Série Certificação Microsoft
Domine o Vista

Queima de Placas-mãe
Aprenda a lidar com esse problema

VoIP Como usar seu número mundial sem precisar de PC



PC & CIA

www.revistapcecia.com.br

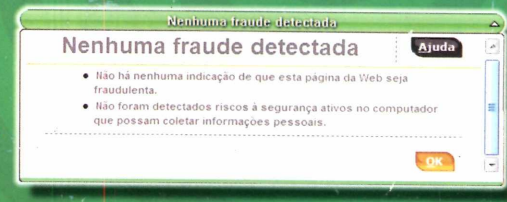
ANO 7 - Nº 73 - Agosto / 2007 Europa €4,30 - Brasil R$12,90

SABER

Proteção máxima na Internet

Testes com as principais suítes

Pegue aqui sua receita para evitar o lixo eletrônico



PC básico e poderoso!

- ✓ Custo, performance e consumo de energia
- ✓ AMD, Intel ou NVIDIA?
- ✓ Testes apontam a plataforma ideal para você

ISSN 1519-5267



Memórias de Alta Performance

9 pares de módulos e muitas surpresas

E mais: overclock do Core 2 Duo mais barato


COOLER MASTER
COSMOS
ALTA PERFORMANCE COM SILÊNCIO ABSOLUTO
Por trás de uma aparência serena, a melhor estrutura térmica e silenciosa que você já viu!
Seis gavetas independentes para HD, pressão interna de ar auto-ajustável e uma inovadora ventilação com dupla entrada de ar inferior, para um sistema high-end à prova de ruído.
VISITE NOSSO SITE
WWW.COOLERMASTER.COM.BR
http://www.coolermaster.com/events/2007/newsitelaunch/

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
Adriano A. Góes, Daniel Appel
Fernando Vieira, Flávio de Souza Oliveira
Igor Humberto, Luiz Felipe de Camargo
Jansen Carlo Sena, Marcus Brandão de Moura
Paulo Roberto Sant´anna Cardoso,
Roberto Cunha

Auxiliar de Redação
Claudia Tozetto
Fabieli de Paula

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

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

Associação Nacional dos Editores de Revistas.
ANATEC ASSOCIAÇÃO DE PUBLICAÇÕES
www.anatec.org.br

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

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.

Basta de "jeitinho" brasileiro



Comigo não, isso jamais acontecerá. Deixar para a última hora e o tradicional jeitinho fazem parte do dia-a-dia da maioria dos brasileiros e estão por trás de trágicos acidentes como o do vôo 3054 da TAM, que resultou na morte de quase 200 pessoas, semanas atrás em São Paulo. O caos aéreo e também no trânsito das grandes cidades estão aí como evidências da falta de planejamento por parte das autoridades. Mas o que isso teria a ver com os problemas que enfrentamos com o nosso mundo de TI? É simples, basta fazer uma análise histórica para rapidamente chegar à conclusão de que grande parte deles tem relação direta com a energia elétrica, e que poucas soluções têm sido propostas.

De um lado, o país infelizmente reúne as condições necessárias para a ocorrência de anomalias, o que não faltam por aqui são raios, por exemplo. Os profissionais de TI, propriamente dito, via de regra possuem um conhecimento muito básico de eletro-eletrônica, muitas vezes faltam-lhes inclusive o mínimo para saber se um prestador de serviço - aquele eletricista de plantão - é um picareta ou não. Eletricidade estática e aterramento elétrico? Que nada, esses conceitos ainda soam como ficção, e com raras exceções vemos cursos superiores de computação tratando disso como se deveria. A reputação da maioria dos cursos de engenharia elétrica também já não é das melhores.

Por último, se traçarmos um paralelo com os países de primeiro mundo, vemos que o Brasil está muito atrás com suas normas técnicas e práticas de certificação e fiscalização do setor. E o que está se fazendo para melhorar este cenário que inevitavelmente nos conduz a prejuízos como o de queima de placas-mãe, analisado na matéria da página 38?

Desde 1988, tramita na ABNT um projeto de uma norma para criar um novo padrão de plugues e tomadas. Deste trabalho resultou a NBR 14136 e uma portaria com força de lei que, dentre outros aspectos, estabeleceu um cronograma com vários prazos limites para a comercialização dos "antigos"plugues e tomadas por parte de fabricantes locais e importadores (plugues de 2 pinos desmontáveis até 01 de agosto de 2007, por exemplo). De liquidificadores a furadeiras, passando por bens de informática, vários aparelhos de uso doméstico estão contemplados. Segundo dados publicados por entidades do setor, menos de 20% dos aparelhos atualmente comercializados não estão com a configuração do novo plugue padrão e demandarão o uso de adaptadores, ou a troca da tomada. Dentro deste porcentual estão, por exemplo, todos os 10 milhões de computadores que devem ser comercializados no Brasil em 2007, além de periféricos como os monitores, cujos plugues são incompatíveis.

Uma vez que esta ação visa oficialmente à segurança das pessoas e das instalações, imediatamente somos levados a pensar que os padrões existentes oferecem riscos e que não haveria opções para adequá-los ao mesmo nível de segurança proposto. Todavia, quem é desta área sabe que isso não procede. Portanto, além de já irmos nos preparando para arcar com mais um aumento do "custo Brasil", somos desafiados a deixar o jeitinho de lado e buscar uma mobilização que seja capaz de provocar as ações realmente amplas e devidas para lidar com esse problema estrutural. Ou continuaremos sendo o país do jeitinho e das operações tapa-buraco?

Fernando Ramos da Silva

Atendimento ao leitor: a.leitor.pcecia@editorasaber.com.br

TESTES

PC básico e poderoso



10



Memórias de alta performance



15

Suítes para proteção máxima na internet

24

HARDWARE

Segurança em ambiente de servidores 33

Queima de placas-mãe 38

Diagnóstico de HDs 50

52 Desenvolvendo Soluções Integradas Parte 1

SISTEMAS OPERACIONAIS

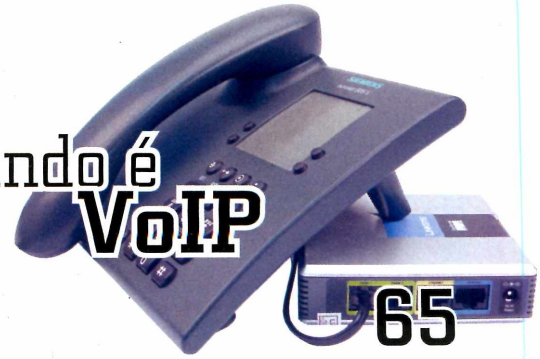
Ambiente seguro com maior facilidade 47

Certificação Microsoft MCST 56

REDES

60 Virtualização de Hardware

O Mundo é VoIP



65

5 Segurança High-Tech: Contando "causos" e melhorando a segurança do seu ambiente

6 A vez do leitor

8 Notícias

Contando "causos" e melhorando a segurança do seu ambiente



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.

Embora a atenção e os investimentos dedicados à área de segurança venham crescendo na medida em que muitas empresas despertam para a importância de proteger suas informações armazenadas em ambientes computacionais, a realidade encontra-se ainda muito aquém do ideal. Muitos ambientes de rede corporativos estão à mercê de ataques cujo sucesso não depende de conhecimentos técnicos tão aprofundados por parte dos atacantes. Tais empresas são vítimas fáceis até mesmo para os atacantes menos experientes, como os *script kiddies*.

O fato é que grande parte dos problemas de segurança poderiam ser facilmente evitados por uma equipe técnica. Entretanto, ter um time de segurança eficiente e preparado para proteger o ambiente computacional de uma corporação é proporcional à quantidade de investimento que se está disposto a fazer na contratação de profissionais bem capacitados, compra de equipamentos adequados, utilização de ferramentas apropriadas, implantação de práticas comuns, aquisição de treinamentos técnicos, dentre outros fatores. O problema para "tirar do papel" a implantação dessas medidas inicia-se quando se tem noção de que é preciso cumprir uma grande e talvez a mais importante etapa desse processo: convencer os gerentes e diretores de que se precisa, de fato, investir recursos para por em prática tais medidas.

O primeiro passo para envolver os responsáveis em tomar a decisão de investir em uma estrutura de segurança adequada à realidade da empresa deve ser, provavelmente, explicar a eles o que pode acontecer. Suponha então que uma argumentação desse tipo seja apresentada: "Na última análise feita nos logs dos firewalls, detectamos que muitas mensagens TCP com a flag SYN estão atravessando nossa rede e alcançando os servidores da DMZ em portas que não executam serviços públicos. Na verdade, como só temos HTTP, DNS e SMTP sendo oferecidos, mas existiam outras portas no estado de *listen*, isso pode representar um risco sério à segurança de nossos servidores. Diante disso, precisamos investir em um software de filtragem mais adequado, que nos permita obter maiores detalhes de logs e recursos para controle dos pacotes IP que trafegam no nosso perímetro de rede, e compor essa solução com um IDS/NIDS capaz de nos auxiliar na detecção de *port scans* ou outros ataques." Essa sopa de letrinhas, recheada com algum jargão técnico, faria seu gerente sentir vontade de dormir e, provavelmente, não teria condições de entender a importância de dedicar mais atenção e recursos ao problema que está sendo relatado.

A falta de uma profunda capacitação técnica na área de segurança, por parte dos administradores de empresas, não é nenhum tipo de demérito a esses profissionais, uma vez que esse conhecimento é bem específico de outro segmento profissional. Mas a dificuldade em repassar de maneira inteligível a necessidade de ter preparo profissional para a segurança da informação agrava-se ainda mais considerando o fato de que profissionais de computação costumam ter dificuldades para explicar assuntos técnicos para pessoas não-técnicas. É comum incorporar em suas explanações uma enxurrada de termos técnicos que não fazem sentido algum para profissionais de outras áreas.

Diante disso, tornar as coisas mais fáceis de explicar numa área que costuma ter um conjunto de termos muito particular, requer criatividade. Criado recentemente por Scott Granneman, professor da Universidade de Washington e autor de diversos artigos de segurança da informação, o site **www.securityanalogies.com** lista termos comuns da área de segurança e para cada um deles existe um conjunto de analogias interessantes para auxiliar na explicação do conceito relacionado. Por exemplo, para explicar o conceito de DoS (Negação de Serviço), uma das analogias descreve uma situação onde mil pessoas combinam de ficar ligando ao mesmo tempo para o telefone de uma recepcionista. O telefone não pode ser desligado por representar um meio de contato importante do seu trabalho e, portanto, durante o período em que essas pessoas estiverem ligando ao mesmo tempo, a recepcionista ficará tão atarefada atendendo às ligações inúteis, que provavelmente não conseguirá fazer mais nada. Como, por exemplo, dar atenção aos clientes que estejam pedindo por informações no balcão. Ficou mais simples?

> **"Essa sopa de letrinhas, recheada com algum jargão técnico, faria seu gerente sentir vontade de dormir e, provavelmente, não teria condições de entender a importância de dedicar mais atenção e recursos ao problema que está sendo relatado."**

O mais interessante é que a solução é feita no melhor estilo de composição colaborativa de conhecimento, uma vez que todo o conteúdo está publicado sobre tecnologia Wiki, de forma que qualquer colaborador criativo pode melhorar uma das estórias ou ainda publicar a sua de maneira a colocar várias analogias para um mesmo conceito. De fato, essa alternativa pode representar uma solução interessante para despertar em pessoas de outras áreas a importância de entender alguns conceitos de segurança da informação e do quão paralelo é o mundo da segurança da informação em ambientes reais e virtuais.

Que tal começar a traduzir suas explicações para o seu coordenador usando de algumas analogias para tentar trazê-lo para o seu lado, ao invés de deixá-lo tonto com tantos termos e siglas técnicas? O primeiro passo é tentar exercitar sua criatividade. Mãos à obra! **PC**

MediaPC

"Como faço para incluir fotos de um DVD/CD no MediaPC, a fim de poder gravá-las no HD e visualizá-las no monitor/TV? Quando acesso a opção ver fotos, o menu mostrado não fica disponível para alterações em suas opções. Gostaria de saber também se está havendo continuidade neste projeto."

Euclides Machado
Brasília - DF

É possível incluir as fotos, mas até o momento o script de importação automática não está funcionando. Por ora, a solução é usar outra máquina para colocar as imagens no diretório de fotos do MediaPC, que está disponível através de um compartilhamento na rede SMB. Ao fazer isso, a interface gráfica do MediaPC passará a exibir as fotos e também oferecerá a possibilidade de fazer Slide Show com vários recursos interessantes, tais como fade e zoom acelerados por OpenGL, ou seja, com processamento no processador gráfico da placa de vídeo. No mais, estamos acertando alguns detalhes para muito em breve apresentar a nova versão com algumas funcionalidades novas. Se precisar de mais algum apoio, fique à vontade para entrar em contato.

PC & CIA #72

Servidor de máquinas virtuais

"Fiz a instalação de um servidor com o Ubuntu e instalei o VMware Server. O que eu realmente preciso agora de início é de somente um servidor que compartilhe arquivos e impressoras numa rede de oito máquinas com Windows XP. Gostaria de saber se devo instalar através do VMware uma máquina virtual com o Linux novamente para executar o Samba, ou instalá-lo na própria instalação que já tenho do Ubuntu."

Wagner Santos Pereira
Administrador de redes - CIATEC
Contagem - MG

Pelo ponto de vista da urgência, certamente é mais viável instalar o Samba e o Cups como servidor de impressão sobre o Ubuntu mesmo. Mas como solução definitiva, dentro do conceito da virtualização e das muitas facilidades oferecidas para a manutenção e gerenciamento de máquinas no dia-a-dia, a opção mais recomendada é instalá-lo em outro sistema que rode em uma máquina virtual e servi-la aos usuários da rede através de sessões remotas. Essas podem ser abertas a partir de terminais leves (os chamados Thin Clients) ou mesmo a partir de PCs "antigos", que poderiam facilmente ser aproveitados. Se você não tiver lido a PC&CIA 71, recomendamos a leitura da matéria "Computação Leve" disponível em nosso site. Ela apresenta os detalhes de como organizamos a infra-estrutura da Editora Saber utilizando os conceitos citados aqui.

VMware Server não instala

"Não estou conseguindo terminar a instalação do VMware Server. Na hora de colocar o número de série, o programa não aceita e retorna algumas mensagens, a exemplo de: "/usr/lib/vmware/bin/vmware-vmx: error while loading shared libraries : libXtst.so.6 : cannot open shared object file : No such file or directory" . Também não consigo instalar o VMware Management. O que devo fazer?"

Sergio Burle Marx Smith
Rio de Janeiro - RJ

O VMware Management depende da instalação do Server. Quanto a este, parece-nos que alguma dependência relacionada à biblioteca em questão não foi resolvida, ou então o diretório em questão de fato não existe. Procure checar todos os passos descritos na matéria e também, como forma de tomar experiência com o processo, realizar a instalação no Ubuntu. Como você não menciona em qual distribuição está fazendo os testes, pode ser que esteja tentando aproveitar a base de uma distro já em uso e, nesse caso, ela pode requerer passos diferentes dos descritos na matéria.

Compatibilidade no socket LGA775

"Li na edição nº 62 que os processadores Intel Core 2 Duo só funcionam em placas-mãe compatíveis com o padrão VRD11.0 por causa da tensão de alimentação. Como verifico se a placa é compatível? Tenho pesquisado várias placas, tanto na Internet quanto em lojas, e não obtive informações sobre esta especificação. As placas Asus P5VD2-X e Asus P5VD2-MX, por exemplo, têm o padrão VRD11.0?"

Luís Carlos Godoy
Sorocaba – SP

Você pode verificar através do datasheet do chip controlador do circuito regulador de tensão utilizado pelo fabricante da placa-mãe. Infelizmente não é fácil obter essa informação na Internet, muitas vezes a confirmação só pode ser feita depois de anotar o código do chip e aí sim poder acessar a informação no site do fabricante do chip. Por outro lado, sob o ponto de vista prático, podemos confirmar o suporte ao processador através do site dos fabricantes de placa, os quais normalmente disponibilizam uma lista de compatibilidade. No caso da Asus, o link direto é o ***http://support.asus.com/cpusupport/cpusupport.aspx?SLanguage=en-us****. Veja que ambas usam um circuito VRD11.0 porque suportam os Core 2 Duo.*

Overclock no Opteron

"Pretendo fazer overclock em uma máquina dual-socket com dois processadores Opteron 265 rodando em uma placa MSI K8N Master2-FAR (chipset nForce Pro 2200), com 3 GB de RAM (PC3200 Registered DDR SDRAM), fonte Corsair CMPSU 620-HX, placa de vídeo GeForce 6800 PCI-E destravada para Quadro FX 4000 pelo Rivatuner e 2 HDs Western Digital, sendo um Raptor WD740GD para sistema e um Caviar RE 250 GB para dados. Existe alguma diferença em relação ao procedimento descrito na matéria "Overclock nos processadores Opteron", publicada na edição nº 56?"

Luiz Paulo Castillus

Servidor de terminais

"Pretendemos instalar um servidor com o Windows Server 2003 e ter 32 estações de trabalho com Thin Clients acessando a Internet, compartilhando arquivos na rede e também rodando um programa gerencial feito em Fox Pro. Qual seria uma configuração ideal para não sofrer com lentidão? Poderia ser, por exemplo, um processador Dual-Core de 3 GHz com 2 GB de RAM, HD de 80 GB e placa-mãe Intel com chipset 945G?"

Paulo Teixeira
Analista de Suporte - Terabyte Informática
Porto Alegre - RS

A princípio esta máquina pode dar conta do tipo de aplicação que você mencionou, no entanto ela deveria receber uma matriz RAID para oferecer tempos de resposta melhores. Outra boa prática é colocar mais uma ou duas placas de rede, e considerar seriamente o

Que ótimo sistema você tem! Se a versão de BIOS instalada suportar ajustes de freqüência e tensão para cada CPU, será exatamente o mesmo procedimento, só tomando o cuidado para elevar as freqüências do processador simultaneamente e para os mesmos valores. Paralelamente, convém ajustar o divisor no barramento de memória para que sua freqüência não ultrapasse 400 MHz.

Diagnóstico de HDs

"No artigo HD Workbench da edição nº 71, o autor menciona que testes de benchmark podem ser feitos pelo HD Tach com resultados bastante confiáveis. Ocorre que usei a versão 3.0.1.0 após a montagem de um novo PC, e neste os resultados destoaram significativamente da realidade e dos apontados pelo Everest. Recentemente usei a versão 3.0.4.0, mas o resultado permaneceu praticamente inalterado. Ao fazer algumas pesquisas, achei a informação de que o Everest seria mais confiável, pois a dupla CPU dual-core + RAID 0 faria com que o HD Tach apresentasse resultados errôneos. É problema de versão do programa?"

Morien H. Bendinelli
Taboão da Serra - SP

*No fórum do HD Tach (**www.simplisoftware.com/Forums/viewtopic.php?t=450**) descobrimos um sistema Core 2 Duo com matriz RAID 0, no qual o programa se comportou bem melhor do que em seu sistema. Nesta outra página **www.simplisoftware.com/Forums/viewtopic.php?t=433** há um caso bastante similar ao seu, e nesta **www.simplisoftware.com/Forums/viewtopic.php?t=392&start=0&postdays=0&postorder=asc** o que pode ser considerado a solução. Procure realizar um teste completo de consistência de disco com a matriz RAID 0 e depois com os discos rígidos individualmente instalados em um outro computador. Deve-se fazer o diagnóstico, mas não o reparo, pois pode haver problemas com o RAID 0 montado.*

Instalação automatizada do Windows Vista

"As soluções implementadas com o kit WAIK, demonstradas na edição nº71, não funcionam com o Windows XP?

Renato Macedo
Consultor - RNM Serviços Ltda
Niterói - RJ

De fato o WAIK não pode ser usado para automatizar uma instalação do Windows XP, pois o funcionamento do processo de automatização adotado pelo Windows XP é diferente do usado no Vista. Não adiantaria sequer tentar renomear o arquivo. Existem determinadas opções de instalação que o Vista usa que não funcionariam no XP, porque o programa de instalação não "imagina" que seria possível configurar tais opções através de um arquivo de respostas. Por exemplo, não teria como determinar quais componentes do Windows seriam instalados. Sendo assim, se uma adaptação fosse possível, o arquivo de respostas ficaria do mesmo jeito que o "velho" Gerenciador de instalação do Windows faz.

No caso do XP, portanto, se o usuário finalizar o processo e lembrar-se de que não realizou uma atualização importante no sistema, terá de repetir todo o processo com o Sysprep e criação da imagem ISO.

Inventário de hardware

"Depois de ler o artigo "De olho no Inventário", da edição nº71, instalei o servidor em uma máquina denominada "Reserva", de IP 192.168.0.10, baseada em um Pentium 4 com 512 MB de RAM e rodando o Windows XP SP2. A instalação do agente AgentSetup.exe, que cria o serviço no sistema, foi realizada em outra máquina com Windows XP SP2 e hardware também baseado em Pentium 4, mas com 1 GB de RAM. O problema é que o agente não está enviando dados para o servidor. O que devo fazer?

Marcelo Ferreira
Certo Atacadista Ltda
Teófilo Otoni - MG

Procure conferir as informações passadas durante a instalação do agente. No campo "Server Name" devemos informar o nome ou IP da máquina onde o OCS Inventory está instalado. No seu caso, portanto, pode ser "Reserva" ou 192.168.0.10. O número da porta deverá ser a 80 (caso não tenha modificado). Tal como mostrado na figura 7 da matéria, insira no campo "Miscellaneous" o parâmetro "/debug". Assim, toda vez que o agente realizar o envio do inventário, um arquivo de log será gerado na máquina cliente. Este log é criado dentro do diretório onde o agente foi instalado, e seu nome será: [nomedamaquinacliente.log]. Ao abrirmos este log teremos registrado todos os passos e resultados obtidos na comunicação entre o servidor e agente. Ali encontraremos os motivos pelos quais o agente não está realizando o envio do inventário.

uso de interfaces e switches gigabit. Lembre-se de que além de usar a rede para alimentar 32 terminais, o computador ainda precisará realizar os acessos a arquivos da rede para satisfazer a essas 32 pessoas, e se só houver uma interface de rede as coisas certamente não vão dar certo.



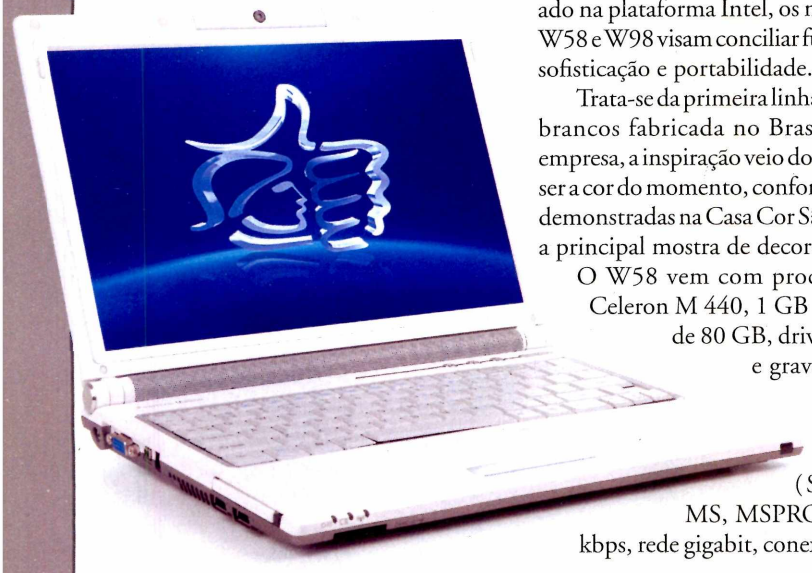
Colaboraram

- WAZ Hardware Store (www.waz.com.br)
Placa-mãe Gigabyte P35-DQ6
- Gênio Informática (www.genioinformatica.com.br)
Phone Adapter Linksys VoIP 2102, módulos de memória Patriot e processador Core 2 Quad Q6600
- T&C (www.telecommunications.com.br)
Placa-mãe Asus M2A-VM

Erramos

Edição 72 - Artigo "1 PC resolve tudo"
-Página 18, durante instalação da interface do VMware Management, códigos devem ser:
sudo rm /bin/sh
sudo ln -s /bin/bash /bin/sh

Novos notebooks da Positivo Informática



Design branco para os novos notebooks W58 e W98 da Positivo.

Com tela 12,1 polegadas widescreen, duas baterias de 4 células, webcam integrada e rotativa de 1,3 megapixel, e hardware baseado na plataforma Intel, os novos portáteis W58 e W98 visam conciliar funcionalidade, sofisticação e portabilidade.

Trata-se da primeira linha de notebooks brancos fabricada no Brasil. Segundo a empresa, a inspiração veio do fato do branco ser a cor do momento, conforme tendências demonstradas na Casa Cor São Paulo 2007, a principal mostra de decoração do país.

O W58 vem com processador Intel Celeron M 440, 1 GB de RAM, HD de 80 GB, drive óptico leitor e gravador de CD e DVD, leitor de cartões 4 em 1 (SD, MMC, MS, MSPRO), modem 56 kbps, rede gigabit, conexão PCMCIA, saída S-Video, 3 entradas USB e 1 Firewire 1394a, além de interface wireless compatível com os padrões 802.11 a/b/g. Com sistema operacional Windows Vista Home Premium e peso de 1,9kg (com bateria), este modelo está cotado a R$ 2999,00.

Já o W98 é o modelo topo de linha. O equipamento utiliza o mesmo hardware base e design, o que muda é o poder computacional. São 2 GB de RAM e, ao invés do Celeron M 440, é entregue um Core 2 Duo T5300 com dois núcleos de processamento operando a 1,73 GHz e contando com 2 MB de cache L2, além de vários recursos extra, a exemplo do suporte às instruções para virtualização do hardware, aos softwares de 64 bits e a um gerenciamento térmico muito mais aprimorado, com reflexos direto na temperatura e no ruído gerado pela ventoinha. O preço sugerido é de R$ 3499. Para maiores informações, acesse **www.positivoinformatica.com.br.**

Novos Pendrives Kingston

A Kingston ampliou a sua linha de Pendrives DataTraveler com dois novos modelos: o DataTraveler II Migo e o DataTraveler 100. O primeiro vem acompanhado do premiado software Migo, que permite o transporte de dados e aplicativos, oferecendo ao usuário a sensação de estar trabalhando no seu próprio computador.

O segundo é um modelo mais simples, sem software adicional. O mais chamativo é o seu design sem tampa. Ele dispõe de um cursor deslizante na lateral que permite a abertura e o fechamento do conector USB usando apenas o polegar. Está disponível em versões de 1, 2, 4 e 8 GB pelos respectivos preços sugeridos de R$ 80, R$ 138, R$ 260 e R$ 490.



Novo Kingston DT 100.

Preço do LCD deverá subir

Hoje em dia existem muitas pessoas que, de alguma forma, desejam ter acesso a conteúdos de alta definição (HD), seja ela pela transmissão do formato HD, com a venda de reprodutores de discos HD Blu-Ray ou HD-DVD, com a reprodução de arquivos de vídeo HD e inclusive com os consoles de última geração: o XBox 360 com o seu leitor externo HD-DVD, ou o PS3 com o seu leitor Blu-Ray integrado.

Como conseqüência, está sendo registrado um aumento considerável na demanda por telas LCD e as estimativas apontam que durante o terceiro trimestre de 2007 recordes de venda serão batidos. E por estar aumentando a procura por telas LCD, os fabricantes estão considerando a possibilidade de aumentar os seus preços. No entanto, os preços destas telas já subiram algo em torno de 15 a 25% desde o mês de abril, e segundo alguns analistas poderão subir ainda mais. O tipo de tela que deverá ter um aumento mais notável durante este trimestre é o de 19 polegadas no formato 16:9, que é o mais procurado.

O Windows Server 2008 chegará em... 2008

Enquanto algumas pessoas o esperavam para o final deste ano, o Windows Server 2008 na verdade deverá ser disponibilizado pela Microsoft apenas em fevereiro de 2008. O código deverá ser finalizado ainda em 2007. A Microsoft deverá anunciar o seu Longhorn Server numa conferência em Los Angeles no próximo dia 27 de fevereiro, assim como o Microsoft SQL Server 2008 e o Visual Studio 2008 (codinome Orcas).

Uma versão beta já se encontra disponível para download gratuito. Através dela é possível ter uma idéia sobre como será o próximo sistema operacional para servidores da editora, o sucessor do atual Windows Server 2003.

AMD e seu CrossFire com quatro GPUs

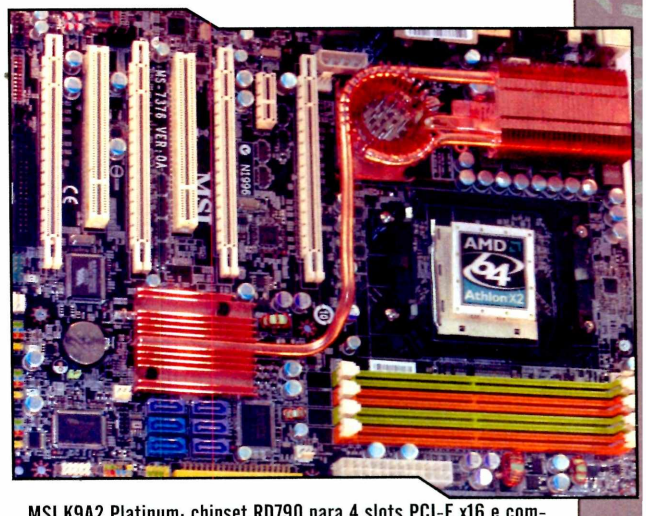
As soluções multi-GPU para entusiastas fazem parte de um pequeno mercado, principalmente porque o número de títulos que realmente são capazes de tirar vantagem deste poder dificilmente compensa pelos altos custos envolvidos.

As configurações Crossfire da AMD são uma parcela ainda menor do mercado, já que a NVIDIA domina nestes sistemas. No entanto, isto não impediu a AMD de continuar a toda velocidade com o seu Crossfire, desenvolvendo a funcionalidade Crossfire de três ou quatro placas para o chipset RD790.

Esta é uma versão totalmente atualizada do chipset 580X, que traz uma ampla variedade de mudanças. Dentre elas, se destacam 41 linhas PCIe 2.0, com suporte a até 4 slots PCI-E x16. Estes slots x16 podem ser usados para conectar 1, 2, 3 ou inclusive quatro placas de vídeo, dando à AMD uma ligeira vantagem sobre a oferta NVIDIA.

A diferença em relação ao SLI da NVIDIA, que tem suporte para duas ou quatro placas em SLI, é que a solução Crossfire melhorada pode ter três placas para incrementar a performance. Aliás, um sistema com três placas Radeon HD 2900XT e um futuro Phenom operando a 3 GHz foi demonstrado durante o último Analyst Day promovido pela AMD no mês passado.

A empresa disse que a escalabilidade Crossfire de três placas oferece um incremento de 2.6 vezes na performance. Duas placas oferecem uma performance 80% superior e, por último, nada foi divulgado sobre o ganho de performance estimado para a configuração Crossfire com quatro GPUs.



MSI K9A2 Platinum: chipset RD790 para 4 slots PCI-E x16 e compatibilidade com futuros processadores Phenom para o socket AM2/AM2+ e memórias DDR2.

O RD790 não está assim tão distante. Espera-se que ele seja lançado antes dos chips Phenom. Isto dará algum espaço para que os fabricantes de placas-mãe possam incluí-lo, mas ainda deverá passar um bom tempo até que ela se torne uma opção padrão.

Executivo da nVidia fala sobre política de preços

O vice-presidente de relações de conteúdo da nVidia, Roy Taylor, escreveu no Developer Blog da companhia um tipo de crítica à atual tendência dos fabricantes de PCs de promoverem os componentes ultra em high end e de tentarem vender PCs otimizados para DirectX 10 por US$ 3000, o que prejudicaria as vendas.

O executivo acredita que os grandes vendedores de PCs tendem a considerar o segmento dos PCs para jogadores como um negócio lucrativo, tolerante à venda de hardware por um preço muito alto. Segundo ele, na prática esta estratégia serviria mais para ganhar análises e comparativos de revistas, do que para proporcionar aos usuários finais o que eles realmente precisam para jogar os jogos modernos.

Em outra parte do texto, ele diz que isso também contribui para confundir os distribuidores de jogos, dando-lhes a falsa impressão de que os únicos equipamentos em condições de satisfazer aos jogadores são os da linha ultra high end. Segundo a análise, isto estaria muito longe da realidade, pois por US$ 1499 (no exterior) seria possível adquirir uma máquina da Gateway com uma placa 8800 GTS, sistema este que seria suficiente para um jogador desfrutar de todos os detalhes durante um ano.

Ele também acredita que uma placa gráfica mais modesta também é capaz de oferecer um padrão de conforto aceitável rodando o DX10, a exemplo de uma GeForce 8600 GT de um sistema Velocity Micro vendido por US$ 1000.



Core 2 Quad Q6600.

Intel reduz os preços

Existiam rumores apontando que isso aconteceria e finalmente, no último dia 22 de julho, a Intel resolveu reduzir seus preços para as linhas de processadores Core 2 Duo e Core 2 Quad. Isso coloca uma pressão ainda maior sobre a atual linha de processadores AMD, que foi brindada com uma redução de preços no início de julho.

A redução maior ocorreu no Core 2 Quad Q6600 (2,4 GHz com FSB de 1066 MHz e 8 MB de cache L2), que custava US$ 530 e agora tem um custo de US$ 266(para lotes de mil unidades), sendo uma boa opção para workstations e configurações de desktop poderosas. Além dele, o Core 2 Duo E4400 (2 GHz, FSB de 800 MHz e 2 MB de L2) saiu de US$ 133 para US$ 113, o mesmo valor do E4300, que até então era o Core 2 Duo de custo mais acessível. Por falar em Dual-Core, o modelo Intel mais barato hoje é o Pentium E2140, cotado a US$ 71 e com freqüência nominal de 1,6 GHz e 1 MB de cache L2.



PC básico e poderoso

Fernando Ramos Silva

Os processadores Dual-Core estão cada vez mais acessíveis por conta da guerra de preços entre AMD e Intel. As placas-mãe com vídeo integrado ainda não são o sonho de consumo de um gamer, mas estão com um poder de processamento gráfico razoável para atender às necessidades de aplicações como Google Earth e, quem diria, os desktops de sistemas operacionais modernos. Soma-se a isso uma pressão cada vez maior por menores níveis de consumo de energia e temos então um cenário complexo para apontar a melhor solução disponível hoje. Os testes a seguir se apresentam como resposta.

Os competidores

Tomando como base as necessidades de um típico desktop básico que hoje pode se dar ao luxo de ter um processador Dual-Core devido aos baixos custos, nossa bateria de testes contará com um Athlon 64 X2 BE-2350 e um Core 2 Duo E4300. Ambos podem ser encontrados no exterior por valores apenas ligeiramente superiores a US$ 100 (102 e 117, respectivamente, utilizando o site **www.newegg.com.br** como referência).

O primeiro faz parte da mais recente safra de processadores da AMD produzidos com o processo de manufatura de 65 nanômetros e que traz como principal diferencial um perfil de potência (TDP – Thermal Design Power) limitado a apenas 45 W. Contando com 1 MB de cache L2 (512 KB por núcleo), sua freqüência de operação interna oscila dinamicamente entre 1000 MHz e 2100 MHz (figura 1).

Por sua vez, o Core 2 Duo E4300 é apenas uma versão ligeiramente inferior aos modelos da série 6000. Ao invés de 4 MB, ele possui 2 MB de cache L2 compondo uma área comum de acesso pelos dois núcleos. Apesar de sua freqüência interna ser menor (oscila entre 1200 e 1800 MHz), o TDP nominal é bem superior (65 W) ao do concorrente.

Já do lado das placas-mãe, além de custo acessível, tecnicamente elas precisam ter um bom conjunto de interfaces e pelo menos satisfazer aos requerimentos para rodar a interface gráfica Aero do Windows Vista. Ou seja, possuir a certificação Vista Premium. Para isso, a compatibilidade com o Pixel Shader 2.0 é mandatória.

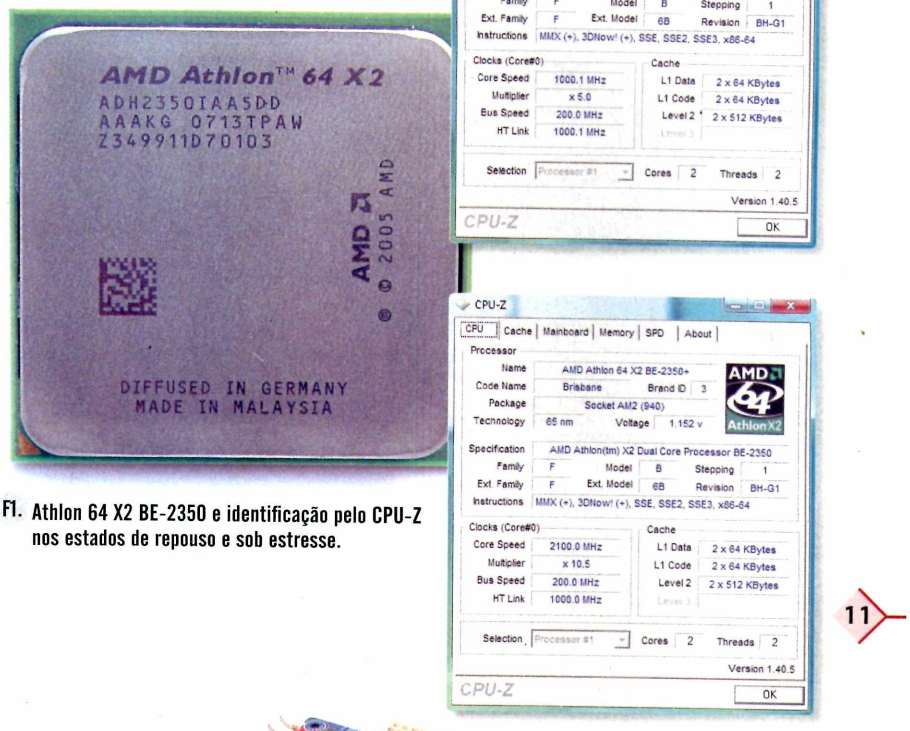
Ajudar na decodificação de conteúdos High Definition também é um "plus" desejável. Essa análise acaba nos levando aos chipsets, e nesse aspecto as opções se dividem atualmente em dois grupos: processador Intel com chipset Intel, notavelmente os da família G/Q965 e o Q963; e processador AMD com o chipset 690G da AMD ou o 7050 da nVidia.

Dentre os da Intel, o mais avançado em recursos é o G965, cujo processador gráfico (GPU) é o único compatível em hardware com o Shader Model 3.0 (nos outros dois, o suporte vai até a versão 2.0) e é capaz de manipular um maior número de etapas para a decodificação de streamings MPEG-2 e VC1 (nos outros, é feito por software), além de poder compartilhar até 384 MB da memória RAM principal do sistema (nos outros, vai até 256 MB).

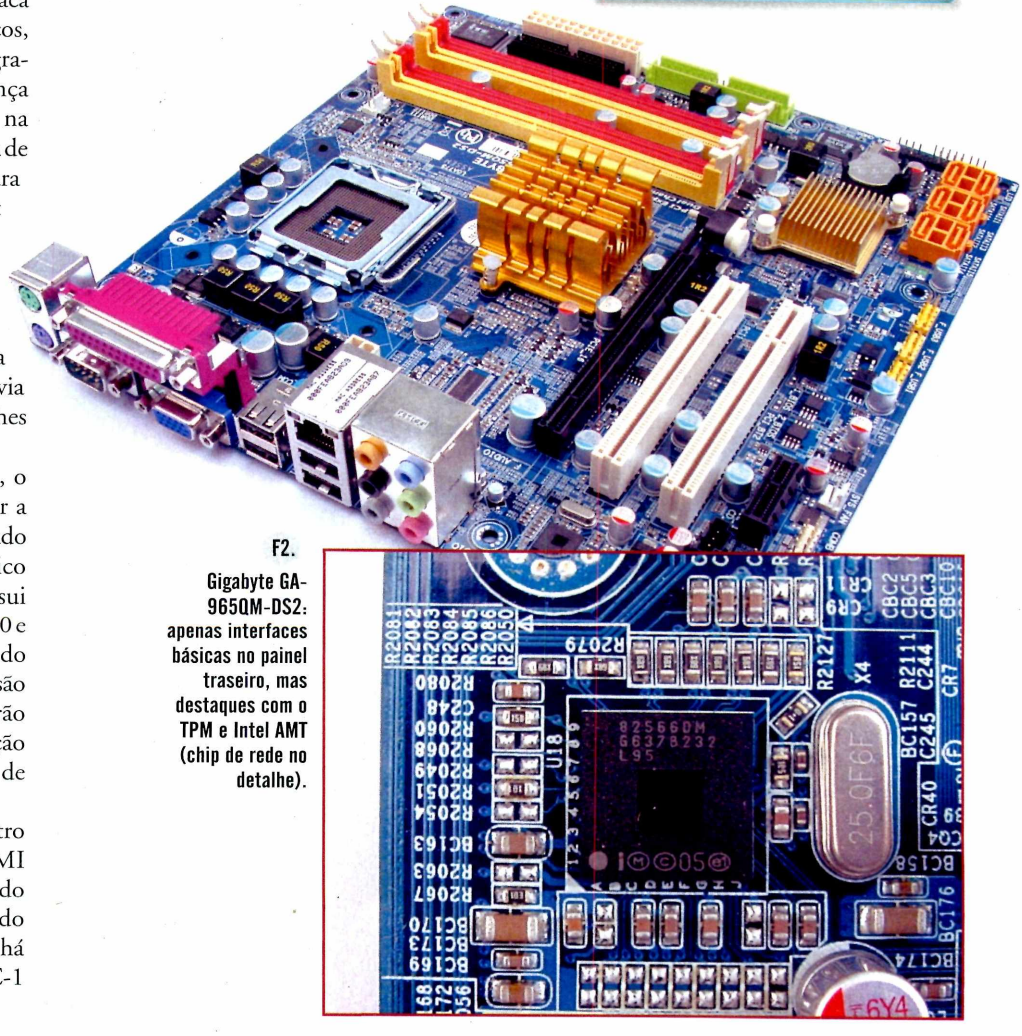
A placa-mãe utilizada foi a Gigabyte GA-965QM-DS2, um modelo baseado no chipset Q963 que tem uma clara vocação para desktop corporativo. Além da maior durabilidade esperada a partir do emprego de capacitores de núcleo sólido em toda a placa (figura 2), em substituição aos eletrolíticos, ela também vem com o chip de criptografia TPM integrado para maior segurança (detalhes da tecnologia e configuração na PC&Cia 60) e ainda oferece a tecnologia de gerenciamento ativo AMT da Intel. Para isso, utiliza o controlador de rede Gigabit 82566DM e o Southbridge ICH8DO, ambos necessários para permitir o chamado acesso out-of-band (OOB). Com o OOB, é possível acessar o BIOS da máquina remotamente e comandar sua inicialização e desligamento. E tudo isso via algum web browser. Para maiores detalhes e configuração, veja PC&CIA 69.

Além desses três chipsets da Intel, o AMD 690G também é capaz de rodar a interface Aero sem problemas. Apresentado na PC&CIA 70, seu processador gráfico Radeon X1250 (baseado no X700) possui compatibilidade com o Shader Model 2.0 e pode compartilhar até 1 GB da memória do sistema. Alguns diferenciais interessantes são a saída HDMI nativa e o suporte ao padrão HDCP 1.1, necessário para a reprodução de conteúdos de alta definição a partir de drives Blu-Ray e HD-DVD (figura 3).

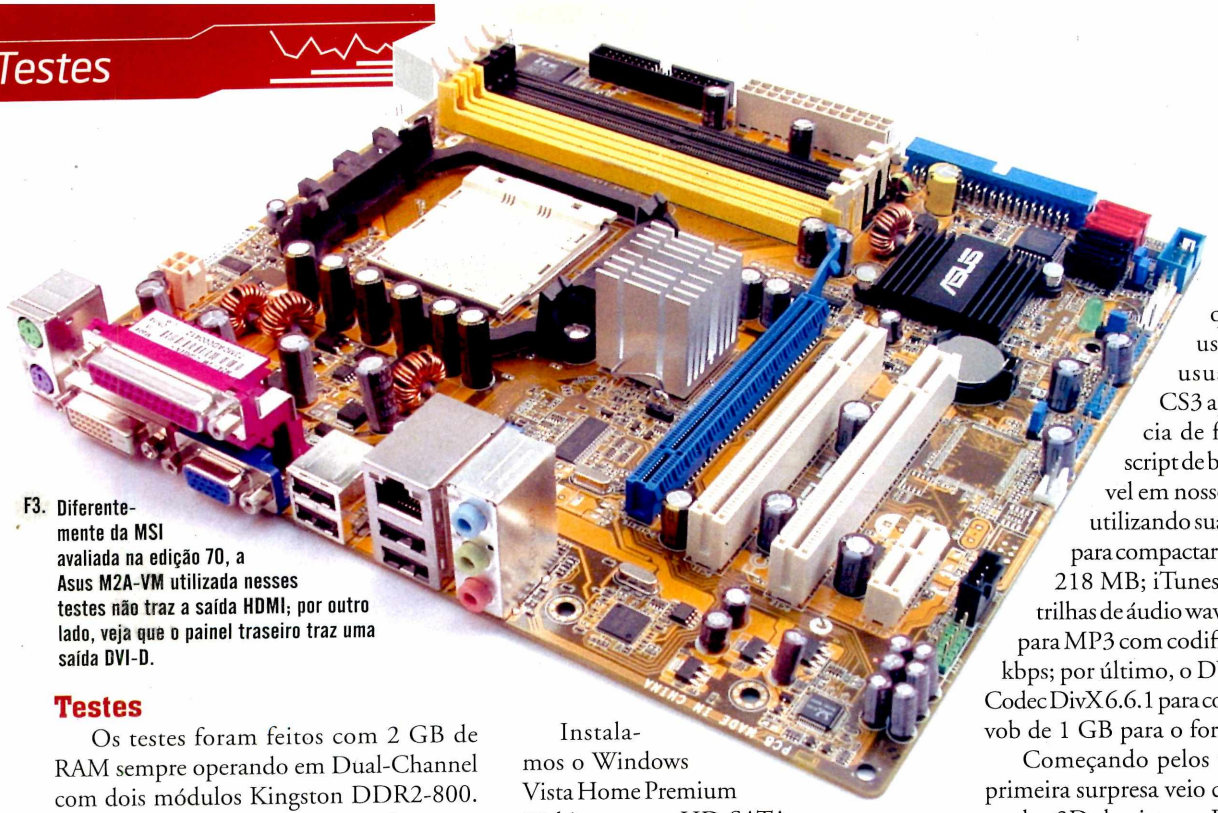
Para finalizar, o GeForce 7050 é outro chipset que já vem com a saída HDMI nativa e com suporte ao HDCP. Segundo a nVidia, o processador gráfico integrado é compatível com o Shader Model 3.0 e há aceleração para streamings MPEG-2, VC-1 e também H.264 (figura 4).



F1. Athlon 64 X2 BE-2350 e identificação pelo CPU-Z nos estados de repouso e sob estresse.



F2. Gigabyte GA-965QM-DS2: apenas interfaces básicas no painel traseiro, mas destaques com o TPM e Intel AMT (chip de rede no detalhe).



F3. Diferentemente da MSI avaliada na edição 70, a Asus M2A-VM utilizada nesses testes não traz a saída HDMI; por outro lado, veja que o painel traseiro traz uma saída DVI-D.

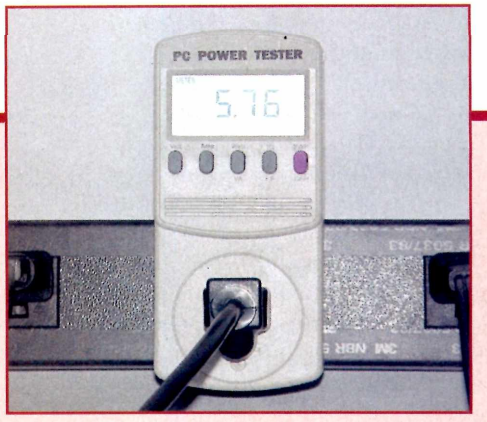
Testes

Os testes foram feitos com 2 GB de RAM sempre operando em Dual-Channel com dois módulos Kingston DDR2-800. Essa medida é importante porque força que toda a vazão de dados esteja disponível no barramento de memória, o qual de outra forma ficaria estrangulado pelos acessos constantes e concorrentes entre o processador gráfico e o restante do sistema. Outra medida tomada, desta vez para garantir igualdade de condições, foi ir até o Setup do BIOS de todas as placas e definir 128 MB como limite para memória de vídeo. Por falar em BIOS, a Biostar rodou com a versão de 31/05/07, a Asus com a revisão 0901 e a Gigabyte com a F4.

Instalamos o Windows Vista Home Premium 32 bits em um HD SATA Barracuda 7200.7 de 120 GB da Seagate e após atualizar os drivers para as últimas versões disponíveis nos sites, instalamos os seguintes programas: os benchmarks sintéticos 3DMark 2005 e PCMark 2005 para aferir o desempenho gráfico 3D e de sistema, respectivamente; os jogos X^2 – The Threat e o Unreal Tournament 2004 sempre com a resolução de 1024x768 e sem qualquer filtro de qualidade ativado (o Unreal rodou com os dois perfis apresentados pelo programa Umark, HP e HQ para maior performance e qualidade, respectivamente); e um conjunto com quatro aplicações de uso comum a todo usuário: Photoshop CS3 aplicando a seqüência de filtros definida no script de benchmark disponível em nosso site; Winrar 3.70 utilizando sua melhor qualidade para compactar um arquivo .dbx de 218 MB; iTunes 7 convertendo 20 trilhas de áudio wav (1,48 GB no total) para MP3 com codificação CBR de 320 kbps; por último, o DVD2AVI usando o Codec DivX 6.6.1 para converter um arquivo vob de 1 GB para o formato avi.

Começando pelos testes sintéticos, a primeira surpresa veio com o bom desempenho 3D do sistema Intel. Afinal, quem diria que um chipset Intel de 2006 fosse superior a um nVidia lançado em 2007? E o detalhe é que nos testes de CPU do 3DMark 2005, o sistema AMD com chipset nVidia foi ligeiramente superior. Ou seja, além de ser superior nos testes 3D, o chipset Intel o foi por uma margem considerável, conforme pode ser visto no índice geral demonstrado no gráfico da figura 5. Enquanto isso, no

PC Power Tester



Esse wattímetro é o mais recente instrumento de medição trazido ao nosso laboratório. Cotado a R$ 360 na T&C (www.telecommunications.com.br), ele é pequeno, leve e muito conveniente nos quesitos instalação e uso. Na parte traseira, estão os três pinos no padrão 2P+T para conectá-lo a uma tomada; a seguir é só conectar o cabo AC de uma fonte de alimentação, por exemplo, em seu painel frontal. A operação não depende de calibração e dispensa quaisquer cuidados com relação à seleção de uma grandeza inadequada para a medição que será realizada, tal como acontece com um multímetro comum, por exemplo. Basta apertar qualquer um dos cinco botões para ter o valor mostrado no display. Não há sequer um botão ou chave de liga/desliga, o instrumento é ligado automaticamente quando conectado ao circuito. Suas funções são:

- KWH / Hour: esse botão apresenta os valores de consumo de energia, em kilowatts.hora (HWH), e o número de horas ligado;
  Hz / PF: freqüência, em Hertz, e o fator de potência da carga alimentada. Em fontes com PFC ativo, por exemplo, é comum ver valores próximos a 1; já nas genéricas, algo em torno de 0,70;
- Watt / VA: potência ativa, em watts, e a potência aparente, em volt-ampères (VA). Vale lembrar que a potência em watts é dada pela expressão W = VA x PF;
- Amp: corrente, em ampères RMS;
- Volt: tensão, em volts RMS.

Ele é especificado para suportar correntes de até 15A e deve ser ligado apenas em tomadas de 120 VCA (potência total de 1870W). Nos testes que fizemos ficamos satisfeitos com os valores apresentados ao compará-los com os amostrados pelos instrumentos tradicionais que comumente utilizamos.

Só sentimos falta de uma função "Hold" para registrar automaticamente os valores máximos, e também de uma interface para comunicação com PC. Mas sua proposta não é substituir os tradicionais, mas sim servir de ferramenta de apoio a técnicos e integradores durante o dia-a-dia. Comportamento de um processador ou placa de vídeo em overclock, por exemplo, e o diagnóstico de uma fonte ou placa-mãe com problemas na linha de alimentação +5V Stand-by podem ser avaliados com facilidade. Além disso, ele também pode ser usado para "pegar" as fontes com baixo valor de fator de potência que podem estar contribuindo para uma sobrecarga nos circuitos de alimentação e distorção da rede elétrica.

PCMark 2005, que reproduz várias atividades do dia-a-dia, tais como edição de texto, varredura por vírus no HD e criptografia de arquivos, o primeiro lugar do sistema Intel sinaliza para uma superioridade imposta pelo processador E4300 frente ao BE-2350.

Continuando um pouco com os jogos, vale lembrar que os títulos avaliados aqui são do início da geração DirectX 9, ou seja, de alguns anos atrás. O gráfico da figura 6 mais uma vez mostra o sistema Intel dando trabalho e sendo inclusive superior ao 690G, por conta do resultado muito superior no X^2.

No entanto, vamos dar uma olhada na qualidade da imagem durante o jogo? Veja a figura 7. Acima, mostramos duas cenas do X^2 no sistema AMD com o 7050 (com o 690G foi similar), enquanto as de baixo no sistema Intel.

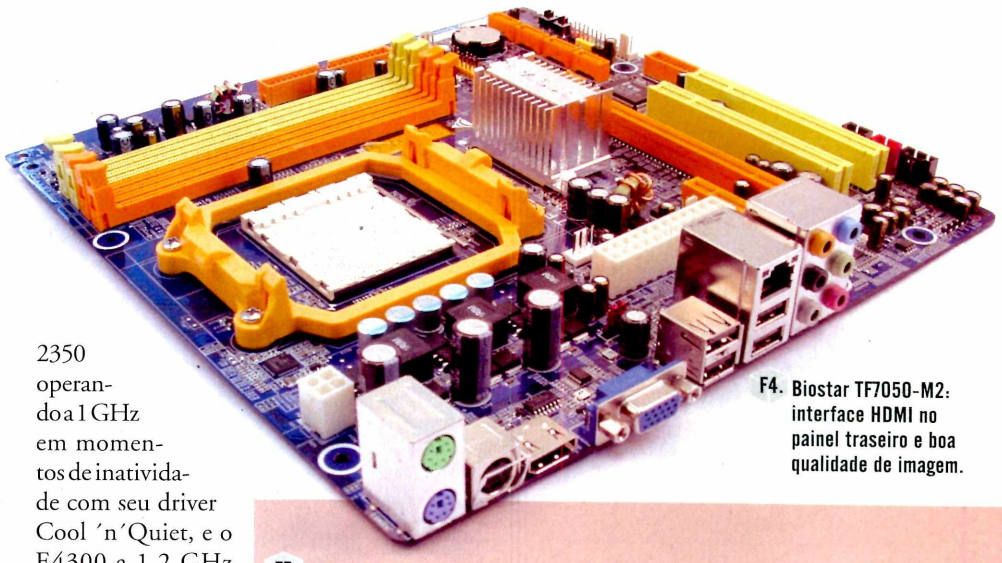
Agora está explicado o desempenho tão superior do Q963, na verdade ele simplesmente está deixando de renderizar boa parte das texturas que compõem o jogo. Seria um problema de compatibilidade com o jogo, ou então uma falta de otimização no driver utilizado pelo chipset Intel? As hipóteses são várias, mas isso reflete um comportamento indesejável que normalmente não vemos nas soluções concorrentes.

Por último, os testes de produtividade vieram para confirmar que o E4300, mesmo com 300 MHz a menos, é superior ao BE-2350 (figura 8).

Outros detalhes

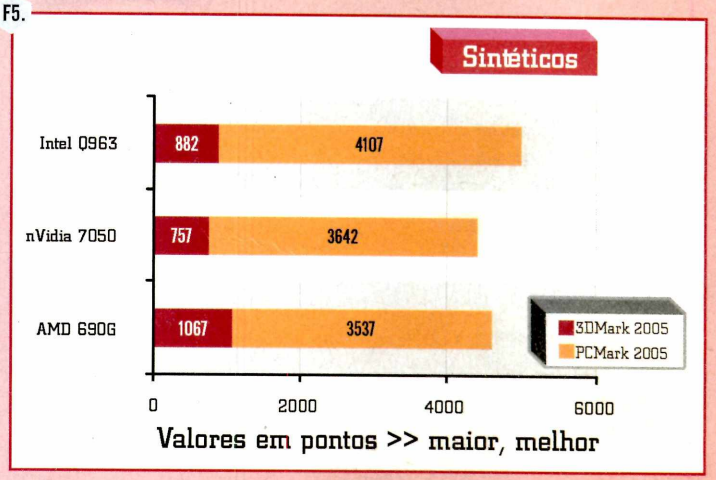
Qual seria a taxa de uso de CPU em cada sistema durante a reprodução de conteúdos High Definition? O teste foi feito com a versão 1080p do arquivo "The Living Sea", disponível para download no site **www.microsoft.com/windows/windowsmedia/musicandvideo/hdvideo/contentshowcase.aspx** com 153 MB. A reprodução foi feita com o Windows Media Player 11 e os resultados capturados a partir da medição com o Gerenciador de Tarefas do próprio Windows. O sistema mais eficiente foi o AMD com chipset 7050, que apresentou uma média de uso de CPU de apenas 32%. Enquanto isso, no Intel foi de 48% e, por último, veio o sistema 690G com 53%.

Para finalizar, vamos à medição do consumo de energia das máquinas, lembrando que todos os modos de gerenciamento térmico e de redução do consumo dos processadores foram ativados no BIOS e funcionaram normalmente em todos os sistemas. Ou seja, o BE-2350 operando a 1 GHz em momentos de inatividade com seu driver Cool 'n' Quiet, e o E4300 a 1,2 GHz com seu SpeedStep.

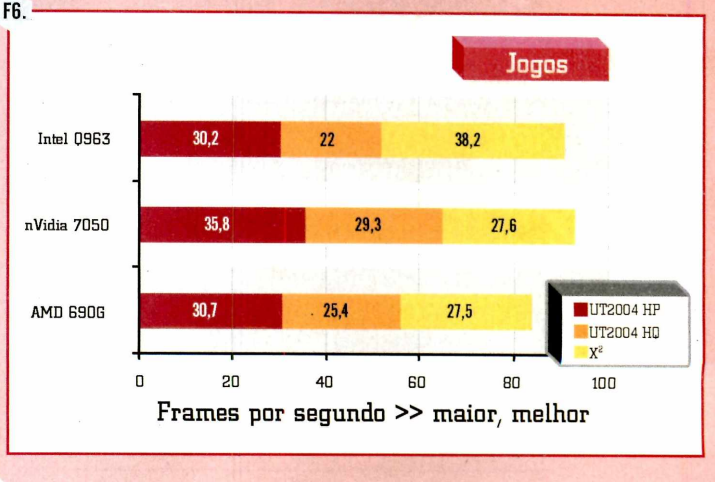


F4. Biostar TF7050-M2: interface HDMI no painel traseiro e boa qualidade de imagem.

F5.



F6.



O consumo máximo foi avaliado durante a execução do "Game 3" do 3DMark 2005, onde o nível de estresse é distribuído pelos principais componentes da máquina. A medição foi feita com um wattímetro (detalhes no box) inserido entre a entrada da fonte de alimentação (modelo Extreeam FEX-60T28 com 600W de potência) e a tomada no filtro de linha. Simultaneamente fazíamos outra medição utilizando um alicate amperímetro e um multímetro TrueRMS.

Na figura 9, vemos um nVidia 7050 muito bem posicionado e o sistema Intel consumindo aproximadamente 20% a mais no repouso e pelo menos 15% a mais em relação ao AMD menos eficiente, ou seja, no sistema com chipset 690G.

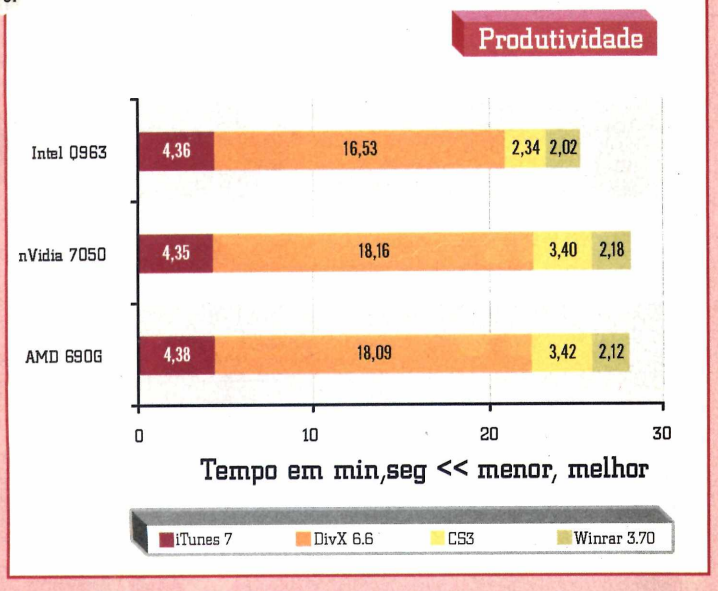
Conclusão

Desde que publicamos o último teste comparativo entre processadores, vários modelos foram lançados e sucessivas reduções nas listas de preço foram anunciadas pela AMD e Intel. Baseados nos testes de performance entre os modelos avaliados aqui, podemos dizer que o cenário permaneceu inalterado, isto é, com o Intel sendo mais caro, mas apresentando um resultado superior mesmo operando com centenas de megahertz a menos.

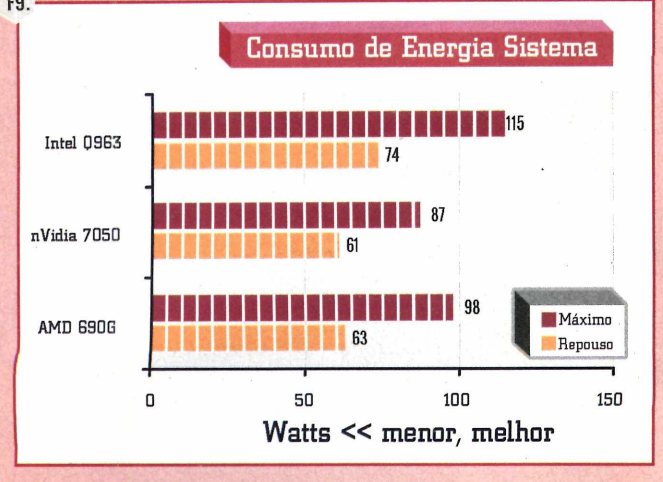


F7. Execução do X²: as duas primeiras cenas foram tiradas do sistema AMD, as demais, do Intel.

F8.



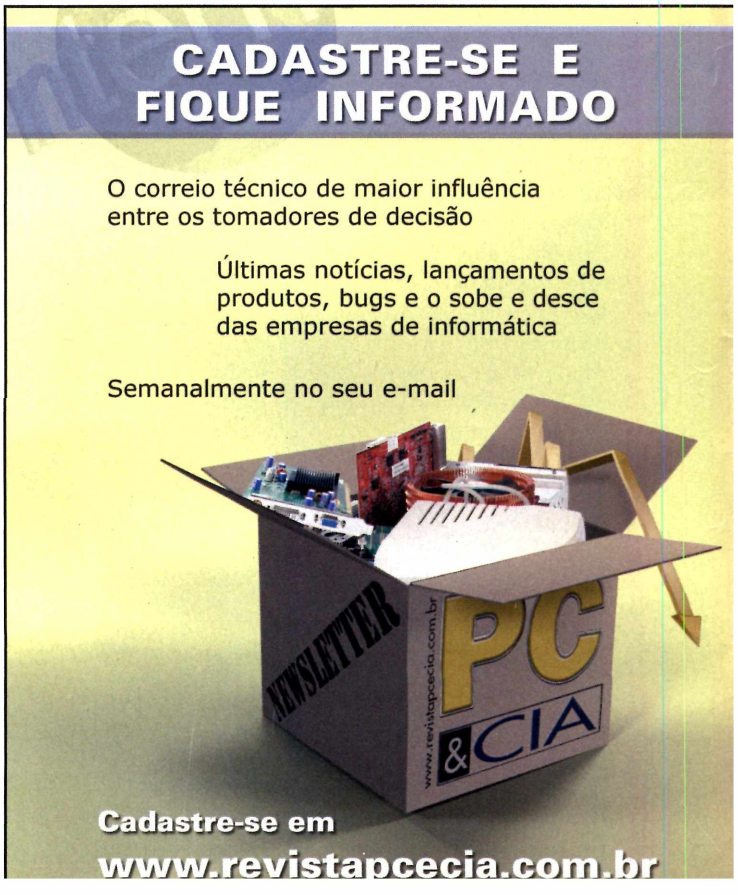
F9.



Por outro lado, os sistemas AMD são mais baratos (placas-mãe), consomem menos energia elétrica e, há de se levar em consideração que nem sempre o maior poder computacional é a variável mais relevante para o processamento de uma determinada aplicação, ou então realmente necessário no dia-a-dia. Além disso, para aplicações gráficas, por exemplo, os GPU's para AMD ainda são superiores. Aliado ao menor consumo de energia, representam a opção ideal para um MediaPC, e com ligeira vantagem para o sistema 690G.

Mas não é só. Para o posto de desktop corporativo, por exemplo, recursos como TPM e a tecnologia de gerenciamento ativo são cada vez mais demandados e, nesse sentido, praticamente ainda não se viu nada com sistemas AMD. Aliás, esse sistema Intel baseado nessa placa-mãe da Gigabyte, feita pela Digitron aqui no Brasil, abre um leque de oportunidades muito grande para integradores que pretendem oferecer soluções de maior valor agregado e a um preço competitivo ao mercado corporativo.

E como último aspecto para esta breve análise tem também a questão do Linux, segmento no qual as placas baseadas em chipsets nVidia e também da Intel continuam oferecendo uma compatibilidade muito mais abrangente que os AMD. Como vemos, portanto, ainda não existe uma solução perfeita de PC básico e poderoso que atenda a todos os casos. É tudo uma questão de avaliar bem as necessidades e, munido das variáveis apresentadas aqui, tomar a decisão mais consciente. **PC**





Memórias de alta performance

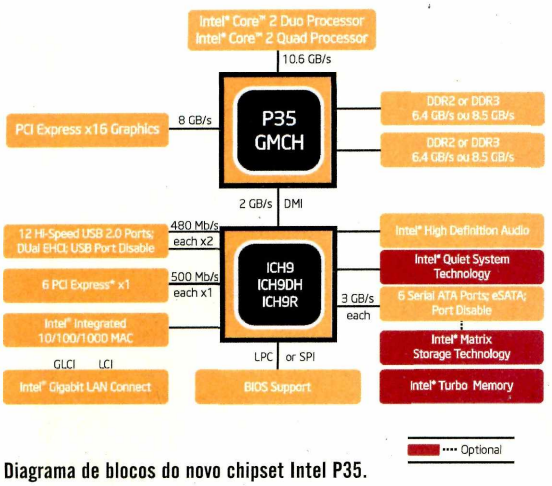
Fernando Ramos Silva

Boa apresentação, garantia vitalícia e flexibilidade para operar em altas freqüências ou baixas latências. O que não faltam são atrativos para recomendar algum dos nove kits Dual-Channel de memórias DDR2 avaliados aqui. Esta matéria lhe mostrará qual deles atende melhor às necessidades do seu sistema.

No início de junho a Intel realizou o lançamento de seus novos chipsets G33 e P35, os quais trouxeram como principais novidades a nova família de Southbridges (Ponte Sul) ICH9 e o suporte ao FSB de 1333 MHz e às memórias DDR3 no Northbridge (Ponte Norte). Eles vieram para substituir os chipsets P965 e 945G, respectivamente, e falando da controladora de memória em específico, ambas suportam a operação em Dual-Channel com dois módulos por canal (figura 1). Os módulos podem ser tanto DDR2 ou DDR3, mas jamais ambos simultaneamente, tendo cada canal com uma determinada tecnologia, por exemplo. Isso vale até mesmo para as atuais placas-mãe conhecidas como "combo", por trazerem dois soquetes para DDR2 e outros dois para DDR3. O fato é que a definição pela utilização de um ou outro tipo deve ser feita antes da inicialização da máquina e isso influencia no ajuste de temporização e na parametrização elétrica exercida sobre a controladora de memória.

O máximo de memória suportado é 8 GB. Além disso, dentre as configurações suportadas em relação à dupla FSB/RAM, o suporte oficial da Intel contempla como topo de linha o ajuste 1333/DDR3-1066. Por outro lado, o que mais nos importa aqui é saber que os módulos DDR3 ainda estão com preços muitos superiores aos DDR2 e, a despeito das maiores freqüências, as latências também estão significativamente superiores às suportadas pelas DDR2. Por sinal, somente agora, alguns meses após o lançamento dessa plataforma Intel, é que começam a surgir módulos DDR3 com latências 7-7-7-18.

Um kit desses da Super Talent, com especificação nominal de 1600 MHz, custa no exterior mais do que o dobro do módulo DDR2 mais rápido apresentado nesta matéria. E detalhe: no caso desses módulos DDR2 digamos "espe-



F1. Diagrama de blocos do novo chipset Intel P35.

ciais", é possível ter a flexibilidade de operar com latências muito baixas, a exemplo de 3-3-3-10, quando o usuário não precisar de freqüências superiores a 800 MHz.

Esse cenário é particularmente interessante para os processadores da AMD, os quais, conforme abordado em edições anteriores da revista, beneficiam-se mais de menores latências por terem a controladora de memória integrada no mesmo encapsulamento do processador. De fato, suas unidades de execução podem ter os dados à disposição rapidamente, mesmo com uma quantidade limitada de cache.

Estima-se que os preços das DDR3 só cheguem ao nível das DDR2 no final deste ano, ou mesmo no decorrer de 2008. E apesar da plataforma Intel continuar sendo a mais rápida do mercado e evidentemente atrair as atenções dos usuários de sistemas de alta performance, há de se considerar alguns aspectos que podem atrapalhar a escalada das DDR3. Um dos principais será o lançamento dos novos processadores Phenom da AMD, que acontecerá neste ínterim. Já sabemos que eles ainda virão com o suporte às DDR2 e podem ser mais rápidos que os concorrentes da Intel. Portanto, o cenário atual é muito favorável para novos investimentos em módulos DDR2.

O Sistema

Seguindo a linha de raciocínio exposta anteriormente, optamos por um hardware base da Intel e utilizamos uma das melhores placas-mãe LGA775 do mercado, a Gigabyte P35-DQ6 (revisão de BIOS F4), que já traz integrado o chipset P35 e em uma implementação suportando apenas módulos DDR2.

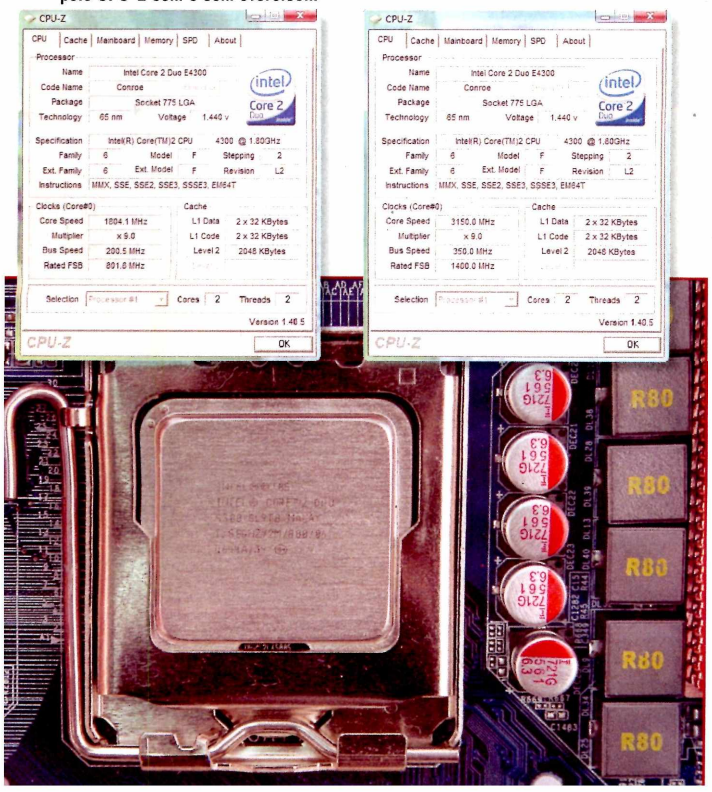
O processador merece alguns comentários à parte. Primeiro, é preciso considerar que, em se tratando dos modelos da família Core da Intel, eles possuem uma grande quantidade de cache L2 e vários circuitos dedicados e algoritmos especializados em trazer os dados da RAM antes que o fluxo de execução do programa necessite. Aqui, vale praticamente tudo para minimizar as latências inerentes de um típico acesso à RAM, via chipset. O que fazer então para evitar que um ótimo – e também caríssimo (em relação aos genéricos, é claro) – módulo de memória tenha seu potencial ofuscado?

Sabendo do bom potencial para overclock desses processadores, a resposta veio com o E4300. Trata-se do Core 2 Duo mais acessível do mercado hoje, estando cotado a pouco mais de US$ 100 no exterior (figura 2). Tecnicamente, ele é inferior no FSB limitado a 800 MHz oficialmente (nos da família E6000, é de 1066 MHz) e no cache L2 de 2 MB (4 MB nos E6000). A lógica, portanto, é economizar o máximo que puder no processador e investir num bom sistema base formado pela placa-mãe e kit de memórias.

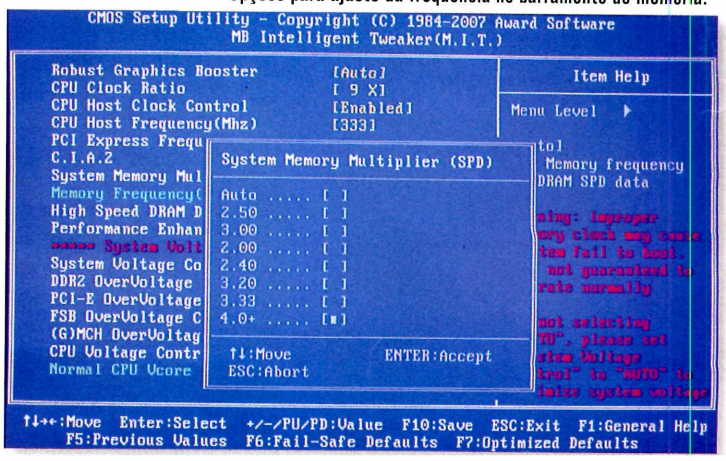
Por falar na placa, ela se comportou muito bem durante o overclock com este E4300. A estabilidade total foi obtida com a freqüência base de 350 MHz no FSB. Esse valor permitiu a execução de todos os testes descritos a seguir e mais uma rotina de estresse com o CPU Stability Test rodando em seu modo de "warming" por 30 minutos. Lembrando que, por se tratar de um barramento QDR (Quad Data Rate) capaz de realizar quatro transferências de dados por ciclo de clock, a taxa efetiva é de 1400 MHz. Para isso, foi necessário elevar a tensão do processador para 1,475V e em 0,3V as tensões do Northbridge (parâmetro denominado "MCH OverVoltage Control no BIOS da Gigabyte) e das vias de alimentação elétrica do barramento FSB (parâmetro "FSB OverVoltage Control"). O resultado foi que internamente o E4300 ganhou 75%, saltando de sua freqüência nominal de 1800 MHz para nada menos que 3150 MHz! Na prática, ele se sai tão bem ou superior que o mais recente modelo E6850, que opera a 3 GHz, já traz o FSB oficial de 1333 MHz (freqüência base de 333 MHz) e está cotado a US$ 266 na lista de preços da Intel.

É importante destacar também que esta elevação foi obtida dentro do concei-

F2. Core 2 Duo E4300 e identificação pelo CPU-Z sem e com overclock.



F3. Opções para ajuste da freqüência no barramento de memória.



Opção	Freq. RAM s/ over	Freq. RAM c/ over 350
Auto	800	1400
3.33	667	1166
3.20	640	1120
3.00	600	1050
2.5	500	875
2.4	480	840
2	400	700

T1. Relação entre freqüências padrão (200 MHz) e com overclock (350 MHz) do FSB do E4300, e respectivas freqüências resultantes no barramento de memória.

to do overclock seguro, segundo o qual o processador continua operando dentro das especificações definidas pelo fabricante e, portanto, sem induzi-lo a uma espécie de envelhecimento precoce.

Na entrada do circuito de alimentação da placa-mãe, ou seja, no conector ATX12, medimos uma potência de entrada máxima de 69,9W. Descontando os 10% tipicamente considerados como parte das perdas do circuito, vemos que a potência de trabalho do E4300 estava abaixo dos 65W definidos pela Intel no site **http://processorfinder.intel.com/details.aspx?sSpec=SL9TB**.

Em relação ao barramento de memória, o BIOS da Gigabyte usa o parâmetro "System Memory Multiplier" para oferecer sete opções para a definição da freqüência (figura 3). Como mostra a tabela 1, será que algum dos módulos avaliados suportaria a operação tal como um DDR2-1400, o qual sequer existe?

KHX6400D2ULK2/2G

O primeiro kit avaliado pertence à tradicional família HyperX da Kingston, linha esta dirigida ao segmento de aplicações que, a exemplo dos jogos, demandam alta performance do subsistema de memória (figura 4). Ele é composto por dois módulos de 1GB contendo 16 chips de densidade 64Mx8 bits cada. São oito chips em cada lado fazendo a interface com o ambiente através do clássico dissipador azul que a Kingston classifica como sendo de alta performance, mas não fornece detalhes sobre o material e pasta térmica empregados.

A temporização padrão gravada no chip EEPROM (SPD) é a definida pelo JEDEC para a operação em 800 MHz, ou seja, 5-5-5-15 e tensão de 1,8V. Esses serão os ajustes definidos automaticamente na inicialização da máquina para os casos em que o BIOS da placa-mãe não oferecer ajustes manuais, ou o usuário optar por deixar o parâmetro SPD em Auto.

Segundo a Kingston, esse kit também é capaz de operar com latências muito agressivas, 3-3-3-10, se a tensão for elevada para 2,3 ou 2,35V. Durante nossos testes, a performance desse kit foi até além disso, operando com total estabilidade a 840 MHz, 3-3-3-10 e tensão de 2,3V.

Já a 875 MHz e com os mesmos ajustes, o Windows Vista não completava o boot, o que só foi possível com uma tensão significativamente superior – 2,5V. Mas para fins de suporte válido e com total respaldo da garantia do fabricante, considere a freqüência de 840 MHz como limite.

Já no outro extremo, ou seja, quando o enfoque passou a ser maiores freqüências de operação no barramento de memória, novamente o kit surpreendeu, atingindo 1120 MHz com estabilidade. As latências de trabalho foram de 5-5-5-15 e com tensão de 2,3V. A operação acima dessa freqüência, ou com menores latências, só é possível mediante a elevação da tensão para valores não descritos como válidos.

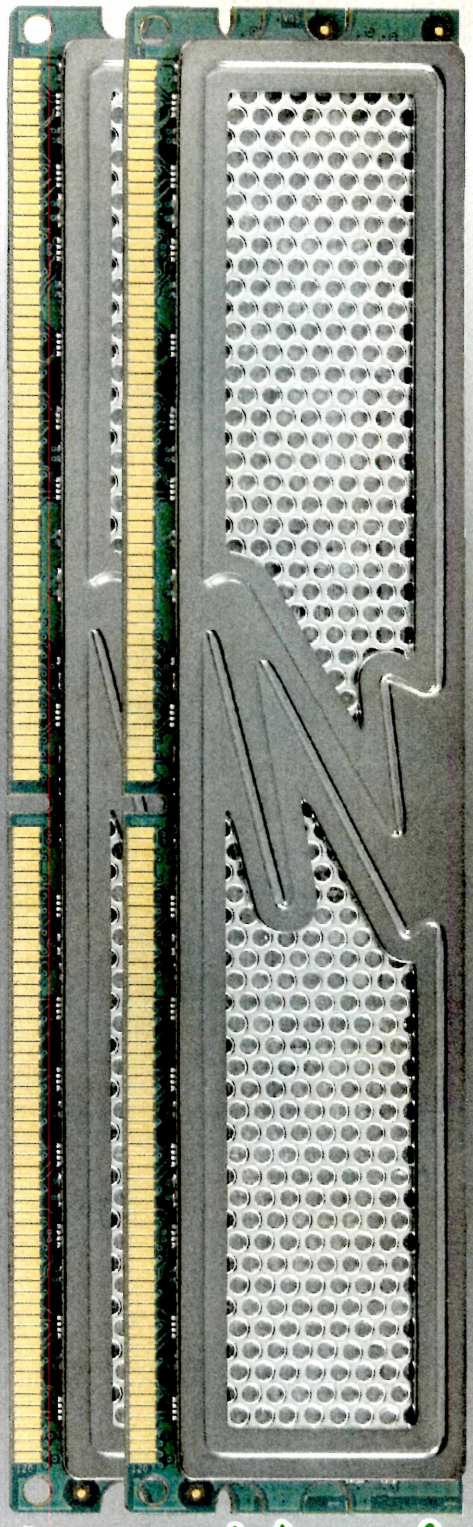
KHX9200D2K2/2G

O código já revela que este kit é similar ao anterior, tanto na densidade e quantidade de chips de memória empregados, quanto no acabamento e projeto térmico. O que muda essencialmente é a especificação de performance dos chips. O "9200" no código faz referência à máxima taxa de transferência oferecida, o que por analogia (considerando que cada módulo opera sobre um barramento de dados de 64 bits) nos indica a máxima freqüência suportada de 1150 MHz (9200/8 bytes) - figura 5.

A programação feita no SPD é idêntica a do kit anterior e a Kingston garante uma operação a 1150 MHz, com latências de 5-5-5-15 na faixa de tensão de até 2,35V. Se o kit anterior é especificado como DDR2-800 e suportou 1120 MHz, será que este 1150 suportaria 1400 MHz?

Os testes disseram que não! Mesmo com alimentação de 2,5V, o Windows Vista não conseguiu inicializar com a freqüência de 1166 MHz. E isso mesmo ao tentar fazê-lo em modo de segurança, quando grande parte dos drivers não são carregados. A operação totalmente estável e com tensão limitada a 2,35V foi obtida com a freqüência de 1120 MHz e latências 5-5-5-15. Ao tentar diminuí-las para 4-4-4-12, por exemplo, era necessário elevar a tensão para 2,5V.

Já no extremo das menores latências possíveis, a configuração 3-3-3-10 só foi possível até 700 MHz. A partir de 840 MHz,


Sovranità Info
www.sovranita.com.br
www.lojasovranita.com.br
DISTRIBUIDOR OFICIAL
OCZ Technology



F4. Kingston KHX6400D2ULK2/2G.



F5. Kingston KHX9200D2K2/2G.



F6. Kingston KHX6400D2K2/2GB.

só funcionou com tensão de 2,5V. Não resta dúvidas de que estamos diante de um kit inferior que o anterior.

KHX6400D2K2/2GB

O último kit avaliado da Kingston também consiste de dois módulos de 1 GB com organização similar de chips e projeto térmico. Mas diferentemente dos anteriores, as especificações não são tão agressivas (figura 6). A começar pelo SPD, a configuração definida é 667 MHz com temporização 5-5-5-15 e tensão de trabalho de 1,8V. Para ir até 800 MHz, a Kingston especifica uma tensão de 2,0V e a temporização continua sendo de 5-5-5-15. O diferencial está em uma pequena etiqueta com os dizeres "CrossFire Certified" colada na embalagem. Portanto, o enfoque principal deste kit está nos usuários de sistemas com duas placas de vídeo operando em CrossFire, que querem ter tranqüilidade ao obter um kit de memórias que seja reconhecidamente compatível com o hardware.

Durante os testes com a tensão limitada a 2,0V, a temporização 3-3-3-10 só foi obtida com a freqüência de 700 MHz. Ao aumentar a freqüência, o melhor ajuste foi 4-4-4-12, e nesse caso fomos até 875 MHz. Tentamos ainda 1050 MHz, porém o sistema sequer era capaz de inicializar o POST, mesmo diante de uma tensão de 2,2V e com latências mais relaxadas (6-6-6, por exemplo).

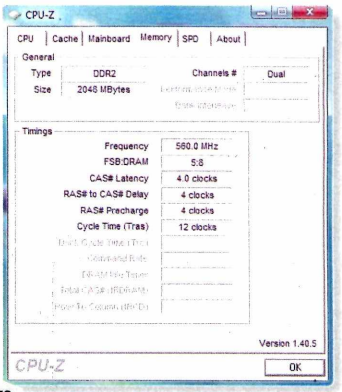
PDC22G9200ELK

Mais um kit Dual-Channel de 2GB certificado para freqüências de até 1150 MHz, desta vez assinado pela Patriot (figura 7), um fabricante não muito conhecido no Brasil, mas que no exterior possui boa reputação. Seguindo uma tendência neste mercado, o site da empresa apresenta um configurador online cujo objetivo é auxiliar o usuário a encontrar a memória mais adequada ao seu sistema. O suporte técnico também chama a atenção pela agilidade na resposta.

A apresentação do kit também é sóbria e apesar de não serem fornecidos detalhes sobre a pasta e a performance térmica do dissipador de alumínio empregados, o produto inspira confiança. Os valores gravados no SPD são de 5-5-5-16 para uma freqüência de 800 MHz. Vale destacar também o suporte ao perfil EPP (Enhanced Performance Profiles) gravado no SPD, que faz com que a memória inicialize automaticamente em 1142 MHz em placas-mãe com chipsets nVidia, também compatíveis com o EPP.

Caracterizado pelo fabricante como sendo um kit "Extreme Performance", ele está certificado para suportar latências 5-5-5-12 quando operando a 1150 MHz e com tensão de 2,3V.

No decorrer dos testes, mesmo com 2,5V ele não suportou com estabilidade a freqüência de 1166 MHz. Porém, surpreendeu positivamente nos testes a 1120 MHz ao suportar a temporização 4-4-4-12 e sob a tensão padrão de 2,3V (figura 8). Nesta condição, o kit apresentou os melhores resultados de todo o comparativo, conforme demonstraremos nos gráficos a seguir.



F8. PDC22G9200ELK: estabilidade a 1120 MHz e latências consideradas baixas para módulos DDR2.

Além disso, ele também se comportou muito bem nos testes com menores latências. A configuração 3-3-3-10, por exemplo, rodou de forma absolutamente estável com a freqüência de 875 MHz e tensão de 2,3V.

PDC22G8500ELK

Esse kit de 2 GB segue a mesma linha de desenvolvimento do anterior. O projeto contempla chips distribuídos nos dois lados da placa de circuito impresso e utiliza o dissipador de alumínio preto. A temporização gravada no SPD também é 5-5-5-16 para a freqüência de 800 MHz, e há o suporte ao perfil EPP da nVidia. A diferença fica por conta dos chips DDR2 empregados, que segundo o fabricante foram homologados para operarem em 1066 MHz com latências 5-5-5-9 e tensão de 2,3V (figura 9).

No início dos testes, era forte a impressão de que esse kit superaria o anterior. A 1166 MHz, latências 4-4-4-9 e tensão de 2,3V, o Windows Vista conseguia inicializar, entretanto logo travava a interface gráfica. Operando a 1120 MHz, o Vista ficou estável, mas alguns testes não eram concluídos com



F7. PDC22G9200ELK.



F9. PDC22G8500ELK.



F10. PEP21G6400EL.

sucesso. Por fim, a estabilidade total veio com 1050 MHz e resultados muito próximos dos apresentados pelo kit anterior. Entre os testes para encontrar a maior freqüência suportada, o melhor ajuste foi de 1120 MHz com latências 5-5-5-9 e preservando a tensão nominal suportada de 2,3V.

PEP21G6400EL

Disponível em módulos de 512 MB, 1 e 2 GB, ou na forma de kit com dois módulos de 2 GB, esse módulo também pertence à linha "Extreme Performance" da Patriot, onde o principal diferencial está nos chips empregados. Diferentemente dos anteriores, nesse caso os chips suportam ajustes apenas medianos, sendo nominalmente classificados como DDR2-800 e latências 5-5-5-12 para uma tensão de 2,0V (figura 10). Aliás, esses são os valores gravados no SPD.

Os valores máximos suportados durante os testes foram de 840 MHz para latências 4-4-4-12 e 875 MHz para 5-5-5-12, sempre respeitando a tensão nominal de 2,0V. Os resultados foram muito próximos, mas no geral a primeira configuração foi superior. Vale dizer que a 1050 MHz o sistema sequer foi capaz de iniciar o POST, mesmo com piores latências e maiores valores de tensão.

OCZ2FX800C32GK

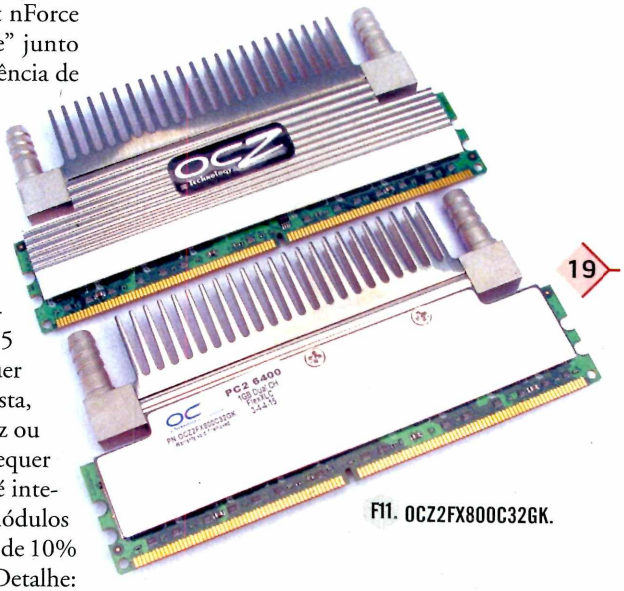
Partindo agora para os módulos da OCZ, outro fabricante de grande prestígio neste segmento, o grande destaque inicial deste kit de 2 GB é o apelo visual. Batizado de Flex XLD, o projeto térmico baseado em um dissipador híbrido, com partes em cobre e em alumínio, também suporta refrigeração líquida a partir de duas conexões com diâmetro interno de ¼"(figura 11).

Curiosamente, seu ponto forte também vem a ser um motivo de preocupação devido à sua maior altura em relação aos projetos tradicionais. Em nosso caso, por exemplo, tivemos de substituir o CPU cooler Gemini II (usado com todos os outros kits) pelo Hyper 6+, ambos da Cooler Master.

Outro detalhe que chama a atenção positivamente neste kit é o suporte oficial a tensões de até 2,4V. Aliás, esse valor inclusive faz parte do perfil EPP gravado no SPD. Em uma placa com chipset nForce 680i SLI, por exemplo, ele "sobe" junto com as latências 3-4-4-15 e freqüência de 800 MHz. Já em placas cujos chipsets não suportam o EPP, o valor pego automaticamente é 5-5-5-15 e freqüência de 800 MHz.

Em nosso teste, ele foi além da especificação oficial ao suportar com estabilidade as latências 3-4-4-15, com uma freqüência de 875 MHz e tensão de 2,35V. Em qualquer configuração mais otimizada que esta, tal como freqüência de 1050 MHz ou latências de 3-3-3-10, a máquina sequer iniciava o POST. Por outro lado, é interessante ver a capacidade desses módulos em fornecerem um ganho gratuito de 10% na freqüência, aproximadamente. Detalhe: e isso sem qualquer refrigeração líquida.

Já entre os testes com maiores freqüências, esse kit foi capaz de iniciar o POST com uma freqüência de 1120 MHz e atingiu a estabilidade total com 1050 MHz, latências 5-5-5-15 e tensão de 2,35V.



F11. OCZ2FX800C32GK.

tende a promover uma transferência térmica mais eficiente (figura 12).

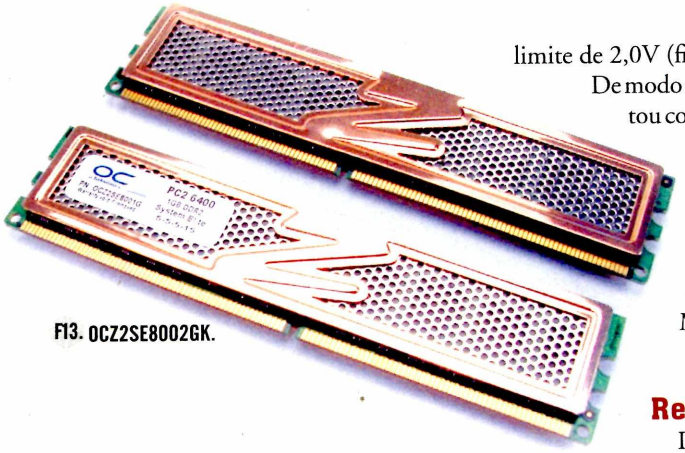
No início dos testes, uma surpresa: não é que esse kit foi capaz de iniciar o POST operando a 1400 MHz! Por outro lado, de modo algum conseguimos fazê-lo concluir a inicialização do Vista. Mesmo com latências

OCZ2N900SR2GK

De forma similar ao Kingston certificado para CrossFire, esse kit da OCZ possui certificação para configurações multi-GPU, nesse caso para o SLI da nVidia. Devido ao perfil EPP também presente, esses 2 GB inicializam com latências 4-4-3-15 e freqüência de 900 MHz em chipsets compatíveis com o EPP. Nos demais chipsets, sobe a configuração padrão 5-5-5-15 e 800 MHz. A tensão de trabalho limite suportada é de 2,2V e o perfil do dissipador vazado



F12. OCZ2N900SR2GK.



F13. OCZ2SE8002GK.

elevadas e tensão de 2,4V. A estabilidade total e o maior desempenho vieram com os ajustes 1120 MHz, latências 5-5-5-9 e tensão de 2,2V.

Já no outro extremo, o das menores latências, a configuração 3-3-3-10 só rodou em 700 MHz. A partir da latência de CAS 4 obtivemos estabilidade com a configuração 875 MHz e latências 4-4-3-15. Com 1050 MHz, o POST era concluído, mas o Vista reiniciava ao carregar a interface gráfica.

OCZ2SE8002GK

Também conhecido como DDR2 PC2-6400 System Elite, nosso último kit de 2 GB avaliado faz parte da linha de entrada, básica da OCZ. Não há o suporte ao EPP da nVidia, e os valores declarados oficialmente são 800 MHz para latências 5-5-5-15 e tensão limite de 2,0V (figura 13).

De modo surpreendente, ele suportou com total estabilidade a freqüência de 875 MHz para o ajuste 5-5-5-15. Porém, em relação à melhor configuração de latência, 3-3-3-10, ele ficou limitado a 700 MHz.

Resultados

Dentre os componentes comuns do sistema avaliado, estiveram uma placa de vídeo Power Color com processador gráfico Radeon HD 2900 XT, um HD SATA modelo Barracuda 7200.8 400 GB da Seagate e uma fonte Cooler Master de 1000W (modelo RS-A00-EMBA). O Windows Vista Home Premium 32 bits foi instalado em uma partição NTFS de 50 GB com os seguintes programas: Sandra XI.SP2 e Everest aferindo a performance bruta do subsistema de memória (vazão de dados pelo barramento e latência de acesso); dentre os jogos, utilizamos o Quake 4 com patch 1.3 para SMP rodando um *timedemo* de 12879 frames gravado por nossa equipe e o Far Cry com patch 1.4 sendo disparado através do programa de benchmark HardwareOC Far Cry e rodando os *timedemos* Steam e Volcano.

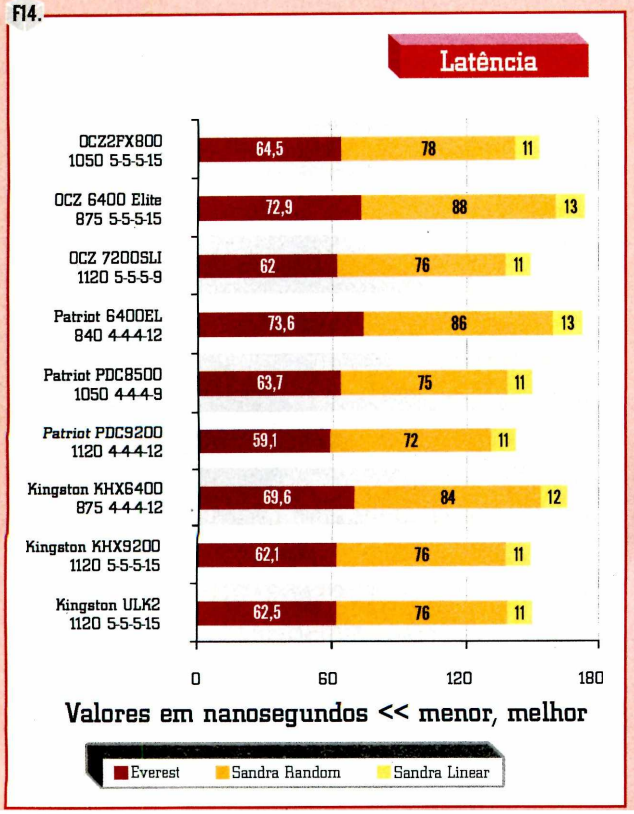
Por último, reproduzimos um cenário com aplicações de uso típico de todo usuário: iTunes 7 convertendo 20 arquivos wav (total de 1,48 GB) para MP3 com codificação CBR de 320 kbps; 3ds Max 9 com Service Pack 2 tomando como entrada o projeto de referência radiosity do programa e produzindo uma animação contendo 20 frames e formato de saída avi (com codec DivX 6.6.1 otimizado para multithreading); e o Winrar 3.70 usando sua melhor taxa de compactação sobre um arquivo de extensão .dbx com 218 MB.

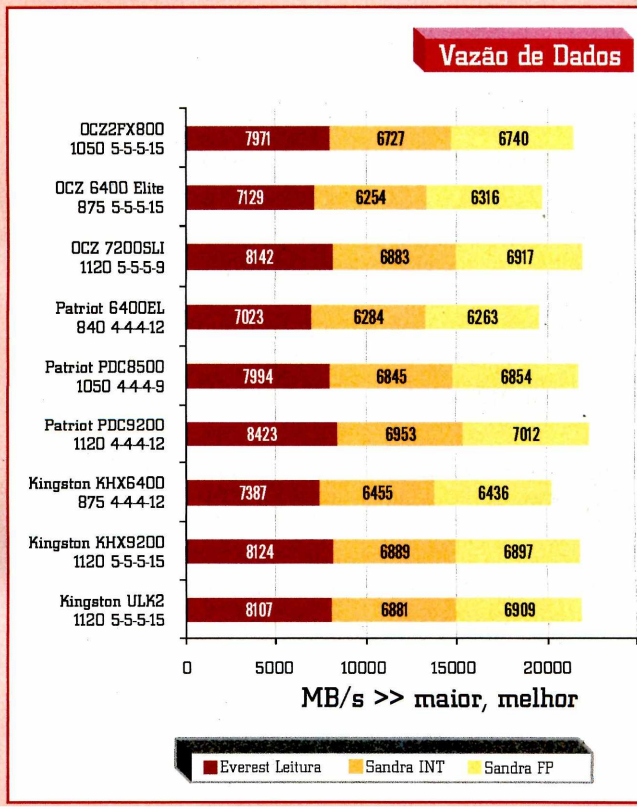
Começando pelos testes sintéticos, já podemos ver a liderança do kit Patriot PDC9200. No geral, ele disponibiliza os dados em um intervalo de tempo 5% inferior que o segundo colocado, e em um dos testes do Sandra ele foi o único a suportar uma vazão de dados superior a 7000 MB/s (figura 14).

Isso foi suficiente para que ele mantivesse a liderança em todos os demais testes que são mais dependentes do acesso à memória. No Winrar, por exemplo, o kit de pior performance foi 20% mais lento que ele (figura 15). E nos jogos, essa diferença ficou entre 5 e 8% (figura 16). Porém, o iTunes e o 3ds Max estão aí para demonstrar que, dependendo do algoritmo do programa, praticamente não haverá diferença entre um kit de 100 e outro de 200 dólares.

É importante ter isso em mente para evitar frustrações. Não é à toa que os fabricantes desses módulos de grife focam em nichos de público como os gamers, que buscam

F14.





a máxima performance do sistema sem se importarem muito com a questão dos custos. Se a princípio parece banal pagar o dobro para ter alguns frames a mais durante os jogos, por outro lado será essa "folga" de frames que fará a diferença entre ter ou não jogabilidade em determinados cenários, tais como em maiores resoluções de imagem ou com filtros de qualidade ativados.

Conclusões

Exploramos nesta matéria os recursos e a performance apresentada por nove dos melhores kits de memória DDR2 disponíveis atualmente no mercado. Uma evidência clara disso é o fato de todos, de uma maneira geral, terem operado com total estabilidade em configurações de freqüências e latências que inclusive excedem as informadas pelos fabricantes. É diferente de módulos genéricos que sofrem de problemas de compatibilidade e para cumprir com o especificado.

Além disso, aspectos não tão discutidos aqui, como estabilidade e confiabilidade mesmo sob condições adversas, estão a favor desses módulos de grife sob a forma da garantia vitalícia dada por seus fabricantes.

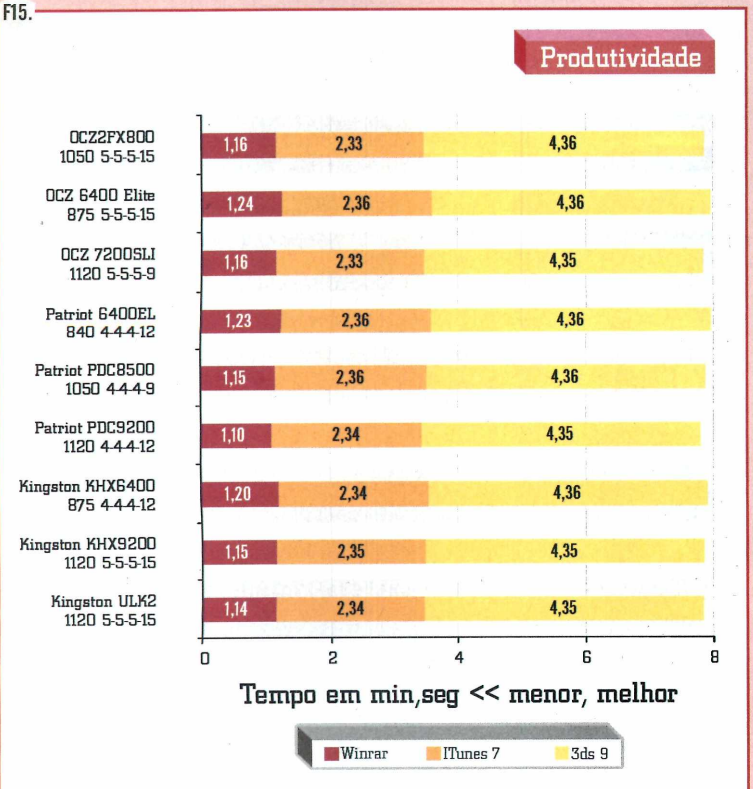
Com os dados publicados e o conhecimento prévio do comportamento da controladora de memória em arquiteturas AMD e Intel atuais, fica fácil decidir qual deles melhor atenderá às suas necessidades. Neste sentido, as informações da tabela 2 são pertinentes porque demonstram o que esperar desses kits em sistemas AMD e mesmo nos Intel sem ou com pouco overclock, cenários estes onde o que mais importará é a capacidade dos módulos em suportar baixas latências. Além disso, estamos informando também os preços praticados nos EUA para termos uma noção um pouco melhor do posicionamento de mercado desses kits.

Deixando de lado o fator custo, o kit Patriot PDC9200 é seguramente a melhor opção. Pois além de entregar a maior performance, também se demonstrou muito versátil ao suportar uma temporização extremamente agressiva de 3-3-3-10, com freqüências de até 875 MHz. Na seqüência, vem o Patriot PDC8500, com um custo significativamente inferior e na mesma faixa de preço de seus concorrentes da OCZ, mas sendo o único a suportar 3-3-3-10 em operação a 875 MHz.

Resta saber agora como está a questão da disponibilidade e dos preços praticados aqui no Brasil por cada representante e/ou distribuidor. Se você precisar de algum auxílio durante a análise, fique à vontade para entrar em contato conosco.

Por último, em uma época de tantas inovações onde vemos refrigeração líquida e outros projetos exóticos de dissipação térmica, perfis específicos de temporização em iniciativas como o EPP da nVidia, além de chips de memória cada vez mais flexíveis e suportando tensões elevadas, fica registrada

F15.



PATRIOT MEMORY
GOPAN IMPORTAÇÃO E EXPORTAÇÃO

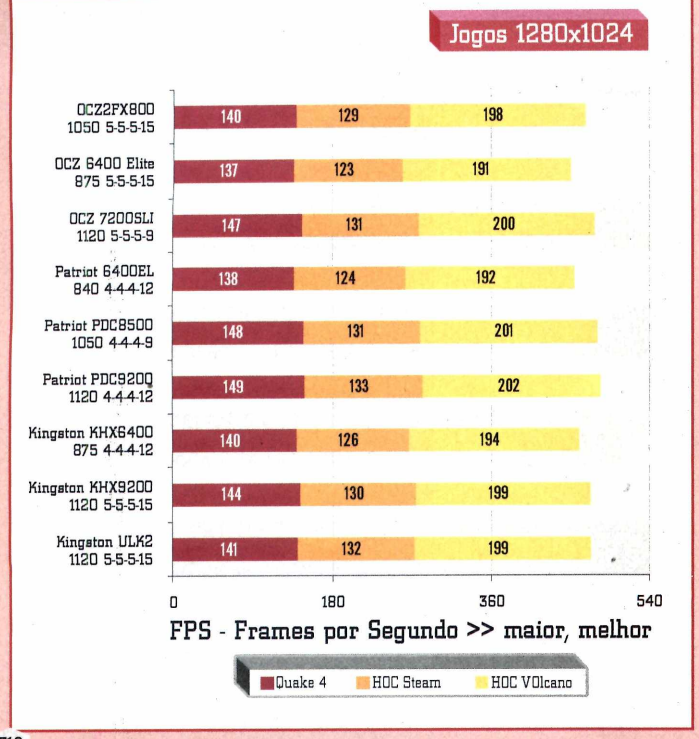


A Patriot Memory mundialmente famosa por seu desempenho impecável, chega oficialmente ao Brasil.

PREÇOS ESPECIAIS PARA O BRASIL !!!

DDR - até 400Mhz
DDR2 - até 1200Mhz
DDR3 - até 1600Mhz
Pen drive com 200x de velocidade
Cartões de memória

Gopan, representante oficial da Patriot no Brasil, procura por distribuidores e/ou integradores em todo o país. Finish goods, SKD e/ou CKD.
Mais informações, por favor, e-mail para:
patriotmemory@gopan.com.br



F16.

Kit 2 GB	Menores Latências	Preço em US$
Kingston ULK2 1120 5-5-5-15	840 3-3-3-10	200
Kingston KHX9200 1120 5-5-5-15	840 3-3-3-10	214
Kingston KHX6400 875 4-4-4-12	700 3-3-3-10	141
Patriot PDC9200 1120 4-4-4-12	875 3-3-3-10	296
Patriot PDC8500 1050 4-4-4-9	875 3-3-3-10	170
Patriot 6400EL 840 4-4-4-12	840 4-4-4-12	110
OCZ 7200SLI 1120 5-5-5-9	875 4-4-3-15	177
OCZ 6400 Elite 875 5-5-5-15	700 3-3-3-10	142
OCZ2FX800 1050 5-5-5-15	875 3-4-4-15	170

T2. Melhor resultado com baixas latências obtida por cada kit.

aqui uma sugestão para que os fabricantes incorporem algum sistema de leitura de temperatura nos módulos, ou ainda um transdutor de corrente. Com isso, os usuários teriam melhores condições para extrair a máxima performance do projeto de cada kit, haja vista o que aferimos em nossos testes, onde em muitas vezes uma tensão ligeiramente superior ao especificado era suficiente para que o módulo melhorasse bastante sua performance. Mas do modo como está hoje, é preciso uma certa engenhosidade para ter alguma idéia quanto à capacidade dos módulos em suportarem uma operação prolongada sob essas condições não documentadas. **PC**





A Tecnologia da Informação e as Telecomunicações estão em Tudo!

Participe do Futurecom 2007 e veja o quanto as aplicações tecnológicas podem impulsionar seus negócios de seus clientes!

Futurecom 2007
Tendências, Negócios e Networking no mais qualificado Evento de Telecom & TI da América Latina.
www.futurecom.com.br

futurecom
1 a 4 de outubro • 2007
FLORIANÓPOLIS

Suítes para proteção total na Internet

Atualmente já não basta só um anti-vírus e um firewall como proteção para a Internet. Veja o que mais é necessário para garantir a máxima proteção e acompanhe um teste com os principais produtos que prometem proteção total.



Marcus Brandão de Moura
Bacharelando em Sistemas de Informação. Certificado Nexans em cabeamento e D-Link DBCex e DBC, atualmente compõe a equipe de redatores da revista.

Riscos e mais riscos na Internet

A cada dia que passa, mais pessoas são pegas em algum tipo de golpe pela Internet como *phishing scan*, cavalo de tróia, vermes, vírus modernos e também os aparentemente nocivos, mas irritantes spams.

No mês passado, uma quadrilha de 65 "hackers" foi condenada por fraudes via Internet. Em um único dia, essa quadrilha desviou aproximadamente R$ 300.000,00 e chegou a causar um prejuízo da ordem de R$ 100.000.000,00 aos maiores bancos brasileiros.

Na maior parte das vezes, o atacante chega através de um e-mail contendo um *phishing scan*. Já passou o tempo em que bastava bloquear a recepção de anexos para conferir segurança às mensagens. As mensagens atuais trazem apenas links e apresentam remetentes falsos, além de uma página de destino falsa também.

Visando proteger o usuário final, as principais empresas de softwares de segurança na Internet lançaram pacotes "completos" que conferem um bom nível de segurança a um computador doméstico ou de uma microempresa.

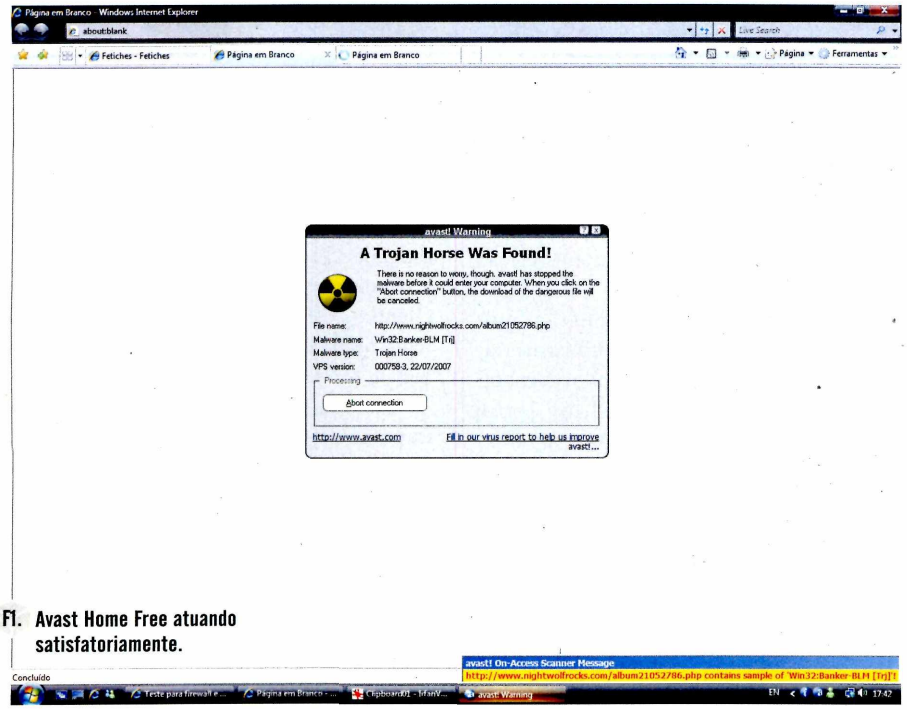
Você pode estar se perguntando do porquê de prestar tanta atenção em um teste com suítes domésticas de segurança para a Internet. É simples, a quase totalidade das pessoas que caem em golpes pela Internet o fazem, involuntariamente, lógico, através dos computadores de suas próprias residências, ou então de uma pequena rede de uma microempresa.

Mas onde você entra nisso? Em duas situações. Na primeira, como possível vítima e que após este artigo, esperamos que não tenha mais esse tipo de problema; e na segunda, como técnico em informática ou "Personal Security Consulting" de clientes pessoa física, que precisam muito dos seus serviços. Não vale a pena recomendar a um usuário doméstico algum tipo de software de segurança de caráter mais profissional. Isso poderia trazer problemas para o seu cliente e muita dor de cabeça para você. Já imaginou ter que retocar várias configurações de diferentes clientes todos os dias?!

Ordem do teste	Firewall
1º	McAfee Internet Security Suite 2007 - http://br.mcafee.com/root/downloads.asp?id=freeTrials
2º	Trend Micro PC Cillin Internet Security 2007 - http://us.trendmicro.com/us/products/personal/trend-micro-internet-security-2007/download/index.html
3º	Symantec Norton Internet Security - http://shop.symantecstore.com/store/symanbr/pt_BR/ContentTheme/pbPage.Trialware_pt_BR/ThemeID.15500
4º	Zone Labs Zone Alarm Internet Security Suite 7.1 - http://www.zonealarm.com/store/content/catalog/products/trial_zaFamily/trial_zaFamily.jsp?dc=12bms&ctry=BR&lang=pt
5º	Grisoft AVG Internet Security - http://www.avgbrasil.com.br/doc/downloads-trials/br-pt/crp/0?prd=isw&simple=1

T1. Ordem de instalação e teste de cada suíte.

Sites usados durante o teste. T2.		
http://security.symantec.com/sscv6/home.asp?langid=ie&venid=sym&close_parent=true	Varredura on-line na Symantec	Bom
http://www.blackcode.com/scripts/toolbox.php	Varredura on-line na Blackcode	Operação manual
http://housecall65.trendmicro.com/	Varredura on-line na Trend Micro	Bom
http://www.zonealarm.com/store/content/promotions/spywarescanner/index.jsp?lid=home_scanner	Varredura on-line na Zone Labs	Bom



F1. Avast Home Free atuando satisfatoriamente.

O teste

Como se testa uma suíte de segurança contendo firewall, anti-vírus, anti-spam, anti-spyware e outras coisas mais?

Já fizemos um teste completo de firewalls gratuitos na edição 45, utilizando a mesma metodologia deste teste atual, por isso vamos evitar uma explicação mais demorada sobre a metodologia de teste e apresentar uma versão mais resumida. É justamente a porção firewall que dá mais trabalho para ser testada.

Já sabemos que não adianta muito fazer apenas os testes de escaneamento das portas TCP e UDP de dentro pra fora e de fora pra dentro. Além desse procedimento, temos que escanear as portas remotamente e o mais importante, tentar abri-las de forma forçada.

Sorteamos uma ordem para os testes dos nossos candidatos, então ficamos tal como mostrado na tabela 1.

Utilizamos serviços gratuitos disponíveis na Internet para ajudar nos testes. Esses serviços escaneavam as portas e verificavam a vulnerabilidade do sistema (tabela 2).

Nesse teste comparativo, nós fizemos tudo isso e fomos além, visitamos sites reconhecidamente maliciosos para ver se nossos oponentes conseguiam se manter inalterados diante do perigo real.

A lista dos sites maliciosos pode ser encontrada no site da revista PC&Cia (www.revistapcecia.com.br). Para cada site oferecemos um tempo de permanência de 5 minutos, com uma conexão a cabo de 450 kbps. Mas antes desses testes dinâmicos com os sites, foram feitos os testes estáticos locais.

Utilizamos o comando "netstat –a –b –n" no prompt de comando do Windows Vista Ultimate. Esse comando lista as portas TCP e UDP, o processo (programa) que as está utilizando e o estado da porta. Quando digitar esse comando, lembre-se de fazê-lo como administrador, caso contrário receberá uma mensagem dizendo que o comando requer "elevação".

Antes de iniciarmos cada teste executávamos uma varredura completa com o AVG Anti Spyware 7.5 em todo o disco de teste.

Além disso, antes de se iniciar cada teste, tanto o Windows Vista Ultimate quanto a suíte recém-instalada era totalmente atualizada via Internet. Ao final de cada teste, um novo escaneamento era realizado pela própria suíte, depois pelo pacote de software da nossa instalação de controle contendo o AVG PRO-Anti Malware 7.5 trabalhando junto com o Zone Alarm Professional 7.0 com anti-spyware. Como fonte de preciosas informações, usamos os sites listados na tabela 3.

T3. Sites usados para informações.

http://www.sans.org/resources/	Lista das portas TCP e UDP e os trojans que as usam.
http://www.simovits.com/trojans/trojans.html	Lista das portas TCP e UDP e os trojans que as usam.
http://www.grc.com/default.htm	Softwares para testes e informações variadas

Cada suíte levou aproximadamente dois dias para ser testada, com uma interrupção à noite. Felizmente sempre conseguimos assegurar que nosso sistema estava totalmente livre de problemas de segurança, antes de iniciar os testes pra valer. Também não precisamos reinstalar o Windows Vista Ultimate, ao contrário do Windows XP Professional que utilizamos no teste anterior, publicado na edição 45.

Utilizamos uma coleção de onze vírus para testar através de disquetes e pen drives o desempenho das suítes. Somente o vírus RavMon deu um pouco de trabalho, os outros foram rápidos e totalmente eliminados.

Através de mensagens *phishing scan* selecionamos uma preciosidade recente de 37 links para páginas em funcionamento com conteúdo comprovadamente nocivo, era uma verdadeira festa de trojans. Por padrão, decidimos baixar propositadamente todos os arquivos que o Internet Explorer 7 avisava existir. Em algumas páginas o IE 7 não emitia o alerta, mas a maior parte das suítes detectou e eliminou o arquivo de forma eficiente.

O Windows XP Pro com o Service Pack 2 não foi utilizado para qualquer tipo de comparação. Nossa instalação de referência foi feita com o próprio Windows Vista Ultimate acompanhado apenas do anti-vírus gratuito Avast! 4.7 e seus componentes nativos. Esse sistema foi usado como forma de comparação da eficiência das suítes; além disso, ele foi uma espécie de "fiel da balança".

Promovemos uma digna disputa entre todos os nossos candidatos e de uma forma geral o resultado foi satisfatório. Assim, já podemos dizer que evidentemente é melhor ter um firewall do que não ter firewall algum, assim como é melhor ter anti-vírus, anti-malware, anti-spam e os adicionais de segurança para os navegadores.

Em todos os testes dinâmicos, usamos o Internet Explorer 7, porque ele é o navegador padrão do Vista Ultimate.

"Fiel da balança"

Nossa primeira instalação foi feita com o Windows Vista Ultimate acompanhado apenas do anti-vírus gratuito Avast! 4.7. Evidentemente, todas as atualizações de segurança do Windows Vista foram feitas antes de se realizar os testes.

Já previámos uma inundação de trojans, spywares e outras coisas mais "interessantes". Que nada. O sistema de referência se comportou quase tão bem quanto os superprotegidos por boas suítes de segurança.

Todas as "infecções digitais" que apareciam para que pudéssemos baixar, nós a baixamos e a instalamos manualmente, mas creditamos tanto ao Internet Explorer 7 quanto à suíte em teste o "ponto" por ter impedido o download automático. No sistema de referência, o "modesto" Avast, que é gratuito, detectou e alertou para três dos 11 arquivos baixados, através de sites maliciosos (figura 1).

O firewall nativo do Windows Vista Ultimate também se comportou bem e manteve as portas TCP e UDP fechadas. De uma forma geral, o desempenho do sistema de referência nos surpreendeu positivamente, apresentando um resultado significativamente melhor do que o Windows XP com Service Pack 1 e sensivelmente melhor do que o XP com Service Pack 2.

No total, fomos contaminados por nove das 11 mazelas digitais, que foram combatidas por um trabalho em conjunto entre Spy Bot 1.4, AdAware SE 1.06, Zone Alarm PRO 7.0 e AVG PRO anti-malware 7.5. Vale lembrar que a instalação de referência foi idealizada mesmo para contrair o maior número possível de mazelas digitais que nos eram servidas. Sob esse aspecto, deu certo, pegamos tudo que podíamos pegar.

Gostaríamos de organizar a apresentação dos resultados de forma a declarar um vencedor e listar as cinco suítes em ordem crescente de posicionamento no teste. Mas a proximidade dos resultados foi tamanha que não seria de todo muito prudente declarar um vencedor, afinal, nossos sites de testes foram apenas uma amostragem de 37 páginas que apresentavam o pior que pudemos encontrar.

Soma-se a isso as novas características de segurança do Windows Vista e do Internet Explorer 7, que nos deu um efetivo acréscimo de proteção disponível igualmente a todas as suítes, encurtando ainda mais a diferença entre cada uma delas. Os resultados dos testes não chegaram a apresentar um empate técnico entre todas as suítes.

Vamos aos resultados!

Zone Alarm Internet Security Suíte 7.1

Testamos a versão 7.1 do Zone Alarm Internet Security, a mais completa e igualmente cara da Zone Labs. Como é comum antes de iniciarmos um teste, fizemos algumas apostas e estas diziam que a porção firewall da suíte se sairia muito bem, mas a porção anti-vírus estaria meio aquém em relação aos concorrentes.

Sem bola de cristal acertamos nas nossas apostas! Porém, só conseguimos acertar mesmo, porque acompanhamos o desenvolvimento dos produtos da Zone Labs, que foi adquirida pela Check Point. Por enquanto, esta empresa só modificou o logo principal do Zone Alarm e alguns ícones, no mais, só retoques e atualizações foram feitas nas versões 7.x.

De cara o Zone Alarm vai muito bem em relação a orientar o usuário a usar e configurar o produto. Um completíssimo tutorial entra em ação logo após a instalação. O usuário doméstico que tiver um conhecimento razoável de inglês poderá realizar uma boa configuração sem qualquer tipo de ajuda de terceiros.

A interface principal (figura 2) do Zone Alarm é muito intuitiva e apresenta na mesma tela todos os menus organizados do lado esquerdo, na vertical. Cada menu selecionado exibe algumas guias que contêm as informações de configuração.

A possibilidade de se escolher ajustes predefinidos de proteção, como alto, médio e baixo, ajuda muito o usuário doméstico que não possua o conhecimento técnico necessário para realizar manualmente uma configuração desse tipo.

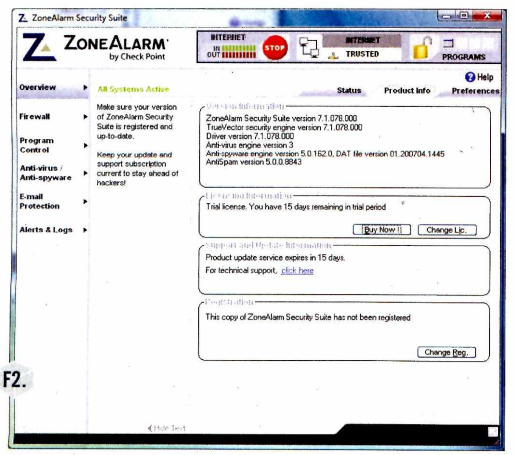
Também é possível promover uma integração entre o Zone Alarm e o anti-vírus instalado, que não precisa ser da Zone Labs, teoricamente. Com a suíte completa essa função funcionou perfeitamente bem, mas na hora de reconhecer um anti-vírus de outro fabricante, nada feito.

O Zone Alarm simplesmente não foi capaz de detectar a presença desses anti-vírus. Entretanto, com a função de interação com clientes de e-mail, nenhum problema foi registrado com o Outlook Express e nem com o Mozilla Thunderbird.

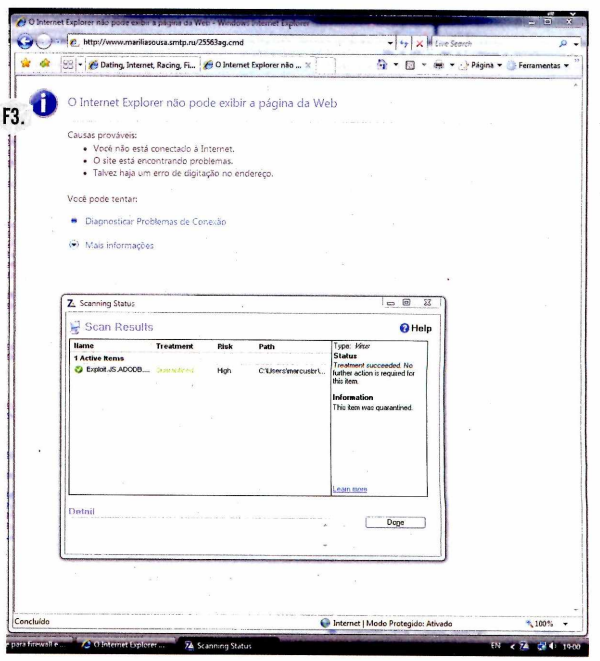
Frente à concorrência, o segundo ponto importante ganho pelo Zone Alarm foi a possibilidade de se acrescentar regras avançadas ou implementadas manualmente. Assim, pode-se bloquear sites, domínios e URLs.

Seu desempenho sempre foi muito bom, mas o produto já não parece ser mais tão extremamente estável quanto fora. O ícone na barra de notificação não é lá muito intuitivo. Ora aparece o logo do Zone Alarm "by Check Point" e ora aparecem barras gráficas verde e vermelho, quando há trafego de rede. Só é possível saber qual barra indica a entrada e qual indica a saída quando se restaura a janela principal da suíte. A barra verde indica o tráfego de entrada. Bem que se poderia utilizar o intuitivo esquema de setinhas como na interface do antigo Sygate.

O Zone Alarm também identifica quais programas estão tentando acessar a Internet e a partir da interface apresentada, o usuário pode tomar sua decisão do que fazer, tendo à sua disposição a opção de salvar as



Interface principal do Zone Alarm Security Suíte. F2.



Ameaça removida em visita à página na Internet. F3.

configurações. Curiosamente essa pequena interface visual pop-up do Zone Alarm é a de lay-out mais inteligível de todas, mas a que apresenta a menor quantidade de informações técnicas.

A maior ausência em termos de recursos por parte da suíte da Zone Labs foi um componente que interagisse com o navegador e que bloqueasse previamente a tentativa de acesso às páginas catalogadas como nocivas. Esse é o primeiro combate contra o download de malwares e também um dos mais importantes por oferecer os melhores resultados de imediato.

Os testes estáticos foram ótimos e sem qualquer tipo de surpresas. Aliás, podemos adiantar logo de uma vez que o resultado dos testes estáticos foi o mesmo para todos, ou seja, todas as portas estavam fechadas quando o sistema se encontrava em estado de inatividade.

A suíte do Zone Alarm é mais indicada para quem precisa fazer configurações de firewall personalizadas com uma razoável freqüência e também para quem não precisa tanto assim de um anti-vírus extremamente "potente". A porção anti-spyware também funciona muito bem. É uma pena que o Windows Vista tenha incluído com sucesso algumas das mais interessantes funções de monitoramento de atividades e interceptação de programas tradicionalmente incluídas nessas suítes. As versões para Windows XP permanecem com essas funções intactas e, diga-se de passagem, funcionando muito bem.

A síntese dos resultados para a suíte da Zone Labs foi a seguinte: 37 sites visitados com sucesso, óbvio, nenhuma página bloqueada previamente, quatro downloads bloqueados previamente (figura 3), 11 arquivos baixados manualmente, dois dos 11 arquivos baixados não foram eliminados.

Grisoft AVG Internet Security 7.5

Chega a ser curioso como cada um dos produtos das suítes começa a apresentar uma especialidade mais marcante. No caso da Suíte AVG, o forte é a detecção de vírus e spywares após o download. É impressionante!

Com essa suíte, tivemos o primeiro contato com as atuações dos softwares componentes em background. A suíte AVG não fica avisando o tempo todo que alguma coisa foi encontrada, pelo contrário, ela apresenta um comportamento mais discreto e sóbrio, o que confere maior tranqüilidade ao usuário, sem prejuízo de segurança ou proteção.

Por conta dessa característica, o AVG passou adiante o troféu de detecção, mas tornou-se um sério candidato ao troféu de eliminação de malwares em silêncio.

Outro bom comportamento da suíte AVG foi sua degradação de desempenho do sistema operacional no dia-a-dia. O reflexo no desempenho foi muito pequeno, sendo superior somente à suíte da Zone Labs, que não é tão eficaz quanto o produto da Grisoft.

A interface do AVG Internet Security 7.5 é boa, mas pode melhorar. As telas de configurações costumam ser muito pequenas e encontram-se uma dentro da outra. É menos intuitivo do que os concorrentes.

Para compensar essa deficiência, a suíte AVG foi a melhor em atualização (figura 4). Todos os dias, quando se entra no sistema operacional, o gerenciador de atualização entra em funcionamento. O mais impressionante é que quase todo dia tem atualização para ser baixada. Esse é um ótimo comportamento dessa suíte.

Vale lembrar que todas as suítes em teste foram mantidas com suas respectivas configurações e composições padrão de fábrica. Evidentemente todas elas ainda podem melhorar sensivelmente através de ajustes finos nas configurações, mas normalmente um usuário doméstico não realiza esse tipo de ajuste.

A suíte AVG não foi capaz de bloquear previamente nenhum site, mas pelo menos há uma razão para isso, ela não apresenta o plugin para o navegador, que fica monitorando os sites que se deseja acessar.

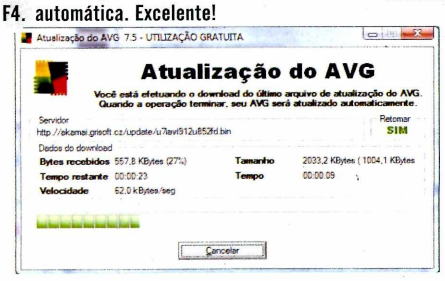
Aliás, em termos de interatividade com o usuário, o AVG só se manifestou uma única vez (figura 5) para impedir declaradamente o download de um arquivo malicioso. Malicioso não, um cavalo de tróia mesmo!

Os testes estáticos não revelaram surpresas, as portas TCP e UDP se mantiveram fechadas e protegidas. As novas redes eram identificadas automaticamente, assim como em todos os produtos testados. As tentativas de acesso externo eram alertadas por uma caixa de diálogo, com um conteúdo bem detalhado (figura 6). Isso ocorria sempre que o Internet Explorer 7 travava, mas ele "só" travou sete vezes.

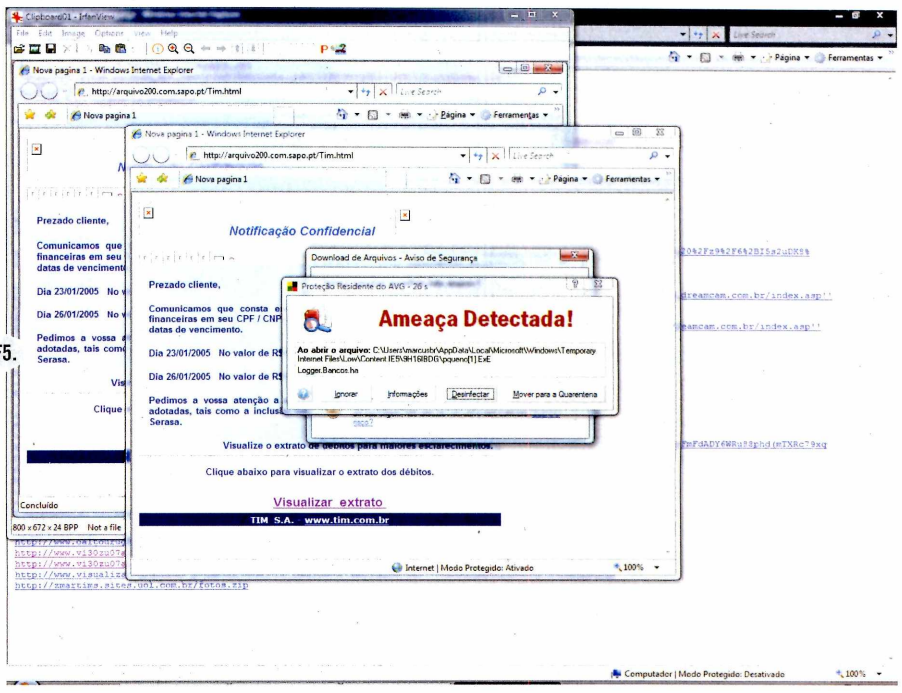
A síntese dos resultados para a suíte da Grisoft foi a seguinte: 37 sites visitados, nenhuma página bloqueada previamente, um download bloqueado previamente, 11 arquivos baixados manualmente, um dos 11 arquivos baixados não foi eliminado.

27

Atualização diária automática. Excelente! F4.



Ameaça removida em visita à página na Internet. F5.



Symantec Norton Internet Security

Talvez a suíte da Symantec tenha a maior fidelização por parte de seus clientes. De uma maneira geral, trata-se de um produto confiável, estável e muito bem acabado. O mais importante é que a ótima interface gráfica passa exatamente essas sensações para os usuários. Isso acaba inspirando confiança.

Os ícones e desenhos da interface gráfica são dignos da sofisticação gráfica do Windows Vista e seu novo padrão.

Os procedimentos de atualização são mais detalhados do que o das outras suítes. Isso ocorre porque a atualização de cada componente da suíte é feita de forma independente, mas seqüencial, o que dispensa o usuário de ter que selecionar esse ou aquele componente, tudo é atualizado a partir de um clique do mouse. O que também difere em relação às outras suítes é que o produto da Symantec instala um software, o LiveUpdate, só para se incumbir das tarefas de atualização dos componentes da suíte. Funciona sem problemas.

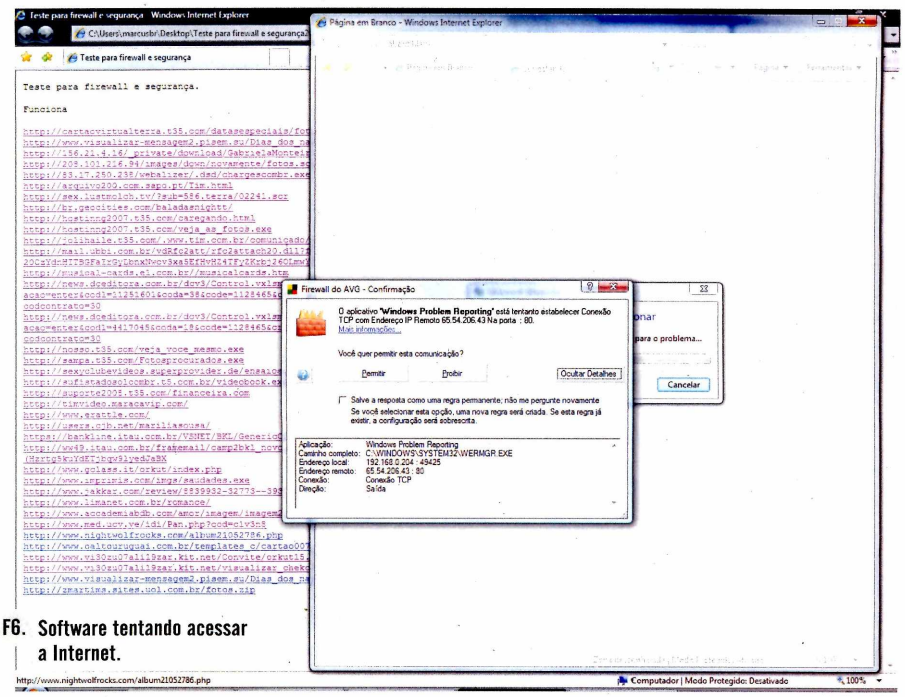
O Norton anti-vírus já é muito conhecido e seu firewall está cada vez mais amadurecido. O que chamou a atenção nesta suíte foi seu comportamento em background. Nenhum aviso sobre problemas em sites visitados foi emitido. A função de "Monitoração de Fraudes" (ver box) também não emitiu um único alerta, o que nos deixou receosos sobre o bom funcionamento deste componente em específico, principalmente depois que o software não encontrou sinais de fraude em uma página falsa de um home banking de um grande banco brasileiro.

O anti-malware funcionou bem e o anti-vírus, melhor ainda. Porém o bom mesmo foi o sistema de auto monitoramento de estado de funcionamento da suíte. Uma espécie de check-list é apresentado e reportado em uma tela do Norton Protection Center. Isso é ótimo para saber se está tudo bem ou se algo requer atenção (figura 7).

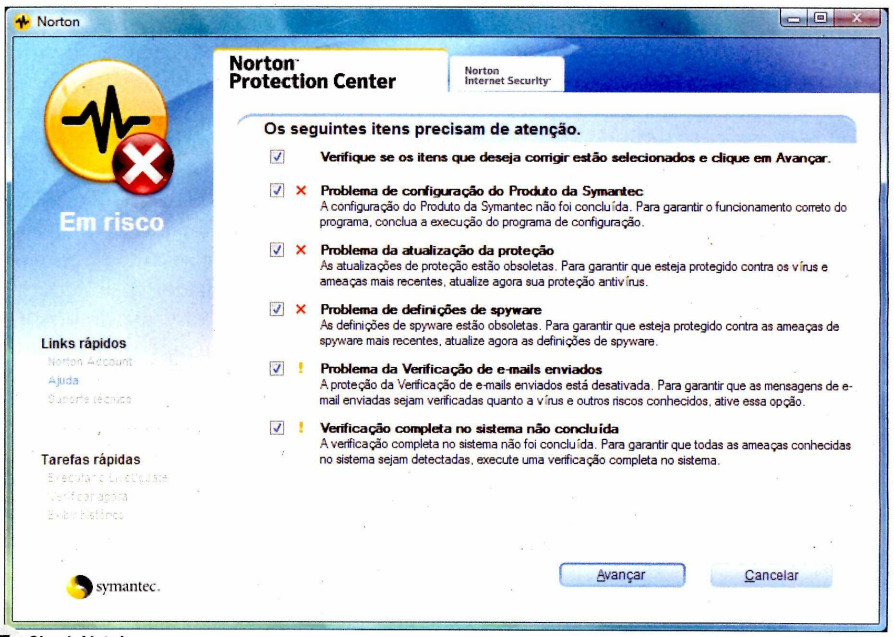
A suíte da Symantec tem um sistema de auto proteção de seus arquivos funcionais, assim como proteção das informações pessoais dos usuários e controle dos pais. Um excelente recurso foi a inclusão de um IPS (Intrude Prevent System – Sistema de Prevenção de Intrusão) que oferece proteção contra intrusões e ainda pode tentar bloquear o atacante por um determinado tempo. O tempo padrão é de 30 minutos (figura 8).

Os registros das atividades do Norton Internet Security são muito bem feitos e detalhados. Ótimo para quem tem conhecimento sobre o assunto e precisa tomar alguma decisão a respeito.

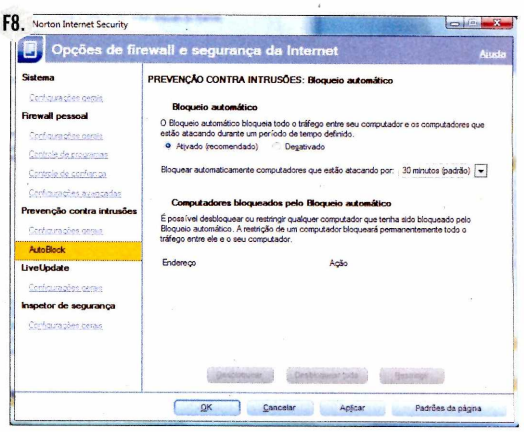
A síntese dos resultados para a suíte da Symantec foi a seguinte: 37 sites visitados, nenhuma página bloqueada previamente, nenhum download bloqueado previamente, 11 arquivos baixados manualmente, todos os 11 arquivos baixados foram eliminados.



F6. Software tentando acessar a Internet.



F7. Check List de segurança. Ótimo para os distraídos.



F8. Configuração do IPS. Bloqueio do atacante por 30 minutos.

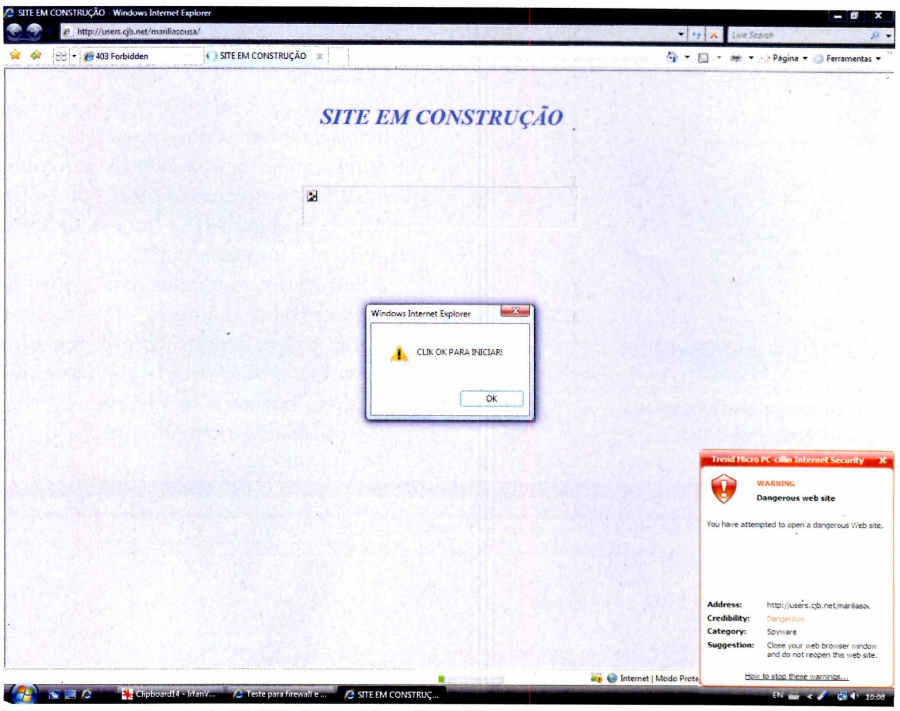
TrendMicro PC Cillin Internet Security 2007

Há quem esteja pensando: PC Cillin não era aquele anti-vírus que vinha de brinde nos CDs das placas-mãe PCChips? Aquele que dificilmente alguém confiava. Isso mesmo. Mas procure ver os produtos atuais dessa empresa sem preconceito. Ofereça uma chance, assim como nós fizemos. Possivelmente você ficará surpreso!

De início já dá pra notar que a interface gráfica chama atenção por ser pobre. Pobre não, limpa, sem excessos, "clean". Isso a torna intuitiva, confortável, organizada e como conseqüência, consome menos recursos do sistema do que seus concorrentes. Talvez a interface do AVG possa consumir menos recursos ainda, mas esta possui telas bem menores do que as do PC Cillin Internet Security 2007.

O PC Cillin Internet Security 2007 está situado entre as cinco suítes que estão sendo testadas no que diz respeito aos recursos que a compõem. Ele só perde em recursos para o Norton Internet Security e para o McAfee Internet Security Suite 2007, porque não tem um componente de verificação on-line de sites como o McAfee Site Adivisor, que tem uma versão gratuita e outra, melhor, paga. Acontece que a própria Trend Micro tem o seu plugin, o Trend Protect, para os navegadores Internet Explorer e Mozilla Firefox, o qual pode ser baixado gratuitamente em **http://www.trendsecure.com/portal/en-US/free_security_tools/trendprotect.php?page=download**.

Nos nossos testes, o Trend Protect não funcionou com o Mozilla Firefox 2.0.0.5, aliás, durante a instalação, recebemos um curioso aviso de que o Firefox não estava instalado.



F9. Alerta contra Spyware do PC Cillin Internet Security 2007.

Na ocasião do download, não encontramos uma versão da suíte da Trend Micro em português, como também ocorreu com a suíte da Zone Labs. Isso pode até representar um ponto decisivo para o cliente deixar de comprar esta boa suíte de proteção.

O processo de atualização é simples e intuitivo, podendo ser feita de forma manual ou automática. Como toda a operação dessa suíte, seu teste estático de firewall se saiu muito bem, sem apresentar problemas.

Atualmente, a maior parte dos malwares vem mesmo pela Internet, por isso o teste dinâmico pela Internet é tão importante. Foi justamente nesse momento que o "patinho feio" se transformou em um elegante cisne. Ele foi o único que identificou um spyware em um dos sites de teste (figura 9).

Sua porção firewall teve um excelente funcionamento e não deu trabalho em momento algum. Mas bem que os alertas para as páginas poderiam ter uma opção que fizesse com que aquela página em questão fosse automaticamente bloqueada, para sempre. Isso realmente seria de grande utilidade.

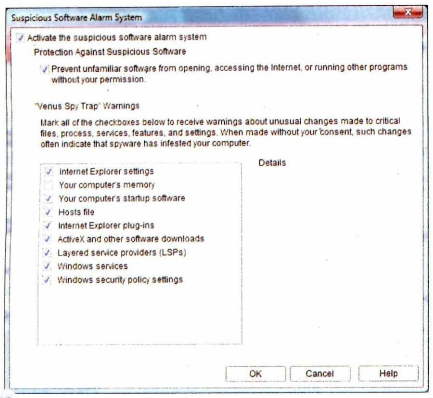
Existem ainda as funções de filtros de sites e anti-spam, como também ocorre nas outras suítes. Além disso, há um monitoramento das vulnerabilidades dos componentes e sistemas da Microsoft e também de alterações

Home Banking falso

Existem várias páginas falsas de vários home bankings brasileiros e internacionais. Caso o amigo leitor tenha alguma dúvida sobre o site do seu home banking ser verdadeiro ou falso, entre em contato com a instituição bancária em questão e tire suas dúvidas. Provavelmente a instituição tomará medidas para que a página em questão seja retirada da Internet.



Site falso de um grande banco brasileiro. Infelizmente, nenhuma das cinco suítes avaliadas aqui foi incapaz de impedir o carregamento desta página.

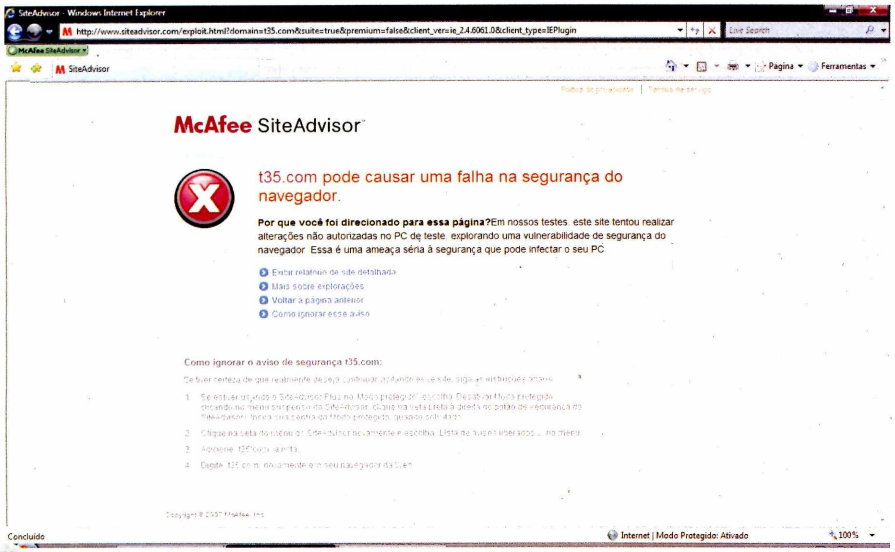


F10. Monitoramento de alterações em arquivos importantes.

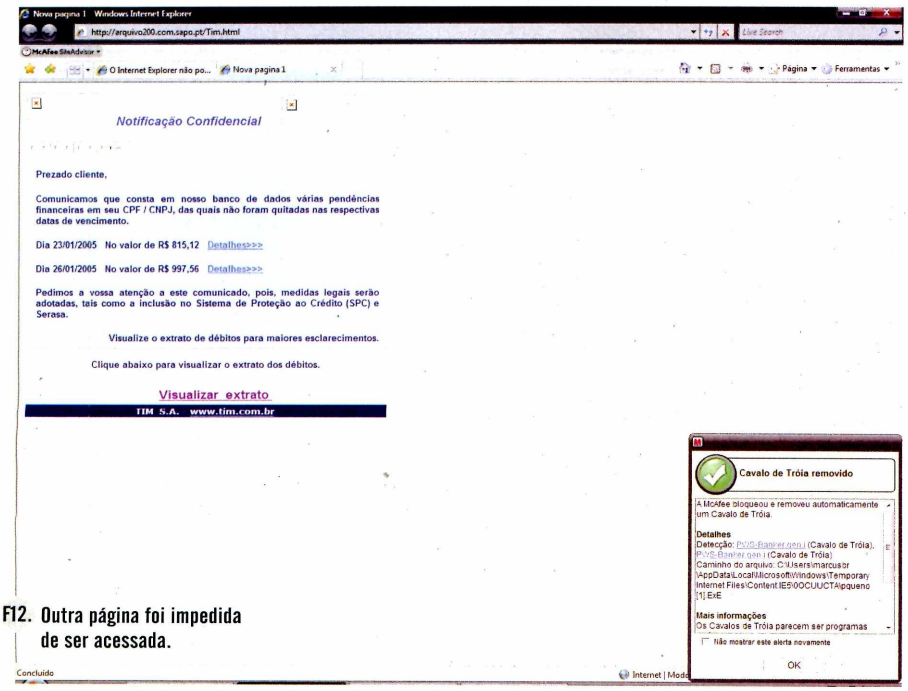
importantes no registro do Windows, assim como uma função de verificação automática de segurança.

Um sistema de alerta em arquivos importantes do sistema operacional e de outros softwares também está presente e atua sempre que qualquer dos arquivos protegidos sofre modificações (figura 10). Trata-se da suíte que mais nos impressionou.

A síntese dos resultados para a suíte da Trend Micro foi a seguinte: 37 sites visitados, nenhuma página bloqueada previamente, 11 downloads bloqueados previamente, 11 arquivos baixados manualmente, oito arquivos baixados foram eliminados.



F11. Página foi impedida de ser acessada.



F12. Outra página foi impedida de ser acessada.

McAfee Internet Security Suite 2007

Tanto a McAfee quanto a Symantec saíram às compras nestes últimos cinco anos e juntaram a si algumas empresas especializadas em segurança on-line. Ambas cresceram razoavelmente bem nesta área. De alguma forma, talvez pelo site oficial da empresa, a McAfee parece estar, pelo menos no momento, um passo à frente da Symantec no que diz respeito à segurança digital on-line. Será mesmo? Sim, está. Não muito à frente, mas em se tratando de suítes para usuários domésticos, está.

Mais uma vez a McAfee conseguiu desenvolver melhor sua suíte de segurança doméstica. Eliminou algumas firulas referentes à versão passada e acrescentou real poder de funcionamento no que mais interessa.

É bem verdade que a suíte da McAfee ficou entre as mais pesadas em termos de carga para o sistema operacional e seu escaneamento também não foi lá muito veloz. Em contrapartida, das cinco suítes testadas foi a única que conseguiu realmente bloquear o acesso a uma página na Internet antes mesmo dela ser aberta (figura 11) e o melhor de tudo é que a página de alerta exibida pela McAfee está em português. Isso pode fazer diferença a favor desta suíte no momento da compra. Trata-se de um excelente ponto conquistado pela McAfee a favor da sua suíte.

Além da suíte impedir o acesso a determinados sites classificados como potencialmente perigosos, ainda demonstrou atuar muito bem quando o site em questão não era classificado dessa forma, removendo a ameaça e relatando através de uma pequena tela com uma boa riqueza de informações (figura 12).

Através do McAfee Site Adivisor é possível classificar alguns sites de forma a "ensinar" ao software como se comportar diante dele. Veja que é a união dos clientes da McAfee que os ajudam a se proteger. Sem dúvida trata-se de uma ótima idéia.

Tanto a suíte da McAfee quanto da Symantec avaliadas aqui não representam as versões topo de linha. Estas são respectivamente **McAfee Total Protection** http://br.mcafee.com/root/package.asp?pkgid=274 e **Norton 360** http://shop.symantecstore.com/store/symanbr/pt_BR/ContentTheme/pbPage.Trialware_pt_BR/ThemeID.15500.

A interface gráfica é muito boa e quase tão "clean" quanto a da suíte da Trend Micro. A configuração é fácil e a quantidade e qualidade de informações gráficas ajuda nesse processo. O processo de atualização é simples e ocorre em segundo plano, aplicando um discreto ícone na área de notificação.

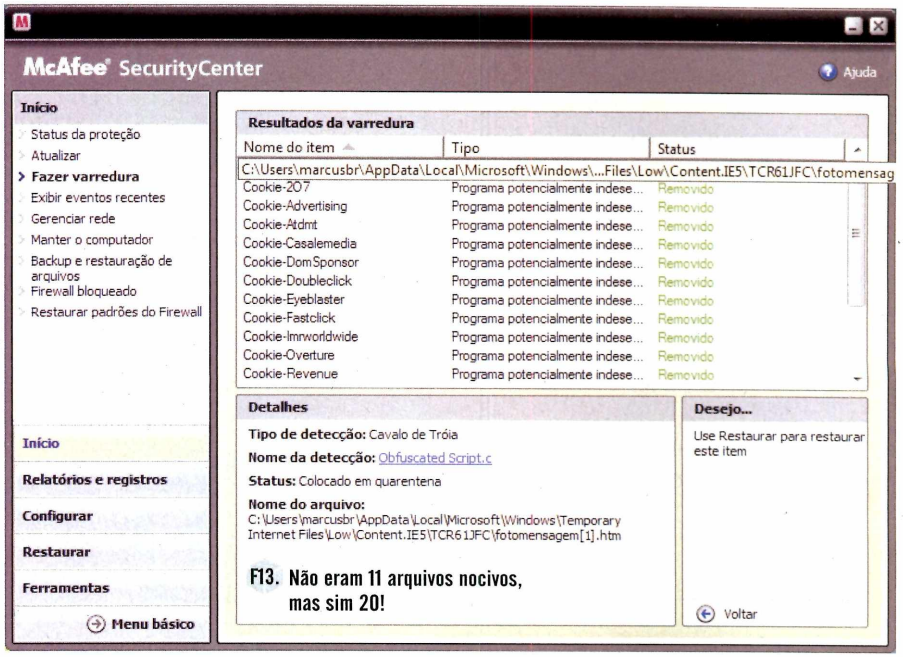
É bem verdade que a varredura demorou um pouco mais do que a das outras suítes, mas em compensação foi a única que detectou todos os itens e mais alguns cookies, elevando para 20 o número de arquivos baixados. Nós baixávamos 11 arquivos manualmente, mas sinceramente só notamos os outros 9 cookies depois de ter testado essa suíte (figura 13).

Os testes estáticos das portas foram ótimos e a instalação da suíte foi diferente das demais. Primeiro tivemos que criar uma conta na McAfee para só depois ter acesso ao download do arquivo de instalação. Este sim baixaria e instalaria os componentes da suíte no computador.

Até agora está tudo ótimo para a suíte da McAfee assumir o primeiro lugar do teste, sem concorrente a altura. Só falta colocar esse disco rígido como slave no nosso sistema de controle e escanear com o AVG Anti-malware 7.5.

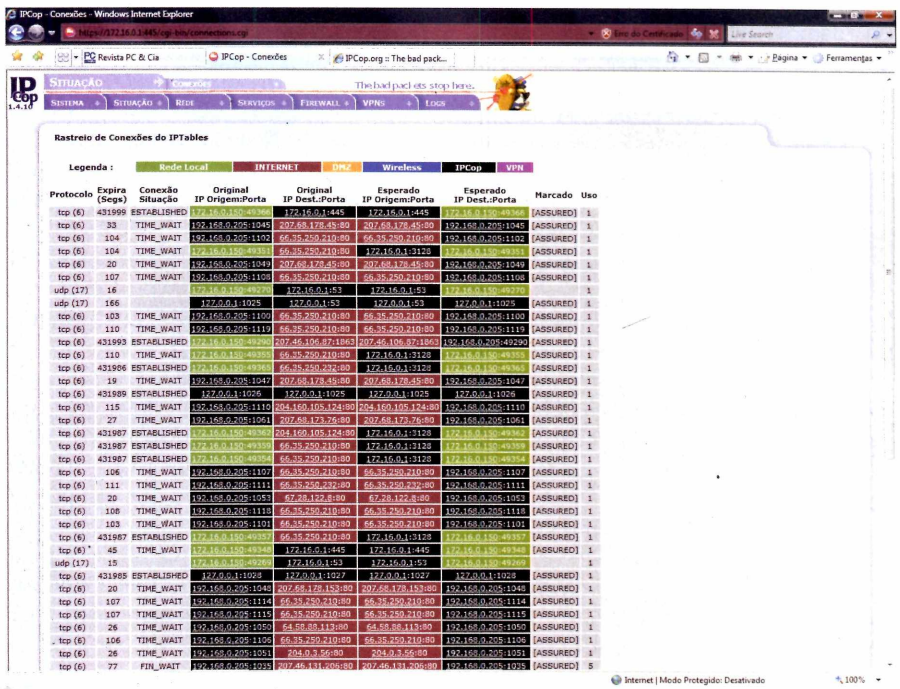
Como nenhum software é realmente perfeito, o AVG encontrou um único arquivo malicioso que a suíte da McAfee havia "esquecido". Que pena. Seria um 10 com louvor...

A síntese dos resultados para a suíte da McAfee foi a seguinte: 37 sites visitados, 7 páginas bloqueadas previamente, 11 downloads bloqueados previamente, 11 arquivos baixados manualmente, 10 arquivos baixados foram eliminados e 20 arquivos nocivos identificados no total.



F13. Não eram 11 arquivos nocivos, mas sim 20!

31



F14. Tráfego de rede na Internet: pode ser de extrema utilidade para "pegar" intruso que conseguiu passar por sua suíte de segurança.

Mais controles

Às vezes, é necessário tomar conhecimento do tráfego de rede interna e externa, principalmente, para dessa forma poder monitorar os processos que estejam de fato acessando a Internet sem o nosso consentimento. Essa característica não costuma ser encontrada em produtos para ambiente doméstico. Mas ela está presente, por exemplo, no IPCop (**www.ipcop.org**), como podemos ver na figura 14.

Outra característica bem-vinda são as *black lists*, utilizadas para impedir o acesso a determinados sites que nelas estejam cadastradas, e as white lists, que declaram os sites nela constantes como confiáveis (figura 15).

O IPCop, portanto, é muito superior aos seus "concorrentes", no que diz respeito às funções de firewall e filtragem. Além disso, possui outras funções mais avançadas, como bloqueio de tráfego P2P, priorização de pacotes, redirecionamento de portas, detecção de intrusão (IDS) e Web Proxy para acelerar a navegação. Isso tudo o torna praticamente indispensável no contexto atual de qualquer computador que se conecta à Internet.

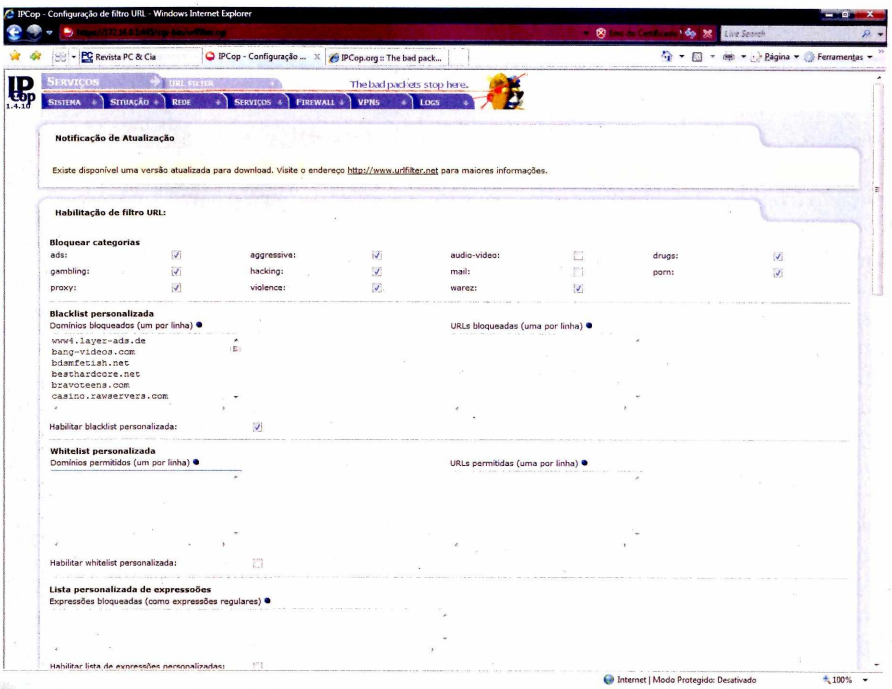
Contudo, é importante entender bem a função dele para evitar surpresa. Primeiro, vale observar que ele requer uma dose extra de configurações manuais. Sem essas, ele deixou passar todos os 11 arquivos. O Avast! Home Free eliminou sete e deixou passar três. Um arquivo era para ambiente DOS de 16 bits e não pôde ser executado, mas passou.

Somente após ser configurado corretamente é que o IPCop deu um banho na "concorrência" e bloqueou todos os sites nocivos. Todos os 37 e não apenas os 11 mais perigosos.

Portanto, se você tiver algum conhecimento de redes, considere a opção de utilizar uma distribuição Linux de segurança como o IPCop e mantenha-a atualizada. Nós utilizamos a máquina virtual do IPCop disponibilizada gratuitamente em nosso site **www.revistapcecia.com.br/downloads/ed62/**, junto com o também gratuito VMware Server 1.0.3 (**www.vmware.com/download/server/**) no Windows Vista Ultimate. Você encontra as instruções para a instalação da máquina virtual no artigo "Internet Segura" publicado em nosso site **www.revistapcecia.com.br/artigos.asp**.

Dica VMWare Server

Antes de instalar o VMWare Server no Windows Vista, instale primeiro o IIS e depois de completada essa instalação, execute o comando "msconfig" e desabilite o UAC. Reinicie o computador após isso.



F15. Os sites listados na black list não podem mais ser acessados. Em geral, suítes de segurança também não dispõem desse recurso.

Conclusão

A conclusão unânime é a seguinte: nenhuma suíte de segurança é perfeita. É a mais pura verdade. A partir disso, a questão passa a ser a escolha da menos imperfeita ou então utilizar diferentes componentes de diferentes fabricantes. Não caia na alegação de que uma dessas suítes vai simplesmente assumir e se responsabilizar pela segurança do seu computador e tudo mais que estiver nele. Isso é uma ilusão que podem estar tentando vender. A tabela 4 apresenta uma comparação entre as principais características das suítes.

Seguindo este raciocínio utilizamos em um Windows XP Professional de 32 bits o Zone Alarm Pro com a porção firewall e anti-spyware e o AVG com a porção anti-vírus e anti-malware. A segurança ficou ótima, mas o desempenho ficou razoavelmente degradado a ponto de gerar uma certa lentidão nas operações de escrita e, às vezes, leitura no disco rígido.

Portanto, em termos de segurança e desempenho é melhor mesmo escolher uma suíte de uma única *softhouse*. Todas as cinco aqui apresentadas são boas. A suíte da Zone Labs fica devendo um pouco mais do que as outras, além disso, não existe uma versão em português e nem suporte técnico por aqui. Só existem no Brasil as empresas parceiras da Check Point, que comprou a Zone Labs.

Qualquer uma das outras quatro será uma boa pedida. Tenha em mente que as deficiências que eventualmente possam ter sido apresentadas neste teste por uma ou outra suíte, simplesmente podem não existir mais agora, no momento em que você, amigo leitor, está lendo esta conclusão. Todo dia tem atualização disponível para essas suítes, que custam entre R$ 75,00 e R$ 115,00 com licenças para um a três computadores durante um ou dois anos, ou mais, conforme opções.

Se seu problema for custo, utilize o anti-vírus Avast! Home Free, que se saiu muito bem e mantenha o firewall e anti-spyware do Windows Vista Ultimate, os quais responderam muito melhor do que os similares do Windows XP Professional. E para os usuários que buscam maior flexibilidade e oferta de opções relacionadas à segurança, recomendamos o uso da máquina virtual gratuita com o IPCop.

Esperamos que tenha gostado de mais esse teste comparativo. Não deixe de mandar suas sugestões e comentários.

Até a próxima!

PC

Características	Zone Labs	AVG	Norton	PC Cillin	McAfee
Anti-vírus	Sim	Sim	Sim	Sim	Sim
Anti-spyware	Sim	Sim	Sim	Sim	Sim
Anti-spam	Sim	Sim	Sim	Sim	Sim
Detecção automática de rede	Sim	Sim	Sim	Sim	Sim
Plugin para navegador	Não	Não	Sim	Sim – Opcional	Sim
Firewall	Sim	Sim	Sim	Sim	Sim
Filtro manual de sites	Sim	Não	Sim	Sim	Sim
Bloqueio automático de sites	Não	Não	Não	Não	Sim
Proteção de informações pessoais	Sim	Sim	Sim	Sim	Sim
Black List	Não	Não	Não	Não	Não
Monitor de conexões ativas	Não	Não	Não	Não	Não
Priorização de tráfego	Não	Não	Não	Não	Não

T4. Comparativo de características.

Segurança em ambiente de servidores

Roberto Luiz R. Cunha



Formado em Engenharia Elétrica, possui 24 anos de experiência no desenvolvimento de projetos em hardware e atualmente compõe a equipe de redatores da revista.

Com o aumento do uso de sistemas wireless, uma grande quantidade de fontes de RF tem sido acrescida ao ambiente computacional. Isso pode vir a representar um problema quando pensamos em processamento de alto desempenho. Por outro lado, as emissões espúrias de RF de cabos, conectores, equipamentos de rede, computadores e seus periféricos podem por em risco a segurança de empresas que trabalham com informações sigilosas. Vamos discutir como esses problemas ocorrem e o que pode ser feito a respeito.

Considerando que a simples presença de uma carga elétrica, estática ou em movimento, irá criar um campo elétrico ou magnético, podemos afirmar com toda a certeza que qualquer equipamento eletrônico em funcionamento provocará o surgimento de sinais eletromagnéticos que se propagarão para fora desse equipamento.

Existe uma área da engenharia chamada de Compatibilidade Eletromagnética, ou EMC (do inglês ElectroMagnetic Compatibility), que se dedica a estudar esse fenômeno e definir limites de emissão e meios de controle. Basta olhar a etiqueta de qualquer equipamento de informática para notar diversos logotipos de agências de certificação, como a FCC (americana), VCCI (japonesa) ou CISPR (internacional).

Essas agências trabalham no sentido de criar limites que permitam que equipamentos de diferentes fabricantes ou países operem satisfatoriamente entre si. Isso significa que um equipamento só poderá ser comercializado nesses países se for aprovado pela agência local (o Brasil se encontra em um caso à parte, onde isso nem sempre é verdade).

Essas certificações representam um custo elevado e os fabricantes procuram obter o maior número possível de aprovações de forma que seus equipamentos possam ser comercializados na maior parte do mundo sem nenhuma restrição.

Apesar dessas certificações serem bem intencionadas e funcionarem na maior parte do tempo, existem casos em que elas não são suficientes. Os limites de emissão são definidos para classes de equipamentos e nada impede que um equipamento em particular seja mais sensível que outros e se torne vítima de interferências. Além disso, existem mecanismos que permitem "enganar" legalmente as normas (se você acha que essa é uma atitude exclusivamente brasileira, sinto informar que está enganado!).

Um exemplo desses "ajustes" à norma consiste na opção de spread spectrum para o clock das placas-mãe. Essa opção faz com que a energia de RF do sinal de clock não fique restrita em uma porção pequena do espectro de RF e a distribui em uma faixa de freqüências maior, fazendo com que, na média, ela apresente menor amplitude e permita que a placa seja aprovada nas medições de emissão de RF. O "truque" vem do fato que essa opção não é habilitada de fábrica na instalação da placa em um computador e, portanto, os níveis de emissão obtidos durante a certificação não condizem com os obtidos no uso normal.

Outro aspecto que faz com que equipamentos certificados acabem provocando interferências elevadas em outros equipamentos é o fato de que as interferências apresentam efeito cumulativo.

Emissões de RF são naturalmente complexas, e seu comportamento dentro de um ambiente é muito difícil de se prever. Esses sinais se somam ou se subtraem dependendo das condições locais e podem facilmente atingir níveis elevados. Quanto mais equipamentos presentes, pior ficará as condições eletromagnéticas do ambiente.

Outro fato que reforça a existência de interferências é a presença dominante de computadores montados a partir de placas individuais, ao invés de computadores completos fornecidos por fabricantes idôneos. Quando um computador é integrado por um fabricante, ele deve passar por testes que comprovem que o sistema atende às normas de compatibilidade eletromagnética especificadas. No entanto, isso não ocorre quando o computador é montado a partir de placas individuais obtidas junto ao mercado eletrônico, placas essas muitas vezes sem nenhuma indicação de fabricante e muito menos de aprovação frente às normas internacionais.

Mas não são só as interferências entre equipamentos que podem causar problemas. Existe uma outra preocupação, bastante séria, que diz respeito à segurança das informações presentes nesses computadores.

Segurança e o termo TEMPEST

O termo TEMPEST é uma palavra código utilizada para definir padrões e procedimentos para a redução de emissões não intencionais em equipamentos de TI que processam informações sigilosas.

Esses padrões e procedimentos são classificados como secretos pelo governo norte-americano e pouca informação real pode ser obtida, mas diversas tecnologias utilizadas em compatibilidade eletromagnéticas, amplamente divulgadas, podem ser empregadas para esse fim.

Tudo se baseia no fato que circuitos eletrônicos, e seu cabeamento, emitem energia em RF especialmente quando os sinais transmitidos são digitais. Essa energia pode ser captada por equipamentos especializados a uma distância bastante grande. Note que não estamos nos referindo às emissões de RF de sistemas wireless, que transmitem seus sinais intencionalmente, mas sim aos sinais emitidos pelo cabo que liga o computador ao monitor ou cabos conectados às portas RS232, por exemplo.

Diversos fabricantes de blindagens de RF e componentes relacionados apresentam produtos compatíveis com as especificações TEMPEST, além de outros padrões de compatibilidade eletromagnética.

Dentre as poucas informações disponíveis, um documento antigo liberado pela National Security Agency, ou NSA, de outubro de 1994, fornece os valores de atenuação esperados, na época, em função da freqüência, conforme o gráfico apresentado na figura 1.

Existem computadores montados de forma a incorporar todas as blindagens e filtragens necessárias para reduzir drasticamente as emissões de RF, entretanto são mais difíceis de se achar e seu custo é elevado (aproximadamente o dobro de um computador de mesma capacidade, mas sem essas proteções). Tudo isso fora do Brasil, é claro!

Interferências e equipamentos de informática

Um fato que é do conhecimento de todos envolvidos na definição de layouts em fábricas ou escritórios é que o custo interno por metro quadrado de área é muito elevado. Isso faz com que qualquer área (seja uma garagem, antigo refeitório ou até mesmo um banheiro) seja considerada para reaproveitamento.

Quando isso acontece, pode ocorrer a instalação de computadores ou servidores em áreas próximas a equipamentos que gerem interferência em níveis que podem ser excessivos para esses computadores. Interferências causadas por linhas de alimentação em 60Hz, ou transformadores de energia em monitores CRT, são os exemplos mais comuns desse tipo de problema.

Equipamentos que comutem correntes elevadas ou operem com freqüências mais altas, poderão causar um tipo de interferência que irá afetar, além dos monitores, os computadores diretamente e, obviamente, as informações neles processadas. A instalação de servidores e computadores próximos a equipamentos industriais ou prediais de alta potência necessita levar em conta esses fatores.

Executando-se um levantamento dos níveis de campos eletromagnéticos (site survey) em toda a faixa de freqüências de interesse, pode-se determinar a necessidade, e a que grau, de medidas devem ser implementadas para a redução de interferências.

Eficiência da blindagem em dB	Relação de atenuação	Atenuação em %
20	10:1	90,0000
40	100:1	99,0000
60	1000:1	99,9000
80	10.000:1	99,9900
100	100.000:1	99,9990
120	1.000.000:1	99,9999

T1. Os valores da tabela foram obtidos aplicando-se a relação: atenuação (dB) = 20logV1/V2 (onde V1 e V2 serão os valores dos campos elétricos interno e externo).

Outra situação bastante comum, mas problemática com relação a interferências de RF, consiste na instalação de servidores em andares altos de edifícios, já que antenas de diversos tipos, freqüências e potências costumam ser instaladas em sua cobertura, seja no próprio edifício ou em edifícios próximos.

Devido à posição elevada, esses andares acabam ficando em linha direta com as antenas, o que provoca altos níveis de campos eletromagnéticos. Um exemplo bastante conhecido desse problema consiste nos escritórios localizados nos andares mais altos dos edifícios localizados na Avenida Paulista, em São Paulo, região que concentra uma enorme quantidade de sistemas de transmissão de TV, FM, celulares, radiocomunicação etc.

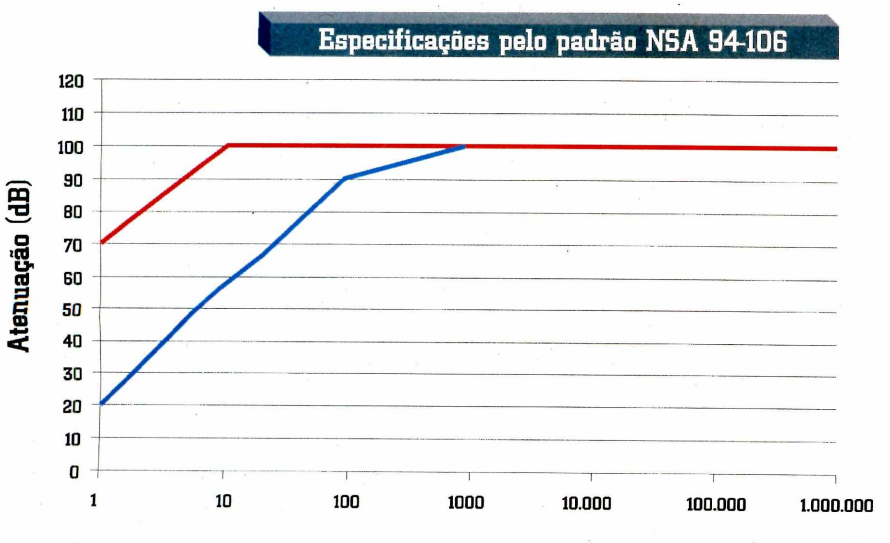
Blindagem de RF e a arquitetura

Historicamente, a necessidade de blindar construções ou salas contra a entrada ou saída de energia eletromagnética nasceu com o aumento da complexidade e sensibilidade dos equipamentos eletrônicos militares.

Essas blindagens, em geral, requeriam atenuações de 100dB, ou maiores, o que significava reduções de 100.000:1, ou mais. A equivalência entre a eficiência da blindagem, a relação de atenuação e a atenuação em porcentagem pode ser vista na tabela 1.

Ao longo dos anos, o aumento de aplicações sensíveis nas áreas comercial, industrial e médica, tornou necessária a utilização de meios de se conter os campos eletromagnéticos para esses setores também. Nesse caso, o que muda em relação às soluções utilizadas em aplicações militares é o grau de atenuação dessas blindagens.

Se uma blindagem militar apresenta atenuações entre 100 e 120dB, uma comercial normalmente não necessitará de atenuações



F1. Gráfico informando a atenuação necessária em função da freqüência, onde a linha vermelha representa os valores para campos elétricos e ondas planas, e a azul para campos magnéticos.

Característica	Estrutura metálica sólida	Painéis modulares	Laminados	Tela metálica	Tinta de cobre e tecido metalizado
Material	Chapas de aço sobre estrutura metálica ou concreto.	Folhas de cobre ou alumínio sobre estrutura de madeira.	Laminado de cobre ou alumínio sobre painéis de compensado ou aglomerado	Tela metálica de cobre, latão ou alumínio sobre estrutura de madeira.	Tinta a base de cobre/prata sobre as paredes com espessura mínima de 0,5 mm. Tecido metalizado especializado aplicado sobre as paredes.
Tipo de Construção	Partes soldadas.	Partes parafusadas.	Prensada, colocada, soldada, grampeada ou fixa por fita adesiva metálica. Quando colada deve ser utilizado adesivo condutivo.	Geralmente parafusada.	Fita adesiva metálica ou fita adesiva comum com pintura condutiva sobre ela. No caso de tecido condutivo pode ser grampeada ou colada com superposição.
Atenuação típica	120 dB para campos elétricos e 20 a 60 dB para campos magnéticos.	100 dB para campos elétricos e 20 a 40 dB para campos magnéticos	60 dB para campos elétricos. Nenhuma atenuação para campos magnéticos;	60 dB para campos elétricos. Nenhuma atenuação para campos magnéticos.	60 dB para campos elétricos. Nenhuma atenuação para campos magnéticos. Alguns tecidos podem apresentar desempenho melhor, atingindo 75 dB.
Vantagens	Atenuação muito alta, grande durabilidade, pouca degradação e pouca manutenção.	Alta atenuação, durável e pode ser desmontada.	Blindagem bastante leve.	Blindagem bastante leve	Leve, de fácil aplicação, durável e de fácil manutenção. A blindagem pode ser facilmente coberta com materiais tradicionais de acabamento.
Desvantagens	Custo bastante elevado, peso elevado e tempo de instalação.	Sensível à umidade (oxidação) com efeitos sobre o desempenho e manutenção difícil.	Frágil, desempenho incerto ao longo da vida útil, difícil manutenção, difícil integração com a sala e extremamente sensível à umidade.	Frágil, sensível à umidade devendo ser protegida e de manutenção difícil.	Pode ser facilmente arranhada ou rasgada resultando em perda de desempenho.
Custo da instalação	O mais alto.	Alto	Moderado	Moderado	O mais baixo.
Custo da manutenção	Baixo.	Moderado a alto	Moderado	Baixo a Moderado	Baixo
Reparos	Difíceis. Implicam em processos de solda.	Difíceis. Normalmente necessitam desmontagem, reparo, remontagem.	Fáceis se a blindagem for acessível e difíceis se as paredes necessitarem ser desmontadas.	Fáceis se a blindagem for acessível e difíceis se as paredes necessitarem ser desmontadas.	Fáceis já que qualquer dano na alvenaria pode ser reparado e a blindagem restabelecida com um nova camada de tinta. No caso de tecidos um remendo pode ser providenciado.

Comparação entre diversas tecnologias de blindagem contra campos eletromagnéticos. T2.

35

acima de 60dB. Claro que cada caso é particular, e a decisão do nível de atenuação necessário deve ser tomada junto com as considerações técnicas e econômicas.

Como exemplo podemos citar que todos os equipamentos de ressonância magnética, instalados em hospitais e clínicas, utilizam blindagens de RF com atenuações variando entre 60 e 100dB, de acordo com cada fabricante, e algumas apresentam, ainda, uma blindagem magnética adicional.

O aspecto de maior impacto na decisão de se utilizar algum tipo de blindagem eletromagnética em aplicações comerciais é o seu custo. Sendo uma tecnologia bastante especializada, onde poucas empresas atuam, seus custos acabam sendo elevados e um detalhado estudo de custo x benefício deve ser preparado. Devido à necessidade de se otimizar o desempenho esperado com o orçamento disponível, diversas opções de blindagem podem ser encontradas, cada qual com suas vantagens e desvantagens. Vamos fazer uma comparação, vista na tabela 2, entre algumas tecnologias, com seus pontos fortes e fracos.

Além da blindagem em si, outros problemas devem ser estudados. Uma blindagem ideal seria como uma casca de ovo, isto é, sem emendas, aberturas ou descontinuidades, mas isso é impraticável e impossível de se conseguir.

No mínimo uma porta será necessária para a utilização da sala. Ventilação e ar condicionado, entrada dos cabos de energia, cabos de rede e telefonia e iluminação também fazem parte da instalação e são fatores limitantes ao desempenho da blindagem. Todos esses aspectos e alguns outros dependentes das condições locais devem ser verificados e tratados com as soluções adequadas.

As linhas de energia e telefonia, além dos demais sinais necessários, devem ser admitidas na área blindada através de filtros de linha especiais que garantam a atenuação da sala e ao mesmo tempo permitam a utilização

desses serviços. Um exemplo de painel de ligações pode ser visto na figura 2.

Ventilação e ar condicionado devem ser direcionados à sala através de filtros que permitam a passagem do ar ao mesmo tempo que bloqueiam a passagem de energia eletromagnética. O tipo mais eficiente de estrutura que executa essa função é conhecida como *honeycomb*, que consiste de pequenos tubos com secção hexagonal, unidos entre si, que permitem a passagem do ar, mas funcionam como filtros de guia de onda para os sinais de RF.

Cabos de rede convencionais (em cobre) são problemáticos, mas cabos de fibra óptica podem ser utilizados sem problema através de guias de onda (um tubo metálico com comprimento adequado para barrar os sinais de RF indesejados). A dimensão do guia de onda deve respeitar a relação: comprimento/diâmetro interno >= 4.

Os itens mais críticos na manutenção do nível de eficiência de uma blindagem de área são janelas e portas, especialmente estas últimas. Para as janelas devemos utilizar telas metálicas de forma que apresentem a atenuação necessária, mas permitam que alguma quantidade de luz consiga atravessá-la. Arranjos com telas duplas de cobre, de malha fina, permitem obter atenuações de até 100dB.

Outros tipos de materiais podem ser utilizados para esse fim, como a membrana plástica apresentada na figura 3, que recebe uma fina deposição metálica em uma de suas superfícies.

Portas sempre serão especialmente problemáticas devido ao fato de serem móveis e, por isso, com um desgaste acelerado em relação aos outros componentes de uma blindagem. Uma porta para blindagem de RF, como o detalhe apresentado na figura 4, deve respeitar alguns requisitos básicos:

- Apresentar nível de atenuação igual ou melhor do que o restante da blindagem;
- Possuir uma estrutura rígida o suficiente para evitar empenamentos;
- As dobradiças devem ser resistentes a desgaste para que a porta não perca sua referência em relação ao batente;
- Os contatos metálicos (conhecidos como fingers) entre a folha da porta e o batente devem ser montados de forma a facilitar sua manutenção;
- Devido ao efeito de mola distribuída causado pelos fingers, deve possuir um sistema de fechamento que não exija muito esforço do operador.

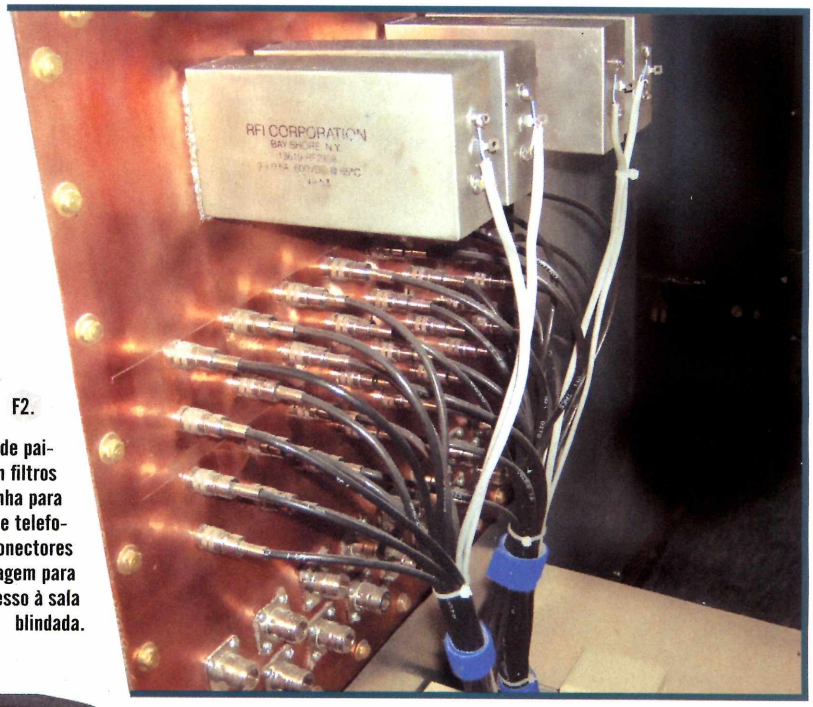
E na prática?

Na prática, muitas empresas de diversos segmentos no Brasil têm se preocupado com o problema de interferências, entretanto poucas com o problema de segurança. Por que isso ocorre?

Problemas de interferência, em menor ou maior grau, sempre estão presentes e afetam de forma direta a operação no dia-a-dia. Seus efeitos nem sempre são prontamente notados ou mesmo relacionados com interferências, porém quando o são, podem ser localizados e medidas podem ser tomadas para eliminá-los ou, mais comumente, minimizá-los. Esses problemas geralmente representam um custo mais fácil de se definir.

Questões de segurança dependem de análises muito mais complexas. A decisão de se implementar soluções de blindagem para reduzir emissões eletromagnéticas que poderão comprometer a segurança das informações processadas, depende de vários fatores. Entre eles, podemos citar:

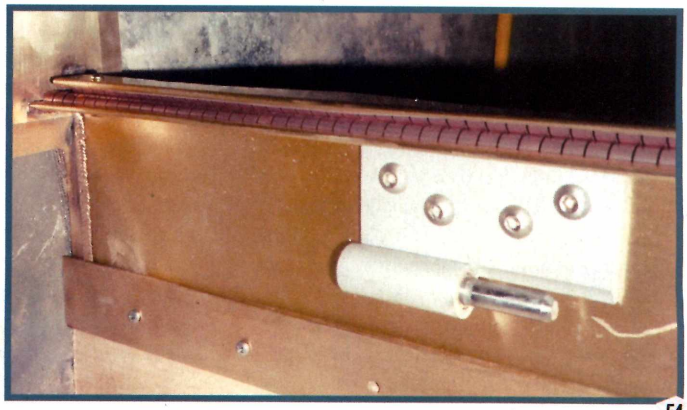
- Valor das informações para outros: ninguém irá assumir o trabalho e os custos



F2. Exemplo de painel com filtros de linha para energia e telefonia e conectores de passagem para acesso à sala blindada.



F3. Material plástico que exibe uma fina camada de metal (ouro) depositado em sua superfície, proporcionando boa transparência aliada à condutibilidade do metal.



F4. Detalhe de uma dobradiça pesada para porta de blindagem de RF. Note o arranjo de contatos elétricos (fingers) em cobre que irão garantir a continuidade elétrica entre a folha da porta e o batente.

de tentar roubar informações que só tenham valor para a própria empresa que as processa. Para valer a pena, a informação obtida deve possuir alto valor de mercado;

• Contenção de emissões eletromagnéticas é o último item entre todas as medidas de segurança. É uma medida extrema que só deve ser tomada após todas as outras, já que é muito mais fácil, rápido e barato obter informações confidenciais de um funcionário descontente. Além disso, vale ressaltar que uma blindagem custará milhares de dólares, por exemplo.

Não é fácil e nem barato obter informações por meio da captura de emissões eletromagnéticas espúrias de equipamentos e cabos de dados. Antenas, pré-amplificadores, receptores sintonizados, analisadores de espectro, analisadores de protocolos, além de ótimos conhecimentos em RF e protocolos de comunicação, representam um elevado investimento e descarta a possibilidade de execução pela grande maioria dos técnicos e engenheiros existentes.

Já o controle de interferências vem sendo feito por diversas empresas com bons resultados. Blindagens de RF são implementações complexas, porque devem atender a dois aspectos básicos geralmente conflitantes.

Em primeiro lugar, devem proporcionar uma região (pode ser um gabinete de computador, um rack, uma sala ou um andar de um prédio) isolada eletromagneticamente, e em segundo lugar essa região precisa permitir o acesso para as pessoas e para as conexões necessárias (energia, ventilação, conexões de dados etc).

Na adaptação desses dois aspectos, estão as definições de eficiência e custo da blindagem. Uma blindagem para proteger monitores contra interferência de campos magnéticos (assunto já discutido na edição 21) pode ser obtida com materiais de baixo custo (chapas de ferro carbono) e de montagem relativamente simples (devido à natureza dos campos magnéticos, uma blindagem parcial ou aberta pode ser utilizada) e sem necessidades especiais como um bom terra, por exemplo.

Já uma blindagem para campos elétricos (muitas vezes chamados simplesmente de RF) necessita que esta envolva totalmente a área a se proteger. Isso implica na criação de superfícies metálicas nas paredes, teto e piso, além das portas e janelas.

Quanto maior a atenuação desejada, mais complexa será sua montagem. Como exemplo podemos considerar os filtros de linha para permitir a entrada de energia na região protegida pela blindagem.

Quando falamos em filtros de linha não nos referimos aos filtros de linha encontrados nas lojas de informática, mas aos filtros de alta taxa de atenuação, produzidos por empresas especializadas no exterior. Esses filtros não são itens de prateleira, e muitas vezes são produzidos por encomenda. Seu custo é alto e os prazos de entrega são longos. Isso ocorre com quase todos os itens que compõem uma blindagem de alto desempenho.

Se falarmos de blindagens com desempenho mais modestos (menores ou iguais a 60 dB), a situação começa a melhorar e outras soluções mais criativas podem ser utilizadas. O simples revestimento das paredes, portas e janelas com chapas metálicas irá proporcionar algum grau de atenuação para os sinais de RF. O quanto é impossível de se prever, mas dependendo do caso pode ser o suficiente para a resolução do problema. O uso de chapas de aço galvanizado, laminado de alumínio, cobre ou aço silício, será definido pelo efeito desejado e pelo custo esperado (figura 5).

O importante é sempre lembrar que uma blindagem que não utiliza filtros apresentará uma eficiência muito inferior à que seria obtida com a inclusão desses itens. Para eficiências menores que 60 dB, empresas locais poderiam projetar e executar esses filtros com um custo bastante razoável.

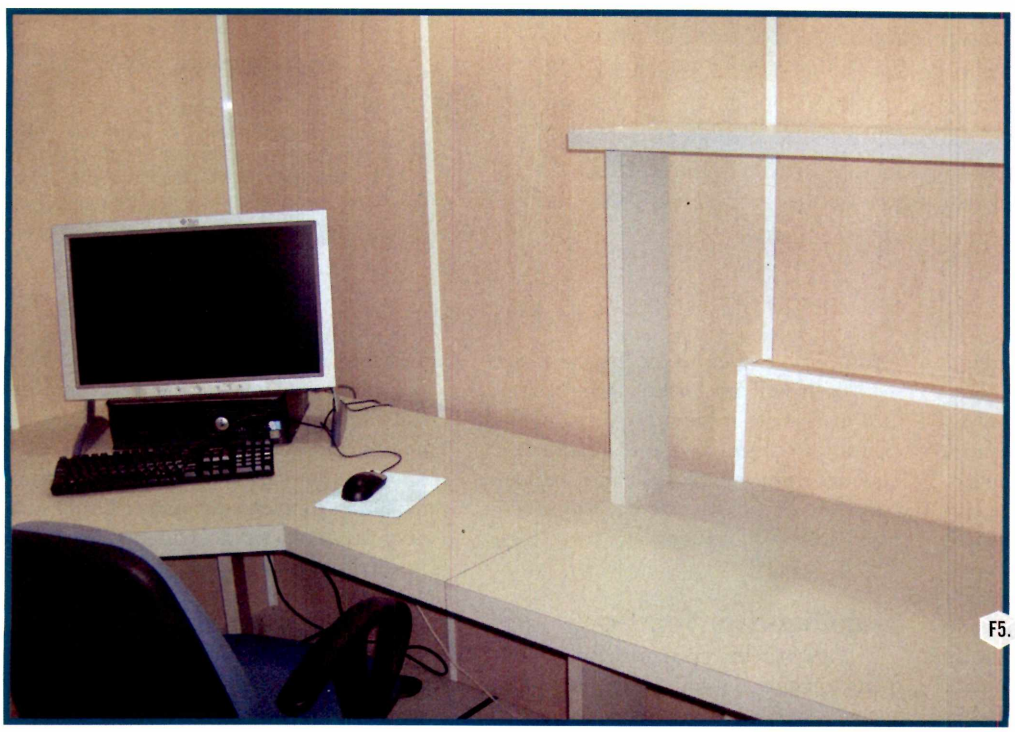
O importante, antes de iniciar qualquer investimento nessa área, é consultar alguma empresa ou profissional especializado que irá sugerir qual o caminho a ser tomado e qual a atenuação que se deve esperar.

Conclusão

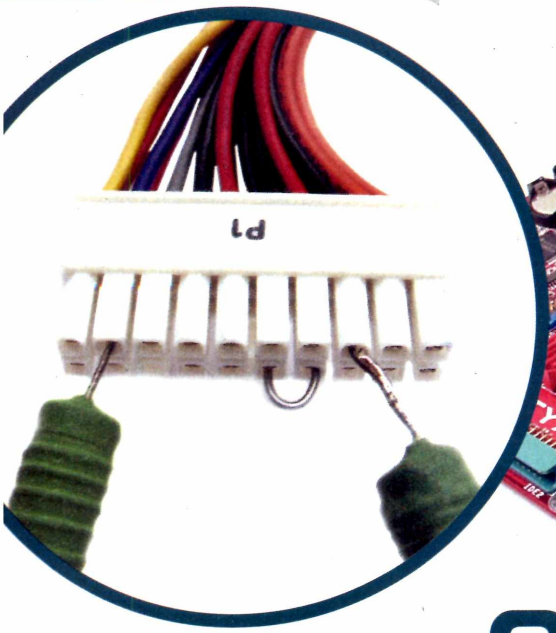
Controle de interferências e emissões é uma atividade complexa devido à natureza dos sinais a serem bloqueados e da necessidade de adaptação com o ambiente onde os equipamentos estão instalados.

Existem diversas opções de implementação para a blindagem, cada uma com suas vantagens e deficiências. O que é comum para todas elas é a baixa, ou nenhuma, mobilidade da solução escolhida. Alguns tipos de blindagem permitem que ela seja desmontada e montada em uma nova locação, porém isso representa custos a mais.

Por isso, um maior cuidado deve ser tomado pelas empresas na escolha do local onde seus servidores serão instalados. Muitas vezes movendo-se a instalação uns poucos metros se evitaria a necessidade de investir em blindagens. **PC**



F5. **Por trás do acabamento simples existe uma blindagem completa com nível de atenuação maior que 100dB.**





Queima de Placas-mãe

Dias atrás nos deparamos com mais uma placa-mãe que sem causa aparente deixou de funcionar. A fonte foi testada isoladamente e respondeu bem aos testes realizados. O sinal de +5V Stand-by estava presente no ATX24 já conectado na placa, o contato do botão Power-On do gabinete foi verificado, mas ao pressioná-lo o pino 14 do ATX24 não caía para 0V e, conseqüentemente, a placa não ligava. Conforme abordado na PC&CIA 54, nesse caso nem mesmo a mais sofisticada placa de diagnóstico do mercado pode nos ajudar. Nesta matéria apresentaremos o responsável por essas queimas tão freqüentes e uma solução eficiente para prevenir este problema.



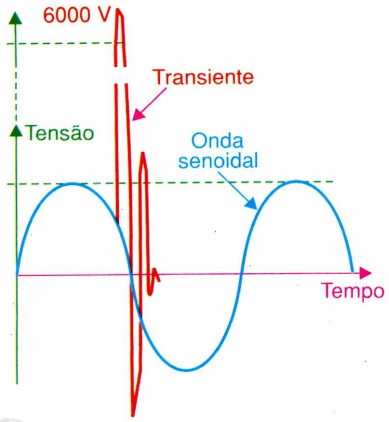
Luiz Felipe de Camargo
Eng. Eletrônico com cursos de Mestrado/Doutorado em Arquitetura de Sistemas Digitais e experiência de mais de 25 anos em telecomunicações, com ênfase em Sistemas Ópticos.

Há algum tempo verifica-se um aumento no número de computadores e também de outros equipamentos que, de repente, param de funcionar por completo. O procedimento para encontrar o defeito sempre toma muito tempo e, no caso dos computadores, quase sempre o problema é a queima da placa-mãe. A questão é que sua troca implica em custo elevado e grande dispêndio de tempo para refazer todas as configurações de software, principalmente se não encontrarmos o modelo idêntico para substituição e tivermos de instalar o sistema e os drivers novamente. Após fazermos "autópsias" em inúmeros equipamentos, chegamos à conclusão que o causador dessas queimas é um transiente de tensão, que se aproveita de diversos aspectos que serão explorados nesta matéria.

Transiente de Tensão

Para aqueles que têm algum conhecimento técnico, o termo transiente significa apenas um pico ou um surto de sobretensão que ocorre nas redes de energia elétrica. Este pico comprovadamente possui a capacidade de danificar, ou mesmo destruir, os equipamentos eletrônicos.

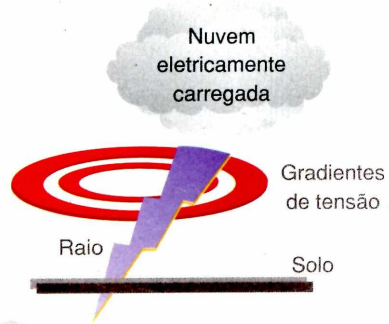
O transiente é um fenômeno extremamente complexo que não se limita só a um pulso de alta tensão, com duração curta (normalmente de poucos microsegundos, mas pode atingir vários milisegundos). Na realidade, ele pode não apenas ser único, como também ser múltiplo, de acordo com as condições das redes de energia elétrica (figura 1).



F1. **Dentre as infinitas formas de onda que um transiente pode apresentar, vemos aqui uma delas na cor vermelha.**

Dentro de uma edificação residencial ou comercial, o transiente pode atingir tensões elétricas de 6.000 Volts ou mais, e em apenas um pulso conter uma quantidade de energia extremamente elevada. Até mesmo de milhares de Joules. Este transiente se sobrepõe à tensão da rede de energia elétrica de baixa tensão (120 ou 220 VCA).

Na grande maioria das vezes, os transientes mais causadores de danos surgem de descargas atmosféricas. Quando um raio cai são formadas ondas de energia eletromagnética de altíssima intensidade, chamadas de Gradientes de Tensão (figura 2).



F2. **Gradientes de tensão durante ocorrência de um raio.**

Estes gradientes se propagam em alta velocidade pelo ar e, ao encontrarem qualquer condutor elétrico, como redes de energia elétrica, fios, torres metálicas etc, transferem grande parte desta elevada energia a estes condutores, ou mesmo a outros elementos que possuam baixa resistividade e estejam relativamente próximos. Quanto mais perto do ponto de impacto, maior será o valor do gradiente de tensão.

Vale lembrar, no entanto, que mesmo quando um raio ocorrer a uma distância razoável de um condutor elétrico, ainda assim ele pode provocar transientes na rede elétrica que alimenta um determinado domicílio.

Em relação aos raios, observações feitas durante muitos anos por vários satélites meteorológicos confirmam que:

- Mais de 90% dos raios ocorrem sobre os continentes e menos de 10% sobre os oceanos;
- No Hemisfério Norte, as principais áreas de ocorrência são: primeiro, a região central da África, depois o sul da Ásia e uma parte do sul dos Estados Unidos. Já no Hemisfério Sul, o Brasil está em primeiro lugar (exceto região nordeste, onde a incidência é baixa), seguido do norte da Argentina, África do Sul, Indonésia e o norte da Austrália. Aliás, até pouco tempo atrás, tinha-se o Brasil como um dos países de maior incidência de raios. Mas esta situação mudou quando o laboratório de eletricidade atmosférica do INPE (Instituto Nacional de Pesquisas Espaciais), instituição de renome mundial, provou que 60 milhões de raios atingem o solo brasileiro por ano. São dois raios por segundo, o que também equivale a uma média de sete raios por quilômetro quadrado! Estes dados foram coletados em um período de aproximadamente um ano e meio, entre 2005 e 2006.
- Na Região Sudeste, caem mais raios no estado de São Paulo. São Caetano é a cidade recordista, seguida de Suzano, Mauá, Santo André. A cidade de São Paulo ocupa o 21º lugar no Brasil.

O IEEE (The Institute of Electrical and Electronic Engineers) e o UL (Underwriters Laboratories) determinaram que:

- Nas redes elétricas internas de imóveis residenciais ou comerciais, raios podem produzir transientes de até 6.000 Volts, com correntes elétricas de 3.000 Ampères.

Além disso, várias outras fontes e instituições informam ainda que:

- Os raios têm correntes elétricas superiores a 200.000 Ampères, apresentam tensões superiores a 100.000 Volts e possuem duração inferior a dois segundos;
- Estudos recentes mostram que a ocorrência de raios tem aumentado significativamente sobre grandes áreas urbanas em relação a outras áreas, em todo o mundo;
- Este efeito pode estar relacionado ao maior grau de poluição sobre estas áreas e ao fenômeno conhecido como "ilha de calor", aquecimento provocado pela presença de muitos prédios ou construções, e pela ausência de áreas verdes;
- Verificou-se ainda que a quantidade de raios em todo o mundo tem aumentado significativamente, sendo as causas prováveis o aquecimento global, o efeito estufa e a poluição atmosférica.

Outras Redes

Transientes também podem existir em outras redes que não sejam as de energia elétrica, como é o caso das redes telefônicas e TV à cabo. Todas essas redes do tipo aéreo possuem uma coisa em comum, que é o uso de postes de energia elétrica como suportes.

Podemos comparar todos estes condutores paralelos como se fossem antenas próximas, que se estendem por muitos quilômetros. Portanto, quando houver uma perturbação elétrica que gere um transiente nas linhas de energia de alta tensão (que são colocadas na parte superior do poste), por exemplo, esta perturbação será induzida nos condutores que se encontram imediatamente abaixo, separadas por poucos centímetros.

Por último, vale destacar a possibilidade de as redes subterrâneas também serem afetadas pela geração de transientes por efeito induzido. Isso dependerá das condições, porém tal fato é raro.

Outras causas

Além dos raios, os transientes podem ser causados pelo chaveamento (isto é, pela energização ou desligamento) de grandes cargas indutivas ou capacitivas. Alguns destes, aliás, são de grande energia.

Curtos-circuitos nas redes de energia de baixa e alta tensão também são geradores de transientes. Eles podem ocorrer de várias maneiras, desde queda de árvores sobre os fios da rede aérea de energia, até queda de postes ou torres de alta tensão.

Com a privatização do setor de energia elétrica no Brasil, muitas empresas terceirizaram os serviços de manutenção da rede de energia elétrica com o principal objetivo de reduzir custos. Nem precisa muito esforço para deduzir que essa medida resultou (e ainda resulta!) em manobras e intervenções tecnicamente incorretas em circuitos energizados, com a conseqüente geração de transientes de tensão. O fato é que nem sempre as empresas terceirizadas executam com perfeição os serviços de manutenção preventiva e corretiva a elas delegadas.

Existe ainda a possibilidade da geração local de transientes causados por eletricidade estática, principalmente quando a umidade relativa do ar, no local, estiver baixa.

Embora remotas, também podemos citar como fontes de transientes de altíssima energia as quedas de meteoros e o chamado EMP (Electromagnetic Pulse), pulsos eletromagnéticos que são gerados durante a explosão de bombas nucleares na atmosfera. Este efeito deu origem a artefatos bélicos que causam a destruição de todos os equipamentos eletrônicos de um inimigo. Isto é feito através de armas que geram ondas de choque contendo pulsos eletromagnéticos de alta potência.

Fontes AT/ATX

Depois dessa explicação sobre transientes, vamos ao nosso tema, a queima das placas-mãe. Dentre os benefícios obtidos da migração do padrão AT para o ATX, um deles foi a retirada da tensão alternada 110 ou 220VAC de dentro do computador, que até então ia até a chave Power-on do gabinete e expunha o usuário a choque.

Com o ATX, quem comanda a inicialização da placa-mãe é a tensão de +5V Stand-by que sempre está presente, mesmo quando a máquina está aparentemente desligada. Basta que o cabo de energia esteja conectado na rede elétrica. Agora fica fácil entender que essa tensão é como se fosse uma porta aberta para que qualquer transiente atinja o circuito de sensoreamento, na placa-mãe, responsável por derrubar para 0V a tensão no pino 14 do conector ATX principal, quando pressionamos o botão Power-on do gabinete.

Proteção

De tudo o que vimos até aqui, fica evidente a necessidade de proteção. Um grave problema é que muitas pessoas compram réguas de tomadas de baixo custo, que são vendidas como protetores de transientes, e consideram-se protegidas. Na prática, a única função destas réguas é o de aumentar o número de tomadas. Conforme demonstraremos aqui, pela análise do tamanho dos componentes usados para se fazer um protetor de transientes tecnicamente correto já se saberia que eles *não caberiam nestas réguas*.

Equipamentos têm proteção?

Verdade seja dita: alguns equipamentos de boa qualidade têm algum tipo de proteção contra transientes, porém são quase sempre limitados e de pequena eficiência. Uma fonte ATX bem projetada geralmente incorpora um circuito simples para a proteção contra transientes. A mesma coisa se aplica à placa-mãe, especificamente no circuito de entrada da interface de rede integrada.

Entretanto, são circuitos simples e não preparados para suportar um transiente de alguma intensidade. Evidentemente há uma razão para os fabricantes de equipamentos e componentes não incluírem sistemas com um grau mais elevado de proteção. Ou melhor, várias razões:

I. Os grandes consumidores de equipamentos eletrônicos são os mercados do Japão, EUA, Canadá e vários países da Europa. Todos estão no Hemisfério Norte, que como aprendemos não são as regiões de maior incidência de raios;

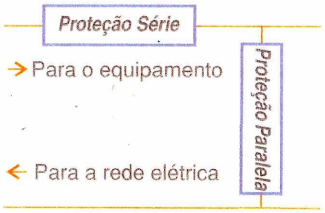
II. Nos países desenvolvidos do Hemisfério Norte, geralmente as redes são subterrâneas, o que minimiza a ocorrência de transientes induzidos;

III. A inclusão de circuitos para um sistema de proteção altamente eficaz eleva o custo do equipamento. Em um mercado altamente competitivo, para que fazer isso se os principais mercados alvo não necessitam?

IV. Como o Brasil e os outros países onde há maior incidência de raios são os menores consumidores de equipamentos eletrônicos, não há o interesse dos fabricantes em produzir modelos com protetores específicos.

Tipos de Proteção

Genericamente falando, existem dois tipos de proteção para um determinado dispositivo (figura 3).



F3. Tipos de proteção que serão citados ao longo do texto.

A proteção série é a que mais estamos acostumados a ver. Ela é normalmente feita por um fusível, mas outros dispositivos também podem ser empregados, a exemplo do PTC (Positive Temperature Coefficient), ou coeficiente de temperatura positivo. Na prática o PTC age como se fosse um resistor, com sua resistência aumentando positivamente em uma proporção não linear com a elevação da temperatura.

O princípio de funcionamento é simples: para baixas correntes o PTC apresenta uma resistência baixa; porém, ao passar uma alta corrente, há uma geração de calor que implica em uma elevação da temperatura e na resistência deste dispositivo, a qual aumenta rapidamente e praticamente provoca a interrupção do circuito. De maneira simplificada, portanto, podemos dizer que ele funciona como um fusível ou um disjuntor.

Porém, ao contrário do fusível que precisa ser trocado, ou do disjuntor que precisa ser manualmente rearmado, o PTC volta à condição normal após a passagem do surto de corrente e diminuição de sua temperatura.

Um tipo comercial de PTC com larga utilização é o PolySwitch, cujo fabricante, Raychem, classifica-o como sendo um PTC a polímero, constituído por uma combinação de um mesmo elemento na mesma proporção, porém com pesos moleculares diferentes.

Nas fontes de alimentação, os PTC's são colocados em série com fusíveis e atuam limitando a corrente de surto que ocorre em qualquer equipamento, quando este é energizado com carga. A proteção série é, quase sempre, ineficaz contra transientes.

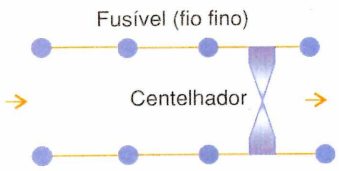
Mudando agora o enfoque para a proteção paralela contra transientes, as tecnologias mais empregadas são aquelas que utilizam dispositivos com características específicas de tempo de atuação, a fim de limitar as sobretensões dos transientes. Estes dispositivos podem ser os centelhadores, os centelhadores à gás, os diodos TVS, os varistores e os circuitos eletrônicos.

Centelhadores

Os centelhadores são usados desde o começo do conhecimento da eletricidade. Os centelhadores de ponta são nada mais que duas lâminas metálicas colocadas muito próximas uma da outra, possuindo o formato de um ângulo agudo. Quando a sobretensão surge, uma faísca ou centelhamento ocorre entre estas duas pontas. Estava inventado o primeiro dispositivo de proteção em paralelo. Nesta época começaram a ser utilizados também os centelhadores com eletrodos de grafite ou de carvão.

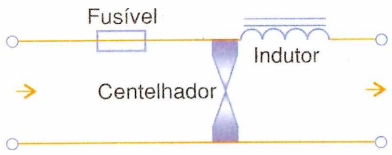
Desde o início do emprego do centelhador, constatou-se a necessidade de utilizar antes dele um dispositivo de proteção para sobrecorrentes. No começo foram usados fios de diâmetro fino que se rompiam quando ocorria uma sobretensão e o conseqüente centelhamento. Este foi talvez o primeiro

dispositivo de proteção série. Com o passar do tempo foram introduzidos os fusíveis e, muito depois, os disjuntores. Na figura 4 apresentamos um circuito básico para quem é saudosista e quer montar um centelhador com o efeito de pontas.



F4. Centelhador metálico.

Nesta época, houve também a transição da rede de distribuição de energia elétrica nas cidades, que no início era em corrente contínua e passou a ser de corrente alternada. Notou-se então que a colocação de um indutor no circuito melhorava consideravelmente a eficácia do centelhador (figura 5).



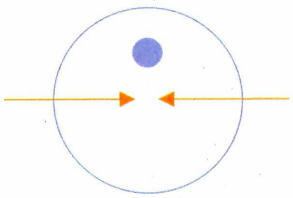
F5. Centelhador à carvão, seguido de indutor.

A explicação é simples. Os indutores possuem alta impedância para as elevadas freqüências dos transientes, agindo, portanto, como uma barreira que facilita o centelhamento. No entanto, este sistema possui alguns pontos fracos. A tensão de ruptura do ar, necessária para a formação do arco de centelhamento, varia muito de acordo com as condições de umidade relativa e de temperatura ambiente a que estão expostas as pontas dos eletrodos. Além disso, se algum detrito como a poeira, por menor que seja, se acumular nas pontas do centelhadores, a tensão de ruptura original será alterada.

Centelhadores à Gás

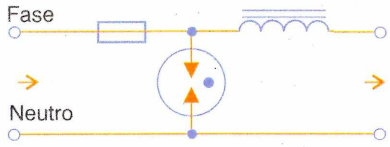
Para evitar estes problemas, ainda no século XIX algum indivíduo genial teve a idéia de colocar estes eletrodos dentro de uma ampola de vidro com gás inerte ou, tecnicamente falando, com um gás nobre. Estava criado o centelhador bipolar (dois eletrodos) à gás raro (figura 6).

Todos os problemas acima relatados foram eliminados e a tensão de ruptura ficou muito mais precisa, pois no momento em que a sobretensão ocorre o gás se ioniza e ajuda a corrente a fluir entre os eletrodos.



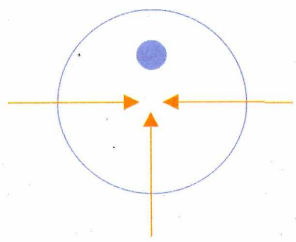
F6. Símbolo do centelhador bipolar à gás raro (bolinha azul indica que a ampola, onde estão os eletrodos, está preenchida com gás).

No século passado, a aplicação deste dispositivo foi intensa, pois não havia outro que fosse tão prático e eficiente contra os transientes (figura 7). O vidro como material da ampola ou envoltório, apesar de continuar a ser usado, cedeu lugar a materiais de maior resistência mecânica e térmica como, por exemplo, cerâmicas especiais.



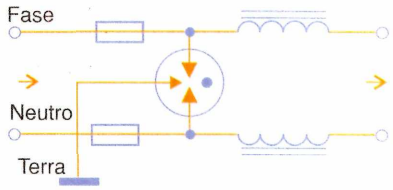
F7. Exemplo de circuito elétrico usando centelhadores à gás raro para proteção contra transientes, em redes de energia elétrica.

Porém estes centelhadores tinham dois problemas que eram críticos para algumas aplicações. O primeiro atinge principalmente os circuitos balanceados, os quais necessitam de aterramento. Abria-se então espaço para o desenvolvimento de um centelhador tripolar, que possui três eletrodos em um mesmo envoltório (figura 8).



F8. Símbolo do centelhador tripolar à gás.

O último problema era que tanto o bi quanto o tripolar são difíceis de atuar, mesmo quando se utiliza indutores após o centelhador. A solução para isso veio com a introdução de um gás chamado Trítio, o qual, por ser radioativo, contribui bastante para a ionização do gás e, conseqüentemente, facilita a ocorrência do centelhamento diante das sobretensões (figura 9). Além do trítio, outro material radioativo também foi e vem sendo empregado. Trata-se do Níquel 63, que produz radiação beta.



F9. Aplicação do centelhador tripolar em redes elétricas.

Note-se que, por estarem na mesma câmara, quando o gás é ionizado por uma descarga, todos os eletrodos estarão em curto, o que é uma grande vantagem. Todavia, a grande aplicação dos centelhadores tripolares à gás não foi na proteção de transientes da rede elétrica, mas para redes telefônicas.

Na época de seu lançamento comercial eram muito superiores aos dispositivos então existentes para proteção das redes telefônicas, que usavam como elementos de proteção bobinas térmicas em série e centelhadores de carvão, em paralelo. Assim sendo, foram instalados em grandes quantidades, tanto em centrais telefônicas, como também no domicílio de assinantes. Foram vendidos milhões, e muitos se encontram em uso.

Mas como alguns utilizam o trítio ou o Ni-63, que são radioativos, foram considerados impróprios para este tipo de aplicação, embora a quantidade de material fosse ínfima. Pouco a pouco foram e estão sendo substituídos por outros dispositivos contra transientes.

Estes dispositivos são os diodos TVS e os varistores, os quais atualmente têm preços mais competitivos para o grau de proteção exigido. Entretanto, nunca é demais frisar que para certas aplicações, como em equipamentos militares e modems ADSL, que podem suportar um tempo de atuação relativamente lento e estejam operando em áreas de alta incidência de raios, estes protetores tripolares à gás raro são imbatíveis. É importante destacar que estes dispositivos têm vida útil e, apesar de longa, precisam ser substituídos depois de algum tempo.

Apesar da sua larga aplicação na proteção de equipamentos conectados a redes de telefonia, até hoje ainda são fabricados certos tipos de centelhadores à gás raro para aplicações especiais em redes de energia elétrica de alta tensão. Geralmente são fabricados em ampolas de vidro de alta resistência e têm pinos para serem encaixados em soquetes,

facilitando desta forma a sua substituição. Além de apresentarem uma vida útil extremamente longa, estes dispositivos têm como vantagem a capacidade de absorção de transientes de grande amplitude, da ordem de centenas de KA (1.000 Ampères).

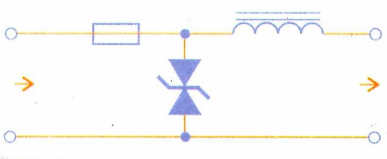
As desvantagens destes centelhadores para alta tensão são o alto custo, o tamanho volumoso e o tempo de atuação relativamente lento.

Diodos TVS

Os diodos TVS (Transient Voltage Suppression), às vezes chamados comercialmente de *transorb*, são dispositivos semicondutores de proteção paralela que possuem uma junção pn. Suas características dependem do tamanho da área de junção, da concentração de dopantes e da resistividade do substrato em que são montados. Na realidade podem ser considerados como um tipo especial de diodo zener. Podem ser do tipo unidirecional, para tensões contínuas, e bidirecionais para tensões alternadas.

Em condições normais, os diodos com tensão de ruptura reversa apresentam uma alta impedância ao circuito a ser protegido. Na prática se comportam como um circuito aberto, porém quando a tensão de operação normal ultrapassa a da junção PN, entra quase que instantaneamente (picosegundos) em estado de avalanche e passam a apresentar um caminho de baixa impedância para o transiente. Uma vez passado o transiente, este semicondutor volta ao seu estado normal, apresentando a alta impedância inicial.

Suas principais desvantagens são o alto custo quando comparado aos varistores de óxido de zinco de mesma potência, e a baixa capacidade de absorção de energia, sendo portanto mais aplicáveis para a proteção de elementos eletrônicos sensíveis do que em equipamentos (figura 10).



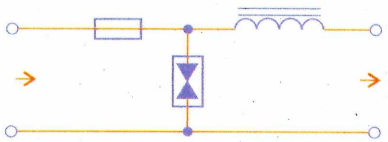
F10. Circuito de proteção utilizando os diodos TVS.

Varistores

Atualmente os varistores de óxido de zinco são considerados um dos melhores dispositivos de proteção contra sobretensões, só perdendo para os protetores que incorporam circuitos eletrônicos. O baixo custo também contribui para eles serem largamente utilizados.

São fabricados mediante a colocação de uma massa de minúsculos grãos de óxido de zinco e também de outros óxidos metálicos, entre duas placas de metal. Imagine como se fosse um sanduíche, onde o recheio seriam os óxidos metálicos e, os pães, seriam os eletrodos formados pelas placas de metal.

Este componente funciona tanto em tensões contínuas (6 VCC a 1.400 VCC), como em tensões alternadas (5 Vrms a 1.000 Vrms). Seu tempo de resposta ou de atuação é inferior a 25 nanosegundos e possuem capacidade para suportar altas correntes. A tensão de operação é muito precisa e as opções para escolha de tensões são enormes (figura 11).



F11. Aplicação dos varistores em redes elétricas.

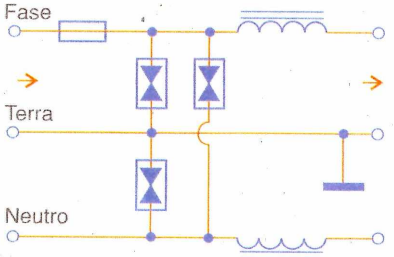
O grande problema dos varistores de óxido de zinco é o tempo de atuação, considerado muito lento para assegurar uma proteção eficaz aos equipamentos eletrônicos mais sensíveis a transientes.

O leitor atento verificará que o circuito acima, com exceção dos elementos de proteção, é o mesmo das figuras anteriores e, para todos estes elementos de proteção, o uso de fusíveis é imprescindível. Os fabricantes de varistores os especificam pelo diâmetro e para cada um indicam a corrente que o fusível deve ter (tabela 1).

DIÂMETRO (mm)	CORRENTE (A)
5,0	1 a 2
7,0	2 a 3
10,0	3 a 5
14,0	3 a 10
20,0	5 a 15

T1. Corrente do fusível é dada em função do diâmetro do varistor.

Para aplicação em redes elétricas que possuam aterramento, a figura 12 nos mostra o circuito aplicável.



F12. Uso dos varistores em redes aterradas.

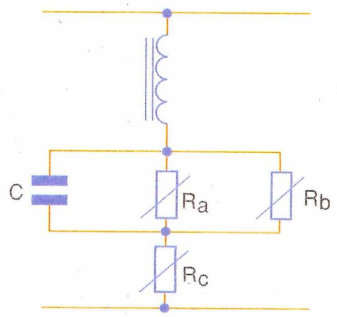
Outra desvantagem dos varistores de óxido de zinco na proteção contra transientes é que, após suportarem alguns transientes, estes dispositivos vão se deteriorando e perdendo as suas propriedades. Nada mais natural, portanto, que eles devem ser substituídos após algum tempo de operação. No entanto, na grande maioria dos protetores contra transientes os varistores são soldados, o que dificulta e, às vezes, impossibilita uma troca periódica.

Quando atingidos por transientes de grande amplitude, os varistores de óxido de zinco podem explodir, esquentar, pegar fogo ou simplesmente se partir ao meio. É por isso que nas placas de circuito impresso os varistores devem ser instalados um pouco afastados dos demais componentes para evitar danos. Materiais inflamáveis não devem ser colocados nas proximidades destes varistores.

Os dispositivos de proteção contra transientes devem estar acondicionados em caixas ou gabinetes adequados para que, no caso de uma explosão, os estilhaços não venham a causar problemas.

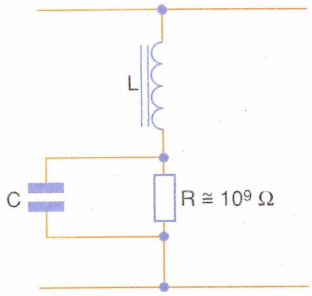
A temperatura afeta as características de disparo deste tipo de varistor e deve ser levada em consideração ao se projetar ou utilizar tais dispositivos. Como os varistores de óxido de zinco são fabricados com várias potências (expressas em Watts = W) e também com várias capacidades de absorção de energia proveniente dos transientes (expressa em Joules = J ou KJ = 1.000 J), deve-se prestar muita atenção nas especificações durante a escolha.

Para uma melhor compreensão do funcionamento deste dispositivo, vamos analisar o modelo do circuito elétrico simplificado equivalente a um varistor de óxido de zinco (figura 13).



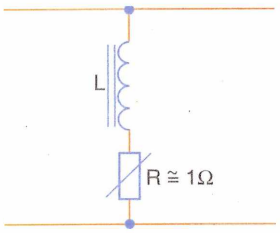
F13. Modelo do circuito elétrico equivalente a um varistor.

Na chamada região de operação, o modelo do circuito elétrico praticamente se limita a um único resistor R de alta impedância, superior a 10 ^{9} Ohms (Ω), como está ilustrado na figura 14.



F14. Circuito equivalente de um varistor em operação normal.

Já na figura 15 vemos o comportamento do varistor diante do transiente. Note que o modelo do circuito elétrico passa simplesmente a ser de um resistor de baixo valor ôhmico, da ordem de 1 Ω a 9 Ω.



F15. Circuito equivalente de um varistor diante do transiente.

Circuitos Eletrônicos

Existem ainda sistemas de proteção contra transientes que são geralmente construídos por circuitos eletrônicos. São os chamados crowbar os quais após detectarem uma sobretensão anormal, como é o caso de um transiente, disparam quase que instantaneamente um conjunto de SCR´s ou de Triac´s.

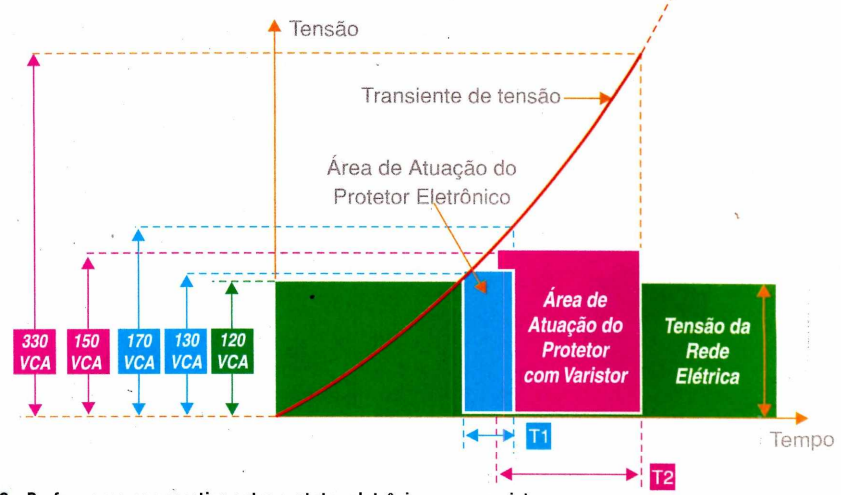
As grandes vantagens deste tipo de protetor eletrônico são:

- Tempo de atuação extremamente rápido, superior a todos os outros dispositivos;
- Tensão de disparo mais precisa, aliado a uma menor faixa de tolerância;
- Exceto em alguns casos, não apresentam deterioração, nem perdem as suas características.

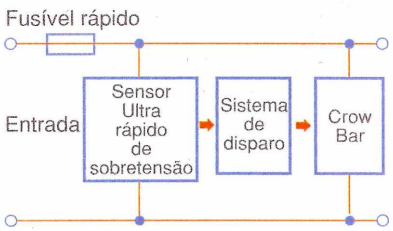
Seu principal inconveniente é o custo mais elevado, daí sua utilização em aplicações críticas, enquanto os varistores ficam em todas as demais. Vale destacar, contudo, uma redução atual nos preços dos semicondutores que tem motivado uma penetração cada vez maior dos sistemas de proteção baseados em circuitos eletrônicos.

A figura 16 nos mostra como o tempo de atuação destes protetores é muito inferior aos demais e, desta forma, evitam a passagem de transientes que normalmente passariam.

A curva em vermelho representa a forma de onda de um transiente cuja tensão está subindo muito rapidamente. A área em verde indica a tensão da rede elétrica, neste caso 120 VCA. Já a área na cor azul indica a faixa de atuação do protetor eletrônico que, neste exemplo, tem um tempo de atuação T1. Note que apesar da sua tensão de disparo ser de 130 VCA, parte da tensão do transiente, cujo pico não chega a atingir 170 VCA, pode passar, porém por um tempo curto, que não causará danos (figura 17).



F16. Performance comparativa entre protetor eletrônico e com varistor.



F17. Diagrama de blocos de um protetor eletrônico.

Por último, na área em violeta temos a faixa de atuação de um protetor com varistor. Se verificarmos as especificações técnicas de um varistor de 20 mm e 130 VCA, notaremos que a sua faixa de disparo situa-se entre 185 a 225 VCA para um tempo que chamaremos de T2, bem maior que T1. Como podemos ver no gráfico, mesmo com o varistor tendo atuado, em uma condição ideal, ao atingir 150 VCA, seu tempo de resposta lento permite que parte da tensão do transiente (aproximadamente 330 VCA) passe e provoque problemas irreversíveis, tal como a queima de uma placa-mãe.

Recapitulação

Fazendo uma breve recapitulação de tudo que vimos até aqui, temos que:

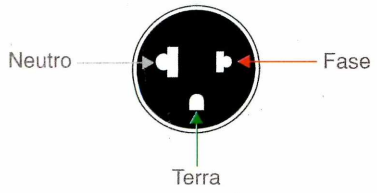
- Os raios são os principais responsáveis pela geração de transientes na rede elétrica;
- O Brasil é o país com maior queda de raios, o mesmo não ocorre nos países que são grandes consumidores;
- Não há interesse dos fabricantes em fazer pequenas produções de equipamentos com melhores níveis de proteção;
- A soma de vários fatores, como a mudança do tipo de energização nas fontes de alimentação dos computadores, o aumento de transientes e o uso de protetores inadequados têm provocado um aumento no número de queimas de placas-mãe;
- No Brasil, a maioria dos equipamentos eletrônicos precisa de protetores contra transientes que realmente funcionem;
- Os melhores dispositivos de proteção são aqueles que usam circuitos eletrônicos.

Pronto, já sabemos todas as verdades e então está tudo resolvido? Ainda não! Veremos a seguir que mesmo quando tivermos o melhor dos protetores eletrônicos, eles serão de pouca ou nenhuma utilidade se não forem instalados corretamente.

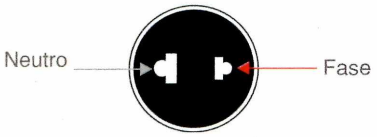
Redes Elétricas

Existem dezenas de aparelhos chamados de protetores contra transientes, como as réguas de tomadas chinesas e outros que inundam o nosso mercado e iludem os compradores. A grande maioria destes protetores não funcionam corretamente, e os poucos que possuem alguma eficácia quase sempre requerem uma rede elétrica com um perfeito sistema de aterramento. Um exemplo é o protetor com varistores mostrado na figura 12.

Mas uma notícia ainda pior é que os órgãos responsáveis no Brasil pelas normas e diretrizes, como é o caso do INMETRO, que deviam



F18. Tomada de três pinos corretamente instalada.



F19. Tomada de dois pinos corretamente instalada.

dar uma clara definição dos dispositivos de proteção, pouco fazem neste sentido.

Não existe no Brasil uma especificação legal, com embasamento tecnicamente correto, que conscientize o consumidor quanto à necessidade de utilização de dispositivos de proteção contra transientes que realmente funcionem.

E os problemas para se obter um bom nível de segurança e proteção para os nossos equipamentos eletrônicos não param aí. Redes elétricas tecnicamente corretas só são encontradas em imóveis recentes, que obedecem às novas normas para construções que obrigam a instalação do fio terra (figura 18).

Todavia, deve-se atentar para que esta tomada não apresente algum dos seguintes erros comumente cometidos durante a instalação: terra ou neutro sem conexão, inversão na posição dos terminais, além do terra e neutro conectados junto.

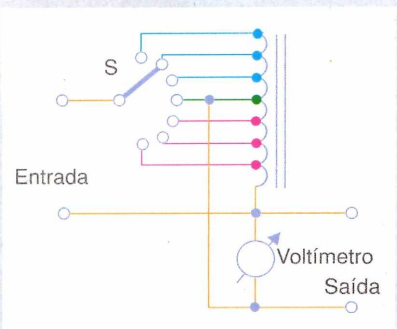
Entretanto, a maioria das tomadas elétricas existentes nos imóveis só possui tomadas para dois pinos (figura 19). E alguns imóveis mais antigos sequer possuem tomadas que possibilitem a identificação do que é fase ou neutro.

Embora seja possível fazer a conversão de uma rede elétrica residencial ou comercial com tomadas de dois pinos para tomadas com três pinos e possuindo aterramento, o processo é difícil. Os principais obstáculos são o custo e a complexidade, pois além da construção do aterramento, é necessária toda uma nova fiação para levar o fio terra até as tomadas. E em alguns casos, torna-se até inviável, de acordo com as condições locais.

Como fazer para termos uma proteção eficaz contra transientes em redes elétricas sem aterramento? Alguns sugerem o uso de transformadores isoladores, que provêem a chamada isolação galvânica; isto é, o equipamento eletrônico ligado ao secundário deste transformador fica eletricamente isolado da rede elétrica.

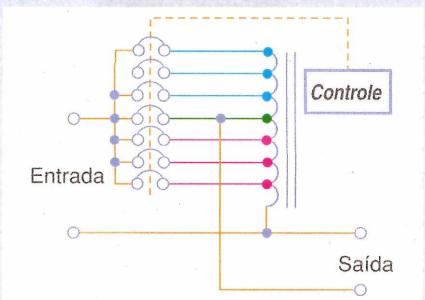
Reguladores e Estabilizadores e de Tensão

Os reguladores de tensão são constituídos, na maioria das vezes, por um autotransformador contendo muitas derivações, conhecidas como taps. Na figura abaixo vemos a versão mais simples de um regulador, onde a variação de tensão, para mais ou para menos, é feita através de uma chave manual S.



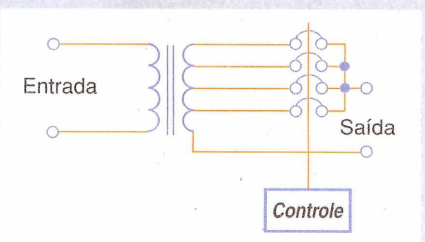
O funcionamento é muito simples: quando a tensão está baixa, a chave seletora S é comutada para um dos taps representados pela cor vermelha. Quando a chave S está na posição do meio, de cor verde, a tensão de entrada é igual à tensão de saída. E finalmente, quando a tensão da rede elétrica está acima do normal, a chave S é comutada para um dos taps azuis. O voltímetro serve para ver a tensão de saída.

Com a evolução da tecnologia surgiram os estabilizadores automáticos, os quais, ao invés de uma chave seletora, fazem a comutação através de elementos elétricos (geralmente relés) ou eletrônicos, utilizando SCR's ou TRIAC's. Estes elementos de comutação são acionados através de um controle que seleciona o tap apropriado para fornecer a tensão elétrica correta, como mostra a figura abaixo.



Como a tensão de saída era mais estabilizada, graças a estes controles o regulador passou a ser chamado de estabilizador de tensão.

Atualmente se usa muito o estabilizador, em alguns modelos o controle dos elementos de comutação (via de regra, TRIAC's) é feito por microprocessadores. Com a evolução tecnológica, os autotrawnsformadores cederam lugar aos transformadores de isolação, que proporcionam a chamada isolação galvânica.



Aparelho ligado no secundário do transformador fica eletricamente isolado da rede elétrica.

Por que abordar reguladores e estabilizadores de modo tão detalhado? Para analisar se há algum fundamento no que dizem muitos fabricantes sobre a proteção oferecida pelos estabilizadores. Alguns, aliás, declaram haver proteção até contra transientes.

Conforme vimos até aqui, nenhum estabilizador possui eficácia contra transientes. Pelo contrário, pode até gerá-los, uma vez que os elementos que comutam os taps, sejam eles relés, SCR's ou TRIAC's, estão chaveando cargas energizadas.

Alguns fabricantes dizem que seus equipamentos incorporam filtros de transientes, mas, como analisado neste artigo, eles não oferecem proteção efetiva. Por sinal, isso nem poderia acontecer num equipamento que custa menos de R$ 100.

Outro ponto que podemos analisar é a real necessidade de um estabilizador "atrás" de um computador. Como sabemos, os computadores usam fontes chaveadas que possuem ou não chave seletora de tensão de entrada (115 VCA / 230 VCA). Por norma, as com chave funcionam para tensões nominais entre 90 e 135 VCA, ou entre 180 e 265 VCA para os modelos 230 VCA. Enquanto isso, as sem chave funcionam desde 90 até 265 VCA.

Em ambos os casos, as normas determinam que estas fontes devem "dar partida" com carga máxima a 90 VCA, e apresentarem completa regulação das tensões de saída.

Diante disso, será que um computador precisa mesmo de um estabilizador?

Entretanto, somente estes transformadores pouco fazem para eliminar os transientes de alta intensidade. Além disso, eles têm um custo considerável e possuem peso e tamanho elevados.

A solução mais apropriada, portanto, quando não há aterramento, consiste em utilizar protetores eletrônicos especificamente projetados para este tipo de rede.

Novos plugs e tomadas

Como se não bastassem todos os problemas mencionados neste artigo, ainda teremos de conviver com um novo tipo de tomada e plug padrão (NBR 14136) a ser exclusivamente adotado no Brasil (figura 20). Isso mesmo, diferente de tudo o que há no mundo!

A adoção, que foi determinada pelo INMETRO sob a tutela do Ministério de Desenvolvimento, Indústria e Comércio Exterior, está descrita na Portaria nº 019, de 16 de Janeiro de 2004 (**www.inmetro.gov.br/rtac/pdf/RTAC000875.pdf**).

Esta medida que é coercitiva, pois tem força de lei, teve como justificativas:

- Existem vários tipos de tomadas e plugs, é preciso padronizá-los;
- O novo tipo de plug/tomada irá evitar choques elétricos;
- Os plugues de dois pinos cilíndricos do padrão NBR14136 poderão ser adotados imediatamente em todos os aparelhos.

O ponto de vista exclusivamente particular deste autor é o seguinte:

- A padronização deveria se feita pela adoção de modelo de maior uso de corrente, como por exemplo o americano;
- Para evitar choque deveria ser empregado um interruptor de corrente de fuga, há vários anos disponível no mercado nacional e de eficiência comprovada;
- Estas tomadas e plugs serão mais caros que os atuais, estima-se de 10% a 25%;
- A partir da data fixada na portaria, todos os equipamentos no Brasil deverão ter tal pino, o que na prática significa que: ou você troca todas as tomadas da sua residência, ou terá de trocar o plug do cabo de força do equipamento. Como as duas soluções não são práticas, veremos uma inundação de adaptadores sem homologação e que certamente trarão algum tipo de risco. Entretanto, pode acontecer pior, se não forem usados os adaptadores. A solução mais prática será a de recorrer às chamadas gambiarras, que constituirão um perigo ainda maior;
- No tocante à justificativa que "os plugs de dois pinos cilíndricos do padrão NBR14136 poderão ser adotados ime-

No-Breaks

Outro equipamento que às vezes é vendido como protetor contra transientes é o No-Break. Para sermos criteriosos, vale esclarecer que sua função principal é fornecer energia quando a concessionária, por algum motivo, interrompe o fornecimento da energia elétrica.

O tempo de fornecimento de energia de um No-Break, chamado de autonomia, é determinado basicamente em função da capacidade do equipamento, das baterias e do consumo dos aparelhos que a ele estiverem conectados. Este tempo é geralmente limitado a minutos, suficiente para que o usuário salve o que for preciso e desligue a máquina.

São fatos conhecidos os danos que a interrupção do fornecimento de energia elétrica pode causar a equipamentos e sistemas computacionais. Não é à toa que alguns data centers também possuem grupos de geradores, capazes de prover energia nos casos em que o período de interrupção for superior à autonomia dos No-Breaks.

Existem várias técnicas construtivas para se fabricar um No-Break, porém a que realmente pode barrar a passagem de transientes é a chamada "Always On". A energia alternada entra no equipamento, passa por uma fonte retificadora onde esta tensão alternada é reduzida e retificada, e após vai para um circuito responsável pelo regime de carga ou flutuação das baterias.

Esta energia contínua, por sua vez, vai alimentar um ou mais inversores CC/CA que irão convertê-la na energia alternada que irá alimentar os equipamentos. Como se vê, a propagação de um transiente por este No-Break no máximo danificará os circuitos de entrada.

Por outro lado, existe outra classe de No-Breaks, os chamados "off-line", nos quais a tensão alternada da rede elétrica vai direto para o equipamento alimentado. Apenas quando ocorre a interrupção de energia é que a saída é comutada para o inversor. A simples menção da palavra comutação lembra o problema apresentado na análise dos estabilizadores de tensão.

Independentemente do elemento comutador, esta comutação de uma carga energizada certamente gerará transientes. Como se isto não bastasse, a simples análise do diagrama abaixo demonstra que, em condições normais, se um transiente for induzido ou conduzido na rede elétrica, atingirá diretamente o equipamento, como indica a linha laranja tracejada.

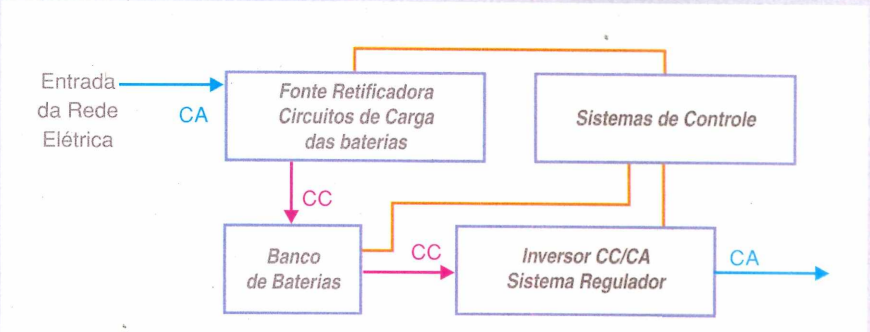


Diagrama de bloco de um No-Break "Always On", também conhecido como on-line

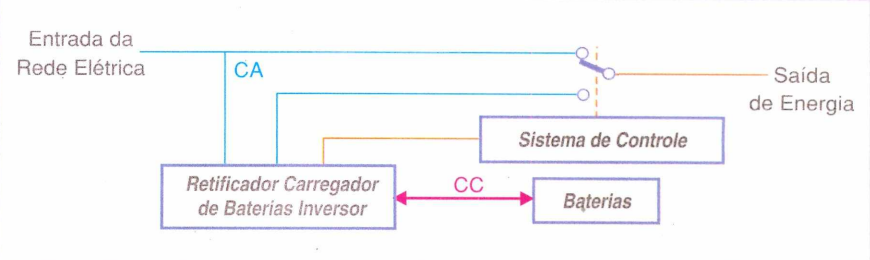
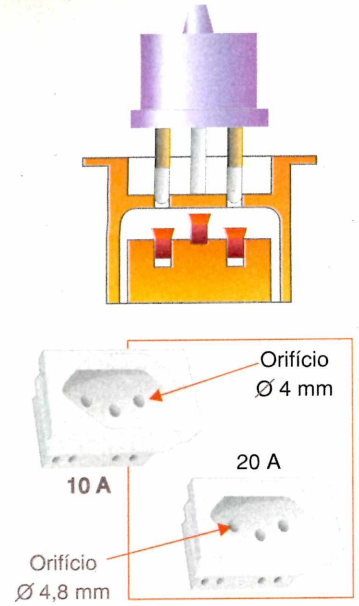


Diagrama de funcionamento de um No-Break "off-line". A maioria dos modelos fabricados no Brasil é deste tipo.



F20. É obrigatório novo plug de 3 pinos e tomadas elétricas de 10 a 20A.

diatamente em todos os aparelhos", é falha na medida que a grande maioria dos equipamentos eletrônicos usa o padrão americano de três pinos, ou o padrão compatível com o americano de dois pinos chatos;

• Os usuários que têm uma rede elétrica domiciliar ou comercial não aterrada, com dois pinos, não serão motivados a evoluírem para uma rede elétrica mais segura com aterramento, que são referidas nas próprias normas;

• Quem arcará com todo este ônus será o consumidor final. Mais uma vez!

• Equipamentos fabricados no Brasil não poderão ser exportados com o plug brasileiro, *pois* em nenhum outro lugar do planeta haverá uma tomada elétrica para este "revolucionário" plug;

• Em meio a tantas discussões sobre o custo elevado do Brasil para os empresários, esta medida será na verdade mais uma que elevará o custo dos equipamentos;

Neste ponto faremos uma analogia com uma história real que aconteceu há alguns anos atrás, não com plug de energia elétrica, mas sim com plugs para telefone. Naquela ocasião, a extinta TELEBRAS obrigou a padronização de plugs para telefone com quatro pinos, que no planeta inteiro só existia no Brasil.

Depois de muitos problemas elétricos e construtivos, tal padrão foi abandonado e hoje se utiliza maciçamente o modular Jack, que é melhor, menor e mais barato. Será que você ainda tem um telefone com este plug, ou foi obrigado a comprar um adaptador, ou ainda acabou trocando o plug de quatro pinos por um modular jack? Talvez seja o que acontecerá quando saírem equipamentos e aparelhos elétricos com a tomada deste novo e exclusivo padrão.

Conclusão

Quando o assunto são as redes elétricas no Brasil, infelizmente o cenário poderia ser melhor. A distribuição de energia está longe de dispensar um equipamento de proteção. Estes, por sua vez, em sua grande maioria deixam a desejar e, não bastasse tudo isso, nossas entidades governamentais pouco têm feito para melhorar este cenário.

Portanto, todo cuidado é pouco. Além de tomar conhecimento da realidade, nesta matéria você foi apresentado ao conhecimento técnico necessário para poder avaliar se um determinado equipamento de proteção pode de fato ser eficaz contra transientes. Tente obter as especificações detalhadas junto aos fabricantes e faça todo o possível para não deixar isso para depois, pois você pode vir a ser mais uma vítima de queima de placas-mãe ou outro equipamento eletrônico.

PC

Road Show

Por: Paulo Roberto Sant'anna Cardoso

Procurando movimentar a comunidade técnica de TI do Rio de Janeiro, os grupos MSInfraRio, Code4All e Wits Brasil realizaram duas etapas do evento Road Show Microsoft - Culminis no mês de junho. Ambos os eventos fazem parte do calendário oficial de eventos da Microsoft, que segue fazendo um trabalho de apoio às comunidades, e da Culminis, uma organização internacional sem fins lucrativos que incentiva e apóia grupos de usuários especializados em Tecnologia MS.

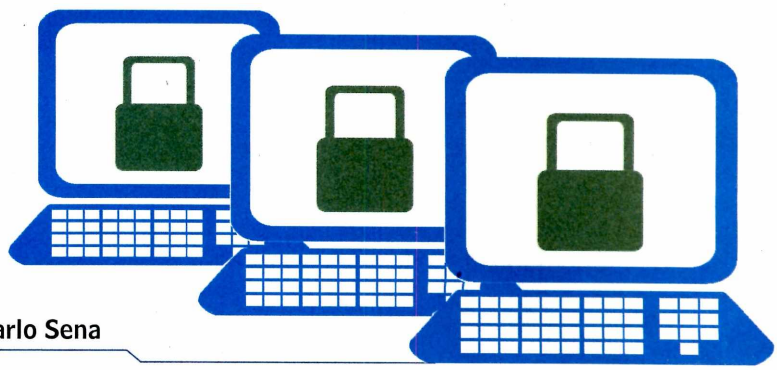
A realização de ambos os eventos marcou a união de profissionais de diversos segmentos da área de TI: infra-estrutura (ITPros), desenvolvedores (DEVs), Microsoft Most Valuable Professionals (MVPs) e Microsoft Student Partners (MSPs). Esta inédita parceria deve propiciar uma série de novos eventos e congressos para todo o estado do Rio de Janeiro. O sentido de comunidade e colaboração foi bem difundido e foi o ponto alto do evento juntamente com as apresentações. Na parte técnica, tivemos palestras com temas bem interessantes, a exemplo da "Windows Vista para Profissionais de TI" (Marcos Aguiar); "Windows Vista para Desenvolvedores" (Ricardo Guerra); "Microsoft Office 2007 & SharePoint" (Igor Humberto); "Windows Server 2008" (Paulo Sant'anna); "Segurança da Informação e Desenvolvimento Seguro" (Rodrigo Moreira); "Best Practices e Refactoring em .NET" (Cláudio Ralha); além de mini-curso sobre desenvolvimento de jogos para PC e e XBox360 (Anderson Ferreira). Na organização dos eventos tivemos o trabalho dos colegas Alexandro Prado, Weliton Junior e Lucas Massena.

A Revista PC&Cia também esteve presente contando com dois colaboradores entre os palestrantes e fazendo a distribuição de revistas e do livro "Redes Locais na prática". No dia 23 de julho foi realizada a primeira etapa na Faculdade Simonsem, em Padre Miguel, e no dia 30, a segunda etapa ocorreu em Cabo Frio, na Universidade Veiga de Almeida.



Equipe reunida: devido ao enorme sucesso e às inúmeras possibilidades que essa união de forças pode proporcionar, desde já prometemos novidades para o segundo semestre deste ano. Aguardem!

Ambiente seguro com maior facilidade



Saiba como controlar o acesso a serviços em sistemas GNU/Linux sem as regras do iptables.

Jansen Carlo Sena

Um dos fatores mais importantes para a popularização do GNU/Linux, fundamentalmente no meio corporativo, consiste na facilidade de se utilizar esse ambiente operacional, junto com suas ferramentas nativas, como uma solução de firewall para controlar o acesso a serviços que possam estar atendendo requisições de clientes. A segurança e robustez dessa plataforma, aliada ao fato de não ser necessário dispender recursos para o pagamento de licenças de uso, ao contrário do que acontece nas soluções proprietárias, torna essa solução uma alternativa que vem se fazendo cada vez mais presente em redes de pequeno, médio e grande porte.

Nesse contexto, o iptables é a ferramenta que interage com o kernel inserindo as regras de filtragem que manipulam os pacotes IP no momento em que esses são repassados à porção do sistema operacional responsável por processar os dados advindos das interfaces de rede. Entretanto, gerenciar um bom conjunto de regras, de forma que elas façam exatamente o que se pretende, exige inevitavelmente um entendimento razoável do funcionamento da arquitetura TCP/IP.

Caso contrário, aumenta-se consideravelmente a probabilidade do conjunto de regras não corresponder ao planejado e deixar potenciais "brechas de segurança" que podem ser silenciosamente exploradas por atacantes. Vale ressaltar que o conhecimento da pilha TCP/IP é inerente à atividade de implementação de regras de filtragem, independente da ferramenta que se deseja utilizar, uma vez que esse tipo de filtragem age sobre os principais protocolos dessa arquitetura.

Existem diversas ferramentas gráficas que buscam facilitar a implementação e manutenção de regras de filtragem. Mesmo diante disso, a complexidade da atividade não deixa os administradores de sistemas, fundamentalmente os menos experientes, confortáveis com a elaboração, implementação e administração das regras baseadas em filtros como o iptables. Entretanto, existe um recurso simples e rápido para atender a essas necessidades.

Preparado? Então vamos lá!

O que será utilizado?

Para "driblar" a complexidade das regras que podem ser elaboradas por ferramentas mais específicas como o iptables, existe uma maneira fácil e rápida para implementar regras de controle de acesso a serviços de rede presentes em sistemas GNU/Linux. Trata-se de dois simples arquivos em formato texto: hosts.allow e hosts.deny, ambos localizados no diretório /etc. Resumidamente, por meio da configuração desses dois arquivos é possível determinar quais máquinas remotas podem ou não acessar cada tipo de serviço que esteja sendo executado em um computador.

De maneira geral, a utilização desses dois arquivos é implementada em sistemas GNU/Linux por meio de uma biblioteca chamada TCP Wrappers. Essa biblioteca foi criada por Wietse Venema, um dos grandes nomes da atualidade da área de segurança e criador do, cada vez mais famoso, sistema de emails Postfix. Além disso, a TCP Wrappers está presente na maioria das distribuições GNU/Linux. Para confirmar a sua instalação em sistemas como o Ubuntu, basta executar o seguinte comando:

```
dpkg -s libwrap0
```

Provavelmente, o resultado retornado será semelhante ao apresentado na figura 1. Caso sua distribuição utilize um mecanismo diferente do apt-get para o gerenciamento de software, consulte a documentação para saber como é possível buscar pelos pacotes de bibliotecas e procure por aquele que contém o TCP Wrappers.

Antes de utilizar os arquivos hosts.allow e hosts.deny...

O controle de acesso por meio dos arquivos hosts.allow e hosts.deny consiste em uma solução de mais alto nível, quando comparada a filtros como o iptables. Isso porque a consulta é feita pelo processo responsável por oferecer um determinado tipo de serviço, ao contrário das soluções de filtragem de pacotes, onde os dados são bloqueados já

na camada do sistema operacional responsável por manipular os dados recebidos por meio das interfaces de rede, antes mesmo de alcançarem os serviços.

Em outras palavras, se o seu servidor SSH, por exemplo, foi compilado com o uso das funcionalidades oferecidas pela biblioteca do TCP Wrappers, os controles de acesso configurados nos arquivos correspondentes serão considerados na hora de permitir ou bloquear a conexão de determinado cliente. Por outro lado, um filtro para o serviço de SSH, implementado através do iptables, por exemplo, irá entrar em ação independentemente do pacote do SSH que você está utilizando, ou mesmo de alguma característica específica utilizada no momento de sua compilação.

Diante disso, uma vez que o suporte aos controles do TCP Wrappers é dependente do software ter sido preparado para tal funcionalidade, antes de implementar filtros para determinados serviços através dos dois arquivos em questão, é preciso verificar se aquele aplicativo foi ou não implementado com suporte ao TCP Wrappers. Isso pode ser analisado por meio do comando "ldd", que relaciona quais bibliotecas dinâmicas são utilizadas por um executável. Na figura 2, é utilizado primeiramente o comando "which" para determinar a localização do arquivo sshd, que é o executável do servidor SSH e, em seguida, é utilizado o "ldd" para apresentar as bibliotecas "linkadas" dinamicamente com esse executável. Caso o aplicativo tenha sido compilado com suporte à biblioteca do TCP Wrappers, será possível encontrar, dentre o resultado retornado, uma linha que indique a utilização da libwrap0.

Para facilitar a análise da saída do comando ldd, é possível utilizar o comando grep como forma de filtrar o resultado da saída do comando ldd para apresentar somente o que é interessante, ou seja, alguma linha que contenha uma referência para a biblioteca libwrap0 (figura 3).

Um pouco sobre o funcionamento do TCP Wrappers

Antes de gerar suas regras para controle de acesso aos serviços que utilizam os recursos da biblioteca TCP Wrappers, é preciso entender como as informações dos arquivos hosts.allow e hosts.deny são processadas. O primeiro arquivo, hosts.allow, contém regras que buscam permitir o acesso a serviços. De maneira análoga, o arquivo hosts.deny contém regras que, uma vez casadas, proíbem o acesso aos serviços associados a cada uma dessas regras.

Primeiramente, os dados que solicitam a abertura de uma nova conexão, como endereço IP de origem e o serviço (SSH, FTP, etc) a ser utilizado pelo cliente, são analisados frente às regras inseridas no arquivo hosts.allow. Caso esses dados casem com alguma das regras relacionadas nesse arquivo, o acesso ao serviço é permitido e o cliente pode estabelecer sua conexão e dar prosseguimento à troca de informações com o servidor.

Caso nenhuma regra relacionada no arquivo hosts.allow permita a abertura daquela conexão, os mesmos dados são verificados junto às regras contidas no arquivo hosts.deny. Se alguma das regras desse arquivo casar com os dados daquela conexão, o acesso àquele serviço é negado e a solicitação de abertura de conexão é cancelada.

Por fim, se nenhuma das regras do arquivo hosts.deny explicitamente proibir o acesso a um determinado serviço, então o acesso será permitido e a conexão será estabelecida normalmente. Seja no arquivo hosts.allow, o primeiro a ser analisado, seja no arquivo hosts.deny, uma vez que uma regra case com os dados de uma tentativa de abertura de conexão, a análise das regras posteriores é desconsiderada imediatamente.

Por exemplo, se o acesso ao serviço SSH, a partir do cliente cujo endereço IP seja 10.1.1.20, tenha sido permitido e proibido nos arquivos hosts.allow e hosts.deny, respectivamente, o acesso ao serviço será permitido porque o arquivo hosts.allow é sempre analisado primeiro.

Em outras palavras, a regra que proíbe o acesso desse cliente nunca será analisada, uma vez que uma regra anterior permite o seu acesso.

De maneira geral, é importante estar atento a esse mecanismo para que não sejam cometidos enganos que podem lhe provocar um grande problema, seja por proibir o acesso de um cliente a um serviço que deveria ser permitido, ou, mais grave ainda, permitir o acesso por parte de um cliente a um serviço em que ele não deveria ter permissão de conexão.

Criando as regras de controle de acesso

Uma das grandes vantagens de se utilizar os recursos do TCP Wrappers é o fato de sua utilização ser menos complexa que a de outras soluções para a implementação de controle de acesso a serviços. A sintaxe para criar regras nos arquivos hosts.allow e hosts.deny é simples e resume-se, basicamente, a duas informações: o serviço que está sendo considerado e a identificação do

```
Arquivo Editar Ver Terminal Abas Ajuda
jansen@scadufax:~$ dpkg -s libwrap0
Package: libwrap0
Status: install ok installed
Priority: important
Section: libs
Installed-Size: 88
Maintainer: Ubuntu Core Developers <ubuntu-devel-discuss@
Architecture: i386
Source: tcp-wrappers
Version: 7.6.dbs-11build1
Depends: libc6 (>= 2.5-0ubuntu1)
Recommends: tcpd
Conflicts: netbase (<< 3.16-1)
Description: Wietse Venema's TCP wrappers library
 Wietse Venema's network logger, also known as TCPD or LO
 .
 These programs log the client host name of incoming teln
 ftp, rsh, rlogin, finger etc. requests. Security options
 access control per host, domain and/or service; detectio
 host name spoofing or host address spoofing; booby traps
 implement an early-warning system.
Original-Maintainer: Anthony Towns <ajt@debian.org>
jansen@scadufax:~$
```

F1. Verificando presença da biblioteca TCP Wrappers.

```
Arquivo Editar Ver Terminal Abas Ajuda
jansen@scadufax:~$ which sshd
/usr/sbin/sshd
jansen@scadufax:~$ ldd /usr/sbin/sshd
        linux-gate.so.1 =>  (0xffffe000)
        libwrap.so.0 => /lib/libwrap.so.0 (0xb7fa4000)
        libpam.so.0 => /lib/libpam.so.0 (0xb7f9c000)
        libdl.so.2 => /lib/tls/i686/cmov/libdl.so.2 (0x
        libselinux.so.1 => /lib/libselinux.so.1 (0xb7f8
        libresolv.so.2 => /lib/tls/i686/cmov/libresolv.
        libcrypto.so.0.9.8 => /usr/lib/i686/cmov/libcry
        libutil.so.1 => /lib/tls/i686/cmov/libutil.so.1
        libz.so.1 => /usr/lib/libz.so.1 (0xb7e14000)
        libnsl.so.1 => /lib/tls/i686/cmov/libnsl.so.1 (
        libcrypt.so.1 => /lib/tls/i686/cmov/libcrypt.so
        libgssapi_krb5.so.2 => /usr/lib/libgssapi_krb5.
        libkrb5.so.3 => /usr/lib/libkrb5.so.3 (0xb7d350
        libk5crypto.so.3 => /usr/lib/libk5crypto.so.3 (
        libcom_err.so.2 => /lib/libcom_err.so.2 (0xb7d0
        libkrb5support.so.0 => /usr/lib/libkrb5support.
        libc.so.6 => /lib/tls/i686/cmov/libc.so.6 (0xb7
        /lib/ld-linux.so.2 (0xb7fbd000)
        libsepol.so.1 => /lib/libsepol.so.1 (0xb7b86000
jansen@scadufax:~$
```

F2. Bibliotecas linkadas com executável do servidor SSH.

```
Arquivo Editar Ver Terminal Abas Ajuda
jansen@scadufax:~$ ldd /usr/sbin/sshd | grep libwrap
        libwrap.so.0 => /lib/libwrap.so.0 (0xb7eda000)
jansen@scadufax:~$
```

F3. Facilitando visualização com o filtro proposto pelo grep.

cliente por meio do seu endereço de rede específico, seu nome, por uma faixa de IPs ou mesmo pelo nome do domínio, conforme mostrado a seguir:

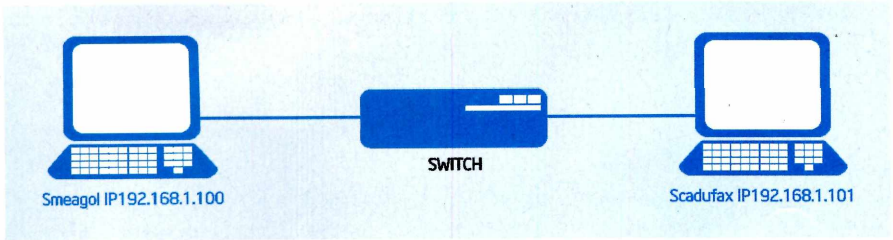
```
nome_do_serviço:  identificação do cliente
```

Ambos os arquivos devem conter uma regra a cada linha.

Considere por exemplo o cenário apresentado na figura 4, onde dois computadores estão conectados por meio de uma rede: smeagol, cujo endereço IP é 192.168.1.100, e scadufax, cujo endereço IP é 192.168.1.101. Diante disso, a regra a seguir poderia ser inserida no arquivo hosts.allow, em scadufax (192.168.1.101), para permitir o acesso de smeagol (192.168.1.100) ao seu serviço de SSH:

```
sshd: 192.168.1.100
```

Nesse caso, conforme mostrado na figura 5, a partir de smeagol é possível estabelecer



F4. Cenário usado como exemplo.

```
jansen@smeagol: ~
Arquivo  Editar  Ver  Terminal  Abas  Ajuda
jansen@smeagol:~$ ssh jansen@192.168.1.101
jansen@192.168.1.101's password:
Linux scadufax 2.6.20.3-ubuntu1-jcs #1 SMP Sun Jun 3 16:46:43 AMT 2007 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.
Last login: Sun Jul 22 21:18:59 2007 from 192.168.1.100
jansen@scadufax:~$
```

F5. Conexão SSH normalmente estabelecida.

uma conexão SSH com o computador scadufax. Note que a senha é solicitada e, após sua inserção, uma sessão remota é aberta em scadufax. Muito embora essa regra seja válida e analisada antes da conexão ser estabelecida, até o momento ela não é muito funcional porque o arquivo hosts.deny está vazio e, portanto, nenhum tipo de tráfego está proibido.

Por outro lado, se essa mesma regra é retirada do arquivo hosts.allow e inserida em hosts.deny no computador scadufax, smeagol não terá mais permissão para conectar-se ao serviço SSH presente em scadufax, conforme exibido na figura 6, onde é apresentada uma mensagem dizendo que a conexão foi encerrada.

Outra alternativa seria utilizar o nome do cliente ao invés do endereço IP:

```
sshd: smeagol.jansen.com.br
```

Para um mesmo serviço é possível acrescentar vários clientes ao mesmo tempo, conforme apresentado a seguir:

```
sshd: 192.168.1.100 192.168.1.102
```

Para permitir acesso a todos os computadores inseridos na rede 192.168.1.X, por exemplo, pode-se criar a seguinte regra:

```
sshd: 192.168.1.
```

ou ainda:

```
sshd: 192.168.1.0/255.255.255.0
```

Por fim, para identificar um conjunto de clientes, é possível ainda utilizar parte do nome DNS desses clientes. Por exemplo:

```
sshd: .outrodominio.com.br
```

Caso essa regra esteja inserida no arquivo hosts.deny, toda abertura de conexão proveniente de computadores cujo endereço IP seja traduzido para algum nome do domínio outrodominio.com.br, será negada.

Embora a utilização de nomes seja adequada e muitas vezes mais prática que os endereços IP, é preciso estar seguro de que o computador onde você inseriu regras baseadas em nomes consegue, de alguma maneira, traduzir os nomes utilizados para os endereços IP correspondentes.

Boas dicas para a criação de regras

Em geral, existem duas abordagens comuns para a elaboração de regras para controle de acesso a serviços: por padrão, tudo é proibido ou permitido. O primeiro caso consiste na solução que traz, na maioria das vezes, maior nível de segurança. Entretanto, será necessário investir um pouco mais de tempo para liberar os serviços necessários para os clientes válidos. Para implementar essa política no TCP Wrappers, basta inserir uma regra genérica no arquivo hosts.deny proibindo o acesso de qualquer cliente ao serviço SSH, por exemplo:

```
sshd: ALL
```

Nesse caso, uma vez que o arquivo hosts.allow é analisado primeiro, somente os clientes identificados explicitamente nesse arquivo para o SSH terão permissão para acessar esse serviço. Por exemplo, considerando que seu arquivo hosts.deny esteja com a regra genérica apresentada anteriormente, para liberar os clientes 192.168.1.100 e

```
jansen@smeagol: ~
Arquivo  Editar  Ver  Terminal  Abas  Ajuda
jansen@smeagol:~$ ssh jansen@192.168.1.101
ssh_exchange_identification: Connection closed by remote host
jansen@smeagol:~$
```

F6. Acesso SSH agora é negado.

192.168.1.102 no computador scadufax, basta inserir no seu arquivo hosts.allow a seguinte regra:

```
sshd: 192.168.1.100 192.168.1.102
```

A segunda política para geração de regras consiste em liberar todo tipo de conexão e proibir somente algumas. Desta forma, basta deixar o arquivo hosts.allow vazio e inserir no arquivo hosts.deny os serviços e os respectivos clientes que serão proibidos de acessá-lo. Somente uma observação: não insira algo do tipo "sshd: ALL" no arquivo hosts.allow para implementar essa segunda política. Lembre-se de que o arquivo hosts.allow é analisado primeiro e uma regra dessas nesse arquivo irá invalidar toda e qualquer regra que possa ser inserida no arquivo hosts.deny para o serviço SSH, por exemplo.

Uma última observação

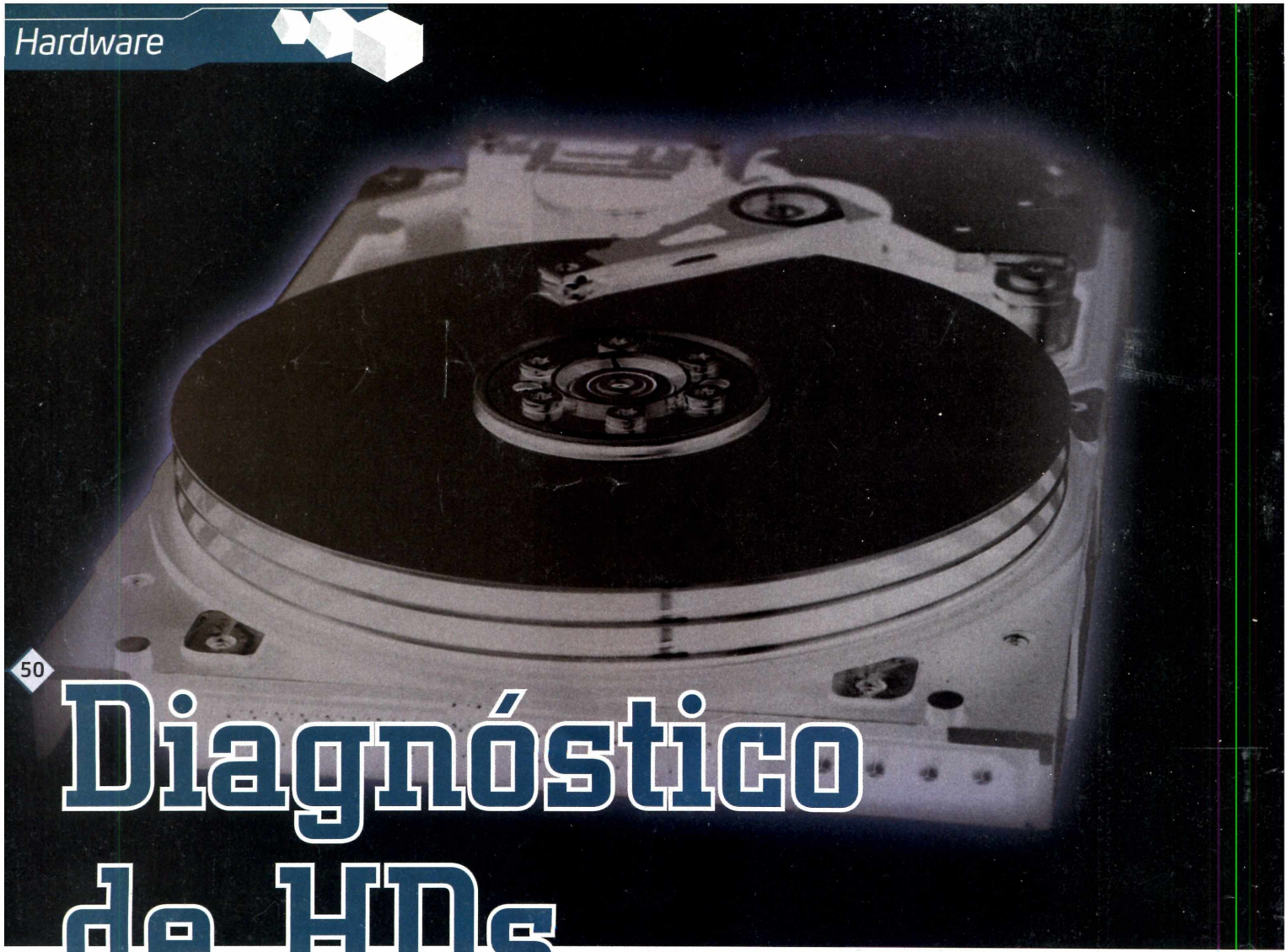
As regras inseridas nos arquivos hosts.allow e hosts.deny são consultadas todas as vezes que uma nova conexão é solicitada a um serviço compilado com suporte aos recursos do TCP Wrappers. Nesse caso, uma vez que as regras sejam inseridas, elas passam a valer imediatamente.

Conclusão

Utilizar os arquivos hosts.allow e hosts.deny representa uma solução rápida e simples para controlar o acesso aos serviços compilados com o suporte do TCP Wrappers, evitando a complexidade natural de outras ferramentas para controle de acesso, como é o caso do iptables. Por outro lado, mesmo considerando o fato de ser um recurso mais simples de ser utilizado, ainda assim é necessário dedicar alguma atenção para não cometer erros graves, conforme as discussões apresentadas no decorrer do texto.

Dependendo do tipo de cenário existente, o uso do iptables e de outras soluções pode ser mais adequado e a necessidade de entender bem a arquitetura TCP/IP e outros recursos pode ser inevitável. Entretanto, a solução correta a ser utilizada é aquela que mais se adequa às suas necessidades.

O mais importante é conhecer as soluções e recursos existentes para poder combiná-los de forma a gerar uma solução capaz de tornar o seu ambiente versátil e, principalmente, seguro. Até a próxima! **PC**



Diagnóstico de HDs

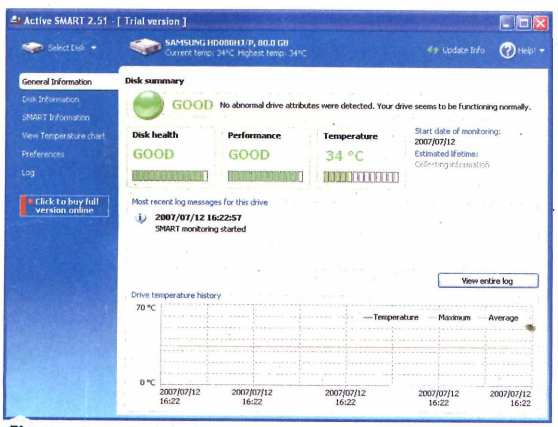
Prevenir é melhor do que remediar. Esta máxima que vale para tantas coisas encontra nos HDs uma razão especial de existir. Afinal de contas, nossos dados - e anos de vida muitas vezes - estão em jogo. Felizmente o que não faltam são softwares disponíveis para este fim, e nesta matéria você encontrará o que há de mais atual.



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

Active SMART 2.51

Além da nova interface gráfica, novos recursos foram adicionados à versão 2.51 do Active SMART (**www.ariolic.com/activesmart/**). A geração de gráficos, indicadores de temperatura, estado de "saúde" e temperatura do HD compõem o remodelado painel principal do software (figura 1). Esses indicadores são apenas um resumo da leitura dos índices do SMART (Self-Monitoring Analysis and Reporting Tecnology – Tecnologia de auto-monitoramento, análise e diagnóstico) realizada pelo Active SMART.

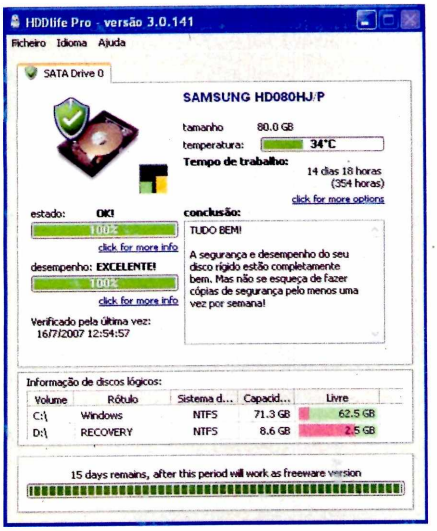


F1. Resultado final do Active SMART 2.51 em relação à versão 2.42 (avaliada na edição 62).

HDDlife Pro 3.0.141

Os bugs existentes desde a versão 2.8.96 com os drivers da controladora VIA VT8237 e VT6420 ainda continuam. Mas nem por isso a nova versão (3.0.141) do HDDlife (**www.hddlife.com**) fica devendo à anterior. O monitoramento em tempo real, exibido na tela principal do programa, traz como exclusividade um gráfico da taxa de leitura e escrita realizada no

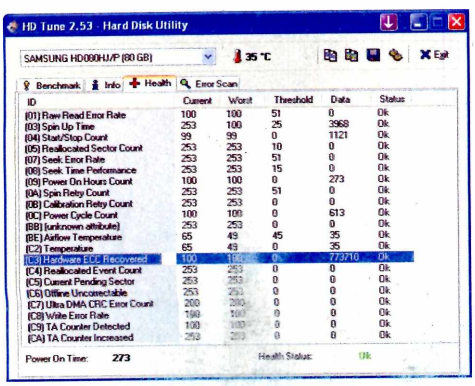
HD da máquina (figura 2). A qualidade e a simplicidade deste programa são os destaques.



F2. Interface gráfica de rápida análise sobre os estado de "saúde", performance e temperatura do HD. A barra na cor verde do gráfico significa a taxa de leitura e ao lado, na cor amarela, é informada a porcentagem da taxa de escrita no HD.

HD Tune 2.53

Apesar de atualizado para a versão 2.53, a única mudança realizada no HD Tune (**www.hdtune.com**) foi na tabela de descrição do SMART. Os demais recursos mantiveram o mesmo nível de funcionalidades em relação à versão anterior. Isto é, o benchmark, as informações detalhadas sobre o HD, a leitura dos índices do SMART e a verificação de blocos defeituosos no disco rígido, continuam fazendo parte do HD Tune (figura 3). O envio de e-mail com alerta de alta temperatura e baixa performance no HD ainda não foi implementado nesta versão. Quem sabe na próxima...



F3. Tela com os respectivos índices do SMART apresentados pelo HD Tune. Entretanto, o mesmo bug de leitura dos valores de temperatura e SMART ocorrem no HD Tune. Ou seja, quando o HD está sob o "comando" da controladora VIA VT8237 e VT6420, não é possível obter qualquer resultado.

Stellar Smart 2.2.1

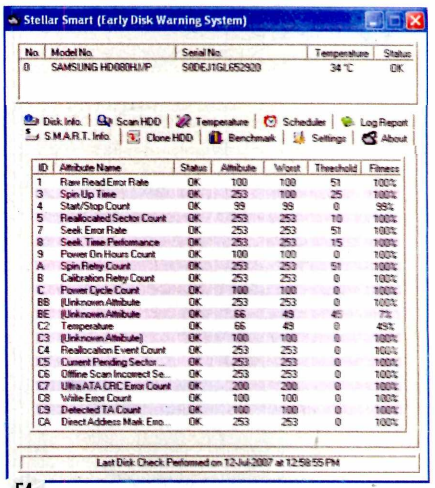
Caracterizado como um completo software de monitoramento de HDs, o Stellar Smart (**www.stellarinfo.com/hard-drive-monitor.htm**) encontra-se atualmente na versão 2.2.1. Seu diferencial está no recurso "Clone HDD", o qual, como o nome sugere, nos permite clonar qualquer HD instalado na máquina (figura 4).

Advanced SmartCheck 3.3

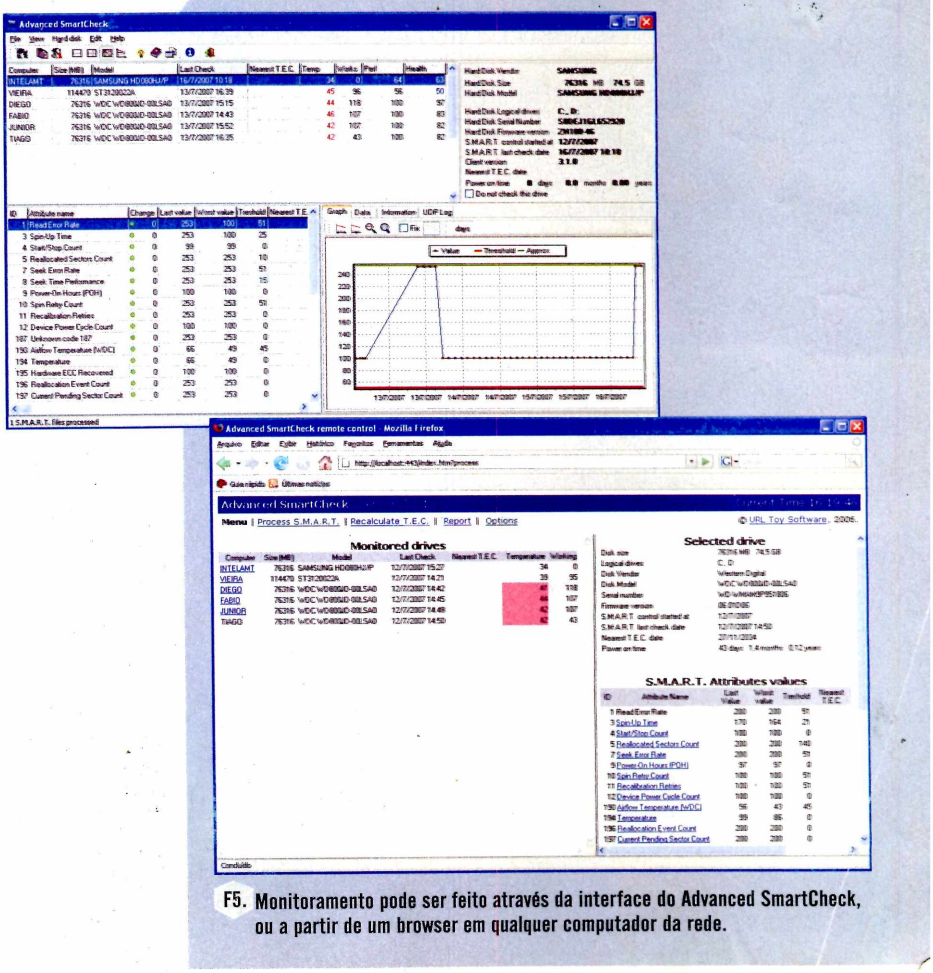
O Advanced SmartCheck (**http://www.urltoy.com/asc.htm**) é uma boa opção para máquinas em rede. Depois de instalado, ele é capaz de monitorar a temperatura e os parâmetros SMART da máquina local e de qualquer outra remota. Para isso, juntamente ao executável do Advanced SmartCheck é disponibilizado um arquivo de instalação dos agentes para as máquinas clientes. Enfim, podemos visualizar e monitorar os resultados de qualquer local da empresa (ou até fora dela) através de um navegador web. Basta abrir um browser e informar o IP da máquina onde o Advanced SmartCheck foi instalado (figura 5).

Conclusão

Tecnicamente, todos os programas apresentados são boas opções de trabalho. E, por este motivo, não são gratuitos (exceto o HD Tune, que é Freeware). Todos possuem versão Trial disponível para download nos sites dos respectivos desenvolvedores. E por fim, além de compatíveis com os tradicionais sistemas operacionais da Microsoft (Windows 98, ME, 2000, XP e 2003), todos também rodam no Vista. **PC**



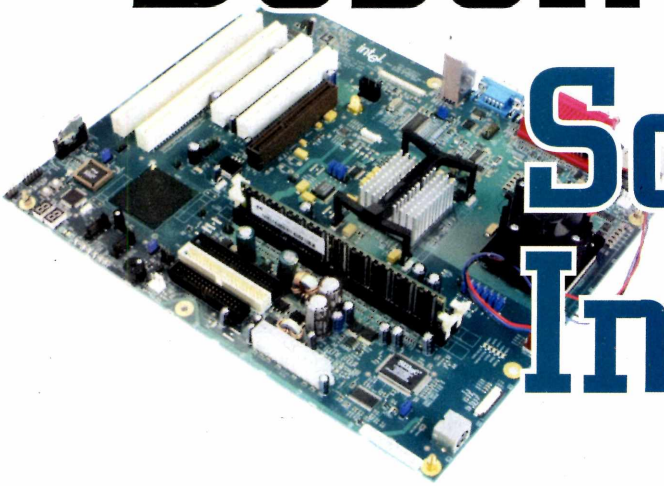
F4. Tela com o menu de opções do Stellar Smart 2.2.1.

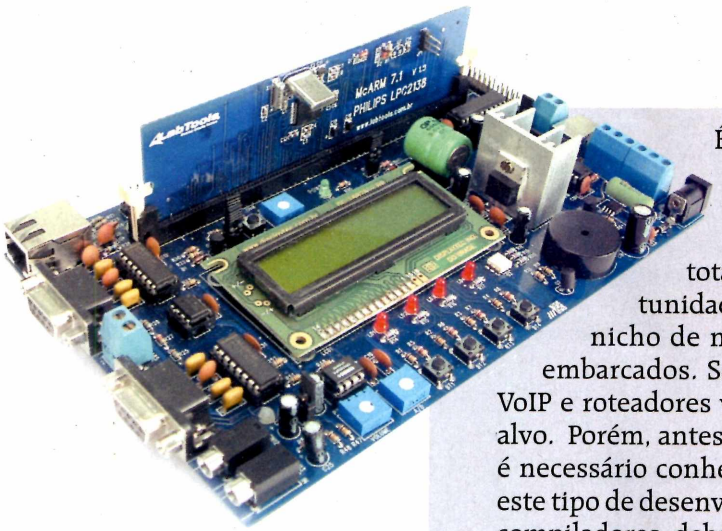


F5. Monitoramento pode ser feito através da interface do Advanced SmartCheck, ou a partir de um browser em qualquer computador da rede.

Desenvolvendo Soluções Integradas

Parte 1





É cada vez mais comum se ouvir falar em convergência de tecnologias, a qual é nada mais nada menos do que o direcionamento de novas soluções para padrões já disseminados e com processamento totalmente digital. Isso abre um grande leque de oportunidades para quem pretende explorar um interessante nicho de negócio, que é o desenvolvimento de hardwares embarcados. Set-top box para TV Digital, tráfego e controle de VoIP e roteadores wireless são apenas alguns exemplos de soluções alvo. Porém, antes de se iniciar qualquer uma destas oportunidades, é necessário conhecer as arquiteturas disponíveis no mercado para este tipo de desenvolvimento, bem como suas ferramentas, tais como compiladores, debuggers, analisadores, etc, e as principais características de cada uma delas, como velocidade, adaptabilidade, resistência, custo, além de outros fatores essenciais para realizar ótimos projetos e com isso alvejar grandes oportunidades.

Este artigo traz as primeiras informações sobre duas diferentes arquiteturas, X86 e ARM, e algumas instruções de como iniciar seus projetos para soluções integradas.



Adriano A. Góes

Formado em Engenharia Elétrica Telecomunicações, possui 10 anos de experiência em desenvolvimento de softwares e gestão de redes. Atualmente é membro do grupo de pesquisas avançadas em redes wireless da PUC Campinas.

Muito se comenta sobre tecnologias e soluções cada vez mais específicas em relação ao seu uso. Com isso é crescente a procura por profissionais especializados em sistemas embarcados. Isto porque trabalhar com este tipo de arquitetura não é uma tarefa simples e requer muito conhecimento e dedicação destes profissionais. Claro que, juntamente com a dificuldade, as pessoas que promovem soluções para os fins mais adversos são muito valorizadas no mercado atual.

Como veremos a seguir, os sistemas embarcados exigem mais processamento, memória e, com certeza, um profissional que consiga desenvolver soluções boas a um custo baixo. Por este motivo a PC&Cia traz este artigo, o primeiro de uma série que mostrará as informações essenciais para você se destacar neste nicho de mercado.

Sistemas embarcados

Sistemas Embarcados (Embedded Systems) são sistemas microprocessados capazes de realizar uma ou mais tarefas *específicas*,

com seus recursos computacionais projetados restritamente para este propósito especial.

Estima-se que em 2010, 90% dos sistemas existentes sejam Sistemas Embarcados, devido à grande busca de soluções específicas e de baixo custo, a fim de não desperdiçar poder de processamento ou memória em sistemas mais simplificados ou com um escopo de trabalho bem definido. Podemos citar como exemplos de Sistemas Embarcados:

- **Telefonia:** telefones celulares, centrais telefônicas;
- **Equipamentos de redes:** roteadores wireless, switches, firewalls;
- **Indústria Automobilística:** controladores do motor e de antibloqueio dos freios ABS;
- **Eletrodomésticos:** fornos microondas, máquinas de lavar, aparelhos de TV, DVD players;
- **Equipamentos médicos**
- **Video Games**
- **Palm Top's e PDA's**

Assim, para iniciar o estudo das ferramentas necessárias para se estruturar um Sistema Embarcado, faremos a seguir um estudo sobre as características e comparações entre dois microprocessadores e suas arquiteturas distintas: Arquitetura ARM (RISC) e Arquitetura X86 (CISC).

Arquitetura ARM (RISC)

Muito utilizada em Sistemas Embarcados de indústrias e em informática, a arquitetura ARM tem atualmente à disposição processadores de 32 bits capazes de atingir um ótimo desempenho em uma implementação simples, ocupar pouca área e ter baixo consumo de energia. Além disso, é uma estrutura muito conhecida pela sua versatilidade, já que possui poucas instruções para programação.

Características da arquitetura

Também denominada de Arquitetura Load-Store, tem como característica principal o fato de que as instruções somente processarão (soma, subtração, etc) valores que estiverem nos registradores e sempre armazenarão os resultados em algum registrador. Ela opera com instruções fixas de 32 bits de largura (com exceção das instruções Thumb compactas de 16 bits) alinhadas em 4 bytes consecutivos da memória, com execução condicional, com poderosas instruções de carga e armazenamento de múltiplos registradores, tem a capacidade de executar operações de deslocamento e na ULA (Unidade Lógica e Aritmética) com uma única instrução executada em um ciclo de clock. Consiste em 15 registradores de 32 bits para uso geral com manipulação de periféricos de I/O, tais como dispositivos mapeados na memória com suporte a interrupções.

Ao contrário da arquitetura CISC (Complex Instruction Set Computers), a RISC (Reduced Instruction Set Computers) é capaz de fazer várias operações em apenas um ciclo de máquina. Já a CISC, arquitetura X86, normalmente gasta alguns ciclos de máquina para executar uma operação. Ela resolve problemas complicados, porém gasta algumas voltas de seu relógio fazendo isso. Por este motivo o microprocessador ARM é muito mais rápido mesmo sendo mais simples.

Os microprocessadores RISC se caracterizam pela simplicidade de sua arquitetura interna, podendo ser construída com menor gasto de área, o que os tornam ideais para aplicações embarcadas. Isto implica em uma relação custo/desempenho bem melhor que a dos microprocessadores convencionais, que consomem mais área e, devido à complexidade de projeto, não conseguem acompanhar o último passo em termos de tecnologia de fabricação. Algumas outras características de projeto permitem que os microprocessadores RISC tenham um desempenho superior ao dos processadores convencionais:

1) Pipeline

A simplicidade das instruções do ARM, com formato fixo em 32 bits, permite uma arquitetura com alto nível de eficiência de "pipeline", ou seja, uma instrução é executada em várias etapas, como em uma linha de montagem: não se espera um produto ficar pronto para se iniciar a montagem do próximo. Com isso o resultado é uma produção muito maior. Com o microprocessador ARM, normalmente se divide a execução das instruções em 4 ou 5 etapas gerando aproximadamente uma instrução a cada ciclo de processador, tendo outras em execução em outras fases do "pipeline". Outros processadores possuem instruções de tamanhos variáveis e, portanto, apresentam maior complexidade, o que dificulta a elaboração de "pipelines" eficientes.

2) Arquitetura orientada a Registrador

Os microprocessadores ARM só possuem instruções que operam em dados que estejam nos seus registradores. As únicas operações de acesso à memória são as operações para carga e armazenamento destes registradores. Isto agiliza bastante as operações aritméticas, permitindo uma alta taxa de execução. A princípio poderíamos dizer que o microprocessador RISC necessita de mais instruções para fazer a mesma tarefa. Contudo, o compilador RISC procura alocar as variáveis nos registradores locais, o que compensa esta diferença ao longo da execução de um programa.

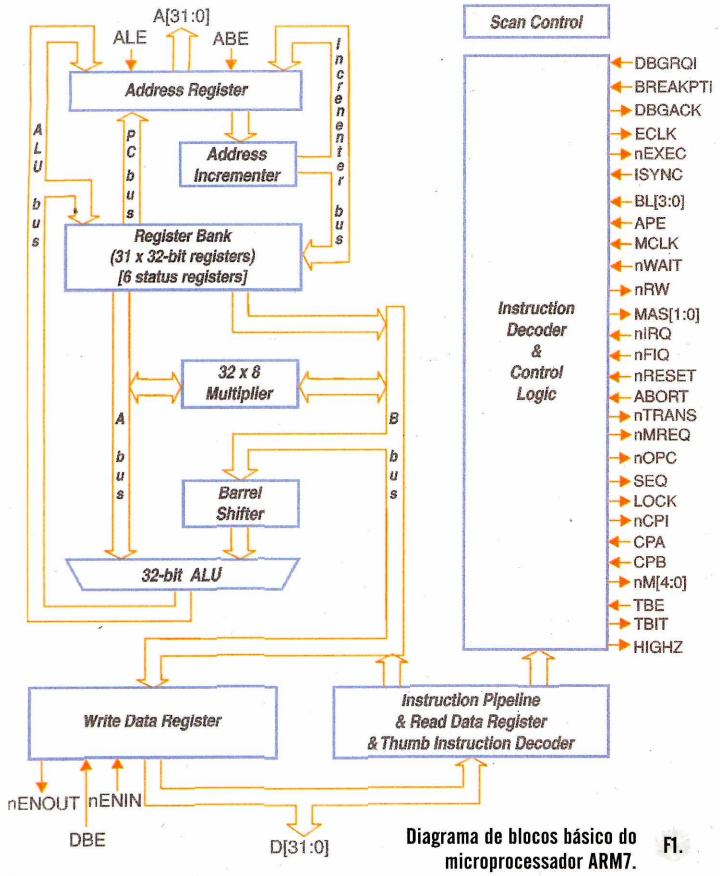
3) Tecnologia de fabricação

Os microprocessadores ARM necessitam de certas características em sua fabricação para que possam ter um bom desempenho. Algumas delas são descritas a seguir:

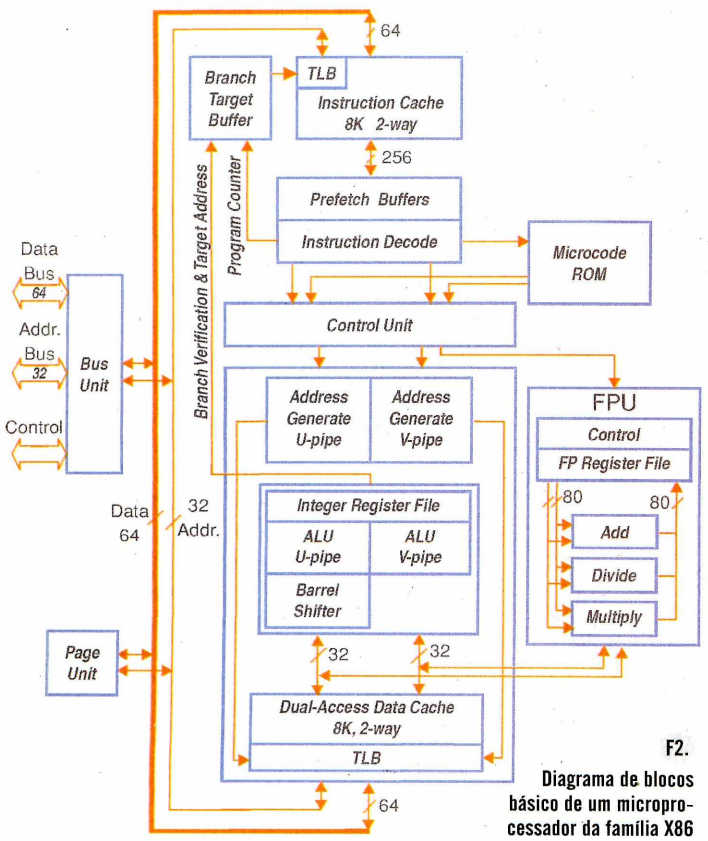
- *Taxa de operação:* Por buscarem praticamente uma instrução a cada ciclo da memória, os microprocessadores RISC precisam ter uma banda passante bastante larga para o acesso à memória. Com ciclos na ordem de 20 a 40 MHz (existem ARM's que vão até 1 GHz, mas aqui estamos considerando projetos embarcados simples e de baixo custo, a exemplo do LPC2138FBD64-S ARM7 da NXP), esta banda passante só pode ser conseguida com o uso de cache de instruções.
- *Compiladores:* Como o conjunto de instruções é bastante simples, a eficiência com que um programa é executado vai depender do código gerado pelo compilador. Existe um questionamento muito grande em relação ao tamanho do código gerado pelos compiladores ARM. Levantamentos indicam que o tamanho total do código de um programa escrito em linguagem C é apenas 25% maior nos microprocessadores ARM do que em outros processadores.
- *Sistema Operacional:* Os sistemas operacionais largamente utilizados nos sistemas elaborados com estes processadores são os

Microprocessador x Microcontrolador

Os microprocessadores nasceram antes e foram desenvolvidos unicamente com o intuito de serem programáveis, ou seja, processar um software. Já os microcontroladores surgiram da necessidade de serem "partes integrantes" de um circuito, ou seja, um software para controlar um circuito. Para isto, os microcontroladores dispõem de um certo número de PORTAS (conjunto de pinos do CI) que podem ser utilizadas como ENTRADA ou SAÍDA de dados.



F1. Diagrama de blocos básico do microprocessador ARM7.



F2. Diagrama de blocos básico de um microprocessador da família X86

UNIX, LINUX, FreeBSD e seus semelhantes. Aliás, o sucesso dos microprocessadores ARM se deve em grande parte à existência de um sistema operacional aberto e portável. Na linha de pesquisa existe um esforço muito grande, em que se destacam a Motorola e a SUN na elaboração de padrões de interfaces binárias para as aplicações. Este tipo de padrão, juntamente com as interfaces de usuário padronizadas, como o MOTIF, permitiria aos aplicativos executar sem necessidade de re-compilação em plataformas de "hardware" com arquiteturas distintas, desde que utilizem um mesmo tipo de processador ARM. Esta seria uma forma de superar o gargalo atual destes sistemas, que é a demanda cada vez maior por aplicativos.

• *Aplicações e mercado*: Os microprocessadores ARM têm uma variação muito grande em relação à velocidade do "clock", partindo de 16/20 MHz até 40 MHz. Com isto uma ampla gama de aplicações é obtida mantendo-se compatibilidade binária dentro de uma mesma família. Possuem também aplicações em sistemas que exijam alta capacidade de processamento, tais como processamento gráfico e de imagem em terminais gráficos e impressoras laser. As versões mais avançadas exploram o paralelismo de instruções, permitindo a execução de mais de uma instrução em cada ciclo de processador (figura 1).

Arquitetura X86 (CISC)

Um processador baseado no projeto CISC tem como base muitas instruções (para cálculos e parâmetros de I/O, por exemplo) embutidas dentro da própria CPU. Logo, um programa pode recuar e deixar a CPU realizar muitas instruções exigidas para uma função específica. Os processadores da família X86 seguem este conceito.

Na arquitetura CISC as instruções de máquina possuem maior complexidade e, por este motivo, se aproximam em definição dos comandos da linguagem de alto nível, o que reduz o consumo de memória com reflexos no custo do sistema. As máquinas com arquitetura CISC executam mais rapidamente os programas escritos em linguagem de alto nível devido à pequena quantidade de códigos binários executáveis.

Porém, isto a conduz a algumas desvantagens, tais como:

- Menor uso de memória na execução de funções;
- Maior quantidade de modos de endereçamento;
- Tempo de decodificação de instruções muito alto.

De fato, a perda de desempenho durante a decodificação, que é quando ocorre a "quebra" deste grande conjunto de instruções em instruções menores, é de menos de 1%. É por este motivo que se justifica a perda de desempenho em detrimento do ganho de flexibilidade. Entretanto, o processador X86 paga um preço relativamente alto por este conjunto de instruções uniformes.

Para minimizar estes efeitos utiliza-se o conceito denominado Microcódigo (Microcode, veremos adiante),

operando de forma que as instruções simples possam ser diretamente processadas. De fato, um programa atual típico é composto por algo em torno de 95 a 97% destas instruções simples. O restante são as instruções complexas que, apesar de raramente usadas, são as que dão mais trabalho, pois precisam passar por um processo de decodificação muito mais lento (figura 2).

Família ARX x X86

A diferença dos processadores ARM para os X86 geralmente usados em PCs é que os ARM são projetados para terem consumo mínimo de energia, baixo aquecimento e sem desperdiçar poder de processamento. Isto porque, conforme dissemos anteriormente, os processadores ARM possuem uma arquitetura muito mais simples que os processadores X86. Os X86 possuem vários estágios para processamento, ou seja, enquanto uma parte carrega uma instrução na memória, outra parte processa os dados que essa instrução vai receber, outra aloca memória cache para receber a saída, outra prevê os dados que essa instrução vai precisar para ser concluída, etc, até juntar todo mundo e dar o resultado. Possuem também um programa interno (microcódigo) que implementa as instruções, permitindo que as mesmas possam ser melhoradas pelo fabricante, por exemplo. Tudo isso torna o X86 muito rápido e eficiente, porém faz com que ele gaste mais espaço físico (para a memória do microcódigo, por exemplo) e consuma mais energia.

Já os processadores ARM não possuem esse microcódigo, possuem menos estágios de processamento (em geral 3 a 8, contra de 10 a 31 nos X86), entre outras simplificações. Mas para compensar a perda de desempenho gerada pela simplificação da arquitetura, os processadores ARM possuem algumas soluções que tornam a execução dos códigos mais eficiente. O conjunto de instruções, por exemplo, é capaz de processar, em certos casos, mais dados por instrução, conforme vimos anteriormente. Por exemplo: Você quer comparar os valores A e B, e se A for menor que B, somar 1 em A. Num X86, você usaria uma instrução para comparar e outra instrução para somar. No ARM existem instruções condicionais, ou seja, tarefas com a comparação já embutida.

No nosso exemplo, faríamos algo assim: SomarSeForMaior A com B, após a inicialização da comparação, ou seja, a comparação e a soma estão unidas em uma única instrução. Isso torna o código mais "denso", com instruções que desempenham mais de uma função ao mesmo tempo.

Utilização do microcódigo

Para soluções embarcadas, muito se fala sobre a utilização do chamado "microcódigo". Esta solução opera de forma que as instruções podem ser fisicamente conectadas a um chip de modo que uma seqüência de bits de instrução execute diretamente a instrução desejada. O resultado disso é que as instruções podem ser executadas em velocidades muito maiores. Por outro lado, a complexidade de um microprocessador com instruções fisicamente conectadas aumenta muito à medida que mais instruções são incluídas. Os projetos mais práticos têm conjuntos de instruções menores.

Sabe-se que a maior parte do trabalho realizado pelos processadores envolve poucas instruções. Por exemplo, em um computador com um conjunto de 200 instruções, dois terços de seu processamento envolve a utilização de mais ou menos 10 instruções. Com isso, podemos dizer que freqüentemente isto se resume à regra do 80/20, em que aproximadamente 20% das instruções de um computador fazem 80% do trabalho.

ARM - RISC (reduced Instruction Set Computers)	X86 - CISC (Complex Instruction Set Computers)
Instruções simples executadas em apenas 1 ciclo	Instruções complexas executadas em vários ciclos
Referências à memória só com LOAD/STORE	Qualquer instrução pode referenciar a memória
Instruções executadas por hardware	Instruções interpretadas pelo microcódigo
Instruções com formato fixo	Instruções com formato variável
Poucas instruções com menos modos de endereçamento	Muitas instruções com muitos modos de enderaçamento
A complexidade está no compilador	A complexidade está no microcódigo
Vários conjuntos de registradores	Um único conjunto de registradores

Resumo das diferenças básicas entre os processadores ARM e X86. T1.

Não há uma linha exata demarcando os limites de complexidade no projeto de um chip e a redução possível em termos de complexidade com os projetos RISC. Por exemplo, o microprocessador RISC M/200, produzido pela Mips Computer Systems, possui um conjunto completo de 115 instruções. O 386 da Intel, que é um antigo microprocessador CISC, possui nada menos que 144 instruções. Ao caracterizar um RISC ou um CISC, o mais importante não é o número de instruções que o computador ou um microprocessador pode entender, mas sim a forma como essas instruções são executadas. Reduzir o conjunto das instruções de um computador é apenas uma das estratégias utilizadas para agilizar seu processamento. À medida que o número de instruções é reduzido, todas as outras deficiências que interferem em seu desempenho também são reduzidas e o que permanece é capaz de oferecer a menor resistência possível à passagem dos dados.

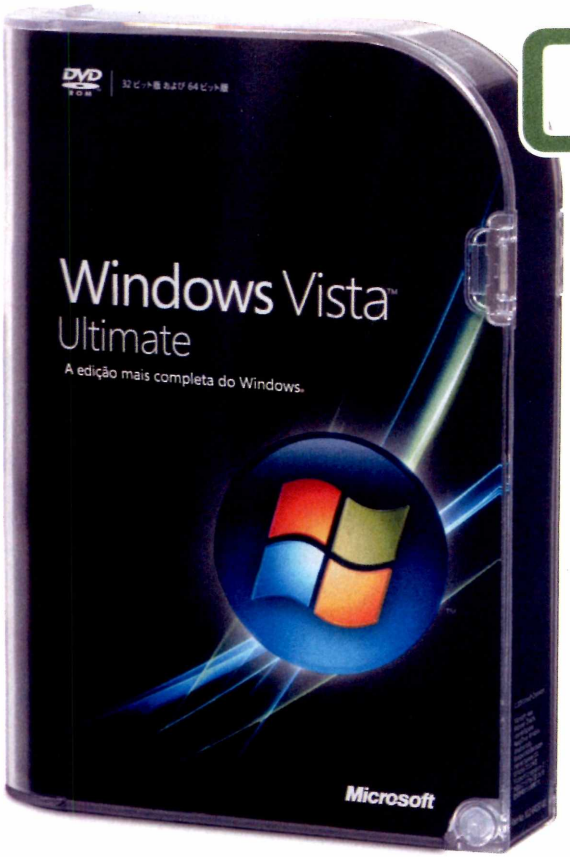
As características mais marcantes da filosofia RISC são a eliminação do microcódigo, a ênfase na agilidade das instruções mais usadas pelo computador, o relacionamento mais estreito entre a máquina e o projeto otimizado de compilador (linguagem de programação). Os projetos RISC exploram técnicas de memória rápida como o Cache e o Pipeline. As próprias instruções RISC são mais centralizadas, cada uma é projetada para realizar uma única função. E as instruções são mais uniformes, modo que todas têm o mesmo tamanho e trabalham de forma semelhante.

Com tudo que vimos, a tabela 1 traz um resumo das principais características essenciais na escolha do microprocessador a ser utilizado em seu projeto.

Conclusão

Mostramos neste primeiro artigo de forma totalmente imparcial as diferenças entre as duas arquiteturas de microprocessadores mais existentes no mercado. Com o que apresentamos você conseguirá escolher com mais precisão qual destas arquiteturas melhor se encaixa em seu projeto.

Nos próximos artigos desta série entraremos mais a fundo nos compiladores e *debuggers*, trazendo as diferenças e vantagens de cada um deles, juntamente com a orientação de como escrever o mesmo escopo de programa para ambas as arquiteturas. **PC**



Certificação Microsoft MCTS

Nesta edição, iniciaremos uma série de matérias preparatórias para o exame 70-620: configurando o Windows Vista. Ao final você deverá estar muito próximo de obter a certificação Microsoft Certified Technology Specialist (MCTS) e com isso ficar em melhores condições para atuar no mercado.

Igor Humberto e Paulo Sant'anna

A questão da necessidade de qualificação dos profissionais de TI no país é um tema freqüente aqui na revista. Temos um mercado de trabalho acirrado, porém com muitas oportunidades para os bem preparados. Neste cenário, o profissional que obtém algumas das certificações técnicas existentes demonstra estar em constante atualização e, de certa forma, parte na frente em disputas por novas oportunidades. Um título de certificação não garante emprego a ninguém. Porém, associado a uma boa experiência e à formação técnica ou superior, pode proporcionar uma ótima colocação no mercado.

Seguindo nessa linha, as certificações oferecidas pela Microsoft possuem ampla aceitação pelo mercado, até mesmo devido à abrangência de suas soluções em todo o mundo. De fato, siglas como MCP, MCSA e MCSE, que correspondem a algumas das categorias de certificação, são comuns em ofertas de emprego e em propagandas de centros de treinamento.

No ano passado, após realizar algumas pesquisas que apontaram uma maior demanda por certificações mais específicas, a Microsoft criou novas categorias de certificações. Com o objetivo de facilitar a identificação das qualificações do profissional em produtos ou tecnologias, foi criada então a MCTS com enfoque no Windows Vista.

É importante ressaltar que a publicação desta série de matérias não visa a garantir a aprovação, até porque vários fatores podem e devem influenciar no momento do exame, tal como a experiência no sistema ou alguma modificação feita pela Microsoft, por exemplo.

Visão Geral do exame 70-620

Este exame é voltado para profissionais de suporte que a Microsoft chama de nível 1 e 2, que são os técnicos e analistas de suporte que atuam no mercado de forma autônoma ou em equipes de help-desk e suporte em empresas. Não se trata de um exame complicado, principalmente para aqueles que já conhecem bem o sistema. Com relação ao idioma, procuramos fazer sempre em inglês devido às traduções de termos técnicos, mas para quem desejar também é possível optar pelo Português. O conteúdo exigido pela Microsoft pode ser visto em **www.microsoft.com/learning/exams/70-620.mspx**.

A inscrição para o exame pode ser feita em um dos dois órgãos credenciados para a aplicação das provas, que são o VUE (**www.vue.com**) e o Prometric (www.prometric.com). Atualmente um exame custa 80 dólares, porém fique atento, pois a Microsoft e Centros de Treinamento costumam realizar promoções.

O exame não possui um formato estático, aliás, pode inclusive ser adaptativo. Podemos ver algumas questões com cenários, exibições, múltipla escolha com uma ou mais opções corretas, e também do tipo drag-and-drop (arrastar e soltar). O bom é estar preparado para não ser pego de surpresa. O conhecimento do sistema é muito importante, pois no exame são exibidas telas onde podem ser feitas configurações. Para ser aprovado, é preciso acertar pelo menos 70% das questões. Agora vamos ao conteúdo.

Planejamento da instalação

Um dos pontos que serão cobrados no exame é a sua habilidade em implantar o Windows Vista no computador, seja ele doméstico ou em ambiente corporativo. Sendo assim, é necessário que você saiba

identificar corretamente quais os requisitos de hardware necessários para cada edição do Vista. Além disso, você precisa pensar também no nível de experiência que o usuário terá com o sistema.

Níveis de experiência

São quatro os níveis de experiência definidos pela Microsoft e que podem ser usados no Vista:

- Basic: nesse nível o sistema apresenta a menor quantidade de recursos visuais. O usuário poderá contar apenas com o novo estilo do menu Iniciar e Windows Explorer, sistema de busca integrada com a Área de trabalho e a Central de compartilhamento e rede. Esse nível de experiência está disponível em qualquer edição do Vista;
- Classic: para entender esse nível de experiência, você deve somar o nível básico com o visual do Windows 2000. Este nível também está disponível em todos as edições do Vista;
- Standard: digamos que nesse nível o Vista fica mais "bonito". Aqui você tem uma soma dos dois níveis de experiência citados anteriormente, além de poder contar com alguns dos recursos visuais oferecidos pelas placas de vídeo que possuem um driver no formato WDDM (Windows Driver Display Model). Esse nível de experiência não está disponível na versão SE (Starter Edition) do Vista;
- Windows Aero: esse é o último nível de experiência disponível, o qual reúne todas as novidades visuais do sistema (Flip de janelas em 3D, visual da janela em vidro etc). Só está disponível nas edições Home Premium, Business, Enterprise e Ultimate.

Requisitos de hardware

A tabela 1 exibe esses requisitos em três colunas: Mínimo, Vista Capable e Premium Ready. Essas três colunas correspondem, basicamente, aos níveis de experiência citados anteriormente. Sendo assim, podemos dizer que a coluna "Mínimo" corresponde ao que é necessário usar para ter o nível de experiência Basic e Classic; o requisito de hardware apresentado na coluna Vista Capable é o adequado para o nível de experiência Standard; por último, vemos a coluna Premium Ready, a qual apresenta os requisitos de hardware(e alguns detalhes de software) necessários para trabalhar com o nível de experiência Windows Aero.

Além de verificar se o sistema atende aos requisitos de hardware e de software necessários para que o nível de experiência desejado seja alcançado com o Windows Vista, também é necessário checar se existe compatibilidade de drivers e de aplicativos. Imagine só descobrir que aquela versão de anti-vírus não funciona, ou que não há driver para a impressora, somente após a instalação do sistema.

	Mínimo	Vista Capable	Premium Ready
CPU	800 MHz	800 MHz	1 GHz
RAM	512 MB	512 MB	1 GB
GPU	SVGA	DirectX 9	Aero Capable*
Memória de vídeo	-	-	128 MB
Espaço em disco usado	20 GB	20 GB	40 GB
Espaço livre	15 GB	15 GB	15 GB
Unidade óptica	CD	CD	DVD

T1. Por Aero Capable entenda como sendo uma placa de vídeo com suporte ao DirectX 9, Pixel Shader 2.0 e profundidade de cores de 32 bits.



F1. Interface inicial durante instalação do Vista

Tipos de instalação

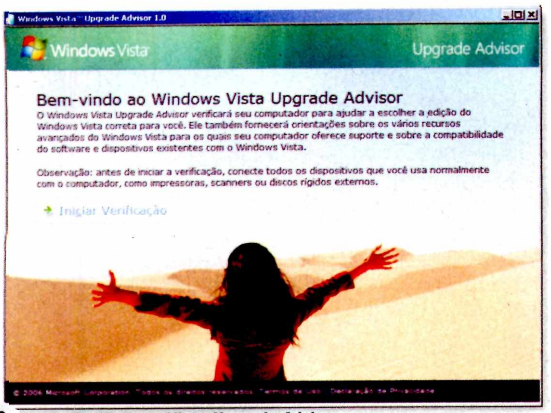
O Windows Vista pode ser instalado basicamente de três maneiras:

- Instalação limpa: ou seja, instalar o sistema em um disco vazio, zerado. Também pode ser considerada uma instalação limpa aquela em que você irá substituir completamente o sistema operacional existente;
- Upgrade: é feita quando queremos atualizar o Windows existente para o Vista. Somente as versões 2000, XP e Vista podem ser atualizadas para o Vista. A Microsoft recomenda o backup dos dados antes de realizar esse procedimento;
- Migração: às vezes esse procedimento é confundido com o Upgrade, mas trata-se de um procedimento diferente (em parte, apenas). Entende-se por migração o processo de levar (migrar) os dados de um usuário de um sistema que esteja executando o Windows Vista para outro computador, também executando o Windows Vista. Uma migração acontece sempre que executamos um dos seguintes procedimentos: Backup e restauração dos arquivos e configurações do usuário; realizamos uma instalação limpa ou upgrade (isso pode ser feito sem necessariamente formatar a unidade); reinstalação de aplicações.

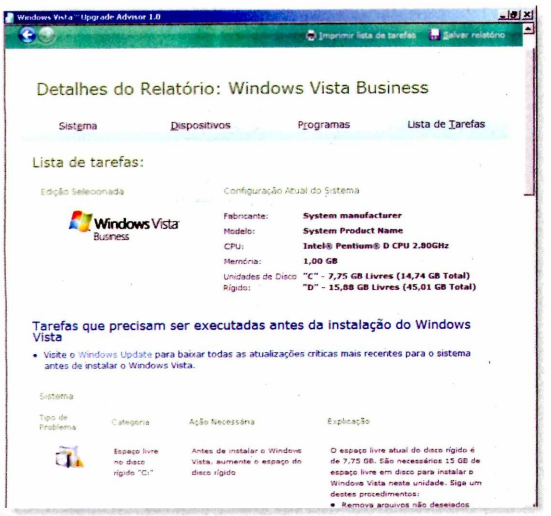
Realizando uma instalação limpa

A Microsoft inovou bastante no que diz respeito ao processo de instalação do Windows Vista. Tanto é verdade que acabou rendendo uma matéria publicada em nossa edição 71 (Junho/2007). Sendo assim, falaremos brevemente sobre os recursos para poder executar esse procedimento. Você pode instalar o Windows Vista das seguintes formas:

- Instalação a partir do DVD: Para fazer isso você deve inserir o DVD de instalação do sistema na unidade, iniciar o computador e seguir as instruções do assistente (figura 1);
- Instalação a partir de um compartilhamento: Inicie o sistema a partir do Windows PE, ou então via software PXE da placa de rede. Você terá duas opções aqui: acessar um compartilhamento na rede que possua o Programa de instalação do sistema, ou então contatar um servidor WDS. No último caso, você precisará de uma infra-estrutura mais complexa, apesar do número de recursos disponíveis também ser maior.
  Se você acessar um compartilhamento, basta executar o arquivo SETUP.EXE para começar. Agora, se decidir iniciar a partir do software PXE, um servidor WDS disponível deverá responder e o processo de instalação terá início de forma automática;
- Instalação usando um arquivo de respostas: Crie um arquivo de respostas (AUTOUNATTEND.XML) usando o Windows SIM. O arquivo resultante pode ser salvo em uma mídia removível, tal como um disquete ou Pen Drive. Insira a mídia removível no computador que deseja instalar e o DVD de instalação do sistema na unidade. Após iniciar o computador, o Programa de instalação do Windows Vista irá detectar automaticamente o arquivo de respostas;
- Implementação usando a ferramenta



F2. Início do Windows Vista Upgrade Advisor.



F3. Identificada a versão adequada para a máquina - Windows Vista Business.

- ImageX: Primeiro é necessário preparar um computador modelo. Logo após, inicie o sistema com o Windows PE para, através da ferramenta ImageX, você poder capturar uma imagem do sistema e salvá-la em um compartilhamento da rede. Essa ferramenta também é a mesma que será usada para fazer a implantação da imagem no sistema destino. Inicie o computador destino usando o Windows PE. Use a ferramenta de linha de comando Diskpart para criar uma partição que atenda aos requisitos mínimos de instalação citados na tabela 1. Use o ImageX para implantar a imagem.

Após a instalação, o procedimento a ser adotado é o mesmo de outras versões do Windows. Ou seja, é importante que se faça ajustes finais, tais como atualizar os drivers ou então instalar os drivers dos dispositivos não suportados nativamente pelo Vista. Esse procedimento pode ser executado através do Gerenciador de dispositivos, contforme veremos mais à frente.

Instalação do Vista

Upgrade / Migração para o Vista

O exame também poderá lhe cobrar conhecimentos sobre a migração segura para o Vista. A palavra "segura" neste caso deve ser entendida como "sem perda de informações e configurações do usuário". A Microsoft disponibiliza algumas ferramentas que visam a ajudar nessa empreitada:

- Windows Easy Transfer (WET): possibilita a migração dos arquivos do usuário e de suas respectivas configurações. Por ser bem simples, você pode usá-la para migrar configurações de uma ou apenas algumas máquinas. Normalmente essa ferramenta é usada quando os dados serão transferidos para um sistema que já esteja executando o Windows Vista. O WET permite que os dados sejam transferidos para um compartilhamento na rede, usando uma mídia removível (Pen drive), ou ainda um CD/DVD gravável;
- USMT 3.0: o User State Migration Tool foi projetado para ambientes que demandem a migração de uma quantidade grande de sistemas, pois possui recursos para automatizar o processo. Ele pode ser usado tanto para transferir dados para outros computadores, quanto para fazer um upgrade no próprio sistema, garantindo que os dados e configurações não serão perdidos. Essa ferramenta executa basicamente duas operações: na primeira, as configurações e arquivos do usuário são transferidos para uma mídia, tal como um compartilhamento na rede; na segunda, essas informações são restauradas no sistema destino.

Uma observação importante a se fazer nesse momento é que essas duas ferramentas são suportadas somente para uso com o Windows 2000, XP e Vista. Em versões anteriores, tais como Windows 9x e Windows NT, você pode fazer uma instalação limpa e depois, manualmente, migrar os arquivos e configurações do usuário.

Migrar para qual edição do Vista?

Como o Vista possui várias versões, a Microsoft desenvolveu uma ferramenta denominada Windows Vista Upgrade Advisor para auxiliar o usuário durante a migração (figura 2). Esse programa analisa se o sistema poderá apresentar problemas com compatibilidade de hardware (devido a drivers, por exemplo) e também com os aplicativos, e se atende aos requisitos mínimos de instalação.

Para instalá-lo, é necessário que o MSXML 6.0 e o .NET Framework estejam instalados no sistema. Todos esses pacotes de software podem ser baixados do site **www.microsoft.com/downloads**. Detalhe: em relação ao .NET Framework, não adianta ter a versão 3.0 instalada, pois ela não é a cumulativa. Você deve ter a versão 2.0.

Por fim, antes de usar o Upgrade Advisor, verifique se todos os dispositivos, tais como câmeras digitais, Pen drives etc, estão conectados para que possam ser submetidos à análise. Quando a análise termina, um relatório indica se o sistema atende aos requisitos mínimos de instalação, aponta a edição do Vista mais adequada e uma relação dos dispositivos suportados e não suportados (figura 3). O mesmo tipo de informação é exibido para as aplicações instaladas, ou seja, você saberá o que deve ou não funcionar depois que o Vista for instalado.

Além do Upgrade Advisor, a Microsoft oferece outras duas ferramentas para análise de compatibilidade entre o sistema e os aplicativos. A primeira, Standard User Analyzer Tool, funciona como um monitor de comportamento de aplicativo. Com ela instalada, você deve executar a aplicação suspeita e realizar algumas operações rotineiras. Ao terminar, a ferramenta exibirá um relatório de compatibilidade. A segunda, denominada Application Compatibility Toolkit, também analisará o sistema para determinar quais aplicações podem não funcionar corretamente no Windows Vista.

Resumo para a migração

Depois do que foi dito até aqui, podemos concluir que a migração e/ou atualização para o Vista requer os seguintes passos:

1) Fazer o backup dos dados do(s) usuário(s) usando o WET ou o USMT;
2) Instalar o Vista;
3) Fazer as atualizações de segurança e de drivers;
4) Se for necessário, fazer a instalação das aplicações (alguns programas podem

exigir uma reinstalação);
5) Restaurar os dados e configurações que foram salvos com o WET ou USMT.

Resolução de problemas

O instalador do Windows vem sendo aprimorado a cada versão, porém alguns problemas podem ocorrer durante o processo. A dica para garantir que eles não surjam é ter a certeza de que todos os componentes de hardware são compatíveis com o sistema e atendem aos requisitos mínimos para a instalação. Com essa atitude diminuímos a probabilidade da instalação ser interrompida. Pode ser utilizado o Windows Vista Upgrade Advisor, no caso de uma máquina com XP sendo migrada para o Vista. Ou então, caso seja feita uma instalação limpa, consulte o Windows Catalog (**http://winqual.microsoft.com/hcl**) para fazer a verificação dos dispositivos.

Se ocorrer algum problema, anote a mensagem de erro exibida e procure alguma explicação para o ocorrido na base de conhecimento (KB) da Microsoft - **http://support.microsoft.com/windowsvista**. Também poderá acontecer problemas com a mídia (DVD) utilizada, com alguma falha na cópia de arquivos. Sendo assim, teste a mídia em outra máquina e solicite outra, caso seja constatado o defeito.

Verifique também se existe uma versão atualizada do BIOS da placa-mãe. Em nosso laboratório, muitos problemas de travamento durante a instalação foram resolvidos após uma simples atualização do BIOS.

Instalação e configuração de drivers

Instalar e configurar drivers faz parte do cotidiano de todo técnico. Atenção especial deve ser dada em relação aos dispositivos antigos. Partindo do princípio que verificamos a compatibilidade dos dispositivos com o Vista antes da instalação, não devemos ter surpresas. Portanto, não deixe de utilizar o Windows Vista Upgrade Advisor. Porém, vale ressaltar que os drivers instalados por padrão com o Vista garantem apenas a estabilidade do sistema. Em outras palavras, se você quiser tirar todo o proveito do seu dispositivo, é necessário instalar os drivers específicos para o mesmo. Sendo assim, é imprescindível uma visita ao site dos fabricantes.

Outro ponto que vale ressaltar - mais como uma observação específica para o exame de certificação - é que você pode buscar drivers mais recentes para os seus dispositivos no site Windows Update. Na prática, contudo, poucos drivers atualizados podem ser encontrados ali, o melhor mesmo é ir ao site do fabricante do dispositivo.

Drivers de dispositivos

Software que faz a comunicação entre o dispositivo de hardware e o sistema operacional. Na instalação do sistema, ou após a inclusão de um novo dispositivo na máquina, o Windows Vista reconhece o novo hardware e instala um driver automaticamente, através do recurso Plug and Play (existente desde o Windows 98). Esse driver possui uma assinatura digital garantindo que foram feitos testes de compatibilidade e o mesmo se demonstrou confiável e estável.

Isso evidentemente só será feito se o driver para o dispositivo em questão já fizer parte da biblioteca do sistema. Se este não for o caso, temos três opções de instalação:

- Fornecido junto do dispositivo de hardware em um CD ou disquete;
- Download a partir do site Windows
- Update;
- Download do site do fabricante do hardware.

Gerenciador de dispositivos (Device Manager)

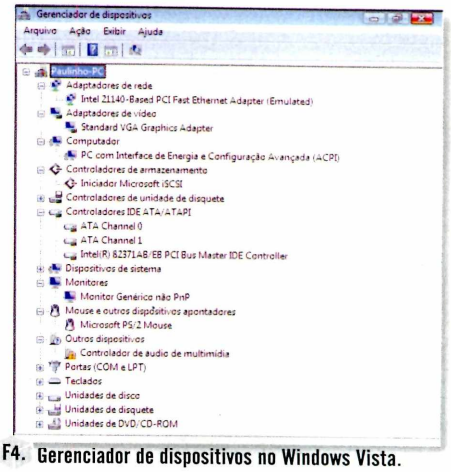
Ferramenta para o gerenciamento e configuração dos dispositivos de hardware identificados pelo sistema operacional (figura 4). Através dele, podemos realizar as seguintes tarefas:

- Visualizar os dispositivos de hardware instalados no sistema operacional;
- Desinstalar um dispositivo;
- Habilitar ou desabilitar um dispositivo;
- Atualizar drivers de dispositivo;
- Após a instalação de um driver defeituoso, retornar para o driver antigo (Roll
- Back) - figura 5.

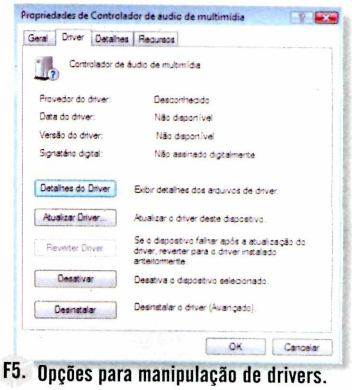
Trata-se de uma das ferramentas mais utilizadas pelo pessoal do suporte, pois sempre existe a necessidade de manipulação nos dispositivos de hardware.

Dynamic Update

Durante o processo de instalação do Windows Vista temos a opção de fazer o download de atualizações críticas de arquivos do sistema (DLLs) e de drivers de dispositivos que não fazem parte do sistema. Esse recurso



F4. Gerenciador de dispositivos no Windows Vista.



F5. Opções para manipulação de drivers.

se chama Dynamic Update e o acesso é feito ao site Windows Update. Lembrando que para isso é necessário ter uma conexão ativa com a Internet e que não é feita a atualização de drivers já existentes no sistema. Para isso, você deve seguir uma das três opções apresentadas anteriormente.

Conclusão

Demos início à nossa série sobre a certificação MCTS, onde vamos abordar o conteúdo cobrado pela Microsoft e apresentar dicas para o exame 70-620. Incentivamos o estudo, porém recomendamos que o candidato avalie a necessidade da realização de um treinamento, caso não tenha o perfil auto-didata. Até por que não temos a pretensão de fazer dessa série o único material de preparação para o exame.

Estamos aqui fornecendo um ponto de partida. É importante também conhecer muito bem o sistema e suas ferramentas. Dito isto, procure instalar o Vista pelo menos em um ambiente de testes que pode ser facilmente criado com virtualização, através de soluções da própria Microsoft, como o Virtual Server 2005 e Virtual PC 2007.

PC

Virtualização do Hardware

Aprenda a instalar uma máquina virtual com o Qemu e veja como a virtualização pode revolucionar a administração de redes.



Flávio Souza Oliveira
Mestre em Administração e Segurança de Sistemas pela Unicamp. Certificado LPI, atualmente trabalha na Total Quality on Information – TQI, em Uberlândia/MG

Com a redução dos custos de máquinas com maior poder computacional, uma prática tem sido cada vez mais utilizada pelos administradores de sistemas. Trata-se da chamada "consolidação". Quando dizemos que vamos consolidar alguns servidores, queremos dizer que vamos agrupar os serviços que eles executam em um número menor de máquinas, isto é, suponha que tenhamos os serviços FTP (File Transfer Protocol) e HTTP (Hypertext Transfer Protocol) rodando em máquinas diferentes. Quando instalamos esses dois serviços em uma única máquina e ela passa a executar todas as funções das antigas, então podemos dizer que fizemos a consolidação destes servidores.

Em geral, os objetivos de uma consolidação são a redução dos custos de manutenção e administração dos equipamentos e dos softwares, além da economia de energia e do espaço cada vez mais precioso nos Datacenters. Diferentemente de outras épocas, entretanto, uma consolidação hoje pode ser mais do que simplesmente instalar dois serviços em uma única máquina. Acontece que com o aumento do poder computacional dos PCs, uma prática que já foi muito utilizada nos primórdios da computação e na era dos Mainframes está voltando com força total. Um computador passa a executar dois ou mais sistemas operacionais (SO) simultaneamente, fazendo com que a consolidação deixe de ser apenas de serviços, mas de toda a infraestrutura de software e hardware, de forma que um único servidor possa virtualmente se passar por várias máquinas completas e independentes umas das outras. É o que chamamos de virtualização.

Como vantagens da virtualização podemos citar:

- **Segurança:** em uma consolidação simples ficamos mais expostos a um efeito colateral indesejado, que é o aumento da complexidade da configuração dos servidores. Contudo, uma regra básica em segurança é que quanto maior a complexidade de algum software ou configuração, maior a probabilidade de haver uma falha de segurança. Com a virtualização, entretanto, as máquinas virtuais são isoladas umas das outras, ou seja, caso haja um incidente de segurança em alguma delas ou nos serviços que elas executam, esse incidente estará isolado das outras máquinas virtuais, diferentemente da consolidação tradicional, onde um incidente em um dos serviços poderá afetar todos os outros executados pelo servidor atingido;
- **Disponibilidade:** como estamos trabalhando com um ambiente virtual, não estaremos limitados ao número de máquinas físicas que possuímos. Dessa forma, podemos manter diversas cópias de nossos servidores prontas para começar a rodar a qualquer instante no caso de um problema;
- **Recuperação de Desastres:** Uma prática também comum atualmente é a manutenção de imagens geradas com o

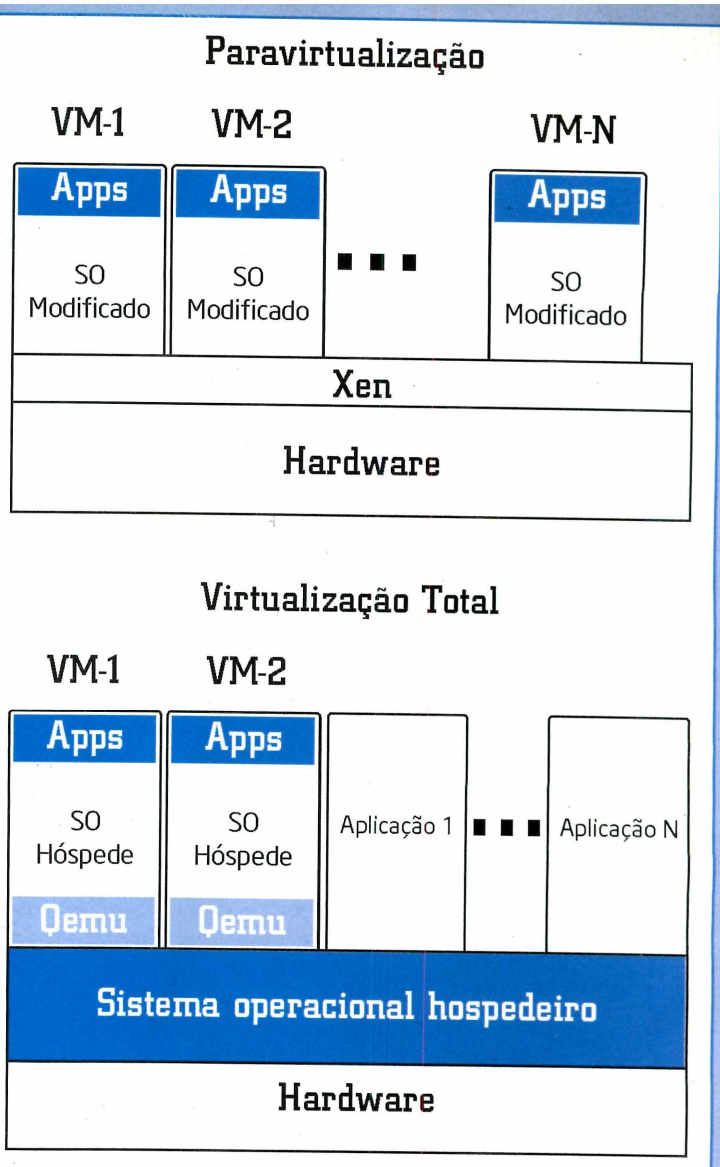
Norton Ghost (**http://www.symantec.com/region/br/home_homeoffice/products/backup_recovery/ghost10/index.html**) ou alguma outra ferramenta para clonagem de discos, para permitir a reinstalação rápida de uma máquina no caso de um problema. Entretanto, ainda teremos que refazer a instalação de drivers se essa recuperação for realizada em um equipamento diferente do qual a imagem foi gerada. Com máquinas virtuais esse problema não existe, já que o hardware virtual também é sempre "clonado". Além disso, o tempo de recuperação é quase nulo, pois temos apenas que dar boot em uma cópia do servidor.

O Mercado

Como era de se esperar, novas soluções e estratégias de virtualização estão surgindo no mercado a uma velocidade impressionante, patrocinadas por pesos pesados da indústria de tecnologia como IBM, EMC, Intel e AMD. Destaque para a IBM, que possui uma linha de servidores de grande porte voltada especificamente para esse segmento, os da série zSeries (**www.ibm.com/br/linux/servers/zseries/**). Outro destaque são os novos processadores da Intel e AMD que também incorporam extensões (Intel VT e AMD-V respectivamente) para dar maior velocidade às máquinas virtuais.

No momento existem basicamente duas estratégias de virtualização que estão se destacando em relação às demais: uma é a chamada Virtualização Total (full virtualization), adotada por softwares como o VMWare Workstation (**http://www.vmware.com**) e Qemu (**http://fabrice.bellard.free.fr/qemu/**), que simulam todos os componentes de hardware de uma máquina e permitem executar sistemas operacionais sem qualquer alteração em seus códigos. Ou seja, os sistemas operacionais que são instalados sobre esses softwares não têm conhecimento de que estão sendo executados sobre um hardware virtual, o que evita o impacto de ter que se reescrever parte do SO.

A outra estratégia é a chamada Paravirtualização, que tem o Xen (**http://www.xensource.com**) como representante mais conhecido. Neste caso, o sistema operacional deve ser preparado para executar na máquina virtual e dessa forma "sabe" que está sendo executado sobre um ambiente virtual. A vantagem da paravirtualização é a velocidade, uma vez que não precisa simular todos os componentes de hardware para a máquina virtual, processo esse complexo e que torna algumas operações lentas. A paravirtualização faz o compartilhamento do hardware da máquina hospedeira com as máquinas virtuais, sem que uma interfira na outra. Isso é feito por meio de uma API (Application Programming Interface) especialmente desenvolvida para esse tipo de aplicação e, que por sua vez, deve acrescentada ao sistema operacional (figura 1).



F1. Implementações de virtualização disponíveis no mercado.

Nessa matéria vamos aprender a instalar e a utilizar alguns dos recursos do Qemu, um software livre que possui versões para Linux, Windows e Mac OS, além de OpenSolaris, e que adota a estratégia de virtualização total. Veremos também como é simples fazer com que o Microsoft Windows rode sobre o Linux em um ambiente totalmente virtual. Vamos lá!

Cenário

Nosso cenário será um dos mais simples e um dos mais comuns para aqueles que estão começando a lidar com virtualização, pois não é raro necessitarmos da instalação de um sistema operacional para realização de testes, ou ainda precisarmos executar aplicações de um outro SO que não possuem versões similares para o nosso sistema operacional principal. Esse tipo de cenário também é muito útil no caso de um teste potencialmente danoso ao SO, pois caso o teste falhe, nenhuma máquina terá que ser reinstalada, basta recuperar uma cópia da máquina virtual, o que economiza muito tempo.

Instalaremos um Windows 2000 Professional Service Pack 4 em uma máquina virtual via Qemu; nosso sistema hospedeiro será uma máquina Linux rodando a distribuição Ubuntu 7.04. Como é de se esperar, a execução de dois sistemas operacionais simultaneamente exige um pouco mais da máquina, em nosso caso conseguimos fazer a instalação sem problemas em um AMD Sempron 2800+ com 512 MB de memória RAM.

Instalação da Máquina Virtual

A instalação do Qemu no Ubuntu é bastante simples, basta abrir um terminal e executar o comando sudo apt-get install qemu (figura 2). Feito isso, o comando sudo solicitará sua senha e então fará o download e a instalação do qemu com privilégios de *root*. Vale lembrar que, dependendo do tempo entre cada utilização do comando sudo, ele poderá solicitar ou não sua senha.

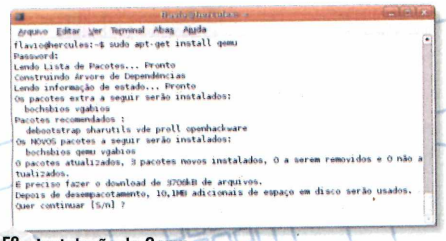
Uma vez instalado, podemos partir para a criação e instalação de nossa primeira máquina virtual, vamos aos passos:

1º Passo: Criação do HD virtual

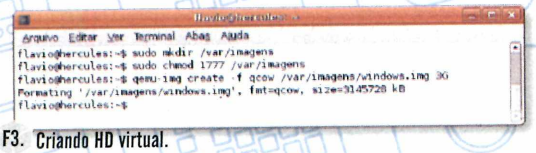
Assim como em um PC comum, uma máquina virtual também precisa de um HD onde o sistema operacional será instalado. Entretanto, na verdade esse "HD" será simulado através de um arquivo, que costumamos chamar de imagem, gravado no disco da máquina hospedeira. Primeiramente crie um diretório para o armazenamento de suas imagens e lembre-se de que vamos lidar com arquivos relativamente grandes. Em nosso caso, criamos o diretório `/var/imagens` com o comando `sudo mkdir /var/imagens` e alteramos as permissões para que um usuário comum possa criar arquivos na pasta, através do comando `sudo chmod 1777 /var/imagens`.

Para fazer a criação da imagem, execute o comando `qemu-img create -f qcow /var/imagens/windows.img 3G`, cujas opções detalhamos a seguir (figura 3):

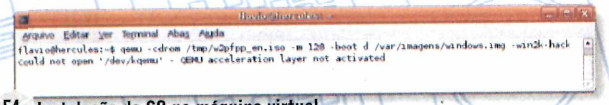
- `qemu-img`: programa responsável pela manipulação das imagens de disco das máquinas virtuais. Para maiores informações digite `man qemu-img`, assim poderá consultar o manual da ferramenta;
- `create`: indica ao `qemu-img` que desejamos fazer a criação de um novo arquivo imagem;
- `f qcow`: indica o formato do arquivo de imagem. Recomendo a utilização do formato qcow, que proporciona maiores recursos e versatilidade. Com esse formato, o Qemu faz com que o arquivo de imagem aumente de acordo com a utilização do disco virtual, ou seja, se definirmos um disco virtual de 4 GB esse espaço não será reservado imediatamente, ele será alocado à medida que houver demanda por ele na máquina virtual. Além disso, esse formato permite a criação de imagens cifradas, através do algoritmo de criptografia AES, ou compactadas para reduzir o consumo de disco do sistema hospedeiro;
- `/var/imagens/windows.img 3G`: indica o nome do arquivo de imagem e seu tamanho máximo. Em nosso caso vamos criar um disco de 3 GB, que é mais do que suficiente para instalar o Windows 2000 e mais alguns programas básicos.



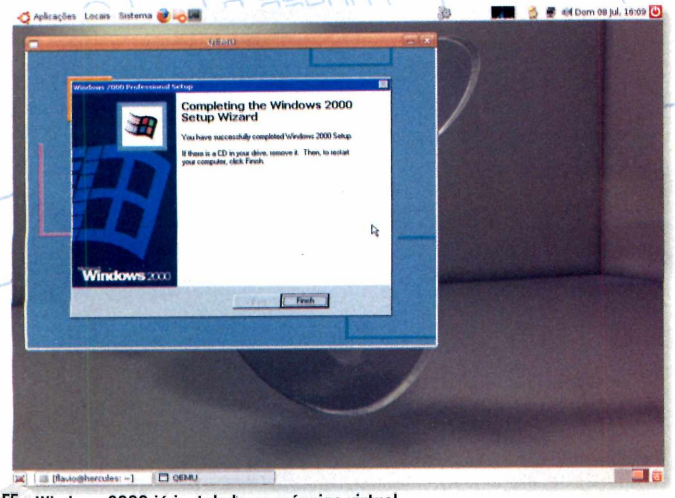
F2. Instalação do Qemu.



F3. Criando HD virtual.



F4. Instalação do SO na máquina virtual.



F5. Windows 2000 já instalado na máquina virtual.

2º Passo: Instalação do sistema visitante

Agora que nosso disco virtual está criado, podemos partir para a instalação do SO em nossa máquina virtual. Insira o CD de instalação do Windows no drive de CD-ROM e execute o comando `qemu -cdrom /dev/cdrom -m 128 -boot d /var/imagens/windows.img`. É possível também utilizar uma imagem ISO no lugar do CD, basta substituir `/dev/cdrom` pelo caminho da imagem ISO: `qemu -cdrom /tmp/imagem.iso -m 128 -boot d /var/imagens/windows.img` (figura 4).

- `cdrom /dev/cdrom` ou `-cdrom /tmp/imagem.iso`: indica o dispositivo de cdrom ou a localização da imagem ISO que fará as vezes de um CD;
- `m 128`: informa a quantidade de memória RAM que será alocada para a máquina virtual. Em nosso caso utilizaremos 128 MB;
- `boot d`: indica qual o dispositivo de boot da máquina virtual. A letra "d" indica que o boot será efetuado através da unidade de cdrom. As letras "a" e "c" indicam boot via disquete e HD virtual, respectivamente;
- `win2k-hack`: Na figura 4 podemos observar esta opção extra que não havia sido mencionada anteriormente. Ela é utilizada especificamente durante a instalação do Windows 2000, para contornar um bug que faz com que o instalador do Windows indique que não há espaço livre em disco. Uma vez terminada a instalação do Windows 2000, ela não é mais necessária.

Uma vez exibida a tela de inicialização do sistema, prossiga com a instalação normal do Windows até o final (figura 5).

3º Passo: Boot

Com a máquina virtual instalada, sua execução é muito simples. Basta utilizar o comando `qemu -localtime -cdrom /dev/cdrom -m 128 -boot c /var/imagens/windows.img`, por exemplo, no qual a opção `-localtime` indica que a máquina virtual deve ter o relógio sincronizado com a máquina hospedeira. Entretanto, as opções e possibilidades são inúmeras, desta forma recomendo uma consulta ao manual da ferramenta, através do comando `man qemu`, para uma análise das outras opções disponíveis.

Instalando Aceleração

O Qemu faz toda a execução da máquina

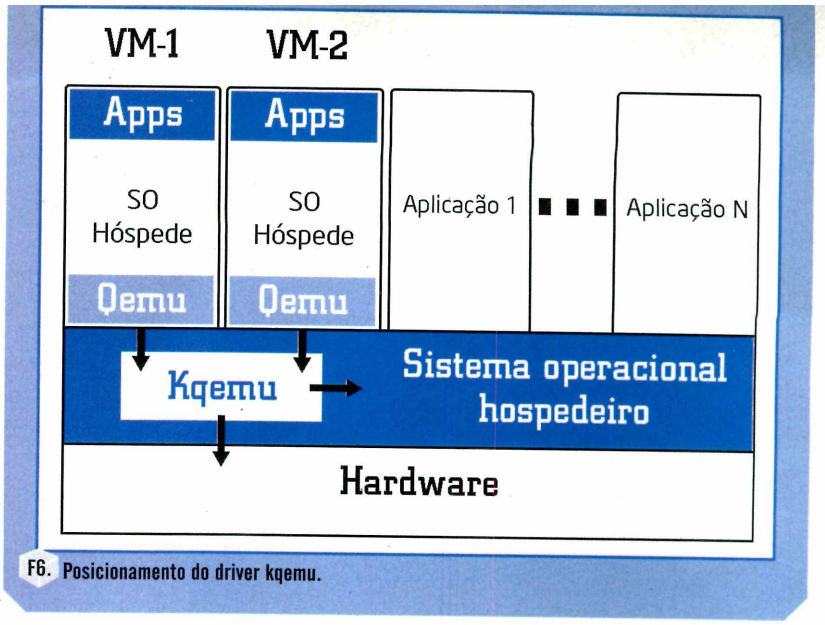
virtual em um processo comum do Linux, não tendo, portanto, nenhum tipo de privilégio no acesso à memória ou aos dispositivos. Além disso, diferente de alguns outros VMMs (*Virtual Machine Monitor*), como são chamados os softwares gerenciadores de máquinas virtuais, o Qemu adota uma política de emulação de CPU, ou seja, o trabalho de processamento não é feito diretamente no processador da máquina hospedeira, ele antes é dinamicamente manipulado para que instruções de acesso à memória, por exemplo, sejam executadas de forma transparente pelo sistema visitante sem causar interferência no sistema hospedeiro. Esse tipo de abordagem é bastante interessante, pois torna possível a emulação de diferentes tipos de processadores e arquiteturas e, dessa forma, a instalação de sistemas como Solaris (para CPU Sparc) ou Mac OS (para CPU PowerPC) em máquinas virtuais rodando sobre um PC comum (processador x86).

Contudo, a versatilidade da emulação tem um preço, já que todo esse processo de manipulação/tradução das instruções de processador acarreta uma certa lentidão à máquina virtual. Quando temos arquiteturas diferentes entre a máquina virtual e a máquina hospedeira não há o que se fazer, mas quando ambas possuem a mesma arquitetura, a tradução dte instruções não é necessária. Para tirar vantagem desse fato é necessário instalar um driver chamado **kqemu**, que possibilite o acesso direto ao processador da máquina hospedeira de maneira segura (figura 6), eliminando toda uma camada de processamento desnecessário.

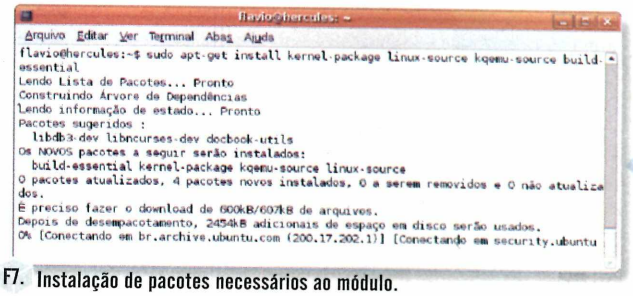
A instalação do driver, que no mundo Linux costumamos chamar de módulo, exige um certo trabalho de compilação, mas não se assuste, o Ubuntu deixa tudo muito simples. Primeiramente faça a instalação dos arquivos fonte do kernel do Linux, do fonte do módulo (driver) de aceleração, além de um pacote essencial de compiladores através do comando **sudo apt-get install kernel-package linux-source kqemu-source build-essential** (figura 7). Acesse o diretório de arquivos fonte (cd /usr/src) e efetue a descompactação dos fontes do kernel. Em nosso caso que estamos utilizando o kernel versão 2.6.20, o comando seria **sudo tar xjvf linux-source-2.6.20.tar.bz2**. Em seguida, crie um link simbólico com o comando **sudo ln -s linux-source-2.6.20 linux** e acesse o diretório de descompactação (cd /usr/src/linux).

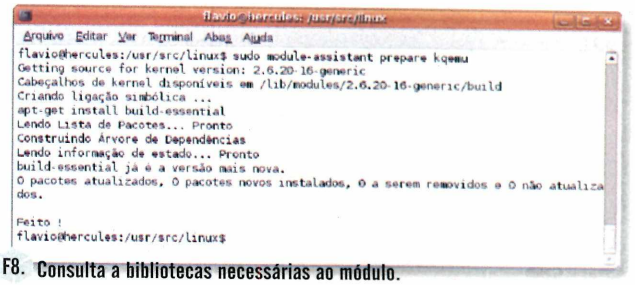
Neste ponto estaremos prontos para iniciar a compilação do módulo, para isso execute a seguinte seqüência de comandos:

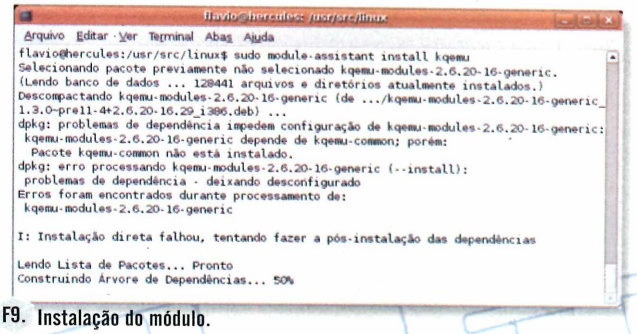
1. sudo module-assistant prepare kqemu: verifica se todas as bibliotecas necessárias ao módulo estão instaladas (figura 8);
2. sudo module-assistant build kqemu: efetua a compilação do módulo de aceleração;
3. sudo module-assistant install kqemu: efetua a instalação no módulo compilado (figura 9). Note que existe uma falha de dependência que é automaticamente corrigida pelo Ubuntu.
4. sudo depmod -a: verifica se todas as dependências entre os módulos instalados estão sendo satisfeitas. Caso esse comando não gere mensagens de erro, o kqemu foi instalado com sucesso;
5. sudo modprobe kqemu: carrega o módulo de aceleração manualmente para a memória;
6. sudo mknod /dev/kqemu c 250 0: cria um dispositivo que fará a interface entre o módulo de aceleração e o Qemu;
7. sudo chmod 666 /dev/kqemu: atribui permissões ao dispositivo recém-criado para que um usuário comum consiga utilizá-lo sem possuir privilégios administrativos (figura 10);



F6. Posicionamento do driver kqemu.


F7. Instalação de pacotes necessários ao módulo.

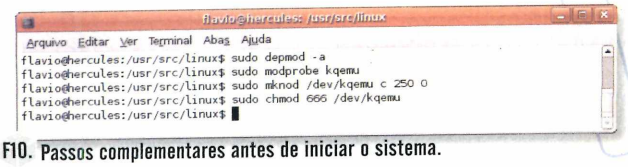

F8. Consulta a bibliotecas necessárias ao módulo.


F9. Instalação do módulo.

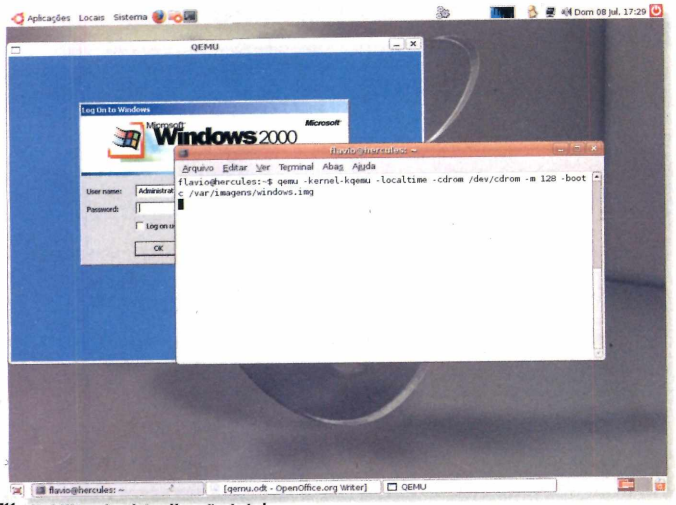
Tendo executado esses sete comandos, já poderemos efetuar o boot na máquina virtual e obter um pouco mais de desempenho, especialmente nas operações de acesso à memória. Entretanto, para obter o desempenho máximo é necessário que o Qemu trabalhe no modo de virtualização total, o que é possível através da opção **kernel-kqemu** (figura 11).

Os itens 5, 6 e 7 apresentados anteriormente dizem respeito à ativação do módulo

de aceleração, e os seus efeitos são perdidos quando a máquina é reiniciada. Para automatizar esse processo e ter o kqemu carregado durante o boot, acrescente esses três comandos no arquivo `/etc/rc.local` com o comando `gksu-do gedit /etc/rc.local` (figura 12) e então não se preocupe mais com eles. Dentro deste arquivo os comandos podem ser utilizados diretamente sem utilização do `sudo`, uma vez que o `rc.local` já é executado com privilégios administrativos.



F10. Passos complementares antes de iniciar o sistema.

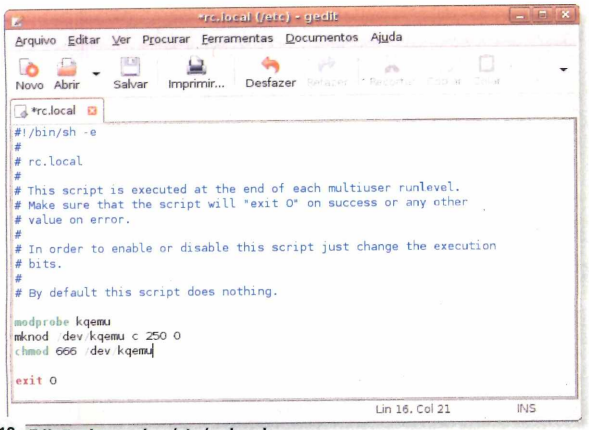


F11. Habilitando virtualização total.

Backup e Recuperação

Anteriormente mencionamos o quanto as máquinas virtuais tornam simples a recuperação de problemas, e agora com nossa máquina finalmente instalada essa afirmação é muito fácil de se comprovar. Para criar uma cópia da máquina virtual, basta copiar seu arquivo de imagem que, por sua vez, pode ser levada para qualquer outro PC com o Qemu instalado e utilizado normalmente sem a necessidade de nenhuma alteração no sistema hóspede.

O próprio Qemu possui mecanismos de recuperação interessantes, um deles é a opção -snapshot (figura 13), que evita que qualquer alteração seja feita no arquivo de imagem durante a utilização da máquina virtual. Isto é, nenhuma das alterações daquela sessão será gravada a menos que forcemos a gravação, através do console de gerenciamento do Qemu. Para acessar o console pressione simultaneamente as teclas Ctrl-Alt-2, digite o comando help para listar os comandos disponíveis e utilize o comando commit (figura 13) para forçar a gravação de todas as alterações feitas até aquele momento no arquivo de imagem. Ao término da execução do comando, pressione as teclas Ctrl-Alt-1 para voltar à tela do sistema.

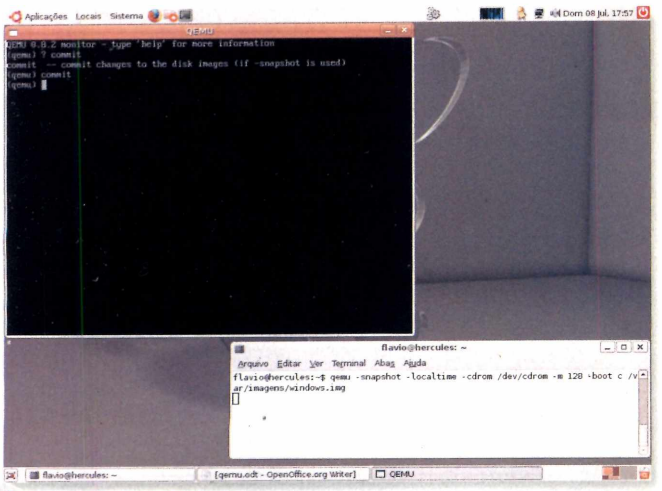


F12. Edição do arquivo /etc/rc.local.

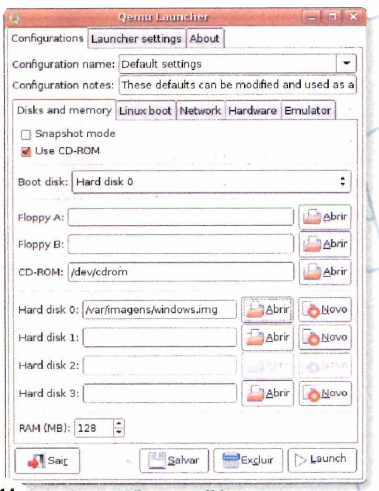
Outros programas

Você pode estar se perguntando se não existiria alguma interface gráfica que facilite sua vida, e a reposta é sim, elas existem. Uma boa opção é o qemu-launcher, que organiza as opções do Qemu em uma interface e torna muito mais fácil a inicialização das máquinas virtuais. Para instalar o programa, basta utilizar o comando `sudo apt-get install qemu-launcher` e, uma vez terminada a instalação, basta se dirigir ao menu Aplicações → Acessórios → Qemu Launcher para executá-lo (figura 14).

Vale mencionar para aqueles que já possuem processadores do tipo Dual Core da linha Intel Core 2 Duo ou AMD Athlon 64 X2, que já é possível tirar vantagem das novas extensões de virtualização que citamos anteriormente. Entretanto, será necessário utilizar uma versão modificada do Qemu denominada Kvm (**http://kvm.qumranet.com/kvmwiki**), cuja utilização é feita de forma praticamente idêntica à do Qemu convencional.



F13. Com virtualização fica fácil recuperar o estado do sistema.



F14. Interface gráfica para lidar com as máquinas virtuais no Qemu.

Conclusão

O potencial das máquinas virtuais é imenso e a sua utilização pode revolucionar a área de administração e segurança de redes. Para aplicações de virtualização em desktops, o Qemu é uma excelente opção, e apesar de não contar com todos os recursos e a velocidade de seu concorrente mais famoso, o VMWare Workstation, ele tem a seu favor o fato de ser um software livre totalmente gratuito. **PC**

O mundo é VoIP

A economia sempre foi a principal bandeira dos serviços VoIP. Aliada a melhoras recentes na qualidade, o resultado não poderia ser outro senão uma verdadeira explosão no número de usuários, que já chega a dezenas de milhões. Confira nesta matéria mais testes com uma solução que pode a ser a que você está procurando há algum tempo.



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

Resultados

A explosão da tecnologia VoIP abriu para o mundo um leque de oportunidades e benefícios. Se antes, ao analisar os relatórios de gastos com telefonia da empresa, qualquer gerente de telecom sentia o mesmo que muitos brasileiros ao verem o holerite, agora o quadro é outro.

Com os serviços VoIP, o sufoco para reduzir os custos com telefonia passou a ser facilmente contornável. Até mesmo nas residências. Basta criar uma conta com algum provedor deste serviço para, em questão de minutos, ter um número alcançável através da Internet.

Atualmente os serviços VoIP são disponibilizados gratuitamente por diversas empresas que, segundo uma pesquisa realizada pela consultoria In-Sat (**www.instat.com/catalog/pcatalogue.asp?id=272#IN0703603WWI**), atingiram a marca de 50 milhões de usuários VoIP em 2006. Isso expressa bem o quanto é o interesse de muitos em trocar o tradicional método de telefonia (chamado PSTN - Public Switched Telephone Network – Rede Telefônica Pública Comutada) por soluções de VoIP.

Como sempre, a locomotiva de inovações é empurrada pelas empresas provedoras de serviços e fabricantes de equipamentos. Entretanto, são poucas as novidades de produtos que chegam ao mercado para atender às necessidades de usuários domésticos e pequenas empresas.

Se quisermos hoje dispor de serviço VoIP, temos duas formas de originar e receber ligações. A primeira é utilizar os cada vez mais comuns *softphones*, se bem que nesse caso haja o custo extra de se manter um computador ligado. Outra opção é comprar um gateway VoIP (comumente chamado por ATA - Adaptador para Telefone Analógico, ou roteador VoIP) e ter a possibilidade de concentrar num único equipamento as funcionalidades de adaptador de telefone, servidor DHCP, parâmetros relacionados à qualidade de recepção e transmissão da voz, entre outros. Com ele a placa de som, o microfone e as caixas acústicas deixam de ser necessários, ou melhor, não precisamos utilizar um computador para ter um telefone.

Além disso, por serem pequenos e leves, podemos levar os gateways VoIP mais simples para qualquer lugar. E quando falamos em expandir o recurso VoIP para mais de um usuário numa casa, por exemplo, ou de estarmos sempre disponíveis para nos comunicarmos, independente do lugar, o gateway VoIP é seguramente a melhor solução. Se vamos viajar, basta levá-lo na mala para, a partir de uma conexão com a Internet, ficarmos "acessíveis". Se o assunto é criar ramais VoIP e mantê-los disponíveis para vários usuários, mais uma vez o gateway de voz sobre IP aparece.

Testes

A fim de demonstrar essas funcionalidades fizemos um teste neste mês com o Phone Adapter VoIP 2102, da LinkSys (**figura 1**), que é apenas um dentre os



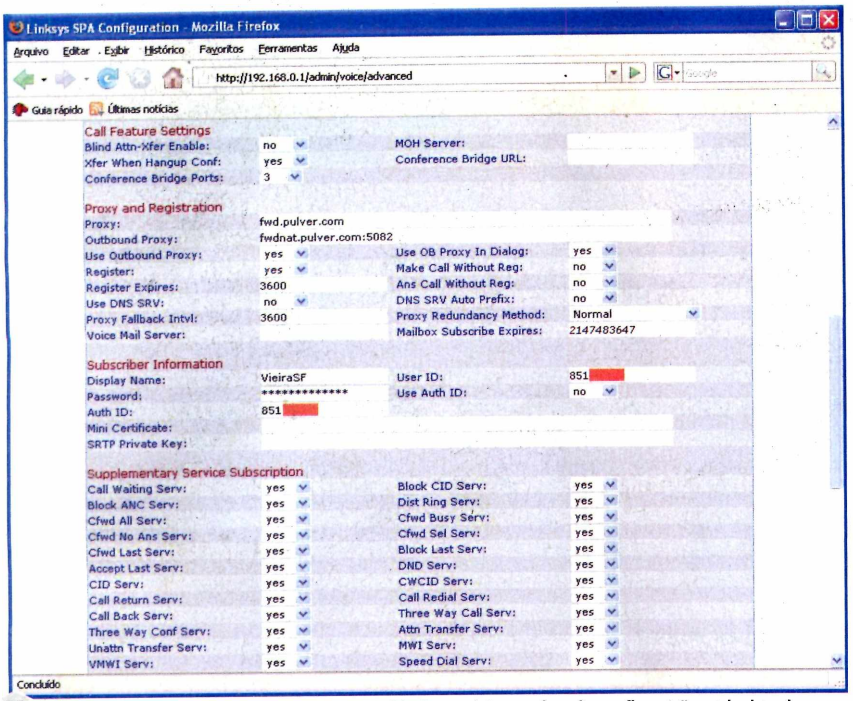
F1.

Com um custo médio de R$ 280, o roteador vem com 2 portas ethernet (WAN e LAN) e FXS (conector RJ-11 para os telefones analógicos). Fabricante não oferece suporte técnico para este produto no Brasil.

diversos modelos existentes no mercado. Ele suporta conexões PPPoE e DHCP na interface WAN, e através de NAT faz o roteamento para máquinas clientes de uma rede interna.

Todas as configurações são feitas a partir de uma interface web (**figura 2**). O manual com maiores detalhes sobre a instalação do Linksys 2102 poderá ser obtido no site **www.sipura.com/support/index.htm.** Para a transmissão da voz, este gateway utiliza o também cada vez mais comum protocolo SIP (Session Initiation Protocol – Protocolo de Iniciação de Sessão), cuja especificação técnica pode ser lida no site **www.ietf.org/rfc/rfc3261.txt.**

Na **figura 3** apresentamos o diagrama da rede criada em nosso laboratório para os testes. O primeiro detalhe é o posicionamento do gateway. Embora ele possa ser colocado na borda da rede, isto é, entre a rede interna e o modem de acesso à Internet, no nosso caso optamos por colocá-lo antes de um roteador, que já estava instalado devido ao fato deste oferecer uma maior quantidade de recursos de segurança. Basta configurar o gateway como bridge, ou então, configurar sua interface WAN para pegar um endereço IP via DHCP do roteador, e neste colocar o IP do gateway na configuração de DMZ ou fazer redirecionamento de portas.



F2. Tela principal de configuração do LinkSys 2102. Por padrão, as demais configurações relacionadas ao serviço VoIP deverão permanecer com os ajustes de fábrica.



F3. Lay-out da rede para testes. Foi possível fazer e receber chamadas de outros usuários SIP rodando o softphone X-Lite, por exemplo.

Ademais, observe que os dois aparelhos de telefone poderiam estar fisicamente em áreas ou departamentos diferentes. Neste exemplo, os dois ramais ficaram habilitados para realizar chamadas entre si, ou para outros telefones IP da Internet. As contas de usuários e, conseqüentemente, os números de chamadas, foram criados no site do provedor Free World Dialup (**www.fwdnet.net**).

Ajuste fino

A maior preocupação daqueles que têm dúvidas sobre soluções VoIP é a questão da qualidade. E com razão! Imagine ter uma conversa com um cliente prejudicada devido a atrasos na propagação dos pacotes de voz que foram digitalizados. Felizmente, se existe algo que não há como contestar é a evolução nos métodos de transmissão de dados multimídia. Seja para transmitir vídeos ou voz pela Internet, os equipamentos disponíveis hoje implementam algoritmos e hardware bastante robustos com vistas a oferecer uma boa qualidade de serviço (QoS – Quality of Service).

Prova disso foi nosso último teste. Depois dos testes preliminares bem-sucedidos, colocamos um micro atrás do gateway e iniciamos um cliente P2P para fazer download de alguns arquivos que totalizavam 5 GB. Foi fazer isso para passar a ouvir a voz "picotada" por diversos momentos.

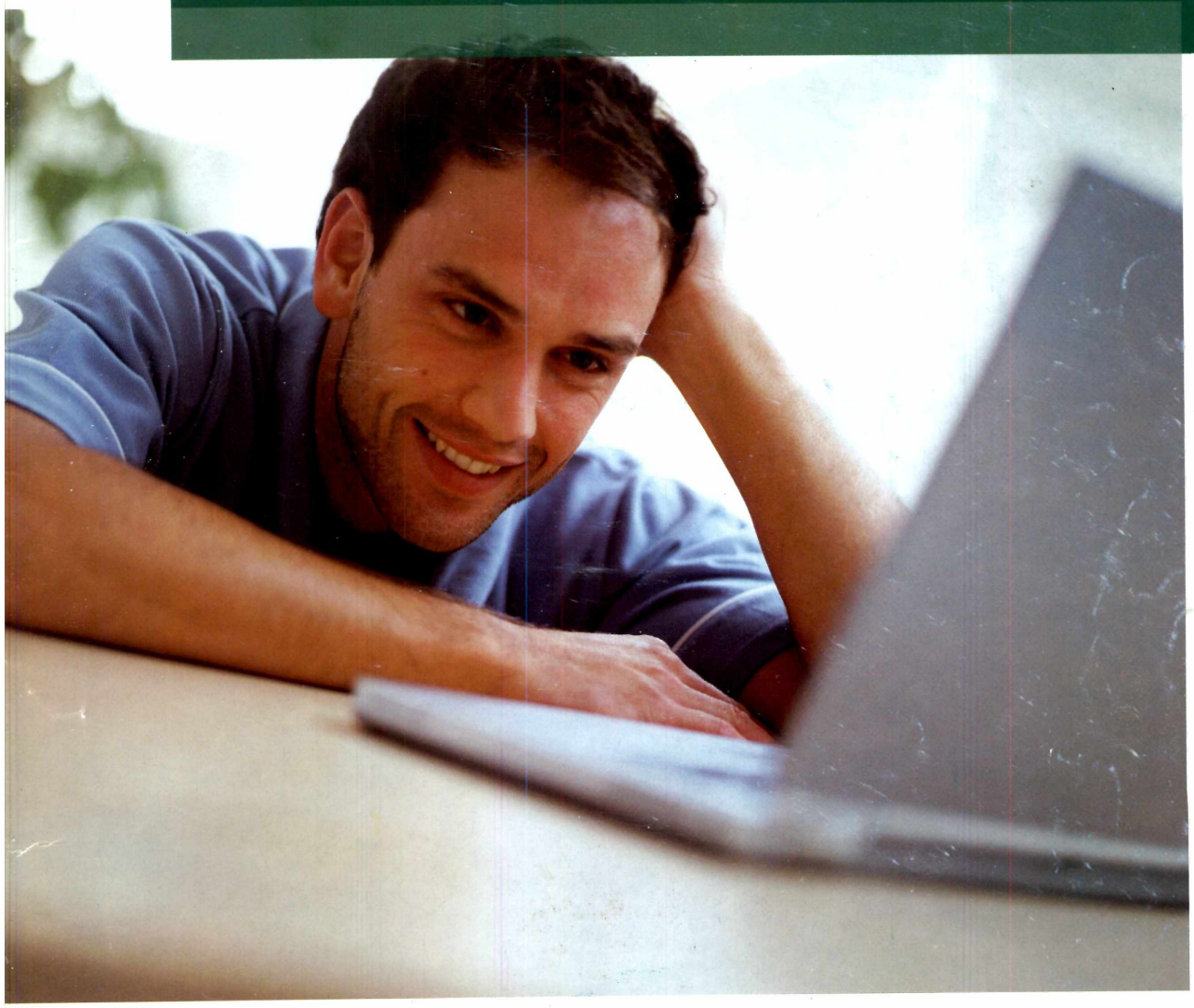
A solução veio com um ajuste no método de QoS do gateway, que curiosamente traz como opção padrão "None" - nenhum. Ao mudar o valor do parâmetro QoS para "TBF" (não documentado nos manuais), os pacotes de voz passaram a ser priorizados e o resultado final foi bastante satisfatório, mesmo durante os downloads.

Conclusão

Telefonia convencional daqui a 5 anos? Embora seja difícil dizer que ela não existirá, o fato é que hoje já existem milhões de usuários VoIP e a cada dia cresce em ritmo mais acelerado.

Com preço relativamente acessível e boas funcionalidades, este gateway da Linksys surge como boa opção para usuários que querem se beneficiar do VoIP, mas sem ficarem presos a um computador e *softphones*. As conveniências são tantas que muito provavelmente você esteja neste momento pensando em um cenário de utilização não abordado aqui e que vai ao encontro de suas necessidades. Aliás, é oportuno admitir que também estamos pensando nisso e já planejando as próximas matérias. **PC**

Ver TV é a menor das coisas que você vai fazer em seu computador.



FCP Publicidade

Imagine digitalizar suas fitas VHS no computador e passá-las para DVD?

Imagine ouvir rádio e gravar sua programação preferida em mp3?

Imagine fazer seus próprios podcastings?

Imagine gravar o que está na filmadora direto para o seu PC?

Imagine jogar para o seu MP4 / MP3 player o conteúdo gravado da TV?

Imagine assistir TV diretamente em seu computador?

Agora tudo isso já é possível com a tecnologia da **NXP Semicondutores**, líder mundial em soluções de TV para PC.

Fale com a **NXP** e abra as portas para um mundo de novas possibilidades.

www.nxp.com

NXP founded by Philips

MSI
MICRO-STAR INTERNATIONAL
innovation with style

AMD 64 Athlon FX

Tenha o melhor desempenho - Sempre!

Inovador, Dinâmico, Exclusivo





K9N6SGM-V

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

Marching to Future Technology

www.msicomputer.com.br

ALCATEIA www.alcateia.com.br 11 3226 2626

Tech Data www.techdata.com.br 11 4166 1300

INGRAM MICRO www.ingrammicro.com.br 11 3677 5980

ABANO www.abano.com.br 21 2196 1100

SND www.snd.com.br 11 2187 8333

BELL MICRO www.bellmicro.com.br 11 2107 7900