

Gavetas Externas para HD
Como ter um servidor de dados na rede com NAS e NDAS

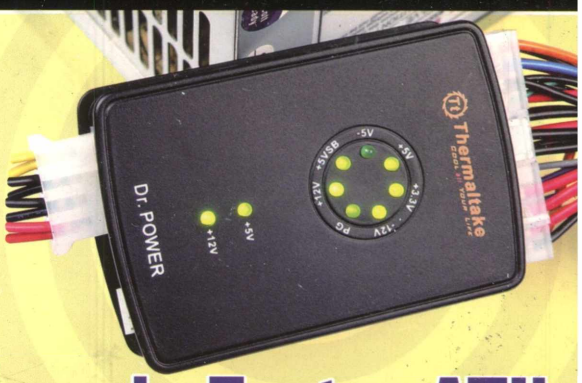
Restrição de Software
Controle o que pode ser executado no Windows

Notebooks
Testamos mais 3 modelos que chegam ao mercado

www.revistapcecia.com.br

PC &CIA

SABER



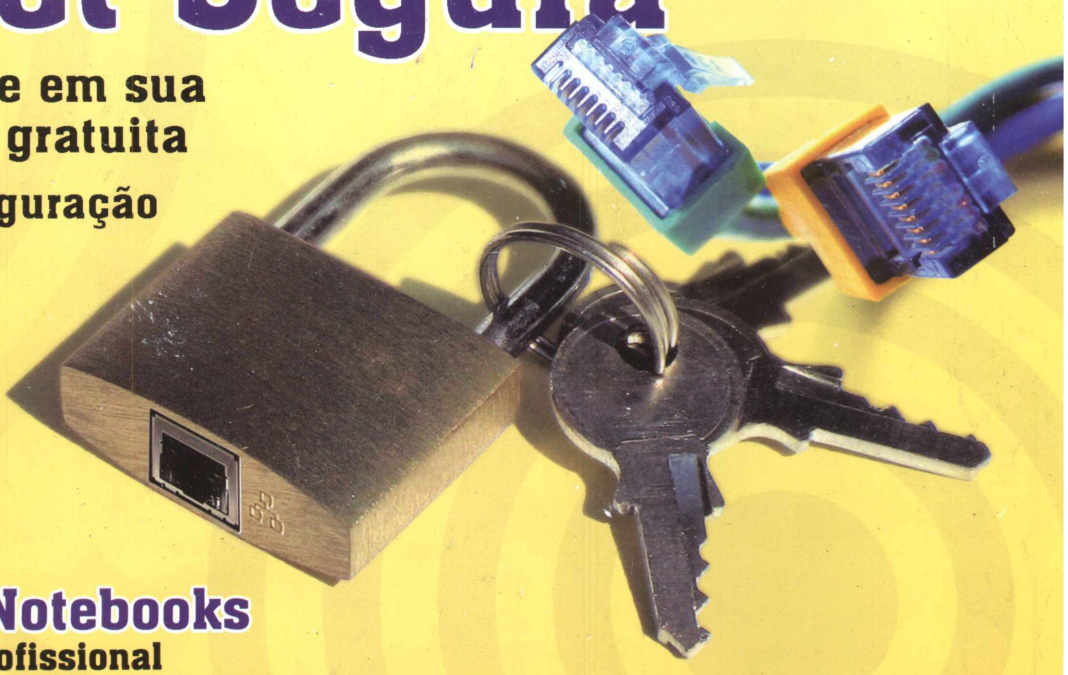
Testadores de Fontes ATX

Chega de mitos! Saiba como realmente fazer um teste conclusivo

ANO 7 - Nº 76 - Novembro / 2007 Europa €4,30 - Brasil R$12,90

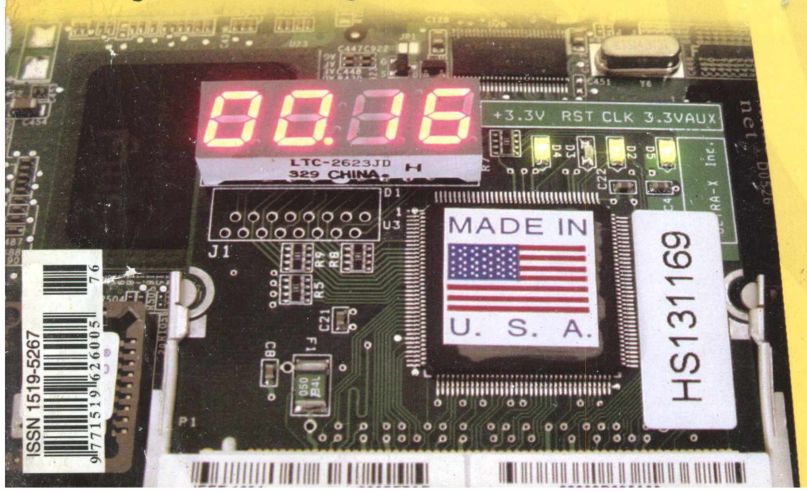
Internet Segura

- ✔ **Faça um upgrade em sua máquina virtual gratuita**
- ✔ **Instalação e configuração passo a passo**
- ✔ **Para PC ou ambientes de rede**



Manutenção de Notebooks

Conheça uma solução profissional



Mandriva Linux 2008

Instalação e uso do sistema
Saudades do Windows?
Pode esquecer!

E mais:

Memórias DDR3 x DDR2
Placas de Vídeo DX10

ISSN 1519-5267

Jogue seus cartuchos originais fora!

Agora você pode ter, em sua casa ou trabalho, economia com qualidade para suas fotos e trabalhos.

BULK PARA NOVA LINHA DE IMPRESSORAS EPSON

Bulk Ink para EPSON

Sistema de tinta com cartuchos sem esponja, Chip Full, Reservatórios Externo de Tinta e Resíduo, Kit de Montagem, Jogo de tintas com 60ml por cor. Manual em Português.

Kit de Cartuchos para EPSON

Cartuchos Recarregáveis de tinta sem esponja com Chip Full, Reservatório de Resíduo, Jogo de tintas com 30ml por cor. Manual em Português.



Preços a partir de R$18,00 por cartucho para Kit de cartuchos recarregáveis.(*)

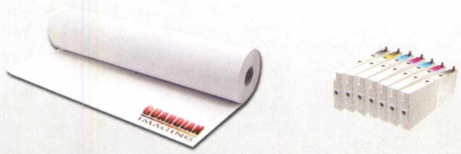
Economize com segurança para seu equipamento

BULK INK SYSTEM

Até **96%** de economia

Veja em: www.photoink.com.br/economize





Bulk Ink para EPSON/HP. Kit de Cartuchos Recarregáveis. Kits de Recarga. Papel Fotográfico Brilhante/Satin resistente a água nos formatos A4/A3 ou em Rolos 43 / 61 / 91,4 / 110 / 127 cm. Tintas Inkjet à base Corante(MGS) / Pigmentada(Ultrachrome) ou para Sublimação(Sublimation). Tudo para sua impressora...

www.photoink.com.br

Tel/Fax: (21) 2223-3673 • e-mail: sac@photoink.com.br

GUARDIAN IMAGING

PRODUTOS DISPONÍVEIS PARA OS MODELOS:
EPSON INKJET: C45 /C63 /C65 /C67 /C79 /C82 /C83 /C85 /C87 /C89 /C92 /C110 /R200 /R220 /R260 /R270 /R290 /R300 /R320 /R340 /R380 /CX3500 /CX3700 /CX4100 /CX4500 /CX4700 /CX4900 /CX5600 /CX5700 /CX5900 /CX6500 /CX6700 /CX7300 /CX8300.
EPSON STYLUS PHOTO 1800 /2200 /2400 /4000 /4600 /4800.
EPSON STYLUS PRO 7000 /7600 /7800 /9600 /9800
HP: K550 /K850 /1100 /1200 /2100 /2200.

PHOTO & INK .com.br

* Para Kits de Cartuchos Recarregáveis, que são vendidos em conjunto de acordo com a configuração da impressora. O preço exibido está expresso em Real, sujeito a alteração mediante data de publicação ou duração de estoque. Todos os direitos reservados. Guardian Imaging Company.

Editora Saber Ltda.

Diretores
Hélio Fittipaldi
Thereza Mozzato Ciampi Fittipaldi

PC &CIA

www.revistapcecia.com.br

Editor e Diretor Responsável
Hélio Fittipaldi

Editor de Tecnologia
Fernando Ramos da Silva

Conselho Editorial
Newton C. Braga, Orlando Gomes Ferreira

Colaboradores
Anderson Costa, Daniel Appel, Fernando Vieira, Flávio de Souza Oliveira, Igor Humberto, Jansen Carlo Sena, Marcus Brandão de Moura, Paulo Roberto Sant'anna Cardoso, Roberto Cunha

Auxiliar de Redação
Claudia Tozetto
Fabieli de Paula

Designers
Diego M. Gomes, Luiz Fernando Almeida, Tiago P. de Lira.

Produção
Yassari Gonçalo

VENDAS DE PUBLICIDADE

André Zanferrari, Carla de Castro Assis, Ricardo Nunes Souza

PARA ANUNCIAR: (11)6195-5339
publicidade@editorasaber.com.br

Impressão
Prol Editora Gráfica Ltda.

Distribuição
Brasil: DINAP
Portugal: Logísta - tel.:121 926-7800

ASSINATURAS
www.revistapcecia.com.br
Fone: (11) 6195-5335 /Fax: (11) 6198-3366
Atendimento das 8:30 às 17:30 h

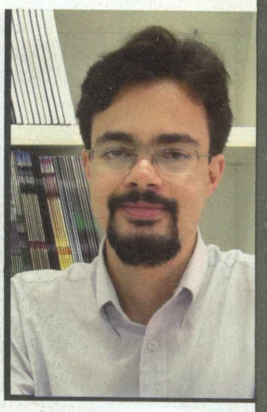
PC & CIA é uma publicação mensal da Editora Saber Ltda, ISSN 1519-6267. Redação, administração, publicidade e correspondência: Rua Jacinto José de Araújo, 315, Tatuapé, CEP 03087-020, São Paulo, SP, tel./ fax (11) 6195-5333. Edições anteriores (mediante disponibilidade de estoque), solicite pelo site www.revistapcecia.com.br, ou pelo tel. 6195-5330, ao preço da última edição em banca.

Associada da:

ANER
www.aner.org.br
Associação Nacional dos Editores de Revistas.

anatec 28 anos
www.anatec.org.br
Associação Nacional das Editoras de Publicações Técnicas, Dirigidas e Especializadas.

Os artigos assinados são de exclusiva responsabilidade de seus autores. É vedada a reprodução total ou parcial dos textos e ilustrações desta revista, sob pena de sanções legais.



Mercado brasileiro de computação

De emergente a sofisticado, esta é a conclusão de um estudo sobre o mercado brasileiro de computação, que a Intel apresentou à imprensa há alguns meses. Vale ressaltar que, diferentemente de outros trabalhos semelhantes, normalmente feitos por empresas de pesquisas de mercado, como a IDC, neste caso em específico as estatísticas foram construídas sobre dados de vendas da Intel em todo o mundo.

Dentre os números mais representativos, constam o da perspectiva de que o Brasil deixará de ser o sétimo maior mercado de computadores no mundo, em 2007, para se tornar o terceiro, em 2010, ficando apenas atrás dos EUA e China, que hoje já estão na ponta, respectivamente. Em números absolutos, estima-se que serão vendidos 9,5 milhões de computadores neste ano – ultrapassando a venda de TVs - e 17,5 milhões, em 2010.

Além de interesses do governo em áreas como a educação, por exemplo, o entretenimento e as necessidades de comunicação dos usuários estariam entre os demais fomentadores deste crescimento. Outros dados indicativos para esta sofisticação são as novidades tecnológicas sendo lançadas por aqui com uma diferença de tempo cada vez menor em relação ao resto do mundo e o franco crescimento da indústria local. Aliás, há muito não se via tantos anúncios de novas fábricas de empresas ligadas à área de informática.

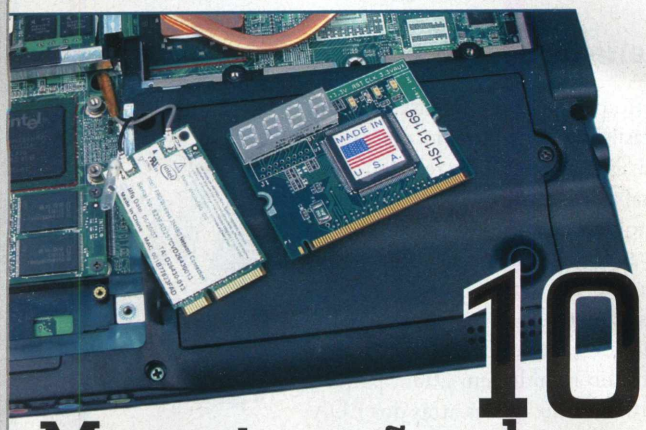
No início deste mês tive a grata satisfação de presenciar a inauguração da nova fábrica da Digitron, em Manaus. Ocupando 14 dos 64 mil metros quadrados da planta, a fábrica foi desenvolvida segundo padrões internacionais de produção e controle ambiental. Para tanto, recebeu US$ 40 milhões em investimentos e está preparada para ampliar em 40% a atual capacidade produtiva da Digitron. Suas 11 linhas de montagem poderão produzir até 1,2 milhão de placas, entre placas-mãe, de rede e fax-modem. Os reflexos já estão sendo sentidos em anúncios como o da produção local de placas-mãe *high-end*, como a P35-DQ6 para a plataforma Intel, em substituição à importação, o que só se justifica pelo ganho de escala de produção e conseqüente diminuição dos custos.

Num futuro não muito distante, acredita-se que o varejo continuará evoluindo em sofisticação. Ao invés de uma seção geral para PCs e outra para notebooks nas prateleiras, deveremos ver diversas seções para diferentes nichos, tais como HTPC (PC Home Theater), Jogos, etc. As opções de modelos personalizáveis também devem aumentar em número. Basicamente, assistiremos a um processo bastante similar ao que já existe em outras partes do mundo, como a rede FRYS, nos EUA.

Agora, se há um problema que precisa ser equacionado é o da prestação de serviço. Infelizmente, a somatória do jeitinho brasileiro de fazer as coisas sem muito critério e a baixíssima qualificação técnica e também cultural faz com que o varejo local ainda esteja muito distante de oferecer o nível de satisfação sequer condizente com a palavra sofisticação. E essa constatação, em geral, também é válida entre revendas e assistência técnica de grandes empresas. Aliás, se é verdade que o portfólio de marcas é cada vez maior, o que não faltam também são produtos com propostas totalmente equivocadas. O que dizer de HTPC, MediaPCs, ou Media Centers, como também são conhecidos, barulhento para sua sala de estar? Ou então, de PCs populares com Linux sem qualquer configuração específica para o hardware instalado e que na verdade só serve de pretexto para entrar no programa de incentivo fiscal do governo? Em resumo, há motivos de sobra para crer na sofisticação e igualmente na abertura de muitas oportunidades para os empreendedores de plantão.

Fernando Ramos da Silva
fernando@editorasaber.com.br

HARDWARE



10 Manutenção de notebooks

14 Testadores de Fontes ATX

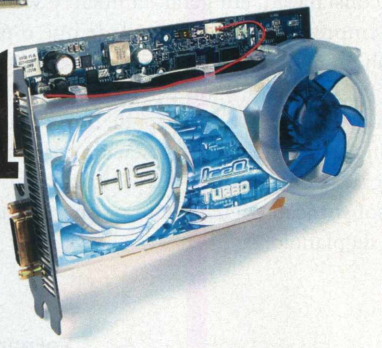
TESTES

17 Notebooks: por dentro das opções

Upgrade na Internet segura **20**



25 DDR3 x DDR2

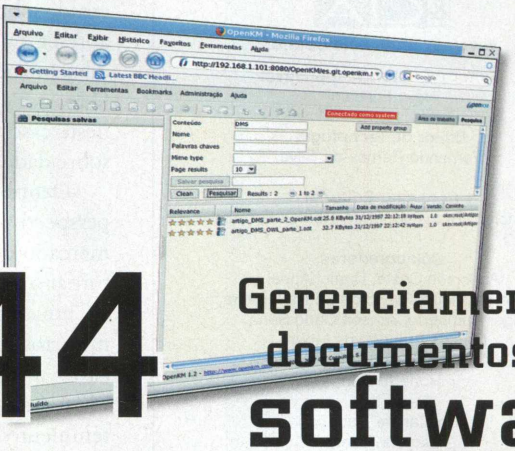


31 Placas de vídeo DX10 para a massa

Gavetas Externas com suporte a NAS e NDAS **36**

SISTEMAS OPERACIONAIS

41 Certificação Microsoft MCTS – Parte 4



44 Gerenciamento de documentos com software livre

Restrição de software: maior controle no Windows **50**

54 Winbind: a chave para a integração entre o Active Directory e o Linux

58 Família Microsoft Forefront



60 Mandriva Linux 2008

5 Segurança High-Tech: Preparar... apontar... pacote IP?

6 A vez do leitor

8 Notícias

Preparar... apontar... ...pacote IP???



Jansen Carlo Sena
Mestre em Segurança de Sistemas pela Unicamp. Certificado LPI, sócio e fundador da ONG Comunidade SOL Software Livre, atualmente trabalha no Centro de Pesquisa e Desenvolvimento da BenQ Mobile.

Achou estranho o título? Acabou o tempo em que a guerra era somente sinônimo de soldados armados até os dentes, caças, tanques e outros tipos de artilharias. A Internet criou um outro disputado campo de batalha: o ciberespaço. Em outras palavras, além de diversão, negócios, notícias e serviços, pelos equipamentos da rede mundial de computadores trafegam pacotes que fazem parte de uma silenciosa guerra que vem sendo travada pelas mesmas nações que disputam posições de maior destaque no cenário mundial. A esse tipo de atividade, convencionou-se chamar de cyberwar ou netwar. A munição utilizada contém paralisação de servidores e serviços, roubo de informações, disseminação de vírus, pichação de sites para publicação de mensagens de caráter político, social e cultural, dentre outros.

E no centro desse processo, os EUA e a China vêm protagonizando as notícias que circulam na mídia especializada. Somente para citar um primeiro exemplo, recentemente atacantes chineses desfiguraram vários sites vinculados ao governo norte-americano, dentre eles o da Força Aérea, Departamento de Energia, Departamento Nacional de Serviços Humanos, dentre outros.

Interessante notar é que as últimas ondas de ataques foram completamente coordenadas. Grupos de atacantes marcaram reuniões pela Internet para traçar as estratégias e as metas a serem atingidas com a ofensiva. Em resposta aos ataques chineses, grupos de atacantes norte-americanos picharam 15 sites do governo chinês inserindo nas páginas mensagens relacionadas à etnia e convidando os atacantes chineses para dar continuidade à guerra promovida no cyberespaço. Em geral, as ondas de ataques aumentam quando ocorrem "deslizes diplomáticos" entre os dois países.

Enfim, não é só treinando soldados com armamentos e técnicas de guerra convencionais que a China se prepara para brigar por maior representatividade no cenário mundial. O gigante vermelho tem procurado garantir o domínio eletromagnético, conforme estudo publicado pelo Pentágono sobre o poderio militar chinês, por meio da capacitação de seus "cyber-guerreiros" e do desenvolvimento, por exemplo, de vírus voltados para atingir os ambientes inimigos. Por outro lado, os norte-americanos, segundo os chineses, também têm promovido ataques constantes a estruturas de rede chinesas, fundamentalmente aquelas que contém alguma relação com o governo.

A cyberwar se agrava ainda mais pelo fato de não ser tão fácil estabelecer fronteiras entre os países envolvidos. Alguns roteadores e links são suficientes para alcançar servidores do inimigo. Nenhum pacote IP precisa apresentar passaporte para adentrar nos segmentos de Internet do país inimigo. Isso faz com que a cyberwar seja uma atividade silenciosa e recheada de boatos e falsas notícias. O fato é que nenhum dos governos confirma atividades oficiais, por meio do uso da rede mundial.

Talvez o agente 007 da era das redes de computadores necessitasse somente de um notebook e uma conexão à Internet para desempenhar suas atividades, ao invés de arriscar a pele em suas aventuras tradicionais.

> **Talvez o agente 007 da era das redes de computadores necessitasse somente de um notebook e uma conexão à Internet para desempenhar suas atividades, ao invés de arriscar a pele em suas aventuras tradicionais.**

Ao contrário do que se possa imaginar, promover pichação de sites ligados ao governo e obter informações inimigas estratégicas, não são os únicos tipos de ataques promovidos nas cyberwars. Obter meios para paralisar serviços de uso comum representam uma alternativa eficaz para disseminar o terror na população do país inimigo, por meio do ataque aos serviços de telecomunicações, energia, telefonia móvel, sistemas televisivos e redes de computadores. Boatos reportam que a China tem procurado meios eletrônicos para poder despejar uma verdadeira artilharia digital contra Taiwan, como forma de ter mais uma "carta na manga" para garantir maior força na frágil relação diplomática entre os dois países.

Sábios da importância do domínio do cyberespaço, os norte-americanos têm uma grande vantagem com relação a qualquer outro país: os softwares mais utilizados nos computadores pessoais do mundo inteiro são de empresas do país do Tio Sam. Como se não bastasse, sendo tais softwares proprietários e, portanto, não sendo possível qualquer acesso amplo ao código-fonte, coloca-se nas mãos dessas empresas a possibilidade de se facilitar em muito o controle sobre as tecnologias utilizadas por inimigos.

Por fim, é preciso estar atento ao fato de que a Internet e os demais recursos de tecnologia da informação representam hoje um importante espaço a ser dominado, estabelecendo-se novas fronteiras e dimensões que podem ajudar a determinar o novo cenário mundial dos próximos anos. Não se pode abrir mão desse processo, sob pena de confortar-se com o papel de país coadjuvante sujeito às pressões daqueles que têm maior representatividade e domínio.

PC

Sou consultor em informática há mais de 20 anos e leitor assíduo da revista. Ela tem ajudado bastante no meu dia a dia com muitas dicas práticas e teóricas. Agora com o lançamento da placa POST estou propenso a assinar. Ela vem com manuais e códigos de BIOS? Vou receber também os 3 livros descritos na promoção?

Antonio Leite
Mogi das Cruzes - SP

Sim, ela vem com manual de uso e uma descrição, em português, dos códigos de erros relacionados às principais revisões de BIOS disponíveis no mercado. A coleção de livros será enviada como brinde aos leitores que se "engajarem" no desenvolvimento do projeto junto conosco. Isso basicamente será feito através de testes de homologação em diferentes sistemas. Pretendemos brindar 10 assinantes a cada mês e haverá um ranking no site, como forma de fomentar o apoio e também prestar um reconhecimento aos participantes. Em breve comunicaremos isso através do link "Participe de Nosso Projeto", disponível no site **www.revistapcecia.com.br/placapost**.

Se tenho um computador com processador queimado ou provocando erros aleatórios como travamentos, essa placa POST pode me avisar através dos displays? E problemas com memórias, também são identificados pela placa?

Luciano Ribeiro Queiroz

*Sim, Luciano, assim que o micro é ligado vários circuitos do processador são inicializados (cache, por exemplo) e algumas operações são feitas, como, por exemplo, a atualização do microcódigo (uma espécie de BIOS interno do processador), ajuste de freqüência, etc. O manual mais recente da American Megatrends (***www.ami.com***), que é um dos principais desenvolvedores de BIOS, diz que o código POST neste momento é D0. Logo, se houver um problema aqui, a placa POST ficará congelada neste código.*

Em relação às memórias, a resposta também é sim, o erro pode ser "pego" porque haverá um código POST específico associado ao teste com elas. Se elas estiverem ruins, a placa POST ficará congelada no código.

Esses códigos POST estarão descritos no manual da placa POST. Mas apenas para você ter uma idéia mais detalhada dos testes que são feitos e de seus respectivos códigos, além dos sites dos desenvolvedores de BIOS (o outro é o da Phoenix-Award, **www.phoenix.com***), recomendamos uma visita ao site* **http://www.bioscentral.com/postcodes/amibios.htm**.

É possível comprar a placa POST Saber separado da assinatura? Quanto custa?

José Carlos C. Dutra

A placa POST foi desenvolvida para ser distribuída como brinde aos assinantes, dessa forma não será comercializada de forma avulsa.

Tenho uma empresa de assistência técnica para computadores e gostaria de obter mais informações sobre a placa POST Saber.

Paulo Roberto
RG Informática
São Paulo - SP

A placa POST se destina à manutenção de computadores. Através dos códigos exibidos em seus 2 displays é possível diagnosticar problemas com o processador, memória e chips diversos de placa-mãe que podem impedir o computador de realizar o boot, ou seja, carregar o sistema operacional. Com isso, permite que ganhemos tempo na manutenção e ainda evita que os problemas sejam analisados através de "achismos" e outras práticas como o troca-troca de peças, que também pode levar a queima de peças.

Para maiores detalhes do funcionamento da placa (é possível inclusive ver um vídeo), acesse o site **www.revistapcecia.com.br/placapost**.

A edição 75 apresentou testes com várias placas POST. Gostaria de saber qual modelo vocês recomendam, haja vista o fato de nenhuma ter o funcionamento 100% garantido, devido aos motivos apresentados na reportagem. Fico no aguardo de uma resposta, porque eu já tive problemas com o display de uma placa de um determinado fabricante.

Ney Penalva
Técnico de rede - SIMM
Salvador - BA

Em relação à qualidade e atualização do projeto eletrônico, as placas QuickPOST e Saber são superiores. Somado às funcionalidades, não resta dúvidas de que a QuickPOST é a melhor opção. A única dúvida em relação a ela diz respeito ao suporte técnico oferecido pelo fabricante. Com a Saber, a vantagem é o fato de ser um projeto nacional e contar com uma equipe local para atender os clientes - que nesse caso são os leitores da PC&CIA.

Emuladores de CPU

Gostaria de saber onde posso comprar os emuladores de CPU apresentados na matéria "Manutenção em placas-mãe", da edição 75.

Francisco Gonçalves Pinto
Técnico em Eletrônica
Ceilândia - DF

Infelizmente não é possível encontrá-los para comprar aqui no Brasil. Tentaremos encontrá-los no exterior, ou então apresentar nas próximas edições um circuito para que os leitores possam montar seus próprios emuladores.

Overclock

Em relação à matéria "Memórias de Alta Performance e Overclock do Core 2 Duo", publicado na edição 73, gostaria de confirmar se foi mantido o cooler original do E4300 para a realização do overclock de 800 para 1400 MHz no FSB?

Wagner J de Almeida Nogueira
Técnico em Eletrônica
Cabo Frio - RJ

O cooler usado foi o demonstrado na foto de entrada da matéria, um Hyper 6+ da Cooler Master. O cooler original, in-a-box, não é adequado para esse overclock porque não é capaz de fazer com que o processador opere sem atividade de Throttling.

Colaboraram

WAZ Hardware Store (**www.waz.com.br**)
Módulo de memória Corsair DDR3

Erramos

PC&CIA 75 – Matéria Manutenção de PCs, pg. 16
O chip Analog Devices ADM9249, utilizado como conversor analógico-digital da placa Quick POST Serial, da Ultra-X, opera com resolução de 9 bits e não 12 bits, conforme publicado.

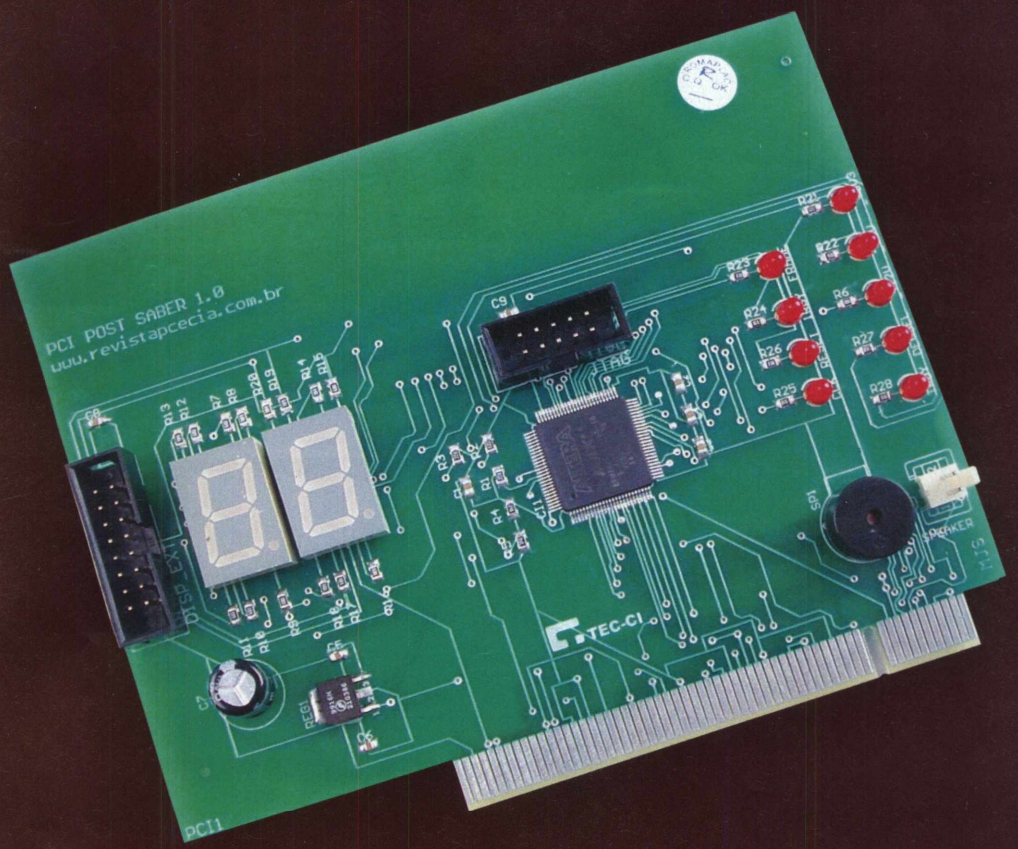
@ Vez do leitor

Comentários, críticas e sugestões:
E-mail: a.leitor.pcecia@editorasaber.com.br
Cartas: R. Jacinto José de Araújo, 315



O PC PAROU? E VOCÊ PRECISA NORMALIZÁ-LO RAPIDAMENTE?

PC &CIA



POST SABER

A 1ª DESENVOLVIDA NO BRASIL E COM SUPORTE LOCAL

A ÚNICA REVISTA BRASILEIRA CAPACITADA TECNICAMENTE PARA AJUDAR VOCÊ, PROJETOU UMA PLACA POST EXCLUSIVA PARA SEUS LEITORES

http://www.revistapcecia.com.br/placapost

Super Máquina Desktop para 2008

A Intel tem um novo processador chegando, mas desta vez direcionado exclusivamente para a plataforma Skulltrail, que estará disponível no primeiro trimestre de 2008. Esta plataforma é baseada no chipset de codinome Seaburg, o qual lembra muito o Stoakley para estações de trabalho de alta performance com dois processadores. Mas além do barramento de 1600MHz e dos 128GB PC2-6400 (800MHz) FB-DIMM de memória, a Skulltrail também oferece quatro slots PCI Express 16X. A Intel pretende "animar" esta plataforma com versões especiais do Intel Core 2 Extreme socket LGA 775. O primeiro chip desta plataforma será o Intel Core 2 Extreme QX9775, com clock de 3,2GHz, gravado em 45nm, multiplicador destravado e consumo de 150W.

Considerando que apenas um processador QX9775 custará 1500 dólares, não é difícil imaginar que um computador baseado nesta plataforma chegue ao consumidor facilmente com valores próximos a 10.000 dólares e 1000W de dissipação de potência.

No mais, sabendo que as CPUs ultra high end para computadores desktop normalmente não vendem muito, podemos imaginar que a Intel provavelmente deseja roubar a atenção do público antes do lançamento dos processadores Phenom.



Placa-mãe para plataforma dual-socket Skulltrail e sistema montado com 2 QX9775 de 3,4 GHz e 2 8800GTX, exposto durante o último IDF: nada menos que 17038 pontos no 3DMark2006! E com possibilidade para mais duas placas de vídeo high-end no futuro para ter "a" super-máquina.

Adobe transformará seus aplicativos em serviços on line

Os aplicativos transformados em serviços são o sonho da Microsoft, mas outras companhias estão trabalhando para que isso vire uma realidade muito mais rapidamente. A Adobe, por exemplo, está preparando a transição de toda sua companhia para um serviço on line, e esta migração estará finalizada na próxima década.

Na convenção Web 2.0, um executivo da Adobe disse que diante da contínua evolução da Internet, ela se transformará numa solução excelente para a distribuição de aplicativos e que o futuro do Office, comparativamente, será "limitado". Enquanto existem pessoas que encontram dificuldade para justificar o pagamento mensal pelo uso de um aplicativo, existem outras que defendem estas vantagens. Por exemplo: uma pequena assinatura mensal garantirá ao usuário o acesso à última versão do programa sem obrigá-lo a pagar por novas versões" (como ocorre com o MS Office).

Photoshop on line? Dreamweaver on line? Este é o objetivo da companhia, e esta transição de aplicativos para um ambiente on line poderá acontecer antes do que muita gente acredita.

Phenom: detalhes oficiais

A AMD revelou um roadmap contendo as datas de lançamento, as freqüências de operação e os modelos da primeira geração de processadores Quad-core da companhia, Phenom, destinados ao mercado dos desktops.

Ainda neste mês, estarão disponíveis os Phenom 9500 e 9600 com freqüências entre 2.2GHz e 2.4GHz. Eles serão os modelos de entrada de linha da nova geração de quatro núcleos da companhia. O modelo intermediário, Phenom 9700, com clock de 2.6GHz, chegaria um mês depois para o socket AM2+.

O topo da linha será ocupado pelos Agena FX-82, que estarão disponíveis no primeiro trimestre do novo ano com freqüências variando entre 2.6 a 3.0GHz.

Um pouco mais tarde, já no segundo trimestre, a companhia confirmou o aumento da freqüência de operação dos modelos Phenom 9 e Phenom FX.

Não foram liberadas informações sobre o Toliman 3X, o processador triple-core da companhia, que foi confirmado pela AMD e que se posicionaria no preço e na performance entre os modelos Dual e Quad-core. A princípio, eles chegariam no primeiro semestre de 2008.

NVIDIA apresenta o GeForce 8800 GT

A NVIDIA escolheu o dia 29 de outubro para anunciar a disponibilidade de seu novo GPU (processador gráfico), o GeForce 8800 GT. Ele é oriundo da família 8800 e em termos de performance se posiciona entre o 8800 GTS e o 8800 GTX, com custo mais acessível. Custando entre 199 e 259 dólares, o GeForce 8800 GT possui 112 stream processors e barramento de memória de 256 bits (até 512 MB podem ser utilizados).

Ele também traz uma nova versão da tecnologia PureVideo, destinada a melhorar ainda mais a performance do vídeo de alta definição (HD – High Definition). Diante da chegada de vários jogos nos próximos dias, o anúncio desta nova GeForce é bem-vindo para as pessoas que desejam se beneficiar de uma performance superior por um preço mais razoável. Estas placas deverão ser disponibilizadas em breve pelos parceiros da NVIDIA.

Preço do Celeron Dual Core

Se atualmente um processador Dual-Core pode ser encontrado mais facilmente, principalmente no que diz respeito à sua acessibilidade, no início do próximo ano isso será ainda mais fácil. Isso porque a Intel lançará os processadores Celeron de dois núcleos voltados para o mercado de computadores mais baratos.

O primeiro Celeron Dual Core sairá no primeiro trimestre de 2008. O Celeron E1200, o primeiro da linha, com freqüência de 1,6GHz e um FSB de 800MHz, será integrado por 512KB de memória cache L2 comprtilhados. Este modelo, gravado em 65nm, vai explorar o socket 775 e terá um TDP (perfil de potência) de 65 watts. Ele será comercializado por 53 dólares, um preço relativamente baixo, pois os modelos Pentium E2140 e E2160 com 1MB de memória cache L2 são vendidos atualmente por 64 e 74 dólares, respectivamente.

A Intel também deverá lançar um Core 2 Duo E4700 com freqüência de 2.6GHz, FSB de 800MHz e 2MB de memória cache L2 pelo preço de 133 dólares. O Core 2 Duo da série 4000 "Penryn", gravado em 45nm, também deverá ver a luz do dia em breve. Estes processadores terão 3MB de memória cache L2 e um FSB de 1066MHz.

As novas placas gráficas Matrox

A Matrox não morreu, não mesmo! O fabricante continua oferecendo novos produtos e na semana passada apresentou a nova linha de placas gráficas Millenium P690. Não são placas "forjadas" para operações 3D, na verdade elas tiram proveito de um bom suporte 2D. O fabricante apresentou suas placas gráficas nas versões PCI Express 16X, 4X, 1X e até mesmo PCI. Elas são integradas por chips de memórias GDDR2 e não consomem mais do que 12W em funcionamento. Seguem os modelos e seus respectivos preços:

- P690 PCIe 16x 128MB : 200 dólares
- P690 PCI 128MB : 200 dólares
- P690 LP PCIe 16x 128MB : 250 dólares
- P690 LP PCIe 1x 128MB : 250 dólares
- P690 Plus LP PCIe 16x 256MB : 290 dólares
- P690 Plus LP PCI 256MB : 290 dólares
- Quad-monitor upgrade cable (CAB-L60-4XAF) : 100 dólares

A Matrox também é especializada no gerenciamento de vários monitores. Desta forma é possível conectar até oito monitores utilizando duas placas gráficas P690 Plus.

O 780G da AMD em janeiro

Segundo algumas fontes, a AMD está preparando o lançamento de novos chipsets com vídeo integrado (IGP), dentre eles um DirectX 10 para o próximo mês de janeiro.

Ainda segundo estas fontes, eles serão batizados de 740G e 780G e diferentes setores do mercado estão sendo visados. O 780G interessa ao segmento high end, com Hypertransport 3.0, PCI Express 2.0, um núcleo gráfico IGP DX10 e com suporte ao Crossfire híbrido. Este se refere à capacidade de associar o vídeo integrado ao de uma placa PCI-E para aumentar a potência da renderização 3D.

Os fabricantes também poderão acrescentar ao 780G um DisplayPort. O 740G será mais modesto, com o seu IGP DX9 e interface padrão PCI Express.

Qual será o primeiro IGP DX10 no mercado? No entanto, a questão aqui é bem diferente: qual a importância disso? Pois já se sabe que muito dificilmente algum processador gráfico integrado, seja ele AMD, NVIDIA ou Intel, será capaz de rodar os efeitos DX10 com uma taxa de frames por segundo decente.

No mais, será que com o Crossfire híbrido os IGPs se transformarão no chip preferido dos jogadores?

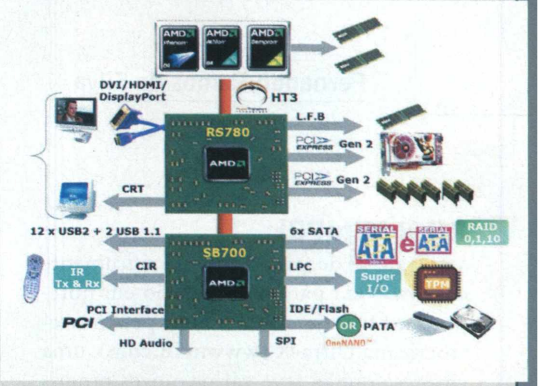
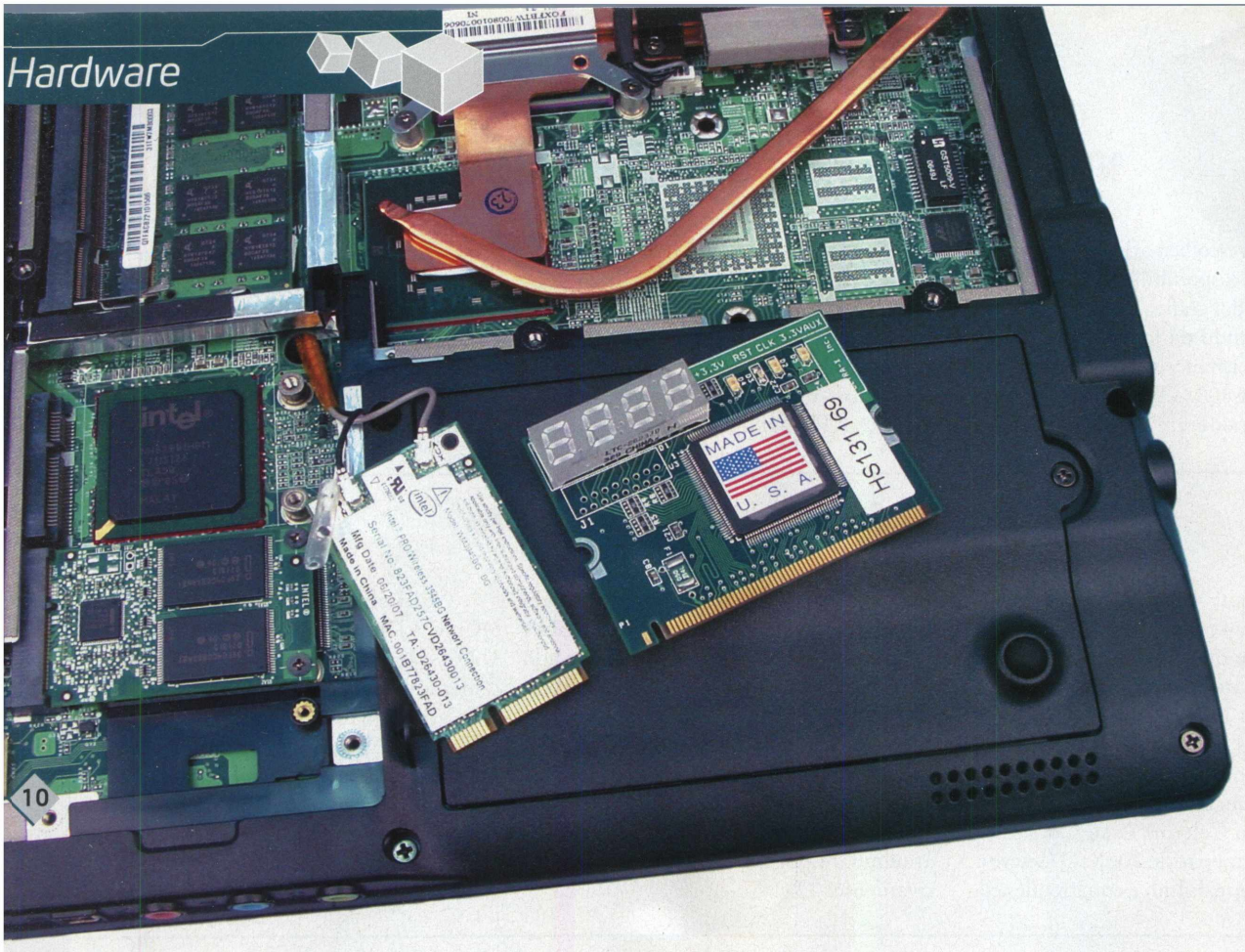


Diagrama de blocos do novo chipset 780G da AMD.



Manutenção de Notebooks

Com os preços em queda livre, uma diversidade de modelos cada vez maior e o onipresente desejo por computação portátil, os notebooks estão caindo na graça do consumidor brasileiro. Será que em breve eles também substituirão os desktops no número de chamados para manutenção? Conheça desde já uma ferramenta que pode auxiliá-lo.

Fernando Ramos da Silva

P.H.D MiniPCI

Trata-se de uma placa especificamente desenvolvida para manutenção em notebooks. O projeto é assinado pela norte-americana Ultra-X (**www.uxd.com**), uma empresa que já teve vários outros produtos avaliados por nossa equipe, a exemplo da P.H.D PCI, destinada aos desktops (PC&CIA 45).

Tal como a P.H.D PCI, a MiniPCI também é considerada uma placa de testes, pois possui circuitos eletrônicos capazes de assumir o controle do notebook mesmo que não haja um sistema operacional instalado. Isso é feito através de seu chip principal, sob a bandeira dos U.S.A, onde estão as instruções que programam o controlador PCI do chipset para entregar o boot à placa MiniPCI, assim que o POST (Power On Self Test – auto teste de inicialização) é finalizado (figura 1).

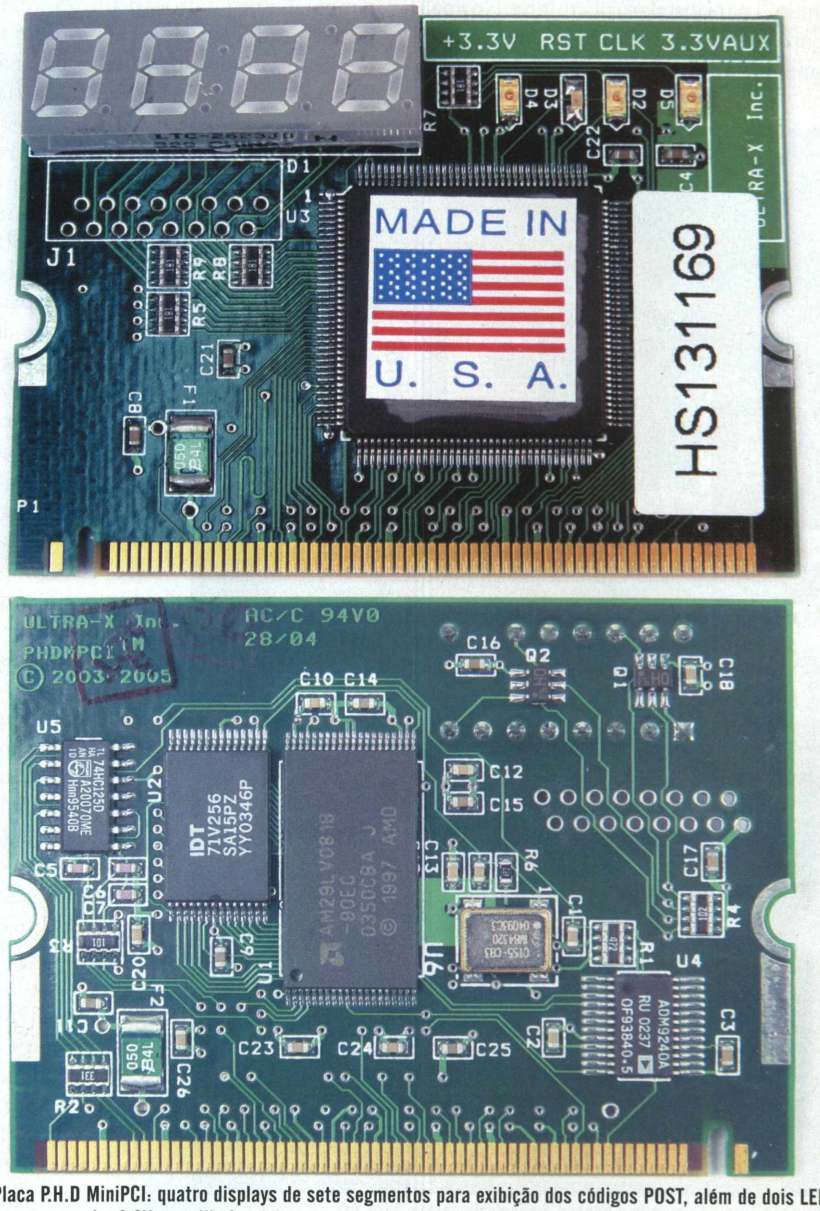
Quer dizer que a placa possui seu próprio sistema operacional? Exatamente, o qual fica armazenado em um chip de memória FlashROM, da AMD, localizado na face traseira da placa (figura 2).

Uma diferença fundamental entre a PCI e a MiniPCI é que a segunda possui um projeto eletrônico mais simples e conseqüentemente não é capaz de suplantar a ausência ou defeito de alguns componentes da máquina, tais como a placa de vídeo, o BIOS e a memória RAM. No caso da PCI, ela possui todos esses componentes na própria placa e, portanto, pode seguir em frente no diagnóstico, carregando o seu software de controle, mesmo que a placa-mãe do PC esteja sem memória, por exemplo.

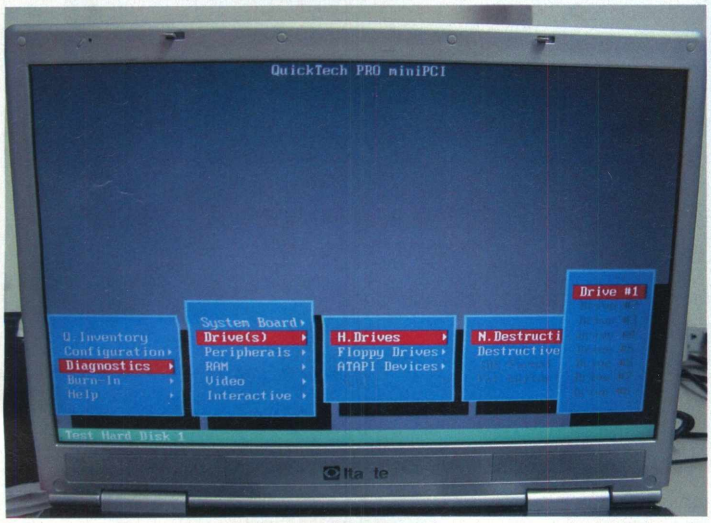
Isso não significa que a MiniPCI fique inútil neste caso, já que os defeitos com memória, processador e algum circuito controlador integrado no chipset podem ser diagnosticados através dos códigos POST exibidos em seus displays. Ou seja, até a carga de seu software de controle, a MiniPCI atua como uma legítima placa POST. Sua lógica foi programada para "ouvir" os códigos que o BIOS envia para os endereços de I/O (entrada/saída) 80 e 81h (o "h" vem do sistema de numeração hexadecimal) durante o POST. Se algum defeito acontecer neste momento, os displays reportarão o código de erro. Bastaria consultar o manual dos códigos POST para encontrar o componente defeituoso.

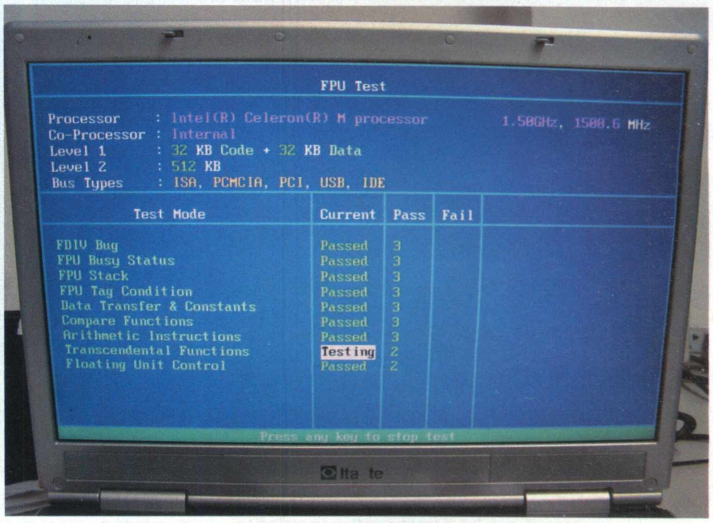
Testes

A instalação é muito simples. Após desconectar a alimentação elétrica, inclusive a bateria, basta remover uma das tampas da traseira do equipamento e encontrar um slot



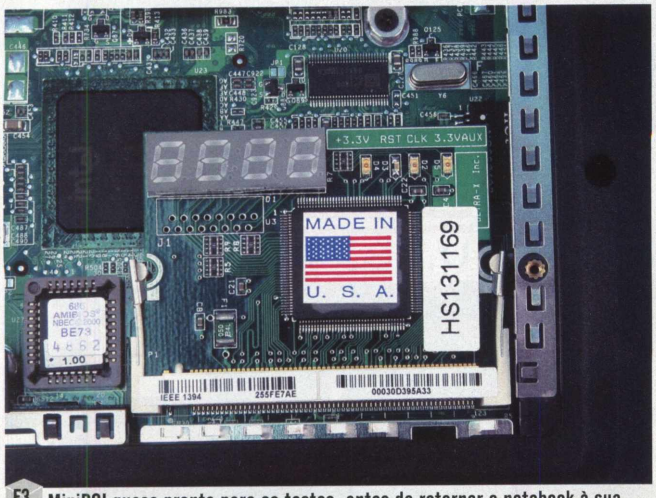
F1. Placa P.H.D MiniPCI: quatro displays de sete segmentos para exibição dos códigos POST, além de dois LEDs para tensão (+3,3V e auxiliar) e dois para sinais de clock e reset.





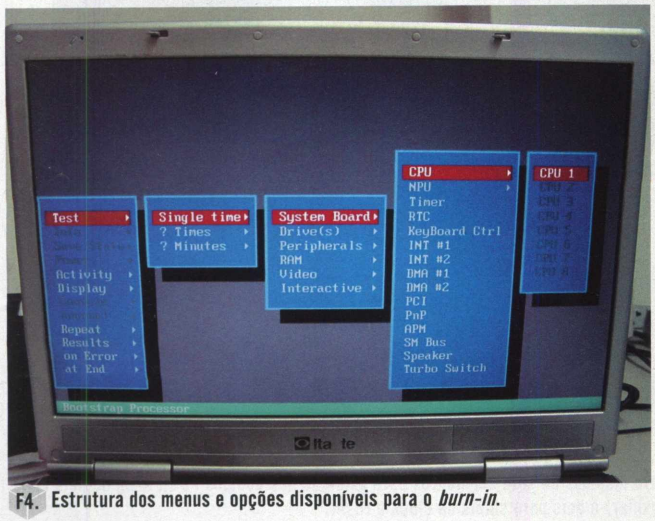
F2. Estrutura de menus do software de controle da placa P.H.D MiniPCI e página para a execução de testes no

MiniPCI para instalar a plaquinha. Normalmente esse slot fica próximo aos soquetes de memória. Se ele estiver ocupado, remova temporariamente a placa periférica, a exemplo do adaptador wireless presente no notebook utilizado em nossos testes, um Infoway W7620, da Itautec (figura 3).



F3. MiniPCI quase pronta para os testes: antes de retornar o notebook à sua posição normal, verifique se os displays não ficarão para fora em relação à base do equipamento, o que certamente danificaria a placa e/ou o slot na placa-mãe.

Se tudo correr bem durante o POST, alguns segundos após o software de controle da MiniPCI aparecerá na tela, indo diretamente à execução de um script de *burn-in* (estresse) configurado por padrão. Para impedir, basta pressionar qualquer tecla na inicialização, ou mesmo ESC durante o estresse. Além disso, vale destacar que o usuário também pode criar seu próprio teste de estresse, definindo os componentes a serem avaliados, a duração, qual ação tomar na presença de falha e o que fazer ao final do processo. É uma ótima solução para atestar o funcionamento de uma máquina nova, ou então que acabou de passar por uma manutenção (figura 4). Em um mercado tão depreciado como o nosso, imagine só como não ficaria positiva sua imagem diante do cliente, no momento em que ele recebesse a máquina e um extenso relatório dos testes executados!?

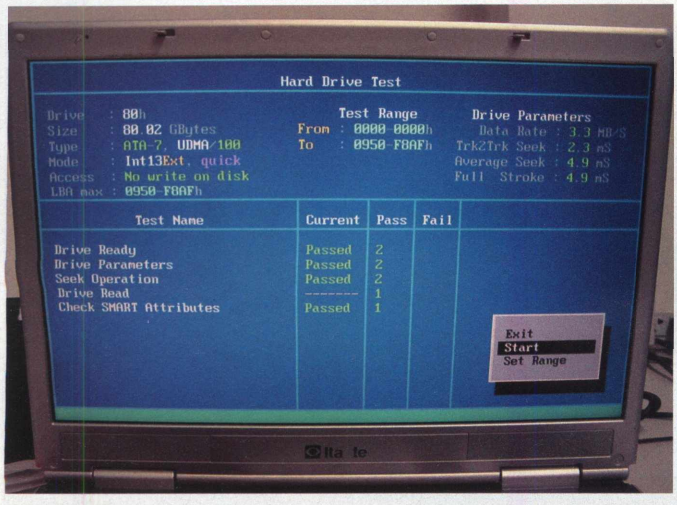


F4. Estrutura dos menus e opções disponíveis para o *burn-in*.

Por falar em testes, o menu "Diagnostics" nos conduz a uma grande quantidade de testes. A figura 2 já nos deu uma prévia dos testes que podem ser feitos de modo individualizado com vários circuitos existentes dentro de um processador. Mas é bom frisar também a possibilidade de se avaliar desde os circuitos mais básicos de toda placa-mãe, como controlador de interrupções e DMA (acesso direto à memória), até os componentes digamos mais visíveis ao usuário, como HD, memória, placa de vídeo, monitor, teclado e até as portas de I/O, como serial, paralela, rede, som e USB (figura 5).

Aliás, o kit da placa é fornecido por padrão com os conectores de *loopback* para as três primeiras interfaces citadas há pouco, além de um CD e um DVD gravados com um perfil de teste para exercitar o drive óptico (figura 6).

Nos demais itens de menu, "Q Inventory" e "Configuration", são exibidas informações sobre a configuração de hardware instalada e os recursos alocados para cada componente. Podemos ver ainda todos os detalhes da temporização e especificações dos chips de memória, uma vez que a MiniPCI lê o chip EEPROM SPD existente em cada módulo. A "saúde" do HD também pode ser verificada a partir da leitura dos valores do SMART. Por último, vale destacar a presença de um monitor de tensões e temperatura da placa (figura 7). O controle neste caso é feito por um chip conversor A/D (analógico/digital) ADM9240A, da Analog Devices, que opera com resolução





F5. Páginas de testes com HD e memória: independência de sistema operacional e algoritmos exclusivos para estresse são diferenciais frente a softwares gratuitos que se propõem a fazer o mesmo.

de 9 bits e está instalado na face de trás da placa MiniPCI.

Limitações

A principal limitação é física, justamente relacionada à instalação da placa. Primeiro, é importante considerar que nem sempre o slot MiniPCI estará tão acessível, principalmente nos notebooks menores, com monitor de 12", por exemplo. Isso significa que pode ser necessário desmontá-lo quase que completamente para instalar a MiniPCI, o que evidentemente pressupõe uma certa habilidade extra do técnico e requer um apoio do fabricante/distribuidor no sentido de disponibilizar os manuais e/ou vídeos de desmontagem.

Depois disso, vem a questão mais séria com a transição das plataformas de hardware dos notebooks para o barramento PCI-Express. Não conseguimos instalar a MiniPCI em alguns outros notebooks que tínhamos à disposição no laboratório, porque todos eles (dois Intel da geração Santa Rosa e um AMD com soquete S1) dispunham apenas de slots Mini PCI Express (figura 8).

Conclusão

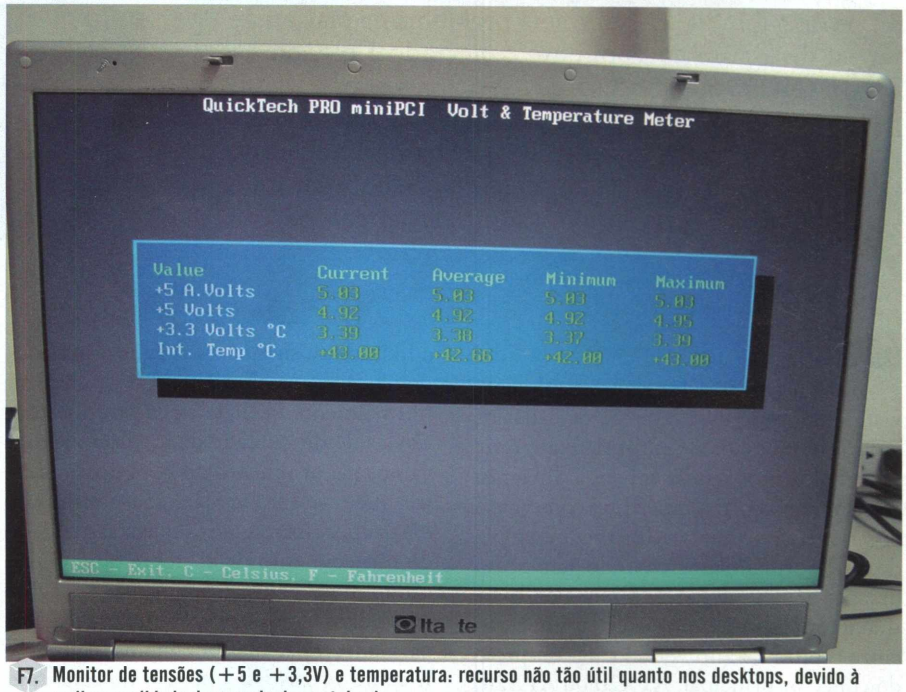
Gostamos do que vimos em relação ao teste da P.H.D MiniPCI, sobretudo por saber que o mesmo nível de sofisticação disponível para a manutenção de desktops também pode ser encontrado para o emergente mercado que se aproxima com os notebooks. A apresentação do kit é sóbria, o projeto eletrônico inspira confiança e os recursos do software são de encher os olhos.

É inevitável concluir que, na pior das hipóteses, o kit servirá como um elemento de diferenciação e profissionalismo para o técnico, que pode se destacar junto a um mercado que não está habituado a olhar tanto para preço. Em resumo, é um investimento que seguramente retornará, embora possa demorar um pouco, já que o kit possui um custo elevado (cotado a R$ 4320,00 em **www.uxdiag.com.br**). Só não se esqueça da incompatibilidade física da placa com a nova geração de notebooks.

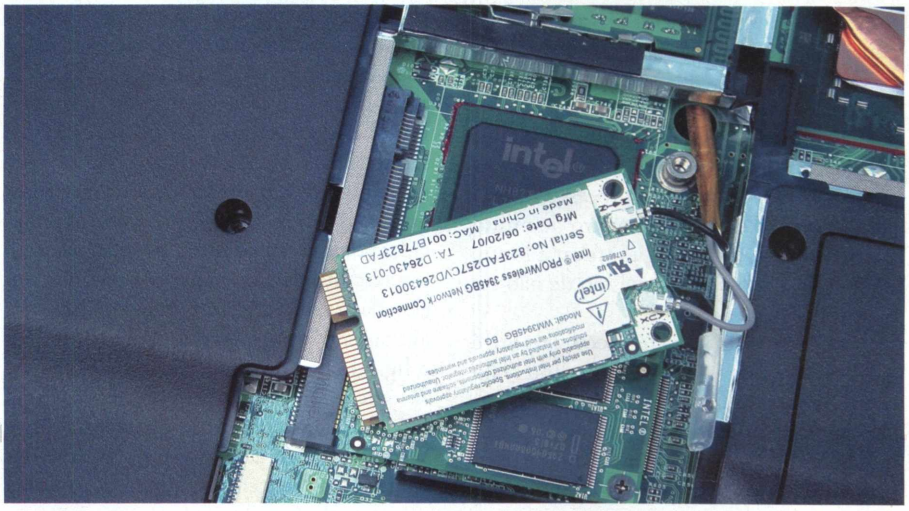
PC



F6. Kit enviado com a MiniPCI: só a maleta já é de fazer inveja!



F7. Monitor de tensões (+5 e +3,3V) e temperatura: recurso não tão útil quanto nos desktops, devido à melhor qualidade da energia dos notebooks.



F8. Placas PCI Express Mini possuem conector com apenas 52 pinos: ganha-se com o menor tamanho e também com a maior performance em relação ao PCI.

Testadores de Fontes ATX

Ontem você desligou a máquina normalmente, mas hoje ela se recusa a ligar. A ventoinha do cooler do processador sequer gira e o mesmo acontece com as do gabinete. E agora, será problema da placa-mãe ou de algum componente conectado a ela, ou da fonte ATX? Já estão disponíveis no mercado há algum tempo alguns modelos de testadores de fontes que se propõem justamente a avaliar a responsabilidade da fonte neste defeito. Resta saber se eles cumprem o que prometem, e este será o assunto desta matéria.



Fernando Ramos

Os mitos

Se há uma classe de assunto geralmente vista como enigmática entre os usuários e mesmo técnicos de informática é o de energia. Muitos sequer sabem a diferença entre tensão e corrente elétrica e começam a disseminar vários mitos na Internet, a exemplo do teste normalmente realizado para o caso descrito acima. "É fácil", dizem eles, basta tirar a fonte da máquina e fechar um curto entre o pino 14 (fio verde) e algum preto do conector principal, ATX20 ou ATX24, e ver o que acontece. Se a ventoinha da fonte virar, é problema da placa-mãe; caso contrário, é só trocar a fonte.

Mal sabem eles que ao fazer esse teste a fonte pode inclusive queimar ou, na melhor das hipóteses, enganá-lo de tal forma no diagnóstico que ele ficará trocando peças aleatoriamente (placa-mãe, processador, etc) para só depois de um dia inteiro de muito suor resolver o problema ao trocar a fonte. E isso por uma simples questão de não ter mais o que fazer.

O primeiro aspecto técnico relevante é que a presença de tensão nos conectores não significa que uma fonte está funcionando normalmente. Significa apenas que ela possui um dos componentes necessários para a realização de trabalho. Comparando com a hidráulica, significaria a água armazenada na caixa. A outra é a corrente elétrica, normalmente negligenciada por questões óbvias de dificuldade de medição. Agora vamos supor um defeito com um capacitor que teve sua capacitância diminuída. Na prática, isso significa que a capacidade de fornecimento de corrente do circuito diminuirá e, conseqüentemente, a máquina poderá ligar normalmente, mas assim permanecerá apenas por alguns segundos. É como se existisse um furo no cano que liga a saída do registro da caixa d'água aos pontos de distribuição na casa.

A fonte só funciona com o curto citado acima, porque simplesmente não há carga alguma em suas saídas "puxando" corrente. Na verdade, contudo, as melhores fontes sequer ligam nessa condição. Isso se deve ao princípio de operação de todas as fontes utilizadas em computadores, também conhecidas por fontes chaveadas, por empregarem um circuito de chaveamento operando em elevadas freqüências e com realimentação para ajustarem a largura dos pulsos que controlam o liga/desliga dos transistores MOSFETs. A lógica é simples: a fim de manter uma elevada eficiência no uso da energia que é consumida da rede AC, as fontes chaveadas só entregam a potência realmente requerida pela carga, que no nosso caso é representada por cada um dos componentes instalados no micro.

Caso não exista carga, como é que elas ajustam a largura dos pulsos, ou melhor, regulam cada uma das tensões de saída? É simples: algumas ligam, porém as tensões ficam totalmente desreguladas, outras queimam porque perdem totalmente o controle, e a classe das melhores detecta essa condição de carga mínima não atendida e simplesmente não ligam.

Em relação à carga mínima requerida por cada fonte, existe uma regra geral especificada pelo padrão ATX. A figura 1 abaixo foi retirada da página 19 do documento disponível para download no site **http://www.formfactors.org/developer%5Cspecs%5CATX12V_PSDG_2_2_public_br2.pdf**. Refere-se a uma distribuição típica de corrente para uma fonte de 450W, mas o que nos interessa aqui é a coluna Min. Current (amps - Corrente Mínima em ampères). Veja que é necessário garantir um consumo de pelo menos 1A nas linhas de alimentação 12V1 (tensão de 12V no conector ATX principal) e 12V2 (tensão de 12V no conector ATX12V usado para a alimentação do processador), além de 0,3A na linha de +5V e 0,5A na de +3,3V.

ATX12V Power Supply Design Guide
Version 2.2

Table 7. Typical Power Distribution for a 450 W ATX12V Configuration

Output	Min. Current (amps)	Max. Current (amps)	Peak Current (amps)
+12 V1DC[1]	1	14	15
+12 V2DC[1, 2]	1	16	19
+5 VDC	0.3	15	
+3.3 VDC	0.5	22	
-12 VDC	0	0.3	
+5 VSB	0	2.5	3.5

Note: Total combined output of 3.3 V and 5 V is ≤ 130 W
Peak currents may last up to 17 seconds with not more than one occurrence per minute
[1] 12V1DC and 12V2DC should have separate current limit circuits to meet 240VA safety requirements
[2] 12V2DC supports processor power requirements and must have a separate current limit and provide19A peak current for 10 ms; minimum voltage during peak is > 11.0 VDC

F1. Correntes sugeridas pelo padrão ATX para uma fonte de 450W.

OUTPUT							
Output Voltage	+3.3V	+5V	+12V1	+12V2	+12V3	-12V	+5Vsb
Max. Load	22A	14A	16A	16A	16A	0.8A	2.5A
Min. Load	0.5A	0.3A	1A	1A	1A	0A	0A
Regulation	3%	3%	3%	3%	3%	6%	3%
Ripple & Noise(mV)	50	50	120	120	120	120	50
Available Power	72.6W	70W	384W			9.6W	12.5W
Total Power	430W continuous output @ 50C ambient temperature						

F2. Especificação de funcionamento da Antec NeoHE 430 (tirada do site www.antec.com/specs/NeoHE430_spe.html): segue na íntegra a recomendação do padrão ATX.





F3. Testador de fonte PC/SPS Tester: dispositivo emite um alerta sonoro quando ligamos e também quando desligamos a fonte.

Vale destacar que a figura 1 funciona apenas no plano das recomendações. Cada fabricante faz o que bem entende de seu produto, de modo que a prática recomendada sob o nosso ponto de vista, como usuário, é checar as especificações no manual da fonte que tivermos em mãos. Na figura 2 visualizamos o que diz um fabricante exemplar neste sentido, a Antec, para a sua fonte NeoHE de 430W.

Antes de continuarmos, vale comentar um caso interessante de "defeito" que você poderá encontrar com fontes sérias. Você acaba de montar uma máquina, a fonte é de ótima qualidade, mas o sistema não liga. Pasme, mas o defeito pode ser do BIOS da placa-mãe. Ocorre que, se as rotinas de software do BIOS contiverem um certo tempo de espera para inicializar o processador, a fonte não ligará porque não haverá uma corrente mínima na linha de +12V. É verdade que os HDs também consomem energia da linha de +12V, mas eles naturalmente demoram um pouco para serem inicializados. E se a placa-mãe estiver com vídeo integrado, pronto, temos um cenário "perfeito" para a máquina não ligar. Algumas ventoinhas de gabinete podem facilmente solucionar esse impasse, pois também consomem da linha de +12V. E a solução definitiva viria com uma atualização de BIOS.

Os testadores

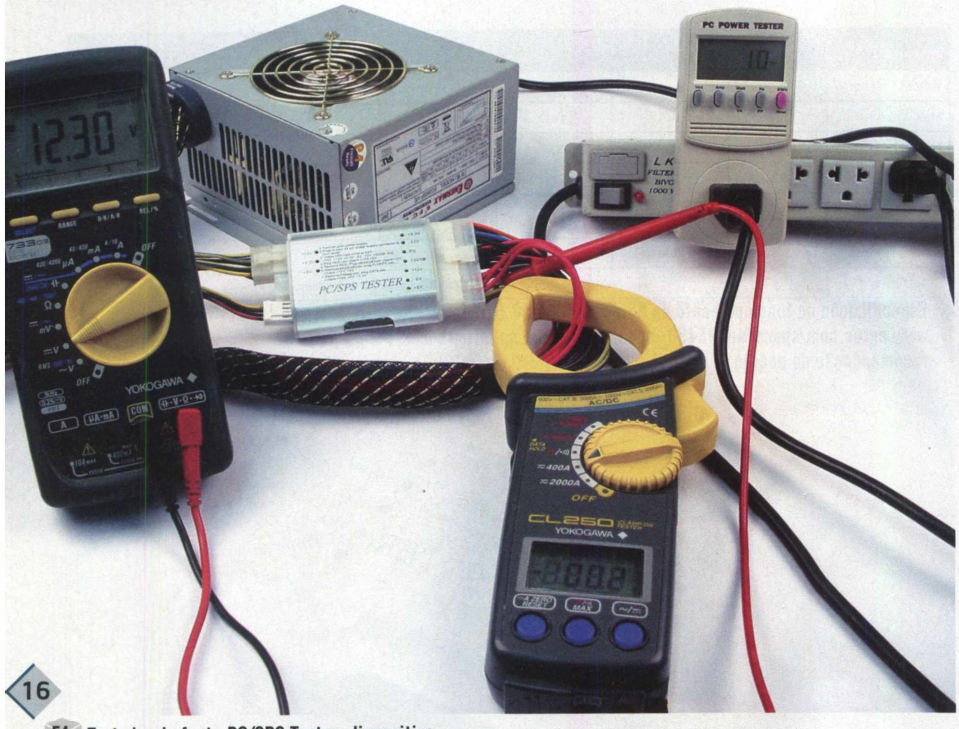
Agora que conhecemos o mínimo sobre o funcionamento das fontes, fica fácil entender a função dos testadores portáteis de fonte, como os que avaliaremos aqui. Ao contrário do que podíamos imaginar inicialmente, a função não é homologar a fonte em relação à sua potência nominal total. Ou seja, não avaliamos se a fonte é capaz ou não de fornecer os 600W declarados na etiqueta. Para realizar essa função, os testadores teriam de ser muito maiores, óbvio.

O objetivo é certificar-se de que a fonte não possui qualquer parcela de culpa com o fato da máquina não estar ligando. Como tal, ela deva possuir internamente um conjunto de resistores compatível com a carga mínima especificada pelo fabricante da fonte, e também ser dimensionada fisicamente para suportar essa operação por pelo menos um minuto. Devido ao calor gerado, há um risco real de incêndio se o dimensionamento do gabinete não for bem feito. Aliás, os testadores trazem uma advertência em relação a isso. Portanto, nada de deixá-lo ligado continuamente.

O primeiro testador avaliado foi o PC/SPS Tester (figura 3), disponível no site **www.uxdiag.com.br** por R$ 85 quando do fechamento da edição. A apresentação é impecável, repare que os conectores foram injetados em moldes especificamente construídos para o formato do gabinete de alumínio. De um lado há o conector ATX24 e um conjunto de LEDs que simboliza a presença de tensão em cada uma das linhas.

Os resistores internos do testador são alimentados por esse conector. Do outro lado, há um ATX12V de oito pinos normalmente usado para processador, um de seis pinos de placas PCI-E e um de floppy. E no rasgo da parte inferior do gabinete, há um conector Molex típico de HDs IDE. Esses quatro últimos conectores nada contribuem para o consumo de energia do testador. Ou seja, estejam eles conectados ou não, o consumo do testador será feito a partir do ATX principal. Na verdade, através dos três LEDs do lado esquerdo do testador é possível apenas certificar-se de que não há um problema com esses conectores, como fio solto, solda mal feita dentro da fonte, etc.

Durante o teste, bastou ligá-lo e observar seu primeiro minuto de funcionamento para perceber que havia algo de errado. Afinal, o aquecimento era muito pequeno, não fazia jus à carga mínima especificada pelo padrão

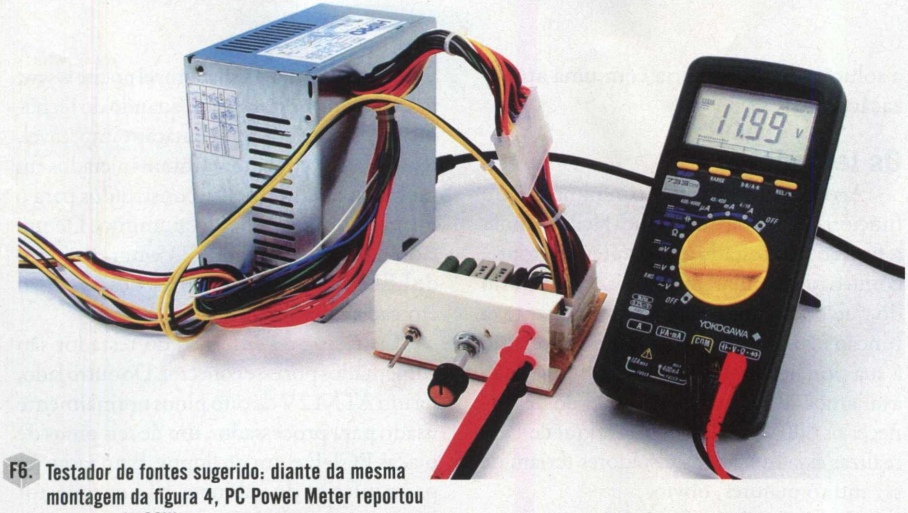


F4. Testador de fonte PC/SPS Tester: dispositivo emite um alerta sonoro quando ligamos e também quando desligamos a fonte.





F5. Thermaltake Dr. Power: conjunto de conectores mais antigo, limitado ao ATX24, Molex de HD e floppy, além de um ATX12V de quatro pinos. Cotado a R$ 70, em média, também emite beeps durante liga/desliga da fonte.



F6. Testador de fontes sugerido: diante da mesma montagem da figura 4, PC Power Meter reportou consumo de 60W.

ATX. Desta forma, decidimos fazer a montagem da figura 4.

Enquanto o alicate amperímetro e o multímetro eram utilizados em paralelo para medir a corrente e a tensão em cada uma das linhas de alimentação, o PC Power Tester ficava "atrás" da fonte medindo o consumo de energia total. Este, aliás, foi de apenas 10W durante o teste de uma fonte Enermax EG565P-VE de 535W. A corrente nas linhas oscilava entre 0,1 e 0,2A apenas.

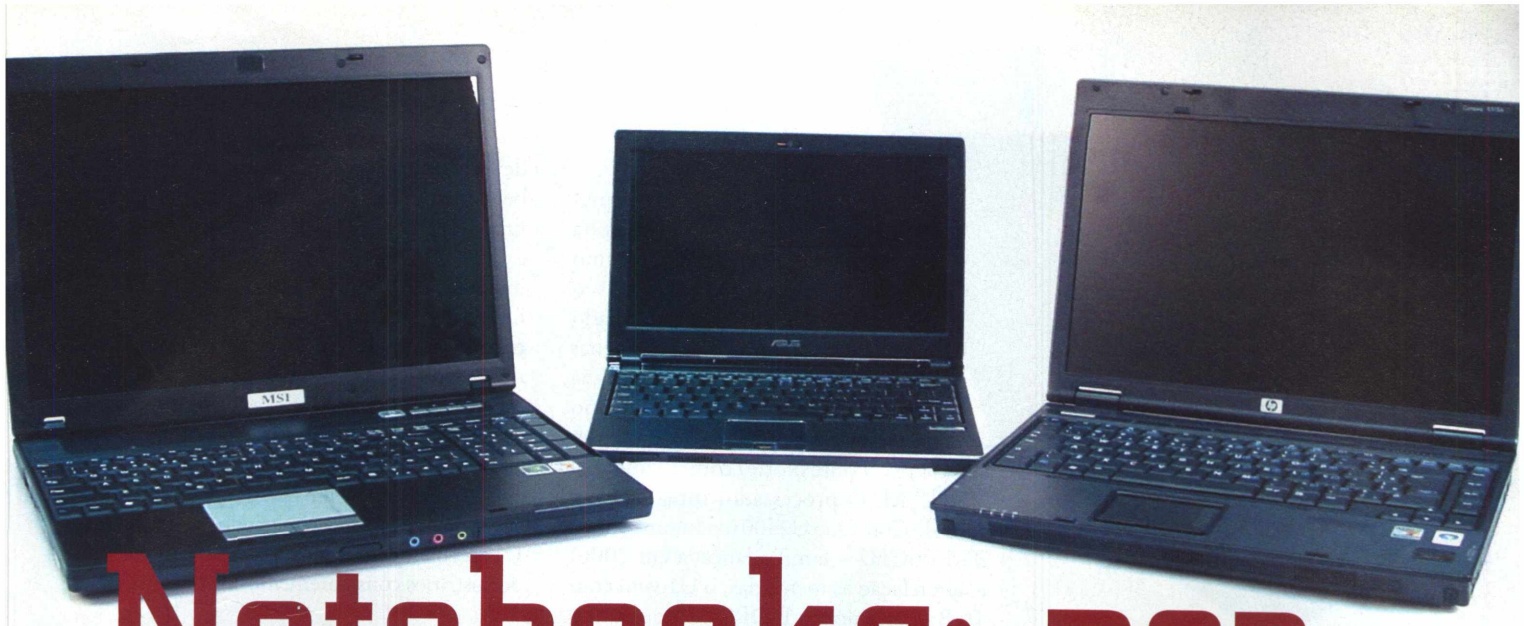
Em outro teste, agora com uma fonte Corsair VX550W, vimos na prática a teoria abordada nesta matéria. Ou seja, diante de um consumo tão baixo, a fonte liga, porém permanece ligada somente por alguns segundos até se desligar sozinha.

Depois disso, partimos para o teste do Thermaltake Dr. Power. Seu gabinete de plástico faz com que ele esquente sensivelmente mais do que o testador anterior (figura 5). Entretanto não é muito mais, até porque seu consumo de energia só é ligeiramente superior (14W). Contudo, foi o suficiente para a fonte da Corsair não desligar sozinha.

Conclusão

Quando o assunto é manutenção, uma das piores coisas que podem acontecer é pegar uma trilha errada no diagnóstico e perder horas preciosas de trabalho. Principalmente porque nesse caso específico, de teste de fonte, vai ser difícil receber do cliente por essas "horas extras" gastas inutilmente.

Pior ainda é quando essa pista errada é dada por um dispositivo que nos custou dinheiro. De fato, nenhum dos testadores avaliados aqui serve como um testador de fontes de propósito geral, pois a carga interna é muito limitada e por diversas vezes não atenderá ao requisito de consumo mínimo especificado pelo fabricante da fonte. Portanto, se você precisa de um testador de fontes testado e aprovado, em conformidade com as normas, continuamos sugerindo apenas o projeto de testador apresentado por nossa equipe na PC&CIA 55. Este sim consome a carga mínima (figura 6). **PC**



Notebooks: por dentro das opções

Nesta edição tivemos a oportunidade de conhecer de perto mais três modelos de notebooks disponíveis em nosso mercado. Acompanhe os resultados!



Fernando Vieira
Bacharelando em Ciência da Computação, atualmente trabalha no suporte técnico da Editora Saber.

MSI Mega Book 670

Mais conhecida no Brasil pela sua linha de placas-mãe e placas de vídeo, a MSI apresentou ao mercado nacional um novo modelo de notebook, o Mega Book 670 (**http://global.msi.com.tw/index.php?func=proddesc&prod_no=1058&maincat_no=135**). A plataforma base do hardware é composta pelo processador AMD Turion 64 X2 TL-52 (codinome Taylor e 1.6GHz) integrado em uma placa-mãe com chipset GeForce Go 6100 (C51MV), na versão com o SouthBridge (Ponte Sul) nForce Go 430 (MCP51M). Aliás, esse chipset da nVidia tem sido muito utilizado pela indústria devido a, basicamente, duas razões: um processador gráfico (GPU) integrado robusto e o bom suporte de drivers ao Linux, o qual é normalmente utilizado em notebooks de baixo custo.

É verdade que o GeForce Go 6100 não é o topo da série 6xxx dos chipsets da nVidia. No entanto, ele possui características de performance que casam perfeitamente com a posição de mercado que o Mega Book pretende atingir. Um público que procura mobilidade sem abrir mão de uma computação eficiente, não tanto em termos gráficos, mas sim no tempo de resposta para a abertura de janelas, por exemplo. Para o subsistema de memória, o M670 oferece dois slots do tipo SO-DIMM DDR2, sendo que um deles sai de fábrica com 1GB de memórias DDR2-667.

Além do disco rígido SATA II de 120GB (modelo MK1234GSX de 2,5", da Toshiba), o M670 traz em suas laterais quatro portas USB 2.0, um RJ-11 para o modem analógico, um RJ-45 para redes de 10/100Mbps, uma porta IEEE1394, um leitor de cartões (compatível com dispositivos SD, MMC, MS e MS PRO), um slot Express Card, uma saída de TV S-Video e outra D-Sub, entradas (linha e microfone) e saídas de áudio (fone e S/PDIF), além do adaptador de rede wireless 802.11b/g e um gravador de DVD (modelo AD-7530A, da Optiarc). A bateria utilizada é uma Li-ion de seis células e a resolução nativa do LCD WXGA de 15,4" é de 1280x800 (figura 1).

Do lado do software, o M670 veio com a distribuição Kurumin 7, um sistema operacional que oferece grandes facilidades na



F1.

Teclado numérico é uma opção normalmente não vista em notebooks, justamente para ocupar menos espaço. Pesando 2,640kg (com a bateria), o Mega Book M670 tem preço sugerido de R$ 2.790,00.

utilização do ambiente Linux, mas que via de regra não é a primeira opção dos integradores porque dá mais trabalho ajustá-lo para um notebook, diferentemente do Mandriva 2007 ou Suse 10.1, por exemplo.

Chamou-nos a atenção o fato do Kurumin vir desatualizado. O kernel, por exemplo, não estava habilitado para trabalhar com os dois núcleos do Turion, apenas um ficava ativo. Portanto, a menos que o usuário tenha bons conhecimentos de Linux para corrigir as imperfeições deixadas pela instalação padrão, terá de utilizar o equipamento aquém do potencial do hardware. Ou então, partir para o Windows. No site da MSI, estão disponíveis drivers para XP e Vista.

Asus U1 Series

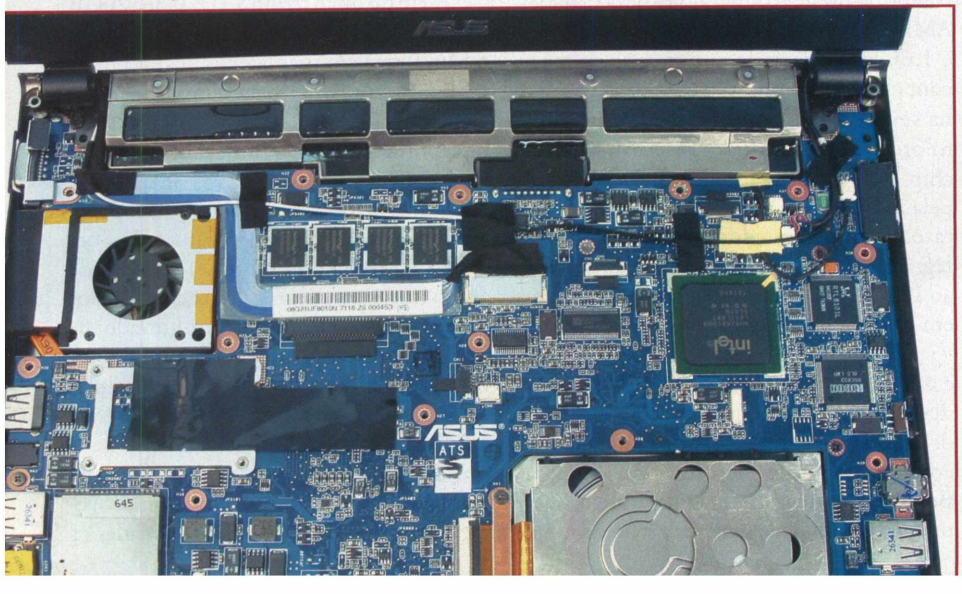
Em termos de miniaturização, o modelo U1 Series da Asus pode ser considerado como o estado da arte tecnológico. É o equipamento mais leve já avaliado em nosso laboratório, pesando apenas 1,08kg. O hardware base não é da última geração da plataforma Intel Centrino Duo, estando baseado ainda no chipset i945GM (Ponte Norte) com o Ponte Sul ICH7-M. O processador integrado é o modelo Core Duo U2400 (codinome Yonah de 1.06GHz – família lançada em 2006) e, em relação às memórias, o U1 vem com 1GB de memórias DDR2-533 operando em Dual-Channel (figura 2)

O subsistema de disco é composto por um HD IDE Ultra/100 de 80GB (modelo MKH8009GAH de 1,8", da Toshiba). Entre as interfaces de comunicação, estão disponíveis quatro portas USB 2.0, 1 IEEE1394, 1 D-Sub, 1 RJ-11 e outra RJ-45 para redes de 10/100Mbps, um leitor de cartões 4 em 1 (MMC, SD, MS e MS-PRO), um slot Express Card 54/34, dois interfaces wireless (Bluetooth 2.0 EDR+A2DP e outra Intel Pro 802.11a/b/g) e dois portas de áudio (microfone e saída). Na parte superior do monitor WXGA de 11"1 (resolução nativa 1366x768), vemos uma conveniente webcam com resolução de 0.3 MP (Mega Pixel).

E o drive óptico? Para suprir a ausência devido à restrição de espaço, a Asus optou por oferecer como opcional uma unidade externa Super Multi Blu-Ray/DVD. As opções de sistemas operacionais são o Vista Business e o Home Premium. Este último veio no modelo que recebemos e recebeu uma classificação de hardware mediano, segundo o próprio benchmark feito pelo Vista. Apesar da nota final 3,1 (processador 3.9, RAM 4.4, desktop e vídeo 3D 3.1 e 3.7 para o HD), o GPU integrado no i945M rodou perfeitamente a interface Aero. A presença do sensor biométrico e da tecnologia TPM (detalhes na edição n°60) são alguns dos recursos de segurança oferecidos no Asus U1F. Para gerenciá-los, a Asus desenvolveu seu próprio software, o Security Protect Manager (figura 3).

Com bateria Li-ion de três células e custo sugerido de R$ 9 mil no mercado local, o Asus U1 é seguramente uma opção a ser considerada por usuários constantemente em trânsito.

F2. **Miniaturização ao extremo: processador, segundo módulo de memória e adaptador wireless estão do outro lado da placa-mãe.**



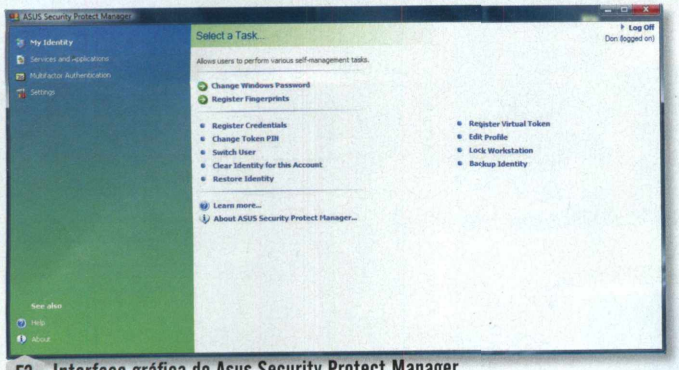
HP Compaq 6515b

Desenvolvido com o usuário corporativo em mente, mas também se apresentando como uma boa opção para os usuários de notebooks preocupados com a segurança dos dados. O Compaq 6515b merece este comentário, porque além de possuir um sensor biométrico, o chip TPM integrado na placa-mãe traz uma ótima suíte de programas para o gerenciamento dos recursos de segurança (detalhes na PC&CIA n°63).

O hardware é baseado no chipset ATI M690T (Ponte Norte), com GPU integrado Radeon X1250, e Ponte Sul SB600. O modelo que recebemos veio com processador Turion X2 TL-56 (codinome Taylor e freqüência nominal de 1.8GHz), um módulo de memória DDR2-667 de 1GB, monitor WXGA de 14,1" com suporte à resolução de 1280x800 e um HD SATA I de 120 GB (modelo MHW2120BH, Fujitsu, com suporte ao NCQ).

Em relação as interfaces, o 6515b traz quatro portas USB, uma saída de TV S-Video e outra de vídeo D-Sub, um IEEE 1394, um RJ-11 para o modem analógico, um RJ-45 para redes de 10/100/1000 Mbps, dois adaptadores wireless (Broadcom 802.11a/b/g e Bluetooth 2.0), um slot PC Card, um leitor de cartões 4 em 1, duas portas de áudio (microfone e saída) e um gravador de DVD SuperMulti com suporte a LightScribe (modelo CDW/DVD TS-L462D, da TSST). Como meios de expansão, ele suporta toda a linha de DockStation e dispositivos MultiBay, da HP. Há um "slot" para a instalação da segunda bateria, por exemplo (figura 4).

Dentre os sistemas operacionais, a HP oferece a versão Business ou Home Premium do Windows Vista, em 32 e 64 bits. A classificação recebida durante testes com um Business de 64 bits foi de 3.0. O processador ficou com a nota 4.7, memória 3.9, desktop 3.2, vídeo 3D 3.0, e HD 4.5.



F3. Interface gráfica do Asus Security Protect Manager, responsável por gerenciar os recurso de segurança.



F4. Compaq 6515b instalado na DockStation NAS 3 em 1 (detalhes na PC&CIA 62). Peso de 2,4kg (com bateria Li-ion de 6 células) e preço sugerido de R$ 3.299,00.

Testes

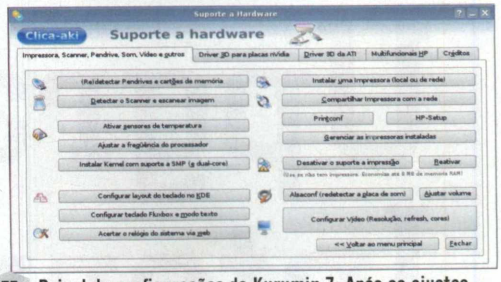
Desta vez optamos por avaliar o hardware, sistema operacional e, o mais importante, a usabilidade. Nesse último critério, entra a *questão da produtividade*, ou seja, será que a miniaturização do Asus U1 dificulta a utilização do sistema? Será que realmente o teclado numérico do Mega Book ajuda? Ou a linha Compaq é indiscutivelmente a melhor em todos os aspectos?

Resultados

Em matéria de hardware não há dúvida. Os três modelos carregam uma sólida plataforma tecnológica, tanto do lado AMD como Intel. No item sistema operacional, o HP Compaq e o Asus U1 deixaram boas impressões. Principalmente em relação à utilização da interface Aero que, durante os testes, não apresentou falhas no sistema. Apenas o Mega Book 670M apresentou pontos negativos. Depois de alguns travamentos no servidor X (responsável por manter o funcionamento da interface gráfica, entre outras funções) e lentidão no carregamento do Kurumin 7, descobrimos que a pós-instalação do sistema operacional não foi realizada da melhor forma. Ao abrirmos o arquivo xorg.conf, obtivemos a confirmação de que os drivers da placa de vídeo não estavam instalados. Isto mesmo, o sistema estava rodando por meio do driver padrão Vesa. Em seguida, através do comando "uname –a", veio a resposta para a lentidão. Na versão de kernel 2.6.18.1-slh-up-2 do Kurumin 7, não havia suporte ao SMP (Symmetric Multiprocessing – multiprocessamento simétrico). Conseqüentemente, apenas um dos núcleos do Turion X2 T-52 operava e, além disso, sob condições desfavoráveis, já que estava configurado para trabalhar apenas na freqüência mínima de 800MHz. Não é difícil resolver esses problemas, uma vez que o Kurumin 7 possui um excelente painel de configuração que permiti corrigir e ajustar o sistema (figura 5). Mas será que um usuário final faria tudo isso?

Na questão usabilidade, o único ponto negativo do Asus U1 é touchpad. O material utilizado em sua superfície não permite que os dedos deslizem facilmente. Já em relação à redução do espaço entre as teclas, após um certo período de adaptação não houve incômodo durante a digitação. O cérebro e as mãos se acostumam rapidamente a um teclado do tipo slim.

O Mega Book M670 também apresenta um bom layout de teclas, com destaque para a região do teclado numérico, que é extremamente bem-vindo para aqueles que fazem uso intenso de planilhas. Apesar de não trazer diferenciais neste sentido, o Compaq 6515b mantém o bom nível de usabilidade visto em versões anteriores da HP.



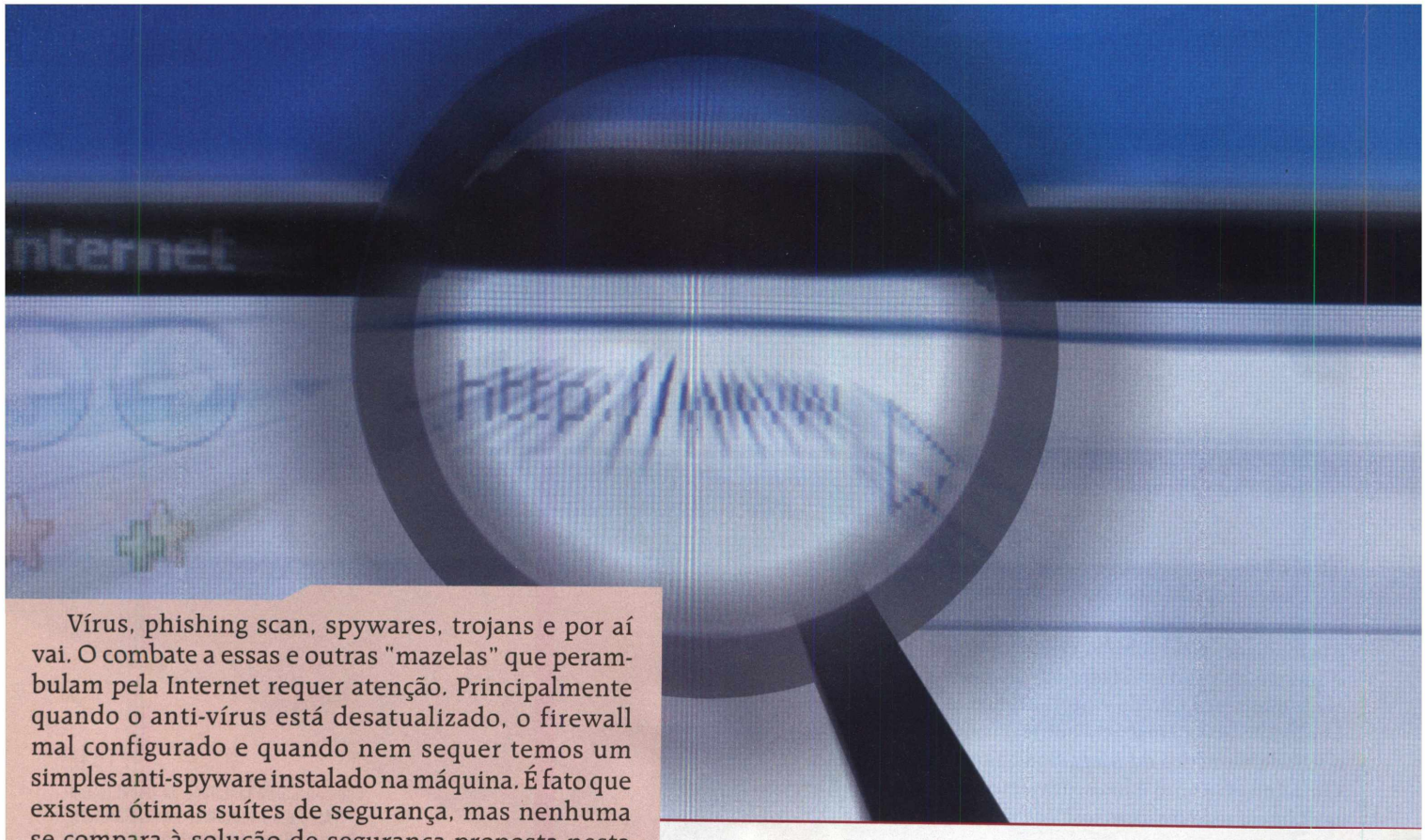
F5. Painel de configurações do Kurumin 7. Após os ajustes, sistema funcionou perfeitamente, sem travamentos e lentidões.

Conclusão

Terminamos essa seção de testes com a certeza de que os fabricantes ainda continuam "despreparados" frente ao Linux. Em menos de três meses tivemos a oportunidade de testar notebooks que dão destaque ao sistema operacional de código aberto, porém com alguns erros. O Sempron 3500+ do Compaq Presario V6210br (avaliado na edição 72), por exemplo, não operava entre 800MHz e 1.8GHz, conforme projetado pela AMD, mas limitado a 1.6GHz, porque o Mandriva 2007 não veio configurado corretamente. A falta de atenção com os detalhes acaba pesando negativamente no ponto de venda, afinal, de que adianta o poder computacional ser alto se ele não é aproveitado pelo sistema?

Diante da relação custo/benefício, se a sua necessidade é baseada somente na segurança, o HP Compaq 6515b é a melhor opção. O Asus U1 é imbatível para o usuário que busca peso leve, enquanto Mega Book M670 se apresenta como mais uma boa opção do mercado aos usuários que buscam um bom hardware base em um equipamento de custo acessível.

PC



Vírus, phishing scan, spywares, trojans e por aí vai. O combate a essas e outras "mazelas" que perambulam pela Internet requer atenção. Principalmente quando o anti-vírus está desatualizado, o firewall mal configurado e quando nem sequer temos um simples anti-spyware instalado na máquina. É fato que existem ótimas suítes de segurança, mas nenhuma se compara à solução de segurança proposta nesta matéria. Confira!

Upgrade na Internet segura

Fernando Vieira

Recordar é viver

Quem acompanhou as edições 60 e 62 da PC&CIA conheceu o IPCop, uma distribuição Linux focada em segurança e que pode ser instalada como máquina virtual sobre qualquer Windows (ver box). Este, como todos os programas dos usuários, sequer vêem a interface de rede da máquina *física, pois ela é simplesmente* impedida de utilizar o TCP/IP, que é o protocolo padrão de acesso à Internet. Ao invés disso, o Windows recebe uma interface de rede virtual criada pelo software de virtualização. Temos aqui, portanto, a primeira grande vantagem da solução, que é isolar totalmente o Windows da Internet.

Para que todos pudessem provar dessa solução, disponibilizamos em nosso site o download de uma máquina virtual do IPCop pronta e funcional. O resultado desse trabalho e o retorno dos leitores que experimentam o IPCop foram, de uma maneira geral, bastante positivos. Porém, de lá para cá não tivemos muitas novidades, ou seja, nenhuma outra funcionalidade foi desenvolvida e implementada no IPCop. Tivemos apenas algumas atualizações e correções de possíveis vulnerabilidades no sistema (ver box). Portanto, assim como tudo na informática, é chegada a hora de realizarmos um upgrade em nossa solução. E, para tal, entra em cena o Smothwall Express 3.0.

Smoothwall Express 3.0

A distribuição Smoothwall Express 3.0 possui o mesmo código genético do IPCop, mas contendo alguns cromossomos "especiais". Baseada na versão de kernel 2.6.x, ela oferece recursos até então presentes apenas em softwares proprietários, conforme veremos adiante. Além da versão Express, no site do desenvolvedor do projeto (**www.smoothwall.org**) também está disponível uma versão para desenvolvedor (Developer) que provê um excelente ambiente de desenvolvimento. Todos os arquivos de bibliotecas do compilador estão presentes, o que nos permite gerar ou modificar algumas das funcionalidades do Smothwall. É claro que em relação à

Express, a versão Developer é mais pesada (69MB contra 126MB, respectivamente). Outra característica interessante é o fato do Smoothwall ser um sistema que atende perfeitamente às necessidades de ambientes domésticos, ou de uma pequena empresa.

Ao final do upgrade na solução "Internet segura", passaremos a ter uma nova máquina virtual e um sistema completamente recente, o qual rodará a partir do também gratuito VMware Server (**www.vmware.com/**). Ou seja, o Smothwall Express 3.0 assumirá o lugar do IPCop como firewall e gateway dentro da rede, e será carregado pelo VMware Server automaticamente durante a inicialização da máquina.

O hardware virtual do Smothwall, provido pelo VMware Server, é composto por dois discos virtuais (um para o cache do proxy e outro para o sistema), duas placas de rede (uma física e outra virtual) e 92MB de memória RAM. A criação desse ambiente não requer profundos conhecimentos técnicos. Na verdade, o esforço será mínimo, pois já fizemos todo o trabalho de criação da máquina virtual (download de arquivo de 65MB em nosso site **www.revistapcecia.com.br**) e você só terá de configurar o sistema de acordo com a conexão utilizada para acessar a Internet. Você não sabe nada de virtualização? Não tem problema, basta colocar a PC&CIA ao seu lado e seguir a receita a seguir.

A receita

O primeiro passo é fazer o download gratuito do VMware Server no site indicado anteriormente (arquivo com 145MB) e instalá-lo no computador onde o Smoothwall rodará. Após, partiremos para a configuração das interfaces de rede. Para tanto, localize o arquivo vmnetcfg.exe dentro da pasta "\arquivos de programas\vmware server" e dê um duplo clique sobre ele para abrir a janela de configuração. Nesta, clique na guia "NAT" e desabilite esse recurso através do campo "Vmnet host"; em seguida, clique no botão "stop". Na guia "DHCP", utilize o botão "remove" para excluir todas as interfaces de rede listadas. Depois disso, clique no botão "stop" para encerrar a execução do serviço DHCP. Na guia "Host Virtual Adapters" utilize o botão "remove" para eliminar a interface VMnet8 (figura 1).

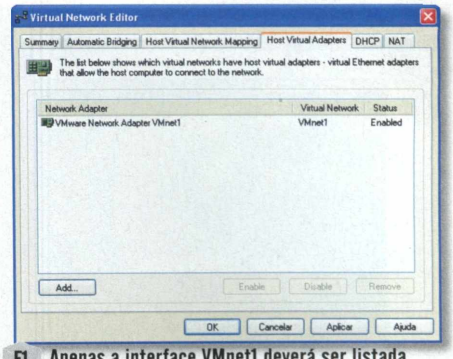
Por último, acesse a guia "Host Virtual Network Mapping". O campo vmnet0 deverá apontar para a placa de rede física instalada na máquina. Já o campo vmnet1 deverá utilizar a interface de rede virtual (figura 2).

As demais guias, "Summary" e "Automatic Bridging", não possuem parâmetros que requeiram ajustes. Aliás, a primeira apenas exibe uma lista das interfaces de rede que serão utilizadas na máquina virtual. Já na segunda, podemos optar por deixar o VMware escolher automaticamente uma das interfaces de rede física do computador que funcionará no modo bridge. Entretanto, como não é o nosso caso, devemos deixar desmarcada a caixa que ativa esse recurso.

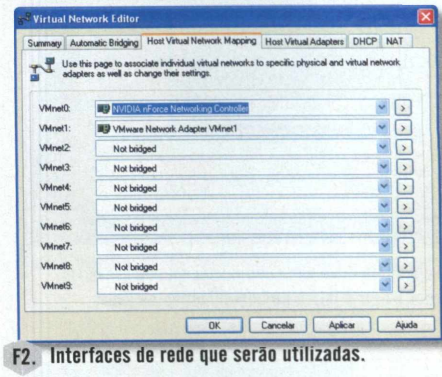
O próximo passo é configurar os protocolos de serviços que estarão habilitados em ambas as interfaces de rede. Primeiro, acesse as propriedades de conexão da placa de rede física e deixe marcado apenas o serviço "VMware Bridge Protocol". Em seguida, faça o mesmo com a interface virtual, atentando-se para deixar todos os serviços selecionados, inclusive o "VMware Bridge Protocol" (figura 3).

A partir deste ponto tanto o sistema operacional host ou hospedeiro (Windows), quanto o VMware Server, estarão prontos para rodar a máquina virtual do Smothwall. Descompacte o arquivo smothwall_express.zip baixado de nosso site. A pasta descompactada poderá ficar em qualquer diretório do HD, tal como sob a unidade C:, que foi o local escolhido em nossos testes. Agora abra o VMware Server e selecione o arquivo smothwall.vmx através da opção de menu File > Open (figura 4).

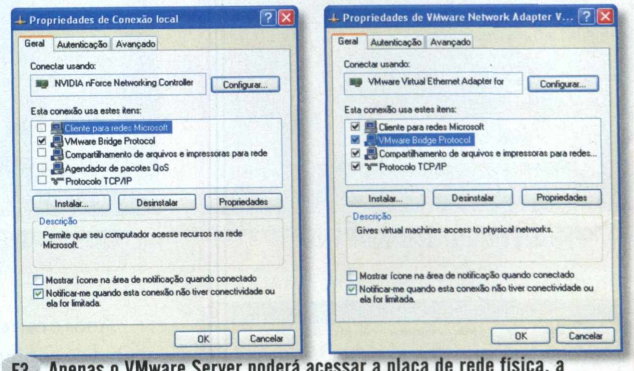
Como resultado, será exibida uma mensagem sobre a possibilidade de manter ou atribuir um



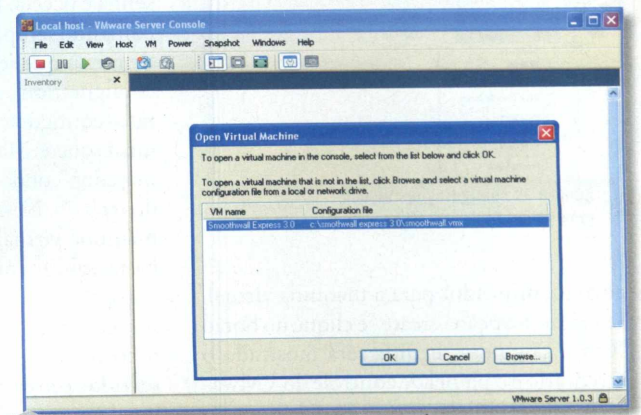
F1. Apenas a interface VMnet1 deverá ser listada nessa tela. Maiores detalhes sobre o vmnetcfg.exe estão disponíveis no link da edição 60, em nosso site.



F2. Interfaces de rede que serão utilizadas.



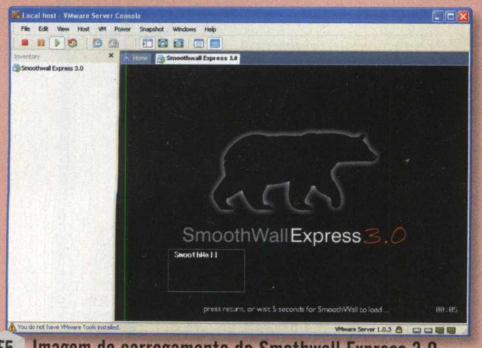
F3. Apenas o VMware Server poderá acessar a placa de rede física, a interface virtual (à direita) é que ficará à disposição do Windows.



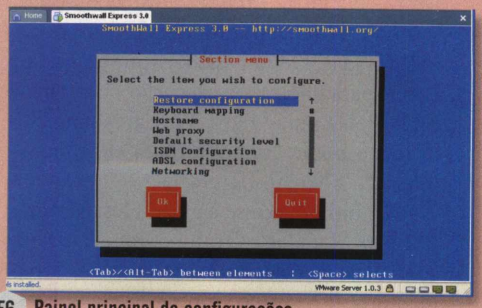
F4. Utilize o botão "browser" para localizar o arquivo de configuração (smothwall.vmx) da máquina virtual.

IPCop

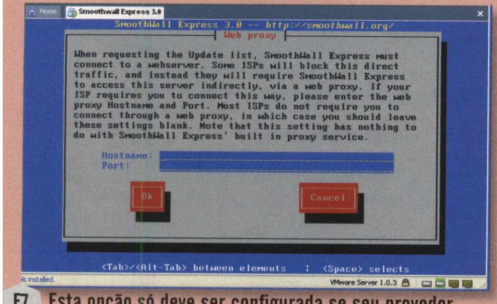
O IPCop é uma distribuição Linux baseada no kernel 2.4.x, que foi desenvolvida exclusivamente para a função de gateway e firewall dentro de uma rede. Com ele temos total flexibilidade para determinar as políticas de segurança no acesso à Web, mesmo se o ambiente em questão não for de rede, mas o de uma única máquina ligada diretamente no modem. Dentre os recursos disponíveis, destaque para o filtro de URL, Web proxy e sistema de detecção de



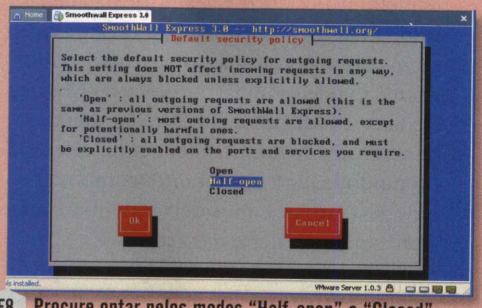
F5. Imagem de carregamento do Smothwall Express 3.0.



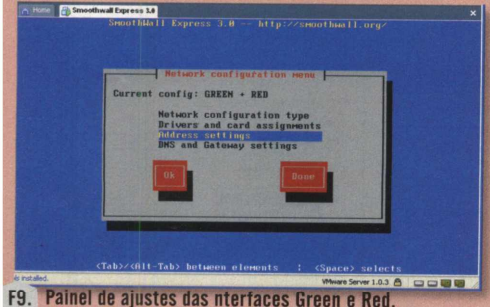
F6. Painel principal de configurações.



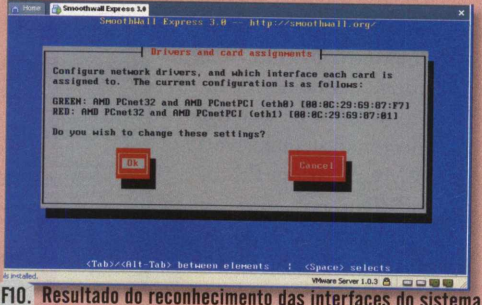
F7. Esta opção só deve ser configurada se seu provedor Internet exigir a porta de comunicação do Proxy.



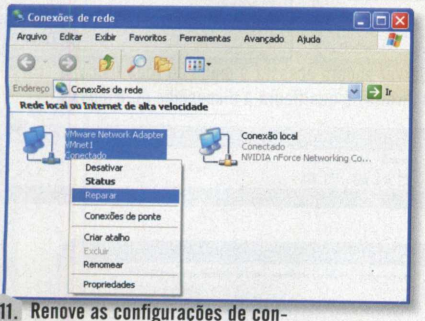
F8. Procure optar pelos modos "Half-open" e "Closed". Após selecionar a política que melhor atende sua rede, tecle "enter".



F9. Painel de ajustes das nterfaces Green e Red.



F10. Resultado do reconhecimento das interfaces do sistema.



F11. Renove as configurações de conexão somente da interface virtual.

novo identificador para a máquina virtual. Selecione a opção "create" e clique no botão "OK". Logo em seguida será mostrado o inventário e o painel de controle do VMware. A fim de iniciar o processo de boot do Smothwall, clique na opção "Start this virtual machine" (figura 5).

Após o carregamento, devemos entrar no painel de configurações do Smothwall. Faça um logon com a conta de usuário root, cuja senha é pcecia. Dentro do terminal digite o comando setup (figura 6). A primeira opção de menu que será apresentada é a "Restore configuration", através dela podemos restaurar as configurações do Smothwall a partir de um disquete. Mais abaixo, temos a "Keyboard mapping", onde é possível configurar o layout do teclado. Nesse momento o hostname da máquina virtual é "smothwall", se preferir basta utilizar a próxima opção para alterá-lo. Já a opção "Web proxy" deverá ser configurada somente se o provedor de Internet requerer o hostname e a porta de comunicação do servidor proxy. Repare que esta opção está ligada ao servidor proxy do provedor de Internet, e não com o serviço de proxy web do Smoothwall (figura 7).

A próxima opção, "Default security level", diz respeito ao nível de segurança oferecido pelo firewall do Smoothwall. Ao acessá-la o sistema nos mostra três modos de operação, o "Open", o "Half-open" e o "Closed". O primeiro libera a entrada de todas as requisições feitas da Internet para o Smoothwall; o segundo é o modo padrão, o qual libera apenas parcialmente as requisições; já no último modo, todas as requisições de comunicação serão descartadas pelo firewall, ou seja, somente os serviços e portas de comunicação previamente configurados manualmente é que poderão passar pelo firewall (figura 8).

As opções "ISDN Configuration" e "ADSL Configuration" deverão ser ajustadas conforme o método de conexão oferecido por seu provedor. Nossa máquina virtual disponível no site sai de "fábrica" configurada para trabalhar apenas com as zonas de redes Green e Red, e em ambas as interfaces o serviço DHCP está habilitado. Portanto, se sua conexão de acesso à Internet funcionar via DHCP, não será necessário realizar quaisquer ajuste. Caso contrário, utilize a opção "Networking" demonstrada na figura 6 e, indo até a opção "Address settings", defina o IP, os servidores de DNS e gateway da interface Red (figura 9). Para a rede local, a interface Green está configurada para distribuir IPs na faixa de endereçamento entre 172.16.0.100/24 até 172.16.0.200.

Para finalizar as configurações das interfaces de rede, entre na opção "Drivers and card assignments" da figura 9. É nela que checamos se as duas placas de rede foram "instaladas" e reconhecidas pelo Smothwall. Observe se as redes Green e Red estão apontando para as interfaces eth0 e eth1, respectivamente (figura 10). Caso seja mostrado o resultado "Unset" ao final da linha de cada interface, significa que realizamos alguma alteração na zona Red e Green. Para "consertar" o sistema, responda com "OK" à pergunta que será exibida na tela.

Uma vez finalizada a etapa de configuração das placas de rede, retorne à tela principal do Swoothwall e altere as senhas das contas de usuário root, setup e admin. Aliás, a última será utilizada para acessarmos a interface Web do Smoothwall. Feito isso,

utilize o botão "Quit" para sair do painel. Nesse momento a interface de rede virtual deverá estar operando, com o IP atribuído pelo Smoothwall. Se isso não acontecer, utilize a função "reparar" existente nas propriedades de conexão da placa de rede (figura 11).

Para acessar a interface Web do Smoothwall, abra seu browser e digite o endereço 172.16.0.1:81. Em seguida, digite o nome e senha do usuário admin. Na primeira página de entrada, são exibidos os endereços IP (rede interna e externa) e a velocidade atual do link de conexão. Na aba "About > status" são mostrados os serviços em funcionamento (figura 12). Na guia ao lado, "advanced", vemos um relatório sobre o estado do sistema, contendo informações sobre o consumo de memória, as partições montadas, o espaço ocupado nos dois discos, o uptime da máquina (funcionamento ininterrupto), as placas de redes, a tabela de roteamento, entre outras informações (figura 13). Repare que além do hardware, os módulos carregados também são descritos nessa página. Isso é algo que nos ajuda, por exemplo, a identificar possíveis falhas de conexão entre o Smothwall e a rede local.

Através das guias "traffic graphs", "bandwidth bar" e "traffic monitor" podemos monitorar em tempo real os dados em tráfego nas redes Green e Red. Não precisamos, portanto, esperar que um novo log seja gerado para daí então confirmarmos alguma suspeita no consumo de banda da rede (figura 14).

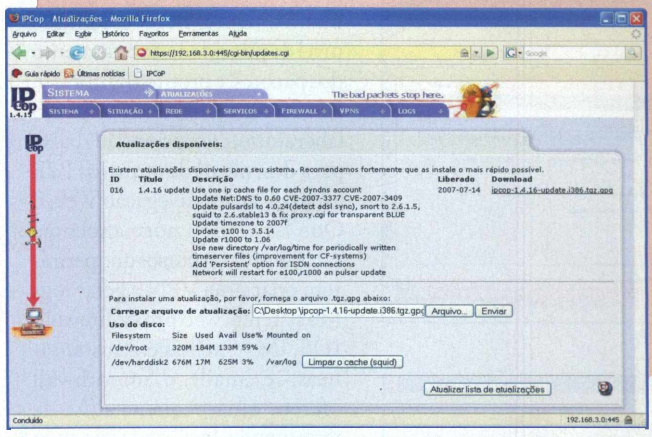
Ao pular de guia, chegamos à parte mais interessante do Smoothwall, os serviços. O famoso Advanced proxy, o servidor DHCP e de DNS (estático e dinâmico), IDS (Intruccion Detection System) e o SSH não são novidade. A surpresa embutida no Swoothwall são os serviços de proxy SIP, POP3 e o de IM (Mesangeiro Instantâneo). O proxy SIP pode ser utilizado para encaminhar, ou não, as chamadas VoIP realizadas de dentro para fora da rede. E por meio do log que é gerado, podemos ter acesso às informações de chamadas realizadas (figura 15).

O serviço de proxy de mensagens instantâneas é, sem dúvida, outro "plus" interessantíssimo. Com ele é possível monitorar toda e qualquer conversação entre os usuários dentro da empresa. Os programas mensageiros compatíveis são listados na guia referente ao serviço (figura 16). Quando habilitado, o proxy pop3 realizará um scan (varredura) em todas as mensagens de email recebidas da Internet para a rede local, a fim de encontrar e remover possíveis vírus. Esse scan, na verdade, será realizado pelo anti-virus ClamAV.

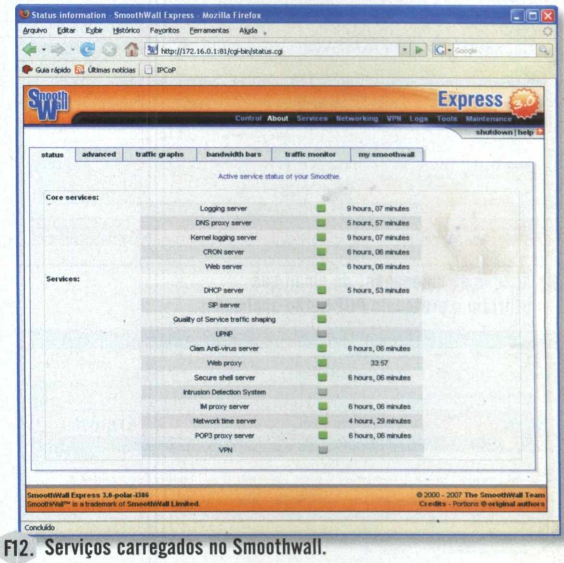
Dentro da guia "Networking", temos acesso a todas as configurações de operação

IPCop e atualizações

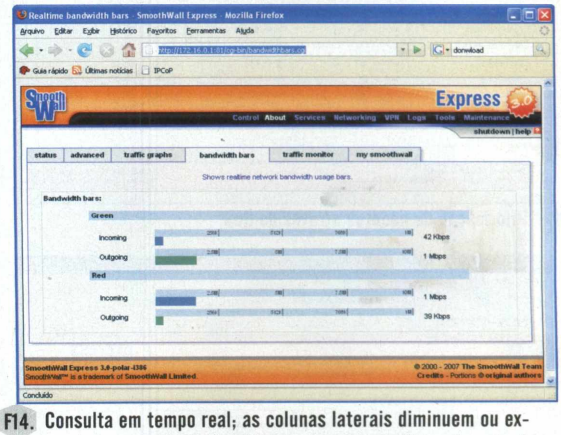
Todas as vezes em que é iniciado, o IPCop executa o script updatelists.pl para realizar uma busca por atualizações, as quais são informadas em sua interface Web. Para baixar e instalá-las, basta seguirmos as instruções exibidas na guia "Atualizações" do IPCop. Isto é, primeiramente devemos baixar o arquivo de update e, logo após, informar o diretório do arquivo recém-baixado no campo "Carregar arquivo de atualização".



Página de atualizações do IPCop.

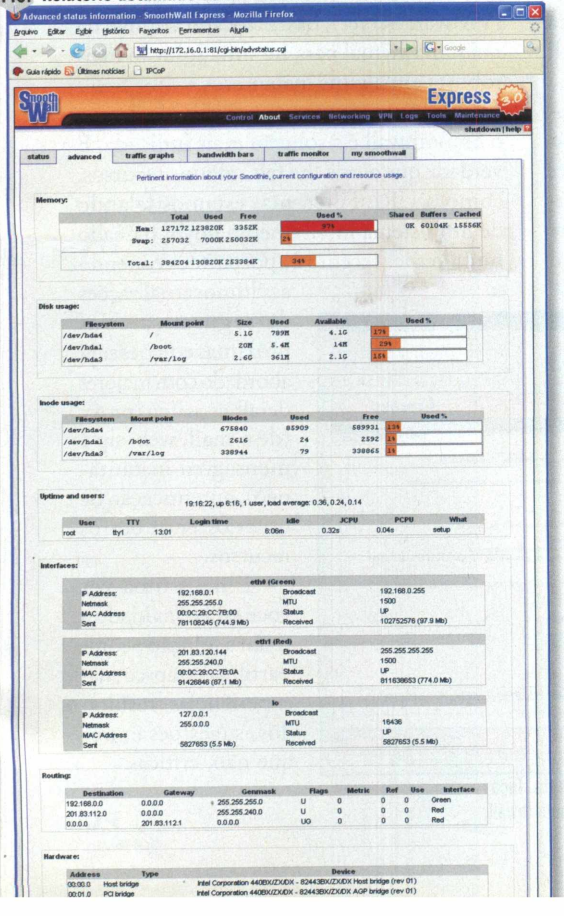


F12. Serviços carregados no Smoothwall.

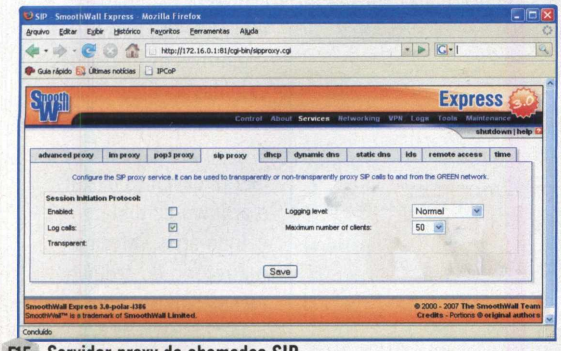


F14. Consulta em tempo real; as colunas laterais diminuem ou expandem conforme a velocidade, expressa em Kbps, de entrada e saída nas interfaces de rede.

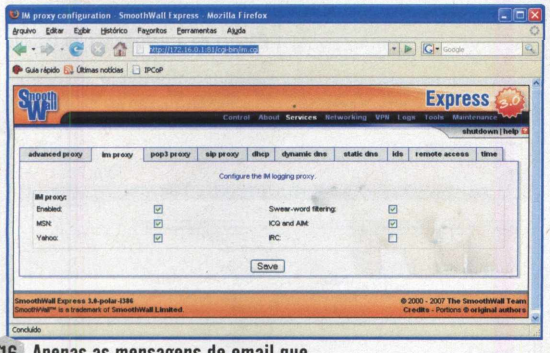
F13. Relatório detalhado do hardware.



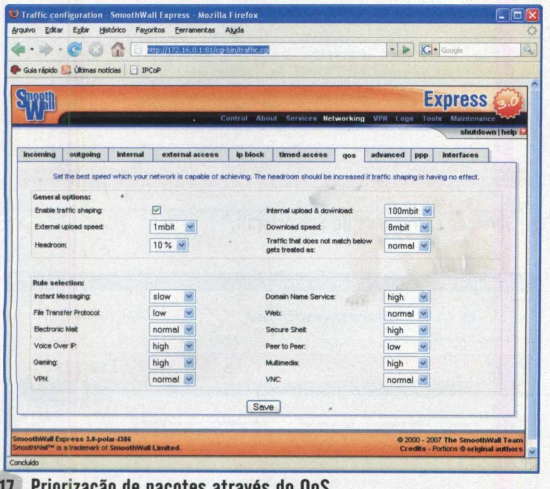
do firewall tanto na zona Green, quanto na Red. Das funções apresentadas nessa tela, a QoS (Quality of Service), ou qualidade de serviço, é a mais interessante. Os serviços de maior presença em uma rede atual podem ser contemplados pelas regras de QoS. Nem precisamos definir o protocolo manualmente. Basta escolher o nível de prioridade de tratamento dos pacotes, e pronto (figura 17). Em testes realizados em nosso laboratório, com prioridade baixa para download de arquivos P2P e máxima para navegação Web, o QoS funcionou normalmente.



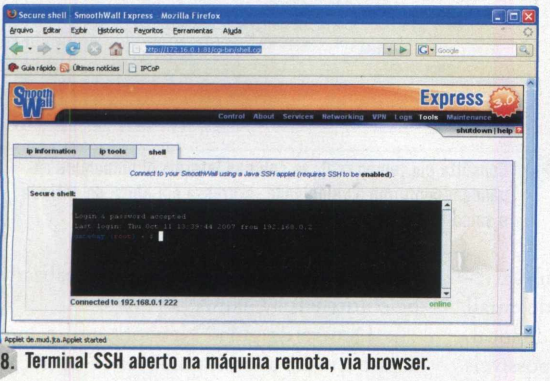
F15. Servidor proxy de chamadas SIP.



F16. Apenas as mensagens de email que utilizam o protocolo POP serão analisadas.



F17. Priorização de pacotes através do QoS.



F18. Terminal SSH aberto na máquina remota, via browser.

Além dos recursos que permitem criar uma VPN e gerar logs (do sistema, web proxy, firewall, IDS, IM – mensagens instantâneas - e email), o Smoothwall oferece uma pequena suíte de ferramentas localizadas na guia "Tools". A ferramenta "ip information" serve para colher e mostrar na tela informações de domínio. Para fazer uma pesquisa, basta digitar o endereço IP ou o nome de domínio sobre o qual queremos obter maiores informações. A ferramenta "ip tool" permite que utilizemos os comandos ping e traceroute na própria interface web. E por último, a ferramenta "shell" nos permite abrir uma conexão de terminal SSH diretamente na máquina onde o Smoothwall está instalado (figura 18).

Dentro da aba "Maintenance" é exibido um painel que suporta a realização de atualizações no sistema, ajustes nas configurações e modificações no firmware de alguns modems ADSL – o que não é recomendado pelos fabricantes. As opções de alterar senha, fazer backup das configurações, e de shutdown também estão presente nesse painel (figura 19).

E os pontos negativos? Mesmo diante de excelentes funcionalidades, é inegável que a falta de suporte ao idioma português é algo relevante. Principalmente para o usuário final. Mas supondo que o técnico é quem o instalará, configurará e até realizará suporte remoto, até que isso não preocupa tanto.

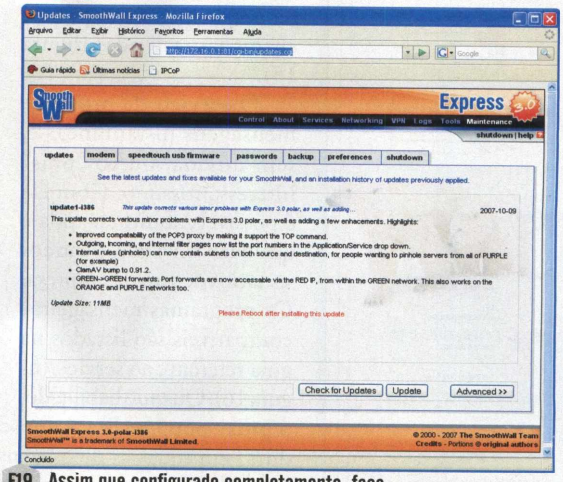
Em relação aos plugins, ainda não há uma boa quantidade disponível. Até o fechamento desse artigo, apenas o addon do Advanced Proxy era compatível com a versão Express 3.0. Repare que, infelizmente, ainda não falamos sobre um dos addon mais importantes, o URL Filter, o qual ainda não está disponível.

Conclusão

Então, abandonamos o IPCop? De forma alguma. Na verdade, como o IPCop é derivado do Smothwall, acreditamos que dentro dos próximos meses vamos ver a versão 2.0. Portanto, continuaremos buscando a melhor solução, através da análise paralela das duas distribuições. Nesse processo, vale ressaltar a grande flexibilidade oferecida por uma solução de virtualização do hardware. Pelo fato de a infra-estrutura já estar instalada (VMware Server), basta trocar o arquivo da máquina virtual para ter uma solução mais robusta em alguns instantes.

No momento, não resta dúvida de que o Smoothwall é a solução mais indicada. É verdade que ainda lhe falta alguns recursos, como o URL Filter, mas estamos falando de um sistema inteiramente novo, baseado num kernel recente e, portanto, contendo as últimos atualizações de segurança. Nas próximas edições será abordado com maiores detalhes os itens proxy (de e-mail, web, sip e mensagem instantâneo), autenticação de usuários, entre outros recursos.

E mais uma vez você está convidado a testar a solução e compartilhar conosco suas experiências, resultados, sugestões e, por que não, críticas.



F19. Assim que configurado completamente, faça um backup das configurações do Smoothwall.

PC



DDR3 X DDR2

Os módulos de memória DDR3 e as placas-mãe que os suportam estão no mercado há apenas alguns meses. Mas alguns fabricantes já lançaram modelos cujas freqüências de operação excedem consideravelmente o máximo regulamentado pelo Jedec, que é a entidade responsável pela padronização nesta área. Esta matéria mostra na prática o quanto esses novos módulos podem ser úteis.

Fernando Ramos da Silva

Na edição anterior apresentamos os detalhes técnicos da especificação das memórias DDR3. Além da menor tensão de trabalho (1,5 contra 1,8 da DDR2), as DDR3 podem atingir até 1,6 GHz, segundo a proposta do Jedec. Na prática, porém, alguns fabricantes oferecem hoje módulos que ostentam a incrível velocidade de 1866 MHz, valor este muito superior à freqüência de operação nominal de qualquer processador atualmente disponível no mercado (figura 1). Só para relembrar, os mais recentes Core 2 Duo da Intel operam com uma freqüência base de 333 MHz e rendimento de 1333 MHz, uma vez que, pelo princípio conhecido como QDR (Quad Data Rate), realizam quatro transferências por ciclo de clock.

A princípio, portanto, um barramento de memória operando além de 1333 MHz estaria superdimensionado às necessidades do processador. Vale lembrar também que ainda não foi lançado qualquer chipset, cuja controladora de memória suporte oficialmente freqüências acima deste valor. Nem para a plataforma AMD e nem para a Intel, que é o enfoque desta matéria. Aliás, os sistemas AMD que suportarão as memórias DDR3 são esperados apenas para o final do próximo ano, ou ainda em 2009.

Mas considerando que durante toda transação entre processador e memória há dois barramentos a serem percorridos



Kit Patriot PDC32G1866LLK: dois módulos de 1 GB operando a 1866 MHz! F1.

e sempre sob o gerenciamento do chip Northbridge (Ponte Norte) do chipset, na prática as maiores freqüências no barramento de memória podem contribuir para compensar o inerente aumento de latência da arquitetura Intel em relação a da AMD. Nesta, o processador pega os *dados* mais rapidamente, porque a controladora de memória está integrada no mesmo chip, onde está a pastilha de silício do processador.

Outra variável a ser considerada é o aumento das latências das memórias DDR3, em relação às DDR2.Se no caso da última vimos recentemente, na edição 73, módulos operando a 1120 MHz com temporização 4-4-4-12, os valores típicos para DDR3 acima de 1333 MHz são 6-6-6-18 e 7-7-7-20. Diante de tantas variáveis, só mesmo um teste comparativo para esclarecer na prática se há ou não ganhos de performance.

Testes

Tivemos acesso a cinco kits Dual-Channel de 2 GB DDR3, sendo três da Patriot, com freqüências variando entre 1333 e 1866 MHz, um da Kingston certificado para 1375 MHz e o último da Corsair, para 1800 MHz.

A primeira grande dificuldade foi encontrar uma placa-mãe que suportasse freqüências dessa magnitude. Isso porque o chipset P35, encontrado atualmente na grande maioria das placas-mãe DDR3, segundo a Intel só suporta oficialmente módulos operando a 1066 MHz. E mesmo o mais recente X38, também da Intel, oficialmente tem uma controladora de memória limitada à freqüência de 1333 MHz.

Das duas placas-mãe P35 que tínhamos à disposição, uma MSI P35 Diamond e uma Asus P5K3 Deluxe, a primeira só foi até valores próximos a 1400 MHz, embora seu BIOS apresentasse os principais parâmetros para o ajuste fino do barramento de memória. Não funcionou além disso por limitação física do projeto, já que com nenhum módulo e mesmo com tensões elevadas (2.0V) a placa ligava com valores acima de 1440 MHz. A P5K3 Deluxe, por sua vez, demonstrou um melhor preparo eletrônico, possivelmente devido a um melhor ajuste com o casamento de impedância no barramento, e suportou a operação a 1800 MHz.

Outra questão importante diz respeito ao processador. Como as atuais revisões de BIOS só oferecem divisores compreendidos entre a faixa 1:1 e 1:2 para a relação entre a freqüência do FSB e a do barramento de memória, isso significa que mesmo se estivermos com um modelo da última geração de processadores, cuja freqüência base do FSB é de 333 MHz, a maior freqüência disponível no barramento de memória será de 333 x 2 (divisor) x 2 (DDR) = 1333 MHz. Quer dizer então que obrigatoriamente teremos de fazer overclock no FSB para ter a memória operando acima de 1333 MHz? Exatamente! Conseqüentemente, para atingir 1800 MHz precisaremos que ambos, placa-mãe e processador, suportem um FSB de 450 MHz (figura 2).

A MSI suportou este valor no FSB, na verdade o problema com ela foi apenas no barramento de memória. O processador escolhido para operar com a P5K3 foi um Core 2 Duo E6600, com freqüência interna de 2,4 GHz, FSB padrão de 266 MHz e multiplicador de clock igual a 9. Como a placa nos permite reduzir o multiplicador para 6, que é o valor mínimo para os Core 2 Duo, com 450 MHz no FSB o E6600 operou internamente a 2,7 GHz. Um overclock tão pequeno que sequer demandou uma elevação na tensão do processador ou troca do CPU cooler. Aliás, os testes foram realizados com o cooler in-a-box padrão da Intel.

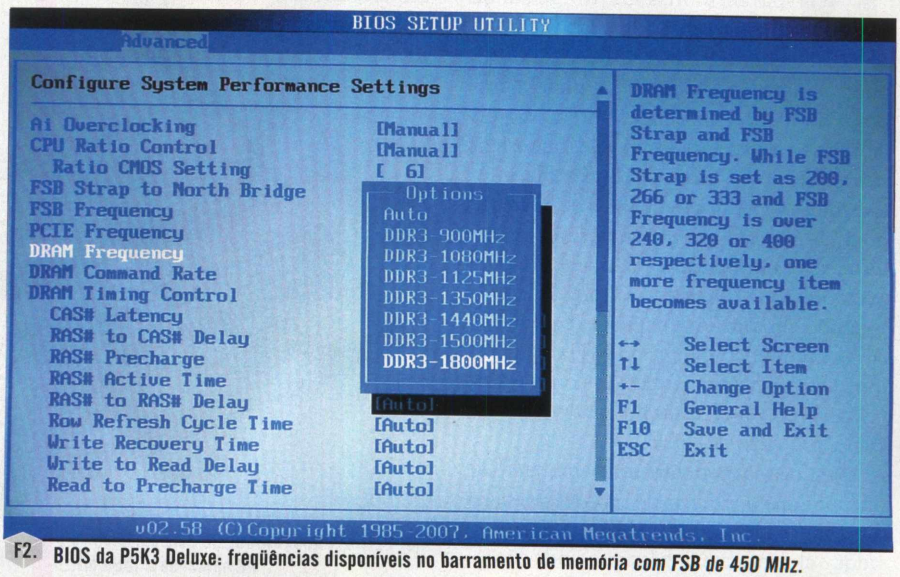
Os demais componentes base do sistema foram uma fonte Cooler Master Real Power Pro de 1000W, placa de vídeo Asus GeForce 8800 GTX, monitor Asus *wide screen* de 20" com resolução nativa de 1680x1050 e um HD Raptor WD740ADFD de 74 GB rodando o Windows Vista Ultimate 32 bits com pacote de drivers Intel da versão 8.3.1.1009 (chipset) e Forceware 163.69 (placa de vídeo). Agora vamos conhecer os módulos.

Módulos

O primeiro kit avaliado foi o Corsair TWIN3X2048-1800C7DF G, pertencente à tradicional família Dominator, tão conhecida dos usuários entusiastas. O fabricante alega que todos os chips utilizados são escolhidos um a um através de testes que certificam a capacidade de suportar as elevadas freqüências e baixas latências dessa linha. Depois disso são montados numa placa de circuito impresso (PCB) com design exclusivo e estressados novamente com o objetivo de verificar a interoperabilidade dentro do conjunto, além da confiabilidade. O dissipador, aliás, chama a atenção pelo alumínio extrusado que tira proveito do princípio da convecção para dissipar o calor no ambiente. E além da área de contato entre a PCB e o dissipador retirando o calor por condução, é possível montar esse kit com um exclusivo suporte contendo três ventoinhas de 40mm forçando a circulação de ar sobre os módulos. Esse "cooler" de memória pode ser encontrado separadamente (código Corsair CMXAF1, cotado a US$ 20 no exterior) ou comprado junto com o kit (figura 3).

O fato é que com ou sem o cooler os dissipadores desses módulos esquentam pouco, mesmo quando operando com 2.0V, que é a tensão máxima especificada pela Corsair. Pena que os módulos não possuem um sensor de temperatura que permita ao usuário acompanhar a elevação térmica.

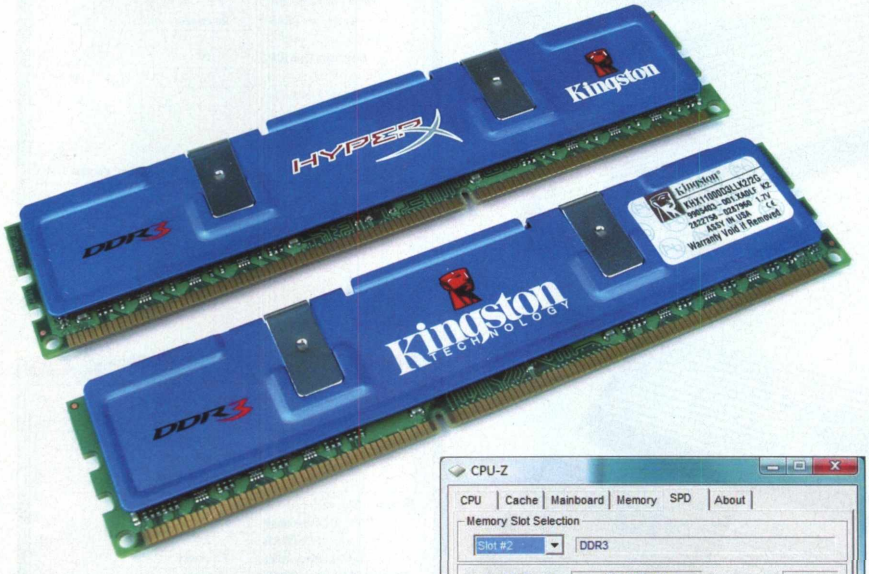
As temporizações gravadas no chip de memória SPD desses módulos são de

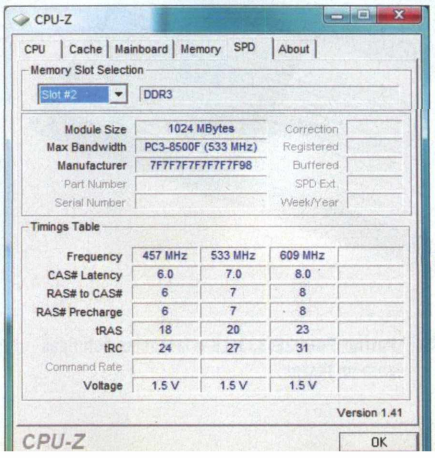


F2. BIOS da P5K3 Deluxe: freqüências disponíveis no barramento de memória *com FSB de 450 MHz.*



F3. Corsair Dominator TWIN3X2048-1800C7DF G com kit completo: "cooler" é facilmente preso às travas dos soquetes de memória.





F4. Kingston KHX11000D3LLK2/2G com CPU-Z mostrando valores gravados no chip EEPROM SPD.

6-6-6-16 para 444 (888 MHz DDR), 8-8-8-22 para 592 (1184 MHz) e 9-9-9-24 para 666 (1332 MHz). Por padrão eles são inicializados na P5K3 com 8-8-8-20 1066 MHz, considerando o E6600 operando sem overclock. Durante os testes, eles suportaram normalmente a configuração Dual-Channel com as temporizações agressivas 7-7-7-20 1800 MHz. Só há um detalhe: a montagem deve obrigatoriamente ser feita nos soquetes pretos, conforme ressalta o site da Corsair. Nos laranjas, não havia estabilidade total a 1800 MHz.

Dos quatro pares de módulos restantes, todos empregam um projeto térmico já conhecido de nossas edições anteriores. A Kingston com seu dissipador azul característico da linha da alta performance HyperX e a Patriot com seu design simples, porém eficiente. Vejamos a seguir os detalhes de cada kit:

- KHX11000D3LLK2/2G: A Kingston certificou os módulos desse kit para operação em 1375 MHz com latências 7-7-7-20 e tensão de 1,7V. Seu chip SPD, contudo, traz valores mais relaxados visando a compatibilidade com um maior número de placas-mãe. A primeira configuração da tabela gravada no SPD é 457 (914 MHz) 6-6-6-18, depois vem 533 (1066 MHz) com 7-7-7-20 e, por último, 609 (1218) com 8-8-8-23. Com os parâmetros em Auto no Setup da placa-mãe P5K3, o kit foi inicializado com os ajustes da segunda configuração. Já no decorrer dos testes de performance, o conjunto surpreendeu positivamente ao suportar as latências 7-7-7-20 com uma freqüência ligeiramente superior, 1440 MHz, e ainda com a tensão de 1,7V (figura 4);
- PDC32G1866LLK: Esse é o kit DDR3 de maior performance disponibilizado até o momento pela Patriot. São 1866 MHz com latências 8-8-8-24 e tensão limite de 1,9V. Em seu chip SPD, há dois registros, um 457 (914 MHz) 6-6-6-18 e outro 533 (1066 MHz) 7-7-7-20, que é a opção carregada por padrão na P5K3. Em nossos testes ele operou com tensão de 1,9V, latências 8-8-8-20 e freqüência de 1800 MHz, devido à limitação de FSB de 450 MHz. Com latências ligeiramente inferiores, por exemplo 7-7-7-20, a máquina era incapaz de inicializar o POST a 1800 MHz e o Windows Vista de finalizar o boot a 1500 MHz;
- PDC32G1600LLK: É a opção intermediária da Patriot, baseada no mesmo projeto do anterior, mas com

chips certificados para operação máxima a 1600 MHz, com latências 7-7-7-18 e tensão de 1,8V. Os valores de SPD e os carregados com tudo em Auto no Setup da P5K3 são os mesmos do kit anterior. Também devido à limitação da quantidade de divisores de memória no Setup, esse kit operou a 1500 MHz e com suas latências padrão 7-7-7-20. A 1350 MHz, ele suportou com total estabilidade os testes com latências 6-6-6-18 e depois 5-5-5-18, a 1125 MHz (figura 5).

• PDC32G1333LLK: Nosso último kit é a opção de entrada de linha DDR3 da Patriot, operando a 1333 MHz, latências 7-7-7-20 e tensão de 1,7V. Esses foram os valores utilizados durante o teste e vale comentar ainda que o kit operou normalmente a 1125 MHz com latências 6-6-8-24 (figura 6).

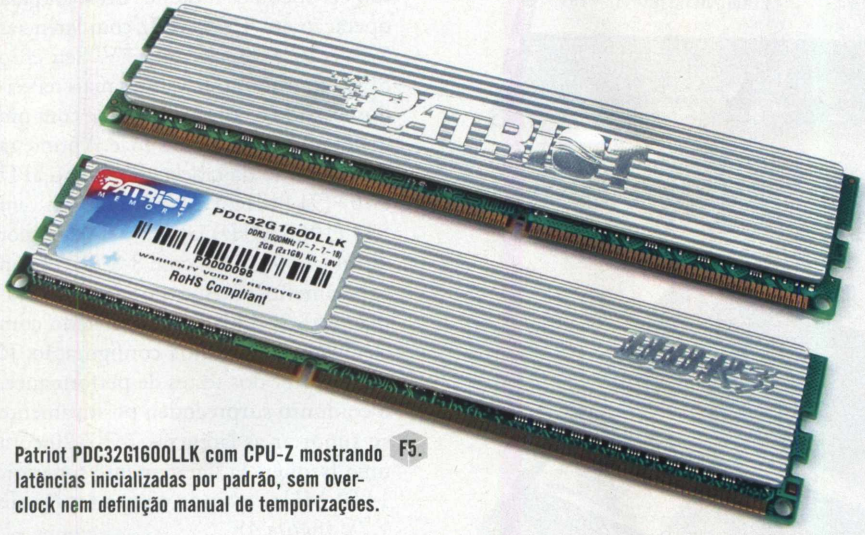
Resultados

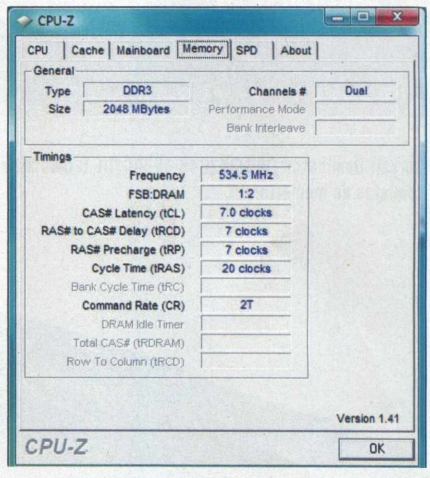
Nos gráficos a seguir, os módulos DDR3 são comparados ao melhor kit DDR2 de 2 GB já testado em nosso laboratório, o Patriot PDC22G9200ELK. Ele operou com total estabilidade a 1120 MHz, com latências extremamente agressivas (4-4-4-12) e com tensão de 2,3V na placa-mãe Gigabyte P35-DQ6. Essa placa também traz o chipset Intel P35 integrado e foi avaliada com os mesmos componentes e sistema operacional do sistema DDR3.

Agora os resultados. Qual seria o intervalo de tempo decorrido entre o comando disparado pela controladora de memória do chipset e os módulos começarem a disponibilizar os dados? A resposta para esse teste de latência foi dada por três programas, o ScienceMark 2.0, o Everest Ultimate e o Sisoftware Sandra Lite XIIc. A combinação maior freqüência e menor latência, representada pelo kit da Corsair, foi a mais rápida, sendo acompanhada logo em seguida pelo Patriot DDR2. Vale destacar que o pior resultado, no caso obtido pelo Patriot 1333, foi em média 18,5% mais lento (figura 7).

Embora com menor diferença percentual entre o melhor e o pior resultado, o cenário descrito acima se repetiu durante o teste de vazão máxima de dados. O Corsair 1800 por pouco não atingiu a taxa de 10000 MB/s, mas ainda foi 2% superior ao segundo colocado, que desta vez foi o kit Patriot 1866 (figura 8).

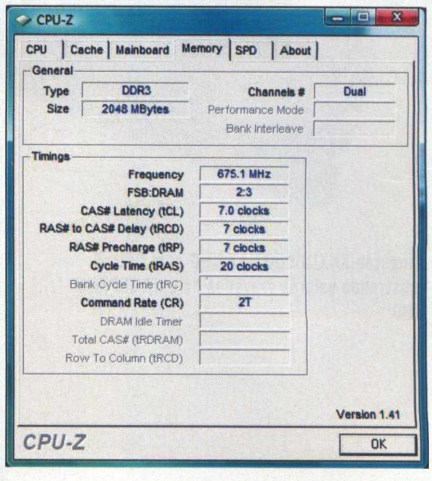
O próximo teste foi com o PCMark2005, especificamente com seu módulo de teste de memória. Leitura e gravação, cópia e aferição da latência com blocos de dados de 4 e 192 KB, 8 e 16 MB, ao todo são realizadas 16 avaliações e ao final é emitido um índice geral indicativo da performance obtida. Mais uma vez, o Corsair 1800 foi





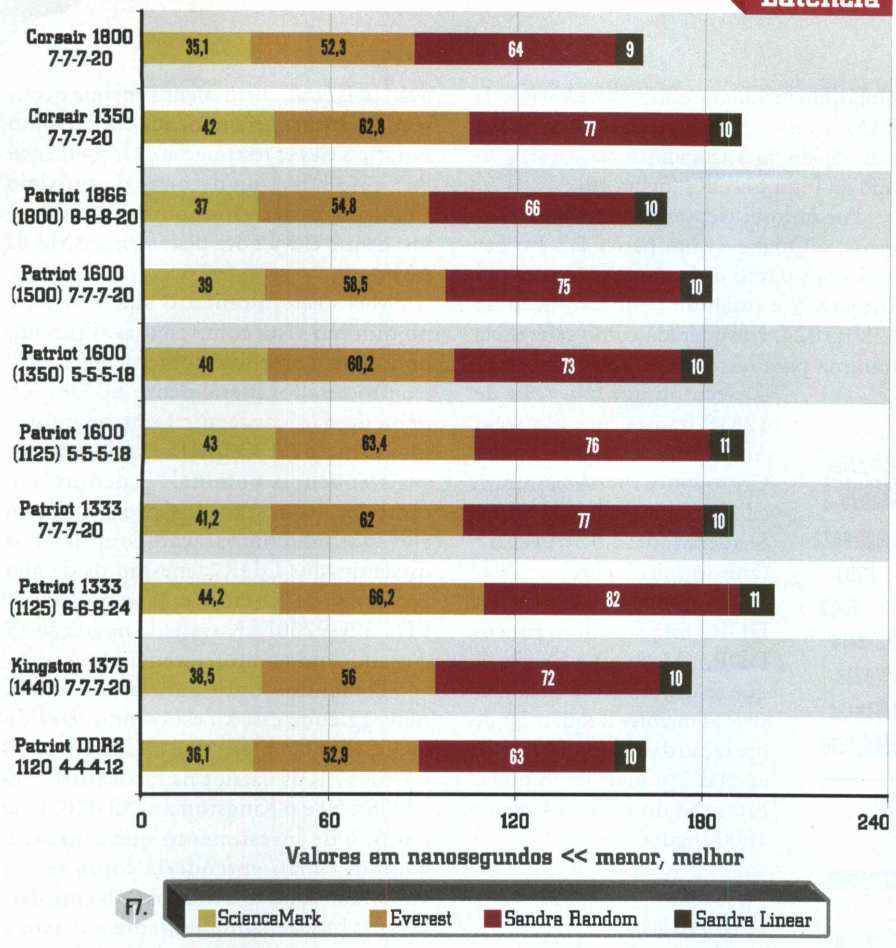
F5. Patriot PDC32G1600LLK com CPU-Z mostrando latências inicializadas por padrão, sem overclock nem definição manual de temporizações.



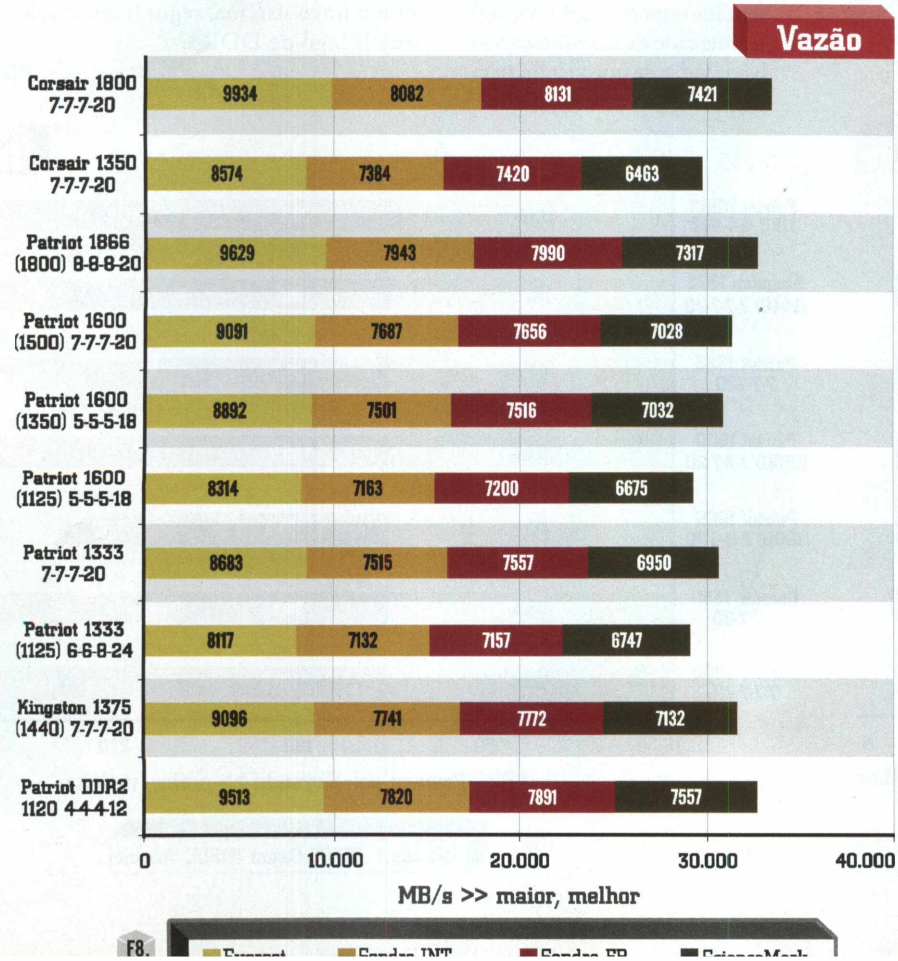


F6. Patriot PDC32G1333LLK e latências definidas para os testes.

Latência



Vazão



GARANTIA PARA TODA A VIDA



waz

DISTRIBUIDORA OFICIAL CORSAIR™

www.waz.com.br

vendas@waz.com.br

31 2126 6666

Preços especiais para lojistas:
revenda@waz.com.br

superior e teve a companhia de perto do Patriot DDR2 (figura 9).

A seguir realizamos testes com dois programas tipicamente utilizados no dia-a-dia da maioria dos usuários. O primeiro com o iTunes 7, convertendo 20 trilhas de áudio, num total de 1,48 GB, para mp3; e depois o 7-Zip 4.56 beta, já com suporte a multithreading, compactando um arquivo .dbx de 218 MB para 113 MB, a partir do nível de compactação Ultra. Ambos fazem muito acesso a disco e à memória RAM. Como era de esperar, o Corsair foi o mais rápido, mas agora finalizando a série ao lado do Patriot DDR2 (figura 10).

Por último, vieram os testes com dois jogos, o Quake 4 com patch 1.3 e o Far Cry com patch 1.4, ambos da geração DirectX 9 e rodando com resolução de 1280x1024, considerada como referência mínima para testes nesta área. O Quake 4 executou um *timedemo* de 12819 frames com filtragem Anti-Aliasing (AA) 4x e o Far Cry rodou os *timedemos* Steam e River com qualidade Ultra, Shader Model 3.0, AA4x e AF (anisotrópico) 16x.

Novamente o kit Patriot DDR2 foi páreo duro para os DDR3. Mesmo no Quake 4, que se demonstrou mais sensível às maiores freqüências de operação das memórias, ele foi apenas 5% mais lento que o campeão do teste, o Corsair 1800 (figura 11).

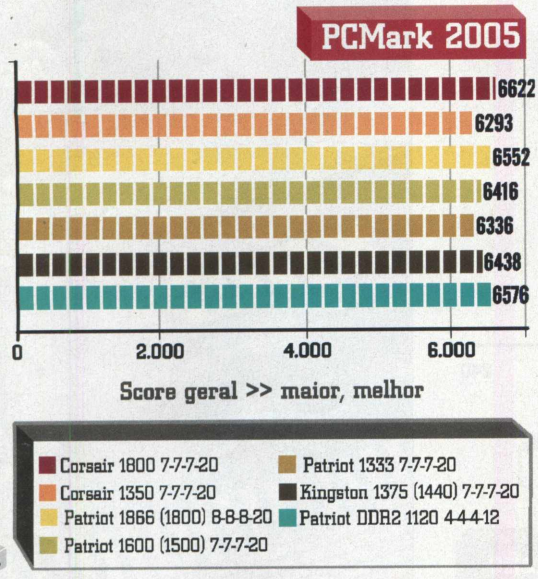
Conclusão

Os módulos DDR3 representam uma evolução natural no mercado de memórias e não há dúvidas de que vieram para ficar, pois consomem menos energia e conseqüentemente geram menos calor. Hoje o suporte a eles se restringe aos chipsets Intel P35 e X38, mas no decorrer do próximo ano devemos ver vários outros lançamentos, dentre eles a nova plataforma AM3 da AMD.

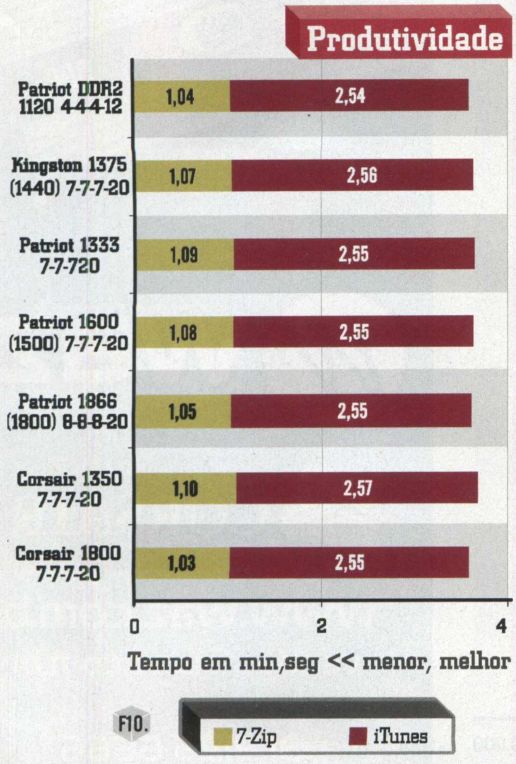
Mas neste momento sua adoção é no mínimo vista com reservas. Primeiro porque será preciso escolher a placa-mãe e o processador literalmente a dedo, sob pena de não conseguir fazer os módulos acima de 1333 MHz rodarem em sua freqüência nominal. E depois tem também a questão dos preços muito elevados em comparação com os mais disseminados DDR2, mesmo os de alta performance, como é o caso do Patriot PDC22G9200ELK avaliado na edição 73 e usado aqui como referência.

Tomando como base o site **www.newegg.com**, esse kit está sendo vendido a US$ 220, ao passo que o Corsair 1800 a US$ 574, os Patriot na faixa entre 500 e US$ 550 e o Kingston a US$ 450! Esse é o tipo de investimento que o usuário comum jamais entenderia como sendo viável. Em contrapartida, para os entusiastas que buscam simplesmente a máxima performance e estejam em vias de investir em um novo sistema, seguramente vale a pena ir logo de DDR3.

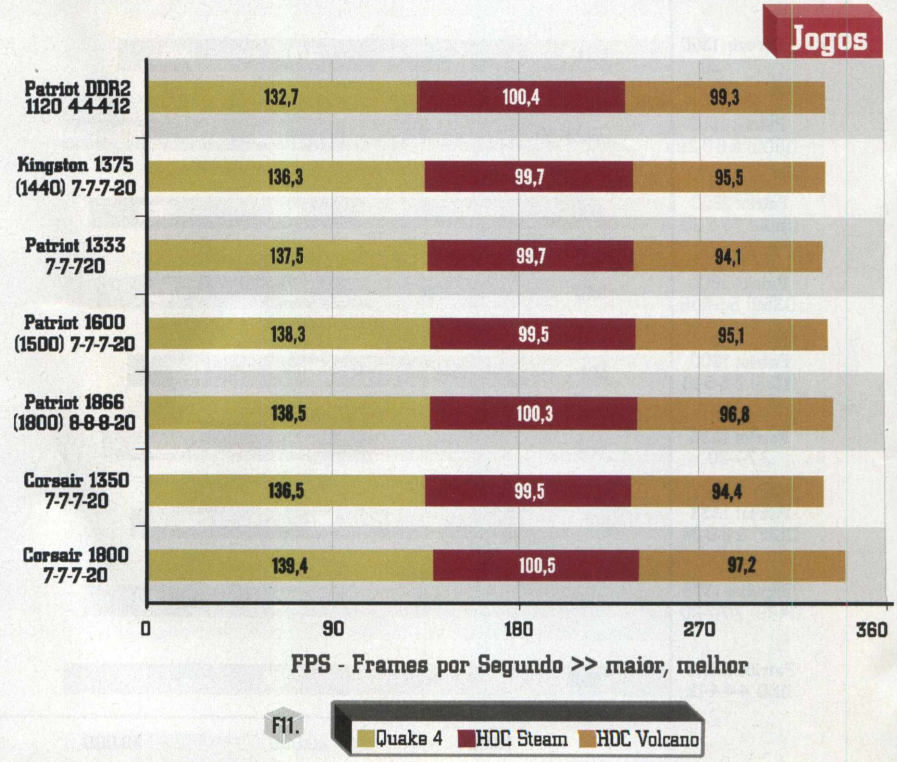
PC



F9.



F10.



F11.

Testes

Placas de vídeo DX10 para a massa

Maior performance e estabilidade, é isso o que se espera de novas versões de drivers. Sobretudo no segmento de placas de vídeo, que teve de lidar com duas grandes mudanças, a primeira com a nova arquitetura de shaders unificados e a segunda com a chegada do Windows Vista e sua API gráfica DirectX10. Nesta matéria, veremos se a nVidia e a AMD conseguiram acrescentar algo de novo às suas placas intermediárias, respectivamente das famílias GeForce 8600 e Radeon 2600.

Fernado Ramos da Silva

As placas

A primeira placa avaliada foi a Radeon HD 2600Pro IceQ Turbo da HIS (**www.hisdigital.com/html/product_ov.php?id=312&view=yes**), que segundo o fabricante tem o preço sugerido no Brasil de R$ 350. A se confirmar este valor no ponto de venda, seguramente será o modelo intermediário de custo mais acessível, uma legítima proposta de DirectX 10 para o grande público. Por outro lado, contudo, pairam dúvidas sobre a performance computacional deste projeto. Conforme testes publicados em nossas edições anteriores, esta família 2600 da AMD tem um desempenho 3D sofrível em jogos DX10, e mesmo nos DX9 deixa a desejar em relação à geração anterior de placas. Será que o driver mais recente mudou isso?

Falando especificamente desta placa da HIS, as freqüências de operação são ligeiramente superiores ao projeto de referência da AMD para um processador gráfico (GPU) 2600Pro. Enquanto neste o GPU e as memórias operam a 600 MHz e 1GHz DDR, respectivamente, nesta HIS as freqüências são de 650 MHz e 1050 MHz. Daí a alusão ao "Turbo" no nome do produto; o IceQ, por sua vez, nos faz pensar em baixas temperaturas, o que de fato se comprovou.

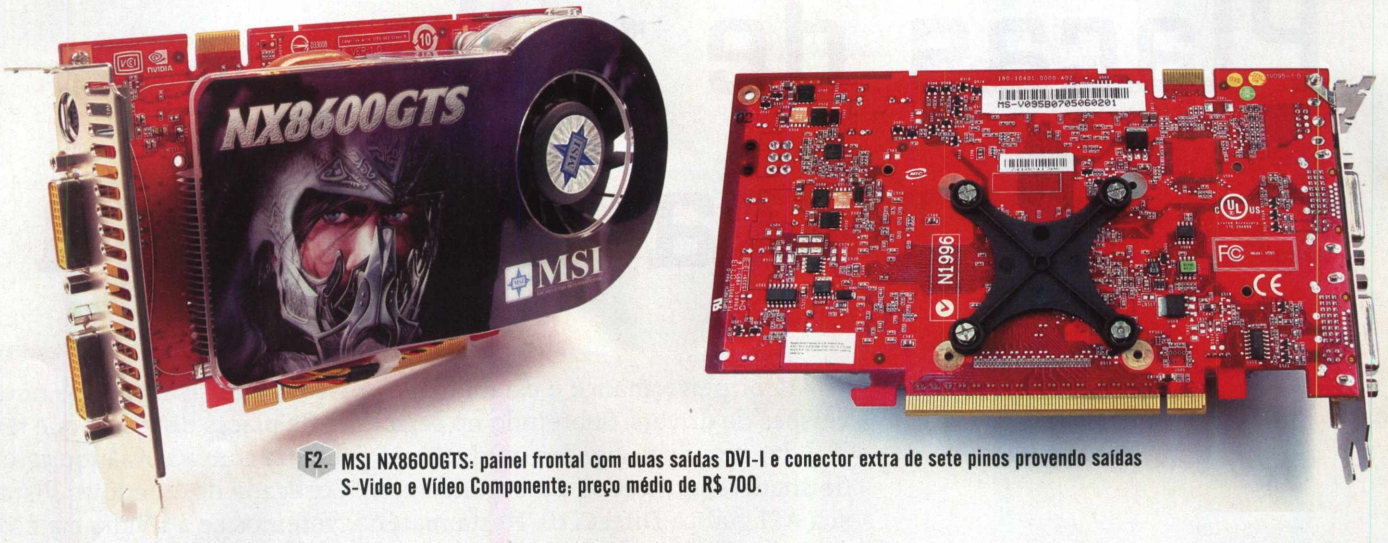
Com temperatura ambiente de 26 °C, o GPU inicia a operação a 35 °C e conclui uma bateria de testes de 1 hora, com o 3DMark, a 45 °C. E o melhor é que sua ventoinha é muito silenciosa, uma proposta perfeita para um HTPC (PC Home Theater).

O segredo é o baixo consumo de energia do GPU, fabricado num processo de manufatura de 65 nanômetros (nm). A qualidade do projeto térmico da placa e a capacidade de overclock do 2600Pro foram aferidas ao conseguirmos uma operação estável com o GPU a 750 MHz e os 256 MB de memórias DDR2 a 1100 MHz. O acréscimo de temperatura foi mínimo, de apenas 1 °C.

Sua oponente neste comparativo foi a NX8600GTS T2D256E OC Edition da MSI, um modelo que apesar de ser classificado como intermediário, representa o modelo topo de linha da série da nVidia. No caso da 2600Pro, a AMD tem um superior na série,



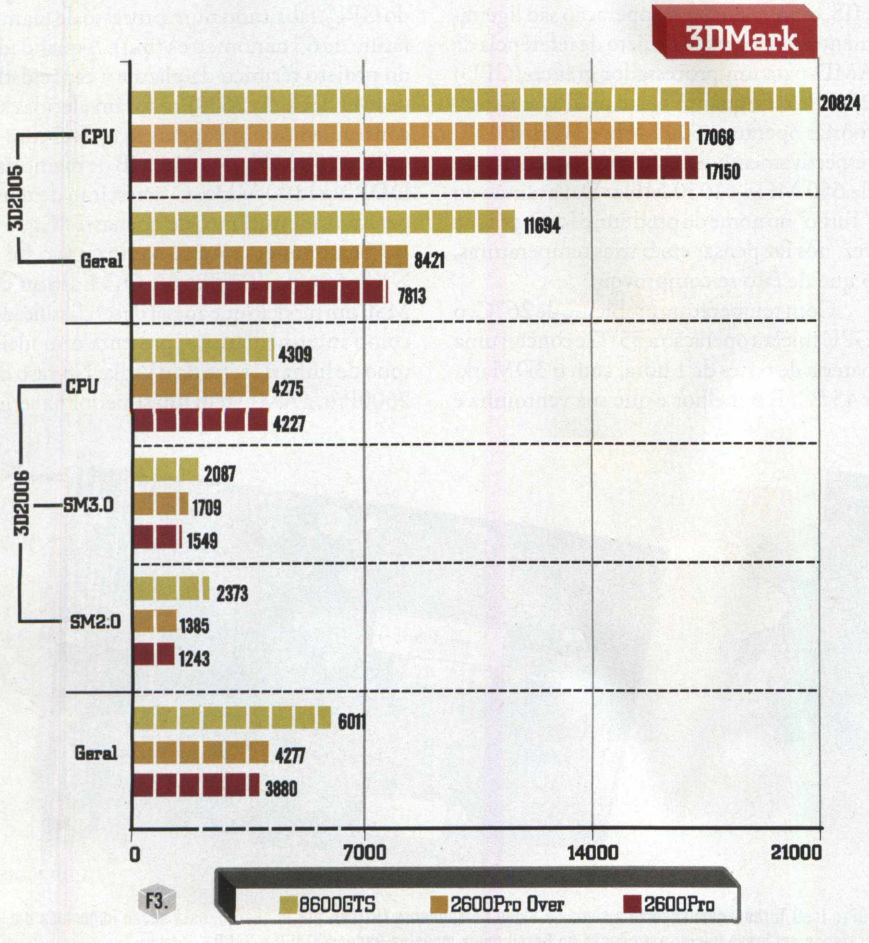
F1. HIS HD 2600Pro IceQ Turbo - sem suporte a saída de Vídeo Componente (HDTV); por enquanto, está sendo importada e o fabricante pretende em breve iniciar a produção no Brasil pelos modelos Radeon X1550 e 2400.



F2. MSI NX8600GTS: painel frontal com duas saídas DVI-I e conector extra de sete pinos provendo saídas S-Video e Vídeo Componente; preço médio de R$ 700.

que é o 2600XT. O projeto da MSI também é ligeiramente superior ao de referência. O GPU e os 256MB de RAM DDR3 operam a 700 e 2100 MHz, enquanto o projeto de referência especifica 675/2000 MHz. Vale lembrar que as arquiteturas da AMD e da nVidia se diferenciam bastante no que diz respeito à quantidade de unidades de processamento integradas (os chamados Stream Processors - SP) e sua freqüência de operação. Enquanto no 2600Pro há 120SP's operando na mesma freqüência dos demais circuitos existentes no GPU, no 8600GTS há apenas 32 SP's, mas operando a uma freqüência muito mais elevada – 1,45 GHz.

Ainda produzido no processo de 80nm, o 8600 GTS consome mais energia que a 2600Pro. As suspeitas levantadas pela presença de um conector auxiliar de alimentação de seis pinos, na lateral direita da placa, se confirmam quando ligamos a máquina e o ruído de sua ventoinha começa a incomodar. Mesmo em 2D e sem qualquer programa carregado. Mais adiante falaremos das medições de consumo realizadas. Para finalizar, vale destacar o conector adicional para o suporte ao SLI e sua configuração multi-GPU, e o fato da placa ocupar lateralmente o espaço de dois slots. Semelhantemente à 2600Pro da HIS.



F3.

Testes

O sistema base utilizado tinha um processador Core 2 Quad Q6600 operando em overclock para 3 GHz, via FSB de 333 MHz, e 2 GB de memórias Patriot operando em Dual-Channel a 1333 MHz com latências 8-8-8-20, instalados na placa-mãe MSI P35 Diamond, com revisão de BIOS 2.1.

O Windows Vista Ultimate 32 bits foi instalado em um HD WD Raptor WD740D com motor de 10.000 RPM e partição única de 74 GB. A fonte utilizada foi uma Cooler Master Real Power Pro com 1.000 Watts de potência nomimal. A Radeon rodou com a suíte de driver Catalyst 7.10 e a GeForce com o ForceWare 163.69.

No quesito estabilidade, os drivers demonstraram um amadurecimento razoável em relação ao nosso último teste. Desta vez, nada de artefatos estranhos na tela, dificuldade extra para instalação dos drivers e nem comportamento errático com softwares de *benchmarking* e alguns títulos. Todos rodaram a contento.

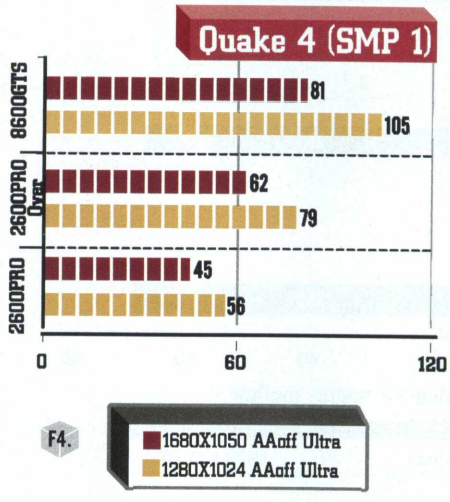
Começando pelos sintéticos 3DMark, tanto na versão 2005 quanto na 2006 a 8600 GTS sempre foi superior – e por uma boa margem. Os 15% de overclock no GPU da 2600Pro não chegaram a proporcionar 10% de ganho.

E este comportamento se repetiu na maioria dos jogos avaliados, com exceção do Quake 4. Repare na figura 4 como a 2600Pro saiu de 56 para 79 quadros por segundo (FPS) com o overclock, um acréscimo de aproximadamente 40% quando rodou com a resolução de 1280x1024.

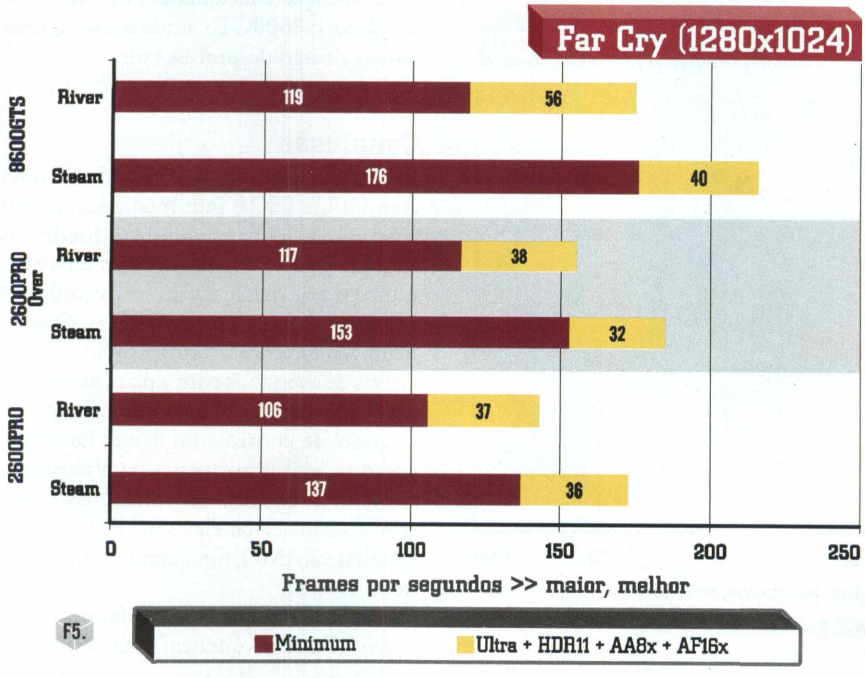
Em outro título da geração DX9, o FarCry, mais uma vez vemos a dificuldade que essas placas intermediárias enfrentam para manter uma performance adequada, quando os filtros de qualidade estão habilitados (figura 5). A 2600Pro só é viável aqui quando operando sem filtros.

Já entre os títulos DX10, tal como ocorreu em edições anteriores novamente o Call of Juarez (figura 6) e o Lost Planet (figura 7) demonstraram que nenhuma dessas placas é adequada. Nem mesmo a mais poderosa 8600GTS foi capaz de atingir a taxa de 30FPS, tida como mínima. Talvez com um overclock, mas o nTune não nos permitiu elevar a freqüência do GPU.

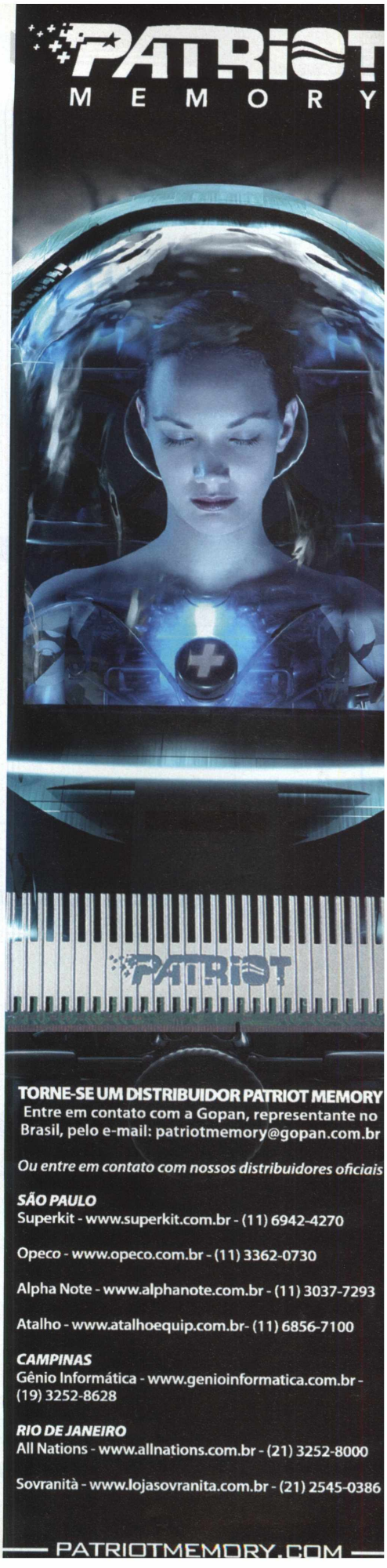
No quesito consumo de energia, realizamos duas aferições. Na primeira, ainda com esse hardware base, medimos o consumo nos estados de repouso, apenas com a área de trabalho carregada, e depois durante a execução do Game 3 do 3DMark 2005, o qual induz a máximo carga de trabalho sobre todo o sistema. Como era de se esperar pela análise feita até aqui, a 8600GTS foi diretamente responsável por um consumo de aproximadamente 10% superior. Foram 203 contra 185W durante o Game 3 e 114 a 106W, no repouso. Vale lembrar que essas medições foram feitas antes da fonte ATX, a partir do wattímetro portátil PC Power Tester, da T&C.



F4.



F5.



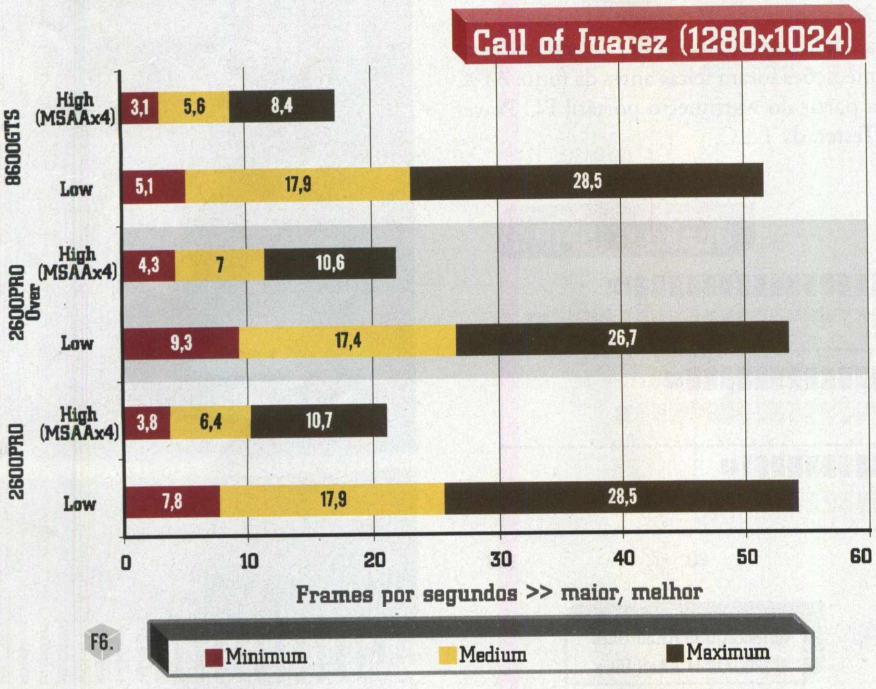
Por último, vieram os testes de reprodução de vídeo. Como sabemos, ambos os GPU's avaliados aqui são capazes de acelerar o processamento de vários formatos de vídeo, inclusive os de alta definição. Isso significa dizer que o processador principal do sistema não participa desta tarefa. Na prática, isso implica numa redução significativa do consumo de energia do sistema e nos faz pensar até em cenários inusitados, como dar vida nova a um processador já meio esquecido, a exemplo do Pentium 4 HT.

A ativação do UVD (Universal Video Decoder) e do Purevideo HD, que são os nomes dados por AMD e nVidia, respectivamente, depende do software usado como player do vídeo. No nosso caso, isso foi feito com o bom Power DVD Ultra 7.2, da Cyberlink. A caixa "mágica" fica no painel de Configurações > Video < Enable hardware acceleration (figura 8).

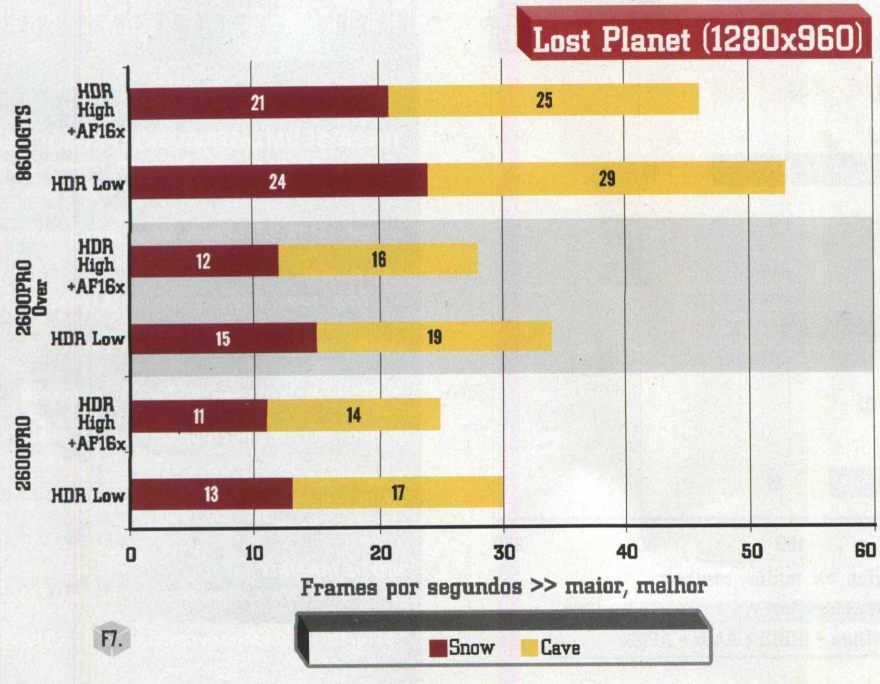
Os testes começaram com o Core 2 Quad e o vídeo usado foi o thrailer do filme "The Greatest Game Ever Player", codificado em High Definition 1080p no formato H.264, que até o momento é um dos mais utilizados para distribuição de filmes. Inicialmente desconfiamos da falta de suporte adequado do Power DVD, pois o Gerenciador de Tarefas do Vista sempre reportava uma taxa média de uso de CPU de 12%, independentemente da caixa de aceleração estar habilitada ou não.

A confirmação veio quando substituímos o processador por um Pentium 4 HT 630, de 3 GHz, e a taxa média permaneceu alta, desta vez oscilando em torno de 60%. Ao ir ao site **www.cyberlink.com/multi/download/patches_112_ENU.html**, descobrimos o patch 3104a.1 que corrigiu o problema. Os resultados estão na figura 9.

Os valores das barras Repouso, Média e Pico se referem aos momentos em que a aceleração não estava habilitada. Repare que no caso da 2600Pro o consumo de energia médio diminuiu 26,5%, enquanto para o 8600GTS, a redução foi de 23,3%. Falando em termos de uso de CPU, enquanto anteriormente víamos picos de 100% e perda de frames, após o patch o pico do P4 foi de 10% com a 2600Pro, e de 12% com a 8600GTS. Optamos por demonstrar os resultados em watts por acreditar que essa medição responda mais diretamente aos benefícios obtidos com a aceleração de vídeo pelo GPU, com reflexos diretos na dissipação de calor dentro do gabinete, dimensionamento da fonte e ruído das ventoinhas. Por último, apenas como um detalhe, vale ressaltar que a superioridade da solução da AMD neste caso deve-se ao fato do GPU participar de todas as etapas relacionadas à decodificação do vídeo; o 8600GTS ainda deixa algumas tarefas a cargo do processador.



F6.



F7.

Conclusão

Depois de mais uma rodada de testes com GPU's DX10 intermediários, o principal avanço foi na estabilidade dos drivers. Basta ir ao site dos fabricantes e baixar a última versão que sua placa será reconhecida e operará sem maiores problemas. O único inconveniente observado foi durante as tentativas de overclock com a placa 8600GTS. Depois da instalação do nTune 5.05.47.00, o painel de controle do driver Forceware passou a exibir as opções para ajuste das freqüências do GPU e das memórias, porém se recusou a aceitar elevações do GPU. Já o Catalyst, da AMD, funcionou normalmente neste aspecto.

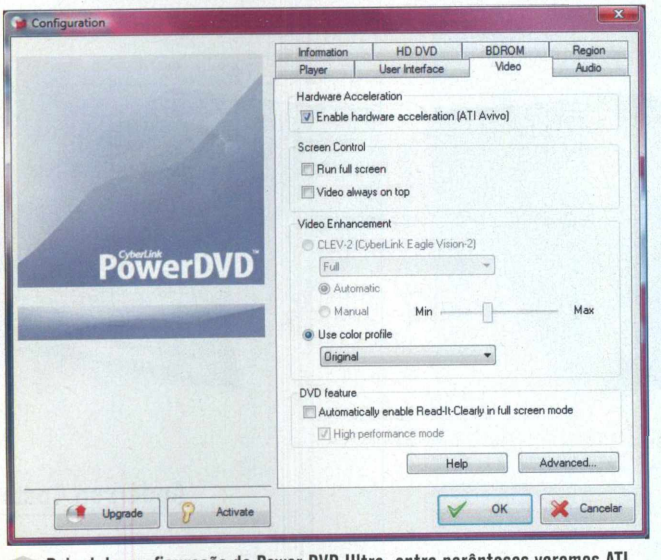
Sobre o desempenho 3D, os números falam por si só. Primeiro, que nenhuma das empresas

oferece no momento uma solução intermediária para títulos DX10. Embora a nVidia esteja melhor posicionada com a 8600GTS, nem ela foi capaz de manter uma taxa de FPS minimamente aceitável, e mesmo com filtros de qualidade desabilitados e considerando a modesta resolução de 1280x1024.

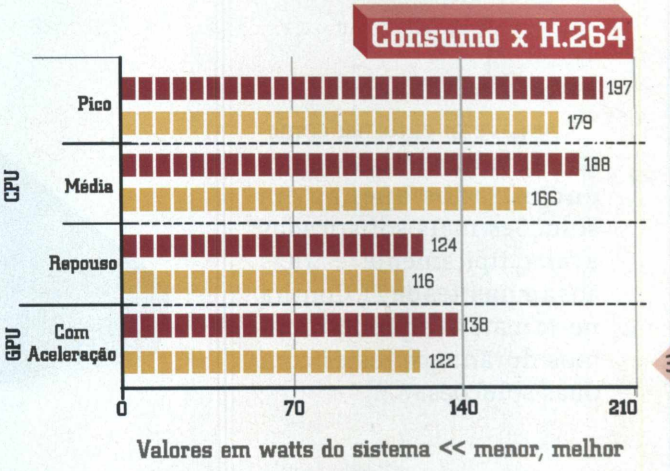
Acreditamos que esse cenário só mudará no momento em que esses projetos ganharem um barramento de memória de 256 bits (hoje, é de 128 bits em ambos) e uma maior quantidade de Stream Processors.

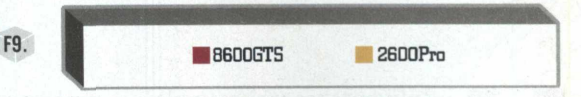
Já para títulos DX9, como Quake 4 e Far Cry, a 8600GTS pode ser considerada uma placa razoável. A 2600Pro, por sua vez, especialmente com esse projeto da HIS, é uma solução de bom custo/benefício para o usuário que é jogador casual e busca um upgrade para um vídeo integrado com uma placa relativamente barata. Também pesam a favor dela o baixo consumo de energia, o ruído praticamente imperceptível e o melhor desempenho para aceleração de vídeo de alta definição. Para as necessidades de um HTPC, é uma ótima solução (figura 10).

PC

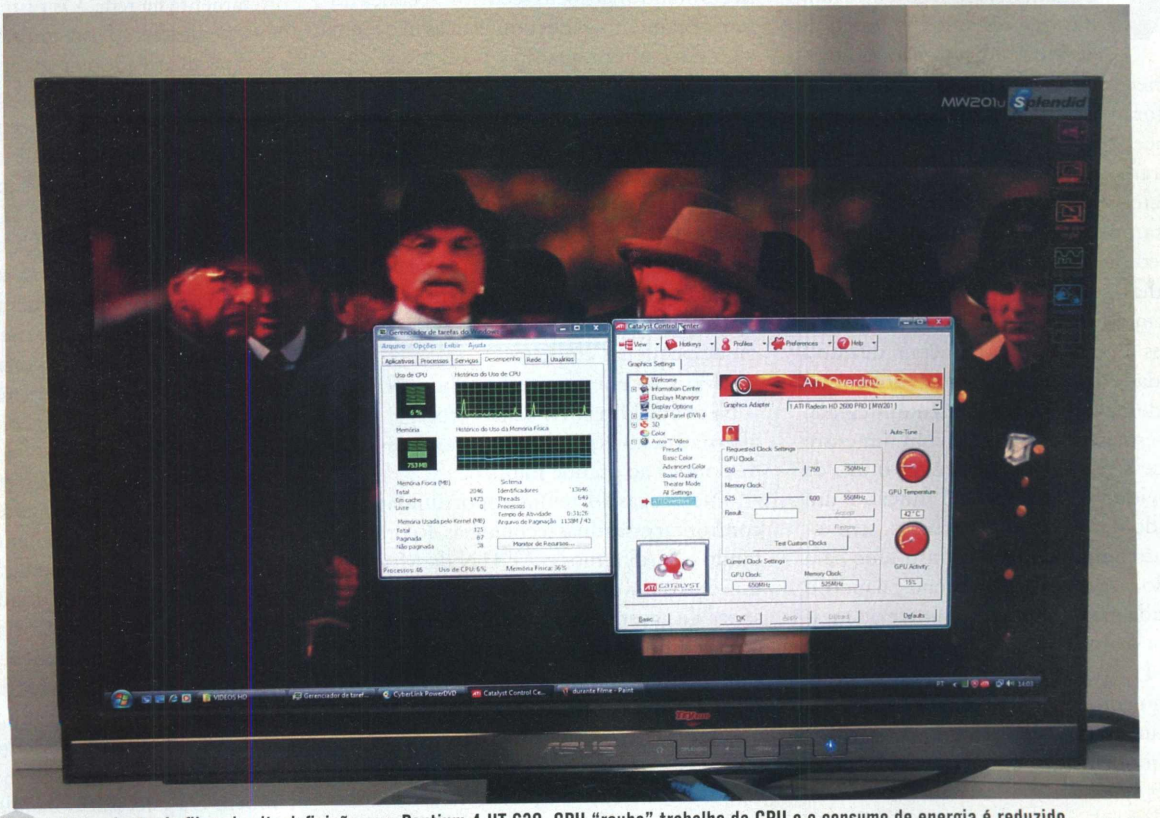


F8. Painel de configuração do Power DVD Ultra: entre parênteses veremos ATI Avivo ou NVIDIA Purevideo, de acordo com o hardware instalado.





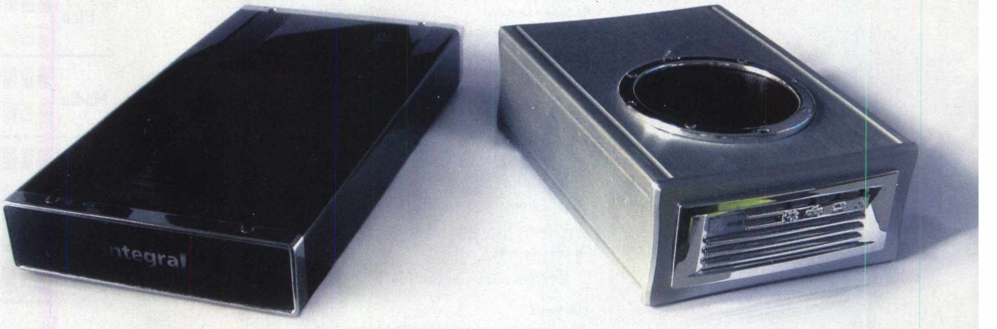
F9.



F10. Reprodução de filme de alta definição com Pentium 4 HT 630: GPU "rouba" trabalho da CPU e o consumo de energia é reduzido.

Gavetas Externas
com suporte a NAS e NDAS

As gavetas externas começam a oferecer recursos antes encontrados apenas em soluções mais sofisticadas e caras, tipicamente restritas aos ambientes de TI. Confira nesta matéria o que descobrimos durante os testes com duas soluções.



Anderson Costa

Nos últimos anos, várias tecnologias deram saltos quantitativos e qualitativos. As gavetas externas que testamos ao longo de algumas edições não são produtos necessariamente novos, mas apenas agora foram popularizados. Elas passaram a oferecer recursos que até pouco tempo atrás eram caros e de uso restrito, devido às características da aplicação.

Citamos como exemplo os Network Attached Storage, ou simplesmente NAS. Em linhas gerais, eles são dispositivos de rede com a função primária de armazenar arquivos. Estas soluções nasceram devido à necessidade de se ter um meio de armazenamento de dados na rede facilmente integrado à infra-estrutura existente e com um custo mais acessível. Em alguns casos, o uso de um servidor apenas para tal função é um tremendo desperdício de recursos, sem esquecer do tempo que seria consumido para "deixá-lo no ponto". Visualmente falando, o NAS nada mais é que um gabinete ou mesmo uma "caixa" com HDs e uma porta de rede RJ45, contando com uma interface de gerenciamento, disponível através do software de administração, ou via web browser.

Os modelos disponíveis tinham configurações agressivas demais para um usuário doméstico, tal como suporte a vários HDs e também operação em RAID. Assim, apenas empresas acabavam desfrutando (ou mesmo necessitando) dos seus recursos. À época do seu lançamento, redes domésticas não eram algo tão comum quanto é hoje.

Com a popularização de diversas tecnologias co-relacionadas ao "ecossistema" de operação de um NAS, não tardaria para que ele estivesse disponível para as massas. E foi o que ocorreu, ao surgir os primeiros modelos de gavetas externas que, além das portas USB, também oferecem o NAS integrado, claro que devidamente dimensionado às necessidades de uso doméstico ou de pequenas empresas.

Mais recentemente, surgiu o NDAS – Network Direct Attached Storage, uma alternativa ao NAS, que hoje também está disponível ao grande público.

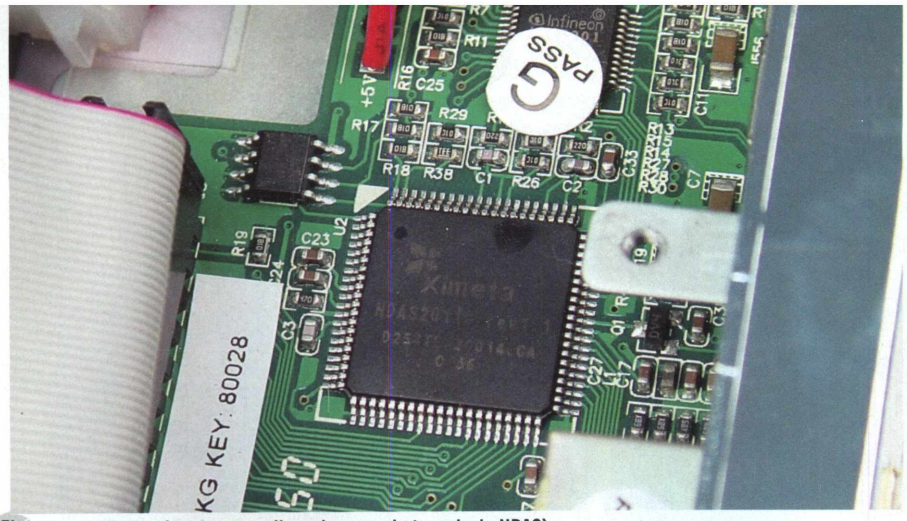
Nessa ocasião, temos a oportunidade de confrontar essas duas tecnologias. Representando o NAS temos o AE31N da Mexton, um derivado do AE31F, uma das poucas séries de gavetas externas que contam com uma ventoinha para auxiliar na refrigeração (um apelo de venda e tanto). O NDAS é representado pelo Integral P2N da Akasa, que faz parte da sua nova safra de gavetas. Mas antes de apresentar os produtos, vamos a uma explanação sobre essas duas tecnologias.

NAS

Foi o primeiro a oferecer armazenamento diretamente na rede. Os primeiros modelos eram dedicados ao uso empresarial, e graças a essa peculiaridade ofereciam recursos compatíveis com esse perfil, como suporte a vários discos e também operação em RAID e *hot swap* (desde que o hardware necessário seja integrado ao sistema). Ele suportava outros protocolos de rede além do TCP/IP, como o IPX da Novell e o NetBEUI da Microsoft.

Embora o TCP/IP seja um protocolo bem antigo e muito maduro, sua utilização só cresceu com o *boom* da internet. Antes disso, os ambientes de rede locais eram dominados pelo IPX da Novell com o seu Netware e de uma maneira mais tímida com o NetBEUI para redes Windows.

O gerenciamento dos recursos, ou seja, a administração propriamente dita, era feita por meio de um software cliente que poderia ser instalado em qualquer estação conectada à rede (preferencialmente a do administrador). O software continha as informações sobre o protocolo utilizado e as funções necessárias à administração. Através dele é feito o controle de acesso, cotas de uso, monitoramento, dentre outras opções. Evidentemente, para que os usuários tivessem acesso ao conteúdo, também era necessário instalar o software cliente em cada uma das estações.



F1. Chip da Ximeta (empresa que licencia o uso da tecnologia NDAS) na placa de controle do Integral P2N.

O software cliente era uma necessidade por causa das características dos protocolos de rede IPX e NetBEUI. Já com o TCP/IP, evidentemente poderia ser utilizado um software, porém ele naturalmente oferece uma versatilidade maior, já que se a rede já o utiliza, o acesso poderia ser feito a partir de qualquer estação com um web browser instalado, dispensando a instalação de outro software.

No caso de uma rede que usa TCP/IP como padrão, o acesso ao compartilhamento é transparente, feito como se fosse uma estação comum, basta achar o nome do "computador" e fazer o mapeamento. O controle de acesso, conforme a sofisticação do NAS, pode ser feito em nível de usuário ou, mais comumente, a nível de compartilhamento.

Atualmente podemos até segmentar os produtos NAS em versões corporativo e doméstico. O corporativo é naturalmente mais robusto, oferecendo recursos sofisticados como uma controladora RAID independente com suporte a hot-swap, compatibilidade com diversos protocolos de rede e interfaces, formatos de sistema de arquivos e integração com serviços de diretório. Alguns mais poderosos são dotados de sistemas operacionais completos, usando alguma distribuição Linux, ou mesmo Windows Server. Um exemplo é a linha NAS da Iomega, que oferece modelos com Linux ou Windows 2000 Server.

Já o doméstico é mais simples, geralmente limitado ao protocolo TCP/IP e ao compartilhamento de arquivos via SMB. A compatibilidade com sistemas de arquivos é limitada, suportando apenas o FAT, mas não deixa de agregar outros recursos interessantes para usuários e até mesmo pequenas empresas. Pode oferecer servidor DHCP, cliente PPPoE para conexão à Internet, servidor FTP, DNS dinâmico, suporte a *queue* torrents, dentre outros.

NDAS

NDAS é um alternativa da Ximeta ao NAS, que procura oferecer melhor segurança, performance, escalabilidade, integração e operação facilitada (figura 1). De acordo com a Ximeta, o NDAS dispensa qualquer tipo de configuração de rede, bem como conhecimento acerca disso. Sendo mais preciso, ele nem mesmo precisa que o TCP/IP esteja instalado nas estações que terão acesso a ele.

Um dos recursos que "de cara" chamam a atenção no NDAS é a capacidade de operação em RAID 0 e 1, e também agregação, que nada mais é que um agrupamento de HDs, formando apenas uma única unidade de maior capacidade. A grosso modo, a agregação é um RAID, entretanto sem o "R".

Ao contrário do NAS, que é acessado como um compartilhamento de rede, as unidades NDAS são disponibilizadas como se fossem unidades físicas, o que também proporciona um outro benefício muito apreciado: a possibilidade de se utilizar qualquer sistema de arquivos. Tal capacidade significa que podemos nos cercar com mais recursos de segurança, oriundos do sistema de arquivos escolhido.

A grosso modo, podemos considerar incrível o modo de operação do NDAS, "sem" protocolo de rede e muito menos configurações adicionais. Mas todo "milagre" em TI tem uma explicação: a conexão de rede é feita através de um outro protocolo de rede embutido no software cliente, o LPX – *Lean Packet Exchange Protocol for NDAS Devices*, e para que o sistema reconheça a gaveta NDAS como se fosse um HD qualquer, é utilizado um *miniport* driver com base no padrão de interface SCSI, que faz a intermediação entre a interface do sistema e a rede, de modo transparente ao usuário.

Fica a impressão de que está acessando um HD local. Essa interface SCSI que será instalada no sistema é encarada como um dispositivo removível, como os demais dispositivos "pendurados", explicando a presença do ícone de dispositivos removíveis na bandeja do Windows.

O controle de acesso é garantido pelo processo de configuração, o qual exige a utilização de um número de identificação para o registro do dispositivo. Cada unidade vem com um número e o acesso num primeiro momento é liberado apenas para leitura. Para liberar a gravação é necessário entrar com a chave.

Outra característica alardeada pela Ximeta é que o dispositivo NDAS dispensa atualização de firmware, com o claro objetivo de facilitar a vida do usuário comum. Segundo a empresa, apenas o software de gerenciamento recebe atualizações. Com as devidas configurações, o NDAS apresentará uma performance maior quando comparado ao NDAS, e de certa forma, segurança também.

Mexton AE31N

O AE31N é dotado de um sistema NAS bem simples, baseado em Posix (a base do Linux) e limitado (figura 2). No entanto, é bem fácil de usar. Seu sistema é compatível apenas com redes TCP/IP, o que significa dizer que seu programa de configuração/administração é acessado via web browser, devidamente protegido por senha de acesso. Os recursos oferecidos são o SMB, o DHCP e o FTP. O SMB nada mais é que o Samba, tão conhecido da turma do pingüim, que provê o compartilhamento de arquivos.

Obviamente, com o TCP/IP e o Samba, a interoperabilidade numa rede mista, com sistemas Linux e Windows, está garantida, de modo fácil e transparente. Do modo como o SMB foi implementado, o acesso é feito no nível de compartilhamento, que não oferece um bom nível de segurança. Entretanto, não permite que a senha de acesso seja salva no cliente para uso posterior.

Na unidade testada, nem mesmo com mapeamento a senha era gravada na estação, na verdade ela é apagada a cada reinicialização do sistema. O mapeamento era possível mesmo sem senha, porém a senha era solicitada no primeiro acesso. Tal ação é um tanto chata, porém necessária para prover maior segurança no acesso aos dados. Imagine ter a senha salva numa estação qualquer e algum usuário apagar dados ou alterá-los.

O DHCP dispensa maiores apresentações, porém a sua capacidade de identificar a presença de um outro servidor DHCP na





F2. Mexton AE31N LAN: suporte ao NAS e cotação média de R$ 360.

rede antes de inicializar o serviço, é digna de nota. Por fim, o FTP permite o acesso a nível de usuário, sendo mais seguro que o SMB. Se por alguma razão o Samba da estação cliente baseada em Linux não conseguir se conectar, o acesso aos dados ainda é possível pelo FTP. Não há uma divisão entre dados acessados via SMB ou FTP, eles são os mesmos, apenas os modos de acesso são diferentes.

O SMB é o único dos recursos que não pode ser desativado. O DHCP e o FTP já vêm inclusive desativados por padrão, a fim de evitar conflitos na rede, caso esses recursos já estejam disponíveis.

A interface de configuração/administração é espartana. Ela é dividida em duas colunas, a da esquerda com os menus e a da direita exibindo as opções referentes ao menu escolhido. São seis menus objetivos: Status, IP Config, Maintenance, SMB Server, FTP Server e Disk Utility.

Tipicamente *Status* serve para exibir informações, mas no AE31N ele vai um pouco além, concentrando o acesso de algumas configurações de rede (nome e grupo do dispositivo, senha do administrador e inicialização do servidor DHCP), bem como outras, como ajuste de data/hora, alteração da senha do administrador, idioma (infelizmente nenhum português – Brasileiro ou Portugal - está disponível), versão do firmware e informações do HD utilizado (modelo, tamanho total e livre).

IP Config é literal: define se o endereço IP é atribuído por DHCP ou manual. *Maintenance* abriga a opção de atualização de firmware, reboot do sistema e restauração dos padrões de fábrica. *SMB server* é composto por duas "caixas", em uma definimos as pastas que existem no AE31N, e na outra definimos quais são compartilhadas e suas respectivas senhas. Quando uma pasta é compartilhada e protegida por senha, ao lado do nome haverá um asterisco. Por padrão é criada uma pasta chamada PUBLIC, sendo compartilhada sem senha.

FTP server é mais sofisticado, abrigando todas as operações co-relacionadas a ele, da execução e porta utilizada, definição do nível de acesso de cada usuário e características do acesso anônimo. As opções de configuração são as mesmas para ambos: se o acesso é autorizado ou não, e se é de leitura ou leitura/gravação.

Por fim, temos a Disk Utility, que abriga *Format Disk*, *Sleep Time* (pode ser desativado, ou configurado entre 5 e 60 minutos) e *Scan Disk*, que realiza um teste simples de varredura e depois informa o resultado, como quantidade de arquivos e pastas, tempo consumido pela operação e erros encontrados.

O uso do AE31N é bem simples. Ele será "enxergado" na rede como se fosse uma estação Windows com arquivos compartilhados. Basta conectá-lo a uma porta livre do switch/hub. O seu cliente DHCP age quase que instantaneamente, deixando-o disponível para as estações de imediato.

O acesso às suas pastas é feito como se fosse um compartilhamento de uma estação Windows: localize-o no Ambiente de Rede/Meus locais de rede e clique nele para visualizar as pastas. Se configurarmos o recurso DMZ do roteador, ou se este prover um recurso normalmente conhecido como "servidores virtuais", o AE31N pode disponibilizar seus dados diretamente na internet.

A fraqueza do AE31N reside na atualização das seções FTP e de administração. No FTP é apenas um contratempo quando o acesso é feito via web browser. O problema acontece quando dois usuários com atributos diferentes fazem o acesso a partir de uma mesma estação, dentro de um intervalo de cinco minutos. Por exemplo, o usuário X tem atributo de leitura/gravação e o Y apenas de leitura. Se X acessou antes o FTP, Y poderá ver todas as pastas e o conteúdo também, se alguma estiver aberta. Mesmo ao fechar o browser a seção não é encerrada, só após cinco minutos de inatividade. Para evitar que isso aconteça, ou seja, forçar o encerramento, basta ir até a pasta raiz e clicar no link para acessar um nível acima, o qual não existe. Essa condição de erro provoca o encerramento da seção e evita o acesso não autorizado.

Já na Administração, o problema é um pouco mais sério, porque simplesmente a seção não expira. Logo, se o administrador acessar a área de administração a partir de qualquer máquina e esquecer de fechar o browser (ação suficiente para encerrar a seção), existe o risco de algum "engraçadinho" causar problemas.

O fator limitante do AE31N é o sistema de arquivos, já que apenas o FAT é suportado. Nem adianta conectar o HD diretamente a uma interface IDE ou USB, usar o gerenciamento de disco do Windows ou qualquer outra ferramenta de disco. Um indicativo é que no status do HD, no módulo de administração, nada além da marca será exibido e as informações sobre tamanho não estarão disponíveis.



F3. Integral P2N LAN: "servidor" de compartilhamento de dados na LAN cotado a R$ 340, em média.

Akasa Integral P2N

O NDAS é um sistema proprietário criado pela Ximeta, que licencia o uso para outros fabricantes, que é o caso do Integral P2N (figura 3). De certa maneira, o Integral P2N (e possivelmente qualquer outra gaveta que use NDAS) apresenta um processo de instalação bem mais simples do que qualquer NAS, que no caso do Windows pode ser resumido no famoso *Next, Next, Finish*.

O acesso aos dados é muito simples, já que o compartilhamento será exibido como mais um HD instalado no sistema. Entretanto, apesar de sua configuração não ser difícil, é preciso tomar cuidado com alguns detalhes. Por padrão, após conectá-lo a rede, devemos instalar o software.

O software que acompanha o CD apresentou diversos problemas, desde não reconhecer as unidades instaladas até demandar um tempo considerável para preparar um arranjo RAID com dois HDs. No site da Akasa de Taiwan, havia um versão mais recente do software que resolveu todos esses problemas, sem falar da melhora considerável da qualidade da interface, que antes era grosseira e ficou com um visual profissional.

De qualquer forma, também testamos a versão disponível no site da Ximeta, para verificar se era compatível com o NDAS de terceiros ou apenas com os fabricados por eles mesmos. Por sorte são compatíveis, ou melhor, é o mesmo, considerando que a versão do site da Akasa era a 3.11 e no site da Ximeta, além dessa havia a 3.20, que acabamos por adotar nos testes definitivos.

Após o *Next, Next, Finish* da instalação, talvez seja necessário reiniciar o computador para finalizar a instalação dos demais drivers. Reiniciado o sistema, o Gerenciador do NDAS (*NDAS Device Management*) é disponibilizado na bandeja do Windows. Caso ele seja fechado por qualquer motivo, não se preocupe, pois ele também está disponível no menu Iniciar > Programas, junto com um outro utilitário, o *NDAS Bind Management*.

Ao utilizar em modo padrão, ou seja, sem recursos de agregação ou RAID, apenas o Gerenciador será utilizado. O Bind só é necessário quando for utilizar a agregação ou RAID, pois ele é o responsável pela configuração desses modos de funcionamento.

O gerenciador também mostra o status de cada gaveta, indicando se está apenas conectado, montado para leitura ou leitura/gravação, etc. A indicação é feita por meio de um quadrado colorido na frente do nome da gaveta correspondente.

Independente de como as gavetas NDAS operarão, o processo de configuração sempre começará pelo registro de cada dispositivo que será utilizado na rede. Localize na bandeja do Windows o ícone do Gerenciador do NDAS, clique e selecione a opção Register New Device.

Como dissemos, cada dispositivo NDAS tem um número ID para registro, necessário para possibilitar sua identificação pelo software, e também uma chave, que permitirá operações de gravação. Pense que o número ID está para o LPX, o protocolo do NDAS, como o endereço IP está para o TCP/IP.

Ao clicar em Register New Device, será aberta a janela do assistente, onde definimos o nome do dispositivo, que por padrão é NDAS Device 1, e na seguinte o número ID, e se desejar a chave para liberar a gravação. No caso do Integral P2N, o número ID e a respectiva chave estão localizados em uma etiqueta, presente na embalagem do CD de instalação. Por último, temos de definir o modo de "montagem" do dispositivo, se leitura/gravação, apenas leitura ou simplesmente não disponível. Feito isso o assistente concluirá a operação

Se for a primeira utilização do dispositivo, serão instalados os drivers necessários para o seu funcionamento, de modo similar à instalação de qualquer outro dispositivo de hardware, com direito a assistente de instalação e tudo mais. Basta usar o velho esquema *Next, Next, Finish* sem qualquer preocupação com a instalação. Nas demais vezes esse processo será desnecessário, porque os drivers já estarão no sistema. Esses drivers não são assinados, e por isso a mensagem "terrorista" da Microsoft vai ser exibida, mas é possível continuar sem problemas.

Optando por utilizar a gaveta para armazenamento simples, ou seja, sem qualquer recurso adicional oferecido pelo NDAS, o trabalho está finalizado. No máximo será necessário particionar e formatar o HD através do Windows. Para adicionar mais gavetas, repita o processo para cada uma delas.

Um detalhe importante diz respeito à chave de permissão de escrita na gaveta. Mesmo que ela seja inserida durante o registro, estará apenas "presente" e não necessariamente "ativa". Mesmo com a presença dela, podemos montar a gaveta em modo somente leitura. Selecione a gaveta a partir do gerenciador e logo após a opção *Mount (Read-only)*. Para mudar para o modo de leitura/gravação, é necessário desmontar (*dismount*, ou *umount*, conforme a versão do software utilizado) e

depois montar novamente com a opção Mount (Read/Write). Em tempo: essa chave pode ser inserida ou removida a qualquer momento, a partir do gerenciador do NDAS.

O processo de instalação e registro das gavetas deve ser feito em todas as estações que terão acesso a ela, seja apenas para leitura ou para leitura/gravação. Considerando apenas o uso de uma unidade, esse trabalho pode ser considerado um tanto dispendioso. Porém, quando se usa mais de uma unidade para, por exemplo, separar os arquivos de cada seção de uma empresa, o trabalho compensa pelo benefício da organização dos arquivos. Todas podem estar disponíveis a todos os setores co-relacionados, montadas apenas para leitura e evidentemente sem a chave para se ter maior segurança. Bastaria colocar a chave nos equipamentos do setor que produz a informação.

Bind Management

Só será empregado se utilizarmos alguma funcionalidade avançada do NDAS, como a agregação e o RAID 0 e 1. Com quaisquer dessas opções, é necessário empregar no mínimo duas gavetas. Durante esse processo de configuração, nenhuma estação deve estar conectada às gavetas. Na pior das hipóteses, isole-as da rede, deixando apenas a estação que será usada para a configuração.

A instalação é igual ao o processo descrito anteriormente, sendo necessário estar com o status *online*, ou seja, reconhecido pelo sistema, mas sem estar montado. Finalizada a instalação, devemos abrir a interface do software Bind Management, que é simples, contando apenas com uma barra de botões e logo abaixo a lista de gavetas presentes no sistema, com base no nome e exibindo parte do registro de identificação, capacidade, status, status do RAID e comentários gerais. Antes de começar, observe se o Status está em *Ready*. Se sim, podemos iniciar sem problemas, caso contrário, exibindo *Online*, significa que elas ainda estão montadas.

Para iniciar a configuração, clique em *Bind* para acessar o assistente *Disk Bind* e após em next. Na janela seguinte, definimos o modo de operação, se Agregação, RAID 0 ou 1. Independente da escolha, na próxima tela selecionaremos as gavetas que farão parte do arranjo. Depois dessa etapa, é mostrado um aviso dizendo que os dados serão destruídos e, se você confirmar, o assistente finalizará o processo para a criação do arranjo. Com o arranjo pronto, basta acessar o Gerenciamento do sistema para particionar e formatar a nova unidade.



Funcionamento

Quando é utilizado o RAID 1 (espelhamento), percebemos que durante os ciclos de escrita os dados sempre serão gravados primeiro em um disco e depois em outro. Isso pode causar problemas em relação à redundância dos dados, como numa situação onde está sendo feito uma gravação de um arquivo grande e o HD "primário" sobre alguma pane, não havendo tempo para duplicar esse arquivo para o HD "secundário".

No caso de uma simples queda de energia, como desligar uma unidade (o teste que fizemos), não há problema, pois ele será executado em modo de emergência enquanto o outro HD não for ligado. E após ser religado, entra em modo de recuperação.

Performance do NDAS

A performance do acesso pode ser prejudicada por causa da performance do computador. Se este estiver sobrecarregado, o acesso poderá ficar mais lento. Isso ocorre em várias situações e com diferentes softwares, mas é especialmente problemático para o NDAS, já que todo o acesso depende de um software que não faz parte do sistema operacional. E como todo componente acessório, ele competirá pelos recursos do sistema. Não há um limite quanto ao número de usuários que podem ser conectados ao NDAS, mas exatamente por questões de performance a Ximeta recomenda 16 conexões simultâneas.

Diagnóstico

Por melhor que seja o produto, sempre pode existir algum tipo de problema ou contratempo. Começando pelo AE31N, o problema básico é não ser localizado na rede. São três soluções possíveis: verificar a configuração do IP, atualizar o Java Runtime ou atualizar o firmware. A grande questão é: como achá-lo se os utilitários de rede não são capazes de identificá-lo, e se pela interface USB tal operação não funciona? Se com a atualização do Java ele voltar a funcionar, ótimo, porém como fica se não solucionar?

No CD de instalação, há o software de atualização de firmware. Além de fazer a operação, ele também informa o nome e o IP da gaveta. A partir daí, podemos diretamente atualizar o firmware ou tentar o acesso via browser. Caso nenhuma delas funcione, possivelmente há algum defeito na unidade.

Agora, o Integral P2. Devido às características do NDAS, todos os problemas que podem ocorrer basicamente são resolvidos com a atualização do software. Se não resolver, a unidade pode estar com algum problema que demande a troca.

Conclusão

Essencialmente todo produto evolui, de um jeito ou de outro. Caso contrário, o destino dele é único: o desuso. A atual demanda de armazenamento móvel é por maior capacidade e versatilidade no uso, coisa que várias gavetas oferecem hoje em dia. É claro que a performance também não deve ser deixada de lado. E há opção para todos os gostos, necessidades e, sobretudo, bolsos.

As gavetas com recursos de LAN, seja NAS ou NDAS, apresentam-se como uma alternativa prática para as situações onde é preciso armazenamento compartilhado de um modo simples, não demandando horas de configuração.

É claro que tais modelos não oferecem grande sofisticação, se comparados com versões mais poderosas (e também mais caras), porém são uma opção viável para aplicações que prezem pela facilidade de uso e versatilidade de aplicação, com um custo acessível e rápida *instalação.* **PC**

Certificação Microsoft MCTS Parte 4

Nesta edição chegamos à quarta parte da série que visa a prepará-lo para o exame de certificação 70-620. Desta vez, finalizamos a abordagem sobre segurança, mostrando as configurações avançadas do Internet Explorer 7 e do novo Windows Firewall, que foi totalmente reescrito e possui algumas opções novas.

Igor Humberto
Paulo Sant' anna

A evolução

Ainda lembramos da época em que era necessário fazer o trabalho da escola na folha de papel almaço, onde havia uma margem que tinha de ser preparada. Além disso, uma pesquisa deveria ser baseada nas informações encontradas em livros e revistas. Figuras em um trabalho? Só se fosse de uma revista, pois não era possível recortar os livros da biblioteca.

Com as tecnologias disponíveis atualmente, para fazer um simples trabalho escolar só precisamos de uma única ferramenta denominada Internet. Agora, eventualmente temos a impressão de que a informática veio para resolver problemas que, sem ela, não existiriam. É possível perceber como isso é verdade quando nos lembramos dos diversos tipos de ameaças a que estamos expostos quando entramos nessa grande rede. Ou seja, a Internet nos entrega aquilo que queremos e também o indesejável.

Como se defender?

Pensando na plataforma Microsoft, até um tempo atrás só era possível contar com o Internet Explorer 6 (IE6). Apesar de atender às necessidades de navegação diária, ele apresentava uma série de deficiências que acabavam por nos deixar expostos na Internet. Podemos afirmar que novos tipos de ataques foram desenvolvidos e, assim, o usuário acabava caindo em diversas armadilhas.

Com o Service Pack 2 (SP2) do Windows XP, o IE6 ganhou diversas funcionalidades que visavam proteger o usuário desses novos métodos de ataque. Mas, o IE6 não era capaz de proteger completamente o usuário. É verdade que é melhor trabalhar com os novos recursos de segurança oferecidos pelo SP2 do que sem eles, mas faltavam ferramentas para proteger o usuário. Além disso, o sistema também sentia a falta de novos recursos para melhorar a navegabilidade.

Para responder a essas necessidades, a Microsoft lançou o Internet Explorer 7 (IE7). Ele está disponível tanto para o Windows XP (via Windows Update, ele é disponibilizado como uma atualização crítica), quanto para o Windows Vista, no qual é o navegador instalado por padrão.

Ao contrário do que muitos pensam, o IE7 para o Windows XP possui apenas alguns dos recursos de segurança que a Microsoft idealizou. Para usufruir de todos os novos recursos de segurança do IE7, é necessário trabalhar com o Windows Vista.

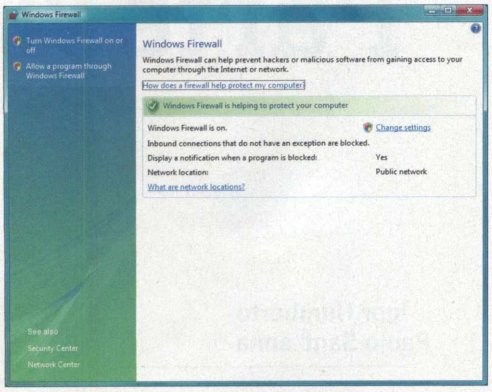
Dynamic Security

O exame 70-620 cobrará do candidato conhecimentos sobre o funcionamento dos novos recursos de segurança disponíveis no IE7 do Windows Vista. Esses recursos formam um pacote que é chamado de Dynamic Security. Uma das razões por trás desse nome é a existência de recursos que visam proteger o usuário dinamicamente. O sistema só solicita sua intervenção quando explicitamente necessário. A seguir, apresentamos uma lista descritiva desses recursos:

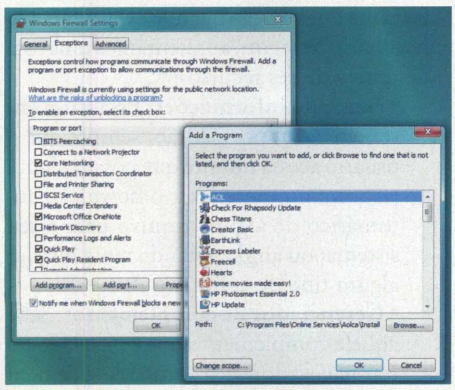
- **Barra de informações**: Essa barra entra em ação, por padrão, sempre que o usuário acessa um site que possua algum pop-up; ou tente fazer o download automático de algum arquivo para o seu sistema; ou ainda, quando tenta instalar algum tipo de aplicativo Active X;
- **Gerenciador de complementos**: Sabe aquele complemento que é instalado no seu navegador, fica "grudado que nem carrapato" e você não consegue desinstalá-lo de forma alguma? Através desse gerenciador, é possível desativar qualquer complemento do IE7 com bastante facilidade. Se algum complemento estiver atrapalhando o correto funcionamento do seu navegador, mas você não sabe exatamente qual é, basta iniciar o navegador sem complementos. Isso pode ser feito a partir da opção correspondente no menu Ferramentas de sistema, presente em Acessórios do menu Iniciar;
- **Barra de Status de segurança**: Um dos problemas do IE6 é que nem sempre o usuário entendia as mensagens de segurança que o informavam sobre a possibilidade de um site não ser confiável. Tais mensagens estavam relacionadas ao certificado apresentado pelo site visitado. Já no IE7, apesar do princípio de opera-

Cor	Significado
Branco	Indica que não existem problemas com o certificado apresentado pelo site. Nesse caso, a comunicação será criptografada.
Verde	Muito semelhante à cor branca. A diferença neste caso é que a autoridade de certificação emissora do certificado apresentado pelo site, confirma que o mesmo é do proprietário.
Amarelo	A autenticidade do certificado não pôde ser verificada, ou a autoridade de certificação não pôde ser contatada.
Vermelho	O certificado está desatualizado, errado ou apresenta erros.

T1. Significado de cada cor que pode ser exibida ao usuário.



F1. Menu de configuração do Firewall do Vista.



F2. Adicionando um programa à lista de exceções do Firewall.

ção permanecer o mesmo, ou seja, lê o certificado do site e apresenta o resultado da análise ao usuário, isso é feito através de um sistema de cores exibido na barra de endereços (tabela 1).

• **Filtro de Phishing**: Alerta o usuário que o site buscado é fraudulento ou possui características de phishing. Há uma base de dados que é constantemente atualizada pela Microsoft e outros parceiros, de forma que o usuário fique mais seguro quando estiver navegando;

• **Barreiras de domínio cruzado**: O navegador protege o usuário contra scripts maliciosos que tentem gravar informações ou instalar programas no sistema;

• **Excluir o histórico de navegação**: Permite ao usuário excluir informações sobre páginas em cache, dados de formulários, cookies e histórico de navegação;

• **Proteção da barra de endereços**: Todas as janelas exibidas para o usuário devem apresentar uma barra de endereços. Assim, fica mais difícil enganar o usuário com janelas que se apresentam como alertas do sistema, mas que na verdade querem levá-lo a uma armadilha;

• **Anti-Spoofing em nomes de domínio internacionais**: Evita que URLs contendo caracteres internacionais que não sejam corretamente exibidos, enganem o usuário ao conduzi-lo para um site com conteúdo hostil;

• **Corrigir configurações para mim**: Através desse recurso, o IE7 pode avisar o usuário quando ele estiver navegando com configurações de segurança que podem expor o sistema a ataques. Isso pode ser feito de duas formas: através de um aviso na Barra de Informações, ou da caixa Opções da Internet. Em síntese, quando o usuário navegar nesta condição, um aviso será exibido na Barra de informações e, mediante confirmação, o sistema auto-configurará as opções do IE7 na tentativa de propiciar uma navegação mais segura. Na prática, isso corresponde a deixar o IE7 no nível de segurança Médio-Alto;

• **Modo Complementos desativados**: Se o IE7 não abrir normalmente, através deste modo de operação é possível abri-lo apenas com os complementos básicos para o funcionamento do mesmo.

• **É importante deixar claro que o IE7** do Windows Vista não é exatamente igual ao IE7 do XP, pois alguns de seus recursos de segurança dependem de interação com módulos só existentes no Vista. Por isso, que a navegação com IE7 e Vista sempre será muito mais segura.

Configurando o Windows Firewall

As conexões de acesso à Internet estão cada vez mais velozes e acessíveis, mas as ameaças encontradas na navegação aumentam na mesma medida. O pior é que muitos micros, até mesmo domésticos, estão constantemente conectados e conseqüentemente são alvos de ataques dos mais diversos tipos, desde *hackers* até softwares maliciosos.

Diante desse cenário, é imprescindível ter muito cuidado ao navegar e possuir um kit básico de proteção, o que hoje compreende um antivírus, antispyware e firewall. Com enfoque neste último componente, agora vamos analisar a configuração do Firewall nativo do Windows. Ele foi introduzido no SP2 do Windows XP e totalmente reescrito na versão para o Vista. As principais novidades são:

Menu de Configurações

O acesso é feito através do ícone correspondente, disponível no Painel de controle (figura 1).

É recomendável deixar o Windows Firewall sempre habilitado e realizar algumas configurações personalizadas, tais como autorizar ou bloquear acessos, programas e conexões. Ao clicar em **Change settings**, vemos três abas de configuração disponíveis no Windows Firewall.

Na primeira, General, podemos ligar (*On*) ou desligar (*Off*) o Firewall e bloquear toda e qualquer tentativa de conexão. Nesse caso, inclusive, serão ignoradas quaisquer exceções que estejam configuradas (*Block all incoming connections*).

Já na guia **Exceptions**, é possível especificar quais programas e portas estarão liberadas para a realização de conexões (figura 2). Por padrão o Firewall, já exibe uma lista pré-definida, porém nada impede que sejam adicionados novos programas (*Add program*) ou portas (*Add port*) à lista de exceções. Ao clicar na caixa ao lado do nome do programa habilitaremos o acesso através do Firewall. Recomendamos que sejam criadas regras de exceção apenas para os softwares que sejam realmente necessários, cujo funcionamento seja conhecido, e removendo aqueles que não serão utilizados para acesso via Firewall. Por padrão, o Firewall notifica o usuário quando bloqueia o acesso de algum programa. Caso você não queira receber os avisos, desmarque a opção "*Notify me when Windows Firewall blocks a new program*".

Por último, na guia *Advanced* podemos selecionar quais conexões de rede

habilitadas na máquina serão monitoradas pelo Firewall. É possível também restaurar as configurações padrão do Firewall, para isso é necessário clicar em *Restore Defaults*.

Configurações avançadas do Firewall

A principal novidade desta versão do Firewall presente no Vista é a integração das configurações do Firewall com as do Internet Protocol Security (IPSec) em uma única console, proporcionando uma maior flexibilidade nas configurações de regras de conexão. Para obter acesso, vá até o Painel de Controle, clique em *Administrative Tools* e depois em *Windows Firewall with Advanced Security*.

Pode-se configurar o Firewall com uma série de regras distintas, definindo o que exatamente será permitido, bloqueado ou seguro no tráfego através dele (figura 3).

As opções de configuração são:

- **Inbound Rules (Regras de entrada):** Regras de proteção contra acessos não autorizados ao sistema, provenientes de outros computadores, como por exemplo softwares copiados para o computador sem o conhecimento do administrador, ou configurações indesejadas feitas no computador a partir de máquinas remotas. Existem regras pré-criadas pelo sistema que podem ser editadas, desabilitadas e apagadas (figura 4). Para criar uma nova regra, clique com o botão direito em *Inbound Rules* e em *New Rule*.
- **Outbound Rules (Regras de saída):** Regras de proteção para tentativas de conexão a outros computadores e serviços como, por exemplo, utilitários do computador que façam o download de conteúdo, ou que acessam recursos de rede sem o conhecimento do Administrador. Existem também regras pré-criadas pelo sistema que podem ser editadas, desabilitadas e apagadas. Para criar uma nova regra, clique com o botão direito em *Outbound Rules* e em *New Rule*.
- **Connection Security Rules:** Regras que podem ser criadas para definir níveis de segurança que o usuário deseja para a comunicação entre computadores. Podemos utilizar IPSec para garantir requisitos de autenticação e criptografia, fazendo com que os computadores se autentiquem para realizar comunicação com o seu computador e que criptografem os dados que serão enviados ou recebidos pelo seu computador. Para criar uma nova regra, clique com o botão direito em *Connection Security Rules* e em *New Rule* (figura 5).

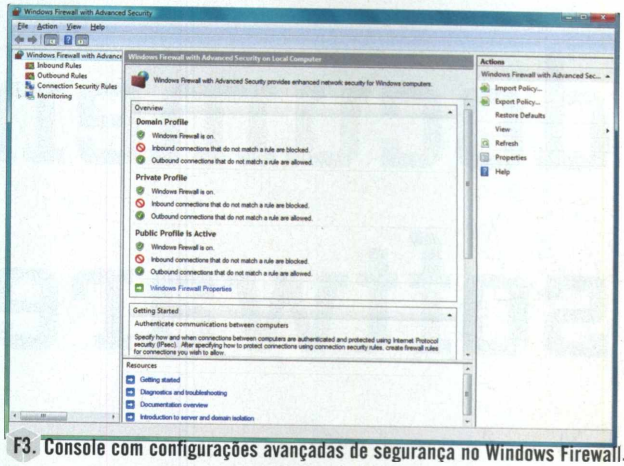
Monitoring

Exibe as informações sobre as regras do Firewall, regras de conexão e monitoramento das interfaces de rede (figura 6).

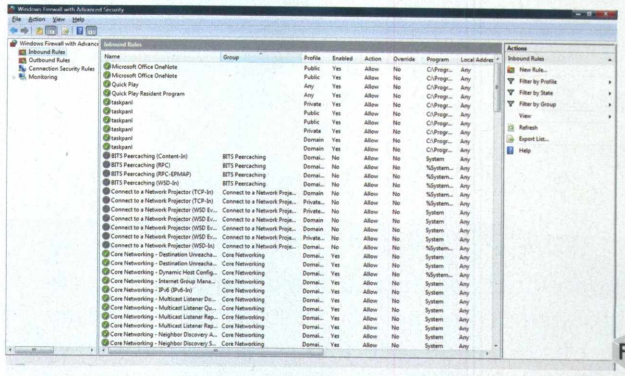
Conclusão

Fechamos nesta matéria os tópicos sobre segurança que são abordados no exame 70-620. Devemos conhecer bem as configurações avançadas do Internet Explorer e do Windows Firewall para garantir uma navegação mais confiável e protegida em máquinas com o Windows Vista.

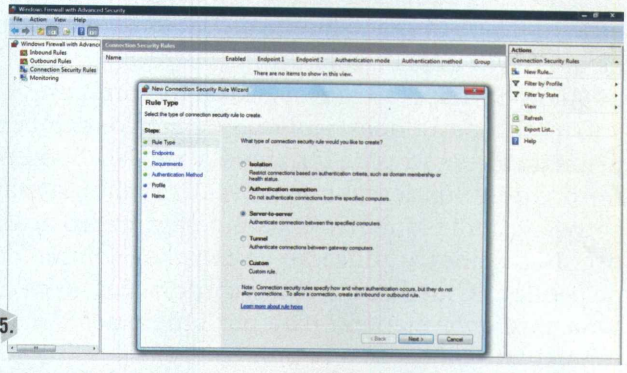
PC



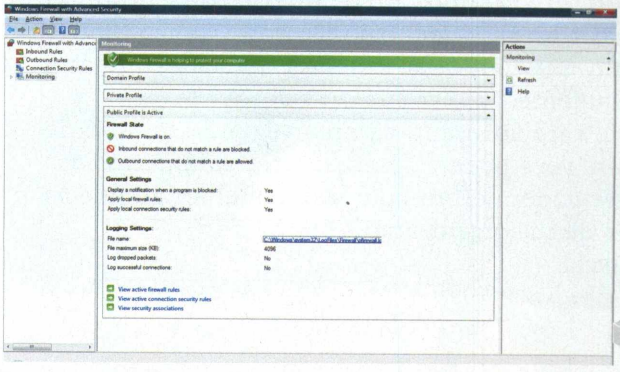
F3. Console com configurações avançadas de segurança no Windows Firewall.



F4. Regras de entrada.



F5. Criação de uma nova regra.



F6. Monitoração das atividades do Windows Firewall.

Gerenciamento de documentos com software livre

Parte II

Jansen Carlo Sena

Uma vez ciente da importância de organizar a desordem de documentos eletrônicos corporativos e até mesmo pessoais que costumam "habitar" os discos locais e os *drives* de rede, é importante conhecer as ferramentas, batizadas pela sigla DMS (*Document Management System* ou Sistema de Gerenciamento de Documentos, em português), capazes de auxiliá-lo nessa tarefa.

Além da discussão a respeito da importância de utilização do DMS, a primeira parte dessa coleção de artigos também apresentou uma primeira alternativa de ferramenta: o OWL. Somente para rememorar, um dos desafios dessa série é discutir as alternativas de DMS que sejam software livre e que não exijam o pagamento de onerosas licenças de uso. Isso coloca a utilização de uma boa solução de DMS à disposição de pequenas, médias e grandes corporações, além de servir ainda como uma excelente maneira para por ordem aos documentos pessoais de um usuário ou de uma família.

Outro aspecto importante está no fato de que se concentrar em ferramentas livres significa ter softwares cujo acesso ao código-fonte é pleno e, portanto, permite que a aplicação possa ser adaptada conforme os requisitos de cada ambiente.

Nessa oportunidade, será apresentada uma segunda solução de DMS: o OpenKM. Assim, você poderá começar a ter parâmetros das alternativas existentes e poder definir aquela que melhor atende às suas ou às necessidades de sua organização.

Pronto? Então, vamos lá!

Um pouco sobre o OpenKM

Da mesma maneira que o OWL, o OpenKM (**www.openkm.org**) está licenciado sob a licença GNU GPL (*General Public License*), a primeira e mais completa licença para software livre, uma vez que garante todas as liberdades previstas, tais como acesso completo ao código-fonte, modificação do produto para atender necessidades específicas, execução do aplicativo para quaisquer finalidades e distribuição de cópias da aplicação original ou das versões modificadas.

Por outro lado, diferente do OWL, o OpenKM não é baseado na arquitetura LAMP (**L**inux, **A**pache, **M**ySQL e **P**HP). Desenvolvido em Java, o OpenKM baseia sua infra-estrutura no cada vez mais popular e consolidado servidor de aplicações Jboss, o qual por sua vez delega a administração dos dados ao Jack Rabbit, que tem recursos para tornar transparente o armazenamento de dados nos mais populares bancos de dados ou mesmo em sistema de arquivos convencionais (figura 1).

Uma das principais vantagens do OpenKM está em sua interface, bastante semelhante aos populares gerenciadores de arquivos presentes em sistemas operacionais como GNU/Linux, Microsoft Windows, FreeBSD, Mac OS X, Solaris, dentre outros. Essa característica *auxilia muito quando*

ferramentas de DMS são implantadas em ambientes corporativos para serem utilizadas pelos mais variados perfis de usuários. Reduz-se a dificuldade de utilização da ferramenta e, conseqüentemente, aumenta-se a probabilidade quanto à sua aceitação e popularidade perante seus usuários.

A última versão do OpenKM, lançada em outubro de 2007, trouxe ainda boas novidades com relação à versão anterior, como, por exemplo, a possibilidade de um usuário "monitorar" arquivos e/ou pastas, sendo informado por email a respeito de qualquer modificação neles. Outros novos recursos interessantes consistem na melhoria dos itens de administração da ferramenta por meio de sua interface gráfica e na possibilidade de inserir vários documentos sem precisar abrir uma janela individual para cada operação.

Obtendo o software

Existem duas versões do OpenKM disponíveis para download: a primeira que está empacotada junto com o JBoss, e a segunda onde o software está disposto de maneira *standalone*. A primeira opção pode ser utilizada caso não exista ainda em seu ambiente uma instalação funcional do Jboss, ou mesmo no caso onde se queira analisar rapidamente na ferramenta sem se preocupar com a instalação e a configuração do seu servidor de aplicações. Nessa primeira versão, o JBoss e todos os seus componentes já vêm completamente configurados para a utilização com o OpenKM. A versão *standalone*, por outro lado, depende de um servidor JBoss corretamente configurado e ainda alguns passos adicionais na instalação para incorporar o OpenKM à sua configuração. Por questões de simplicidade, utilizaremos a primeira versão do software como base no decorrer do texto. Caso você possua um servidor JBoss completamente configurado e tenha vontade trabalhar com a versão *standalone*, consulte a documentação do software para identificar os passos adicionais para instalação do OpenKM em seu ambiente.

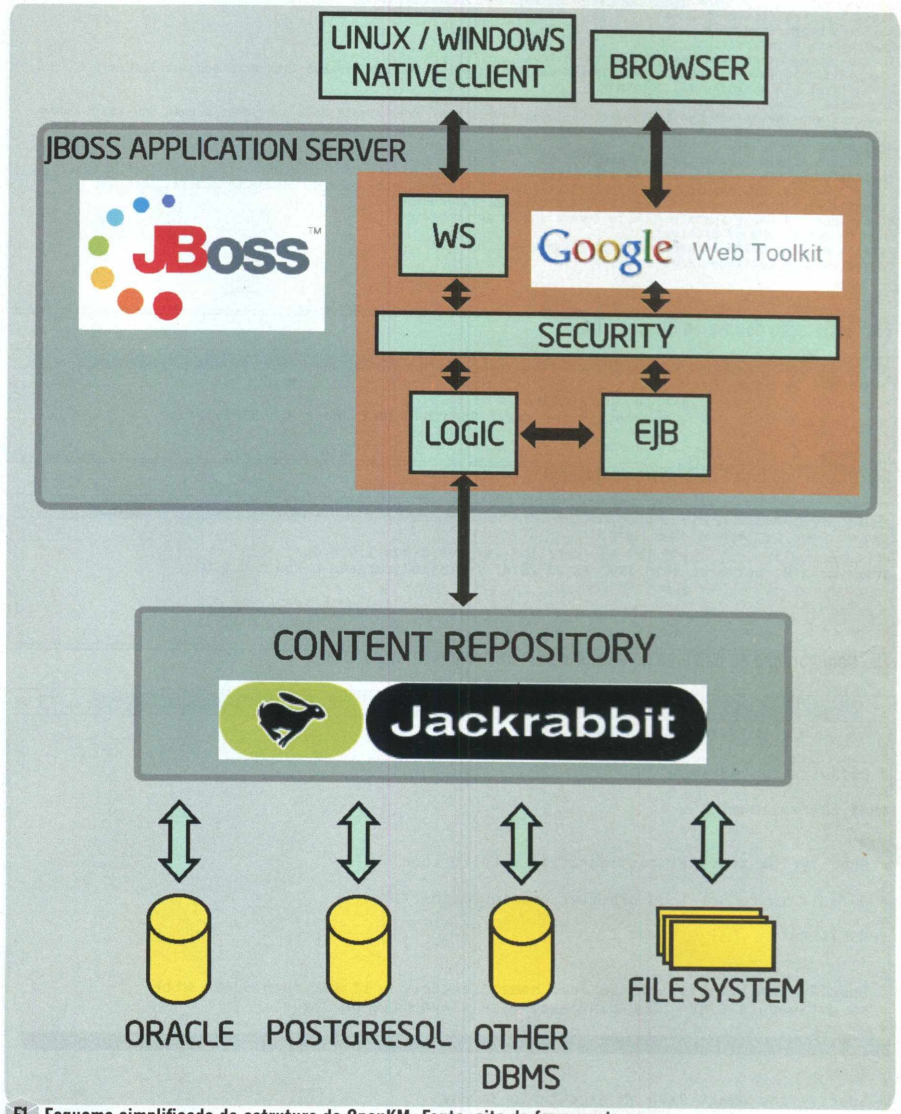
O ambiente utilizado consiste de um servidor com Ubuntu Linux 7.04 Server (Feisty Fawn) com kernel versão 2.6.20-15 (figura 2). Outras distribuições GNU/Linux, tais como Debian GNU/Linux, Fedora, Mandriva ou OpenSuSE, podem ser utilizadas e provavelmente não serão encontradas grandes diferenças no processo de configuração, uma vez que o pacote do OpenKM que está sendo utilizado traz consigo todas as dependências de software inclusas.

O OpenKM pode ser obtido diretamente a partir da página do projeto, na seção de download do Source Forge (**http://sourceforge.net/projects/openkm**). A versão considerada será a 1.2RC1 empacotada no arquivo (OpenKM-1.2RC1_JBoss-4.0.3SP1.tar.gz), que possui pouco mais de 90MB devido à inclusão do JBoss.

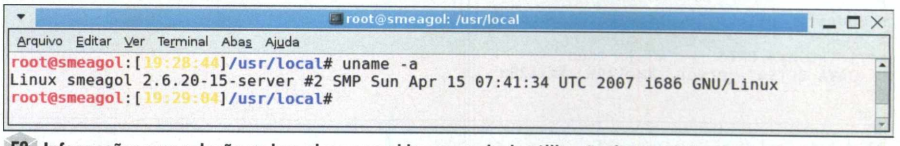
Um pouco antes de instalar o OpenKM

Em geral, ferramentas de DMS baseadas na estrutura LAMP, como é caso do OWL, exigem a preparação de uma estrutura de banco de dados para ser utilizada pelo aplicativo. Esse procedimento deve ser feito antes da instalação da ferramenta para que, durante sua configuração, sejam indicados os parâmetros para acesso e manipulação da base de dados.

No caso do OpenKM, entretanto, esse procedimento não será necessário, uma vez que o Jack Rabbit, camada de software responsável pelo gerenciamento de dados, já utiliza um mecanismo padrão para armazenamento de arquivos e sua configuração, no caso do pacote do OpenKM que contém o JBoss, já



F1. Esquema simplificado da estrutura do OpenKM. Fonte: site da ferramenta.



F2. Informações com relação ao kernel e ao servidor por meio da utilização do comando *uname*.

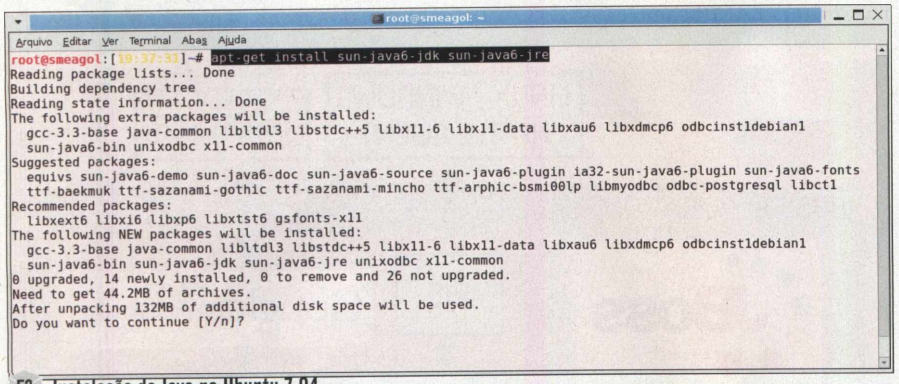
vem completamente integrada ao restante dos componentes do software. Se após sua avaliação do OpenKM você decidir colocá-lo em produção em seu ambiente corporativo, fica a sugestão de alterar sua configuração para que um banco de dados passe a ser o responsável pelo armazenamento dos dados. Além disso, encontrará mais informações sobre esse assunto na documentação do OpenKM, disponibilizada no site do software.

Entretanto, se por um lado não há a necessidade de instalar e pré-configurar um banco de dados para o OpenKM, por outro, é fundamental que o servidor que está sendo utilizado para instalar o software tenha o JDK e o JRE do Java instalados e funcionando.

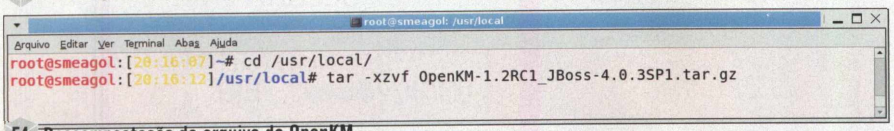
Tomando como base que o servidor é Ubuntu 7.04, a instalação do Java pode ser feita por meio do sistema apt-get, uma vez que já existem pacotes do JRE e do JDK do Java nos repositórios da própria da distribuição. Para isso, basta executar o comando apresentado na figura 3. A velocidade desse processo dependerá, evidentemente, da velocidade de sua conexão à Internet, uma vez que os pacotes de softwares serão obtidos a partir dos servidores públicos do Ubuntu configurado em seu sistema.

Caso utilize outra distribuição, consulte a sua documentação para verificar o procedimento de instalação do Java. Outra alternativa mais geral, e que funciona na maioria das distribuições GNU/Linux, consiste em obter o pacote Linux do Java diretamente do site da Sun e descompactá-lo, simplesmente executando-o no servidor.

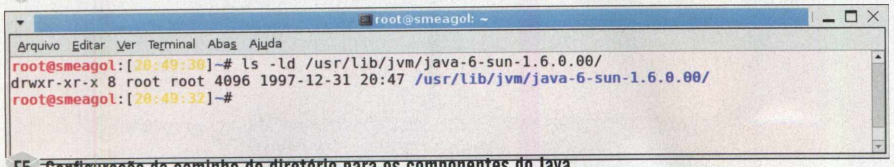
Terminada a instalação do JRE e do JDK, seja pelo sistema apt-get, ou por qualquer outro mecanismo, você está pronto para dar continuidade à sua instalação do OpenKM.



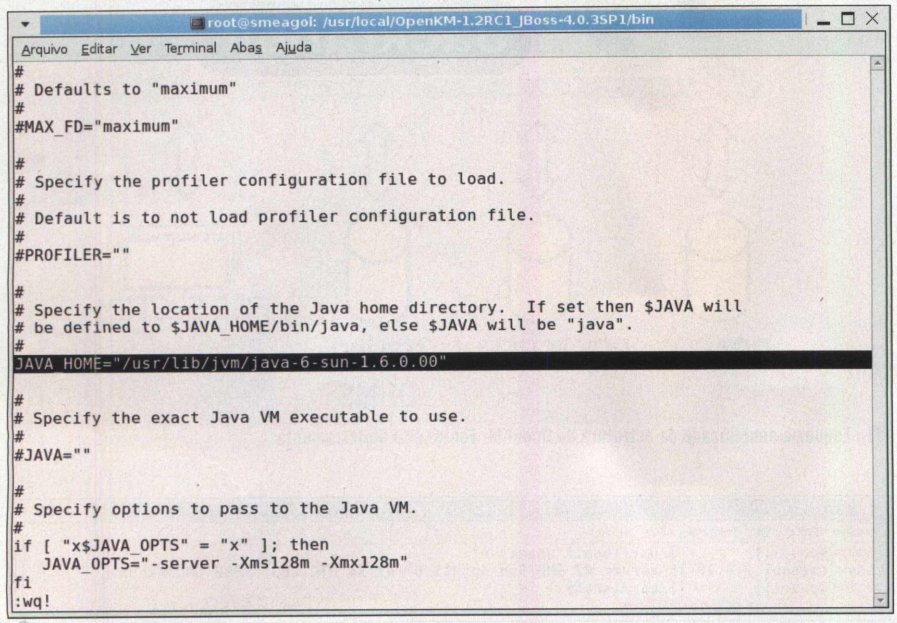
F3. Instalação do Java no Ubuntu 7.04.



F4. Descompactação do arquivo do OpenKM.



F5. Configuração do caminho do diretório para os componentes do Java.



F6. Estado final do arquivo *run.conf*.

Instalando o OpenKM no servidor

Uma vez que o arquivo contendo o OpenKM está armazenado no servidor, o primeiro passo consiste em copiá-lo para um diretório adequado à sua instalação. Fica como sugestão a utilização do diretório `/usr/local`, destinado a arquivos referentes a softwares que foram colocados em seu servidor, através de meios diferentes do sistema de gerenciamento padrão de pacotes. Outro diretório interessante para essa finalidade pode ser o `/opt`. Em seguida, é necessário descompactar o arquivo, conforme apresentado na figura 4.

Antes de executar o servidor do OpenKM, é preciso configurar o caminho do diretório onde os componentes do Java estão instalados. Novamente considerando o Ubuntu Linux 7.04, os arquivos do Java devem estar dispostos no diretório `/usr/lib/jvm/java-6-sun-1.6.0.00`, conforme apresentado na figura 5. Se outro diretório estiver sendo utilizado para a instalação do Java, certifique-se do caminho correto, uma vez que ele será necessário para o OpenKM.

Estando certo a respeito da pasta onde se encontra o Java, vá até o diretório `bin` que fica dentro da pasta onde o OpenKM foi descompactado. Em nosso caso, o caminho completo do diretório a acessar é `/usr/local/OpenKM-1.2RC1_JBoss-4.0.3SP1/bin`. Em seguida, utilizando o editor de sua preferência, abra o arquivo run.conf e procure pela variável `JAVA_HOME`. Altere o valor dessa variável para que seja refletido o caminho da instalação do Java no seu servidor. A seguir, retire o "#" do início da linha para descomentar o comando e salve o arquivo modificado (*figura 6*).

Iniciando o servidor do OpenKM

Mesmo que o OpenKM não dependa do Apache como servidor Web, é preciso iniciar o servidor de aplicação que atenderá às conexões para o aplicativo. Isso deve ser feito por meio do *script* denominado `run.sh`, localizado no diretório `bin` presente dentro da pasta onde foram extraídos os arquivos do OpenKM. No nosso ambiente tomado como exemplo, o comando a seguir é suficiente para iniciar o servidor JBoss que carregará o OpenKM:

```
# /usr/local/OpenKM-1.2RC1_JBoss-4.0.3SP1/bin/run.sh
```

Passados alguns segundos, o servidor JBoss estará funcionando e o OpenKM está pronto para ser acessado. Como fazer isso? Simples, abra um *browser* a partir de um computador que tenha acesso à rede na qual reside o servidor utilizado para a instalação do OpenKM, e digite na sua barra de endereços a seguinte URL:

http://<ENDERECO DO SERVIDOR>:8080/OpenKM

Tomando como exemplo que o servidor utilizado possui endereço IP 192.168.1.101, o acesso ao OpenKM deve ser feito através da seguinte URL:

http://192.168.1.101:8080/OpenKM

Se tudo ocorrer bem, a página de *login* do OpenKM deve ser apresentada. Para entrar no sistema, você pode utilizar a conta do administrador, cujo *login default* é *system*(figura 7).

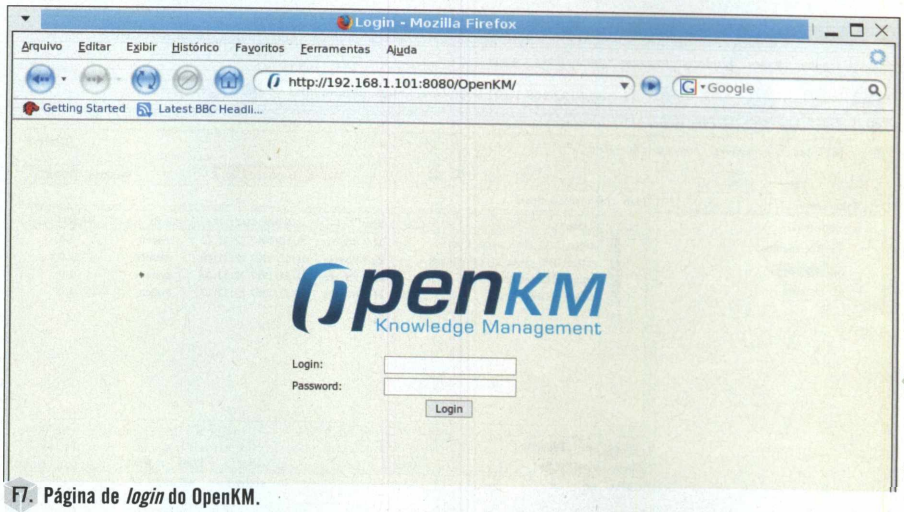
Existem outros usuários criados para teste da ferramenta. As senhas de todos os usuários, incluindo o `system`, podem ser consultadas no arquivo `users.properties`, presente no diretório `server/default/conf`, na pasta onde foi instalado o OpenKM (figura 8).

Utilizando um dos usuários, insira o login e senha correspondentes e, caso tudo esteja correto, a tela inicial do OpenKM é apresentada (figura 9).

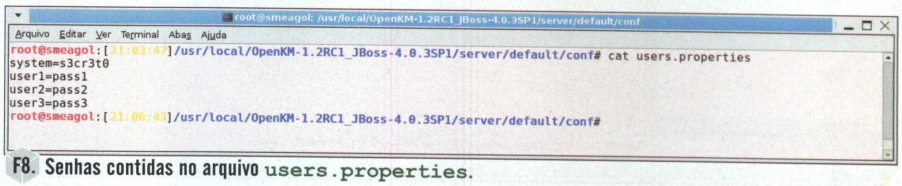
Testando a ferramenta

Não é só na aparência que o OpenKM se assemelha aos gerenciadores de arquivos. A sua manipulação também não é muito diferente: para manipular arquivos e diretórios, pode-se valer das opções que são apresentadas simplesmente clicando-se com o botão direito do mouse nas partes das suas janelas, ou ainda utilizando as opções presentes nos menus apresentados na barra superior. Poucos minutos são suficientes para que seus usuários comecem a trabalhar com o OpenKM, criando pastas e submetendo arquivos, de acordo com o exibido na figura 10.

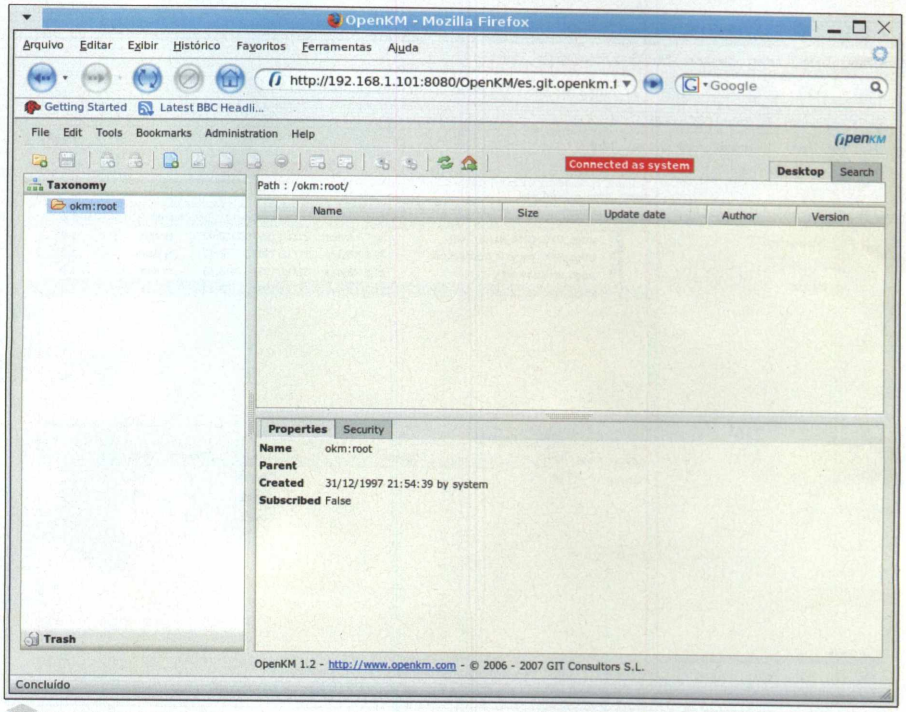
Na tela de baixo do lado direito da tela, existem duas abas, *Properties* e *Security*, a partir das quais é possível visualizar os detalhes de cada pasta ou arquivo, e configurar suas permissões de acesso, respectivamente. Essa funcionalidade é fundamental para utilização do DMS por parte dos seus usuários, uma vez que permite criar listas de controle de acesso a fim de proteger o acesso às informações submetidas ao sistema. Quando um arquivo está selecionado, uma terceira aba é apresentada nessa tela: *History*. Como o



F7. Página de *login* do OpenKM.



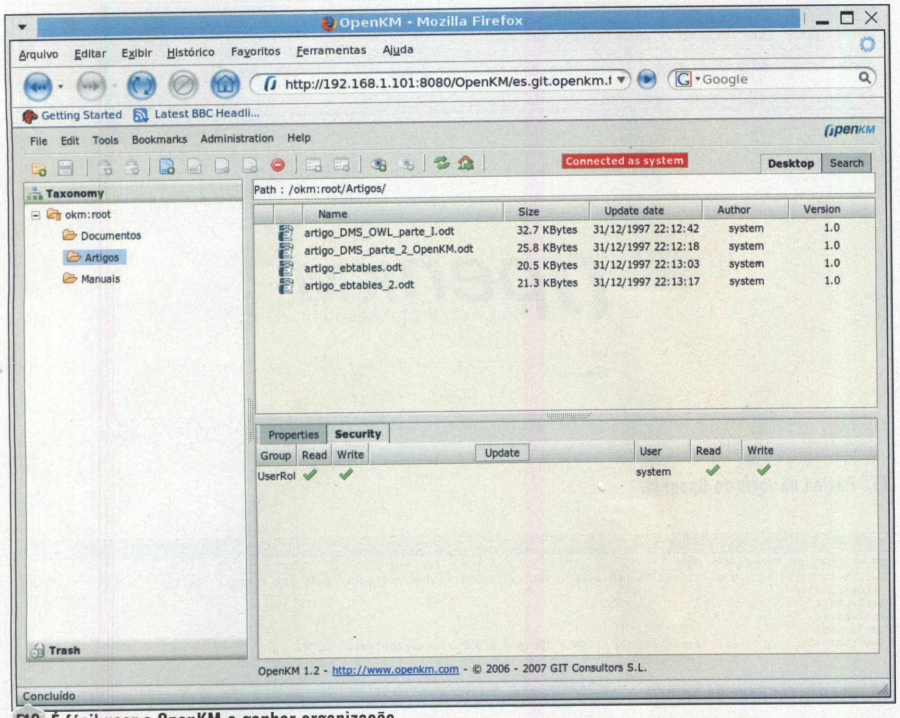
F8. Senhas contidas no arquivo `users.properties`.



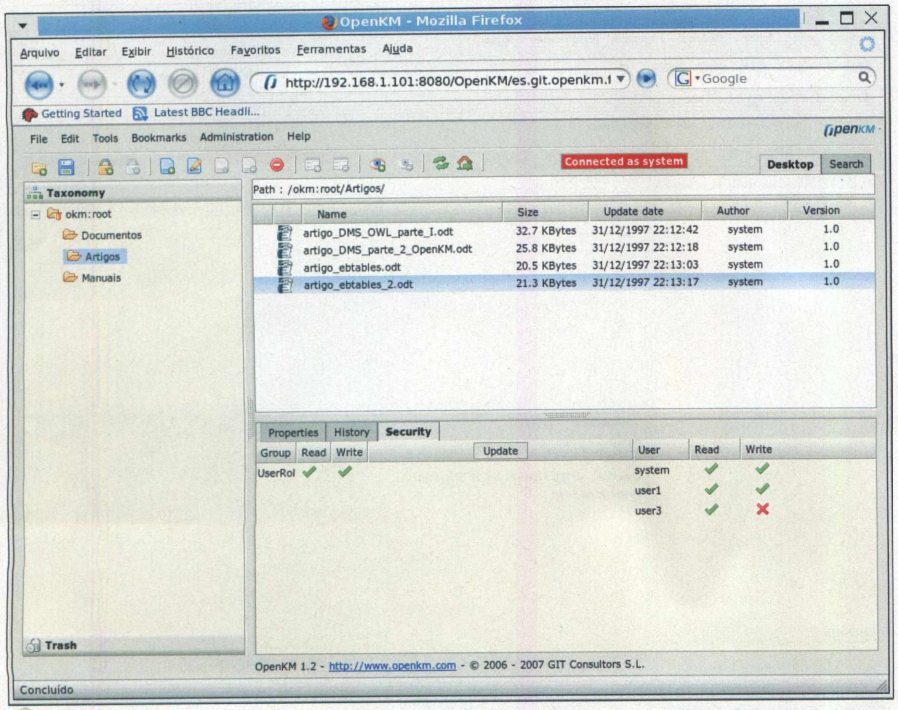
F9. Tela inicial do OpenKM.

tory. Como o próprio nome sugere, essa opção apresenta um histórico do arquivo no sistema. Por exemplo, caso tenha sido submetida mais de uma versão de um determinado arquivo, elas estarão apresentadas no histórico e disponíveis para recuperação. Interessante, não?

A opção *Security* apresenta as permissões (leitura e/ou escrita) do arquivo ou pasta selecionado, considerando os grupos do sistema e os seus usuários. Para remover ou adicionar novas permissões, basta selecionar a opção *Update* e configurar as permissões para os grupos ou para usuários individuais. O resultado de um controle de acesso mais refinado está exibido na figura 11. Uma dica importante consiste em acostumar seus usuários com a utilização desses recursos.



F10. É fácil usar o OpenKM e ganhar organização.



F11. Permissões disponíveis para um arquivo.

Caso contrário, seu DMS pode se transformar num repositório de documentos onde qualquer usuário manipula o arquivo que desejar.

Um outro recurso importante a ser testado não só no OpenKM como em qualquer DMS, uma vez que essa é uma das grandes vantagens de ferramentas dessa natureza, consiste na busca de informações referentes ao arquivo. Apesar de ser importante poder recuperar arquivos a partir de dados como nome, palavras-chave, dentre outros, uma das principais vantagens está na possibilidade de buscar arquivos a partir de pesquisas que procuram pelos termos em seus conteúdos. Na opção Pesquisa, localizada na parte superior direita da figura 12, é possível realizar esse tipo de ação. Observe como mediante o uso do termo "DMS" como chave de busca, dois documentos foram retornados. E mais: eles foram retornados com classificações de importância representadas por estrelas dispostas à esquerda do nome.

Talvez você possa estar incomodado com o fato de precisar utilizar a ferramenta com o idioma inglês. Esse problema é muito simples de ser resolvido no OpenKM. Para isso, basta acessar o menu *Tools->Languages* e selecionar a nova linguagem, "Português do Brasil", por exemplo.

Um pouco sobre a administração do OpenKM

Após um reboot do seu computador utilizado para a instalação do OpenKM, o aplicativo não estará mais disponível para seus usuários, porque o servidor da aplicação não será iniciado automaticamente. Para que isso seja feito sem a necessidade de executar o script `run.sh` manualmente, você poderá criar *links* simbólicos nos diretórios `/etc/rcX.d` apontando para o *script* `run.sh`. Feito isso, ele será executado todas as vezes que o seu servidor for iniciado. Consulte a documentação de sua distribuição GNU/Linux para mais informações a respeito desse processo.

Caso seja necessário realizar alguma atividade de manutenção (deve ser feito somente com o servidor do OpenKM paralisado), é preciso executar o *script* `shutdown.sh`, localizado no diretório `bin`, o qual, por sua vez, está dentro do diretório onde os arquivos do OpenKM foram instalados.

É óbvio que se você desejar colocar o OpenKM em modo de *produção, de forma*

criar usuários e grupos de acordo com suas necessidades. Por mais estranho que possa parecer, esse processo se dará por meio da edição manual dos arquivos `users.properties` e `roles.properties`, ambos presentes no diretório `server/default/conf`, localizado na pasta onde foram instalados os arquivos do OpenKM. Esse ainda é um dos pontos fracos do OpenKM

No primeiro arquivo, cada usuário é representado em uma linha. Após o login do usuário, um sinal de "=" é seguido do valor da senha a ser utilizada por aquele usuário. A senha, acredite, é inserida diretamente sem qualquer proteção criptográfica. Diante disso, para criar um novo usuário, o primeiro passo corresponde a inserir uma nova entrada nesse arquivo, de acordo com o mostrado na figura 13.

O segundo passo é criar uma entrada para o novo usuário no arquivo `roles.properties`. Na "linguagem" do OpenKM, uma *role* é o mesmo que um grupo de usuários. Dessa maneira, o formato das entradas nesse arquivo é o *login* do usuário, seguido de um sinal de "=" e pela lista de grupos a que esse usuário pertence, separados por vírgulas. Vale lembrar que todo usuário precisa participar pelo menos do grupo `UserRol` para ter acesso mínimo à aplicação. No exemplo exibido na figura 14, o usuário jansen faz parte dos grupos `UserRol` e `sysadmin`.

Por fim, para que o novo usuário seja validado, será necessário reiniciar o servidor do OpenKM, executando, em seqüência, os *scripts* `shutdown.sh` e `run.sh`. Como foi dito anteriormente, esse é um dos pontos fracos do OpenKM. Outros recursos podem ser considerados para melhorar o processo de autenticação dos usuários, utilizando-se, por exemplo, um servidor LDAP. Entretanto, o suporte do OpenKM ao LDAP não está completamente desenvolvido, e para fazê-lo funcionar será necessário "arregaçar mangas" e implementar a classe Java responsável por esse processo. Essa não é uma tarefa complicada para um profissional que tem algum conhecimento na linguagem. Por outro lado, pode parecer incômodo quando se precisa de uma ferramenta com um processo de autenticação mais robusto já implementado. Segundo o próprio time de desenvolvimento da ferramenta, essa será uma característica a ser implementada nas próximas versões do software.

Conclusão

A empresa responsável pelo desenvolvimento e manutenção do OpenKM vende serviços de suporte para a ferramenta. Essa pode ser uma maneira para conseguir modificar e adaptar certas funcionalidades do software sem a necessidade de ter alguém, dentro de sua organização, trabalhando com os códigos-fonte da aplicação. Por outro lado, é importante salientar que ainda não existe uma comunidade de programadores, independente da empresa que desenvolve o OpenKM, ajudando no seu desenvolvimento. Isso faz com que todas as novas funcionalidades sejam desenvolvidas sempre pela empresa que mantém o software, o que por sua vez acaba priorizando as solicitações feitas pelos clientes que pagam pelo serviço de suporte.

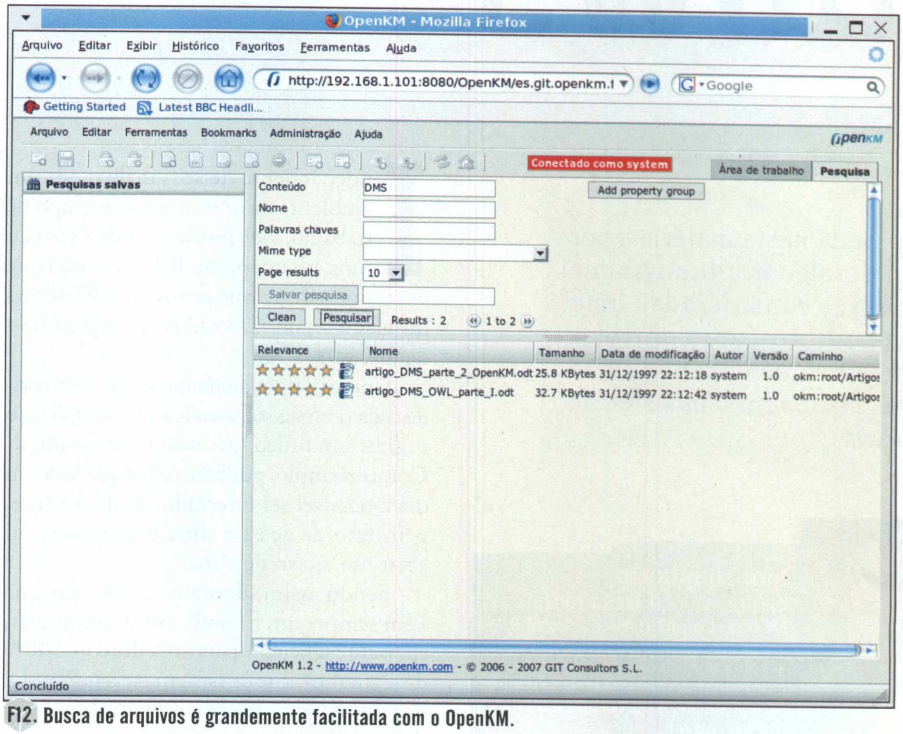
Outro ponto negativo do OpenKM consiste em sua documentação. Apesar de existirem manuais separados para finalidades como administração, instalação e utilização, as informações ainda não estão organizadas de maneira muito clara, por meio de uma abordagem passo a passo.

Por outro lado, caso esses sejam pontos fracos aceitáveis para o seu ambiente, onde talvez uma interface mais próxima àquelas dos gerenciadores de arquivos seja desejável, o OpenKM será uma boa alternativa a ser considerada, fundamentalmente se sua organização possui desenvolvedores Java dispostos a acertar as "arestas" do aplicativo para atender às necessidades específicas da empresa nos pontos que ainda não estejam implementados.

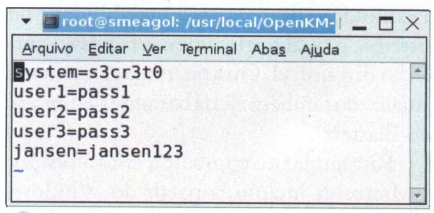
No mais, aí está uma segunda alternativa de DMS para colocar ordem nos seus documentos eletrônicos.

Até a próxima!

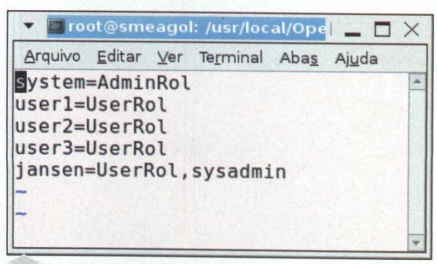
PC



F12. Busca de arquivos é grandemente facilitada com o OpenKM.



F13. Conteúdo do arquivo `users.properties`.



F14. Conteúdo do arquivo `roles.properties`.

Restrição de software: maior controle no Windows

Aprenda nesta matéria a por em prática algumas diretivas que podem ser consideradas uma ótima solução para controlar quais softwares podem ou não ser executados em seus sistemas Windows.



Igor Humberto
Certificado MCP, MCSA 2003, MCDST, CompTIA A+ e Asus ACP. Trabalha há 10 anos com suporte e gerenciamento de redes Microsoft e atualmente ministra treinamentos preparatórios para certificação na M.Cury, no RJ.

Independente de se trabalhar em um ambiente de domínio ou de grupo de trabalho, todo profissional de TI possui uma preocupação básica: evitar que os computadores que possuem o Windows instalado sejam infectados por algum tipo de malware.

Como os tipos de ataques estão se tornando cada vez mais sofisticados, fica complicado utilizar um único mecanismo de combate. Como exemplo, podemos citar que hoje em dia é possível ser infectado, simplesmente, pelo fato de acessar uma página web ou abrir um anexo de e-mail.

Sendo assim, devemos considerar que nem sempre um firewall, antivírus ou anti-spyware é suficiente para impedir, com 100% de segurança, que um sistema seja infectado. Por outro lado, vale ressaltar que boa parte dos problemas ligados com invasão ou "aquisição" de algum malware está relacionada à exploração de alguma vulnerabilidade do sistema, o qual normalmente já possui correção disponível. Ou seja, manter o sistema atualizado também ajuda bastante (lembra-se do Blaster?).

Para ajudar no combate a essas ameaças, a Microsoft incluiu, a partir do Windows XP, uma ferramenta que permite determinar aquilo que pode, ou não, ser executado no sistema. Essa ferramenta se resume a um conjunto de diretivas que conhecemos como Diretivas de restrição de software.

Através desse conjunto de diretivas, é possível combater malware, determinar como controles Active X poderão ser baixados, executar somente os scripts que sejam assinados digitalmente, garantir que somente os softwares aprovados pelo administrador sejam instalados no sistema, enfim, bloquear a estação. Vale ressaltar que esse conjunto de diretivas não deve ser visto como único meio de prevenção contra os problemas citados, mas como uma ferramenta que reduz bastante a possibilidade dos mesmos em afetarem os sistemas.

Como funcionam?

As Diretivas de restrição de software podem ser configuradas de diversas formas. Você poderá criar regras baseadas nos seguintes pontos: Certificados, Hash, Caminho e Zona de Internet. Cada uma dessas possibilidades atende a uma necessidade específica. A seguir, veremos como cada método funciona e como pode ser aplicado.

Regra de certificado

Através deste tipo de regra, você poderá determinar que somente software (scripts ou

controles Active X, por exemplo) assinado digitalmente por uma Autoridade de certificação (CA) poderá funcionar no sistema. Essa CA pode ser a Verisign ou aquela que está disponível através do próprio Serviço de certificados do Windows. O problema desse método é que, apesar de ser extremamente seguro, dá bastante trabalho utilizar regras baseadas em certificados. Antes de implementar Diretivas de restrição de software com regras baseadas em certificado, é importante considerar os seguintes pontos:

- Caso trabalhe em um ambiente onde só exista o Windows XP, ou seja, num ambiente baseado em grupo de trabalho, você deverá assinar os códigos autorizados usando certificados de uma Autoridade de certificação pública, tal como a Verisign. Nesse caso, o problema será o gasto;
- Para profissionais de infra-estrutura, é complicado assinar código digitalmente. Aliás, para uma grande parte dos profissionais de TI que conheço é uma dificuldade entender o funcionamento dos certificados digitais. Isso não deveria ser assim, mas é.

Regras de Hash

De uma forma bastante sucinta, podemos dizer que o Hash de um arquivo seria a impressão digital criptografada do mesmo. Assim, por exemplo, caso você quisesse que o WINWORD.EXE (executável que abre o aplicativo Microsoft Office Word) fosse executado usando uma regra baseada no Hash do referido arquivo, seria necessário recolher a "impressão digital do mesmo". A idéia, nesse caso, é a de evitar que você alterasse o nome de um arquivo para WINWORD.EXE a fim de que o mesmo pudesse ser executado. Como a regra não é baseada no nome e sim na tal impressão digital do arquivo, não tem como enganar o sistema. Sendo assim, o arquivo WINWORD.EXE poderia ser renomeado ou movido dentro do sistema sem afetar a sua forma de execução, pois a regra de Hash é baseada no cálculo criptográfico feito sobre o conteúdo do arquivo.

Uma regra de Hash é dividida em três partes de dados separadas por ":", ou seja, você irá encontrar a seguinte formatação: [Valor de Hash SHA1 ou MD5]:[Comprimento do arquivo]:[ID do algoritmo de Hash]. Arquivos que são assinados digitalmente irão usar o valor de Hash contido na assinatura, que pode ser *SHA1* ou MD5. Arquivos que não são assinados digitalmente só podem usar o Hash MD5.

Como exemplo, vamos analisar a seguinte informação: 7bc04acc0d6480af862d22d724c3b049:126:32771. Essa regra de Hash é baseada em um arquivo com comprimento de 126 Bytes e com o conteúdo que atende ao Hash MD5 7bc04acc0d6480af862d22d724c3b049, com o identificador 32771. Se apenas 1 bit for alterado no arquivo, o cálculo do Hash resultante já seria bastante diferente.

Regras de caminho

Neste tipo de regras você pode especificar os caminhos dos softwares liberados para execução. São aceitos caminhos locais, caminhos UNC ou caminhos de registro. Sendo assim, são válidos os seguintes exemplos, respectivamente: "C:\Arquivos de programas\Microsoft Office", \\SRV\Aplicativos, ou ainda HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\PlatformSDK\Directories\Install Dir.

Vale ressaltar aqui que regras baseadas em caminho permitem o uso de variáveis de ambiente e de caracteres coringa. Isso significa que você poderá usar %WINDIR%, \\DC-??\aplicativos$, ou ainda C:\Win* como opções. No entanto, é importante observar que não é possível atribuir listas de controle de acesso (ACLs) em variáveis de ambiente. Ou seja, se o usuário tiver acesso ao Prompt de comandos, seria possível alterar configurações nas variáveis de forma que arquivos executáveis, presentes em um caminho não autorizado, pudessem funcionar. Está certo que só um usuário esperto deve ser capaz de fazer isso, mas é importante considerar a hipótese para evitar surpresas!

Regras de caminhos de registro

Anteriormente comentamos sobre a possibilidade de se trabalhar com caminhos de registro para determinar quais softwares podem ser executados (ou não). A questão é: Por que usar regras baseadas em caminhos de registro? Nossa idéia é atender aos softwares que não possuam um caminho padrão (C:\Arquivos de programas) de funcionamento e que não usam variáveis de ambiente para determinar a sua localização (%ProgramFiles%). É para casos como esses que os caminhos de registro podem ser úteis. Para trabalhar com esse tipo de regras, você precisa atender aos seguintes requisitos:

- Caminhos de registro devem terminar com o símbolo de porcentagem (%);
- Os valores do registro devem ser REG_SZ ou REG_EXPAND_SZ. Você também não pode usar abreviações, tais como HKLM ou HKCU para abreviar HKEY_LOCAL_MACHINE ou HKEY_CURRENT_USER, respectivamente;
- Se no valor de registro existirem variáveis de ambiente, estes valores serão expandidos quando a diretiva for aplicada;
- Estas regras podem possuir sufixos de caminho. Por exemplo, para permitir que executáveis de e-mails recebidos via Microsoft Outlook XP sejam abertos, você precisaria criar uma regra para o caminho %HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Cache%OLK, pois o local onde os arquivos temporários desses anexos é aberto seria C:\Documents and Settings\Nome-do-usuário\Configurações locais\Temporary Internet Files\OLK4.

Verifique também qual é a permissão que o usuário possui no caminho especificado. Por exemplo, se o usuário tiver a permissão de escrita no caminho autorizado, ser-lhe-ia possível copiar para lá executáveis não autorizados por você.

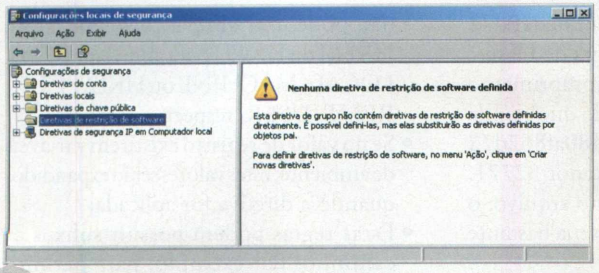
51

Regras de zonas

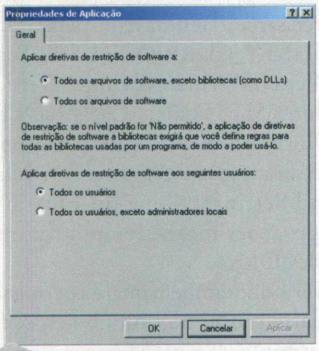
Este tipo de regra é menos utilizada, porque se aplica apenas aos pacotes de instalação do Windows Installer (MSI). As regras de zonas funcionam sobre as zonas existentes no Internet Explorer, ou seja, Internet, Intranet, Sites restritos, Sites confiáveis e Meu computador. Vale ressaltar que essas regras não se aplicam aos softwares baixados pelo navegador.

Como configurar?

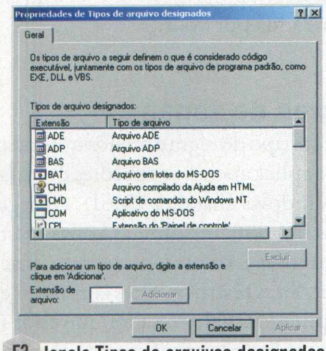
Agora que você já possui uma idéia sobre o que são as Diretivas de restrição de software e como elas atuam, vamos ver como podemos configurá-las. Se estiver trabalhando no ambiente de domínio, será necessário criar uma GPO no local onde você deseja controlar a utilização de softwares. Caso trabalhe em grupo de trabalho, ou seja, com configurações locais, é possível fazer essa configuração através do console de Configurações locais de segurança (SECPOL.MSC). Vale lembrar a importância de se fazer testes num ambiente apropriado para isso, tal como o provido por máquinas virtuais, pois configurações incorretas nas Diretivas de restrição de software podem impedir que o sistema funcione corretamente. É importante também que você planeje bem o objetivo de sua diretiva. Ou seja, determine antecipadamente aquilo



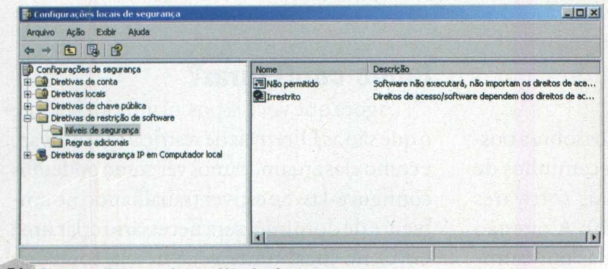
F1. Console de Configurações locais de segurança.



F2. Janela Propriedades de Aplicação.



F3. Janela Tipos de arquivos designados.



F4. Opções disponíveis em Níveis de segurança.

que você precisa que funcione, ou não, no sistema que será configurado. Em nossos exemplos, demonstraremos a configuração em um sistema local.

Sendo assim, ao abrir o console de Configurações locais de segurança, navegue até Configurações de segurança\Diretivas de restrição de software, conforme exibido na figura 1.

Repare na figura 1 a mensagem informando que não existe um conjunto de diretivas definidas para esse fim. Na verdade, já existe uma diretiva padrão (Diretiva pai) definida, a qual diz que qualquer software pode ser executado.

Para definir uma nova configuração de diretiva, basta clicar com o botão direito do mouse em Diretivas de restrição de software e selecionar a opção Criar novas diretivas. Feito isso, cinco novos objetos serão apresentados: Níveis de segurança, Regras adicionais, Aplicação, Tipos de arquivos designados e Editores confiáveis. Para começar a configuração, iremos abrir o item Aplicação (figura 2).

Aqui você configura como o sistema irá trabalhar com as DLLs e a quem a regra se aplica. Com relação às DLLs, poderá definir se as regras serão aplicadas apenas aos arquivos executáveis, ou se serão aplicadas às DLLs também. Para a maioria dos casos, basta definir as regras sobre os executáveis, pois, sem o executável, o software não poderá ser iniciado de qualquer forma. Caso determine que até as DLLs serão afetadas pelas regras, você deverá considerar também que isso irá impactar na performance do sistema. Para ilustrar isso, basta pensar que, caso um usuário tenha de executar 10 aplicações, as regras serão analisadas 10 vezes. Se cada aplicação tiver 200 DLLs e a verificação de DLLs estiver ativada, serão 210 avaliações, ou seja, o sistema terá muito mais trabalho. Sem contar que, caso o seu sistema esteja configurado para o nível de segurança Não permitido (falaremos sobre isso adiante), será necessário criar regras para permitir cada uma das DLLs que forem necessárias ao funcionamento das aplicações. Sendo assim, por que você faria uma configuração desse tipo? Como alguns vírus atacam também as DLLs do sistema, se o ambiente exigir esse nível de segurança existe a possibilidade de escolher exatamente quais DLLs poderiam ser executadas e, no caso destas serem infectadas, impedi-las de serem carregadas.

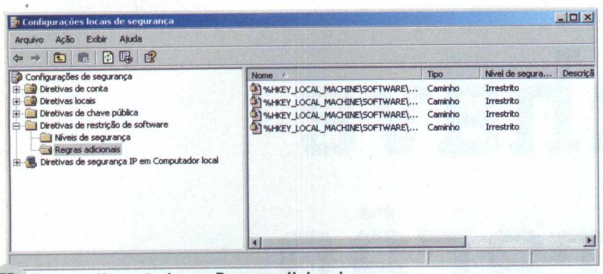
Além disso, conforme já foi dito, você poderá determinar se as regras serão aplicadas também aos administradores locais. Essa medida é recomendada principalmente quando ainda estiver realizando os testes, porque dessa forma você poderá reverter eventuais erros de configuração cometidos. Faça as configurações conforme a necessidade e clique em Ok. Agora abra o item de configuração Tipos de arquivos designados (figura 3).

Aqui você poderá definir o que será considerado software pelo sistema. Normalmente essa lista não precisa de alteração, mas, caso seja necessário, coloque as extensões que não estejam na lista através desta caixa. Ressaltamos que não adianta colocar uma extensão tal como a MP3 na lista, porque os arquivos deste tipo não são executáveis. O que acontece quando você aplica dois cliques sobre um arquivo desses é que devido à associação de arquivos feita no sistema, a aplicação (Windows Media Player, por exemplo) abre e carrega o referido arquivo. Caso não seja necessário fazer qualquer configuração extra, clique em Ok.

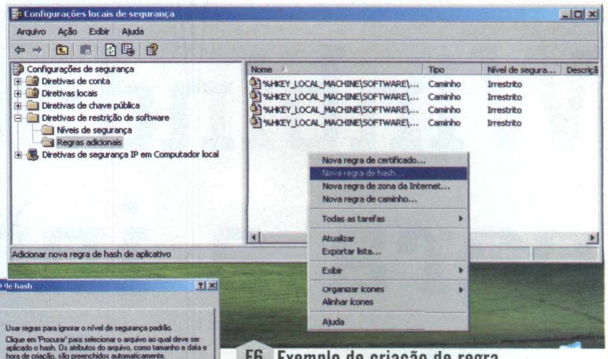
Agora vamos para o item de configuração Níveis de segurança (figura 4). Neste item você define o nível de segurança padrão que o sistema irá usar. O nível padrão é Irrestrito, ou seja, qualquer software poderá ser executado, porém, será possível criar regras que definam quais softwares não devem ser executados (criar uma Black list). O uso do nível Não permitido adiciona uma pitada extra de emoção na configuração, já que neste caso nenhum software poderá ser executado. Sendo assim, somente os softwares que você determine explicitamente, via regras, é que poderão ser executados. Porém é necessário saber exatamente o que precisa estar liberado no sistema que você estiver configurando. Para os nossos exemplos, iremos manter configurado o nível Irrestrito, mas é possível definir outro tipo de configuração ao simplesmente clicar com o botão direito do mouse sobre a configuração desejada e selecionar a opção Definir como padrão.

Agora chegou o momento de configurar as regras que irão determinar, no nosso exemplo, o que não poderá ser executado no sistema. Para isso, clique no item de configuração Regras adicionais. Repare que já existe um conjunto de regras baseadas em caminhos de registro, o qual define que o conteúdo da pasta Windows e da pasta Arquivos de programas estarão liberados (figura 5).

A regra que criaremos determinará que a Calculadora do Windows não será permitida. Para isso, a regra criada será baseada no Hash do arquivo CALC.EXE. Clique com o botão direito do mouse na área livre e selecione Nova regra de Hash. Na janela que será aberta localize a aplicação que deseja liberar (figura 6). No nosso caso, você deverá localizar o arquivo CALC.EXE que se encontra dentro da pasta %WINDIR%\System32. Ao abrir o arquivo perceba que o Hash do arquivo já é calculado automaticamente. Agora, no campo Nível de segurança, você deve definir se a aplicação será executada, ou não. No



F5. Opções disponíveis em Regras adicionais.



F6. Exemplo de criação de regra para bloqueio de programa.

caso, devemos deixar a configuração como Não permitido. Feito isso, clique em Ok.

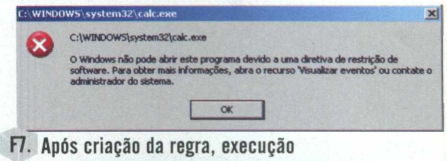
Pronto, ao tentar executar a Calculadora a partir de agora, você receberá uma tela informando que a mesma foi bloqueada pelo administrador (figura 9). E não adiantaria nem tentar renomear o arquivo. Como a nossa regra foi baseada no Hash do arquivo CALC.EXE, não importa qual o nome do arquivo e sim o conteúdo do mesmo, conforme dito anteriormente.

Conclusão

Através deste recurso é possível controlar bastante o seu ambiente, mas é importante testar tudo antes de colocar as novas configurações em produção. Se algo for configurado incorretamente, o software que desejar bloquear poderá ser executado, ou aquele que você deseja permitir pode acabar não funcionando. Portanto, não deixe esta etapa de lado. Além disso, considere que as Diretivas de restrição de software só funcionam com o Windows XP, 2003 e Vista. Ou seja, sistemas anteriores a estes não irão se beneficiar deste recurso.

Até a próxima!

PC



F7. Após criação da regra, execução do programa é bloqueada.

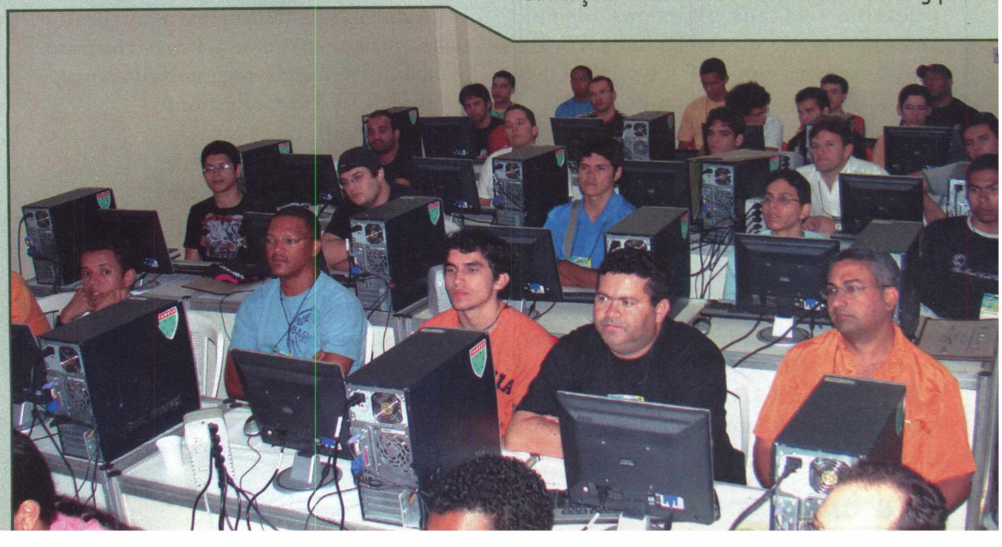
O jeito nordestino de fazer software livre

por Jansen Carlo Sena

A beleza das praias de Aracaju e a hospitalidade dos seus habitantes foram o cenário perfeito para mais uma reunião de comunidade de software livre nacional. Por três dias, Aracaju tornou-se a capital nordestina do software livre. Tudo isso por conta da realização do II ENSL (Encontro Nordestino de Software Livre), ocorrido nos dias 28, 29 e 30 de setembro. Segundo a organização do evento, mais de 1000 pessoas estiveram participando das atividades do II ENSL incluindo palestras, minicursos, sessões técnicas e apresentação de *cases* envolvendo software livre.

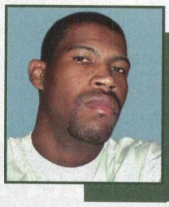
Junto com o II ENSL, ocorreram também o I LIVRE-SE (Encontro Sergipano de Software *Livre*) e o IV Fórum Gnome. Por conta de toda essa reunião, estiveram presentes palestrantes de renome nacional do cenário de software livre, como Izabel Valverde (Gnome Brasil), Júlio César Nevez (Autor do livro "Programação Shell Linux"), Sérgio Amadeu (Faculdade Cásper Líbero e Rede Livre), Rubens Queiroz de Almeida (Centro de Computação da Unicamp), Márcia Schuler (Ex-diretora da Celepar), Everaldo Canuto (Novell), Rodrigo Padula (Projeto Fedora Brasil), dentre outros. Palestrantes internacionais também fizeram parte do evento como Nathan Wilson, da Dreamworks (estúdio responsável pela produção de filmes como Shrek e vídeos) e Henri Belgius, da Gnome. Houve ainda entre os palestrantes um "pequena" novidade: Rodrigo Moresco, que é do Grupo de Usuários Debian do Paraná. E daí? E daí que o Rodrigo tem apenas 12 anos de idade e foi até o evento fazer uma palestra a respeito de sua experiência com software livre. Quer incentivo maior para mostrar o mundo do software livre para a garotada que está iniciando a utilização do computador?

A quantidade de eventos de software livre de qualidade que vem acontecendo no País é o reflexo do processo de consolidação do Brasil nesse tipo de tecnologia e nos seus desdobramentos. Para quem foi, ficam as boas lembranças e uma ótima impressão com relação ao resultado do esforço da organização do evento. Para os que não foram, fica o convite para participar da terceira edição do evento, que será realizada em Salvador... Isso mesmo, o ENSL é um evento itinerante e a cada ano é realizado em uma localização diferente do Nordeste. Saudações livres a toda comunidade de Sergipe!



Winbind: a chave para a integração entre o Active Directory e o Linux

Veja como fazer uma máquina Linux autenticar no Active Directory e usufrua das vantagens de uma base de usuários centralizada.



Flávio de Souza Oliveira
Mestre em Administração e Segurança de Sistemas pela Unicamp. Certificado LPI, atualmente trabalha na Callink - Serviços de Callcenter,em Uberlândia/MG

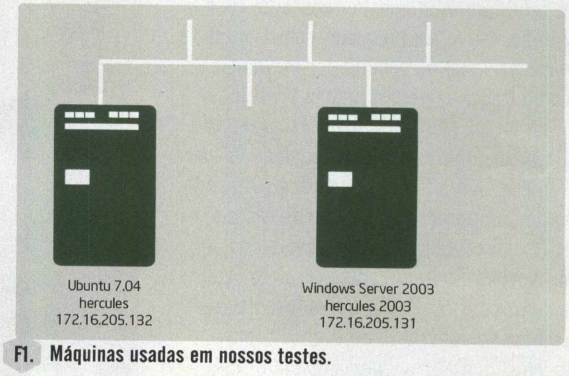
As redes compostas por mais de um sistema operacional são uma realidade há muito tempo. Os personagens dessa mistura mudam com o passar dos anos, mas o desafio é sempre o mesmo: integração.

Atualmente os ambientes com os quais mais freqüentemente nos deparamos tentando superar essa barreira, são aqueles compostos pelos sistemas Linux e Windows. Algumas vezes, quem está no comando da rede é o Linux e, nesse caso, ele é responsável pelo armazenamento das contas de usuários e por realizar a autenticação em toda a rede. Para estações também rodando Linux isso é feito através de LDAP (*Lightweight Directory Access Protocol* - **www.openldap.org**) ou NIS (*Network Information Service* - **www.linux-nis.org**) e para estações rodando Windows a integração é feita por meio do Samba (**www.samba.org**). Em outras ocasiões, o cenário é diferente e quem dita as regras na rede é o Windows e seu Active Directory (AD), o qual, embora seja uma implementação proprietária, é fortemente baseado em padrões abertos como LDAP e Kerberos (**http://web.mit.edu/Kerberos**). Como era de se esperar, a Microsoft tem pouco ou nenhum interesse na integração de sua plataforma de rede com outros sistemas operacionais, muito menos com o Linux, que é um concorrente direto. Dessa maneira, o trabalho foi todo feito pela equipe de desenvolvimento do Samba.

A autenticação de máquinas Linux no AD pode ser feita através de um *daemon* chamado Winbind (**www.samba.org/samba/docs/man/Samba-HOWTO-Collection/winbind.html**), que possibilita aos usuários/grupos da rede Windows serem mapeados em usuários/grupos Unix e permite a autenticação em máquinas Linux utilizando o mesmo usuário e senha utilizado nas máquinas Windows. Nessa matéria, veremos como configurar passo-a-passo uma estação Linux para esse tipo de integração. Vamos lá!

Cenário

Como acontece em milhares de redes ao redor do mundo, estações Linux são minoria em nosso cenário, e toda a base de usuários está organizada em um servidor Windows Server 2003 rodando o Active Directory. Nosso objetivo é integrar uma estação rodando o Ubuntu Linux versão 7.04 nessa estrutura e assim utilizar a mesma base de usuários tanto para máquinas Linux quanto para máquinas Windows. As vantagens da integração são muitas, já que assim teremos



F1. Máquinas usadas em nossos testes.

que administrar apenas uma base de usuários e evitar todo o custo de manter uma segunda estrutura de autenticação. Os dados de nosso domínio são descritos na tabela 1 e o cenário está representado na figura 1.

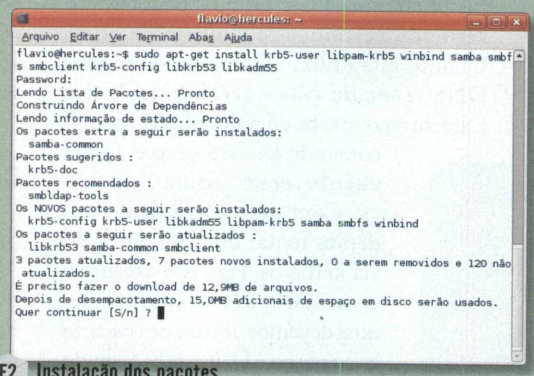
Instalando pacotes

Para que o Linux possa se integrar à rede Windows, precisamos instalar dois programas e suas bibliotecas auxiliares. São eles:

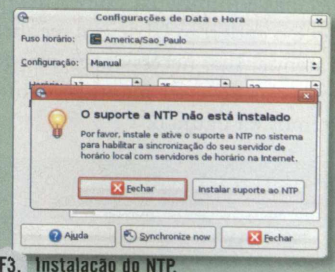
samba com winbind: para mapeamento e autenticação de usuários;

kerberos: para autenticação de máquinas e outros objetos do domínio e assim garantir que uma estação é realmente quem ela diz ser.

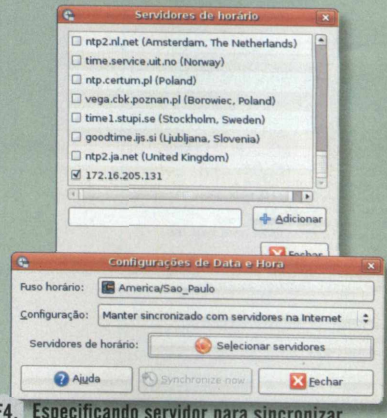
A instalação desses componentes é muito simples no Ubuntu, basta executar o comando `sudo apt-get install krb5-user libpam-krb5 winbind samba smbfs smbclient krb5-config libkrb53 libkadm55` (figura 2). Após a execução do comando, a senha do seu usuário será solicitada e, após isso, basta responder 'S' para a pergunta de confirmação.



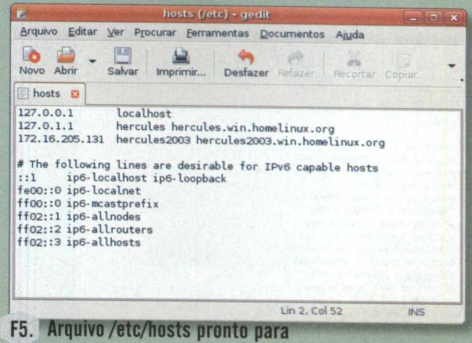
F2. Instalação dos pacotes.



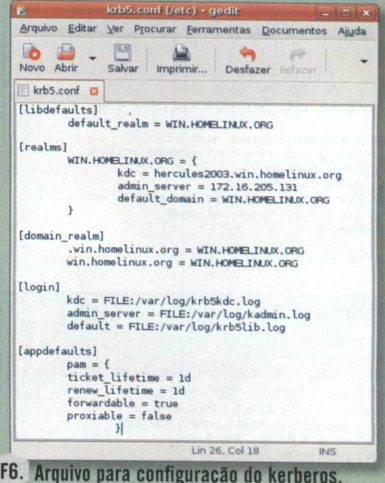
F3. Instalação do NTP.



F4. Especificando servidor para sincronizar relógio.



F5. Arquivo /etc/hosts pronto para resolver o nome do servidor de domínio.



F6. Arquivo para configuração do kerberos.

Configuração

Kerberos

O protocolo kerberos é extremamente rigoroso, como era de se esperar de um protocolo de segurança. Ele trabalha com um mecanismo de *tickets* criptográficos que se expiram ao longo do tempo, ou seja, uma vez autenticado, o cliente recebe um *ticket* contendo uma chave criptográfica para se comunicar com o servidor, mas essa chave tem um período de validade e deve ser renovada dentro de determinados intervalos de tempo.

O primeiro requisito para o funcionamento do protocolo é a sincronização de relógio entre as máquina envolvidas. Sendo assim, configure o Ubuntu para sincronizar seu relógio com o servidor de domínio, em nosso caso a máquina `hercules2003.win.homelinux.org`. Para isso, clique com o botão direito no relógio do canto superior direito da tela e selecione a opção "Ajustar Data e Hora". O Ubuntu então solicitará a senha de seu usuário para abrir a janela de configuração. Uma vez na janela de configuração de data, altere o campo "Configuração" de "Manual" para "Manter sincronizado com servidores da Internet". Feito isso, o Ubuntu solicitará a instalação do serviço NTP (*Network Time Protocol*). Pressione o botão "Instalar suporte ao NTP", e aguarde o término da instalação (figura 3).

Após a instalação, pressione o botão "Selecionar servidores", adicione o endereço IP de nosso controlador de domínio na lista, desmarque todos os outros servidores e deixe apenas ele ativo (figura 4). Feito isso, pressione o botão "Fechar", seguido do botão "Fechar" da janela principal de configuração.

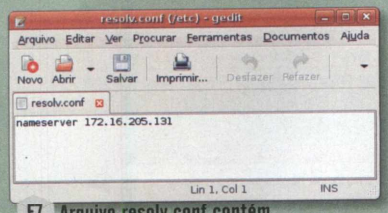
Com os relógios sincronizados precisamos garantir que o Ubuntu será capaz de resolver o nome do servidor de domínio. Para isso inclua o endereço IP do servidor no arquivo /etc/hosts, o que pode ser feito com o comando gksudo gedit `/etc/hosts` (figura 5). Note que a senha do seu usuário pode ser solicitada pelo comando `gksudo`, dependendo do período decorrido desde sua última autenticação.

Agora estamos prontos para configurar o kerberos propriamente dito. Para isso edite o arquivo `/etc/krb5.conf` com o comando `gksudo gedit /etc/krb5.conf` e indique o nome de domínio, nome do servidor e seu endereço IP, de maneira semelhante ao que observamos na figura 6. Fique atento pois as configurações nesse arquivo diferenciam letras

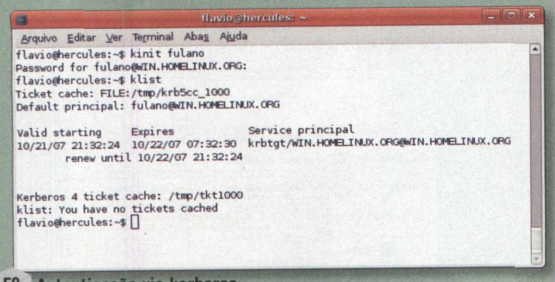
Nome	Valor
Domínio Active Directory	win.homelinux.org
Nome do Servidor Windows	hercules2003.win.homelinux.org
Endereço IP do Servidor Windows	172.16.205.131
Servidor DNS	172.16.205.131

T1. Informações do Domínio Windows.

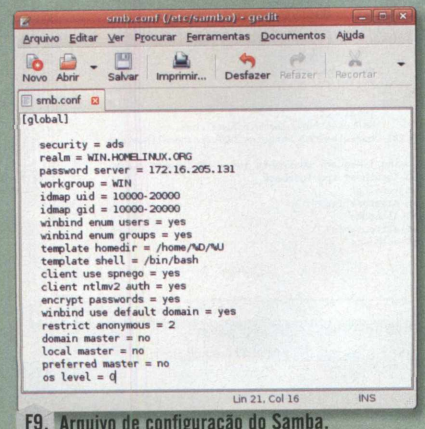
maiúsculas e minúsculas, de forma que os nomes e o endereço IP devem ser alterados para atender suas necessidades, mas a caixa das palavras deve ser mantida idêntica ao que temos na figura 6.



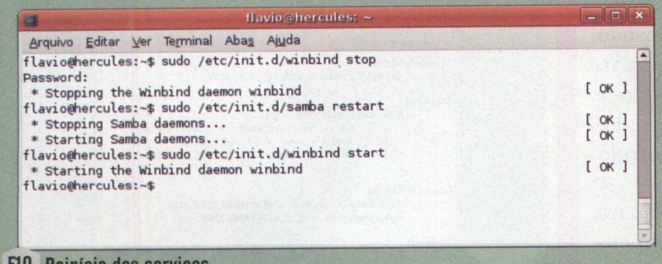
F7. Arquivo resolv.conf contém endereço do servidor DNS.



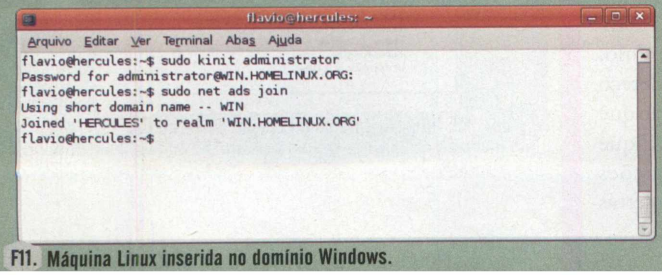
F8. Autenticação via kerberos.



F9. Arquivo de configuração do Samba.



F10. Reinício dos serviços.



F11. Máquina Linux inserida no domínio Windows.

Já estamos quase prontos para testar o kerberos, certifique-se também de que o Ubuntu está utilizando o mesmo servidor DNS (*Domain Name Service*) do Active Directory, o que pode ser conferido com o comando `gksudo gedit /etc/resolv.conf` (figura 7).

Com tudo configurado podemos tentar uma autenticação via kerberos. Para isso execute o comando `kinit <usuario>`, no qual devemos utilizar um usuário existente no AD (figura 8), seguido de sua senha. Feito isso execute o comando `klist` e, se o resultado for semelhante ao da figura 8, a operação foi um sucesso.

Winbind

O Samba é o responsável pelo mapeamento dos usuários do Active Directory, por meio do Winbind. Toda a configuração desse serviço está concentrada no arquivo `/etc/samba/smb.conf` e para alterá-lo utilize o comando `gksudo gedit /etc/samba/smb.conf`. Na figura 9 temos um exemplo de configuração, no qual você deve alterar as opções:

- `realm:` para o nome completo do seu domínio em letras maiúsculas;
- `password server:` para o endereço IP de seu servidor de domínio;
- `workgroup:` para o que seria o nome curto de seu domínio.

Reinicie os serviços na ordem indicada na figura 10 e então insira a máquina no domínio com o comando sudo `kinit administrator`. Feito isso utilize o comando `sudo net ads join` e, caso o resultado seja semelhante ao da figura 11, a máquina foi inserida com sucesso no domínio Windows.

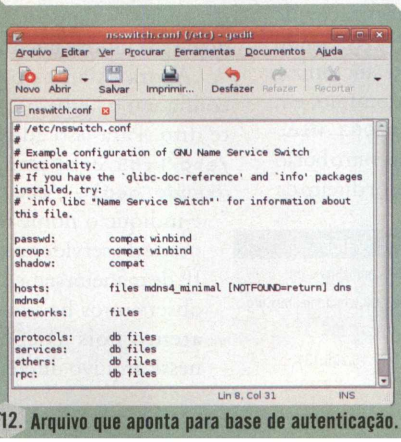
Configurando a autenticação

Uma vez dentro do domínio, precisamos preparar o Linux para a autenticação no AD. O primeiro passo é indicar a ele onde buscar os nomes de usuários e suas senhas. Para isso, edite o arquivo `/etc/nsswitch` (`gksudo gedit /etc/nsswitch.conf`) e acrescente `winbind` aos itens `passwd` e `group` (figura 12).

Depois de configurar o arquivo `nsswitch.conf`, podemos então testar se o winbind está conseguindo obter os usuários e os grupos do AD. Agora utilize o comando `getent passwd` (figura 13) para listar os usuários e `getent group` para listar os grupos (figura 14). Caso você consiga obter usuários que existiam apenas no AD, a configuração foi um sucesso.

No primórdio dos sistemas Unix, toda a autenticação se baseava apenas em conferir a senha do usuário no arquivo `/etc/passwd`, entretanto inúmeros outros meios de autenticação foram criados e se popularizaram, tais como os *smart cards* e os serviços de diretório como o AD. O problema que existia antes é que a cada novo método de autenticação, todas as aplicações que quisessem utilizá-lo teriam de ser reescritas para oferecer suporte a ele. Com o objetivo de solucionar esse problema foi criado o PAM (*Pluggable Authentication Modules*), que permite que as aplicações sejam desenvolvidas sem se preocuparem como a autenticação será realizada. Elas apenas repassam os *tokens* (usuário e senha por exemplo) para o PAM e ele se responsabiliza por verificar a informação, esteja ela onde estiver.

Em nosso caso precisamos configurar o PAM para que ele, além de realizar a autenticação tradicional, também seja capaz de consultar o AD durante o processo de validação de um usuário. Essa configuração pode ser feita editando os arquivos `/etc/pam.d/common-account` (figura 15), `/etc/pam.d/common-auth` (figura 16) e `/etc/pam.d/common-password` (figura 17) com o comando `gksudo gedit <nome-do-arquivo>` e, em seguida, acrescentando o módulo de autenticação



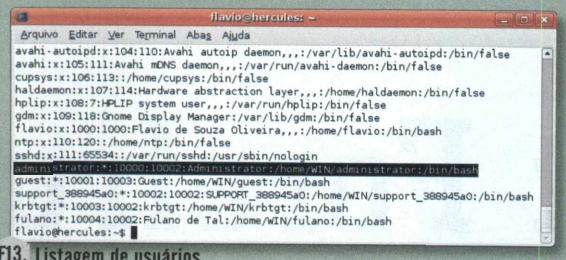
F12. Arquivo que aponta para base de autenticação.

`pam_winbind.so` logo acima do módulo `pam_unix.so` em cada um deles.

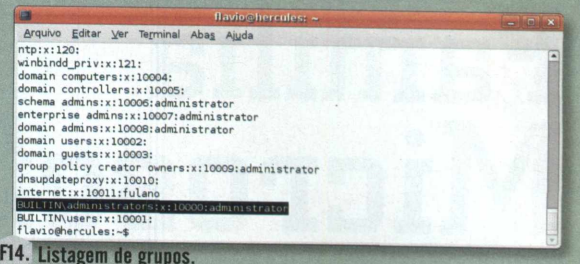
Antes de efetuarmos nossa primeira autenticação, edite também o arquivo `/etc/pam.d/common-session` e acrescente a linha `session required pam_mkhomedir.so umask=0022 skel=/etc/skel` para que o diretório *home* do usuário seja criado caso não exista (figura 18). Em nosso exemplo devemos criar também o diretório `/home/WIN` (`sudo mkdir /home/WIN`), no qual os diretórios *home* dos usuários autenticados via AD serão criados. Feito isso basta efetuar o *logon* com um usuário do Active Directory no Ubuntu e veremos a integração funcionando!

Conclusão

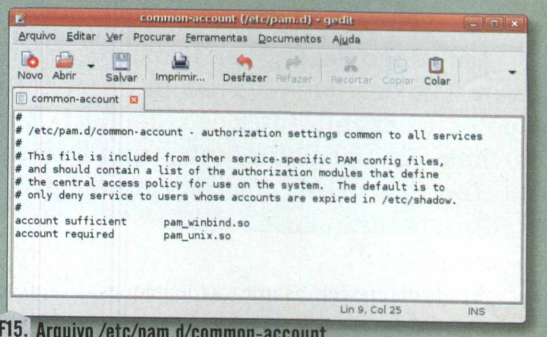
A integração entre o Linux e o Windows através de uma estrutura de autenticação única foi perseguida por muito tempo e nesse momento ela está funcional. Embora já possamos inclusive alterar a senha do AD a partir da estação Linux, ainda restam algumas pequenas lacunas a serem preenchidas, principalmente no que diz respeito à manipulação das políticas de grupo, as famosas GPOs. Mas, no geral, o Winbind pode atender às necessidades da grande maioria dos ambientes e a economia de esforço administrativo proporcionado por sua utilização é extremamente interessante. **PC**



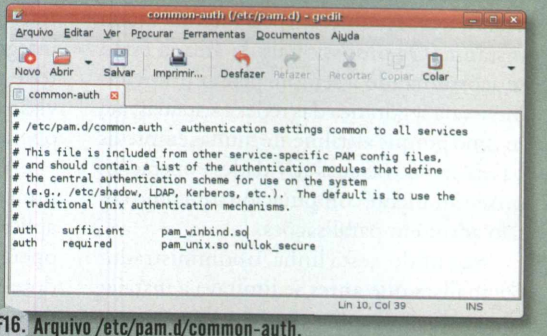
F13. Listagem de usuários.



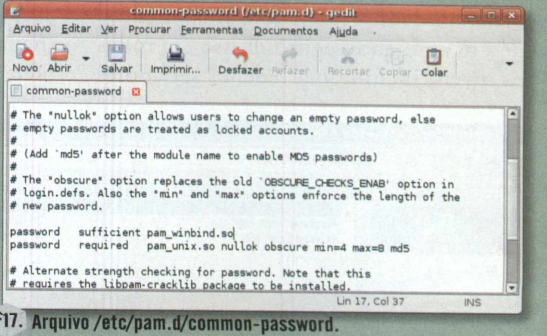
F14. Listagem de grupos.



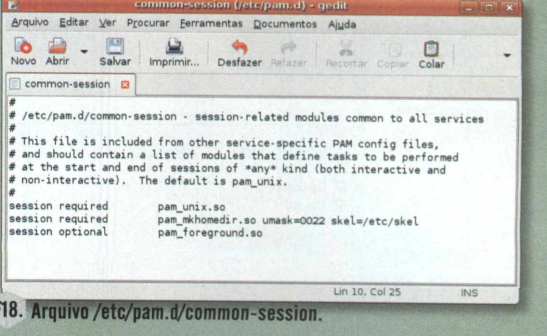
F15. Arquivo /etc/pam.d/common-account.



F16. Arquivo /etc/pam.d/common-auth.



F17. Arquivo /etc/pam.d/common-password.



F18. Arquivo /etc/pam.d/common-session.



Família Microsoft Forefront

Em Junho de 2005, a Microsoft comprou a empresa Sybari Software, que desenvolvia a família de produtos Antigen, voltados para a proteção em ambientes de rede. Nesta matéria, você confere alguns detalhes do trabalho de integração feito às soluções já existentes da Microsoft, e a visão atual da empresa para o aspecto segurança.



Paulo Roberto Sant'anna Cardoso
Formado em Gestão de Redes, possui 6 anos de experiência na área de TI, atuando como técnico, analista e instrutor. Atualmente é MVP na categoria Windows Server - Management Infrastructure.

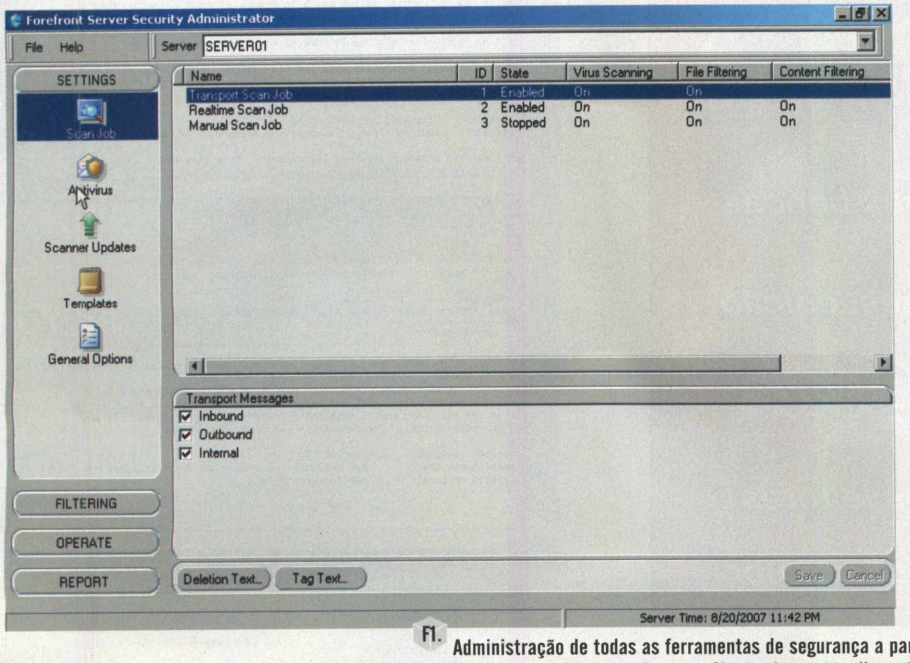
A cada dia crescem as ameaças de ataques a ambientes de rede corporativos. Novas técnicas de acesso, vulnerabilidades descobertas e malwares se proliferam pela Internet a todo instante. Os profissionais da área já estão se acostumando a sempre pensar primeiramente na segurança das redes e sistemas, até mesmo porque atualmente muitas empresas baseiam todas as suas atividades e operações no seu ambiente computacional e, como tal, não admitem paralisações.

Seguindo nesta linha, o administrador ou analista que antes se limitava a instalar o servidor e a aplicação, e se preocupava apenas quando o problema ocorria, agora se preocupa desde o início com a manutenção de um ambiente seguro. E isso em todos os níveis, incluindo a rede, os servidores e as estações de trabalho, o website e a Intranet. Para isso são necessárias diferentes ferramentas, com consoles de administração distintas e conseqüentemente não integradas. Com isso o administrador da rede tem que se desdobrar para ter uma visão de toda a rede e manter o ambiente operacional.

A família Forefront oferece soluções de proteção a estações de trabalho, servidores de aplicação e redes, integrando-se ao ambiente operacional já existente baseado em servidores Windows com Active Directory, por exemplo, e soluções Microsoft para serviços da rede. A simplificação no gerenciamento e a integração são os pontos fortes do Forefront (figura 1). Outra proposta da Microsoft é oferecer uma solução de antivírus e anti-spyware para todo o ambiente, integrando diversos mecanismos de varredura (*engines*) de empresas de segurança líderes da indústria no oferecimento de proteção.

Atualmente a família Forefront é composta pelos seguintes produtos:

- **Forefront Client Security (anteriormente chamado de Microsoft Client Protection)**: utilizado para proteção contra vírus e malwares em estações de trabalho e servidores;
- **Forefront Security for Exchange Server (antigo Antigen for Exchange)**: desenvolvido para trabalhar com o Exchange Server 2007, é utilizado para monitorar e fazer varreduras em e-mails antes que sejam entregues aos destinatários. Aprimora a segurança (até nove *engines* diferentes no antivírus, dentre elas Kaspersky, Computer Associates, Sophos e a própria Microsoft) porque a estação do usuário pode estar sem o cliente do antivírus (Forefront Client, por exemplo) e, nesse caso, a contaminação seria inevitável. Também possui um filtro de conteúdo;
- **Forefront Security for SharePoint (antigo Antigen for SharePoint)**: criado para trabalhar em ambientes de colaboração com o Office SharePoint 2007 e SharePoint Services 3.0, atua prevenindo a publicação de documentos possivelmente contaminados com códigos maliciosos ou conteúdo inadequado;
- **Forefront Security for Office Communications Server 2007 (antigo Antigen for Instant Messaging)**: desenvolvido para monitorar em tempo real as conversas instantâneas e trans-



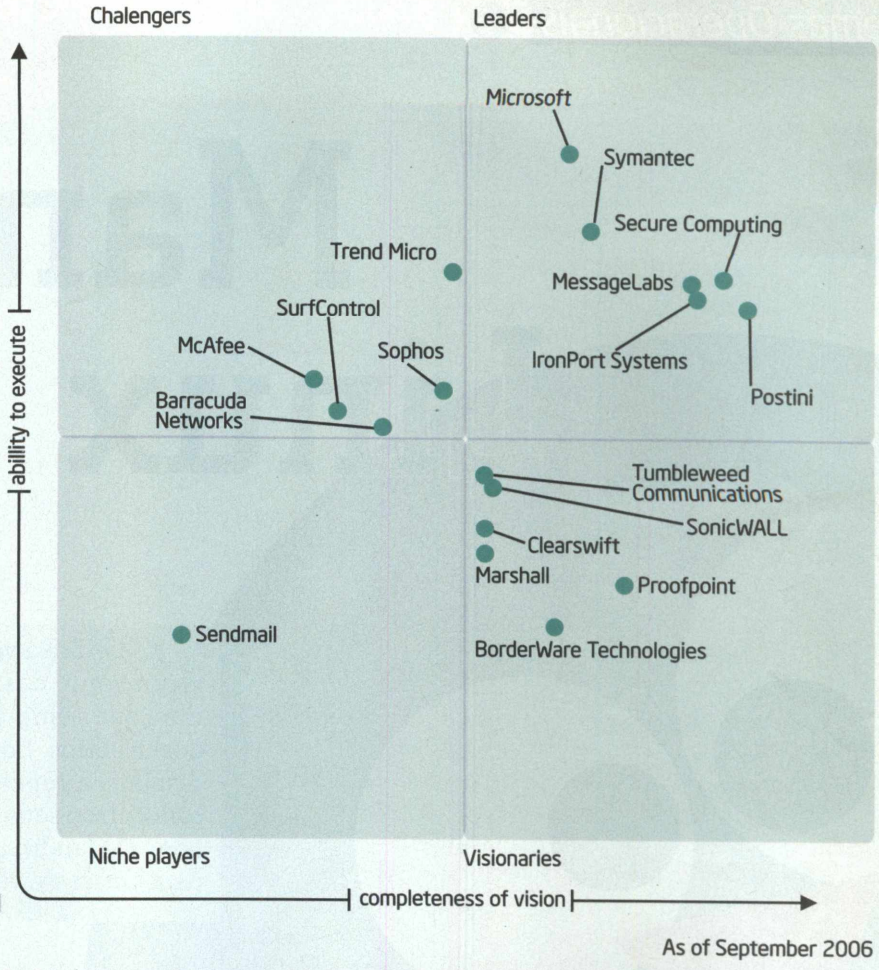
F1. Administração de todas as ferramentas de segurança a partir de uma única console (versões trial do Forefront Security para Exchange Server e Sharepoint, estão disponíveis em www.microsoft.com/forefront/serversecurity/

ferências de arquivos feitas a partir do Office Communications Server 2007. Realiza buscas por vírus e malwares em geral;

• **Internet Security and Acceleration (ISA) Server 2006**: solução de firewall e proxy para proteção à rede e no acesso remoto a partir da Internet.

Vale destacar ainda o armazenamento de eventos centralizado no SQL Server 2005, o que facilita a geração de relatórios e evita a redundância de informações. Além disso, as soluções dessa família também podem ser utilizadas em cenários heterogêneos, com o Forefront para o servidor de colaboração Sharepoint, por exemplo, e uma outra solução de antivírus para servidores e estações de trabalho.

Após o lançamento do Forefront, veja na figura 2 como ficou o posicionamento da Microsoft, no quesito segurança de borda para e-mail, na visão do Gartner. Pretendemos trazer mais detalhes sobre a família ForeFront nas próximas edições. **PC**



Quadrante "mágico" de segurança em e-mails. Fonte: Gartner (detalhes em http://mediaproducts.gartner.com/reprints/microsoft/vol4/article1and2/article1and2.html) F2.

Você já pensou sobre a importância do aterramento da sua máquina?

Assuntos como este você encontra na revista:

SABER ELETRÔNICA
TECNOLOGIA - INFORMÁTICA - AUTOMAÇÃO

Mensalmente nas bancas

www.sabereletronica.com.br

Buscando informações para seu aperfeiçoamento profissional em Automação Industrial?

Encontre-as na revista:

MECATRÔNICA Atual
AUTOMAÇÃO INDUSTRIAL DE PROCESSOS E MANUFATURA

Bimestralmente nas bancas

www.mecatronicaatual.com.br

Mandriva Linux 2008



A Mandriva vem fazendo muito barulho! O sucesso retumbante das versões 2007 e Spring 2007, deixou claro que a empresa havia contemplado as expectativas dos usuários. Com uma receita de sucesso nas mãos e disposta a repetir o bom desempenho, a companhia concentrou seus esforços em melhorar aquilo que já era bom. O Mandriva Linux 2008 é o que muitos esperavam para entrar de vez no mundo Linux.

Daniel Appel

Há algum tempo a revista PC&CIA quer publicar um artigo sobre alguma distribuição GNU/Linux "arrasadora" para uso em Desktops, capaz de substituir o Windows para a maioria das pessoas sem deixar queixas. Acreditamos que este seja o momento para falar do Mandriva Linux 2008.

A versão 2007 foi extremamente aceita pelo público. Pela primeira vez, até quem não gostava do "jeito" do Mandriva reconheceu que eles tinham um belo sistema em mãos. A Mandriva percebeu o que tinha agradado o público e manteve-se fiel à receita na versão 2007.1, lançada na metade do ano, que trouxe muitas atualizações e melhorias, sem destoar da versão anterior. Também foi um sucesso. E aparentemente a Mandriva quer entrar em 2008 com o pé direito, pois o ano nem começou e a família 2008 já foi lançada.

A empresa oferece quatro linhas de produtos. O Mandriva One é um LiveCD, ou seja, um sistema operacional contido em um CD de 700MB e que não precisa ser instalado, pois, todo ele é carregado diretamente na memória RAM do computador. As

restrições de espaço do CD limitam a oferta de softwares, mas nem por isso o One é incompleto. É um sistema muito interessante para quem quiser experimentar sem ter que sair particionando seu HD.

O Mandriva Free é a versão "completa", em DVD. São 4,3GB de programas compactados, devidamente testados e prontos para instalar. Ele vem com tudo que se possa imaginar, desde editores de texto a modeladores de imagens 3D.

O mais poderoso de todos é o Mandriva Powerpack. Ele é a versão comercial, custa U$ 39, tem tudo que o Free tem e ainda uma série de softwares proprietários, dentre eles os tão controversos drivers proprietários para placas de vídeo da nVidia e ATI/AMD. Isso significa que o Free não suporta estas placas? Não, o Free suporta elas também, porém os drivers não estão no DVD e precisam ser baixados do repositório online. Tudo que o Powerpack tem pode ser facilmente instalado no Free também. O atrativo do Powerpack é o suporte técnico oferecido pelo fabricante e a facilidade de ter tudo pronto em um único DVD, sem ter que ficar instalando drivers posteriormente.

Por fim, temos o interessante Mandriva Flash, que é uma variante do One, entretanto roda de um pendrive de 2GB. O Flash também é uma versão paga, e vem em um pendrive personalizado da Mandriva.

Agora que conhecemos os produtos que a Mandriva oferece, podemos escolher aquele que atenda melhor nossas necessidades. Neste artigo vamos falar sobre o Mandriva Free, por ser gratuito e completo. Caso você goste dele vai acabar comprando o Powerpack, já que seu valor de U$ 39 é baixo quando comparado com um pacote de licenças do Windows, Office, Photoshop, 3D Studio, Autocad, etc.

Por que migrar?

No geral os sistemas baseados em Linux estão crescendo muito em aceitação, principalmente por pequenas e médias empresas. Com alto custo e requisitos de hardware inviáveis, muitos usuários e empresas optaram por evitar o Windows Vista, o que cria um momento muito conveniente para uma migração para o Linux.

O Linux não tem as falhas que o Windows XP tem, não pega vírus, além de não ter problemas com spywares. Seus componentes são mais modernos, atualizados constantemente, enquanto o XP continua essencialmente o mesmo desde o seu lançamento no final do ano de 2000. Afinal, sete anos é um tempo longo demais na informática, os ciclos de atualização são de poucos meses.

O Vista é novo e conta com tecnologias muito mais recentes. É uma evolução obrigatória, porém que demorou para chegar e veio com requisitos altos demais. Poucos têm computadores potentes o suficiente para executá-lo com tranqüilidade, a maior parte vai ter uma má experiência ao esbarrar em limitações de memória, já que o Vista só funciona bem mesmo com 2 gigabytes ou mais. Somando isso ao alto custo das licenças, o montante gasto para atualizar um computador e instalar o Vista nele é bastante alto.

O Linux não é tão exigente. Com 512MB é possível trabalhar muito bem, e 1GB são suficientes para comportar vários usuários simultaneamente. O custo com upgrades será virtualmente zero e o custo com licenças pode nem existir se optarmos por uma distribuição gratuita.

É uma oportunidade boa demais para se descartar. Muitas empresas estão fazendo testes piloto com sistemas Linux e muitas já migraram. Por exemplo, em 2007 a Peugeot/Citröen migrou todas as suas vinte mil estações de trabalho para o Suse Linux. O Banco do Brasil converteu 60 mil estações de trabalho, todos os seus servidores já foram convertidos e ainda esperam migrar todos os seus 15 mil caixas eletrônicos para o sistema do pingüim. E a maior parte dos funcionários da rede bancária é de usuários normais de computadores, sem grandes conhecimentos em GNU/Linux, portanto se eles podem utilizar o novo sistema, você também pode. A propósito, o Banco do Brasil alega ter economizado R$ 89 milhões desde 2004, com a substituição das licenças comerciais pelas livres.

Obtendo o mandriva

Acho que todos concordam que vale a pena pelo menos experimentar este sistema. Ele é gratuito, vale a máxima "não custa nada tentar". Para obtê-lo, acesso o site da Mandriva em **www.mandriva.com.br** e clique no link "Download". Neste site você pode escolher se quer baixar o One ou o Free, que são gratuitos. Selecione o país de onde prefere baixar (há um mirror brasileiro) e ele lhe apresentará o link para download. Existe a possibilidade de baixar um arquivo .torrent se você preferir.

O Free tem aproximadamente 4,3GB, portanto o download pode demorar bastante.

Quando terminar, você terá um arquivo ISO gigante. Utilize o Nero ou outro programa de gravação para gerar um CD a partir desta imagem. Este é um procedimento que muita gente erra, portanto é importante saber que não devemos criar um DVD de dados e arrastar o arquivo ISO lá para dentro. Você precisa utilizar uma função especial chamada "Gravar imagem de DVD", ou "Criar DVD a partir de imagem" (o nome pode variar dependendo do programa usado) e então, selecionar o arquivo ISO.

Instalação

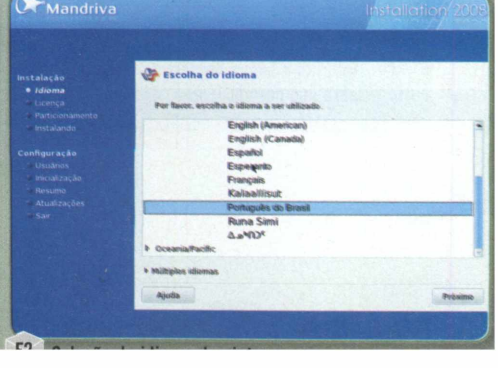
Inicie o computador no qual o sistema será instalado com seu novo DVD no drive. Certifique-se de ter configurado o BIOS de forma que o CD-ROM seja o primeiro dispositivo de boot (ou utilize o recurso boot-menu, se sua placa suportá-lo).

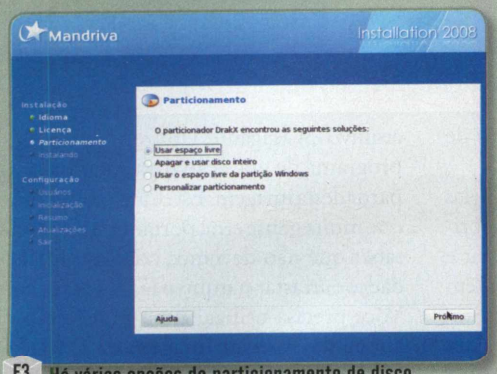
O DVD apresentará um menu de opções em inglês, a língua padrão da informática. Não é difícil trocar para o português, basta pressionar F2 e selecione "Português (Brasil)". O menu de boot muda seu idioma automaticamente, mas não há real necessidade de fazer isso aqui, pois logo adiante o instalador perguntará novamente qual a língua desejada. Além disso, a opção "Install Mandriva Linux 2008 on your system" é clara o suficiente mesmo para quem não domina a língua inglesa (figura 1).

Ao iniciar o processo de instalação devemos esperar o sistema realizar o boot. Durante esta etapa ele analisará seu hardware e carregará os

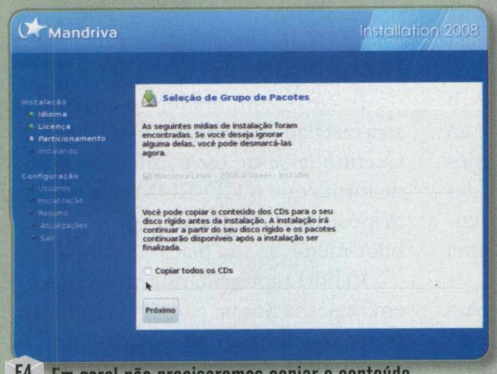


F1. Menu de inicialização do DVD

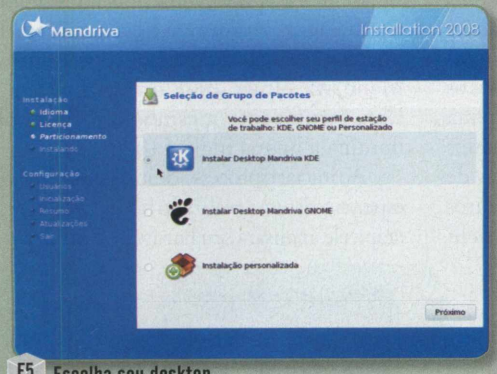




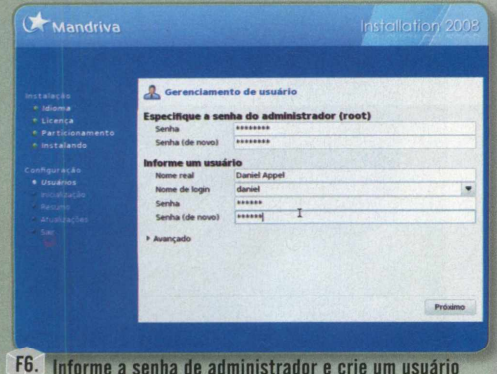
F3. Há várias opções de particionamento de disco. Escolha cuidadosamente e tenha sempre um backup dos seus dados.



F4. Em geral não precisaremos copiar o conteúdo do DVD, exceto se quisermos usá-lo em outros computadores ao mesmo tempo.



F5. Escolha seu desktop.



F6. Informe a senha de administrador e crie um usuário para uso normal.

drivers adequados, identificando inclusive a maioria das controladoras SCSI do mercado. Não deve demorar mais do que um minuto ou dois, dependendo da velocidade do seu computador, e logo ele perguntará o idioma a ser usado (figura 2). Selecionamos "Português do Brasil", porque a configuração "Português" representa o idioma de Portugal, ligeiramente diferente do nosso.

Na próxima tela será mostrado o contrato de licença, que tem apenas cinco itens de rápida leitura. Se você concordar com os termos da licença, clique em "Próximo" para continuar a instalação.

Agora é o momento mais crítico da instalação: o particionamento do disco rígido.

Se a intenção for instalar um único sistema, o Mandriva, as coisas são fáceis. No menu da figura 3, basta selecionar "Usar espaço livre" se o disco não tiver nenhuma partição. Se ele tiver dados que você não queira mais, selecione "Apagar e usar disco inteiro".

Mas muitos preferem manter uma cópia do Windows em Dual-Boot para ter como recorrer a ele, caso não saibam fazer algo no novo sistema. Isso infelizmente não funciona: a tendência natural do ser humano é ser preguiçoso e o usuário vai estacionar no Windows, o Mandriva vai acabar esquecido no HD. Se você estiver decidido a migrar seus computadores para o Linux, é muito mais interessante criar uma máquina virtual Windows rodando no VirtualBox (que vem com o Mandriva) do que fazer Dual-Boot.

É claro que em alguns casos é realmente necessário ter uma cópia do Windows (para rodar jogos exclusivos desta plataforma, por exemplo), portanto vou explicar como fazê-lo. Em primeiro lugar, não é recomendável "reciclar" uma instalação já existente. O Mandriva precisa de uma partição para si e redimensionar uma já existente (e ocupada) para abrir espaço é uma técnica não recomendável. Os riscos envolvidos são grandes, de forma que um backup total não é apenas recomendável como é mandatório. E se tivermos que fazer um backup do conteúdo do disco, por quê não reparticioná-lo logo e reinstalar o Windows? Se você estiver 100% seguro de que quer arriscar o redimensionamento da partição do Windows (e tiver feito um backup), a opção a escolher é a "Usar o espaço livre da partição Windows". O Mandriva fará automaticamente a redução e criará suas partições.

A propósito, só no parágrafo anterior você encontrou três vezes a palavra "backup", não encontrou? Com essa última já são quatro, depois não venha nos dizer que não avisamos!

Particularmente não confio no redimensionamento de partições, portanto tenho como prática padrão reparticionar o disco, mesmo que isso signifique ter que reinstalar o Windows (o que é bom fazer de vez em quando). No próprio instalador da Microsoft há uma ferramenta de particionamento, capaz de remover as partições e criar uma nova com tamanho definido (crie apenas uma e não ocupe o disco todo). A versão em DVD do Mandriva vem com muitos programas e pode exigir muito espaço em disco, portanto é recomendável reservar-lhe de 5 a 10 Gigabytes. Ainda temos que contar com os documentos de usuário, portanto procure deixar mais do que isso.

Instale o Windows normalmente. Em sistemas Dual-Boot ele deve sempre ser instalado antes do Linux, o motivo para isso, é que o Windows não admite a existência de outros sistemas e remove seus gerenciadores de boot do MBR. Se você já tivesse instalado o Mandriva antes, teria a desagradável surpresa de vê-lo "desaparecer" e o computador entrar diretamente no Windows. Após a instalação do Windows e tendo uma reserva de espaço não particionado no seu HD, basta iniciar o instalador do Mandriva e selecionar "Usar espaço livre" no menu da figura 3.

Na tela da figura 4, o Mandriva quer saber se deve copiar o conteúdo do DVD para o disco rígido antes de instalar. Quando a instalação é feita a partir de CDs pode ser muito prático copiá-los todos para o HD e ir embora sem ficar se preocupando em voltar para inserir o próximo CD. Como o DVD é um só e não precisamos ficar trocando de disco, o único uso desta função é poder removê-lo do leitor e iniciar a instalação em outro computador simultaneamente, sem ter que gravar várias mídias. A maioria simplesmente clicará em "Próximo".

Última pergunta antes de começar a instalação dos pacotes: qual o ambiente Desktop será usado (figura 5)? As duas opções: KDE e Gnome representam as duas interfaces mais tradicionais do mundo Open-Source, am-

bas muito eficientes. O KDE tem um layout mais parecido com o Windows e muitos se familiarizam mais rapidamente com ele, mas isto não é sinônimo de qualidade e ambos são excelentes. Há também a opção de personalizar sua instalação, que exige um pouco mais de conhecimento sobre os diferentes pacotes que compõe o mundo GNU/Linux.

Não se preocupe, pois é possível (e por sinal muito fácil) instalar a outra interface depois que tudo estiver pronto. Para os exemplos deste artigo a escolha foi o KDE.

Escolha o seu e inicie a instalação. Esta é a etapa mais demorada de todo o processo. Faça outra coisa enquanto o sistema descompacta vários gigabytes de programas e os instala no seu HD. O tempo total dependerá da velocidade do seu hardware.

Quando ele terminar será iniciado a configuração do sistema. Você precisará informar a senha do usuário root (o administrador do sistema) e criar um usuário de trabalho (figura 6). No Linux sempre se trabalha usando um usuário normal, sem poderes de administrador, ou seja, que não pode afetar as configurações nem alterar o sistema. Quando for necessário alterar algo basta informar a senha do administrador, depois faça a alteração e logo em seguida retorne ao trabalho com o usuário normal. Jamais misture os dois, nunca se usa o root para trabalhar, e também não se deve colocar a mesma senha em ambos.

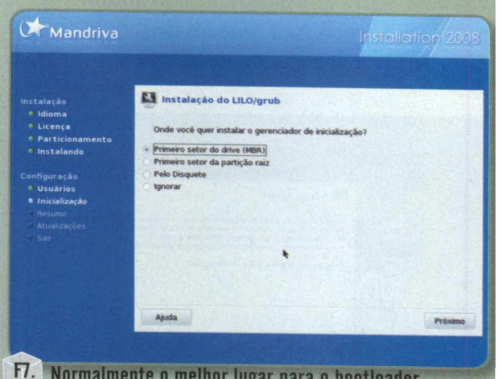
A próxima etapa é instalar o gerenciador de boot (figura 7), mas esta tela só aparece se o instalador encontrar um MBR já ocupado, o que é normal em discos rígidos que já tinham um boot-loader instalado. Se o seu disco estiver com o MBR livre o instalador o utilizará automaticamente. O melhor lugar para colocar o boot-loader do Mandriva é mesmo no MBR e você pode aceitar esta opção. Não utilize o primeiro setor da partição raíz, porque é lá que o Windows coloca o seu próprio gerenciador de boot e você não conseguirá mais iniciá-lo.

Agora a resolução da tela (figura 8). Escolha seu monitor em uma lista de vários fabricantes e modelos, ou simplesmente selecionar um tipo genérico. Quem já tiver um monitor LCD não precisa se preocupar com taxas de atualização, simplesmente selecione "Flat Panel" e a resolução esperada. Usuários de CRT precisam acertar a taxa de atualização, e esta informação pode ser encontrada no manual do produto.

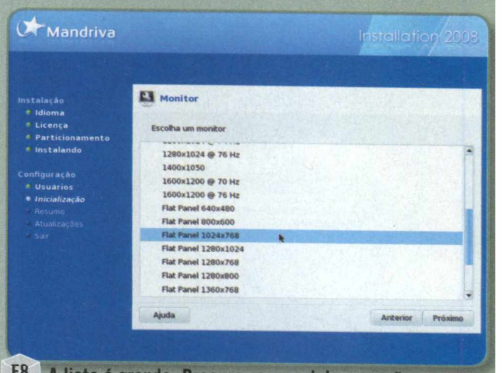
Estamos quase no final, o instalador nos apresenta o resumo das configurações do sistema (figura 9) e oferece a chance de mudá-las. Não deixe de conferir suas configurações de rede, especialmente se você precisa de algum tipo de autenticação PPPoE. O restante normalmente está correto. No entanto, há algo que incomoda os usuários na configuração do gerenciador de boot do Mandriva. Nossa sugestão é que faça algumas mudanças, clicando no botão "Configurar" ao lado do item "Inicialização".

O gerenciador de inicialização é o boot-loader, e aqui podemos modificar os itens do menu de boot. Segundo a figura 10, vemos que há quatro opções de boot, chamadas "linux", "linux-nonfb", "failsafe" e "windows", que não são muito explicativas e por sinal muito deselegantes, já que são exatamente estes os nomes que aparecerão na inicialização do computador. Selecionando a opção "linux", pressione o botão "Modificar" e você irá para a tela da figura 11. Aqui, substitua o nome "linux" pelo que você quiser, como "Mandriva Linux".

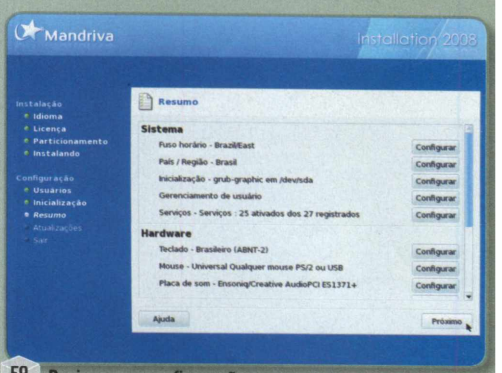
Você pode colocar o nome que quiser aqui, mas não altere as demais configurações. Pressione "Ok" e observe que você voltou para a tela anterior, mas agora o primeiro item mudou de nome. Existe a possibilidade de alterar os outros nomes e também de remover itens indesejados. A figura 12 mostra nossas configurações prontas. Veja que foi removida a opção "linux-nonfb", pois não vamos usá-la. Além disso, foram editados os demais



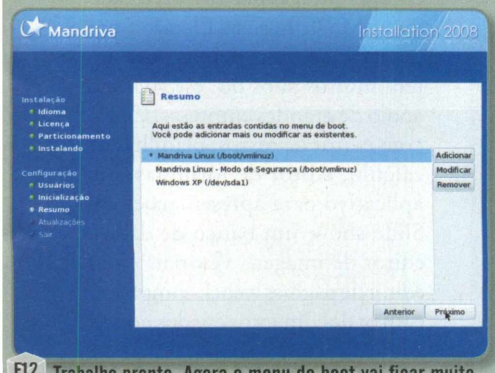
F7. Normalmente o melhor lugar para o bootloader é o MBR.



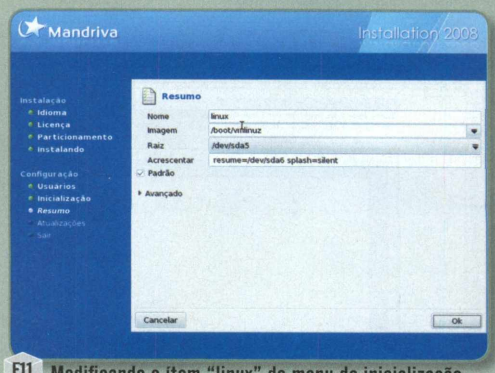
F8. A lista é grande. Procure seu modelo e se não encontrá-lo, utilize um genérico.



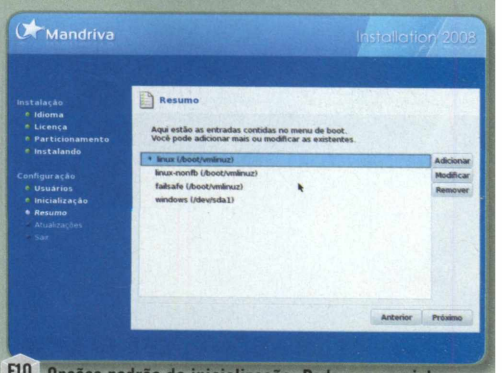
F9. Revise suas configurações.



F12. Trabalho pronto. Agora o menu de boot vai ficar muito mais claro



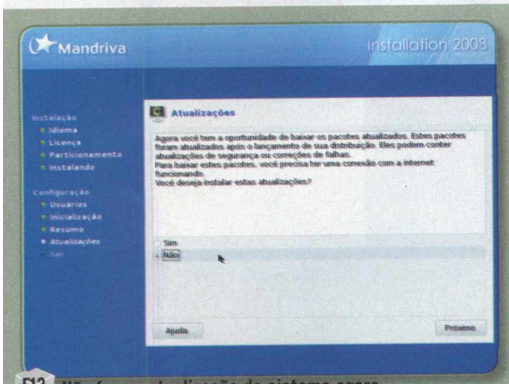
F11. Modificando o item "linux" do menu de inicialização. Coloque o nome que mais lhe agradar.



F10. Opções padrão de inicialização. Podemos caprichar aqui

nomes para "Mandriva Linux – Modo de seguranca" e "Windows XP".

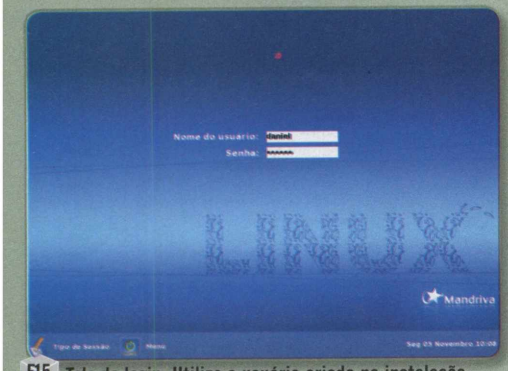
Com as configurações devidamente ajustadas, clique em "Próximo" para voltar à tela da figura 9 e avance clicando novamente em "Próximo". Se a rede foi detectada corretamente o instalador oferecerá a possibilidade de instalar as atualizações disponíveis no site da Mandriva (figura 13), porém este procedimento pode demorar bastante e não recomendo fazê-lo agora. Selecione "Não" e avance para a última tela, onde você terá a função de reiniciar o sistema. Parabéns, a instalação está concluída, mas não se esqueça de remover o DVD do drive ou correrá o risco de iniciar a instalação novamente.



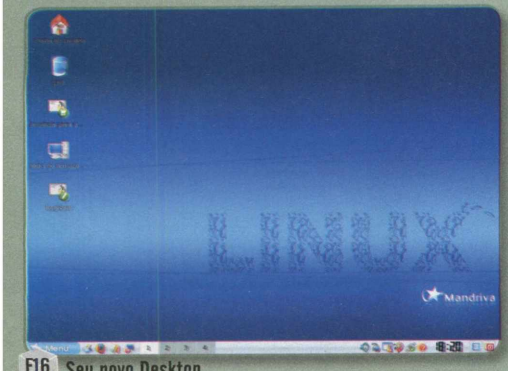
F13. Não faça a atualização do sistema agora.



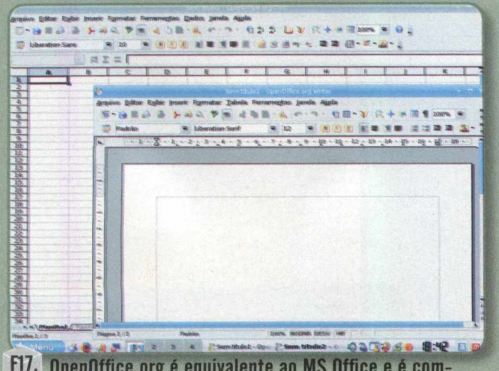
F14. Menu de boot do Mandriva, exatamente da forma que foi configurado nos passos anteriores.



F15. Tela de login. Utilize o usuário criado na instalação.



F16. Seu novo Desktop.


F17. OpenOffice.org é equivalente ao MS Office e é compatível com seus documentos

Iniciando

Ao reiniciar o computador ele não entrará mais diretamente no Windows, mas apresentará a tela da figura 14, onde é possível escolher o sistema a ser usado. Se você caprichou na configuração do gerenciador de inicialização, verá nomes de sistemas bastante explicativos.

Aqui vemos uma diferença muito importante entre o Windows e o Mandriva. Enquanto o Windows apaga o MBR da forma mais desrespeitosa se encontrar outro sistema instalado, o Mandriva cria este útil menu, é por isso que sempre se instala o Windows primeiro e o Linux depois.

Ao entrar no Mandriva pela primeira vez, ele solicita algumas informações sobre você e oferece a possibilidade de criar uma conta no Mandriva Club, que oferece acesso gratuito a comunidade online, artigos técnicos e etc. Você pode optar se quer preencher os formulários de registro ou se quer cancelá-los e simplesmente avançar para a tela de login (figura 15), onde você deve utilizar o usuário criado durante a instalação (lembre-se que não se deve usar o root para trabalhar).

Bem-vindo ao desktop do seu Mandriva Free 2008 (figura 16). Este é o KDE, que foi o ambiente desktop escolhido para este exemplo. Quem optou pelo Gnome perceberá um layout de tela um pouco diferente, mas as funções são exatamente as mesmas. Este desktop já está plenamente funcional e você já pode trabalhar. Nele já foram instalados editores de texto, planilhas de cálculo, editores de imagens, navegadores e praticamente tudo que se possa precisar.

Saiba um pouco mais sobre alguns dos programas instalados:

OpenOffice.org

O pacote de aplicativos de escritório que acompanha o Mandriva é o famoso OpenOffice.org (figura 17).

Desenvolvido pela StarDivision em 1984 para computadores baseados no chip Z80 e posteriormente portado para DOS e Windows, o StarWriter era apenas um editor de textos até que em 1994 tornou-se uma suíte completa com o nome de Star Office. Programado em linguagem C++ e utilizando bibliotecas multi-plataforma, tornou-se propriedade da Sun Microsystems (a criadora do Java) quando esta comprou a StarDivision em 1999.

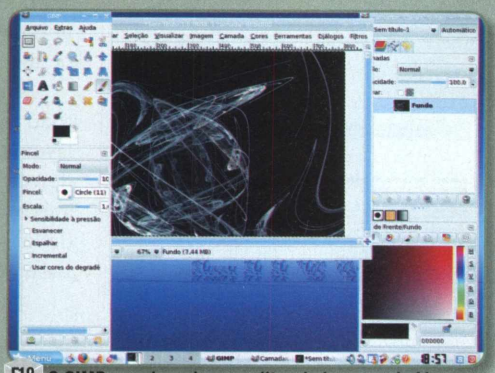
Naquele momento a Sun tinha mais de 40 mil funcionários, cada um com uma estação de trabalho Unix e um notebook com Windows. Ao invés de comprar 40 mil licenças do MS Office (para os notebooks) e quarenta mil do StarOffice (para as workstations), a Sun comprou toda a StarDivision. Logo lançou a versão 5 do StarOffice, gratuita e compatível com Solaris, Unix, Linux e Windows.

A empresa então abriu a maior parte do código do StarOffice e deu o chute inicial para a o projeto OpenOffice.org, que é mantido pela comunidade de programadores que adotou o projeto e recebe contribuições também da própria Sun. Além de ter se livrado dos problemas com licenças e incompatibilidades por ter uma suíte que funciona em qualquer sistema, a Sun agora faz concorrência com o Office da Microsoft. Aparentemente a compra da StarDivision foi um bom negócio.

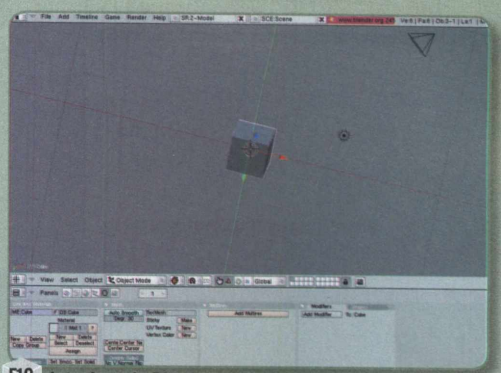
O OpenOffice.org é um pacote de aplicativos de escritório muito competente, capaz de fazer tudo que o MS Office faz. Ele não é um projeto amador, pelo contrário, tem muitos anos de "estrada" e o apoio de grandes empresas. Conta com editor de textos, planilhas de cálculo, editor de fórmulas, um aplicativo para apresentações em Slide-show, um banco de dados, editor de imagens vetoriais e um editor de páginas web. É compatível com os documentos criados no MS

Office e também conta com suporte ao ODF, o formato de documentos mais bem aceito atualmente, e que inclusive foi aceito como padrão ISO.

Sua interface é muito parecida com a do MS Office, portanto mesmo quem estiver muito bem adaptado a este conseguirá migrar sem nenhuma dificuldade.



F18. O GIMP, o mais poderoso editor de imagens do Linux.



F19. Interface do Blender.

The GIMP

O principal editor de imagens bitmap do mundo Open-Source, é muitas vezes comparado ao Photoshop. Mas não se trata de um "clone", o GIMP (figura 18) é um programa com identidade própria que tem capacidades muito semelhantes as do software da Adobe, mas de forma alguma tenta ser igual.

O resultado final é um programa que tem ferramentas próprias, apesar de algumas também existirem no Photoshop, afinal muitas funções são básicas para edição de imagens e não há como não tê-las. Já outras são exclusivas do GIMP e não são encontradas em nenhum outro programa. Isso faz do GIMP um programa de edição de imagens extremamente poderoso e capaz de fazer qualquer coisa.

Blender

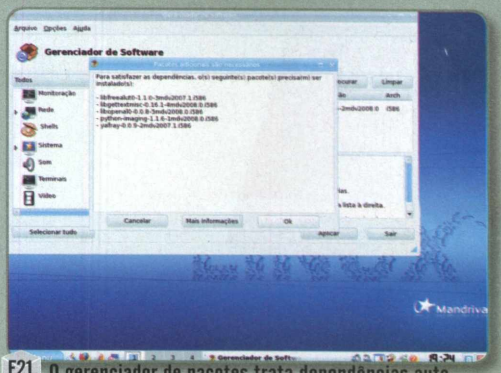
É um dos programas de modelagem 3D mais conhecidos do mundo, comparável em qualidade e recursos aos grandes nomes da indústria como Maya e 3D Studio.

Este programa também tem uma história interessante. Criado pela Not a Number Technologies, o Blender era um software comercial até 2002, quando a empresa faliu. Os detentores dos direitos concordaram em abrir o código-fonte mediante um pagamento de mais de U$ 100 mil dólares, que foi arrecadado através de doações da comunidade open-source. Em pouco mais de um mês o dinheiro foi recolhido e os direitos do software adquiridos pela Fundação Blender, que imediatamente mudou sua licença para a GPL e tornou-o eternamente open-source (figura 19).

Desde então, o Blender vem sendo usado para modelar personagens de jogos 3D, peças de engenharia, desenvolvimento de design de embalagens e até na criação de filmes. O exemplo mais famoso é o filme Elephants Dream (figura 20), que foi criado utilizando apenas softwares Open-Source e se encontra disponível para download gratuito em: **www.elephantsdream.org**. Há outros como o Peach e o Plumíferos em franco desenvolvimento.



F20. Cena de Elephants Dream, o primeiro Open-Film do mundo.



F21. O gerenciador de pacotes trata dependências automaticamente. Mas ele toma o cuidado de lhe avisar o que será instalado além do software solicitado.

Instalando mais softwares

Por padrão o Mandriva Free não instala todos os softwares contidos no DVD, apenas os mais usados. Por exemplo, o software Blender, que foi citado acima, não é instalado por padrão, pois a verdade é que poucas pessoas trabalham com modelos tridimensionais. Agora vamos mostrar como instalá-lo, e este procedimento vale para qualquer outro software.

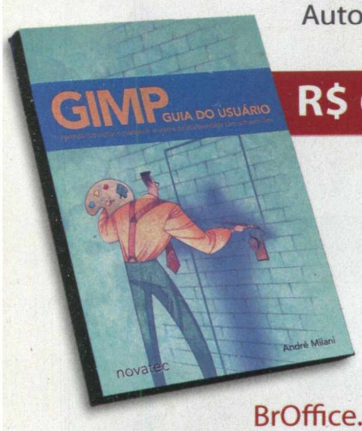
Ao contrário do Windows, no Linux não devemos baixar o instalador do software e executá-lo. Distribuições como a da Mandriva contam com um gerenciador de pacotes, que é um tipo de instalador-mestre, que serve para instalar qualquer programa de forma padronizada. É muito prático.

Clique no botão "Menu" e selecione "Instalar & Remover Softwares". Você será solicitado a digitar a senha de root, aquela senha de administração criada durante a instalação do sistema. Logo após, receberá uma mensagem de boas-vindas e em seguida deverá responder se deseja adicionar novas fontes de mídia. Por hora responda "Não", porque o software que vai ser instalado está presente no DVD.

Agora que você chegou até o gerenciador de pacotes, verá várias categorias de softwares disponíveis para instalação. Como o nome do programa é conhecido, digite "blender" no campo de pesquisa na parte superior da janela. Aparecerá uma lista com os softwares encontrados com aquele nome, neste caso apenas um, e ao lado uma caixinha vazia, onde você deve clicar para "marcar" a instalação daquele software. Se o software a ser instalado precisar de outros componentes, surgirá uma janela dizendo quais outros componentes serão instalados (figura 21). Aceite estes componentes clicando em "Ok" e verá que o Blender foi marcado para instalação, representado pela seta verde na figura 22. Clique em "Aplicar" e o software será instalado, junto com todas as suas dependências. Se o DVD não estiver

Literatura Técnica
Que não pode faltar em sua biblioteca
www.sabermarketing.com.br

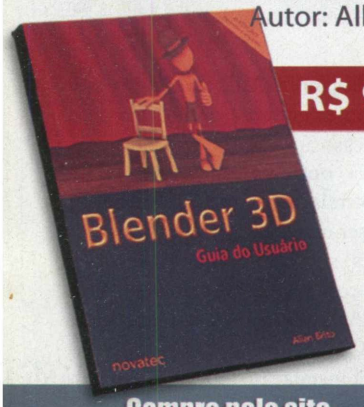
GIMP - Guia do usuário
336 páginas
Autor: André Milani
R$ 68,00



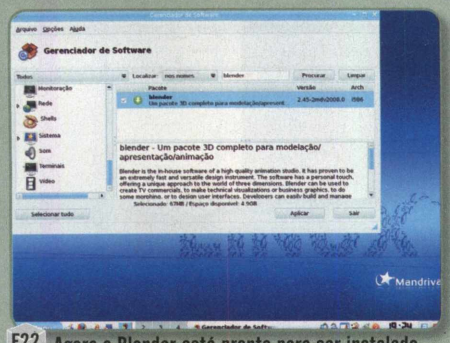
BrOffice.org – da teoria à prática
192 páginas
Inclui CD com vídeos de exemplo
Autor: Edgard Alves Costa
R$ 38,25



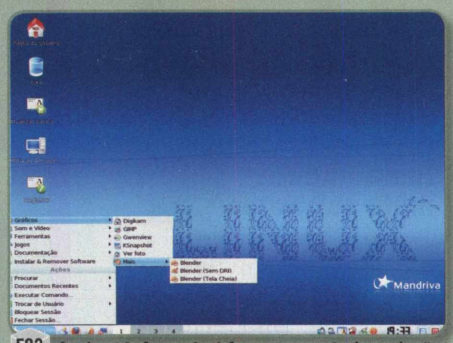
Blender 3D - Guia do usuário - 2ª edição
496 páginas
Autor: Allan Brito
R$ 98,00



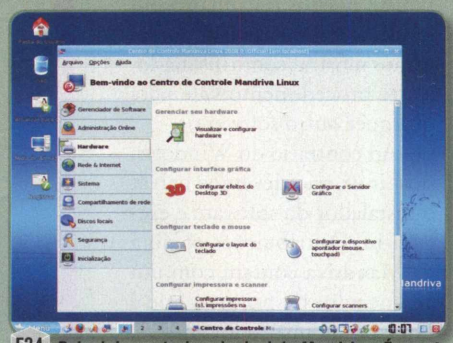
Compre pelo site
www.sabermarketing.com.br
ou fone (11) 6195-5330
Para acesso ao catálogo completo:



F22. Agora o Blender está pronto para ser instalado. É só aplicar sua seleção de softwares.



F23. Aqui está. Agora é só fazer suas próprias criações tridimensionais.



F24. Painel de controle principal do Mandriva. É possível mudar qualquer coisa no sistema.

no leitor, ele será solicitado.

Após instalado, podemos acessar o Blender pelo pelo menu "Gráficos", como na figura 23.

Configurações

Durante a instalação foram apresentadas configurações básicas sobre o hardware do computador. Você não está, no entanto, limitado a isso. Há um painel de controle muito completo que você pode acessar pelo botão "Menu", "Ferramentas", "Ferramentas do Sistema", "Configure seu computador". Este programa também pede a senha de administrador, portanto fique tranqüilo, pois nenhum usuário vai mexer sem sua permissão.

Aqui (figura 24) você pode alterar todo tipo de configuração, desde simples layout de teclado até compartilhamentos de rede. Pode adicionar novos usuários, ou até configurar o Compiz-Fusion, aquele desktop 3D que tem feito tanto sucesso. Basta seguir os passos do assistente.

Conclusão

Aqui você teve uma breve introdução ao Mandriva Linux 2008, seu download, instalação, configuração e apresentação de alguns dos principais softwares que o acompanham. Com apenas um DVD é possível ter uma enorme gama de softwares sem ter que pagar por nenhuma licença. Isto reduz drasticamente o custo de implantação, por exemplo, de uma rede de computadores de uma empresa ou escola.

Conhecendo este sistema você terá a certeza de que o Linux está pronto sim, para ser usado em sistemas Desktop, tanto pessoais quanto corporativos. A verdade é que, exceto por alguns aplicativos altamente específicos, para os quais os fabricantes insistem em não criar versões para Linux, tudo que usuários normais e avançados necessitam pode ser oferecido por um desktop Linux.

E ao contrário do que alguns "engraçadinhos" gostam muito de espalhar por aí, o Linux não exige que se saiba usar a linha de comando. Esta ferramenta está lá e é muito poderosa, mas quem não quiser usá-la não precisará fazê-lo, pois é perfeitamente possível fazer tudo no ambiente gráfico. Você pôde comprovar isto neste artigo.

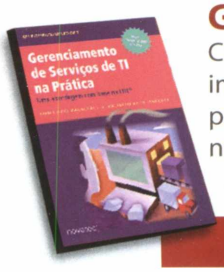
O que não é possível fazer, infelizmente, é falar sobre todas as qualidades deste sistema em apenas um artigo. Temos ainda uma série de coisas para mostrar, mas terá que ficar para a próxima edição. Até lá, explore seu novo sistema e se acostume com ele. Aproveite para se inscrever em uma das diversas comunidades online para trocar experiências com outros usuários, há tanto iniciantes quanto pessoas já mais experientes. Muitas pessoas se tornam especialista nestes sistemas ao trocar idéias cada vez mais avançadas com pessoas com os mesmos interesses.

E não deixe de nos mandar sua opinião e sugestões por email.

PC

LITERATURA TÉCNICA

Que não pode faltar em sua biblioteca



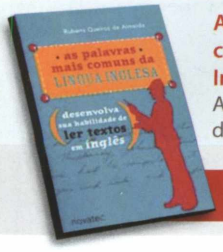
Gerenciamento de Serviços de TI na Prática - Uma abordagem com base na ITIL

Com o crescente aumento da dependência das organizações em relação à Tecnologia da Informação (TI), a importância do Gerenciamento de Serviços de TI torna-se maior a cada dia. É uma excelente oportunidade para a TI demonstrar seu valor e competência no sentido de alavancar e levar inovação aos processos de negócio. Mas não é uma tarefa simples. Demanda clareza de foco e muita atenção da área de TI.

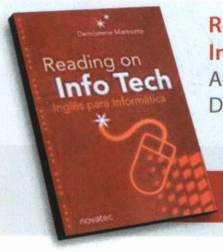
Autores: Ivan L. Magalhães / Walfrido B. Pinheiro

R$ 129,00

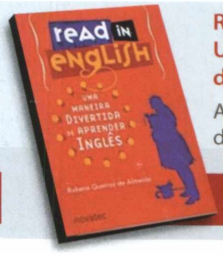
LANÇAMENTO



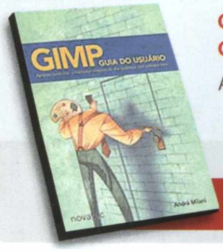
As palavras mais comuns da Língua Inglesa - 2ª edição
Autor: Rubens Queiroz de Almeida
R$ 53,00



Reading on Info Tech: Inglês para informática
Autor: Demóstene Marinotto
R$ 39,00



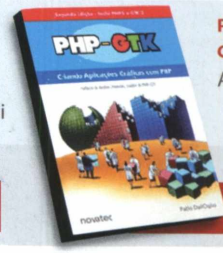
Read in English: Uma Maneira Divertida de Aprender Inglês
Autor: Rubens Queiroz de Almeida
R$ 48,00



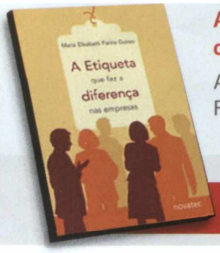
GIMP
Guia do Usuário
Autor: André Milani
R$ 68,00



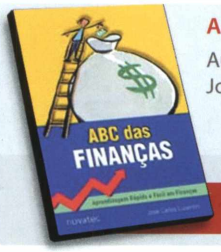
Blender 3D
Guia do Usuário
(2ª edição)
Autor: Allan BritoFranchi
R$ 98,00



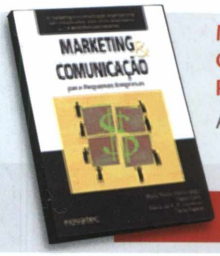
PHP-GTK
Criando Aplicações Gráficas
Autor: Pablo Dall'Oglio
R$ 75,00



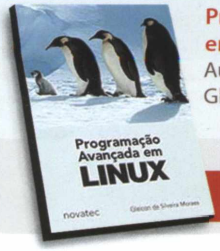
A Etiqueta que faz a diferença nas empresas
Autor: Maria Elisabeth Farina Guirao
R$ 39,00



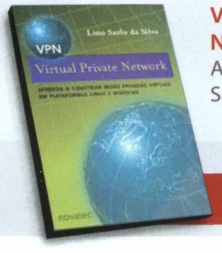
ABC das Finanças
Autor: José Carlos Lucentini
R$ 33,00



Marketing & Comunicação para Pequenas Empresas
Autor: Diversos
R$ 32,00



Programação Avançada em Linux
Autor: Gleicon da Silveira Moraes
R$ 46,00



Virtual Private Network - VPN
Autor: Lino Sarlo da Silva
R$ 43,00



Comandos do Linux Guia de Consulta Rápida
Autor: Roberto G. A. Veiga
R$ 22,00

Compre pelo site **www.sabermarketing.com.br**
ou fone **(11) 6195-5330**

*Os preços estão sujeitos a alteração sem prévio aviso. Para maiores informações acesse www.sabermarketing.com.br
*O frete não esta incluído no valor do produto, sendo calculado de acordo com a localidade e tipo de envio.

MSI
MICRO-STAR INTERNATIONAL

innovation with style

Tenha o melhor desempenho - Sempre!

Inovador, Dinâmico, Exclusivo



K9N6SGM-V



- NVIDIA MCP61S Chipset
- Suporta AM2 AMD Athlon 64/X2/FX Processadores
- Suporta HyperTransport 2GT/s
- Suporta Dual Ch. DDR2-800/667/533
- 1 x Slot PCI Express 16x
- 2 PCI v2.3 slots
- 2 SATA2 3Gb/s
- Suporta 7.1Ch.HD áudio
- LAN 10/100

945GCM5-F



- Intel 945GC Express Chipset Based
- Suporta LGA775 Intel Core 2 Duo Processador
- Suporta 2 DIMMs Dual Ch. DDR2-667
- 1 PCI Express x16& 2 PCI slots
- Suporta 4 SATA 2 3Gb/s
- Suporta HD áudio
- Suporta Gb Lan

20th Marching to Future Technology

www.msicomputer.com.br

ABANO www.abano.com.br 21 2196 1100

ALCATEIA www.alcateia.com.br 11 3226 2626

ALDO www.aldo.com.br 44 3261 2000

handytech DISTRIBUIDORA www.handytech.com.br 71 2107-7700

INGRAM MICRO www.ingrammicro.com.br 11 3677 5900

SND www.snd.com.br 11 2187 8333