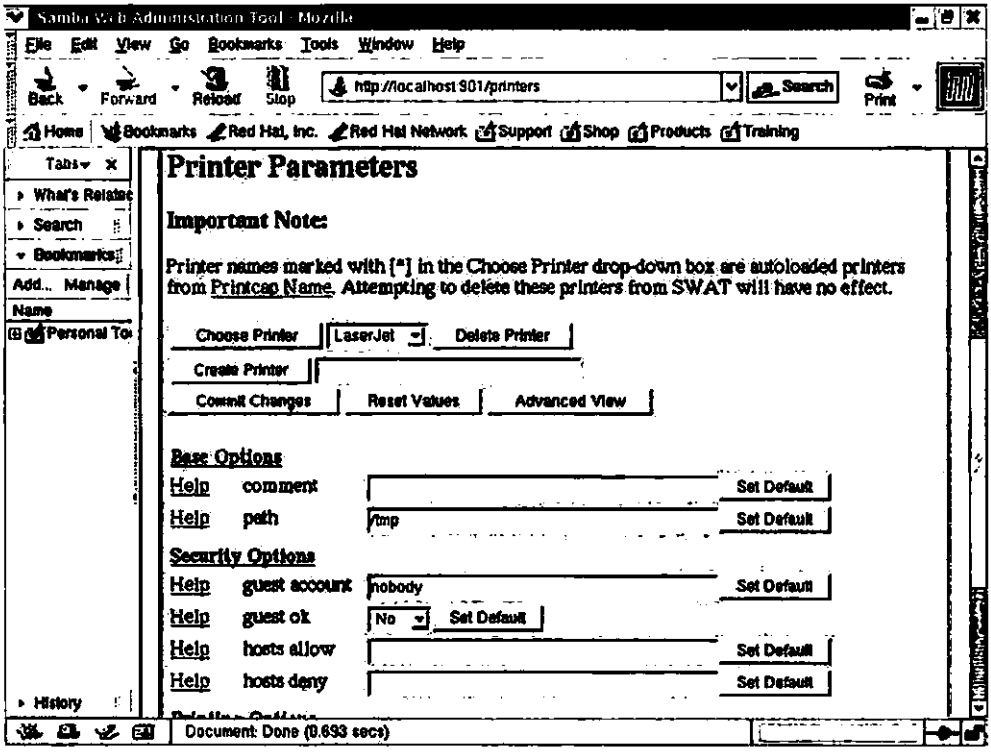


شکل ۱۴-۲۹ منوی تنظیمات منبع مشترک جدید

منوی Printers

محتوای منوی Printers شبیه به منوی Shares است. با امکانات موجود در این منو می‌توانید شرایط دسترسی به یک چاپگر را تغییر داده یا در صورت لزوم چاپگر جدیدی را به لیست چاپگرهای مشترک موجود اضافه کنید. بسته به اقدام موردنظر یکی از دکمه‌های Choose Printer یا Create Printer را کلیک کنید. اقلام لیست موجود در کنار دکمه Choose Printer از فهرست /etc/printcap تأمین می‌شود. به خاطر بیاورید که این فهرست حاوی لیست تمام چاپگرهای CUPS و LPD موجود است. پس از انتخاب چاپگر موردنظر می‌توانید تنظیمات مربوط به آن‌را تغییر دهید. شکل ۱۵-۲۹ منوی Printers را نشان می‌دهد.

پس از انجام تنظیمات موردنظر دکمه Commit Changes را جهت ثبت دایمی آن‌ها در فایل پیکربندی smb.conf کلیک کنید.

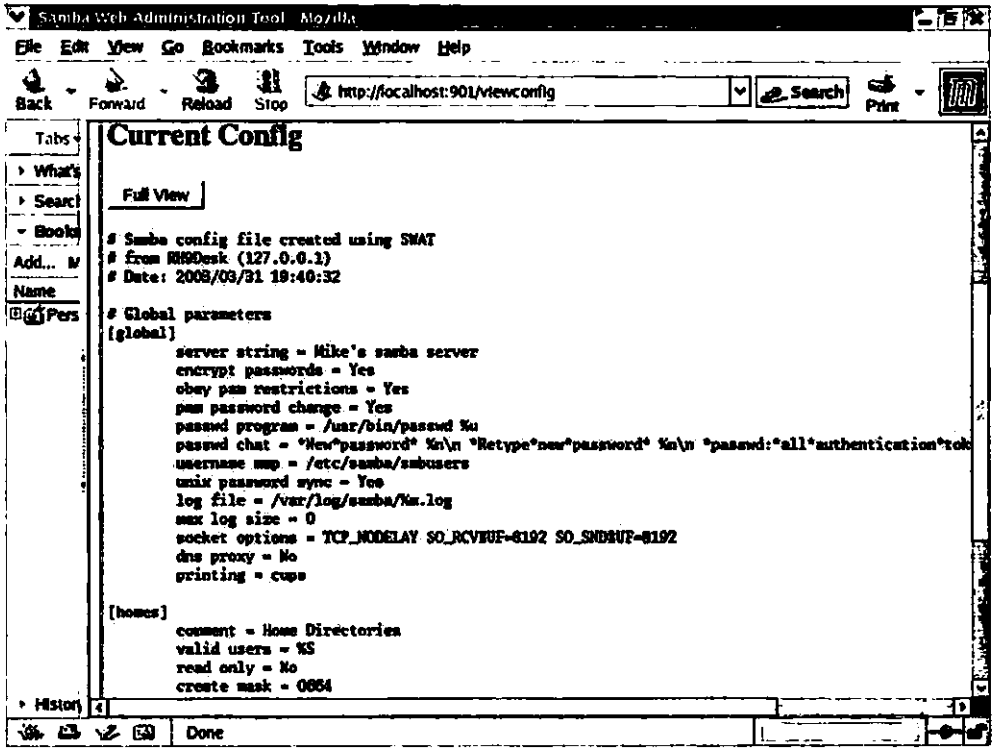


شکل ۱۵-۲۹ منوی Printers

منوی View

منوی View امکان مشاهده محتوای فعلی فایل پیکربندی smb.conf را در دو نمای عادی و کامل فراهم می‌کند. در نمای عادی، چنان‌که شکل ۱۶-۲۹ نشان می‌دهد، از نمایش بخش اعظم توضیحات مندرج در فایل مذکور و متغیرهای دارای مقادیر پیش‌فرض خودداری می‌شود.

با کلیک دکمه Full View محتوای فایل پیکربندی smb.conf در نمای کامل، شامل تنظیمات مربوط به تمام متغیرها (از جمله متغیرهای دارای مقادیر پیش‌فرض) به نمایش درمی‌آید. در این حالت برای دستیابی به نمای عادی کافی است دکمه Normal View را کلیک کنید.



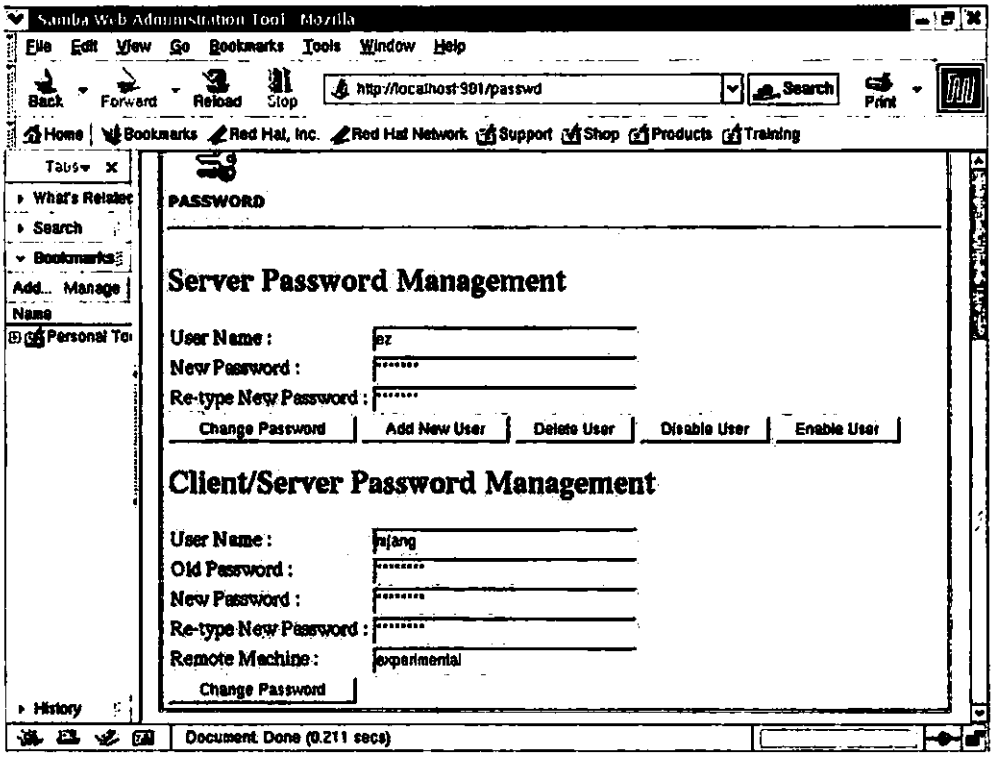
شکل ۱۶-۲۹ محتوای فایل پیکربندی smb.conf در نمای عادی

منوی Password

با امکانات موجود در منوی Password می‌توان تنظیمات مربوط به کلمات عبور موردنیاز جهت دسترسی به کامپیوترهای محلی یا راه دور میزبان سرور Samba یا ویندوز را انجام داد. چنان‌که در شکل ۱۷-۲۹ مشاهده می‌کنید، این امکانات به دو بخش Server Password Management و Client/Server Password Management تقسیم شده است. در قسمت‌های بعد به بررسی این دو بخش می‌پردازیم.

امکانات بخش Server Password Management

بخش Server Password Management از منوی Password امکان تغییر کلمات عبور مستقر روی کامپیوتر محلی میزبان سرور Samba را که هنگام برقراری ارتباط با کامپیوترهای راه دور میزبان سرور Samba یا ویندوز برای آن‌ها ارسال می‌شود، در اختیار قرار می‌دهد. شرح عملکرد دکمه‌های این منو در جدول ۱۰-۲۹ آمده است.



شکل ۱۷-۲۹ منوی Password

جدول ۱۰-۲۹ شرح عملکرد دکمه‌های منوی Password

عنوان دکمه	شرح عملکرد
Change Password	این دکمه امکان تغییر کلمات عبور کاربران سرویس Samba را در اختیار می‌گذارد. مشخصات این کاربران باید در فایل پیکربندی /etc/passwd موجود باشد.
Add New User	این دکمه امکان تعریف کاربر جدیدی را با درج مشخصات مربوطه در فایل /etc/samba/smbpasswd فراهم می‌کند. مشخصات کاربر موردنظر باید در فایل پیکربندی /etc/passwd موجود باشد. با وجود این، در مقایسه با فرمان smbadduser، این دکمه امکانات کمتری را در اختیار قرار می‌دهد.
Delete User	این دکمه امکان لازم برای حذف هریک از کاربران موجود را به واسطه حذف مشخصات مربوطه از فایل /etc/samba/smbpasswd در اختیار می‌گذارد.
Disable User	این دکمه امکان لازم برای پیشگیری از برقراری ارتباط هریک از کاربران با سرور Samba یا سرور ویندوز را در اختیار می‌گذارد.

عنوان دکمه	شرح عملکرد
Enable User	این دکمه امکان لازم برای برقراری ارتباط هریک از کاربران با سرور Samba یا سرور ویندوز را در اختیار آن‌ها قرار می‌دهد.

امکانات بخش Client/Server Password Management

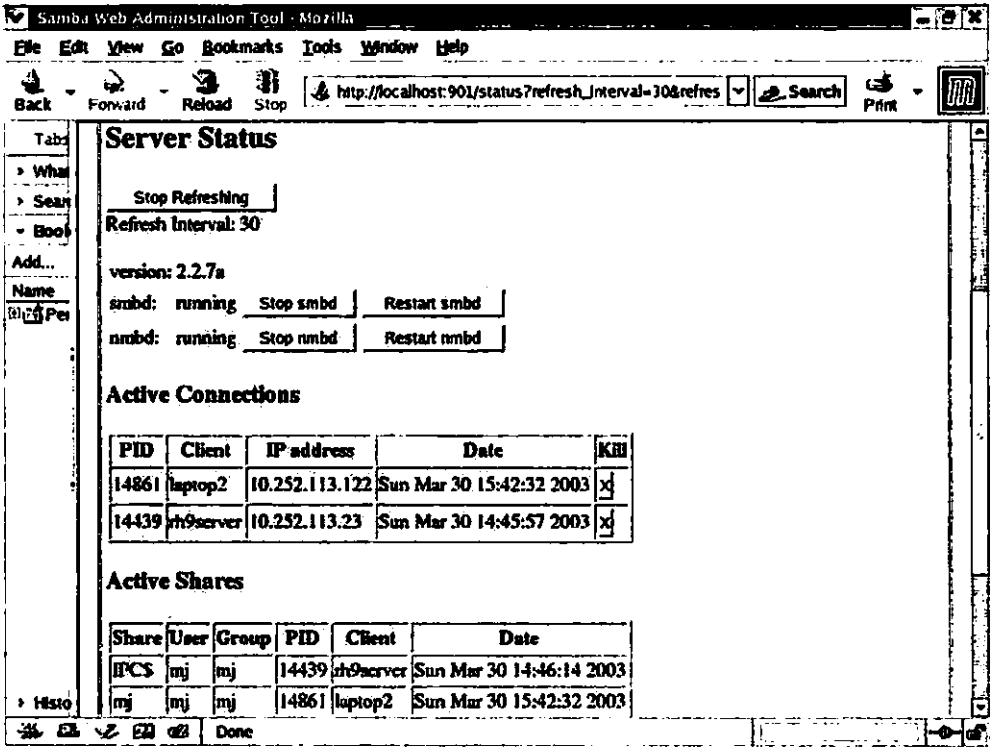
بخش Client/Server Password Management از منوی Password امکانات لازم برای تغییر کلمات عبور مستقر روی کامپیوترهای راه دور میزبان سرور Samba یا ویندوز را در اختیار می‌گذارد. چنان‌که در شکل ۱۷-۲۹ مشاهده می‌کنید، اقدام لازم برای تغییر کلمه عبور کاربری با شناسه mjang از کامپیوتری با نام experimental که میزبانی سرور ویندوز 2000 را به عهده دارد، انجام شده است. چنان‌چه کامپیوتری با نام experimental در فایل /etc/hosts، یا بانک اطلاعاتی سرویس DNS یا WINS به ثبت نرسیده باشد، این اقدام با شکست مواجه خواهد شد. اقدام فوق هم‌چنین در صورتی که شناسه کاربر mjang روی کامپیوتر نامبرده (یعنی کامپیوتری با نام experimental) فاقد اعتبار باشد، محکوم به شکست خواهد بود.

منوی Status

بازبینی وضعیت سرور Samba یکی از اقدامات مهمی است که باید آن‌را پس از شروع برقراری ارتباط کاربران با آن به طور مرتب انجام دهید. منوی Status امکانات لازم برای این کار را در اختیار قرار می‌دهد. برای مثال، شکل ۱۸-۲۹ وضعیت سرور Samba را پس از برقراری ارتباط کامپیوترهای rh9server و laptop2 با آن نشان می‌دهد.

این منو یکی از قابلیت‌های چشمگیر ابزار SWAT است. چنان‌که مشاهده می‌کنید، به روز رسانی این اطلاعات هر ۳۰ ثانیه یکبار انجام می‌شود. با کلیک دکمه Stop Refreshing می‌توان از به روز رسانی خودداری کرد. علاوه بر این، دکمه‌هایی نیز به منظور متوقف کردن و راه‌اندازی مجدد برنامه‌های smbd و nmbd پیش‌بینی شده‌اند. جدول Active Connections حاوی برخی اطلاعات مفید درباره کامپیوترهایی است که اقدام آن‌ها برای برقراری ارتباط با سرور Samba موفقیت‌آمیز بوده است. با کلیک دکمه X در ستون Kill از هر سطر این جدول می‌توان به ارتباط کامپیوتر مربوطه با سرور Samba پایان داد.

فراموش نکنید کمترین تغییر در فایل پیکربندی smb.conf مستلزم راه‌اندازی مجدد برنامه smbd است. برنامه نامبرده به طور خودکار برنامه nmbd را راه‌اندازی می‌کند.

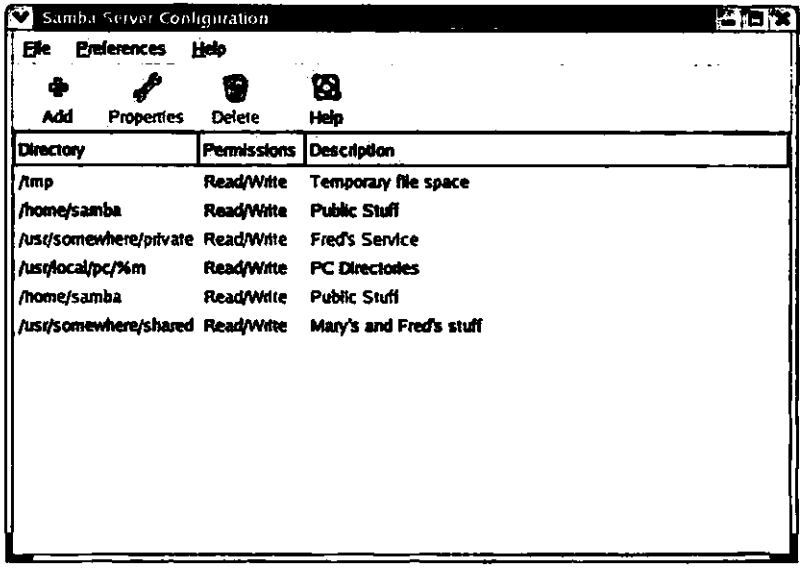


شکل ۱۸-۲۹ وضعیت سرور Samba پس از برقراری ارتباط موفقیت‌آمیز دو کامپیوتر rh9server و laptop2 با آن

ابزار پیکربندی redhat-config-samba

ابزار SWAT تا اندازه‌ای ممکن است پیچیده به نظر برسد. برنامه redhat-config-samba ابزاری است که توسط شرکت Red Hat به منظور پیکربندی سرویس Samba طراحی شده و با وجود قابلیت‌های محدودتر نسبت به ابزار SWAT کار کردن با آن ساده‌تر است. برای استفاده از این ابزار ابتدا باید بسته نرم‌افزاری مربوطه را نصب و سپس فرمانی با همین نام، یعنی redhat-config-samba را اجرا کنید. شکل ۱۹-۲۹ پنجره مربوط به این برنامه را نشان می‌دهد.

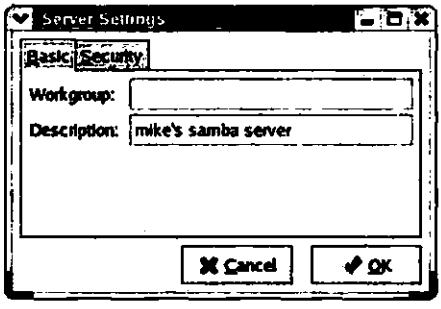
در قسمت‌های بعد نحوه تنظیمات اصلی سرور Samba، مدیریت کاربران و تعریف یک فهرست مشترک جدید را با استفاده از این ابزار مورد بررسی قرار می‌دهیم.



شکل ۱۹-۲۹ پنجره برنامه redhat-config-samba

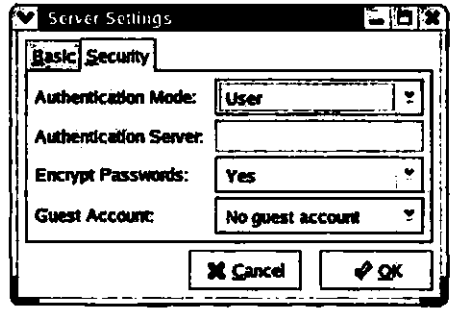
تنظیمات اصلی سرور Samba

برای دسترسی به این تنظیمات گزینه Server Settings از منوی Preferences واقع در پنجره اصلی برنامه redhat-config-samba را انتخاب کنید تا کادر محاوره‌ای مربوطه با عنوان Server Settings باز شود. شکل ۲۰-۲۹ بخش Basic از این کادر محاوره‌ای را نشان می‌دهد. چنان‌که مشاهده می‌کنید، این تنظیمات بسیار ساده هستند. خالی بودن فیلد متنی Workgroup به معنی استفاده از مقدار پیش‌فرض متغیر workgroup است. (مقدار پیش‌فرض این متغیر WORKGROUP است.) توصیف کامپیوتر میزبان سرور Samba نیز به صورت "Mike's Samba Server" در فیلد متنی Description درج شده است.



شکل ۲۰-۲۹ تنظیمات بخش Basic از کادر محاوره‌ای Server Settings

بخش Security از کادر محاوره‌ای Server Settings حاوی تنظیماتی در ارتباط با امنیت سرور Samba است. خط مشی سرور مذکور جهت احراز هویت کاربران با انتخاب یکی از گزینه‌های موجود در لیست Authentication Modes مشخص می‌شود. این لیست شامل چهار گزینه Share، User، Server و Domain است. در صورت انتخاب گزینه Server یا Domain، در فیلد متنی Authentication Server نام کامپیوتری را وارد کنید که وظیفه احراز هویت را انجام می‌دهد. هم‌چنین در صورت رمزگذاری کلمات عبور، گزینه Yes را از لیست Encrypt Passwords انتخاب کنید. رمزگذاری کلمات عبور در اغلب سرورهای ویندوز متداول است. چنان‌چه مشخصات کاربر میهمان قبلاً در فایل پیکربندی /etc/passwd درج شده باشد، اکنون می‌توان آن‌را از لیست Guest Account انتخاب کرد. شکل ۲۱-۲۹ تنظیمات موجود در بخش Security از کادر محاوره‌ای Server Settings را نشان می‌دهد.

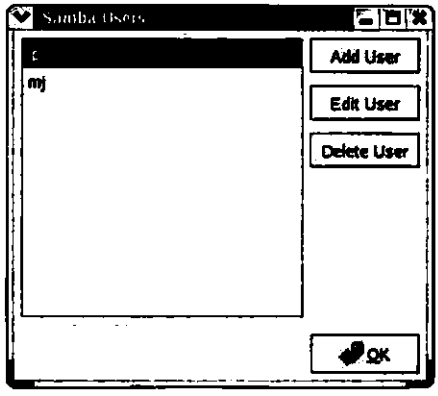


شکل ۲۱-۲۹ تنظیمات بخش Security از کادر محاوره‌ای Server Settings

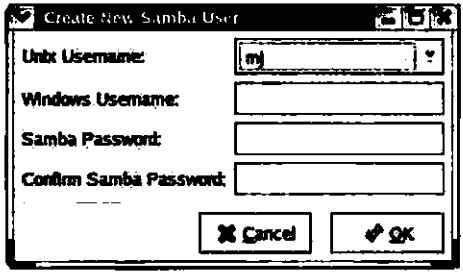
مدیریت کاربران

کادر محاوره‌ای Samba Users در برنامه redhat-config-samba شامل تمام امکانات موردنیاز برای مدیریت کاربران است. برای دسترسی به کادر محاوره‌ای مذکور کافی است گزینه Samba Users را از منوی Preferences انتخاب کنید. شکل ۲۲-۲۹ این کادر محاوره‌ای را نشان می‌دهد.

به‌کمک این امکانات می‌توان کاربر جدیدی را با درج مشخصات مربوطه در فایل /etc/samba/smbusers تعریف کرد. هم‌چنین می‌توان مشخصات هریک از کاربران را مورد ویرایش قرار داده یا کاربر دلخواهی را از لیست کاربران موجود حذف کرد. برای تعریف کاربر جدید دکمه Add User را کلیک کنید تا مطابق شکل ۲۳-۲۹ کادر محاوره‌ای دیگری با عنوان Create New Samba User باز شود. چنان‌چه قبلاً قسمت مربوط به فرمان smbadduser از این فصل را مطالعه کرده باشید، اکنون با نحوه تنظیمات این کادر محاوره‌ای آشنا خواهید بود.



شکل ۲۲-۲۹ کادر محاوره‌ای Samba Users

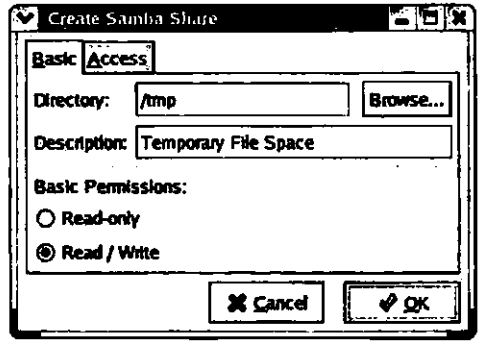


شکل ۲۳-۲۹ کادر محاوره‌ای Create New Samba User

تعریف فهرست‌های مشترک جدید

در برنامه redhat-config-samba امکانات لازم برای تعریف فهرست‌های مشترک نیز پیش‌بینی شده است. برای این منظور دکمه Add از پنجره اصلی برنامه مذکور را کلیک کنید تا مطابق شکل ۲۴-۲۹ امکانات موردنیاز برای انجام این کار در قالب کادر محاوره‌ای Create Samba Share در دسترس قرار بگیرد.

با وجودی که این تنظیمات بسیار ساده هستند، به دلیل تفاوت عناوین فیلدهای متنی موجود در بخش Basic از این کادر محاوره‌ای با عناوین متغیرهای مشابه در فایل پیکربندی smb.conf، شرح مختصری از آن‌ها را در جدول ۱۱-۲۹ آورده‌ایم.



شکل ۲۴-۲۹ کادر محاوره‌ای Create Samba Share

جدول ۱۱-۲۹ شرح تنظیمات بخش Basic از کادر محاوره‌ای Create Samba Share

عنوان فیلد متنی	توضیح
Directory	این فیلد حاوی نام فهرست مشترک است.
Browse	با کلیک روی این دکمه کادر محاوره‌ای Select Directory باز شده و تسهیلاتی را به منظور انتخاب فهرست مشترک در اختیار می‌گذارد.
Description	این فیلد حاوی توصیفی از فهرست مشترک است.
Read-Only	انتخاب این گزینه از نوشتن در فهرست مشترک جلوگیری می‌کند.
Read/Write	انتخاب این گزینه امکان نوشتن در فهرست مشترک را در اختیار کاربران قرار می‌دهد.

به کمک تنظیمات بخش Access از کادر محاوره‌ای Create Samba Share می‌توان مجوز دسترسی به فهرست مشترک را در اختیار تمام کاربران یا تنها کاربرانی که مشخصات آن‌ها در فایل /etc/samba/smbusers درج شده است، قرار داد.

جمع‌بندی

سرویس Samba به منظور پر کردن خلأ میان کامپیوترهای ویندوز و Linux طراحی شده است. قابلیت‌های این سرویس به اندازه‌ای است که می‌توان کامپیوتر میزبان سرور Samba را در یک حوزه یا گروه کاری به عنوان Member Server و حتی کنترل کننده اصلی حوزه (اصطلاحاً PDC) در شبکه‌های ویندوز پیکربندی کرد.

علاوه بر این، کامپیوترهای Linux را می‌توان به عنوان کلاینت Samba نیز پیکربندی کرد. با نصب بسته‌های نرم‌افزاری مناسب حتی می‌توان فرمان mount را از سطر فرمان کامپیوتر دیگری که میزبانی سرور Samba یا ویندوز را به عهده دارد، جهت دسترسی به فهرست مشترک اجرا کرد. مشابه سرویس FTP، سرویس Samba دسترسی به فهرست‌های مشترک را از طریق ترمینال نیز در اختیار کاربران قرار می‌دهد.

فایل‌های پیکربندی سرویس Samba در فهرست /etc/samba واقع هستند. عنوان فایل پیکربندی اصلی این سرویس smb.conf است. فایل مذکور که در قالب بسته نرم‌افزاری *-samba روی کامپیوتر میزبان نصب می‌شود، حاوی توضیحاتی درباره نحوه پیکربندی آن است.

فایل پیکربندی smb.conf شامل یکسری تنظیمات سراسری است. با این تنظیمات می‌توان نحوه برقراری ارتباط کامپیوتر میزبان سرور Samba با کامپیوترهای ویندوز را مشخص کرد. تنظیمات مزبور مواردی از قبیل خط‌مشی امنیت دسترسی به سرور Samba، لیست چاپگرهای مشترک و فایل‌های ثبت وقایع را شامل می‌شود. فایل پیکربندی smb.conf شامل تنظیمات دیگری است که به کمک آن می‌توان خط‌مشی دسترسی به فهرست‌ها و چاپگرهای مختلف را تعیین کرد. همین تنظیمات امکان محدود کردن دسترسی برخی از کاربران به منابع مشترک، خواندن و نوشتن در فهرست‌های مشترک و سایر موارد را در اختیار قرار می‌دهد. پس از انجام تنظیمات موردنظر در فایل smb.conf، با استفاده از برنامه testparm می‌توان خطاهای پیکربندی را تشخیص داده و برای رفع آن‌ها اقدام کرد.

ابزار پیکربندی SWAT یک برنامه تحت وب است که به منظور پیکربندی فایل smb.conf طراحی شده است. برای استفاده از این ابزار لازم است در برنامه xinted سرویس swat را فعال کنید. تنظیمات ابزار پیکربندی SWAT از طریق منوهای Home، Global، Share، View، Password و Status قابل دستیابی است.

شرکت Red Hat نیز برنامه‌ای با نام redhat-config-samba را به عنوان ابزاری برای پیکربندی سرویس Samba به همراه سیستم‌عامل خود توزیع می‌کند. از آن‌جا که مدت زمان زیادی از معرفی این برنامه نمی‌گذرد، باید در استفاده از آن دقت کنید. با آن‌که این برنامه امکانات قابل قبولی را به منظور پیکربندی منابع مشترک در اختیار می‌گذارد، فاقد برخی قابلیت‌های مفید ابزار پیکربندی SWAT است. به عقیده بسیاری از صاحبنظران، برنامه تحت وب SWAT تا به حال مناسب‌ترین ابزار پیکربندی سرویس Samba محسوب می‌شود.

در فصل بعد به بررسی مهم‌ترین وب سرور موجود یعنی Apache خواهیم پرداخت. ضمن این بررسی با چگونگی پیکربندی آن به منظور سرویس‌دهی صفحات وب در شبکه محلی و موارد دیگر آشنا خواهید شد.

فصل سی‌ام

سرویس‌های وب

سیستم عامل Linux تقریباً به موازات رشد وب توسعه پیدا کرد. چنان‌که در فصل اول نیز اشاره شد، این سیستم‌عامل نتیجه فعالیت داوطلبانه مجموعه‌ای از توسعه دهندگان نرم‌افزار است. کار توسعه وب سرور Apache نیز که امروزه متداول‌ترین نرم‌افزار در این زمینه محسوب می‌شود، توسط اعضای همین مجموعه انجام شده است. به این ترتیب، جای تعجب نیست که موفقیت سیستم‌عامل Linux با محبوبیت وب سرور Apache و گسترش روزافزون استفاده از وب رابطه مستقیم داشته باشد.

در سال ۱۹۹۵ متداول‌ترین وب سرور موجود با عنوان HTTP daemon محصول بخش ویژه‌ای از دانشگاه ایلی‌نویز با نام NCSA یا اصطلاحاً National Center for Supercomputing Applications بود. پس از آن‌که توسعه‌دهندگان این وب سرور مرکز NCSA را ترک گفتند، بسیاری از توسعه دهندگان نرم‌افزار در تمام کشورها با توسعه قطعات نرم‌افزارهای متعددی موسوم به patch برای گسترش و رواج هرچه بیشتر آن تلاش کردند. کم‌کم به دلیل کثرت قابل توجه این قطعات نرم‌افزاری عنوان آن به "a patchy server" تغییر کرد. امروزه این نرم‌افزار با عنوان Apache به شهرت جهانی رسیده است.

سیستم‌عامل Linux یکی از محیط‌های مناسب برای بهره‌برداری از وب سرور Apache است. البته این وب سرور در سایر محیط‌ها از جمله UNIX و Microsoft Windows نیز قابل استفاده است. بر اساس تحقیقات شرکت Netcraft، وب سرور Apache از سال ۱۹۹۶ متداول‌ترین نرم‌افزار در این زمینه محسوب می‌شود. (برای مشاهده گزارشات مربوطه به وب سایت http://www.netcraft.com/survey مراجعه کنید.)

در این فصل به بررسی نگارشی از وب سرور Apache که با شاخص 2.0.40 منتشر شده است، خواهیم پرداخت. (این نگارش از نرم‌افزار نامبرده به همراه سیستم‌عامل Red Hat Linux 9 توزیع می‌شود.) دسترسی به جدیدترین نسخه این نرم‌افزار همواره با مراجعه به وب سایت http://httpd.apache.org امکان‌پذیر است. عنوان وب سرور دیگری که به همراه نگارش Advanced Server سیستم‌عامل Red Hat Linux توزیع می‌شود، Stronghold Enterprise است. کار توسعه این وب سرور بر اساس Apache انجام شده است.

عنوان وب سرور دیگر مورد بررسی در این فصل Content Accelerator است که سابقاً Tux نامیده می‌شد. از ان‌جا که کد این نرم‌افزار درون هسته سیستم‌عامل جاسازی شده است، کارآیی قابل توجهی در سرویس‌دهی، به ویژه سرویس‌دهی محتوای استاتیک (هم‌چون تصاویر) دارد. کار توسعه این وب سرور توسط شرکت Red Hat و بر اساس Apache انجام شده است. به طور خلاصه، در فصل حاضر به بررسی این موضوعات می‌پردازیم:

- مروری بر وب سرورهای موجود
- مقدمه‌ای بر وب سرور Apache
- پیکربندی وب سرور Apache
- بررسی اجمالی وب سرور Content Accelerator

مروری بر وب سرورهای موجود

نرم‌افزار Apache تنها یکی از وب سرورهای موجود است. در حالی‌که برخی از آن‌ها رایگان است، برای تهیه برخی دیگر باید بهای آن‌را به شرکت مربوطه پرداخت کنید. شرح تعدادی از این وب سرورها در جدول ۱-۳۰ آمده است. بنا به گزارشات منتشر شده از جانب شرکت Netcraft، چهار وب سرور Apache، Microsoft Internet Information Server، Zeus و Sun One به ترتیب بیشترین سهم را در این زمینه به خود اختصاص داده‌اند.

جدول ۱-۳۰ شرح مختصری درباره برخی از وب سرورهای متداول

عنوان وب سرور	توضیح
AOLServer	این وب سرور یک نرم‌افزار کد باز است که اغلب به منظور استفاده در شبکه AOL (اصطلاحاً America Online) مورد استفاده قرار می‌گیرد. برای توضیح بیشتر به وب سایت مربوطه در آدرس http://www.aolserver.com مراجعه کنید.
Apache	این وب سرور متداول‌ترین نرم‌افزار در این زمینه است. برای اطلاع بیشتر به وب سایت مربوطه در آدرس http://httpd.apache.org مراجعه کنید.
Boa	این وب سرور یک نرم‌افزار کد باز با کارایی بالا در این زمینه است. برخلاف نرم‌افزارهای مشابه، این وب سرور بیشتر اتصالات استاندارد را تنها در قالب یک فرآیند ساده کنترل می‌کند. برای اطلاع بیشتر به وب سایت مربوطه در آدرس http://www.boa.org مراجعه کنید.

عنوان وب سرور	توضیح
Caudium	این وب سرور یک نرم‌افزار کد باز است. ساختار آن متشکل از ماجول‌های متعدد است و مشابه وب سرور Boa بیشتر اتصالات استاندارد را تنها در قالب یک فرآیند ساده کنترل می‌کند. برای اطلاع بیشتر به وب سایت http://www.caudium.net مراجعه کنید.
Jigsaw	این وب سرور محصول کنسرسیوم W3C یا به اختصار World Wide Web Consortium است. برای اطلاع بیشتر درباره آن به وب سایت مربوطه در آدرس http://www.w3c.org/Jigsaw مراجعه کنید. (کلیه نرم‌افزارهای تولید شده توسط این‌کنسرسیوم تحت‌لیسانس نرم‌افزارهای کد باز توزیع می‌شود.)
Red Hat Content Accelerator	این وب سرور (که سابقاً TUX نامیده می‌شد) نرم‌افزاری با کارایی بالاست که توسط شرکت Red Hat طراحی و تولید شده است. کد این نرم‌افزار درون هسته سیستم‌عامل جاسازی شده است. برای اطلاع بیشتر در این زمینه مستندات مربوطه در آدرس http://www.redhat.com/docs/manuals/tux را مورد مطالعه قرار دهید.
Resin	این وب سرور به منظور سرویس‌دهی محتوای JSP (اصطلاحاً Java Server Pages) طراحی شده است. برای خریداری آن یا دسترسی به اطلاعات بیشتر به وب سایت مربوطه در آدرس http://www.caucho.com/resin مراجعه کنید.
Roxin	این وب سرور دارای شاخص‌های امنیتی قابل توجه بوده و به عنوان یک نرم‌افزار کد باز تحت لیسانس GPL منتشر شده است. برای اطلاع بیشتر درباره‌آن به‌وب‌سایت مربوطه‌درآدرس http://www.roxin.com مراجعه کنید.
Servertec	این وب سرور یک نرم‌افزار کد باز است که به زبان Java نوشته شده است. برای‌اطلاع‌بیشتر به وب سایت مربوطه در آدرس http://www.servertec.com مراجعه کنید.
Stronghold	این وب سرور دارای شاخص‌های امنیتی قابل توجه بوده و توسعه آن بر اساس وب سرور Apache انجام شده است. وب سرور Stronghold متعلق به شرکت Red Hat بوده و در قالب نگارش Advanced Server سیستم‌عامل Red Hat Linux توزیع می‌شود. برای اطلاع بیشتر درباره آن به وب سایت مربوطه در آدرس http://www.redhat.com/software/stronghold مراجعه کنید.

عنوان وب سرور	توضیح
Sun One	این وب سرور که سابقاً iPlanet نامیده می‌شد، محصول شرکت Sun Microsystem است. برای اطلاع بیشتر به وب سایت مربوطه در آدرس http://www.sun.com/software مراجعه کنید.
WN	این وب سرور یک نرم‌افزار کوچک با شاخص‌های امنیتی بالاست که تحت لیسانس GPL منتشر می‌شود. برای اطلاع بیشتر درباره آن به وب سایت http://hopf.math.nwu.edu مراجعه کنید.
Zeus	این وب سرور یک نرم‌افزار تجاری با ظرفیت سرویس‌دهی قابل توجه است. برای اطلاع بیشتر درباره آن به وب سایت مربوطه در آدرس http://www.zeus.co.uk مراجعه کنید.

مقدمه‌ای بر وب سرور Apache

نرم‌افزار Apache یک وب سرور است. به بیان دقیق‌تر، سرویسی است که روی یک سیستم‌عامل سرور هم‌چون Linux به اجرا درآمده و به درخواست‌های مربوطه پاسخ می‌دهد. پس از درج آدرس سند وب موردنظر در فیلد آدرس مرورگر وب، کامپیوتر میزبان جهت اطلاع از آدرس IP وب سرور مربوطه جستجویی را در بانک‌های اطلاعاتی سرورهای DNS انجام می‌دهد. پس از اطلاع از این آدرس IP، درخواست سند موردنظر از طریق پورت شماره ۸۰ برای کامپیوتر میزبان آن وب سرور ارسال می‌شود. در نهایت، وب سرور سند درخواستی را برای مرورگر ارسال می‌کند.

تا زمان انتشار کتاب حاضر، نگارش 1.3.x جدیدترین نگارش قابل اطمینان از وب سرور Apache محسوب می‌شود. در صورتی که به استفاده از نگارش‌های جدیدتر، هم‌چون 2.0.40 تمایل دارید، باید تنظیمات مربوط به چند پیکربندی را تغییر دهید. پیش از اطمینان درباره عملکرد صحیح نگارش‌های جدید وب سرور Apache در میزبانی وب سایت‌های موجود، از به کارگیری آن‌ها خودداری کنید.

وب سرور Apache 2.0

نگارش 2.0.x از وب سرور Apache نخستین بار به همراه سیستم‌عامل Red Hat Linux 8.0 توزیع شد. با این وجود، نگارش 1.3.x از وب سرور مذکور هم‌چنان متداول است. در ادامه به تغییرات عمده‌ای که در نگارش 2.0.x نسبت به نگارش‌های قبلی صورت گرفته است، اشاره می‌کنیم:

- ویژگی Virtual Hosting در نگارش جدید امکان پیکربندی وب سایت‌های مختلف را با یک آدرس IP واحد در اختیار می‌گذارد.

- دستورالعمل‌ها تا اندازه‌ای دستخوش تغییر شده‌اند. برای دستورالعمل‌های Perl، PHP، Python، SQL و SSL در فهرست /etc/httpd/conf.d فایل‌های پیکربندی مجزایی پیش‌بینی شده است.
- برخی از متغیرها دستخوش تغییر شده‌اند. برای مثال، متغیر Listen در ویرایش جدید امکان تغییر پورت TCP/IP مورد استفاده وب سرور Apache را در اختیار می‌گذارد.
- ویژگی ماجولار اکنون بیش از پیش محسوس است به‌طوری که نسبت به گذشته اجزای نرم‌افزاری بیشتری در قالب ماجول پیاده‌سازی شده‌اند.
- استفاده از مکانیزم thread به طور مؤثرتری نسبت به قبل انجام شده است. این مکانیزم روش مؤثری برای اشتراک داده‌ها محسوب می‌شود. در نگارش جدید، این مکانیزم بر اساس فرآیندها پیاده‌سازی شده است. این موضوع باعث پیشگیری از اختلال در کار سرور می‌شود. اکنون ماجول‌های MPM (اصطلاحاً Multi-Processing Modules) را می‌توان به منظور حصول بیشترین کارآیی با توجه به سیستم‌عامل میزبان پیکربندی کرد.
- آدرس‌دهی به روش IPv6 امکان‌پذیر شده است. این قابلیت در نگارش‌های قبلی به واسطه یک قطعه نرم‌افزاری جداگانه تأمین می‌شد.

تمام ویژگی‌های فوق ابتدا در نگارش جدید Apache 2.0 معرفی شدند. با وجود این، برخی از آن‌ها در قالب قطعات نرم‌افزاری جداگانه به نگارش 1.3.x نیز اضافه شده‌اند. (همین موضوع یکی از دلایلی است که نگارش مذکور در حال حاضر نیز به طور گسترده مورد استفاده قرار می‌گیرد.)

بسته‌های نرم‌افزاری موردنیاز برای نصب وب سرور Apache

وب سرور Apache نرم‌افزاری متشکل از ماجول‌هاست. چنان‌که در فصل پنجم از فصول اینترنتی کتاب نیز توضیح داده شده، عنوان تنها بسته نرم‌افزاری موردنیاز برای نصب این وب سرور httpd-* است. با وجود این، بسته‌های نرم‌افزاری دیگری نیز در همین زمینه وجود دارد. شرح مختصری از آن‌ها در جدول ۲-۳۰ آمده است.

جدول ۲-۳۰ بسته‌های نرم‌افزاری قابل استفاده در وب سرور Apache

عنوان بسته نرم‌افزاری	توضیح
httpd	این بسته نرم‌افزاری حاوی فایل‌های اصلی وب سرور Apache است.
httpd-manual	این بسته نرم‌افزاری حاوی مستندات وب سرور Apache است.
hwcrypto	این بسته نرم‌افزاری به منظور پشتیبانی از سیستم‌های رمزگذاری ویژه‌ای موسوم

عنوان بسته نرم‌افزاری	توضیح
	به Hardware Cryptographic System طراحی شده است.
mod-auth-pgsql	این بسته نرم‌افزاری به منظور احراز هویت کاربران در دسترسی به بانک‌های اطلاعاتی PostgreSQL طراحی شده است.
mod-auth-mysql	این بسته نرم‌افزاری به منظور احراز هویت کاربران در دسترسی به بانک‌های اطلاعاتی MySQL طراحی شده است.
mod-python	این بسته نرم‌افزاری به منظور پشتیبانی از برنامه‌های Python طراحی شده است.
mod-perl	این بسته نرم‌افزاری به منظور پشتیبانی از برنامه‌های Perl طراحی شده است.
mod-ssl	این بسته نرم‌افزاری به منظور پشتیبانی از مکانیزم امنیتی SSL طراحی شده است.
php	این بسته نرم‌افزاری به منظور پشتیبانی از برنامه‌های PHP طراحی شده است.
php-imap	این بسته نرم‌افزاری به منظور پشتیبانی از سرور پست الکترونیکی IMAP طراحی شده است.
php-ldap	این بسته نرم‌افزاری به منظور پشتیبانی از مکانیزم LDAP طراحی شده است.
php-mysql	این بسته نرم‌افزاری به منظور پشتیبانی از برنامه‌های PHP جهت دسترسی به بانک‌های اطلاعاتی MySQL طراحی شده است.
php-odbc	این بسته نرم‌افزاری به منظور پشتیبانی از برنامه‌های PHP جهت دسترسی به بانک‌های اطلاعاتی از طریق رابط ODBC طراحی شده است.
php-pgsql	این بسته نرم‌افزاری به منظور پشتیبانی از برنامه‌های PHP جهت دسترسی به بانک‌های اطلاعاتی PostgreSQL طراحی شده است.
squid	این بسته نرم‌افزاری حاوی فایل‌های موردنیاز برای نصب پروکسی سرورsquid است.
tux	این بسته نرم‌افزاری حاوی فایل‌های موردنیاز برای نصب وب سرور TUX است.
webalizer	این بسته نرم‌افزاری حاوی برنامه‌ای برای تحلیل میزان دسترسی به وب سرور Apache است.

پیکربندی وب سرور Apache

پس از نصب بسته‌های نرم‌افزاری مورد نظر، وب سرور Apache آماده پاسخ‌گویی به درخواست‌های ارسالی از کامپیوتر میزبان است. برای این منظور کافی است سرویس httpd را راه‌اندازی کنید. برای اطمینان از این موضوع عبارت localhost را در نوار آدرس مرورگر وب درج کرده و کلید Enter را فشار دهید. با این اقدام باید صفحه خوش‌آمدگویی وب سرور Apache را مشاهده کنید.

با وجود این، عملکرد وب سرور نباید محدود به درخواست‌های ارسالی از کامپیوتر میزبان باشد. به بیان دیگر، باید بتواند به درخواست‌های ارسالی از سایر کامپیوترها نیز پاسخ داده و اسناد موردنظر را در اختیار آن‌ها قرار دهد. در این فصل فایل پیکربندی اصلی وب سرور Aapache با عنوان httpd.conf را مورد بررسی نسبتاً دقیق قرار خواهیم داد.

این تنظیمات بر اساس مشخصات نگارش 1.1 از پروتکل Hypettext Transform Protocol یا به اختصار HTTP انجام می‌شود. در این بررسی، وب سرور Apache 2.0 را به طور خلاصه مورد توجه قرار خواهیم داد. برای اطلاع بیشتر در این زمینه توصیه می‌کنیم ویرایش دوم از کتاب Linux Apache Web Server Administration را که در سال ۲۰۰۲ توسط انتشارات Sybex چاپ و منتشر شده است، مطالعه کنید.

در صورت نصب بسته نرم‌افزاری *-httpd-manual می‌توانید مستندات وب سرور Apache را با دسترسی به فهرست /var/www/manual مورد مطالعه قرار دهید.

راه‌اندازی وب سرور Apache

راه‌اندازی وب سرور Apache بسیار ساده است. مشابه سایر سرویس‌هایی که در فصل‌های مختلف این کتاب توضیح داده شد، برای راه‌اندازی آن کافی است برنامه مربوطه از فهرست /etc/rc.d/init.d را به این صورت اجرا کنید:

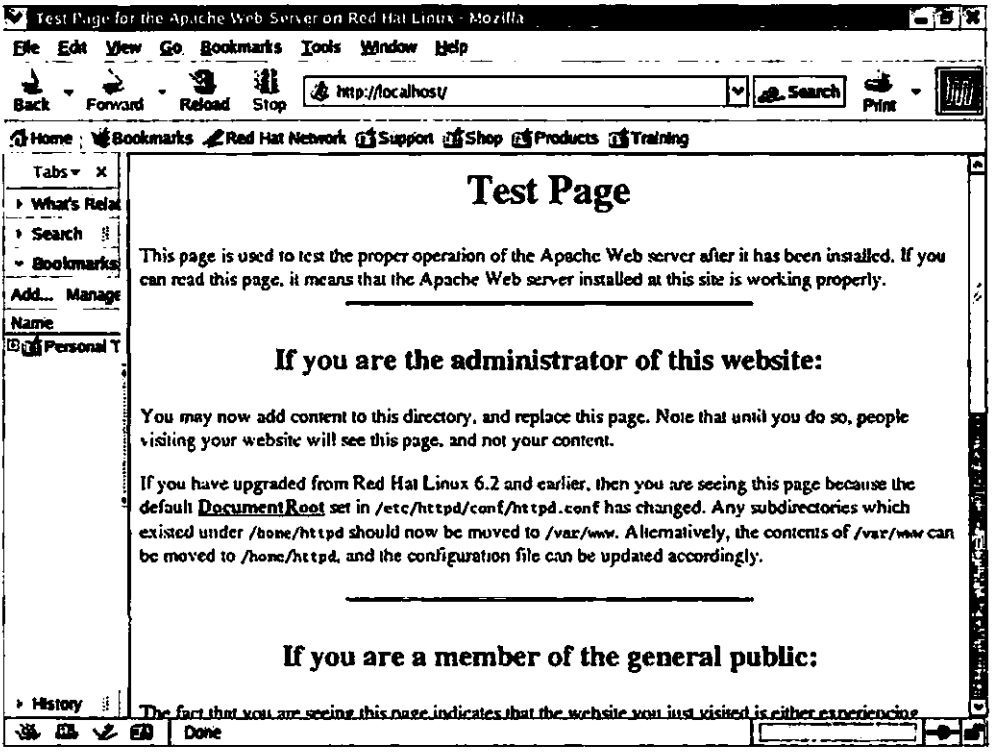
```
# service httpd start
```

اگر تاکنون فایل پیکربندی اصلی وب سرور Apache را مورد ویرایش قرار نداده‌اید، با اقدام فوق احتمالاً این پیغام را مشاهده خواهیدکرد:

```
qualified domain name, using 127.0.0.1 for ServerName
```

اکنون مرورگر وب موردنظر خود را باز کرده و پس از درج عبارت localhost در نوار آدرس آن کلید Enter را فشار دهید. عبارت مذکور به یک آدرس IP به خصوص یعنی 127.0.0.1 که بیانگر کامپیوتر

محلی است، اشاره دارد. (برای اطلاع بیشتر در این زمینه به فصل بیستم مراجعه کنید.) شکل ۱-۳۰ نتیجه این اقدام را در مرورگر Mozilla نشان می‌دهد.



شکل ۱-۳۰ با مشاهده این صفحه می‌توانید از صحت نصب وب سرور Apache اطمینان حاصل کنید.

ضمناً با استفاده از فرمان chkconfig می‌توانید مطمئن شوید که وب سرور Apache طی دفعات آتی راه‌اندازی سیستم‌عامل Linux به طور خودکار در سطح اجرایی موردنظر راه‌اندازی خواهد شد. به عنوان مثال، برای آن‌که این وب سرور طی دفعات آتی راه‌اندازی سیستم‌عامل Linux به طور خودکار در سطوح اجرای دوم، سوم و پنجم راه‌اندازی شود، این فرمان را اجرا کنید:

```
# chkconfig --level 235 httpd on
```

در قسمت بعد به پیکربندی وب سرور Apache می‌پردازیم.

پیکربندی وب سرور Apache

فایل پیکربندی اصلی وب سرور Apache در فهرست /etc/httpd/conf مستقر است. این فایل متشکل از سه قسمت است. قسمت مربوط به متغیرهای سراسری امکان انجام تنظیمات اولیه وب سرور Apache را در اختیار می‌گذارد. قسمت مربوط به سرور اصلی امکان انجام تنظیمات پیش‌فرض وب سایت‌های مستقر روی کامپیوتر میزبان وب سرور Apache را فراهم می‌کند. قسمت آخر که در این فایل با برچسب <VirtualHost> مشخص شده است، امکان انجام تنظیمات موردنیاز برای میزبانی وب سایت‌های مختلف از طریق یک آدرس IP واحد را در اختیار قرار می‌دهد.

پیکربندی نسخه‌های قدیمی‌تر وب سرور Apache از طریق سه فایل مختلف با عناوین access.conf، srm.conf و http.conf انجام می‌شد. علیرغم آن‌که از نگارش 1.3.x به بعد دو فایل پیکربندی access.conf و srm.cof در httpd.conf ادغام شدند، وجود این دو فایل (دست کم نسخه‌ای از این دو فایل که فاقد محتوا باشند) هم‌چنان ضروری است. در نگارش 2.0.x این ضرورت غیرمنطقی حذف شده است.

فرامین‌موجود در فایل پیکربندی‌وب‌سرور Apache را اغلب با عنوان directive یا اصطلاحاً دستورالعمل می‌شناسیم. در قسمت‌های بعد با کاربرد دستورالعمل‌های موجود در فایل پیکربندی httpd.conf آشنا خواهید شد. فایل مذکور به واسطه وجود توضیحات مفصل از خوانایی بسیار خوبی برخوردار است.

تأثیر برخی از این دستورالعمل‌ها با درج علامت # در ابتدای خط مربوطه غیرفعال شده است. اگر در زمینه کار با وب سرور Apache بی‌تجربه هستید، توصیه می‌کنیم مهارت خود را با تجربه کردن افزایش دهید. برای شروع می‌توانید چند وب سایت طراحی کرده و در فهرستی که توسط دستورالعمل DocumentRoot مشخص شده است، مستقر کنید. (این فهرست که با عنوان فهرست ریشه وب سرور نیز شناخته می‌شود، در بیشتر موارد /var/www/html است.) سپس پیکربندی برخی از دستورالعمل‌ها را تغییر داده و پس از راه‌اندازی مجدد سرویس httpd تأثیر آن را از طریق مرورگر وب مشاهده کنید. مطمئناً در مواردی متعجب خواهید شد.

تنظیمات مربوط به متغیرهای سراسری

در این قسمت دستورالعمل‌هایی از فایل پیکربندی httpd.conf را که به منظور تنظیم متغیرهای سراسری پیش‌بینی شده‌اند، مورد بررسی قرار می‌دهیم. مقادیر این متغیرها کلیه تنظیماتی را که با برچسب <VirtualHost> مشخص شده است، تحت تأثیر قرار می‌دهد. این قسمت شامل تنظیمات

مربوط به متغیرهای اولیه، متغیرهای مربوط به برنامه‌های کلاینت، تنظیمات پورت‌ها، نحوه دسترسی به سایر فایل‌های پیکربندی و تعیین موقعیت ماجول‌هاست.

چنان‌چه به متغیری مقدار صفر منسوب شود، به این معنی است که هیچ محدودیتی برای ویژگی مربوطه در نظر گرفته نمی‌شود. برای مثال، اگر مقدار صفر به متغیر Timeout منسوب شده باشد، هیچ اقدامی برای خاتمه دادن به تلاشی که کاربران با استفاده از برنامه مرورگر خود برای برقراری ارتباط با وب سرور انجام می‌دهند، صورت نخواهد گرفت.

متغیرهای اولیه

مقدار متغیر ServerTokens بیانگر اطلاعاتی است که درباره وب سرور Apache و سیستم‌عامل مورد استفاده جهت میزبانی آن در اختیار کاربران قرار می‌گیرد. نمونه‌ای از دستورالعمل مربوطه چنین است:

```
ServerTokens OS
```

جدول ۳-۳۰ سایر دستورالعمل‌های موجود برای مقداردهی متغیر ServerTokens را شرح می‌دهد.

جدول ۳-۳۰ دستورالعمل‌های Server Tokens

عنوان دستورالعمل	توضیح
ServerTokens Prod	این دستورالعمل کاربر را از نوع وب سرور مطلع می‌کند.
ServerTokens Min	این دستورالعمل کاربر را از نوع وب سرور و شماره ویرایش آن مطلع می‌کند.
ServerTokens Os	این دستورالعمل کاربر را از نوع وب سرور، شماره ویرایش آن و نوع سیستم‌عامل میزبان مطلع می‌کند.
ServerTokens Full	این دستورالعمل کاربر را از نوع وب سرور، شماره ویرایش آن، ماجول‌های موجود و نوع سیستم‌عامل میزبان مطلع می‌کند.

دستورالعمل ServerRoot فهرست حاوی فایل‌های پیکربندی و فایل‌های مورد استفاده به منظور ثبت خطاها و وقایع را مشخص می‌کند. تنظیمات پیش‌فرض این متغیر چنین است:

```
ServerRoot "/etc/httpd"
```

با اجرای فرمان ls -l /etc/httpd موقعیت فهرست‌های واقعی مشخص می‌شود. برای مثال، با اجرای فرمان فوق می‌توان مشاهده کرد که پیوند /etc/httpd/logs به فهرست /var/log/httpd اشاره دارد.

وب سرور Apache درخواست‌های ارسالی از مرورگرهای وب را به کمک دو فرآیند مختلف (یکی فرآیند پدر و دیگری فرآیند فرزند) کنترل می‌کند. پارامتر ScoreBoardFile جهت برقراری ارتباط میان فرآیندها پیش‌بینی شده است. در صورت عدم استفاده از این پارامتر، ارتباط لازم میان این دو فرآیند از طریق حافظه کامپیوتر میزبان وب سرور Apache برقرار خواهد شد.

```
# ScoreBoardFile run/httpd.scoreboard
```

هنگام به کارگیری متغیر ScoreBoardFile احتیاط کنید. استفاده از این پارامتر تنها در مورد برخی از کامپیوترها با معماری به خصوص قابل توجیه است.

چنان‌که مشاهده می‌کنید، run عنوان زیرفهرستی است که به طور نسبی مورد دستیابی واقع شده است. آدرس‌دهی مطلق آن به مقدار متغیر ServerRoot بستگی دارد. از آن‌جا که مقدار این متغیر برابر با /etc/httpd است، دسترسی به زیرفهرست موردنظر از طریق آدرس مطلق /etc/httpd/run امکان پذیر است.

مقدار متغیر PidFile بیانگر موقعیت فایلی است که وب سرور Apache شناسه فرآیندها را در آن‌جا ذخیره می‌کند. تنظیمات پیش‌فرض این متغیر چنین است:

```
PidFile run/httpd.pid
```

مقدار متغیر Timeout بیانگر حداکثر مدت زمانی بر حسب ثانیه است که وب سرور Apache فرصت لازم را برای برقراری ارتباط در اختیار برنامه‌های کلاینت قرار می‌دهد. تنظیمات پیش‌فرض این متغیر چنین است:

```
Timeout 300
```

در حالت عادی مرورگرهای وب در هر بار برقراری ارتباط با وب سرور می‌توانند درخواست‌های متعددی را برای آن ارسال کنند. با مقداردهی متغیر KeepAlive به ترتیبی که در ادامه مشاهده می‌کنید، می‌توان این ویژگی را غیر فعال کرد. تنظیمات پیش‌فرض این متغیر چنین است:

```
KeepAlive Off
```

هم‌چنین در صورت مقداردهی متغیر مذکور به صورت KeepAlive On، با مقداردهی متغیر دیگری تحت عنوان MaxKeepAliveRequest می‌توان حداکثر تعداد درخواست‌های ارسالی در هر بار برقراری ارتباط مرورگرهای وب با وب سرور Apache را محدود کرد. تنظیمات پیش‌فرض این متغیر چنین است:

```
MaxKeepAliveRequest 100
```

مقدار متغیر KeepAliveTimeout حداکثر مدت زمان انتظار وب سرور Apache پس از برقراری ارتباط آن با مرورگر وب جهت دریافت درخواست بعدی را بر حسب ثانیه مشخص می‌کند. تنظیمات پیش‌فرض این متغیر چنین است:

```
KeepAliveTimeout 15
```

متغیرهای مربوط به برنامه‌های کلاینت

وب سرور Apache شامل تعدادی ماجول MPM یا اصطلاحاً Multi-Processing Module است. این ماجول‌ها را می‌توان به سه دسته مختلف به این شرح تقسیم کرد:

- **ماجول‌های Prefork MPM**: این ماجول‌ها برای نگارش‌هایی از وب سرور Apache هم‌چون نگارش 1.3.x طراحی شده که هریک از درخواست‌های دریافتی را نه در قالب یک thread بلکه در قالب یک فرآیند مستقل کنترل می‌کنند.
- **ماجول‌های Worker MPM**: این ماجول‌ها هم برای نگارش‌هایی از وب سرور Apache که درخواست‌های دریافتی را در قالب یک فرآیند مستقل کنترل می‌کنند و هم برای نگارش‌هایی از این وب سرور که هر کدام از درخواست‌ها را در قالب یک thread کنترل می‌کنند، طراحی شده است. با وجود این، بهتر است از به کارگیری این ماجول‌ها در نگارش 1.3.x خودداری کنید، چرا که در این نگارش کنترل درخواست‌های دریافتی در قالب therad موجب بروز مشکلاتی در کار وب سرور می‌شود.
- **ماجول‌های Pre-child MPM**: این ماجول‌ها برای پشتیبانی از مرورگرهایی طراحی شده است که برای ارتباط با وب سرور به یک شناسه منحصر به فرد نیاز دارند.

ماجول‌های MPM در دو سیستم‌عامل Windows NT و Novell Netware به ترتیب با عناوین mpm_winnt و mpm_netware معرفی شده‌اند.

تعدادی از دستورالعمل‌ها موجود را می‌توان به همراه ماجول‌های هریک از این سه گروه مورد استفاده قرار داد.

مقدار متغیر StartServer تعداد فرآیندهای فرزند را که پس از راه‌اندازی وب سرور Apache آماده سرویس‌دهی هستند، مشخص می‌کند. مقدار پیش‌فرض این متغیر چنین است:

```
StartServer 8
```

چنان‌چه پس از راه‌اندازی وب سرور Apache به دلیل سرویس‌دهی متعدد تعداد فرآیندهای بلااستفاده به کمتر از مقدار متغیر MinSpareServers تقلیل پیدا کند، وب سرور مذکور برای جبران آن تعدادی فرآیند راه‌اندازی خواهد کرد. تنظیمات پیش‌فرض این متغیر چنین است:

```
MinSpareServers 5
```

بدیهی است که تعداد فرآیندهای بلااستفاده با کاهش تعداد درخواست‌های ارسالی به وب سرور Apache افزایش می‌یابد. مقدار متغیر MaxSpareServers بیشترین تعداد فرآیندهای بلااستفاده را مشخص می‌کند. تنظیمات پیش‌فرض این متغیر چنین است:

```
MaxSpareServers 20
```

مقدار متغیر MaxClient بیشترین تعداد کلاینت‌ها را برای ارسال درخواست به وب سرور Apache مشخص می‌کند. مقدار پیش‌فرض این متغیر برابر با 150 است، به این معنی که حداکثر ۱۵۰ کلاینت می‌توانند درخواست‌های خود را به طور هم‌زمان برای وب سرور مذکور ارسال کنند:

```
MaxClient 150
```

مقدار متغیر MaxRequestsPerClient بیشترین تعداد درخواست‌های ارسالی از هر کلاینت را مشخص می‌کند. تنظیمات پیش‌فرض این متغیر چنین است:

```
MaxRequestsPerClient 1000
```

در نگارش 2.0 از وب سرور Apache هر کدام از درخواست‌های دریافتی در قالب یک بند یا اصطلاحاً thread سرویس‌دهی می‌شوند. کاربرد مقدار متغیر MinSparThread شبیه به MinSpareServers است، به طوری که اگر تعداد بندهای بلااستفاده به دلیل سرویس‌دهی مکرر به کمتر از مقدار متغیر MinSpareThreads تقلیل پیدا کند، وب سرور مذکور برای جبران آن تعدادی بند ایجاد خواهد کرد. تنظیمات پیش‌فرض این متغیر چنین است:

```
MinSpareThreads 25
```

هنگامی که به دلیل کاهش تعداد درخواست‌ها تعداد بندهای بلااستفاده افزایش می‌یابد، وب سرور Apache برای کاهش آن‌ها تا رسیدن به تعداد مجاز اقدام خواهد کرد. این تعداد مجاز توسط مقدار متغیر MaxSpareThreads مشخص می‌شود. تنظیمات پیش‌فرض این متغیر چنین است:

```
MaxSpareThreads 75
```

فرآیندهای فرزند می‌توانند برای سرویس‌دهی به درخواست‌های دریافتی تعدادی thread ایجاد کنند. مقدار متغیر ThreadsPerChils بیانگر تعداد بندهایی است فرآیند فرزند به محض آن‌که توسط فرآیند پدر تولید شد، برای ایجاد آن‌ها اقدام می‌کند. تنظیمات پیش‌فرض این متغیر چنین است:

```
ThreadsPerChild 25
```

متغیر MaxRequestsPerChild بیانگر محدودیت سرویس‌دهی هر فرآیند فرزند است. مقدار پیش‌فرض این متغیر برابر با 0 است، به این معنی که در این مورد هیچ محدودیتی به طور پیش‌فرض وجود ندارد:

```
MaxRequestsPerChild 0
```

مقدار متغیر MaxThreadsPerChild بیانگر بیشترین تعداد بندهایی است که هر فرآیند فرزند می‌تواند ایجاد کند. تنظیمات پیش‌فرض این متغیر برابر با 20 است:

```
MaxThreadsPerChild 20
```

متغیرهای مربوط به تنظیم پورت‌ها

به کمک متغیر Listen می‌توان وب سرور Apache را وادار کرد تا تنها به درخواست‌های ارسالی از یک آدرس IP به خصوص یا درخواست‌های دریافتی از یک پورت خاص سرویس‌دهی کند. تنظیمات پیش‌فرض متغیر Listen چنین است:

```
# Listen 12.34.65.78:80
Listen 80
```

اگر جهت دسترسی به چند شبکه مختلف بیش از یک کارت شبکه روی کامپیوتر میزبان وب سرور Apache پیکربندی شده باشد، به کمک این متغیر می‌توان سرویس‌دهی را به یک شبکه خاص محدود کرد. برای مثال، این تنظیمات سرویس‌دهی را محدود به درخواست‌هایی می‌کند که از شبکه‌ای با آدرس 192.168.13.64 به پورت TCP/IP شماره ۸۰ از کامپیوتر میزبان وب سرور Apache ارسال می‌شوند:

```
Listen 192.168.13.64:80
```

از نگارش 1.3.x به بعد، مقدار متغیر Listen نسبت به مقادیر متغیرهای BindAddress و Port ارجحیت دارد.

برخورداری از تنظیمات سایر فایل‌های پیکربندی

چنان‌که قبلاً نیز اشاره شد، وب سرور Apache 2.0.x دارای چند فایل پیکربندی است. این فایل‌ها به طور پیش‌فرض در فهرست /etc/httpd/conf.d مستقر می‌شوند. موقعیت این فایل‌ها توسط مقدار متغیر ServerRoot تعیین می‌شود. (به خاطر بیاورید که مقدار پیش‌فرض متغیر ServerRoot برابر با /etc/httpd است.) مقدار متغیر Include بیانگر فایلی است که محتوای آن باید درست در موقعیتی از فایل موردنظر که متغیر مذکور در آن مورد استفاده قرار گرفته است، ضمیمه شود. تنظیمات پیش‌فرض متغیر Include چنین است:

```
Include conf.d/*.conf
```

تعیین موقعیت ماجول‌ها

برای استفاده از ماجول‌های موردنظر باید دستورالعمل بارگذاری آن‌ها را در فایل پیکربندی httpd.conf درج کنید. الگوی عمومی دستورالعمل‌های مورد استفاده برای بارگذاری ماجول‌های وب سرور Apache به این صورت است:

```
LoadModule module_type location
```

برای مثال، این دستورالعمل را می‌توان به منظور بارگذاری ماجول access_module از فهرست modules واقع در موقعیتی که توسط مقدار متغیر ServerRoot مشخص می‌شود، مورد استفاده قرار داد: (در واقع موقعیت مذکور پیوندی برای دسترسی به فهرست /usr/lib/httpd است.)

```
LoadModule access_module modules/mod_access.so
```

ماجول‌های متعددی به روش فوق در نسخه پیش‌فرض از فایل پیکربندی httpd.conf بارگذاری شده‌اند. جدول ۴-۳۰ کاربرد این ماجول‌ها را به اختصار شرح می‌دهد. (ترتیب ماجول‌ها در این جدول به همان صورتی است که در فایل مذکور آمده است.)

جدول ۴-۳۰ شرح مختصری درباره کاربرد ماجول‌های استاندارد وب سرور Apache

عنوان ماجول	توضیح
access_module	این ماجول به منظور پشتیبانی از کنترل دسترسی از طریق یک شناسه، هم‌چون نام کامپیوتر یا آدرسIP طراحی شده است.
auth_module	این ماجول به منظور احراز هویت از طریق ارسال شناسه کاربری و کلمه عبور در قالب متنی ساده طراحی شده است.
auth_anon_module	این ماجول به منظور پشتیبانی از دسترسی ناشناس به منابعی طراحی شده که دسترسی به آن‌ها مستلزم احراز هویت است.
auth_dbm_module	این ماجول به منظور پشتیبانی از احراز هویت در دسترسی به بانک‌های اطلاعاتی طراحی شده است.
auth_digest_module	این ماجول به منظور پشتیبانی از مکانیزم رمزگذاری MD5 طراحی شده است.
include_module	این ماجول به منظور پشتیبانی از مکانیزم Server-Side Include یا به اختصار SSI جهت پیاده‌سازی از صفحات پویا (اصطلاحاً dynamic web page) طراحی شده است.
log_config_module	این ماجول به منظور پشتیبانی از مکانیزم ثبت درخواست‌های ارسالی به وب سرور طراحی شده است.

عنوان ماجول	توضیح
env_module	این ماجول به منظور ارسال متغیرهای سیستمی و مقادیر مربوطه به برنامه‌های CGI یا اصطلاحاً Common Gateway Interface و صفحات حاوی برنامه‌های SSI طراحی شده است.
mime_magic_module	این ماجول به منظور پشتیبانی از وب سرور Apache در تشخیص نوع فایل از روی چند بایت نخست محتوای ارسالی طراحی شده است.
cern_meta_module	این ماجول به منظور پشتیبانی از اطلاعات مضاعفی که به همراه محتوای اصلی در قالب یک صفحه وب برای درخواست کننده ارسال می‌شود، طراحی شده است. این اطلاعات کاملاً استاندارد است به طوری که ساختار آن توسط کنسرسیوم W3C واقع در مرکز تحقیقات فیزیک هسته‌ای اروپا موسوم به CERN (که کوتاه شده عبارت فرانسوی معادلEuropean Laboratory for Particle Physics است.) متخص شده است.
expires_module	این ماجول به منظور تعیین موعد انقضای داده‌های موجود در سند ارسالی طراحی شده تا به این ترتیب وب سرور Apache بتواند نسخه تازه‌ای از سند را پس از انقضای داده‌های موجود در آن مجدداً برای درخواست کننده ارسال کند.
headers_module	این ماجول به منظور اطمینان از صحت عناوین (اصطلاحاً header) درخواست‌ها و پاسخ‌های ارسالی طراحی شده است.
usertrack_module	این ماجول به منظور پشتیبانی از مکانیزم Cookie جهت ردیابی کاربران به واسطه درخواست‌های ارسالی به وب سرور Apache طراحی شده است.
unique_id_module	این ماجول به منظور تخصیص یک شناسه منحصر به فرد به هر کدام از درخواست‌های ارسالی به وب سرور Apache طراحی شده است.
setenvif_module	این ماجول به منظور تنظیم مقادیر متغیرهای سیستمی بر اساس مشخصات درخواست‌های ارسالی، از جمله نوع مرورگر مورد استفاده کاربر طراحی شده است.
mime_module	این ماجول به منظور شناسایی نوع سند از روی پسوند عنوان فایل، هم‌چون txt. طراحی شده است.
dav_module	این ماجول به منظور پشتیبانی از مکانیزم تألیف غیر متمرکز یا اصطلاحاً distributed authoring و کنترل نگارش‌های مختلف نرم‌افزار (اصطلاحاً versioning functionality) طراحی شده است.
status_module	این ماجول جهت دسترسی به اطلاعاتی در زمینه کارایی سرویس‌دهی و میزان فعالیت وب سرور Apache طراحی شده است.

عنوان ماجول	توضیح
autoindex_module	این ماجول به منظور نمایش محتوای فهرست‌ها در قالب یک صفحه وب طراحی شده است.
asis_module	این ماجول به منظور ارسال فایل بدون درج عناوین یا اصطلاحاً header اضافی طراحی شده است.
info_module	این ماجول به منظور پشتیبانی از دسترسی کاربران به اطلاعات پیکربندی وب سرور Apache طراحی شده است.
dav_fs_module	این ماجول به منظور پشتیبانی از ماجول dav_module طراحی شده است.
vhost_alias_module	این ماجول امکان پیکربندی میزبان‌های مجازی را به شیوه پویا در اختیار می‌گذارد.
negotiation_module	این ماجول به منظور پشتیبانی از وب سرور Apache در تطبیق مشخصات محتوا، از جمله زبان مورد استفاده با تنظیمات مرورگر وب طراحی شده است.
dir_module	این ماجول به منظور مشاهده محتوای فهرست‌های وب سرور Apache طراحی شده است.
imap_module	این ماجول به منظور پشتیبانی از دستورالعمل‌های imagemap طراحی شده و ربطی به سرور پست الکترونیکی IMAP ندارد.
actions_module	این ماجول به منظور پشتیبانی از اجرای برنامه‌های CGI طراحی شده است.
speling_module	این ماجول به منظور چشم‌پوشی از اشتباهات کوچک در اسامی صفحات درخواستی طراحی شده است.
userid_module	این ماجول به منظور پشتیبانی از دسترسی به فهرست‌ها مخصوص کاربران طراحی شده است.
alias_module	این ماجول به منظور پشتیبانی از تغییر آدرس‌های URL در دسترسی به یک صفحات وب طراحی شده است.
rewrite_module	این ماجول به منظور پشتیبانی از بازنویسی آدرس‌های URL طراحی شده است.
proxy_module	این ماجول به منظور حفاظت از وب سرور Apache توسط پروکسی سرور طراحی شده است.
proxy_ftp_module	این ماجول به منظور حفاظت وب سرور Apache توسط پروکسی سرور (در دسترسی کاربران به داده‌های موردنظر از طریق پروتکل FTP) طراحی شده است.
proxy_http_module	این ماجول به منظور حفاظت وب سرور Apache توسط پروکسی سرور (در

عنوان ماجول	توضیح
	دسترسی کاربران به داده‌های موردنظر از طریق پروتکل HTTP) طراحی شده است.
proxy_connect_module	این ماجول به منظور پشتیبانی از دسترسی به وب سرور Apache از طریق پروکسی سرور طراحی شده است.
cgi_module	این ماجول به منظور پشتیبانی از اجرای برنامه‌های CGI طراحی شده است.
cgid_module	این ماجول به منظور پشتیبانی از اجرای برنامه‌های CGI توسط یک برنامه شبح (اصطلاحاً daemon) طراحی شده است.

در این میان info_module یکی از جالب توجه‌ترین ماجول‌هاست. چنان‌که به زودی خواهید دید، این ماجول امکان مشاهده جزییات پیکربندی وب سرور Apache را از طریق مرورگر وب در اختیار می‌گذارد. برای این منظور کافی است عبارت localhost/server-info/ را در نوار آدرس مرورگر وب وارد کرده و کلید Enter را فشار دهید.

متغیرهای اصلی پیکربندی سرور

پیش از پرداختن به نحوه پیکربندی میزبان‌های مجازی یا اصطلاحاً Virtual Host، در این قسمت متغیرهای اصلی پیکربندی وب سرور Apache را مورد بررسی قرار می‌دهیم. ضمن این بررسی با مقادیر پیش‌فرض این متغیرها آشنا می‌شوید. بررسی متغیرها بر اساس همان ترتیبی است که در فایل پیکربندی httpd.conf آمده است.

از آن‌جا که این قسمت از فصل طولانی است، چنان‌چه هر قسمت را در یک جلسه مطالعه می‌کنید، توصیه می‌کنیم تا انتهای قسمت مورد بحث به چند استراحت کوتاه بپردازید تا قوای لازم برای مطالعه هرچه دقیق‌تر موضوعات مورد بررسی را به دست آورید.

شناسه کاربری و گروه

متغیرهای User و Group به ترتیب، شناسه کاربری مدیر وب سرور Apache و شناسه گروه مربوطه را مشخص می‌کند. بدیهی است که مشخصات شناسه کاربری و گروه مورد استفاده برای این منظور باید در فایل‌های پیکربندی /etc/passwd و /etc/group ثبت شده باشد. مقادیر پیش‌فرض متغیرهای مذکور چنین است:

```
User apache
Group apache
```

اطلاعات موردنیاز به منظور تماس با مدیر وب سرور Apache

متغیر ServerAdmin بیانگر اطلاعات موردنیاز برای تماس با مدیر وب سرور Apache است. این اطلاعات در کلیه صفحاتی که توسط وب سرور مذکور تولید می‌شود، به نمایش درمی‌آید. مقدار پیش‌فرض متغیر ServerAdmin چنین است:

```
ServerAdmin root@localhost
```

نام کامپیوتر میزبان وب سرور Apache

متغیر ServerName بیانگر نام کامپیوتر میزبان وب سرور Apache است. در صورتی که کامپیوتر مزبور فاقد نام حوزه کامل باشد، برای این منظور می‌توانید از آدرس IP استفاده کنید. مقدار پیش‌فرض متغیر ServerName چنین است:

```
# ServerName new.host.name:80
```

(دستورالعمل فوق به طور پیش‌فرض غیر فعال شده است.) تنظیمات مربوط به میزبان‌های مجازی، که با برچسب <VirtualHost> مشخص می‌شود، بر مقدار این متغیر ارجحیت دارد.

نام کانونی

استفاده از علامت slash (با نماد /) در انتهای آدرس‌های URL، هم‌چون http://www.sybex.com/ از ابتدای ظهور پدیده وب متداول بوده است. اما کاربران امروزی به ندرت آن‌را مورد استفاده قرار می‌دهند. بدون وجود این علامت در انتهای آدرس URL مورد نظر، تلاش برای دسترسی به آن آدرس منجر به بازیابی سندی می‌شود که مقدار متغیر ServerName مشخص کرده است. ویژگی مزبور که توسط متغیر UseCanonicalName مشخص می‌شود، در نسخه پیش‌فرض فایل پیکربندی httpd.conf به این صورت غیر فعال شده است:

```
UseCanonicalName Off
```

فهرست اصلی

متغیر DocumentRoot بیانگر فهرست اصلی حاوی اسنادی است که وب سرور Apache وظیفه سرویس‌دهی آن‌ها را به عهده دارد. مقدار پیش‌فرض این متغیر چنین است:

```
DocumentRoot "/var/www/html"
```

دسترسی به فهرست‌ها

تعیین مجوزهای دسترسی به فهرست‌های مختلف، حاوی اسنادی از کامپیوتر میزبان وب سرور Apache که سرویس‌دهی آن‌ها به عهده وب سرور مذکور است، به واسطه تنظیماتی در قالب برچسب

<Directory /> انجام می‌شود:

```
<Directory />
      Options FollowSymLinks
      AllowOverride None
</Directory>
```

متغیر Options بیانگر میزان تنوع در دسترسی به اسناد مختلف است. جدول ۵-۳۰ کاربرد مقادیر مختلف این متغیر را به اختصار شرح می‌دهد. در حالی که مقداردهی AllowOverride .htaccess امکان انجام این تنظیمات را از طریق فایل پیکربندی htaccess. در اختیار می‌گذارد، مقدار پیش‌فرض این متغیر، یعنی None منجر به چشم پوشی از فایل پیکربندی مذکور می‌شود.

جدول ۵-۳۰ کاربرد مقادیر متغیر Options

عنوان مقدار	توضیح
All	این مقدار به منظور پشتیبانی از سایر مقادیر دیگر به غیر از مقدار MultiView پیش‌بینی شده است.
ExecCGI	این مقدار امکان اجرای برنامه‌های CGI را در اختیار می‌گذارد.
FollowSymLinks	این مقدار امکان دسترسی به فایل‌ها و فهرست‌ها را از طریق پیوند نمادین مربوطه (اصطلاحاً symbolic link) در اختیار می‌گذارد.
Includes	این مقدار امکان دسترسی به صفحاتی را که پیاده‌سازی آن‌ها با استفاده از مکانیزم SSI یا اصطلاحاً Server-Side Include انجام شده است، فراهم می‌کند.
IncludesNOEXEC	این مقدار امکان دسترسی به صفحاتی را که حاوی برنامه‌های CGI نبوده و پیاده‌سازی آن‌ها با استفاده از مکانیزم SSI انجام شده است، فراهم می‌کند.
Indexes	این مقدار در صورت عدم وجود فایلی با خاصیت index.html در فهرست موردنظر، امکان مشاهده فایل‌ها و زیرفهرست‌های موجود در آن فهرست را فراهم می‌کند. متغیر DirectoryIndex جهت انجام تنظیمات مربوط به این قبیل فایل‌ها پیش‌بینی شده است.
MultiViews	این مقدار امکان پشتیبانی از ویژگی‌های مکانیزمContent Negotiation، هم‌چون انتخاب زبان موردنظر برای نمایش محتوا را در اختیار می‌گذارد.
SymLinksIfOwnerMatch	این مقدار در صورتی که فایل یا فهرست موردنظر متعلق به همان کاربر باشد، امکان دسترسی به آن‌ها را از طریق پیوند نمادین مربوطه فراهم می‌کند.

توضیحی درباره فایل htaccess.

فایل htaccess. نوعی فایل پیکربندی است که می‌توان نسخه‌های مختلف آن‌را جهت تنظیمات مربوط به فهرست‌های مختلف در آن فهرست‌ها مستقر کرد. استفاده از این فایل یکی از روش‌های بسیار متداول برای دسترسی محدود به فهرست‌های مختلف است.

البته در بیشتر موارد نیازی به استفاده از این فایل نیست، چراکه می‌توان دسترسی به فهرست‌ها را از طریق فایل اصلی پیکربندی وب سرور Apache یعنی httpd.conf نیز محدود کرد. با مطالعه دستورالعمل‌های مندرج در قالب برچسب <Directory> از نسخه پیش‌فرض فایل اصلی پیکربندی وب سرور Apache هرچه بیشتر با نحوه محدود کردن دسترسی به فهرست‌های مختلف آشنا می‌شوید.

با وجود این، اگر تعداد وب سایت‌های مستقر روی کامپیوتر میزبان وب سرور Apache (مثلاً به دلیل تعداد زیاد صفحات شخصی کاربران) قابل توجه باشد، با استفاده از فایل پیکربندی htaccess. می‌توان به دقیق‌ترین روش ممکن، دسترسی به آن‌ها را محدود کرد. (برای اطلاع بیشتر در این زمینه به قسمت "حقوق دسترسی به فهرست‌های کاربران" مراجعه کنید.)

در استفاده از فایل‌های پیکربندی htaccess. جنبه‌های امنیتی را نیز در نظر بگیرید. در این رابطه توصیه می‌کنیم مقدار دیگری غیر از htaccess. را به متغیر AccessFileName نسبت دهید. (مقدار پیش‌فرض این متغیر htaccess. است.) برای توضیحات بیشتر به قسمت "کنترل دسترسی" مراجعه کنید.

حقوق دسترسی به فهرست‌های خاص

حقوق دسترسی به فهرست /var/www/html در قالب برچسب خاصی به این صورت مشخص شده است: `<Directory "/var/www/html">`

در قالب برچسب مذکور، مقادیر متغیر Options که با یک فضای خالی از یکدیگر جدا شده‌اند، نحوه دسترسی به فایل‌های موجود در این فهرست را مشخص می‌کنند. مقداردهی پیش‌فرض این متغیر چنین است: `Options Indexes FollowSymLinks`

در این میان، مقدار Indexes امکان مشاهده عناوین فایل‌ها و زیرفهرست‌های موجود در فهرست /var/www/html را (در صورت عدم وجود فایلی با خاصیت index.html در فهرست نامبرده) و مقدار FollowSymLinks امکان دسترسی به فایل‌ها و فهرست‌ها را از طریق پیوندهای نمادین مربوطه یا اصطلاحاً symbolic link در اختیار قرار می‌دهند. (در این رابطه شکل ۲-۳۰ را ببینید.)

چنان‌که در قسمت قبل نیز اشاره شد، مقداردهی AllowOverride .htaccess امکان انجام تنظیمات از طریق فایل پیکربندی .htaccess را در اختیار می‌گذارد. با وجود این، مقداردهی پیش‌فرض متغیر AllowOverride که به این صورت است منجر به چشم‌پوشی از فایل پیکربندی مذکور می‌شود:

```
AllowOverride None
```

متغیر Oredr ترتیب اولویت متغیرهای کنترل دسترسی یعنی Allow و Deny را مشخص می‌کند. مقدار پیش‌فرض متغیر مذکور بیانگر بالا بودن اولویت متغیر کنترل دسترسی Allow نسبت به Deny است:

```
Order allow,deny
Allow from all
```

متغیرهای Allow و Deny امکان دسترسی به فایل‌ها و زیرفهرست‌های موجود در یک فهرست را مشخص می‌کنند. مقداردهی پیش‌فرض Allow from all در صورتی که اولویت کنترل دسترسی Allow بیش از Deny باشد، (یعنی به ترتیبی که در تنظیمات پیش‌فرض مشخص شده است) امکان دسترسی به تمام فایل‌ها و زیرفهرست‌های موجود در فهرست موردنظر (در این مورد /var/www/html) را فراهم می‌کند. (روش بهتر تنظیمات فوق به این صورت است که با مقداردهی Order deny,allow اولویت متغیر کنترل دسترسی Deny را نسبت به Allow افزایش داده و با مقداردهی Deny from all امکان دسترسی به هیچ یک از فایل‌ها و زیرفهرست‌های موجود از فهرست موردنظر را در اختیار قرار ندهید. سپس تنظیمات فوق را در مورد هریک از زیرفهرست‌ها به نحوی رونویسی کنید تا امکان دسترسی محدود به آن‌ها فراهم شود. ـ مترجم)

حقوق دسترسی به فهرست اصلی وب سایت

تنظیماتی را که در این قسمت مورد بررسی قرار می‌دهیم به منظور کنترل دسترسی به فهرست اصلی وب سایت (که با مقدار متغیر DocumentRoot مشخص می‌شود) پیش‌بینی شده‌اند:

```
<LocationMatch "^/$">
   Options -Indexes
   ErrorDocument 403 /error/noindex.html
</LocationMatch>
```

ظاهر برچسب <LocationMatch "^/$"> تا اندازه‌ای نامتعارف است. دستورالعمل‌های مشخص شده توسط این برچسب (یعنی Options و ErrorDocument) برای محدود کردن دسترسی به فهرست ریشه (با نماد /) پیش‌بینی شده‌اند.

مقداردهی Options -Index به واسطه وجود علامت - در مقابل مقدار Index از مشاهده زیرفهرست‌ها و فایل‌های موجود در فهرست اصلی وب سایت جلوگیری به عمل می‌آورد. چنان‌چه فهرست اصلی فاقد فایلی با خاصیت index.html باشد، دسترسی به فهرست اصلی به واسطه مقداردهی متغیر ErrorDocument به صورت فوق، موجب نمایش صفحه‌ای شامل پیغام خطا می‌شود. موقعیت صفحه حاوی پیغام خطا با توجه مقدار متغیر ServerRoot سنجیده می‌شود. بنابراین، صفحه noindex.html در تنظیمات فوق از فهرست /etc/httpd/error بازیابی می‌شود.

نکته عجیب دیگر این‌که در دسترسی به آدرس http://localhost، صفحه noindex.html به صورتی که قبلاً در شکل ۱-۳۰ مشاهده کردید، به نمایش درمی‌آید.

حقوق دسترسی به فهرست‌های کاربران

مقدار متغیر UserDir بیانگر امکان دسترسی به فهرست‌های کاربران است. مقدار پیش‌فرض این متغیر، disable است، به این معنی که امکان دسترسی به این فهرست‌ها وجود ندارد:

```
UserDir disable
```

در غیر این صورت، برای دسترسی به فهرست‌های مزبور باید متغیر UserDir را به این صورت مقداردهی کنید:

```
UserDir public_html
```

به عنوان مثال، فرض کنید کاربری با شناسه ez صفحات وب خود را در قالب فهرست /home/ez/public_html از کامپیوتر میزبان وب سرور Apache سازمان‌دهی کرده باشد. هم‌چنین فرض کنید آدرس وب سایتی که امکان دسترسی به این فهرست‌ها را فراهم می‌کند، http://www.example.abc باشد. بدیهی است که برای دسترسی به صفحات مورد بحث قبلاً باید این فرامین را اجرا کرده باشید:

```
# chmod 711 /home/ez
# chmod 755 /home/ez/public_html
# chmod 744 /home/ez/public_html/*
```

اکنون در صورتی که آدرس http://www.example.abc/~ez را در نوار ادرس مرورگر وارد کرده و کلید Enter را فشار دهید، محتوای صفحه‌ای با خاصیت index.html موجود در فهرست /home/ez/public_html را مشاهده خواهید کرد.

در صورت تمایل می‌توانید تنظیمات بیشتری را نیز در ارتباط با دسترسی به صفحات وب و فایل‌های مستقر در فهرست‌های کاربران انجام دهید. در این رابطه به بخشی از نسخه اصلی فایل پیکربندی httpd.conf توجه کنید:

```
#<Directory /home/*/public_html>
```

```
#    AllowOverride FileInfo AuthConfig Limit
#         Options MultiViews Indexes SymLinksIfOwnerMatch
IncludesNoExec
#    <Limit GET POST OPTIONS>
#        Order allow,deny
#        Allow from all
#    </Limit>
#    <LimitExcept GET POST OPTIONS>
#        Order deny,allow
#        Deny from all
#    </LimitExcept>
#</Directory>
```

با فعال کردن دستورالعمل‌های فوق وب سرور Apache امکان دسترسی به محتوای فهرست public_html را در اختیار می‌گذارد. (برای توضیح بیشتر در این زمینه به قسمت "نمایش لیست محتویات فهرست‌ها" مراجعه کنید.)

چنان‌که قبلاً نیز اشاره شد، با مقداردهی AllowOverride .htaccess می‌توان ترتیبی داد تا وب سرور Apache تنظیمات موجود در فایل پیکربندی htaccess. از فهرست مربوطه را مورد توجه قرار دهد. جدول ۶-۳۰ سایر مقادیر متغیر AllowOverride را به طور مختصر شرح می‌دهد. کلیه توضیحات مندرج در این جدول به تنظیمات موجود در فایل پیکربندی htaccess. اشاره دارد.

جدول ۶-۳۰ شرح کاربر مقادیر متغیر AllowOverride

عنوان مقدار	توضیح
AuthConfig	این مقدار به منظور پشتیبانی از دستورالعمل‌های مربوط به احراز هویت، از جمله AuthName، AuthType و مانند آن پیش‌بینی شده است.
FileInfo	این مقدار به منظور پشتیبانی از دستورالعمل‌های مربوط به تعیین نوع اسناد، از جمله AddEncoding، AddLanguage و مانند آن پیش‌بینی شده است.
Indexes	این مقدار به منظور پشتیبانی از دستورالعمل‌های مربوط به ایندکس‌گذاری فهرست، از جمله DirectoryIndex، FancyIndexing و مانند آن پیش‌بینی شده است.
Limit	این مقدار به منظور پشتیبانی از متغیرهای مورد استفاده برای کنترل دسترسی، شامل Order، Allow و Deny پیش‌بینی شده است.

متغیر Options که قبلاً در قالب جدول ۵-۳۰ مورد بررسی قرار گرفت، امکان پشتیبانی از مکانیزم Content Negotioation، ایندکس‌گذاری فایل‌ها، دسترسی به فایل‌ها و فهرست‌ها از طریق پیوندهای نمادین مربوطه و هم‌چنین پشتیبانی از صفحاتی را که حاوی برنامه‌های CGI نبوده اما در پیاده‌سازی آن‌ها از مکانیزم SSI استفاده شده است، در اختیار می‌گذارد.

دستورالعمل Limit امکان انجام تنظیمات موردنیاز جهت ارسال و دریافت فایل‌ها از فهرست‌های خانگی را در اختیار می‌گذارد. دستورالعمل LimitExcept تأثیر استفاده از سایر دستورالعمل‌های مربوط به کنترل دسترسی را بی‌اثر می‌کند.

ایندکس‌گذاری فهرست‌ها

دسترسی به وب سایت در واقع دسترسی به یک فهرست است. متغیر DirectoryIndex نوع صفحه‌ای را را مشخص می‌کند که هنگام دسترسی به وب سایت نمایش داده می‌شود. مقدار پیش‌فرض این متغیر چنین است:

```
DirectoryIndex index.html index.html.var
```

صفحه Index.html فایل استانداردی است که توسط بسیاری از وب سایت‌ها مورد استفاده قرار می‌گیرد. صفحه index.html.var نمونه‌ای از یک سند پویاست. نمونه دیگری از فایل‌های var. را می‌توانید با مراجعه به فهرست /var/www/error مشاهده کنید. فایل مزبور حاوی پیغام‌های خطای استاندارد است که در موقع مقتضی نمایش داده می‌شود.

کنترل دسترسی

چنان‌که قبلاً نیز اشاره شد، با استفاده از فایل‌های پیکربندی htaccess. می‌توان دسترسی به فهرست‌های مختلف را به طور دقیق کنترل کرد. فایل htaccess. به طور پیش‌فرض از نوع فایل‌های مخفی است. متغیر AccessFileName امکان استفاده از نام دیگری را برای این فایل در اختیار می‌گذارد. (تغییر نام این فایل یک اقدام امنیتی مناسب تلقی می‌شود. ـ مترجم) مقدار پیش‌فرض این متغیر چنین است: `AccessFileName .htaccess`

خطوطی که در ادامه مشاهده می‌کنید، اطمینان می‌دهد که امکان مشاهده فایل‌هایی را که اسامی آن‌ها با ht. آغاز می‌شود، وجود ندارد:

```
<Files ~ "^\.ht">
      Order allow,deny
      Deny from all
</Files>
```

پشتیبانی از استاندارد MIME

با وجودی که استاندارد Multipurpose Internet Mail Extensions یا به اختصار MIME در ابتدا برای تبادل پیغام‌های الکترونیکی از طریق اینترنت تدوین شد، امروزه نمی‌توان نقش آن‌را در تبادل صفحات وب نادیده گرفت. برای مثال، می‌توان مرورگر وب را به نحوی پیکربندی کرد که اسناد PDF موجود روی اینترنت را با استفاده از برنامه‌ای مانند Adobe Acrobat Reader که به منظور بازخوانی اسناد PDF روی کامپیوتر میزبان نصب شده است، باز کند. مقدار متغیر TypeConfig بیانگر فایلی است که ارتباط میان انواع اسناد استاندارد MIME را با پسوندهای مختلف مورد استفاده برای نام‌گذاری فایل‌ها نشان می‌دهد. مقدار پیش‌فرض این متغیر چنین است:

```
TypeConfig /etc/mime.types
```

با وجود این، برخی از فایل‌ها فاقد پسوند هستند. مقدار متغیر DefaultType ماهیت چنین فایل‌هایی را مشخص می‌کند. مقدار پیش‌فرض این متغیر بیانگر فایل‌های متنی است:

```
DefaultType text/plain
```

در مورد فایل‌های باینری کافی است متغیر DefaultType را به این صورت مقداردهی کنید تا به این ترتیب از نمایش کاراکترهای عجیب و غریب در پنجره مرورگری که سند مور نظر را درخواست کرده است، جلوگیری به عمل آید:

```
DefaultType application/octet-stream
```

اگر پسوند فایل به اندازه کافی قانع کننده نباشد، با مقداردهی متغیر MIMEMagicFile می‌توانید ماجول mod_mime_magic را برای این منظور مورد استفاده قرار دهید: (برای توضیح بیشتر به جدول ۴-۳۰ مراجعه کنید.)

```
<IfModule mod_mime_magic.c>
#    MIMEMagicFile /usr/share/magic.mime
    MIMEMagicFile conf/magic
</IfModule>
```

بار دیگر یادآوری می‌کنیم که موقعیت نسبی /conf/magic با توجه به مقدار متغیر ServerRoot تعیین می‌شود. از این‌رو، در صورتی که مقدار متغیر ServerRoot همان مقدار پیش‌فرض یعنی /etc/httpd باشد، موقعیت مطلق فایل مورد اشاره در خطوط فوق عبارت از /etc/httpd/conf/magic خواهد بود.

نکته آخر این‌که مقدار متغیر AddType نسبت به اطلاعات مندرج در فایلی که توسط مقدار متغیر TypesConfig مشخص شده است، دارای اولویت بیشتری است. به نمونه‌ای از مقداردهی این متغیر توجه کنید:

```
AddType application/x-tar .tgz
```

پشتیبانی از ثبت وقایع

حجم وقایع ثبت شده توسط وب سرور Apache بسیار زیاد است، به طوری که در مورد وب سایت‌ها تجاری روزانه به چند صد مگابایت می‌رسد. عدم دقت در پیکربندی قابلیت ثبت وقایع توسط وب سرور Apache می‌تواند به اختلال در سیستم کامپیوتر میزبان منجر شود.

مقدار متغیر HostnameLookups خط مشی وب سرور Apache را در مورد ثبت یا عدم ثبت نام کامل حوزه میزبان کامپیوترهایی که اقدام به ارسال درخواست کرده‌اند، مشخص می‌کند. مقدار پیش‌فرض این متغیر موجب می‌شود تا وب سرور Apache از بازیابی نام کامل حوزه میزبان این کامپیوترها منصرف شود. توصیه می‌کنیم که این تنظیمات را تغییر ندهید، مگر آن‌که از وجود یک سرور DNS قابل اعتماد و ظرفیت شبکه میزبان برای جابه‌جایی این حجم از اطلاعات اطمینان داشته باشید. مقدار پیش‌فرض این متغیر چنین است:

```
HostnameLookups Off
```

مقدار متغیر ErrorLog بیانگر موقعیت فایل error_log است. این فایل، همان‌طور که از نام آن نیز پیداست، به منظور ثبت خطاها پیش‌بینی شده است. مقدار پیش‌فرض این متغیر چنین است:

```
ErrorLog logs/error_log
```

چنان‌که مشاهده می‌کنید، این فایل در موقعیت نسبی logs/error_log واقع است. این موقعیت نسبت به مقدار متغیر ServerRoot سنجیده می‌شود؛ بنابراین با توجه به مقدار پیش‌فرض متغیر ServerRoot یعنی /etc/httpd، موقعیت مطلق فایل error_log عبارت از /etc/httpd/logs/error_log است.

به کمک مقادیر متغیر LogLevel یعنی debug، info، notice، warn، error، crit، alert و emerg می‌توان هر آن‌چه را که در قالب فایل error_log (یا به طور دقیق‌تر، مقدار متغیر ErrorLog) به ثبت می‌رسد، کنترل کرد. (برای اطلاع از کاربرد این مقادیر به توضیحات مربوط به فایل پیکربندی /etc/syslog.conf در فصل سیزدهم مراجعه کنید.) مقدار پیش‌فرض این متغیر چنین است:

```
LogLevel warn
```

قالب تمام وقایع ثبت شده در فایل error_log تابع الگوی خاصی است که توسط مقدار متغیر LogFormat تعریف شده است. مقادیر پیش‌فرض این متغیر چنین است:

```
LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\"
\"%{User-Agent}i\"" combined
LogFormat "%h %l %u %t \"%r\" %>s %b" common
LogFormat "%{Referer}i -> %U" referer
LogFormat "%{User-agent}i" agent
```

هر کدام از این مقادیر بیانگر قالب خاصی هستند. چنان‌که مشاهده می‌کنید، عناوین این قالب‌ها به ترتیب عبارت از combined، common، referer و agent است.

جدول ۷-۳۰ حاوی شرح مختصری درباره پارامترهای مورد استفاده در مقادیر متغیر LogFormat است. برای اطلاع از لیست کامل پارامترهای موجود در این زمینه مستندات مربوط به ماجول mod_log_config در آدرس /var/www/manual/mod/mod_log_config.html را ببینید. سند موجود در آدرس http://www.w3.org/Protocols/HTTP/HTRQ_Headers.html نیز حاوی اطلاعات مفیدی در این زمینه است.

جدول ۷-۳۰ پارامترهای مورد استفاده در مقادیر متغیر LogFormat

عنوان پارامتر	توضیح
%a	این پارامتر بیانگر آدرس IP کامپیوتر راه دور است.
%b	این پارامتر بیانگر تعداد بایت‌های ارسالی (بدون احتساب تعداد بایت‌های قالب بندی شده در هدرهای HTTP) است.
%h	این پارامتر بیانگر نام کامپیوتر راه دور است.
%l	این پارامتر بیانگر نام فایل ثبت وقایع است.
%r	این پارامتر بیانگر نخستین خط از درخواست ارسالی توسط کلاینت است.
%s	این پارامتر بیانگر وضعیت درخواست ارسالی از جانب کلاینت است.
%t	این پارامتر بیانگر ساعت ارسال درخواست است.
%u	این پارامتر بیانگر شناسه کاربر راه دور است.
referer	این پارامتر بیانگر آدرس صفحه‌ای است که کاربر روی پیوندی از آن کلیک کرده و این اقدام وی منجر به درج یک پیغام خطا در فایل ثبت وقایع شده است. (با وجود املای نادرست referer واژه مزبور به همین صورت مورد استفاده قرار گرفته است.)
user-agent	این پارامتر بیانگر شناسه مرورگر وب (هم‌چون Mozilla) است.

با مقداردهی متغیر CustomLog می‌توان موقعیت سایر فایل‌های مورد استفاده جهت ثبت وقایع را مشخص کرد. چنان‌چه مقداردهی این متغیر در قالب برچسب <VirtualHost> انجام شود، وقایع هر وب سایت را می‌توان به طور جداگانه در فایل مستقلی ثبت کرد. مقادیر پیش‌فرض متغیر CustomLog چنین است:

```
# CustomLog logs/access_log common
```

```
CustomLog logs/access_log combined
#CustomLog logs/referer_log referer
#CustomLog logs/agent_log agent
#CustomLog logs/access_log combined
```

خطوط فوق بیانگر موقعیت فایل‌های ثبت وقایع است. موقعیت نسبی این فایل‌ها با توجه به مقدار متغیر ServerRoot سنجیده می‌شود. از آن‌جا که مقدار پیش‌فرض متغیر مذکور به فهرست /etc/httpd اشاره دارد، موقعیت مطلق این فایل‌ها عبارت از /etc/httpd/logs خواهد بود. اطلاعات ارسالی به هریک از این فایل‌ها با توجه به مقدار متغیر LogFormat مربوطه قالب بندی می‌شود. برای مثال، با توجه به تنظیمات فوق، اطلاعات ارسالی به فایل ثبت وقایع /etc/httpd/logs/access_log بر اساس الگوی combined یعنی به این صورت قالب بندی می‌شود:

```
LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\"
\"%{User-Agent}i\"" combined
```

امضای وب سرور Apache

مقدار متغیر ServerSignature خط مشی وب سرور Apache را در مورد درج امضای این وب سرور در پایین کلیه صفحاتی که به طور پویا تولید می‌شوند، مشخص می‌کند. مقدار پیش‌فرض این متغیر چنین است:

```
ServerSignature On
```

با مقداردهی فوق، نام وب سرور، نگارش مربوطه، نام کامپیوتر میزبان و شماره پورتی که از طریق آن درخواست‌های ارسالی را دریافت می‌کند در پایین صفحاتی که به طور پویا تولیدمی‌شوند، درج می‌شود. به نمونه‌ای از این امضا توجه کنید:

```
Apache/2.0.40 Server at localhost Port 80
```

در صورت مقداردهی متغیر مذکور به صورت ServerSignature Email آدرس پست الکترونیکی مدیر وب سرور Apache (با توجه به مقدار متغیر ServerAdmin) در قالب پیوندی قابل کلیک در پایین صفحاتی که به طور پویا تولید می‌شوند، درج می‌شود.

پیوند میان فهرست‌های مندرج در آدرس‌های URL با فهرست‌های محلی

به کمک متغیر Alias می‌توان پیوندی را میان فهرست نامبرده در یک آدرس URL و فهرست محلی موردنظر که روی کامپیوتر میزبان وب سرور Apache مستقر است، برقرار کرد. برای مثال، این مقداردهی بیانگر پیوند میان فهرست /icons/ از آدرس URLبا فهرست محلی /var/www/icons/ از کامپیوتر میزبان است:

```
Alias /icons/ "/var/www/icons/"
```

پس از این تنظیمات، مناسب است حقوق دسترسی به فهرست محلی (در این مورد فهرست /var/www/icons) را نیز مشخص کنید:

```
<Directory "/var/www/icons">
   Options Indexes MultiViews
   AllowOverride None
   Order allow,deny
   Allow from all
</Directory>
```

چنان‌که مشاهده می‌کنید، تنظیمات فوق امکان مشاهده محتوای فهرست /var/www/icons/ را مگر در صورت وجود فایلی با خاصیت index.html و پشتیبانی از مکانیزم Content Negotiation (که به واسطه مقداردهی Options Indexes MultiViews تحمیل شده‌اند) در اختیار کاربران قرار می‌دهد.

چنان‌چه بسته نرم‌افزاری *-httpd-manual را روی کامپیوتر میزبان وب سرور Apache نصب کرده باشید، در صورت تمایل می‌توانید ترتیبی بدهید تا کاربران به مستندات وب سرور Apache دسترسی داشته باشند. برای این منظور، کافی است مقداردهی Alias /manual "/var/www/manual" را به Alias /etc/httpd/manual "/var/www/manual" تغییر دهید. (در این تنظیمات فرض بر آن است که مقدار متغیر ServerRoot برابر با /etc/httpd باشد.)

بار دیگر، پس از مقداردهی متغیر Alias مناسب است حقوق دسترسی به فهرست محلی موردنظر (در این مورد فهرست /var/www/manual) را مشخص کنیم. به تنظیمات مربوطه که شامل بانک اطلاعاتی WebDAV (اصطلاحاً Web-based Distributed Authoring and Versioning) نیز می‌شود، توجه کنید:

```
<Directory "/var/www/manual">
   Options Indexes FollowSymLinks MultiViews
   AllowOverride None
   Order allow,deny
   Allow from all
</Directory>

<IfModule mod_dav_fs.c>
   # Location of the WebDAV lock database.
   DAVLockDB /var/lib/dav/lockdb
</IfModule>
```

پشتیبانی برنامه‌های CGI

برنامه‌های CGI عموماً به برنامه‌هایی اطلاق می‌شود که روی کامپیوتر میزبان وب سرور Apache به اجرا درمی‌آیند. مقدار متغیر ScriptAlias بیانگر فهرست میزبان این قبیل برنامه‌هاست. (مقداردهی این متغیر مشابه متغیر Alias انجام می‌شود.) مقدار پیش‌فرض این متغیر چنین است:

```
ScriptAlias /cgi-bin/ "/var/www/cgi-bin/"
```

اجرای برخی از برنامه‌های CGI مستلزم دسترسی به سرویس CGI (با عنوان /httpd.cgid) است. نحوه دسترسی به این سرویس با مقداردهی متغیر Scriptsock مشخص می‌شود. به نحوه مقداردهی این متغیر توجه کنید:

```
<IfModule mod_cgid.c>
   Scriptsock    run/httpd.cgid
</IfModule>
```

مشابه متغیر Alias، بهتر است پس از مقداردهی متغیر ScriptAlias حقوق دسترسی به فهرست محلی حاوی برنامه‌های CGI را تعیین کنیم. به چگونگی انجام این کار توجه کنید:

```
<Directory "/var/www/cgi-bin">
   AllowOverride None
   Options None
   Order allow,deny
   Allow from all
</Directory>
```

با توجه به این تنظیمات، امکان استفاده از فایل‌های پیکربندی htaccess. وجود ندارد اما امکان اجرای برنامه‌های CGI توسط تمام کاربران موجود است.

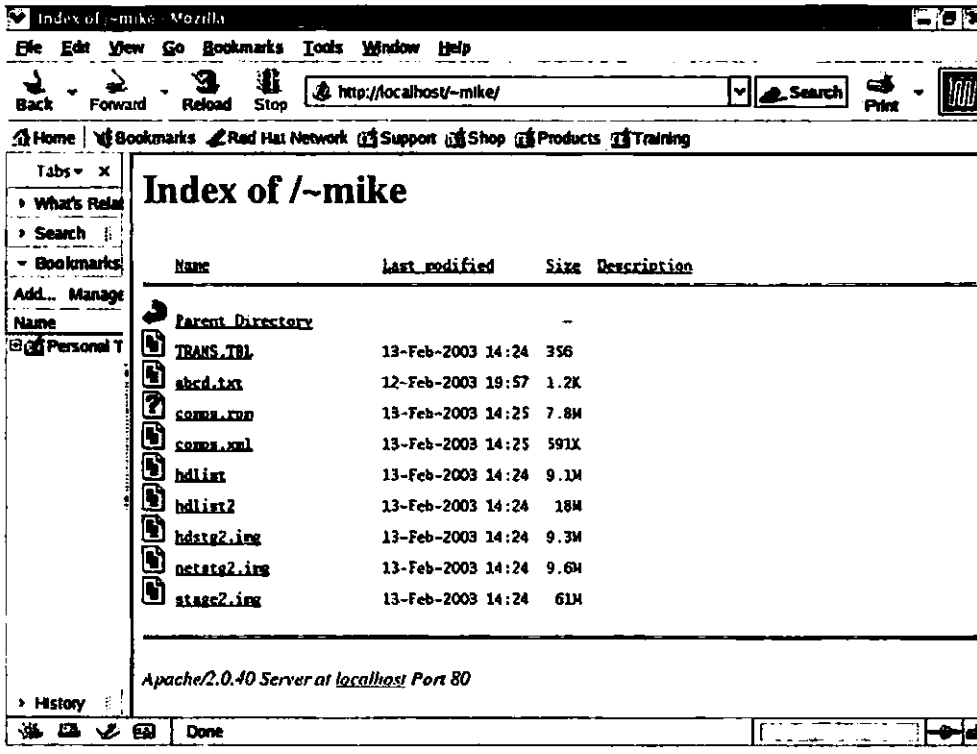
در صورت تغییر نام وب سایت، جهت دسترسی کاربران به آن لازم است از مکانیزم تغییر مسیر استفاده کنید. تغییر مسیر با مقداردهی متغیر Redirect امکان‌پذیر است. برای مثال، با این مقداردهی می‌توانید امکان تغییر مسیر دسترسی از فهرست محلی /bears به وب سایت http://www.mommabears.com را برای کاربران فراهم کنید:

```
Redirect permanent /bears http://www.mommabears.com
```

نمایش لیست محتویات فهرست‌ها

گاهی اوقات به دلایلی مایلیم تا امکان مشاهده محتوای برخی از فهرست‌ها را برای کاربران فراهم کنیم. برای مثال، شکل ۲-۳۰ لیست فایل‌های موجود در فهرست /home/mike/public_html را که با

دسترسی به آدرس http://localhost/~mike/ حاصل شده است، نشان می‌دهد: (برای اطلاع درباره کاربرد متغیر UserDir به قسمت "حقوق دسترسی به فهرست‌های کاربران" مراجعه کنید.)



شکل ۲-۳۰ مشاهده لیست فایل‌های موجود در فهرست خانگی یکی از کاربران

مقدار متغیر IndexOptions نحوه نمایش این لیست را مشخص می‌کند. برای مثال، این مقداردهی را در نظر بگیرید:

```
IndexOptions FancyIndexing VersionSort NameWidth=*
```

مقدار FancyIndex منجر به نمایش اندازه فایل‌ها و آیکن‌ها مربوطه در قالبی فانتزی می‌شود. مقدار VersionSort موجب مرتب سازی لیست فایل‌ها بر اساس اعدادی می‌شود که بیانگر نگارش بسته‌های نرم‌افزاری هستند. مقدار NameWidth نیز منجر به نمایش عنوان کامل فایل‌ها می‌شود.

پشتیبانی از آیکن‌ها

در وب سرور Apache آیکن‌های مختلفی برای انواع فایل‌ها و شناسه‌های مربوطه (پسوندها) تدارک

دیده شده است. در صورت مقداردهی IndexOptions FancyIndexing وب سرور Apache این آیکن‌ها را در نمایش لیست فایل‌های موجود در یک فهرست مورد استفاده قرار دهد. تنظیمات مربوط به آیکن‌ها از طریق سه متغیر AddIconByEncoding، AddIconByType و AddIcon انجام می‌شود. به نمونه‌ای از مقداردهی متغیر AddIconByEncoding که بیانگر آیکن مربوط به فایل‌های فشرده است، توجه کنید:

```
AddIconByEncoding (CMP,/icons/compressed.gif)  x-compress x-gzip
```

این چهار مقداردهی متغیر AddIconByType بیانگر آیکن‌های مربوط به فایل‌های متنی، تصویری، صوتی و ویدیویی هستند:

```
AddIconByType (TXT,/icons/text.gif) text/*
AddIconByType (IMG,/icons/image2.gif) image/*
AddIconByType (SND,/icons/sound2.gif) audio/*
AddIconByType (VID,/icons/movie.gif) video/*
```

این سری از تنظیمات را نیز می‌توان جهت تعیین آیکن‌های مربوط به فایل‌هایی با پسوندهای مختلف مورد استفاده قرار داد:

```
AddIcon /icons/binary.gif .bin .exe
AddIcon /icons/binhex.gif .hqx
AddIcon /icons/tar.gif .tar
AddIcon /icons/world2.gif .wrl .wrl.gz .vrml .vrm .iv
AddIcon /icons/compressed.gif .Z .z .tgz .gz .zip
AddIcon /icons/a.gif .ps .ai .eps
AddIcon /icons/layout.gif .html .shtml .htm .pdf
AddIcon /icons/text.gif .txt
AddIcon /icons/c.gif .c
AddIcon /icons/p.gif .pl .py
AddIcon /icons/f.gif .for
AddIcon /icons/dvi.gif .dvi
AddIcon /icons/uuencoded.gif .uu
AddIcon /icons/script.gif .conf .sh .shar .csh .ksh .tcl
AddIcon /icons/tex.gif .tex
AddIcon /icons/bomb.gif core
AddIcon /icons/back.gif ..
AddIcon /icons/hand.right.gif README
AddIcon /icons/folder.gif ^^DIRECTORY^^
AddIcon /icons/blank.gif ^^BLANKICON^^
```

کاربرد متغیر AddIcon کاملاً آشکار است. برای مثال، وب سرور Apache در مواجهه با فایلی دارای پسوند exe. آیکن /icons/binary.gif را نمایش می‌دهد. مقدار متغیر DefaultIcon بیانگر آیکن مربوط به فایل‌هایی با پسوند ناشناخته است. به نمونه‌ای از مقداردهی این متغیر توجه کنید:

```
DefaultIcon /icons/unknown.gif
```

در صورت تمایل، با مقداردهی متغیر AddDescription می‌توانید اطلاعات بیشتری را درباره فایل‌هایی با پسوند موردنظر در اختیار کاربران قرار دهید. به نمونه‌هایی در این رابطه توجه کنید:

```
#AddDescription "GZIP compressed document" .gz
#AddDescription "tar archive" .tar
#AddDescription "GZIP compressed tar archive" .tgz
```

هم‌چنین در صورت تمایل می‌توانید فهرست‌های مختلف را با استفاده از فایل‌های HTML پیکربندی کنید. برای مثال، مقادیر متغیرهای HeaderName و ReadmeName بیانگر فایل‌هایی هستند که محتویات آن‌ها به ترتیب قبل و بعد از نمایش لیست فایل‌های موجود در یک فهرست به نمایش درمی‌آید. به تنظیمات پیش‌فرض این دو متغیر توجه کنید:

```
ReadmeName README.html
HeaderName HEADER.html
```

با مقداردهی مناسب متغیر IndexIgnore می‌توان ترتیبی داد تا وب سرور Apache از نمایش لیست فایل‌های موجود در فهرست‌ها جلوگیری به عمل آورد. مقدار پیش‌فرض این متغیر چنین است: (به کاربرد فایل‌های HEADER.html و README.html، یعنی مقادیر پیش‌فرض متغیرهای ReadmeName و HeaderName توجه کنید.)

```
IndexIgnore .??* *~ *# HEADER* README* RCS CVS *,v *,t
```

باز کردن فایل‌های فشرده

برخی از مرورگرهای وب می‌توانند فایل‌های فشرده را باز کنند. به منظور پشتیبانی از این قابلیت در وب سرور Apache کافی است متغیر AddEncoding را طور مناسبی مقداردهی کنید. مقداردهی پیش‌فرض این متغیر چنین است:

```
AddEncoding x-compress Z
AddEncoding x-gzip gz tgz
```

پشتیبانی از زبان‌ها

وب سایت‌های چند زبانه حاوی صفحاتی با چند زبان مختلف هستند. مقدار متغیر DefaultLanguage بیانگر زبان مورد استفاده در تمام صفحات وب سایت است. برای مثال، این مقداردهی زبان هلندی را به

عنوان زبان مورد استفاده در تمام صفحات وب سایت معرفی می‌کند:

```
# DefaultLanguage nl
```

با مقداردهی متغیر AddLanguage می‌توان زبان‌های دیگری را نیز مورد پشتیبانی قرار داد. برای این منظور، کافی است کد زبان و پسوند فایل‌های حاوی صفحاتی به آن زبان را مشخص کنید. به عنوان نمونه، زبان مورد استفاده در صفحه index.html.fr فرانسوی است. به مقداردهی متغیر AddLanguage جهت پشتیبانی از این زبان توجه کنید:

```
AddLanguage fr .fr
```

جدول ۸-۳۰ حاوی کد زبان‌های مختلف است.

جدول ۸-۳۰ کد زبان‌های مختلف برای مقداردهی متغیر AddLanguage

زبان	کد مربوطه
کاتالان	ca
چک و اسلواکی	cz
دانمارکی	da
آلمانی	de
انگلیسی	en
یونانی	le
اسپانیایی	es
استونی	et
فرانسوی	fr
عبری	he
مجارستانی	hr
ایتالیایی	it
ژاپنی	ja
کره‌ای	kr
لوکزامبورگی	ltz
هلندی	nl
نروژی نایینورسک	nn
نروژی استاندارد	no

زبان	کد مربوطه
لهستانی	pl
پرتغالی استاندارد	pt
پرتغالی برزیلی	pt-br
روسی	ru
سوئدی	sv
چینی*	tw
چینی	zh-tw

ظاهراً این کد در نسخه‌های بعدی وب سرور Apache مورد پشتیبانی قرار نخواهد گرفت. (چنین پیداست که توسعه دهندگان وب سرور مذکور تنها به پشتیبانی از کد zh علاقه‌مند هستند.)

مرورگرهای وب باید زبان پیش‌فرض خود را به وب سرورها اعلام کنند. حتی در صورتی که مرورگرهای وب چنین اقدامی را صورت ندهند، با مقداردهی متغیر LanguagePriority می‌توان زبان‌های مورد پشتیبانی را به ترتیب اولویت مشخص کرد. مقدار پیش‌فرض این متغیر چنین است:

```
LanguagePriority en da nl et fr de el it ja kr no pl pt pt-br
ltz ca es sv tw
```

عملکرد متغیر ForceLanguagePriority در ارتباط مستقیم با مقادیر متغیر LanguagePriority است. چنان‌که در فایل‌پیکربندی httpd.conf نیز توضیح‌داده‌شده‌است، مقدار متغیر ForceLanguagePriority از میان زبان‌هایی که کد آن‌ها به عنوان مقدار متغیر LanguagePriority ذکر شده و مورد پشتیبانی مرورگر وب است، انتخاب می‌شود. به بیان دیگر، زبان مورد استفاده در صفحه‌ای که برای مرورگر وب ارسال می‌شود باید در لیست مقادیر متغیر LanguagePriority موجود بوده و مرورگر وب نیز امکان پشتیبانی از آن‌را داشته باشد. چنان‌چه صفحه‌ای با این مشخصات موجود نباشد، نخستین زبان موجود در لیست مزبور (در این مورد، زبان انگلیسی با کد en) ملاک قرار گرفته و صفحه‌ای که با آن زبان قالب‌بندی شده است، برای مرورگر ارسال می‌شود.

پشتیبانی از برخی زبان‌ها به سادگی امکان‌پذیر نبوده و تنها در صورتی ممکن است که وب سرور Apache به مجموعه کاراکترهای آن زبان دسترسی داشته باشد. بیشتر مجموعه‌های کاراکتری در قالب خاصی است که توسط سازمان استاندارد جهانی یا ISO سازمان‌دهی شده است. مجموعه کاراکتری پیش‌فرض که برای پشتیبانی از زبان انگلیسی و چند زبان مشابه مناسب است در قالب استاندارد ISO-

8859-1 قابل دسترسی است. مقدار متغیر AddDefaultCharset خطمشی وب سرور Apache را در استفاده از مجموعه کاراکتری پیش‌فرض تعیین می‌کند. مقدار پیش‌فرض متغیر AddDefaultCharset وب سرور Apache را وادار می‌کند تا برای این منظور مجموعه کاراکتری ISO-8859-1 را ملاک قرار دهد. مقدار پیش‌فرض این متغیر چنین است: `AddDefaultCharset ISO-8859-1`

مقادیر متغیر AddCharset بیانگر سایر مجموعه‌های کاراکتری است. (برای اطلاع بیشتر در این زمینه به آدرس http://www.iana.org/assignments/character-sets مراجعه کنید.) به نمونه‌هایی از مقداردهی این متغیر توجه کنید:

```
AddCharset ISO-8859-1  .iso8859-1  .latin1
AddCharset ISO-8859-2  .iso8859-2  .latin2 .cen
AddCharset ISO-8859-3  .iso8859-3  .latin3
AddCharset ISO-8859-4  .iso8859-4  .latin4
AddCharset ISO-8859-5  .iso8859-5  .latin5 .cyr .iso-ru
AddCharset ISO-8859-6  .iso8859-6  .latin6 .arb
AddCharset ISO-8859-7  .iso8859-7  .latin7 .grk
AddCharset ISO-8859-8  .iso8859-8  .latin8 .heb
AddCharset ISO-8859-9  .iso8859-9  .latin9 .trk
AddCharset ISO-2022-JP .iso2022-jp .jis
AddCharset ISO-2022-KR .iso2022-kr .kis
AddCharset ISO-2022-CN .iso2022-cn .cis
AddCharset Big5        .Big5       .big5
# For Russian, more than one charset is used (depends on
client, mostly):
AddCharset WINDOWS-1251 .cp-1251   .win-1251
AddCharset CP866       .cp866
AddCharset KOI8-r      .koi8-r .koi8-ru
AddCharset KOI8-ru     .koi8-uk .ua
AddCharset ISO-10646-UCS-2 .ucs2
AddCharset ISO-10646-UCS-4 .ucs4
AddCharset UTF-8       .utf8
AddCharset GB2312      .gb2312 .gb
AddCharset utf-7       .utf7
AddCharset utf-8       .utf8
AddCharset big5        .big5 .b5
AddCharset EUC-TW      .euc-tw
AddCharset EUC-JP      .euc-jp
```

```
AddCharset EUC-KR       .euc-kr
AddCharset shift_jis    .sjis
```

پردازش فایل‌ها با توجه به پسوند نام آن‌ها

متغیر AddHandlet خط‌مشی وب سرور Apache را در مورد نحوه پردازش فایل‌ها با توجه به پسوند نام آن‌ها تعیین می‌کند. برای مثال، به فرض مقداردهی Options ExecCGI، وب سرورApache با این مقداردهی فایل‌هایی با پسوند cgi. را به عنوان برنامه‌های CGI مورد پردازش قرار می‌دهد:

```
AddHandler cgi-script .cgi
```

هم‌چنین، این مقداردهی باعث می‌شود تا وب سرور Apache فایل‌های HTML را مورد پردازش قرار ندهد:

```
AddHandler send-as-is asis
```

(دو دستورالعمل اخیر به طور پیش‌فرض در فایل پیکربندی httpd.conf غیر فعال شده‌اند. برای فعال کردن آن‌ها کافی است علامت # را از ابتدای خطوط حاوی این دستورالعمل‌ها را حذف کنید.)

به طور مشابه، این دستورالعمل به منظور پردازش فایل‌های image map (به اختصار IMAP) پیش‌بینی شده است:

```
AddHandler imap-file map
```

این دستورالعمل نیز به منظور پشتیبانی از فایل‌های دارای پسوند var. پیش‌بینی شده است:

```
AddHandler type-map var
```

نمایش پیغام‌های خطا

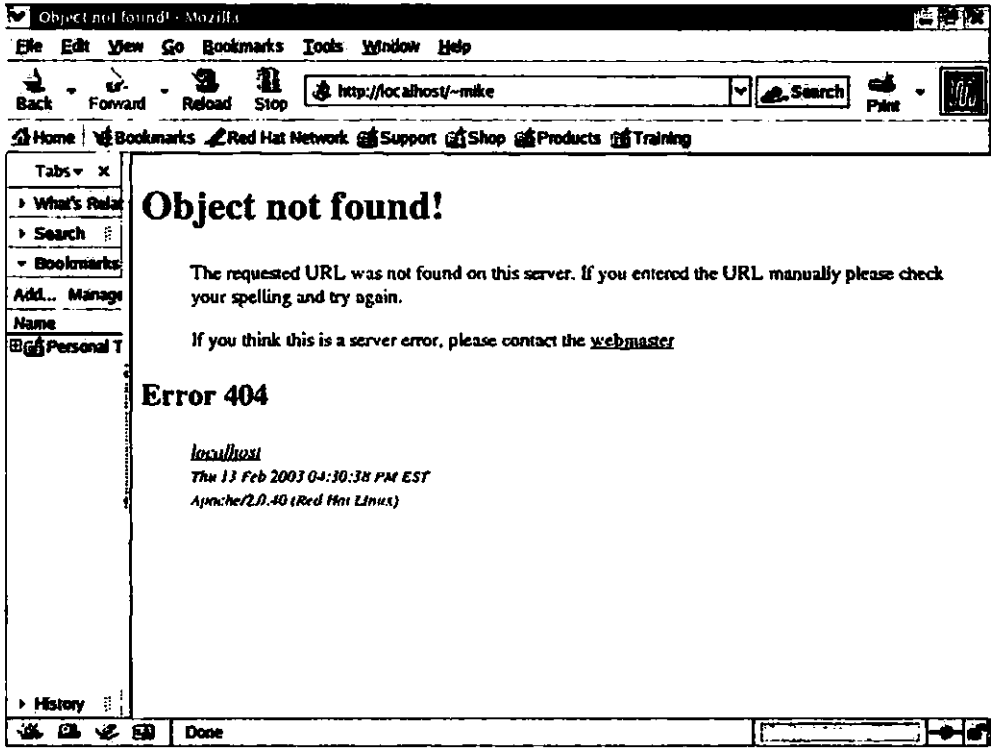
چنان‌چه وب سرور Apache در بازیابی سند درخواستی به هر دلیل با مشکل مواجه شود، پیغام خطایی را در مرورگر وب نمایش می‌دهد. شکل ۳-۳۰ پیغام خطای متناظر با کد ۴۰۴ را نشان می‌دهد. (این خطا اصطلاحاً به خطای "file not found" شهرت دارد.)

به طور پیش فرض، فایل‌های حاوی پیغام‌های خطا در فهرست /var/www/error نگهداری می‌شوند. در این رابطه به نحوه مقداردهی متغیر Alias توجه کنید:

```
Alias /error/ "/var/www/error"
```

دو ماجول mod_negotiation.c و mod_include.c به ترتیب جهت پشتیبانی از مکانیزم‌های Content Negotiation و SSI پیش‌بینی شده‌اند:

```
<IfModule mod_negotiation.c>
<IfModule mod_include.c>
```



شکل ۳۰-۳ نمونه‌ای از یک پیغام خطا در عدم دسترسی به سند مورد درخواست

بار دیگر، پس از مقداردهی متغیر Alias بهتر است حقوق دسترسی به فهرست /var/www/error را نیز تعیین کنیم: (برای اطلاع درباره کاربرد این دستورالعمل‌ها به قسمت‌های قبل از همین فصل مراجعه کنید.)

```
<Directory "/var/www/error">
   AllowOverride None
   Options IncludesNoExec
   AddOutputFilter Includes html
   AddHandler type-map var
   Order allow,deny
   Allow from all
   LanguagePriority en es de fr
   ForceLanguagePriority Prefer Fallback
</Directory>
```

چنان‌که در تنظیمات فوق مشاهده می‌کنید، اولویت در نمایش پیغام‌های خطا به ترتیب با زبان‌های انگلیسی، اسپانیایی، آلمانی و فرانسوی است.

محتوای صفحه‌ای که کاربر به عنوان پیغام خطا مشاهده می‌کند، به کد خطا و نحوه مقداردهی متغیر ErrorDocument بستگی دارد. مقادیر پیش‌فرض این متغیر چنین است:

```
ErrorDocument 400 /error/HTTP_BAD_REQUEST.html.var
ErrorDocument 401 /error/HTTP_UNAUTHORIZED.html.var
ErrorDocument 403 /error/HTTP_FORBIDDEN.html.var
ErrorDocument 404 /error/HTTP_NOT_FOUND.html.var
ErrorDocument 405 /error/HTTP_METHOD_NOT_ALLOWED.html.var
ErrorDocument 408 /error/HTTP_REQUEST_TIME_OUT.html.var
ErrorDocument 410 /error/HTTP_GONE.html.var
ErrorDocument 411 /error/HTTP_LENGTH_REQUIRED.html.var
ErrorDocument 412 /error/HTTP_PRECONDITION_FAILED.html.var
ErrorDocument
413/error/HTTP_REQUEST_ENTITY_TOO_LARGE.html.var
ErrorDocument 414 /error/HTTP_REQUEST_URI_TOO_LARGE.html.var
ErrorDocument 415 /error/HTTP_SERVICE_UNAVAILABLE.html.var
ErrorDocument 500 /error/HTTP_INTERNAL_SERVER_ERROR.html.var
ErrorDocument 501 /error/HTTP_NOT_IMPLEMENTED.html.var
ErrorDocument 502 /error/HTTP_BAD_GATEWAY.html.var
ErrorDocument 503 /error/HTTP_SERVICE_UNAVAILABLE.html.var
ErrorDocument 506 /error/HTTP_VARIANT_ALSO_VARIES.html.var
```

تطبیق سند ارسالی با نوع مرورگر وب

مرورگرهای وب مشخصات خود را در قالب درخواست‌های ارسالی به وب سرور Apache در اختیار آن قرار می‌دهند. متغیر BrowserMatch امکان تطبیق اسناد ارسالی به مرورگرهای وب را با نوع آن مرورگرها فراهم می‌کند. در ارتباط با مقداردهی این متغیر به چند نمونه توجه کنید:

```
BrowserMatch "Mozilla/2" nokeepalive
BrowserMatch "MSIE 4\.0b2;" nokeepalive downgrade-1.0
        force-response-1.0
BrowserMatch "RealPlayer 4\.0" force-response-1.0
BrowserMatch "Java/1\.0" force-response-1.0
BrowserMatch "JDK/1\.0" force-response-1.0
```

دو دستورالعمل نخست وب سرور Apache را وادار می‌کند تا اسناد ارسالی را برای مرورگرهای قدیمی قالب‌بندی کند. مقادیر Mozilla/2 و MSIE4\.0b2 در این دستورالعمل‌ها به دو مرورگر Netscatw 2.x و Microsoft Internet Explorer 4.x اشاره دارند. برخلاف مرورگرهای جدید، هیچ کدام از این مرورگرها، استاندارد HTTP 1.1 را مورد پشتیبانی قرار نمی‌دهند. سه دستورالعمل آخر وب سرور Apache را وادار می‌کند تا قالب‌بندی اسناد ارسالی را با توجه به مشخصات استاندارد مذکور انجام دهد.

این دو دستورالعمل BrowserMatch برای جبران مشکل مرورگر Microsoft Internet Explorer در دسترسی به بانک‌های اطلاعاتی WebDAV پیش بینی شده‌اند:

```
BrowserMatch "Microsoft Data Access Internet
        PublishingProvider" redirect-carefully
BrowserMatch "^WebDrive" redirect-carefully
```

تهیه گزارش

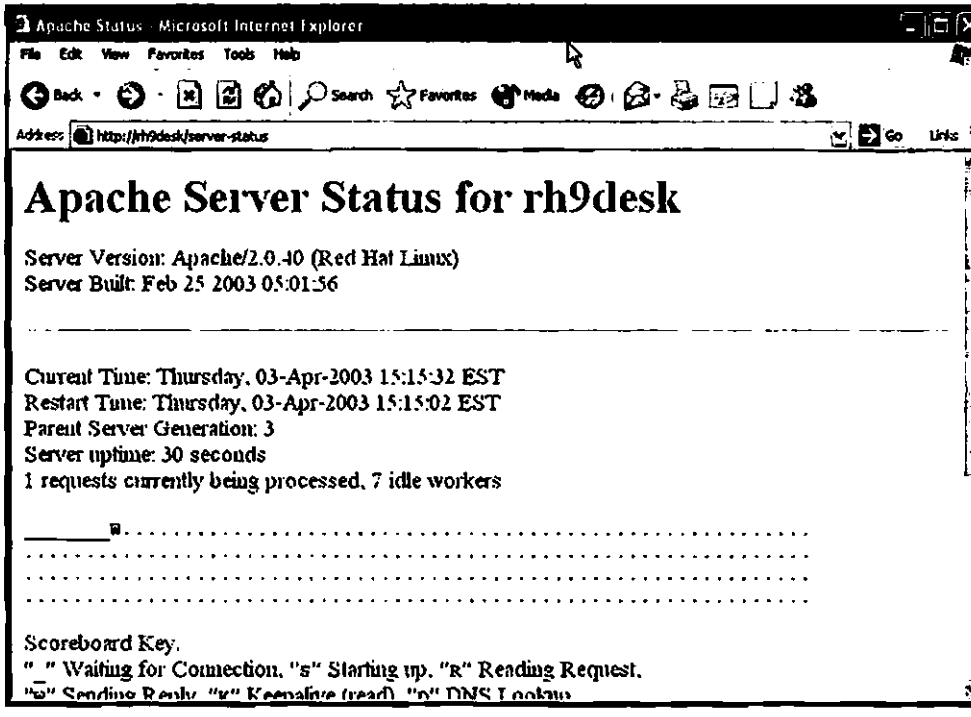
در صورت تمایل می‌توانید گزارشی از وضعیت وب سرور Apache و مشخصات پیکربندی آن‌را مشاهده کنید. برای مثال، با فعال کردن این تنظیمات در نسخه پیش‌فرض فایل پیکربندی httpd.conf می‌توانید گزارش مربوط به وضعیت وب سرور Apache را مشاهده کنید:

```
#<Location /server-status>
#     SetHandler server-status
#     Order deny,allow
#     Deny from all
#     Allow from .your-domain.com
#</Location>
```

با وجود این، دستورالعمل Deny from all از دسترسی به آدرس http://servername/server-status جلوگیری به عمل می‌آورد. به فرض آن‌که آدرس شبکه میزبان 192.168.13.0/24 باشد، تنظیمات فوق را به این صورت انجام دهید تا امکان مشاهده گزارش فراهم آید:

```
<Location /server-status>
   SetHandler server-status
   Order deny,allow
   Deny from all
   Allow from 192.168.13.0/24
</Location>
```

شکل ۴-۳۰ گزارشی را که به واسطه این تنظیمات حاصل شده است، نشان می‌دهد. این گزارش از روی کامپیوتر دیگری (غیر از کامپیوتر میزبان وب سرور Apache) که روی شبکه میزبان مستقر است، تهیه شده است.

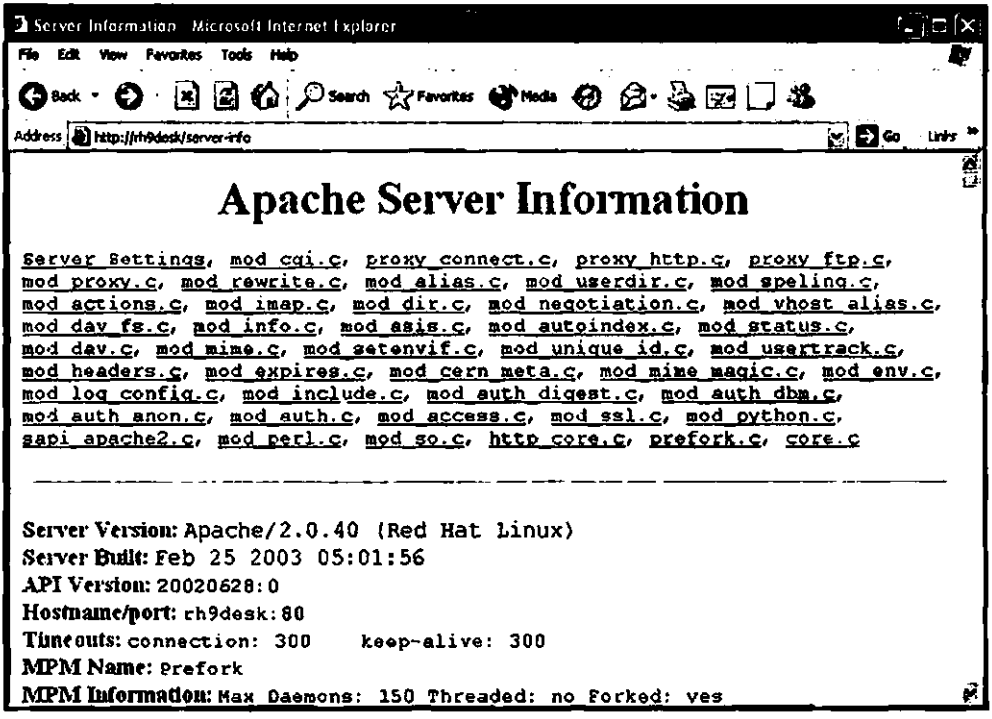


شکل ۴-۳۰ گزارشی درباره وضعیت وب سرور Apache

با فعال کردن این تنظیمات می‌توانید گزارش دیگری را که حاوی مشخصات پیکربندی وب سرور Apache است، مشاهده کنید:

```
#<Location /server-info>
#    SetHandler server-info
#    Order deny,allow
#    Deny from all
#    Allow from .your-domain.com
#</Location>
```

فراموش نکنید که باید مقدار your-domain.com. در دستورالعمل Allow from .your-domain.com را به نحوی تغییر دهید که امکان دسترسی به آدرس http://servername/server-info حاصل شود. شکل ۵-۳۰ گزارش حاصل را نشان می‌دهد.



شکل ۵-۳۰ گزارشی درباره مشخصات پیکربندی وب سرور Apache

پشتیبانی از پروکسی سرور

وب سرور Apache خود دارای یک پروکسی سرور اختصاصی است. با پیکربندی این پروکسی سرور می‌توان اسناد درخواستی را در موقعیتی از هارددیسک کامپیوتر میزبان وب سرور Apache موسوم به cache نگهداری کرد. (برای اشاره به این موقعیت از اصطلاح "حافظه cache" استفاده خواهیم کرد.) به نمونه‌ای از تنظیمات مربوط به‌پیکربندی پروکسی‌سرور که درمورد شبکه‌ای با آدرس 192.168.13.0/24 انجام شده است، توجه کنید:

```
#<IfModule mod_proxy.c>
#ProxyRequests On
#
#<Proxy *>
```

```
#     Order deny,allow
#     Deny from all
#     Allow from 192.168.13.0/24
#</Proxy>
```

در صورت وجود چند پروکسی سرور، با مقداردهی متغیر ProxyVia می‌توان وب سرور Apache را وادار کرد تا در حافظه cache تمام آن‌ها به جستجوی اسناد درخواستی بپردازد. مقدار پیش‌فرض این متغیر قابلیت مذکور را در اختیار می‌گذارد:

```
# ProxyVia On
```

پروکسی سرورها تنها به منظور برخورداری از حافظه cache مورد استفاده قرار می‌گیرند. جدول ۹-۳۰ متغیرهای مربوط به پیکربندی این حافظه را به اختصار شرح می‌دهد.

جدول ۹-۳۰ متغیرهای مربوط به پیکربندی حافظه cache در پروکسی سرور

عنوان متغیر	توضیح
CacheDefaultExpire	مقدار این متغیر بیانگر مدت زمان نگهداری سند در حافظه cache بر حسب ثانیه است.
CacheGcInterval	مقدار این متغیر بیانگر مدت زمانی برحسب ساعت است که پس از سپری شدن آن وب سرور Apache برای پاکسازی حافظه cache اقدام می‌کند.
CacheLastModifiedFactor	مقدار این متغیر بیانگر ساعت انقضای اعتبار اسناد موجود در حافظه cache است. چنان‌چه این اسناد فاقد تاریخ و ساعت انقضا باشند، وب سرور Apache مدت زمان اعتبار آن‌ها را از زمان آخرین تغییرات اعمال شده به این اسناد درنظر می‌گیرد.
CacheMaxExpire	مقدار این متغیر بیانگر حداکثر مدت زمانی بر حسب ثانیه است که وب سرور Apache اسناد را در حافظه cache نگه می‌دارد.
CacheRoot	مقدار این متغیر بیانگر فهرستی از کامپیوتر میزبان وب سرور Apache است که به عنوان حافظه cache مورد استفاده قرار می‌گیرد.
CacheSize	مقدار این متغیر بیانگر اندازه حافظه cache بر حسب کیلو بایت است.

به کمک این دستورالعمل‌ها می‌توانید عملکرد پروکسی سرور را در ارتباط با حافظه cache کنترل کنید. برای مثال، در صورت تمایل می‌توانید فضایی به اندازه ۵ کیلو بایت از حافظه کامپیوتر میزبان را به عنوان حافظه cache مورد استفاده قرار دهید. به نمونه‌ای از این تنظیمات توجه کنید:

```
#CacheRoot "/etc/httpd/proxy"
```

```
#CacheSize 5
#CacheGcInterval 4
#CacheMaxExpire 24
#CacheLastModifiedFactor 0.1
#CacheDefaultExpire 1
#NoCache a-domain.com another-domain.edu joes.garage-sale.com
```

میزبان‌های مجازی

یکی از بارزترین توانایی‌های وب سرور Apache 2.0.x قابلیت آن در پیکربندی وب سایت‌های متعدد با یک آدرس IP واحد است. این قابلیت اغلب با عنوان "میزبان‌های مجازی" یا اصطلاحاً Virtual Hosts شناخته می‌شود.

در نگارش‌های قبلی این وب سرور به هر وب سایت باید یک آدرس IP تعلق می‌گرفت. به بیان دیگر، در نگارش‌های قبلی، قابلیت میزبان‌های مجازی بر اساس آدرس‌های IP پیاده‌سازی می‌شد، حال آن‌که این قابلیت در نگارش جدید بر اساس نام میزبان پیاده‌سازی می‌شود.

با این رویکرد، سرورهای DNS اسامی حوزه‌های مختلف هم‌چون www.mommabears.com و www.sybex.com را به یک آدرس IP واحد مانند 10.111.123.45 نسبت می‌دهند. به کمک تنظیمات فایل پیکربندی httpd.conf می‌توان ترتیبی داد تا وب سرور Apache اسامی حوزه‌ها را به سادگی تشخیص داده و وب سایت مربوط به آن‌را مورد دستیابی قرار دهد.

استفاده از قابلیت شناسایی وب سایت بر اساس نام حوزه مربوطه تحت شرایطی امکان‌پذیر نیست. برای مثال، از این قابلیت نمی‌توان جهت دسترسی به مکان‌های حفاظت شده وب سایت (هم‌چون وب سایت‌های تجاری یا اصطلاحاً e-business) دسترسی پیدا کرد. علاوه بر این، مرورگرهای قدیمی از جمله Netscape 2.0 و Internet Explorer 4.0 از این قابلیت پشتیبانی به عمل نمی‌آورند. (عموماً امکانات پشتیبانی از پروتکل استاندارد HTTP 1.1 در این قبیل مرورگرها پیش‌بینی نشده است.)

مقدار متغیر NameVirtualHost بیانگر شناسه کامپیوتری است که با استفاده از قابلیت میزبان‌های مجازی امکان دسترسی به وب سایت‌ها را فراهم می‌کند. مقدار پیش‌فرض این متغیر چنین است:

```
NameVirtualHost *
```

تنظیماتی را که در ادامه مشاهده می‌کنید، امکان دسترسی به وب سایت www.sybex.com را از طریق قابلیت میزبان‌های مجازی فراهم می‌کند: (در صورت لزوم می‌توانید به جای علامت * از آدرس IP کامپیوتر میزبان نیز استفاده کنید.)

```
<VirtualHost *>
   ServerAdmin webmaster@sybex.com
   DocumentRoot /www/site1/sybex.com
   ServerName sybex.com
   ErrorLog logs/sybex.com-error_log
   CustomLog logs/sybex.com-access_log common
</VirtualHost>
```

تنظیمات فوق به هر گونه تنظیمات دیگری که در این رابطه در فایل پیکربندی httpd.conf انجام شده باشد، ارجحیت دارد. تنظیمات مشابهی را نیز می‌توان در مورد وب سایت www.mommabears.com انجام داد. به نحوه انجام این کار توجه کنید:

```
<VirtualHost *>
   ServerAdmin webmaster@mommabears.com
   DocumentRoot /www/site2/mommabears.com
   ServerName mommabears.com
   ErrorLog logs/mommabears.com-error_log
   CustomLog logs/mommabears.com-access_log common
</VirtualHost>
```

بار دیگر یادآوری می‌کنیم که موقعیت نسبی فهرست‌ها با توجه به مقدار متغیر ServerRoot تعیین می‌شود. این متغیر در نسخه پیش‌فرض از فایل اصلی پیکربندی وب سرور Apache (یعنی httpd.conf) به صورت ServerRoot /etc/httpd مقداردهی شده است.

پیکربندی ماجول‌ها

فهرست /etc/httpd/conf.d حاوی فایل‌های پیکربندی متعددی در ارتباط با ماجول‌های وب سرور Apache است که برخی از آن‌ها به همراه وب سرور مذکور و برخی دیگر در قالب سایر بسته نرم‌افزاری روی کامپیوتر میزبان نصب می‌شوند. دستورالعمل Include conf.d/*.conf در فایل پیکربندی httpd.conf امکان دسترسی وب سرور Apache به تمام این ماجول‌ها را فراهم می‌کند. جدول ۱۰-۳۰ حاوی شرح مختصری درباره فایل های پیکربندی مورد بحث است.

جدول ۱۰-۳۰ شرح مختصری درباره فایل‌های پیکربندی برخی ماجول‌ها

عنوان فایل پیکربندی	توضیح
auth_mysql.conf	این فایل پیکربندی شامل تنظیمات موردنیاز جهت دسترسی به بانک‌های اطلاعاتی MySQL است. نسخه پیش‌فرض این فایل حاوی فرامین مختلفی برای احراز هویت کاربران در دسترسی به این بانک‌های اطلاعاتی است.
auth_pgsql_conf	این فایل پیکربندی شامل تنظیمات موردنیاز جهت دسترسی به بانک‌های اطلاعاتی PostgreSQL است. نسخه پیش‌فرض این فایل حاوی فرامین مختلفی برای احراز هویت کاربران، در دسترسی به این بانک‌های اطلاعاتی است.
perl.conf	این فایل پیکربندی حاوی تنظیمات لازم برای دسترسی به مفسر زبان برنامه‌نویسی Perl است.
php.conf	این فایل پیکربندی حاوی تنظیمات لازم برای دسترسی به مفسر زبان برنامه‌نویسی PHP است.
python.conf	این فایل پیکربندی حاوی تنظیمات لازم برای دسترسی به مفسر زبان برنامه‌نویسی Python است.
ssl.conf	این فایل پیکربندی حاوی تنظیمات لازم به منظور پشتیبانی از مکانیزم امنیتی Secure Socket Layer یا به اختصار SSL و دستورالعمل‌هایی برای پشتیبانی از روش‌های مختلف رمزگذاری است. دسترسی به این مکانیزم به طور پیش‌فرض از طریق پورت TCP/IP شماره ۴۴۳ انجام می‌شود.

رفع اشکالات وب سرور Apache

چنان‌چه دسترسی به وب سایتی که روی وب سرور Apache پیکربندی شده است، مقدور نباشد، باید موارد مختلفی را بررسی کنید. پیش از هر اقدامی در این رابطه، ابتدا اتصالات شبکه را مورد بررسی قرار دهید، چراکه بیشتر اشکالات شبکه‌ها از نوع فیزیکی است. برای این منظور محل اتصالات را مورد بازبینی قرار داده و از سالم بودن کابل‌ها اطمینان حاصل کنید. سپس با صدور فرامین مربوطه، هم‌چون ping از سالم بودن اتصالات مطمئن شوید. (برای اطلاع بیشتر در این زمینه به فصل بیست و یکم مراجعه کنید.)

بازبینی اولیه

پس از اطمینان خاطر درباره صحت عملکرد شبکه، باید مطمئن شوید که وب سرور Apache در حال سرویس‌دهی است. برای اطمینان از این موضوع کافی است این فرمان را اجرا کنید:

```
# service httpd status
```

اگر وب سرور Apache بدون هیچ مشکلی درحال سرویس‌دهی باشد، با اقدام فوق باید پیغامی شبیه به این را مشاهده کنید:

```
httpd (pid 3464 3463 3462 3461 3460 3459 3458) is running
```

پیغام فوق به این معنی است که مجموعه‌ای از سرویس‌ها (موسوم به httpd) که برای سرویس‌دهی وب سرور Apache ضروری است، راه‌اندازی شده‌اند. تعداد این سرویس‌ها به مقادیر برخی از متغیرهای موجود در فایل پیکربندی httpd.conf از جمله متغیر StartServers بستگی دارد. از طرف دیگر، چنان‌چه در ارتباط با سرویس‌دهی وب سرور Apache مشکلی وجود داشته باشد، بسته به شرایط موجود ممکن است سه پیغام مختلف دریافت کنید. مضمون پیغام نخست چنین است:

```
httpd is stopped
```

پیغام فوق از بازایستادن سرویس httpd خبر می‌دهد. برای رفع این اشکال فرمان start httpd را اجرا کرده و سپس برای اطمینان از راه‌اندازی آن فرمان service httpd status را اجرا کنید. مضمون پیغام دوم چنین است:

```
httpd is dead but pid file exists
```

پیغام فوق به این معنی است که وب سرور Apache به دلیل وجود فایلی با عنوان httpd.pid در فهرست var/run/ قادر به سرویس‌دهی نیست. این اشکال ممکن است ناشی از قطع ناگهانی برق باشد، چرا که تحت این شرایط وب سرور Apache فرصت حذف فایل httpd.pid را از فهرست نامبرده به دست نمی‌آورد. برای رفع این اشکال فایل مذکور را از فهرست var/run/ حذف کنید. سپس برای راه‌اندازی سرویس httpd فرمان service httpd.start را اجرا کرده و برای اطمینان از راه‌اندازی آن، فرمان service httpd status را اجرا کنید. مضمون پیغام سوم چنین است:

```
httpd dead but subsys locked
```

پیغام فوق به این معنی است که اشکال دیگری غیر از عدم راه‌اندازی سرویس httpd یا وجود فایل httpd.pid در فهرست var/run/ موجود است. برای رفع این اشکال باید محتوای فایل‌های ثبت وقایع را مورد بازبینی و مطالعه قرار دهید.

بازبینی محتوای فایل‌های ثبت وقایع

چنان‌که در فایل پیکربندی httpd.conf نیز اشاره شده است، فهرست etc/httpd/logs/ به طور

پیش‌فرض میزبان فایل‌های ثبت وقایع وب سرور Apache است. با وجود این، فهرست مذکور چیزی جز یک پیوند نمادین برای دسترسی به فهرست /var/log/httpd نیست. به بیان دیگر، موقعیت واقعی فایل‌های ثبت وقایع وب سرور apache فهرست /var/log/httpd است. البته در صورت تمایل می‌توان با مقداردهی متغیر CustomLog در تنظیمات مربوط به وب سایت مورد نظر، که در قالب برچسب <VirtualHost> انجام می‌شود، موقعیت دیگری را برای این منظور مورد استفاده قرار داد.

برای دستیابی به سرنخ‌ها باید وقایع ثبت شده در این فایل‌ها را به دقت مورد مطالعه قرار دهید. تنوع پیغام‌های خطا به قدری است که در این‌جا فرصت پرداختن به آن‌ها وجود ندارد. با وجود این، مفهوم بسیاری از آن‌ها کاملاً روشن است.

بازبینی تنظیمات موجود در فایل‌های پیکربندی از لحاظ قواعد دستوری

چنان‌که تاکنون متوجه شده‌اید، تنظیمات موجود در فایل‌های پیکربندی وب سرور Apache تابع قواعد خاصی است. با اجرای این فرمان وب سرور Apache تنظیمات موجود در فایل پیکربندی httpd.conf را به لحاظ قواعد دستوری مورد بررسی قرار می‌دهد:

```
# httpd -t
```

در صورت وجود اشکالی (هم‌چون املای نادرست یک متغیر) در فایل پیکربندی httpd.conf، شماره خط مربوطه نمایش داده می‌شود. با اجرای این فرمان می‌توانید حالت اشکال‌زدایی (اصطلاحاً debug mode) را فعال کرده و اشکالات بیشتری را پیدا کنید:

```
# httpd -X
```

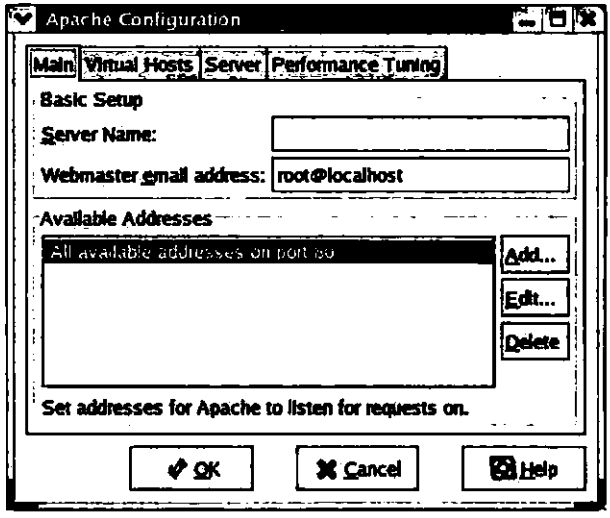
بازبینی مکانیزم بازدارنده دیوار آتش

گاهی اوقات نارسایی وب سرور Apache در دریافت پیغام‌های ارسالی به دلیل سهل‌انگاری در تنظیمات قوانین مربوط به مکانیزم بازدارنده دیوار آتش است. چنان‌چه بر اساس این قوانین پورت TCP/IP شماره ۸۰ (یعنی پورت مربوط به پروتکل استاندارد HTTP) مسدود شده باشد، وب سرور Apache قادر به دریافت پیغام‌های ارسالی از جانب کاربران نخواهد بود. برای مشاهده قوانین مکانیزم بازدارنده دیوار آتش فرمان iptables -L را اجرا کنید. (جهت اطلاع از نحوه رفع اشکالات مربوط به پیکربندی نادرست این مکانیزم به فصل بیست و دوم مراجعه کنید.)

هم‌چنین برای دسترسی به اسناد محرمانه باید پورت TCP/IP مربوطه را باز کنید. پورت TCP/IP شماره ۴۴۳ مربوط به پروتکل استاندارد HTTPS است که مشخصاتی مشابه پروتکل استاندارد HTTP دارد اما متضمن ایمنی بیشتری است. (برای اطلاع از لیست پورت‌های TCP/IP به سند /etc/services مراجعه کنید.)

پیکربندی وب سرور Apache با استفاده از ابزار گرافیکی تهیه شده توسط شرکت Red Hat

ابزار گرافیکی redhta-config-httpd توسط شرکت Red Hat و به منظور پیکربندی وب سرور Apache طراحی شده است. برای دسترسی به آن کافی است فرمانی با همان عنوان را در سطر فرمان محیط گرافیکی مورد استفاده اجرا کنید. شکل ۶-۳۰ تنظیمات موجود در بخش Main از پنجره این ابزار را با عنوان Apache Configuration نشان می‌دهد.



شکل ۶-۳۰ تنظیمات موجود در بخش Main از پنجره Apache Configuration

چنان‌که مشاهده می‌کنید، امکانات این ابزار پیکربندی در قالب چهار بخش مختلف با عناوین Main، Virtual Hosts، Server و Performance Tuning سازمان‌دهی شده است. در قسمت‌های بعد به بررسی این امکانات خواهیم پرداخت. پس از انجام تنظیمات کافی است دکمه OK را کلیک کنید تا تغییرات موردنظر در فایل اصلی پیکربندی وب سرور Apache یعنی httpd.conf به ثبت برسد.

ابزار redhat-config-httpd هم‌چنان در حال توسعه و پیشرفت است. از این‌رو، پیش از به کارگیری آن توصیه می‌کنیم از فایل پیکربندی httpd.conf یک نسخه پشتیبان تهیه کنید. پس از انجام تنظیمات موردنظر با استفاده از این ابزار، فرمان httpd -t را به منظور اطمینان از صحت تغییرات اجرا کنید. هم‌چنین می‌توانید فایل مذکور را در ویرایشگر متنی مورد نظرتان باز کرده و تغییرات را به طور دستی

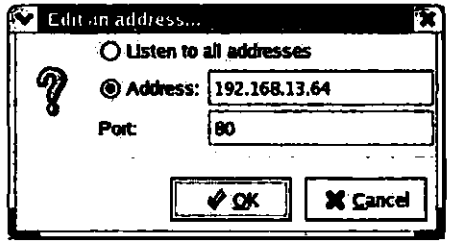
دنبال کنید. با وجود این، استفاده از ابزار redhat-config-httpd روش بسیار خوبی برای فراگیری نحوه پیکربندی وب سرور Apache است.

تنظیمات اصلی

تنظیمات بخش Main بسیار ساده بوده و شامل این موارد هستند:

- فیلد متنی Server Name متناظر با متغیر ServerName از فایل پیکربندی httpd.conf است. چنان‌که می‌دانید، مقدار این متغیر بیانگر نام کامپیوتر میزبان وب سرور Apache است. از این‌رو پیش از دسترسی به سایر بخش‌های ابزار گرافیکی باید نام یا آدرس IP کامپیوتر مزبور را در این فیلد متنی وارد کنید. اگر قصد استفاده از قابلیت میزبان‌های مجازی را دارید، نام حوزه هیچ کدام از آن‌ها را در این فیلد متنی وارد نکنید. توصیه می‌کنیم به منظور اجتناب از افزایش ترافیک ارسالی به کامپیوترهای میزبان سرور DNS مستقر در شبکه، به جای نام کامپیوتر از آدرس IP استفاده کنید.
- فیلد متنی Webmaster Email Address متناظر با متغیر ServerAdmin از فایل پیکربندی httpd.conf است. به خاطر بیاورید که مقدار این متغیر بیانگر آدرس پست الکترونیکی مدیر وب سرور Apache است. (این آدرس در پایین تمام صفحات تولید شده توسط این وب سرور به نمایش درمی‌آید.) از این‌رو، در فیلد نامبرده آدرس پست الکترونیکی مدیر وب سرور Apache را درج‌کنید. چنان‌که‌در شکل ۶-۳۰ مشاهده می‌کنید، به طور پیش‌فرض از آدرس root@localhost برای این منظور استفاده شده است.
- فیلد متنی Available Address متناظر با متغیر Listen است. مقدار این متغیر بیانگر شماره پورت‌های TCP/IP مورد استفاده برای دریافت درخواست‌های ارسالی از جانب کاربران است. با وجودی که پورت TCP/IP شماره ۸۰ به عنوان پورت پیش‌فرض برای تبادل برنامه‌های کلاینت با وب سرورها پیش‌بینی شده است، وب سرور Apache به واسطه دستورالعمل Allow from all قادر است درخواست‌های ارسالی به تمام پورت‌ها را مورد توجه قرار دهد.

در صورت تمایل می‌توانید ترتیبی دهید تا وب سرور Apache تنها درخواست‌های ارسالی به آدرس IP یکی از کارت‌های شبکه نصب شده روی کامپیوتر میزبان را مورد توجه قرار دهد. برای این منظور ابتدا گزینه All Available Addresses On Port 80 را انتخاب کرده و سپس دکمه Edit را کلیک کنید تا به این ترتیب پنجره‌ای با عنوان Edit An Address باز شود. شکل ۷-۳۰ امکانات موجود در این پنجره را نشان می‌دهد.



شکل ۷-۳۰ پنجره Edit An Address

چنان‌که در تنظیمات این شکل مشاهده می‌کنید، دسترسی به وب سرور Apache تنها از طریق کارت شبکه‌ای به آدرس 192.168.13.64 و پورت TCP/IP شماره ۸۰ امکان‌پذیر است. با این تنظیمات، مقدار متغیر Listen از فایل پیکربندی httpd.conf به این صورت تغییر می‌کند:

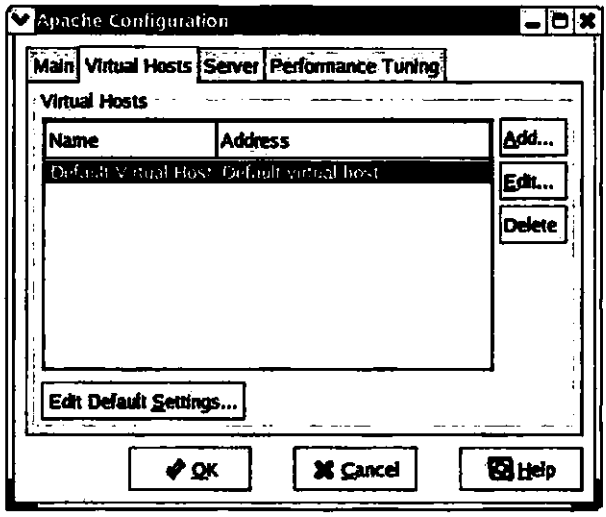
```
Listen 192.168.13.64:80
```

در صورت تمایل می‌توانید تنظیمات دیگری (هم‌چون دسترسی به اسناد محرمانه از طریق پروتکل HTTPS) را نیز انجام دهید. برای این منظور دکمه Add را کلیک کنید تا به این ترتیب پنجره دیگری با عنوان Add New Address که کم‌وبیش شبیه به پنجره شکل ۷-۳۰ است باز شود. از طریق امکانات موجود در پنجره نامبرده می‌توانید آدرس IP کارت شبکه موردنظر و پورت TCP/IP مربوطه را جهت دسترسی مشخص کنید.

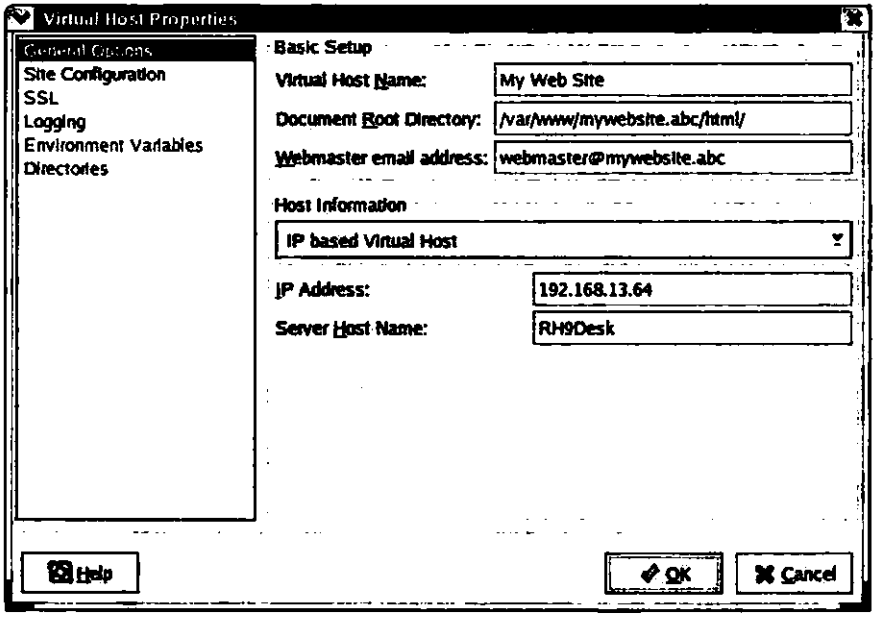
پیکربندی میزبان‌های مجازی

تنظیمات موجود در بخش Virtual Hosts از پنجره Apache Configuration به منظور بهره‌برداری از قابلیت میزبان‌های مجازی پیش‌بینی شده است. شکل ۸-۳۰ امکانات موجود در این بخش را نشان می‌دهد.

گزینه Default Virtual Host امکان مشاهده و ویرایش تنظیمات مربوط به میزبان‌های مجازی پیش‌فرض را در اختیار می‌گذارد. برای مشاهده جزییات مربوطه دکمه Edit یا Edit Default Settings را کلیک کنید. هم‌چنین برای پیکربندی یک میزبان مجازی جدید می‌توانید دکمه Add را کلیک کنید. با این اقدام پنجره Virtual Host Properties که شامل شش بخش مختلف با عناوین General Options ، Site Configuration، SSL، Logging، Environment Variables و Directories است، باز می‌شود. شکل ۹-۳۰ امکانات موجود در بخش General Options را نشان می‌دهد.



شکل ۸-۳۰ تنظیمات موجود در بخش Virtual Hosts از پنجره Apache Configuration



شکل ۹-۳۰ پنجره Virtual Host Properties

در قسمت‌های بعد نحوه پیکربندی میزبان‌های مجازی جدید را با استفاده از تنظیمات پنجره مذکور مورد بررسی قرار می‌دهیم.

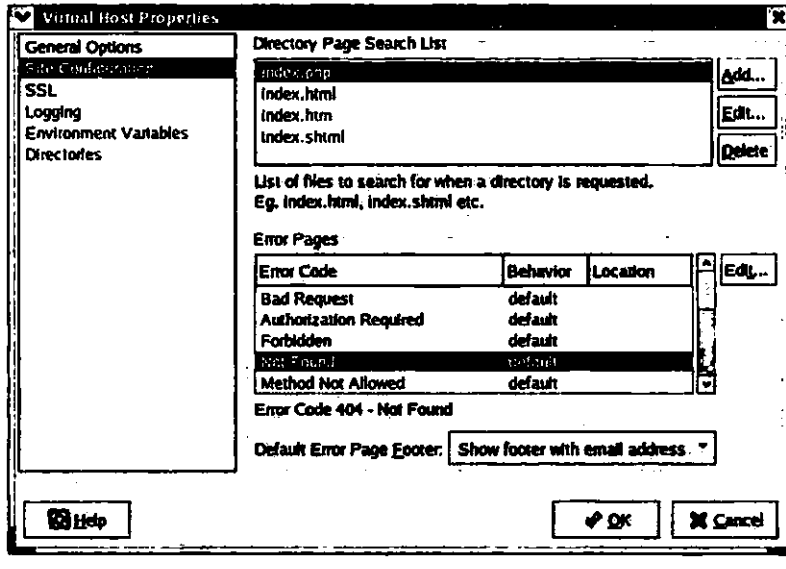
تنظیمات General Options

بخشی‌ازتنظیمات تمام میزبان‌های مجازی در بخش General Options پیش بینی شده است. تنظیمات شکل ۹-۳۰ مربوط به پیکربندی میزبان مجازی یک وب سایت فرضی با عنوان mywebsite.abc است.

چنان‌که قبلاً نیز اشاره شد، وب سرور Apache 2.0.x امکان پیکربندی چندین میزبان مجازی را تنها با یک آدرس IP واحد در اختیار می‌گذارد. این ویژگی با انتخاب گزینه IP based Virtual Hosting در لیست Host Information از پنجره شکل ۹-۳۰ قابل دستیابی است. در نگارش‌های قبلی وب سرور Apache این کار تنها با تخصیص آدرس‌های IP مستقل به هر یک از وب سایت‌ها امکان‌پذیر بود. قابلیت مذکور با پیش‌بینی گزینه دیگری از لیست مذکور با عنوان Name based Virtual Hosting هم‌چنان در ویرایش جدید وب سرور Apache مورد پشتیبانی قرار گرفته است.

تنظیمات Site Configuration

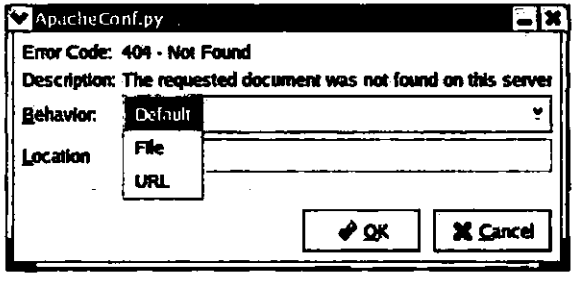
با انتخاب گزینه Site Configuration از قاب سمت چپ پنجره Virtual Host Properties تنظیمات مربوطه در قاب سمت راست ظاهر می‌شود. چنان‌که در شکل ۱۰-۳۰ مشاهده می‌کنید، این تنظیمات به منظور تعیین سند پیش‌فرض موجود در فهرست‌ها و فایل‌های مربوط به صفحات حاوی پیغام خطا پیش‌بینی شده‌اند.



شکل ۱۰-۳۰ تنظیمات بخش Site Configuration از پنجره Virtual Host Properties

هنگام دسترسی به یک وب سایت، سند پیش‌فرض موجود در فهرست متناظر با آن وب سایت، که توسط مقدار متغیر DocumentRoot مشخص می‌شود، به نمایش درمی‌آید. در شکل ۹-۳۰ این فهرست با عنوان /var/www/mywebsite.abc/html مشخص شده است. لیست Directory Page Search List از شکل ۱۰-۳۰ حاوی اسامی اسناد پیش‌فرض در این قبیل فهرست‌هاست. به طور متداول، اغلب از اسنادی با اسامی index.html، index.htm، index.php و index.shtml برای این منظور استفاده می‌شود.

لیست Error Pages در قسمت پایین شکل مذکور شامل لیست اسامی اسنادی است که حاوی پیغام خطا هستند. برای مثال، گزینه منتخب در بخش Error Pages از این شکل مربوط به صفحه‌ای با پیغام خطای page not found (خطای شماره ۴۰۴) است. رفتار پیش‌فرض به هنگام وقوع خطا بستگی به نحوه مقداردهی متغیر ErrorDocument از فایل پیکربندی httpd.conf دارد. در صورت تمایل می‌توان این رفتار را با انتخاب گزینه موردنظر از لیست Error Pages و کلیک دکمه Edit تغییر داد. این اقدام چنان‌که در شکل ۱۱-۳۰ مشاهده می‌کنید، منجر به نمایش پنجره دیگری با عنوان ApacheConf.py می‌شود.



شکل ۱۱-۳۰ پنجره ApacheConf.py

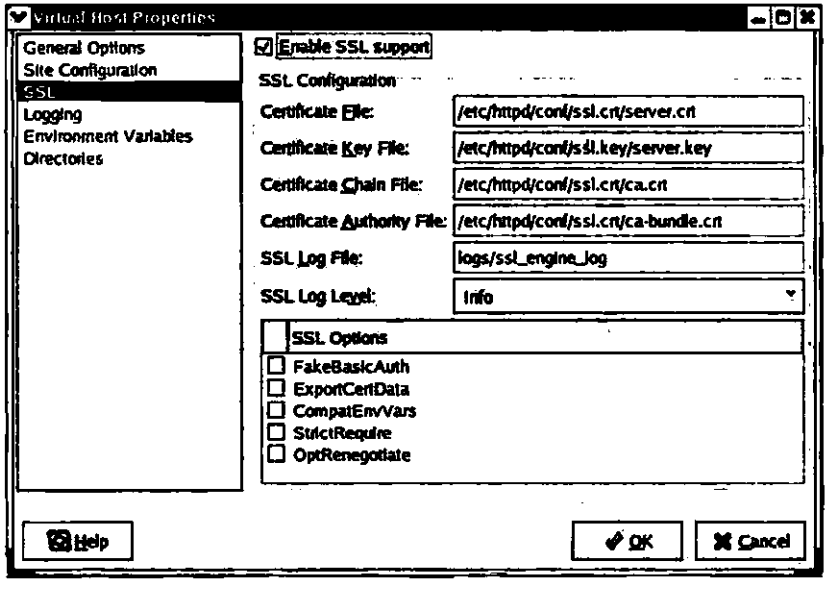
شکل فوق نحوه تعیین رفتار پیش‌فرض به هنگام وقوع خطای page not found را نشان می‌دهد. رفتار پیش‌فرض را می‌توان با انتخاب گزینه موردنظر از لیست Behavior تعیین کرد. برای مثال، در مورد خطای نامبرده، انتخاب گزینه Default موجب نمایش پیغام خطای پیش‌فرض که کد مربوط به آن در قالب مقدار متغیر ErrorDocument از فایل پیکربندی httpd.conf مشخص شده است، می‌شود. گزینه File امکان تعیین موقعیت فایلی را در اختیار می‌گذارد که حاوی پیغام موردنظر است. انتخاب گزینه URL نیز امکان تعیین آدرس صفحه حاوی پیغام خطای موردنظر را در اختیار قرار می‌دهد.

لیست Default Error Page Footer واقع در پایین‌ترین قسمت شکل ۱۰-۳۰ گزینه‌هایی را به منظور قالب بندی پانویس صفحات حاوی پیغام خطا در اختیار می‌گذارد. پانویس استاندارد بر اساس فایل

/var/www/error/include/bottom.html قالب بندی شده است. در این لیست گزینه‌های به منظور درج یا عدم درج آدرس پست الکترونیکی مدیر وب سرور Apache در پانویس صفحات حاوی پیغام خطا و هم‌چنین گزینه‌ای را به منظور صرف نظر از نمایش پانویس در اختیار قرار می‌دهد.

تنظیمات SSL

با انتخاب گزینه SSL از قاب سمت چپ پنجره Virtual Host Properties تنظیمات مربوطه در قاب سمت راست ظاهر می‌شود. چنان‌که در شکل ۱۲-۳۰ مشاهده می‌کنید، این تنظیمات به منظور پشتیبانی از مکانیزم امنیتی Secure Socket Layer یا به اختصار SSL پیش‌بینی شده‌اند. در صورت نصب بسته نرم‌افزاری mod-ssl-* مجموعه‌ای از کلیدهای مورد استفاده جهت رمزنگاری از طریق مراجعه به فهرست /etc/httpd/conf قابل دستیابی خواهد بود.



شکل ۱۲-۳۰ تنظیمات بخش SSL از پنجره Virtual Host Properties

اگر قصد سرویس‌دهی با ایمنی فوق‌العاده را دارید، توصیه می‌کنیم جهت دریافت اعتبارنامه‌هایی تحت عنوان CA یا اصطلاحاً Certificate Authority از شرکت‌هایی چون VeriSign یا Thawte اقدام کنید. (برای اطلاع بیشتر در این زمینه به وب سایت‌های مربوطه در آدرس http://www.verisign.com و http://www.thawte.com مراجعه کنید.) کادری را که در ادامه با عنوان "تولید کلیدهای امنیتی" مطالعه می‌کنید حاوی مطالبی درباره چگونگی پیکربندی وب سرور Apache برای سرویس‌دهی با

ایمنی بالاست. با وجود این، موضوع فوق به قدری مفصل است که مجال بررسی آن در این کتاب وجود ندارد. برای اطلاع بیشتر درباره این موضوع توصیه می‌کنیم کتاب Linux Apache Web Server را که در سال ۲۰۰۲ توسط انتشارات Sybex به چاپ رسیده است، مطالعه کنید. هم‌چنین برای اطلاع بیشتر درباره ویژگی‌های امنیتی وب سرور Apache به دو وب سایت http://httpd.apache.org و http://www.apache-ssl.org مراجعه کنید.

تغییرات اعمال شده از طریق تنظیمات شکل ۱۲-۳۰ نهایتاً در فایل /etc/httpd/conf.d/ssl.conf به ثبت می‌رسد.

تولید کلیدهای امنیتی

در این قسمت به بررسی نحوه تولید کلیدهای امنیتی برای وب سرور Apache می‌پردازیم. با فرض این‌که قبلاً به نصب بسته‌های نرم‌افزاری موردنیاز مبادرت کرده‌اید، این اقدامات را انجام دهید:

۱- با اجرای این دو فرمان کلیدهای موجود سرور را حذف کنید:

```
# rm /etc/httpd/conf/ssl.key/server.key
# rm /etc/https/conf/ssl.crt/server.crt
```

۲- فهرست جاری را با اجرای این فرمان به فهرست /user/share/ssl/certs تغییر دهید:

```
# cd /usr/share/ssl/certs
```

۳- با اجرای این فرمان کلید جدیدی برای سرور ایجاد کنید:

```
# make genkey
```

با این اقدام دو بار پیاپی اعلانی را جهت دریافت کلمه عبور موسوم به passphrase مشاهده خواهید کرد. در تعیین کلمه عبور احتیاط کنید، چرا که رمز دستیابی به اطلاعات محرمانه موجود روی وب سرور Apache است.

۴- با اجرای این فرمان اعتبارنامه CA موردنیاز را درخواست کنید:

```
# make certreq
```

با اقدام فوق اعلانی را برای دریافت کلمه عبور (یا به عبارت دیگر، passphrase) و اطلاعات مدیریتی وب سرور Apache مشاهده خواهید کرد. پس از تکمیل اطلاعات مورد درخواست، فایلی با عنوان /etc/httpd/conf/ssl.csr/server.csr ایجاد می‌شود که می‌توانید آن‌را به درخواست خود جهت تأمین اعتبارنامه CA ضمیمه کنید.

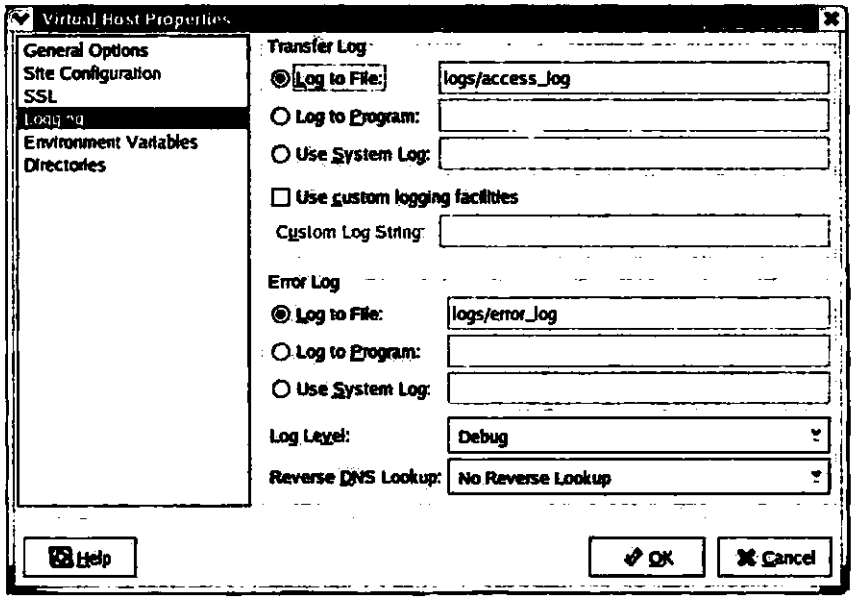
۵- پس از دریافت اعتبارنامه آن‌را با عنوان server.crt در فهرست /etc/httpd/conf/ssl.crt ذخیره کنید.

در صورت تمایل، با اجرای فرمان make testcert در مرحله چهارم می‌توانید یک اعتبارنامه غیررسمی و البته غیر معتبر برای اطمینان از عملکرد وب سرور Apache در محافظت از صفحات محرمانه ایجاد کنید.

طی دفعات بعدی راه‌اندازی وب سرور Apache اعلانی را جهت ورود کلمه عبور یا همان passphrase مشاهده خواهید کرد. در صورتی که این کلمه عبور را به اشتباه وارد کنید، وب سرور نامبرده به هیچ وجه راه‌اندازی نخواهد شد.

تنظیمات Logging

با انتخاب گزینه Logging از قاب سمت چپ پنجره Virtual Host Properties تنظیمات مربوطه در قاب سمت راست ظاهر می‌شود. چنان‌که در شکل ۱۳-۳۰ مشاهده می‌کنید، این تنظیمات به منظور پیکربندی قابلیت ثبت وقایع در وب سرور Apache پیش‌بینی شده‌اند.



شکل ۱۳-۳۰ تنظیمات بخش Logging از پنجره Virtal Host Properties

دو فایل logs/access_log و logs/error_log فایل‌هایی هستند که به منظور ثبت وقایع در وب سرور Apache پیش‌بینی شده‌اند. موقعیت نسبی این فایل‌ها با توجه به مقدار متغیر ServerRoot از فایل پیکربندی httpd تعیین می‌شود. از آن‌جا که مقدار پیش‌فرض این متغیر برابر با /etc/httpd است،

موقعیت مطلق این فایل‌ها عبارت از /etc/httpd/logs/access_log و /etc/httpd/logs/error_log خواهد بود. با وجود این، در صورت تمایل می‌توانید فایل‌های دیگری مانند mywebsite.abc/logs/access_log و mywebsite.abc/logs/error_log را برای ثبت وقایع وب سایتی چون www.mywebsite.abc مورد استفاده قرار دهید.

با فعال کردن گزینه Use Custom Logging Facilities می‌توانید الگوی عمومی مورد استفاده برای ثبت وقایع را در فیلد متنی Custom Log String وارد کنید. این فیلد متنی متناظر با متغیر LogFormat از فایل پیکربندی httpd.conf است.

گزینه‌های موجود در لیست Log Level شامل Emergency، Alert، Critical، Error، Warn، Notice، Info و Debug متناظر با مقادیر متغیر LogLevel از فایل پیکربندی httpd.conf هستند.

لیست Reverse DNS Lookup حاوی گزینه‌هایی است که خط مشی وب سرور Apache را در ارسال درخواست ترجمه آدرس‌های IP به اسامی حوزه متناظر با آن‌ها به سرور DNS مستقر در شبکه مشخص می‌کند. با انتخاب گزینه No Reverse Lookup (مگر در صورتی که از سرعت مطلوب انتقال داده‌ها در شبکه میزبان مطمئن باشید) می‌توانید ترتیبی بدهید تا وب سرور Apache از ارسال مکرر این گونه درخواست‌ها به کامپیوتر میزبان سرور DNS که نهایتاً منجر به افزایش ترافیک شبکه و کاهش کارایی آن می‌شود اجتناب کند.

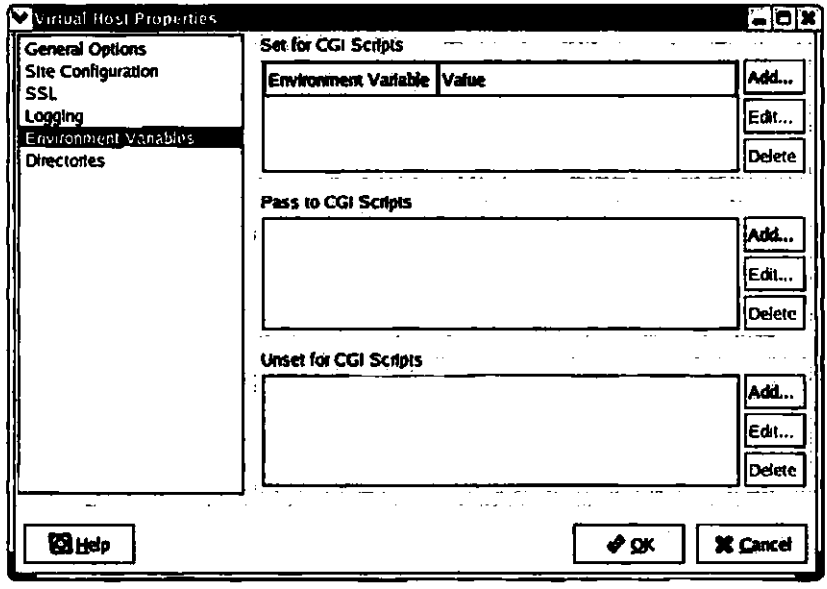
تنظیمات Environment Variables

با انتخاب گزینه Environment Variables از قاب سمت چپ پنجره Virtual Host Properties تنظیمات مربوطه در قاب سمت راست ظاهر می‌شود. چنان‌که در شکل ۱۴-۳۰ مشاهده می‌کنید، این تنظیمات به منظور مقداردهی دسته‌ای از متغیرهای سیستمی موسوم به environment variable که اغلب در صفحات حاوی برنامه‌های CGI و SSI مورد استفاده قرار می‌گیرند، پیش‌بینی شده‌اند.

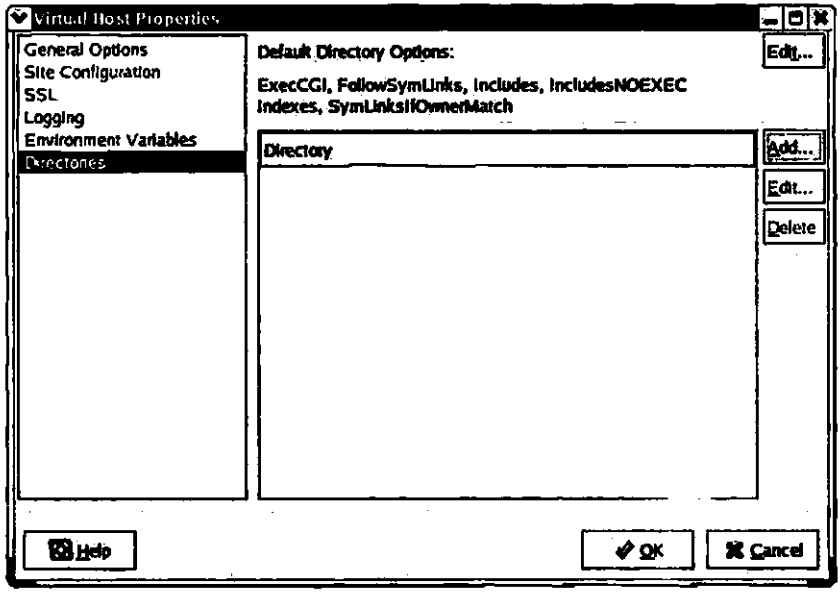
کاربرد این متغیرها مشابه متغیرهای سیستمی مورد استفاده در برنامه‌های پوسته سیستم‌عامل Linux یا اصطلاحاً shell script است، با این تفاوت که تنها صفحات حاوی برنامه‌های CGI و SSI را تحت تأثیر قرار می‌دهند.

تنظیمات Directories

با انتخاب گزینه Directories از قاب سمت چپ پنجره Virtual Host Properties تنظیمات مربوطه در قاب سمت راست ظاهر می‌شود. چنان‌که در شکل ۱۵-۳۰ مشاهده می‌کنید، این تنظیمات به منظور مقداردهی متغیر Options مربوط به فهرست‌های مختلف پیش‌بینی شده‌اند.



شکل ۱۴-۳۰ تنظیمات بخش Environment Variable از پنجره Virtual Host Properties



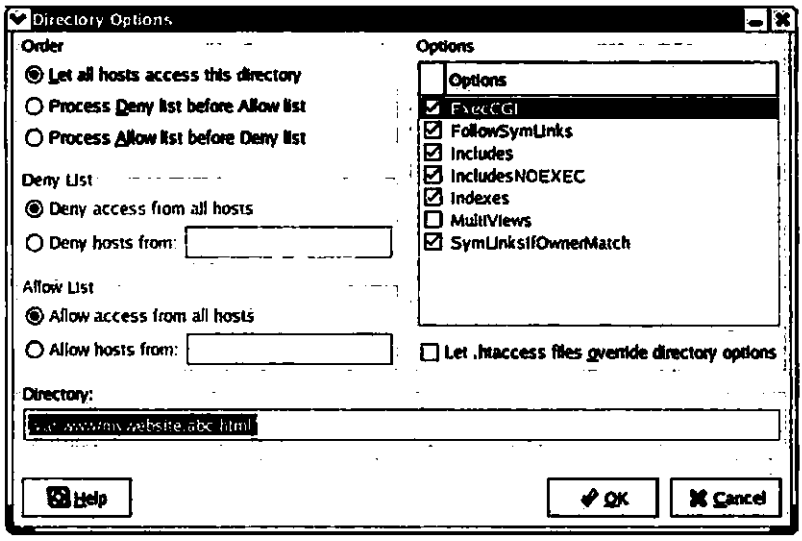
شکل ۱۵-۳۰ تنظیمات بخش Directories از پنجره Virtual Host Properties

به منظور ویرایش تنظیمات مربوط به فهرست‌های موجود ابتدا فهرست موردنظر را از لیست Directory انتخاب کرده و سپس دکمه Edit واقع در گوشه بالای سمت راست از شکل فوق را کلیک کنید. (برای اطلاع در مورد کاربر مقادیر متغیر Options شامل ExecCGI، FollowSymLinks، Includes، IncludesNOEXEC، Indexes و SymLinuxIfOwnerMatch به توضیحات مندرج در جدول ۱۵-۳۰ مراجعه کنید.)

برای تعریف یک فهرست جدید و تعیین مقادیر متغیر Options مربوط به آن روی دکمه Add کلیک کنید تا به این ترتیب پنجره Directory Options باز شده و امکانات موردنیاز را در اختیار قرار دهد. شکل ۱۶-۳۰ این پنجره را نشان می‌دهد. جدول ۱۱-۳۰ حاوی شرح مختصری درباره تنظیمات موجود در این پنجره است.

جدول ۱۱-۳۰ شرح تنظیمات موجود در پنجره Directory Options

عنوان تنظیمات	توضیح
Order	گزینه‌های موجود در این بخش به منظور تعیین اولویت در نحوه دسترسی به فهرست موردنظر پیش‌بینی شده‌اند. این گزینه‌ها به ترتیب متناظر با دستورالعمل‌های Allow from all، Order deny,allow و Order allow,deny هستند.
Deny List	گزینه‌های موجود در این بخش به منظور پیشگیری از دسترسی تمام یا تعدادی از میزبان‌ها به فهرست موردنظر پیش‌بینی شده‌اند.
Allow List	گزینه‌های موجود در این بخش به منظور دسترسی تمام یا تعدادی از میزبان‌ها به فهرست موردنظر پیش‌بینی شده‌اند.
Directory	مقدار مندرج در این فیلد متنی بیانگر فهرستی است که تنظیمات پنجره Directory Options در مورد آن انجام می‌شود.
Options	گزینه‌های موجود در این بخش امکان تعیین مقادیر متغیر Options مربوط به فهرست موردنظر را در اختیار می‌گذارد.
.htaccess	این گزینه امکان رونویسی تنظیمات پنجره Directory Options با تنظیمات مندرج در فایل پیکربندی htaccess. مربوط به فهرست موردنظر را در اختیار می‌گذارد.



شکل ۱۶-۳۰ پنجره Directory Options

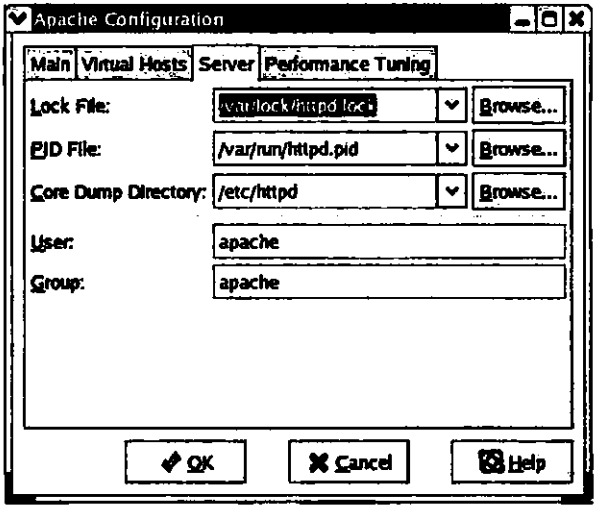
تنظیمات سرور

بخش Server از پنجره Apache Configuration شامل تنظیمات اولیه وب سرور Apache است. شکل ۱۷-۳۰ تنظیمات موجود در این بخش را نشان می‌دهد. جدول ۱۲-۳۰ حاوی شرح مختصری درباره این تنظیمات است.

جدول ۱۲-۳۰ شرح تنظیمات موجود در بخش Server از پنجره Apache Configuration

عنوان تنظیمات	توضیح
Lock File	این گزینه فایلی را مشخص می‌کند که به محض راه‌اندازی وب سرور Apache باز شده و تا توقف آن در همین وضعیت باقی می‌ماند.
PID File	این گزینه فایلی را مشخص می‌کند که حاوی شناسه فرآیندهای مربوط به سرویس‌های httpd است. فایل مزبور نیز به هنگام راه‌اندازی وب سرور Apache باز شده و تا توقف آن در همین وضعیت باقی می‌ماند.
Core Dump Directory	این گزینه فهرست مورد استفاده به منظور اشکال‌زدایی (موسوم به core dump) را مشخص می‌کند. این فهرست تنها توسط مدیر وب سرور Apache (که اغلب با شناسه apache مشخص می‌شود) قابل نوشتن است.
User	این گزینه شناسه کاربری مدیر وب سرور Apache را مشخص می‌کند.

عنوان تنظیمات	توضیح
Group	این گزینه شناسه گروهی را که مدیر وب سرور Apache در آن عضویت دارد، مشخص می‌کند.



شکل ۱۷-۳۰ تنظیمات موجود در بخش Server از پنجره Apache Configuration

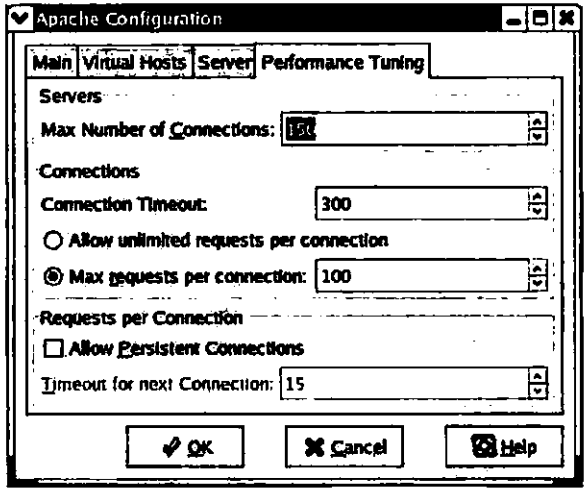
تنظیمات مربوط به کارایی وب سرور

بخش Performance Tuning از پنجره Apache Configuration شامل تنظیمات مربوط به کارایی وب سرور Apache است. شکل ۱۸-۳۰ تنظیمات موجود در این بخش را نشان می‌دهد. جدول ۱۳-۳۰ حاوی شرح مختصری درباره این تنظیمات است.

جدول ۱۳-۳۰ شرح تنظیمات موجود در بخش Performance Tuning

عنوان تنظیمات	توضیح
Max Number Of Connections	این گزینه که متناظر با متغیر MaxClients از فایل پیکربندی httpd.conf است، بیشترین تعداد برنامه‌های کلاینتی را که به طور هم‌زمان می‌توانند به وب سرور Apache متصل شوند، مشخص می‌کند.
Connection Timeout	این گزینه که متناظر با متغیر TimeOut از فایل پیکربندی httpd.conf است، بیانگر مدت زمانی بر حسب ثانیه است که وب سرور Apache برای برقراری ارتباط از جانب برنامه کلاینت منتظر می‌ماند. پس از سپری

عنوان تنظیمات	توضیح
	شدن این مدت زمان، برنامه کلاینت برای ارتباط با وب سرور Apache باید مجدداً اقدام کند.
Requests Per Connection	این گزینه که متناظر با متغیر MaxRequestsPerChild از فایل پیکربندی httpd.conf است، بیانگر بیشترین تعداد درخواست‌هایی است که هر برنامه کلاینت طی هر بار برقراری ارتباط با وب سرور Apache می‌تواند برای آن ارسال کند.
Allow Persistent Connection	این گزینه که متناظر با متغیر KeepAlive از فایل پیکربندی httpd.conf است، ارتباط با برنامه کلاینت را صرف نظر از تنظیمات متغیر TimeOut هم‌چنان حفظ می‌کند.
Timeout For Next Connection	این گزینه که متناظر با متغیر KeepAliveTimeout از فایل پیکربندی httpd.conf است، در صورت فعال بودن گزینه Allow Persistent Connection (که منجر به مقداردهی KeepAlive On در فایل پیکربندی مذکور می‌شود) امکان تعیین حداکثر مدت زمانی را که ضمن آن برنامه کلاینت، مجاز به ارسال درخواست بعدی به وب سرور Apache است بر حسب ثانیه مشخص می‌کند.



شکل ۱۸-۳۰ تنظیمات موجود در بخش Performance Tuning از پنجره Apache Configuration

وب سرور Red Hat Content Accelerator

نرم‌افزار Red Hat Content Accelerator که سابقاً با عنوان TUX شناخته می‌شد، وب سروری است که توسط شرکت Red Hat و به منظور سرویس‌دهی صفحات ایستا طراحی شده است. این نرم‌افزار در قالب هسته سیستم‌عامل Linux پیاده‌سازی شده و از این‌رو سرعت سرویس‌دهی آن بسیار قابل توجه است. با وجودی که می‌توان این نرم‌افزار را برای سرویس‌دهی صفحات پویا نیز به کار گرفت، شرکت Red Hat استفاده از آن‌را تنها برای صفحات ایستا توصیه می‌کند. ویژگی جالب توجه وب سرور مذکور این است که می‌توان آن‌را به همراه وب سرور Apache مورد استفاده قرار داد. بهترین پیکربندی ممکن در این رابطه به نحوی است که برای سرویس‌دهی صفحات ایستا از وب سرور Red Hat Content Accelerator و برای سرویس‌دهی صفحات پویا از وب سرور Apache استفاده شود.

در حال حاضر این نرم‌افزار را در صورتی می‌توان به همراه وب سرور Apache مورد استفاده قرار داد که هر دو روی یک کامپیوتر واحد نصب شده باشند. چنین شرایطی برای سرویس‌دهی در مقیاس بزرگ که مستلزم به کارگیری چندین وب سرور Apache در موقعیت‌های جغرافیای مختلف است به هیچ عنوان مناسب نیست. توسعه‌دهندگان شرکت Red Hat هم‌اینک در تلاش هستند تا این محدودیت را برطرف کنند. از آن‌جا که بسته نرم‌افزاری وب سرور Red Hat Content Accelerator تحت عنوان TUX منتشر می‌شود، از این به بعد جهت سادگی از عنوان TUX برای اشاره به وب سرور مذکور استفاده خواهیم کرد.

اصطلاح TUX کوتاه شده عبارت Threaded Linux web server و ضمناً نام پنگوئنی است که به عنوان نماد سیستم‌عامل Linux دارای شهرت جهانی است.

نصب و راه‌اندازی وب سرور TUX

از آن‌جا که هر دو وب سرور TUX و Apache سرویس‌دهی خود را از طریق پورت TCP/IP شماره ۸۰ انجام می‌دهند، بدیهی است که نمی‌توان این دو نرم‌افزار را به طور هم‌زمان راه‌اندازی کرد. از این‌رو، پیش از نصب و راه‌اندازی وب سرور TUX باید وب سرور Apache را متوقف کرد. به مراحل انجام این کار توجه کنید:

۱- بسته نرم‌افزاری tux-* را روی کامپیوتر میزبان نصب کنید.

۲- سند وب دلخواهی را به index.html تغییر نام داده و آن‌را در فهرستی که توسط مقدار متغیر DOCROOT از فایل پیکربندی این وب سرور مشخص شده است، کپی کنید. (این فهرست

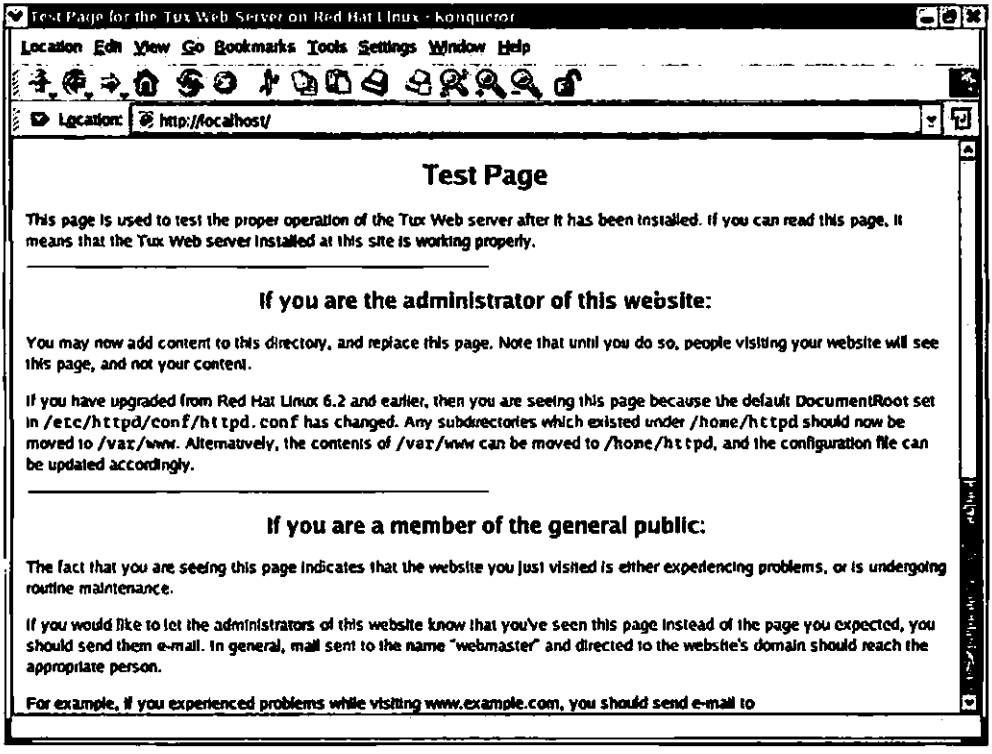
مشخصاً /var/www/html است.) برای این منظور می‌توانید فایل noindex.html از فهرست /var/www/error را مورد استفاده قرار دهید.

۳- با اجرای فرمان service httpd stop وب سرور Apache را متوقف کنید.

۴- با اجرای فرمان service tux start وب سرور TUX را راه‌اندازی کنید.

۵- آدرس http://localhost را در نوار آدرس مرورگر موردنظر خود وارد کرده و کلید Enter را فشار دهید.

شکل ۱۹-۳۰ نتیجه چنین اقدامی را در قالب مرورگر Konqueror نشان می‌دهد.



شکل ۱۹-۳۰ سرویس‌دهی سند index.html توسط وب سرور TUX

با مشاهده این شکل می‌توانید از عملکرد وب سرور TUX در بازیابی سند index.html از فهرست میزبان، یعنی /var/www/html اطمینان حاصل کنید. در قسمت‌های بعد جزییات بیشتری را درباره وب سرور TUX مورد بررسی قرار می‌دهیم.

بنا به توصیه شرکت Red Hat، بهتر است فهرست ریشه وب سرور TUX را که توسط مقدار متغیر DOCROOT از فایل پیکربندی مربوطه مشخص می‌شود، روی دیسک RAID دیگری مستقر کنید. متغیر مذکور متناظر با متغیر DocumentRoot در وب سرور Apache است. (برای اطلاع درباره دیسک‌های RAID به فصل چهاردهم مراجعه کنید.)

پیکربندی وب سرور TUX

از آن‌جا که وب سرور TUX در قالب هسته سیستم‌عامل Linux پیاده‌سازی شده، تنظیمات پیش‌فرض آن در نه فایل پیکربندی این نرم‌افزار بلکه در فایل /etc/sysconfig/tux منظور شده است. این فایل شامل شش متغیر است که جدول ۱۴-۳۰ به اختصار آن‌ها را شرح می‌دهد.

جدول ۱۴-۳۰ شرح متغیرهای پیکربندی وب سرور TUX

عنوان متغیر	توضیح
TUXTHREADS	مقدار این متغیر بیانگر بیشترین تعداد threadهایی است که وب سرور TUX مجاز به ایجاد آن است. این مقدار متغیر به هیچ وجه نباید بیش از تعداد پردازنده‌های کامپیوتر میزبان باشد.
DOCROOT	این متغیر متناظر با متغیر DocumentRoot از وب سرور Apache بوده و مقدار آن بیانگر فهرست اصلی وب سرور TUX است. انتظار می‌رود که فایلی با خاصیت index.html در این فهرست موجود باشد. مقدار پیش‌فرض این متغیر /var/www/html است.
LOGFILE	این متغیر بیانگر موقعیت فایل ثبت وقایع وب سرور TUX است. چنان‌که انتظار می‌رود، مقدار پیش‌فرض این متغیر /va/log/tux است.
DAEMON_UID	این متغیر با مقدار پیش‌فرض nobody بیانگر یک شناسه کاربری مجاز در وب سرور TUX است.
DAEMON_GID	این متغیر با مقدار پیش‌فرض nobody بیانگر یک شناسه گروه مجاز در وب سرور TUX است.
CGIROOT	این متغیر بیانگر فهرست میزبان برنامه‌های CGI است.
MAX_KEEPALIVE_TIMEOUT	این متغیر بیانگر حداکثر مدت زمانی است که وب سرور TUX جهت برقراری ارتباط از جانب برنامه کلاینت منتظر می‌ماند. پس از سپری شدن این مدت زمان، برنامه مزبور برای برقراری ارتباط با وب سرور

عنوان متغیر	توضیح
	TUX باید مجدداً اقدام کند.
TUXMODULES	این متغیر بیانگر ماجول‌های مورد استفاده وب سرور TUXاست.
MODULEPATH	این متغیر بیانگر فهرست میزبان ماجول‌های مورد استفاده وب سرور TUX است.

وب سرور TUX دارای تعدادی فایل ثبت وقایع است که در قالب یک باینری فشرده با عنوان tux در فهرست var/log/ مستقر شده‌اند. فرمان tux2w3c امکان بازخوانی این فایل‌ها را در اختیار می‌گذارد. شکل ۲۰-۳۰ نحوه استفاده از این فرمان برای بازخوانی فایل ثبت وقایع var/log/tux/ را نشان می‌دهد.

```
[root@RH9Desk root]# tux2w3c /var/log/tux
127.0.0.1 - - [03/Apr/2003:16:08:08 -0500] "GET / HTTP/1.0" 200 2898 "-" ""
10.252.113.122 - - [03/Apr/2003:16:09:48 -0500] "GET / HTTP/1.1" 200 2898 "-" ""
10.252.113.122 - - [03/Apr/2003:16:09:48 -0500] "GET /icons/apache_pb.gif HTTP/1
.1" 404 0 "-" ""
10.252.113.122 - - [03/Apr/2003:16:09:48 -0500] "GET /icons/powered_by.gif HTTP/
1.1" 404 0 "-" ""
10.252.113.122 - - [03/Apr/2003:16:09:55 -0500] "GET / HTTP/1.1" 304 0 "-" ""
10.252.113.122 - - [03/Apr/2003:16:09:55 -0500] "GET /icons/apache_pb.gif HTTP/1
.1" 404 0 "-" ""
10.252.113.122 - - [03/Apr/2003:16:09:55 -0500] "GET /icons/powered_by.gif HTTP/
1.1" 404 0 "-" ""
10.252.113.122 - - [03/Apr/2003:16:09:55 -0500] "GET / HTTP/1.1" 304 0 "-" ""
10.252.113.122 - - [03/Apr/2003:16:09:56 -0500] "GET /icons/apache_pb.gif HTTP/1
.1" 404 0 "-" ""
10.252.113.122 - - [03/Apr/2003:16:09:56 -0500] "GET /icons/powered_by.gif HTTP/
1.1" 404 0 "-" ""
[root@RH9Desk root]#
```

شکل ۲۰-۳۰ نحوه بازخوانی محتوای فایل باینری var/log/tux/ با استفاده از فرمان tux2w3c

چنان‌که مشاهده می‌کنید، یکی از وقایع ثبت شده، اقدام برای دسترسی به وب سرور TUX از طریق کامپیوتر میزبان این وب سرور (با شاخص 127.0.0.1) و دیگری از کامپیوتری با شاخص 10.252.113.122 بوده است.

استفاده توأم از وب سرورهای TUX و Apache

چنان‌چه وب سرورهای TUX و Apache برای سرویس‌دهی از پورت‌های TCP/IP مختلفی استفاده کنند، می‌توان آن‌ها را به طور هم‌زمان در کنار یکدیگر مورد بهره‌برداری قرار داد. برای این منظور باید

تغییراتی را حداقل در فایل پیکربندی یکی از این دو وب سرور صورت دهید. چنان‌که به زودی خواهید دید، انجام این کار با فایل پیکربندی وب سرور Apache یعنی httpd.conf مستلزم تغییر مقادیر دو متغیر Listen و NameVirtualHost است.

مقدار متغیر Listen در حقیقت بیانگر کانالی است که وب سرور Apache از طریق آن درخواست‌های ارسالی از جانب برنامه‌های کلاینت را دریافت می‌کند. مقدار این متغیر به طور پیش‌فرض برابر با 80 است، به این معنی که وب سرور نامبرده تنها از طریق پورت TCP/IP شماره ۸۰ درخواست‌های ارسالی را دریافت می‌کند. برای پیشگیری از تناقض با تنظیمات مشابه در وب سرور TUX، متغیر Listen را به این صورت در فایل پیکربندی httpd.conf مقداردهی کنید:

```
Listen 127.0.0.1:8080
```

با این تغییرات، وب سرور Apache تنها درخواست‌های ارسالی به پورت TCP/IP شماره ۸۰ از کامپیوتر محلی را مورد توجه قرار خواهد داد.

تغییرات فوق تنظیمات وب سرور TUX را نیز تحت تأثیر قرار می‌دهد، به طوری که اکنون محتوای فایل clientport از فهرست تنظیمات مربوط به وب سرور TUX یعنی /proc/sys/net/tux باید عبارت از 8080 باشد.

اکنون فرض کنید میزبان مجازی مورد نظرتان را از طریق تنظیمات فایل httpd.conf پیکربندی کرده و متغیر NameVirtualHost مربوطه را به این صورت مقداردهی می‌کنید:

```
NameVirtualHost 192.168.13.64:80
```

با تنظیمات فوق این بار فایل پیکربندی دیگری از وب سرور TUX با عنوان /proc/net/tux/0/listen/0 تحت تأثیر قرار می‌گیرد. محتوای فایل مذکور پس از این تنظیمات عبارت از این خواهد بود:

```
http://0.0.0.0:80
```

این بدان معنی است که وب سرور TUX کلیه درخواست‌های ارسالی به پورت TCP/IP شماره ۸۰ از جانب هر کامپیوتر دلخواهی را مورد توجه قرار خواهد داد.

با انجام این تغییرات اکنون می‌توان دو وب سرور TUX و Apache را در کنار یکدیگر مورد استفاده قرار داد. چنان‌چه قبلاً وب سرور apache را متوقف کرده‌اید، اکنون با اجرای این فرمان برای راه‌اندازی مجدد آن اقدام کنید:

```
service httpd start
```

جمع‌بندی

سیستم‌عامل Linux دارای قابلیت‌های سرویس‌دهی مختلفی در شبکه است. این سیستم‌عامل از سرویس وب به عنوان یکی از سرویس‌های متداول شبکه به خوبی پشتیبانی می‌کند. وب سرورهای

مختلفی از جمله Apache، TUX، AOLServer، BOA و Zeus را می‌توان روی سیستم عامل Linux پیکربندی کرده و مورد استفاده قرار داد.

در حال حاضر، نرم‌افزار Apache رایج‌ترین وب سرور موجود روی اینترنت محسوب می‌شود. ویرایش 2.0.x از این وب سرور دارای قابلیت‌های جدیدی از جمله پشتیبانی از میزبان‌های مجازی مختلف با استفاده از یک آدرس IP واحد است.

فایل اصلی پیکربندی وب سرور Apache با عنوان httpd.conf یک فایل طولانی اما نه پیچیده است. در این فصل تنظیمات این فایل را در قالب سه گروه مختلف با عنوان متغیرهای سراسری، متغیرهای اصلی پیکربندی سرور و متغیرهای موردنیاز برای پیکربندی میزبان‌های مجازی با استفاده از یک آدرس IP واحد مورد بررسی قرار دادیم.

شرکت Red Hat نیز مبادرت به طراحی و پیاده‌سازی یک وب سرور با عنوان Red Hat Content Accelerator کرده است. این وب سرور که پیش از این TUX نامیده می‌شد، دارای سرعت بسیار قابل توجهی در سرویس‌دهی صفحات ایستاست. این قابلیت به مدد پیاده‌سازی کد مربوطه در قالب هسته سیستم‌عامل Linux حاصل شده است. در صورت تمایل، با چند تغییر ساده می‌توان دو وب سرور TUX و Apache را در کنار یکدیگر مورد استفاده قرار داد. بنا به توصیه شرکت Red Hat بهتر است نرم‌افزار TUX را به عنوان وب سرور اصلی پیکربندی کرده و نرم‌افزار Apache را جهت سرویس‌دهی صفحات پویا پیکربندی کنید.

با اتمام این فصل بخش اصلی کتاب نیز به پایان می‌رسد.

ضمناً پنج فصل تکمیلی نیز روی وب مستقر شده که از طریق آدرس وب سایت انتشارات Sybex می‌توانید آن‌ها را مورد بازبینی و مطالعه قرار دهید. فصل نخست از این مجموعه به بررسی مهم‌ترین برنامه‌های اعطای گواهی‌نامه Linux می‌پردازد. در این زمینه تنوع نسبتاً زیادی وجود دارد. برای مثال، آزمون CompTIA Linux+ برای کاربران کم‌تجربه‌ای که سابقه کار تقریباً ۶ ماهه با این سیستم‌عامل دارند، تهیه شده است. در حالی که آزمون‌های SAIR و LPI برای کاربران با تجربه‌ای که دست کم دو سال مشغول کار با سیستم‌عامل Linux هستند، تدارک دیده شده است. فصل دوم به بررسی گواهی‌نامه‌های شرکت Red Ha می‌پردازد. آزمون‌های این شرکت به واقع یکی از کاربردی‌ترین و در عین حال مشکل‌ترین‌ها در صنعت کامپیوتر محسوب می‌شود. فصل سوم به معرفی منابع online اختصاص دارد. فصل چهارم حاوی نسخه کاملی از سند GNU/Linux General Public License است. فصل پنجم حاوی لیستی از عناوین بسته‌های نرم‌افزاری عرضه شده به همراه سیستم‌عامل Red Hat Linux است که بر اساس گروه‌های نرم‌افزاری مربوطه سازمان‌دهی شده‌اند. این فصل مرجع خوبی برای پیکربندی برنامه Kickstart است.