Anti-Vírus
Testes com 4 suítes completas
Descubra a melhor

iPhone
Testes com a
revolução dos celulares

RAM Check
Conheça uma solução
profissional para testes de
memórias

www.revistapcecia.com.br

PC &CIA

Voz sobre IP

Servidor PBX com Asterisk
Grande redução de custos
de telefonia
Configuração passo-a-passo

SABER

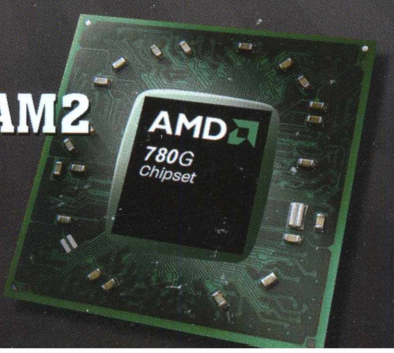
ANO 7 - Nº 81 - 2008 - Europa €4,30 - Brasil R$13,90

Suporte Remoto

- ✔ POST, acesso ao BIOS e manutenção no sistema
- ✔ Solução imbatível integrada no hardware
- ✔ Como fazer remotamente

Novas placas-mãe AM2

A evolução do vídeo onboard
Testes com 3 modelos



PC e Home Theater

Saiba como integrá-los e
obter áudio de qualidade

ISSN 1519-5267

VENHA FAZER PARTE
DA REVOLUÇÃO DA ELETRÔNICA NO BRASIL!

TENHA ACESSO AO MELHOR
CONTEÚDO DA ÁREA DE ELETRÔNICA
PAGANDO R$ 48,00 / ano
(Apenas R$ 4,00 / mês)

www.saberetronica.com.br

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 G. Ferreira

Colaboradores
Anderson Costa, Daniel Appel, Fernando Vieira, Flávio de Souza Oliveira, Igor Humberto, Jansen Carlo Sena, Marcus Brandão de Moura, Paulo Roberto Sant'anna, Pedro Henrique Gomes, Renato da Silva Junior, Roberto Cunha, Tatiane Silvia Leite,

Auxiliar de Redação
Claudia Tozetto, Fabieli De Paula

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

Produção
Diego M. Gomes

VENDAS DE PUBLICIDADE
Carla de C. Assis,
Ricardo Nunes Souza

PARA ANUNCIAR: (11) 2095-5339
publicidade@editorasaber.com.br

Capa
Tango Desktop Project (Ícone do globo)

Impressão
PROL Editora Gráfica Ltda.

Distribuição
Brasil: DINAP
Portugal: Logista Portugal tel.: 121-9267 800

ASSINATURAS
www.revistapcecia.com.br
Fone: (11) 2095-5335 / fax: (11) 2098-3366
Atendimento das 8:30 às 17:30h
Edições anteriores (mediante disponibilidade de estoque), solicite pelo site ou pelo tel. 2095-5330, ao preço da última edição em banca.

PC&CIA é uma publicação mensal da Editora Saber Ltda, ISSN 0101-6717. Redação, administração, publicidade e correspondência: Rua Jacinto José de Araújo, 315, Tatuapé, CEP 03087-020, São Paulo, SP, tel./fax (11) 2095-5333.

Associada da:
ANER www.aner.org.br Associação Nacional dos Editores de Revistas
anatec www.anatec.org.br
Associação Nacional das Editoras de Publicações Técnicas, Dirigidas e Especializadas

Foco no suporte técnico


Fernando Ramos

O suporte técnico é um dos componentes de maior impacto na equação de custos de operação com a área de TI. É o que apontam os mais diversos levantamentos realizados por empresas independentes, ou estudos de TCO (Custo Total de Propriedade) feitos por comitês internos às organizações. E se nas grandes a questão já é crítica, sobretudo por ter de levar em consideração a segurança da rede na interligação entre sites, o que dizer das pequenas? Os recursos humanos aqui normalmente são mais escassos e elas não podem se dar ao "luxo" de ter qualquer funcionário de braço cruzado esperando o técnico externo chegar para resolver o problema.

Foi com que esses cenários em mente que mobilizamos a equipe nessa edição. Que tal ter a possibilidade de acessar o programa Setup do BIOS de uma máquina remota? Ou então, poder acompanhar as mensagens durante os testes de inicialização e, se preciso for, realizar um boot controlado remotamente a fim de substituir um arquivo crítico do sistema operacional?

São muitos os cenários possíveis, mas o principal item descoberto é que agora não é necessário investir um real a mais em suítes de software complexas ou hardware especial de rede para ter essas funcionalidades em seu ambiente. O mérito é da plataforma vPro da Intel, que há pouco tempo ganhou um componente extra, exclusivo às suas placas-mãe, que se beneficia dos recursos de hardware integrados no chipset e interface de rede integrada, além de outros componentes.

Confira os detalhes a partir da página 8 e não deixe de acompanhar também outras duas ótimas soluções para suporte remoto. A primeira com o WebDAV, que se apresenta como uma opção altamente viável em relação às configurações de VPN normalmente realizadas entre sites remotos; e a segunda com uma variante do tradicionalíssimo VNC, onde destacamos alguns recursos normalmente pouco explorados, a exemplo da configuração de criptografia para o estabelecimento de uma sessão remota segura.

No mais, como de costume, ficamos no aguardo de seus comentários e observações. Aliás, se conhecer alguma solução diferente das abordadas aqui, sinta-se convidado a entrar em contato e, por que não, a participar de nossas próximas edições.

Tenha uma boa leitura!

Fernando Ramos da Silva: **fernando@editorasaber.com.br**

Investir em ferramentas é a solução ideal para segurança?

Jansen C. Sena

Ainda são muitas as corporações que não estão preparadas o suficiente para lidar com os constantes riscos advindos do mundo virtual criado pelas redes de computadores. Em muitas organizações, fundamentalmente nas de menor porte, ainda impera o desconhecimento generalizado com relação às reais necessidades de se manter seguro com relação ao seu ambiente computacional. Nesse cenário, não são raras as oportunidades em que tais organizações são surpreendidas com problemas tais como vírus, *worms*, *spam*, *web pishing*, negação de serviço, etc. Em outros casos, muitas vezes ainda mais sérios e danosos, é possível identificar problemas tais como roubo de dados corporativos e outras invasões que põem em risco a segurança de muita informação de caráter crítico e sigiloso. E, infelizmente, somente após sofrer um sério problema de segurança é que algumas corporações despertam para a necessidade de investir nesse segmento.

Seja de maneira planejada, seja após ter tido prejuízos das mais variadas escalas, muitas organizações concentram seus investimentos na aquisição de equipamentos e softwares para compor suas blindagens corporativas. Anti-vírus, anti-spam, *firewalls*, sistemas de detecção/prevenção de intrusos, sistemas de autenticação mais robustos, mecanismos de auditoria de serviços, VPNs, são somente algumas das parafernalhas que passam a fazer parte desse novo contexto corporativo onde a segurança da informação torna-se, ainda que de maneira tímida frente aos constantes perigos advindos da rede mundial, um segmento digno de atenção.

Entretanto, é preciso estar atento ao fato de que, nem sempre, o volume de investimento financeiro é, ao contrário do que se possa imaginar, diretamente proporcional ao aumento significativo do nível corporativo de segurança.

Mesmo com um bom conjunto de ferramentas, nenhum ambiente pode ser considerado seguro se não tiver uma equipe de profissionais tecnicamente bem capacitada e preparada para enfrentar as situações de risco oriundas das redes de computadores. Recentemente, uma empresa norte-americana deixou que milhares de dados pessoais de seus clientes, incluindo números de cartões de crédito, caíssem nas mãos de impostores. O fato não é novo, uma vez que em muitas outras oportunidades fatos semelhantes já aconteceram. Entretanto, o volume de dados comprometidos e o tempo em que essa falha já perdurava no sistema da empresa acabaram trazendo atenção especial para esse fato. Sob o ponto de vista de segurança da informação, seria possível mitigar ou mesmo evitar tal ocorrência apenas com um time tecnicamente mais capacitado.

Em outra perspectiva, analistas de segurança de redes e informação não são os únicos responsáveis pela segurança corporativa. Todos os usuários fazem parte do processo. Entretanto, envolver esses usuários em políticas de segurança não é o tipo de trabalho que pode ser feito por uma ferramenta. Diga-se de passagem, esse é um dos maiores desafios na tarefa de tornar um ambiente corporativo mais seguro.

Não é à toa que, muitas vezes, o diferencial de um bom analista de segurança da informação está na sua habilidade em saber fazer da segurança uma prática inerente ao trabalho de todos os colaboradores de uma instituição. É preciso lançar, muitas vezes, mão de uma aguçada habilidade em ser criativo na aplicação das recomendações de segurança a serem seguidas.

> *Não é à toa que, muitas vezes, o diferencial de um bom analista de segurança da informação está na sua habilidade em saber fazer da segurança uma prática inerente ao trabalho de todos os colaboradores de uma instituição.*

Por fim, considerar a segurança da informação como uma estratégia corporativa para manter saudáveis os negócios da organização, não significa apenas arrendar investimentos e recursos. É preciso saber onde e como investir. É preciso ir muito além das ferramentas. **PC**

Estabilizadores de tensão

Gostaria de sugerir um artigo com testes de estabilizadores de tensão. A PC&CIA já realizou vários testes em fontes de alimentação, mas em relação a esse que é um dos principais componentes utilizados pelos usuários, praticamente não há comparativos publicados.

Jean dos Santos
Perito Criminal
Instituto Geral de Perícias SC
Chapecó – SC

Já faz um bom tempo mesmo que não falamos sobre isso, o último teste comparativo foi publicado na edição 47 (**www.revistapcecia.com.br/edicoes/edicoes.asp?comando=047**). Agradecemos a sugestão e pretendemos contemplá-la no decorrer deste ano.

Máquina virtual para Internet Segura

Desde a matéria sobre o Endian Firewall (edição 62), tenho acompanhado todas as matérias sobre o tema. Agora resolvi apostar no smoothwall, uma vez que o Endian, após algum tempo de uso e estando com todos os serviços ativos, demora para carregar depois do boot e fica parado logo após a inicialização do IDS. É uma pena porque é um ótimo firewall. Bom, depois de instalar e por o smoothwall no controle de minha rede, não estou encontrando a opção para implementar a função de \"alias\", a qual estava disponível tanto no Ipcop quanto no Endian.

Técnico – WS Computadores
Rio de Janeiro – RJ

Para implementar a função de "Aliases" no Smoothwall, devemos instalar o módulo Full Firewall Control. Este, de fato, será o responsável por modificar o sistema do smoothwall de modo a evitar comportamentos "estranhos" no roteador. O arquivo tar.gz (de 210 KB) do Full Firewall Control encontra-se disponível no site **https://sourceforge.net/project/showfiles.php?group_id=114890&package_id=262627**. Após baixar este arquivo, remova-o, via ssh ou winscp, para o diretório "/addon" localizado na raiz do sistema. Descompacte-o através do comando "tar zxvf nome do arquivo". Em seguida será criada uma pasta chamada "tmp", deixando a árvore de diretórios da seguinte maneira: "addon/tmp". Agora execute o script de instalação do Full Firewall Control através da seguinte linha de comando: tmp/install.sh. Por último, responda "y" para a solicitação de reinicialização do roteador, que surgirá no terminal. Depois disso, abra uma janela de browser e acesse a página "Networking" do Smoothwall. Nesta, surgirá uma nova guia chamada "Firewall Control", que permitará a atribuição de múltiplos endereços IP's a uma interface de rede.

Placas LGA775 de baixo custo

Comprei a revista e li o artigo, mas quando entrei no site da Asus para pegar o manual da placa P5GC-M2/1333, não o encontrei. Há referência para P5GC-MX/1333. Foi um erro de edição?

Gilmar Alexandre
Analista de Suporte
Medidata Informática S/A
Belo Horizonte - MG

Realmente foi um erro de edição. Obrigado pelo contato e queira, por gentileza, desculpar-nos pelo equívoco.

MediaPC

Depois de utilizar o MediaPC através de um monitor de vídeo, resolvi direcionar a saída para uma TV, no caso uma Sharp Apex 21 (não é digital). Fiz a ligação da saída de vídeo composto da placa M2NPV-VM com a entrada AV da TV, configurei o BIOS e dei boot no MediaPC. Até o prompt de login, a imagem aparece na TV. Após efetuar o login e executar o "startx", a imagem passa para o monitor e não aparece mais na TV. O que devo configurar para poder utilizar a TV como saída para o MythTV?

Euclides Machado
Brasília – DF

O BIOS do sistema está identificando a saída padrão como TV, por conseqüência toda a operação "Modo Texto" sai pela TV. Após a carga inicial do sistema, o driver gráfico da NVIDIA chama a saída correta, porém ele não considera o que está setado no BIOS. Para facilitar o "chaveamento" entre saída de TV e monitor, foram criados dois scripts denominados tv e monitor. Basta digitar na linha de comando para ele setar a saída desejada e após fazer a carga com o startx.

Placa POST Saber

Há pouco tempo, recebi uma placa POST Saber. Entretanto, nas duas placas-mãe (K8VSE-Deluxe) que testei, a POST indica 02 e não dá boot. Ela pode estar com defeito?

Vilmar de Jesus Benedito

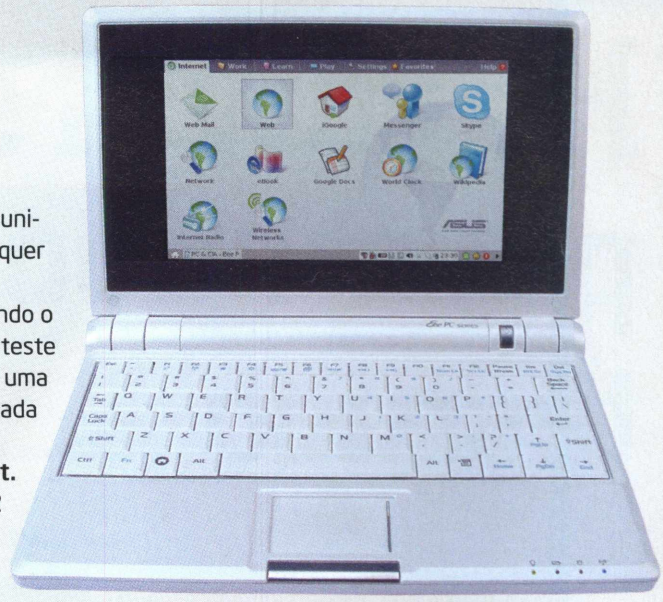
Você tentou por a placa em outros slots PCI? Quando você diz que a placa não dá boot, significa que nem sequer aparece imagem na tela? E por último: o led do clock da placa post fica piscando?

Réplica: *Tentei em todos os slots, inclusive em um computador que está funcionando perfeitamente, mas mesmo nesse obtive o mesmo resultado. É só colocar a POST que o vídeo nem entra e o computador fica travado. No display só aparece o número 02 e o led de clock pisca direto.*

Se o led de clock permanece piscando é porque o chip da placa post está minimamente funcional. Nesse caso, o problema do travamento se deve a alguma incompatibilidade com as placas-mãe avaliadas. Conforme comentado na edição 75, os controladores PCI integrados nos chips SouthBridge (Ponte Sul) de alguns chipsets infelizmente não implementam totalmente as especificações definidas no padrão PCI. No momento, nosso objetivo é trabalhar numa segunda versão da placa post, que seja capaz de contornar essa limitação e, consequentemente, ser capaz de operar mesmo nesse caso.

@ Vez do leitor
Envie seus comentários, críticas e sugestões:
a.leitor.pcecia@editorasaber.com.br
Rua Jacinto José de Araújo, 315
Tatuapé, CEP 03087-020 - São Paulo - SP

Asus libera kit de desenvolvimento do Eee PC



Depois de alguns meses de espera, e também de reclamações da comunidade, a Asus disponibilizou o SDK do EeePC. O SDK permitirá que qualquer desenvolvedor melhore e estenda as funcionalidades do produto.

O SDK oferece uma plataforma de desenvolvimento completa, incluindo o ambiente de desenvolvimento Eclipse, um ambiente multilingual de teste e debug baseado no VMware, um toolkit Qt4, aplicações de exemplo, uma edição de circulação aberta do Xandros (a distribuição Linux adotada pela Asus) e também o guia do desenvolvedor.

O download pode ser feito pelo site da Asus, no link **http://support.asus.com.tw/download/download.aspx?model=Eee%20PC%202G%20Surf/Linux&SLanguage=en-us,** ou mesmo pelo Sourceforge.net, no link **http://sourceforge.net/project/showfiles.php?group_id=215613**.

Novidades no mercado de gamers

O mês de março foi marcado por alguns lançamentos. A Evolute, com menos de um ano de vida, que já oferece desktops e notebooks, decidiu ampliar sua linha de produtos apostando no mercado de games, criando a Evolute Gaming.

Inicialmente são três sistemas baseados nos processadores Intel Core 2 Quad com interfaces de vídeo da NVIDIA.

O modelo de entrada é o Flame, que é integrado com um processador Core 2 Quad Q6600, placa-mãe Gigabite P35-DS, placa de vídeo EVGA Geforce 8800GT, 2GB de memória da OCZ, HD da Western Digital e gravador de DVD da LG. A fonte de alimentação, de 500W, e o gabinete são da Cooler Master.

O modelo intermediário, o Celerity, tem basicamente a mesma configuração de hardware, diferenciando-se na fonte de alimentação e no gabinete, ambos da Gigabyte, e ao invés de um gravador de DVD, foi integrado uma unidade Blu-Ray.

Comet é o nome do modelo high-end, sendo integrado com um processador Core 2 Extreme Edition, duas interface de vídeo EVGA GeForce 8800 Ultra em SLI, dois HDs Western Digital Raptor X operando em RAID 0, e apresenta o diferencial de utilizar refrigeração líquida, no caso, foi utilizado o Aquagate Max da Cooler Master para as placas de vídeo e o chipset da placa-mãe, e um Aquagate S1 para o processador. Ainda da Cooler Master, foi utilizado o gabinete Cosmos S e a fonte de alimentação.

O preço do Flame é de R$ 3599 e o do Celerity, R$ 3999. Ambos serão vendidos na rede credenciada, mas à época do lançamento estariam disponíveis apenas pela loja virtual Extra.com.br. O Comet possui preço inicial sugerido de R$ 17999 e final que dependerá da personalização realizada pelo cliente sobre os itens do hardware. Nesse caso, os pedidos devem ser feitos diretamente com a Evolute e a entrega, segundo a empresa, é feita dentro de um prazo estimado em 15 dias.

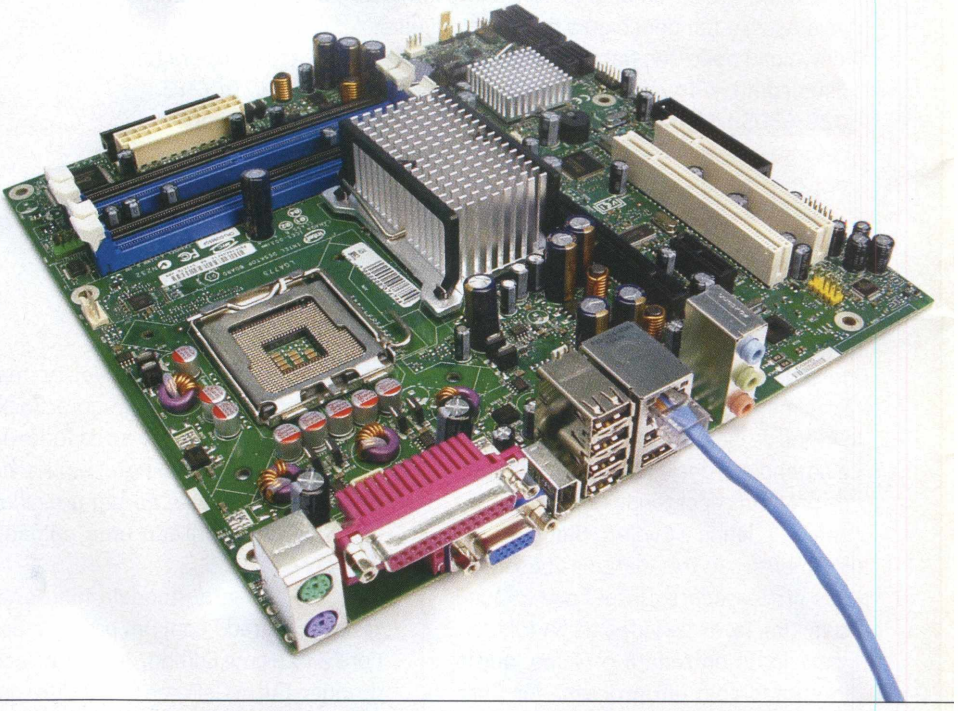
Amazon Gamer, uma aposta diferente da AmazonPC, no mercado de games

A AmazonPC, que já atua há alguns anos no mercado de desktops de baixo custo, agora lança o notebook Amazon Gamer. Embora o nome e a configuração sejam bem direcionadas aos gamers, ou seja, alta performance, ele acaba sendo um produto de uso mais amplo, como comentado pelo próprio fabricante.

Baseado na plataforma Intel Centrino, o Amazon Gamer utiliza um Core 2 Duo T9300 de 2.5GHz, 4GB de memória RAM, HD de 200GB, interface de vídeo NVIDIA GeForce 8700M, saída HDMI, som HD Audio, leitor de cartões, gravador de DVD dual layer, webcam e microfone integrados, além de tela widescreen de 17" com resolução de 1680x1050WSXGA.

Ainda no pacote, é oferecido o jogo Need for Speed Prostreet, mochila e joystick. O sistema operacional instalado é o Windows Vista Ultimate de 64 bits. O Amazon Gamer possui preço sugerido de R$ 7999.

Hardware imbatível para suporte técnico



Há exatamente um ano, na edição 69, apresentamos uma matéria prática sobre a tecnologia de gerenciamento ativo AMT (Active Management Technology), da Intel, que traz integrado no hardware recursos para facilitar – e muito – o suporte técnico remoto aos desktops. Nesta matéria você confere o que mudou de lá para cá e terá a oportunidade de conferir se ela realmente faz jus à palavra imbatível.

Fernando Ramos da Silva

vPro

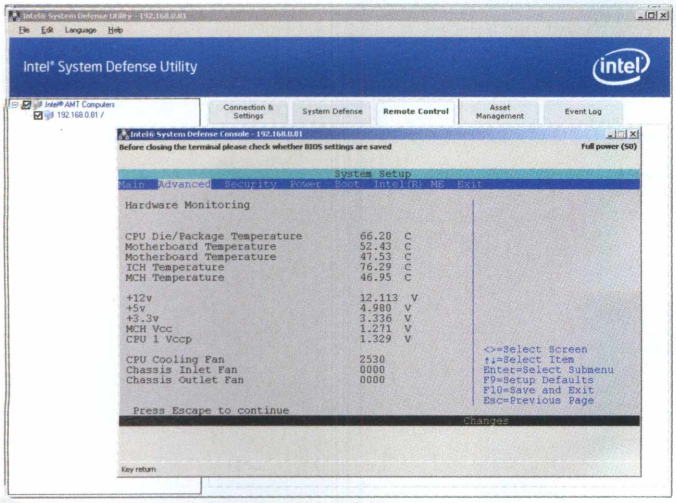
Este é o nome comercial da tecnologia AMT. O importante para nós aqui é saber que por trás desse termo estão os componentes de hardware e software que habilitam as funcionalidades de suporte técnico remoto e outras que já tivemos a oportunidade de avaliar no passado. Que tal, por exemplo, poder ligar ou desligar um PC à distância, de qualquer lugar do mundo, bastando para isso uma conexão com a Internet? Ou então, acessar o BIOS da máquina remota para verificar as temperaturas de funcionamento (**figura 1**), ou poder alterar o valor do parâmetro que gerencia a controladora de disco SATA, de modo a habilitar o boot da mesma?

E não é só: é possível também colocar um disquete de boot (ou CD, ou imagem de sistema gravada no HD) qualquer em sua máquina e usá-lo para inicializar a máquina remota, a fim de, por exemplo, poder atualizar o BIOS ou então substituir um arquivo de sistema corrompido que está impedindo o usuário de trabalhar, ou ainda usar um LiveCD mais poderoso para subir o sistema remoto e depois estabelecer uma conexão com maiores recursos à disposição, via SSH ou VNC (**figura 2**).

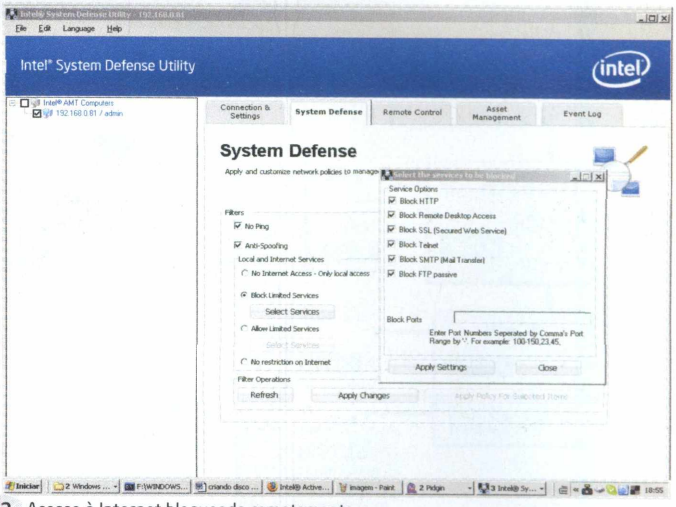
Outro destaque é a possibilidade de configurar filtros de acesso à rede diretamente no hardware, ou seja, na própria placa de rede. Imagine a criação de uma regra que impeça o tráfego do protocolo FTP. Ao invés de configurá-la no firewall que está rodando no sistema operacional da máquina do usuário, a configuração numa máquina com vPro é feita no que poderíamos considerar como sendo a interface de configuração do firmware da placa de rede (**figura 3**). Ou seja, a máquina do usuário sequer precisa ter um sistema operacional instalado no HD para podermos fazer este ajuste. Aliás, é bom frisar desde já aqui, que o comentário anterior vale para todas as funcionalidades descritas acima.

Qual é o segredo? Primeiro, no hardware. Tudo começa na placa de rede, que precisa de um circuito eletrônico extra que a capacita a suportar o chamado acesso *out-of-band*. Na prática, isso significa que podemos atribuir um endereço e demais parâmetros IP a ela (gateway, máscara e DNS), independentemente da máquina ter ou não sistema operacional instalado. A partir de então, esteja esse desktop atrás de um roteador ou diretamente conectado ao modem de acesso à Internet, o fato é que ela fica alcançável a qualquer máquina do mundo que tenha um browser e conectividade com a Internet (**figura 4**).

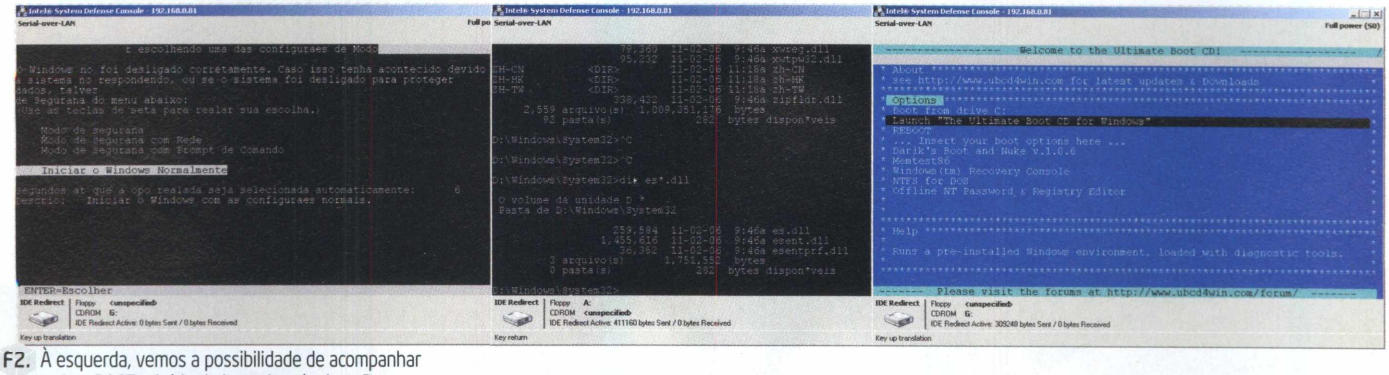
Veja na **figura 5** que os filtros e sensores de configuração da placa de rede estão,



F1. BIOS da máquina vPro na sua frente, é você com controle total no sistema remoto.

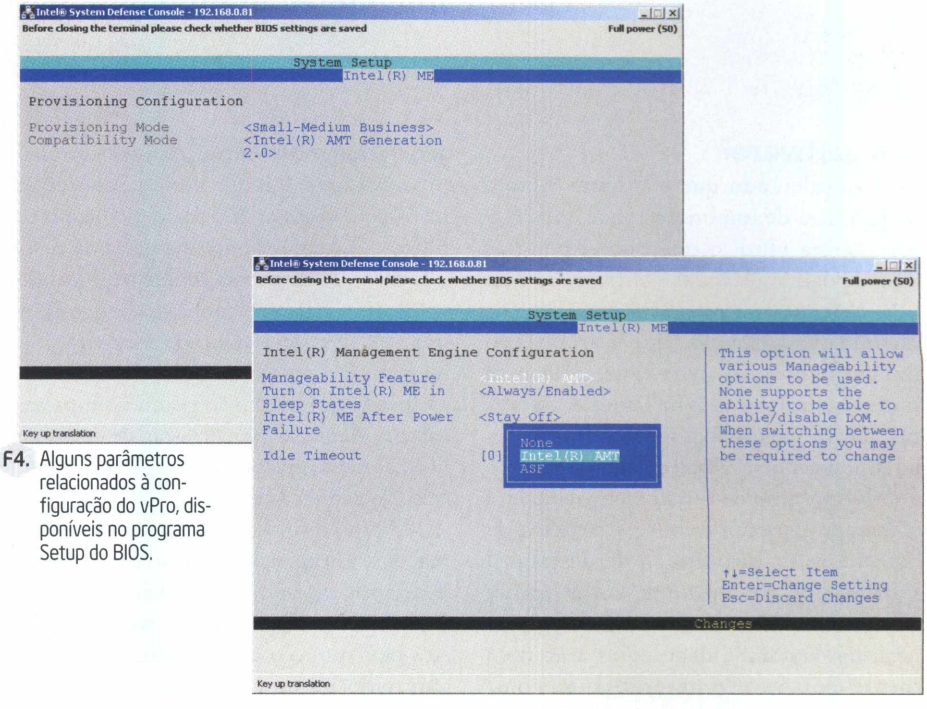


F3. Acesso à Internet bloqueado remotamente e direto no hardware.

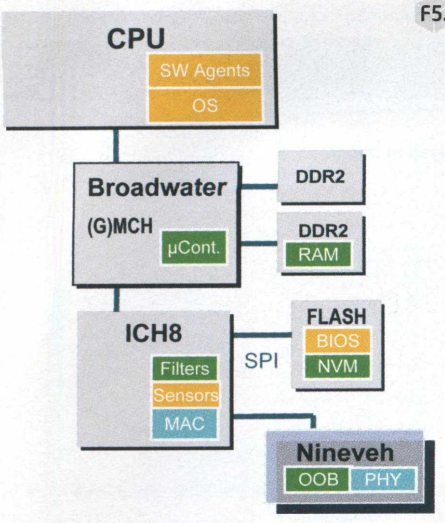


F2. À esquerda, vemos a possibilidade de acompanhar todo o POST e início do boot da máquina vPro remota; dependendo do problema, podemos fazer um boot remoto controlado e corrigi-lo rapidamente.

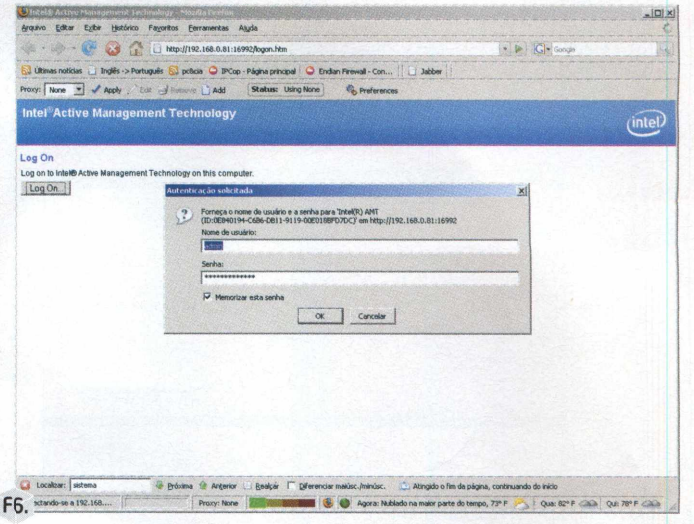
junto com o componente responsável pela camada MAC, integrados no SouthBridge (Ponte Sul) do chipset. Fica evidente, portanto, que esse Ponte Sul não pode ser qualquer chip, tem que ser um modelo específico (no caso do ICH8, é o ICH8DO) provido dos sensores, por exemplo, necessários para desconectar automaticamente a máquina da rede no momento em que se detecta um tráfego malicioso passando pela interface. Continuando, o próximo "segredo" está no chip Flash ROM da placa-mãe, onde normalmente está o BIOS. Além deste e do programa Setup, as placas-mãe vPro também trazem neste chip o software que é carregado durante esses acessos *out-of-band* recepcionados pela interface de rede. E quem carrega esse software na memória RAM é um microcontrolador presente no NorthBridge (Ponte Norte) do chipset.



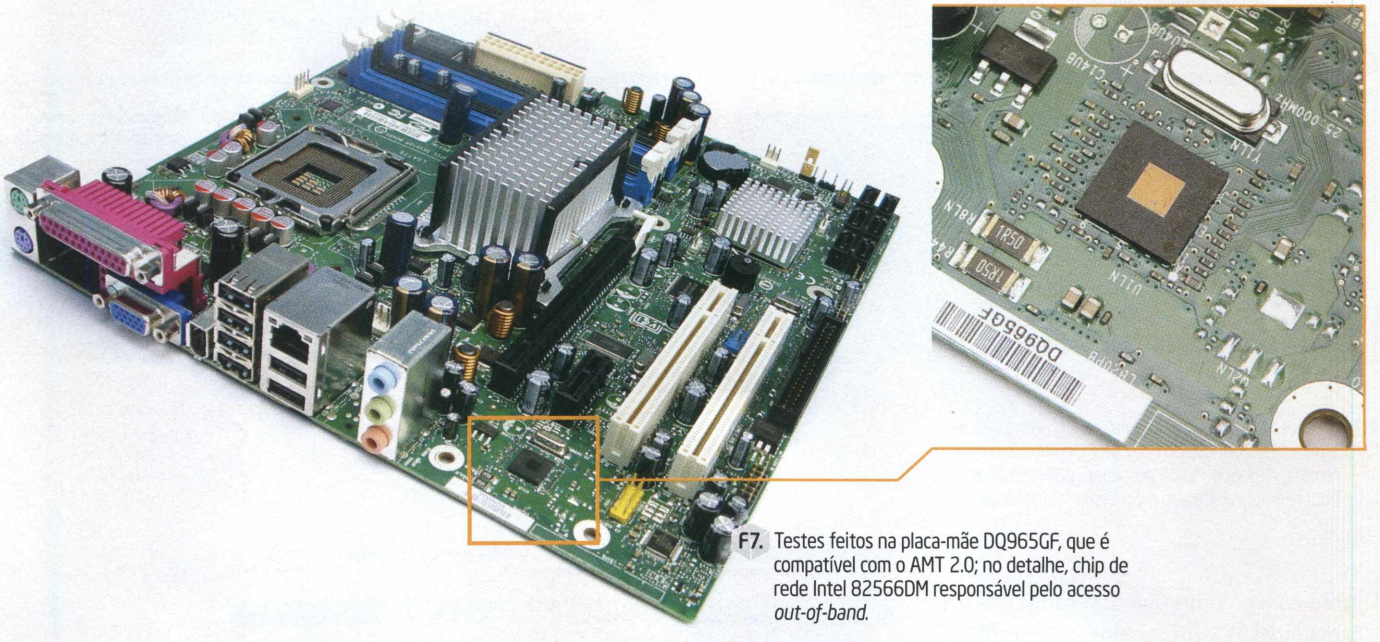
F4. Alguns parâmetros relacionados à configuração do vPro, disponíveis no programa Setup do BIOS.



F5. Componentes do hardware relacionados com vPro.



Após configurar o vPro na máquina do cliente, essa é a interface que você verá durante o acesso remoto, via browser; note, na barra de endereços, a necessidade de especificar a porta TCP 16992. **F6.**



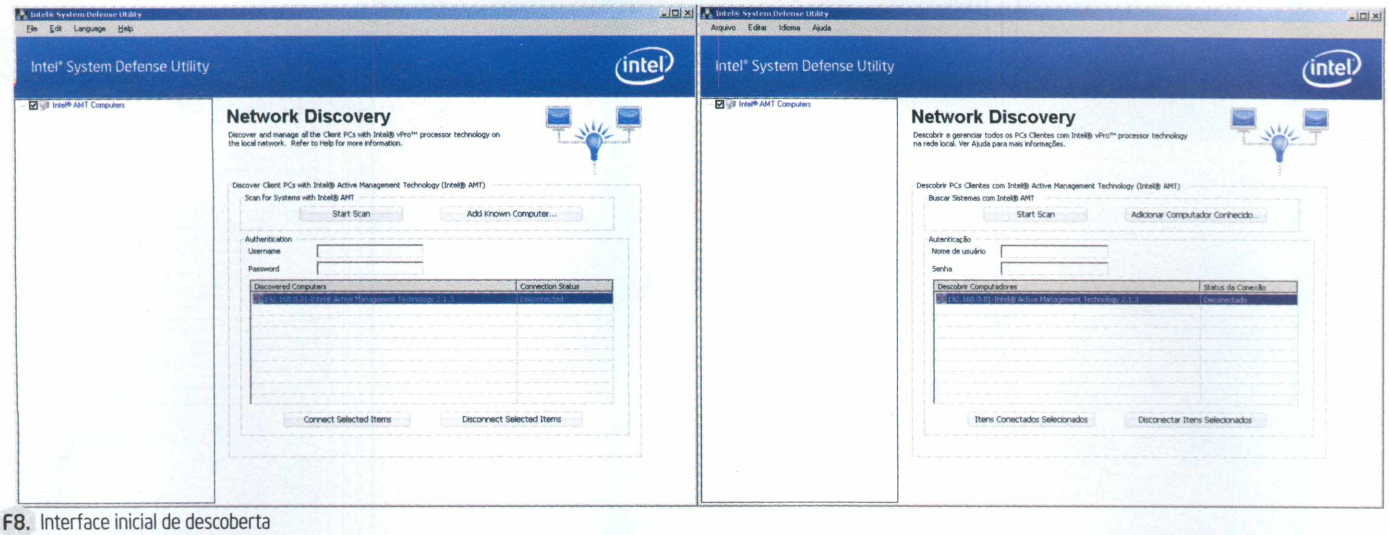
F7. Testes feitos na placa-mãe DQ965GF, que é compatível com o AMT 2.0; no detalhe, chip de rede Intel 82566DM responsável pelo acesso *out-of-band*.

E o software?

Considerando que o usuário remoto só precisará de um browser para controlar a máquina vPro, o que estaria por trás dos supostos softwares compatíveis com vPro? A resposta para a questão está na quantidade de recursos que fica visível ao usuário remoto em cada caso. Com uma suíte de gerenciamento da Landesk, Altiris, HP, entre outros, há agentes instalados no sistema operacional da máquina vPro e todo um ambiente de desenvolvimento preparado para aproveitar os recursos do hardware. Nesse ponto, vale destacar a existência de um kit de desenvolvimento de software (SDK - Software Development Kit), de disponibilidade pública gratuita (**http://softwarecommunity.intel.com/articles/eng/1023.htm**), através do qual uma Software House pode conhecer as instruções necessárias para implementar os filtros que bem entender na placa de rede, por exemplo. E depois cobrar pelo uso do software, é claro. O "problema" é que até o momento a visão de mercado acerca do vPro foi fundamentalmente elitista, ou melhor, só focada em médias e grandes empresas capazes de pagar por licenças de software normalmente inacessíveis à realidade financeira de pequenas empresas e escritórios.

Mas no outro caso, o da solução mínima, baseada apenas no acesso feito a partir de um browser remoto, não seria possível fazer um boot controlado, por exemplo? Até bem pouco tempo, não. Conforme abordado na edição 69, as funções de software nativas da placa-mãe eram bem limitadas. As funções mais úteis se limitavam a um inventário de hardware (modelo de processador, HD, versão de BIOS e quantidade de módulos de RAM instalados), ao log de erros durante a inicialização e a um controle remoto mínimo, do tipo liga/desliga (**figura 6**).

Felizmente, isso mudou com a chegada de um software desenvolvido pela Intel e que roda apenas em suas placas-mãe da série "Executive": o System Defense Utility (SDU). Na atual versão 1.7, ele é distribuído em um arquivo zipado de 3,3 MB e pode ser instalado nos Windows XP e Vista 32 bits. Ele deve ser instalado na máquina do técnico, administrador ou analista de suporte responsável pelas

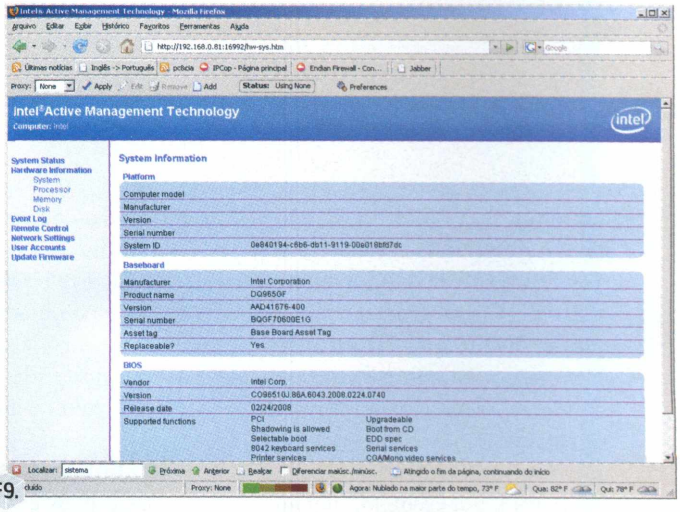


F8. Interface inicial de descoberta do SDU: software pode ser usado em português, mas tradução ainda precisa de muitos retoques.

máquinas vPro remotas. Quer dizer que não muda nada na máquina vPro? Exatamente. Nesta, os passos continuam sendo os analisados anteriormente na PC&CIA 69. Ou seja, após montar a máquina, basta ir até o Setup do BIOS (figura 4), habilitar o vPro e configurar os parâmetros básicos relacionados, tais como endereço IP, senha de acesso e modo de funcionamento (no *caso aqui, a opção* que deve ser escolhida é a "Small-Medium Business). O manual fornecido traz um guia bem detalhado a esse respeito.

Testes

Além da placa-mãe Intel DQ965GF (**figura 7**), utilizamos dois módulos de memória DDR2-800 de 1 GB operando em Dual-Channel e um processador Pentium 4 HT 630 rodando o Windows Vista Ultimate 32 bits. Não é a configuração vPro idealizada pela Intel porque não usa um processador da família Core 2, mas por outro lado é plenamente funcional. Na prática, para os testes e funcionalidades comentados nesta matéria, tanto faz usar um Core 2 ou um Celeron, por exemplo. Em relação às memórias, o Dual-Channel não é obrigatório, a única exigência é a instalação de um módulo no primeiro soquete, o DIMM 0, em cuja área é feito o mapeamento de 8 MB para a carga do software de controle (firmware) da placa de rede.



Informações de inventário disponíveis na interface web. **F9.**

Agora vamos à prática. Após instalar o SDU no estilo Next > Finish, na primeira página podemos tanto adicionar um computador vPro manualmente, ou então realizar a sua descoberta através da rede. Para isso, é necessário fornecer o nome de usuário e a senha configurada na máquina vPro (**figura 8**).

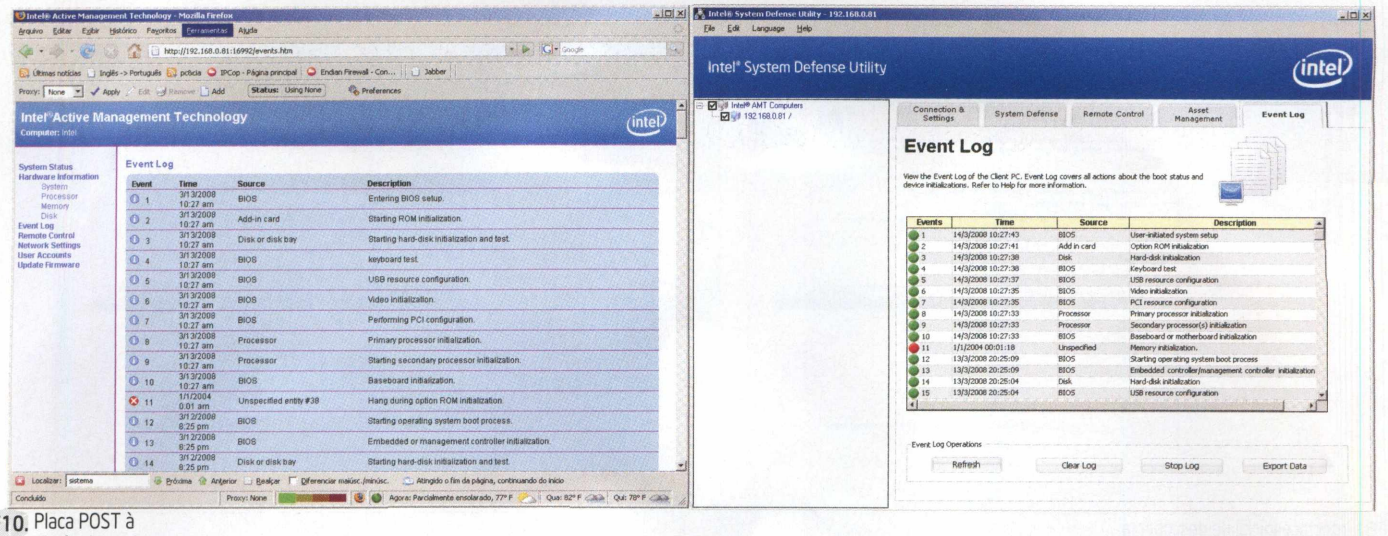
A fim de facilitar nosso estudo, o objetivo agora é realizar um comparativo de funções disponibilizada pelo SDU e pelo acesso direto ao browser:

1) Estado do sistema:

- O SDU só mostra que a máquina vPro está ligada, tal como no estado S0_Powered, e gerenciada remotamente;
- Já o browser web, além de mostrar o status ligado (On), também exibe o endereço IP, ID do sistema, data e hora.

2) Inventário do Hardware

- No SDU, o menu é o Asset Management, o qual mostra o fabricante, modelo e versão da placa-mãe, modelos de HD e drive óptico, informação básica do processador e módulos de RAM instalados (número do slot ocupado, tecnologia da RAM, capacidade e freqüência máxima de operação);
- A interface Web, é dividida em 4 telas: em system, mostra a mais o número serial da placa-mãe, string de inicialização do BIOS com revisão (**figura 9**), data e funções suportadas; em processador, vemos como funções extras a identificação do soquete, freqüência máxima suportada, ID, enfim, informações mais completas; em memória, mostra o Part Number e código do fabricante.



F10. Placa POST à distância: web x SDU.

3) Logging

- Com ambos, SDU e web, os registros dos testes realizados durante o POST ficam armazenados na página Event Log (**figura 10**). Além disso, ambos exibem essencialmente as mesmas informações registradas, mas com diferenças sutis no texto, em vários registros. No item 14, por exemplo, enquanto o SDU usa a expressão "Hard-disk initialization" para se referir à inicialização do HD, a interface Web registra como "Starting hard-disk initialization and test". No item 10, o SDU cita "Baseboard or motherboard initialization" para a inicialização da placa-mãe, ao passo que, via Web, vemos "Baseboard initialization". E no item 11, que registrou o erro forçado durante os nossos testes, que foi o de ligar a máquina sem nenhum módulo de memória instalado, o SDU registrou como "Memory Initialization", enquanto o Web o fez como "Hang during option ROM initialization", em uma referência indireta ao fato de não haver RAM instalada para receber a carga da memória Flash ROM. Apesar das diferenças nas mensagens, o importante a destacar aqui é a agilidade que a equipe de suporte ganha ao poder acompanhar o POST da máquina remota. Neste último caso simulado acima, pelo menos o técnico já sairia da "base" ciente da necessidade de substituição do módulo de memória.

4) Contas de usuário

Neste item é possível criar contas de usuários que poderão acessar a máquina vPro. O recurso só está disponível através da interface web e as permissões incluem a possibilidade de visualizar o inventário (Hardware Information), o log de eventos de POST (Event Log), fazer o controle remoto (Remote Control) e atualizar o firmware (Update Firmware).

Já no SDU, só é possível ver quais usuários estão cadastrados no sistema. Um detalhe interessante aqui é a existência de um número de permissões muito maior (16 ao todo), exemplificada, por exemplo, pelas opções "Circuit Breaker" (poder configurar a desconexão automática da máquina vPro da rede em casos de tráfego malicioso), "Agent presence local" (informar o técnico remoto caso o agente da suíte de gerenciamento vPro seja impedido de atuar no sistema operacional), etc. Acreditamos que em futuras versões do SDU seja possível definir ou alterar as permissões através de sua interface.

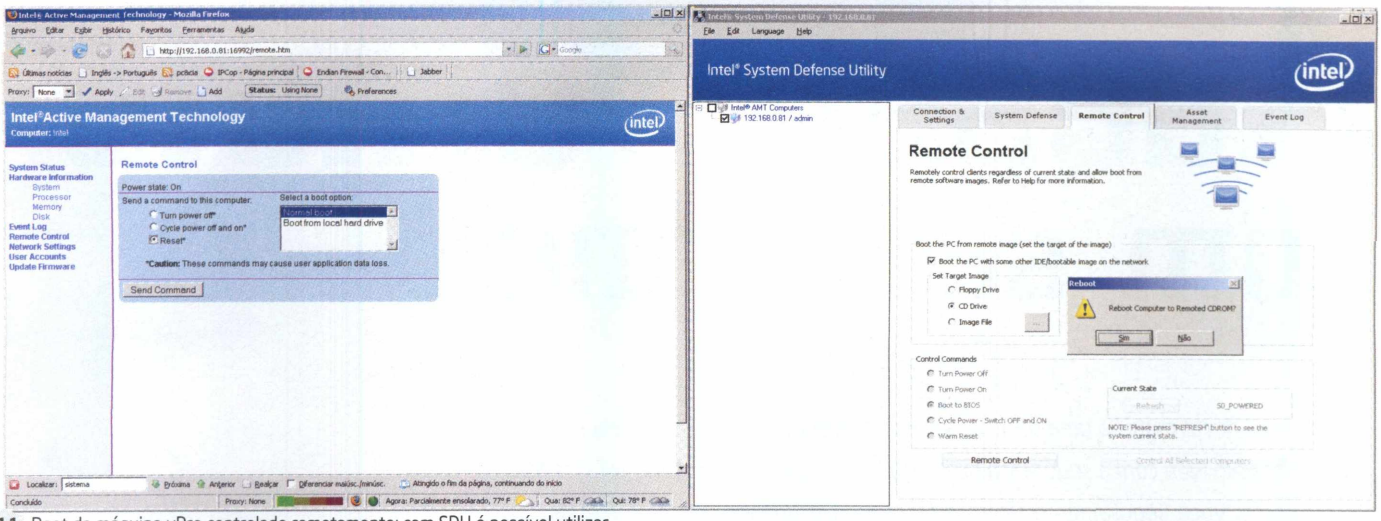
5) Configurações da placa de rede vPro

- Pela interface web é possível alterar todos os parâmetros relacionados à configuração da rede, as quais são definidas primeiramente na própria máquina vPro, via Setup do BIOS. Assim, podemos ajustar remotamente o nome de máquina, os endereços do protocolo TCP/IP, a identificação da VLAN (Virtual LAN, caso exista na infra-estrutura);
- O SDU, por sua vez, além de não trazer as informações de IP e nome de computador (e ainda mostrou incorretamente uma suposta configuração de DHCP, sendo que o IP havia sido definido como fixo), não mostra opção para VLAN. Basicamente, ele só permite entrar com os endereços dos parâmetros TCP/IP.

6) Mais segurança

Neste item entra um trunfo do SDU: a segurança. É aqui que começa a valer aquele comentário feito anteriormente acerca da possibilidade de configurar controles normalmente disponíveis apenas em firewalls. O que na "linguagem" vPro é conhecido como System Defense.

Os filtros mais simples dizem respeito a bloquear a resposta a ping (o que a in-



F11. Boot da máquina vPro controlado remotamente; com SDU é possível utilizar floppy, drive óptico e inclusive disparar uma instalação nova de sistema operacional pela rede, basta criar uma imagem do sistema com arquivo de resposta configurado.

terface web também disponibiliza, mas é só) e habilitar a contenção contra pacotes de *anti-spoofing*. Mais abaixo na figura 3 vemos algumas opções interessantes que podem ser vistas como perfis de atuação da placa de rede: sem acesso Internet, apenas local; bloquear ou liberar protocolos comuns (HTTP, remote desktop, SSL, Telnet e SMTP), ou ainda toda uma faixa de portas (pode ser todas, por exemplo, de 0 a 65535), e por último definir a opção "sem restrições no uso da Internet" (No restriction on Internet). Os testes realizados corresponderam com a nossa expectativa e o que mais chamou a atenção foi a rapidez para a efetivação dos ajustes. Por exemplo, estando o usuário da máquina vPro navegando normalmente com o seu Windows Vista Ultimate, bastava clicar na opção "No Internet Access" e em "Apply Changes" do SDU, na máquina remota, para imediatamente após o usuário do Vista perder conectividade com a Internet. É interessante notar que o System Defense não retorna qualquer mensagem para o navegador ou qualquer outro programa que tente acessar a Internet na máquina vPro. Ou seja, o usuário simplesmente perde a conexão e não há o que possa fazer para restabelecê-la. Usar o SDU na máquina local? Esquece, pois a interface de rede vPro não aceita conexões provenientes da própria máquina;

7) Controle Remoto

- Em ambos, é acessado via menu Remote Control, porém o SDU é bem mais completo, pois permite ligar, desligar, forçar a inicialização do Setup do BIOS durante a inicialização da máquina vPro e transferir o console para o seu PC, além de também permitir um boot remoto totalmente controlado (**figura 11**).

Enquanto isso, pela interface web só é possível ligar, desligar e fazer um reset, além de controlar o boot, mas sempre carregando o sistema a partir de alguma unidade de disco da própria máquina vPro. Ou seja, seria necessário pedir ao usuário para inserir um CD no drive óptico para disparar uma nova instalação do sistema.

Conclusão

Acessar o BIOS, conhecer a causa de um problema que esteja impedindo a inicialização e, se preciso for, poder puxar o console da máquina remota para o seu monitor a fim de substituir um arquivo crítico do sistema operacional, além de ter literalmente um firewall integrado no hardware. São muitos os benefícios trazidos pelo software System Defense Utility. É verdade que ainda há muito a se melhorar, a exemplo do que deve ter ficado claro ao demonstrarmos as opções que só estão disponíveis em uma ou outra interface (a web) e dos erros de tradução para o idioma português. Mas uma coisa é certa: trata-se de um tremendo valor agregado!

Só para se ter uma idéia, não faz muito tempo que este tipo de funcionalidade ficava restrito a hardware de equipamentos "especiais", nos quais somente o hardware de rede (um Terminal Server, por exemplo) custava mais do que o dobro do que custa uma placa-mãe como a DQ965GF (cotada a R$ 450 em **www.viabrasil.net**). No site **http://downloadcenter.intel.com/Detail_Desc.aspx?agr=N&DwnldID=15362** você encontra uma listagem dos 5 modelos de placas-mãe compatíveis com a tecnologia vPro, com destaque para as duas primeiras, DQ35JO e DQ35MP, as quais utilizam um chipset compatível com a especificação AMT 3.0 (Q35 com Ponte Sul ICH9DO) e, como tal, oferecem ainda outros recursos adicionais, a exemplo do Circuit Breaker descrito neste artigo.

Portanto, se hora de máquina parada à toa e especulação na hora de realizar um suporte técnico são questões que você pretende abolir de seu ambiente de TI ou círculo de relacionamento com clientes, estamos sim diante de uma solução de ótima relação custo/benefício e que deve seguramente ser considerada nos próximos investimentos. **PC**

Acesso remoto com segurança

Conheça nesta matéria uma solução para ambientes Windows que une a flexibilidade do acesso web com a segurança proposta pela dupla de protocolos HTTPS/SSL. Depois disso, você seguramente ficará mais tranqüilo quando precisar acessar um recurso remoto.

Com o preço dos notebooks caindo a cada dia e com o aumento da oferta de produtos que oferecem acesso à Internet sem fio por parte das operadoras de telefonia do nosso país, torna-se impossível não pensar numa palavra que está começando a fazer parte do nosso dia-a-dia: "mobilidade".

É grande a tentação de poder levar conosco um computador completo com acesso sem fio à Internet. Hoje podemos comprar um notebook com gravador de DVD e tudo o mais por um preço médio de R$ 1.500,00. Isto somado ao acesso à Internet sem fio por um preço médio de R$ 100,00. Sendo assim, além daqueles *cases* com diversas ferramentas de suporte, um técnico de campo pode levar consigo um sistema completo que pode ser usado para salvar o cliente de qualquer situação.

Apesar disso, não é uma idéia interessante sair por aí com um computador contendo todos os seus dados, pois algum incidente (um assalto, por exemplo) poderia fazê-lo perder todas essas informações.

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

Mesmo quando pensamos em ter um backup dos dados, que se torna imprescindível em cenários como este, o transtorno de ter que instalar e reconfigurar tudo em um novo equipamento, além do próprio prejuízo causado pela perda do equipamento, torna-se um limitador para o uso deste tipo de solução.

Diante desse cenário, é bem provável que muitos técnicos continuem usando os referidos *cases* por um bom tempo. Ocorre que nestas situações o técnico precisa de algum tipo de ferramenta que ofereça acesso remoto aos dados existentes em seu computador desktop de casa, através da máquina do cliente usando a Internet.

Outro cenário interessante para expor aqui é aquele no qual o seu cliente possui uma empresa que trabalha com uma matriz com, pelo menos, uma filial. Imagine que lá na filial seja necessário atualizar, via Internet, uma réplica de uma planilha também usada na matriz.

Nos dois cenários apresentados, o protocolo para transferência de arquivos FTP (File Transfer Protocol) é uma solução bastante interessante. A questão que fica é a seguinte: o que fazer quando, em qualquer uma das situações expostas, precisarmos de segurança durante a transferência dos dados? O FTP não pode ajudar porque não possui nenhum recurso de segurança.

Existem diversas maneiras de contornar esta situação. Uma delas seria com a utilização de uma VPN, por exemplo. O problema é que implementar uma solução assim nem sempre é uma tarefa simples.

Bem, a proposta desta matéria é exatamente a de apresentar mais uma alternativa para essas situações, ou seja, cenários onde seja necessário usar a Internet para fazer uma transferência dos dados de forma segura.

O que é WebDAV?

É a sigla para Web Distributed Authoring and Versioning, uma tecnologia que oferece a possibilidade de transferir arquivos usando os protocolos HTTP ou HTTPS. Ao usar o HTTPS, o WebDAV se equipara em segurança à tecnologia que protege o tráfego de dados em sites de bancos, por exemplo.

Uma solução baseada em WebDAV é especialmente interessante porque ela é mais simples de implementar. Quem já teve de configurar uma conexão VPN (PPTP ou L2TP) e precisou liberar o seu respectivo tráfego através de um firewall, sabe que estas duas etapas de configuração são trabalhosas. Porém, a implementação de um site seguro com a sua respectiva liberação no firewall é bem mais simples.

Preparando o laboratório de testes

No cenário que utilizaremos para explicar o funcionamento do WebDAV, uma empresa fictícia possui um site denominado **www.meusite.com.br** e precisa habilitar a transferência dos arquivos do

site para o servidor de forma segura, através da Internet.

Para reproduzirmos este cenário, precisaremos de um servidor web executando o Windows Server 2003 SP2 (o SP2 não é obrigatório para o laboratório) que será configurado com o endereço IP 192.168.100.1/24. Além disso, configure o gateway desta interface para apontar para o endereço 192.168.100.4, que será o endereço IP do roteador da rede. Este servidor também irá desempenhar o papel de controlador de domínio e de servidor DNS.

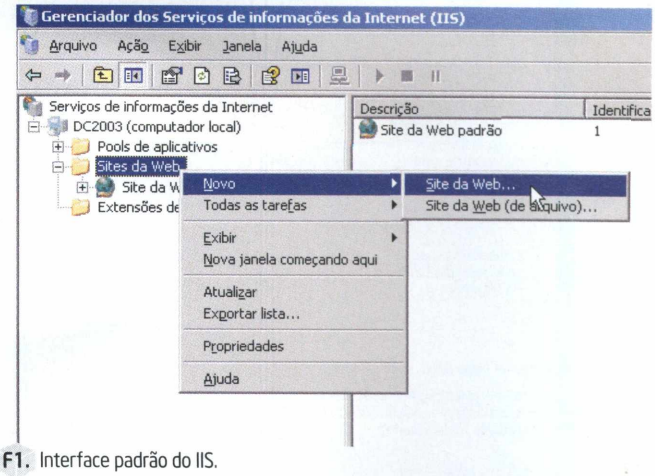
Um segundo servidor também com Windows Server 2003 SP2 será configurado com duas interfaces de rede. Uma delas será configurada com o IP 192.168.100.4/24 e representa a interface que será usada para a comunicação com a rede local. Nesta mesma interface, configure o endereço do servidor DNS preferencial como 192.168.100.1. A segunda interface será configurada com o endereço IP 200.200.200.1/24 e representa o endereço IP externo desta máquina. Este computador será o roteador da rede e executará o serviço de Roteamento e Acesso Remoto (RRAS) do Windows.

Uma última máquina, executando o Windows XP Professional SP2, será usada para representar o computador da rede externa, ou seja, a máquina que está na Internet. Nesta máquina, configure a interface de rede para usar o IP 200.200.200.2/24.

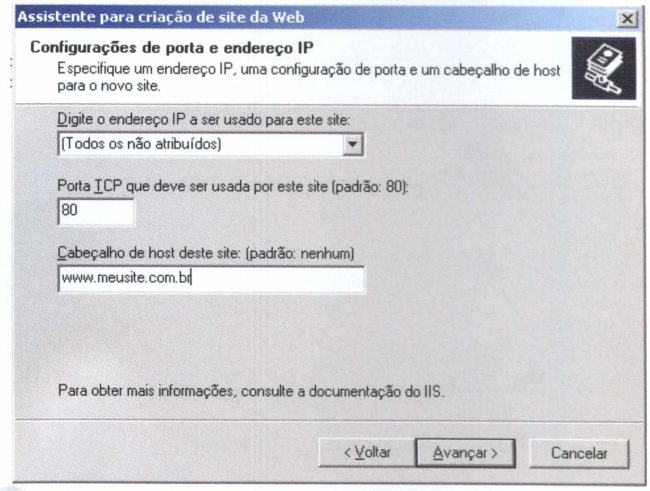
Como configurar?

Para começarmos, use o comando DCPROMO para configurar o servidor da rede interna como controlador de domínio para o domínio meusite.local. Não se esqueça de instalar o serviço DNS como parte do processo de criação do domínio.

Feito isso, vamos configurar o Web Server. Para isso, insira o CD de instalação do Windows Server 2003 na unidade e aguarde a tela de boas vindas. Quando a mesma aparecer, clique na opção **Instalar componentes opcionais do Windows**. A caixa para adicionar ou remover componentes do Windows será aberta. Role a lista até encontrar a opção **Servidor de aplicativos** e marque a caixa para seleção. Clique em **Avançar** e aguarde o término da configuração. Esse procedimento instalará o **Serviço de Informações da Internet** (IIS 6.0) no servidor usando as opções padrão, ou seja, permitindo apenas o funcionamento de sites com HTML estático. Vale ressaltar que quando nos referimos a conteúdo estático, estamos falando sobre extensões que são executadas diretamente no servidor (ASP, PHP etc). JavaScript, por exemplo, é executado na máquina cliente e, desta forma, sites que utilizam código nesta linguagem não são afetados pelo comportamento padrão do IIS 6.0.



F1. Interface padrão do IIS.



F2. Dados para confihuração do site.

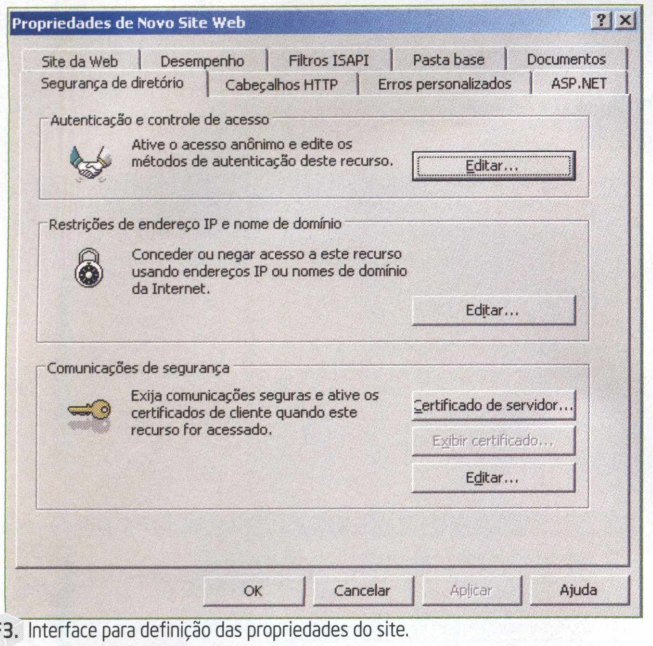
Depois que o processo for concluído, você precisa verificar se o IIS foi corretamente instalado. Para isso, abra uma janela de browser e digite "localhost", sem aspas, na barra de endereços. Se tudo estiver certo, será exibida uma página informando que o site se encontra em construção.

Com o IIS funcionando, abra o console **Gerenciamento do Serviço de Informações da Internet** dentro de **Ferramentas administrativas**. No painel da esquerda, clique com o botão direito do mouse sobre **Sites da web > Novo > Site da Web** (**figura 1**).

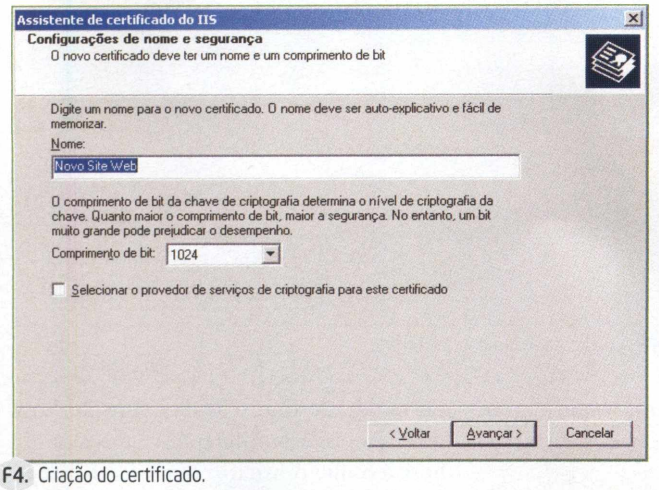
Na primeira janela do assistente que se abre, clique no botão **Avançar**. Na próxima tela, o assistente irá lhe pedir uma descrição para o site, informação esta que será usada apenas para exibição dentro do console de gerenciamento do IIS. Para o nosso exemplo, colocamos **Novo Site Web**. Feito isso, clique em **Avançar**.

Agora você deverá definir um endereço IP para o site que está sendo criado e informar a porta de escuta que será usada. É possível ter vários sites web funcionando com o mesmo endereço IP e na mesma porta, desde que o **Cabeçalho de host** dos mesmos seja diferente. Cabeçalho de host é o que o usuário digita na barra de endereços do navegador para acessar o site. Por exemplo, **www.registro.br** e **www.revistapcecia.com.br** são dois cabeçalhos de host diferentes. Se você deixar o campo Cabeçalho de host em branco, o IIS entenderá que você deseja que o site seja referenciado pelo endereço IP da máquina. Como o site da web padrão está no ar e o mesmo já é referenciado desta forma (usando o cabeçalho com apenas o endereço IP do servidor Web), o IIS só poderá deixar um dos sites no ar. O site da web padrão ou o **Novo Site** da Web. Para evitar este problema, informaremos o cabeçalho de host **www.meusite.com.br** (**figura 2**). Depois de digitar essa informação, clique em **Avançar**.

Na próxima tela, você deverá informar a pasta onde estão os arquivos do site que será publicado. Vale ressaltar que



F3. Interface para definição das propriedades do site.



F4. Criação do certificado.

o site usado no exemplo já está pronto, ou seja, a página web já foi previamente desenvolvida. No nosso caso, os arquivos se encontram em C:\Meus Sites. A outra opção desta tela, **Permitir acesso anônimo a este site**, pode permanecer marcada, uma vez que nosso objetivo é disponibilizar um site web público que poderá ser acessado por qualquer pessoa. Com as opções preenchidas, clique em **Avançar**.

Agora você deve informar as permissões que serão aplicadas ao site. O site de nosso exemplo utiliza recursos em ASP e, conseqüentemente, precisa das permissões **Leitura** e **Executar scripts**. Marque as duas e clique em **Avançar**. Na última tela do assistente, basta clicar no botão **Concluir** para finalizar o processo.

Com o site Web no ar, iremos para a segunda etapa da configuração do mesmo. Como foi dito no início da matéria, o WebDAV permite fazer a transferência de arquivos usando HTTP ou HTTPS. Este último trabalha de forma criptografada usando SSL e para isso é necessário usar um certificado digital. A nossa próxima tarefa, portanto, será a de associar o nosso site a um certificado digital. Para isso, será necessário que uma **Autoridade de certificação** emita o referido certificado para o nosso site e que todas as partes envolvidas (servidor web e a máquina cliente) confiem na mesma. Se esta confiança não existir, ao abrir o site o cliente verá um aviso de segurança informando que não confia na Autoridade de certificação emissora do certificado que está sendo usado pelo site.

Para completar esta tarefa iremos instalar o **Serviço de certificados** do próprio Windows Server 2003. Abra o **Adicionar/Remover componentes do Windows** da mesma forma como foi feito anteriormente quando adicionamos o IIS no sistema. Na lista de opções, selecione **Serviço de certificados** e siga as informações do assistente até que o serviço esteja instalado (como a configuração de uma Autoridade de certificação possui diversos detalhes que fogem ao escopo desta matéria, você precisará de algum conhecimento prévio sobre esta tarefa).

Por estarmos trabalhando em um ambiente baseado num domínio, você terá de realizar a atualização das diretivas para que o sistema comece a confiar na Autoridade de certificação recém-criada. Isso pode ser feito manualmente com o comando **GPUPDATE** ou depois de 5 minutos (90 minutos para as estações), que é o tempo padrão utilizado pelos controladores de domínio para atualizar as diretivas.

Com as diretivas devidamente atualizadas, abra o console de gerenciamento do IIS, expanda a pasta Sites da Web e clique com o botão direito do mouse sobre o site que nós criamos. Selecione propriedades. Na caixa de propriedades do site, clique na guia **Segurança de diretório** (**figura 3**) e depois no botão **Certificado de servidor**.

No assistente que se abre, clique em **Avançar** na tela de apresentação. Na próxima tela, selecione **Criar um novo certificado** e clique em **Avançar**. O assistente irá lhe perguntar se você deseja criar um arquivo contendo as informações que a Autoridade de certificação precisará para emitir o certificado, ou se você deseja emitir o mesmo para uma Autoridade de certificação que esteja on-line. Como nós configuramos a nossa própria Autoridade de certificação, não é necessário criar um arquivo para envio posterior. Sendo assim, clique na opção **Enviar a solicitação imediatamente a uma autoridade de certificação on-line** e clique no botão **Avançar**.

Agora informe um nome para o certificado (normalmente o nome do próprio site) e o comprimento de bits que será usado na chave. 1024 bits é o valor padrão e já é suficiente (**figura 4**). Depois de preencher as informações, clique em **Avançar**.

Preencha a próxima tela com informações sobre o site. Por exemplo, você poderia fornecer o nome da empresa no campo **Organização** e o nome do departamento no campo **Unidade organizacional**. Estas informações não afetarão a operação do certificado. Ao terminar de preencher, clique em **Avançar**.

Na próxima tela temos um item de configuração bem importante. Devemos fornecer o nome que o cliente usará para acessar o site. Sendo assim, se o usuário for digitar o cabeçalho de host configurado quando criamos o site anteriormente, este cabeçalho deverá ser fornecido no campo **Nome comum** (**figura 5**). Se os dados preenchidos aqui não baterem com o que o usuário digitar na barra de endereços do navegador, um aviso de segurança será exibido. Ao terminar, clique novamente em **Avançar**.

Agora preencha os campos da próxima tela com as informações sobre o **Estado** e a **Cidade** e clique em **Avançar**. Na tela seguinte, deixe a configuração de porta segura padrão

configurada (443), depois informe de qual Autoridade de certificação o certificado será solicitado (**figura 6**) e clique em **Avançar** até concluir o assistente.

Depois que o assistente for concluído, você será levado novamente para a folha de propriedades do site que estamos trabalhando. Se quiser ver o certificado que foi emitido para o seu site, clique no botão **Exibir certificado** (**figura 7**).

Com o site no ar, agora nós iremos configurar o WebDAV. Para isso, em primeiro lugar será necessário ativar o suporte para o referido recurso no IIS. Além disso, iremos aproveitar para habilitar o suporte para a execução de scripts ASP, pois apesar de termos ativado o suporte para a execução de scripts durante o assistente de criação de sites web, por padrão o IIS não irá processar este tipo de extensão (Lembra?). Vale ressaltar aqui que, nesse laboratório especificamente, o suporte para a execução de scripts ASP já estará habilitado, uma vez que o Serviço de certificados fará isso durante o seu processo de instalação (o diretório virtual do Serviço de certificados usa ASP).

Continuando o raciocínio, com o console de gerenciamento do IIS aberto, clique em **Extensões de serviços da web** no painel da esquerda. No painel da direita selecione o componente **WebDAV** e clique no botão **Permitir** (**figura 8**). Faça o mesmo com o componente **Páginas do Active Server**. Feito isso, o suporte para páginas ASP e para WebDAV será habilitado.

Com as extensões habilitadas, iremos criar o diretório virtual que será acessado via WebDAV. Para isso, clique com o botão direito do mouse sobre o site criado e selecione a opção **Novo\ Diretório virtual**.

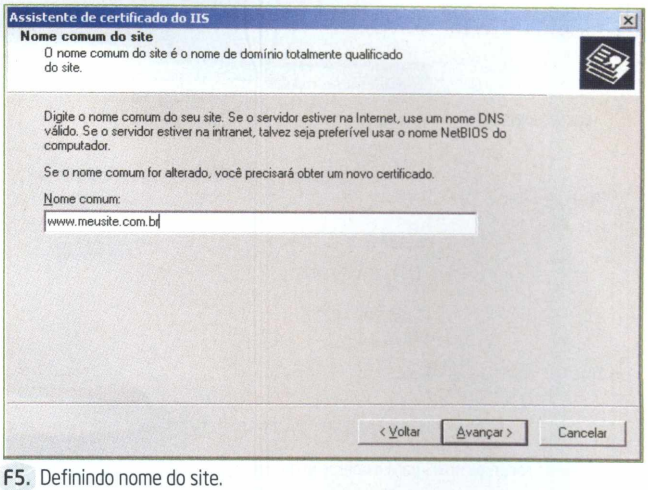
No Assistente que será aberto, clique no botão **Avançar** na primeira tela. Na tela seguinte, o assistente lhe perguntará o nome usado pelo diretório virtual. Aqui vem uma dica importante ao funcionamento: o alias do diretório virtual deve ser "WebDAV" (sem aspas). Na tela seguinte, indique o caminho da pasta do site, o qual pode ser a própria raiz do site criado. No nosso exemplo, é C:\Meus sites.

Na próxima tela você deverá configurar as permissões que serão usadas no diretório virtual. Aqui temos outro ponto importante. Obrigatoriamente as permissões devem ser definidas como **Leitura, Gravação e Procurar** (**figura 9**). Marque as opções apropriadas e clique em **Avançar** para, na última tela de configuração do assistente, clicar no botão **Concluir**.

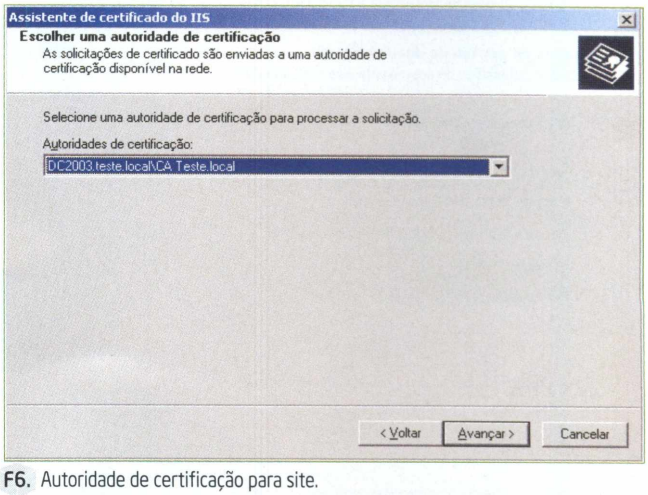
Web site pronto, diretório virtual configurado. Agora precisamos disponibilizar esses conteúdos na Internet. Para alcançar este objetivo, assim como você faria com qualquer roteador, será necessário redirecionar a porta TCP 80 para o tráfego HTTP e a TCP 443 para o tráfego HTTPS, a fim de que o computador que está executando o Windows Server 2003 possa acessar os sites.

Agora precisamos oferecer à máquina cliente as condições necessárias para fazer o acesso. Pelo termo "condições" entenda os seguintes pontos: 1) Podem ser clientes WebDAV as máquinas que estiverem executando o Windows 2000 Professional e/ou Windows XP Professional; 2) A máquina externa deve ser capaz de resolver o nome **www.meusite.com.br**; 3) Permitir que o site seguro (HTTPS) seja acessado pela máquina externa.

Para ultrapassar o primeiro obstáculo, basta criar uma entrada no arquivo **Hosts** da máquina externa, a qual deve apontar o

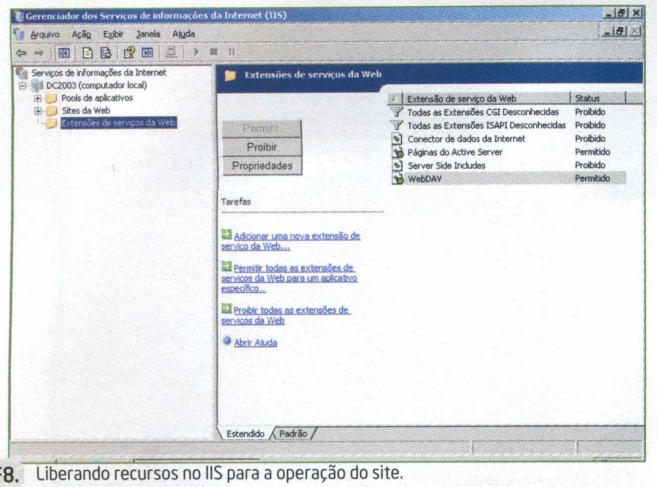


F5. Definindo nome do site.

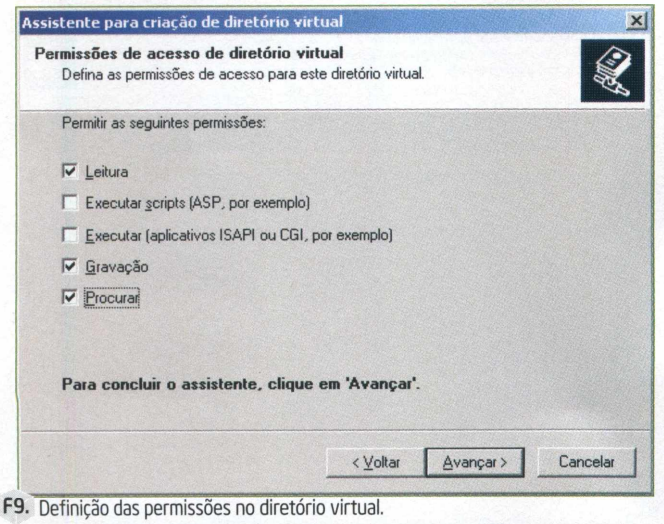


F6. Autoridade de certificação para site.

F7. Resumo das propriedades do certificado.



F8. Liberando recursos no IIS para a operação do site.



F9. Definição das permissões no diretório virtual.

endereço IP 200.200.200.1 como sendo o nome **www.meusite.com.br**. Se fosse num cenário real, seria necessário registrar o domínio **meusite.com.br** para habilitar a resolução do referido nome DNS.

Com relação ao segundo objetivo, será necessário fazer com que a estação confie na autoridade de certificação configurada por você, dentro da rede interna. Para isso, você poderá usar o próprio site do serviço de certificados. Sendo assim, na máquina Windows XP externa, abra o navegador e informe o seguinte endereço: **http://200.200.200.1/certsrv**. Como o redirecionamento do tráfego HTTP e HTTPS foi feito para o servidor web dentro da rede interna, o site do serviço de certificados será aberto (**figura 10**).

Nesta tela, clique na terceira opção, iniciada por "**Fazer o download de um certificado..**". Na próxima página, clique no link **Instale esta cadeia de certificados de autoridade de certificação**. Feito isso, será aberta uma página informando que o certificado da autoridade de certificação foi instalado adequadamente no computador.

Para verificar se tudo está funcionando corretamente, digite na janela do navegador o endereço **https://www.meusite.com.br** (**figura 11**).

Agora precisamos apenas criar a conexão com o diretório WebDAV. Essa tarefa pode ser executada de duas maneiras: 1) Usando o Internet Explorer; 2) Adicionando um novo local de rede. Vejamos como os dois métodos funcionam.

Fazendo a conexão com o Internet Explorer

O Internet Explorer possui um recurso que permite abrir pastas usando o protocolo HTTP/HTTPS. Com o navegador aberto, clique no menu **Arquivo/Abrir**. Se a barra de menus do Internet Explorer (apenas na versão 7) não estiver visível, basta apertar a tecla ALT da esquerda uma vez, para que a mesma seja exibida.

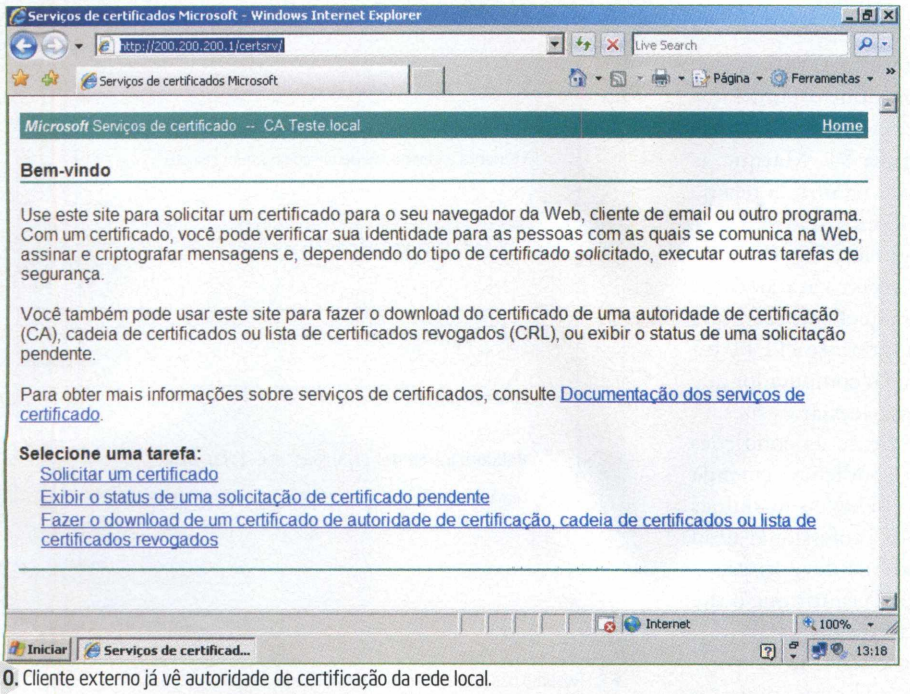
Na caixa que se abre, digite o endereço completo da página, incluindo o diretório virtual (no nosso caso, **https://www.meusite.com.br/webdav**), e marque a opção **Abrir como pasta da Web** (**figura 12**).

Ao clicar em **Ok**, o navegador irá automaticamente adicionar uma entrada em **Meus locais de rede** (**figura 13**).

A outra forma de abrir o diretório remoto é via **Meus locais de rede**. Clique duas vezes em **Adicionar local de rede** nessa janela, na seguinte selecione **Escolher outro local de rede** e clique em **Avançar**. Na próxima tela, informe o caminho completo para chegar ao diretório WebDAV e clique em **Avançar** (**figura 14**).

Na próxima tela basta definir o nome que o diretório remoto terá dentro de **Meus locais de rede**, clicar em **Avançar** e depois em **Concluir**.

Pronto! Independente do método de acesso escolhido, abra a pasta usando o ícone criado em **Meus locais de rede** e desfrute da segurança deste recurso (**figura 15**).



F10. Cliente externo já vê autoridade de certificação da rede local.

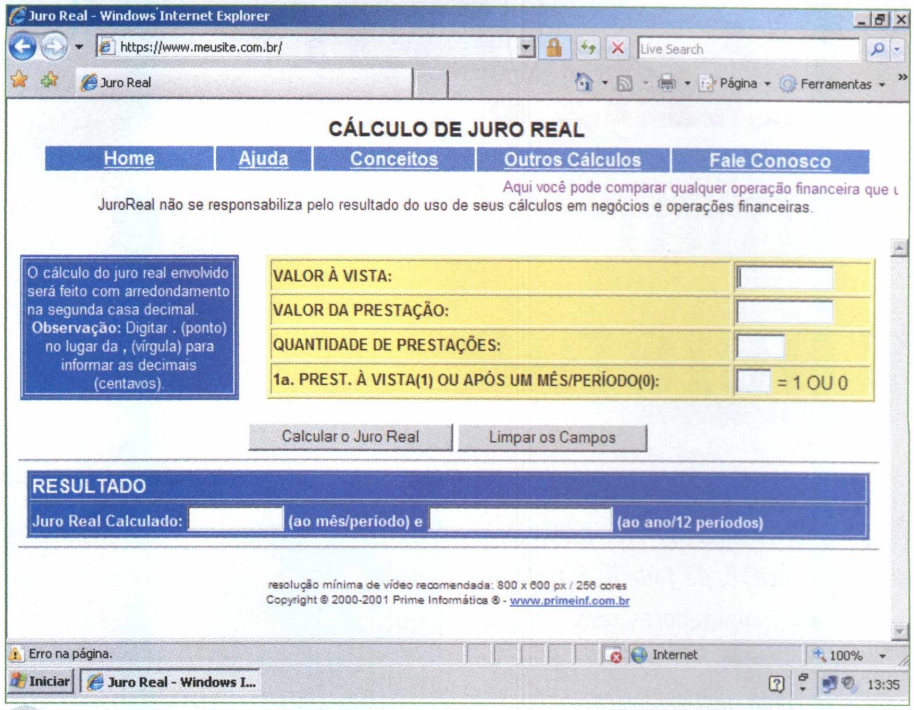
Conclusão

O recurso WebDAV funciona tanto com o protocolo HTTP quanto com o protocolo HTTPS. No exemplo trabalhado neste artigo, apresentamos um modelo que usa o HTTPS pelo fato de se tratar de uma conexão segura e, desta forma, acabar oferecendo um "plus" se comparado às transferências normalmente feitas na web, com o protocolo FTP. Aliás, o recurso torna-se interessante apenas neste tipo de necessidade.

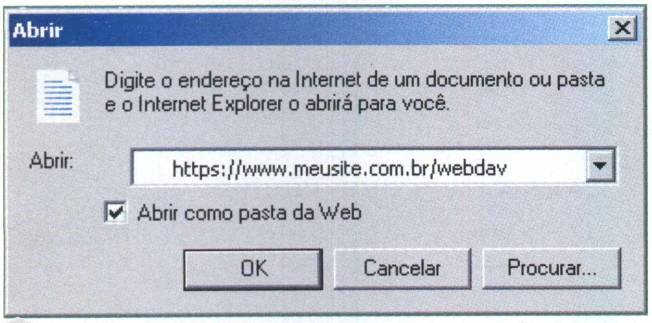
Uma outra possibilidade de uso seria quando a pessoa responsável pela segurança da rede corporativa precisa liberar uma quantidade mínima de portas no firewall. Nesta situação, pode-se usar o WebDAV com o protocolo HTTP mesmo, ou seja, sem a criptografia do tráfego.

Até a próxima e se tiver dúvidas, fique à vontade para entrar em contato conosco!

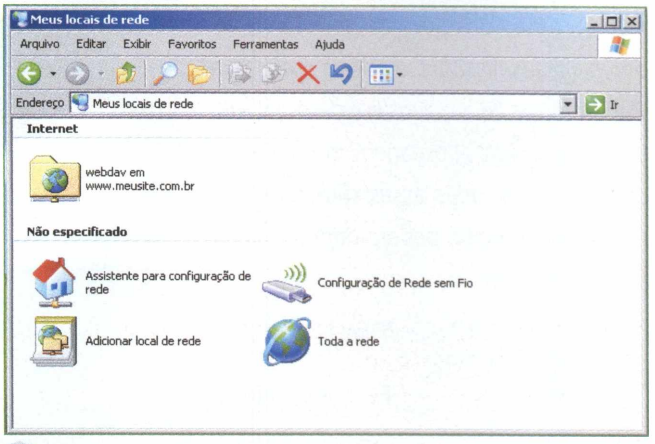
PC



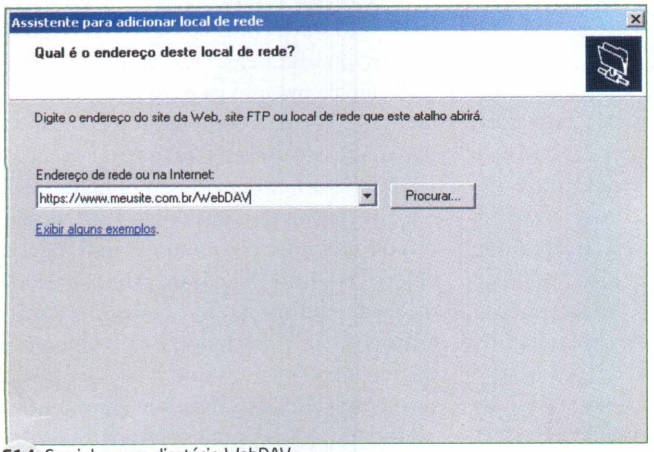
F11. Se você visualizar a página do seu site aqui, está tudo certo.



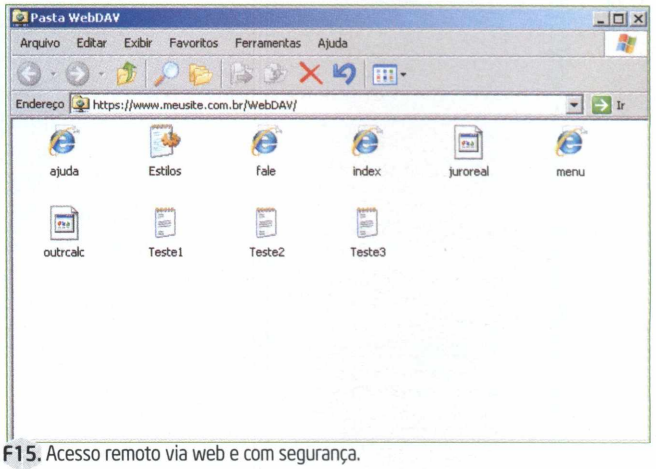
F12. Opção "Abrir como pasta da Web" faz com que IE abra o conteúdo do local especificado como uma pasta do Windows Explorer.



F13. Diretório remoto mapeado e com segurança.



F14. Caminho para diretório WebDAV.



F15. Acesso remoto via web e com segurança.

UltraVNC

Suporte rápido e eficiente

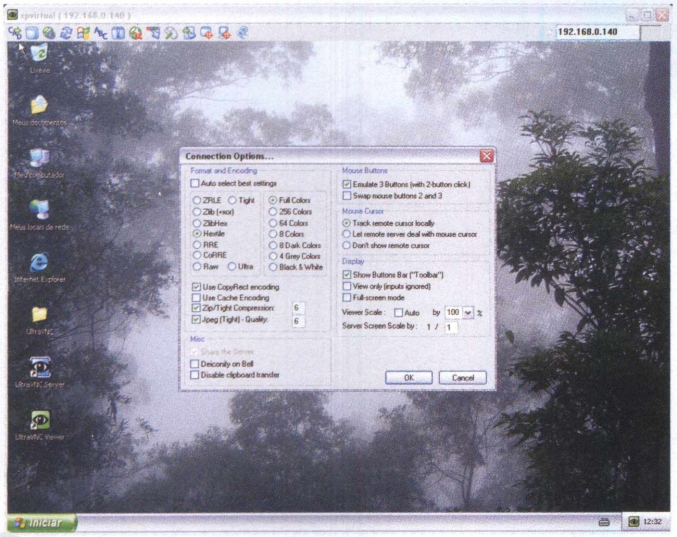
O suporte remoto é visto como uma das tarefas mais básicas de todo profissional de informática. E, de fato, é. Entretanto, acessar os computadores remotamente envolve questões que às vezes não são pensadas, como, por exemplo: a criptografia dos dados, o envio de streaming de áudio, a compressão dos pacotes de rede referentes à transmissão das janelas gráficas, a transferência de arquivos e, é claro, o custo. Em uma rápida abordagem, conheça um software com todas essas características e que, certamente, poderá otimizar o seu suporte técnico.

Fernando Vieira

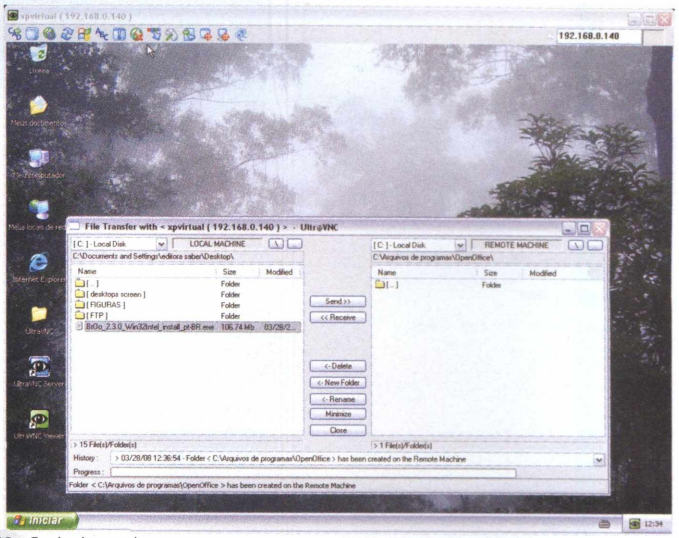
F1. Acesso simultâneo a múltiplas sessões remotas também é possível.

UltraVNC

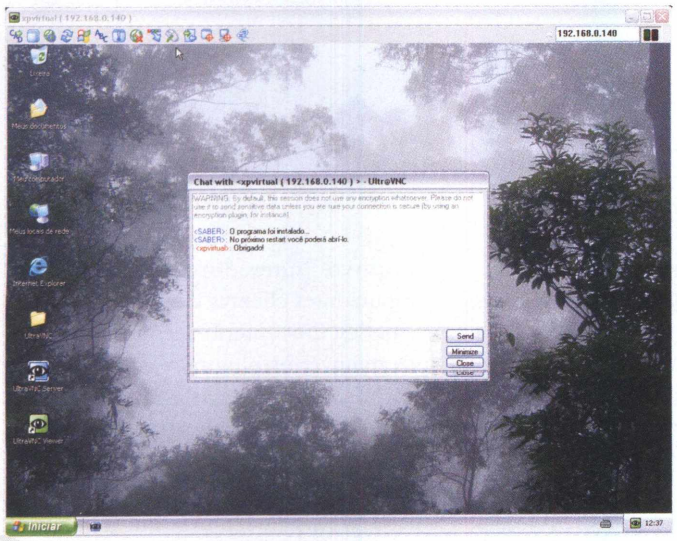
Além de ser um software totalmente livre, o UltraVNC é um dos poucos a reunir as características capazes de fazer frente a qualquer outra versão comercial de VNC. Seu arquivo fonte (2,31 MB) e de instalação (1,67 MB) encontram-se disponíveis para download no site **www.uvnc.com**. Atualmente o UltraVNC é suportado pelas versões Win98, ME, NT4, 2000, XP e 2003 da Microsoft, e é compatível com outros softwares, a exemplo do RealVNC e TightVNC. Seu processo de instalação é simples. Durante a definição do modo de funcionamento, são apresentadas as opções de servidor, *viewer* (cliente) ou ambas. A instalação do modo servidor é indicada para os computadores que queremos acessar remotamente. O modo *viewer* é utilizado na máquina a partir da qual acessaremos os demais computadores. Quando instaladas na mesma máquina, as duas opções permitem que o computador sirva e acesse sessões remotas. Uma vez definido o modo de funcionamento e após alguns "Next", o UltraVNC estará pronto para ser utilizado (**figura 1**). Para a comunicação entre o cliente e servidor, assim como em qualquer software do tipo VNC, é utilizado o protocolo RFP – Remote FrameBuffer - (documentação no site **www.realvnc.com/docs/rfbproto.pdf**).



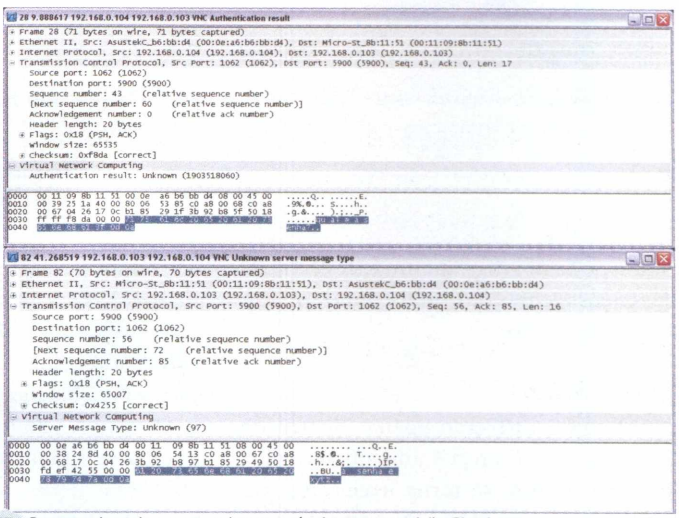
F2. Testes realizados em uma rede de 100 Mbps.



F3. Envio de arquivo para a máquina remota.



F4. Troca de mensagens entre o servidor e o cliente.



F5. Pacotes de redes capturados através do programa WireShark (www.wireshark.org). Repare que as mensagens de texto do "Chat VNC" podem ser facilmente monitoradas.

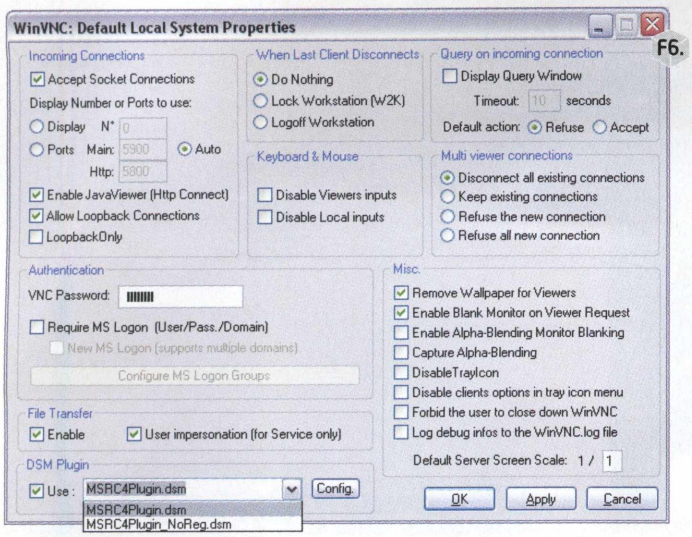
Ferramentas

Na parte superior da interface gráfica é apresentada uma barra com as ferramentas que ficam disponíveis durante a conexão. Para modificarmos os parâmetros utilizados durante a conexão, devemos abrir a ferramenta "Connection Option" (terceiro ícone da esquerda para a direita). Nela podemos definir a quantidade de cores e a codificação (encoding) utilizada durante as transferências das imagens (**figura 2**).

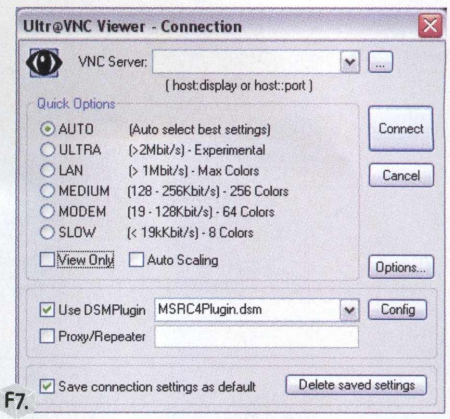
O *encoding* é responsável por formatar os pacotes de rede e, basicamente, especificar o tamanho que eles terão. Ou seja, cada *encoder* da lista possui sua particularidade em relação a vantagens e desvantagens. Por este motivo é que normalmente se utiliza a opção "Auto select best settings". Neste caso, em meio ao processo de *handshaking* o servidor e o cliente iniciam uma negociação para definir o melhor *encoder* e a quantidade de cores. Lembrando que esse processo leva em consideração a vazão do link de conexão e a compatibilidade de *encoders* entre ambos os computadores. Enquanto isso, as demais opções da ferramenta "Connection Option" permitem ajustar o comportamento de eventos do mouse e teclado.

Para iniciar a transferência de arquivos entre os computadores, basta abrir a ferramenta "File Transfer" (quarto ícone da direita para a esquerda). A transferência poderá ocorrer em ambos os sentidos, do cliente para o servidor ou vice-versa. Assim, de forma rápida, podemos instalar qualquer programa sem termos de nos deslocar até a máquina do usuário (**figura 3**).

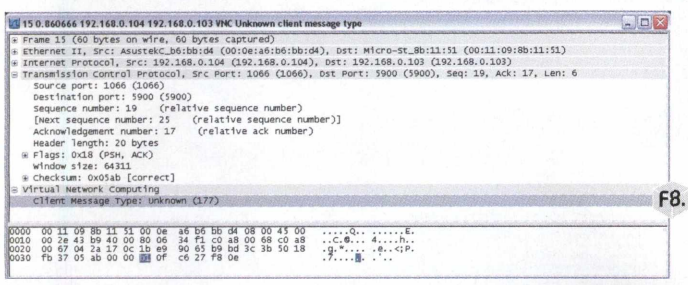
Após a instalação de um programa, ou drivers, podemos utilizar a ferramenta "Chat" para informar ao usuário, através de mensagens instantâneas, que o problema foi resolvido (**figura 4**). Esta ferramenta vem, por exemplo, para auxiliar nos momentos em que é necessário verificar as configurações de som do sistema remoto. Pois o UltraVNC, por enquanto, não faz o envio de *streeming* de áudio pela rede.



F6. Configuração do plugin de criptografia no servidor.



Plugin de criptografia no cliente. **F7.**



F8. Pacotes de dados capturados, mas agora criptografados.

Assim podemos disparar um teste e, através das mensagens, confirmar com o usuário a saída de áudio.

Segurança

Quando utilizado apenas dentro da empresa, a segurança é uma questão que, até certo ponto, se torna irrelevante nas conexões do tipo VNC. No entanto, se o acesso é feito através da Internet, este panorama muda radicalmente, uma vez que sem a criptografia dos dados entre o computador cliente e servidor, nada impede que outra pessoa monitore a sua comunicação VNC. O que na prática significa que todas as informações trafegadas pela Internet, incluído as senhas e mensagens de texto da ferramenta "Chat", estarão passíveis de visualização através de um programa do tipo *sniffer* de rede (**figura 5**).

A fim de resolver esta questão, o UltraVNC passou a suportar a inclusão de plugins que se encarregam de criptografar os dados. Por padrão, o UltraVNC deixa dois plugins pré-disponíveis, o MSRC-4Plugin.dsm e o MSRC4Plugin_NoReg.dsm, dentro da pasta "plugins", localizada no diretório onde o programa foi instalado (Unidade:\PastadeInstalacão\UltraVNC\plugins\). Para utilizarmos estes plugins devemos removê-los (ou copiá-los) para o diretório: Unidade:\PastadeInstalação\UltraVNC. Na interface de administração do UltraVNC, marque a caixa "Use" e, em seguida, selecione o plugin desejado (**figura 6**). Agora clique no botão "Config" e, na janela que será exibida, clique em "Gen Key". Uma nova chave criptográfica será gerada e salva dentro do diretório Unidade:\PastadeInstalacão\UltraVNC\. Renomeie a chave de forma que a parte "new_" seja apagada do nome do arquivo. Por último devemos acrescentar a variável de ambiente "msrc4pluginkey" no sistema. Para isso, acesse as propriedades do ícone meu computador. Na aba "Avançado" clique em "Variáveis de ambiente" e, logo após, no botão "Nova" da caixa "Variáveis do sistema". No campo "Nome da variável:" coloque "msrc4pluginkey"(sem aspas). Em "Valor da Variável:" informe o seguinte diretório: Unidade:\PastadeInstalacão\UltraVNC\nomedachave.key.

Caso você tenha seguido os passos acima na máquina servidora, copie para as demais máquinas (cliente/servidores) o arquivo "nomedoplugin.key". Nos computadores clientes devemos repetir os passos descritos anteriormente, entretanto, após remover os plugins para o diretório do VNC, será necessário apenas marcar a caixa "Use DSMPlugin" (**figura 7**), pois a chave já foi gerada e copiada para o diretório Unidade:\PastadeInstalacão\UltraVNC\. Vale lembrar que a máquina "viewer" também deverá ter a variável de ambiente "msrc4pluginkey" configurada.

Uma vez configurado o recurso de criptografia, a exposição do tráfego dos dados através da Internet deixará de ser um problema (**figura 8**).

Conclusão

Apesar de compatível apenas com a plataforma de sistemas operacionais Windows, o UltraVNC atende muito bem as necessidades de qualquer suporte técnico. Aliás, por se tratar de um software de código aberto, escrito em C ++, nada impede de utilizarmos seu arquivo fonte para gerarmos uma versão para ambientes Linux. Portanto, fica a dica para aqueles que gostariam de otimizar ou melhorar o UltraVNC conforme a necessidade. **PC**

Testador de memória

Anderson Costa

Várias ferramentas excepcionais para manutenção têm um grande contra: o custo elevado. É por isso que elas não são tão populares apesar de proporcionarem um excelente ganho de produtividade e confiabilidade. Um exemplo disso são os testadores standalone de memória, como o RAMCHECK, o alvo desse artigo.

Para os técnicos de manutenção, algumas ferramentas são verdadeiros sonhos de consumo, como as placas POST, gravadores de memória flash e dispositivos de teste especializados (ou testadores *standalone*) em geral. Há alguns anos, alguns deles foram ficando mais baratos, mas isso não significa que ficou mais fácil de encontrá-los. Como não podemos ter tudo, temos que "comer pelas beiradas".

Um dos testadores *standalone* muito apreciados são os de memória. Eles têm uma aura quase mítica para muitos profissionais, oferecendo a promessa de identificar qualquer problema existente no módulo de memória, poupando um precioso tempo e apresentando um veredito final e absoluto sobre o estado da memória: se saudável ou defeituoso.

Não há muitos fabricantes desses dispositivos, e um deles é o RAMCHECK da Innoventions, Inc (**figura 1**).

O RAMCHECK é uma evolução de um outro produto da Innoventions, o SIMMCHECK II, que como o nome sugere, suporta memórias SIMM FPM e EDO e através de um adaptador, módulos SDRAM. A Innoventions ainda oferece o SIMMCHECK II, e para quem já tem um, há a possibilidade de um upgrade para o RAMCHECK.

Com base nas informações disponíveis no site, o RAMCHECK está disponível em 4 versões, que são identificadas pelos sufixos Base Tester, DDR1, DDR2 e DDR2/1. O mais dinâmico de todos é o Base Tester, que já vem preparado para testar módulos SDRAM PC-66, PC-100 e PC-133 e pode abrigar os adaptadores para os módulos DDR1, DDR2 e padrões legados, como o SIMM de 60 e 72 vias. Há também adaptadores para módulos SODIMM, TSOP, outros padrões de memória e uma interface paralela para conexão direta à impressora, para a impressão direta de um relatório de testes. No nosso caso, estamos usando o Base Tester sem adaptadores.

Segundo informações no site acerca dos adaptadores, não é necessário nenhuma configuração adicional ao utilizar um deles. Basta conectá-la ao RAMCHECK, que o identificará automaticamente e o disponibilizará para uso.

Um outro ponto importante sobre o RAMCHECK é que ele é um produto para testes e não para certificação de módulos. Tal informação consta no FAQ online, e tal esclarecimento se faz importante para evitar o emprego não apropriado do dispositivo.

Responsabilidade e cuidados

Só de observar a existência de uma opção de upgrade para usuários do antigo SIMMCHECK II para o RAMCHECK, podemos concluir que a Innoventions se preocupa com o investimento feito pelo cliente. E tal preocupação é ratificada

F1. O RAMCHECK Base Tester, que testa apenas módulos SDRAM. Mas com o uso de adaptadores, podemos aumentar o seu escopo de atuação até para módulos DDR2.

com o fato de a empresa recomendar que o RAMCHECK seja enviado para a matriz num intervalo de tempo que varia de 12 a 18 meses, para ajuste fino e calibração do dispositivo. Tal informação também está no manual do usuário.

Várias outras informações estão disponíveis no manual, seja no impresso ou na versão online disponível no site. No manual impresso, recomenda-se que o manual online seja consultado para verificar se há alguma observação adicional ou mesmo uma nova versão do manual, a fim de evitar o uso de informações desatualizadas.

O manual não é perfeito, peca em alguns pontos, mas sem dúvida é extremamente realista, pois a primeira seção, a Quick Setup, começa com a frase traduzida livremente: "se você não gosta de ler manuais e não pode esperar para usar seu RAMCHECK com todas as várias opções, aqui está um atalho". E realmente é um guia rápido de uso, objetivo e direto.

É muito importante que seja feito o registro do RAMCHECK junto à Innoventions para se ter acesso às atualizações de firmware e também do software de comunicação que o acompanha.

Quanto aos cuidados, um dos pontos críticos é o slot de memória, que segundo a Innoventions tem uma vida útil estimada entre 10000 e 30000 inserções. Após o término do ciclo da vida útil, é recomendada a troca. Os slots para substituição estão disponíveis para venda. Esse cuidado com o slot não deve ser negligenciado, já que por ser uma parte mecânica, ele invariavelmente vai se desgastar e deverá ser substituído, a fim de evitar quaisquer possibilidades de problemas com mau-contato e co-relacionados.

O RAMCHECK em uso

Por padrão, o RAMCHECK vem configurado para operação automática, o que contempla a maioria das configurações utilizados nos módulos, porém, vez por outra, tal condição pode resultar em falso positivo, ou seja, indicar um erro que na realidade não existe. Para contornar tal possibilidade, é possível configurar o RAMCHECK com base na informações presentes no SPD do módulo, bastando acessar o SPD Management, ler e programar os dados e pronto, basta iniciar as baterias de teste. Caso o erro persista, então o módulo realmente está com defeito.

O ponto forte do RAMCHECK é a operação *standalone*, dispensando a conexão a um computador, embora exista essa opção. Também é comentado no manual que a simplicidade de operação é tamanha que até pessoal não técnico pode usá-lo, porém limitado às funções básicas. Há três grupos de teste: o básico (Basic Test), o extensivo (Extensive Test) e o de repetição (Auto-Loop).

O ambiente onde estamos considerando a utilização do RAMCHECK é um distribuidor, revenda ou assistência técnica de PCs, onde o objetivo é encontrar módulos defeituosos e não consertá-los, embora o RAMCHECK ofereça informações mais do que suficientes para proceder com a manutenção de fato. Isso, porém, é história para outra hora, já que envolve a criação de um ambiente preparado para o manuseio dos componentes eletrônicos altamente sensíveis a descargas eletrostáticas (ESD) e ferramental apropriado para a tarefa.

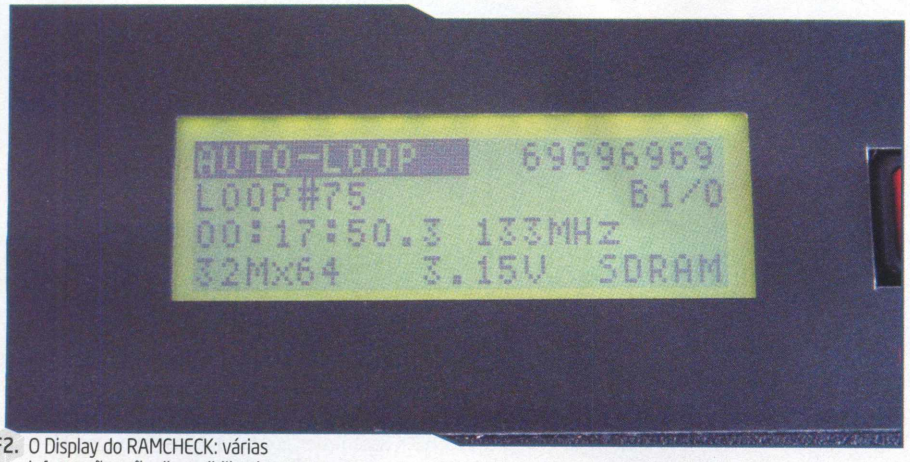
Vamos começar nossa análise pelo teste básico, que procura por falhas nas trilhas, endereços e bits de dados. Ele é suficiente em cenários onde estamos recebendo memórias novas de um fornecedor e se faz necessário aferir a integridade delas, apenas para não correr o risco de vender um módulo com defeito de fabricação. Geralmente quando ocorre um erro no teste básico, ele é do tipo crítico.

O teste extensivo já apresenta uma maior sofisticação, o que é natural e faz jus ao nome. São testados os elementos inerentes a voltagem (ciclo, picos e variação), temperatura, passo (*March Up/Down*), atualização e perda relativa (*refresh/leakage*) da célula de memória. Acerca desse último, no manual, é destacado que todos os testes são seguros e que nenhuma tensão ou corrente será excedida. Por padrão, ele será executado logo na seqüência do teste básico, sendo extremamente conveniente para aferir se há algo mais complexo no módulo que não foi contemplado pelo teste básico.

O teste de repetição é perfeito para *burn-in*, estressando o módulo com padrões diferentes de bits de dados, sendo gerados por algorítmos diversos. Seu uso é indicado para cenários onde a memória já foi utilizada e o erro se evidencia apenas sob determinadas condições. Tal característica é muito apropriada para identificar erros aleatórios ou intermitentes, que não se evidenciam sob as mesmas condições. No FAQ online, os erros intermitentes são organizados em quatro grupos: o primeiro relacionado a temperatura, o segundo com a sensibilidade de padrões, o terceiro a erros de software e o último a picos de temperatura.

Em dois minutos aproximadamente, um módulo de memória passa pelo teste básico e extensivo. O teste de repetição tem duração indeterminada por padrão, mas é possível configurar um limite de tempo. Tivemos a oportunidade de testar mais de 30 módulos com defeito, onde sua condição de erro foi acusada por diversos softwares de teste.

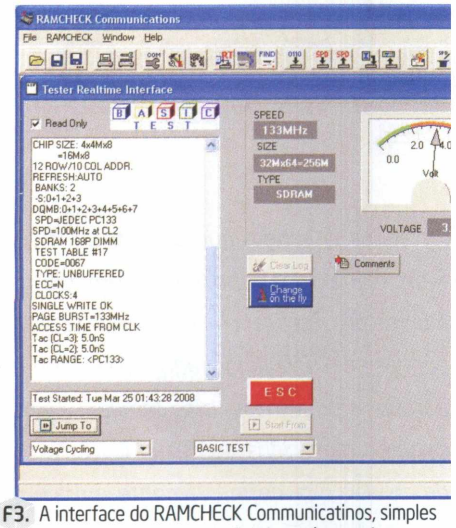
Ao utilizá-los no RAMCHECK, não apenas o erro é encontrado, mas também vários outros dados são informados (**figura 2**), como o número do pino e o identifi-



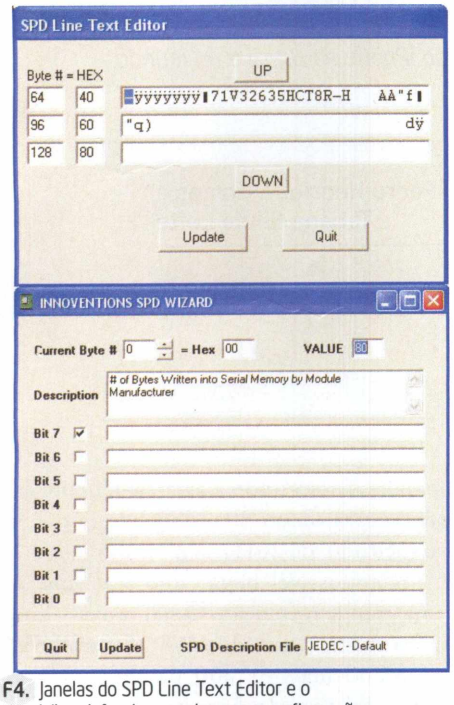
F2. O Display do RAMCHECK: várias informações são disponibilizadas, e na ocorrência de erros, possibilitam até mesmo identificar o chip de memória e substituí-lo.

cador JEDEC correlacionado, bem como o endereço onde o erro foi localizado. No ambiente proposto, só o fato dele indicar o erro já é mais do que suficiente.

Se o módulo é saudável, a bateria de testes vai continuar até que seja interrompida manualmente ou que o tempo limite pré-determinado se esgote. O resultado do teste fica armazenado no buffer ate a realização de uma próxima bateria.



F3. A interface do RAMCHECK Communicatinos, simples e eficiente. Nesse exemplo, ele está com a interface de tempo real (menu RAMCHECK > Realtime Interface) em ação.



F4. Janelas do SPD Line Text Editor e o Wizard, fundamentais para a configuração avançada do módulo.

Uso avançado

O que configura o uso avançado do RAMCHECK é a personalização das baterias de testes, que não se limita apenas a mudar os padrões usados para "escrever" na memória e definir o tempo de duração das mesmas, mas sim transcende e muito tal conceito.

O RAMCHECK permite configurar completamente a temporização do módulo utilizado bem como a tensão e a freqüência de operação; além disso, é possível limitar a quantidade de memória que será testada. Exemplificando, imagine receber um lote de memórias com defeito de fabricação e já se sabendo previamente que os módulos apresentam problemas sempre nos primeiros 128 MB. Diante disso, podemos limitar o tamanho que será testado e poupar tempo no processo.

Outra possibilidade diz respeito às operações relacionadas ao SPD do módulo de memória, que vão além da simples leitura e abrange a edição dos valores armazenados.

Com todo esse poder, a configuração através do painel de controle é muito complexa, exigindo um "vai e vem" nos menus até concluir todas as configurações, o que torna o processo um tanto dispendioso.

Para facilitar a manipulação e conseqüentemente aumentar a produtividade, é fornecido no conjunto o software RAMCHECK Communications (**figura 3**). A comunicação entre o computador e o RAMCHECK é feita através de uma porta serial DB9.

Através desse software é realizada a atualização de firmware, que pode ser automática, bastando simplesmente escolher essa opção para que todo o processo seja realizado, ou manual, caso ocorra algum problema ou apenas se deseje manter controle sobre o processo. Continuando, também é através dele que toda a configuração de testes pode ser realizada, da configuração da freqüência, temporização e tensões, e principalmente a edição do SPD.

Há outras funções que em um primeiro momento são até consideradas menores, como a captura do conteúdo do display LED para bitmap. Mas dependendo do caso, essas imagens podem ser de grande valia, auxiliando num processo de treinamento ou mesmo para documentar uma bateria de testes e enviar esses dados como referência para o fabricante da memória, quando cabível.

Conforme a situação, é possível operar o RAMCHECK a partir do software, através da opção Realtime Interface. Por contar com muito mais espaço para a visualização de status, a operação fica facilitada através dele.

Voltando ao ponto de maior interesse, a edição do SPD, além das funções de ler/gravar o SPD no buffer do RAMCHECK, ele conta com mais dois utilitários: o SPD Line Text Editor e o SPD Wizard (**figura 4**).

A edição do SPD é interessante para o caso de módulos de memórias que tiveram o chip de SPD trocado, ou mesmo para realizarmos a reconfiguração de um que esteja com dados incorretos ou inconsistentes. O manual alerta que a configuração incorreta dos parâmetros do SPD pode causar danos ao sistema onde o módulo editado será utilizado.

Lembre-se de que para editar corretamente os dados para o novo SPD é preciso ter a documentação técnica (datasheet) dos chips de memória, cuja maioria é facilmente encontrada na internet.

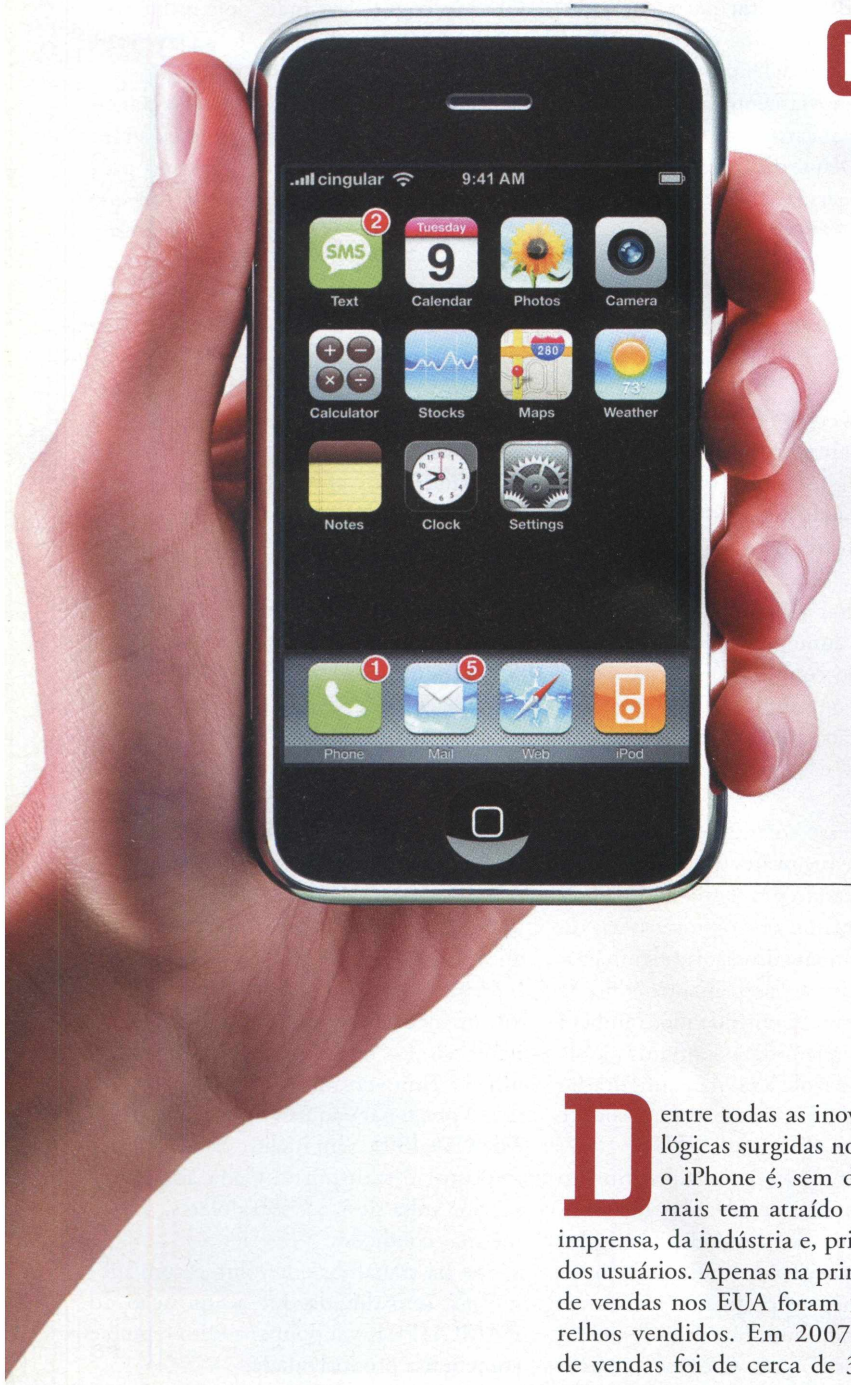
Conclusão

O que torna um testador de memória eficiente, independente do tipo, é o algoritmo de teste. Esse é o grande segredo dos testadores mais eficientes e o calcanhar de Aquiles dos mais simples. Evidentemente, o algoritmo do RAMCHECK é proprietário, ou seja, de uso exclusivo e devidamente protegido pela lei. Como ele está em constante evolução, pode até mesmo ser otimizado através da atualizações de firmware ou, se for refinadamente sofisticado, apenas depois de um dos envios para calibração. Por isso é vital o registro do RAMCHECK junto à Innoventions.

O preço para aquisição do Base Tester é de US$ 1995, sem incluir os custos com impostos e transporte. Cada adaptador sai por volta de US$ 550 dólares, sob as mesmas condições.

Se há trabalhos em volume com memórias, sem dúvida que a aquisição do RAMCHECK vai poupar muito tempo e aumentar a produtividade. **PC**

iPhone, a revolução dos celulares!



Todos já sabem que o iPhone é uma febre revolucionária no mercado de telecomunicações. Essa revolução não foi causada apenas pelo design inovador e software e hardware poderosos, mas também pelos serviços oferecidos aos usuários através do celular, que definitivamente uniram o mundo da Internet ao mundo da telefonia móvel. Conheça um pouco mais sobre essa quebra de paradigmas, os recursos que são oferecidos hoje e as previsões para o futuro do iPhone no Brasil e no mundo.

Pedro Henrique Gomes e Tatiane Silvia Leite

Dentre todas as inovações tecnológicas surgidas no último ano, o iPhone é, sem dúvida, a que mais tem atraído a atenção da imprensa, da indústria e, principalmente, dos usuários. Apenas na primeira semana de vendas nos EUA foram 500 mil aparelhos vendidos. Em 2007 o montante de vendas foi de cerca de 3 milhões de aparelhos e, segundo a agência iSuppli, as previsões são de até 30 milhões de produtos no mercado até 2011.

É impossível negar que o iPhone é uma grande revolução. O seu projeto, que se estima ter custado US$ 150 milhões e rendido mais de 200 patentes para a Apple, foi cercado de mistérios até o dia do lançamento. Até antes da MacWorld

F1. iPhone e seu design inovador.

2007 apenas 30 executivos do alto escalão haviam visto o aparelho. Todo esse mistério tem um motivo: o iPhone veio para quebrar paradigmas. O acordo entre Apple e AT&T viabilizou o grande objetivo do novo produto: unir definitivamente o mundo da Internet com o mundo dos celulares e acabar com o domínio que as operadoras de telefonia têm sobre o conteúdo veiculado em suas redes. Com o iPhone a rede celular tornou-se apenas o meio de acesso às informações, não mais a origem delas. Todos devem imaginar que não foi uma tarefa fácil para Jobs convencer os conservadores executivos de telecom a abrirem as suas custosas redes para o livre acesso à web. Mas ele conseguiu. E quem mais saiu ganhando foi o usuário.

Software e hardware: o que há de novo no iPhone?

O iPhone veio de maneira ousada integrar diferentes funcionalidades em um único aparelho. Ele pode ser usado não apenas para fazer e receber chamadas, mas também para ouvir músicas, assistir a filmes, tirar fotos, ver emails, visitar sites web e até mesmo ver mapas através do Google Maps.

Com seu tamanho de 11,5 cm de altura, 6,1 cm de largura e uma espessura discreta de pouco mais que 1 cm, o design do aparelho é o que mais chama a atenção dos usuários (**figura 1**). O iPhone possui apenas um botão na parte frontal, fugindo do padrão dos celulares convencionais. Além deste, temos apenas mais 3 botões posicionados lateralmente, um para controlar o volume, outro para o modo silencioso e o último para ligar/desligar a tela.

Sua tela sensível ao toque, diferentemente dos *smartphones* tradicionais, foi projetada para ser utilizada exclusivamente com o uso dos dedos, sem a necessidade de se usar uma caneta. Na realidade não existe nem a possibilidade de se usar esse tipo de caneta, já que a tela é sensível às cargas elétricas presentes nos dedos das pessoas.

A maior inovação desta tela é o fato dela ser *multi-touch*, reconhecendo assim mais do que uma região de toque simultaneamente. Até mesmo para usuários acostumados com *smartphones* a experiência com o iPhone é diferente. Através do toque o usuário pode rolar a tela, aumentar e diminuir o zoom de páginas web ou fotos, avançar ou retroceder em um *slide show*, digitar texto e teclar o número a ser discado. Os recursos disponíveis muitas vezes não são intuitivos, por isso a Apple preparou uma série de dicas a respeito do *multi-touch*, que podem ser vistas na página **www.apple.com/iphone/fingertips**.

As telas sensíveis ao toque normalmente monitoram mudanças na superfície da tela quando ela é pressionada, que podem ser detectadas através da variação de corrente elétrica, de ondas sonoras ou mesmo luz infra-vermelha. Porém, a maioria destes sistemas tradicionais não é capaz de identificar o multi-toque. No iPhone o sistema é diferente, diversas tecnologias existentes foram combinadas para possibilitar a identificação de toques simultâneos. Assim como outros dispositivos *touchscreen*, a tela do iPhone inclui uma camada de material capacitivo, mas seu diferencial está em como os capacitores são dispostos no sistema de coordenadas. No iPhone o circuito apresenta um arranjo 2D e pode sentir mudanças e gerar sinais elétricos em mais de um ponto da tela simultaneamente.

O segundo recurso interessante de interação com o usuário é o acelerômetro. Cada vez mais utilizado em equipamentos eletrônicos, esse dispositivo é capaz de sentir a mudança de posição do aparelho e adaptar o conteúdo para uma melhor interação com o usuário. A aplicação de fotos e o browser web são exemplos clássicos do uso desse recurso; o acelerômetro sente quando o usuário posiciona o iPhone na vertical ou na horizontal e rapidamente ajusta o conteúdo para uma melhor visualização. O acelerômetro tem sido usado também de maneira interessante em jogos, melhorando a interação com os usuários.

Os aparelhos atualmente comercializados têm uma capacidade de memória de 8 GB e 16 GB (recentemente lançado). Seu processador é um modelo de ARM e o seu sistema operacional, uma versão enxuta do Mac OS X, adaptada para as instruções da arquitetura ARM.

O iPhone é um celular para redes GSM, funcionando nas bandas de 850, 900, 1800, 1900 MHz. Nas funcionalidades de celular, o iPhone apresenta um sistema bastante interessante de gerenciamento de mensagens SMS. Todas as mensagens são separadas pelo número de destino e apresentadas em formato de chat, dentro de balões coloridos e de forma cronológica, facilitando a visualização de todas as mensagens trocadas.

Para a comunicação de dados o iPhone possui suporte tanto de Bluetooth 2.0 quanto Wifi (802.11b/g) e EDGE. O grande pecado do iPhone nesse primeiro momento é a ausência de suporte às redes celulares 3G.

iPhone no Brasil

Atualmente o iPhone ainda não é vendido oficialmente no Brasil. De maneira contraditória, porém, segundo a agência de notícias Reuters, metade dos acessos à Internet via celular no Brasil, em fevereiro, foram feitos a partir de um iPhone. E mais: nos últimos seis meses os acessos à web com iPhone aumentaram 1.129% !

Mesmo sem dispor de lojas que vendam o iPhone, é fácil encontrá-lo em sites da Internet por cerca de R$ 1.600,00. Além disso, os aparelhos à venda normalmente já vêm destravados. Apesar de todos os esforços da Apple em travar o iPhone para o seu uso exclusivo com as operadoras licenciadas, já existem ferramentas disponíveis na Internet que destravam todas as versões de seu firmware – até o fechamento da edição a última atualização 1.1.4 já havia sido quebrada. A ferramenta mais comum chama-se ZiPhone e pode ser encontrada nos sites **www.ziphone.org** (em inglês) e **http://br.ziphone.org** (em português). É importante, de antemão, alertar os leitores que o procedimento de destravamento faz com que o aparelho perca a garantia.

Desde o início de 2008 diversas especulações rodeiam o lançamento oficial do iPhone no Brasil. As últimas notícias, não confirmadas pela assessoria de imprensa da Apple, são de que a Vivo lançará o aparelho no Brasil até o Dia das Mães, em maio. Ainda não se sabe quais modelos

serão comercializados - atualmente são comercializados nos EUA os modelos de 8 e 16 GB -, muito menos como serão os planos especiais de tráfego de dados. Nos EUA, a AT&T oferece planos individuais mensais a partir de US$ 59,99, que inclui 450 minutos de conversação, e até US$ 119,99, que oferece tempo ilimitado de conversão. O maior detalhe, porém, é que todos os planos oferecem acesso ilimitado à rede de dados; isso quer dizer que você pode baixar seus emails, navegar na Internet, assistir aos vídeos do YouTube e utilizar o Google Maps de graça! Aqui no Brasil, mais especificamente em São Paulo, os planos especiais oferecidos pelas operadoras para acesso à Internet custam cerca de R$ 100,00 por mês e possuem limite de 1 a 2 GB de tráfego, com um custo por MB adicional que varia de R$ 0,25 a R$ 2,00.

O uso da Internet pelo celular no Brasil, apesar de crescente, ainda não é expressivo – segundo levantamento da consultoria Predicta, foram feitos 200.000 acessos em fevereiro deste ano –, principalmente devido ao custo proibitivo. Não se sabe também o quanto as redes de telefonia celular brasileiras estão aptas a receber essa nova demanda pelos serviços web. Restanos esperar pelas novidades; enquanto isso os usuários amargam um serviço caro e de qualidade muitas vezes sofrível.

F2. Fino e leve.

Testes: os recursos do iPhone

A experiência com a tecnologia *multi-touch* foi a primeira grande novidade notada durante os nossos testes. Com exceção do botão central, que invoca o ambiente de trabalho do sistema operacional, todos as outras interações com o usuário são feitas através do *multi-touch* ou de movimentos sentidos pelo acelerômetro.

O iPhone já vem de fábrica com diversas aplicações instaladas. Além do iPod, Safari (browser), leitor de emails e telefone, temos aplicações básicas de um celular como a câmera, bloco de notas, calculadora, relógio, calendário e SMS; as novidades ficam por conta do YouTube, que dispensa comentários, do Stocks, uma aplicação de cotação online de ações, do Google Maps e do Weather, que apresenta as previsões do tempo em tempo real de todas as cidades do mundo, além do iTunes, onde é possível comprar músicas e vídeos. Todas essas aplicações requerem o acesso à Internet, que pode ser feito através da rede celular ou do Wifi. Aliás, a configuração do acesso à Internet no iPhone é feita de maneira transparente para o usuário: o telefone sempre tenta se conectar a alguma rede Wifi já cadastrada que esteja disponível e, caso isso não seja possível, faz o acesso através da rede celular.

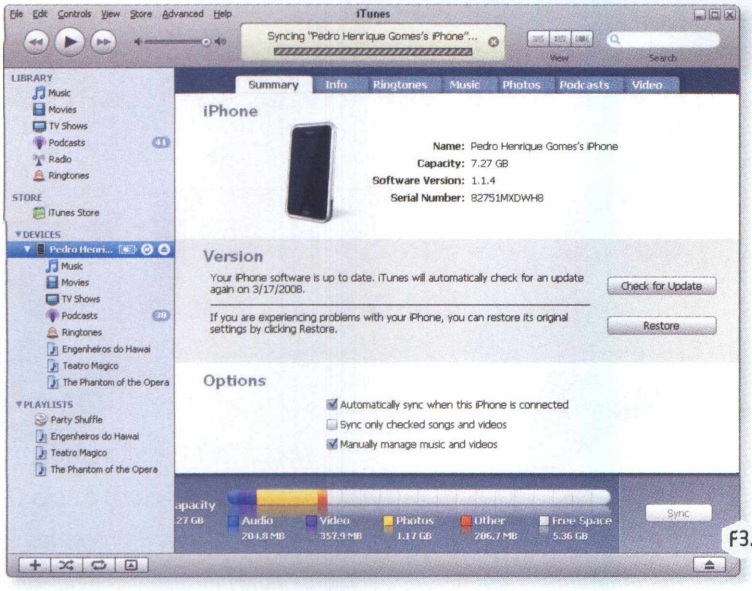
Apesar da Apple ainda não ter liberado o desenvolvimento de aplicações para o iPhone, diversos programas estão disponíveis em repositórios espalhados pela Internet. Juntamente com o software de destravamento é possível instalar um gerenciador de repositórios, denominado Installer, para baixar novas aplicações e turbinar o iPhone. É claro que todos esses aplicativos não possuem um controle da Apple e oferecem perigo à segurança dos dados do celular. É possível encontrar jogos, utilitários, aplicativos multimídia, de desenvolvimento, etc. Uma outra forma, mais segura, de aumentar os recursos do iPhone é acessando aplicativos baseados na web. Uma relação de diversas aplicações web está disponível no site da Apple **www.apple.com/webapps** ou em sites de terceiros, como **http://iphoneapplicationlist.com**.

Durante os testes a câmera de 2 megapixels mostrou-se boa para fotos, com bastante luz, mas deixou a desejar quando comparada às câmeras de celulares modernos. O design e leveza do aparelho impressionaram, assim como o seu tamanho, relativamente pequeno quando comparado aos outros *smartphones* do mercado (**figura 2**). O iPhone, como todos os modelos de iPod, integra-se perfeitamente com o software iTunes. Quando ele é conectado ao computador, rapidamente o iTunes inicia o sincronismo de dados pessoais, como contatos e agenda, além das músicas, fotos, vídeos, *podcasts*, *ringtones* e episódios de TV (**figura 3**). Todo esse conteúdo pode ser extraído de CDs, importado a partir de arquivos mp3 ou comprado pela loja iTunes Store. Infelizmente esse último serviço não está disponível para os usuários brasileiros, já que o registro no iTunes requer um endereço nos EUA e um número de cartão de crédito internacional.

Novidades e o futuro

A última grande novidade anunciada pela Apple no início de março foi a liberação de uma versão beta do kit de desenvolvimento de softwares (SDK) para o iPhone e iPod Touch. O SDK, que até o fechamento da edição era disponibilizado apenas para a plataforma Mac OS, é composto por um ambiente integrado de desenvolvimento, denominado XCode, um simulador e uma ferramenta de coleta e análise de desempenho.

Além de liberar o SDK, a Apple criou um programa de desenvolvimento que tem como objetivo auxiliar e incentivar a criação e distribuição dos softwares desenvolvidos pelos programadores independentes e também por empresas. Com uma taxa de US$ 99,00 para o plano pessoal e US$ 299,00 para o plano empresarial, os desenvolvedores tornam-se membros do programa e podem usufruir de recursos exclusivos, como o suporte de engenheiros da Apple e a hospedagem gratuita da aplicação na App Store, aplicação centralizada de distribuição de softwares para o iPhone, criada pela Apple. Maiores



F3. Sincronismo com o iTunes.

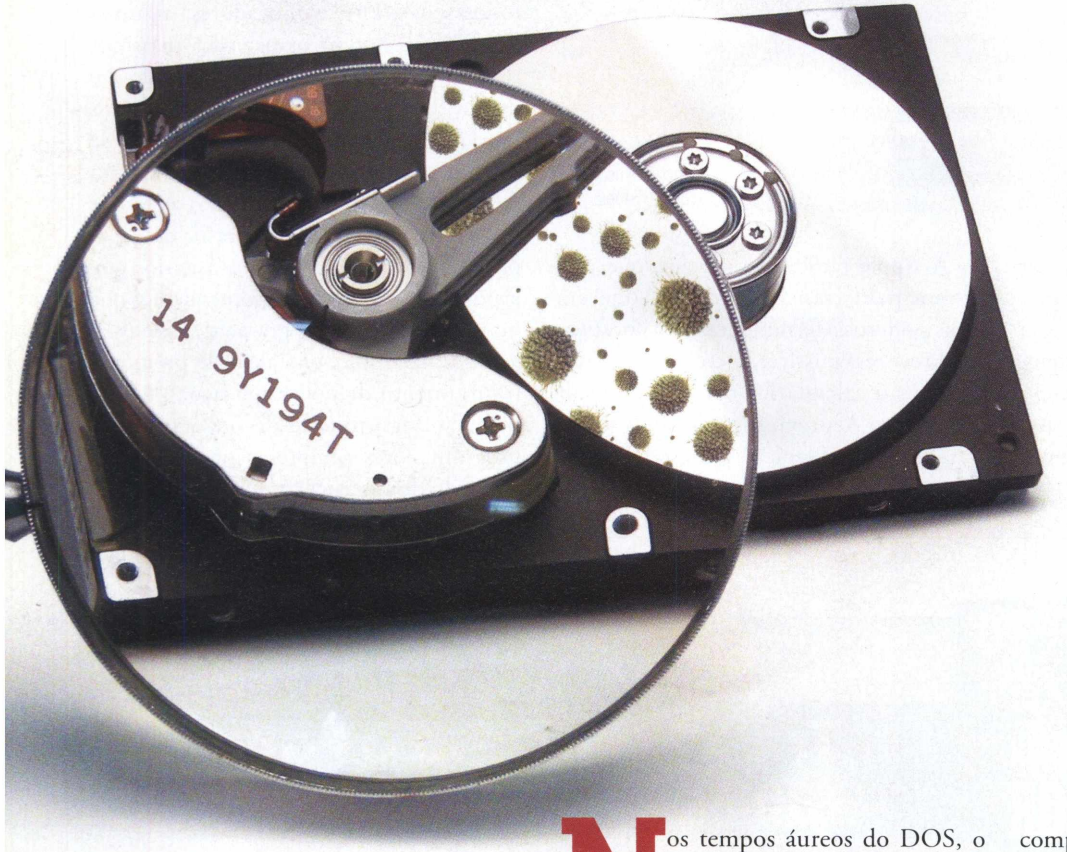
detalhes sobre o programa podem ser encontrados em **http://developer.apple.com/iphone/program.** Certamente essa é uma grande oportunidade para pequenos e médios desenvolvedores venderem aplicações e divulgarem o nome de suas empresas, com um baixo investimento e grandes expectativas de retorno.

A Apple também anunciou que está pronta para transformar o iPhone em uma poderosa ferramenta coorporativa. Em breve será possível sincronizar e-mails, contatos e calendários com o Microsoft Exchange. A previsão é de que ocorra uma melhor integração entre os sistemas corporativos e o celular, a exemplo do que acontece com o seu concorrente BlackBerry, e que recursos avançados, como busca por mensagens, sejam incorporados ao aplicativo de emails nativo do iPhone.

Conclusão

Além de um excelente celular, o iPhone é um poderoso tocador de MP3 e um terminal móvel de serviços web. Um ótimo aparelho, que infelizmente ainda não é comercializado no Brasil. Apesar de todos seus recursos inovadores, algumas falhas desapontam os usuários mais críticos; é possível, porém, que a versão 2.0 de seu sistema operacional e os próximos modelos de aparelhos resolvam grande parte desses problemas. Para quem gostou de seus recursos recomendamos aguardar o lançamento oficial no Brasil, que está previsto para 2008. Para os usuários que já possuem um iPhone, recomendamos que fiquem atentos ao programa de desenvolvedores da Apple, que além de promover o surgimento de novas aplicações, é uma ótima oportunidade de negócios para programadores e empresas interessadas no mercado de Internet móvel. **PC**

Comparativo de anti-vírus



Nunca foi tão chato lidar com pragas virtuais como é hoje. O que antes causava transtornos e problemas localizados e resolvidos com certa facilidade, agora é um problema mundial que pode atingir qualquer sistema, principalmente os conectados à Internet, o grande meio de propagação.

Anderson Costa

Nos tempos áureos do DOS, o grande propagador de vírus eram os disquetes, principalmente através das cópias de jogos, que eram os softwares que mais sofriam com a pirataria, e depois os softwares de produtividade, que hoje podem ser chamados de "tríade anciã": WordStar, dBase e Lotus 1-2-3.

Também havia a possibilidade da disseminação na troca de arquivos via BBS, que até poderiam ser a origem, o meio pelo qual os vírus aportavam no país, porém a disseminação em massa era através dos disquetes.

Ping-Pong, Michelangelo, Madonna e Sexta-feira 13 eram as pragas mais populares, e também havia o temido Natas, que poderia destruir todos os dados do computador e se propagar através de qualquer mídia.

E assim surge o mais temido vírus de computador criado até o momento, o Chernobyl, também conhecido por C.I.H, que poderia apagar todo o conteúdo do HD ao gravar 1 MB com o caractere "0" no primeiro setor da trilha 0, onde fica o MBR, e em casos mais extremos, inutilizar o computador, já que tinha a capacidade de sobrescrever 1 bit do BIOS, o que impedia a inicialização do sistema. Chegou ao cúmulo de vários fabricantes de placas-mãe implementarem um mecanismo de proteção especialmente por causa da ação desse vírus.

Depois disso, vieram o I loveYou, Sasser, BugBear, Blaster, Melissa, Code Red, para citar apenas alguns entre os mais

populares, que estão em diversas listas dos mais perigosos vírus já criados.

Nos últimos tempos, não temos ações virais como antigamente, que visavam mais provar a capacidade de programação/desenvolvimento do criador do que qualquer outra coisa, como as técnicas de invadir e tomar parcial ou totalmente o controle da estação, tal como era possível fazer através do ICQ quando o Xobobus não era instalado. Isso para citar um exemplo.

Hoje enfrentamos uma nova geração de pragas, a palavra "vírus" não é suficientemente abrangente para defini-las, e assim temos os malwares, os quais não causam apenas danos locais e servem como prova de capacidade, mas sim lesam o usuário de um modo mais cruel ao roubar senhas e escravizar o computador de várias formas, seja para aumentar a sua propagação ou para realizar um ataque a um determinado servidor na rede.

Atualmente não podemos abrir mão de boas práticas de segurança, não apenas para manter a integridade dos nossos sistemas, mas sim para preservar a nossa integridade como indivíduo, como cidadão.

Sem sombra de dúvida, qualquer usuário precisa de alguma solução para proteção, seja apenas um anti-vírus ou uma solução mais completa, dotada de firewall e proteção dinâmica, verificando sites, e-mails, conexões P2P, etc.

Fato

Todo e qualquer tipo de proteção, seja uma blindagem automotiva, cerca elétrica ou servidores em geral, tem um ponto fraco, alguma vulnerabilidade que pode ser explorada.

Diante disso, no caso dos sistemas de TI, sejam domésticos ou distribuídos em dezenas de servidores corporativos, por mais que os mecanismos de proteção estejam atualizados, sempre existe uma brecha para a contaminação, um ataque de negação de serviço (DoS), ou qualquer outro tipo de ação que tenha como objetivo a invasão e ações co-relacionadas.

A brecha existe, porém quanto mais sofisticado é o sistema, mais complexa se torna a exploração, demandando mais tempo e maior capacidade do invasor para conseguir concluir a sua ação. E assim as opções mais fáceis são os PCs domésticos, onde uma brecha de segurança leva muito mais tempo para ser identificada e corrigida.

São dois os objetivos típicos nos ataques a PCs domésticos: transformá-los em zumbis e utilizá-los em ações maiores, ou simplesmente para a coleta de senhas bancárias. Nesses últimos tempos, várias quadrilhas especializadas nessas ações foram desbaratas pela Polícia Federal, e em alguns casos, suspeita-se até que estejam envolvidas com o crime organizado "tradicional".

As empresas proprietárias de sistemas sofisticados se protegem e tomam todo o cuidado possível para evitar problemas, já o usuário doméstico nem sempre tem, ou melhor, dá alguma atenção à segurança. Quando muito instala o anti-vírus e não se lembra de atualizá-lo.

Sempre há um intervalo entre o surgimento de um vírus e a disponibilidade de uma vacina, e conforme as características do vírus, apenas esse tempo é suficiente para causar estragos em escala global, como já aconteceu em outras oportunidades. E são essas brechas que os vírus mais perigosos de todos os tempos utilizaram para se propagar rapidamente em escala mundial. Enfatizando: sempre há algum tipo de brecha, por mais sofisticado que seja o anti-vírus e suas capacidades heurísticas.

Um anti-vírus desatualizado só tem duas funções: consumir mais recursos do sistema e proporcionar um péssimo efeito colateral expresso na falsa sensação de segurança. Sem esquecer que isso é como deixar a porta de casa aberta a qualquer um e deixá-lo fazer o que quiser, desde apenas olhar e sair, ou levar tudo e ainda trocar a fechadura.

EICAR

A EICAR (*European Institute for Computer Antivirus Research*), segundo a apresentação disponível em seu site, é um instituto que representa de modo independente e imparcial uma plataforma de segurança de TI para experts nos campos da ciência, pesquisa, desenvolvimento, implementação e gerenciamento.

A exemplo de outros institutos, ele organiza suas ações através de grupos de projeto, ou força-tarefa (task-forces). No presente momento, são seis força-tarefas: Working group 2 on Anti-Virus-Practices, RFID Task Force, Wireless LAN-Security Task Force, Task Force on European Cyber Crime Initiative, Task Force on Awareness and Education e Task Force on Biometrics.

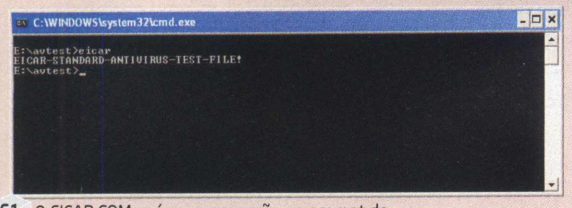
A colaboração do EICAR para os nossos objetivos é a disponibilização de um arquivo de teste padronizado, o EICAR.COM, que tem a função de verificar se os mecanismos anti-vírus ou anti-malwares estão operacionais. Antes disso, cada fabricante de anti-vírus tinha o seu próprio mecanismo de teste, ou tinha que usar vírus reais para executar os testes de funcionalidade de seus produtos.

Na página da EICAR (**www.eicar.org**) onde o arquivo de testes é disponibilizado, existe uma explicação objetiva de cenários de uso, falando sobre os riscos de usar um vírus real para a execução de testes, e sobretudo, questões legais que envolvem o uso de vírus reais. Embora seja um pouco longo, o texto traça de forma prática e didática um paralelo entre os testes de vírus e os de sistemas de prevenção de incêndios, citando que o uso de um vírus real para testar um anti-vírus pode ser até mais conclusivo e eficiente, porém é tão perigoso quanto acender uma fogueira no meio do escritório para verificar se o sistema anti-chamas está funcionando corretamente.

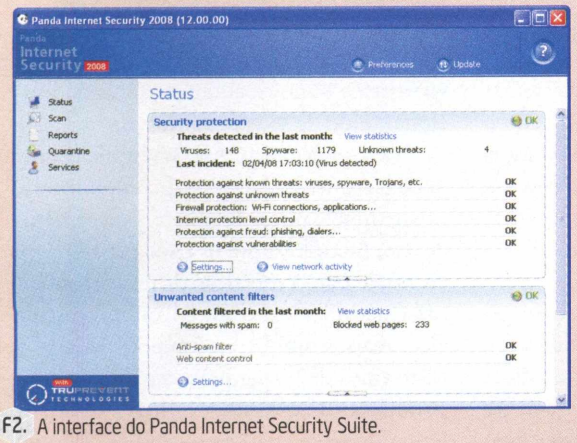
Segundo a descrição do site, o EICAR.COM é um legitimo programa MS-DOS que ao ser executado exibirá a mensagem "EICAR-STANDARD-ANTIVIRUS-TEST-FILE!" (**figura 1**).

O EICAR é disponibilizado de quatro formas diferentes no site. O primeiro é o próprio EICAR.COM, já pronto para ser executado. O segundo é o EICAR.COM.TXT, que é igual ao primeiro, mas com a adição da extensão TXT, bastando removê-la para usar o arquivo. Segundo o site, essa opção foi disponibilizada para contornar os problemas com download relatados por usuários. O terceiro é o EICAR_COM.ZIP, que é o EICAR.COM zipado, usado para averigüar se o anti-vírus está conseguindo verificar o conteúdo do arquivo. Por fim, o quarto, EICAR_COM2.ZIP, é o EICAR_COM.ZIP re-compactado, o qual é usado para verificar a capacidade do anti-vírus de varrer mais profundamente um arquivo compactado.

Caso não queira fazer o download, podemos criá-lo a partir de um editor de textos simples, como o Edit do MS-DOS



F1. O EICAR.COM após sua execução no prompt de comando. Nesse exemplo, o sistema não continha nenhum sistema anti-vírus.



F2. A interface do Panda Internet Security Suite.

ou o Notepad do Windows, bastando copiar a linha abaixo e salvar como EICAR.COM:

```
5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
```

Para os programadores da velha guarda, ou aos da nova guarda que gostam de "escovação de bits", os caracteres utilizados na confecção do EICAR.COM são padrão ASCII e o seu tamanho é de 68 bytes, que é o mesmo número de caracteres que o compõe. Há mais informações técnicas no site, mas são pouco relevantes para o nosso objetivo no momento, que é verificar o funcionamento dos anti-vírus testados.

Produtos

Os produtos envolvidos nos testes são facilmente encontrados no mercado brasileiro, seja via site da empresa ou em grandes magazines ou lojas que os ofereçam, as quais podem ser desde lojas de informática em si a livrarias do tipo megastore.

Para o teste, optamos por usar as suítes ao invés de apenas o anti-vírus, e analisar o conjunto da obra, já que hoje outros fatores inerentes a uma proteção mais completa transcendem à funcionalidade tradicional do anti-vírus. E pensar que nos tempos iniciais do MS-DOS sequer havia proteção residente, além de ter sido bastante instável quando surgiu, ao ponto de muitos usuários e técnicos preferirem executar o anti-vírus no disquete antes de abrir o seu conteúdo a confiarem na proteção residente. Havia outros detalhes, como o consumo de memória base ser muito alto, ao ponto de inviabilizar o uso de outro software, e também o conflito entre os sistemas: um acusava o outro de ser um vírus! Hoje é praticamente impensável não usar uma proteção residente.

Claro que os produtos da McAfee e da Symantec não poderiam ficar de fora, são os mais populares e também velhos conhecidos de boa parte dos profissionais de TI. Podemos até chamá-los de a "velha guarda" dos sistemas de proteção. Da McAfee temos o Internet Security Suite 2008, e da Symantec o Norton Internet Security 2008.

A "nova guarda" não foi deixada de lado. Alguns deles, aliás, "cavaram" seu espaço com uma tática agressiva de mercado, ao se fazerem visíveis ao grande público por oferecerem versões gratuitas para uso não comercial, que foi uma novidade muito bem-vinda e vigente até hoje. Um deles é a AVG, representado pelo AVG Internet Security. Um outro que vem ganhado espaço também é a Panda Security com o seu Panda Internet Security

Cenário

Um detalhe apreciável dos produtos selecionados é que a maioria deles é para até três computadores, o que contempla um bom número de pequenos escritórios e proporciona uma redução de custo na aquisição, administração e manutenção de licenças. Os usuários domésticos também agradecem, sobretudo os que já possuem mais de um computador, cenário este cada vez mais comum.

Assim, em ambientes de rede, sejam domésticos, pequenas empresas ou SOHO, esses pacotes de segurança são alternativas interessantes. Basta apenas descobrir qual é o melhor com base nas necessidades individuais de cada usuário e de quem fará a administração.

É um tanto estranho ouvir "administração do anti-vírus", ainda mais quando se está falando de redes pequenas. Mas é bom lembrar que devido à sua gama de opções, as suítes de proteção demandam isso.

Os testes foram realizados no Windows XP SP2, cujo uso ainda é bem superior ao do Windows Vista.

Panda

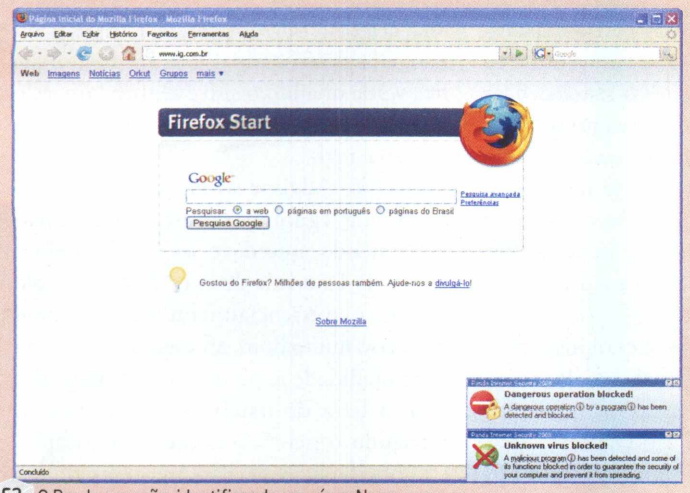
O Panda Internet Security (**figura 2**) tem uma vocação mais voltada ao uso empresarial do que doméstico, o que em termos práticos significa dizer que ele exige do usuário algum conhecimento de termos técnicos. É evidente que isso não é um problema para um profissional, é no máximo uma questão de se adaptar com a interface da suíte.

Os recursos do Panda não são agrupados e batizados conforme a seleção, mas apenas listados, sendo eles o anti-vírus, o anti-spyware/adware, anti-phishing, anti-rootkit, bloqueio de páginas maliciosas, Firewall, proteção de identidade, anti-spam, controle de acesso, backup/restore de arquivos em geral e otimizador do sistema.

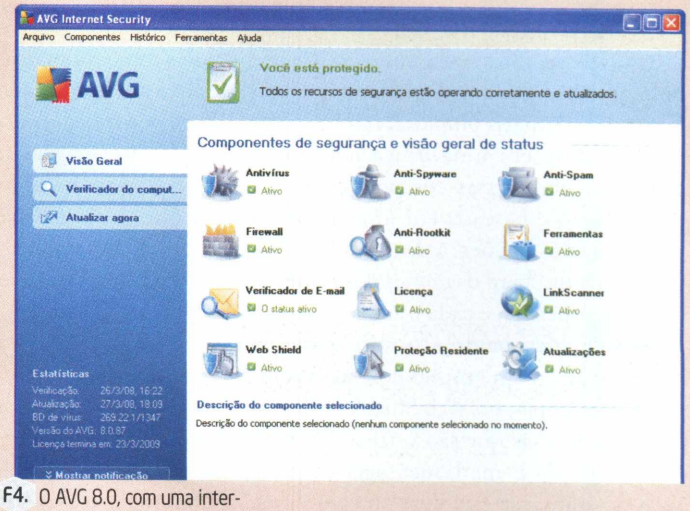
Alguns recursos recebem nomes diferenciados, como a tecnologia TruPrevent, que faz uma análise do comportamento do usuário e gera uma espécie de perfil para tornar a proteção mais efetiva, e o PC Tuneup, que é otimizador do sistema.

Ao instalar, notamos a ausência de suporte ao português do Brasil. Português, só de Portugal. Acabamos optando pelo inglês.

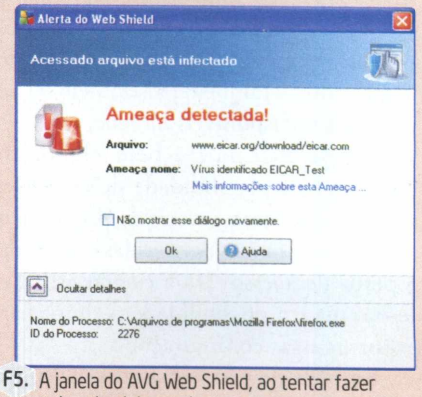
O primeiro aviso gerado pelo Panda fazia referência às vulnerabilidades do sistema, indicando quais eram com base nos números de identificação da Microsoft e também as opções para corrigi-las. E logo após disso, informou sobre o registro do produto, necessário para ter acesso às atualizações e serviços co-relacionados. O registro é feito pela Internet e confirmado por e-mail. Uum nome de usuário e senha são disponibilizados para permitir o acesso ao site da Panda Security e obter as atualizações. Uma vez configurado, o processo é totalmente transparente.



F3. O Panda em ação, identificando um vírus. Nesse caso, era uma praga real, que tentou invadir o sistema devido a uma falha em uma das atualizações de segurança.



F4. O AVG 8.0, com uma interface simples e objetiva.



F5. A janela do AVG Web Shield, ao tentar fazer o download do arquivo com praga, nesse caso, é o arquivo de teste EICAR.COM

O Panda se comporta de maneira discreta no sistema: apenas um ícone na bandeja do Windows é exibido. Quando um vírus é encontrado ou alguma atividade suspeita é identificada, é exibida uma janela informativa do tipo de ação, se vírus, trojam, malware (**figura 3**). Mas para saber qual é o nome da praga e o arquivo relacionado, é necessário posicionar o ponteiro do mouse sobre o ícone de informação. O Panda nos permite definir o tempo de exibição dessa janela e a transparência.

A sua janela principal é simples e objetiva, organizada em duas colunas. A mais estreita, à direita, fica com os menus e a da direita, com o conteúdo. O padrão é status, que exibe a condição dos principais elementos, a proteção, os filtros de conteúdo, o backup e otimização e, por fim, a atualização dos arquivos de definição das pragas. Os outros são: Scan (a varredura em si e também a identificação de vulnerabilidades no sistema), Reports (relatório das atividades), Quarantine (a quarentena, onde os arquivos de riscos ficam bloqueados) e Services (um conjunto de ações disponíveis para os usuários registrados). Um dos serviços que chama atenção é a criação de arquivos de recuperação. Não se assuste com o termo serviço, pois ele só está nessa guia. Os arquivos são criados pelo próprio usuário e pode facilitar a vida em casos extremos.

Essa versão do Panda permite que um local dentro da rede seja indicado para armazenar os arquivos de definições de pragas atualizados, o que proporciona redução no uso de banda de acesso à Internet, além de proporcionar um controle centralizado na atualização.

É oferecida também a possibilidade do controle de acesso à Internet, com base em perfis pré-determinados e personalizados. Ao acessar a Internet, é exibida uma tela de logon para liberar o acesso. O firewall é bem completo, oferecendo a criação de regras e o controle de programas específicos, permitindo ou não o acesso deles à Internet.

AVG

O AVG Antivirus conseguiu popularidade e, conseqüentemente, seu lugar no mercado, ao ser distribuído com funcionalidade total e além disso, gratuitamente para uso não-comercial através da Internet, via download. O sucesso da empreitada foi tanto que outros fabricantes adotaram o mesmo modelo.

Atualmente na versão 8.0, o AVG é um dos poucos produtos disponíveis no mercado que não adotou o sufixo Internet Security.

O AVG oferece os seguintes recursos: anti-vírus, anti-spyware, anti-spam, firewall, proteção na navegação na web e e-mails, além de verificação de links nocivos.

A janela principal é organizada em guias (**figura 4**), sendo a Visão Geral, Verificador do computador e atualizar agora, e um menu tradicional acima, contendo as opções Arquivo (apenas para fechar, tanto que poderia receber esse nome), Componentes (nada mais que um link para os mesmos componentes listados na janela), Histórico (que exibe o relatório de verificação, da detecção da proteção residente e do verificador de e-mail, quarentena de vírus e log do histórico de eventos) e Ferramentas (Verificar o computador, pasta selecionada ou arquivo, atualizar via Internet ou diretório, configurações avançadas e de Firewall).

Assim como o Panda, a presença do AVG no sistema é bem discreta, apenas com o ícone na bandeja do Windows e uma barra nos browsers instalados no sistema, que tem o atalho para o mecanismo de busca do Yahoo e os botões do Active Suft Shield, Search Shield e o AVG Info, que são links de informação para o site da AVG. Ocorreu apenas uma falha com a barra no Firefox, que insistiu em não funcionar. Segundo a documentação, basta iniciar o programa de instalação do AVG e escolher a opção restaurar, a fim de resolver esse problema. Embora seja discreto, sua ação ao identificar é bem clara (**figura 5**).

O AVG apresenta um interessante contraste: sua interface é simples, o que é bom, pois facilita o uso, porém a sua configuração já é mais complexa, centralizadas praticamente em uma única janela que disponibiliza diversas configurações. Sua organização é baseada em uma árvore, à esquerda, e as opções, à direita. Os ramos principais recebem os nomes dos respectivos componentes, e cada uma delas é bem completa, oferecendo a possibilidade de fazer um ajuste fino muito bom nos recursos. Por exemplo, no Web Shield, podemos definir as portas que são verificadas, e no Verificador de E-mail, mensagens indicativas do status, se está livre ou com vírus, se os anexos são removidos sumariamente, etc. O Anti-Spam não fica atrás também, permitindo configurar até os IP's de origem indesejados, e também países, além de usar Black Lists disponíveis na rede, etc.

O seu Firewall é bem elaborado, oferecendo a possibilidade de configurar interfaces seguras, escopo de IPs, serviços, aplicativos e portas permitidas e proibidas, e perfis de acesso. Uma característica interessante é a possibilidade de importar e exportar essas configurações.

Embora ele não tenha uma plena integração com os usuários do Windows, ele ao menos permite que se defina qual é o tipo de usuário que pode alterar as configurações do Firewall, entre administradores, administradores e usuários avançados, ou todos os usuários.

McAfee Internet Security

A fama da McAfee vem do seu velho VirusScan para o DOS, considerado praticamente imbatível na época, de funcionamento simples e eficiência impecável, um verdadeiro salvador da pátria. Bastava um simples boot do DOS e com a linha de comando apropriada para o sistema ficar livre de vírus depois de alguns minutos. A boa prática exigia que fosse executado pelo menos mais uma vez para se ter certeza de que nenhum resquício de vírus havia ficado para trás. Se bem que poucas eram as vezes em que se encontrava algo nessa segunda verificação.

O pacote da McAfee é composto pelo Security Center, o VirusScan, Personal Firewall, Site Advisor, Anti-Spam, Privacy Service, Easy Network e o Data Backup.

O visual da janela principal (**figura 6**) é bem sóbrio e há dois modos de operação, o básico e o avançado. Independente da escolha, o status da proteção do sistema é exibido por padrão. A diferença entre as duas é mínima, a primeira contém botões para a execução da varredura e atualização bem destacados; na segunda eles são removidos, sendo posicionados dentro das opções apresentadas nos painéis, através dos quais realizamos as configurações de cada componente.

A sua presença no sistema é bem discreta, a exemplo do Panda e do AVG, evidenciando-se apenas por um ícone na bandeja e o Site Advisor nos navegadores. Quando está fazendo alguma varredura, um outro ícone é adicionado à bandeja. Ou seja, nada de janelas, a não ser que o usuário as acesse através do duplo clique no ícone correspondente ou alguma praga apareça (**figura 7**). O Firewall tem configuração de nível de segurança, IP's e programas permitidos e proibidos, detecção de instrução, etc.

Nos browsers do sistema, é adicionado o Site Advisor, que indica o potencial de risco do site visitado, bem como suas relações com outros sites, se perigosos ou não, e os downloads. Ele é um botão que fica verde quando o site é seguro, amarelo quando há algum risco e vermelho quando o risco é real.

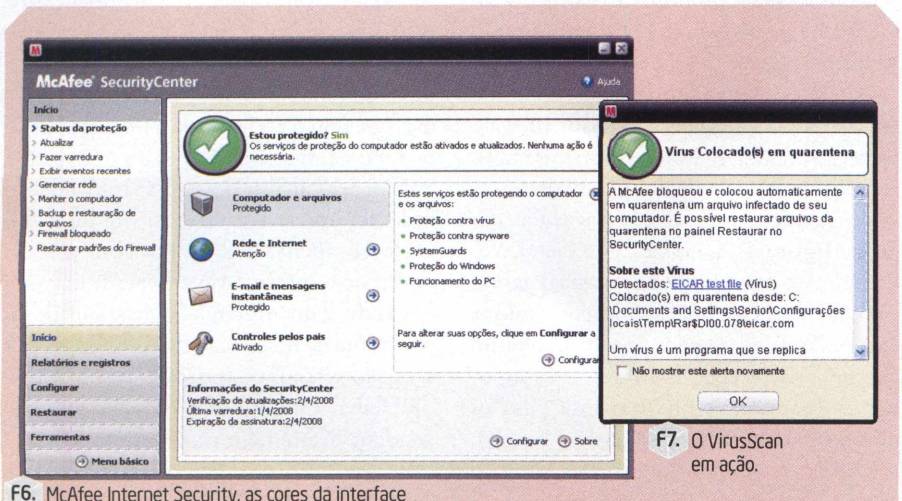
O Site Advisor só faz uma avaliação técnica da segurança do site visitado e não de conteúdo, que deve ser configurado à parte, no Controle de Pais. Esse Controle de Pais, que essencialmente é um controle de acesso muito bom, apresenta uma ótima funcionalidade e, além disso, é integrado com a lista de usuários do Windows, tornando o gerenciamento mais simples e também eficiente. Pode ser definido em Perfil e hora de uso. Há também a proteção de identificação, que ao ser configurada só permite o envio dos dados pessoais (do endereço a números de cartão de crédito) mediante autorização.

Dos produtos testados, é o único que exigiu a instalação do pacote .NET Framework da Microsoft, que é um componente necessário ao mecanismo de backup, inicializado pela janela principal do VirusScan, porém acomodado em uma outra janela apenas para ele. Um outro componente que tem sua janela própria é o Virtual Technician, que auxilia o usuário a encontrar respostas. Ele é instalado à parte.

Há outros componentes focados na otimização do sistema, como o QuickClean (que limpa todos os temporários e outros elementos do sistema), o Shredder (para apagar arquivos definitivamente e com segurança), o programador de tarefas (para agendar algumas atividades para execução automática), o Gerenciador da rede (que verifica quais são os computadores e dispositivos existentes na rede, exibindo o IP e o respectivo nome), Monitor de Tráfego de rede, e links para os utilitários existentes no sistema, como o desfragmentador de disco e a restauração do sistema. Há recursos para maiores informações acerca de vírus, como o Virus Map e o HackerHatch.

Norton Internet Security 2008

No começo, não existia o Norton Antivirus, mas sim o Norton Utilities, um conjunto extremamente poderoso de softwares de diagnóstico e manutenção de hardware, que deu origem à fama que dura até hoje.



F6. McAfee Internet Security, as cores da interface dão um tom mais sóbrio.

F7. O VirusScan em ação.

Claro que as primeiras versões do Norton Antivirus, pesadas e lentas, não faziam frente ao VirusScan, mas a história mudou quando surgiu o Windows, e se tornou um adversário à altura. Por um bom tempo, a disputa no mercado foi muito acirrada entre eles. Atualmente, com os novos "jogadores" em campo, novamente a história se mostra diferente.

O Norton Internet Security 2008 (**figura 8**) oferece, além do anti-vírus e o firewall em si, proteção em conexões sem fio, e-mails, mensagens instantâneas, navegação na web, phishing, intrusão e downloads. Há também o Identify Safe, que protege informações de cartões de crédito, sendo armazenadas nele.

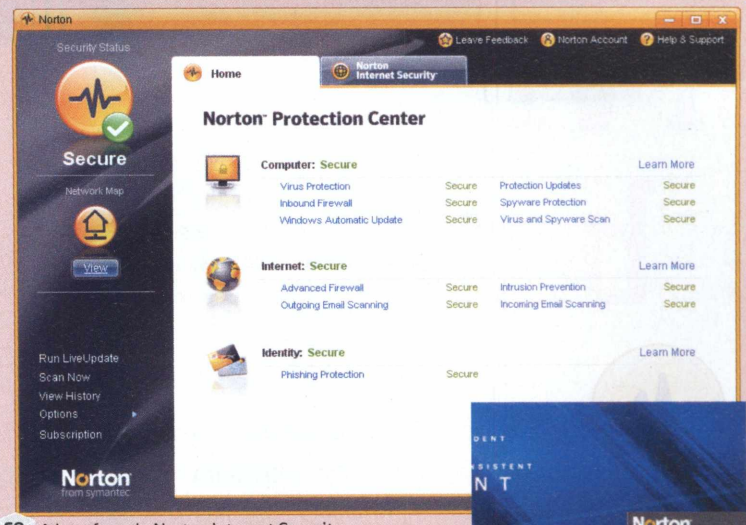
Antes de proceder com a cópia dos arquivos, o programa de instalação faz a atualização via Internet, o que no nosso caso durou aproximadamente 15 minutos. Durante a primeira instalação, é preciso ativar o produto para poder ter acesso às atualizações. A ativação é feita através de um cadastro e confirmado via e-mail.

Dos produtos testados, o Norton é mais "exibido" (**figura 9**). Ao invés de usar um ícone na bandeja do Windows, é empregado um botão, quase um banner, logo ao lado da bandeja, na cor amarela, característica da marca, chamando bastante atenção.

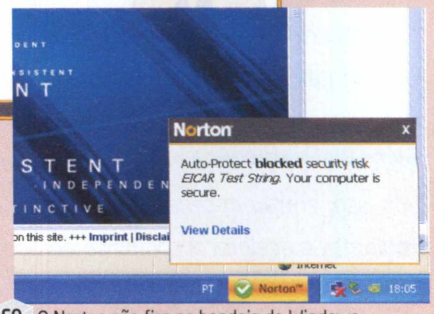
A janela principal, como hábito da Symantec, é personalizada com as cores da empresa, sendo organizada em colunas e guias. São duas colunas com funções independentes: a da direita lista algumas ações, com a de varredura, o Live Update, a função de mapear a rede e o status da proteção; e a da esquerda para exibição do conteúdo dos menus. Nessa parte há duas guias, a Home, que exibe o status individual de cada mecanismo de proteção, e a Norton Internet Security, que abriga as funções de varredura do sistema, atividade da proteção (firewall, spyware e intrusão), relatórios e estatísticas.

Chama atenção o funcionamento do firewall, que oferece opções de desligamento temporário de 15 minutos a 1 hora, e por fim sua desativação completa, que evidentemente não é recomendada. No browser é adicionada uma barra referente à proteção de phishing e também o Identify Safe.

Nessa versão do Norton Internet Security, o controle de acesso (Parental Control) e o anti-spam são oferecidos à parte, sendo necessário acessar a guia Norton Internet Security > Transaction Security e clicar em Download Parental Control or Antispam. Após a instalação, uma nova guia é adicionada à janela principal, a Norton Add-on Pack. O bloqueio é baseado em perfis, porém permite a adição de sites de modo específico. Ao tentar abrir um site proibido, é exibida uma página informando acerca da impossibilidade do acesso. Diversos sites que passaram desapercebidos por outros produtos, foram bloqueados. Em tempo, o bloqueio é realizado com base nos usuários do Windows, tornando a administração muito mais fácil.



F8. A interface do Norton Internet Security, com as cores características da marca.



F9. O Norton não fica na bandeja do Windows, mas logo ao lado dela. Note ele em ação no exemplo, novamente através do arquivo de teste EICAR.COM

Conclusão

Um breve resumo que podemos fazer com relação aos produtos avaliados aqui é o seguinte: o Norton é para os fãs da marca, que confiam de olhos fechados na "bandeira amarela", além de já estarem habituados com as suas ferramentas. O McAfee é uma ótima opção para redes domésticas e pequenas empresas onde os usuários não seguem uma boa conduta de uso e se exija um bloqueio específico. Um ponto muito positivo do Norton e da McAfee é a integração com o Windows, permitindo o controle de acesso com base na lista de usuários do sistema.

O AVG e o Panda podem ser empregados em SOHO e em empresas com redes pequenas, nas quais os usuários são responsáveis e não haja demanda para bloqueios específicos a determinados acessos.

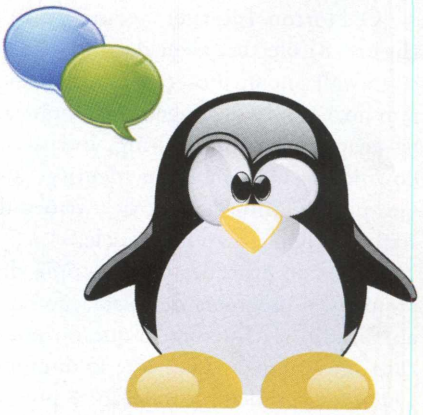
Algumas suítes fornecidas em CD oferecem um mecanismo de boot para verificação offline, mas não contemplamos sua funcionalidade nesse momento.

A grande questão atualmente é que várias pessoas, mesmo as que não abrem mão de usar uma solução anti-vírus, não levam a segurança de dados a sério. Apenas quando surge um problema com conseqüências bem reais é que talvez (apenas talvez) haja mudança de postura.

Enquanto não há essa mudança, o uso de uma solução anti-vírus, por melhor que ela seja, não será eficiente, já que a brecha de segurança está no comportamento humano. E não há software que resolva essa falha.

Todos os produtos, à sua maneira, protegeram o sistema, evitando a ação da praga, seja em modo furtivo, onde houve uma tentativa de explorar uma vulnerabilidade, pelo e-mail, pelo comunicador de mensagens instantâneas ou na navegação. Mas não devemos esquecer que a eficiência desses softwares depende diretamente do quão atualizado está o sistema operacional. Caso contrário, é quase certo que seu sistema enfrentará problemas com infecções e outras pragas. **PC**

Servidor de bate-papo



A capacidade de interação e comunicação entre as pessoas é, sem dúvida, uma das ferramentas mais importante no ambiente de trabalho. Entretanto, nem sempre é possível exigir que estas ferramentas estejam funcionais a todo momento. Uma hora é o telefone que está ocupado, em outra o "fulano" não está na mesa e como se não bastasse tudo isso, entra em cena a questão dos custos com ligações. Saiba como driblar estes problemas e acelerar a comunicação dentro de sua empresa com custo zero, e através de uma única solução.

Solução

Por ser um meio termo entre o email e o telefone, os servidores de IM (ou MI – Mensageiro Instantâneo) se transformaram em um recurso indispensável para muitas empresas, pois permitem que os funcionários interajam de forma rápida e eficiente. E no quesito custo promovem uma grande redução, afinal, imagine o valor da conta telefônica para entrar em contato com clientes ou fornecedores espalhados pelo Brasil. Mesmo que pouca, seguramente a economia na conta telefônica seria algo de grande interesse.

Atualmente existem duas formas de dispor do uso de mensageiros instantâneos. Uma delas é a partir de servidores públicos mantidos na Internet, tal como o MSN, que não oferece recursos (tal como a criptografia dos dados) capazes de garantir o sigilo das informações transferidas nos textos entre os usuários pela Internet. Desta forma, nada impede que as mensagens em um bate-papo sejam monitoradas. A outra forma é a criação de um servidor privado. Este, por sua vez, será de uso exclusivo da empresa onde for implantado, permitindo um total controle e gerenciamento sobre as contas de usuários, bem como das funcionalidades do servidor. Neste último cenário, mesmo que o usuário estivesse fora da empresa poderia se comunicar com os demais funcionários de forma transparente, bastando ter acesso à Internet.

Dentre os melhores softwares para criação de um servidor de bate-papo está o Openfire (**www.igniterealtime.org**), um software escrito em Java e disponível na versão open source e comercial. A única diferença significativa entre as versões diz respeito ao suporte técnico e à função de geração de relatórios, ambas presentes apenas no Openfire comercial. Ademais, são idênticos. A versão open source encontra-se disponível atualmente para download (arquivo com 10,6 MB) no site da empresa desenvolvedora. O Openfire poderá ser instalado em ambiente Windows, Linux e MacOs.

A questão é: em que hardware instalar? De tão simples e leve, é difícil justificar a destinação de uma máquina especificamente para o Openfire, e é aí que entra em cena – por sinal, mais uma vez aqui na PC&CIA - uma ótima oportunidade para usarmos a técnica de virtualização. Portanto, uniremos os recursos do Openfire com os benefícios da virtualização em uma única solução (multi-plataforma) que exigirá apenas um browser para a configuração e administração do sistema. Vamos ao passo-a-passo.

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

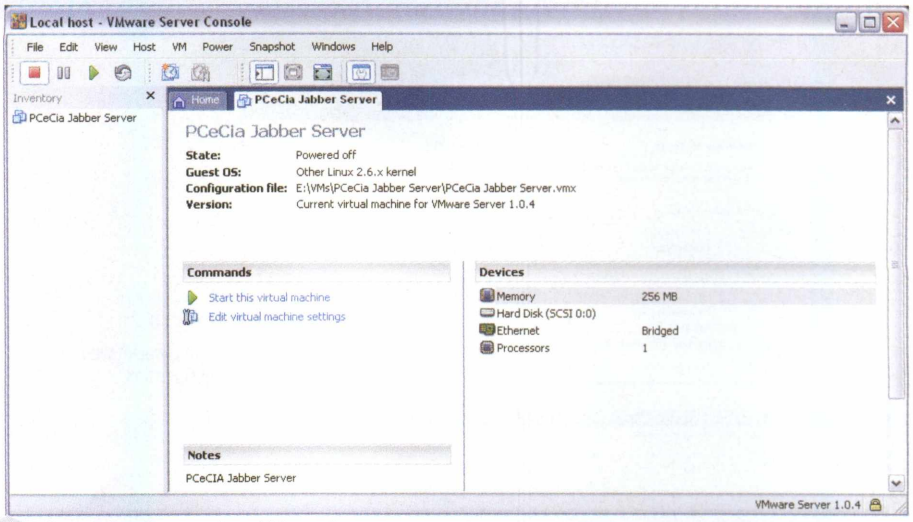
Openfire

O servidor de IM construído com o Openfire funciona através do protocolo XMPP(**www.xmpp.org**) e tem como finalidade oferecer uma comunicação que seja a mais próxima possível da real entre os usuários. Ou seja, sem lentidões (ou gargalos) sob o ponto de vista da camada de protocolo de comunicação. Quando falamos em servidores de IM que utilizam o protocolo XMPP, na verdade estamos nos referindo a um servidor Jabber (**www.jabber.org**). Por ser um padrão aberto, podemos utilizar um servidor Jabber público (tal como o ICQ, AIM e Yahoo) ou criarmos um privado que, aliás, poderá ser totalmente virtualizado. Conseqüentemente, ficamos livres de novos investimentos em hardware.

Com virtualização

Para disponibilizarmos o Openfire (versão 3.4.4) em uma máquina virtual (download em nosso site **www.revistapcecia.com.br**), utilizamos o VMware Server, o qual também pode ser obtido gratuitamente através do site **www.vmware.com**. Além de ter o Openfire pronto para o uso, esta máquina virtual (VM) tem como diferencial o seu sistema operacional, no caso uma distribuição Gentoo Linux enxuta, cujo kernel (versão 2.6.24.) foi otimizado para consumir o mínimo de recursos sob o ponto vista do hardware real e virtual. O que na prática significa que poucos serviços e processos serão inicializados no sistema, diminuindo a carga de processamento tanto na VM como na máquina hospedeira.

O hardware da VM é composto por um disco rígido virtual (interface SCSI) de 8 GB, uma interface de rede operando em modo *bridge* e 256 MB de memória RAM. O HD virtual foi ajustado para utilizar o método de armazenamento dinâmico, tendo seu tamanho aumentado conforme as gravações são realizadas dentro de um arquivo de extensão .vmdk, o qual é utilizado pelo VMware Server para encapsular o funcionamento do disco virtual. Para quem ainda não conhece os meandros da virtualização, vale lembrar que o funcionamento de uma VM no VMware Server só requer dois arquivos, um de extensão .vmx, contendo as configurações da VM, e outro .vmdk, que é o disco virtual.



F1. Máquina virtual carregada no VMware Server.

Instalação

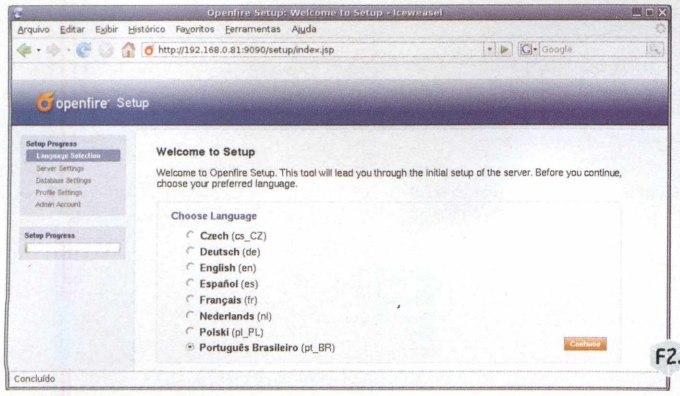
O primeiro passo é instalar o VMware Server no hardware "real", sobre o sistema operacional de sua preferência (Windows ou Linux, consulte no site da VMware as opções suportadas). Tendo sanado isso, faça o download (60 MB) da VM (PCeCIA Jabber Server.7z) do Openfire em nosso site **www.revistapcecia.com.br/downloads.htm**). Agora descompacte o arquivo recém-baixado e dê um clique duplo sobre o "PCeCia Jabber Server.vmx" para, em seguida, fazer com que as configurações da VM sejam carregadas no VMware Server (**figura 1**).

Feito isso, surgirá uma mensagem solicitando uma confirmação para a criação de um novo identificador para a VM. Marque a opção "create", clique em "OK" e dê um "play" na VM, através do botão verde ("Power On") exibido na interface do VMware Server. Neste momento a VM está operando como cliente DHCP. Portanto, logo após o carregamento do sistema virtual, devemos verificar qual foi o endereço IP atribuído a placa de rede da VM. Para isso faça um logon no sistema através a conta de usuário "root" e a senha "pcecia". Em seguida digite no terminal o comando "ifconfig eth0". O resultado apontará o endereço IP ao qual utilizaremos para acessar a interface web do OpenFire. A partir deste ponto a janela (ou interface) do VMware poderá ser fechada, pois para os demais passos utilizaremos apenas o browser. Repare que fechamos apenas a interface gráfica, mas na verdade os processos referentes à VM continuam rodando, só que em segundo plano. Caso você precise alterar as configurações de rede, utilize as instruções do arquivo LEIA-ME.txt, descompactado junto com a máquina virtual. Aliás, é neste arquivo que estão as instruções para configurarmos as interfaces de rede virtuais.

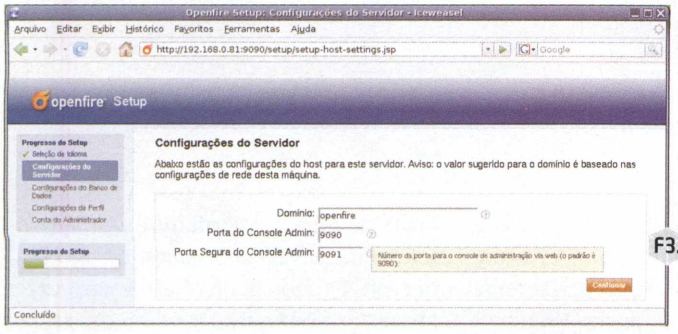
Interface Web

Uma vez obtido o endereço IP, abra um navegador web e no campo da URL digite **http://endereçoIPdamáquinavirtual:9090** (**figura 2**). Selecione o idioma a ser utilizado pelo Openfire e, em seguida, clique no botão "Continue". Na próxima tela você poderá configurar o nome de host do servidor dentro de um domínio e as portas de acesso web. Preencha o campo "Domínio" com o próprio nome de host do sistema, no caso, "openfire". As portas de comunicação do servidor (9090 e 9091) também poderão ser alteradas. Entretanto, dê preferência à configuração padrão (**figura 3**). Agora clique no botão "Continuar" para entrarmos nas opções relacionadas ao mecanismo de armazenamento dos dados (**figura 4**).

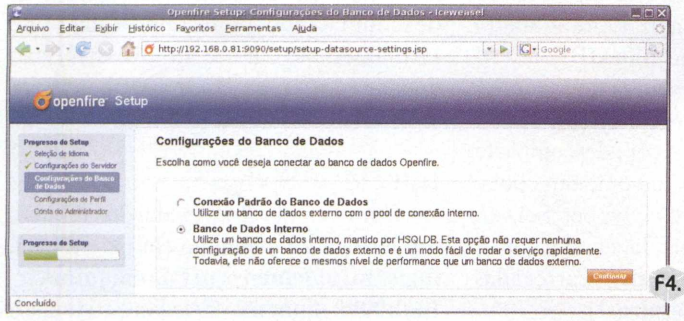
Para armazenar os dados cadastrados no Openfire podemos utilizar um banco de dados (BD) interno ou externo. A primeira opção, exibida na figura 4, habilita o uso de um BD externo. O Openfire é compatível atualmente com os BD's MySQL, Oracle, Microsoft SQL, PostGreSQL e IBM DB2. A segunda opção



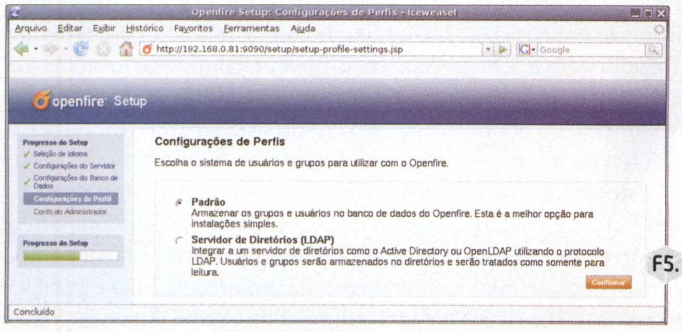
F2. Configuração web do Openfire.



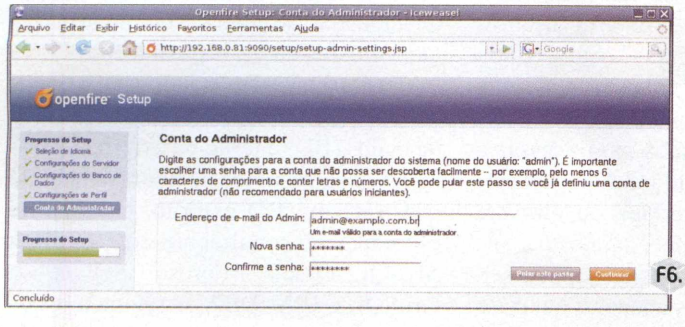
F3. Opções de host do Openfire. Durante os testes, esta foi a configuração utilizada em laboratório.



F4. Mecanismo de armazenamento dos dados.



F5. Durante os testes utilizamos apenas a opção "Padrão".



F6. Configuração da conta "admin".

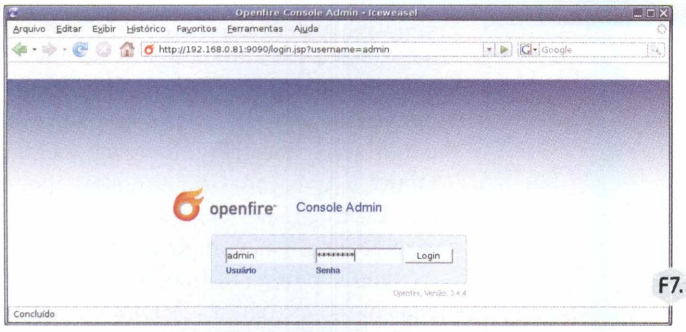
faz com que o Openfire crie e gerencie seu próprio banco de dados interno. Embora a primeira opção seja mais interessante sob o ponto de vista da performance, nos nossos testes utilizamos a segunda opção. O Openfire foi ajustado para gerenciar o armazenamento e o método de consulta aos dados, os quais, a propósito, são encapsulados em um BD HSQLDB (**www.hsqldb.org**). Em nenhum momento o sistema ficou lento e apenas para fins de dimensionamento, vale mencionar que o hardware da VM foi configurado de forma a suportar até 30 usuários logados no Openfire. O uso de um banco de dados externo, portanto, só é recomendável para os casos nos quais você precise exceder esta quantidade de usuários. Aliás, se isto acontecer, você também deverá aumentar o tamanho da memória RAM da VM.

Prosseguindo, escolha sua forma de armazenamento e clique em "Continuar". Na próxima página serão apresentadas as opções referentes aos usuários que farão parte do Openfire (**figura 5**). Na opção "Padrão" as contas de usuários serão criadas e armazenadas no Openfire. A opção "Servidor de Diretórios (LDAP)" faz com o que Openfire trabalhe com as contas de usuários cadastradas em servidores AD (Active Directory) ou OpenLDAP. Selecione uma das opções e avance na configuração.

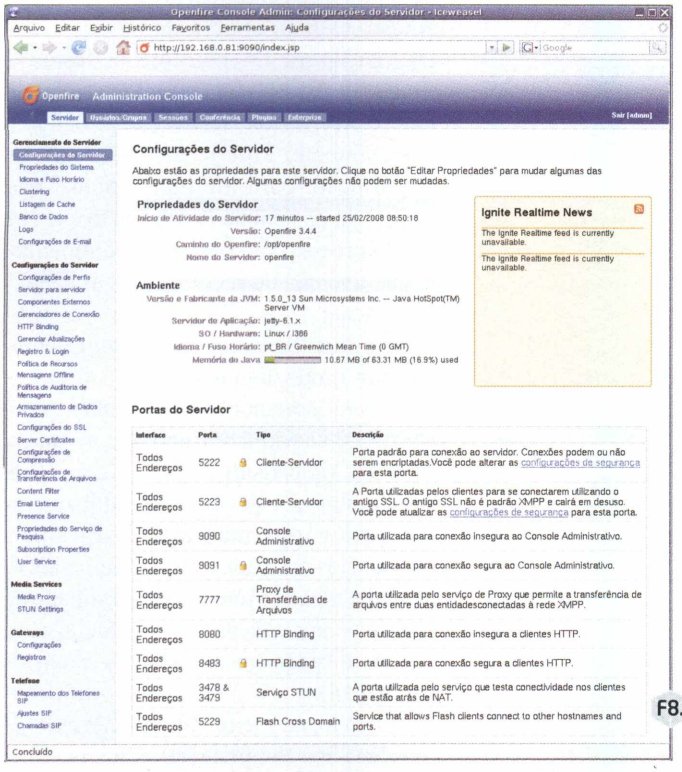
A última etapa é a configuração de uma senha para a conta do usuário "admin", o qual, por sinal, será o único com poderes administrativos dentro da interface web do Openfire (**figura 6**). Informe nos respectivos campos o endereço de email e senha de login do usuário "admin". Ao avançar nesta tela, surgirá uma nova página informando que a instalação foi concluída. Clique no botão "Logue-se no console de administração", exibido nesta mesma página, para acessarmos a interface web do Openfire (**figura 7**).

Digite nos respectivos campos o nome de usuário e a senha da conta "admin". Após a autenticação teremos acesso a todas funcionalidades do Openfire (**figura 8**).

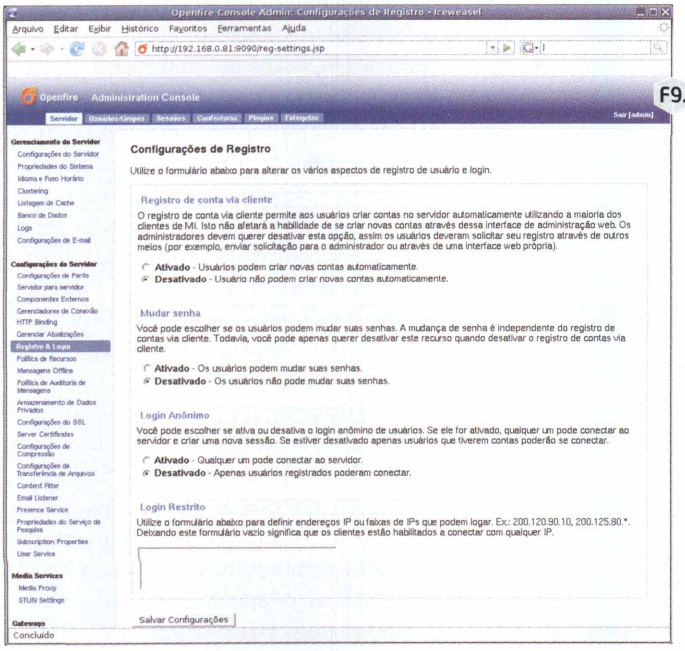
Nesta página vemos todas as configurações do servidor Openfire. Acesse a opção "Registro & Login" localizada dentro do submenu "Configurações do Servidor". Certifique-se de que o recurso



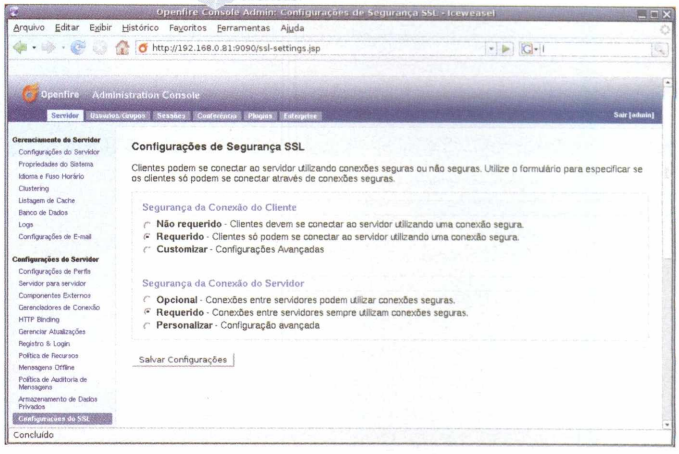
F7. Tela de logon do Openfire.



F8. Interface web de administração do servidor.



F9. Recurso "Registro & Login".

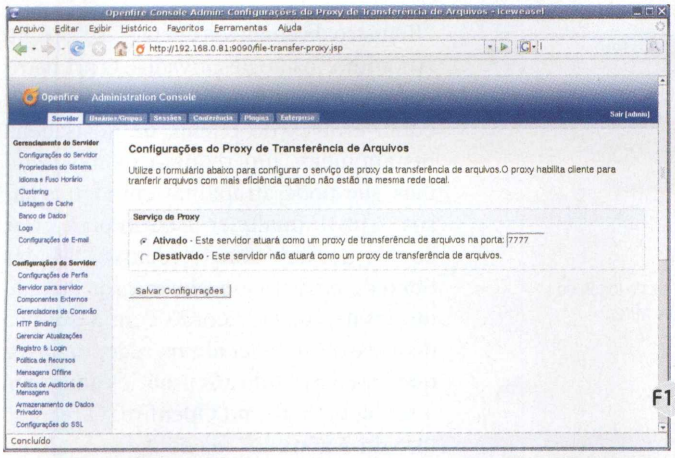


F10. Opções de segurança para o servidor e clientes.

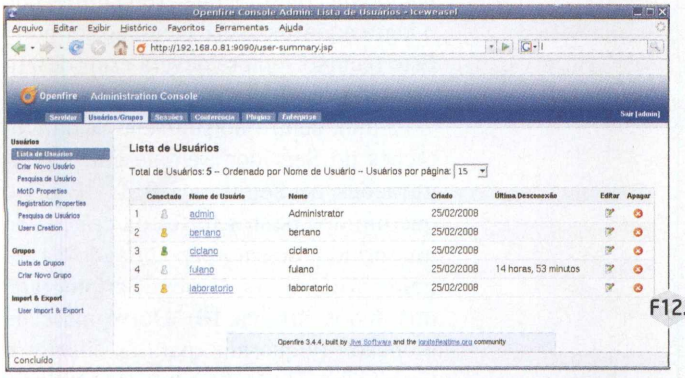
"Registro de conta via cliente" e o "Login Anônimo" estão desativados. O primeiro permitirá que os usuários registrem uma conta através do cliente de mensagens instantâneas, um recurso interessante, mas que pode atrapalhar em alguns casos. Afinal, qualquer usuário pode criar contas no servidor. O recurso "Mudar Senha", na verdade, deverá ser ativado ou desativado de acordo com a política de acesso estabelecida na rede, uma vez que será permitido aos usuários alterarem a senha de login no Openfire. O recurso "Login Anônimo" faz com que qualquer pedido de conexão, que esteja utilizando o login anônimo, seja aceito no servidor. Este recurso sempre deverá estar desativado (**figura 9**).

Ainda dentro do submenu "Configuraçoes do Servidor", clique em "Configurações de Segurança SSL". É certo que um dos pontos fortes da criação de um servidor de bate-papo privado é a segurança oferecida através da criptografia dos dados (**figura 10**). Deixe marcada a opção "Requerido" para os clientes e o servidor. Desta forma, a criptografia será realizada nas duas pontas da conexão (cliente/servidor). Feito isso, clique em "Configurações de transferência de arquivos" e, em seguida, marque a opção de habilitar este recurso. Assim todos os usuários poderão utilizá-lo para realizar a transferência de arquivos durante um bate-papo (**figura 11**).

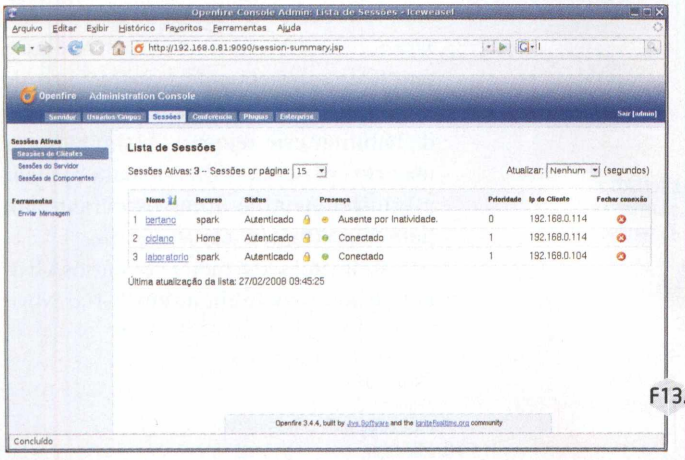
Agora acesse o menu "Usuários/Grupos" e dentro dele clique em "Criar Novo



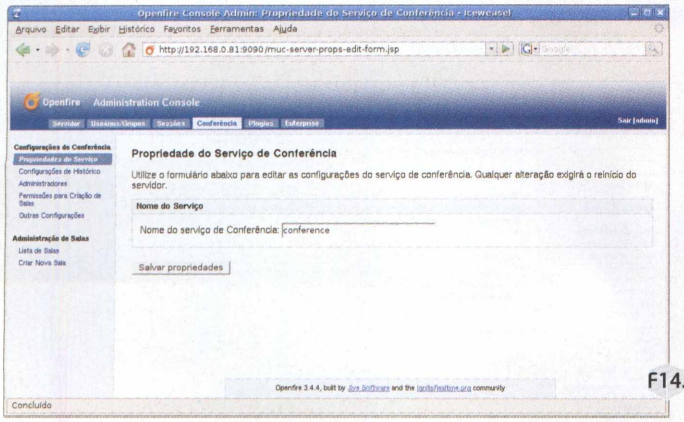
F11. Recursos de transferência de arquivos.



F12. Lista de usuários cadastrados.



F13. Sessões abertas no servidor.



F14. Sala de conferência Openfire.

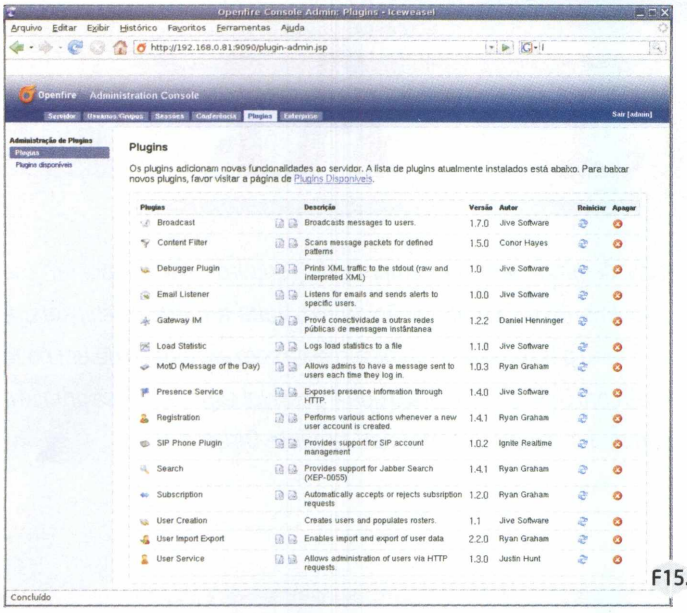
Usuário" (**figura 12**). Utilize o formulário que surgirá para adicionar as contas de usuários no Openfire. Assim que tiver preenchido todos os campos, clique no botão "Criar Usuário"(ou "Criar & Criar Outro"). Após cadastrar as contas clique em "Lista de Usuários", isso fará com seja exibida uma lista completa dos usuários e o status (online, offline ou ausente) de cada um deles (figura 12). Para modificar uma conta, basta clicarmos no ícone de edição, exibido abaixo da coluna "Editar" da figura 12. Durante os testes, a função de exportação (último recurso do lado esquerdo da figura 12) funcionou corretamente. Porém, a ferramenta de importação, para algumas contas, não transferiu as senhas dos usuários, o que fez do processo algo não tão automático, já que tivemos de reconfigurar as senhas novamente.

O menu "Sessões" nos permite acompanhar quais usuários estão logados e, conseqüentemente, com uma sessão aberta no servidor (**figura 13**). A opção "Enviar Mensagem", exibido dentro de "Ferramentas", permite ao administrador enviar uma mensagem para todos os usuários (online) simultaneamente. O próximo menu se refere à possibilidade de criarmos uma sala de "Conferência" para a troca de mensagens entre os usuários (**figura 14**).

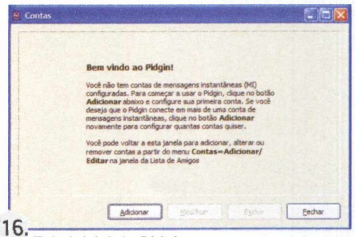
Ao lado, no menu "Plugins", é exibida uma lista dos componentes adicionais que estão instalados no Openfire. Aliás, todos os plugins disponíveis estão instalados (**figura 15**). O menu "Enterprise" apenas exibe um resumo da versão comercial do Openfire. O próximo passo agora é configurar os clientes.

Clientes Jabber

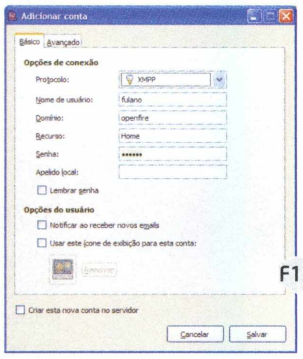
Dentre os vários programas clientes de mensagens instantâneas, podemos destacar o Pidgin (**www.pidgin.im**) e o Spark (**www.igniterealtime.org**). Além de suportarem o protocolo XMPP (entre outros protocolos), ambos são open source, rodam em plataforma Windows ou Linux e estão disponíveis para download no site do desenvolvedor - o arquivo de instalação do Pidgin possui 12 MB de tamanho, enquanto o Spark, 31 MB. Porém, apenas o Pidgin oferece suporte ao idioma português do Brasil,



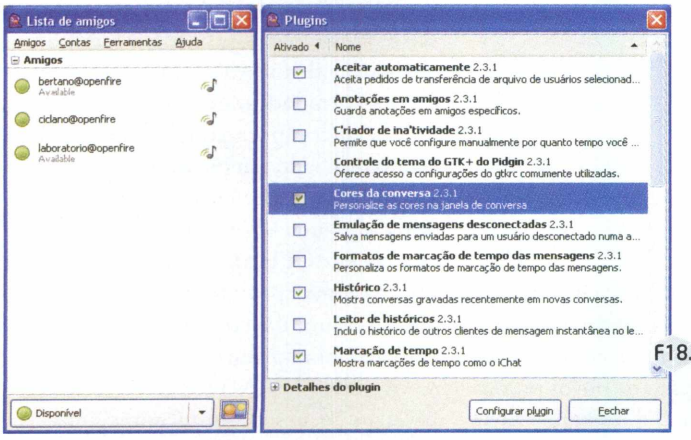
F15. Plugins instalados no Openfire.



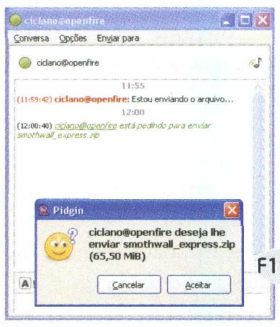
F16. Tela inicial do Pidgin (versão 2.3.1).



F17. Durante os testes nós utilizamos um servidor de DNS para fazer a resolução do hostname openfire.



F18. Lista de contatos (à esquerda) e painel de seleção dos plugins (à direita).



F19. Bate-papo e envio de arquivo entre usuários.

o que foi decisivo para o utilizarmos na apresentação, a seguir, de um exemplo de configuração de cliente de IM.

Após baixar e instalar o Pidgin, seja ele na versão Windows ou Linux, inicie o programa. A primeira tela solicitará o cadastro de uma conta de usuário. Clique em "Adicionar" (**figura 16**) e selecione o protocolo XMPP no campo "Protocolo". Em seguida, preencha os campos referentes ao nome de usuário, domínio, recurso e senha. Os campos "nome de usuário" e senha deverão ser preenchidos com os dados cadastrados no servidor Openfire. Já no campo "Domínio" devemos inserir o endereço IP ou o nome de host (**figura 17**). Aliás, o nome de host funcionará apenas se você tiver um servidor de DNS em sua rede e que nele seja possível atribuirmos o servidor Openfire na tabela de DNS estático. Isso se deve ao fato de o sistema da VM não possuir um software tal como o SAMBA, que se apresente na rede através do hostname. Agora acesse a guia "Avançado" (na parte superior da figura 17) e marque a opção "Requerer SSL/TLS". Desta forma a autenticação ocorrerá sem problemas, uma vez que o servidor foi configurado para apenas responder às requisições de conexões criptografadas. Clique no botão "Salvar".

Para adicionar um contato, basta utilizarmos a opção de menu "Amigos > adicionar amigo...". Na janela seguinte, digite o nome de usuário e apelido que deverá aparecer em sua lista de contatos. Feito isso, clique em "Adicionar". Agora que todos os contatos foram adicionados, vá até a opção de menu "Ferramentas > Plugins". No painel que surgirá, selecione os plugins a serem utilizados no Pidgin (**figura 18**). A partir deste ponto todos os usuários já podem transferir mensagens e arquivos entre si (**figura 19**).

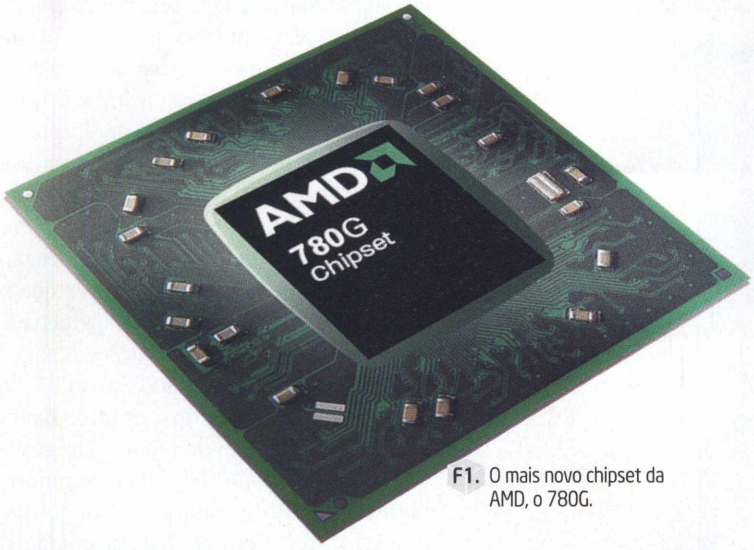
Conclusão

Rápida, eficiente e segura. Através desta máquina virtual você poderá, certamente, eliminar as possíveis brechas de segurança na utilização de mensageiros instantâneos instalados que, por sinal, também são alvos de malwares e spams. Por fim, caso esta entre para a sua lista de soluções da revista PC&CIA, não deixe de compartilhar suas experiências com mais esta máquina virtual. **PC**

Placas-mãe AMD

Depois de vários anos dependendo inteiramente de terceiros para suportar sua plataforma, a AMD, principalmente com a aquisição da ATI, volta a oferecer chipsets. A plataforma Spider foi o primeiro passo, agora a família cresce com a chegada de um novo membro, o 780G. Em testes com 3 placas, confira o que é possível esperar desse primeiro chipset a trazer, integrado no hardware, um GPU nativamente DirectX 10.

Anderson Costa



F1. O mais novo chipset da AMD, o 780G.

Há alguns meses, para dar uma suporte maior ao Phenon, a AMD lançou a plataforma Spider, focada em alto desempenho, e apresentou a série 7 de chipsets: os high-end 790X e 790FX, e o entry-level 770. Agora um novo membro se junta à família: o 780G, apresentando as mesmas qualidades dos "irmãos", mas contando com uma interface de vídeo integrada, a RADEON HD 3200, que traz atributos comuns aos outros modelos RADEON HD, como o suporte nativo ao DirectX 10, um diferencial e tanto para sistemas baseados no Windows Vista.

O 780G (**figura 1**) foi feito para os mercados Mainstream e Value. Alguns definem o termo "Value" como igual a entry-level, já outros como um intermediário entre o entry-level e o Mainstream. No momento, a definição que melhor se encaixa é a segunda.

De qualquer forma, vai chegar uma hora que o produto, seja ele qual for, será reposicionado. Por exemplo, com o passar do tempo e o lançamento de novos produtos, o que hoje é high-end irá para o nível mainstream ou mesmo para entry-level. E pensar que tal reposicionamento é aplicado dinamicamente a diversos elementos de TI. Há alguns anos, por exemplo, a resolução de 1024x768 com 32 bits de cor era considerada uma configuração high-end e a aplicação dos filtros anti-aliasing e anisotrópico eram ultra high-end; e hoje isso é considerado mainstream, principalmente levando em consideração o poder de processamento dos dispositivos.

O 780G

Financeiramente falando, a AMD sofreu perdas ao comprar a ATI. Já do ponto de vista técnico, foi uma aquisição e tanto, já que agora a empresa possui o *know-how* de dois mundos, o das CPUs e o dos GPUs (processadores gráficos), abrindo um número enorme de oportunidades, em um tempo que o potencial computacional dos GPUs está sendo utilizado em outros atividades que extrapolam o universo das imagens. E isso é algo que a NVIDIA não tem (foco apenas em GPU's) e que a Intel buscar obter com o projeto Larabee (CPU e GPU em um único chip), o qual ainda é apenas uma promessa.

A série 7 (AMD 7-Series) oferece diversos recursos muito apreciados, suportando o que há de mais moderno em termo de tecnologias disponíveis atualmente, como o DirectX 10, o Universal Video Decoding (decodificação de vídeos nos formatos VC-1, H.264 e MPEG-4 realizado pelo GPU), barramento HyperTransport 3.0, PCI Express 2.0, ACPI 3.0, escalabilidade e baixo consumo de energia.

Pelo seu enfoque no baixo consumo e não esquecendo que ele dispensa o uso de

uma controladora de memória (que já está no CPU), não é de se espantar que sua implementação seja feita sem uma solução de refrigeração ativa. De fato, uma solução passiva é mais do que suficiente, e conseqüentemente, pode operar com baixa emissão de ruídos.

Num primeiro momento, foram disponibilizados dois A780: o A780G (codinome RS780), que é o modelo empregado em todas as placas-mãe testadas nessa oportunidade; e o A780V (codinome RS780V). A diferença entre os dois se dá na interface de vídeo integrada, respectivamente a Radeon HD 3200 e a 3100.

A Radeon HD 3200 suporta a integração de conexões D-Sub, DVI e também a HDMI. Segundo a documentação, o HDMI foi integrado por completo, suportando vídeo e áudio, e claro, o HDCP, que é a proteção do conteúdo. Em tempo, embora ele ofereça a tecnologia SurroundView para o uso de até quatro monitores independentes quando em conjunto com uma interface de vídeo discreta, não é possível usar simultaneamente o DVI e o HDMI, apenas um deles com o D-Sub. Há também o suporte à conexão DisplayPort.

Um dos pontos fortes do 780G é a tecnologia Hybrid Graphics, que permite a configuração de um arranjo multi-GPU Crossfire entre a interface onboard e uma solução discreta. Até o momento, é compatível apenas com as Radeon HD 3400 (**figura 2**) e HD 2900.

O chip SouthBridge (Ponte Sul) SB700 é o par natural do 780G, trazendo integrado uma controladora SATA II com suporte a seis portas e a múltiplas configurações RAID, além do barramento PCI Express.

Ambientes de Testes

Os chipsets da série 7 foram desenvolvidos pensando no Phenon, porém a AMD não abriu mão da retrocompatibilidade com os processadores Athlon 64 já existentes, os quais podem ser usados sem qualquer problema nos novos sistemas, sendo necessário apenas se atentar à compatiblidade do soquete.

No caso, utilizamos um Athlon 64 X2 3800+ AM2, 2 GB de memórias Patriot modelo PDC22G8500ELK operando em Dual-Channel, HD Raptor de 10000 RPM da Western Digital, um DVD-RW da TSST e fonte de alimentação da OCZ, a OCZ-600ADJ SLI.

Devido ao suporte ao DirectX 10, a escolha do sistema operacional não poderia ser outra além do Windows Vista (utilizamos a versão Ultimate 32 bits). As versões do Catalyst para o 780G e para a placa de vídeo Radeon HD 3400 foi a 8.3, a mais recente à época do teste.

Os produtos

Tivemos a oportunidade de testar três modelos de diferentes fabricantes que se valem do 780G. Da ECS, temos a A780GM-A Black Series, da Biostar, a TA780G M2+ e da Asus, a M3A78-EMH HDMI.

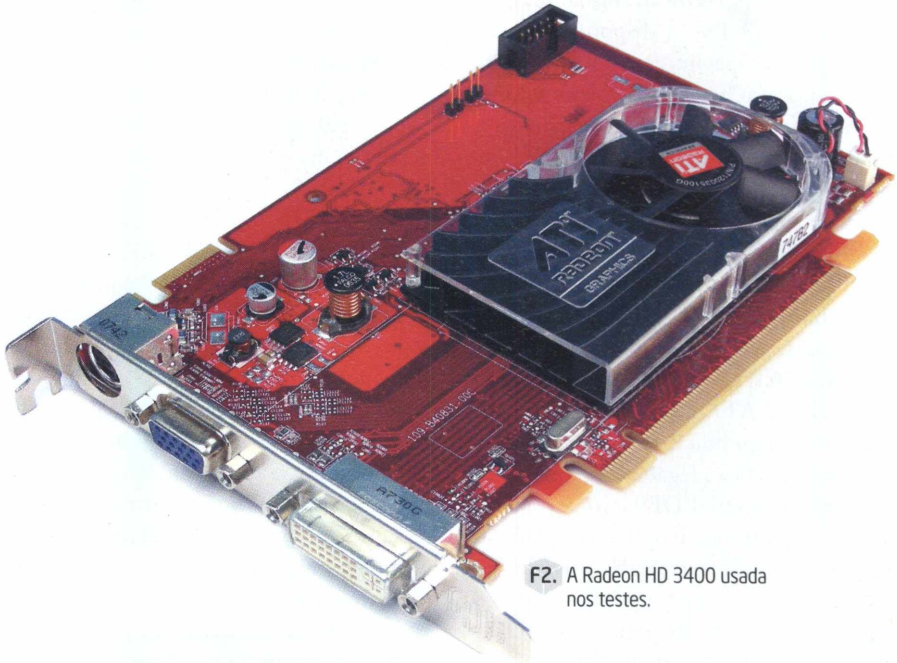
Procurando eliminar a má reputação adquirida pela PC Chips, nos últimos anos a ECS tem lançado produtos com qualidade bem superior. Melhoraram, mas ainda terão trabalho pela frente.

A Biostar, de certa forma, sempre correu por fora no Brasil, sendo que a sua principal característica era oferecer bons produtos com preços muitos convidativos, apresentando uma excelente relação entre custo e benefício.

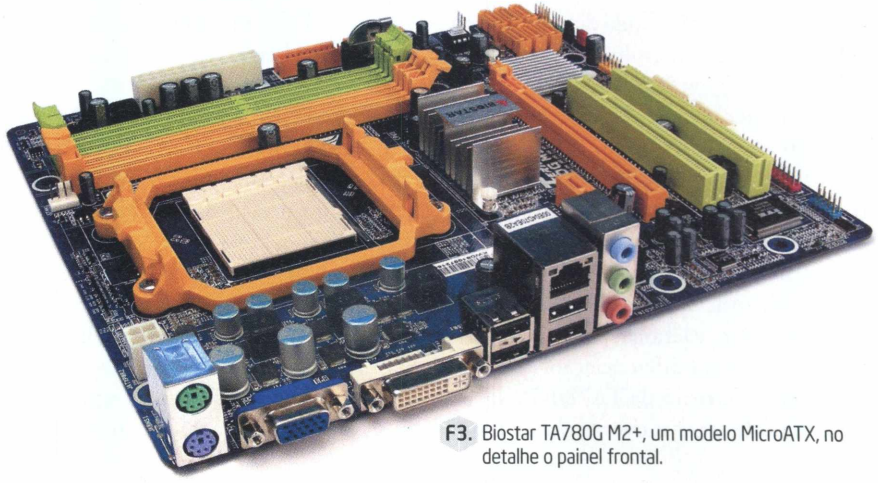
A Asus dispensa maiores comentários, embora alguns digam que a empresa só conseguiu uma boa fama no país porque só encontrou um concorrente quando aportou por aqui, no caso, a já fragilizada PC Chips. De qualquer forma, isso não passa de história, especulações e opiniões.

Biostar TA780G M2+

A TA780G M2+ (**figura 3**) é uma placa-mãe de formato MicroATX, integrante da T-Series. Infelizmente não encontramos nenhuma informação que diferencie os



F2. A Radeon HD 3400 usada nos testes.



F3. Biostar TA780G M2+, um modelo MicroATX, no detalhe o painel frontal.

F4. ECS A780GM-A Black Series: é a ECS fazendo a "lição de casa" para mudar sua reputação.

modelos da T-Series dos das demais séries, tal como a T-Power. Visualmente o único modelo T-Power disponível no site utiliza apenas capacitores de estado sólido, enquanto os da T-Series se valem de uma solução mista, inferior, com capacitores sólidos e eletrolíticos.

O soquete é o AM2+, como não poderia deixar de ser, já que o grande apelo do chipset 780G é o suporte ao Phenon. São quatro slots de memória DDR2 suportando até 8 GB, dois PCI 32 bits tradicionais, um PCI Express x16 e um x1, seis portas SATA e dez portas USB (quatro no painel I/O ATX e as outras seis para o painel frontal ou brackets adicionais). Em relação às interfaces legadas, há uma IDE, um floppy, um serial DB9 e uma paralela DB25, mas os respectivos brackets não são fornecidos, sendo necessário adquiri-los separadamente.

Além dos USB no painel I/O ATX, temos os PS/2 para teclado e mouse, um RJ45 da interface Ethernet, as conexões de áudio padrão AC'97 (saída de som estéreo, entrada de linha e microfone), um D-SUB e um DVI.

A interface de rede e a de áudio são da Realtek, respectivamente RTL8111C 10/100/1000 e a ALC662, que é padrão HD Audio de 5.1 canais.

O acabamento da placa é muito bom, cantos arredondados, headers e jumpers claramente identificados. Os slots usam duas cores, verde claro e laranja, para o equilíbrio estético e não para diferenciação.

Um característica da TA780GM2+ é a sua inclinação para o overclock, algo que não é comum a placas-mãe no formato MicroATX. O menu é bem completo, oferecendo grande gama de opções, tanto automáticas quanto manuais.

O processo de instalação do sistema operacional foi tranqüilo, isento de problemas, bem como a instalação dos demais componentes.

ECS A780GM-A Black Series

A A780GM-A (**figura 4**) é uma placa-mãe full ATX, que realmente se destaca do velho legado deixado pela PC Chips e das primeiras ECS. Embora a ECS seja freqüentemente alvo de críticas quanto a qualidade, nos últimos tempos tem procurado oferecer bons produtos e mesmo nos tempos mais obscuros, oferecia um ou outro produto de destaque, como a K7S5A, que no seu tempo foi uma excelente opção com uma relação de custo x benefício excepcional.

Em relação ao nome do produto, tal como aconteceu com a Biostar, não há aqui uma explicação sobre o que é a Black Series da ECS, mas pelo menos o produto faz uso do "black": sua caixa e a placa-mãe em si são da cor preta.

É empregado o soquete AM2+, quatro slots de memória DDR2, três slots PCI tradicionais, um PCI Express x16 e dois x1, cinco portas SATA e dez portas USB (quatro no painel I/O ATX e as outras seis para o painel frontal ou brackets adicionais). Quanto a interfaces legadas, há uma IDE, um floppy e um serial DB9, e como na Biostar, os bracket não são fornecidos, sendo necessário adquiri-los separadamente. A porta paralela não foi integrada.

O painel I/O ATX dispõe, além das USB, dos PS/2 para mouse e teclado, um RJ45 da interface Ethernet, um D-SUB, um HDMI, um eSATA e as conexões de áudio padrão HD Audio (seis portas de conexão). A presença do eSATA no painel I/O ATX explica a disponibilidade de apenas cinco portas SATA na PCB (placa de circuito impresso).

A interface de rede é a Atheros L1 da Atlansic, e a de áudio é a 92HD205XX5 da IDT. Para referência, a IDT adquiriu a Sigmatel, que tem, há anos, um bom know-how em codecs. Tipicamente vemos "dobradinhas" da Realtek nessas interfaces, porém nos últimos temos, temos visto um aumento do uso do Atheros L1 e uma diversidade maior nos de áudio, citando a Analog Devices como exemplo.

O acabamento da placa-mãe é bom, demostra bem as melhorias que a ECS tem feito em seus produtos. *São usadas mais* cores para os slots, mas não completamente distintivas, apenas quase. Os PCI tradicionais e o conector de floppy são na cor preta, o PCI Express x16 é vermelho, bem como dois slots de memória; os dois PCI Express x1 são amarelos, como também são os dois slots de memória restantes, o conector IDE e o header da porta serial; os SATA e os headers USB são laranja.

A ECS usa e abusa da identificação serigráfica, são feitas referências aos recursos, como SATA II, Hybrid Graphics, HDMI, USB 2.0, HT 3.0, AM2+, Phenon CPU, DDR2 1066, etc.

Falando em DDR2 1066, ele só vai operar quando o processador estiver nessa mesma freqüência, já que ao inicar, ele vai indicar uma condição de erro de configuração. É um inconveniente, porém a configuração definida pode ser iniciada após teclar para continuar.

Na instalação do sistema operacional, tivemos um problema. Quando a interface SATA era configurada para AHCI, os discos não eram mais identificados pelo sistema, só funcionava em modo IDE nativo. Esse problema foi corrigido ao atualizar o BIOS, e o processo continuou sem problemas.

Asus M3A78-EMH HDMI

A Asus oferece produtos para todas as faixas de preço, mas sempre mantendo sua qualidade, uma referência para diversos profissionais e também usuários. E assim

temos de produtos excepcionalmente exóticos aos incrivelmente simples. No caso, a M3A78-EMH HDMI (**figura 5**), de formato MicroATX, é um produto sem apelo visual, concentrando suas qualidades nos detalhes técnicos.

È utilizado o soquete AM2+, tem quatro slots de memória, dois PCI tradicionais, um PCI Express x16 e um x1, seis portas SATA e doze portas USB (quatro no painel I/O ATX e as outras oito para o painel frontal ou brackets adicionais). Quanto a interfaces legadas, há uma IDE, um floppy e um serial DB9 e uma paralela DB25. Os bracket não são fornecidos, sendo necessário adquiri-los separadamente.

O painel I/O oferece, além das USB, os PS/2 para mouse e teclado, um RJ45 da interface Ethernet, um D-SUB, um DVI, um HDMI, e as conexões de áudio padrão HD audio (seis portas de conexão). Como o chipset não permite o uso simultâneo das conexões DVI e HDMI, há um conjunto de jumpers, imediamente atrás deles, que define qual dos dois será usado. O padrão é o DVI.

A Asus optou por usar uma "dobradinha" da Realtek: para a interface de rede foi o RTL8111C, e para a de aúdio, o ALC882, um HD Audio.

Durante a instalação ocorreram alguns problemas, como o congelamento do sistema que foi resolvido ao mudar os slots de memória. Possivelmente era algum mau-contato, pois refizemos o processo algumas vezes para nos certificar da existência de algum problema grave que exigisse a troca.

"Botando para funcionar"

O comportamento padrão de qualquer interface onboard atualmente é ser desativada quando uma solução discreta é instalada no sistema. Com o 780G, não é diferente. Para ativar o CrossFire entre as interfaces onboard e a placa discreta, é preciso primeiro reconfigurar a ordem de inicialização de vídeo (**figura 6**). Embora a instrução para "ligar" o Crossfire seja ativar o SurroundView no BIOS, só conseguimos configurá-lo após fazer exatamente o contrário.

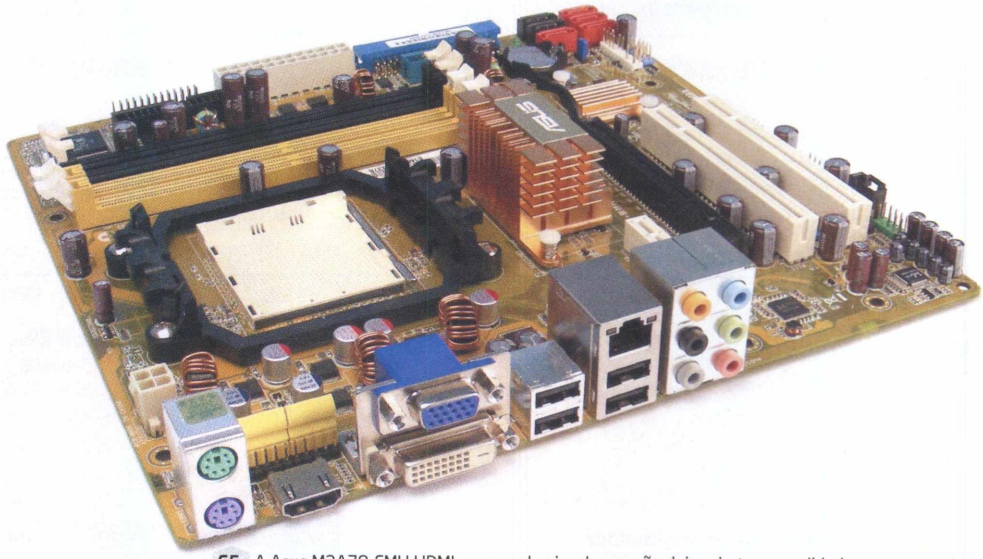
Conforme a versão de BIOS da placa-mãe utilizada, pode ser necessário configurar o BIOS a partir da placa de vídeo discreta e depois voltá-la para a onboard. Como se trata de BIOS, o processo pode ficar mais simples nas próximas revisões, como por exemplo, identificar a compatibilidade entre a interface de vídeo onboard e a offboard, e já se auto-ajustar.

Se tudo correr bem, ou seja, usar a versão mais recente do Catalyst Control Center e o BIOS devidamente configurado, a opção Crossfire será disponibilizada. Basta clicar na caixa de checagem para ativar. Se houver qualquer problema, simplesmente não será exibida a opção Crossfire.

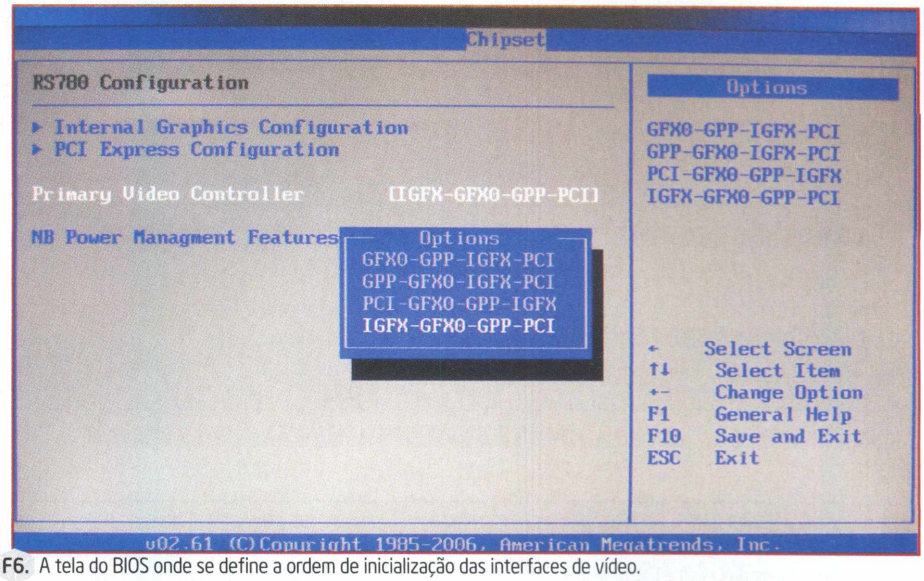
Testes

Os testes de benchmark foram feitos com os softwares PCMark2005, 3DMark05 e 3DMark06 focados no DirectX 9; Crysis e o Call of Juarez focados no DirectX 10. Também foi abordado o consumo de energia, sendo medido o consumo geral e as linhas de +12V.

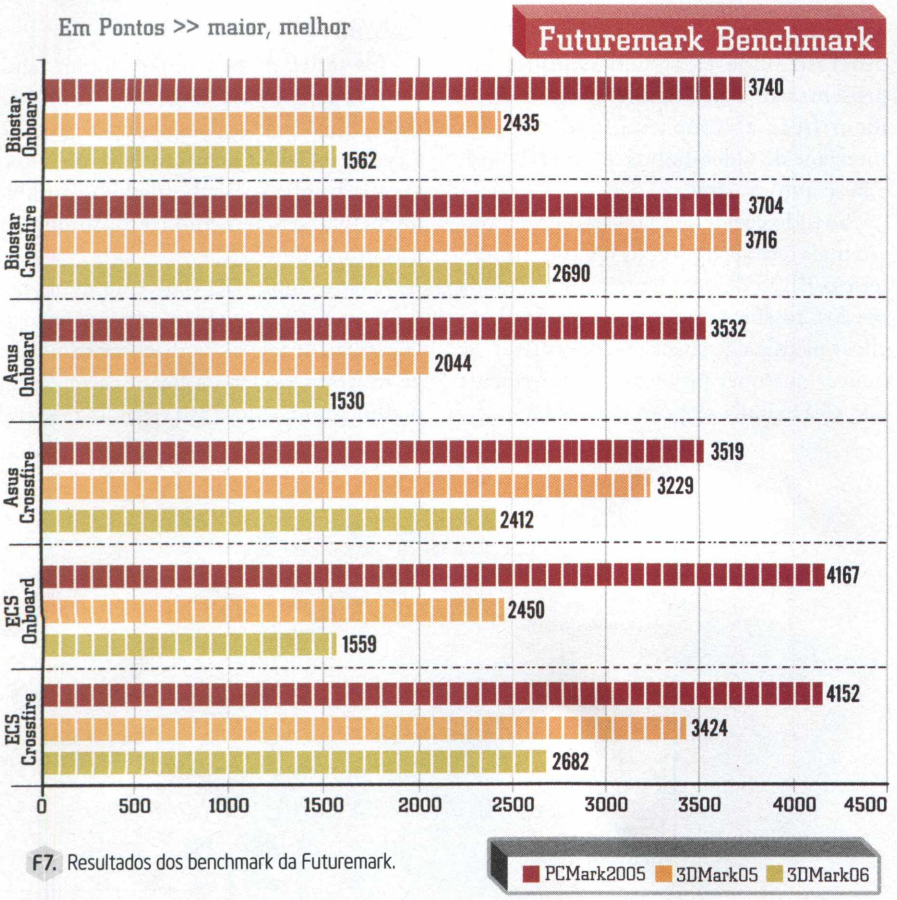
Começando pela vedete do momento, o DirectX 10. Considerando que os jogos que se valem dele são vorazes consumidores de recursos, podemos classificar o desempenho gráfico do 780G como razoável.



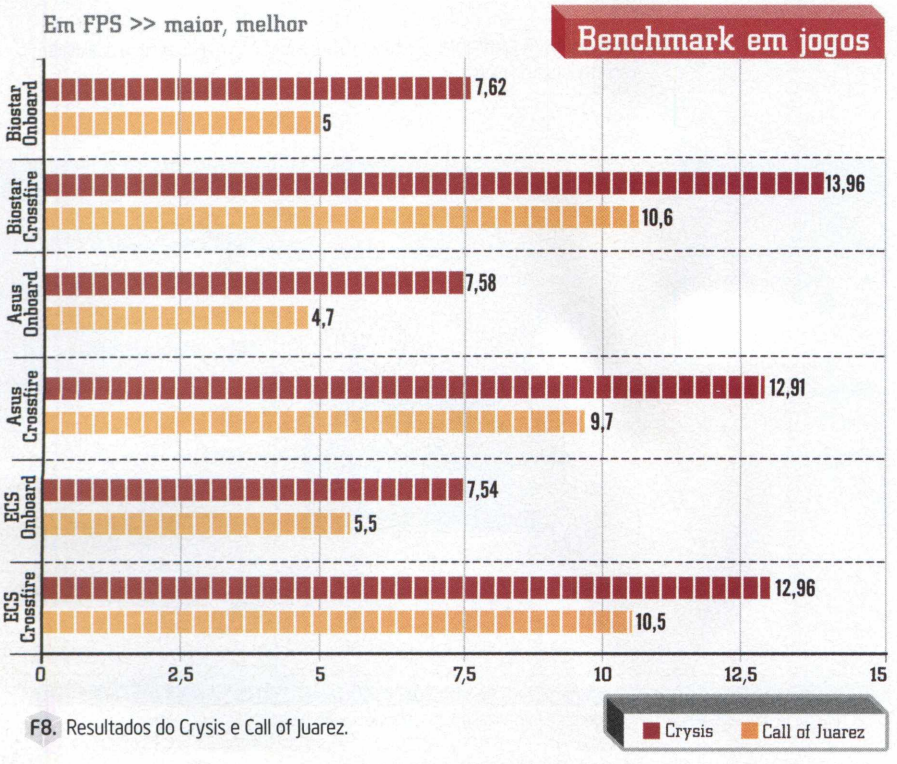
F5. A Asus M3A78-EMH HDMI, sem apelo visual, mas não deixa de ter a qualidade característica da marca.



F6. A tela do BIOS onde se define a ordem de inicialização das interfaces de vídeo.



F7. Resultados dos benchmark da Futuremark.



F8. Resultados do Crysis e Call of Juarez.

Evidentemente sua performance não vai rivalizar com uma solução discreta, mas é funcional. A tendência é que com o tempo e a natural evolução tecnológica, essa diferença diminua.

No Crysis e Call of Juarez, o uso do Hybrid Graphics praticamente dobra a performance dos jogos em termos percentuais. Em valores brutos, esses números têm pouca força, mas considerando que tanto o Crysis quanto o Call of Juarez fazem com que até mesmo sistemas de alta performance sofram para manter 30 fps, podemos dizer que o 780G não faz feio. Feio era na época do Quake III Arena, quando pouquíssimas interfaces onboard tinham poder para executá-la. E dentro desse grupo seleto, boa parte delas tinha memória dedicada.

Não há muito o que falar do DirectX 9, mas seus resultados continuam sendo relevantes diante da grande quantidade de jogos disponíveis no mercado, que foram feitos para ele. A diferença dos resultados entre a solução integrada e o Hybrid ficou em torno de 55%.

Já no PCMark2005, um software que reproduz o desempenho do sistema como um todo durante a execução de atividades comuns a todo usuário, não houve diferença entre as duas configurações.

Sobre o consumo de energia, teremos que rever alguns conceitos. O pico atingido pelo 780G foi de 140W, contra uma média de 85W das demais soluções existentes no mercado. Vale lembrar que esse pico foi atingido pela ECS A780GM-A, nas duas configurações.

A Biostar apresentou o mesmo comportamento, mas o seu pico ficou em torno de 120W. Já o modelo da Asus se comportou um pouco diferente. O pico em Hybrid Graphics foi também em torno de 120W, mas apenas com o onboard foi de 90W. Uma explicação possível para tal comportamento de consumo é que a Asus limitou a quantidade de memória para até 256 MB, contra 512 MB da ECS e da Biostar.

Todas as unidades testadas têm a opção de configuração automática de alocação de memória, que foi a opção definida. Conforme o caso, o sistema pode iniciar com toda a quantidade reservada, ou apenas com o mínimo possível. Tal detalhe foi aferido através da Central de Boas vindas do Windows, que exibe a quantidade de

memória do sistema, que variou entre 1.5 GB e 1.9 GB.

Ao usar o Hybrid Graphics, o consumo do processador cai em torno de 35%, o que indica que o poder do processador vai impactar na performance de vídeo. Novamente a Asus foi a única exceção, apresentando elevação no consumo.

Talvez o fato de possuir mais slots explique o maior consumo da ECS, e o limite de memória da Asus ajude a entender a diferença nos resultados dos benchmarks e no consumo de energia.

Conclusão

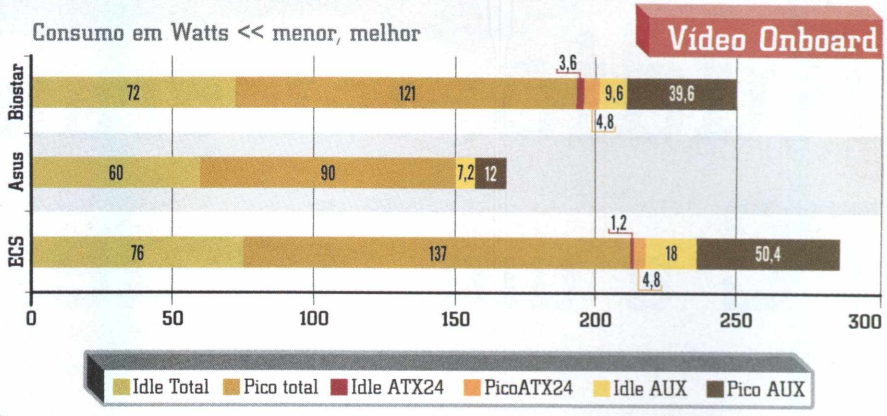
Respeitando o posicionamento atual do mercado para o 780G e também as suas respectivas características técnicas, não resta dúvidas de que este chipset apresenta um desempenho digno de nota. Além disso, traz um GPU nativamente DirectX 10 e oferece um bom caminho de upgrade no sistema de vídeo ao suportar um arranjo multi-GPU CrossFire com uma placa de vídeo discreta. E por último, é uma ótima solução para montar um Media PC devido ao circuito UVD, integrado no GPU, o qual cuida da aceleração do processamento de vídeos em diferentes formatos, incluindo alta definição.

Podemos encará-lo como o primeiro de uma nova série de produtos que chegarão ao mercado no decorrer deste ano, já que a questão custo, principalmente nos países em desenvolvimento, é muito importante, e nesse caso, as soluções que oferecem as melhores condições serão vencedoras e conseguirão seu lugar ao sol.

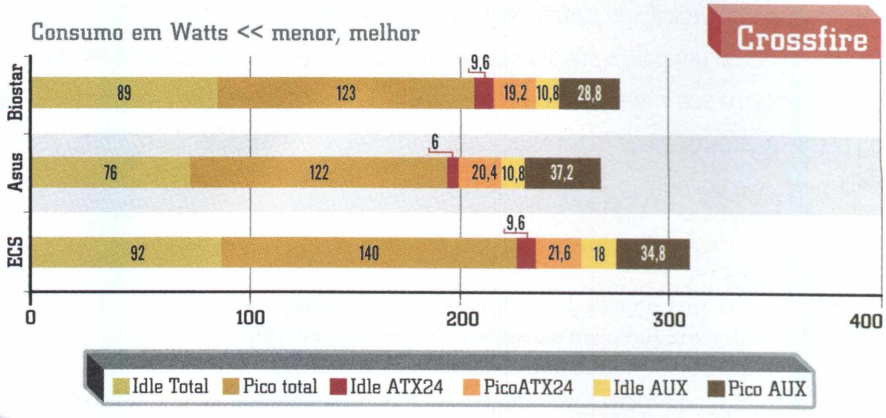
Dentre os modelos testados, a escolha será definida pelos recursos oferecidos por cada um ao confrontar com as necessidades do usuário. Por exemplo, se a necessidade é por mais slots PCI, a escolha é a ECS; se a opção for um upgrade com suporte a dispositivos legados ou disponibilidade de opções para overclock, a escolha é a Biostar; mas se a opção é pela disponibilidade de saídas digitais de vídeo, a escolha é a Asus.

Com o lançamento da plataforma Spider e agora com o novo integrante da família, a AMD ganha um novo folego na disputa no mercado, encorpando o seu fronte de combate.

PC



F9. Consumo do sistema usando video onboard



F10. Consumo do sistema em Crossfire

Áudio: integrando um PC a um Home Theater

Integrar um Media Center ou computador a um sistema de Home Theater ficou mais fácil com a substituição do padrão AC'97 pelo HD Audio.

Vamos falar um pouco sobre essas arquiteturas e como planejar e obter o melhor desempenho na sua interligação com um sistema de Home Theater convencional. Existem diversas características e funções que merecem ser exploradas, embora, como sempre, nem tudo seja perfeito.

Até há uns poucos anos atrás o padrão de áudio em placas-mãe era o AC'97, ou Audio Codec '97. Esse padrão foi criado pela Intel para a implementação de sistemas de áudio onboard em placas-mãe e outros dispositivos como modems, por exemplo. Ele consiste de um conjunto de conversores A/D (analógico/digital) e D/A (digital/analógico) que permitem converter os sinais de áudio de analógico para digital e vice-versa.

Na implementação da Intel, esse sistema possui duas partes: um controlador embutido no Southbridge ICH (I/O Controller Hub – Ponte Sul) do chipset e um chip Codec, como o chip AD1981B AC'97 SoundMAX CODEC, da Analog Devices Em chipsets de outros fabricantes, como a AMD, nVidia, SIS, etc, a implementação é semelhante, ou seja, também utilizando um controlador no Southbridge e um codec externo.

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.

Algumas características e funções disponíveis no chip AD1981B são:

- Possui 2 DAC's com faixa dinâmica de 90dB e 2 ADC's com faixa dinâmica de 85dB;
- Apresenta função equalizador integrada e detecção automática dos conectores (jack sense);
- A saída SPDIF suporta as taxas de amostragem de 48kHz e 44,1kHz com o formato PCM de 20 bits.

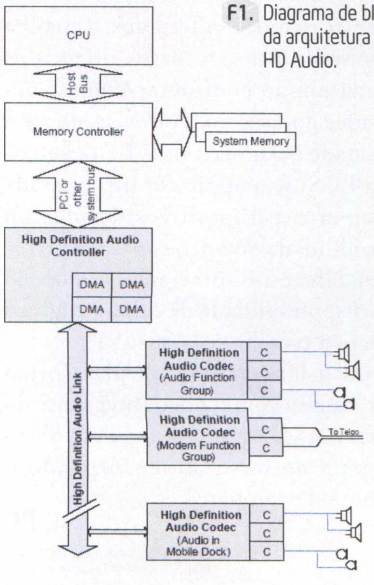
Devido ao aumento do interesse na utilização de computadores como fonte de entretenimento, a Intel introduziu em 2004 o padrão HD Audio como substituição ao, já limitado, AC'97. O HD Audio foi implementado a partir do chip Southbridge ICH6.

Esse padrão apresenta diversas melhorias em relação ao antecessor, tais como: arquitetura similar à empregada nas placas de som, melhora nas características de faixa dinâmica, relação sinal/ruído e distorção, embora esses fatores dependam da implementação e do esforço do fabricante da placa-mãe, além do chip codec.

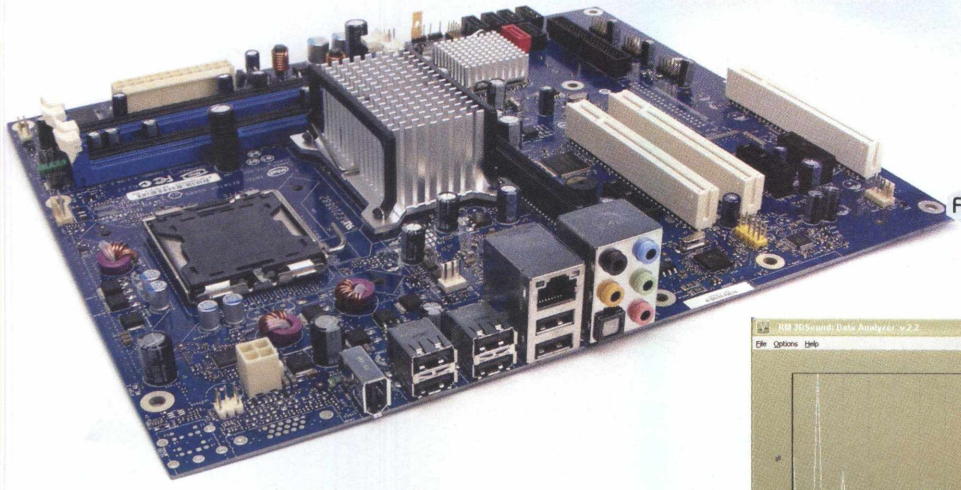
Sua função de detecção de conectores, que permite ao driver descobrir que tipo de equipamento foi conectado, e a reatribuição de função aos conectores, permitem uma simplificação na conexão de microfones, fones e caixas acústicas de forma que mesmo quando ligados a conectores originalmente dedicados a outras funções, o driver irá detectar esse fato e redirecionar as funções a fim de manter o sistema funcionando corretamente.

Outro aspecto importante do HD Audio, talvez o mais importante para o usuário, é que ele permite gerenciar vários *streams* de áudio independentes simultaneamente. Pelo menos é o que se espera...

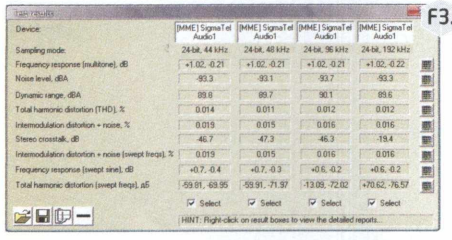
A arquitetura do HD Audio contempla o uso de vários canais de acesso direto à memória para uma operação mais suave e sem falhas (**figura 1**).



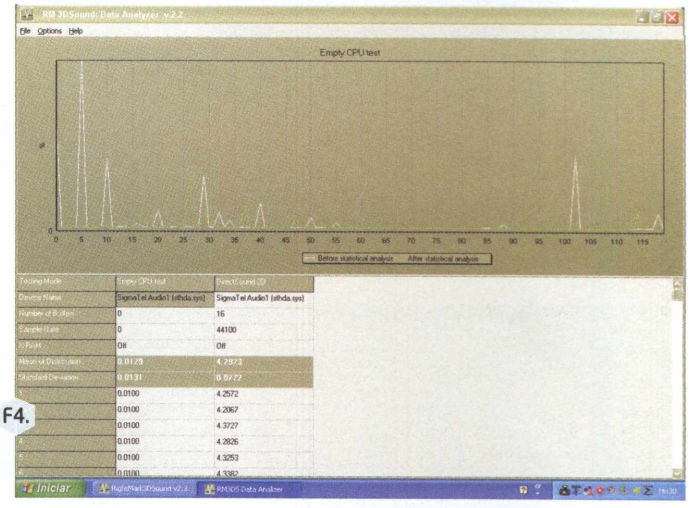
F1. Diagrama de blocos da arquitetura Intel HD Audio.



F2. Placa-mãe Intel DP35DP.



F3. Resultados obtidos no teste da placa-mãe Intel DP35DP, no modo 24 bits.



F4. Resultado do teste de utilização de CPU para a placa DP35DP.

Dentro das melhoras no sistema de áudio podemos citar a possibilidade de trabalhar com sinais de 24 bits com taxa de amostragem de 192kHz, embora isso irá trazer pouca, ou nenhuma, diferença para o ouvinte em relação a um som de 16 bits com taxa de 44,1kHz.

O importante é a evolução do sistema de som integrado com relação às placas de som independentes. A carga de trabalho do processador com relação à interface de áudio foi reduzida em relação ao padrão AC'97. Essa é uma melhoria muito bem-vinda.

Algumas placas HD Audio

Resolvemos fazer alguns testes com duas placas que implementam a arquitetura HD Audio, uma Intel e outra AMD. O modelo escolhido da Intel foi o DP35DP, da Media Series, e do lado da AMD ficamos com o modelo M3A78, fabricado pela Asus. Ambas são opções modernas e estão disponíveis no mercado.

Para a avaliação das interfaces foram utilizados os softwares RightMark Audio Analyzer versão 6.0.6 e RM 3DSound 2.3 (**http://audio.rightmark.org/download.shtml**).

Intel modelo DP35DP Media Series

A placa DP35DP (**www.intel.com/products/motherboard/DP35DP/index.htm**) utiliza o chipset Northbridge P35 e Southbridge ICH9R, além do chip codec IDT STAC9271D (**http://www.idt.com/?genID=STAC9271**). O subsistema de áudio onboard é formado pelos dois últimos chips citados acima, pelo conjunto de conectores do painel traseiro, além dos headers para conectores do painel frontal e HD Audio Link (**figura 2**).

Esse subsistema suporta o padrão Dolby Home Theater, com uma relação sinal/ruído (S/N) de 95dB, capacidade de áudio multicanal 7.1 através de 8 conversores digital/analógico (DAC) independentes usando os conectores do painel traseiro, mais um sinal estéreo usando o conector do painel frontal (HD Audio Header), totalizando dez DACs, e uma interface óptica digital através da porta S/PDIF no painel traseiro.

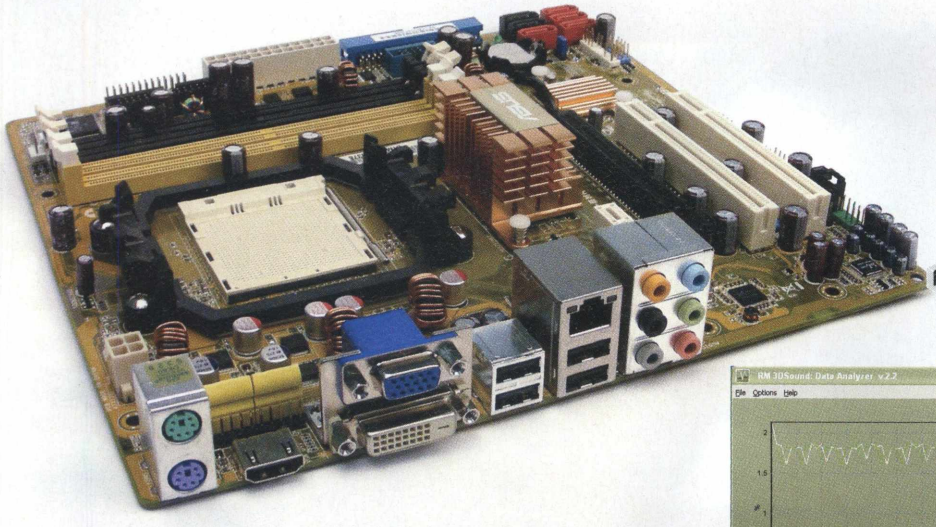
O codec utilizado, STAC9271, apresenta dez canais com nível de qualidade para Home Theater e permite que o sistema opere com oito canais (sinal 7.1) e mais dois canais para um sinal estéreo independente. Os resultados obtidos na implementação da Intel, operando com 24 bits, podem ser vistos na **figura 3**.

O resultado do teste de utilização de CPU pode ser visto na **figura 4**.

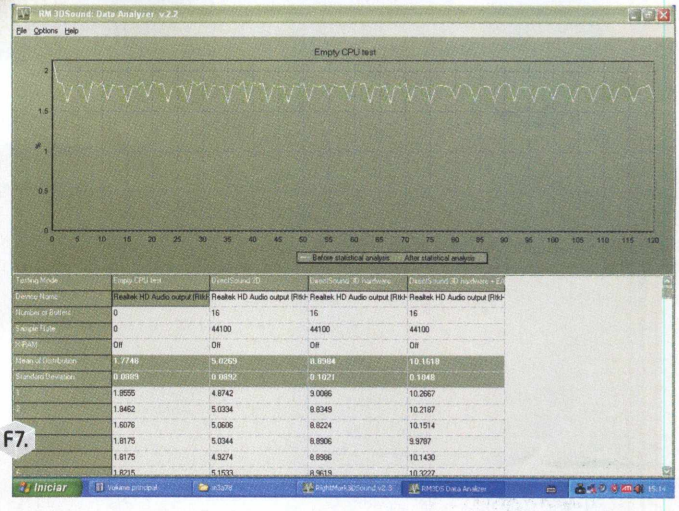
De um modo geral, os resultados foram bons para um sistema onboard, com exceção do teste de interferência entre canais (stereo crosstalk), que resultou em valores bastante altos, especialmente com a taxa de amostragem em 192kHz. Os valores obtidos foram semelhantes aos lidos com resoluções de 8, 16 e 32 bits também.

Esse problema pode ser causado pela implementação elétrica do circuito, por alguma inconsistência do software (driver e/ou software de teste), ou simplesmente defeito na unidade testada.

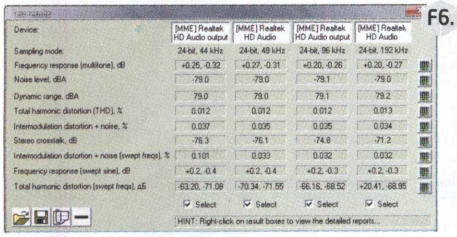
Essa deficiência irá causar uma diminuição da separação entre canais, reduzindo a imagem estereofônica. Já no teste de uso de CPU o resultado foi muito bom, com um uso médio de 4,29%, mas deve ficar claro que o modo detectado utilizou apenas o DirectSound 2D.



F5. Asus M3A78-EHM HDM.



Resultados para o teste de utilização de CPU com a placa M3A78-EHM HDMI. F7.



F6. Resultados dos testes da placa-mãe Asus M3A78-EHM HDMI para o modo de 24 bits.

Asus modelo M3A78-EHM HDMI

A placa M3A78, da Asus, **http://www.asus.com/products.aspx?l1=3&l2=149&l3=639&l4=0&model=2064&modelmenu=1**, utiliza o chipset AMD 780G na combinação com o Southbridge SB700, além do chip CODEC Realtek ALC883 (**figura 5**).

Como possui vídeo onboard, a M3A78 apresenta ainda uma interface HDMI, o que facilita muito sua integração com sistemas de Home Theater. Além do HDMI, esta placa possui a opção de instalar uma interface S/PDIF externa, opcional. Os resultados obtidos podem ser vistos na **figura 6**.

Para o teste de uso de CPU, os resultados estão demonstrados na **figurar 7**.

Esta placa apresenta bons resultados com valores compatíveis para todas as resoluções (8, 16, 24 e 32 bits), mesmo com taxa de amostragem de 192kHz.

No caso do nível de ruído (Noise Level) o valor obtido (79dB) é bastante alto, já que o codec ALC883 informa os valores de 95dB para os DAC's e 85dB para os ADC's. Isso pode ser atribuído à implementação do circuito elétrico mais à placa de circuito impresso.

O teste de uso de CPU apresentou os valores médios de 5,02% para o modo DirectSound 2D, 8,89% para o modo DirectSound 3D e 10,16% para o modo DirectSound 3D + EAX.

Considerando as duas soluções avaliadas, a que apresentou os resultados mais equilibrados foi a M3A78, a qual ainda conta com uma interface HDMI, o que irá facilitar muito sua inclusão em um sistema de Home Theater.

Já a placa DP35DP, por sua vez, embora tenha proporcionado resultados melhores na maioria dos testes, apresentou um resultado muito ruim no teste de crosstalk e essa é uma deficiência facilmente percebida, mesmo para ouvidos sem muita experiência. O que aliado à facilidade apresentada pela interface HDMI da placa Asus, faz com que a escolha recaia sobre a M3A78-EHM HDMI. Observe que essa avaliação é apenas do ponto de vista do sistema de áudio onboard.

Sistemas de Home Theater

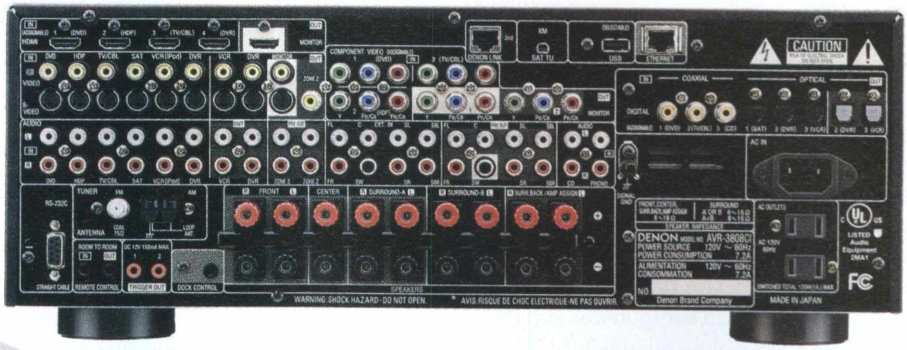
Qualquer sistema de Home Theater é baseado em um equipamento central que tem como função selecionar a fonte de sinais, fazer seu processamento e enviar esses sinais para os alto-falantes.

Essas funções podem ser executadas por um computador ou por um equipamento próprio, conhecido como receiver A/V. Se o Home Theater for montado sobre um computador ele irá apresentar algumas limitações como, por exemplo, o número de entradas de sinal disponíveis. Além disso, padrões como o SACD (Super Audio CD), que apresenta áudio multicanal, não possuirão suporte sem o uso de um DVD player externo que aceite esse formato. Não existe nenhum player para computador (e aparentemente nunca existirá!) que aceite o formato SACD. Aqui me refiro ao formato multicanal, já que existem discos SACD híbridos. Neste caso, contudo, o áudio será PCM estéreo tal como o é em um CD comum. Para um computador, funções como o setup automático da instalação, com o uso de microfones calibrados, também não estarão disponíveis.

Um receiver A/V possui entradas para as diversas fontes de sinal, como DVD player, receptor de satélite, vídeo cassete, CD player, player de MP3, etc. Dependendo da classe, e obviamente do custo, mais ou menos entradas e recursos estarão disponíveis. Da mesma forma que para a interface de som dos computadores, receivers 5.1, 6.1 ou 7.1 poderão ser encontrados.

Como exemplo podemos citar o Receiver A/V Denon, modelo AVR3808, que possui capacidade de 7.1 canais com potência de 130W cada, e uma grande quantidade de conexões e recursos. Na **figura 8** podemos ver seu painel traseiro com os conectores de entrada e saída. Praticamente qualquer fonte de sinal pode ser conectada nesse equipamento.

Um computador com função de Media Center e uma saída SPDIF, seja coaxial ou óptica, pode fornecer seu sinal para o receiver. Neste caso o receiver irá tratar a decodificação do sinal multicanal com seu decodificador interno. Caso o computador não possua uma saída S/PDIF, ainda assim poderemos utilizá-lo como fonte de sinal, só que escolhendo um receiver que possua as entradas analógicas para os sinais surround. É o caso, por exemplo, do modelo AVR-788, também da Denon (**http://usa.denon.com/ProductDetails/3641.asp**).



F8. Receiver AVR3808, da Denon (http://usa.denon.com/ProductDetails/3510.asp). Note a extensa gama de opções de conexão, incluindo 6 entradas digitais (3 coaxiais e 3 ópticas) e 2 saídas digitais ópticas. Esse equipamento pode decodificar diversos formatos Dolby Surround e mais alguns outros padrões.

Neste caso os sinais das caixas frontais, central, surround laterais, surround traseiras e subwoofer serão ligados a entradas específicas do receiver, do mesmo modo como são feitas as ligações de caixas acústicas multicanal amplificadas normais.

Para se conectar as saídas da interface de som do computador (conectores P2) com as entradas analógicas do receiver, deve-se usar adaptadores P2 macho/RCA fêmea.

Se forem utilizadas as saídas multicanal do computador, todo o processamento do sinal será executado por este.

Sistemas de Home Theater também permitem a criação e controle de zonas diferentes de uso. Isso significa que enquanto se assiste a um filme com áudio surround na sala, pode-se desfrutar da audição de ▶

música estéreo em outra sala a partir do mesmo receiver, da mesma forma como prometido pela plataforma HD Audio.

Alguns receivers permitem a criação de mais de duas zonas de utilização, como é o caso do Denon ADR3808, o qual suporta a criação de três zonas com o auxílio de um amplificador externo para a terceira (neste caso poderiam ser utilizadas as caixas amplificadas do computador, supondo que elas sejam de boa qualidade).

Se a interface de som do computador for de boa qualidade e possuir entrada S/PDIF, este poderá ser utilizado como gravador com capacidade multicanal. Uma placa que apresenta essa possibilidade é a Creative X-Fi Xtreme Audio, que possui entrada e saída SPDIF ópticas.

Além dessas possibilidades, também existem as interfaces HDMI, que em muitos equipamentos permitem a transmissão apenas de vídeo, mas que foi projetada para transmitir também o áudio digital.

Na escolha de um computador para ser utilizado junto com um Home Theater, é importante verificar se a interface HDMI também trabalha com o áudio. Isso também se aplica ao receiver, já que alguns modelos aceitam apenas a transmissão de vídeo. A função dessa interface é permitir a transmissão digital com alta largura de banda e simplificar as conexões. Para exemplificar, podemos dizer que um simples cabo HDMI, funcionando com áudio e vídeo, irá substituir um cabo DVI (mais rígido e de maior diâmetro, sem falar no tamanho do conector!) e um coaxial ou óptico no caso de se utilizar a saída SPDIF. A situação ficará pior se forem utilizadas as saídas de áudio analógicas do computador (8 canais ou 4 cabos RCA duplos). Olhe novamente a imagem do painel traseiro do receiver e tente imaginar a confusão de cabos se todas as entradas analógicas forem utilizadas.

Interligando as coisas

Ligar um computador a um sistema de Home Theater é um trabalho relativamente simples.

Como o receiver trabalha como um seletor de entradas, bastará conectar as saídas de áudio e vídeo do computador em uma entrada de áudio e vídeo do receiver.

Se a interface for HDMI completa (áudio e vídeo), bastará um cabo para completar o serviço.

Se forem utilizadas uma saída DVI e uma SPDIF, serão dois cabos mais um adaptador DVI para HDMI (entrada do receiver).

Caso não seja utilizada uma saída digital de vídeo, poderão ser utilizadas as saídas S-Video ou de vídeo composto mais a conexão de áudio, que pode ser digital (preferível) ou analógica (última opção).

De qualquer maneira, a escolha do modo de conexão depende dos recursos disponíveis tanto no computador quanto no receiver. A escolha desses componentes poderá simplificar ou complicar a implementação do sistema.

Conclusão

Aplicações de Home Theater estão a cada dia mais comuns e os computadores vêm constantemente apresentando melhores opções de uso como central de entretenimento. Parece óbvio que estes dois componentes iriam terminar se encontrando.

Hoje em dia é possível encontrar ambos com boa qualidade e recursos compatíveis, em uma ampla faixa de preços. Tudo irá depender de uma escolha criteriosa e uma busca cuidadosa.

No lado do computador, a interface de áudio é o componente de interesse. Seja uma placa de áudio separada ou a interface integrada, a escolha do padrão HD Audio ou sistema compatível é desejada. Computadores mais antigos, ou mais baratos com o padrão AC'97, são bons para as caixas de computador. Se forem ligados a um sistema de áudio de boa qualidade, poderão mostrar suas limitações em nível de ruído, distorção e faixa dinâmica, resumindo, mostrar suas limitações devido a implementações de baixo custo e menos cuidadosas.

Com relação ao HD Áudio, devemos observar que a característica de *multi-streaming*, que é citada por todos, desde o fabricante do codec até os manuais das placas-mãe, não pôde ser testada porque não encontramos uma única referência de como fazê-lo.

Sempre que um *headphone* ou caixa acústica é ligado ao conector frontal, os conectores do painel traseiro são silenciados. O que falta para essa característica funcionar? Drivers? Software (players)? O fato é que embora especificamente implementada, a operação *multi-streaming* (um sinal multicanal sendo reproduzido através dos conectores do painel traseiro ao mesmo tempo que um sinal estéreo é reproduzido através do conector do painel frontal) não foi possível. Mesmo com a utilização do Windows Vista.

Devemos lembrar que o padrão HD Audio foi lançado em 2004.

Voltando à escolha de uma placa-mãe, outro aspecto que deve ser observado é o chip CODEC utilizado na interface de áudio. Dentro do padrão HD Audio existem diversas opções de implementação, cada uma com suas vantagens e desvantagens. Um mesmo CODEC em duas placas diferentes apresentará resultados diferentes. Infelizmente isso se aplica a todos os componentes do sistema e não seria diferente para as interfaces de áudio.

Uma forma de escolha, que embora não seja garantia de bons resultados, mas já é um bom começo, é procurar os modelos de placa-mãe voltados para aplicações de Media Center. É de se imaginar que os fabricantes se esforcem para obter bons resultados na interface de áudio desses modelos. Dentro dessa linha avaliamos dois modelos, um da Intel e outro da Asus. A placa-mãe DP35DP, da Intel, não possui vídeo onboard e, portanto, não possui interface HDMI, que deverá ser obtida através da placa de vídeo. Possui todas as conexões para áudio digital e analógico integradas em seu painel traseiro.

A placa M3A78-EMH HDMI, da Asus, totalmente baseada em uma solução AMD, possui a interface HDMI integrada, mas a conexão de áudio digital, óptica e coaxial, necessita a instalação de uma interface opcional.

Quanto mais recursos de conectividade existirem, melhor, especialmente a interface digital S/PDIF. No caso dos receivers, a escolha dependerá dos recursos desejados e do orçamento disponível, é claro.

Interfaces HDMI e S/PDIF irão facilitar muito a integração de computadores com sistemas de Home Theater.

Por último, vale dizer que o estudo das especificações e a leitura atenta dos manuais dos equipamentos envolvidos são fundamentais para a obtenção do resultado desejado com o mínimo de investimento e dor de cabeça.

PC

Asterisk: o nome da revolução no mercado de telefonia

Veja como instalar e configurar um PABX baseado em software livre, capaz de reduzir drasticamente os custos de telefonia em sua empresa.

Flávio de Souza Oliveira

Há tempos o movimento software livre vem quebrando paradigmas no mercado de computação, permitindo a difusão de conhecimento e a quebra de monopólios. Mas desde 1999 uma nova frente de batalha foi aberta: o milionário mercado das telecomunicações, graças a um software revolucionário chamado Asterisk (**www.asterisk.org**).

O Asterisk é um programa que implementa todas as funções de um PABX convencional e muito mais. Totalmente baseado em software livre, ele proporciona muitos benefícios devido ao seu suporte a diversos protocolos de Voz sobre IP (VoIP). Além de substituir seu PABX convencional, ele torna possível, a um custo extremamente reduzido, a agregação de funções disponíveis apenas em equipamentos de PABX de grande porte, os quais custam algumas centenas de milhares de reais. O VoIP também permite cenários como:

- Oferecer um ramal a funcionários que estão em casa via Internet;
- Integrar ramais telefônicos de escritórios em diversas partes do mundo via Internet (**figura 1**);
- Correio de voz;
- Construir aplicações de resposta automática por voz e integrá-lo a sistemas internos de controle de estoque ou confirmação de entrega de pedidos, por exemplo. Entre outras possibilidades.

Com essa matéria, iniciamos uma pequena série onde apresentaremos e configuraremos passo-a-passo algumas das principais funções do Asterisk. Nessa edição, em específico, faremos uma introdução ao software, aprenderemos a instalá-lo e configuraremos alguns ramais utilizando apenas comunicação VoIP. Vamos lá então!

Conceitos

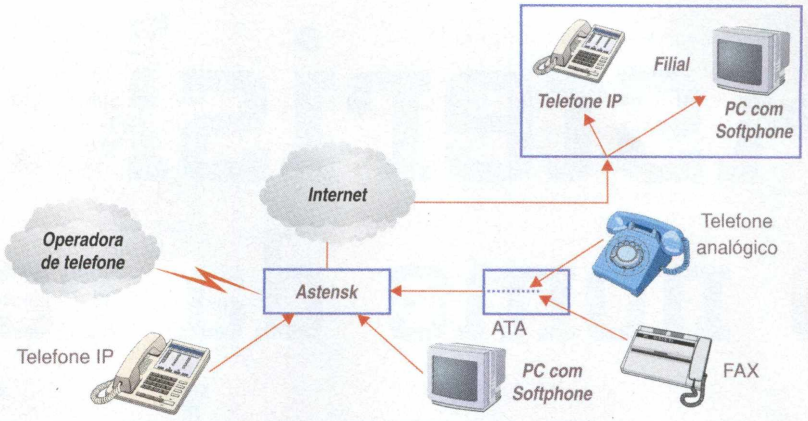
O primeiro ponto importante é entender que tipos de agentes podem participar de uma sessão VoIP. Naturalmente, os agentes que vão participar de uma comunicação desse tipo devem obrigatoriamente implementar uma pilha TCP/IP para poderem se comunicar via Internet. Dessa forma, os agentes mais comuns são PCs equipados com Softphones como o Xlite (**www.counterpath.com**), Twinkle (**www.twinklephone.com**) ou Ekiga (**http://ekiga.org**), além de Telefones IP como o modelo BudgeTone-100, da Grandstream Networks, que utilizaremos durante essa matéria (**figura 2**).

Entretanto, uma pergunta muito comum durante a implantação do Asterisk em uma instituição é se não há como aproveitar os aparelhos de telefone e fax existentes. A resposta é sim, graças à utilização de pequenos adaptadores conhecidos como ATA (Adaptador para Telefone Analógico). Durante essa matéria utilizaremos o modelo HandyTone-496, também produzido pela Grandstream Networks (**figura 3**).

Para que uma comunicação via VoIP seja estabelecida, nós precisamos da combinação de dois elementos: um CODEC para codificação de áudio no formato digital e um protocolo de sinalização capaz de lidar com questões relacionadas à sinalização de telefonia. Quando esses dois elementos são combinados, permitindo a comunicação entre dois pontos da rede, nós temos o que chamamos de canal VoIP, que é análogo a um circuito formado quando temos uma comunicação via linha telefônica convencional.

O protocolo de sinalização mais difundido atualmente é o SIP (Session Initiation Protocol), principalmente por se tratar de um padrão aberto e documentado via RFC (**www.faqs.org/rfcs/rfc3261.html**). Entretanto, existem outros protocolos, alguns proprietários, como são os casos do Nortel Unistim, Cisco SCCP, entre outros. Em relação ao modelo de referência OSI (**http://pt.wikipedia.org/wiki/Modelo_OSI**), o SIP pode ser classificado como um protocolo de aplicação que utiliza o modelo "requisição-resposta", muito similar ao protocolo HTTP (*HyperText Transfer Protocol*).

Para finalizar nossa pequena introdução teórica, resta ainda falar do último elemento para a composição de um canal VoIP, os CODECs. Na natureza, o som é uma onda analógica que, por sua vez, necessita ser convertida em um sinal digital para trafegar na Internet. Essa conversão cabe a algoritmos conhecidos como CODECs. Os mais utilizados são o G.711 alaw (utilizado na Europa e no Brasil), G.711 ulaw (utilizado nos EUA), GSM, entre outros.



F1. Arquitetura típica para implementação do Asterisk.

A negociação do CODEC a ser utilizado em uma conversação é feita entre as duas partes com a mediação do Asterisk, sendo que ele pode, se necessário for, atuar como tradutor quando as duas partes não conseguirem firmar um acordo para utilizar um CODEC único.

Cenário

Nosso objetivo nessa primeira matéria é instalar o Asterisk em uma instituição, considerando que teremos que configurar ramais em softphones, telefones IP e aproveitar aparelhos telefônicos convencionais através da utilização de ATAs. Nas matérias subseqüentes vamos aprender a configurar uma URA (Unidade de Resposta Audível) e filas de atendimento, como as que são utilizadas em *Call Centers*, além de aprendermos como realizar a integração com a rede de telefonia convencional.

O servidor PABX de nossa instituição será um computador instalado com Linux utilizando a distribuição Debian na versão Etch. Devido à grande defasagem da versão do Asterisk que acompanha o Etch, iremos fazer a instalação do PABX a partir dos fontes, o que gera um pouco mais de trabalho, mas garante que estaremos usando a versão mais atual do software e ainda teremos um binário totalmente adaptado ao nosso hardware.

Instalação

A compilação do Asterisk começa pela obtenção de suas dependências. Sendo assim, o primeiro passo é conferir se o ar-

F2. Telefone IP BudgeTone-100.

quivo /etc/apt/sources.list está configurado corretamente e com todos os repositórios necessários, conforme demonstrado na **figura 4**. Lembrando que as alterações do arquivo sources.list e todas as demais ações administrativas que executaremos aqui devem ser realizadas utilizando o usuário root.

Com o arquivo sources.list corretamente configurado, precisamos atualizar a lista de pacotes disponíveis para instalação. Para isso abra um terminal *shell* e execute o comando apt-get update (**figura 5**).

Em seguida podemos obter as bibliotecas necessárias para a compilação do Asterisk com o comando apt-get apresentado na **figura 6**.

Uma vez instaladas as bibliotecas podemos fazer o download dos arquivos-fonte do Asterisk. Para isso acesse o diretório /usr/src (cd /usr/src) e utilize o comando wget para fazer o download dos seguintes arquivos: asterisk-1.4-current.tar.gz (**figura 7**), zaptel-1.4-current.tar.gz (**figura 8**) e libpri-1.4-current.tar.gz (**figura 9**).

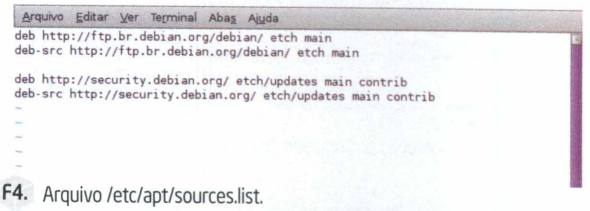
Após o download dos fontes, efetue a descompactação primeiramente do pacote zaptel, que contém os módulos de kernel utilizados pelo Asterisk para se comunicar com as placas de telefonia da Digium e similares. Mesmo que sua máquina não vá possuir nenhuma placa para comunicação com a rede de telefonia convencional, é necessário instalar esse pacote, pois nele existe um módulo chamado ztdummy utilizado para oferecer ao Asterisk uma referência de clock de telefonia, na falta de uma placa para esse propósito. Para efetuar a compilação e instalação dos módulos, execute o comando tar zxvf zaptel-1.4-current.tar.gz, acesse o diretório recém-criado (cd zaptel-1.4.9.2/ em nosso caso) e execute o comando ./configure && make && make install (**figura 10**).

Em nosso caso ainda não teremos uma placa para comunicação com a rede de telefonia convencional, sendo assim, faremos uso apenas do módulo ztdummy, o qual pode ser carregado através da execução do comando modprobe ztdummy (**figura 11**). Para que esse módulo seja carregado automaticamente durante o boot da máquina, utilize o comando echo "ztdummy" >> /etc/modules.

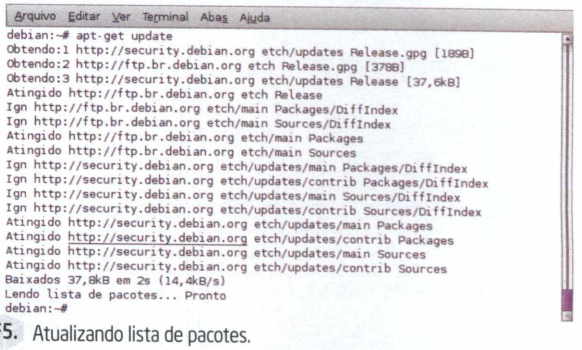
A próxima etapa é a instalação da biblioteca libpri, que é uma implementação em linguagem C da Interface de Taxa Primária ISDN (*Integrated Services Digital Network*), utilizada quando temos uma placa Digium, ou compatível, ligada a um link de voz ISDN. Portanto, a instalação da libpri não é obrigatória. Para instalá-la, acesse novamente o diretório /usr/src (cd /usr/src), efetue a descompactação do pacote com o comando tar zxvf libpri-1.4-current.tar.gz, em seguida acesse o diretório recém-criado (cd libpri-1.4.3/ em nosso caso) e execute o comando make clean && make && make install (**figura 12**).

Com todas as dependências instaladas podemos finalmente iniciar a instalação do Asterisk propriamente dito. Para isso, acesse o diretório de download dos fontes (cd /usr/src), em seguida efetue a descompactação dos fontes através do comando tar zxvf asterisk-1.4-current.tar.gz, em seguida acesse o diretório recém-criado (cd asterisk-1.4.18.1/ em noso caso) e execute o comando ./configure && make && make install && make samples && make config (**figura 13**). Para iniciar o Asterisk, execute o comando /etc/init.d/asterisk start e pronto, nosso PABX está instalado.

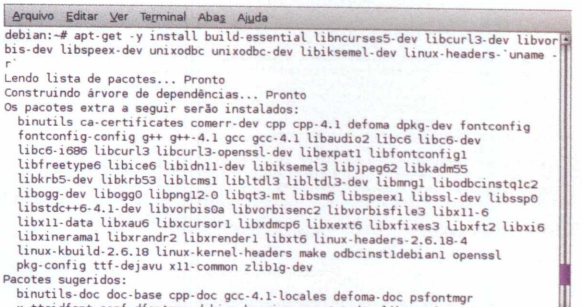
F3. Adaptador ATA HandyTone-496: para equipamentos analógicos, como telefones e fax, poderem participar da rede IP. Disponível em www.turbolink.com.br.



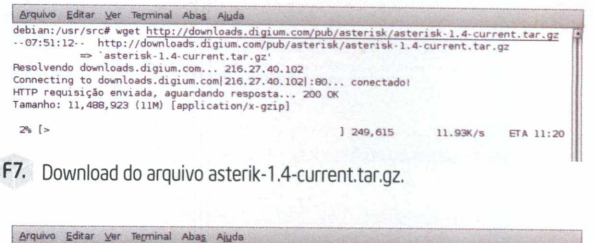
F4. Arquivo /etc/apt/sources.list.



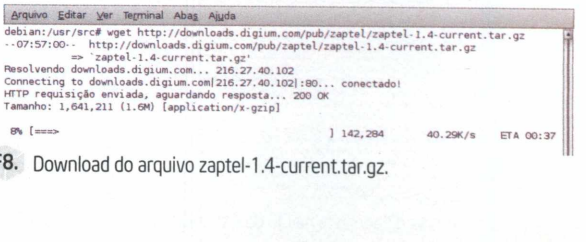
F5. Atualizando lista de pacotes.



F6. Download das bibliotecas para a compilação do Asterisk.



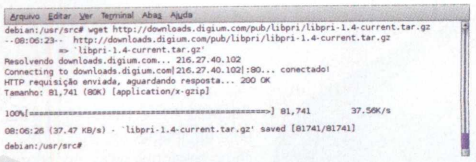
F7. Download do arquivo asterik-1.4-current.tar.gz.



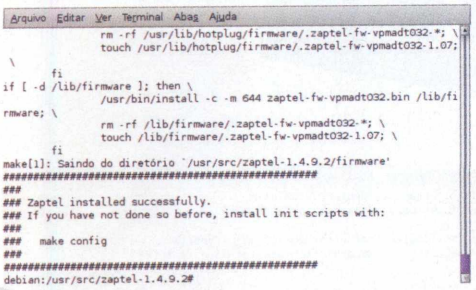
F8. Download do arquivo zaptel-1.4-current.tar.gz.

Configuração

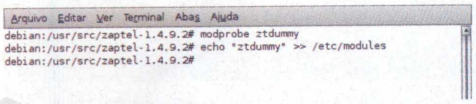
Apesar do Asterisk suportar diversos protocolos VoIP, em nossa instituição vamos adotar como padrão o uso de SIP em conjunto com



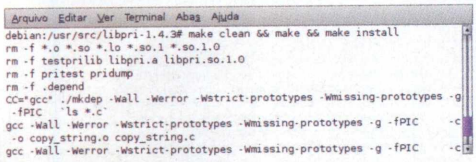
F9. Download do arquivo libpri-1.4-current.tar.gz.



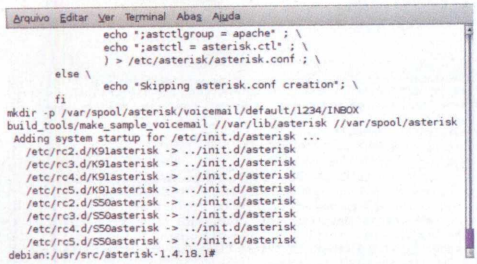
F10. Resultado da execução do comando ./configure.



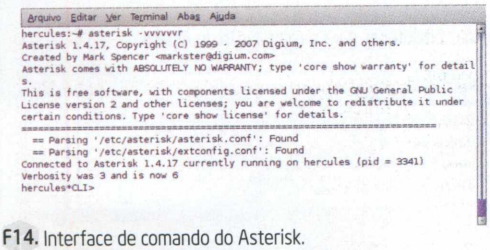
F11. Inicialização do módulo ztdummy.



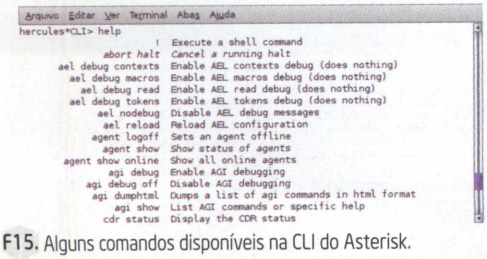
F12. Instalação da biblioteca libpri.



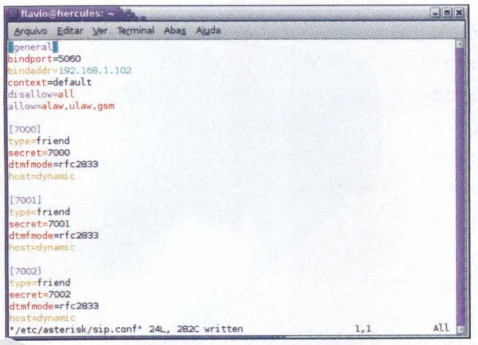
F13. Resultado da execução do comando ./configure para instalação do Asterisk.



F14. Interface de comando do Asterisk.



F15. Alguns comandos disponíveis na CLI do Asterisk.



F16. Conteúdo do arquivo /etc/asterisk/sip.conf.

o CODEC G.711 alaw, configurados em três tipos de agentes: Softphones, Telefones IP e ATAs.

Interface de comando

O Asterisk possui uma poderosa interface de comando (CLI) que pode ser utilizada para monitorar o comportamento do software. Ela é importante durante a depuração de problemas, pois quando colocada em modo *verbose*, exibe informações detalhadas de tudo que está sendo executado pelo PABX. É também através dessa interface de comando que obrigamos o Asterisk a reler arquivos de configuração, o que para nós é o mais importante no momento.

Para acessar a CLI, utilize o comando asterisk -vvvvvr, por exemplo (**figura 14**), no qual a quantidade de "v's" indica o quanto de informação será exibida no modo *verbose*. E o r indica que não queremos iniciar uma nova instância de Asterisk, mas sim se conectar em uma que esteja em execução. Para maiores informações sobre os comandos da CLI, execute o comando help (**figura 15**).

Criação dos Ramais

Os ramais SIP são definidos no arquivo /etc/asterisk/sip.conf. Primeiro execute o comando mv /etc/asterisk/sip.conf /etc/asterisk/sip.conf.bk para fazer um backup do exemplo trazido pelo Asterisk e utilize um editor de textos para criar um novo arquivo /etc/asterisk/sip.conf com as configurações exibidas na **figura 16**.

Note na figura 16 que configuramos três ramais: 7000, 7001 e 7002, cujas opções detalharemos a seguir:

- [general] : a seção "general" do arquivo sip.conf indica as opções *default* para todos os ramais;
- bindport=5060 : porta utilizada para comunicação SIP;
- bindaddr=192.168.1.102 : endereço IP no qual o Asterisk estará ouvindo conexões;
- context=default: é possível definir contextos de ramais, dessa forma um mesmo PABX poderia ser usado, por exemplo, por diferentes instituições, cada uma com seu próprio ctontexto de ramais. Em nosso caso, teremos apenas o contexto *default*;
- disallow=all: por *default*, todos os CODECs que não forem explicitamente permitidos serão proibidos;
- allow=alaw,ulaw,gsm : CODECs permitidos por *default* em sua ordem de preferência;
- [7000]: início da configuração do ramal 7000;
- type=friend: indica que o ramal pode receber e originar chamadas SIP. Existem também o tipo "peer", que apenas recebe chamadas, e o tipo "user", que apenas origina chamadas;
- secret=7000 : senha para autenticação SIP;
- dtmfmode=rfc2833 : padrão utilizado para tratamento dos digitos DTMF (Dual-Tone MultiFrequency) de telefonia;
- host=dynamic: podemos especificar o endereço IP do equipamento que poderá se registrar com esse ramal. Em nosso caso deixamos dinâmico, que indica que a autenticação pode ser feita a partir de qualquer endereço IP da rede.

As alterações nesse arquivo podem ser ativadas através da execução do comando sip reload na CLI (**figura 17**).

Plano de discagem

O plano de discagem indica o que o Asterisk deve fazer quando recebe uma chamada. Armazenado no arquivo /etc/asterisk/extensions.conf, esse plano se assemelha a um *script* e nele podemos encadear

as mais variadas ações, tanto através das aplicações oferecidas nativamente pelo Asterisk, quanto por outras que podem ser construídas pelo administrador.

Vamos agora criar um plano de discagem simples para nossa instituição. Para isso faça um backup do exemplo trazido pelo Asterisk com o comando mv /etc/asterisk/extensions.conf /etc/asterisk/extensions.conf.bk e utilize um editor de textos para construir um novo arquivo /etc/asterisk/extensions.conf com as configurações da **figura 18**, que detalhamos a seguir:

- [default]: indica o contexto ao qual as próximas configurações se referem;
- exten=>7000,1,Dial(SIP/7000,20,t): indica que ao receber uma chamada para o ramal 7000, o Asterisk deve encaminhar para o agente SIP que estiver logado com esse ramal através da aplicação Dial. O parâmetro 20 indica o tempo máximo que o ramal deve permanecer tocando em segundos. Já o último parâmetro da aplicação Dial pode conter diversas opções; a opção t que estamos utilizando indica que o destinatário da chamada será capaz de transferi-la para um outro ramal;
- exten=>7001,1,Dial(SIP/7001,20,t): idem ao item anterior;
- exten=>7002,1,Dial(SIP/7002,20,t): idem ao item anterior.

Até o momento, quando um ramal de nosso PABX era acionado, apenas uma aplicação era executada, a aplicação Dial, o que já é suficiente para termos ramais ligando uns para os outros. Entretanto, é possível fazer com que várias aplicações sejam executadas em lote quando uma chamada é recebida, graças ao segundo parâmetro do plano de discagem. Vejamos:

exten = {1º parametro}, {2º parametro}, {3º parametro},

- {1º parametro}: serve para comparar com os números recebidos pelo PABX. É possível criar expressões regulares seguindo uma gramática que analisaremos mais adiante nessa série de matérias;
- {2º parametro}: indica a prioridade (ordem) de execução de uma aplicação, caso o primeiro parâmetro combine com o número recebido pelo PABX;
- {3º parametro}: indica a aplicação a ser executada caso o primeiro parâmetro combine com o número recebido pelo PABX. Nos casos vistos anteriormente, tínhamos a aplicação Dial. É possível obter uma lista das aplicações disponíveis através da execução do comando core show applications, na CLI (**figura 19**)

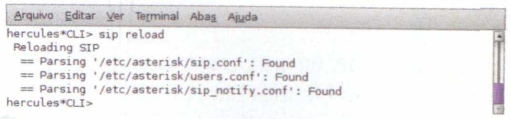
A seguir descrevemos as demais linhas de nosso plano de discagem:

- exten=>6000,1,Answer(): indica que ao receber o número 6000, o PABX deve atender a ligação através da aplicação Answer();
- exten=>6000,2,PlayBack(demo-thanks): após a execução da aplicação de prioridade 1, o PABX deve executar a aplicação PlayBack(), que por sua vez reproduzirá um arquivo Wav chamado demo-thanks;
- exten=>6000,3,HangUp(): após a execução das aplicações de prioridade 1 e 2, o PABX deve executar a aplicação HangUp(), que por sua vez desliga a chamada.

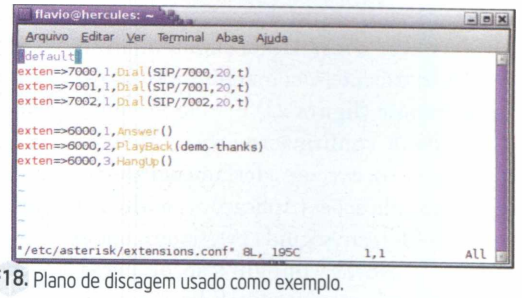
Ao final da configuração do novo arquivo extensions.conf, acesse a CLI do Asterisk e digite o comando dialplan reload para carregar as alterações do plano de discagem (**figura 20**).

Configurando os agentes

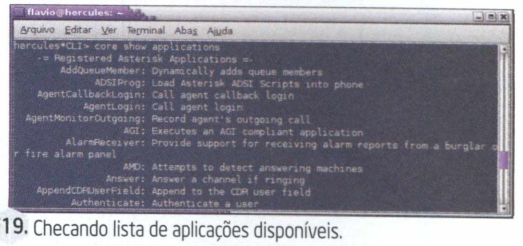
Agora vamos para a parte mais divertida de nossa implantação, que é finalmente testar todas as configurações feitas até agora. Configuraremos cada um dos três ramais que criamos em três agentes diferentes: um no softphone (Twinkle), um no telefone IP e um no ATA, para depois poderemos realizar chamadas entre eles. Vamos lá!



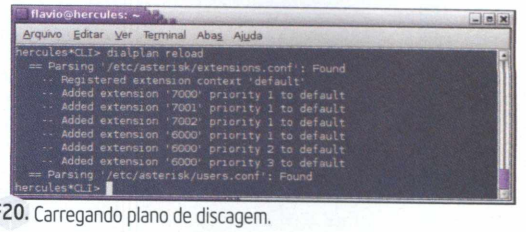
F17. Ativando configuração do Asterisk.



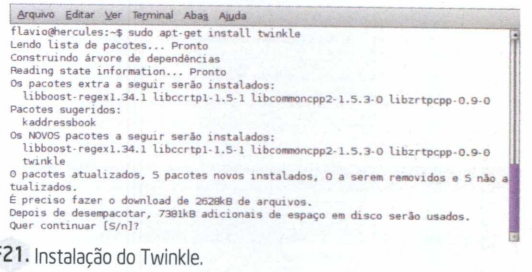
F18. Plano de discagem usado como exemplo.



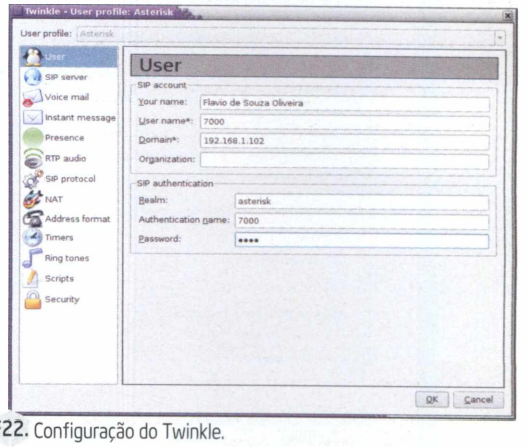
F19. Checando lista de aplicações disponíveis.



F20. Carregando plano de discagem.



F21. Instalação do Twinkle.



F22. Configuração do Twinkle.

Softphone

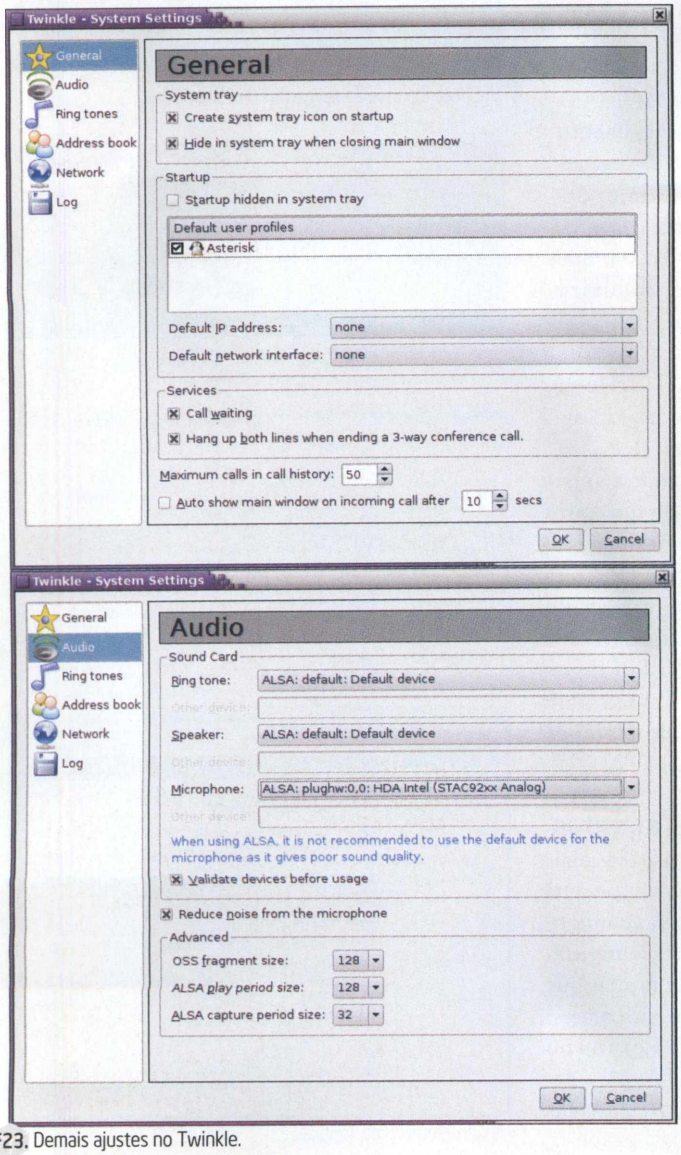
A máquina na qual instalaremos o softphone é um Ubuntu Linux versão 7.10. Escolhemos para esse exemplo o Twinkle, mas as configurações são semelhantes para todos os outros citados anteriormente. Para realizar a instalação, abra um terminal *shell*, execute o comando sudo apt-get install twinkle (**figura 21**) e responda sim à pergunta de confirmação.

Feito isso, execute a ferramenta através do menu aplicações (Aplicações → Internet → Twinkle), em seguida pressione o botão OK no aviso de configuração de perfil, pressione o botão "Profile Editor" na tela subseqüente e então escolha um nome para o perfil (no nosso caso, escolhemos Asterisk).

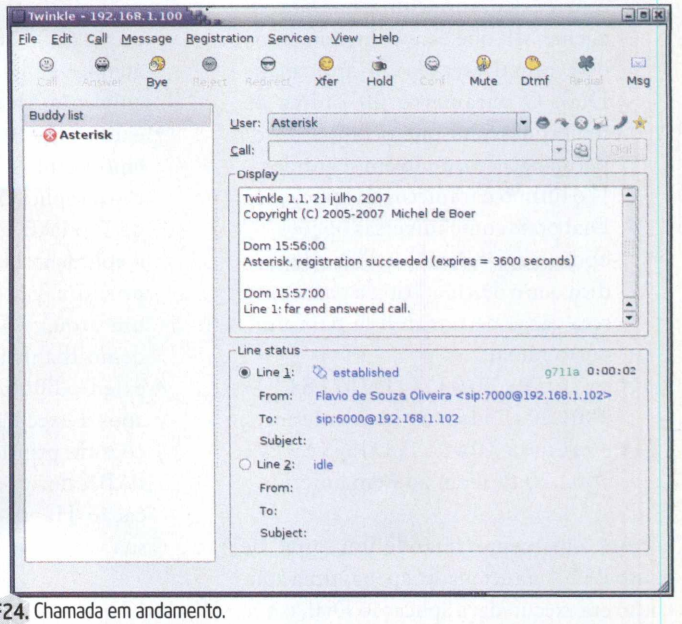
Nas opções de usuário, digite seu nome no campo "Your name", preencha com o ramal o campo "User name" (7000 no nosso caso) e digite o endereço IP do servidor Asterisk no campo "Domain". Na sessão de autenticação, digite asterisk no campo "Realm", o número do ramal no campo "Authentication name" e a senha para ele no campo "Password" (**figura 22**), lembrando que essa senha deve ser a mesma que está configurada no arquivo sip.conf (figura 16).

Nas opções de servidor (SIP Server), indique o endereço IP do servidor Asterisk no campo "Registrar" e pressione o botão "OK". Em seguida você deverá ajustar as opções de sistema, para isso pressione o botão "OK" do novo diálogo. Em nosso caso, apenas assinalamos o profile Asterisk como *default* e alteramos as opções de áudio para que o Twinkle utilize o driver Alsa ao invés de OSS (**figura 23**). Fique atento às opções de áudio caso o Twinkle não funcione para você. Feito isso, pressione o botão OK e pronto!

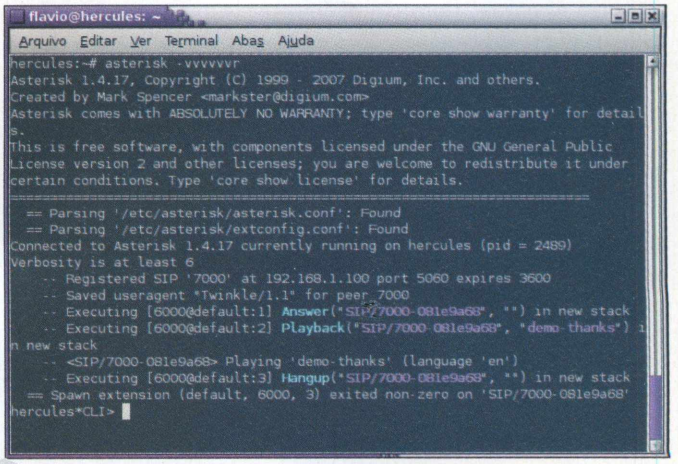
Para testar, utilize um fone ou ligue as caixas de som do PC e disque para o ramal 6000, digitando o número no campo "Call" seguido de "enter". Você deverá então ouvir a reprodução do arquivo demo-thanks que configuramos no plano de discagem (**figura 24**), enquanto na CLI será possível acompanhar o registro do Twinkle e a execução da chamada (**figura 25**).



F23. Demais ajustes no Twinkle.



F24. Chamada em andamento.



F25. CLI provendo acompanhamento da chamada.

Telefone IP

A configuração do telefone IP também é muito simples, principalmente em nosso caso que utilizamos DHCP (Dynamic Host Configuration Protocol). Basta ligá-lo na rede, verificar o endereço IP que foi configurado através do botão Menu (figura 2) e acessar a sua ferramenta de administração via Web. Em nosso caso, o endereço IP configurado no aparelho foi o 192.168.1.101.

Ao apontar o navegador Web para o endereço IP do BudgeTone, ele solicita uma senha de autenticação que por *default* é "admin". Uma vez na tela de administração, preencha os campos SIP Server e Outbound Proxy com o endereço IP do servidor Asterisk, os campos "SIP User" e "IDAuthenticate ID" com o número do ramal desejado (**figura 26**) e o no campo "Authenticate Password" insira a senha que foi configurada para este ramal no arquivo sip.conf.

Outro detalhe se refere à ordem de preferência dos CODECs do aparelho. É interessante colocar o G.711 alaw, que foi adotado como padrão no nosso teste, em primeiro lugar na ordem de preferência do BudgeTone, de modo a evitar que o Asterisk seja obrigado a fazer conversões de formato de áudio durante as chamadas. Para isso, selecione a opção PCMA no campo "*Choice 1*" da sessão "*Preferred Vocoder*" (**figura 26**). Após concluir as configurações, pressione o botão "*Update*" seguido do botão "*Reboot*" no fim da página.

Adaptador ATA

Por estarmos trabalhando com um mesmo fabricante, a configuração do ATA é muito semelhante em relação a do telefone IP. E da mesma forma que o agente anterior, o primeiro passo para a configuração do equipamento é determinar qual endereço IP foi recebido por ele de nosso servidor DHCP. Para isso, aguarde a luz vermelha do HandyTone ficar acesa de forma contínua, retire do gancho o telefone analógico que está conectado ao ATA e pressione asterisco cinco vezes para ouvir o endereço recebido.

De posse do endereço IP, aponte um dos navegadores da rede para ele e autentique-se utilizando a senha *default* (admin). Note que esse equipamento possui duas portas para conexão de telefones analógicos, o que nos dá a possibilidade de configurar dois ramais nele. Em nosso caso configuraremos apenas o ramal 7002 e sua respectiva senha na porta 1 (**figura 27**), lembrando que para o HandyTone também é aconselhável a configuração correta da ordem dos CODECs. Feitos os devidos ajustes, pressione o botão "Update" seguido do botão "Reboot" no fim da página.

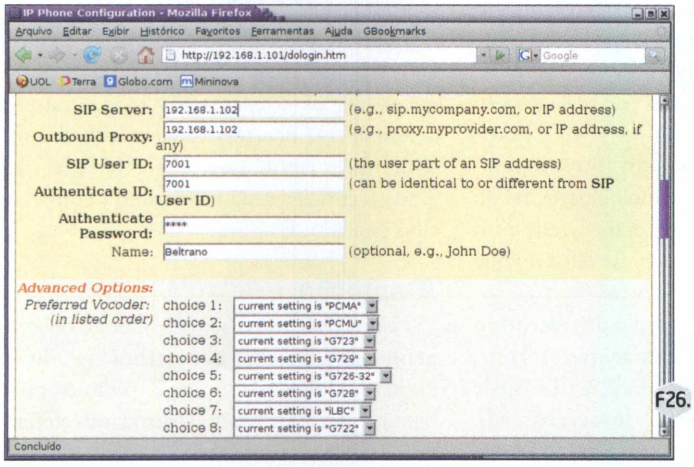
Ao final do boot do equipamento, a luz vermelha deve se apagar, indicando que tudo correu bem. Para comprovar o sucesso, disque para o ramal 6000 e verifique se é possível ouvir a gravação Demo-Thanks. O registro do HandyTone também pode ser acompanhado via CLI.

Com todos os agentes configurados, já é possível efetuar ligações entre os três ramais normalmente. Para finalizar, é possível listar os ramais ativos com o comando sip show peers na CLI (**figura 28**). Já para listar as chamadas em curso, utilize o comando *core show channels* (**figura 29**).

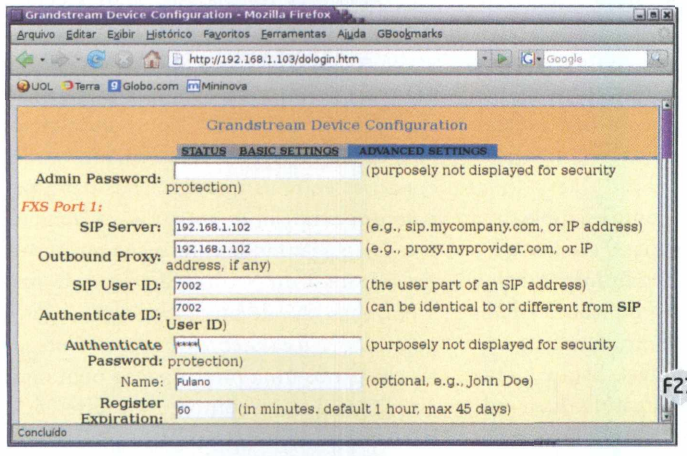
Conclusões

A flexibilidade do Asterisk impressiona, pois ele exerce com maestria a função de PABX, agregando funções e oferecendo possibilidades antes encontradas apenas em equipamentos caríssimos e de grande porte, e tudo isso a custo zero em termos de licença de software. Como dica para maiores informações ficam os sites **www.voip-info.org** e **www.asteriskbrasil.org**.

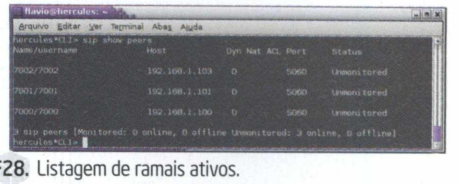
Essa introdução é apenas um aperitivo do que vem por aí. Não perca! **PC**



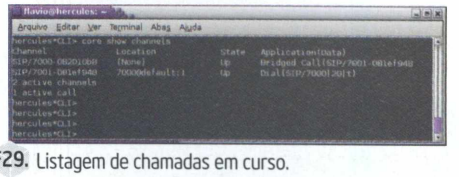
F26. Configurando telefone IP para "falar" com Asterisk.



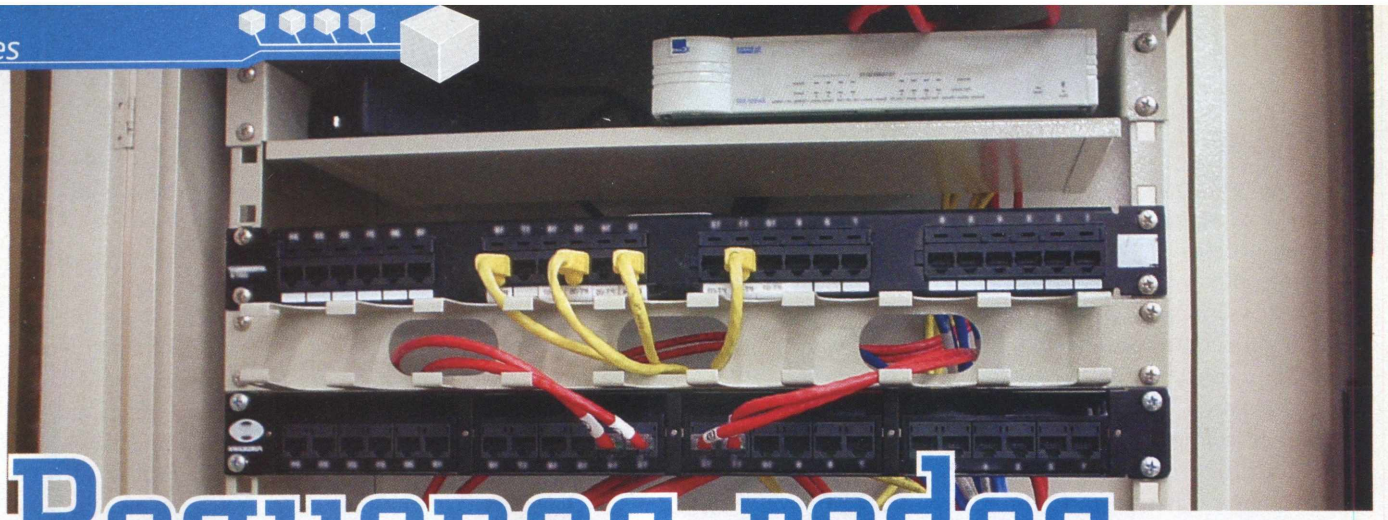
F27. Configuração do Adaptador ATA HandyTone-496.



F28. Listagem de ramais ativos.



F29. Listagem de chamadas em curso.



Pequenas redes profissionais

Tem achado conectores RJ45 Categoria 6 ou 6A à venda no comércio? Difícil, não é mesmo? Então, como fazer uma pequena rede com cabeamento Categoria 6 ou 6A? Saiba neste artigo.

Pequenas redes

Comumente as questões referentes às pequenas redes são: uma pequena rede é uma rede tecnologicamente simples? Insegura? "Vagabunda"? Arcaica? Ou Diminuta?

É possível uma rede com 100 computadores ser mais simples tecnologicamente do que uma com 8? É possível uma rede com 8 computadores ser bem mais veloz do que uma com 100 computadores?

Tomemos como exemplo um escritório de advocacia em cuja rede temos 40 computadores, servidor de email, anti-vírus e seu principal tráfego de dados seja baseado em cópias de arquivos textos e documentos formatados. Nesse caso, uma rede a 100 Mbps já pode suprir a necessidade, mas não é mais indicado. É melhor mesmo que preparemos uma rede totalmente Categoria 6 para que possa funcionar a 1000 Mbps. E vai funcionar muitíssimo bem por bons anos.

Agora vamos tomar como exemplo uma "pequena rede" com apenas 9 computadores. São três em funções administrativas e seis em produção. Que produção?! Vídeos para campanhas publicitárias, artes gráficas, jingles e outras mídias. Esta é a rede de uma agência de propaganda. Essa rede simplesmente não pode mais funcionar a 100 Mbps. Em 1000 Mbps é uma boa melhora, mas por que não em 10Gbps?

Mas aí vem a questão: como fazer o cabeamento dessa rede? Onde se pode encontrar os conectores RJ45? Quando se encontra, é somente para cabos com condutores retorcidos ou flexíveis, e não é possível fazer uma rede inteira com esse tipo de cabo. E agora?

A solução

Como sabemos, quanto maior o desempenho de uma rede com cabos metálicos de pares trançados, maiores serão os problemas que de alguma forma interferem nesse bom desempenho.

Embora as tecnologias mais recentes façam com que os cabos estejam cada vez melhores e suportem freqüências cada vez maiores, são justamente essas freqüências que acabam "causando" alguns problemas. Nos cabos Categoria 5e, as maiores preocupações eram as interferências par-a-par e de um cabo sobre outro; nos Categoria 6 o septo separador com seção em forma de cruz reduziu as interferências de par-a-par, mas não de um cabo sobre o outro adjacente; e finalmente nos cabos Categoria 6A temos uma preocupação bem mais ampla, na qual se combate a interferência par-a-par, mesmo com um septo separa-

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.

dor, e entre cabos adjacentes, apesar de o aumento da bitola de 24 AWG para 23 AWG (quanto maior o índice AWG, menor é a bitola) ajudar no suporte a freqüências mais altas.

Se os pares de condutores dos cabos se mantiverem trançados entre si, os problemas de interferências serão minimizados, mas infelizmente não é possível mantê-los permanentemente trançados entre si ao longo de todo o cabeamento lançado. É necessário realizar um pequeno destrançamento nas conectorizações das tomadas fêmeas e nos plugues RJ45 machos.

É justamente nessa parte que surgem os maiores problemas. Com os condutores destrançados tem-se mais interferências e é justamente dentro dos conectores RJ45 machos que há o maior destrançamento e, conseqüentemente, as maiores interferências.

Cientes disso, os fabricantes de equipamentos passivos acharam por bem desencorajar a crimpagem direta de conectores RJ45 machos, em favor do uso de tomadas fêmeas. Se pensarmos também que um conector RJ45 dos bons não custa mais do que R$ 2,50 e que uma tomada fêmea não fica por menos de R$ 7,50, logo podemos imaginar que os fabricantes estão mesmo é querendo lucrar mais, afinal, uma tomada é três vezes mais cara do que um RJ45. Nas duas extremidades do cabo, teremos então um custo seis vezes maior para as tomadas. Mas espere um momento, "duas tomadas fêmeas não se bicam". Como faremos para ligar uma tomada fêmea da área de trabalho à tomada fêmea de uma placa de rede? Ah, devemos usar um adapter cable.

O adapter cable é utilizado na área de trabalho e é formado por dois conectores RJ45 machos, duas capas de proteção emborrachadas e um trecho de cabo com condutores retorcidos. Além do adapter cable, também há o patch cable (ou patch cord), que é muito similar ao seu "irmão" da área de trabalho, mas tem conectores RJ45 mais compactos e às vezes, sem capa de proteção, mas com boot de proteção (**figura 1**), uma capa termoplástica e não emborrachada. Esses cabos são montados pelos próprios fabricantes, em gabaritos específicos e têm a vantagem de ser totalmente certificados e aprovados tecnicamente, incluindo também a recente certificação por parte da Anatel, através da Resolução 242 de 30 de novembro de 2000 (**www.anatel.gov.br/Portal/documentos/biblioteca/resolucao/2000/res_242_2000.pdf?numeroPublicacao=100346&assuntoPublicacao=Resolu%E7%E3o%20n.%B0%20242&caminhoRel=Cidadao-Biblioteca-Acervo%20Documental**). Todo patch cord e line cord fabricado a partir de 30 de novembro de 2007 deve ser certificado pela Anatel.

Retomando o raciocínio financeiro, a solução de conectorização com tomadas fêmeas e adapter cables pode ficar até 18 vezes mais cara do que a conectorização direta com RJ45.

Quero os RJ45 de volta!

Se você está pensando em um meio para ter seus plugues RJ45 de volta, dê meia volta no seu pensamento. Na realidade, um serviço de cabeamento que utiliza conectorização direta com RJ45 em cabos de condutores sólidos não é considerado profissional. Acaba ficando daqueles que qualquer um pode fazer e isso é muito ruim. Lembre-se de que uma pequena rede não é uma rede vagabunda, é uma rede de pequeno porte, mas importante e tão profissional quanto algumas de maior porte.

Já tentou certificar uma rede com conectorização direta de RJ45 machos? Já tentou conseguir os certificados das garantias estendidas oferecidas pelos fabricantes de cabos, que podem ir a até 25 anos? Se tentou, já é possível presumir que você, amigo leitor, não faz mais rede com conectorização direta de RJ45, mas se ainda não tentou...Nem tente.

É bem verdade que sem a utilização da conectorização direta as redes ficam mais caras e isso é comercialmente ruim. O que vamos usar no lugar dos onipresentes plugues RJ45 macho? Um patch panel?! Não, isso seria um absurdo, que trambolho!

Não é um absurdo. Além de ser o certo a se fazer, não é tão caro e é perfeitamente plausível, além de ficar um serviço muito mais profissional.

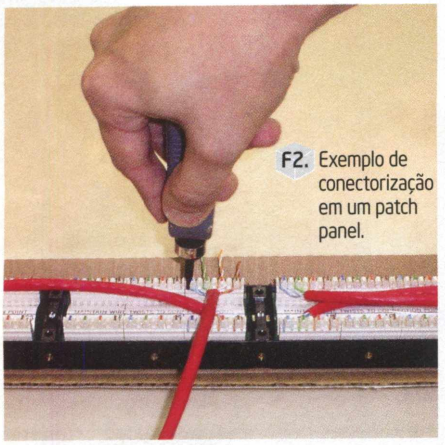
Quando usamos um patch panel, devemos usar também tomadas fêmeas na área de trabalho. Isso traz muitas vantagens. De início, os cabos com condutores sólidos não sofrerão danos mecânicos como antes sofreriam, porque agora eles estarão totalmente protegidos nas estruturas de passagens (eletrodutos, canaletas); os cabos com

F1. Plugue RJ45 de um patch cord com boot termoplástico.

condutores flexíveis (patch cord e adapter cable) serão comprados prontos e já vêm certificados de fábrica, o que garante o melhor desempenho possível. Estes cabos têm uma resistência mecânica muito maior do que os cabos com condutores rígidos, isso vai dispensar aquelas irritantes reconectorizações constantes. Parece somente ruim, mas esses cabos apresentam uma atenuação 20% maior, em média, se comparada aos cabos com condutores sólidos. Isso reduz muito pouco o desempenho, mas é importante para reduzir a potência de inserção do sinal elétrico no meio físico, o que evita danos a alguns equipamentos ativos.

Então teremos que utilizar os cabos com condutores sólidos dentro das estruturas de passagem, as tomadas fêmeas na área de trabalho (como exemplo **www.furukawa.com.br/portal/page?_pageid=393,231171&_dad=portal&_schema=PORTAL**), junto com os adapter cables. Próximo ao switch teremos que usar patch cords e um patch panel?! Não vai querer uma guia de cabos também, ô, patrão?!

Sim, queremos sim. E vamos usar um patch panel, aliás, é justamente este equipamento passivo que será o segredo do sucesso da rede. Como switch, podemos ficar com os modelos SOHO ou desktop totalmente Gigabit Ethernet, tais como o D-Link DGS-1016D (**www.dlinkla.com/home/productos/producto.jsp?idp=669**), um equipamento Gigabit Ethernet de 16 portas, ou o 3Com Office Connect Gigabit Switch 16 (**http://www.3com.com/prod/pt_LA_AMER/detail.jsp?tab=features&sku=3C167160**). Ambos são muito bons. Existem também outros modelos de 8 e até mesmo 5 portas Gigabit Ethernet, mas só são indicados para redes domésticas. Fique com um modelo de 16 portas.



F2. Exemplo de conectorização em um patch panel.

E o patch panel, qual comprar e como trabalhar com ele?

Indicamos três modelos perfeitamente adequados a esse tipo de rede: o Furukawa E220 (**http://www.furukawa.com.br/portal/page?_pageid=393,231139&_dad=portal&_schema=portal**) e os Panduit CWPP-12WBL (**http://www.panduit.com/search/product_details.asp?Ntt=patch+panel&N=5000001+3000096+&Nty=1&Ntx=mode+matchallpartial&id=5001186&recName=CWPP12WBL&Nao=5&Ntk=All**) e CPP-12WBL (**http://www.panduit.com/search/product_details.asp?Ntt=patch+panel&N=5000001+3000096+&Nty=1&Ntx=mode+matchallpartial&id=5001186&recName=CPP12WBL&Nao=5&Ntk=All**). O primeiro modelo apresenta uma característica muito boa para esse porte de equipamento, que é o fato de ser descarregado. Isso significa que se compra um chassi e, de acordo com as necessidades de portas ativas, compram-se mais módulos de tomadas que podem ser de Categoria 5e, 6 ou 6A. É uma excelente idéia que pode levar ao encarecimento do produto, mas nada que o torne economicamente inviável. Todos os três modelos apresentam uma prática guia de cabos por trás do painel de conexão. Essa guia de cabos também é o próprio suporte de parede do equipamento passivo como um todo.

Normalmente a estrutura desses patch panels vem preparada para se aplicar presilhas de PVC para conter os cabos. Veja se consegue usar as sintas velcro no lugar dessas presilhas. As sintas não causam dano algum aos cabos, mas as presilhas de PVC podem introduzir problemas se forem muito apertadas.

Agora vamos aos passos para instalação completa desses patch panels (**figura 2**).

Escolha um bom local para a fixação do suporte do patch panel. Esse suporte também tem a função de guia de cabos e deve ser fixado com buchas e parafusos, normalmente quatro de 5 ou 6 milímetros de diâmetro. Apóie a face frontal do patch panel sobre uma superfície plana para poder preparar a conectorização dos cabos.

Inspecione a extremidade do cabo e veja se ela não apresenta algum tipo de avaria como rasgos da capa de PVC ou uma marca muito acentuada de dobras. Se apresentar, corte o trecho avariado fora e prossiga com a conectorização, tendo o cuidado de limpar muito bem a superfície do cabo com um pano levemente (põe levemente nisso) umedecido em água potável.

Em seguida decape 5,0 cm do cabo. Após isso, afaste os quatro pares de fios condutores, deixando o septo separador central, com seção em forma de cruz, livre para ser cortado. Esse procedimento requer bastante atenção. Primeiro para que qualquer um dos quatro pares não seja demasiadamente dobrado e segundo, para que a capa isolante de nenhum dos condutores seja atingida. Corte agora o septo separador central, bem próximo da capa isolante de PVC.

Separe os quatro pares de forma que eles já fiquem posicionados sobre os suportes onde serão encaixados. Preste muita atenção às etiquetas que definem o padrão de conectorização T568A ou T568B. Destrance somente um trecho estritamente necessário para que os condutores possam ser encaixados em seus respectivos suportes, de forma independente. Procure acomodar bem o condutor até o fim do curso do suporte e tenha muito cuidado para não avariar a capa isolante de algum conector. Depois que os condutores estiverem nos seus respectivos lugares, utilize um alicate com corte transversal bem rente, ou um alicate de cutícula, e corte os trechos excedentes dos condutores o mais rente possível do suporte de plástico.

Agora utilize a ferramenta de inserção, com uma lâmina 110 sem a ponta afiada e realize as oito inserções dos condutores. Em seguida corte os trechos de fios excedentes que costumam ficar para fora das tomadas. Repita este procedimento para todas as tomadas. Se seu patch panel for descarregado, faça a conectorização de todas as tomadas e depois encaixe-as de dentro para fora na face frontal do patch panel.

Vamos então encaixar a tomada no patch panel descarregado. Encaixe a tomada por trás da parte frontal, posicionando primeiro a trava metálica (em baixo) e em seguida inclinando o conjunto da tomada para cima até que se ouça o click sonoro emitido pelo encaixe da trava plástica.

Terminada esta etapa, fixe esta face ao suporte do patch panel que já está preso no anteparo, normalmente uma parede. Se puder colocar uma prateleira ao lado do patch panel para instalar o switch sobre ela, será melhor, assim será possível acompanhar os leds de sinalização das portas e suas atividades.

Seguidos esses passos, suas tomadas já estarão conectorizadas. Não esqueça de conectorizar também as tomadas da área de trabalho, que seguem o mesmo procedimento descrito aqui, e lembre-se de encaixar estas tomadas em um *outlet* ou tomada externa na área de trabalho.

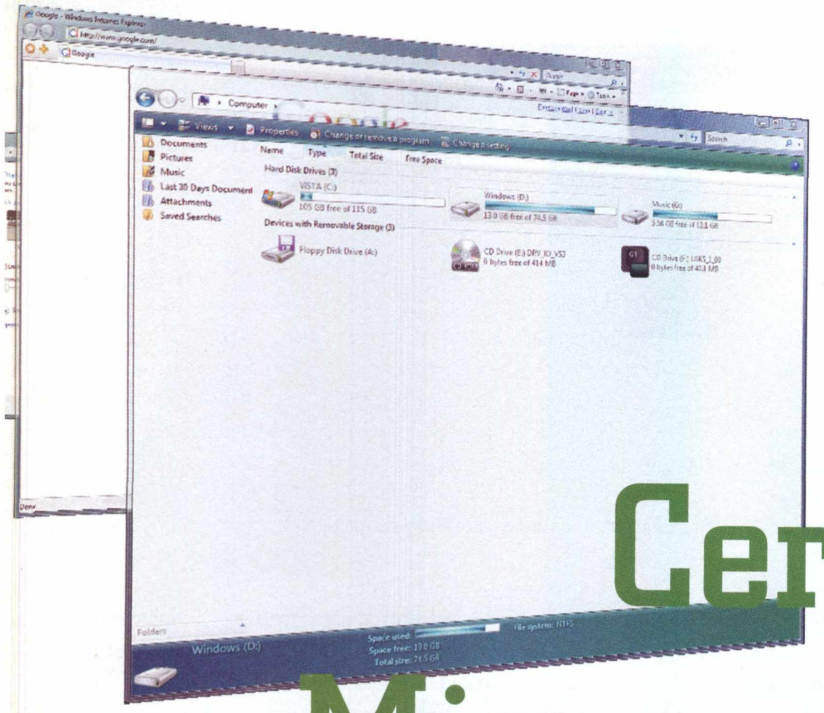
Outra vantagem do patch panel descarregado é que ele também pode ser compatível com os cabos blindados FTP e suas tomadas apropriadas.

Conclusão

Como vimos, não é difícil fazer uma rede de pequeno porte com cabos Categoria 6 e 6A. Se todos procedermos como descrito aqui, não enfrentaremos problemas técnicos e nossas redes durarão muito mais tempo. Em caso de danos aos cabos, somente os adapter cables precisarão ser substituídos, pois são eles que ficam expostos ao ambiente. Vale lembrar que todos os componentes envolvidos devem ser da mesma Categoria, pois a rede estará sempre nivelada pelo componente cuja Categoria seja a mais inferior. Nem pense em economizar nas tomadas ou nos patch cords, por exemplo.

Um serviço realizado conforme descrito aqui só trará vantagens, tanto ao contratante quanto ao contratado, que se diferenciará daqueles prestadores de serviço "meia sola" existentes por aí.

Por fim, o contratante pagará mais por uma rede bem melhor. E por falar em pagar, você, como prestador de serviço, também receberá mais por uma rede de pequeno porte, mas de alto desempenho e organização. Não esqueça de identificar os cabos e tomadas. Até a próxima. **PC**



Certificação Microsoft MCTS

PARTE 9

Igor Humberto e
Paulo Sant'anna

Se há pouco tempo não era possível pensar na compra de um notebook por um valor inferior a R$ 3 mil, o aumento da concorrência entre os fabricantes e a valorização do real frente ao dólar criou um cenário muito favorável para a massificação dos portáteis no Brasil. De fato, hoje já é possível encontrar muitos modelos cujos preços giram em torno de R$ 1,5 mil.

Por esta também ser uma realidade mundial, os novos sistemas operacionais devem ser capazes de acompanhar esta tendência e, assim, dispor de uma série de opções que visa a melhorar a experiência do usuário no uso da plataforma de dispositivos móveis. Como profissional MCTS, você deverá demonstrar domínio sobre elas e ser capaz de auxiliar o usuário durante a configuração.

Tipos de computadores móveis

Antes de falarmos sobre as opções de configuração disponíveis no Windows Vista, vamos nos familiarizar com alguns termos comuns a esta categoria de dispositivos:

- **Laptops e Notebooks:** ambos os termos podem ser usados de maneira intercambiável para um computador portátil;
- **Tablet PC:** Similar ao notebook, a diferença a favor do Tablet PC está na tela, a qual é sensível ao toque de um tipo de caneta especial, parecida com aquelas que usamos em um Palm. Vale ressaltar que a referida tela não funciona como uma tela *Touch Screen*. É possível fazer o arrastar e soltar de objetos, escrever (desde que o editor de textos trabalhe com o reconhecimento de escrita), selecionar, mas tudo isso deve ser feito através da tal caneta especial;
- **Computadores Ultra portáteis:** Conhecidos no exterior pela sigla UMPC (Ultra-Mobile PC), esses são os famosos computadores de mão, ou seja, uma daquelas pequenas maravilhas tecnológicas que suporta praticamente tudo o que é realizado em um computador comum. Normalmente são sistemas que possuem conectividade através de redes Bluetooth ou Wi-Fi.

Onde fazer os ajustes?

A fim de aproveitarmos ao máximo o potencial dos equipamentos portáteis, é necessário que o sistema operacional seja

capaz de gerenciar adequadamente os seus recursos. O Windows Vista possibilita isso através dos seguintes elementos presentes no Painel de controle:

Gerenciamento de energia (Opções de energia)

Através dele podemos definir esquemas de energia que permitem ao usuário planejar de forma mais adequada a utilização do dispositivo. Imagine o caso de um usuário que, longe de uma ligação com a rede elétrica, pode utilizar um esquema de energia que privilegie a autonomia de suas baterias. Normalmente os notebooks são acompanhados por uma suíte de aplicativos que desempenham esta tarefa. Dependendo do fabricante do produto, você encontrará muitas funcionalidades interessantes.

Central de mobilidade

É aqui que o Windows Vista concentra a maioria das configurações relacionadas a este tema. Controle de brilho de tela, ajuste de volume, planos de energia e status de sincronização, por exemplo, estão entre as opções suportadas.

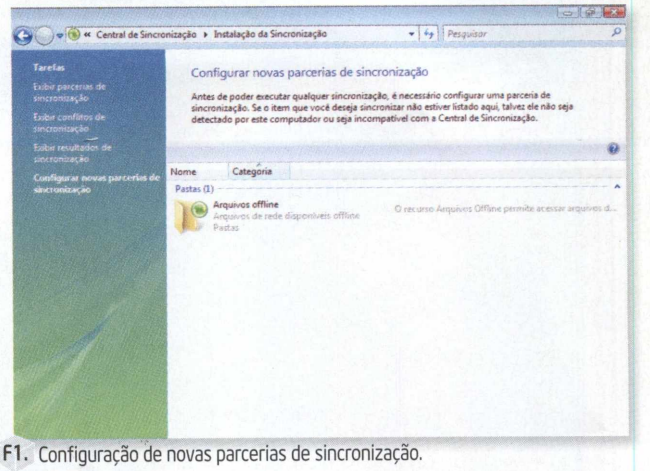
Central de sincronização

Um lugar único para controlar a sincronização de informações entre computadores (estações e servidores, por exemplo) e dispositivos que você conecta ao seu computador, tais como PDAs, telefones celulares e MP3 players.

Com esta ferramenta, fica mais fácil gerenciar o processo de sincronização entre os dispositivos citados anteriormente, apesar do método de sincronização usado em cada um não ser exatamente igual. É importante ressaltar que este processo pode ser executado manualmente, ou então você pode configurar um parceiro de sincronização de forma que uma espécie de agendamento de sincronização possa ser feito. Determinados arquivos poderiam ser copiados automaticamente para um pen drive conectado ao computador, quando este evento ocorrer.

Práticas recomendadas para computadores móveis

Como o próprio nome já diz, um computador móvel é um sistema portátil que, por assim ser, pode ser levado para fora do escritório. O problema é que no mundo externo este dispositivo estará suscetível a diversos tipos de ataques, inclusive roubos e furtos. Neste caso, como garantir que o atacante não acessará nenhuma informação confidencial? No Windows Vista, uma das várias maneiras de alcançar este objetivo seria configurando o Bitlocker, um recurso apresentado na PC&CIA 67 e que serve para criptografar toda a área de dados do disco, de forma a impossibilitar acessos não autorizados aos dados.



F1. Configuração de novas parcerias de sincronização.

Além de saber proteger adequadamente os dados que serão transportados, é importante garantir que o computador estará levando as últimas versões dos arquivos que se encontram na rede (arquivos off-line). Isso pode ser feito com a configuração de um parceiro de sincronização.

Para executar esta tarefa, é necessário que o profissional de TI possua um conhecimento prévio sobre os padrões e o funcionamento de tecnologias existentes em dispositivos, tais como PDAs, SmartPhones, Mídia Players, dispositivos Bluetooth etc. Como hoje em dia é comum conectar o telefone celular ao PC usando estas tecnologias, não iremos entrar em mais detalhes sobre as mesmas. Mas lembre-se de que é fundamental conhecer padrões de funcionamento da tecnologia Bluetooth, por exemplo, para saber como aproveitar o recurso de pareamento entre dois dispositivos quaisquer.

A fim de configurar a sincronização dos arquivos existentes, por exemplo, em uma câmera digital, basta conectá-la ao computador através do cabo USB e aguardar alguns segundos. Normalmente o próprio Windows fornecerá os drivers necessários para que o dispositivo funcione adequadamente, mas pode ser necessário se conectar ao site Windows Update, ou então ao site do fabricante (melhor opção), ou ainda usar o CD que normalmente acompanha o dispositivo para fornecer estes drivers.

Feito isso, clique em Configurar novas parcerias de duplicação dentro da Central de sincronização (**figura 1**). Selecione os arquivos que deseja transferir para o seu sistema, e clique em Iniciar a sincronização.

Vale ressaltar que essa tarefa já podia ser executada no Windows XP. A diferença é que agora existe um local específico para a execução dessa sincronização.

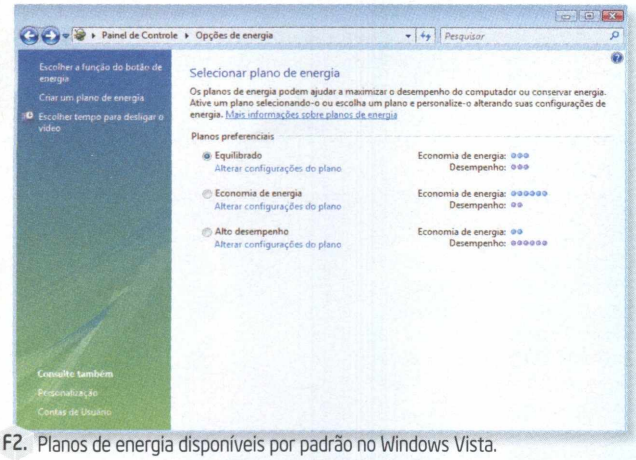
Configurando as opções de energia

São muitas as opções que podem ser ajustadas para otimizar o uso de um notebook, principalmente no que diz respeito à autonomia da bateria. É o caso, por exemplo, da freqüência de clock do processador e da intensidade de brilho do monitor, que se diminuídos podem ocasionar uma grande redução no consumo de energia.

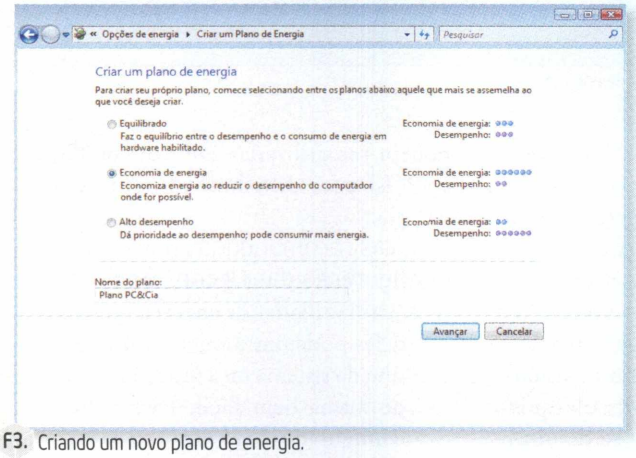
O que deve ficar claro é que, via de regra, a performance do equipamento é proporcional à utilização de energia. Ou seja, quando o processador é muito exigido, maior será o gasto de energia e menor o tempo de vida da bateria. Tanto a AMD quanto a Intel possuem mecanismos em seus processadores para controlar dinamicamente, no próprio hardware, a tensão e a freqüência de operação, tais como o PowerNow! e o SpeedStep, respectivamente.

Planos de energia

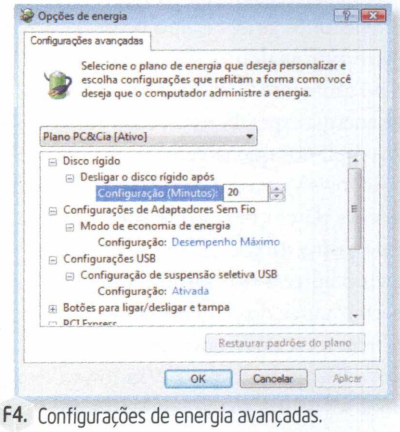
Chamados de Esquemas de energia em versões anteriores do Windows, os Planos de energia auxiliam na otimização do computador portátil e da bateria, modificando uma série de configurações no sistema de acordo com o cenário de uso do equipamento. Por padrão, o Windows Vista suporta três planos de energia que



F2. Planos de energia disponíveis por padrão no Windows Vista.



F3. Criando um novo plano de energia.



F4. Configurações de energia avançadas.

atendem às necessidades da maioria das ocasiões. São eles:

- Equilibrado (*Balanced*): Como o próprio nome diz, este plano equilibra o consumo de energia e a performance do sistema conforme a demanda dos programas do usuário. Essa é a opção padrão;
- Economia de energia (*Power saver*): Economiza energia ao reduzir a performance do sistema. Deve ser usado diante da necessidade de otimização máxima da autonomia da bateria;
- Alto desempenho (*High performance*): É o contrário da opção anterior, normalmente configurado quando o equipamento está ligado na rede elétrica (**figura 2**).

Acesse as Opções de energia através do Painel de controle ou execute o comando control powercfg.cpl. Os planos de energia padrão do Windows podem ser alterados e customizados clicando na opção Alterar configurações do plano, embaixo de cada um deles. Podem ser criados também planos de energia adicionais, customizados de acordo com alguma necessidade específica. Aliás, alguns fabricantes de computadores podem disponibilizar ainda planos de energia adicionais que determinem algum tipo de configuração ou característica especial com relação ao controle de energia.

É possível também excluir os planos de energia, com exceção dos que já vêm por padrão em uma instalação do Windows Vista. Além disso, vale ressaltar a impossibilidade de se excluir um plano criado, mas que esteja ativo no momento.

Criando um novo Plano de energia

Em Opções de energia, clique em Criar um plano de energia, depois selecione qual plano, dentre os fornecidos por padrão, mais se assemelha ao que será criado. Repare que ao lado de cada plano são listados dois itens, Economia de energia e Desempenho, onde são exibidas de forma bem intuitiva e colorida os indicadores de energia e desempenho referente a cada plano. Defina o nome do novo plano no campo Nome do plano e clique em Avançar (**figura 3**).

Em alterar configurações do plano, defina o tempo de inatividade após o qual o vídeo será desligado. Depois clique em Criar.

Se a criação do novo plano ocorreu com sucesso, o mesmo já será exibido em Selecionar plano de energia. Podemos definir várias outras configurações para o plano, para isso clique em Alterar configurações do plano e depois em Alterar configurações de energia avançadas. Agora podem ser especificados valores de acordo com a necessidade da ocasião, como, por exemplo, o tempo de Desligamento do Disco rígido, Modo de economia de energia em Adaptadores sem fio e Gerenciamento de energia do processador, onde podem ser definidas as porcentagens do Estado de desempenho mínimo e máximo (**figura 4**).

Opções de desligamento

Outro ponto importante e que deve ser considerado diz respeito às definições para ligar e desligar o computador. Existem 3 formas:

Definindo a função do botão de energia

O Windows Vista também nos permite definir a ação que será tomada quando o botão de energia do equipamento for pressionado ou a tampa do notebook for fechada. As configurações podem ser feitas de acordo com o perfil de uso do equipamento no momento, se alimentado pela bateria ou pela rede elétrica. As opções de desligamento são: Nada a fazer, Dormir, Hibernação e Desligar.

Proteção de senha ao retornar do estado Dormir ou Hibernação

Outro recurso interessante é forçar a realização de um novo login quando o computador retorna do estado Dormir ou Hibernação. Imagine a situação de você ir

Tipo	Armazenamento de dados	Requisitos de energia
Desligar (Shutdown)	Todos os dados são salvos no disco, todas as aplicações são encerradas, o arquivo de paginação é limpo, a atividade do usuário é encerrada e o computador é desligado.	Não necessita.
Hibernação (Hibernate)	O estado do sistema é salvo em disco (no arquivo oculto hiberfil.sys, que possui o mesmo tamanho da memória RAM física do computador), assim como o conteúdo existente na RAM; o computador é desligado; são necessários drivers do fabricante do computador para utilizar a hibernação em nível de sistema operacional no Windows Vista.	Não necessita, pois os dados estão armazenados no HD.
Dormir (Sleep)	O estado do sistema é salvo em memória; se ocorrer alguma falha de energia, os dados serão perdidos.	Consome uma pequena quantidade de energia, pois o equipamento não é desligado.

T1. Estado do computador x requisitos de energia.

almoçar e fechar a tampa do notebook, depois de tê-lo configurado para hibernar automaticamente quando detectasse essa condição. Pois bem, caso não tenha sido configurada a política que exige uma senha para retornar o equipamento do estado de hibernação, basta alguém ligar o notebook para obter acesso à sua sessão de usuário, com seus programas, emails e arquivos disponíveis. Portanto, trata-se de um recurso indispensável sob o ponto de vista de segurança da informação e que, como tal, já vem habilitado por padrão.

No entanto, podemos desabilitar essa configuração em todos os planos de energia existentes no equipamento. Para isso, acesse as Opções de energia no Painel de Controle. Em Selecionar plano de energia, clique em Exigir uma senha ao ativar. Em Definir botões de energia e ativar proteção por senha, clique em Não exigir senha e depois em Salvar alterações.

Para desabilitá-la em apenas um Plano de energia específico, vá até Selecionar plano de energia e clique em Alterar configurações do plano, no plano em que será feita a configuração. Em Alterar configurações do plano, clique em Alterar configurações de energia avançadas. Em Configurações avançadas, clique em Configurações adicionais, depois em Exigir uma senha ao ativar e defina como Não, independente do equipamento estar conectado na tomada ou na bateria. Para finalizar a configuração, clique em OK.

Para facilitar a configuração em um ambiente de rede com Active Directory, podem ser utilizadas Políticas de Grupo (GPOs) para distribuir as definições de energia.

Práticas recomendadas para Configuração das Opções de Energia

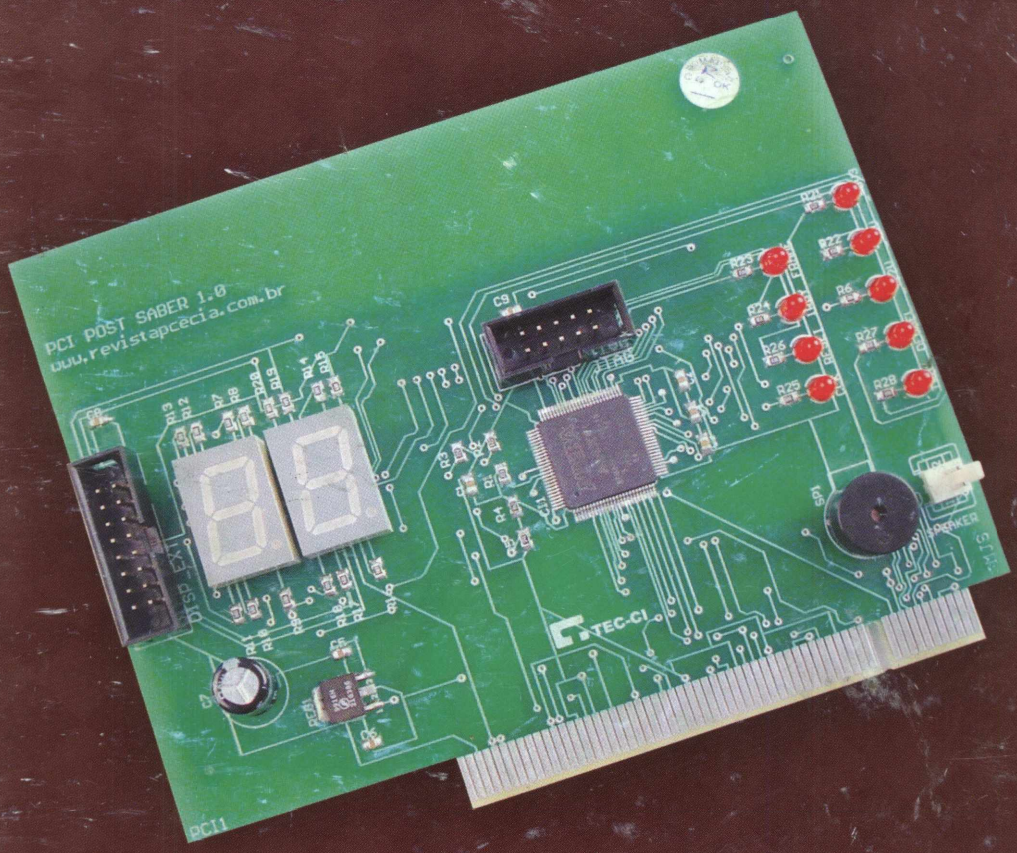
1. Utilize Planos de energia, pois através deles podemos aumentar o desempenho do sistema ou a duração da bateria de forma bem fácil. Para facilitar a configuração em um ambiente de rede com Active Directory, podem ser utilizadas Políticas de Grupo (GPOs) para distribuir as definições de energia;
2. No ambiente corporativo, crie Planos de energia específicos ou customize um dos 3 planos que já vem por padrão no Windows Vista, de acordo com as necessidades da empresa onde você trabalha e de forma que seja feito um balanceamento entre a utilização da bateria e a performance dos equipamentos;
3. Procure conscientizar os usuários demonstrando como o Windows Vista pode ser utilizado para reduzir o consumo de energia e otimizar a performance do equipamento de acordo com a sua necessidade e cenário existente.

Conclusão

Estamos quase finalizando a nossa série de preparação para o exame 70-620 e nesta penúltima parte aprendemos mais sobre dispositivos móveis e sua utilização no Windows Vista, bem como as configurações de energia que podem sem personalizadas de acordo com o equipamento e cenário de utilização. **PC**

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

PC &CIA



POST SABER

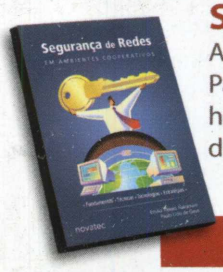
A 1ª DESENVOLVIDA NO BRASIL E COM SUPORTE LOCAL

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

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

LITERATURA TÉCNICA

Que não pode faltar em sua biblioteca

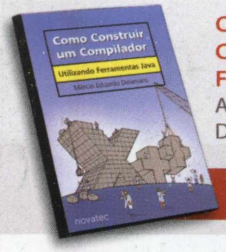


Segurança de Redes em Ambientes Cooperativos

A segurança da informação possui influência cada vez maior no sucesso dos negócios. Para aplicar a melhor estratégia de defesa, é preciso conhecer os principais riscos e ataques realizados por hackers, além de entender os principais conceitos de segurança e tecnologias, mecanismos e protocolos disponíveis para a proteção.

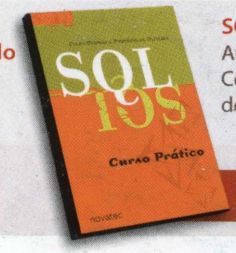
R$ 81,00

LANÇAMENTO



Como Construir um Compilador Utilizando Ferramentas Java
Autor: Márcio Eduardo Delamaro

R$ 69,00

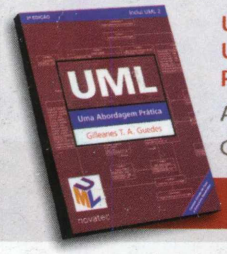


SQL - Curso Prático
Autor:
Celso Henrique Poderoso de Oliveira

R$ 42,00

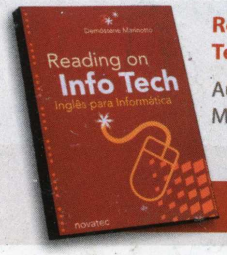
Java Guia do Programador
Autor: Peter Jandl Junior

R$ 119,00



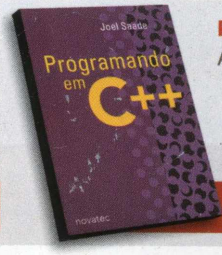
UML - Uma Abordagem Prática
Autor: Gilleanes T. A. Guedes

R$ 69,00



Reading on Info Tech – 2ª edição
Autor: Demóstene Marinotto

R$ 39,00

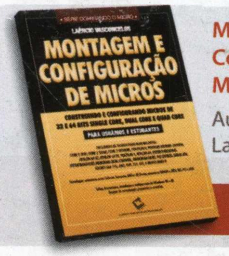


Programando em C++
Autor: Joel Saade

R$ 79,00

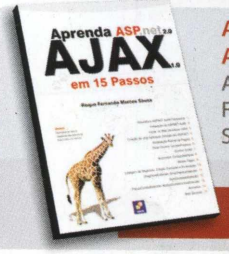
Manutenção de micros na prática
Autor: Laércio Vasconcelos

R$ 99,00



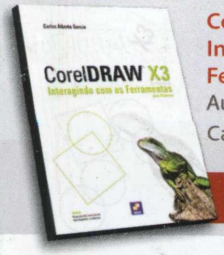
Montagem e Configuração de Micros
Autor:
Laércio Vasconcelos

R$ 39,00



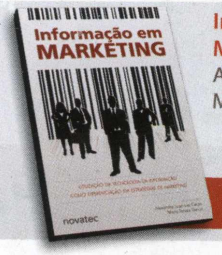
Aprenda ASP.NET AJAX em 15 Passos
Autor: Roque Fernando Marcos Sousa

R$ 53,10



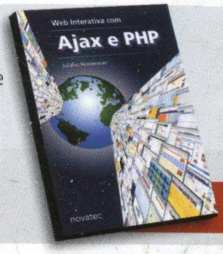
CorelDRAW X3 - Interagindo com as Ferramentas
Autor:
Carlos Alberto Garcia

R$ 74,70



Informação em Marketing
Autor: Alexandre Luzzi e Maria Tereza Garcia

R$ 63,00



Web Interativa com Ajax e PHP
Autor: Juliano Niederauer

R$ 62,00

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

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